



Cisco Secure Web Appliance 向け AsyncOS 15.5 ユーザーガイド (一般導入)

最終更新：2026 年 1 月 6 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

はじめに 1

Secure Web Appliance について 1

AsyncOS 15.5 の新機能 2

関連項目 4

アプライアンス Web インターフェイスの使用 4

Web インターフェイスのブラウザ要件 4

仮想アプライアンスでの Web インターフェイスへのアクセスのイネーブル化 6

アプライアンス Web インターフェイスへのアクセス 6

Web インターフェイスでの変更内容のコミット 8

Web インターフェイスでの変更内容のクリア 8

サポートされている言語 8

Cisco SensorBase ネットワーク 9

SensorBase の利点とプライバシー 9

Cisco SensorBase ネットワークへの参加の有効化 9

第 2 章

接続、インストール、設定 11

接続、インストール、設定の概要 11

操作モードの比較 12

タスクの概要：接続、インストール、設定 18

アプライアンスの接続 18

設定情報の収集 22

システム セットアップ ウィザード 24

システム セットアップ ウィザードの参照情報 26

ネットワーク/システムの設定 26

ネットワーク/ネットワーク コンテキスト	28
ネットワーク/クラウド コネクタの設定	28
ネットワーク/ネットワーク インターフェイスおよび配線	29
ネットワーク/レイヤ 4 トラフィック モニターの配線	30
管理およびデータ トラフィックのネットワーク/ルートの設定	30
ネットワーク/透過的接続の設定	30
ネットワーク/管理の設定	31
セキュリティ/セキュリティ設定	32
アップストリーム プロキシ	33
アップストリーム プロキシのタスクの概要	33
アップストリーム プロキシのプロキシ グループの作成	34
ネットワーク インターフェイス	35
IP アドレスのバージョン	36
ネットワーク インターフェイスのイネーブル化または変更	37
ネットワーク インターフェイス カードの設定	40
イーサネット インターフェイスのメディア設定	40
ネットワーク インターフェイス カードのペアリングおよびチーミング	41
etherconfig コマンドを使った NIC ペアリングのイネーブル化	42
NIC ペアリングを設定するためのガイドライン	48
ハイ アベイラビリティを実現するためのフェールオーバー グループの設定	50
フェールオーバー グループの追加	52
高可用性グローバル設定の編集	53
フェールオーバー グループのステータスの表示	53
Web プロキシ データに対する P2 データ インターフェイスの使用	54
TCP/IP トラフィック ルートの設定	55
発信サービス トラフィック	56
デフォルト ルートの変更	56
ルートの追加	57
ルーティング テーブルの保存およびロード	57
ルートの削除	58
トランスペアレント リダイレクションの設定	58

透過リダイレクション デバイスの指定	58
L4 スイッチの使用	59
WCCP サービスの設定	60
VLAN の使用によるインターフェイス能力の向上	66
VSAN の設定と管理	66
リダイレクト ホスト名とシステム ホスト名	69
リダイレクト ホスト名の変更	69
システム ホスト名の変更	69
SMTP リレー ホストの設定	70
SMTP リレー ホストの設定	70
DNS の設定	71
セキュア DNS の注意事項と制約事項	71
スプリット DNS	72
DNS キャッシュのクリア	72
DNS 設定の編集	72
接続、インストール、設定に関するトラブルシューティング	74

第 3 章

認証および承認	75
エンドユーザー クレデンシャルの取得の概要	75
認証タスクの概要	76
認証に関するベスト プラクティス	76
認証の計画	77
Active Directory/Kerberos	78
Active Directory/基本	79
Active Directory/NTLMSSP	80
LDAP/基本	81
ユーザーの透過的識別	81
透過的ユーザー識別について	82
透過的ユーザー識別のルールとガイドライン	85
透過的ユーザー識別の設定	86
CLI を使用した透過的ユーザー識別の詳細設定	86

シングルサインオンの設定	87
ハイ アベイラビリティ展開で Kerberos 認証を行うための Windows Active Directory におけるサービス アカウントの作成	88
認証レルム	90
外部認証	91
LDAP サーバーによる外部認証の設定	91
RADIUS 外部認証のイネーブル化	92
Kerberos 認証方式の Active Directory レルムの作成	92
Active Directory 認証レルムの作成 (NTLMSSP および基本)	97
Active Directory 認証レルムの作成の前提条件 (NTLMSSP および基本)	97
複数の NTLM レルムとドメインの使用について	98
Active Directory 認証レルムの作成 (NTLMSSP および基本)	98
LDAP 認証レルムの作成	100
複数の NTLM レルムとドメインの使用	107
認証レルムの削除について	107
グローバル認証の設定	108
認証シーケンス	117
認証シーケンスについて	117
認証シーケンスの作成	118
認証シーケンスの編集および順序変更	119
認証シーケンスの削除	119
認証の失敗	119
認証の失敗について	120
問題のあるユーザー エージェントの認証のバイパス	120
認証のバイパス	122
認証サービスが使用できない場合の未認証トラフィックの許可	122
認証失敗後のゲスト アクセスの許可	123
ゲスト アクセスをサポートする識別プロファイルの定義	123
ゲスト アクセスをサポートしている識別プロファイルのポリシーでの使用	124
ゲスト ユーザーの詳細の記録方法の設定	124
認証の失敗：異なるクレデンシャルによる再認証の許可	125

異なるクレデンシャルによる再認証の許可について	125
異なるクレデンシャルによる再認証の許可	125
識別済みユーザーの追跡	125
明示的要求でサポートされる認証サロゲート	126
透過的要求でサポートされる認証サロゲート	126
再認証ユーザーの追跡	127
資格情報	127
セッション中のクレデンシャルの再利用の追跡	128
認証および承認の失敗	128
クレデンシャルの形式	128
基本認証のクレデンシャルの暗号化	129
基本認証のクレデンシャルの暗号化について	129
クレデンシャル暗号化の設定	129
認証に関するトラブルシューティング	130

第 4 章

システム設定 131

システム管理タスクの実行	131
システム管理の概要	132
アプライアンス設定の保存、ロード、およびリセット	132
アプライアンス設定の表示と印刷	132
アプライアンス設定ファイルの保存	133
アプライアンス設定ファイルのロード	134
アプライアンス設定の出荷時デフォルトへのリセット	135
設定ファイルのバックアップの保存	135
Cisco Secure Web Appliance ライセンス	136
スマートソフトウェア ライセンシング	136
仮想アプライアンスのライセンス	169
仮想アプライアンスのライセンスのインストール	170
リモート電源再投入の有効化	170
ユーザー アカウントの管理	171
ローカル ユーザー アカウントの管理	172

RADIUS ユーザー認証	175
ユーザー プリファレンスの定義	178
管理者の設定	178
管理ユーザーのパスワード要件の設定	178
アプライアンスの割り当てに対するセキュリティ設定の追加	179
ユーザー ネットワーク アクセス	181
管理者パスワードのリセット	182
生成されたメッセージの返信アドレスの設定	182
アラートの管理	183
アラートの分類と重大度	183
アラート受信者の管理	184
アラート設定値の設定	184
アラート リスト	185
FIPS Compliance	194
FIPS 証明書の要件	194
FIPS 証明書の検証	195
FIPS モードの有効化または無効化	195
システムの日時の管理	196
タイム ゾーンの設定	196
NTP サーバーによるシステム クロックの同期	197
SSL の設定	197
証明書の管理	200
厳格な証明書検証について	200
証明書およびキーについて	201
信頼できるルート証明書の管理	201
証明書の更新	202
ブロックされた証明書の表示	202
証明書とキーのアップロードまたは生成	203
AsyncOS for Web のアップグレードとアップデート	206
AsyncOS for Web をアップグレードするためのベスト プラクティス	206

AsyncOS およびセキュリティ サービス コンポーネントのアップグレードとアップデート	206
自動および手動によるアップデート/アップグレードのクエリー	209
ローカルおよびリモート アップデート サーバ	210
アップグレードおよびサービス アップデートの設定	214
以前のバージョンの AsyncOS for Web への復元	215
仮想アプライアンスの AsyncOS を復元した場合のライセンスへの影響	215
復元プロセスでのコンフィギュレーションファイルの使用	215
SMA によって管理されるアプライアンスの AsyncOS の復元	215
以前のバージョンへの Web 用の AsyncOS の復元	216
SNMP を使用したシステムの状態のモニタリング	217
MIB ファイル	218
SNMP モニタリングのイネーブル化と設定	219
ハードウェア オブジェクト	219
SNMP トラップ	219
CLI の例 : snmpconfig	220
Web トラフィック タップ (Web Traffic Tap)	220
Web トラフィック タップの有効化	222
Web トラフィック タップ ポリシーの設定	223
HTTP 2.0 プロトコルの設定	224
Cisco クラウド Web セキュリティ プロキシへのアプライアンスの接続	225
クラウド コネクタ モードで機能を設定および使用する方法	225
クラウド コネクタ モードでの展開	226
クラウド コネクタの設定	226
クラウドのディレクトリ グループの使用による Web アクセスの制御	230
クラウド プロキシ サーバーのバイパス	230
クラウド コネクタ モードでの FTP および HTTPS の部分的サポート	231
セキュア データの漏洩防止	231
グループ名、ユーザー名、IP アドレスの表示	232
クラウド コネクタ ログへの登録	232
クラウド Web セキュリティ コネクタの使用による識別プロファイルと認証	232

ポリシーの適用に対するマシンの識別	233
未認証ユーザーのゲスト アクセス	234
Web 要求の代行受信	234
Web 要求の代行受信の概要	234
Web 要求の代行受信のためのタスク	235
Web 要求の代行受信のベスト プラクティス	236
Web 要求を代行受信するための Web プロキシ オプション	236
Web プロキシの設定	237
Web プロキシ キャッシュ	241
Web プロキシの IP スプーフィング	244
Web プロキシのカスタム ヘッダー	246
Web プロキシのバイパス	247
ポリシーごとの Web プロキシ カスタム ヘッダー	249
Web プロキシ使用規約	252
ドメイン マップ	252
特定アプリケーションのドメインマップ	252
Web 要求をリダイレクトするためのクライアント オプション	254
クライアント アプリケーションによる PAC ファイルの使用	255
プロキシ自動設定 (PAC) ファイルのパブリッシュ オプション	255
プロキシ自動設定 (PAC) ファイルを検索するクライアント オプション	255
Secure Web Applianceでの PAC ファイルのホスト	256
クライアント アプリケーションでの PAC ファイルの指定	257
FTP プロキシ サービス	258
FTP プロキシ サービスの概要	259
FTP プロキシの有効化と設定	259
SOCKS プロキシ サービス	261
SOCKS プロキシ サービスの概要	261
SOCKS トラフィックの処理のイネーブル化	262
SOCKS プロキシの設定	262
SOCKS ポリシーの作成	263
要求の代替受信に関するトラブルシューティング	264

第 5 章

アクセス制御 265

ポリシーの適用に対するエンドユーザーの分類	265
ユーザーおよびクライアント ソフトウェアの分類：概要	265
ユーザーおよびクライアント ソフトウェアの分類：ベスト プラクティス	266
識別プロファイルの条件	267
ユーザーおよびクライアント ソフトウェアの分類	267
ID の有効化/無効化	277
識別プロファイルと認証	277
識別プロファイルのトラブルシューティング	279
識別プロファイルでのサロゲートタイプのトラブルシューティング	280
ポリシーの適用に対する URL の分類	280
URL トランザクションの分類の概要	280
失敗した URL トランザクションの分類	281
未分類の URL	282
URL と URL カテゴリの照合	283
未分類の URL と誤って分類された URL の報告	283
URL カテゴリ データベース	284
URL フィルタリング エンジンの設定	284
URL カテゴリ セットの更新の管理	285
URL カテゴリ セットの更新による影響について	285
マージされたカテゴリ：例	290
URL カテゴリ セットの更新の制御	291
新規および変更されたカテゴリのデフォルト設定	292
カテゴリおよびポリシーの変更に関するアラートの受信	293
URL カテゴリ セットの更新に関するアラートへの応答	293
URL カテゴリによるトランザクションのフィルタリング	293
アクセス ポリシー グループの URL フィルタの設定	294
復号ポリシー グループの URL フィルタの設定	298
データ セキュリティ ポリシー グループの URL フィルタの設定	299
YouTube の分類	301

YouTube 分類機能の有効化	303
カスタム URL カテゴリの作成および編集	305
カスタムおよび外部 URL カテゴリのアドレス形式とフィードファイル形式	312
アダルト コンテンツのフィルタリング	314
セーフサーチおよびサイト コンテンツ レーティングの適用	315
アダルト コンテンツ アクセスのロギング	316
アクセス ポリシーでのトラフィックのリダイレクト	317
ロギングとレポート	318
ユーザーへの警告と続行の許可	318
[エンドユーザー フィルタリング警告 (End-User Filtering Warning)] ページの設定	318
時間ベースの URL フィルタの作成	319
URL フィルタリング アクティビティの表示	320
フィルタリングされない未分類のデータについて	320
アクセス ログへの URL カテゴリの記録	320
正規表現	321
正規表現の形成	321
検証エラーを回避するための注意事項	322
正規表現の文字テーブル	323
URL カテゴリについて	325
HTTPS トラフィックを制御する復号ポリシーの作成	343
HTTPS トラフィックを制御する復号ポリシーの作成：概要	344
復号ポリシー タスクによる HTTPS トラフィックの管理の概要	344
復号ポリシーによる HTTPS トラフィックの管理：ベストプラクティス	345
復号ポリシー	345
HTTPS プロキシのイネーブル化	348
HTTPS トラフィックの制御	350
復号オプションの設定	352
認証および HTTPS 接続	353
ルート証明書	353
証明書の検証と HTTPS の復号の管理	355
ルート証明書およびキーのアップロード	356

HTTPS プロキシ用の証明書およびキーの生成	356
無効な証明書の処理の設定	357
信頼できるルート証明書	360
HTTPS トラフィックのルーティング	361
暗号化/HTTPS/証明書のトラブルシューティング	362
インターネット要求を制御するポリシーの作成	362
ポリシーの概要：代行受信されたインターネット要求の制御	362
代行受信された HTTP/HTTPS 要求の処理	363
ポリシー タスクによる Web 要求の管理：概要	364
ポリシーによる Web 要求の管理：ベスト プラクティス	364
ポリシー	364
ポリシー タイプ	365
ポリシーの順序	368
ポリシーの作成	369
ポリシーの設定	376
アクセス ポリシー：オブジェクトのブロッキング	380
トランザクション要求のブロック、許可、リダイレクト	385
クライアント アプリケーション	388
クライアント アプリケーションについて	388
ポリシーでのクライアント アプリケーションの使用	388
認証からのクライアント アプリケーションの除外	389
時間範囲およびクォータ	389
ポリシーおよび使用許可コントロールの時間範囲	390
時間およびボリューム クォータ	391
URL カテゴリによるアクセス制御	394
URL カテゴリによる Web 要求の識別	394
URL カテゴリによる Web 要求へのアクション	395
リモートユーザー	396
リモート ユーザーについて	396
リモート ユーザーの ID を設定する方法	397
ASA のリモート ユーザー ステータスと統計情報の表示	399

ポリシーに関するトラブルシューティング	399
SaaS アクセス コントロール	399
SaaS アクセス コントロールの概要	400
ID プロバイダとしてのアプライアンスの設定	401
SaaS アクセス コントロールと複数のアプライアンスの使用	404
SaaS アプリケーション認証ポリシーの作成	404
シングルサインオン URL へのエンドユーザー アクセスの設定	407
発信トラフィックでの既存の感染のスキャン	407
発信トラフィックのスキャンの概要	408
要求が DVS エンジンによってブロックされた場合のユーザー エクスペリエンス	408
アップロード要求について	408
アウトバウンドマルウェア スキャン ポリシーの設定	410
アップロード要求の制御	412
DVS スキャンのロギング	413
第 6 章	統合 415
Cisco Identity Services Engine (ISE) / ISE パッシブ ID コントローラ (ISE-PIC) の統合	415
Identity Services Engine (ISE) / ISE パッシブ ID コントローラ (ISE-PIC) サービスの概要	415
pxGrid について	418
ISE/ISE-PIC サーバーの展開とフェールオーバーについて	418
ISE/ISE-PIC の証明書	419
自己署名証明書の使用	419
CA 署名付き証明書の使用	420
フォールバック認証	420
ISE/ISE-PIC サービスを統合するためのタスク	420
ISE/ISE-PIC を介した証明書の生成	422
Secure Web Applianceにアクセスするための ISE/ISE-PIC サーバーの設定	422
ISE/ISE-PIC サービスへの接続	423
自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC スタンドアロン展開へのインポート	426

自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC 分散型展開へのインポート	426
ISE/ISE-PIC へのロギングの設定	428
ISE/ISE-PIC からの ISE/ISE-PIC ERS サーバー詳細情報の取得	429
ISE-SXP 統合の設定	430
SGT から IP へのアドレスマッピングの ISE-SXP プロトコルについて	430
注意事項と制約事項	430
前提条件	431
SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化	431
ISE-SXP プロトコルのコンフィギュレーションの確認	432
ISE/ISE-PIC 統合での VDI（仮想デスクトップ インフラストラクチャ）ユーザー認証	432
Identity Services Engine に関する問題のトラブルシューティング	433
Cisco XDR との統合	433
アプライアンスと Cisco XDR の統合	434
アプライアンスと Cisco XDR の統合方法	435
前提条件	436
Cisco Secure Web Appliance での Cisco XDR の有効化	436
登録が成功したかどうかの確認	437
Cisco XDR プラグインを使用した脅威分析の実行	438
Cisco XDR プラグインのインストール	438
例：NGUI を介して Cisco XDR プラグインを使用 Secure Web Appliance	439
Cisco Secure Web Appliance と Cisco Umbrella の統合	439
Cisco Secure Web Appliance（SWA）と Cisco Umbrella について	440
統合のためのガイドライン	440
エンドツーエンドの手順	440
Cisco Secure Web Appliance と Cisco Umbrella を統合する方法	441
前提条件	441
Cisco Secure Web Appliance を Cisco Umbrella に登録する	442
登録が成功したかどうかの確認	443
Cisco Umbrella からの Cisco Secure Web Appliance の登録解除	444
Cisco Umbrella レポーティング ダッシュボードの表示	445

Web ポリシーと接続先リストの設定	445
識別プロファイルの設定	445
カスタムおよび外部 URL カテゴリの設定	446
アクセスポリシーの設定	446
復号ポリシーの設定	447
アクセスポリシーでのアプリケーションの設定	448
AD ユーザーまたは AD グループの設定	449
Microsoft 365 の互換性の設定	450
ポリシーの競合管理とポリシーの順序付け	450
ブロックされているページの管理	451
Cisco Umbrella シームレス ID	451
Cisco Umbrella シームレス ID の設定	452
Cisco Umbrella SWG のルーティング先の設定	453

第 7 章

ネットワーク セキュリティ	455
セキュリティ サービスの設定	455
セキュリティ サービスの設定の概要	456
Web レピュテーション フィルタの概要	456
Web レピュテーション スコア	456
Web レピュテーション フィルタの動作のしくみについて	457
マルウェア対策スキャンの概要	459
DVS エンジンの動作のしくみについて	459
複数のマルウェア判定の使用	460
Webroot スキャン	460
McAfee スキャン	461
Sophos スキャン	462
適応型スキャンについて	462
適応型スキャンとアクセス ポリシー	462
マルウェア対策とレピュテーション フィルタの有効化	463
Advanced Malware Protection サービスのキャッシュのクリア	465
ポリシーにおけるマルウェア対策およびレピュテーションの設定	465

アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定	466
Web レピュテーション スコアの設定	469
AMP for Endpoints コンソールとアプライアンスの統合	471
データベース テーブルの保持	474
Web レピュテーション データベース	474
Web レピュテーション フィルタリング アクティビティおよび DVS スキャンのロギング	474
適応型スキャンのロギング	475
キャッシング	475
マルウェアのカテゴリについて	475
ファイル レピュテーション フィルタリングとファイル分析	477
ファイル レピュテーション フィルタリングとファイル分析の概要	477
ファイル脅威判定のアップデート	478
ファイル処理の概要	478
ファイル レピュテーションおよび分析サービスでサポートされるファイル	480
クラウドに送信される情報のプライバシー	482
ファイル レピュテーションと分析機能の設定	483
ファイル レピュテーションと分析サービスとの通信の要件	483
オンプレミスのファイル レピュテーション サーバの設定	486
オンプレミスのファイル分析サーバの設定	487
ファイル レピュテーションと分析サービスの有効化と設定	488
重要：ファイル分析設定に必要な変更	495
(パブリック クラウド ファイル分析サービスのみ) アプライアンス グループの設定	495
アクセス ポリシーごとのファイル レピュテーションおよび分析サービスのアクション の設定	497
Advanced Malware Protection の問題に関するアラートの確実な受信	498
Advanced Malware Protection 機能の集約管理レポートの設定	499
ファイル レピュテーションおよびファイル分析のレポートとトラッキング	499
SHA-256 ハッシュによるファイルの識別	499
ファイル レピュテーションとファイル分析レポートのページ	500
その他のレポートでのファイル レピュテーション フィルタ データの表示	501

Web トラッキング機能と Advanced Malware Protection 機能について	502
ファイルの脅威判定の変更時のアクションの実行	503
ファイルレピュテーションと分析のトラブルシューティング	503
ログファイル	504
ファイルレピュテーションサーバまたはファイル分析サーバへの接続失敗に関する各種アラート	504
API キーのエラー（オンプレミスのファイル分析）	505
ファイルが予想どおりにアップロードされない	505
クラウド内のファイル分析の詳細が完全でない	506
分析のために送信できるファイルタイプに関するアラート	506
Web アプリケーションへのアクセスの管理	506
Web アプリケーションへのアクセスの管理：概要	507
AVC または ADC エンジンを実効にする	508
アプリケーションエンジンとデフォルトのアクション	508
要求が AVC または ADC エンジンによりブロックされた場合のユーザー体験	509
アプリケーション制御のポリシー設定	509
範囲要求の設定（Range Request Settings）	510
アプリケーション制御の設定のためのルールとガイドライン	511
アクセス ポリシー グループのアプリケーション管理設定	512
帯域幅の制御	513
全体の帯域幅制限の設定	514
ユーザーの帯域幅制限の設定	514
インスタント メッセージ トラフィックの制御	516
AVC または ADC アクティビティの表示	517
アクセスログファイルの AVC または ADC 情報	517
機密データの漏洩防止	518
機密データの漏洩防止の概要	518
最小サイズ以下のアップロード要求のバイパス	519
要求が機密データとしてブロックされた場合のユーザー エクスペリエンス	520
アップロード要求の管理	520
外部 DLP システムにおけるアップロード要求の管理	521

データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップの評価	522
クライアント要求とデータ セキュリティおよび外部 DLP ポリシー グループとの照合	522
データ セキュリティ ポリシーおよび外部 DLP ポリシーの作成	523
アップロード要求の設定の管理	526
URL カテゴリ	526
Web レピュテーション	526
コンテンツのブロック	527
外部 DLP システムの定義	528
外部 DLP サーバーの設定	528
外部 DLP ポリシーによるアップロード要求の制御	531
データ損失防止スキュンのロギング	532
エンドユーザーへのプロキシ アクションの通知	533
エンドユーザー通知の概要	533
通知ページの一般設定項目の設定	534
エンドユーザー確認応答ページ	535
エンドユーザー確認ページによる HTTPS および FTP サイトへのアクセス	536
エンドユーザー確認応答ページについて	536
エンドユーザー確認応答ページの設定	537
エンドユーザー通知ページ	539
オンボックス エンドユーザー通知ページの設定	539
オフボックス エンドユーザー通知ページ	540
エンドユーザー URL フィルタリング警告ページの設定	544
FTP 通知メッセージの設定	545
通知ページ上のカスタム メッセージ	545
通知ページのカスタム メッセージでサポートされる HTML タグ	545
通知ページの URL とロゴに関する注意事項	546
通知ページ HTML ファイルの直接編集	547
通知 HTML ファイルを直接編集するための要件	547
通知 HTML ファイルの直接編集	548
通知 HTML ファイルでの変数の使用	548

通知 HTML ファイルのカスタマイズのための変数	549
通知ページのタイプ	552
非標準ポートでの不正トラフィックの検出	572
不正トラフィックの検出の概要	572
L4 トラフィック モニターの設定	573
既知のサイトのリスト	573
L4 トラフィック モニターのグローバル設定	574
L4 トラフィック モニター アンチマルウェア ルールのアップデート	575
不正トラフィック検出ポリシーの作成	575
有効な形式	577
L4 トラフィック モニターのアクティビティの表示	577
モニターリング アクティビティとサマリー統計情報の表示	577
L4 トラフィック モニターのログ ファイルのエントリ	578

第 8 章

レポートとアラート	579
エンドユーザーのアクティビティをモニターするレポートの生成	579
レポートの概要	579
レポートでのユーザー名の使用	580
レポート ページ	580
レポート ページの使用	581
時間範囲の変更	581
レポートの時間範囲の選択	582
データの検索	583
チャート化するデータの選択	583
カスタム レポート	584
レポートおよびトラッキングにおけるサブ ドメインとセカンド レベル ドメインの比較	585
レポート ページからのレポートの印刷とエクスポート	586
新しい Web インターフェイスでのインタラクティブ レポート ページの使用	587
レポートの有効化	588
レポートのスケジュール設定	588

スケジュール設定されたレポートの追加	589
スケジュール設定されたレポートの編集	590
スケジュール設定されたレポートの削除	590
オンデマンドでのレポートの生成	590
アーカイブ レポート	591
L4 トラフィック モニタ レポートのトラブルシューティング	591
セキユア アプライアンス レポート	592
[概要 (Overview)] ページ	593
[ユーザ (Users)] ページ	595
[ユーザーの詳細 (User Details)] ページ	595
[ユーザー数 (User Count)] ページ	596
[Webサイト (Web Sites)] ページ	596
[URLカテゴリ (URL Categories)] ページ	597
URL カテゴリ セットの更新とレポート	598
[アプリケーションの表示 (Application Visibility)] ページ	598
[マルウェア対策 (Anti-Malware)] ページ	599
[マルウェア カテゴリ (Malware Category)] レポート ページ	600
[マルウェア脅威 (Malware Threats)] レポート ページ	600
Advanced Malware Protection	ページ 600
[ファイル分析 (File Analysis)] ページ	600
[セキユアエンドポイント判定のアップデート (AMP Verdict Updates)] ページ	600
[クライアント マルウェア リスク (Client Malware Risk)] ページ	600
[Webプロキシ : マルウェア リスク別クライアント (Web Proxy: Clients by Malware Risk)] の [クライアントの詳細 (Client Detail)] ページ	601
[Web レピュテーションフィルタ (Web Reputation Filters)] ページ	602
[L4 トラフィック モニター (L4 Traffic Monitor)] ページ	602
[SOCKS プロキシ (SOCKS Proxy)] ページ	603
[ユーザー ロケーション別のレポート (Reports by User Location)] ページ	603
[Web トラッキング (Web Tracking)] ページ	604
Web プロキシによって処理されるトランザクションの検索	605
L4 トラフィック モニタによって処理されたトランザクションの検索	608

SOCKS プロキシによって処理されるトランザクションの検索	609
[システム容量 (System Capacity)] ページ	609
[システムステータス (System Status)] ページ	609
新しい Web インターフェイスでのセキュア アプライアンス レポート	611
新しい Web インターフェイスの Web レポート ページの概要	612
[滞留時間 (Time Spent)] について	615
[概要 (Overview)] ページ	616
[アプリケーションの表示 (Application Visibility)] ページ	618
[レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor)] ページ	620
[SOCKS プロキシ (SOCKS Proxy)] ページ	623
[URLカテゴリ (URL Categories)] ページ	625
[HTTPSレポート (HTTPS Reports)] ページ	627
[ユーザ (Users)] ページ	629
[Webサイト (Web Sites)] ページ	634
Advanced Malware Protection ページ	635
[マルウェア対策 (Anti-Malware)] ページ	637
[クライアントマルウェア リスク (Client Malware Risks)] ページ	641
[Web レピュテーションフィルタ (Web Reputation Filters)] ページ	642
(Web レポートのみ) チャート化するデータの選択	644
新しい Web インターフェイスでの Web トラッキング	645
Web プロキシサービスによって処理されたトランザクションの検索	645
レイヤ4トラフィック モニターによって処理されたトランザクションの検索	650
SOCKS プロキシによって処理されるトランザクションの検索	651
Web トラッキングの検索結果の使用	651
詳細な Web トラッキング検索結果の表示	652
Web トラッキング検索結果について	652
Web トラッキング検索結果のトランザクションの詳細の表示	652
Web トラッキングおよびアップグレードについて	653
新しい Web インターフェイスでの Web レポートのスケジューリングとアーカイブ	653
新しい Web インターフェイスでの Web レポートのスケジューリング	653
新しい Web インターフェイスでの Web レポートのアーカイブ	655

新しい Web インターフェイスの [システムステータス (System Status)] ページ	656
ステータス	657
容量 (Capacity)	659
サービス	661

第 9 章

モニタリングおよびトラブルシューティング	665
ログによるシステム アクティビティのモニター	665
ロギングの概要	666
ロギングの共通タスク	666
ロギングのベスト プラクティス	667
ログによる Web プロキシのトラブルシューティング	667
ログ ファイルのタイプ	668
ログ サブスクリプションの追加および編集	676
W3C ログ フィールドの非匿名化	682
別のサーバへのログ ファイルのプッシュ	683
ログ ファイルのアーカイブ	684
ログのファイル名とアプライアンスのディレクトリ構造	685
ログ ファイルの閲覧と解釈	685
ログ ファイルの表示	686
アクセス ログ ファイル内の Web プロキシ情報	686
トランザクション結果コード	691
ACL デシジョン タグ	692
アクセス ログのスキャン判定エントリの解釈	703
W3C 準拠のアクセス ログ ファイル	712
W3C フィールド タイプ	712
W3C アクセス ログの解釈	712
アクセス ログのカスタマイズ	714
アクセス ログのユーザ定義フィールド	714
標準アクセス ログのカスタマイズ	715
W3C アクセス ログのカスタマイズ	716
トラフィック モニタのログ ファイル	720

トラフィック モニタ ログの解釈	720
ログ ファイルのフィールドとタグ	721
アクセス ログのフォーマット指定子と W3C ログ ファイルのフィールド	721
マルウェア スキャンの判定値	737
ロギングのトラブルシューティング	739
トラブルシューティング	739
一般的なトラブルシューティングとベスト プラクティス	740
FIPS モードの問題	740
CSP 暗号化	740
証明書の検証	740
認証に関する問題	741
認証の問題のトラブルシューティング ツール	741
認証の失敗による通常動作への影響	741
LDAP に関する問題	742
基本認証に関する問題	742
シングル サインオンに関する問題	743
オブジェクトのブロックに関する問題	743
一部の Microsoft Office ファイルがブロックされない	743
DOS の実行可能オブジェクトタイプをブロックすると、Windows OneCare のアップデートがブロックされる	743
ブラウザに関する問題	744
Firefox で WPAD を使用できない	744
DNS に関する問題	744
アラート : DNS キャッシュのブートに失敗 (Failed to bootstrap the DNS cache)	744
フェールオーバーの問題	744
フェールオーバーの誤った設定	745
仮想アプライアンスでのフェールオーバーに関する問題	745
機能キーの期限切れ	745
FTP に関する問題	745
URL カテゴリが一部の FTP サイトをブロックしない	746
大規模 FTP 転送の切断	746

ファイルのアップロード後に FTP サーバーにゼロ バイト ファイルが表示される	746
Chrome ブラウザが FTP-over-HTTP 要求でユーザー エージェントとして検出されない	746
アップロード/ダウンロード速度の問題	746
ハードウェアに関する問題	748
アプライアンスの電源の再投入	748
アプライアンスの状態およびステータス インジケータ	748
アラート : 380 または 680 ハードウェアでバッテリー再学習タイムアウト (RAID イベント) (Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware)	748
HTTPS/復号/証明書に関する問題	748
URL カテゴリ 基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス	749
HTTPS 要求の失敗	749
特定 Web サイトの復号のバイパス	750
埋め込み/参照コンテンツのブロックの例外に対する条件および制約事項	750
アラート : セキュリティ証明書に関する問題 (Problem with Security Certificate)	751
Identity Services Engine に関する問題	751
ISE 問題のトラブルシューティング ツール	751
ISE サーバーの接続に関する問題	752
ISE 関連の重要なログ メッセージ	754
カスタム URL カテゴリおよび外部 URL カテゴリに関する問題	755
外部ライブ フィード ファイルのダウンロードに関する問題	755
.CSV ファイルの IIS サーバでの MIME タイプに関する問題	756
コピー アンド ペーストの後にフィード ファイルの形式が不正になる	756
ロギングに関する問題	756
アクセス ログ エントリにカスタム URL カテゴリが表示されない	757
HTTPS トランザクションのロギング	757
アラート : 生成データのレートを維持できない (Unable to Maintain the Rate of Data Being Generated)	757
W3C アクセス ログでサードパーティ製ログ アナライザ ツールを使用する場合の問題	758
ポリシーに関する問題	758

HTTPS に対してアクセス ポリシーを設定できない	758
オブジェクトのブロックに関する問題	758
識別プロファイルがポリシーから削除される	759
ポリシーの照合に失敗	759
ポリシーのトラブルシューティング ツール：ポリシー トレース	761
ファイル レピュテーションとファイル分析に関する問題	764
リブートの問題	765
KVM で動作する仮想アプライアンスがリブート時にハングアップ	765
ハードウェア アプライアンス：アプライアンスの電源のリモート リセット	765
サイトへのアクセスに関する問題	766
認証をサポートしていない URL にアクセスできない	766
POST 要求を使用してサイトにアクセスできない	767
アップストリーム プロキシに関する問題	767
アップストリーム プロキシが基本クレデンシャルを受け取らない	767
クライアント要求がアップストリーム プロキシで失敗する	767
アップストリーム プロキシ経由で FTP 要求をルーティングできない	768
仮想アプライアンス	768
AsyncOS の起動中に強制リセット、電源オフ、リセットのオプションを使用しないでください	768
KVM 展開でネットワーク接続が最初は機能するが、その後失敗する	768
KVM 展開におけるパフォーマンスの低下、ウォッチドッグ問題、および高 CPU 使用率	768
Linux ホスト上で実行されている仮想アプライアンスの一般的なトラブルシューティング	769
WCCP に関する問題	769
最大ポート エントリ数	769
パケット キャプチャ	769
パケット キャプチャの開始	770
パケット キャプチャ ファイルの管理	771
サポートの使用	771
効率的なサービス提供のための情報収集	771
テクニカル サポート要請の開始	772

仮想アプライアンスのサポートの取得	772
アプライアンスへのリモート アクセスのイネーブル化	773

第 10 章

コマンドライン インターフェイス	775
コマンドライン インターフェイスの概要	775
コマンドライン インターフェイスへのアクセス	775
初回アクセス	776
以降のアクセス	776
コマンドプロンプトの使用	776
コマンドの構文	777
選択リスト	777
Yes/No クエリー	777
サブコマンド	777
サブコマンドのエスケープ	778
コマンド履歴	778
コマンドのオートコンプリート	778
CLI を使用した設定変更の確定	778
汎用 CLI コマンド	779
CLI の例：設定変更の確定	779
CLI の例：設定変更のクリア	779
CLI の例：コマンドライン インターフェイス セッションの終了	779
CLI の例：コマンドライン インターフェイスでのヘルプの検索	779
Secure Web Appliance CLI コマンド	780

付録 A :

その他の情報	805
Cisco 通知サービス	805
ドキュメント セット	805
トレーニング	806
ナレッジ ベースの記事	806
シスコサポートコミュニティ	806
カスタマー サポート	807

リソースにアクセスするためのシスコ アカウントの登録 807

マニュアルに関するフィードバック 807

サードパーティ コントリビュータ 807

個人情報の取り扱い 808

付録 B :

エンド ユーザ ライセンス契約書 809

Cisco Systems エンド ユーザ ライセンス契約書 809

Cisco コンテンツ セキュリティ ソフトウェア用エンド ユーザ ライセンス契約補則 816



第 1 章

はじめに

この章で説明する内容は、次のとおりです。

- [Secure Web Appliance について, on page 1](#)
- [AsyncOS 15.5 の新機能 \(2 ページ\)](#)
- [関連項目, on page 4](#)
- [アプライアンス Web インターフェイスの使用, on page 4](#)
- [サポートされている言語 \(8 ページ\)](#)
- [Cisco SensorBase ネットワーク, on page 9](#)

Secure Web Appliance について

Cisco Secure Web Appliance (SWA) はインターネットトラフィックを代行受信してモニターし、ポリシーを適用することによって、マルウェア、機密データの漏洩、生産性の低下などのインターネットベースの脅威から内部ネットワークを保護します。Cisco Secure Web Appliance はプロキシサーバーとして機能し、ユーザーからの Web 要求を代行受信して、要求された Web コンテンツをスキャンし、マルウェア、ウイルス、フィッシング攻撃などの潜在的な脅威を検出します。URL フィルタリング、ウイルス対策スキャン、レピュテーションベースのフィルタリング、高度なマルウェア防御などのさまざまなセキュリティテクノロジーを使用して、Web トラフィックのセキュリティを確保します。全体として、Secure Web Appliance は、組織が Web トラフィックを保護し、使用ポリシーを適用し、Web ベースの脅威から保護するのに役立ち、より安全で制御された Web ブラウジング環境をユーザーに提供します。

AsyncOS 15.5 の新機能

特長	説明
FIPS 140-3 コンプライアンス	Cisco Secure Web Appliance は FIPS に準拠し、FIPS 140-3 承認の Cisco Common Crypto Module と統合されています。 [システム管理 (System Administration)] > [FIPS モード (FIPS Mode)] > [設定の編集 (Edit Setting)] に移動して、FIPS モードを有効にします。 (注) [有効化 (Enable)] オプションは、[現在のサービス ステータス (Current Service Status)] にリストされているすべてのサービスと証明書が FIPS に準拠している場合にのみ選択できます。
新しいバージョンの AMP エンジンのサポート	Secure Web Appliance ゲートウェイでは、高度なマルウェア防御 (AMP) エンジンの新しいバージョンを使用するようになりました。この新しい AMP エンジンは、TCP の代わりに HTTPS (ポート 443) を使用して、Web アプリアンス ゲートウェイと Cisco Secure Endpoint Cloud 間の安全な通信を保証します。 詳細については、ファイル レピュテーション フィルタリングとファイル分析 (477 ページ) を参照してください。

特長	説明
Microsoft 更新バイパス	Microsoft 更新は、Microsoft がオペレーティング システムやソフトウェアアプリケーション向けにリリースする重要なパッチ、セキュリティ更新、および機能拡張です。これらの更新は、コンピュータとネットワーク デバイスのセキュリティ、安定性、およびパフォーマンスを維持するために重要です。これらの更新では、多くの場合、大きなファイルや多数の小さなファイルをダウンロードする必要があります。これにより、プロキシサーバで大量の帯域幅および処理リソースが消費されることがあります。これにより、輻輳が発生し、ネットワーク パフォーマンスが低下し、SWA インフラストラクチャの負荷が増加する可能性があります、全体のユーザーエクスペリエンスやその他の重要なネットワーク運用に影響を与える可能性があります。 プロキシサーバからの Microsoft 更新トラフィックをバイパスするのが、これらの課題に安全で効果的に対処できる方法です。Microsoft 更新は信頼できる Microsoft サーバから取得されるため、このトラフィックがプロキシサーバをバイパスできるようにすると、ネットワーク セキュリティを損なうことなくプロキシサーバの負荷を軽減できます。これにより、他のセキュリティおよびコンテンツ フィルタリング タスクのプロキシ リソースを維持しながら、重要な更新が効率的に配信されます。 [Web セキュリティ マネージャの > バイパス設定 (Web Security Manager Bypass Settings)] > [アプリケーション バイパス設定の編集 (Edit Application Bypass Settings)]に移動して、Microsoft 更新バイパス機能を有効にできるようになりました。

特長	説明
Cisco XDR との Cisco Secure Web Appliance の統合	SecureX は、機能強化され、より堅牢になったプラットフォームである Cisco XDR（Extended Detection and Response）に移行しています。この移行の一環として、XDR を Cisco Secure Web Appliance と統合することが不可欠です。Cisco Secure Web Appliance と Cisco XDR を統合させることで、測定可能な分析情報を提供し、必要な結果とこれまでにないチーム間コラボレーションを実現します。Cisco XDR は、セキュリティインフラストラクチャの可視性を統一し、自動化を実現します。また、インシデント対応ワークフローの加速化と脅威検出の強化を図ります。 セキュア Web アプライアンスと Cisco XDR を統合する方法の詳細については、アプライアンスと Cisco XDR の統合（434 ページ） を参照してください。
NTP 認証での AES-CMAC 暗号化方式のサポート	SHA1 および MD5 暗号化方式に加えて、AES-CMAC のサポートが導入されました。 NTP サーバで、AES-CMAC 暗号化方式を選択できるようになりました。詳細については、NTP サーバーによるシステムクロックの同期（197 ページ） を参照してください。

関連項目

- <http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html>
- <https://docs.umbrella.com/umbrella-user-guide/docs/umbrella-integration-with-secure-web-appliance>

アプライアンス Web インターフェイスの使用

- [Web インターフェイスのブラウザ要件, on page 4](#)
- [仮想アプライアンスでの Web インターフェイスへのアクセスのイネーブル化, on page 6](#)
- [アプライアンス Web インターフェイスへのアクセス, on page 6](#)
- [Web インターフェイスでの変更内容のコミット, on page 8](#)
- [Web インターフェイスでの変更内容のクリア, on page 8](#)

Web インターフェイスのブラウザ要件

Web インターフェイスにアクセスするための要件は次のとおりです。

- ブラウザで Cookie と JavaScript がサポートされ、有効になっている必要があります。
- また、ブラウザでは Cascading Style Sheet (CSS) を含む HTML ページをレンダリングできる必要があります。
- Cisco Secure Web Appliance は YUI (<http://yuilibrary.com/yui/environments/>) で設定されたターゲット環境に準拠しています。
- セッションは、非アクティブな状態が 30 分続くと自動的にタイムアウトします。
- Web インターフェイス内の一部のボタンとリンクを使用すると、さらにウィンドウが開きます。そのため、Web インターフェイスを使用するには、ブラウザのポップアップブロックを設定する必要があります。

**Note**

アプライアンスの設定を編集する場合は、一度に1つのブラウザウィンドウまたはタブを使用します。また、Web インターフェイスおよび CLI を同時に使用してアプライアンスを編集しないでください。複数の場所からアプライアンスを編集すると、予期しない動作が発生するので、サポートされません。

GUI にアクセスするには、ブラウザが JavaScript および Cookie をサポートし、受け入れるよう設定されている必要があります。さらに、Cascading Style Sheet (CSS) を含む HTML ページを描画できる必要があります。

Table 1: サポートされるブラウザおよびリリース

ブラウザ	Windows 10	MacOS 10.6
Safari	—	7.0 以降
Google Chrome	最新の安定バージョン	最新の安定バージョン
Microsoft Internet Explorer	11.0	—
Mozilla Firefox	最新の安定バージョン	最新の安定バージョン
Microsoft Edge	最新の安定バージョン	最新の安定バージョン

ブラウザは、そのブラウザの公式なサポート対象オペレーティング システムに対してのみサポートされます。

インターフェイスの一部のボタンまたはリンクからは追加のウィンドウがオープンされるため、GUI を使用するには、ブラウザのポップアップブロックの設定が必要な場合があります。

サポートされているブラウザのいずれかで、アプライアンスのレガシー Web インターフェイスにアクセスできます。

アプライアンスの新しい Web インターフェイス（AsyncOS 11.8 以降）でサポートされている解像度は、1280x800～1680x1050 です。サポートされるすべてのブラウザに対して最適に表示される解像度は 1440X900 です。



Note シスコでは、より高い解像度でアプライアンスの新しい Web インターフェイスを表示することは推奨していません。

仮想アプライアンスでの Web インターフェイスへのアクセスのイネーブル化

デフォルトでは、HTTP および HTTPS インターフェイスは仮想アプライアンスで有効化されません。これらのプロトコルを有効にするには、コマンドラインインターフェイスを使用する必要があります。

Procedure

ステップ 1 コマンドライン インターフェイスにアクセスします。 [コマンドライン インターフェイスへのアクセス, on page 775](#) を参照してください。

ステップ 2 `interfaceconfig` コマンドを実行します。

プロンプトで Enter を押すと、デフォルト値が受け入れられます。

HTTP および HTTPS のプロンプトを検索し、使用するプロトコルをイネーブルにします。

HTTP および HTTPS の AsyncOS API（モニターリング）のプロンプトを探し、使用するプロトコルをイネーブルにします。

アプライアンス Web インターフェイスへのアクセス

仮想アプライアンスを使用している場合は、[仮想アプライアンスでの Web インターフェイスへのアクセスのイネーブル化, on page 6](#) を参照してください。

Procedure

ステップ 1 ブラウザを開き、Secure Web Appliance の IP アドレス（またはホスト名）を入力します。アプライアンスが事前に設定されていない場合は、デフォルト設定を使用します。

`https://192.168.42.42:8443`

または

`http://192.168.42.42:8080`

ここで、192.168.42.42 はデフォルト IP アドレス、8080 は HTTP のデフォルトの管理ポートの設定、8443 は HTTPS のデフォルトの管理ポートです。

アプライアンスが現在設定されている場合は、M1 ポートの IP アドレス（またはホスト名）を使用します。

Note

アプライアンスに接続するときはポート番号を使用する必要があります（デフォルトはポート 8080）。Web インターフェイスにアクセスするときにポート番号を指定しないと、デフォルト ポート 80 になり、[ライセンスなしプロキシ（Proxy Unlicensed）] エラー ページが表示されます。

ステップ 2 （新しい Web インターフェイスのみ）レガシー Web インターフェイスにログインし、[Secure Web Appliance のデザインが新しくなりました。お試ください! リンクで新しい Web インターフェイスにアクセスできます。このリンクをクリックすると、Web ブラウザの新しいタブが開き、

`https://wsa_appliance.com:<trailblazer-https-port>/ng-login` に移動します。ここで、`wsa_appliance.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスに設定されている TRAILBLAZER HTTPS ポートです。

Note

- アプライアンスのレガシー Web インターフェイスにログインする必要があります。
- 指定したアプライアンスのインターフェイスホスト名を DNS サーバーが解決できることを確認します。
- デフォルトでは、新しい Web インターフェイスでは、TCP ポート 6080、6443、および 4431 が動作可能である必要があります。これらのポートがエンタープライズファイアウォールでブロックされていないことを確認します。
- 新しい Web インターフェイスにアクセスするためのデフォルト ポートは 4431 です。これは、`trailerblazerconfig CLI` コマンドを使用してカスタマイズできます。`trailblazerconfig CLI` コマンドの詳細については、[Secure Web Appliance CLI コマンド, on page 780](#)を参照してください。
- 新しい Web インターフェイスでは、HTTP および HTTPS の AsyncOS API（モニタリング）ポートも必要です。デフォルトでは、これらのポートは 6080 および 6443 です。AsyncOS API（モニタリング）ポートは、`interfaceconfig CLI` コマンドでカスタマイズすることもできます。`interfaceconfig CLI` コマンドの詳細については、[Secure Web Appliance CLI コマンド, on page 780](#)を参照してください。

Note

ポートはデフォルトで有効になっていますが、これらのポートを無効にすると、アップグレード後に再び有効になります。

- これらのデフォルトポートを変更した場合は、新しい Web インターフェイスのカスタマイズされたポートもエンタープライズ ファイアウォールでブロックされないことを確認してください。

ステップ 3 アプライアンスのログイン画面が表示されたら、アプライアンスにアクセスするためのユーザー名とパスワードを入力します。

デフォルトで、アプライアンスには以下のユーザー名とパスワードが付属します。

- ユーザー名 : **admin**

- パスフレーズ : **ironport**

admin のユーザー名でログインするのが初めての場合は、パスフレーズをすぐに変更するよう求められます。

ステップ 4 自分のユーザー名での最近のアプライアンスへのアクセス試行（成功、失敗を含む）を表示するには、アプリケーション ウィンドウの右上の [ログイン (Logged in as)] エントリの前にある [最近のアクティビティ (recent-activity)] アイコン（成功は **i**、失敗は **!**）をクリックします。

Web インターフェイスでの変更内容のコミット

Procedure

ステップ 1 [変更を確定 (Commit Changes)] をクリックします。

ステップ 2 選択する場合、[コメント (Comment)] フィールドにコメントを入力します。

ステップ 3 [変更を確定 (Commit Changes)] をクリックします。

Note

すべてをコミットする前に、複数の設定変更を行うことができます。

Web インターフェイスでの変更内容のクリア

Procedure

ステップ 1 [変更を確定 (Commit Changes)] をクリックします。

ステップ 2 [変更を破棄 (Abandon Changes)] をクリックします。

サポートされている言語

AsyncOS は次の言語のいずれかで GUI および CLI を表示できます。

- ドイツ語
- 英語
- スペイン語
- フランス語

- イタリア語
- 日本語
- 韓国語
- ポルトガル語
- ロシア語
- 中国語
- 台湾語

Cisco SensorBase ネットワーク

Cisco SensorBase ネットワークは、世界中の何百万ものドメインを追跡し、インターネットトラフィックのグローバルウォッチリストを維持する脅威の管理データベースです。SensorBase は、既知のインターネットドメインの信頼性の評価をシスコに提供します。Cisco Secure Web Appliance は、SensorBase データフィードを使用して、Web レピュテーションスコアを向上させます。

SensorBase の利点とプライバシー

Cisco SensorBase ネットワークへの参加は、シスコがデータを収集して、SensorBase 脅威管理データベースとそのデータを共有することを意味します。このデータには要求属性に関する情報およびアプライアンスが要求を処理する方法が含まれます。

シスコはプライバシーを維持する重要性を理解しており、ユーザー名やパスワードなどの個人情報または機密情報も収集または使用しません。また、ファイル名とホスト名に続く URL 属性は、機密性を保証するために難読化されます。復号された HTTPS トランザクションでは、SensorBase ネットワークは IP アドレス、Web レピュテーションスコア、および証明書内のサーバー名の URL カテゴリのみを受信します。

SensorBase ネットワークへの参加に同意する場合、アプライアンスから送信されたデータは HTTPS を使用して安全に転送されます。データを共有すると、Web ベースの脅威に対応して、悪意のあるアクティビティから企業環境を保護するシスコの機能が向上します。

Cisco SensorBase ネットワークへの参加の有効化

**Note**

システムの設定時にデフォルトで [標準 SensorBase ネットワークに参加 (Standard SensorBase Network Participation)] がイネーブルにされています。

Procedure

ステップ 1 [セキュリティ サービス (Security Services)] > [SensorBase (SensorBase)] を選択します。

ステップ 2 [SensorBase ネットワークに参加 (SensorBase Network Participation)] がイネーブルであることを確認します。

ディセーブルの場合、アプライアンスが収集するデータは SensorBase ネットワーク サーバーには戻されません。

ステップ 3 [加入レベル (Participation Level)] セクションで、以下のレベルのいずれかを選択します。

- **[制限 (Limited)]**。基本的な参加はサーバー名情報をまとめ、SensorBase ネットワーク サーバーに MD5 ハッシュ パス セグメントを送信します。
- **[標準 (Standard)]**。拡張された参加は、unobfuscated パス セグメントを使用した URL 全体を SensorBase ネットワーク サーバーに送信します。このオプションは、より強力なデータベースの提供を支援し、継続的に Web レピュテーション スコアの整合性を向上させます。

ステップ 4 [AnyConnect ネットワークへの参加 (AnyConnect Network Participation)] フィールドで、Cisco AnyConnect クライアントを使用して Cisco Secure Web Appliance に接続するクライアントから収集された情報を含めるかどうかを選択します。

AnyConnect クライアントは、Secure Mobility 機能を使用してアプライアンスに Web トラフィックを送信します。

ステップ 5 [除外されたドメインと IP アドレス (Excluded Domains and IP Addresses)] フィールドで、任意でドメインまたは IP アドレスを入力して、SensorBase サーバーに送信されたトラフィックを除外します。

ステップ 6 変更を送信し、保存します。



第 2 章

接続、インストール、設定

この章で説明する内容は、次のとおりです。

- [接続、インストール、設定の概要, on page 11](#)
- [仮想アプライアンスの展開, on page 12](#)
- [操作モードの比較, on page 12](#)
- [タスクの概要：接続、インストール、設定, on page 18](#)
- [アプライアンスの接続, on page 18](#)
- [設定情報の収集, on page 22](#)
- [システム セットアップ ウィザード, on page 24](#)
- [アップストリーム プロキシ, on page 33](#)
- [ネットワーク インターフェイス, on page 35](#)
- [ハイ アベイラビリティを実現するためのフェールオーバー グループの設定, on page 50](#)
- [Web プロキシ データに対する P2 データ インターフェイスの使用, on page 54](#)
- [リダイレクト ホスト名とシステム ホスト名, on page 69](#)
- [DNS の設定, on page 71](#)
- [接続、インストール、設定に関するトラブルシューティング, on page 74](#)

接続、インストール、設定の概要

Secure Web Applianceでは、次の動作モードを提供しています。

- **標準：** Secure Web Applianceの標準動作モードには、オンサイトの Web プロキシサービスとレイヤ 4 トラフィックモニタリングが含まれます。これらのサービスはクラウド Web セキュリティコネクタモードでは使用できません。
- **クラウド Web セキュリティコネクタ：** クラウド Web セキュリティコネクタモードでは、アプライアンスは、Web セキュリティポリシーが適用されている Cisco Cloud Web Security (CWS) プロキシに接続してトラフィックをルーティングします。

アプライアンスには複数のポートが搭載されており、各ポートは割り当てられた1つ以上の特定のデータ型を管理します。

アプライアンスは、ネットワークルート、DNS、VLAN、およびその他の設定とサービスを使用して、ネットワーク接続とトラフィック代行受信を管理します。システムセットアップウィザードでは基本的なサービスと設定項目をセットアップでき、アプライアンスの Web インターフェイスでは設定の変更や追加オプションの設定ができます。

仮想アプライアンスの展開

仮想 Secure Web Applianceを展開するには、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。このドキュメントは、
<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html>
から入手できます。

物理アプライアンスから仮想アプライアンスへの移行

物理アプライアンスから仮想アプライアンスに展開を移行するには、前のトピックで言及した『Virtual Appliance Installation Guide』、および使用している AsyncOS のバージョンに応じたリリース ノートを参照してください。

操作モードの比較

以下の表では、標準モードとクラウド コネクタ モードで使用可能なさまざまなメニュー コマンドを示し、それにより各モードで使用可能なさまざまな機能について説明します。

メニュー	標準モードで使用可能	クラウドコネクタモードで使用可能
レポート	システム ステータス (System Status) 概要 (Overview) ユーザー (Users) ユーザー数 (User Count) Web サイト (Web Sites) URL カテゴリ (URL Categories) アプリケーションの表示 (Application Visibility) マルウェア対策 (Anti-Malware) Advanced Malware Protection ファイル分析 (File Analysis) AMP 判定の更新 クライアント マルウェア リスク (Client Malware Risk) Web レピュテーション フィルタ (Web Reputation Filters) レイヤ 4 トラフィック モニタ (Layer-4 Traffic Monitor) ユーザの場所別レポート (Reports by User Location) Web トラッキング (Web Tracking) システム容量 (System Capacity) システム ステータス (System Status) スケジュール設定されたレポート (Scheduled Reports) アーカイブ レポート (Archived Reports)	システム ステータス (System Status)

メニュー	標準モードで使用可能	クラウドコネクタモードで使用可能
Web セキュリティ マネージャ (Web Security Manager)	識別プロファイル (Identification Profiles) クラウドルーティング ポリシー (Cloud Routing Policies) SaaS ポリシー 復号ポリシー (Decryption Policies) ルーティング ポリシー アクセス ポリシー 全体の帯域幅の制限 (Overall Bandwidth Limits) Cisco データ セキュリティ 発信マルウェアスキャン (Outbound Malware Scanning) 外部データ消失防止 Web トラフィック タップ ポリシー SOCKS ポリシー (SOCKS Policies) カスタム URL カテゴリ 時間範囲およびクォータの定義 (Define Time Ranges and Quotas) バイパス設定 (Bypass Settings) レイヤ 4 トラフィック モニタ (Layer-4 Traffic Monitor)	識別プロファイル (Identification Profiles) クラウドルーティング ポリシー (Cloud Routing Policies) 外部データ消失防止 (External Data Loss Prevention) カスタム URL カテゴリ (Custom URL Categories)

メニュー	標準モードで使用可能	クラウドコネクタ モードで使用可能
セキュリティ サービス	Web プロキシ (Web Proxy) FTP プロキシ (FTP Proxy) HTTPS プロキシ (HTTPS Proxy) SOCKS プロキシ (SOCKS Proxy) PAC ファイル ホスティング (PAC File Hosting) 使用許可コントロール (Acceptable Use Controls) マルウェア対策とレピュテーション (Anti-Malware and Reputation) データ転送フィルタ (Data Transfer Filters) AnyConnect セキュア モビリティ (AnyConnect Secure Mobility) ユーザ通知 (End-User Notification) L4 トラフィック モニタ (L4 Traffic Monitor) SensorBase レポート Cisco Cloudlock Cisco Cognitive Threat Analytics	Web プロキシ (Web Proxy)

メニュー	標準モードで使用可能	クラウドコネクタモードで使用可能
ネットワーク (Network)	インターフェイス (Interfaces) 透過リダイレクション (Transparent Redirection) ルート DNS 高可用性 (High Availability) 内部 SMTP リレー (Internal SMTP Relay) 上位プロキシ (Upstream Proxy) 外部 DLP サーバ (External DLP Servers) Web トラフィック タップ (Web Traffic Tap) 証明書の管理 (Certificate Management) 認証 SaaS のアイデンティティプロバイダー Identity Services Engine	インターフェイス (Interfaces) 透過リダイレクション (Transparent Redirection) ルート DNS 高可用性 (High Availability) 内部 SMTP リレー (Internal SMTP Relay) 外部 DLP サーバ (External DLP Servers) 証明書の管理 (Certificate Management) 認証 マシン ID サービス (Machine ID Service) クラウドコネクタ (Cloud Connector)

メニュー	標準モードで使用可能	クラウドコネクタモードで使用可能
システム管理	ポリシー トレース (Policy Trace) アラート (Alerts) ログ サブスクリプション (Log Subscriptions) 返信先アドレス (Return Addresses) SSL の設定 (SSL Configuration) ユーザー (Users) Network Access タイム ゾーン 時刻設定 (Time Settings) 設定の概要 設定ファイル (Configuration File) 機能キーの設定 (Feature Key Settings) ライセンス キー (Feature Keys) アップグレードとアップデートの設定 (Upgrade and Update Settings) システム アップグレード (System Upgrade) システム セットアップ ウィザード (System Setup Wizard) FIPS モード (FIPS Mode) 次の手順	アラート (Alerts) ログ サブスクリプション (Log Subscriptions) SSL の設定 (SSL Configuration) ユーザー (Users) Network Access タイム ゾーン 時刻設定 (Time Settings) 設定の概要 設定ファイル (Configuration File) ライセンス キー (Feature Keys) アップグレードとアップデートの設定 (Upgrade and Update Settings) システム アップグレード (System Upgrade) システム セットアップ ウィザード (System Setup Wizard)
Cisco CWS ポータル (Cisco CWS Portal) (ハイブリッド Web セキュリティ モードでのみ使用可能)	なし	N/A

タスクの概要：接続、インストール、設定

タスク	詳細情報
アプライアンスをインターネット トラフィックに接続する。	アプライアンスの接続, on page 18
設定情報を収集して記録する。	設定情報の収集, on page 22
システム セットアップ ウィザードを実行する。	システム セットアップ ウィザード, on page 24
HTTPS プロキシ設定、認証レلم、識別プロファイルを設定する。この手順はハイブリッド Web セキュリティ モードで実行する必要があります。	HTTPS プロキシのイネーブル化, on page 348 認証レلم, on page 90 識別プロファイルと認証, on page 277
(任意) アップストリーム プロキシを接続する。	アップストリーム プロキシ, on page 33

アプライアンスの接続

Before you begin

- アプライアンスを設置するには、管理用アプライアンスにケーブルを配線して電源に接続し、そのアプライアンスのハードウェア ガイドの手順に従います。ご使用のモデルのマニュアルの場所については、[ドキュメント セット, on page 805](#) を参照してください。
- 透過リダイレクションのためにアプライアンスを物理的に WCCP v2 ルータに接続する場合は、まず、WCCP ルータがレイヤ 2 リダイレクションに対応していることを確認します。
- 以下のシスコ推奨設定に注意してください。
 - パフォーマンスとセキュリティの向上のために、可能な場合はシンプレックスケーブル（着信と発信トラフィック用の個別のケーブル）を使用します。

Procedure

ステップ 1 管理インターフェイスを接続します（まだ接続していない場合）。

イーサネット ポート	注記
M1	接続可能な場所に M1 を接続します。 - 管理トラフィックを送受信します。 (オプション) Web プロキシ データ トラフィックを送受信します。 M1 にラップトップを直接接続して、アプライアンスを管理できます。 ホスト名 (http://hostname:8080) を使用して管理インターフェイスに接続するには、アプライアンスのホスト名と IP アドレスを DNS サーバ データベースに追加します。
P1 および P2 (オプション)	- 発信方向の管理サービス トラフィックで使用可能ですが、管理には使用できません。 [ポート M1 は管理目的でのみ使用 (Use M1 port for management only)] ([ネットワーク (Network)] > [インターフェイス (Interfaces)] ページ) をイネーブルにします。 - データ インターフェイスを使用するように、サービスのルーティングを設定します。

ステップ 2 (オプション) アプライアンスをデータ トラフィックに直接接続するか、透過リダイレクション デバイスを介して接続します。

イーサネット ポート	明示的な転送	透過リダイレクション
P1/P2	P1 のみ： • [ポートM1は管理目的でのみ使用 (Use M1 port for management only)] をイネーブルにします。 • P1 と M1 を異なるサブネットに接続します。 • 着信と発信の両方のトラフィックを受信できるように、デュプレックスケーブルを使用してP1を内部ネットワークとインターネットに接続します。 P1 および P2 • P1 をイネーブルにします。 • M1、P1、P2 を異なるサブネットに接続します。 • P2をインターネットに接続し、着信インターネットトラフィックを受信します。 システムセットアップウィザードの実行後、P2 をイネーブルにします。	デバイス：WCCP v2 ルータ： • レイヤ2リダイレクションの場合は、ルータを物理的に P1/P2 に接続します。 • レイヤ3リダイレクションの場合は、総称ルーティングカプセル化 (GRE) でパフォーマンス上の問題が発生する可能性があるので注意してください。 • アプライアンス上に WCCP サービスを作成します。 デバイス：レイヤ4スイッチ： • レイヤ2リダイレクションの場合は、スイッチを物理的に P1/P2 に接続します。 • レイヤ3リダイレクションの場合は、総称ルーティングカプセル化 (GRE) でパフォーマンス上の問題が発生する可能性があるので注意してください。 Note アプライアンスはインラインモードをサポートしていません。
M1 (オプション)	[ポートM1は管理目的でのみ使用 (Use M1 port for management only)] がディセーブルの場合は、M1 がデフォルトのデータトラフィック用ポートになります。	該当なし

ステップ3 (オプション) レイヤ4トラフィックをモニタするには、プロキシポートの後ろと、クライアントIPアドレスのネットワークアドレス変換 (NAT) を実行するデバイスの前に、タップ、スイッチ、またはハブを接続します。

イーサネット ポート	注記
T1/T2	レイヤ 4 トラフィックモニタのブロッキングを許可するには、Secure Web Appliance と同じネットワーク上にレイヤ 4 トラフィックモニタを配置します。 推奨設定： デバイス：ネットワーク タップ： • ネットワーク タップに T1 を接続し、発信クライアントトラフィックを受信します。 • ネットワーク タップに T2 を接続し、着信インターネットトラフィックを受信します。 その他のオプション： デバイス：ネットワーク タップ： • T1 でデュプレックス ケーブルを使用し、着信および発信トラフィックを受信します。 デバイス：スイッチ上のスパン化またはミラー化されたポート • 発信クライアント トラフィックを受信するように T1 を接続し、着信インターネット トラフィックを受信するように T2 を接続します。 • (準推奨) 半二重または全二重ケーブルを使用して T1 を接続し、着信と発信の両方のトラフィックを受信します。 デバイス：ハブ： • (低推奨) デュプレックス ケーブルを使用して T1 を接続し、着信と発信の両方のトラフィックを受信します。 アプライアンスは、これらのインターフェイス上のすべての TCP ポートでトラフィックをリッスンします。

ステップ 4 外部プロキシをアプライアンスのアップストリームに接続し、外部プロキシがアプライアンスからデータを受信できるようにします。

What to do next

[設定情報の収集, on page 22](#)

関連項目

- [ネットワーク インターフェイスのイネーブル化または変更, on page 37](#)
- [Web プロキシ データに対する P2 データ インターフェイスの使用 , on page 54](#)

- [WCCP サービスの追加と編集, on page 61](#)
- [トランスペアレント リダイレクションの設定, on page 58](#)
- [アップストリーム プロキシ, on page 33](#)

設定情報の収集

以下のワークシートを使用して、システム セットアップ ウィザードの実行時に必要な設定値を記録できます。各プロパティの詳細については、[システム セットアップ ウィザードの参照情報, on page 26](#)を参照してください。

システム セットアップ ウィザードのワークシート			
プロパティ	値	プロパティ	値
アプライアンスの詳細 (Appliance Details)		ルート	
デフォルトの SystemHostname (Default SystemHostname)		管理トラフィック (Management Traffic)	
ローカル DNS サーバ (Local DNS Server(s)) (インターネットルー トサーバを使用しない 場合に必要)		デフォルトゲートウェ イ (Default Gateway)	
DNS サーバ 1 (DNS Server 1)		(オプション) スタ ティック ルート テー ブル名 (Static Route Table Name)	
(オプション) DNS サーバ 2 (DNS Server 2)		(オプション) スタ ティック ルート テー ブルの宛先ネットワー ク (Static Route Table Destination Network)	
(オプション) DNS サーバ 3 (DNS Server 2)		(オプション) 標準 サービスのルータアド レス (Standard Service Router Addresses)	

システム セットアップ ウィザードのワークシート			
プロパティ	値	プロパティ	値
(オプション) 時間の設定 (Time Settings)		(オプション) データトラフィック (Data Traffic)	
ネットワーク タイム プロトコル サーバ (Network Time Protocol Server)		デフォルトゲートウェイ (Default Gateway)	
(オプション) 外部プロキシの詳細 (External Proxy Details)		スタティック ルート テーブル名 (Static Route Table Name)	
プロキシ グループ名 (Proxy Group Name)		スタティック ルート テーブルの宛先ネット ワーク (Static Route Table Destination Network)	
プロキシサーバのアドレス (Proxy Server Address)		(オプション) WCCP 設定 (WCCP Settings)	
プロキシ ポート番号 (Proxy Port Number)		WCCP ルータ アドレス (WCCP Router Address)	
インターフェイスの詳細 (Interface Details)		WCCP ルータ パスフレーズ (WCCP Router Passphrase)	
管理 (M1) ポート (Management (M1) Port)		管理設定 (Administrative Settings)	
IPv4 アドレス (IPv4 Address) (必須) IPv6 アドレス (IPv6 Address) (オプション)		管理者パスフレーズ (Administrator Passphrase)	

システム セットアップ ウィザードのワークシート			
プロパティ	値	プロパティ	値
ネットワーク マスク (Network Mask)		システム アラート メールの送信先 (Email System Alerts To)	
ホスト名 (Hostname)		(オプション) SMTP リレー ホスト (SMTP Relay Host)	
(オプション) データ (P1) ポート (Data (P1) Port)			
IPv4 (オプション) IPv6 アドレス (IPv6 Address) (オプション)			
ネットワーク マスク (Network Mask)			
ホスト名 (Hostname)			

システム セットアップ ウィザード

Before you begin

- アプライアンスをネットワークとデバイスに接続します。 [アプライアンスの接続, on page 18](#)を参照してください。
- システム セットアップ ウィザードのワークシートを完成させます。 [設定情報の収集, on page 22](#)を参照してください。
- 仮想アプライアンスを設定する場合は、以下の手順に従います。
 - loadlicense コマンドを使用して、仮想アプライアンスのライセンスをロードします。詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。このドキュメントは、
<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html>から入手できます。

- HTTP、および/または HTTPS インターフェイスを有効にします（コマンドライン インターフェイス（CLI）で、`interfaceconfig` コマンドを実行します）。
- システムセットアップウィザードのセットアップ中に、スマートライセンスが有効になっている場合は、クラウドサービスの設定も有効になり、[クラウドサービスの設定（Cloud Services Settings）] ページにリダイレクトされます。
- システム セットアップ ウィザードで使用される各設定項目の参照情報は、[システム セットアップ ウィザードの参照情報, on page 26](#)に記載されています。

**Warning**

初めてアプライアンスをインストールする場合、または既存の設定を完全に上書きする場合にのみ、システム セットアップ ウィザードを使用してください。

Procedure

ステップ 1 ブラウザを開き、Secure Web Applianceの IP アドレスを入力します。初めてシステム セットアップ ウィザードを実行するときは、以下のデフォルトの IP アドレスを使用します。

`https://192.168.42.42:8443`

または

`http://192.168.42.42:8080`

ここで、192.168.42.42 はデフォルト IP アドレス、8080 は HTTP のデフォルトの管理ポートの設定、8443 は HTTPS のデフォルトの管理ポートです。

あるいは、アプライアンスが現在設定されている場合は、M1 ポートの IP アドレスを使用します。

ステップ 2 アプライアンスのログイン画面が表示されたら、アプライアンスにアクセスするためのユーザー名とパスワードを入力します。デフォルトで、アプライアンスには以下のユーザー名とパスワードが付属します。

- ユーザー名 : admin
- パスワード : ironport

ステップ 3 パスワードをただちに変更する必要があります。

ステップ 4 [システム管理（System Administration）] > [システム セットアップウィザード（System Setup Wizard）] を選択します。

アプライアンスがすでに設定されている場合は、設定がリセットされるという警告が表示されます。システム セットアップ ウィザードを続行するには、[ネットワーク設定のリセット（Reset Network Settings）] をオンにしてから [構成のリセット（Reset Configuration）] ボタンをクリックします。アプライアンスがリセットされ、ブラウザが更新されてアプライアンスのホーム画面が表示されます。

ステップ 5 エンドユーザー ライセンス契約が表示されたら、内容を読んで同意します。

ステップ 6 続行するには、[セットアップの開始 (Begin Setup)] をクリックします。

ステップ 7 必要に応じて、以下のセクションで提供されるリファレンステーブルを使用して、すべての設定を行います。[システムセットアップウィザードの参照情報](#), [on page 26](#)を参照してください。

ステップ 8 設定情報を確認してください。オプションを変更する必要がある場合は、そのセクションで[編集 (Edit)] をクリックします。

ステップ 9 [この設定をインストール (Install This Configuration)] をクリックします。

What to do next

設定がインストールされると、[次のステップ (Next Steps)] ページが表示されます。ただし、セットアップ中に設定した IP、ホスト名、DNS 設定によっては、この段階でアプライアンスへの接続が失われることがあります。「ページが見つかりません (Page Not Found)」というメッセージがブラウザに表示される場合は、新しいアドレス設定が反映されるように URL を変更し、ページをリロードします。その後、実行する必要があるポストセットアップタスクを続行します。

システムセットアップウィザードの参照情報

- ネットワーク/システムの設定, [on page 26](#)
- ネットワーク/ネットワーク インターフェイスおよび配線, [on page 29](#)
- 管理およびデータ トラフィックのネットワーク/ルートの設定, [on page 30](#)
- ネットワーク/透過的接続の設定, [on page 30](#)
- ネットワーク/管理の設定, [on page 31](#)

ネットワーク/システムの設定

プロパティ	説明
デフォルト システム ホスト名 (Default System Hostname)	システム ホスト名は、以下の領域でアプライアンスの識別に使用される完全修飾ホスト名です。 • コマンドライン インターフェイス (CLI) • システム アラート • エンドユーザ通知ページおよび確認ページ • Secure Web Applianceが Active Directory ドメインに参加するときに、マシンの NetBIOS 名を作成する場合 システム ホスト名はインターフェイスのホスト名と直接対応しておらず、クライアントがアプライアンスに接続するために使用されません。

プロパティ	説明
DNS サーバ (DNS Server(s))	• [インターネットのルートDNSサーバを使用 (Use the Internet's Root DNS Servers)] : アプライアンスがネットワーク上のDNSサーバにアクセスできない場合に、ドメイン名サービス ルックアップにインターネットのルート DNS サーバを使用することを選択できます。 Note インターネット ルート DNS サーバは、ローカル ホスト名を解決しません。アプライアンスでローカル ホスト名を解決する必要がある場合は、ローカル DNS サーバを使用して解決するか、CLI からローカル DNS に適切なスタティック エントリを追加する必要があります。 • [以下のDNSサーバを使用 (Use these DNS Servers)] : アプライアンスがホスト名の解決に使用できるローカル DNS サーバにアドレスを提供します。 これらの設定の詳細については、DNS の設定, on page 71 を参照してください。
NTP サーバ (NTP Server)	システムクロックをネットワークまたはインターネット上の他のサーバと同期させるために使用する、Network Time Protocol (NTP) サーバ。 デフォルトは、time.sco.cisco.com です。
タイム ゾーン	アプライアンスの場所に応じたタイムゾーン情報を提供します。メッセージヘッダーおよびログファイルのタイムスタンプに影響します。
アプライアンスの動作モード (Appliance Mode of Operation)	• 標準 : 標準的なオンプレミス ポリシーの適用に使用します。 • クラウド Web セキュリティ コネクタ : 主に、Cisco クラウド Web セキュリティ サービスにトラフィックをダイレクトし、ポリシーを適用して脅威から防御するために使用します。 • ハイブリッド Web セキュリティ : クラウドとオンプレミス ポリシーの適用および脅威防御のために、Cisco クラウド Web セキュリティ サービスと併用されます。 これらの動作モードの詳細については、操作モードの比較, on page 12 を参照してください。

ネットワーク/ネットワーク コンテキスト



Note 別のプロキシサーバを含むネットワークで Secure Web Applianceを使用する場合は、プロキシサーバのダウンストリームで、クライアントのできるだけ近くに Secure Web Applianceを配置することを推奨します。

プロパティ	説明
ネットワークには他の Web プロキシがありますか? (Is there another web proxy on your network?)	ネットワークに以下のような別のプロキシがあるかどうか。 トラフィックがパススルーする必要のある他のプロキシがネットワークにありますか。この場合、Secure Web Applianceのアップストリームになりますか。 両方とも該当する場合は、チェックボックスをオンにします。これにより、1つのアップストリーム プロキシのプロキシ グループを作成できます。後で、さらにアップストリーム プロキシを追加できます。
プロキシ グループ名 (Proxy group name)	アプライアンスでプロキシ グループの識別に使用される名前。
アドレス (Address)	アップストリーム プロキシ サーバーのホスト名または IP アドレス。
ポート (Port)	アップストリーム プロキシ サーバーのポート番号。

関連項目

- [アップストリーム プロキシ, on page 33](#)

ネットワーク/クラウド コネクタの設定

ページ名と設定を確認する必要があります。

設定	説明
クラウド Web セキュリティ プロキシ サーバー (Cloud Web Security Proxy Servers)	クラウド プロキシ サーバー (CPS) のアドレス (例: proxy1743.scansafe.net)。
失敗のハンドリング (Failure Handling)	AsyncOS がクラウド Web セキュリティ プロキシ への接続に失敗した場合、インターネットに [直接接続 (Connect directly)] するか、[要求をドロップ (Drop requests)] します。

設定	説明
Cloud Web Security 認証スキーム (Cloud Web Security Authorization Scheme)	トランザクションを認証する方式： - Secure Web Appliance 公開 IPv4 アドレス。 - 各トランザクションに含まれている認証キー。Cisco Cloud Web Security Portal 内で認証キーを生成できます。

ネットワーク/ネットワーク インターフェイスおよび配線

Secure Web Applianceの管理および（デフォルトで）プロキシ（データ）トラフィック用に使用される IP アドレス、ネットワーク マスク、ホスト名。

アプライアンス管理インターフェイスに接続するときに（または、M1 がプロキシデータに使用される場合はブラウザプロキシ設定で）、ここで指定したホスト名を使用できます。ただし、そのホスト名を組織の DNS に登録しておく必要があります。

設定	説明
イーサネット ポート (Ethernet Port)	（オプション）データ トラフィック用に個別のポートを使用する場合は、[ポートM1は管理目的でのみ使用（Use M1 Port For Management Only）] をオンにします。 M1 インターフェイスを管理トラフィック専用として設定する場合は、データ トラフィック用の P1 インターフェイスを設定する必要があります。また、管理トラフィックとデータ トラフィック用に異なるルートを定義する必要があります。ただし、管理トラフィックとデータ トラフィックの両方を M1 インターフェイスとして使用する場合でも、P1 インターフェイスを設定できます。 システム セットアップ ウィザードでは、P1 ポートのみをイネーブルにして設定できます。P2 インターフェイスをイネーブルにする場合は、システム セットアップ ウィザードを終了してから行う必要があります。
IP アドレス/ネットマスク (IP Address / Netmask)	このネットワークインターフェイス上の Secure Web Applianceを管理する際に使用する IP アドレスとネットワークマスク。
ホスト名 (Hostname)	このネットワークインターフェイス上の Secure Web Applianceを管理する際に使用するホスト名。

ネットワーク/レイヤ4トラフィック モニターの配線

プロパティ	説明
レイヤ4トラフィック モニター (Layer-4 Traffic Monitor)	「T」 インターフェイスに接続されている有線接続のタイプ： • デュプレックス タップ。T1 ポートは、着信と発信の両方のトラフィックを受信します。 • シンプレックス タップ。T1 ポートは（クライアントからインターネットへの）発信トラフィックを受信し、T2ポートは（インターネットからクライアントへの）着信トラフィックを受信します。 シスコでは、パフォーマンスおよびセキュリティを向上させることができるため、可能な限りシンプレックスを使用することを推奨します。

管理およびデータ トラフィックのネットワーク/ルートの設定



Note [ポートM1は管理目的でのみ使用（Use M1 port for management only）] をイネーブルにした場合、このセクションには、管理トラフィックとデータトラフィック用の個別のセクションが表示されます。それ以外の場合は1つの結合されたセクションが表示されます。

プロパティ	説明
デフォルトゲートウェイ (Default Gateway)	管理およびデータ インターフェイスを通過するトラフィックに使用するデフォルト ゲートウェイの IP アドレス。
スタティック ルート テーブル (Static Routes Table)	管理およびデータ トラフィック用のオプションのスタティック ルート。複数のルートを追加できます。 • 名前 (Name) : スタティック ルートの識別に使用する名前。 • 内部ネットワーク (Internal Network) : このルートのネットワーク上の宛先の IPv4 アドレス。 • 内部ゲートウェイ (Internal Gateway) : このルートのゲートウェイ IPv4 アドレス。ルート ゲートウェイは、それが設定されている管理インターフェイスまたはデータ インターフェイスと同じサブネット上に存在する必要があります。

ネットワーク/透過的接続の設定



Note デフォルトでは、クラウドコネクタはトランスペアレントモードで展開され、レイヤ4スイッチまたは WCCP バージョン 2 ルータと接続する必要があります。

プロパティ	説明
レイヤ4スイッチまたはデバイスなし (Layer-4 Switch or No Device)	Secure Web Applianceが透過リダイレクション用にレイヤ4スイッチに接続されていること、または透過リダイレクション デバイスを使用せず、クライアントがアプライアンスに明示的に要求を転送することを指定します。
WCCP v2 ルータ (WCCP v2 Router)	Secure Web Applianceが WCCP バージョン 2 対応ルータに接続されていることを指定します。 WCCP バージョン 2 ルータに接続する場合、少なくとも 1 つの WCCP サービスを作成する必要があります。この画面で、またはシステム セットアップ ウィザードの終了後に、標準サービスをイネーブルにでき、複数のダイナミック サービスを作成することもできます。 標準サービスをイネーブルにすると、ルータ セキュリティをイネーブルにして、パスフレーズを入力することもできます。ここで使用されるパスフレーズは、同じサービス グループ内のすべてのアプライアンスと WCCP ルータで使用する必要があります。 標準サービス タイプ (別名「Web キャッシュ」サービス) には、固定 ID「ゼロ」、固定リダイレクト方式「宛先ポート別」、固定宛先ポート「80」が割り当てられます。 ダイナミック サービス タイプでは、カスタム ID、ポート番号、およびリダイレクト オプションとロード バランシング オプションを定義できます。

ネットワーク/管理の設定

プロパティ	説明
管理者パスフレーズ (Administrator Passphrase)	管理のために Secure Web Applianceにアクセスするときに使用されるパスフレーズ。
システム アラートメールの送信先 (Email System Alerts To)	アプライアンスがシステム アラートを送信する宛先の電子メールアドレス。
SMTP リレー ホスト経由で電子メールを送信 (Send Email via SMTP Relay Host) (オプション)	AsyncOS がシステムで生成された電子メール メッセージの送信に使用できる、SMTP リレー ホストのアドレスとポート。 SMTP リレー ホストが定義されていない場合、AsyncOS は MX レコードにリストされているメール サーバを使用します。

プロパティ	説明
オートサポート (AutoSupport)	アプライアンスがシステムアラートと毎週のステータス レポートをシスコ カスタマー サポートに送信するかどうかを指定します。
SensorBase ネットワークに参加 (SensorBase Network Participation)	Cisco SensorBase ネットワークに参加するかどうかを指定します。参加する場合、制限付き参加または標準 (完全な) 参加を設定できます。デフォルトは標準です。 SensorBase ネットワークは、世界中の何百万ものドメインを追跡し、インターネット トラフィックのグローバルな監視リストを保持する脅威管理データベースです。SensorBase ネットワーク参加をイネーブルにすると、Secure Web Applianceは SensorBase ネットワーク データの価値を高めるために、HTTP 要求に関する匿名の統計情報をシスコに送信します。

セキュリティ/セキュリティ設定

オプション	説明
グローバルポリシーのデフォルトアクション (Global Policy Default Action)	システム セットアップ ウィザードの完了後、デフォルトで、すべての Web トラフィックをブロックするか、モニターするかを選択します。グローバル アクセス ポリシーのプロトコルとユーザー エージェントの設定を編集することで、後でこの動作を変更できます。デフォルトの設定は、トラフィックのモニターです。
L4 トラフィック モニター (L4 Traffic Monitor)	システム セットアップ ウィザードの完了後、デフォルトで、レイヤ 4 トラフィック モニターでモニターするか、疑わしいマルウェアをブロックするかを選択します。この設定は後で変更できます。デフォルトの設定は、トラフィックのモニターです。
使用許可コントロール (Acceptable Use Controls)	[使用許可コントロール (Acceptable Use Controls)]をイネーブルにするかどうかを指定します。 イネーブルにすると、使用許可コントロールにより、URL フィルタリングに基づいてポリシーを設定できます。また、アプリケーションの可視性と制御に加えて、セーフサーチの適用などの関連オプションを使用できるようになります。デフォルトの設定はイネーブルです。
評価フィルタリング (Reputation Filtering)	グローバルポリシー グループに対して Web レピュテーション フィルタリングをイネーブルにするかどうかを指定します。 Web 評価フィルタは、Web サーバーの動作を分析し、評価スコアを URL に割り当て、URL ベースのマルウェアを含む可能性を判定するセキュリティ機能です。デフォルトの設定はイネーブルです。

オプション	説明
マルウェアとスパイウェアのスキャン (Malware and Spyware Scanning)	Webroot、McAfee、またはSophosによるマルウェアやスパイウェアのスキャンをイネーブルにするかどうかを指定します。デフォルトの設定では、3つのオプションがすべて有効になります。クラウドポリシーで通常使用可能なサービスに対応して、ほとんどのセキュリティサービスは自動的に有効/無効になります。同様に、ポリシー関連のデフォルトは適用されません。少なくとも1つのスキャンオプションをイネーブルにする必要があります。 オプションをイネーブルにした場合は、検出されたマルウェアをモニターするかブロックするかも選択します。デフォルトの設定は、マルウェアのモニターです。 システムセットアップウィザードを完了後、マルウェア スキャンを追加設定することもできます。
Cisco データ セキュリティ フィルタリング (Cisco Data Security Filtering)	Cisco データ セキュリティ フィルタをイネーブルにするかどうかを指定します。 イネーブルにすると、Cisco データ セキュリティ フィルタはネットワークから発信されるデータを評価し、ユーザーは、特定タイプのアップロード要求をブロックするシスコ データ セキュリティ ポリシーを作成できます。デフォルト設定はイネーブルです。

アップストリーム プロキシ

Web プロキシは、Web トラフィックを宛先 Web サーバに直接転送することも、ルーティングポリシーを使用して外部アップストリーム プロキシにリダイレクトすることもできます。

- [アップストリーム プロキシのタスクの概要, on page 33](#)
- [アップストリーム プロキシのプロキシ グループの作成, on page 34](#)

アップストリーム プロキシのタスクの概要

タスク	詳細情報
• Cisco Secure Web Appliance のアップストリームに外部プロキシに接続する。	アプライアンスの接続, on page 18。
• アップストリーム プロキシのプロキシ グループを作成して設定する。	アップストリーム プロキシのプロキシ グループの作成, on page 34。
• プロキシ グループのルーティング ポリシーを作成し、アップストリームプロキシにルーティングするトラフィックを管理する。	インターネット要求を制御するポリシーの作成, on page 362

アップストリーム プロキシのプロキシ グループの作成

Procedure

ステップ 1 [ネットワーク (Network)] > [アップストリームプロキシ (Upstream Proxies)] を選択します。

ステップ 2 [グループの追加 (Add Group)] をクリックします。

ステップ 3 プロキシ グループの設定を完了させます。

プロパティ	説明
名前 (Name)	ルーティング ポリシーなどでアプライアンス上のプロキシ グループの識別に使用される名前など。
プロキシ サーバ (Proxy Servers)	グループのプロキシ サーバのアドレス、ポート、再接続試行 (プロキシが応答しない場合)。必要に応じて、各プロキシ サーバの行を追加または削除できます。 Note 同じプロキシサーバを複数回追加して、プロキシグループのプロキシ間に不均衡に負荷を分散できます。

プロパティ	説明
ロード バランシング (Load Balancing)	複数のアップストリームプロキシ間のロードバランス要求のために Web プロキシが使用する方法。次から選択します。 • [なし (フェールオーバー) (None (failover))]。Web プロキシは、グループ内の 1 つの外部プロキシにトランザクションを送信します。一覧表示されている順序でプロキシへの接続を試みます。あるプロキシに到達できない場合、Web プロキシはリストの以下のプロキシに接続を試みます。 • [最少接続 (Fewest connections)]。Web プロキシは、グループ内のさまざまなプロキシにおけるアクティブな要求の数を追跡し、その時点で接続数が最も少ないプロキシにトランザクションを送信します。 • [ハッシュベース (Hash based)]。[最も長い間使われていない (Least recently used)]。すべてのプロキシがアクティブである場合、Web プロキシは、最も長い間トランザクションを受信していないプロキシにトランザクションを送信します。この設定はラウンドロビンに似ています。異なる点は、Web プロキシが、異なるプロキシグループのメンバーであるプロキシが受信したトランザクションも考慮するということです。つまり、あるプロキシが複数のプロキシグループのリストに含まれている場合でも、[最も長い間使われていない (least recently used)] オプションによってそのプロキシが過負荷になることはほとんどありません。 • [ラウンドロビン (Round robin)]。Web プロキシは、リストに記載されている順序で、グループ内のすべてのプロキシにトランザクションを均等に割り当てます。 Note 複数のプロキシを定義するまで、[ロードバランシング (Load Balancing)] オプションはグレー表示されます。
失敗のハンドリング (Failure Handling)	このグループのすべてのプロキシが失敗した場合のデフォルト アクションを指定します。次から選択します。 • [直接接続 (Connect directly)]。宛先サーバに直接、要求を送信します。 • [要求をドロップ (Drop requests)]。要求を転送しないで、廃棄します。

ステップ 4 変更を送信し、保存します。

What to do next

- [ポリシーの作成, on page 369](#)

ネットワーク インターフェイス

- [IP アドレスのバージョン, on page 36](#)
- [ネットワーク インターフェイスのイネーブル化または変更, on page 37](#)

IP アドレスのバージョン

標準モードでは、Cisco Secure Web Appliance は大部分の場合に IPv4 と IPv6 アドレスをサポートします。



Note クラウドコネクタモードでは、Secure Web Appliance は IPv4 のみをサポートします。

DNS サーバは、IPv4 と IPv6 の両方のアドレスと共に結果を返すことができます。DNS の設定項目には [IP アドレスバージョン設定 (IP Address Version Preference)] が含まれているので、以下の場合における AsyncOS の動作を設定できます。

インターフェイス/サービス	IPv4	IPv6	注記
M1 インターフェイス	必須	オプション	IPv6 アドレスを使用するには、デフォルトの IPv6 ゲートウェイを定義する IPv6 ルーティングテーブルが必要です。ネットワークによっては、ルーティングテーブルで IPv6 スタティックルートも指定する必要があります。
P1 インターフェイス	オプション	オプション	P1 インターフェイスに IPv6 アドレスが設定されており、アプライアンスが分割ルーティング（個別の管理ルートとデータルート）を使用している場合、P1 インターフェイスは管理ルート上に設定された IPv6 ゲートウェイを使用できません。代わりに、データルーティングテーブルに IPv6 ゲートウェイを指定します。
P2 インターフェイス	オプション	オプション	—
データ サービス	サポート対象	サポート対象	—
制御および管理サービス	サポート対象	一部サポートあり	イメージ（エンドユーザ通知ページのカスタム ロゴなど）には IPv4 が必要です。
AnyConnect セキュア モビリティ (MUS)	サポート対象	非対応	—

関連項目

- [ネットワーク インターフェイスのイネーブル化または変更, on page 37](#)
- [DNS の設定, on page 71](#)

ネットワーク インターフェイスのイネーブル化または変更

- インターフェイス IP アドレスの追加または変更
- レイヤ 4 トラフィック モニタの配線タイプの変更
- 管理およびデータ トラフィックの分割ルーティングのイネーブル化

Procedure

ステップ 1 [ネットワーク (Network)] > [インターフェイス (Interfaces)] を選択します。

ステップ 2 [設定の編集 (Edit Settings)] をクリックします。

ステップ 3 インターフェイスのオプションを設定します。

Note

Data 1 および Data 2 インターフェイスはサポートされていません。代わりに P1 または P2 インターフェイスを使用できます。

オプション	説明
インターフェイス (Interfaces)	M1、P1、または P2 インターフェイスの新しい IPv4 または IPv6 アドレス、ネットマスク、ホスト名の詳細を追加するか、既存の詳細を変更します。 • M1 : AsyncOS には M1 (管理) ポートの IPv4 アドレスが必要です。IPv4 アドレスに加えて、IPv6 アドレスも指定できます。デフォルトで、管理インターフェイスはアプライアンスおよび Web プロキシ (データ) のモニタリングを管理するために使用されます。ただし、管理用途専用の M1 ポートを設定できます。 • P1 および P2 : データ ポートの IPv4 アドレス、IPv6 アドレス、または両方を使用します。データ インターフェイスは Web プロキシによるモニタリングとレイヤ 4 トラフィック モニタによるブロッキング (オプション) で使用されます。これらのインターフェイスを設定して、DNS、ソフトウェア アップグレード、NTP、および traceroute データ トラフィックなどの発信サービスをサポートすることもできます。 Note 管理およびデータ インターフェイスをすべて設定する場合、それぞれに異なるサブネット上の IP アドレスを割り当てる必要があります。 Note 分割ルーティングが有効になっている場合、管理インターフェイスはスマートライセンスポータルと通信できません。Secure Web Appliance をスマートライセンスポータルに登録するには、データインターフェイスを選択します。 Note 分割ルーティングが設定されている場合、Secure Web Appliance はデータインターフェイスを使用して外部 DLP サーバーに接続し、管理インターフェイスは管理トラフィックのみに制限されます。これにより、トラフィックを DLP サーバーにルーティングする間、すべての DLP トラフィックが管理トラフィックではなくデータトラフィックと見なされます。 たとえば、DLP アドレスでフィルタリングされる P1 インターフェイスと M1 インターフェイスを持つ 2 つのパケットキャプチャがある場合、DLP トラフィックは両方のインターフェイスで検出されます。これは、キープアライブパケットを DLP サーバーに送信する管理インターフェイスと、データインターフェイスからの DLP トラフィックによるものです。

オプション	説明
管理サービス用の 分離ルーティング (Separate Routing for Management Services)	M1 を管理トラフィック専用 に制限して、データ トラフィック用に別のポートを使用する必要がある場合は、[M1ポートをアプライアンス管理サービスのみに限定する (Restrict M1 port to appliance management services only)] をオンにします。 Note M1 を管理トラフィック専用にする場合は、別のサブネットにプロキシ トラフィック用のデータ インターフェイスを少なくとも 1 つ設定します。管理トラフィックとデータ トラフィック用に異なるルートを定義してください。 Note AsynOS バージョン 15.0 では、M1 および P1 ゲートウェイは、それぞれのサブネット内に個別で一意のゲートウェイを持つ必要があります。M1 および P1 インターフェイスがサブネットにない静的ゲートウェイを指すようにネットワークルートを変更してから AsynOS バージョン 15.01 にアップグレードすると、Cisco Secure Web Appliance (SWA) はネットワーク接続とユーザー補助を失います。このような設定不備が発生した場合、システムを再起動すると SWA が復元され、CLI または GUI に再びアクセスできるようになります。
アプライアンス管理サービス (Appliance Management Services)	以下のネットワーク プロトコルの使用をイネーブルまたはディセーブルにして、そのデフォルトのポート番号を指定します。 • FTP : デフォルトでディセーブルになります。 • SSH • HTTP • HTTPS また、HTTP トラフィックの HTTPS へのリダイレクションをイネーブルまたはディセーブルにできます。

ステップ 4 変更を送信し、保存します。

What to do next

IPv6 アドレスを追加する場合は、IPv6 ルーティング テーブルを追加します。

関連項目

- [アプライアンスの接続, on page 18.](#)
- [IP アドレスのバージョン, on page 36](#)
- [TCP/IP トラフィック ルートの設定, on page 55](#)

ネットワーク インターフェイス カードの設定

この章で説明する内容は、次のとおりです。

- [イーサネット インターフェイスのメディア設定 \(40 ページ\)](#)
- [ネットワーク インターフェイス カードのペアリングおよびチーミング \(41 ページ\)](#)
- [etherconfig コマンドを使った NIC ペアリングのイネーブル化 \(42 ページ\)](#)
- [NIC ペアリングを設定するためのガイドライン \(48 ページ\)](#)

イーサネット インターフェイスのメディア設定

etherconfig コマンドを使用して、イーサネット インターフェイスのメディア設定にアクセスできます。個々のイーサネット インターフェイスが現在の設定と共に一覧表示されます。インターフェイスを選択すると、適切なメディア設定が表示されます。

etherconfig を使ったイーサネット インターフェイスのメディア設定の編集

etherconfig コマンドを使って、イーサネット インターフェイスのデュプレックス設定（全二重/半二重）や速度（10/100/1000 Mbps）を設定できます。デフォルトでは、インターフェイスはメディア設定を自動的に選択します。これはオーバーライドできます。



- (注) 「[セットアップとインストール](#)」のトピックの説明に従って GUI のシステム設定ウィザード（またはコマンドライン インターフェイスの **systemsetup** コマンド）を実行し、変更を確定していれば、アプライアンス上でデフォルトのイーサネット インターフェイス設定が構成されているはずです。

メディア設定の編集例

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
[]> MEDIA
Ethernet interfaces:
1. Management (Autoselect: <1000baseT full-duplex>) 00:50:56:87:a6:46
2. P1 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:1c:3f
3. P2 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:6a:42
4. T1 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:1c:3f
5. T2 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:fc:01

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>
```

ネットワーク インターフェイス カードのペアリングおよびチーミング

NIC ペアリングで 2 つの物理データポートを組み合わせることにより、NIC からアップストリームのイーサネットポートへのデータパスに障害が発生した場合に、バックアップイーサネットインターフェイスを提供できます。ペアリングでは、基本的に各イーサネットインターフェイスをプライマリ インターフェイスおよびバックアップ インターフェイスとして設定します。プライマリインターフェイスに障害が発生した場合（NIC とアップストリームノード間のキャリアが途切れた場合など）は、バックアップインターフェイスがアクティブになり、アラートが送信されます。プライマリインターフェイスが有効になると、このインターフェイスがアクティブになります。この製品のマニュアルでは、「NIC ペアリング」と「NIC チーミング」は同義語です。



Note NIC ペアリングは、S170、S190、および S195 Web ゲートウェイでは使用できません。

十分な数のデータポートがあれば、複数の NIC ペアを作成できます。ペアを作成するときは、任意のデータポートを組み合わせることができます。次に例を示します。

- Data 1 と Data 2
- Data 3 と Data 4
- Data 2 と Data 3

一部の Web ゲートウェイは、光ファイバネットワーク インターフェイス オプションを備えています。その場合は、各 Web ゲートウェイ上の使用可能なインターフェイスのリストに 2 つの追加イーサネット インターフェイス（Data 3 と Data 4）が表示されます。異種混在構成では、これらのギガビット光ファイバインターフェイスは、銅線（Data 1、Data 2、および Management）インターフェイスとペアにすることができます。

Secure Web Appliance は、NIC ペアリングインターフェイスのパケットキャプチャをサポートしていません。パケットキャプチャは、アクティブなインターフェイスにのみ適用されます。たとえば、P1 と P2 の両方がペアになっている場合、P1 と P2 のどちらもユーザーインターフェイスまたは CLI で設定されません。

NIC ペアリングと VLAN

VLAN（「[仮想ローカルエリアネットワーク（VLAN）](#)」を参照）は、プライマリインターフェイスでのみ許可されます。

NIC ペアの名前

NIC ペアを作成するときは、ペアの名前を指定する必要があります。バージョン 4.5 よりも前の AsyncOS で作成した NIC ペアには、アップグレード後、自動的に「Pair 1」というデフォルト名が指定されます。

NIC ペアリングで生成されたアラートは、特定の NIC ペアをその名前で参照します。

NIC ペアリングと既存のリスナー

リスナーが割り当てられたインターフェイスでNIC ペアリングをイネーブルにすると、バックアップインターフェイスに割り当てられた全リスナーの削除、再割り当て、ディセーブル化のいずれかを選択するように求められます。

etherconfig コマンドを使った NIC ペアリングのイネーブル化



Note NIC ペアリングは、S170、S190、および S195 Web ゲートウェイでは使用できません。

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> PAIRING
Paired interfaces:
Choose the operation you want to perform:
- NEW - Create a new pairing.
[]> NEW
Please enter a name for this pair (Ex: "Pair 1"):
[]> DP1

1. P1
2. P2
Enter the name or number of the primary ethernet interface you wish bind to.
[]> 1

1. P2
2. T1
3. T2
Enter the name or number of the backup ethernet interface you wish to pair.
[]> 2

Paired interfaces:
1. DP1:
    Primary (P1)
    Backup (T1)

Choose the operation you want to perform:
- NEW - Create a new pairing.
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
example.com> commit
Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
Warning: Processing of network configuration changes might
cause a brief interruption in network availability.
```

```

Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Thu Sep 24 01:40:34 2020 MST
example.com> interfaceconfig

Currently configured interfaces:
1. Management (10.10.192.167/24 on Management: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]> NEW
Ethernet interface:
1. Management
2. DP1
3. P2
[1]> 2
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
IPv4 Address (Ex: 192.168.1.2 ):
[]> 10.10.102.66
Netmask (Ex: "24", "255.255.255.0" or "0xffffffff00"):
[255.255.255.0]> 27
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
Hostname:
[]> example.com
Currently configured interfaces:
1. Management (10.10.192.167/24 on Management: example.com)
2. P1 (10.10.102.66/27 on DP1: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]>
example.com>example.com> commit
Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
Warning: Processing of network configuration changes might
cause a brief interruption in network availability.
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Thu Sep 24 01:43:18 2020 MST
example.com> exitexample.com:rtestuser 53] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:50:56:87:a6:46
hwaddr 00:50:56:87:a6:46
inet 10.10.192.167 netmask 0xffffffff00 broadcast 10.10.192.255
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:50:56:87:1c:3f
hwaddr 00:50:56:87:1c:3f
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)

```

P1 インターフェイスの停止

```

        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:50:56:87:6a:42
    hwaddr 00:50:56:87:6a:42
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:50:56:87:1c:3f
    hwaddr 00:50:56:87:dd:89
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:50:56:87:fc:01
    hwaddr 00:50:56:87:fc:01
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=600003<RXCSUM, TXCSUM, RXCSUM_IPV6, TXCSUM_IPV6>
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
    inet 127.0.0.1 netmask 0xff000000
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
    groups: lo
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:50:56:87:1c:3f
    inet6 fe80::250:56ff:fe87:a646%lagg0 prefixlen 64 scopeid 0x7
    inet 10.10.102.66 netmask 0xffffffe0 broadcast 10.10.102.95
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
    media: Ethernet autoselect
    status: active
    groups: lagg
    laggproto failover lagghash 12,13,14
    laggport: nic1 flags=5<MASTER,ACTIVE>
    laggport: nic3 flags=0<>
example.com:rtestuser 54]

```

P1 インターフェイスの停止

P1 と T1 はペアになっており、DP1 と名付けられています。P1 が停止すると、T1 がアクティブになります。次の例では、**lagg0** インターフェイスを参照します。

```

example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[ ]> PAIRING
Paired interfaces:
1. DP1:
    Backup (T1) Standby, Link is up
    Primary (P1) Active, Link is up
2. DP2:
    Backup (T2) Standby, Link is up
    Primary (P2) Active, Link is up

Choose the operation you want to perform:

```

```
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
example.com>
example.com> exit

example.com:rtestuser 115] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:50:56:87:a6:46
    hwaddr 00:50:56:87:a6:46
    inet 10.10.192.167 netmask 0xfffff00 broadcast 10.10.192.255
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:50:56:87:1c:3f
    hwaddr 00:50:56:87:1c:3f
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:50:56:87:6a:42
    hwaddr 00:50:56:87:6a:42
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:50:56:87:1c:3f
    hwaddr 00:50:56:87:dd:89
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:50:56:87:6a:42
    hwaddr 00:50:56:87:fc:01
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=600003<RXCSUM, TXCSUM, RXCSUM_IPV6, TXCSUM_IPV6>
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
    inet 127.0.0.1 netmask 0xff000000
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    ether 00:50:56:87:dd:89
    nd6 options=1<PERFORMNUD>
    id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
    maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
    root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
    member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
        ifmaxaddr 0 port 5 priority 128 path cost 20000
    member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
```

```

        ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:50:56:87:1c:3f
inet 10.10.102.66 netmask 0xffffffe0 broadcast 10.10.102.95
nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
media: Ethernet autoselect
status: active
laggproto failover lagghash l2,l3,l4
laggport: nic1 flags=5<MASTER,ACTIVE>
laggport: nic3 flags=0<>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:50:56:87:6a:42
inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
inet 10.10.166.66 netmask 0xffffffe0 broadcast 10.10.166.95
nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
media: Ethernet autoselect
status: active
laggproto failover lagghash l2,l3,l4
laggport: nic2 flags=5<MASTER,ACTIVE>
laggport: nic4 flags=0<>
example.com:rtestuser 116]
example.com:rtestuser 116] ifconfig nic1 down
example.com:rtestuser 117] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:50:56:87:a6:46
hwaddr 00:50:56:87:a6:46
inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nic1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:50:56:87:1c:3f
hwaddr 00:50:56:87:1c:3f
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:50:56:87:6a:42
hwaddr 00:50:56:87:6a:42
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:50:56:87:1c:3f
hwaddr 00:50:56:87:dd:89
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
ether 00:50:56:87:6a:42
hwaddr 00:50:56:87:fc:01
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
options=600003<RXCSUM, TXCSUM, RXCSUM_IPV6, TXCSUM_IPV6>
inet6 ::1 prefixlen 128

```

```

        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xffffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash 12,13,14
        laggport: nic1 flags=1<MASTER>
        laggport: nic3 flags=4<ACTIVE>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xffffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash 12,13,14
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 118]

```

P1 インターフェイスの起動

```

example.com:rtestuser 118] ifconfig nic1 up
example.com:rtestuser 119] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xfffffff0 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>

```



```

ether 00:50:56:87:1c:3f
hwaddr 00:50:56:87:dd:89
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
ether 00:50:56:87:6a:42
hwaddr 00:50:56:87:fc:01
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
options=600003<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
inet 127.0.0.1 netmask 0xff000000
nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 00:50:56:87:dd:89
nd6 options=1<PERFORMNUD>
id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
ifmaxaddr 0 port 5 priority 128 path cost 20000
member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
ether 00:50:56:87:1c:3f
inet 10.10.102.66 netmask 0xffffffe0 broadcast 10.10.102.95
nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
media: Ethernet autoselect
status: active
laggproto failover lagghash 12,13,14
laggport: nic1 flags=5<MASTER,ACTIVE>
laggport: nic3 flags=0<>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
ether 00:50:56:87:6a:42
inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
inet 10.10.166.66 netmask 0xffffffe0 broadcast 10.10.166.95
nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
media: Ethernet autoselect
status: active
laggproto failover lagghash 12,13,14
laggport: nic2 flags=5<MASTER,ACTIVE>
laggport: nic4 flags=0<>
example.com:rtestuser 120]
example.com:rtestuser 120]

```

NIC ペアリングを設定するためのガイドライン

M2、Data 1、Data 2 は、プライマリまたはセカンダリとして使用したり、IP アドレスで設定したりできません。

表 2:

ポート	IP アドレスとして設定	操作	対処方法	分割ルーティング有効	
				プライマリ	セカンダリ
P1 (プロキシ)	対応	有効	着信と発信の両方に対応するネットワークに P1 を接続します。 。	P1 を NIC ペアリングのプライマリとして選択できます (注) P2 をプライマリとして選択した場合は、P1 の IP アドレスを削除する必要があります。	P2、T1、T2
P1 + P2 (プロキシ)	対応	有効	P1 を内部ネットワークに接続し、 P2 をインターネットに接続します。	P2 をプライマリとして、P1 をセカンダリとして選択した場合は、P1 の IP アドレスを削除する必要があります。 NIC ペアリング中に、IP を削除するように求められます。	T1、T2
T1 (トラフィックモニタリング)	非対応	デュプレックススタップ	1 本のケーブルですべての着信および発信トラフィックに対応します。	N/A	該当なし

ポート	IP アドレスとして設定	操作	対処方法	分割ルーティング有効	
				プライマリ	セカンダリ
T1 + T2 (トラフィックモニタリング)	対応	シンプルタッ プ	1 本のケーブルでインターネットに宛てたすべてのパケットに対応し (T1)、もう 1 本のケーブルでインターネットから着信するすべてのパケットに対応します (T2)。	N/A	該当なし



(注) P1 の IP を削除することを選択した場合、P1 は分割ルーティングで設定されません。P2 または作成された NIC ペアに IP アドレスが割り当てられると、P2 のみが設定された状態で分割ルーティングが有効になります。リンクアグリゲーション (LAGG) インターフェイスは、IP アドレスがプライマリ (P2) または NIC ペアに割り当てられない限り表示されません。プライマリ (P2) または NIC ペアに IP アドレスが割り当てられると、LAGG インターフェイスが作成されます。

ハイ アベイラビリティを実現するためのフェールオーバー グループの設定

共通アドレス冗長プロトコル (CARP) を使用すると、Secure Web Appliance ではネットワーク上の複数のホストで IP アドレスを共有できるようになります。これにより IP 冗長性が実現され、それらのホストから提供されるサービスのハイアベイラビリティを確保できます。

フェールオーバーはプロキシ サービスでのみ使用できます。フェールオーバー グループが作成されると、プロキシは動的にフェールオーバー インターフェイスにバインドします。したがって、プロキシが何らかの理由でダウンすると、フェールオーバーがトリガーされます。

CARP には、ホスト用の 3 種類のステータスがあります。

- primary : 各フェールオーバーグループのプライマリホストは 1 つだけです。
- backup
- init

CARP フェールオーバーグループ内のプライマリホストは、ローカルネットワークにアドバタイズメントを定期的に送信して、バックアップホストにまだ活動中であることを知らせます（このアドバタイズメント間隔は **Secure Web Appliance** で設定できます）。バックアップホストが（プロキシのダウン、**Secure Web Appliance** のダウンまたはネットワークからの切断が原因で）指定した期間中にプライマリからアドバタイズメントを受信しなかった場合は、フェールオーバーがトリガーされ、いずれかのバックアップがプライマリの役割を引き継ぎます。

プライマリ **Secure Web Appliance** からのアドバタイズメントは、次の条件を満たす場合、残りのバックアップホストに到達しません。

- ネットワークまたはインターフェイスが使用不可
- OS の正常性と可用性



Note **Secure Web Appliance** の高可用性機能を使用するには、アプリケーション セントリック インフラストラクチャ（ACI）でデータプレーン IP ラーニングを無効にします。



Note アプライアンス間のロードバランシング方式として高可用性を使用することはできません。デバイス間のトラフィックをロードバランシングするには、WCCP またはハードウェア ロードバランサを使用します。



Note フェールオーバーグループ構成での NIC ペ어링はサポートされていません。

次に、高可用性スイッチオーバーの原因となる設定を示します。

- 認証レールの追加、削除、または更新
- ISE 設定の追加、削除、または更新
- HTTPS 証明書の追加または更新
- ログレベルの更新（プロキシログ）
- 透過的なリダイレクト設定の更新
- FTP プロキシの有効化、無効化、または更新
- SOCKS プロキシの有効化、無効化、または更新
- PAC ファイルの追加または変更
- アプライアンスからのインターフェイスの追加または削除
- フェールオーバーグループの追加または更新

- アップストリームプロキシの有効化または無効化
- WTT (Web Traffic Tap) の有効化または無効化

フェールオーバー グループの追加

Before you begin

- このフェールオーバー グループ専用使用する仮想 IP アドレスを特定します。クライアントはこの IP アドレスを使用して、明示的な転送プロキシモードでフェールオーバー グループに接続します。
- 以下のパラメータに対して、フェールオーバー グループ内のすべてのアプライアンスに同じ値を設定します。
 - フェールオーバー グループ ID (Failover Group ID)
 - ホスト名 (Hostname)
 - 仮想 IP アドレス (Virtual IP Address)
- 仮想アプライアンスにこの機能を設定する場合は、各アプライアンス固有の仮想スイッチと仮想インターフェイスが無差別モードを使用するように設定されていることを確認します。詳細については、各自の仮想ハイパーバイザのマニュアルを参照してください。

Procedure

- ステップ 1** [ネットワーク (Network)] > [ハイアベイラビリティ (High Availability)] を選択します。
- ステップ 2** [フェールオーバーグループの追加 (Add Failover Group)] をクリックします。
- ステップ 3** [フェールオーバーグループ ID (Failover Group ID)] に 1 ~ 255 の値を入力します。
- ステップ 4** (任意) [説明 (Description)] に説明を入力します。
- ステップ 5** [ホスト名 (Hostname)] にホスト名を入力します (www.example.com など)。
- ステップ 6** [仮想 IP アドレスとネットマスク (Virtual IP Address and Netmask)] に値を入力します。例: 10.0.0.3/24 (IPv4) または 2001:420:80:1::5/32 (IPv6)。
- ステップ 7** [インターフェイス (Interface)] メニューからオプションを選択します。[インターフェイスの自動選択 (Select Interface Automatically)] オプションを選択すると、指定した IP アドレスに基づいてインターフェイスが選択されます。

Note

[インターフェイスの自動選択 (Select Interface Automatically)] オプションを選択しない場合は、指定した仮想 IP アドレスと同じサブネット内のインターフェイスを選択する必要があります。

- ステップ 8** 優先順位を選択します。[プライマリ (Primary)] をクリックし、優先順位を 255 に設定します。または、[バックアップ (Backup)] を選択し、[優先順位 (Priority)] フィールドに 1 (最下位) ~ 254 の優先順位を入力します。

- ステップ 9** (任意)。サービスに対してセキュリティをイネーブルにするには、[サービスのセキュリティ有効化 (Enable Security Service)] チェックボックスをオンにし、共有シークレットとして使用する文字列を [共有シークレット (Shared Secret)] と [共有シークレットの再入力 (Retype Shared Secret)] フィールドに入力します。

Note

共有シークレット、仮想 IP、フェールオーバー グループ ID は、フェールオーバー グループ内のすべてのアプライアンスで同一でなければなりません。

- ステップ 10** [アドバタイズメントの間隔 (Advertisement Interval)] フィールドに、アベイラビリティをアドバタイズするホスト間の遅延を秒単位 (1 ~ 255) で入力します。

- ステップ 11** 変更を送信し、保存します。

What to do next

関連項目

- [フェールオーバーの問題, on page 744](#)

高可用性グローバル設定の編集

Procedure

- ステップ 1** [ネットワーク (Network)] > [ハイアベイラビリティ (High Availability)] を選択します。
- ステップ 2** [高可用性グローバル設定 (High Availability Global Settings)] 領域で、[設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** [フェールオーバー処理 (Failover Handling)] メニューからオプションを選択します。
- [プリエンプティブ (Preemptive)] : 使用可能な場合、優先順位が最も高いホストが制御を担います。
 - [プリエンプティブでない (Non-preemptive)] : より優先順が高いホストが使用可能になった場合でも、現在制御を担っているホストが制御を続行します。
- ステップ 4** [送信 (Submit)] をクリックします。または、[キャンセル (Cancel)] をクリックして変更を破棄します。

フェールオーバー グループのステータスの表示

[ネットワーク (Network)] > [ハイアベイラビリティ (High Availability)] を選択します。
[フェールオーバーグループ (Failover Groups)] 領域に現在のフェールオーバー グループが表示されます。[ステータスの更新 (Refresh Status)] をクリックすると、表示を更新できます。
また、[ネットワーク (Network)] > [インターフェイス (Interfaces)] または [レポート (Report)]

>[システム ステータス (System Status)] を選択すると、フェールオーバーの詳細を表示できます。

Web プロキシ データに対する P2 データ インターフェイスの使用

デフォルトでは、イネーブルになっている場合でも、Web プロキシは P2 で要求をリスンしません。ただし、Web プロキシデータをリスンするように P2 を設定できます。



Note

advancedproxyconfig > miscellaneous CLI コマンドを使用して、クライアント要求をリスンするために P2 をイネーブルにする場合、発信トラフィックに P1 を使用するか、P2 を使用するかを選択できます。発信トラフィックに P1 を使用するには、データ トラフィックのデフォルトルートを変更して、P1 インターフェイスが接続されている以下の IP アドレスを指定します。

Before you begin

P2 をイネーブルにします (P1 がイネーブルになっていない場合は P1 もイネーブルにする必要があります) ([ネットワーク インターフェイスのイネーブル化または変更, on page 37](#)を参照)。

Procedure

ステップ 1 CLI にアクセスします。

ステップ 2 advancedproxyconfig > miscellaneous コマンドを使用して、必要なエリアにアクセスします。

```
example.com> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
```

ステップ 3 []> miscellaneous

ステップ 4 下記の質問が表示されるまで、Enter キーを押して各質問をパスします。

```
Do you want proxy to listen on P2?
```

この質問に対して「y」を入力します。

ステップ 5 Enter キーを押して、残りの質問をパスします。

ステップ 6 変更を保存します。

What to do next

関連項目

- [アプライアンスの接続, on page 18。](#)
- [TCP/IP トラフィック ルートの設定, on page 55。](#)
- [トランスペアレント リダイレクションの設定, on page 58](#)

TCP/IP トラフィック ルートの設定

ルートは、ネットワーク トラフィックの送信先（ルーティング先）を指定するために使用されます。Secure Web Applianceは、以下の種類のトラフィックをルーティングします。

- **データ トラフィック。** Web を参照しているエンドユーザからの Web プロキシが処理するトラフィック。
- **管理トラフィック。** Web インターフェイスを介してアプライアンスを管理することによって作成されるトラフィック、およびアプライアンスが管理サービス（AsyncOS のアップグレード、コンポーネントのアップデート、DNS、認証など）用に作成するトラフィック。

デフォルトでは、どちらのトラフィックも、すべての設定済みネットワーク インターフェイス用に定義されたルートを使用します。ただし、管理トラフィックが管理ルーティングテーブルを使用し、データ トラフィックがデータ ルーティング テーブルを使用するように、ルーティングを分割することを選択できます。これらのトラフィックはそれぞれ以下のように分割されます。

管理トラフィック	データ トラフィック
• WebUI • SSH • SNMP • NTLM 認証（ドメインコントローラによる） • Syslogs • FTP プッシュ • DNS（設定可能） • アップデート/アップグレード/機能キー（設定可能）	• HTTP • HTTPS • FTP • WCCP ネゴシエーション • 外部 DLP サーバによる ICAP 要求 • DNS（設定可能） • アップデート/アップグレード/機能キー（設定可能） • LDAP/NTLM 認証（ドメインコントローラにより設定可能）

[ネットワーク (Network)] > [ルート (Routes)] ページのセクションの数は、分割ルーティングがイネーブルかどうかに応じて決まります。

- **管理トラフィックとデータ トラフィック用の個別のルート設定セクション**（分割ルーティングがイネーブルの場合）。管理インターフェイスを管理トラフィック専用を使用する場合（[M1ポートをアプライアンス管理サービスのみに限定する（Restrict M1 port to appliance management services only）] がイネーブルの場合）、このページには、ルートを入力する 2 つのセクション（管理トラフィック用とデータ トラフィック用）が表示されます。
- **すべてのトラフィックに対して 1 つのルート設定セクション**（分割ルーティングがディセーブルの場合）。管理トラフィックとデータ トラフィックの両方に管理インターフェイスを使用する場合（[M1ポートをアプライアンス管理サービスのみに限定する（Restrict M1 port to appliance management services only）] がディセーブルの場合）、このページには、Secure Web Applianceから送信されるすべてのトラフィック（管理トラフィックとデータ トラフィックの両方）のルートを入力する 1 つのセクションが表示されます。



Note

ルート ゲートウェイは、それが設定されている管理インターフェイスまたはデータ インターフェイスと同じサブネット上に存在する必要があります。複数のポートがイネーブルになっている場合、Web プロキシは、データ トラフィック用に設定されているデフォルト ゲートウェイと同じネットワーク上のデータ インターフェイスでトランザクションを送信します。

発信サービス トラフィック

Secure Web Applianceは管理インターフェイスとデータ インターフェイスを使用して、サービス用の発信トラフィック（DNS、ソフトウェア アップグレード、NTP、traceroute データ トラフィックなど）もルーティングします。発信トラフィックに使用されるルートを選択することで、各サービスに対してこれを個々に設定できます。デフォルトでは、すべてのサービスに対して管理インターフェイスが使用されます。

関連項目

- 管理トラフィックとデータ トラフィックの分割ルーティングをイネーブルにするには、[ネットワーク インターフェイスのイネーブル化または変更, on page 37](#)を参照してください。

デフォルト ルートの変更

Procedure

ステップ 1 [ネットワーク (Network)] > [ルート (Routes)] を選択します。

- ステップ 2** 必要に応じて、[管理 (Management)] テーブルまたは [データ (Data)] テーブルの [デフォルト ルート (Default Route)] をクリックします (分割ルーティングがイネーブルになっていない場合は、統合された [管理/データ (Management/Data)] テーブル)。
- ステップ 3** [ゲートウェイ (Gateway)] カラムで、編集するネットワーク インターフェイスに接続されているネットワークのネクスト ホップ上のコンピュータ システムの IP アドレスを入力します。
- ステップ 4** 変更を送信し、保存します。

ルートの追加

Procedure

- ステップ 1** [ネットワーク (Network)] > [ルート (Routes)] を選択します。
- ステップ 2** ルートを作成するインターフェイスに対応する [ルートを追加 (Add Route)] ボタンをクリックします。
- ステップ 3** 名前、宛先ネットワーク、およびゲートウェイを入力します。
- ステップ 4** 変更を送信し、保存します。

ルーティング テーブルの保存およびロード

Procedure

[ネットワーク (Network)] > [ルート (Routes)] を選択します。

ルートテーブルを保存するには、[ルートテーブルを保存 (Save Route Table)] をクリックし、ファイルの保存場所を指定します。

保存されているルートテーブルをロードするには、[ルートテーブルをロード (Load Route Table)] をクリックし、ファイルを探して開き、変更を送信して確定します。

Note

宛先アドレスが物理ネットワーク インターフェイスの 1 つと同じサブネット上にある場合、AsyncOS は同じサブネット内のネットワーク インターフェイスを使用してデータを送信します。ルーティングテーブルは参照されません。

ルートの削除

Procedure

-
- ステップ 1** [ネットワーク (Network)] > [ルート (Routes)] を選択します。
- ステップ 2** 該当するルートの [削除 (Delete)] 列のチェックボックスをオンにします。
- ステップ 3** [削除 (Delete)] をクリックして確認します。
- ステップ 4** 変更を送信し、保存します。
-

What to do next

関連項目

- [ネットワーク インターフェイスのイネーブル化または変更, on page 37。](#)

トランスペアレント リダイレクションの設定

- [透過リダイレクション デバイスの指定, on page 58](#)
- [WCCP サービスの設定, on page 60](#)

透過リダイレクション デバイスの指定

Before you begin

レイヤ 4 スイッチまたは WCCP v2 ルータにアプライアンスを接続します。

Procedure

-
- ステップ 1** [ネットワーク (Network)] > [トランスペアレント リダイレクション (Transparent Redirection)] を選択します。
- ステップ 2** [デバイスの編集 (Edit Device)] をクリックします。
- ステップ 3** [タイプ (Type)] ドロップダウン リストから、アプライアンスに透過的にトラフィックをリダイレクトするデバイスのタイプとして [レイヤ 4 スイッチもしくはデバイスなし (Layer 4 Switch or No Device)] または [WCCP v2 ルータ (WCCP v2 Router)] を選択します。
- ステップ 4** 変更を送信し、保存します。
- ステップ 5** WCCP v2 デバイスの場合は、以下の追加手順を実行します。
- a) デバイスのマニュアルを参照して、WCCP デバイスを設定します。
 - b) Secure Web Appliance の [透過リダイレクション (Transparent Redirection)] ページで、[サービスの追加 (Add Service)] をクリックし、[WCCP サービスの追加と編集, on page 61](#)で説明している手順に従って WCCP サービスを追加します。

- c) アプライアンスで IP スプーフィングがイネーブルになっている場合は、セカンド WCCP サービスを作成します。

What to do next

関連項目

- [アプライアンスの接続, on page 18。](#)
- [WCCP サービスの設定, on page 60。](#)

L4 スイッチの使用

透過リダイレクションのためにレイヤ4スイッチを使用している場合、スイッチの設定によっては、Secure Web Applianceでいくつかの追加オプションを設定する必要があります。

- 通常は IP スプーフィングを有効にしないでください。アップストリーム IP アドレスのスプーフィングを行う場合は、非同期ルーティンググループを作成します。
- [Web プロキシ設定の編集 (Edit Web Proxy Settings)] ページ ([セキュリティ サービス (Security Services)] > [Web プロキシ (Web Proxy)]) の[受信ヘッダーを使用する (Use Received Headers)] セクション (詳細設定) にある [X-Forwarded-For を使用したクライアント IP アドレスの識別を有効にする (Enable Identification of Client IP Addresses using X-Forwarded-For)] をオンにします。次に、1 つ以上の出力 IP アドレスを [信頼できるダウンストリーム プロキシまたはロードバランサ (Trusted Downstream Proxy or Load Balancer)] リストに追加します。
- 次に示すプロキシ関連パラメータを必要に応じて設定するには、CLI コマンド `advancedproxyconfig>miscellaneous` を使用できます。
 - `Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)?` : Secure Web Applianceがヘルスチェックに応答できるようにするには Y と入力します。
 - `Would you like proxy to perform dynamic adjustment of TCP receive window size?` : ほとんどの場合はデフォルトの Y を使用します。Secure Web Applianceの別のプロキシデバイスアップストリームがある場合は N と入力します。
 - `Do you want to pass HTTP X-Forwarded-For headers?` : X-Forwarded-For (XFF) ヘッダーの要件アップストリームがない場合は不要です。
 - `Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?` : トラブルシューティングを支援するには Y と入力できます。クライアント IP アドレスがアクセス ログに表示されます。
 - `Would you like the proxy to use client IP addresses from X-Forwarded-For headers?` : ポリシー設定とレポートを支援するには Y と入力できます。

- X-Forwarded-For (XFF) ヘッダーを使用する場合は、XFF ヘッダーをログに記録するため、アクセス ログ サブスクリプションに %f を追加します。W3C ログ形式の場合は `cs(X-Forwarded-For)` を追加します。

WCCP サービスの設定

WCCP サービスは、WCCP v2 ルータにサービス グループを定義するアプライアンスの設定です。使用するサービス ID やポートなどの情報が含まれます。サービス グループを使用して、Web プロキシは WCCP ルータとの接続を確立し、ルータからリダイレクトされたトラフィックを処理することができます。

WCCP プロキシのヘルスチェックがイネーブルの場合、Secure Web Appliance の WCCP デーモンは Web プロキシサーバーで実行されている xmlrpc サーバーに 10 秒おきにヘルスチェック メッセージ (xmlrpc クライアント要求) を送信します。プロキシが稼働している場合、WCCP サービスはプロキシから応答を受信し、Secure Web Appliance は指定された WCCP 対応ルータに WCCP 「here I am」 (HIA) メッセージを 10 秒おきに送信します。WCCP サービスがプロキシから応答を受信しない場合、HIA メッセージは WCCP ルータに送信されません。

WCCP ルータが HIA メッセージを 3 回連続して受信しなかった場合、ルータはサービスグループから Secure Web Appliance を削除し、Secure Web Appliance にトラフィックが転送されないようになります。

CLI コマンド `advancedproxyconfig>miscellaneous>Do you want to enable WCCP proxy health check?` を使用して、プロキシヘルスチェックメッセージをイネーブルまたはディセーブルすることができます。ヘルスチェックはデフォルトでディセーブルです。



Note WCCPv2 サービスは、IPv4 ネットワークおよび IPv6 ネットワークで動作します。1 つのアプライアンスに最大 15 個のサービス グループを設定できます。WCCP ルータの各サービスグループには、最大 32 のアプライアンスを含めることができます。WCCPv2 サービスは、ロードバランシングメカニズムにも使用され、コンテンツエンジンの過負荷とデータブロッキングを軽減します。



Note 同じアプライアンスで WCCP とハイアベイラビリティを設定することはサポートされていません。設定されている場合、Secure Web Appliance は期待どおりに機能しません。

- [WCCP ロードバランシングについて, on page 61](#)
- [WCCP サービスの追加と編集, on page 61](#)
- [IP スプーフィングの WCCP サービスの作成, on page 65](#)

WCCP ロードバランシングについて

WCCP サービス定義の [割り当ての重み付け (Assignment Weight)] パラメータは、この Secure Web Appliance が WCCP プールのメンバーまたはサービスグループとして動作している場合に、WSA の負荷を調整するために使用されます。この重み付けは、処理するためにこの Secure Web Appliance に送信できる WCCP の合計トラフィックに対する比率を表します。

割り当ての重み付けを調整する必要があるのは、さまざまなタイプのゲートウェイアプライアンスが同じ WCCP プールのメンバーになっていて、強力なアプライアンスに振り分けるトラフィックの量を増やす必要がある場合のみです。



- (注) WCCP プールのメンバーになっているすべての Secure Web Appliance で、WCCP ロードバランシングを利用するには、割り当ての重み付けをサポートする AsyncOS のバージョンが実行されている必要があります。



- (注) WCCP は、最大 32 のアプライアンスの透過的なトラフィックを負荷分散します。ハッシュまたはマスクに基づいてトラフィックフローのバランスをとり、ネットワークに複数のアプライアンスモデルが存在する場合はトラフィックが重み付けされます。ダウンタイムなしでサービスプールにデバイスを追加したり、サービスプールからデバイスを削除したりできます。ただし、8 つ以上のアプライアンスを使用している、または使用する予定の場合は、専用のロードバランサを用意することをお勧めします。

[割り当ての重み付け (Assignment Weight)] パラメータの詳細については、[WCCP サービスの追加と編集 \(61 ページ\)](#) を参照してください。

WCCP サービスの追加と編集

Before you begin

WCCP v2 ルータを使用するようにアプライアンスを設定します ([透過リダイレクションデバイスの指定](#), on page 58 を参照)。

Procedure

- ステップ 1 [ネットワーク (Network)] > [透過リダイレクション (Transparent Redirection)] を選択します。
- ステップ 2 [サービスの追加 (Add Service)] をクリックします。または、WCCP サービスを編集するには、[サービスプロファイル名 (Service Profile Name)] 列にある WCCP サービスの名前をクリックします。
- ステップ 3 以下の手順に従って、WCCP のオプションを設定します。

WCCP サービス オプション	説明
サービス プロファイル名 (Service Profile Name)	WCCP サービスの名前。 Note このオプションを空のままにして、標準サービス（下記を参照）を選択すると、「web_cache」という名前が自動的に割り当てられます。
サービス	ルータのサービス グループのタイプ。次から選択します。 [標準サービス (Standard service)]。このサービス タイプには、固定 ID 「ゼロ」、固定リダイレクト方式「宛先ポート別」、固定宛先ポート「80」が割り当てられます。1 つの標準サービスのみ作成できます。アプライアンスに標準サービスがすでに存在している場合、このオプションはグレー表示されます。 [ダイナミックサービス (Dynamic service)]。このサービス タイプでは、カスタム ID、ポート番号、およびリダイレクト オプションとロード バランシング オプションを定義できます。WCCP ルータでサービスを作成するときは、ダイナミック サービスで指定したパラメータと同じパラメータを入力します。 ダイナミック サービスを作成する場合は、以下の情報を入力します。 • [サービス ID (Service ID)]。[ダイナミックサービス ID (Dynamic Service ID)] フィールドに 0 ～ 255 の任意の数字を入力できます。ただし、このアプライアンスには 15 個以上のサービス グループを設定することはできません。 • [ポート番号 (Port number(s))]。[ポート番号 (Port Numbers)] フィールドにリダイレクトするトラフィックに最大 8 つのポート番号を入力します。 • [リダイレクションの基礎 (Redirection basis)]。送信元ポートまたは宛先ポートに基づいてトラフィックをリダイレクトするように選択します。デフォルトは宛先ポートです。 Note 透過リダイレクションと IP スプーフィングを使用してネイティブ FTP を設定するには、[ソースポート (リターンパス)] に基づいてリダイレクト (Redirect based on source port (return path))] を選択し、送信元ポートを 13007 に設定します。 • [ロード バランシングの基礎 (Load balancing basis)]。ネットワークが複数の Secure Web Applianceを使用している場合、アプライアンス間でパケットを配布する方法を選択できます。サーバまたはクライアントアドレスに基づいてパケットを配布できます。クライアントアドレスを選択した場合、クライアントからのパケットは常に同じアプライアンスに配布されます。デフォルトはサーバアドレスです。

WCCP サービス オプション	説明
ルータ IP アドレス	1 つまたは複数の WCCP 対応ルータの IPv4 または IPv6 アドレスを入力します。各ルータ固有の IP を使用します。マルチキャストアドレスは入力できません。1 つのサービス グループ内に IPv4 と IPv6 アドレスを混在させることはできません。
ルータ セキュリティ	このサービス グループに対してパスフレーズを要求する場合は、[サービスのセキュリティ有効化 (Enable Security for Service)] をオンにします。イネーブルにした場合、そのサービス グループを使用するアプライアンスと WCCP ルータは同じパスフレーズを使用する必要があります。 使用するパスフレーズと確認パスフレーズを入力します。

WCCP サービス オプション	説明
詳細設定 (Advanced)	ロード バランシング方式。複数の Secure Web Appliance 間においてルータがパケットのロードバランシングを実行する方法を決定します。次から選択します。 • [マスクのみ許可 (Allow Mask Only)]。WCCP ルータは、ルータのハードウェアを使用して決定を行います。この方式は、ハッシュ方式よりもルータのパフォーマンスを向上させます。ただし、すべての WCCP ルータがマスク割り当てをサポートしているわけではありません。(IPv4 のみ) • [ハッシュのみ許可 (Allow Hash Only)]。この方式は、ハッシュ関数に依存して、リダイレクションに関する決定を下します。この方式はマスク方式ほど効率的ではありませんが、ルータがこのオプションしかサポートしていない場合もあります。(IPv4 および IPv6) • [ハッシュもしくはマスクを許可 (Allow Hash or Mask)]。AsyncOS がルータと方式をネゴシエートできるようになります。ルータがマスクをサポートしている場合、AsyncOS はマスクを使用します。サポートしていない場合は、ハッシュが使用されます。 [マスクのカスタマイズ (Mask Customization)]。[マスクのみ許可 (Allow Mask Only)] または [ハッシュのみ許可 (Allow Hash Only)] を選択する場合、マスクをカスタマイズしたり、ビット数を指定したりできます。 • [カスタム マスク (最大 6 ビット)]。マスクを指定できます。Web インターフェイスは、提供するマスクに関連付けられたビット数を表示します。IPv4 ルータの場合は最大 5 ビット、IPv6 ルータの場合は最大 6 ビットを使用できます。 • [システム生成マスク (System generated mask)]。システムがマスクを生成するように設定できます。任意で、システムにより生成されたマスクにビット数 (1 ～ 5) を指定できます。 [重みの割り当て (Assignment Weight)]：この Secure Web Appliance の WCCP 重み付け。有効な値は 0 ～ 255 です。この重み付けは、WCCP サービスグループのメンバーとしてのこの Secure Web Appliance に送信して処理できる合計トラフィックに対する比率を表します。ゼロの値は、この Secure Web Appliance はサービスグループのメンバーであっても、ルータからリダイレクトされるトラフィックを受信しないことを意味します。詳細については、WCCP ロード バランシングについて, on page 61 を参照してください。 [転送方式 (Forwarding method)]。この方式では、リダイレクトされたパケットがルータから Web プロキシに転送されます。 [リターン方式 (Return Method)]。この方式では、リダイレクトされたパケットが Web プロキシからルータに転送されます。

WCCP サービス オプション	説明
	転送方式およびリターン方式では、以下のいずれかのメソッドタイプが使用されます。 • [レイヤ 2 (L2) (Layer 2 (L2))]。パケットの宛先 MAC アドレスをターゲット Web プロキシの MAC アドレスに置き換えることで、レイヤ 2 のトラフィックをリダイレクトします。L2 メソッドはハードウェアレベルで動作し、通常、最高のパフォーマンスを実現します。ただし、すべての WCCP ルータが L2 転送をサポートしているわけではありません。また、WCCP ルータは、（物理的に）直接接続されている Secure Web Appliance との L2 ネゴシエーションのみを許可します。 • [総称ルーティングカプセル化 (GRE) (Generic Routing Encapsulation (GRE))]。この方式は、GRE ヘッダーとリダイレクト ヘッダーを含む IP パケットをカプセル化することで、レイヤ 3 でトラフィックをリダイレクトします。GRE はソフトウェア レベルで動作し、パフォーマンスに影響する可能性があります。 • [L2 または GRE (L2 or GRE)]。このオプションを指定すると、アプライアンスはルータがサポートしている方式を使用します。ルータとアプライアンスの両方が L2 と GRE をサポートする場合、アプライアンスは L2 を使用します。 ルータが直接アプライアンスに接続されていない場合、GRE を選択する必要があります。

ステップ 4 変更を送信し、保存します。

IP スプーフィングの WCCP サービスの作成

Procedure

ステップ 1 Web プロキシで IP スプーフィングがイネーブルになっている場合は、2 つの WCCP サービスを作成します。標準の WCCP サービスを作成するか、宛先ポートに基づいてトラフィックをリダイレクトするダイナミック WCCP サービスを作成します。

ステップ 2 宛先ポートに基づいてトラフィックをリダイレクトするダイナミック WCCP サービスを作成します。

ステップ 1 で作成したサービスで使用するポート番号、ルータ IP アドレス、ルータセキュリティの設定と同じ設定を使用します。

Note

- シスコでは、リターンパスに使用する（送信元ポートに基づく）WCCP サービスには 90 ～ 97 のサービス ID 番号を使用することを推奨します。

- WCCP ロードバランシング方式を [マスクのみ許可 (Allow Mask Only)] または [ハッシュもしくはマスクを許可 (Allow Hash or Mask)] に設定して、複数のアプライアンスにトラフィックを分散する場合は、なりすましの IP アドレスを適切に設定します。なりすましの IP アドレスの設定では、WCCP ルータと Secure Web Appliance 間のトラフィックを適切にルーティングする必要があります。

What to do next

関連項目

- [Web プロキシ キャッシュ, on page 241.](#)

VLAN の使用によるインターフェイス能力の向上

1 つまたは複数の VLAN を設定することで、組み込まれている物理インターフェイスの数を超えて、Secure Web Appliance が接続可能なネットワークの数を増加できます。

VLAN は、「VLAN DDDD」という形式の名前を持つ動的な「データポート」として表示されます。「DDDD」は最大 4 桁の ID です (VLAN 2、VLAN 4094 など)。AsyncOS は、最大 30 の VLAN をサポートします。

物理ポートは、VLAN に配置するために IP アドレスを設定する必要がありません。VLAN を作成した物理ポートに VLAN 以外のトラフィックを受信する IP アドレスを設定できるため、VLAN のトラフィックと VLAN 以外のトラフィックの両方を同じインターフェイスで受信できます。

VLANs は、M1、内部データポートには P1、外部データポートには P2 を使用して、管理インターフェイスで作成できます。

VSAN の設定と管理

VLAN の作成、編集、および削除を行うには、`etherconfig` コマンドを使用します。作成した VLAN は、CLI の `interfaceconfig` コマンドを使用して設定できます。



Note VLAN 設定を変更する場合は、必ずアプライアンスをリブートしてください。

例 1 : 新しい VLAN の作成

この例では、P1 1 ポート上に 2 つの VLAN (VLAN 31 と VLAN 34) を作成します。



Note T1 または T2 インターフェイス上で VLAN を作成しないでください。

Procedure

ステップ 1 CLI にアクセスします。

ステップ 2 以下の手順を実行します。

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> vlan
VLAN interfaces:
Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 34
Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2
VLAN interfaces:
1. VLAN 34 (P1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 31
Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2
VLAN interfaces:
1. VLAN 31 (P1)
2. VLAN 34 (P1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>
```

ステップ 3 変更を保存します。

例 2 : VLAN 上の IP インターフェイスの作成

この例では、VLAN 34 イーサネットインターフェイス上に新しい IP インターフェイスを作成します。



Note インターフェイスに変更を加えると、アプライアンスとの接続が閉じることがあります。

Procedure

ステップ 1 CLI にアクセスします。

ステップ 2 以下の手順を実行します。

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> new
IP Address (Ex: 10.10.10.10):
[]> 10.10.31.10
Ethernet interface:
1. Management
2. P1
3. VLAN 31
4. VLAN 34
[1]> 4
Netmask (Ex: "255.255.255.0" or "0xffffffff00"):
[255.255.255.0]>
Hostname:
[]> v.example.com
Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
3. VLAN 34 (10.10.31.10 on VLAN 34: v.example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>
example.com> commit
```

ステップ 3 変更を保存します。

What to do next

関連項目

- [ネットワーク インターフェイスのイネーブル化または変更, on page 37。](#)
- [TCP/IP トラフィック ルートの設定, on page 55。](#)

リダイレクトホスト名とシステムホスト名

システムセットアップウィザードを実行すると、システムホスト名とリダイレクトホスト名が同一になります。ただし、`sethostname` コマンドを使用してシステムのホスト名を変更しても、リダイレクトホスト名は変更されません。そのため、複数の設定に異なる値が含まれることになります。

AsyncOS は、エンドユーザー通知と応答確認にリダイレクトホスト名を使用します。

システムホスト名は、次のエリアでアプライアンスの識別に使用される完全修飾ホスト名です。

- コマンドラインインターフェイス (CLI)
- システムアラート
- Secure Web Applianceが Active Directory ドメインに参加するときに、マシンの NetBIOS 名を作成する場合

システムホスト名はインターフェイスのホスト名と直接対応しておらず、クライアントがアプライアンスに接続するために使用されません。

リダイレクトホスト名の変更

Procedure

- ステップ1 Web ユーザー インターフェイスで、[ネットワーク (Network)] > [認証 (Authentication)] に移動します。
- ステップ2 [グローバル設定を編集 (Edit Global Settings)] をクリックします。
- ステップ3 [リダイレクトホスト名 (Redirect Hostname)] に新しい値を入力します。

システムホスト名の変更

Procedure

- ステップ1 CLI にアクセスします。
- ステップ2 Secure Web Applianceの名前を変更するには、`sethostname` コマンドを使用します。

```
example.com> sethostname
```

```
example.com> hostname .com
```

```
example.com> commit
...
hostname.com>
```

ステップ 3 変更を保存します。

SMTP リレー ホストの設定

AsyncOS は、通知、アラート、Cisco IronPort カスタマー サポート 要求など、システムにより生成された電子メール メッセージを定期的送信します。デフォルトでは、AsyncOS はドメインの MX レコードにリストされている情報を使用して電子メールを送信します。ただし、アプライアンスが MX レコードにリストされているメール サーバーに直接到達できない場合、アプライアンス上に少なくとも 1 つの SMTP リレー ホストを設定します。



Note

Secure Web Appliance が MX レコードまたは設定済み SMTP リレー ホストにリストされているメール サーバと通信できない場合、電子メール メッセージを送信できず、ログファイルにメッセージを書き込みます。

1 つまたは複数の SMTP リレー ホストを設定できます。複数の SMTP リレー ホストを設定する場合、AsyncOS は、使用可能な最上位の SMTP リレー ホストを使用します。SMTP リレー ホストが使用できない場合、AsyncOS は、そのリスト 1 つ下のリレー ホストの使用を試みます。

SMTP リレー ホストの設定

Procedure

ステップ 1 [ネットワーク (Network)] > [内部SMTPリレー (Internal SMTP Relay)] を選択します。

ステップ 2 [設定の編集 (Edit Settings)] をクリックします。

ステップ 3 [内部SMTPリレー (Internal SMTP Relay)] の設定を完成させます。

プロパティ	説明
リレー ホスト名または IP アドレス (Relay Hostname or IP Address)	SMTP リレー に使用するホスト名または IP アドレス。
ポート (Port)	SMTP リレー に接続するためのポート。このプロパティを空欄にした場合、アプライアンスはポート 25 を使用します。

プロパティ	説明
SMTP への接続に使用するルーティングテーブル (Routing Table to Use for SMTP)	SMTP リレーへの接続に使用するアプライアンスのネットワーク インターフェイス（管理またはデータのいずれか）に関連付けられているルーティングテーブル。リレーシステムと同じネットワークにあるインターフェイスを選択します。

ステップ 4 （任意）[行を追加（Add Row）] をクリックして別の SMTP リレー ホストを追加します。

ステップ 5 変更を送信し、保存します。

DNS の設定

AsyncOS for Web は、インターネット ルート DNS サーバまたはユーザ独自の DNS サーバを使用できます。インターネット ルート サーバを使用する場合、特定のドメインに使用する代替サーバを指定できます。代替 DNS サーバは単一のドメインに適用されるため、当該ドメインに対する権威サーバ（最終的な DNS レコードを提供）である必要があります。

セカンダリ DNS ネーム サーバを指定して、プライマリ ネーム サーバで解決されないクエリを解決することもできます。セカンダリ DNS サーバはフェールオーバー DNS サーバとして使用されません。プライマリ DNS サーバから [DNS 設定の編集, on page 72](#) で指定されたエラーが返された場合は、優先順位に従ってセカンダリ DNS サーバがクエリされます。

認証の失敗を防ぐには、Secure Web Appliance 認証リダイレクト名が一意であることを確認してください。

- [スプリット DNS, on page 72](#)
- [DNS キャッシュのクリア, on page 72](#)
- [DNS 設定の編集, on page 72](#)

セキュア DNS の注意事項と制約事項



(注) デフォルトでは、セキュア DNS は無効になっています。

セキュア DNS を有効にする場合：

- ローカルドメインとプライベートドメインのホスト名で FQDN を使用する必要があります。
- 下位互換性がないため、DNS サーバーは DNSSEC を使用して構成するようにしてください。これを使用しないと、未解決のホスト名を使用した無効な応答が返される可能性があります。

- 次のシステムログは表示されません。
 - インターネットルートの DNS 要求に対するサーバーの詳細
 - デバッグログとトレースログに関する詳細情報
- CNAME はキャッシュされません。
- 無効な DNSSEC 応答はキャッシュされません。
- DNS キャッシュは、セキュア DNS の設定が[無効化 (disabled)] から[有効化 (enabled)] に変更されたときにクリアされ、その逆も同様です。
- [ネットワーク設定のロード (Load Network Settings)] を選択して、セキュア DNS の構成を確実にロードします。

スプリット DNS

AsyncOS は、内部サーバが特定のドメインに設定され、外部またはルート DNS サーバが他のドメインに設定されたスプリット DNS をサポートします。ユーザ独自の内部サーバを使用している場合は、例外のドメインおよび関連する DNS サーバを指定することもできます。

DNS キャッシュのクリア

Before you begin

このコマンドを使用すると、キャッシュの再投入中に一時的にパフォーマンスが低下することがあるので注意してください。

Procedure

ステップ 1 [ネットワーク (Network)] > [DNS] を選択します。

ステップ 2 [DNS キャッシュを消去 (Clear DNS Cache)] をクリックします。

DNS 設定の編集

Procedure

ステップ 1 [ネットワーク (Network)] > [DNS] を選択します。

ステップ 2 [設定の編集 (Edit Settings)] をクリックします。

ステップ 3 必要に応じて、DNS 設定値を設定します。

プロパティ	説明
プライマリ DNS サーバ (Primary DNS Servers)	[これらのDNSサーバを使用 (Use these DNS Servers)]。アプライアンスがホスト名の解決に使用できるローカル DNS サーバ。 [優先代替DNSサーバ (オプション) (Alternate DNS servers Overrides (Optional))]。特定のドメイン用の権威 DNS サーバ [インターネットのルートDNSサーバを使用 (Use the Internet's Root DNS Servers)]。アプライアンスがネットワーク上のDNSサーバにアクセスできない場合に、ドメイン名サービス ルックアップにインターネットのルート DNS サーバを使用することを選択できます。 Note インターネット ルート DNS サーバは、ローカル ホスト名を解決しません。アプライアンスでローカル ホスト名を解決する必要がある場合は、ローカル DNS サーバを使用して解決するか、コマンドライン インターフェイスからローカル DNS に適切なスタティック エントリを追加する必要があります。これは、新しい Web インターフェイスにアクセスするためにも必要です。
セカンダリ DNS サーバ (Secondary DNS Servers)	プライマリ ネーム サーバで解決されなかったホスト名を解決するためにアプライアンスが使用できるセカンダリ DNS サーバ。 Note プライマリ DNS サーバから次のエラーが返されると、セカンダリ DNS サーバがホスト名クエリを受信します。 - エラーなし、応答セクションを受信しませんでした。(No Error, no answer section received.) - サーバが要求を完了できませんでした。応答セクションがありません。(Server failed to complete request, no answer section.) - 名前エラー、応答セクションを受信しませんでした。(Name Error, no answer section received.) - 実装されていない機能です。(Function not implemented.) - サーバがクエリへの応答を拒否しました。(Server Refused to Answer Query.)
DNS トラフィック用ルーティングテーブル (Routing Table for DNS Traffic)	DNS サービスがルート トラフィックをルーティングする際に経由するインターフェイスを指定します。
IP アドレスバージョン設定 (IP Address Version Preference)	DNS サーバが IPv4 と IPv6 の両方のアドレスを提供する場合、AsyncOS はこの設定を使用して IP アドレスのバージョンを選択します。 Note AsyncOS は、透過的 FTP 要求のバージョン設定に従いません。

プロパティ	説明
セキュア DNS	DNS サーバーから受信した DNS 応答の認証を検証するには、[セキュア DNS (Secure DNS)] チェックボックスをオンにします。 Note セキュア DNS を有効にすると、解決までの時間が長くなります。
DNS 逆引きタイムアウト (Wait Before Timing out Reverse DNS Lookups)	無応答逆引き DNS ルックアップがタイムアウトするまでの待機時間（秒単位）。
ドメイン検索リスト (Domain Search List)	簡易ホスト名（「.」記号がないホスト名）宛てに要求を送信する際に使用される DNS ドメイン検索リスト。ドメイン名を加えたホスト名に一致する DNS が存在するかどうかを調べるために、指定されたドメインが入力順に照合されます。

ステップ 4 変更を送信し、保存します。

What to do next

関連項目

- [TCP/IP トラフィック ルートの設定, on page 55](#)
- [IP アドレスのバージョン, on page 36](#)

接続、インストール、設定に関するトラブルシューティング

- [フェールオーバーの問題, on page 744](#)
- [アップストリーム プロキシが基本クレデンシャルを受け取らない, on page 767](#)
- [クライアント要求がアップストリーム プロキシで失敗する, on page 767](#)
- [最大ポート エントリ数, on page 769](#)



第 3 章

認証および承認

この章で説明する内容は、次のとおりです。

- [エンドユーザー クレデンシャルの取得の概要, on page 75](#)
- [認証に関するベスト プラクティス, on page 76](#)
- [認証の計画, on page 77](#)
- [認証レルム, on page 90](#)
- [認証シーケンス, on page 117](#)
- [認証の失敗, on page 119](#)
- [資格情報, on page 127](#)
- [認証に関するトラブルシューティング, on page 130](#)

エンドユーザー クレデンシャルの取得の概要

サーバー タイプ/ レルム	認証方式	サポートされるネットワークプロ トコル	注記
Active Directory	Kerberos NTLMSSP 基本	HTTP、HTTPS ネイティブ FTP、FTP over HTTP SOCKS（基本認証）	Kerberos は標準モードでのみサポートされます。クラウドコネクタモードではサポートされません。
LDAP	基本	HTTP、HTTPS ネイティブ FTP、FTP over HTTP SOCKS	—

認証タスクの概要

手順	タスク	関連項目および手順へのリンク
1	認証レルムを作成する。	• Active Directory 認証レルムの作成 (NTLMSSP および基本), on page 97 • LDAP 認証レルムの作成, on page 100
2	グローバル認証を設定する。	• グローバル認証の設定, on page 108
3	外部認証を設定する。 外部 LDAP または RADIUS サーバーからユーザーを認証できます。	• 外部認証, on page 91
4	(任意) 追加の認証レルムを作成して順序を決定する。 使用する予定の各認証プロトコルとスキームの組み合わせに対して、少なくとも1つの認証レルムを作成する。	• 認証シーケンスの作成, on page 118
5	(任意) クレデンシャルの暗号化を設定する。	• クレデンシャル暗号化の設定, on page 129
6	認証要件に基づいてユーザーとクライアントソフトウェアを分類する識別プロファイルを作成する。	• ユーザーおよびクライアントソフトウェアの分類, on page 267
7	識別プロファイルの作成対象となったユーザーとユーザーグループからの Web 要求を管理するポリシーを作成する。	• ポリシーによる Web 要求の管理 : ベスト プラクティス, on page 364

認証に関するベスト プラクティス

- できる限り少数の Active Directory レルムを作成します。多数の Active Directory レルムを作成すると、認証で追加のメモリが必要になります。
- NTLMSSP を使用する場合は、Secure Web Appliance またはアップストリーム プロキシ サーバを使用してユーザを認証します（両方は使用できません）。（Secure Web Appliance を推奨）
- Kerberos を使用する場合は、Secure Web Applianceを使用して認証します。
- 最適なパフォーマンスを得るには、1 つのレルムを使用して同じサブネット上のクライアントを認証します。

- 一部のユーザー エージェントには、通常の動作に悪影響を及ぼすマシン クレデンシャルや認証失敗の問題があることが判明されています。これらのユーザー エージェントとの認証をバイパスする必要があります。[問題のあるユーザー エージェントの認証のバイパス, on page 120](#) を参照してください。
- クライアントをアクティブに認証することは、リソースを大量に消費するタスクです。認証サロゲートを使用すると、認証が完了した後、設定された期間（デフォルトは 3600 秒）、**[グローバル認証 (Global Authentication)] > [サロゲートタイムアウト (Surrogate Timeout)]** で構成可能な認証されたユーザーを記憶することにより、認証パフォーマンスを向上させることができます。アクティブな認証イベントの数を制限するために、可能な場合は常に IP サロゲートを使用する必要があります。
- 信頼された Active Directory (AD) を使用した認証設定の場合、信頼ドメインの DC 解決が成功しないと、認証は失敗します。これは、Samba 4.11.15 が導入されたためであり、信頼ドメインのルックアップが成功する必要があります。DC の名前解決が失敗し続ける場合は、**[ネットワーク (Network)] > [認証 (Authentication)] > [認証サーバーのタイプとスキーム (Authentication Server and Type and Scheme(s))]** に移動し、[信頼されたドメインの正常性チェックの有効化 (Enable Trusted Domain Health Check)] チェックボックスをオフにする必要があります。

認証の計画

- [Active Directory/Kerberos, on page 78](#)
- [Active Directory/基本, on page 79](#)
- [Active Directory/NTLMSSP, on page 80](#)
- [LDAP/基本, on page 81](#)
- [ユーザーの透過的識別, on page 81](#)

Active Directory/Kerberos

明示的な転送	透過、IP ベースのキャッシング	透過、Cookie ベースのキャッシング
利点： • NTLM と比べた場合、パフォーマンスと相互運用性が向上 • ドメインに参加している Windows クライアントと非 Windows クライアントの両方と連携 • すべてのブラウザ、および他のほとんどのアプリケーションでサポートされている • RFC ベース • 最小限のオーバーヘッド（再認証は必要ありません） • HTTPS (CONNECT) 要求で利用できる • パスフレーズが認証サーバーに送信されないため、より安全である • ホストや IP アドレスではなく、接続が認証される • クライアントアプリケーションが Secure Web Appliance を信頼するように設定されている場合に、Active Directory 環境で真のシングルサインオンを実現	利点： • NTLM と比べた場合、パフォーマンスと相互運用性が向上 • ドメインに参加している Windows クライアントと非 Windows クライアントの両方と連携 • すべての主要ブラウザで利用できる • 認証をサポートしていないユーザー エージェントを使用する場合、ユーザーはサポートされるブラウザで最初に認証されるだけでよい • オーバーヘッドが比較的低い • ユーザーが以前に HTTP 要求で認証されている場合は、HTTPS 要求で利用できる	利点： • NTLM と比べた場合、パフォーマンスと相互運用性が向上 • ドメインに参加している Windows クライアントと非 Windows クライアントの両方と連携 • すべての主要ブラウザで利用できる • 認証が、ホストや IP アドレスではなく、ユーザーに関連付けられる 欠点： • Cookie はドメイン固有であるため、新規の各 Web ドメインで認証プロセス全体が必要 • Cookie をイネーブルにする必要がある • HTTPS 要求で使えない

Active Directory/基本

明示的な転送	透過、IP ベースのキャッシング	透過、Cookie ベースのキャッシング
利点： • すべてのブラウザ、および他のほとんどのアプリケーションでサポートされている • RFC ベース • 最小限のオーバーヘッド • HTTPS (CONNECT) 要求で利用できる • パスフレーズが認証サーバーに送信されないため、より安全である • ホストや IP アドレスではなく、接続が認証される • クライアントアプリケーションが Secure Web Applianceを信頼するように設定されている場合に、Active Directory 環境で真のシングルサインオンを実現 欠点： • すべての要求でパスフレーズがクリアテキスト (Base64) として送信される • シングル サインオンなし • 中程度のオーバーヘッド：新規の接続ごとに再認証が必要 • 主に Windows および主要ブラウザでのみサポート	利点： • すべての主要ブラウザで利用できる • 認証をサポートしていないユーザーエージェントを使用する場合、ユーザーはサポートされるブラウザで最初に認証されるだけでよい • オーバーヘッドが比較的低い • ユーザーが以前に HTTP 要求で認証されている場合は、HTTPS 要求で利用できる 欠点： • 認証クレデンシャルが、ユーザーではなく、IP アドレスに関連付けられる (Citrix および RDP 環境では使用できず、ユーザーが IP アドレスを変更した場合も使用できない) • シングル サインオンなし • パスフレーズがクリアテキスト (Base64) として送信される	利点： • すべての主要ブラウザで利用できる • 認証が、ホストや IP アドレスではなく、ユーザーに関連付けられる 欠点： • Cookie はドメイン固有であるため、新規の各 Web ドメインで認証プロセス全体が必要 • Cookie をイネーブルにする必要がある • HTTPS 要求で使用できない • シングル サインオンなし • パスフレーズがクリアテキスト (Base64) として送信される

Active Directory/NTLMSSP

明示的な転送	透過
利点： • パスフレーズが認証サーバーに送信されないため、より安全である • ホストや IP アドレスではなく、接続が認証される • クライアント アプリケーションが Secure Web Appliance を信頼するように設定されている場合に、Active Directory 環境で真のシングル サインオンを実現 欠点： • 中程度のオーバーヘッド：新規の接続ごとに再認証が必要 • 主に Windows および主要ブラウザでのみサポート	利点： • より柔軟性が高い 透過 NTLMSSP 認証は透過基本認証と似ています。ただし、Web プロキシはクライアントとの通信に、基本的なクリアテキストのユーザー名とパスワードではなく、チャレンジ/レスポンス認証を使用します。 透過 NTLM 認証を使用する利点と欠点は、透過基本認証を使用する場合と同様です。ただし、透過 NTLM 認証には、パスワードが認証サーバーに送信されないというさらなる利点があり、クライアント アプリケーションが Secure Web Appliance を信頼するように設定されている場合はシングルサインオンを実現できます。

LDAP/基本

明示的な転送	透過
利点： • RFC ベース • NTLM よりも多くのブラウザをサポート • 最小限のオーバーヘッド • HTTPS (CONNECT) 要求で利用できる 欠点： • シングル サインオンなし • すべての要求でパスフレーズがクリア テキスト (Base64) として送信される 回避策： • 認証の失敗, on page 119	利点： • 明示的な転送よりも柔軟。 • NTLM よりも多くのブラウザをサポート • 認証をサポートしていないユーザー エージェントを使用する場合、ユーザーはサポートされるブラウザで最初に認証されるだけでよい • オーバーヘッドが比較的低い • ユーザーが以前に HTTP 要求で認証されている場合は、HTTPS 要求で利用できる 欠点： • シングル サインオンなし • パスフレーズがクリア テキスト (Base64) として送信される • 認証クレデンシャルが、ユーザーではなく、IP アドレスに関連付けられる (Citrix および RDP 環境では使用できず、ユーザーが IP アドレスを変更した場合も使用できない) 回避策： • 認証の失敗, on page 119

ユーザーの透過的識別

従来、ユーザーの識別および認証では、ユーザーにユーザー名とパスフレーズの入力を求めています。ユーザーが入力したクレデンシャルは認証サーバーによって認証され、その後、Web プロキシが、認証されたユーザー名に基づいてトランザクションに適切なポリシーを適用します。

しかし、Secure Web Applianceは、ユーザを透過的に認証するように設定することができます。つまり、エンドユーザにクレデンシャルを要求しません。透過的な識別では、別の信頼できるソースによってユーザーが認証済みであると想定し、そのソースから取得したクレデンシャルを使用してユーザーを認証して、適切なポリシーを適用します。

ユーザーを透過的に識別して以下を実行する場合があります。

- ユーザーがネットワーク上のプロキシの存在を意識しないように、シングル サイン オン環境を構築する。
- エンドユーザーに認証プロンプトを表示できないクライアント アプリケーションからのトランザクションに、認証ベースのポリシーを適用する。

ユーザーの透過的識別は、Web プロキシがユーザー名を取得して識別プロファイル割り当ての方法にのみ影響を与えます。ユーザー名を取得して識別プロファイル割り当てた後、Web プロキシは、識別プロファイルの割り当て方法に関係なく、通常どおり他のすべてのポリシーを適用します。

透過認証が失敗した場合、トランザクションを処理する方法を設定できます。ユーザーにゲストアクセスを許可するか、またはユーザーに認証プロンプトを表示することができます。

透過的ユーザー ID の失敗によりエンドユーザーに認証プロンプトが表示され、ユーザーが無効なクレデンシャルにより認証に失敗した場合、ユーザーのゲストアクセスを許可するかどうかを選択できます。



Note

再認証をイネーブルにしたが、URL フィルタリングによってトランザクションがブロックされている場合、エンドユーザー通知ページが表示され、別のユーザーとしてログインするオプションが提供されます。ユーザーがリンクをクリックすると、認証を求めるプロンプトが表示されます。詳細については、「[認証の失敗：異なるクレデンシャルによる再認証の許可, on page 125](#)」を参照してください。

透過的ユーザー識別について

透過的ユーザー識別は以下の方式で使用できます。

- [ISE によってユーザーを透過的に識別 (Transparently identify users with ISE)] : Identity Services Engine (ISE) サービスまたは Passive Identity Connector (ISE-PIC) サービスがイネーブルの場合に使用可能 ([ネットワーク (Network)] > [Identity Services Engine])。これらのトランザクションの場合、ユーザー名と関連するセキュリティグループタグは Identity Services Engine サーバーから取得されます。ISE-PIC を使用している場合は、ユーザー名と関連する ISE セキュリティグループが取得されます。[ISE/ISE-PIC サービスを統合するためのタスク, on page 420](#)を参照してください。
- [ASA によってユーザーを透過的に識別 (Transparently identify users with ASA)] : ユーザーは、Cisco 適応型セキュリティアプライアンスから受信した現在の IP アドレス対ユーザー名のマッピングによって識別されます (リモートユーザーのみ)。このオプションは、AnyConnect Secure Mobility がイネーブルになっており、ASA と統合されている場合に使用できます。ユーザー名は ASA から取得され、関連するディレクトリグループは Secure Web Appliance で指定された認証レルムまたはシーケンスから取得されます。[リモートユーザー, on page 396](#)を参照してください。
- [認証レルムによってユーザーを透過的に識別 (Transparently identify users with authentication realms)] : このオプションは、1 つ以上の認証レルムが、以下のいずれかの認証サーバーを使用して透過的識別をサポートするように設定されている場合に使用できます。
 - Active Directory : NTLM または Kerberos 認証レルムを作成し、透過的ユーザー識別をイネーブルにします。また、Cisco Context Directory Agent などの Active Directory エージェントを個別に展開する必要があります。詳細については、[Active Directory による透過的ユーザー識別, on page 83](#)を参照してください。

- LDAP : eDirectory として設定した LDAP 認証レルムを作成し、透過的ユーザー識別をイネーブルにします。詳細については、[LDAP による透過的ユーザー識別, on page 84](#) を参照してください。

AsyncOS for Web は eDirectory または Active Directory エージェントと定期的に通信して、認証されたユーザー名と現在の IP アドレスを照合するマッピングを保守します。

Active Directory による透過的ユーザー識別

Active Directory は、Secure Web Appliance などの他のシステムから簡単に照会できる形式でユーザー ログイン情報を記録しません。Cisco Context Directory Agent (CDA) などの Active Directory エージェントは、認証済みユーザーの情報を Active Directory セキュリティ イベント ログで照会する必要があります。

AsyncOS for Web は Active Directory エージェントと通信して、IP アドレス対ユーザー名のマッピングのローカル コピーを保守します。AsyncOS for Web は IP アドレスをユーザー名に関連付ける必要がある場合、最初にマッピングのローカルコピーをチェックします。一致が見つからない場合、Active Directory エージェントに照会して一致するものを見つけます。

Active Directory エージェントのインストールと設定については、以下の「Secure Web Appliance に情報を提供する Active Directory エージェントの設定」を参照してください。

Active Directory を使用してユーザーを透過的に識別する場合は、以下を考慮してください。

- Active Directory による透過的ユーザー識別は、NTLM または Kerberos 認証スキームでのみ機能します。Active Directory インスタンスに対応する LDAP 認証レルムでは使用できません。
- 透過的ユーザー ID は Active Directory エージェントがサポートする Active Directory のバージョンで動作します。
- 高可用性を実現するために、別のマシンに Active Directory エージェントの 2 番目のインスタンスをインストールできます。その場合、各 Active Directory エージェントは、他方のエージェントとは別個に、独自の IP アドレス対ユーザー名 マッピングを保持します。AsyncOS for Web は、プライマリ エージェントに対する ping の試行が 3 回失敗した後にバックアップとして Active Directory エージェントを使用します。
- Active Directory エージェントは、Secure Web Appliance と通信する際にオンデマンド モードを使用します。
- Active Directory エージェントは、Secure Web Appliance にユーザのログアウト情報をプッシュします。ただし、ユーザーのログアウト情報が Active Directory セキュリティ ログに記録されないことがあります。これは、クライアント マシンがクラッシュしたり、ユーザーがログアウトせずにマシンをシャットダウンした場合に発生します。ユーザーのログアウト情報がセキュリティ ログにないと、Active Directory エージェントは、IP アドレスがそのユーザーに割り当てられていないことをアプライアンスに通知できません。これを回避するために、Active Directory エージェントからのアップデートがない場合に AsyncOS が IP アドレス対ユーザーのマッピングをキャッシュしておく時間の長さを定義できます。

詳細については、[CLI を使用した透過的ユーザー識別の詳細設定, on page 86](#)を参照してください。

- Active Directory エージェントは、ユーザー名の一意性を確保するために、特定の IP アドレスからログインする各ユーザーの `sAMAccountName` を記録します。
- クライアント マシンが Active Directory サーバに提供するクライアントの IP アドレスと Secure Web Appliance は同一である必要があります。
- AsyncOS for Web はユーザーが属する上位の親グループだけを検索します。ネストされたグループは検索しません。

Secure Web Appliance に情報を提供する Active Directory エージェントの設定

AsyncOS for Web OS は、Active Directory から直接クライアントの IP アドレスを取得できないので、Active Directory エージェントから IP アドレス対ユーザー名のマッピング情報を取得する必要があります。

Secure Web Appliance にアクセスでき、表示されるすべての Windows ドメイン コントローラと通信できるネットワーク上のマシンに、Active Directory エージェントをインストールします。最高のパフォーマンスを実現するために、このエージェントは Secure Web Appliance に物理的にできるだけ近いところに配置する必要があります。小規模なネットワーク環境では、Active Directory サーバーに直接 Active Directory エージェントをインストールすることもできます。



Note Secure Web Appliance との通信に使用される Active Directory エージェントのインスタンスは、シスコの適応型セキュリティアプライアンスやその他の Secure Web Appliance など、他のアプライアンスもサポートできます。

Cisco Context Directory Agent の取得、インストール、および設定

Cisco Context Directory Agent のダウンロード、インストール、および設定に関する詳細については、http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda10.html を参照してください。



Note Secure Web Appliance と Active Directory エージェントは、RADIUS プロトコルを使用して相互に通信します。アプライアンスとエージェントは、ユーザーのパスワードを難読化するために同じ共有秘密キーを使用して設定する必要があります。その他のユーザー属性は難読化されません。

LDAP による透過的ユーザー識別

AsyncOS for Web は、Lightweight Directory Access Protocol (LDAP) レルムとして設定されている eDirectory サーバーと通信し、IP アドレス対ユーザー名のマッピングを保守できます。eDirectory クライアントを介してログインする場合、ユーザーは eDirectory サーバーに対して

認証されます。認証に成功すると、ログインしたユーザーの属性（NetworkAddress）としてクライアントの IP アドレスが eDirectory サーバーに記録されます。

LDAP（eDirectory）を使用してユーザーを透過的に識別する場合は、以下を考慮してください。

- eDirectory クライアントを各クライアント ワークステーションにインストールし、エンドユーザーがそれを使用して eDirectory サーバーによる認証を受けるようにする必要があります。
- eDirectory クライアントのログインで使用する LDAP ツリーは、認証レルムに設定されている LDAP ツリーと同一である必要があります。
- eDirectory クライアントが複数の LDAP ツリーを使用する場合は、ツリーごとに認証レルムを作成し、各 LDAP 認証レルムを使用する認証シーケンスを作成します。
- eDirectory として LDAP 認証レルムを設定する場合は、クエリー クレデンシャルのバインド DN を指定する必要があります。
- eDirectory サーバーは、ユーザーのログイン時にユーザー オブジェクトの NetworkAddress 属性を更新するように設定する必要があります。
- AsyncOS for Web はユーザーが属する上位の親グループだけを検索します。ネストされたグループは検索しません。
- eDirectory ユーザーの NetworkAddress 属性を使用して、ユーザーの最新のログイン IP アドレスを特定できます。

透過的ユーザー識別のルールとガイドライン

任意の認証サーバーで透過的ユーザー ID を使用する場合は、以下のルールとガイドラインを考慮してください。

- DHCP を使用してクライアント マシンに IP アドレスを割り当てる場合は、Secure Web Appliance 上の IP アドレス対ユーザ名のマッピングが DHCP リースよりも頻繁に更新されるようにします。tuiconfig CLI コマンドを使用して、マッピングの更新間隔を更新します。詳細については、[CLI を使用した透過的ユーザー識別の詳細設定, on page 86](#)を参照してください。
- IP アドレス対ユーザ名のマッピングが Secure Web Appliance 上で更新される前に、ユーザーがマシンからログアウトし、別のユーザが同じマシンにログインした場合、Web プロキシは前のユーザをクライアントとして記録します。
- 透過的ユーザー識別に失敗した場合に Web プロキシがトランザクションを処理する方法を設定できます。ユーザーにゲストアクセスを許可するか、または認証プロンプトをエンドユーザーに強制的に表示することができます。
- 透過的ユーザー ID の失敗によりユーザーに認証プロンプトが表示され、ユーザーが無効なクレデンシャルにより認証に失敗した場合、ユーザーのゲストアクセスを許可するかどうかを選択できます。
- 割り当てられた識別プロファイルが、ユーザーが存在する複数のレルムを含む認証シーケンスを使用している場合、AsyncOS for Web はシーケンスで示される順序でレルムからユーザー グループを取得します。

- ユーザーを透過的に識別するように識別プロファイルを設定する場合、認証サロゲートは IP アドレスでなければなりません。別のサロゲートタイプを選択することはできません。
- ユーザーの詳細なトランザクションを表示すると、透過的に識別されたユーザーが [Web トラッキング (Web Tracking)] ページに表示されます。
- `%m` および `x-auth-mechanism` カスタムフィールドを使用して、透過的に識別されたユーザーをアクセスログと WC3 ログに記録することができます。SSO_TUI のログエントリは、ユーザー名が、透過的ユーザー識別により認証されたユーザー名をクライアント IP アドレスと照合することによって取得されたことを示しています。（同様に、SSO_ASA の値は、ユーザーがリモートユーザーであり、ユーザー名が AnyConnect Secure Mobility を使用して Cisco ASA から取得されたことを示しています）。

透過的ユーザー識別の設定

透過的なユーザーの識別と認証の設定については、[エンドユーザー クレデンシャルの取得の概要, on page 75](#)に詳しく記載されています。基本的な手順は以下のとおりです。

- 認証レルムを作成して、順序付けます。
- 識別プロファイルを作成し、ユーザーおよびクライアント ソフトウェアを分類します。
- 識別されたユーザーとユーザー グループからの Web 要求を管理するポリシーを作成します。

CLI を使用した透過的ユーザー識別の詳細設定

AsyncOS for Web は以下の TUI 関連の CLI コマンドを備えています。

- **tuiconfig** : 透過的ユーザー識別に関連する詳細設定を設定します。バッチ モードを使用して、複数のパラメータを同時に設定できます。
 - **Configure mapping timeout for Active Directory agent** : AD エージェントからのアップデートがない場合に、AD エージェントによって取得された IP アドレスに対して、IP アドレス対ユーザーのマッピングをキャッシュしておく時間の長さ（分単位）。
 - **Configure proxy cache timeout for Active Directory agent** : プロキシ固有の IP アドレス対ユーザーのマッピングをキャッシュしておく時間の長さ（秒単位）。有効な値は 5～1200 秒です。デフォルト値および推奨値は 120 秒です。より低い値を指定すると、プロキシのパフォーマンスに悪影響を及ぼします。
 - **Configure mapping timeout for Novell eDirectory** : サーバーからのアップデートがない場合に、eDirectory サーバーから取得された IP アドレスに対して、IP アドレス対ユーザーのマッピングをキャッシュしておく時間の長さ（秒単位）。
 - **Configure query wait time for Active Directory agent** : Active Directory エージェントからの応答を待機する時間の長さ（秒単位）。クエリーに要する時間がこのタイムアウト値を上回った場合、透過的ユーザー識別は失敗したと見なされます。これにより、エンドユーザーが体験する認証遅延が限定されます。

- **Configure query wait time for Novell eDirectory** : eDirectory サーバーからの応答を待機する時間の長さ（秒単位）。クエリーに要する時間がこのタイムアウト値を上回った場合、透過的ユーザー識別は失敗したと見なされます。これにより、エンドユーザーが体験する認証遅延が限定されます。

Active Directory の設定は、透過的ユーザー識別に AD エージェントを使用するすべての AD レルムに適用されます。eDirectory の設定は、透過的ユーザー識別に eDirectory を使用するすべての LDAP レルムに適用されます。

いずれかのパラメータの検証に失敗した場合は、どの値も変更されません。

- **tuistatus** : このコマンドには、以下のような AD 関連のサブコマンドがあります。
 - **adagentstatus** : すべての AD エージェントの現在のステータス、および Windows ドメイン コントローラとの接続に関する情報を表示します。
 - **listlocalmappings** : Secure Web Appliance に保存されているすべての IP アドレス対ユーザー名のマッピングを、AD エージェントによって取得された順序で一覧表示します。このコマンドは、エージェントに保存されているエントリや、現在クエリーが進行中のマッピングを一覧表示しません。

シングル サインオンの設定

透過的にクレデンシャルを取得することにより、シングルサインオン環境を実現できます。透過的ユーザー識別は認証レルムの設定項目の 1 つです。

Internet Explorer の場合は、リダイレクト ホスト名として、完全修飾ドメイン名ではなく、（ドットを含まない）短縮形のホスト名または NetBIOS 名を必ず使用してください。または、Internet Explorer の [ローカル イントラネット] ゾーンにアプライアンスのホスト名を追加することができます（[ツール] > [インターネット オプション] > [セキュリティ] タブ）。ただし、この操作をすべてのクライアントで実行する必要があります。これに関する詳細については、『[How do I properly set up NTLM with SSO \(credentials sent transparently\)?](#)』を参照してください。

Firefox およびその他の Microsoft 以外のブラウザでは、パラメータ **network.negotiate-auth.delegation-uris**、**network.negotiate-auth.trusted-uris**、**network.automatic-ntlm-auth.trusted-uris** を透過モードのリダイレクト ホスト名に設定する必要があります。『[Firefox is not sending authentication credentials transparently \(SSO\)](#)』も参照してください。この[記事](#)には、Firefox パラメータの変更に関する一般情報が記載されています。

リダイレクト ホスト名については、[グローバル認証の設定, on page 108](#)、または CLI コマンド `sethostname` を参照してください。

ハイ アベイラビリティ展開で Kerberos 認証を行うための Windows Active Directory におけるサービス アカウントの作成

Kerberos 認証でハイ アベイラビリティに関する問題が発生している場合は、この手順を使用します。ハイ アベイラビリティ展開で Kerberos 認証を使用するときに問題が発生する場所のシナリオは次のとおりです。

- ハイ アベイラビリティのホスト名の servicePrincipalName は、Active Directory 内の複数のコンピュータ アカウントに追加されます。
- Kerberos 認証は servicePrincipalName が Active Directory の 1 つのコンピュータ アカウントに追加されている場合に機能します。異なるアプライアンスノードでは、ケルベロスサービスチケットの復号に異なる暗号化文字列が使用されるため、プライマリノードが変更されると高可用性に影響を及ぼす可能性があります。

始める前に

- ハイ アベイラビリティで Kerberos 認証に使用するユーザー名を選択します。この目的のためだけに使用する新しいユーザー名を作成することをお勧めします。
- 既存のユーザー名を使用する場合には、次の設定を行います。
 - ユーザー名にパスワードがない場合は、パスワードを設定します。
 - ユーザー アカウントのプロパティ ダイアログボックス ([Active Directory ユーザーとコンピュータ (Active Directory users and computers)]) で、次のことを行います。

[ユーザーは次のログオン時にパスワード変更が必要 (User must change password at next logon)] チェック ボックスがオフになっていることを確認します。

[パスワードを無期限にする (Password Never Expires)] チェックボックスをオンにします。

手順

ステップ 1 [Active Directory ユーザーとコンピュータ (Active Directory users and computers)] で新しいユーザー名を作成します。

- パスワードを指定します。
- [ユーザーは次のログオン時にパスワード変更が必要 (User must change password at next logon)] チェックボックスをオフにします。
- [パスワードを無期限にする (Password Never Expires)] チェックボックスをオンにします。

ステップ 2 ハイ アベイラビリティのホスト名の SPN が、作成または選択した Active Directory ユーザー オブジェクトに関連付けられているかどうかを確認します。SPN には、http/ のプレフィックスが付けられ、その後にア

プライアンスのハイ アベイラビリティのホスト名が付けられます。クライアントが、ホスト名を解決できることを確認します。

1. Windows の `setspn -q` コマンドを使用して、既存の関連付けをクエリーします。

例 : `setspn -q http/highavail.com`

この例では、**highavail.com** は、アプライアンスのハイ アベイラビリティのホスト名です。

2. クエリの結果に応じて、SPN を削除するか、追加します。

(注)

ケルベロス HA サービスアカウントのパスワードには、文字、数字、スペース、および特殊文字 (~!@#%^&()-{}'/:;.,|+=*?<>) のみを含めることができます。これらの3つの特殊文字 \$、`、または " のいずれかがケルベロス HA サービスアカウントのパスワードで使用されている場合、GUI と CLI の両方からの事前認証中にエラーが発生します。ただし、認証はパスワードに使用されるあらゆる種類の文字で成功します。

クエリ結果	操作
「このようなSPNは見つかりませんでした。(No such SPN found.)」	ハイ アベイラビリティのホスト名の SPN を Active Directory ユーザーオブジェクトに関連付けます。 • 次のように <code>setspn -s</code> コマンドを使用します。 <pre>setspn -s http/highavail.com hausername</pre> この例で、highavail.com はアプライアンスのハイ アベイラビリティのホスト名で、hausername は作成または選択したユーザー名です。
「既存のSPNが見つかりました。(Existing SPN found!)」 「共通名 (CN) は、作成または選択したユーザー名を示しています。(The common name (CN) shows the user name created or chosen.)」 「例: CN=hausername (Example: CN=hausername)」	Active Directory でこれ以上の作業は必要ありません。

クエリ結果	操作
「既存のSPNが見つかりました。 (Existing SPN found!)」 「共通名 (CN) によって、作成または選択したユーザー名は表示されません。(The common name (CN) does not show the user name created or chosen.)」	1. SPN を削除します。 次のように <code>setspn -d</code> コマンドを使用します。 <pre>setspn -d http/highavail.com johndoe</pre> この例で、highavail.com は、アプライアンスのハイ アベイラビリティのホスト名で、johndoe は関連付けを解除するユーザー名です。 2. SPN を追加します。 次のように <code>setspn -s</code> コマンドを使用します。 <pre>setspn -s http/highavail.com hausername</pre> この例で、highavail.com はアプライアンスのハイ アベイラビリティのホスト名で、hausername は作成または選択したユーザー名です。

(注)

関連する Active Directory レلمで **keytab** 認証が有効になっていることを確認します。[Kerberos 認証方式の Active Directory レلمの作成 \(92 ページ\)](#) を参照してください。レلمがすでに作成されている場合は、レلمを編集し、**keytab** 認証を有効にします。

認証レلم

認証レلمによって、認証サーバーに接続するために必要な詳細情報を定義し、クライアントと通信するときに使用する認証方式を指定します。AsyncOS は複数の認証レلمをサポートしています。レلمを認証シーケンスにグループ化することにより、認証要件が異なるユーザーを同じポリシーで管理することができます。

認証フェールオーバー

現在のレلم設定では、プライマリ AD または LDAP が 1 つ、バックアップサーバーが 2 つあります。最初のプライマリサーバーに到達できない場合、クエリーは最初のバックアップサーバーに到達します。最初のバックアップサーバーにも到達できない場合、クエリーは 2 番目のサーバーに到達します。

Table 3: IPFW ルールを使用したフェールオーバー時間

フェールオーバー時間	プライマリからセカンダリへのバックアップへのフェールオーバーにかかる時間 (秒)
プライマリ AD と Secure Web Appliance の間の接続を切断するまでの時間	75 ~ 80

フェールオーバー時間	プライマリからセカンダリへのバックアップへのフェールオーバーにかかる時間（秒）
プライマリ AD と Secure Web Applianceの間の接続を切断し、かつ最初のバックアップと Secure Web Applianceの間の接続も切断するまでの時間	180 ～ 250
プライマリ AD を再起動するまでの時間	42 秒
プライマリ AD の電源がオフになるまでの時間	75 ～ 80
プライマリ AD と最初のバックアップサーバーの電源がオフになるまでの時間	180 ～ 250

複数のサーバーがダウンしている場合は、動作しているドメインコントローラが見つかるまで、Secure Web Applianceで接続の確立を再試行します。

- [外部認証, on page 91](#)
- [Kerberos 認証方式の Active Directory レルムの作成, on page 92](#)
- [Active Directory 認証レルムの作成（NTLMSSP および基本）, on page 97](#)
- [LDAP 認証レルムの作成, on page 100](#)
- [認証レルムの削除について, on page 107](#)
- [グローバル認証の設定, on page 108](#)

関連項目

- [認証シーケンス, on page 117](#)
- [RADIUS ユーザー認証, on page 175](#)

外部認証

外部 LDAP または RADIUS サーバーからユーザーを認証できます。

LDAP サーバーによる外部認証の設定

Before you begin

LDAP 認証レルムを作成し、それに 1 つ以上の外部認証クエリーを設定します。[LDAP 認証レルムの作成, on page 100](#)。

Procedure

ステップ 1 アプライアンスで外部認証を有効にします。

- [システム管理 (System Administration)] > [ユーザー (Users)] に移動します。
- [外部認証 (External Authentication)] セクションで [有効 (Enable)] をオンにします。
- 以下のオプションを設定します。

オプション	説明
外部認証を有効にする (Enable External Authentication)	—
認証タイプ (Authentication Type)	[LDAP] を選択します。
外部認証キャッシュタイムアウト (External Authentication Cache Timeout)	再認証のために LDAP サーバーに再接続するまで、AsyncOS が外部認証クレデンシャルを保存する秒数。デフォルトはゼロ (0) です。
LDAP 外部認証クエリー (LDAP External Authentication Query)	LDAP レルムにより設定されたクエリー。
サーバーからの有効なレスポンス待ちタイムアウト (Timeout to wait for valid response from server)	AsyncOS がサーバーからのクエリーに対する応答を待機する秒数。
グループ マッピング (Group Mapping)	ディレクトリ内の各グループ名にロールを割り当てます。

ステップ 2 変更を送信し、保存します。

RADIUS 外部認証のイネーブル化

「[RADIUS を使用した外部認証の有効化, on page 176](#)」を参照してください。

Kerberos 認証方式の Active Directory レルムの作成

Before you begin

- アプライアンスが (クラウドコネクタモードではなく) 標準モードで設定されていることを確認します。
- 高可用性を設定する場合、**手順 9** で指定した [ケルベロス高可用性 (Kerberos High Availability)] セクションの [キータブ認証を使用する (Use keytab authentication)] チェックボックスもオンにしてください。

アプライアンスが、ロードバランサなどの HTTP/HTTPS トラフィック分散デバイスの背後にある場合は、Active Directory 内のトラフィック分散デバイスの SPN をユーザーアカウントに関連付けて、[ケルベロス高可用性 (Kerberos High Availability)] セクションでそのユーザーアカウントのログイン情報を入力する必要があります。ネットワークポロジで、トラフィックをリダイレクトする最初のデバイスの SPN を追加する必要があります。たとえば、クライアントデバイスの送信ネットワークトラフィックがトラフィックマネージャ、ロードバランサ、および Secure Web Appliance を通過する場合、トラフィックマネージャの SPN を Active Directory のユーザーアカウントに追加し、このセクションでユーザークレデンシャルを入力する必要があります。これは、トラフィックマネージャがクライアントデバイスのトラフィックを検出する最初のデバイスであるためです。

- Active Directory サーバーを準備します。
 - 次のサーバーのいずれかに Active Directory をインストールします。Windows Server 2003、2008、2008R2、2012、2016 (coeus 11.8、12.0、12.5、14.0、14.5)、または 2019 (coeus 14.5 のみ)。
coeus 12.5 用の Active Directory Windows Server 2019 をインストールできます。
 - Active Directory サーバーでユーザーを作成します。
 - ドメイン管理者グループまたはアカウント オペレータ グループのメンバーであるユーザーを Active Directory サーバー上に作成します。
または
 - 次の権限を持つユーザー名を作成します。
 - Active Directory でのパスワードリセット権限
 - servicePrincipalName への検証済み書き込み
 - アカウント制限事項の書き込み
 - dNSHost 名の書き込み
 - servicePrincipalName の書き込み
- クライアントをドメインに参加させます。サポートされるクライアントは、Windows XP、Windows 10、Mac OS 10.5+ です。
- Windows Resource Kit の krbtray ツールを使用して、クライアントの Kerberos チケットを確認します (<http://www.microsoft.com/en-us/download/details.aspx?id=17657>)。
- Mac クライアントでは、[メイン メニュー (Main Menu)] > [Keychain Access] で、Ticket Viewer アプリケーションを使用して Kerberos チケットを確認できます。

- 認証元となる Active Directory ドメインに Secure Web Applianceを参加させるために必要な権限とドメイン情報を取得済みであることを確認します。
- Secure Web Applianceの現在の時刻と Active Directory サーバの現在時刻を比較して、その差が Active Directory サーバの [コンピュータ クロック同期の最大許容時間 (Maximum tolerance for computer clock synchronization)] オプションで指定されている時間を超えていないことを確認します。
- Secure Web Applianceがセキュリティ管理アプライアンスで管理されている場合は、異なる Secure Web Appliance上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同一になるように設定しておきます。
- Secure Web Applianceの設定 :
 - 明示的モードでは、Secure Web Applianceのホスト名 (sethostname CLI コマンド) をブラウザで設定されているプロキシ名と同じにする必要があります。
 - 透過モードでは、Secure Web Applianceのホスト名をリダイレクトホスト名と同じにする必要があります (グローバル認証の設定, on page 108を参照)。さらに、Kerberos レルムを作成する前に、Secure Web Applianceのホスト名とリダイレクトホスト名を設定する必要があります。
- 新しいレルムを確定すると、レルムの認証プロトコルを変更できなくなるので注意してください。
- シングルサインオン (SSO) をクライアントブラウザで設定する必要があります (シングルサインオンの設定, on page 87 を参照)。
- ログの使用を簡素化するため、%mのカスタムフィールドのパラメータを使用してアクセス ログをカスタマイズします。アクセス ログのカスタマイズ, on page 714を参照してください。

**Note**

ケルベロス HA サービスアカウントのパスワードには、文字、数字、スペース、および特殊文字 (~!@#%^&()_-{}'/:;.,|+=*?<>) のみを含めることができます。これらの3つの特殊文字 \$、`、または " のいずれかがケルベロス HA サービスアカウントのパスワードで使用されている場合、GUI と CLI の両方からの事前認証中にエラーが発生します。ただし、認証はパスワードに使用されるあらゆる種類の文字で成功します。

Procedure

- ステップ 1 Cisco Secure Web Applianceの Web インターフェイスで、[ネットワーク (Network)] > [認証 (Authentication)] を選択します。
- ステップ 2 [レルムを追加 (Add Realm)] をクリックします。
- ステップ 3 英数字とスペース文字だけを使用して、認証レルムに一意の名前を割り当てます。

ステップ 4 [認証プロトコル (Authentication Protocol)] フィールドで [Active Directory] を選択します。

ステップ 5 Active Directory サーバーの完全修飾ドメイン名または IP アドレスを 3 つまで入力します。

例: ntlm.example.com

IP アドレスが必要なのは、アプライアンスで設定されている DNS サーバーが Active Directory サーバーのホスト名を解決できない場合だけです。

レルムに複数の認証サーバーを設定した場合、アプライアンスは、そのレルム内のトランザクションの認証に失敗するまでに最大 3 つの認証サーバーで認証を試みます。

ステップ 6 アプライアンスをドメインに参加させます。

a) Active Directory アカウントを設定します。

設定	説明
Active Directory ドメイン (Active Directory Domain)	Active Directory サーバーのドメイン名。DNS ドメインまたはレルムとも呼ばれます。
NetBIOS ドメイン名 (NetBIOS domain name)	ネットワークで NetBIOS を使用する場合は、ドメイン名を入力します。 Tip このオプションを使用できない場合は、setntlmsecuritymode CLI コマンドを使用して、NTLM セキュリティ モードが [ドメイン (domain)] に設定されていることを確認します。
コンピュータ アカウント (Computer Account)	ドメイン上のコンピュータを一意的に識別する Active Directory コンピュータ アカウント (別名「マシン信頼アカウント」) が作成される、Active Directory ドメイン内の場所を指定します。 Active Directory 環境で、コンピュータ オブジェクトが一定の間隔で自動的に削除される場合は、自動削除から保護されているコンテナ内にコンピュータ アカウントの場所を指定します。
信頼できるドメインのヘルスチェックを有効にする	レルムの信頼できるドメインルックアップの動作を制御するために、 [信頼できるドメインのヘルスチェックを有効にする (Enable Trusted Domain Health Check)] オプションが [Active Directory アカウント (Active Directory Account)] セクション ([ネットワーク (Network)] > [認証 (Authentication)] > [レルムの追加 (Add Realm)]) に追加されました。 このオプションは、デフォルトでは有効になっています。

b) [ドメインに参加 (Join Domain)] をクリックします。

Note

すでに参加しているドメインに参加しようとする (同じクレデンシャルを使用している場合でも)、Active Directory が新しいキーセットをこの Secure Web Appliance を含むすべてのクライアントに送信するため、既存の接続は閉じます。影響を受けるクライアントは、ログオフしてから再度ログインする必要があります。

Note

AWS に展開された Secure Web Appliance のホスト名は一意である必要があります。一意のホスト名を作成するには、ホスト名の最初の文字列を変更する必要があります。

たとえば、「mgmt」が最初の文字列としてホスト名に追加されている場合、「mgmt<wsa_hostname>」として変更できます。

- c) Active Directory 上のアカウントにログイン クレデンシャル（ユーザー名およびパスワード）を指定し、[アカウントの作成（Create Account）] をクリックします。

ステップ 7 (オプション) 透過的ユーザー識別を設定します。

設定	説明
Active Directory を使用して透過ユーザー識別を有効にする（Enable Transparent User Identification using Active Directory agent）	プライマリ Context Directory エージェントがインストールされているマシンのサーバー名と、それにアクセスするために使用する共有秘密の両方を入力します。 （オプション）バックアップ Context Directory エージェントがインストールされているマシンのサーバー名とその共有秘密を入力します。

ステップ 8 ネットワーク セキュリティを設定します。

設定	説明
クライアントの署名が必須（Client Signing Required）	クライアントの署名を要求するように Active Directory サーバーが設定されている場合は、このオプションを選択します。このオプションを選択すると、以下の場合に SMB 署名が有効になります。 • アプライアンスが Active Directory に接続するときにデジタル署名を配置する場合。 • 中間者攻撃を防ぐ場合。

ステップ 9 ハイ アベイラビリティを使用する場合は、[Kerberos ハイアベイラビリティ（Kerberos High Availability）] セクションで [キータブ認証を使用する（Use keytab authentication）] チェックボックスをオンにします。

- a) [ユーザー名（Username）] と [パスワード（Password）] を入力します。

ハイ アベイラビリティ クラスターの IP アドレスまたはホスト名に対応する SPN に関連付けられている Active Directory ユーザーの名前を入力します。ユーザー名にドメイン名を含めないでください（たとえば、「DOMAIN\johndoe」や「johndoe@domain」ではなく、「johndoe」と入力します）。ハイ アベイラビリティ展開の認証に使用されるサービス アカウントの作成に関する情報については、[ハイ アベイラビリティ展開で Kerberos 認証を行うための Windows Active Directory におけるサービス アカウントの作成](#), on page 88 を参照してください。

- b) ハイ アベイラビリティ クラスター内のすべてのアプライアンスについて、この手順を繰り返します。

Note

アプライアンスが、ロード バランサなどの HTTP/HTTPS トラフィック分散デバイスの背後にある場合は、Active Directory 内のトラフィック分散デバイスの SPN をユーザー アカウントに関連付けて、

[Kerberosハイアベイラビリティ (Kerberos High Availability)] セクションでそのユーザー アカウントのクレデンシャルを入力する必要があります。ネットワーク トポロジで、トラフィックをリダイレクトする最初のデバイスの SPN を追加する必要があります。たとえば、クライアントデバイスの送信ネットワークトラフィックがトラフィックマネージャ、ロードバランサ、および Secure Web Applianceを通過する場合、トラフィックマネージャの SPN を Active Directory のユーザーアカウントに追加し、このセクションでユーザークレデンシャルを入力する必要があります。これは、トラフィック マネージャがクライアント デバイスのトラフィックを検出する最初のデバイスであるためです。

- ステップ 10** (オプション) [テスト開始 (Start Test)] をクリックします。これにより、ユーザーが実際にそれらを使用して認証を受ける前に、入力した設定をテストして正しいかどうかを確認できます。テストの具体的な実行方法については、「[複数の NTLM レルムとドメインの使用, on page 107](#)」を参照してください。
- ステップ 11** テスト中に発生した問題をトラブルシューティングします。[認証の問題のトラブルシューティング ツール, on page 741](#)を参照してください。
- ステップ 12** 変更を送信し、保存します。

What to do next

Kerberos 認証方式を使用する識別プロファイルを作成します。[ユーザーおよびクライアント ソフトウェアの分類, on page 267](#)。

Active Directory 認証レルムの作成 (NTLMSSP および基本)

Active Directory 認証レルムの作成の前提条件 (NTLMSSP および基本)

- 認証元となる Active Directory ドメインに Secure Web Applianceを参加させるために必要な権限とドメイン情報を取得済みであることを確認します。
- NTLMセキュリティモードとして「domain」を使用する場合は、ネストした Active Directory グループのみを使用します。Active Directory グループがネストされていない場合は、デフォルト値の「ads」を使用します。このガイドの「コマンドライン インターフェイス」のトピックで `setntlmsecuritymode` を参照してください。
- Secure Web Applianceの現在の時刻と Active Directory サーバの現在時刻を比較して、その差が Active Directory サーバの [コンピュータ クロック同期の最大許容時間 (Maximum tolerance for computer clock synchronization)] オプションで指定されている時間を超えていないことを確認します。
- Secure Web Applianceがセキュリティ管理アプライアンスで管理されている場合は、異なる Secure Web Appliance上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同一になるように設定しておきます。
- 新しいレルムを確定すると、レルムの認証プロトコルを変更できなくなるので注意してください。

- Secure Web Applianceは、信頼できるすべてのドメインのドメインコントローラと、NTLM レalm に設定されたドメインコントローラに接続する必要があります。認証が正しく機能するように、内部ドメインおよび外部ドメインのすべてのドメインコントローラに対して次のポートを開く必要があります。
 - LDAP (389 UDP および TCP)
 - Microsoft SMB (445 TCP)
 - Kerberos (88 TCP)
 - エンドポイント解決：ポート マッパー (135 TCP) Net Log-on 固定ポート
- NTLMSSP の場合は、クライアントブラウザにシングルサインオン (SSO) を設定できません。「[シングルサインオンの設定, on page 87](#)」を参照してください。

複数の NTLM レalm とドメインの使用について

以下のルールは、複数の NTLM レalm とドメインを使用する場合に該当します。

- 最大 10 の NTLM 認証レalm を作成できます。
- ある NTLM レalm のクライアント IP アドレスが、別の NTLM レalm のクライアント IP アドレスと重複しないようにする必要があります。
- 各 NTLM レalm は 1 つの Active Directory ドメインにのみ参加できますが、そのドメインが信頼しているあらゆるドメインのユーザーを認証できます。この信頼は、同じフォレスト内の他のドメインにデフォルトで適用され、少なくとも一方向の信頼が存在しているフォレスト外部のドメインに適用されます。
- 既存の NTLM レalm が信頼していないドメインのユーザーを認証するには、追加の NTLM レalm を作成します。

Active Directory 認証レalm の作成 (NTLMSSP および基本)

Before you begin

アプライアンス内の番号の大きなポート (49152 ~ 65535) がファイアウォールでブロックされないことを確認します。これらのポートは、非同期グループルックアップ要求を実行する必要があります。これらのポートをブロックすると、断続的な認証エラーが発生する可能性があります。

Procedure

-
- ステップ 1 [ネットワーク (Network)] > [認証 (Authentication)] を選択します。
 - ステップ 2 [レalm を追加 (Add Realm)] をクリックします。
 - ステップ 3 英数字とスペース文字だけを使用して、認証レalm に一意の名前を割り当てます。
 - ステップ 4 [認証プロトコルと方式 (Authentication Protocol and Scheme(s))] フィールドで [Active Directory] を選択します。

ステップ5 Active Directory サーバーの完全修飾ドメイン名または IP アドレスを 3 つまで入力します。

例: active.example.com

IP アドレスが必要なのは、アプライアンスで設定されている DNS サーバーが Active Directory サーバーのホスト名を解決できない場合だけです。

レルムに複数の認証サーバーを設定した場合、アプライアンスは、そのレルム内のトランザクションの認証に失敗するまでに最大 3 つの認証サーバーで認証を試みます。

ステップ6 アプライアンスをドメインに参加させます。

a) Active Directory アカウントを設定します。

設定	説明
Active Directory ドメイン (Active Directory Domain)	Active Directory サーバーのドメイン名。DNS ドメインまたはレルムとも呼ばれます。
NetBIOS ドメイン名 (NetBIOS domain name)	ネットワークで NetBIOS を使用する場合は、ドメイン名を入力します。
コンピュータ アカウント (Computer Account)	ドメイン上のコンピュータを一意的に識別する Active Directory コンピュータ アカウント (別名「マシン信頼アカウント」) が作成される、Active Directory ドメイン内の場所を指定します。 Active Directory 環境で、コンピュータ オブジェクトが一定の間隔で自動的に削除される場合は、自動削除から保護されているコンテナ内にコンピュータ アカウントの場所を指定します。
信頼できるドメインのヘルスチェックを有効にする	レルムの信頼できるドメインルックアップの動作を制御するために、 [信頼できるドメインのヘルスチェックを有効にする (Enable Trusted Domain Health Check)] オプションが [Active Directory アカウント (Active Directory Account)] セクション ([ネットワーク (Network)]) > [認証 (Authentication)] > [レルムの追加 (Add Realm)] に追加されました。 このオプションは、デフォルトでは有効になっています。

b) [ドメインに参加 (Join Domain)] をクリックします。

Note

すでに参加しているドメインに参加しようとする (同じクレデンシャルを使用している場合でも)、Active Directory が新しいキーセットをこの Secure Web Appliance を含むすべてのクライアントに送信するため、既存の接続は閉じます。影響を受けるクライアントは、ログオフしてから再度ログインする必要があります。

Note

AWS に展開された Secure Web Appliance のホスト名は一意である必要があります。一意のホスト名を作成するには、ホスト名の最初の文字列を変更する必要があります。

たとえば、「mgmt」が最初の文字列としてホスト名に追加されている場合、「mgmt<wsa_hostname>」として変更できます。

- c) そのドメインにコンピュータ アカウントを作成する権限を持つ、既存の Active Directory ユーザーの sAMAccountName ユーザー名とパスワードを入力します。

例: 「jazzdoe」 (「DOMAIN\jazzdoe」や「jazzdoe@domain」は使用しないでください)。

この情報は、コンピュータ アカウントを確立するために一度だけ使用され、保存されません。

- d) [アカウントの作成 (Create Account)] をクリックします。

ステップ 7 (任意) 透過的認証を設定します。

設定	説明
Active Directory を使用して透過ユーザー識別を有効にする (Enable Transparent User Identification using Active Directory agent)	プライマリ Context Directory エージェントがインストールされているマシンのサーバー名と、それにアクセスするために使用する共有秘密の両方を入力します。 (オプション) バックアップ Context Directory エージェントがインストールされているマシンのサーバー名とその共有秘密を入力します。

ステップ 8 ネットワーク セキュリティを設定します。

設定	説明
クライアントの署名が必須 (Client Signing Required)	クライアントの署名を要求するように Active Directory サーバーが設定されている場合は、このオプションを選択します。このオプションを選択すると、以下の場合に SMB 署名が有効になります。 • アプライアンスが Active Directory に接続するときにデジタル署名を配置する場合。 • 中間者攻撃を防ぐ場合。

ステップ 9 (オプション) [テスト開始 (Start Test)] をクリックします。これにより、ユーザーが実際にそれらを使用して認証を受ける前に、入力した設定をテストして正しいかどうかを確認できます。

ステップ 10 変更を送信し、保存します。

LDAP 認証レルムの作成

Before you begin

- 組織の LDAP に関する以下の情報を取得します。
- LDAP のパージョン

- サーバーのアドレス
- LDAP ポート
- Secure Web Applianceがセキュリティ管理アプライアンスで管理されている場合は、異なる Secure Web Appliance上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同じであることを確認します。

Procedure

ステップ 1 [ネットワーク (Network)] > [認証 (Authentication)] を選択します。

ステップ 2 [レルムを追加 (Add Realm)] をクリックします。

ステップ 3 英数字とスペース文字だけを使用して、認証レルムに一意の名前を割り当てます。

ステップ 4 [認証プロトコルと方式 (Authentication Protocol and Scheme(s))] フィールドで [LDAP] を選択します。

ステップ 5 LDAP 認証の設定を入力します。

設定	説明
LDAP のバージョン (LDAP Version)	LDAP のバージョンを選択し、セキュア LDAP を使用するかどうかを選択します。 アプライアンスは、LDAP バージョン 2 および 3 をサポートしています。セキュア LDAP には LDAP バージョン 3 が必要です。 この LDAP サーバーが透過的ユーザー識別で使用する Novell eDirectory をサポートしているかどうかを選択します。

設定	説明
LDAP サーバー (LDAP Server)	LDAP サーバーの IP アドレスまたはホスト名、およびポート番号を入力します。最大 3 つのサーバーを指定できます。 ホスト名は、完全修飾ドメイン名である必要があります。例：ldap.example.com。IP アドレスが必要なのは、アプライアンスで設定されている DNS サーバーが LDAP サーバーのホスト名を解決できない場合のみです。 標準 LDAP のデフォルトのポート番号は 389 です。セキュア LDAP のデフォルトの番号は 636 です。 LDAP サーバーが Active Directory サーバーの場合は、ドメイン コントローラのホスト名または IP アドレス、およびポートを入力します。可能な限り、グローバル カタログ サーバーの名前を入力し、ポート 3268 を使用します。ただし、グローバル カタログ サーバーが物理的に離れた場所にあり、ローカル ドメイン コントローラのユーザーのみを認証する必要がある場合は、ローカル ドメイン コントローラを使用することもできます。 注： レールに複数の認証サーバーを設定した場合、アプライアンスは、そのレール内のトランザクションの認証に失敗するまでに最大 3 つの認証サーバーで認証を試みます。 AsyncOS バージョン 11.5 以降では、LDAP/NTLM（ドメインコントローラ通信）の送信元インターフェイスを指定できます。[送信元インターフェイスの設定（Set Source Interface）] チェックボックスをオンにし、ドロップダウンから送信元インターフェイスを選択します。
LDAP 持続的接続 (LDAP Persistent Connections) ([詳細設定 (Advanced)] セクションの下)	以下の値のいずれかを選択します。 • [永続的接続の使用（無制限）（Use persistent connections (unlimited)）]。既存の接続を使用します。使用できる接続がない場合は、新しい接続が開かれます。 • [永続的接続の使用（Use persistent connections）]。既存の接続を使用して、指定された数の要求に使用します。最大値に達すると、LDAP サーバーへの新しい接続が確立されます。 • [永続的接続を使用しない（Do not use persistent connections）]。必ず、LDAP サーバーへの新しい接続を作成します。

設定	説明
ユーザー認証 (User Authentication)	以下のフィールドに値を入力します。 [ベース識別名 (ベース DN) (Base Distinguished Name (Base DN))] LDAP データベースはツリー型のディレクトリ構造になっており、アプライアンスはベース DN を使用して、LDAP ディレクトリ ツリー内の適切な場所に移動し、検索を開始します。有効なベース DN フィルタ文字列は、object-value 形式の 1 つ以上のコンポーネントから構成されます。たとえば、「dc=companyname, dc=com」のように入力します。 Note このリリースにアップグレードした後で、このフィールドが空の場合、LDAP 認証の [テスト開始 (Start Test)] を実行できません。 [ユーザー名属性 (User Name Attribute)] 以下の値のいずれかを選択します。 • [uid]、[cn]、[sAMAccountName]。 ユーザー名を指定する、LDAP ディレクトリで一意の ID。 • [カスタム (custom)]。 「UserAccount」などのカスタム ID。 [ユーザーフィルタクエリー (User Filter Query)] ユーザー フィルタ クエリーは、ユーザーのベース DN を見つける LDAP 検索フィルタです。これは、ユーザー ディレクトリがベース DN の下の階層にある場合、またはそのユーザーのベース DN のユーザー固有コンポーネントにログイン名が含まれていない場合に必要です。 以下の値のいずれかを選択します。 • [なし (none)]。 すべてのユーザーを抽出します。 • [カスタム (custom)]。 ユーザーの特定のグループを抽出します。

設定	説明
クエリー クレデンシアル (Query Credentials)	認証サーバーが匿名クエリーを受け入れるかどうかを選択します。 認証サーバーが匿名クエリーを受け入れる場合は、[サーバーは、匿名の質問に対応します (Server Accepts Anonymous Queries)] を選択します。 認証サーバーが匿名クエリーを受け入れない場合は、[バインド DN を使用 (Use Bind DN)] を選択し、以下の情報を入力します。 • [バインド DN (Bind DN)]。LDAP ディレクトリの検索を許可された外部 LDAP サーバー上のユーザー。通常、バインド DN はディレクトリ全体の検索を許可されます。 • [パスフレーズ (Passphrase)]。[バインド DN (Bind DN)] フィールドに入力したユーザーに関連付けられているパスフレーズ。 以下のテキストは、[バインド DN (Bind DN)] フィールドに入力するユーザーの例を示しています。 cn=administrator,cn=Users,dc=domain,dc=com sAMAccountName=jdoe,cn=Users,dc=domain,dc=com. LDAP サーバーが Active Directory サーバーの場合は、「DOMAIN\username」の形式でバインド DN ユーザー名を入力することもできます。

ステップ 6 (オプション) グループ オブジェクトまたはユーザー オブジェクトを介して [グループ認証 (Group Authorization)] をイネーブルにし、選択したオプションを設定します。

グループ オブジェクト設定	説明
グループ オブジェクト内のグループ メンバーシップ属性 (Group Membership Attribute Within Group Object)	このグループに属するすべてのユーザーをリストする LDAP 属性を選択します。 以下の値のいずれかを選択します。 • [member] および [uniquemember]。グループ メンバを指定する、LDAP ディレクトリで一意的 ID。 • [カスタム (custom)]。 「UserInGroup」などのカスタム ID。
グループ名を含む属性 (Attribute that Contains the Group Name)	ポリシー グループの設定で利用できるグループ名を指定する LDAP 属性を選択します。 以下の値のいずれかを選択します。 • [cn]。グループ名を指定する、LDAP ディレクトリで一意的 ID。 • [カスタム (custom)]。 「FinanceGroup」などのカスタム ID。

グループオブジェクト設定	説明
オブジェクトがグループかどうかを判別するクエリ文字列 (Query string to determine if object is a group)	LDAP オブジェクトがユーザー グループを表しているかどうかを判別する LDAP 検索フィルタを選択します。 以下の値のいずれかを選択します。 • objectclass=groupofnames • objectclass=groupofuniquenames • objectclass=group • [カスタム (custom)]。 「objectclass=person」などのカスタム フィルタ。 注：クエリによって、ポリシー グループで使用できる一連の認証グループが定義されます。
ユーザーオブジェクト設定	説明
ユーザーオブジェクト内のグループメンバーシップ属性 (Group Membership Attribute Within User Object)	このユーザーが属するすべてのグループをリストする属性を選択します。 以下の値のいずれかを選択します。 • [memberOf]。ユーザー メンバを指定する、LDAP ディレクトリで一意的 ID。 • [カスタム (custom)]。 「UserInGroup」などのカスタム ID。
グループメンバーシップ属性は DN (Group Membership Attribute is a DN)	グループメンバーシップ属性が、LDAP オブジェクトを参照する識別名 (DN) であるかどうかを指定します。Active Directory サーバーの場合は、このオプションをイネーブルにします。 これをイネーブルにした場合は、以下の設定を指定する必要があります。
グループ名を含む属性 (Attribute that Contains the Group Name)	グループメンバーシップ属性が DN である場合に、ポリシー グループ設定でグループ名として使用できる属性を指定します。 以下の値のいずれかを選択します。 • [cn]。グループ名を指定する、LDAP ディレクトリで一意的 ID。 • [カスタム (custom)]。 「FinanceGroup」などのカスタム ID。

ユーザーオブジェクト 設定	説明
オブジェクトがグループかどうかを判別するクエリ文字列 (Query string to determine if object is a group)	LDAP オブジェクトがユーザー グループを表しているかどうかを判別する LDAP 検索フィルタを選択します。 以下の値のいずれかを選択します。 • objectclass=groupofnames • objectclass=groupofuniqueNames • objectclass=group • [カスタム (custom)]。「objectclass=person」などのカスタム フィルタ。 注：クエリーによって、Web Security Manager ポリシーで使用できる一連の認証グループが定義されます。

ステップ 7 (オプション) ユーザーに対する外部 LDAP 認証を設定します。

- [外部認証クエリ (External Authentication Query)] を選択します。
- ユーザー アカウントを特定します。

ベース DN (Base DN)	検索を開始する LDAP ディレクトリ ツリー内の適切な場所に移動するためのベース DN。
クエリ文字列	一連の認証グループを返すクエリー。例： <pre>(&(objectClass=posixAccount)(uid={u}))</pre> または <pre>(&(objectClass=user)(sAMAccountName={u}))</pre>
ユーザのフルネームが格納されている属性 (Attribute containing the user's full name)	LDAP 属性 (例：displayName、gecos)。

- (オプション) RFC 2307 アカウント有効期限 LDAP 属性に基づき、有効期限切れのアカウントはログインが拒否されます。
- ユーザーのグループ情報を取得するクエリーを入力します。

1 人のユーザーが複数の LDAP グループに属しており、それぞれユーザー ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザーに付与されます。

ベース DN (Base DN)	検索を開始する LDAP ディレクトリ ツリー内の適切な場所に移動するためのベース DN。
クエリ文字列	<pre>(&(objectClass=posixAccount)(uid={u}))</pre>

ベース DN (Base DN)	検索を開始する LDAP ディレクトリ ツリー内の適切な場所に移動するためのベース DN。
ユーザのフル ネームが格納されている属性 (Attribute containing the user's full name)	gecos

ステップ 8 (オプション) [テスト開始 (Start Test)] をクリックします。これにより、ユーザーが実際にそれらを使用して認証を受ける前に、入力した設定をテストして正しいかどうかを確認できます。テストの具体的な実行方法については、「[複数の NTLM レルムとドメインの使用, on page 107](#)」を参照してください。

Note

変更を送信して確定すると、後でレルムの認証プロトコルを変更できなくなります。

ステップ 9 変更を送信し、保存します。

What to do next

Kerberos 認証方式を使用する識別プロファイルを作成します。[ユーザーおよびクライアントソフトウェアの分類, on page 267](#) を参照してください。

関連項目

- [外部認証, on page 91](#)

複数の NTLM レルムとドメインの使用

以下のルールは、複数の NTLM レルムとドメインを使用する場合に該当します。

- 最大 10 の NTLM 認証レルムを作成できます。
- ある NTLM レルムのクライアント IP アドレスが、別の NTLM レルムのクライアント IP アドレスと重複しないようにする必要があります。
- 各 NTLM レルムは 1 つの Active Directory ドメインにのみ参加できますが、そのドメインが信頼しているあらゆるドメインのユーザーを認証できます。この信頼は、同じフォレスト内の他のドメインにデフォルトで適用され、少なくとも一方向の信頼が存在しているフォレスト外部のドメインに適用されます。
- 既存の NTLM レルムが信頼していないドメインのユーザーを認証するには、追加の NTLM レルムを作成します。

認証レルムの削除について

認証レルムを削除すると関連する ID がディセーブルになり、さらに、関連するポリシーからそれらの ID が削除されます。

認証レルムを削除すると、そのレルムがシーケンスから削除されます。

グローバル認証の設定

認証レルムの認証プロトコルとは別途に、グローバル認証の設定項目を設定してすべての認証レルムに設定を適用します。

Web プロキシの展開モードは、設定できるグローバル認証の設定項目に影響します。明示的な転送モードよりも、透過モードで展開されている場合の方がより多くの設定項目を使用できます。

Before you begin

以下の概念をよく理解しておいてください。

- [認証の失敗, on page 119](#)
- [認証の失敗：異なるクレデンシャルによる再認証の許可, on page 125](#)

Procedure

ステップ 1 [ネットワーク (Network)] > [認証 (Authentication)] を選択します。

ステップ 2 [グローバル設定を編集 (Edit Global Settings)] をクリックします。

ステップ 3 [グローバル認証設定 (Global Authentication Settings)] セクションで、設定を編集します。

設定	説明
認証サーバーが利用できない場合のアクション (Action if Authentication Service Unavailable)	以下の値のいずれかを選択します。 • [認証なしでトラフィックの通過を許可 (Permit traffic to proceed without authentication)]。処理が、ユーザーが認証されたかのように続行されます。 • [認証に失敗した場合にすべてのトラフィックをブロック (Block all traffic if user authentication fails)]。処理が中止され、すべてのトラフィックがブロックされます。
失敗した認証手続き (Failed Authentication Handling)	識別プロファイル ポリシーでユーザーにゲストアクセスを許可する場合は、この設定項目により、Web プロキシがユーザーをゲストとして識別してアクセス ログに記録する方法を指定します。 ユーザーのゲスト アクセス許可の詳細については、認証失敗後のゲストアクセスの許可, on page 123を参照してください。

設定	説明
再認証 (Re-authentication) (URLカテゴリまたはユーザーセッションの制限によりエンドユーザーがブロックされた場合に再認証プロンプトをイネーブルにする (Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction))	制限が厳しいURLフィルタリングポリシーによって、または別のIPアドレスへのログインの制限によってユーザーが Web サイトからブロックされた場合に、ユーザーに再認証を許可します。 新しい認証クレデンシアルを入力できるリンクが記載されたブロック ページがユーザーに表示されます。より多くのアクセスを許可するクレデンシアルをユーザーが入力すると、要求されたページがブラウザに表示されます。 注：この設定は、制限が厳しいURLフィルタリングポリシーまたはユーザーセッションの制限によってブロックされた、認証済みユーザーにのみ適用されます。認証されずに、サブネットによりブロックされたトランザクションには適用されません。 詳細については、認証の失敗：異なるクレデンシアルによる再認証の許可, on page 125を参照してください。
ベーシック認証トークン TTL (Basic Authentication Token TTL)	認証サーバーによって再検証されるまで、ユーザーのクレデンシアルがキャッシュ内に保管される期間を制御します。これには、ユーザー名とパスフレーズ、およびユーザーに関連付けられているディレクトリ グループが含まれます。 デフォルト値は推奨されている設定です。[サロゲートタイムアウト (Surrogate Timeout)]が設定されており、その値が[ベーシック認証トークン TTL (Basic Authentication Token TTL)] よりも大きい場合は、サロゲート タイムアウトの値が優先され、Web プロキシは、サロゲート タイムアウトの期限が切れた後に認証サーバーに連絡します。

その他の設定可能な認証設定項目は、Web プロキシが展開されているモード（透過モードまたは明示的な転送モード）に応じて異なります。

ステップ 4 Web プロキシが透過モードで展開されている場合は、以下の設定項目を編集します。

設定	説明
クレデンシアルの暗号化 (Credential Encryption)	クライアントが暗号化 HTTPS 接続を介して Web プロキシにログイン クレデンシアルを送信するかどうかを指定します。 この設定は基本認証方式と NTLMSP 認証方式の両方に適用されますが、特に基本認証方式の場合に役立ちます。基本認証方式では、ユーザー クレデンシアルがプレーン テキストで送信されるからです。 詳細については、認証の失敗, on page 119を参照してください。

設定	説明
HTTPS リダイレクト ポート (HTTPS Redirect Port)	HTTPS 接続を介してユーザー認証要求をリダイレクトする場合に使用する TCP ポートを指定します。 これによって、クライアントが HTTPS による Web プロキシへの接続を開始するポートが指定されます。これは、クレデンシャルの暗号化がイネーブルになっている場合や、アクセス コントロールの使用時にユーザーに認証を求める場合に発生します。
リダイレクト ホスト名 (Redirect Hostname)	Web プロキシが着信接続をリッスンするネットワーク インターフェイスの短いホスト名を入力します。 透過モードで展開されているアプライアンスに認証を設定した場合、Web プロキシは、ユーザーの認証のためにクライアントに送信するリダイレクション URL でこのホスト名を使用します。 以下の値のいずれかを入力できます。 • [1 語のホスト名 (Single word hostname)]。クライアントと Secure Web Appliance が DNS 解決可能な 1 語のホスト名を入力できます。これにより、クライアントは、ブラウザ側を設定することなく、Internet Explorer で真のシングル サインオンを実現できます。必ず、クライアントと Secure Web Appliance が DNS 解決可能な 1 語のホスト名を入力してください。たとえば、クライアントがドメイン <code>mycompany.com</code> にあり、Web プロキシがリッスンしているインターフェイスの完全なホスト名が <code>proxy.mycompany.com</code> である場合は、このフィールドに「<code>proxy</code>」と入力する必要があります。クライアントはプロキシに対してルックアップを実行し、<code>proxy.mycompany.com</code> を解決できます。 • [完全修飾ドメイン名 (FQDN) (Fully qualified domain name (FQDN))]。このフィールドに、FQDN または IP アドレスを入力することもできます。ただし、その場合、Internet Explorer や Firefox ブラウザで真のシングル サインオンを実現するには、入力する FQDN または IP アドレスが、クライアントブラウザのクライアント信頼済みサイト リストに追加されていることを確認する必要があります。デフォルト値は、プロキシ トラフィックに使用されるインターフェイスに応じて、M1 または P1 インターフェイスの FQDN です。

設定	説明
クレデンシャル キャッシュ オプション: (Credential Cache Options:) サロゲートタイムアウト (Surrogate Timeout)	クライアントに認証クレデンシャルを再度要求するまでに、Web プロキシが待機する時間を指定します。クレデンシャルを再度要求するまで、Web プロキシはサロゲートに保存された値 (IP アドレスまたは Cookie) を使用します。 一般的に、ブラウザなどのユーザー エージェントでは、ユーザーが毎回クレデンシャルを入力する必要がないように、認証クレデンシャルがキャッシュされます。
クレデンシャル キャッシュ オプション: (Credential Cache Options:) クライアント IP アイドルタイムアウト (Client IP Idle Timeout)	IP アドレスを認証サロゲートとして使用する場合は、この設定で、クライアントがアイドル状態のときに、認証クレデンシャルをクライアントに再要求するまで Web プロキシが待機する時間を指定します。 この値がサロゲートタイムアウト値よりも大きい場合、この設定には効力がなく、サロゲートタイムアウトに達した後にクライアントへの認証要求が行われます。 この設定を使用すると、コンピュータの前にはいない時間が多いユーザーの脆弱性を低減できます。
ユーザー セッション制限 (User Session Restrictions)	認証済みユーザーが複数の IP アドレスから同時にインターネットにアクセスすることを許可するかどうかを指定します。 ユーザーが未認証ユーザーと認証クレデンシャルを共有しないように、1つのマシンへのアクセスを制限できます。ユーザーが別のマシンでログインできない場合は、エンドユーザー通知ページが表示されます。このページの [再認証 (Re-authentication)] 設定を使用し、ユーザーがボタンをクリックして別のユーザー名でログインできるかどうかを指定することもできます。 この設定をイネーブルにする場合は、制限タイムアウト値を入力します。この値によって、別の IP アドレスでマシンにログインできるようになるまでのユーザーの待機時間を指定します。制限タイムアウト値は、サロゲートタイムアウト値よりも大きい値でなければなりません。 authcache CLI コマンドを使用して、認証キャッシュから特定のユーザーやすべてのユーザーを削除できます。

設定	説明
ヘッダー ベースの認証 (Header Based Authentication)	この設定により、Active Directory のヘッダー ベース認証スキームを構成できます。 ヘッダーベース認証のキャッシュ設定： • 認証キャッシュはデフォルトで有効になっています。 • 認証キャッシュのタイムアウトは、サロゲートタイムアウトと同じです。 • キャッシュには、ユーザー名とユーザーグループが保存されます。 Note ユーザーグループ設定を更新する場合は、認証キャッシュをクリアします。 テキスト エンコーディングとして ASCII を使用し、デフォルト設定の [バイナリのエンコーディングなし (No encoding for Binary)] を使用する [標準ヘッダー (Standard Header)] チェックボックスをオンにします。 着信グループヘッダーを考慮するために、[アクセスポリシーの照合に X-Authenticate-Groups ヘッダー/カスタムヘッダーのグループを使用する (Use Groups in X-Authenticate-Groups Header / Custom Header for match Access Policies)] チェックボックスをオンにします。カスタムヘッダー名を設定する場合は、[カスタムヘッダー名 (Custom Header Name)] オプションを使用します。 Note [アクセス ポリシーの照合に X-Authenticate-Groups ヘッダー/カスタムヘッダーのグループを使用する (Use Groups in X-Authenticate-Groups Header / Custom Header for match Access Policies)] チェックボックスをオンにして、X-Authenticated-Groups ヘッダーを入力しない場合は、アクセスポリシーの照合が失敗することがあります。有効になっていない場合は、Active Directory から取得されたグループがアクセス ポリシーと照合されます。 出力でヘッダー (ユーザーおよびグループヘッダー) を保持するには、[出力に認証詳細を残す (Retain Authentication Details on Egress)] チェックボックスをオンにします。
詳細設定 (Advanced)	クレデンシャルの暗号化またはアクセス コントロールを使用している場合は、アプライアンスがそれに付属しているデジタル証明書とキー (Cisco IronPort Web セキュリティアプライアンス デモ証明書) を使用するか、ここでアップロードするデジタル証明書を使用するかを選択できます。

ステップ 5 Web プロキシが明示的な転送モードで展開されている場合は、以下の設定項目を編集します。

設定	説明
クレデンシャルの暗号化 (Credential Encryption)	クライアントが暗号化HTTPS接続を介して Web プロキシにログインクレデンシャルを送信するかどうかを指定します。クレデンシャルの暗号化をイネーブルにするには、[HTTPS リダイレクト (セキュア) (HTTPS Redirect (Secure))] を選択します。クレデンシャルの暗号化をイネーブルにすると、認証のためにクライアントを Web プロキシにリダイレクトする方法を設定する追加フィールドが表示されます。 この設定は基本認証方式と NTLMSP 認証方式の両方に適用されますが、特に基本認証方式の場合に役立ちます。基本認証方式では、ユーザー クレデンシャルがプレーン テキストで送信されるからです。 詳細については、認証の失敗, on page 119を参照してください。
HTTPS リダイレクト ポート (HTTPS Redirect Port)	HTTPS 接続を介してユーザー認証要求をリダイレクトする場合に使用する TCP ポートを指定します。 これによって、クライアントがHTTPS による Web プロキシへの接続を開始するポートが指定されます。これは、クレデンシャルの暗号化がイネーブルになっている場合や、アクセス コントロールの使用時にユーザーに認証を求める場合に発生します。

設定	説明
リダイレクト ホスト名 (Redirect Hostname)	Web プロキシが着信接続をリッスンするネットワーク インターフェイスの短縮形のホスト名を入力します。 上記の認証モードをイネーブルにすると、Web プロキシは、ユーザーの認証のためにクライアントに送信するリダイレクション URL でこのホスト名を使用します。 以下の値のいずれかを入力できます。 • [1 語のホスト名 (Single word hostname)]。クライアントと Secure Web Appliance が DNS 解決可能な 1 語のホスト名を入力できます。これにより、クライアントは、ブラウザ側を設定することなく、Internet Explorer で真のシングル サインオンを実現できます。必ず、クライアントと Secure Web Appliance が DNS 解決可能な 1 語のホスト名を入力してください。たとえば、クライアントがドメイン mycompany.com にあり、Web プロキシがリッスンしているインターフェイスの完全なホスト名が proxy.mycompany.com である場合は、このフィールドに「proxy」と入力する必要があります。クライアントはプロキシに対してルックアップを実行し、proxy.mycompany.com を解決できます。 • [完全修飾ドメイン名 (FQDN) (Fully qualified domain name (FQDN))]。このフィールドに、FQDN または IP アドレスを入力することもできます。ただし、その場合、Internet Explorer や Firefox ブラウザで真のシングル サインオンを実現するには、入力する FQDN または IP アドレスが、クライアントブラウザのクライアント信頼済みサイト リストに追加されていることを確認する必要があります。デフォルト値は、プロキシトラフィックに使用されるインターフェイスに応じて、M1 または P1 インターフェイスの FQDN です。
クレデンシャル キャッシュ オプション: (Credential Cache Options:) サロゲートタイムアウト (Surrogate Timeout)	クライアントに認証クレデンシャルを再度要求するまでに、Web プロキシが待機する時間を指定します。クレデンシャルを再度要求するまで、Web プロキシはサロゲートに保存された値 (IP アドレスまたは Cookie) を使用します。 一般的に、ブラウザなどのユーザー エージェントでは、ユーザーが毎回クレデンシャルを入力する必要がないように、認証クレデンシャルがキャッシュされます。

設定	説明
クレデンシャル キャッシュ オプション: (Credential Cache Options) クライアント IP アイドル タイムアウト (Client IP Idle Timeout)	IP アドレスを認証サロゲートとして使用する場合は、この設定で、クライアントがアイドル状態のときに、認証クレデンシャルをクライアントに再要求するまで Web プロキシが待機する時間を指定します。 この値がサロゲート タイムアウト値よりも大きい場合、この設定には効力がなく、サロゲート タイムアウトに達した後にクライアントへの認証要求が行われます。 この設定を使用すると、コンピュータの前にはいない時間が多いユーザーの脆弱性を低減できます。
ユーザー セッション制限 (User Session Restrictions)	認証済みユーザーが複数の IP アドレスから同時にインターネットにアクセスすることを許可するかどうかを指定します。 ユーザーが未認証ユーザーと認証クレデンシャルを共有しないように、1つのマシンへのアクセスを制限できます。ユーザーが別のマシンでログインできない場合は、エンドユーザー通知ページが表示されます。このページの [再認証 (Re-authentication)] 設定を使用し、ユーザーがボタンをクリックして別のユーザー名でログインできるかどうかを指定することもできます。 この設定をイネーブルにする場合は、制限タイムアウト値を入力します。この値によって、別の IP アドレスでマシンにログインできるようになるまでのユーザーの待機時間を指定します。制限タイムアウト値は、サロゲートタイムアウト値よりも大きい値でなければなりません。 authcache CLI コマンドを使用して、認証キャッシュから特定のユーザーやすべてのユーザーを削除できます。

設定	説明
ヘッダー ベースの認証 (Header Based Authentication)	この設定により、Active Directory のヘッダー ベース認証スキームを構成できます。 ヘッダーベース認証のキャッシュ設定： • 認証キャッシュはデフォルトで有効になっています。 • 認証キャッシュのタイムアウトは、サロゲートタイムアウトと同じです。 • キャッシュには、ユーザー名とユーザーグループが保存されます。 Note ユーザーグループ設定を更新する場合は、認証キャッシュをクリアします。 テキスト エンコーディングとして ASCII を使用し、デフォルト設定の [バイナリのエンコーディングなし (No encoding for Binary)] を使用する [標準ヘッダー (Standard Header)] チェックボックスをオンにします。 着信グループヘッダーを考慮するために、[アクセスポリシーの照合に X-Authenticate-Groups ヘッダー/カスタム ヘッダーのグループを使用する (Use Groups in X-Authenticate-Groups Header / Custom Header for match Access Policies)] チェックボックスをオンにします。カスタムヘッダー名を設定する場合は、[カスタムヘッダー名 (Custom Header Name)] オプションを使用します。 Note [アクセス ポリシーの照合に X-Authenticate-Groups ヘッダー/カスタムヘッダーのグループを使用する (Use Groups in X-Authenticate-Groups Header / Custom Header for match Access Policies)] チェックボックスをオンにして、X-Authenticated-Groups ヘッダーを入力しない場合は、アクセスポリシーの照合が失敗することがあります。有効になっていない場合は、Active Directory から取得されたグループがアクセス ポリシーと照合されます。 出力でヘッダー (ユーザーおよびグループ ヘッダー) を保持するには、[出力に認証詳細を残す (Retain Authentication Details on Egress)] チェックボックスをオンにします。

設定	説明
詳細設定 (Advanced)	クレデンシャルの暗号化またはアクセス コントロールを使用している場合は、アプライアンスがそれに付属しているデジタル証明書とキー (Cisco IronPort Web セキュリティ アプライアンス デモ証明書) を使用するか、ここでアップロードするデジタル証明書を使用するかを選択できます。 デジタル証明書とキーをアップロードするには、[参照 (Browse)] をクリックして、ローカルマシン上の必要なファイルに移動します。次に、目的のファイルを選択してから、[ファイルのアップロード (Upload Files)] をクリックします。

ステップ 6 変更を送信し、保存します。

認証シーケンス

- [認証シーケンスについて, on page 117](#)
- [認証シーケンスの作成, on page 118](#)
- [認証シーケンスの編集および順序変更, on page 119](#)
- [認証シーケンスの削除, on page 119](#)

認証シーケンスについて

認証シーケンスを使用すると、さまざまな認証サーバーやプロトコルで 1 つの ID によってユーザーを認証できます。認証シーケンスは、プライマリ認証オプションを使用できなくなった場合にバックアップ オプションを提供する上でも役立ちます。

認証シーケンスは複数の認証レルムの集合です。使用するレルムには、さまざまな認証サーバーや認証プロトコルを指定できます。認証レルムの詳細については、[認証レルム, on page 90](#) を参照してください。

2 番目の認証レルムを作成すると、[ネットワーク (Network)] > [認証 (Authentication)] に、[すべてのレルム (All Realms)] というデフォルトの認証シーケンスを含む [レルム シーケンス (Realm Sequences)] セクションが自動的に表示されます。[すべてのレルム (All Realms)] シーケンスには、ユーザーが定義した各レルムが自動的に含まれます。[すべてのレルム (All Realms)] シーケンス内のレルムの順序は変更できますが、[すべてのレルム (All Realms)] シーケンスを削除したり、そこからレルムを削除することはできません。

複数の NTLM 認証レルムを定義した場合、Secure Web Appliance は、各シーケンスの 1 つの NTLM 認証レルムだけを NTLMSSP 認証方式で使します。[すべてのレルム (All Realms)] シーケンスを含め、各シーケンス内から、NTLMSSP で使用する NTLM 認証レルムを選択できます。複数の NTLM レルムで NTLMSSP を使用するには、2 つの認証レルムに対して 1 つの識

別プロファイルを設定し、1つのアイデンティティがすべてのレルムに使用されるようにします。レルム間には相互信頼関係がある必要があります。

認証で使用されるシーケンス内の認証レルムは、以下によって決まります。

- 使用される認証方式。通常これは、クライアントに入力したクレデンシャルタイプで指定されます。
- シーケンス内でのレルムの順序（1つの NTLMSSP レルムだけを使用できるので、基本レルムのみ）。



Tip 最適なパフォーマンスを得るには、1つのレルムを使用して同じサブネット上のクライアントを認証します。

認証シーケンスの作成

Before you begin

- 複数の認証レルムを作成します（[認証レルム](#), on page 90を参照）。
- Secure Web Applianceがセキュリティ管理アプライアンスで管理されている場合は、異なる Secure Web Appliance上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同じであることを確認します。
- AsyncOS では、レルムを使用して認証を処理する際に、リストの先頭のレルムから順番に使用されることに注意してください。

Procedure

ステップ 1 [ネットワーク (Network)] > [認証 (Authentication)] を選択します。

ステップ 2 [シーケンスを追加 (Add Sequence)] をクリックします。

ステップ 3 英数字とスペース文字を使用して、シーケンスの一意の名前を入力します。

ステップ 4 [基本スキームのレルムシーケンス (Realm Sequence for Basic Scheme)] 領域の最初の行で、シーケンスに含める最初の認証レルムを選択します。

ステップ 5 [基本スキームのレルム シーケンス (Realm Sequence for Basic Scheme)] 領域の 2 番目の行で、シーケンスに含める以下のレルムを選択します。

ステップ 6 (オプション) 基本クレデンシャルを使用する他のレルムを追加するには、[行の追加 (Add Row)] をクリックします。

ステップ 7 NTLM レルムを定義したら、[NTLMSSP スキームのレルム (Realm for NTLMSSP Scheme)] フィールドで NTLM レルムを選択します。

Web プロキシは、クライアントが NTLMSSP 認証クレデンシャルを送信するときに、この NTLM レルムを使用します。

ステップ 8 変更を送信し、保存します。

認証シーケンスの編集および順序変更

Procedure

ステップ 1 [ネットワーク (Network)] > [認証 (Authentication)] を選択します。

ステップ 2 編集または順序変更するシーケンスの名前をクリックします。

ステップ 3 レalmを配置するシーケンス内の位置番号に対応する行で、[レalm (Realms)] ドロップダウン リストからレalm名を選択します。

Note

[すべてのレalm (All Realms)] シーケンスの場合は、レalmの順序のみを変更できます。レalm自体を変更することはできません。[すべてのレalm (All Realms)] シーケンス内のレalmの順序を変更するには、[順序 (Order)] 列の矢印をクリックして、該当するレalmの位置を変更します。

ステップ 4 すべてのレalmをリストして順序付けするまで、必要に応じてステップ 3 を繰り返し、各レalm名が 1 つの行にのみ表示されていることを確認します。

ステップ 5 変更を送信し、保存します。

認証シーケンスの削除

Before you begin

認証レalmを削除すると関連する ID がディセーブルになり、さらに、関連するポリシーからそれらの ID が削除されるので注意してください。

Procedure

ステップ 1 [ネットワーク (Network)] > [認証 (Authentication)] を選択します。

ステップ 2 シーケンス名に対応するゴミ箱アイコンをクリックします。

ステップ 3 [削除 (Delete)] をクリックして、シーケンスを削除することを確定します。

ステップ 4 変更を保存します。

認証の失敗

- [認証の失敗について, on page 120](#)

- [問題のあるユーザー エージェントの認証のバイパス](#) , on page 120
- [認証のバイパス](#) , on page 122
- [認証サービスが使用できない場合の未認証トラフィックの許可](#) , on page 122
- [認証失敗後のゲスト アクセスの許可](#) , on page 123
- [認証の失敗：異なるクレデンシアルによる再認証の許可](#) , on page 125

認証の失敗について

以下の理由により認証に失敗したため、ユーザーが Web からブロックされることがあります。

- **クライアント/ユーザー エージェントの制限。**一部のクライアント アプリケーションでは、認証が適切にサポートされないことがあります。認証を必要としない識別プロファイルを設定し、識別プロファイルの基準をそのクライアント（およびアクセスする必要がある URL（オプション））に基づかせることで、これらのクライアントの認証をバイパスできます。
- **認証サービスを使用できない。**ネットワークまたはサーバーの問題によって、認証サービスを使用できない場合があります。このような状況が生じた場合に未認証トラフィックを許可することを選択できます。
- **クレデンシアルが無効である。**ユーザーによっては、適切な認証を得るための有効なクレデンシアルを提供できないことがあります（ビジターやクレデンシアルを待っているユーザーなど）。そのようなユーザーに制限付きの Web アクセスを許可するかどうかを選択できます。

関連項目

- [問題のあるユーザー エージェントの認証のバイパス](#) , on page 120
- [認証のバイパス](#) , on page 122
- [認証サービスが使用できない場合の未認証トラフィックの許可](#) , on page 122
- [認証失敗後のゲスト アクセスの許可](#) , on page 123

問題のあるユーザー エージェントの認証のバイパス

一部のユーザーエージェントには、通常の動作に影響する認証問題があることが判明されています。

以下のユーザー エージェント経由で認証をバイパスする必要があります。

- Windows Update エージェント
- MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT
- Microsoft BITS
- SLSSoapClient
- Akamai NetSession Interface
- Microsoft CryptoAPI
- NCSI
- MSDW
- Gnotify

- msde
- Google Update

**Note**

トラフィックのフィルタリング（URL カテゴリに基づく）とスキャン（McAfee、Webroot）は、引き続き、アクセス ポリシー設定に従い、アクセス ポリシーによって実行されます。

Procedure

ステップ 1 指定したユーザー エージェントとの認証をバイパスするように識別プロファイルを設定します。

- [Web セキュリティ マネージャ（Web Security Manager）]>[識別プロファイル（Identification Profile）] を選択します。
- [識別プロファイルの追加（Add Identification Profile）] をクリックします。
- 情報を入力します。

オプション	値
名前（Name）	ユーザー エージェントの AuthExempt 識別プロファイル。
上に挿入（Insert Above）	処理順序の最初のプロファイルに設定します。
サブネット別メンバの定義（Define Members by Subnet）	ブランクのままにします。
認証ごとにメンバを定義（Define Members by Authentication）	認証は不要です。

- [詳細設定（Advanced）]>[ユーザー エージェント（User Agents）] をクリックします。
- [選択なし（None Selected）] をクリックします。
- [カスタムユーザーエージェント（Custom User Agents）] で、問題のあるユーザー エージェントの文字列を指定します。

ステップ 2 アクセス ポリシーの設定

- [Web セキュリティ マネージャ（Web Security Manager）]>[アクセス ポリシー（Access Policies）] を選択します。
- [ポリシーを追加（Add Policy）] をクリックします。
- 情報を入力します。

オプション	値
ポリシー名	ユーザー エージェントの認証免除
上記ポリシーを挿入（Insert Above Policy）	処理順序の最初のポリシーに設定します。

オプション	値
識別プロファイル ポリシー (Identification Profile Policy)	ユーザー エージェントの AuthExempt 識別プロファイル。
詳細設定 (Advanced)	なし

ステップ 3 変更を送信し、保存します。

認証のバイパス

	手順	詳細情報
1	[詳細設定 (Advanced)] プロパティを設定して、影響を受ける Web サイトを含むカスタム URL カテゴリを作成します。	カスタム URL カテゴリの作成および編集, on page 305
2	以下の特性を持つ識別プロファイルを作成します。 • 認証を必要とする ID が特に配置されている。 • カスタム URL カテゴリが含まれている。 • 影響を受けるクライアント アプリケーションが含まれている。 • 認証を必要としない。	ユーザーおよびクライアント ソフトウェアの分類, on page 267
3	識別プロファイルのポリシーを作成します。	ポリシーの作成, on page 369

関連項目

- [Web プロキシのバイパス](#)

認証サービスが使用できない場合の未認証トラフィックの許可



Note

この設定は、認証サービスを使用できない場合にのみ適用されます。恒久的に認証をバイパスするわけではありません。代替の方法については、[認証の失敗について, on page 120](#)を参照してください。

Procedure

ステップ 1 [ネットワーク (Network)] > [認証 (Authentication)] を選択します。

ステップ 2 [グローバル設定を編集 (Edit Global Settings)] をクリックします。

ステップ 3 [認証サーバーが利用できない場合のアクション (Action if Authentication Service Unavailable)] フィールドで、[認証なしでトラフィックの通過を許可 (Permit traffic to proceed without authentication)] をクリックします。

ステップ 4 変更を送信し、保存します。

認証失敗後のゲスト アクセスの許可

ゲスト アクセスを許可するには、以下の手順を実行する必要があります。

1. [ゲスト アクセスをサポートする識別プロファイルの定義, on page 123](#)
2. [ゲスト アクセスをサポートしている識別プロファイルのポリシーでの使用, on page 124](#)
3. (オプション) [ゲスト ユーザーの詳細の記録方法の設定, on page 124](#)



Note

識別プロファイルがゲスト アクセスを許可しており、その識別プロファイルを使用しているユーザー定義のポリシーがない場合、認証に失敗したユーザーは適切なポリシー タイプのグローバルポリシーと照合されます。たとえば、MyIdentificationProfile がゲスト アクセスを許可し、MyIdentificationProfile を使用するユーザー定義のアクセス ポリシーがない場合、認証に失敗したユーザーはグローバル アクセス ポリシーに一致します。ゲスト ユーザーをグローバル ポリシーと照合しない場合は、ゲスト ユーザーに適用してすべてのアクセスをブロックするポリシー グループを、グローバル ポリシーよりも上に作成します。

ゲスト アクセスをサポートする識別プロファイルの定義

Procedure

ステップ 1 [Web セキュリティ マネージャ (Web Security Manager)] > [識別プロファイル (Identification Profiles)] を選択します。

ステップ 2 [識別プロファイルの追加 (Add Identification Profile)] をクリックして新しい ID を追加するか、使用する既存の ID の名前をクリックします。

ステップ 3 [ゲスト権限をサポート (Support Guest Privileges)] チェックボックスをオンにします。

ステップ 4 変更を送信し、保存します。

ゲスト アクセスをサポートしている識別プロファイルのポリシーでの使用

Procedure

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] メニューからポリシー タイプを選択します。
- ステップ 2** ポリシー テーブル内のポリシー名をクリックします。
- ステップ 3** [識別プロファイルおよびユーザー (Identification Profiles And Users)] ドロップダウンリストから、[1 つ以上の識別プロファイルを選択 (Select One Or More Identification Profiles)] を選択します (まだ選択していない場合)。
- ステップ 4** [識別プロファイル (Identification Profile)] 列のドロップダウン リストから、ゲスト アクセスをサポートしているプロファイルを選択します。
- ステップ 5** [ゲスト (認証に失敗したユーザー) (Guests (Users Failing Authentication))] オプション ボタンをクリックします。

Note

このオプションを使用できない場合は、選択した **プロファイル** がゲスト アクセスをサポートするように設定されていないことを示しています。ステップ 4 に戻って別のものを選択するか、[ゲスト アクセスをサポートする識別プロファイルの定義, on page 123](#) を参照して、新しいポリシーを定義してください。

- ステップ 6** 変更を送信し、保存します。

ゲスト ユーザーの詳細の記録方法の設定

Procedure

- ステップ 1** [ネットワーク (Network)] > [認証 (Authentication)] を選択します。
- ステップ 2** [グローバル設定を編集 (Edit Global Settings)] をクリックします。
- ステップ 3** [失敗した認証手続き (Failed Authentication Handling)] フィールドで、次に示す [ゲストユーザーのログ方法 (Log Guest User By)] のオプション ボタンをクリックします。

オプション ボタン	説明
IP アドレス (IP Address)	ゲスト ユーザーのクライアント IP アドレスがアクセス ログに記録されます。
エンドユーザーが入力したユーザー名 (User Name As Entered By End-User)	最初に認証に失敗したユーザー名がアクセス ログに記録されます。

- ステップ 4** 変更を送信し、保存します。

認証の失敗：異なるクレデンシャルによる再認証の許可

- 異なるクレデンシャルによる再認証の許可について, [on page 125](#)
- 異なるクレデンシャルによる再認証の許可, [on page 125](#)

異なるクレデンシャルによる再認証の許可について

前に使用したクレデンシャルが認証に失敗した場合に、ユーザーが別のクレデンシャルを使用して再認証を受けることを許可するには、再認証機能を使用します。ユーザーは正常に認証されますが、アクセスが許可されない限り、Web リソースにはアクセスできません。これは、認証は、検証したクレデンシャルをポリシーに渡すためにユーザーを識別するだけであり、リソースへのユーザーのアクセスを許可（または禁止）するのはポリシーだからです。

再認証を受けるには、ユーザーは正常に認証されている必要があります。

- ユーザー定義のエンドユーザー通知ページで再認証機能を使用するには、リダイレクト URL を解析する CGI スクリプトで `Reauth_URL` パラメータを解析して使用する必要があります。

異なるクレデンシャルによる再認証の許可

Procedure

-
- ステップ 1 [ネットワーク (Network)] > [認証 (Authentication)] を選択します。
 - ステップ 2 [グローバル設定を編集 (Edit Global Settings)] をクリックします。
 - ステップ 3 [URL カテゴリまたはユーザー セッションの制限によりエンドユーザーがブロックされた場合に再認証プロンプト (Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction)] チェックボックスをオンにします。
 - ステップ 4 [Submit] をクリックします。
-

識別済みユーザーの追跡



Note

アプライアンスがクッキーベースの認証サロゲートを使用するように設定されている場合、アプライアンスは HTTP 要求を介した HTTPS および FTP のクライアントからクッキー情報を取得しません。このため、クッキーからユーザー名を取得できません。

明示的要求でサポートされる認証サロゲート

サロゲート タイプ	クレデンシャルの暗号化がディセーブルの場合			クレデンシャルの暗号化がイネーブルの場合		
プロトコル:	HTTP	HTTPS および FTP over HTTP	ネイティブ FTP	HTTP	HTTPS および FTP over HTTP	ネイティブ FTP
サロゲートなし	対応	対応	対応	該当なし	該当なし	該当なし
IP ベース	対応	対応	対応	対応	対応	対応
Cookie ベース	対応	対応***	あり***	対応	非対応/対応**	対応***

透過的要求でサポートされる認証サロゲート



Note ユーザーおよびクライアントソフトウェアの分類, on page 267 の [認証サロゲート (Authentication Surrogates)] オプションの説明も参照してください。

サロゲート タイプ	クレデンシャルの暗号化がディセーブルの場合			クレデンシャルの暗号化がイネーブルの場合		
プロトコル:	HTTP	HTTPS	ネイティブ FTP	HTTP	HTTPS	ネイティブ FTP
サロゲートなし	N/A	該当なし	該当なし	該当なし	該当なし	該当なし
IP ベース	対応	非対応/対応*	非対応/対応*	対応	非対応/対応*	非対応/対応*
Cookie ベース	対応	非対応/対応**	非対応/対応**	対応	非対応/対応**	非対応/対応**

* クライアントが HTTP サイトに要求を送信し、認証された後に機能します。その前の動作は、トランザクションタイプによって異なります。

- **ネイティブ FTP トランザクション。** トランザクションが認証をバイパスします。
- **HTTPS トランザクション。** トランザクションがドロップされます。ただし、認証を目的とする最初の HTTPS 要求を復号するように HTTPS プロキシを設定できます。

** Cookie ベースの認証を使用している場合、Web プロキシは、HTTPS、ネイティブ FTP、および FTP over HTTP の各トランザクションに対してユーザーを認証できません。この制限により、すべての HTTPS、ネイティブ FTP、FTP over HTTP の要求が認証をバイパスするため、認証は要求されません。

*** この場合は、Cookie ベースのサロゲートが設定されていても、サロゲートは使用されません。

関連項目

- [識別プロファイルと認証](#), on page 277

再認証ユーザーの追跡

再認証の場合、より強力な権限を持つユーザーが認証を求め承認されると、Web プロキシは、設定されている認証サロゲートに応じた期間だけこのユーザーの ID をキャッシュします。

- **[セッション Cookie (Session cookie)]**。特権ユーザーのアイデンティティが、ブラウザを閉じるか、セッションがタイムアウトになるまで使用されます。
- **[永続的な Cookie (Persistent cookie)]**。特権ユーザーのアイデンティティが、サロゲートがタイムアウトするまで使用されます。
- **[IP アドレス (IP Address)]**。特権ユーザーのアイデンティティが、サロゲートがタイムアウトするまで使用されます。
- **[サロゲートなし (No surrogate)]**。デフォルトでは、Web プロキシは新しい接続ごとに認証を要求しますが、再認証がイネーブルの場合は新しい要求ごとに認証を要求します。そのため、NTLMSSP を使用すると認証サーバーの負荷が増大します。ただし、認証アクティビティの増加はユーザーにはわからない場合があります。ほとんどのブラウザでは、ブラウザが閉じられるまで特権ユーザーのクレデンシャルがキャッシュされ、再入力を求めることなく認証が行われるからです。また、Web プロキシが透過モードで展開され、**[明示的転送要求に同じサロゲート設定を適用 (Apply same surrogate settings to explicit forward requests)]** オプションがイネーブルでない場合は、明示的な転送要求に認証サロゲートが使用されず、再認証により負荷が増加します。



Note

Secure Web Applianceが認証サロゲートに Cookie を使用する場合は、クレデンシャルの暗号化をイネーブルにすることを推奨します。

資格情報

認証クレデンシャルは、ユーザーのブラウザまたは別のクライアントアプリケーションを介してユーザーに認証クレデンシャルの入力を求めることによってユーザーから取得されるか、または別のソースから透過的に取得されます。

- [セッション中のクレデンシャルの再利用の追跡](#), on page 128

- [認証および承認の失敗, on page 128](#)
- [クレデンシャルの形式, on page 128](#)
- [基本認証のクレデンシャルの暗号化, on page 129](#)

セッション中のクレデンシャルの再利用の追跡

セッション中に1回ユーザーを認証した後、認証サロゲートを使用すると、新しい要求ごとにユーザーを認証するのではなく、そのセッション全体におけるクレデンシャルの再利用を追跡できます。認証サロゲートは、ユーザーのワークステーションの IP アドレスまたはセッションに割り当てられた Cookie に基づくことができます。

Internet Explorer の場合は、リダイレクト ホスト名として、完全修飾ドメイン名ではなく、（ドットを含まない）短縮形のホスト名または NetBIOS 名を必ず使用してください。または、Internet Explorer の [ローカル イントラネット] ゾーンにアプライアンスのホスト名を追加することができます ([ツール] > [インターネット オプション] > [セキュリティ] タブ)。ただし、この操作をすべてのクライアントで実行する必要があります。これに関する詳細については、『[How do I properly set up NTLM with SSO \(credentials sent transparently\)?](#)』を参照してください。

Firefox およびその他の Microsoft 以外のブラウザでは、パラメータ **network.negotiate-auth.delegation-uris**、**network.negotiate-auth.trusted-uris**、**network.automatic-ntlm-auth.trusted-uris** を透過モードのリダイレクト ホスト名に設定する必要があります。『[Firefox is not sending authentication credentials transparently \(SSO\)](#)』も参照してください。この[記事](#)には、Firefox パラメータの変更に関する一般情報が記載されています。

リダイレクト ホスト名については、[グローバル認証の設定, on page 108](#)、または CLI コマンド `sethostname` を参照してください。

認証および承認の失敗

互換性のないクライアントアプリケーションなど、容認できる理由で認証に失敗した場合は、ゲスト アクセスを許可できます。

認証に成功したが、承認に失敗した場合は、要求したリソースへのアクセスが許可される可能性がある別のクレデンシャルセットによる再認証を許可できます。

関連項目

- [認証失敗後のゲスト アクセスの許可, on page 123](#)
- [異なるクレデンシャルによる再認証の許可, on page 125](#)

クレデンシャルの形式

認証方式	クレデンシャルの形式
NTLMSSP	MyDomain\jsmith

認証方式	クレデンシャルの形式
基本	jsmith MyDomain\jsmith Note ユーザーが Windows ドメインを入力しなかった場合は、Web プロキシによってデフォルトの Windows ドメインが付加されます。

基本認証のクレデンシャルの暗号化

基本認証のクレデンシャルの暗号化について

暗号化した形式でクレデンシャルを HTTPS 経由で送信するには、クレデンシャルの暗号化をイネーブルにします。これによって、基本認証プロセスのセキュリティが向上します。

デフォルトでは、Secure Web Applianceは、認証の安全を確保するために、自身の証明書と秘密キーを使用してクライアントとの HTTPS 接続を確立します。ただし、大部分のブラウザでは、この証明書が無効であることがユーザーに警告されます。無効な証明書に関するメッセージをユーザーに表示しないようにするには、組織で使用している有効な証明書とキーのペアをアップロードします。

クレデンシャル暗号化の設定

Before you begin

- IP サロゲートを使用するようにアプライアンスを設定します。
- (任意) 証明書と暗号化された秘密キーを取得します。ここで設定した証明書とキーは、アクセス コントロールでも使用されます。

Procedure

- ステップ 1 [ネットワーク (Network)] > [認証 (Authentication)] を選択します。
- ステップ 2 [グローバル設定を編集 (Edit Global Settings)] をクリックします。
- ステップ 3 [クレデンシャルの暗号化 (Credential Encryption)] フィールドで、[認証には暗号化された HTTPS 接続を使用 (Use Encrypted HTTPS Connection For Authentication)] チェックボックスをオンにします。
- ステップ 4 (任意) 認証時のクライアントの HTTPS 接続に対して、[HTTPSリダイレクトポート (HTTPS Redirect Port)] フィールドでデフォルトのポート番号 (443) を編集します。
- ステップ 5 (任意) 証明書とキーをアップロードします。
 - a) [詳細設定 (Advanced)] セクションを展開します。
 - b) [証明書 (Certificate)] フィールドで [参照 (Browse)] をクリックし、アップロードする証明書ファイルを検索します。

- c) [キー (Key)] フィールドで [参照 (Browse)] をクリックし、アップロードする秘密キー ファイルを検索します。
- d) [ファイルのアップロード (Upload File)] をクリックします。

ステップ 6 変更を送信し、保存します。

What to do next

関連項目

- [証明書の管理, on page 200。](#)

認証に関するトラブルシューティング

- [NTLMSSP に起因する LDAP ユーザーの認証の失敗, on page 742](#)
- [LDAP 参照に起因する LDAP 認証の失敗, on page 742](#)
- [基本認証の失敗, on page 743](#)
- [エラーによりユーザーがクレデンシャルを要求される, on page 743](#)
- [HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する, on page 759](#)
- [認証をサポートしていない URL にアクセスできない, on page 766](#)
- [クライアント要求がアップストリーム プロキシで失敗する, on page 767](#)



第 4 章

システム設定

この章で説明する内容は、次のとおりです。

- システム管理タスクの実行 (131 ページ)
- Cisco クラウド Web セキュリティ プロキシへのアプライアンスの接続 (225 ページ)
- Web 要求の代行受信 (234 ページ)

システム管理タスクの実行

この章で説明する内容は、次のとおりです。

- システム管理の概要 (132 ページ)
- アプライアンス設定の保存、ロード、およびリセット (132 ページ)
- Cisco Secure Web Appliance ライセンス (136 ページ)
- 仮想アプライアンスのライセンス (169 ページ)
- リモート電源再投入の有効化 (170 ページ)
- ユーザー アカウントの管理 (171 ページ)
- ユーザー プリファレンスの定義 (178 ページ)
- 管理者の設定 (178 ページ)
- ユーザー ネットワーク アクセス (181 ページ)
- 管理者パスフレーズのリセット (182 ページ)
- 生成されたメッセージの返信アドレスの設定 (182 ページ)
- アラートの管理 (183 ページ)
- FIPS Compliance (194 ページ)
- システムの日時の管理 (196 ページ)
- SSL の設定 (197 ページ)

- [証明書の管理 \(200 ページ\)](#)
- [AsyncOS for Web のアップグレードとアップデート \(206 ページ\)](#)
- [以前のバージョンの AsyncOS for Web への復元 \(215 ページ\)](#)
- [SNMP を使用したシステムの状態のモニタリング \(217 ページ\)](#)
- [Web トラフィック タップ \(Web Traffic Tap\) \(220 ページ\)](#)
- [HTTP 2.0 プロトコルの設定 \(224 ページ\)](#)

システム管理の概要

S シリーズ アプライアンスは、システム管理用の各種のツールを提供します。[システム管理 (System Administration)] タブの機能は、以下のタスクの管理を支援します。

- アプライアンスの設定
- 機能キー
- ユーザー アカウントの追加、編集、および削除
- AsyncOS ソフトウェアのアップグレードとアップデート
- システム時刻

アプライアンス設定の保存、ロード、およびリセット

Secure Web Appliance のすべての設定は、1 つの XML コンフィギュレーション ファイルで管理できます。

- [アプライアンス設定の表示と印刷, on page 132](#)
- [アプライアンス設定ファイルの保存, on page 133](#)
- [アプライアンス設定ファイルのロード, on page 134](#)
- [アプライアンス設定の出荷時デフォルトへのリセット, on page 135](#)

アプライアンス設定の表示と印刷

Procedure

ステップ 1 [システム管理 (System Administration)] > [設定のサマリー (Configuration Summary)] を選択します。

ステップ 2 必要に応じて、[設定のサマリー (Configuration Summary)] ページを表示または印刷します。

アプライアンス設定ファイルの保存

Procedure

ステップ 1 [システム管理 (System Administration)] > [設定ファイル (Configuration File)] を選択します。

ステップ 2 [設定ファイル (Configuration File)] のオプションを設定します。

オプション	説明
ファイル処理オプションの指定	生成された設定ファイルの処理方法を選択します。 • [表示または保存するローカルコンピュータにファイルをダウンロード (Download file to local computer to view or save)] • [ファイルをこのアプライアンス (wsa_example.com) に保存 (Save file to this appliance (example.com))] • [ファイルをメールで送信 (Email file to)] (1つまたは複数の電子メールアドレスを指定します)。
パスフレーズ処理オプションの指定	• [設定ファイルでパスフレーズをマスクする (Mask passphrases in the Configuration Files)] : エクスポートまたは保存されるファイルで、元のパスフレーズを「*****」に置き換えます。パスフレーズがマスクされた設定ファイルを直接 AsyncOS for Web にリロードすることはできません。 • [設定ファイル内のパスワードを暗号化する (Encrypt passphrases in the Configuration Files)] : FIPS モードが有効にされている場合、このオプションが使用可能になります。FIPS モードの有効化については、FIPS モードの有効化または無効化, on page 195を参照してください。
ファイル命名オプションの選択	設定ファイルに名前を付ける方法を選択します。 • [システムにより生成されたファイル名を使用 (Use system-generated file name)] • [ユーザー定義ファイル名を使用 : (Use user-defined file name:)]

ステップ 3 [Submit] をクリックします。

アプライアンス設定ファイルのロード



Caution

設定をロードすると、現在の設定がすべて完全に削除されます。以下の操作を実行する前に設定を保存することを強く推奨します。

以前のリリースから最新のリリースに設定をロードすることは推奨しません。パスをアップグレードすると構成時の設定を保持できます。

手動で変更した構成ファイルをロードすると、パフォーマンスと機能の問題が発生する可能性があります。



Note

互換性のあるコンフィギュレーションファイルが、アプライアンスの現在インストールされているバージョンより URL カテゴリのセットの古いバージョンに基づいている場合、コンフィギュレーション ファイルのポリシーと ID が自動的に変更される場合があります。



Note

設定ファイルをロードするときに証明書検証エラーが発生した場合は、証明書のルート CA を Secure Web Appliance の信頼されたルートディレクトリにアップロードしてから、設定ファイルを再度ロードします。ルート CA をアップロードする方法については、[証明書の管理](#), on page 200 を参照してください。

Procedure

ステップ 1 [システム管理 (System Administration)] > [設定ファイル (Configuration File)] を選択します。

ステップ 2 [設定をロード (Load Configuration)] オプションとロードするファイルを選択します。(注)

Note

- パスフレーズがマスクされているファイルはロードできません。
- ファイルには以下のヘッダーが必要です。

```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd">
```

また、正しくフォーマットされた **config** セクションも必要です。

```
<config> ...your configuration information in valid XML </config>
```

ステップ 3 [ロード (Load)] をクリックします。

ステップ 4 表示される警告を確認します。処理の結果を確認したら、[続行 (Continue)] をクリックします。

アプライアンス設定の出荷時デフォルトへのリセット

アプライアンス設定をリセットするときに、既存のネットワーク設定を保持するかどうかを選択できます。

このアクションでは、コミットする必要はありません。

Before you begin

アプライアンスから任意の場所に設定を保存します。

Procedure

- ステップ 1 [システム管理 (System Administration)] > [設定ファイル (Configuration File)] を選択します。
- ステップ 2 下方向にスクロールして、[構成のリセット (Reset Configuration)] セクションを表示します。
- ステップ 3 ページに表示された情報を読み、オプションを選択します。
- ステップ 4 [リセット (Reset)] をクリックします。

設定ファイルのバックアップの保存

設定ファイルバックアップ機能により、すべての変更でアプライアンスの設定が記録され、現在の設定ファイルよりも古い設定ファイルが、リモートに配置されたバックアップサーバーに FTP または SCP で送信されます。

手順

- ステップ 1 [システム管理 (System Administration)] > [設定ファイル (Configuration File)] を選択します。
 - ステップ 2 [設定のバックアップの有効化 (Enable Config Backup)] チェックボックスをオンにします。
 - ステップ 3 設定ファイルにパスフレーズを含める場合は [はい (Yes)] を選択します。設定ファイルからパスフレーズを除外する場合は [いいえ (No)] を選択します。
 - ステップ 4 取得方法を選択します。次のオプションを使用できます。
 - [リモートサーバー上のFTP (FTP on Remote Server)] : FTP ホスト名、ディレクトリ、ユーザー名、およびパスフレーズを入力します。
 - [リモートサーバー上のSCP (SCP on Remote Server)] : SCP ホスト名、ポート番号、ディレクトリ、およびユーザー名を入力します。
 - [ホストキーチェック (Host Key Checking)] : SSH は、使用されたすべてのホストの ID のデータベースを SSH が自動的に維持およびチェックします。ホストキーは、ディレクトリ `/.ssh/known_hosts` にあるユーザーのホームディレクトリに保存されます。
- [リモートサーバー上のSCP (SCP on Remote Server)] を選択し、[ホストキーチェックを有効化 (Enable Host Key Checking)] を選択する場合、次のオプションを使用できます。

- [自動 (Automatic)] : ホストキーは Cisco Secure Web Appliance によって自動的に設定されます。
- [手動 (Manual)] : ホストキーはユーザーが手動で入力できます。

変更を送信すると、Cisco Secure Web Appliance はリモートホスト上の承認されたキーファイルに追加する SSH キーを提供します。これにより、構成ファイルを Cisco Secure Web Appliance からリモートホストにアップロードできます。33 その結果、SSH は接続したことのあるすべてのホストの識別情報を含むデータベースを維持し、チェックします。ホストキーは、ディレクトリ `./ssh/known_hosts` にあるユーザーのホームディレクトリに保存されます。

ステップ 5 [送信 (Submit)] をクリックします。

CLI コマンドの `configbackup` を使用して設定ファイルバックアップ機能を有効にすることもできます。

Cisco Secure Web Appliance ライセンス

- [スマートソフトウェア ライセンシング \(136 ページ\)](#)

スマートソフトウェア ライセンシング

- [概要 \(Overview\) \(136 ページ\)](#)
- [Cisco Smart Software Manager でのアプライアンスの登録 \(140 ページ\)](#)
- [ライセンスの要求 \(143 ページ\)](#)
- [Cisco Smart Software Manager からのアプライアンスの登録解除 \(144 ページ\)](#)
- [Cisco Smart Software Manager でのアプライアンスの再登録 \(144 ページ\)](#)
- [転送設定の変更 \(145 ページ\)](#)
- [認証と証明書の更新 \(145 ページ\)](#)
- [機能ライセンスの予約 \(145 ページ\)](#)
- [スマート エージェントの更新 \(153 ページ\)](#)
- [アラート \(153 ページ\)](#)
- [コマンドライン インターフェイス \(154 ページ\)](#)

概要 (Overview)

スマートソフトウェア ライセンシングを使用すると、Cisco Secure Web Appliance のライセンスをシームレスに管理およびモニターできます。スマートソフトウェアライセンスをアクティブ化するには、Cisco Smart Software Manager (CSSM) でアプライアンスを登録する必要があります。CSSM は、購入して使用するすべてのシスコ製品についてライセンスの詳細を管理する一元化されたデータベースです。スマートライセンスを使用すると、製品認証キー (PAK) を

使用して Web サイトで個別に登録するのではなく、単一のトークンで登録することができます。

アプライアンスに登録すると、アプライアンスのライセンスを追跡し、CSSM ポータル経由でライセンスの使用状況を監視できます。アプライアンスにインストールされているスマートエージェントは、アプライアンスと CSSM を接続し、ライセンスの使用状況に関する情報を CSSM を渡して、CSSM が使用状況を追跡できるようにします。

Cisco Smart Software Manager については、
https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html
を参照してください。

始める前に

- ご利用のアプライアンスからインターネットに接続できることを確認します。
- Cisco Smart Software Manager ポータル (<https://software.cisco.com/#module/SmartLicensing>) でシスコ セールス チームに問い合わせるか、Cisco Smart Software Manager サテライトをネットワークにインストールしてください。

Cisco Smart Software Manager のユーザー アカウントの作成または Cisco Smart Software Manager サテライトのインストールの詳細については、「https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html」を参照してください。

ライセンスの使用状況に関する情報を直接インターネットに送信したくないユーザの場合、CSSM 機能のサブセットを提供する Smart Software Manager サテライトをオンプレミスにインストールすることもできます。サテライトアプリケーションをダウンロードして導入した後は、インターネットを使用して CSSM にデータを送信せずに、ライセンスをローカルで安全に管理できます。CSSM サテライトは、情報をクラウドに定期的に送信します。



(注) Smart Software Manager サテライトを使用する場合、Smart Software Manager サテライト Enhanced Edition 6.1.0 を使用してください。

- アプライアンスのシステム クロックを CSSM のシステム クロックと同期させる必要があります。アプライアンスのシステム クロックと CSSM のシステム クロックのずれは、スマート ライセンス操作の失敗の原因となります。



(注) インターネットに接続してプロキシ経由で CSSM に接続する場合、[システム管理 (System Administration)] > [アップグレードとアップデートの設定 (Upgrade and Update Settings)] を使用して、アプライアンスに設定されているプロキシと同じプロキシを使用する必要があります。



- (注) 仮想ユーザーの場合、新しい PAK ファイル（新規または更新）を受信するたびに、ライセンス ファイルを生成し、アプライアンスのファイルを読み込みます。ファイルを読み込んだ後は、PAK をスマート ライセンスに変換する必要があります。スマート ライセンス モードでは、ファイルのロード中、ライセンス ファイルの機能キー セクションは無視され、証明書情報のみが使用されます。

ライセンス予約

Cisco Smart Software Manager (CSSM) ポータルに接続せずに、Cisco Secure Web Appliance で有効になっている機能のライセンスを予約できます。これは主に、インターネットや外部デバイスとの通信がない高度にセキュリティ保護されたネットワーク環境に Cisco Secure Web Appliance を展開するユーザーにとって有益です。

機能ライセンスは、次のいずれかのモードで予約できます。

- [特定ライセンスの予約 (SLR) (Specific License Reservation (SLR))] : このモードを使用して、特定の期間の個々の機能（「HTTPS 復号」など）のライセンスを予約できます。
- [永久ライセンスの予約 (PLR) (Permanent License Reservation (PLR))] : このモードを使用して、すべての機能のライセンスを永久に予約できます。

Cisco Secure Web Appliance でライセンスを予約する方法の詳細については、[機能ライセンスの予約 \(145 ページ\)](#) を参照してください。

アプライアンスに対してスマート ソフトウェア ライセンシングを有効にするには、次の手順を実行する必要があります。

	操作内容	詳細情報
ステップ 2	Cisco Smart Software Manager でのアプライアンスの登録	Cisco Smart Software Manager でのアプライアンスの登録 (140 ページ)
(オプション) ステップ 3	必要に応じて、Cisco Secure Web Appliance で機能ライセンスを予約することができます。	機能ライセンスの予約 (145 ページ)
ステップ 3	ライセンス (機能キー) の要求	ライセンスの要求 (143 ページ)

スマートソフトウェア ライセンシングのイネーブル化

手順

ステップ 1 [システム管理 (System Administration)] > [スマートソフトウェアライセンスング (Smart Software Licensing)] を選択します。

ステップ 2 [スマートソフトウェアライセンスングの有効化 (Enable Smart Software Licensing)] をクリックします。

スマートソフトウェアライセンスングの詳細については、[スマートソフトウェアライセンスングの詳細](#)のリンクをクリックします。

ステップ 3 スマートソフトウェアライセンスングについての情報を読んだ後、[OK] をクリックします。

ステップ 4 変更を保存します。

次のタスク

スマートソフトウェアライセンスングを有効すると、クラシックライセンスモードのすべての機能がスマートライセンスモードでも自動的に使用可能になります。クラシックライセンスモードの既存ユーザーの場合、CSSMでアプライアンスを登録せずに、スマートソフトウェアライセンスング機能を使用できる 90 日間の評価期間があります。

有効期限および評価期間の期限の前に、一定の間隔（90 日前、60 日前、30 日前、15 日前、5 日前、および最終日）で通知が表示されます。評価期間の間または終了後に、CSSMでアプライアンスを登録できます。



(注)

- クラシック ライセンス モードにおけるアクティブなライセンスを持たない仮想アプライアンスの新規ユーザーの場合、スマート ソフトウェア ライセンシング機能を有効にしても、評価期間は提供されません。クラシック ライセンス モードにおけるアクティブなライセンスを持つ仮想アプライアンスの既存ユーザーのみに、評価期間が提供されます。新規仮想アプライアンス ユーザーがスマート ライセンス機能の評価を希望する場合には、シスコ セールス チームに連絡し、スマート アカウントに評価ライセンスを追加してください。評価ライセンスは、登録後に評価目的で使用されます。
- アプライアンスでスマート ライセンシング機能を有効にすると、スマート ライセンシングからクラシック ライセンシングモードにロールバックすることができなくなります。
- スマート ライセンス機能を有効にすると、次の機能が自動的に再起動されます。
 - Secure Web Appliance Web レピュテーションフィルタ (Web Reputation Filters)
 - Secure Web Appliance ウイルス対策 (Sophos)
 - Secure Web Appliance ウイルス対策 (Webroot)
 - Secure Web Appliance Web プロキシと DVS エンジン
- AsyncOS バージョン 15.0 では、新しい Cisco Secure Web Appliance 仮想展開に対してスマートライセンスを有効にできます。クラシックライセンスは必須ではありません。詳細については、「[Overview of Smart Licencing](#)」セクションにある前提条件を参照してください。

Cisco Smart Software Manager でのアプライアンスの登録

アプライアンスを Cisco Smart Software Manager (CSSM) に登録するには、[システム管理 (System Administration)] メニューでスマート ソフトウェア ライセンシング機能を有効にする必要があります。



(注)

- 複数のアプライアンスを単一のインスタンスで登録することはできません。アプライアンスを 1 つずつ登録する必要があります。
- 初回登録の有効期間は 1 年です。登録の更新は、アプライアンスが CSSM に接続できる場合、6 か月ごとに自動的に実行されます。

手順

ステップ 1 [システム管理 (System Administration)] > [スマート ソフトウェア ライセンシング (Smart Software Licensing)] を選択します。

ステップ 2 [スマートライセンスの登録 (Smart License Registration)] オプションを選択します。

ステップ 3 [確認 (Confirm)] をクリックします。

ステップ 4 [トランスポート設定 (Transport Settings)] を変更する場合には、[編集 (Edit)] をクリックします。次のオプションを使用できます。

- **[直接 (Direct)]** : アプライアンスを HTTPS 経由で Cisco Smart Software Manager に直接接続します。このオプションは、デフォルトで選択されます。
- **[トランスポートゲートウェイ (Transport Gateway)]** : アプライアンスをトランスポートゲートウェイまたは Smart Software Manager サテライト経由で Cisco Smart Software Manager に接続します。このオプションを選択した場合、トランスポートゲートウェイまたは Smart Software Manager サテライトの URL を入力してから [OK] をクリックする必要があります。このオプションは HTTP および HTTPS をサポートします。FIPS モードの場合、トランスポートゲートウェイは HTTPS のみをサポートします。

トランスポートゲートウェイについては、

https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

ステップ 5 (オプション) [テストインターフェイス (Test Interface)] : スマートライセンス機能用にアプライアンスを登録するときに、[管理インターフェイス (Management interface)] または [データインターフェイス (Data interface)] を選択します。これは、分割ルーティングを有効にし、スマートライセンス用に登録する場合にのみ適用されます。

(注)

分割ルーティングが有効になっていない場合は、[テストインターフェイス (Test Interface)] ドロップダウンリストで [管理インターフェイス (Management interface)] オプションのみを使用できます。

ステップ 6 ログイン クレデンシアルを使用して、Cisco Smart Software Manager ポータル

(<https://software.cisco.com/#module/SmartLicensing>) にアクセスしてください。新しいトークンを作成するには、このポータルの [仮想アカウント (Virtual Account)] ページに移動して [全般 (General)] タブにアクセスします。アプライアンス用の製品インスタンス登録トークンをコピーします。製品インスタンス登録トークンの作成については、

https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

Scheduled Downtime Notification - License Registration Portal (LRP), Manage Smart Account & Account Administration, Plug-N-Play (PnP), Smart Software Manager

Cisco Software Central > Smart Software Manager > Virtual Account

Virtual Account: [Virtual Account Name]

General | Licenses

Virtual Account

Description: [Description]

Default Virtual Account: [Default Virtual Account]

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account: [Virtual Account Name]

Description: [Description]

Expire After: 30 Days

Between 1 - 365, 30 days recommended

Max. Number of Uses: [Max. Number of Uses]

The token will be expired when either the expiration or the maximum uses is reached

☒ Allow export-controlled functionality on the products registered with this token

Create Token Cancel

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

ステップ 7 アプライアンスに戻り、[登録 (Register)] をクリックします。

Smart Software Licensing [Learn More about Smart Software Licensing](#)

Smart Software Licensing Status	
Registration Mode: ?	Smart license (Change type)
Action: ?	Register
Evaluation Period: ?	In Use
Evaluation Period Remaining: ?	89 days 23 hours 42 minutes
Registration Status: ?	Unregistered
License Authorization Status: ?	Evaluation Mode
Last Authorization Renewal Attempt Status: ?	No Communication Attempted
Product Instance Name: ?	
Transport Settings: ?	Direct (https://smartreceiver.cisco.com/licservice/license) (Edit)
Test Interface: ?	Management ▼
Device Led Conversion Status: ?	Not Started

ステップ 8 製品インスタンス登録トークンをテキストボックスに貼り付けます。

[スマートソフトウェアライセンシング (Smart Software Licensing)] ページで、[すでに登録されている場合は、この製品インスタンスを再登録します (Reregister this product instance if it is already registered)] チェックボックスをオンにして、アプライアンスを再登録することもできます。

Smart Software Licensing

Smart Software Licensing Product Registration

To register the product for Smart Software Licensing:

1. Ensure this product has access to the internet or a Smart Software Manager satellite installed on your network. This might require you to edit the Transport Settings. Product communicates directly or via proxy to Smart Software Licensing.
URL - <https://smartreceiver.cisco.com/licservice/license>
2. Create or login into your Smart Account in [Smart Software Manager](#) or your Smart Software Manager satellite.
3. Navigate to the Virtual Account containing the licenses to be used by this Product Instance.
4. Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it here :

☐ Reregister this product instance if it is already registered

[Cancel](#) [Register](#)

次のタスク

製品登録プロセスには数分かかります。[スマートソフトウェアライセンシング (Smart Software Licensing)] ページで登録ステータスを表示できます。

Smart Software Licensing [Learn More about Smart Software Licensing](#)

Smart Software Licensing Status	
Registration Mode: ?	Smart license
Action: ?	--Select an Action-- Go
Evaluation Period: ?	Not In Use
Evaluation Period Remaining: ?	89 days 23 hours 37 minutes
Registration Status: ?	Registered (16 Jun 2023 04:15) Registration Expires on: (15 Jun 2024 04:11)
License Authorization Status: ?	Authorized (16 Jun 2023 04:16) Authorization Expires on: (14 Sep 2023 04:11)
Smart Account: ?	
Virtual Account: ?	
Last Registration Renewal Attempt Status: ?	SUCCEEDED on 16 Jun 2023 04:15
Last Authorization Renewal Attempt Status: ?	SUCCEEDED on 16 Jun 2023 04:16
Product Instance Name: ?	wsa276.cs1
Transport Settings: ?	Direct (https://smartreceiver.cisco.com/licservice/license)
Test Interface: ?	Management Go

ライセンスの要求

登録プロセスが正常に完了した後、アプライアンスの機能のライセンスを要求しなければならない場合があります。

手順

ステップ 1 [システム管理 (System Administration)] > [ライセンス (Licenses)] を選択します。

ステップ 2 [設定の編集 (Edit Settings)] をクリックします。

ステップ 3 要求するライセンスに対応する [ライセンスの要求/リリース (License Request/Release)] 列のチェックボックスをオンにします。

ステップ 4 [送信 (Submit)] をクリックします。

Licenses

License Name	License Authorization Status ?	License Request ?
Secure Web Appliance Cisco Web Usage Controls	Not requested	☒
Secure Web Appliance Anti-Virus Webroot	Not requested	☒
Secure Web Appliance L4 Traffic Monitor	Not requested	☒
Secure Web Appliance Cisco AnyConnect SM for AnyConnect	Not requested	☒
Secure Web Appliance Secure Endpoint Reputation	Not requested	☒
Secure Web Appliance Anti-Virus Sophos	Not requested	☒
Secure Web Appliance Web Reputation Filters	Not requested	☒
Secure Web Appliance Secure Endpoint	Not requested	☒
Secure Web Appliance Anti-Virus McAfee	Not requested	☒
Secure Web Appliance Web Proxy and DVS Engine	Not requested	☒
Secure Web Appliance HTTPs Decryption	Not requested	☒
Cancel		Submit

次のタスク

ライセンスは、期限超過また期限切れになるとコンプライアンス違反（OOC）モードになり、各ライセンスに 30 日間の猶予期間が提供されます。有効期限および OOC 猶予期間の期限の前に、一定の間隔（30 日前、15 日前、5 日前、および最終日）で通知が表示されます。

OOC 猶予期間の有効期限が過ぎると、ライセンスは使用できず、機能を利用できなくなります。機能にもう一度アクセスするには、CSSM ポータルでライセンスをアップデートして、認証を更新する必要があります。

ライセンスのリリース

手順

ステップ 1 [システム管理（System Administration）] > [ライセンス（Licenses）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 リリースするライセンスに対応する [ライセンスの要求（License Request）] 列のチェック ボックスをオフにします。

ステップ 4 [Submit] をクリックします。

Cisco Smart Software Manager からのアプライアンスの登録解除

手順

ステップ 1 [システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）] を選択します。

ステップ 2 [アクション（Action）] ドロップダウン リストから、[登録解除（Deregister）] を選択し、[実行（Go）] をクリックします。

ステップ 3 [Submit] をクリックします。

Cisco Smart Software Manager でのアプライアンスの再登録

手順

ステップ 1 [システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）] を選択します。

ステップ 2 [アクション（Action）] ドロップダウン リストから、[登録（Register）] を選択し、[実行（Go）] をクリックします。

次のタスク

登録プロセスについては、[Cisco Smart Software Manager でのアプライアンスの登録（140 ページ）](#) を参照してください。

回避できないシナリオにおいては、アプライアンスの設定をリセットした後にアプライアンスを登録することができます。

転送設定の変更

CSSM でアプライアンスを登録する前にのみ、トランスポート設定を変更できます。



- (注) スマート ライセンス機能が有効になっている場合にのみ、トランスポート設定を変更できます。アプライアンスがすでに登録されている場合、トランスポート設定を変更するには、アプライアンスの登録を解除する必要があります。トランスポート設定を変更した後に、アプライアンスを再登録する必要があります。

トランスポート設定を変更する方法については、[Cisco Smart Software Manager でのアプライアンスの登録（140 ページ）](#) を参照してください。

認証と証明書の更新

Cisco Smart Software Manager でアプライアンスを登録した後に、証明書を更新できます。



- (注) アプライアンスが正常に登録された後にのみ、認証を更新できます。

手順

ステップ 1 [システム管理 (System Administration)] > [スマートソフトウェアライセンシング (Smart Software Licensing)] を選択します。

ステップ 2 [アクション (Action)] ドロップダウン リストから、適切なオプションを選択します。

- 認証を今すぐ更新
- 証明書を今すぐ更新

ステップ 3 [移動 (Go)] をクリックします。

次のタスク

機能ライセンスの予約

- [ライセンス予約の有効化（146 ページ）](#)

- [ライセンス予約の登録](#) (147 ページ)
- [ライセンス予約の更新](#) (149 ページ)
- [ライセンス予約の削除](#) (150 ページ)
- [ライセンス予約の有効化](#) (151 ページ)
- [ライセンス失効通知：ライセンスの有効期限が切れる前](#) (152 ページ)
- [ライセンス失効通知：ライセンスの有効期限が切れた後](#) (152 ページ)

表 4: ライセンスのステータス

ステータス	説明
コンプライアンスで予約済み	アプライアンスはライセンスの要求を正常に実行し、ライセンスの使用を承認されています。
未承認	アプライアンスはライセンスを予約していません。

ライセンス予約の有効化

始める前に

Cisco Secure Web Appliance でスマート ライセンシング モードが有効になっていることを確認します。



(注) CLI で `license_smart > enable_reservation` サブコマンドを使用して、機能ライセンスを予約することもできます。



(注) 認証コードをすでにインストールし、スマートライセンシングを有効にしている場合、デバイスは有効に予約された登録済み状態に自動的に移行します。

手順

- ステップ 1** Cisco Secure Web Appliance で [システム管理 (System Administration)] > [スマート ソフトウェア ライセンシング (Smart Software Licensing)] ページに移動します。
- ステップ 2** [特定/永久ライセンス予約 (Specific/Permanent License Reservation)] オプションを選択します。
- ステップ 3** [確認 (Confirm)] をクリックします。

次のタスク

[ライセンス予約の登録（147 ページ）](#)

ライセンス予約の登録

手順

ステップ 1 Cisco Secure Web Applianceで[システム管理（System Administration）]>[スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページに移動します。

ステップ 2 [登録（Register）] をクリックします。

ステップ 3 [コードをコピー（Copy Code）] をクリックして、リクエストコードをコピーします。

（注）

リクエストコードを CSSM ポータルで使用して承認コードを生成します。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 CSSM ポータルに移動して、特定の機能またはすべての機能のライセンスを予約するための承認コードを生成します。

（注）

承認コードの生成方法の詳細については、[スマート ソフトウェア ライセンシング オンライン ヘルプ（cisco.com）](#)にあるヘルプドキュメントの *Inventory: License Tab > Reserve Licenses* セクションを参照してください。

General Licenses Product Instances Event Log

Available Actions Manage License Tags License Reservation... ☒ Show License Transactions Search by License

Smart License Reservation

STEP 1 Enter Request Code STEP 2 Select Licenses STEP 3 Review and Confirm STEP 4 Authorization Code

1) Enter the Reservation Request Code below
2) Select the licenses to be reserved
3) Generate a Reservation Authorization Code
4) Enter the Reservation Authorization Code on the product instance to activate the features

Reservation Request Code:

Upload File Browse Upload

To learn how to enter this code, see the configuration guide for the product being licensed

ステップ 6 [SLR/PLR] を選択し、[次へ（Next）] をクリックします。

Smart License Reservation

STEP 1 ✓
Enter Request Code

STEP 2
Select Licenses

STEP 3
Review and Confirm

STEP 4
Authorization Code

Product Instance Details

Product Type:
UDI PID:
UDI Serial Number:

Licenses to Reserve

In order to continue, ensure that you have a surplus of the licenses you want to reserve in the Virtual Account.

☐ WSA PLR

☐ Reserve a specific license

ステップ 7 CSSM ポータルで、SLR オプションに必要なライセンスを選択し、[次へ (Next)] をクリックします。

STEP 1 ✓
Enter Request Code

STEP 2
Select Licenses

STEP 3
Review and Confirm

STEP 4
Authorization Code

Licenses to Reserve

In order to continue, ensure that you have a surplus of the licenses you want to reserve in the Virtual Account.

☐ WSA PLR

☒ Reserve a specific license

License	Expires	Purchased	Available	Reserve
Secure Web Appliance Advanced Malware Protection Add On Secure Web Appliance Advanced Malware Protection Add On	multiple terms	102	98	1
Secure Web Appliance Advanced Malware Protection Reputation Secure Web Appliance Advanced Malware Protection Reputation	multiple terms	102	100	0
Secure Web Appliance Anti-Virus McAfee Add On Secure Web Appliance Anti-Virus McAfee Add On	2024-Jan-25	100	100	0
Secure Web Appliance Anti-Virus Sophos Add On Secure Web Appliance Anti-Virus Sophos Add On	multiple terms	102	101	0

Cancel Next

ステップ 8 次のいずれかの方法で、CSSM ポータルから取得した承認コードを Cisco Secure Web Appliance に貼り付けます。

- [承認コードをコピーして貼り付ける (Copy and Paste authorization code)] オプションを選択し、[承認コードをコピーして貼り付ける (Copy and Paste authorization code)] オプションの下テキストボックスに承認コードを貼り付けます。
- [システムから承認コードをアップロード (Upload authorization code from the system)] オプションを選択し、[ファイルの選択 (Choose File)] をクリックして承認コードをアップロードします。

ステップ 9 [承認コードをインストール (Install Authorization Code)] をクリックします。

インストール予約のバッチコマンドはサポートされていません。

(注)

承認コードがインストールされるまで、24 時間ごとにアラートが送信されます。

リクエストコードをキャンセルする方法：

承認コードがインストールされる前に予約プロセスをキャンセルするには、`CANCEL_REQUEST_CODE` コマンドを使用します。予約処理の状態をクリアします。

(注)

CSSM ポータルで承認コードを生成したが、アプライアンスでリクエストコードをキャンセルした場合、CSSM ポータルで生成したライセンスはアプライアンスにインストールできません。承認コードの削除については、TAC にお問い合わせください。

必要なライセンス予約 (SLR または PLR) は、Cisco Secure Web Appliance にインストールされています。

ライセンスのステータスは、SLR 用に予約されたライセンスの [コンプライアンスで予約済み (Reserved in Compliance)] 状態に移行します。PLR の場合、すべてのライセンスが [コンプライアンスで予約済み (Reserved in Compliance)] に移行します。

次のタスク

- (SLR のみに適用) : 必要に応じて、ライセンス予約を更新できます。詳細については、[ライセンス予約の更新 \(149 ページ\)](#) を参照してください。
- (SLR および PLR に適用) : 必要に応じて、ライセンス予約を削除できます。詳細については、[ライセンス予約の削除 \(150 ページ\)](#) を参照してください。
- (SLR および PLR に適用) : 必要に応じて、ライセンス予約を無効化できます。詳細については、[ライセンス予約の無効化 \(151 ページ\)](#) を参照してください。

ライセンス予約の更新

新しい機能のライセンスを予約したり、機能の既存のライセンス予約を変更したりできます。



(注) 特定ライセンス予約のみを更新でき、永久ライセンス予約は更新できません。



(注) CLI で `license_smart > reauthorize` サブコマンドを使用して、ライセンス予約を更新することもできます。

手順

ステップ 1 CSSM ポータルに移動して、すでに予約済みのライセンスを更新するための承認コードを生成します。

(注)

承認コードの生成方法の詳細については、[スマート ソフトウェア ライセンシング オンライン ヘルプ \(cisco.com\)](#) にあるヘルプドキュメントの *Inventory: Product Instances Tab > Update Reserved Licenses* セクションを参照してください。

ステップ 2 Cisco Secure Web Appliance で [システム管理 (System Administration)] > [スマート ソフトウェア ライセンシング (Smart Software Licensing)] ページに移動します。

ステップ 3 [アクション (Action)] ドロップダウンリストから [再承認 (Reauthorize)] を選択し、[実行 (GO)] をクリックします。

ステップ 4 次のいずれかの方法で、CSSM ポータルから取得した承認コードを Cisco Secure Web Appliance に貼り付けます。

- [承認コードをコピーして貼り付ける (Copy and Paste authorization code)] オプションを選択し、[承認コードをコピーして貼り付ける (Copy and Paste authorization code)] オプションの下テキストボックスに承認コードを貼り付けます。
- [システムから承認コードをアップロード (Upload authorization code from the system)] オプションを選択し、[ファイルの選択 (Choose File)] をクリックして承認コードをアップロードします。

ステップ 5 [再承認 (Re-authorize)] をクリックします。

ステップ 6 [コードをコピー (Copy Code)] をクリックして、確認コードをコピーします。

(注)

CSSM ポータルで確認コードを使用して、ライセンス予約を更新します。

ステップ 7 [OK] をクリック

ステップ 8 Cisco Secure Web Appliance から取得した確認コードを CSSM ポータルに貼り付けます。

(注)

承認コードの追加方法の詳細については、[スマート ソフトウェア ライセンシング オンライン ヘルプ \(cisco.com\)](#) にあるヘルプドキュメントの *Inventory: Product Instances Tab > Update Reserved Licenses* セクションを参照してください。

ライセンス予約が更新されます。

ライセンスのステータスは、SLR 用に予約されたライセンスの [コンプライアンスで予約済み (Reserved in Compliance)] 状態に移行します。ライセンスが連続して予約されていない場合、ライセンスの状態は [未承認 (Not-Authorized)] 状態に移行します。

ライセンス予約の削除

Cisco Secure Web Appliance で有効になっている特定のライセンス予約または永久ライセンスの予約を削除できます。



(注) CLI で `license_smart > return_reservation` サブコマンドを使用して、ライセンスの予約を削除することもできます。



(注) 予約済みライセンスを削除するとアラートが送信されます。

手順

ステップ 1 Cisco Secure Web Applianceで[システム管理 (System Administration)] > [スマートソフトウェアライセンスング (Smart Software Licensing)] ページに移動します。

ステップ 2 [アクション (Action)] ドロップダウンリストから[リターンコード (Return code)] を選択し、[実行 (GO)] をクリックします。

ステップ 3 [コードをコピー (Copy Code)] をクリックして、リターンコードをコピーします。

(注)

CSSM ポータルにリターンコードを貼り付けて、ライセンス予約を削除します。

ステップ 4 [OK] をクリック

ステップ 5 Cisco Secure Web Appliance から取得したリターンコードを CSSM ポータルで使

(注)

リターンコードの追加方法の詳細については、[スマートソフトウェアライセンス オンライン ヘルプ \(cisco.com\)](#) にあるヘルプ ドキュメントの *Inventory: Product Instances Tab > Removing a Product Instance* セクションを参照してください。

Cisco Secure Web Appliance で有効化されている機能のライセンス予約が削除され、すべてのライセンスが評価期間中になります。

次のタスク

- [ライセンス予約の更新 \(149 ページ\)](#) で確認コードの詳細を確認します。
- (SLR および PLR に適用) : 必要に応じて、ライセンス予約を無効化できます。詳細については、[ライセンス予約の無効化 \(151 ページ\)](#) を参照してください。

ライセンス予約の無効化

Cisco Secure Web Appliance でライセンス予約を無効化できます。



(注) CLI で `license_smart > disable_reservation` サブコマンドを使用して、ライセンス予約を無効にすることもできます。

- 予約リクエストが開始されたが認証コードがインストールされていない場合、予約リクエストはデバイス上でキャンセルされます。

- 認証コードがインストールされている場合、予約リクエストは削除されません。「license smart reservation return」コマンドを使用して認証コードを削除するように警告メッセージが表示されます。このメッセージは、ライセンスの予約機能が無効になっている可能性があるが、認証コードがインストールされたままであることを意味します。この状態はshowコマンドに反映されます。



(注) コードを返して予約を無効化するか、コマンドを使用して予約を無効化できます。

- 認証コードがインストールされると、アプライアンスは認証状態になります。無効化すると、ステータスは有効化モードに移行します。

手順

ステップ1 Cisco Secure Web Applianceで[システム管理 (System Administration)]>[スマートソフトウェアライセンスング (Smart Software Licensing)]ページに移動します。

ステップ2 [登録モード (Registration Mode)]フィールドで[タイプの変更 (Change Type)]をクリックします。

ステップ3 [登録モードの変更 (Change registration mode)]ダイアログボックスで[送信 (Submit)]をクリックします。

ライセンス予約は、Cisco Secure Web Applianceで無効化されます。

ライセンス失効通知：ライセンスの有効期限が切れる前

ライセンスの有効期限が切れる前のアラートの頻度は、60、30、15、5、2、および1日です。

ライセンス失効通知：ライセンスの有効期限が切れた後

ライセンスの有効期限が切れると、ライセンス失効通知が送信されます。SLR/PLRライセンスのライセンス状態は、有効期限が切れた後も**[コンプライアンスで予約済み (Reserved in Compliance)]**のままになります。ライセンスの有効期限が切れると、クリティカルシステムアラートがトリガーされ、電子メールが送信されます。



(注) ライセンス失効通知は、特定ライセンス予約のみが対象です。永久ライセンス予約では送信されません。

CLIでlicense_smart > reauthorize サブコマンドを使用して、ライセンス予約を更新することもできます。

ライセンスの有効期限が切れると、次のメッセージが表示されます。

「Cisco Secure Web Appliance Secure Endpoint アドオンの有効期限が切れています。（The Secure Web Appliance Secure Endpoint Add on entitlement expired.）」

再承認するためのメッセージがお客様に送信されます。

手順

ステップ 1 CSSM ポータルに移動して、すでに予約済みのライセンスを更新するための承認コードを生成します。

（注）

承認コードの生成方法の詳細については、[スマート ソフトウェア ライセンシング オンライン ヘルプ \(cisco.com\)](https://cisco.com) にあるヘルプドキュメントの *Inventory: Product Instances Tab > Update Reserved Licenses* セクションを参照してください。

ステップ 2 Cisco Secure Web Applianceで [システム管理 (System Administration)] > [スマート ソフトウェア ライセンシング (Smart Software Licensing)] ページに移動します。

ステップ 3 [再承認 (Re-authorize)] をクリックします。

スマート エージェントの更新

アプライアンスにインストールされているスマート エージェントのバージョンを更新するには、次の手順を実行します。

手順

ステップ 1 [システム管理 (System Administration)] > [スマートソフトウェアライセンス (Smart Software Licensing)] を選択します。

ステップ 2 [スマートエージェントの更新ステータス (Smart Agent Update Status)] セクションで、[今すぐ更新 (Update Now)] をクリックし、プロセスに従います。

（注）

CLI コマンド `saveconfig` を使用して、または [システム管理 (System Administration)] > [設定サマリー (Configuration Summary)] を使用して Web インターフェイス経由で設定変更を保存しようとする、スマート ライセンス関連の設定は保存されません。

アラート

次のシナリオで通知が送信されます。

- スマート ソフトウェア ライセンシングが正常に有効化された
- スマート ソフトウェア ライセンシングの有効化に失敗した

- 評価期間が開始された
- 評価期間が終了した（評価期間中および期間終了時に一定の間隔で送信）
- 正常に登録された
- 登録に失敗した
- 正常に認証された
- 認証に失敗した
- 正常に登録解除された
- 登録解除に失敗した
- ID 証明書が正常に更新された
- ID 証明書の更新に失敗した
- 認証の有効期限が切れた
- ID 証明書の有効期限が切れた
- コンプライアンス違反猶予期間の期限が切れた（コンプライアンス違反猶予期間中および期間終了時に一定の間隔で送信）
- 機能の有効期限に関する最初のインスタンスが発生した

コマンドラインインターフェイス

- [license_smart](#)（154 ページ）
- [show_license](#)（164 ページ）
- [cloudserviceconfig](#)

license_smart

- [説明](#)（155 ページ）
- [使用方法](#)（155 ページ）
- [例：Smart Software Manager でのアプライアンスの登録](#)（155 ページ）
- [例：スマート ライセンスのステータス](#)（156 ページ）
- [例：スマート ライセンスのステータスの概要](#)（156 ページ）
- [例：スマート トランSPORT URL の設定](#)（157 ページ）
- [例：ライセンスの要求](#)（157 ページ）
- [例：ライセンスのリリース](#)（157 ページ）
- [例：ライセンス予約の有効化](#)（158 ページ）

- [例：ライセンス予約の登録（159 ページ）](#)
- [例：ライセンス予約の更新（161 ページ）](#)
- [例：ライセンス予約の削除（162 ページ）](#)
- [例：ライセンス予約の無効化（162 ページ）](#)

説明

スマート ソフトウェア ライセンス機能の設定

使用方法

確定：このコマンドは「commit」が必要です。

バッチ コマンド：このコマンドはバッチ形式をサポートしています。詳細については、`help license_smart` コマンドを入力して、インライン ヘルプを参照してください。

例：スマート エージェント サービス用ポートの設定

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[]> setagentport

Enter the port to run smart agent service.
[65501]>
```

例：スマート ライセンスの有効化

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
[]> enable
After enabling Smart Licensing on your appliance, follow below steps to activate
the feature keys (licenses):

a) Register the product with Smart Software Manager using license_smart > register command
in the CLI.
b) Activate the feature keys using license_smart > requestsmart_license command in the
CLI.

Note: If you are using a virtual appliance, and have not enabled any of the
features in the classic licensing mode; you will not be able to activate the
licenses, after you switch to the smart licensing mode. You need to first register
your appliance, and then you can activate the licenses (features) in the smart licensing
mode.
Commit your changes to enable the Smart Licensing mode on your appliance.
All the features enabled in the Classic Licensing mode will be available in the Evaluation
period.
Type "Y" if you want to continue, or type "N" if you want to use the classic licensing
mode [Y/N] []> y

> commit

Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
```

例：Smart Software Manager でのアプライアンスの登録

例：スマートライセンスのステータス

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> register
Reregister this product instance if it is already registered [N]> n

Enter token to register the product:
[]>
ODRlOTM5MjItOTQzOS00YjY0LWExZTUtZTdmMmY3OGNlNDZmLTElMzMzMzgw%0AMDEzNTR8WlpCQ1lMbGVMQWRx

OXhuenN4OWZDdktFckJLQzF5V3VibzkyTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status
of registration.
```

例：スマートライセンスのステータス

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode

Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

例：スマートライセンスのステータスの概要

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> summary
```

FeatureName	LicenseAuthorizationStatus
Web Security Appliance Cisco	Eval
Web Usage Controls	

```
Web Security Appliance Anti-Virus Webroot    Eval
Web Security Appliance Anti-Virus Sophos     Eval
```

例：スマートトランスポート URL の設定

```
example.com> license_smart

Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> url

1. DIRECT - Product communicates directly with the cisco license servers
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software
manager satellite.

Choose from the following menu options:
[]> 1
Note: The appliance uses the Direct URL
(https://smartreceiver.cisco.com/licservice/license) to communicate with Cisco
Smart Software Manager (CSSM) via the proxy server configured using the updateconfig
command.
Transport settings will be updated after commit.
```

例：ライセンスの要求



(注) 仮想アプライアンスのユーザーは、ライセンスを要求またはリリースする場合、そのアプライアンスを登録する必要があります。

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> requestsmart_license

Feature Name                                License Authorization Status
1. Web Security Appliance Anti-Virus Sophos    Not Requested
2. Web Security Appliance                      Not requested
   L4 Traffic Monitor

Enter the appropriate license number(s) for activation.
Separate multiple license with comma or enter range:
[]> 1
Activation is in progress for following features:
Web Security Appliance Anti-Virus Sophos
Use license_smart > summary command to check status of licenses.
```

例：ライセンスのリリース

例：ライセンス予約の有効化

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> releasesmart_license
```

Feature Name	License Authorization Status
1. Web Security Appliance Cisco Web Usage Controls	Eval
2. Web Security Appliance Anti-Virus Webroot	Eval
3. Web Security Appliance L4 Traffic Monitor	Eval
4. Web Security Appliance Cisco AnyConnect SM for AnyConnect	Eval
5. Web Security Appliance Advanced Malware Protection Reputation	Eval
6. Web Security Appliance Anti-Virus Sophos	Eval
7. Web Security Appliance Web Reputation Filters	Eval
8. Web Security Appliance Advanced Malware Protection	Eval

例：ライセンス予約の有効化

この例では、`license_smart > enable_reservation` サブコマンドを使用して、Cisco Secure Web Appliance でライセンスの予約を有効化できます。

```
example.com > license_smart

Choose the operation you want to perform:

REQUESTSMART_LICENSE - Request licenses for the product.
RELEASESMART_LICENSE - Release licenses of the product.
REGISTER - Register the product for Smart Licensing.
URL - Set the Smart Transport URL.
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure Web Appliance.
[]> ENABLE_RESERVATION
Would you like to reserve license,then type "Y" else type "N" [Y/N] []> N

License reservation is not enabled.

Choose the operation you want to perform:

REQUESTSMART_LICENSE - Request licenses for the product.
RELEASESMART_LICENSE - Release licenses of the product.
REGISTER - Register the product for Smart Licensing.
URL - Set the Smart Transport URL.
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure Web Appliance.
[]> ENABLE_RESERVATION
Would you like to reserve license,then type "Y" else type "N" [Y/N] []> Y
```

```
License reservation is enabled
[]>
```

例：ライセンス予約の登録

この例では、`license_smart>enable_reservation` サブコマンドを使用して、Cisco Secure Web Appliance でライセンスの予約を有効化できます。

```
example.com > license_smart
```

Choose the operation you want to perform:

```
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance. []>
REQUEST_CODE
The generation of the request code is initiated...
Copy the request code obtained on your Secure Web Appliance and paste it in the Cisco
Smart Software Manager portal to select the required license
Request code: CG-xxxxxxxxxxxxxxxx-39
```

Choose the operation you want to perform:

```
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance.
INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your Secure Web Appliance.
CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Web Appliance.
[]> INSTALL_AUTHORIZATION_CODE
Paste via CLI
Import the Authorization Code from a file How would you like to install Authorization
Code? [1]> 1
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version><piid>3c54a7ce-3b9c-
450e-9338-2f16e5801155</piid><timestamp>1650362032178</timestamp><entitlements>
<entitlement><tag>regid.2018-05.com.cisco.WSA_MUS,1.0_d3f3389a-cdc4-48e3-bc84-8b590ea2d908
</tag><count>1</count><startDate>2022-Apr-08 UTC</startDate><endDate>2022-May-08 UTC
</endDate><licenseType>TERM</licenseType><displayName>
Web Security Appliance Cisco AnyConnect SM for AnyConnect</displayName><tagDescription>
Web Security Appliance Cisco AnyConnect SM for AnyConnect</tagDescription>
<subscriptionID></subscriptionID></entitlement></entitlements>
</authorizationCode><signature>MEYCIQCiy1VlTxBDYxxSagexFEK4ThHVvXEJprhgK83j72FAAIhAJBqyc450uxiZ1pA
/phZ/PR/Xf17e3rxc2AZCY3GH002</signature><udi>P:WSA,S:2AE28096313B</udi></specificPLR>^D
```

The SPECIFIC license reservation is successfully installed on your Secure Web Appliance

Choose the operation you want to perform:

```
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Web Appliance.
REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Web Appliance.
CONFIRM_CODE - Provide the confirmation code generated on your Secure Web Appliance.
RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
```



```
Web Appliance.
[]>
```

リクエストコード生成後のアプライアンスのステータス

```
[]> STATUS
```

```
Smart Licensing is : Enabled
```

```
License Reservation is: Enabled
Reservation Type: IN_PROGRESS
Return Code: CAT6Dx-G8K1Qn-dEY8qs-EFQyyA-nk5NFY-s6hZNi-PnpXmb-rxjGWV-QjP
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 54 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: wsa281.cs1
```

設置後のアプライアンスのステータス

```
[]> STATUS
```

```
Smart Licensing is : Enabled
```

```
License Reservation is: Enabled
Reservation Type: SPECIFIC
Evaluation Period: Not In Use
Evaluation Period Remaining: 83 days 3 hours 32 minutes
Registration Status: Registered ( 28 Apr 2022 04:42 )
Last Registration Renewal Attempt Status: SUCCEEDED on 28 Apr 2022 04:42
License Authorization Status: Not Authorized ( 28 Apr 2022 04:42 )
Last Authorization Renewal Attempt Status: SUCCEEDED on 28 Apr 2022 04:42
Product Instance Name: wsa281.cs1
Status of the Install Authorization Code :
```

要求コードのキャンセル

```
Choose the operation you want to perform:
```

```
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance.
INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your Secure Web Appliance.
CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Web Appliance.
>[]> CANCEL_REQUEST_CODE
If you want to cancel the generated request code, the authorization code generated from
the Cisco Smart Software Manager portal will be locked.
```

```
Are you sure you want to cancel the request code? [Y/N] [N]> N
```

```
The request code is not cancelled
```

```
Choose the operation you want to perform:
```

```
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance.
INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your Secure Web Appliance.
```

```

CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Web Appliance.
[]> CANCEL_REQUEST_CODE
If you want to cancel the generated request code, the authorization code generated from
the Cisco Smart Software Manager portal will be locked.

Are you sure you want to cancel the request code? [Y/N] [N]> Y

The cancellation of the request code is initiated...
The request code is cancelled successfully

Choose the operation you want to perform:

STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance.

```

キャンセル後のアプライアンスのステータス

```

[]> STATUS

Smart Licensing is : Enabled

License Reservation is: Enabled
Reservation Type: NONE
Return Code: CAT6Dx-G8KlQn-dEY8qs-EFQyyA-nk5NFY-s6hZNi-PnpXmb-rxjGWV-QjP
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: wsa281.csl

```

例：ライセンス予約の更新

この例では、`license_smart>reauthorize` サブコマンドを使用して、新しい機能のライセンスを予約したり、機能の既存のライセンス予約を変更したりできます。

```

example.com > license_smart

Choose the operation you want to perform:
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Web Appliance.
REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Web Appliance.
CONFIRM_CODE - Provide the confirmation code generated on your Secure Web Appliance.
RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
Web Appliance. []> REAUTHORIZE
[]> reauthorize
Paste via CLI
Import the Authorization Code from a file How would you like to install Authorization
Code? [1]>
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<pid>3c54a7ce-3b9c-450e-9338-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
</authorizationCode><signature>
MEUCIH5ypYX6GMB9wgZy+8tT4q+JqLlqU/05JlOyS/25qpH8AiEAjEubvaYMy0Vm2DV45TIFUY09c7OZ/JUXQBHLMcT4yDk=</signature>
<udi>P:WSA,S:2AE28096313B</udi></specificPLR>
^D

```

例：ライセンス予約の削除

```
The SPECIFIC license reservation is successfully installed on your Secure Web Appliance
Copy the confirmation code obtained from Smart Agent and add it to the Cisco Smart
Software Manager portal to update the specific reservation.
Confirmation code: fxxxxfeb
```

```
CONFIRMATION CODE:
```

```
Choose the operation you want to perform:
```

```
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Web Appliance.
REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Web Appliance.
CONFIRM_CODE - Provide the confirmation code generated on your Secure Web Appliance.
RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
Web Appliance. []> CONFIRM_CODE
Copy the confirmation code obtained on your Secure Web Appliance and paste it in the
Cisco Smart Software Manager portal to update the specific license reservation.
Confirmation Code: fxxxxfeb
[]>
```

例：ライセンス予約の削除

この例では、`license_smart>return_reservation` サブコマンドを使用して、Cisco Secure Web Appliance で有効になっている機能の特定または永続的なライセンスの予約を削除できます。

```
example.com > license_smart
```

```
Choose the operation you want to perform:
```

```
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Web Appliance.
REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Web Appliance.
CONFIRM_CODE - Provide the confirmation code generated on your Secure Web Appliance.
RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
Web Appliance.
[]> RETURN_RESERVATION
After you return the license reservation, you cannot use any of the product features,
if
the evaluation period has exceeded 90 days. After the 90 days evaluation period,
you must register your product with Cisco Smart Software Manager to continue
to use the product features. [N]> Y
```

```
The generation of the return code is initiated...
Copy the return code obtained on your Secure Web Appliance and paste it in the Cisco
Smart Software Manager portal.
Return Code: CLFSav-xxxxxxxxxxxxxxxxxxxxxxxxxxxx-Ef2
[]>
```

例：ライセンス予約の無効化

この例では、`license_smart>disable_reservation` サブコマンドを使用して、Cisco Secure Web Appliance でライセンスの予約を無効化できます。

```
example.com > license_smart
```

```
Choose the operation you want to perform:
```

```
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
```

```

Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance. []>
DISABLE_RESERVATION
Do you want to disable the specific or permanent reservation? [Y/N] []> Y

License reservation is disabled
Choose the operation you want to perform:

REQUESTSMART_LICENSE - Request licenses for the product.
RELEASESMART_LICENSE - Release licenses of the product.
REGISTER - Register the product for Smart Licensing.
URL - Set the Smart Transport URL.
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure
Web Appliance. []> STATUS
Smart Licensing is : Enabled

License Reservation is: Disabled
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 46 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: wsa281.cs1
Transport Settings: Direct (https://smartreceiver-stage.cisco.com/licservice/license)
Device Led Conversion Status: Not Started

Choose the operation you want to perform:

REQUESTSMART_LICENSE - Request licenses for the product.
RELEASESMART_LICENSE - Release licenses of the product.
REGISTER - Register the product for Smart Licensing.
URL - Set the Smart Transport URL.
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure
Web Appliance. []>
[]>

```

例 : Device Led Conversion (DLC) プロセスの手動による有効化

この例では、`license_smart > conversion_start` サブコマンドを使用して、Cisco Secure Web Appliance で Device Led Conversion (DLC) を手動で有効化できます。

DLC 失敗のサンプルコード :

```

example.com > license_smart

Deregister the Secure Web Appliance from the Cisco Smart Software Manager portal to
enable the license reservation

Choose the operation you want to perform:
- URL - Set the Smart Transport URL.
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- DEREGISTER - Deregister the product from Smart Licensing.
- REREGISTER - Reregister the product for Smart Licensing.
- RENEW_AUTH - Renew authorization of Smart Licenses in use.
- RENEW_ID - Renew registration with Smart Licensing.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- CONVERSION_START - To manually convert the classic license keys to smart licensing.
[]> conversion_start

```

show_license

- [説明 \(164 ページ\)](#)
- [例：スマート ライセンスのステータス \(164 ページ\)](#)
- [例：スマート ライセンスのステータスの概要 \(164 ページ\)](#)

説明

スマート ライセンスのステータスとステータスの概要を表示します。

例：スマート ライセンスのステータス

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> status
Smart Licensing is: Enabled
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: example.com
Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

例：スマート ライセンスのステータスの概要

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> summary
```

FeatureName	LicenseAuthorizationStatus
Web Security Appliance Cisco	Eval
Web Usage Controls	
Web Security Appliance	Eval
Anti-Virus Webroot	
Web Security Appliance	Eval
Anti-Virus Sophos	

cloudserviceconfig



(注) SLR/PLR を介してスマートライセンスを登録すると、クラウドサービスは有効化されず、自動登録は行われません。このサポートは、トークン登録を通じて登録されたスマートライセンスにのみ適用されます。

- [説明](#)
- [使用量](#)
- [例：Secure Web Applianceでの Cisco Cloud Services の有効化](#)

- 例：Secure Web Applianceでの Cisco Cloud Services の無効化
- 例：Cisco Cloud Services ポータルへの Secure Web Applianceの登録
- 例：Cisco Cloud Services ポータルへの Secure Web Applianceの自動登録
- 例：Cisco Cloud Services ポータルからの Secure Web Applianceの登録解除
- 例：Secure Web Applianceを Cisco Cloud Services ポータルに接続する Cisco Secure Cloud Server の選択
- 例：証明書とキーのダウンロード
- 例：クライアント証明書 updateconfig

説明

cloudserviceconfig コマンドは次の目的で使用します。

- Secure Web Applianceで Cisco Cloud Services ポータルを有効にします。
- Secure Web Applianceで Cisco Cloud Services ポータルを無効にします。
- Cisco Cloud Services ポータルに Secure Web Applianceを登録します。
- Cisco Cloud Services ポータルに Secure Web Applianceを自動的に登録します。
- Cisco Cloud Services ポータルから Secure Web Applianceの登録を解除します。
- Cisco Secure Cloud サーバーを選択して、Secure Web Applianceを Cisco Cloud Services ポータルに接続します。
- Cisco Talos Intelligence Services ポータルから Cisco Cloud Services 証明書とキーをダウンロードします。
- クライアント証明書とキーをアップロードします。



(注) このコマンドは、スマートライセンスモードでのみ適用できます。

使用方法

- **確定**：このコマンドに **commit** は必要ありません。
- **バッチ コマンド**：このコマンドはバッチ形式をサポートしています。

例：Secure Web Applianceでの Cisco Cloud Services の有効化

次に、`cloudserviceconfig> enable` サブコマンドを使用して、Secure Web Applianceで Cisco Cloud Services を有効にする例を示します

```
example.com > cloudserviceconfig
Choose the operation you want to perform:
- ENABLE - The Cisco Cloud Service is currently disabled on your appliance.
[]> enable
```

例：Secure Web Applianceでの Cisco Cloud Services の無効化

```
The Cisco Cloud Service is currently enabled on your appliance.
Currently configured Cisco Secure Cloud Server is: api.apj.sse.itd.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 1
Selected Cisco Secure Cloud Server is api-sse.cisco.com.
Make sure you run "commit" to make these changes active.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:23:19 2020 GMTexample.com >
```

例：Secure Web Applianceでの Cisco Cloud Services の無効化

次に、cloudserviceconfig>disable サブコマンドを使用して、Secure Web Applianceで Cisco Cloud Services を無効にする例を示します。

```
example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> disable
The Cisco Cloud Service is currently disabled on your appliance.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:01:07 2020 GMT
example.com >
```

例：Cisco Cloud Services ポータルへの Secure Web Applianceの登録

次に、cloudserviceconfig>register サブコマンドを使用して、Cisco Cloud Services ポータルに Secure Web Applianceを登録する例を示します。



(注) このサブコマンドは、スマート ソフトウェア ライセンシングが有効になっていない状態で、Secure Web Applianceが Cisco Smart Software Manager に登録されていない場合にのみ使用できます

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> register

Enter a registration token key to register your appliance
[]> c51fa32bd9a31227eaab50dea873062c
```

```
Registering
The Web Security appliance is successfully registered with the Cisco Cloud Service portal.
example.com >
```

例：Cisco Cloud Services ポータルへの Secure Web Applianceの自動登録

次に、cloudserviceconfig> autoregister コマンドを使用して、Cisco Cloud Services ポータルに Secure Web Applianceを登録する例を示します。

```
example.com > cloudserviceconfig
```

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:

- AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically using SL Payload.
 - SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
 - STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
- ```
[> autoregister
```

The Web Security appliance successfully auto-registered with the Cisco Cloud Service portal.

#### 例：Cisco Cloud Services ポータルからの Secure Web Applianceの登録解除

次に、cloudserviceconfig> deregister サブコマンドを使用して、Cisco Cloud Services ポータルから Secure Web Applianceの登録を解除する例を示します。

```
example.com > cloudserviceconfig
```

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:

- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
  - DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
  - STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
- ```
[> deregister
```

Do you want to deregister your appliance from the Cisco Cloud Service portal.
If you deregister, you will not be able to access the Cloud Service features. [N]> y

The Web Security appliance successfully deregistered from the Cisco Cloud Service portal.
example.com >

例：Secure Web Applianceを Cisco Cloud Services ポータルに接続する Cisco Secure Cloud Server の選択

次に、cloudserviceconfig> settrs サブコマンドを使用して、Secure Web Applianceを Cisco Cloud Services ポータルに接続するために必要な Cisco Secure Cloud Server を選択する例を示します。

```
example.com > cloudserviceconfig
```

The appliance is not registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:

- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
 - REGISTER - To register the appliance with the Cisco Cloud Service portal.
 - SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- ```
[> settrs
```

Currently configured Cisco Secure Cloud Server is: api-sse.cisco.com

Available list of Cisco Secure Cloud Servers:

1. AMERICAS (api-sse.cisco.com)



```

2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 3
Selected Cisco Secure Cloud Server is api.eu.sse.itd.cisco.com.
Make sure you run "commit" to make these changes active.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:37:40 2020 GMT

```

#### 例 : Cisco Talos Intelligence Services ポータルからの Cisco Cloud Services 証明書とキーのダウンロード

次に、cloudserviceconfig>fetchcertificate サブコマンドを使用して、Cisco Talos Intelligence Services ポータルから Cisco Cloud Services 証明書とキーをダウンロードする例を示します。



(注) このサブコマンドは、既存の Cisco Cloud Services 証明書の有効期限が切れている状態で、Cisco Smart Software Manager に Secure Web Appliance を登録している場合にのみ使用できます。

```

example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- FETCHCERTIFICATE - Download the Cisco Talos certificate and key
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> fetchcertificate

Successfully downloaded the Cisco Talos certificate and key
example.com >

```

#### 例 : クライアント証明書 updateconfig

次に、Updateconfig>clientcertificate サブコマンドを使用して証明書とキーをアップロードする例を示します。

```

example.com > updateconfig

Service (images): Update URL:

Web Reputation Filters Cisco Servers
Support Request updates Cisco Servers
Timezone rules Cisco Servers
How-Tos Updates Cisco Servers
HTTPS Proxy Certificate Lists Cisco Servers
Cisco AsyncOS upgrades Cisco Servers
Smart License Agent Updates Cisco Servers

Service (list): Update URL:

Web Reputation Filters Cisco Servers
Support Request updates Cisco Servers
Timezone rules Cisco Servers
How-Tos Updates Cisco Servers
HTTPS Proxy Certificate Lists Cisco Servers
Cisco AsyncOS upgrades Cisco Servers
Smart License Agent Updates Cisco Servers

```

```

Update interval for Web Reputation and Categorization: 5m
Update interval for all other services: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Routing table for updates: Management
 The following services will use this routing table:
 - Web Reputation Filters
 - Support Request updates
 - Timezone rules
 - How-Tos Updates
 - HTTPS Proxy Certificate Lists
 - Cisco AsyncOS upgrades
 - Smart License Agent Updates

Upgrade notification: enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- CLIENTCERTIFICATE - Upload the client certificate and key.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> clientcertificate

Current Cisco certificate is valid for 179 days

Do you like to overwrite the existing certificate and key [Y|N] ? []> y

Paste the certificate.
Press CTRL-D on a blank line when done.
^D

```

証明書と秘密キーの詳細を貼り付けます。証明書とキーは正常に保存されます。

## AsyncOS 14.0 以降のスマート ソフトウェア ライセンス キー ポイント

- スマート ソフトウェア ライセンスを有効にして登録すると、Cisco Cloud Service が有効になり、自動的に登録されます。
- Cisco Cloud Services 証明書の有効期限が切れている場合は、CLI で `cloudserviceconfig > fetchcertificate` サブコマンドを使用して Cisco Talos Intelligence Services ポータルから新しい証明書をダウンロードできます。
- スマートライセンスが評価モードの場合、Cisco Cloud Services の自動登録は実行できません。

## 仮想アプライアンスのライセンス

Cisco Web Security 仮想アプライアンスでは、ホスト上で仮想アプライアンスを実行する追加ライセンスが必要です。

仮想アプライアンスのライセンスの詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは、<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html> から入手できます。



**Note** 仮想アプライアンスのライセンスをインストールする前に、テクニカルサポートのトンネルを開くことはできません。

ライセンスの期限が切れた後、アプライアンスは、180 日間セキュリティ サービスなしで、Web プロキシとして動作を継続します。この期間中、セキュリティ サービスは更新されません。

ライセンスの期限切れに関する警告を受信するように、アプライアンスを設定できます。

#### 関連項目

- [アラートの管理, on page 183](#)

## 仮想アプライアンスのライセンスのインストール

『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。このドキュメントは、

<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html>

[英語] から入手できます。

## リモート電源再投入の有効化

### Before you begin

- 専用のリモート電源再投入 (RPC) ポートをセキュアネットワークに直接、ケーブル接続します。詳細については、お使いのアプライアンス モデルのハードウェア ガイドを参照してください。このドキュメントの場所については、[ドキュメント セット, on page 805](#)を参照してください。
- ファイアウォールを通過するために必要なポートを開くなど、アプライアンスがリモート アクセス可能であることを確認します。
- この機能を使用するには、専用のリモート電源再投入インターフェイスの一意の IPv4 アドレスが必要です。このインターフェイスは、このセクションで説明されている手順でのみ設定可能です。ipconfig コマンドを使用して設定することはできません。
- アプライアンスの電源を再投入するには、Intelligent Platform Management Interface (IPMI) バージョン 2.0 をサポートするデバイスを管理できるサードパーティ製ツールが必要です。このようなツールを使用できるように準備されていることを確認します。
- コマンドラインインターフェイスへのアクセスに関する詳細については、[を参照してください。コマンドライン インターフェイス, on page 775](#)

RPC を設定して変更を確定したら、10 ～ 15 分待ってから呼び出しを RPC に送信します。この待機時間中に、Secure Web Appliance が RCP サービスを初期化します。

アプライアンスシャーシの電源をリモートでリセットする機能は、x80、x90、x95 シリーズのハードウェアでのみ使用できます。

アプライアンスの電源をリモートでリセットする場合は、このセクションで説明されている手順を使用して、この機能を事前に有効にし、設定しておく必要があります。

## Procedure

**ステップ 1** SSH またはシリアルコンソールポートを使用して、コマンドラインインターフェイスにアクセスします。

**ステップ 2** 管理者権限を持つアカウントを使用してログインします。

**ステップ 3** 以下のコマンドを入力します。

```
remotepower
```

```
setup
```

**ステップ 4** プロンプトに従って、以下の情報を指定します。

- この機能専用の IP アドレスと、ネットマスクおよびゲートウェイ。
- 電源の再投入コマンドを実行するために必要なユーザ名とパスワード。

これらのクレデンシャルは、アプライアンスへのアクセスに使用する他のクレデンシャルに依存しません。

**ステップ 5** `commit` を入力して変更を保存します。

**ステップ 6** 設定をテストして、アプライアンスの電源をリモートで管理できることを確認します。

**ステップ 7** 入力したクレデンシャルが、将来、いつでも使用できることを確認します。たとえば、この情報を安全な場所に保管し、このタスクを実行する必要がある管理者が、必要なクレデンシャルにアクセスできるようにします。

## What to do next

### 関連項目

- [ハードウェア アプライアンス : アプライアンスの電源のリモート リセット](#), on page 765

## ユーザー アカウントの管理

以下のタイプのユーザーは、アプライアンスにログインして、アプライアンスを管理できます。

- **ローカル ユーザー。** アプライアンス自体にローカルにユーザーを定義できます。
- **外部システムに定義されたユーザー。** アプライアンスにログインするユーザーを認証するために、外部 LDAP または RADIUS サーバーに接続するようにアプライアンスを設定できます。



**Note** Web インターフェイスにログインするか、SSH を使用するなどの任意の方法を使用して、アプライアンスにログインできます。

#### 関連項目

- [ローカル ユーザー アカウントの管理, on page 172](#)
- [RADIUS ユーザー認証, on page 175](#)
- [LDAP サーバーによる外部認証の設定, on page 91](#)

## ローカル ユーザー アカウントの管理

Secure Web Appliance に任意の数のユーザをローカルに定義できます。

デフォルトのシステム admin アカウントは、すべての管理者権限を持っています。admin アカウントのパスワードは変更できますが、このアカウントを編集したり削除することはできません。



**Note** admin ユーザーのパスワードを紛失した場合は、シスコ サポート プロバイダに問い合わせしてください。詳細については、「[管理者パスワードをリセットし、管理者ユーザーアカウントをロック解除する](#)」を参照してください。

### ローカル ユーザー アカウントの追加

#### Before you begin

すべてのユーザーアカウントが従うべきパスワード要件を定義します。[管理ユーザーのパスワード要件の設定, on page 178](#)を参照してください。

#### Procedure

**ステップ 1** [システム管理 (System Administration)] > [ユーザー (Users)] を選択します。

**ステップ 2** [ユーザーの追加 (Add User)] をクリックします。

**ステップ 3** 以下のルールに注意して、ユーザー名を入力します。

- ユーザー名に小文字、数字、およびダッシュ (-) 記号を使用することはできますが、最初の文字をダッシュにすることはできません。
- ユーザー名は 16 文字以下です。
- ユーザー名としてシステムで予約されている特殊名（「operator」や「root」など）を指定することはできません。

- 外部認証も使用する場合は、ユーザー名が外部認証されたユーザー名と重複しないようにしてください。

**ステップ4** ユーザーの氏名を入力します。

**ステップ5** ユーザー タイプを選択します。

| ユーザタイプ                                | 説明                                                                                                                                                                                                                                                               |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 管理者<br>(Administrator)                | すべてのシステム設定に対する完全なアクセス権を許可します。ただし、 <code>upgradecheck</code> および <code>upgradeinstall</code> CLI コマンドは、システム定義の「 <code>admin</code> 」アカウントからのみ発行できます。                                                                                                              |
| オペレータ<br>(Operator)                   | ユーザーアカウントを作成、編集、および削除できません。オペレータグループでは、以下の CLI コマンドの使用も制限されます。 <ul style="list-style-type: none"> <li>• <code>resetconfig</code></li> <li>• <code>upgradecheck</code></li> <li>• <code>upgradeinstall</code></li> </ul> オペレータグループでは、システム セットアップ ウィザードの使用も制限されます。 |
| オペレータ（読み取り専用）<br>(Read-Only Operator) | このロールのユーザー アカウントは、 <ul style="list-style-type: none"> <li>• 設定情報を表示できます。</li> <li>• 機能の設定方法を確認するために変更を行って送信はできますが、コミットはできません。</li> <li>• キャッシュをクリアしたり、ファイルを保存するなどのアプライアンスへの他の変更を加えることはできません。</li> <li>• ファイル システム、FTP、または SCP にアクセスできません。</li> </ul>             |
| ゲスト (Guest)                           | ゲストグループのユーザーは、レポートやトラッキングなど、システムのステータス情報の参照のみを実行できます。                                                                                                                                                                                                            |

**ステップ6** パスフレーズを入力するか、または作成します。

**ステップ7** 変更を送信し、保存します。

## ユーザーアカウントを削除する

### Procedure

**ステップ1** [システム管理 (System Administration)] > [ユーザー (Users)] を選択します。

**ステップ 2** プロンプトが表示されたら、一覧表示されているユーザー名に対応するゴミ箱アイコンをクリックして確認します。

**ステップ 3** 変更を送信し、保存します。

---

## ユーザー アカウントの編集

### Procedure

---

**ステップ 1** [システム管理 (System Administration)] > [ユーザー (Users)] を選択します。

**ステップ 2** ユーザー名をクリックします。

**ステップ 3** 必要に応じて、[ユーザーの編集 (Edit User)] ページでユーザーに変更を加えます。

**ステップ 4** 変更を送信し、保存します。

---

## パスフレーズの変更

現在ログインしているアカウントのパスフレーズを変更するには、ウィンドウの右上で、[オプション (Options)] > [パスフレーズの変更 (Change Passphrase)] を選択します。

他のアカウントの場合は、[ローカルユーザー設定 (Local User Settings)] ページで、アカウントを編集してパスフレーズを変更します。

### 関連項目

- [ユーザー アカウントの編集, on page 174](#)
- [管理ユーザーのパスフレーズ要件の設定, on page 178](#)

## 制限的なユーザ アカウントとパスフレーズの設定値の構成

ユーザー アカウントとパスフレーズの制限を定義して、組織全体にパスフレーズ ポリシーを強制的に適用することができます。ユーザー アカウントとパスフレーズ制限は、Cisco アプリアンスに定義されたローカル ユーザーに適用されます。次の設定値を設定できます。

- **ユーザアカウントのロック。** ユーザのアカウントがロックアウトされる失敗ログインの試行回数を定義できます。ユーザーログイン試行回数は 1 ～ 60 の範囲で設定できます。デフォルト値は 5 です。
- **パスフレーズ存続期間のルール。** ログイン後にユーザがパスフレーズの変更を要求されるまでの、パスフレーズの存続期間を定義できます。
- **パスフレーズのルール。** 任意指定の文字や必須の文字など、ユーザが選択できるパスフレーズの種類を定義できます。



(注) AsyncOS バージョン 14.0 以降では、パスフレーズルールはデフォルトで有効になります。ただし、**パスフレーズルールで拒否する 3 文字以上の反復文字または連続文字**、および**パスフレーズルールで拒否する単語のリスト**は例外です。

- **パスフレーズの強度**。管理ユーザーが新しいパスフレーズを入力するときに、パスフレーズ強度インジケータを表示できます。

詳細については、「[管理ユーザーのパスフレーズ要件の設定](#)」を参照してください。

ユーザ アカウントとパスフレーズの制限は、[システム管理 (System Administration)] > [ユーザ (Users)] ページの [ローカル ユーザ アカウントとパスフレーズの設定 (Local User Account & Passphrase Settings)] セクションで定義します。

## RADIUS ユーザー認証

Secure Web Appliance は RADIUS ディレクトリ サービスを使用して、HTTP、HTTPS、SSH、および FTP によりアプライアンスにログインするユーザを認証します。PAP または CHAP 認証を使用して、認証のために複数の外部サーバーと連携するように、アプライアンスを設定できます。外部ユーザのグループを Secure Web Appliance のさまざまなユーザ ロール タイプにマッピングできます。

### RADIUS 認証のイベントのシーケンス

外部認証がイネーブルになっている場合にユーザが Secure Web Appliance にログインすると、アプライアンスは以下を実行します。

1. ユーザーがシステム定義の「admin」アカウントであるかどうかを確認します。
2. 「admin」アカウントでない場合は、まず、設定されている外部サーバーをチェックし、ユーザーがそのサーバーで定義されているかどうかを確認します。
3. 最初の外部サーバーに接続できない場合、アプライアンスはリスト内の次の外部サーバーをチェックします。
4. アプライアンスが外部サーバに接続できない場合、アプライアンスは Secure Web Appliance で定義されたローカル ユーザとしてユーザを認証しようとします。
5. そのユーザーが外部サーバーまたはアプライアンスに存在しない場合、またはユーザーが間違ったパスフレーズを入力した場合は、アプライアンスへのアクセスが拒否されます。



## RADIUS を使用した外部認証の有効化

## Procedure

- 
- ステップ 1** [システム管理 (System Administration)] > [ユーザー (Users)] ページで、[外部認証を有効にする (Enable External Authentication)] をクリックします。
- ステップ 2** 認証タイプとして [RADIUS] を選択します。
- ステップ 3** RADIUS サーバーのホスト名、ポート番号、共有シークレット パスフレーズを入力します。デフォルトのポートは 1812 です。
- ステップ 4** タイムアウトまでにアプライアンスがサーバーからの応答を待つ時間を秒単位で入力します。
- ステップ 5** RADIUS サーバーが使用する認証プロトコルを選択します。
- ステップ 6** (任意) [行を追加 (Add Row)] をクリックして別の RADIUS サーバーを追加します。各 RADIUS サーバーについて、**1 ~ 5** のステップを繰り返します。

**Note**

最大 10 個の RADIUS サーバーを追加できます。

- ステップ 7** 再認証のために再び RADIUS サーバーに接続するまでに、AsyncOS が外部認証クレデンシャルを保存する秒数を [外部認証キャッシュ タイムアウト (External Authentication Cache Timeout)] フィールドに入力します。デフォルトは 0 です。

**Note**

RADIUS サーバーがワンタイム パスフレーズ (トークンから作成されたパスフレーズなど) を使用している場合は、ゼロ (0) を入力します。値をゼロに設定すると、AsyncOS は、現在のセッション中に認証のために RADIUS サーバーに再アクセスしません。

- ステップ 8** グループマッピングを設定します。すべての外部認証されたユーザー全員を管理者ロールにマッピングするか、異なるアプライアンス ユーザー ロール タイプにマッピングするかを選択します。

| 設定                            | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 外部認証されたユーザを複数のローカル ロールにマッピング。 | <p>RADIUS CLASS 属性で定義されたグループ名を入力し、アプライアンス ロールタイプを選択します。[行の追加 (AddRow)] をクリックして、さらにロール マッピングを追加できます。</p> <p>AsyncOS は、RADIUS CLASS 属性に基づいて、RADIUS ユーザをアプライアンス ロールに割り当てます。CLASS 属性の要件：</p> <ul style="list-style-type: none"> <li>• 最小 3 文字</li> <li>• 最大 253 文字</li> <li>• コロン、カンマ、または改行文字なし</li> <li>• 各 RADIUS ユーザに対し 1 つ以上のマップ済み CLASS 属性（この設定を使用する場合、AsyncOS は、マップ済み CLASS 属性のない RADIUS ユーザへのアクセスを拒否します）。</li> </ul> <p>複数の CLASS 属性のある RADIUS ユーザの場合、AsyncOS は最も制限されたロールを割り当てます。たとえば、Operator ロールにマッピングされている CLASS 属性と、Read-Only Operator ロールにマッピングされている CLASS 属性の 2 つが RADIUS ユーザにある場合、AsyncOS は、Operator ロールよりも制限された Read-Only Operator ロールに RADIUS ユーザを割り当てます。</p> <p>以下のアプライアンス ロールは、最も制限が厳しいものから順番に並んでいます。</p> <ul style="list-style-type: none"> <li>• 管理者 (Administrator)</li> <li>• オペレータ (Operator)</li> <li>• Read-Only Operator</li> <li>• ゲスト (Guest)</li> </ul> |
| 外部認証されたすべてのユーザを管理ロールにマップします。  | <p>AsyncOS はすべての RADIUS ユーザーを Administrator ロールに割り当てます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**ステップ 9** 変更を送信し、保存します。

## What to do next

### 関連項目

- [外部認証, on page 91](#)
- [ローカル ユーザー アカウントの追加, on page 172。](#)

## ユーザー プリファレンスの定義

レポートの表示形式などのプリファレンス設定は、各ユーザーごとに保存され、ユーザーがどのクライアントマシンからアプライアンスにログインするかに関係なく同じ設定が適用されます。

### Procedure

**ステップ 1** [オプション (Options)] > [環境設定 (Preferences)] を選択します。

**ステップ 2** [ユーザー設定 (User Preferences)] ページで、[設定を編集 (Edit Preferences)] をクリックします。

**ステップ 3** 必要に応じて、プリファレンスを設定します。

| プリファレンス設定                                              | 説明                                            |
|--------------------------------------------------------|-----------------------------------------------|
| 言語の表示 (Language Display)                               | Web インターフェイスおよび CLI で使用する言語の Web 用 AsyncOS。   |
| ランディング ページ (Landing Page)                              | ユーザーがアプライアンスにログインするときに表示されるページ。               |
| 表示されるレポート時間範囲 (Reporting Time Range Displayed) (デフォルト) | [レポート (Reporting)] タブでレポートに対して表示するデフォルトの時間範囲。 |
| 表示するレポート行の数 (Number of Reporting Rows Displayed)       | デフォルトで各レポートに表示されるデータの行数。                      |

**ステップ 4** 変更を送信し、保存します。

## 管理者の設定

### 管理ユーザーのパスフレーズ要件の設定

アプライアンスでローカル定義された管理ユーザーのパスフレーズ要件を設定するには、以下の手順を実行します。

### Procedure

**ステップ 1** [システム管理 (System Administration)] > [ユーザー (Users)] を選択します。

**ステップ2** [パスフレーズの設定 (Passphrase Settings)] セクションで、[設定を編集 (Edit Settings)] をクリックします。

**ステップ3** 以下のオプションから選択します。

| オプション                                                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| パスフレーズで許可しない単語の一覧 (List of words to disallow in passphrases) | 1行ごとに各禁止単語を記入した .txt ファイルを作成し、そのファイルを選択してアップロードします。後続のアップロードによって以前のアップロードが上書きされます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| パスフレーズの強度 (Passphrase Strength)                              | <p>管理ユーザーが新しいパスフレーズを入力するときに、パスフレーズ強度インジケータを表示できます。</p> <p>この設定によって強固なパスフレーズが作成されるわけではありません。この設定は、入力したパスフレーズの推測されやすさを示すだけです。</p> <p>インジケータを表示する対象ロールを選択します。次に、選択したロールごとにゼロより大きい数字を入力します。数値が大きいほど、強固なパスフレーズとして登録されるパスフレーズの実現が困難になります。この設定には最大値がありませんが、非常に大きな数値を指定するとパスフレーズの作成が非常に困難になります。</p> <p>さまざまな値を試すことで、最も要件を満たす数値を確認してください。</p> <p>パスフレーズの強度は対数目盛で測定されます。評価は、トラブルシューティングトピックの NIST SP 800-63 で定義されている米国立標準技術研究所のエントロピーのルールに基づいています。</p> <p>一般的に、強固なパスフレーズは以下のような特徴を備えています。</p> <ul style="list-style-type: none"> <li>• 長い。</li> <li>• 大文字、小文字、数字、および特殊文字を含む。</li> <li>• あらゆる言語の辞書にある語を含まない。</li> </ul> <p>これらの特徴を備えたパスフレーズを適用するには、このページの他の設定を使用します。</p> |

**ステップ4** 変更を送信し、保存します。

## アプライアンスの割り当てに対するセキュリティ設定の追加

CLI コマンド `adminaccessconfig` を使用すると、管理者がアプライアンスにログインする際のアクセス要件をさらに厳格にするように Secure Web Applianceを設定できます。

| コマンド                              | 説明                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adminaccessconfig ><br>banner     | <p>管理者がログインを試みるときに指定したテキストが表示されるようにアプライアンスを設定します。Web UI、CLI、FTP などの任意のインターフェイスを使用して管理者がアプライアンスにアクセスすると、カスタムのログイン バナーが表示されます。</p> <p>CLI プロンプトに貼り付けるか、Secure Web Appliance 上のテキスト ファイルからコピーすることによって、カスタム テキストをロードできます。ファイルからテキストをアップロードするには、まず FTP を使用してアプライアンスの <b>configuration</b> ディレクトリにファイルを転送します。</p>                                                                           |
| adminaccessconfig ><br>welcome    | <p>これは、管理者がログインに成功したときに表示されるポストログインバナーです。このテキストは、ログインの adminaccessconfig &gt; banner テキストと同じ方法でアプライアンスの設定に追加されます。</p>                                                                                                                                                                                                                                                                 |
| adminaccessconfig ><br>ipaccess   | <p>管理者が Secure Web Appliance にアクセスするときの接続元の IP アドレスを制御します。管理者は、任意のマシンまたは指定した一覧内の IP アドレスを持つマシンからアプライアンスにアクセスできます。</p> <p>アクセスを許可リストに制限する場合は、IP アドレス、サブネット、または CIDR アドレスを指定できます。デフォルトでは、アプライアンスにアクセスできるアドレスを一覧表示すると、現在のマシンの IP アドレスが許可リストの最初のアドレスとして一覧表示されます。許可リストから現在のマシンの IP アドレスは削除できません。この情報は、Web UI を使用して表示することもできます。<a href="#">ユーザー ネットワーク アクセス, on page 181</a> を参照してください。</p> |
| adminaccessconfig > csrf          | <p>悪意のある要求、またはなりすました要求を識別して、これから保護するために使用される、Web UI のクロスサイト要求偽造保護機能を有効/無効にします。最大のセキュリティを確保するには、CSRF 保護をイネーブルにすることを推奨します。</p>                                                                                                                                                                                                                                                          |
| adminaccessconfig ><br>hostheader | <p>HTTP 要求でホスト ヘッダーを使用するよう設定します。</p> <p>デフォルトでは、Web UI は、HTTP 要求内で Web クライアントから送信されたホスト ヘッダーを使用して応答します。セキュリティを高めるために、アプライアンス固有のホスト名、つまりアプライアンスに設定された名前 (wsa_04.local など) のみを使用して応答するように Web UI を設定することができます。</p>                                                                                                                                                                      |

| コマンド                                             | 説明                                                                                                                                                                                                                                    |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>adminaccessconfig &gt; timeout</code>      | 非アクティビティのタイムアウト間隔、つまりユーザーがログアウトするまでに非アクティブでいられる期間（分数）を指定します。5～1440 分（24 時間）の値を指定できます。デフォルト値は 30 分です。この情報は、Web UI を使用して表示することもできます。 <a href="#">ユーザー ネットワーク アクセス, on page 181</a> を参照してください。                                           |
| <code>adminaccessconfig &gt; how-tos</code>      | 特定の設定タスク実行をサポートするウォークスルーを有効にします。                                                                                                                                                                                                      |
| <code>adminaccessconfig &gt; strictssl</code>    | 管理者がより強力な SSL 暗号（56 ビット暗号化以上）を使用してポート 8443 の Web インターフェイスにログインできるように、アプライアンスを設定します。<br><br>より強力な SSL 暗号を必要とするようにアプライアンスを設定すると、その変更は HTTPS を使用して管理の目的でアプライアンスにアクセスする管理者にのみ適用されます。HTTPS を使用して Web プロキシに接続されている他のネットワーク トラフィックには適用されません。 |
| <code>adminaccessconfig &gt; loginhistory</code> | ログイン履歴を保持する日数を設定します。                                                                                                                                                                                                                  |
| <code>adminaccessconfig &gt; maxsessions</code>  | 同時ログインセッションの最大数を設定します（CLI および Web インターフェイス）。                                                                                                                                                                                          |

## ユーザー ネットワーク アクセス

AsyncOS が、アプライアンスから非アクティブなユーザーをログアウトするまでの時間を指定できます。また、許可するユーザー接続のタイプを指定することもできます。

セッション タイムアウトは、管理者を含め、Web UI または CLI にログインしているすべてのユーザーに適用されます。AsyncOS がログアウトしたユーザーは、アプライアンスのログインページにリダイレクトされます。



(注) このタイムアウトの値を設定するには、CLI `adminaccessconfig > timeout` を使用することもできます。

### 手順

**ステップ 1** [システム管理（System Administration）]>[ネットワーク アクセス（Network Access）]を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** [セッション非アクティブ タイムアウト (Session Inactivity Timeout)] フィールドに、ログアウトするまでに許容するユーザーの非アクティブ時間を分数で入力します。

5 ～ 1440 分 (24 時間) の範囲でタイムアウト間隔を定義できます。デフォルト値は 30 分です。

**ステップ 4** [ユーザー アクセス (User Access)] セクションで、ユーザーのシステム アクセスを制御します。[任意の接続を許可 (Allow Any Connection)] または [特定の接続のみを許可 (Only Allow Specific Connections)] のいずれかをオンにします。

[特定の接続のみを許可 (Only Allow Specific Connections)] をオンにする場合、特定の接続を IP アドレス、IP 範囲、または CIDR 範囲として定義します。クライアント IP アドレスとともに、アプライアンス IP アドレスが [ユーザー アクセス (User Access)] セクションに自動的に追加されます。

**ステップ 5** 変更を送信し、保存します。

---

## 管理者パスワードのリセット

### Before you begin

- admin アカウントのパスワードが不明な場合は、カスタマーサポートプロバイダに連絡してパスワードをリセットしてください。
- パスワードの変更は即座に有効になり、変更を送信する必要はありません。

すべての管理者レベルのユーザーは、「admin」ユーザーのパスワードを変更できます。

### Procedure

---

**ステップ 1** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ユーザー (Users)] を選択します。

**ステップ 2** [User (ユーザー)] リストで [admin] リンクをクリックします。

**ステップ 3** [パスワードの変更 (Change Passphrase)] を選択します。

**ステップ 4** 新しいパスワードを作成するか、または入力します。

---

## 生成されたメッセージの返信アドレスの設定

レポート用に AsyncOS によって生成されたメールの返信アドレスを設定できます。

### Procedure

---

**ステップ 1** [システム管理 (System Administration)] > [返信先アドレス (Return Addresses)] を選択します。

**ステップ2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ3** 表示名、ユーザー名、およびドメイン名を入力します。

**ステップ4** 変更を送信し、保存します。

## アラートの管理

アラートとは、Cisco Secure Web Applianceで発生しているイベントに関する情報が記載されている、電子メールによる通知のことです。これらのイベントにはマイナー（情報）からメジャー（クリティカル）までの重要度（または重大度）レベルがあり、一般的にアプライアンスの特定のコンポーネントまたは機能に関連しています。



### Note

アラートと通知メール通知を受信するには、アプライアンスが電子メールメッセージへの送信に使用する SMTP リレー ホストを設定する必要があります。

## アラートの分類と重大度

アラートに含まれる情報は、アラートの分類と重大度によって決まります。アラート受信者に送信するアラート分類と重大度を指定できます。

### アラートの分類

AsyncOS は以下のタイプのアラートを送信します。

- システム (System)
- ハードウェア (Hardware)
- アップデータ (Updater)
- Web プロキシ (Web Proxy)
- マルウェア対策 (Anti-Malware)
- AMP
- L4 トラフィック モニター (L4 Traffic Monitor)
- 外部 URL カテゴリ (External URL Categories)
- ポリシーの有効期限 (Policy Expiration)

### アラートの重大度

アラートは、次の重大度に従って送信されます。

- クリティカル：ただちに対処する必要があります。



- 警告：今後モニタリングが必要な問題またはエラー。すぐに対処が必要な場合もあります。
- 情報：デバイスのルーティン機能で生成される情報。

## アラート受信者の管理

**Note**

システムのセットアップ時に **AutoSupport** をイネーブルにした場合、指定した電子メールアドレスにすべての重大度およびクラスのアラートを受信します（デフォルト）。この設定はいつでも変更できます。

### アラート受信者の追加および編集

**Procedure**

- ステップ 1** [システム管理 (System Administration)] > [アラート (Alerts)] を選択します。
- ステップ 2** [アラート受信者 (Alert Recipients)] リストで受信者をクリックして編集するか、[受信者の追加 (Add Recipient)] をクリックして新しい受信者を追加します。
- ステップ 3** 受信者の電子メールアドレスを追加または編集します。複数のアドレスをカンマで区切って入力することもできます。
- ステップ 4** 各アラート タイプごとに、受信するアラートの重大度を選択します。
- ステップ 5** 変更を送信し、保存します。

### アラート受信者の削除

**Procedure**

- ステップ 1** [システム管理 (System Administration)] > [アラート (Alerts)] を選択します。
- ステップ 2** [アラート受信者 (Alert Recipient)] のリストで、アラート受信者に対応するゴミ箱アイコンをクリックして確定します。
- ステップ 3** 変更を保存します。

## アラート設定値の設定

アラート設定はグローバルな設定であるため、すべてのアラートの動作に影響します。

## Procedure

**ステップ 1** [システム管理 (System Administration)] > [アラート (Alerts)] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** 必要に応じて、アラートの設定値を設定します。

| オプション                                                  | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アラートの送信元アドレス (From Address to Use When Sending Alerts) | アラートを送信するときに使用する RFC 2822 準拠の「Header From:」アドレス。システムのホスト名 (「alert@<hostname>」) に基づいてアドレスを自動生成するオプションが用意されています。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 重複アラート送信時の待ち時間 (Wait Before Sending a Duplicate Alert) | <p>重複アラートの時間間隔を指定します。2 つの設定があります。</p> <p>[重複アラート初回送信時の待ち時間 (秒) (Initial Number of Seconds to Wait Before Sending a Duplicate Alert)]。この値を 0 に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます (短時間に大量の電子メールを受信する可能性があります)。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。増加する秒数は、前回の待機間隔の 2 倍の値を足した秒数です。つまり、この値を 5 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後といった間隔で送信されます。</p> <p>[重複アラート送信時の最大待ち時間 (秒) (Maximum Number of Seconds to Wait Before Sending a Duplicate Alert)]。[重複するアラートメッセージを送信する前に待機する最大の秒数 (Maximum Number of Seconds to Wait Before Sending a Duplicate Alert)] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を 5 秒に設定し、最大値を 60 秒に設定すると、アラートは 5 秒、15 秒、35 秒、60 秒、120 秒などの間隔で送信されます。</p> |

### Note

AsyncOS 12.0 以降、Cisco AutoSupport オプションはアラート設定から削除されています。AutoSupport 機能は **alertconfig** CLI を使用してのみ有効または無効にできます。

**ステップ 4** 変更を送信し、保存します。

## アラート リスト

以下の項では、分類別にアラートを一覧表示します。各項の表には、アラート名 (内部で使われる **descriptor**)、アラートの実際のテキスト、説明、重大度 (クリティカル、情報、または警告) およびメッセージのテキストに含まれるパラメータ (存在する場合) が含まれています。

## ハードウェア アラート

以下の表は、AsyncOS で生成されるさまざまなハードウェア アラートのリストです。アラートの説明と重大度が記載されています。

| メッセージ                                 | アラートの重大度        | パラメータ                           |
|---------------------------------------|-----------------|---------------------------------|
| A RAID-event has occurred:<br>\$error | 警告<br>(Warning) | <b>\$error</b> : RAID エラーのテキスト。 |

## システム アラート

以下の表は、AsyncOS で生成されるさまざまなシステム アラートのリストです。アラートの説明と重大度が記載されています。

| メッセージ                                                                                            | アラートの重大度              | パラメータ                                                              |
|--------------------------------------------------------------------------------------------------|-----------------------|--------------------------------------------------------------------|
| Startup script \$name exited with error: \$message                                               | クリティカル<br>(Critical)。 | <b>\$name</b> : スクリプトの名前。<br><b>\$message</b> : エラー メッセージ テキスト。    |
| System halt failed: \$exit_status: \$output',                                                    | クリティカル<br>(Critical)。 | <b>\$exit_status</b> : コマンドの終了コード。<br><b>\$output</b> : コマンドからの出力。 |
| System reboot failed: \$exit_status: \$output                                                    | クリティカル<br>(Critical)。 | <b>\$exit_status</b> : コマンドの終了コード。<br><b>\$output</b> : コマンドからの出力。 |
| Process \$name listed \$dependency as a dependency, but it does not exist.                       | クリティカル<br>(Critical)。 | <b>\$name</b> : プロセスの名前。<br><b>\$dependency</b> : 一覧表示されている依存性の名前。 |
| Process \$name listed \$dependency as a dependency, but \$dependency is not a wait_init process. | クリティカル<br>(Critical)。 | <b>\$name</b> : プロセスの名前。<br><b>\$dependency</b> : 一覧表示されている依存性の名前。 |
| Process \$name listed itself as a dependency.                                                    | クリティカル<br>(Critical)。 | <b>\$name</b> : プロセスの名前。                                           |

| メッセージ                                                                                                                                                                                                                   | アラートの重大度           | パラメータ                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Process \$name listed \$dependency as a dependency multiple times.                                                                                                                                                      | クリティカル (Critical)。 | <b>\$name</b> : プロセスの名前。<br><b>\$dependency</b> : 一覧表示されている依存性の名前。                                                                 |
| Dependency cycle detected: \$cycle.                                                                                                                                                                                     | クリティカル (Critical)。 | <b>\$cycle</b> : サイクルに関係するプロセス名のリスト。                                                                                               |
| An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider:<br><br>Error: \$error.                       | 警告 (Warning)。      | <b>\$error</b> : 例外に関連付けられたエラー メッセージ。                                                                                              |
| There is an error with “\$name”.                                                                                                                                                                                        | クリティカル (Critical)。 | <b>\$name</b> : コア ファイルを生成したプロセスの名前。                                                                                               |
| An application fault occurred: “\$error”                                                                                                                                                                                | クリティカル (Critical)。 | <b>\$error</b> : エラーのテキスト (通常はトレースバック)。                                                                                            |
| Appliance: \$appliance, User: \$username, Source IP: \$ip, Event: Account locked due to X failed login attempts.<br><br>User \$username is locked after X consecutive login failures. Last login attempt was from \$ip. | 情報 (Information)。  | <b>\$appliance</b> : 特定の Secure Web Appliance の ID。<br><b>\$username</b> : 特定のユーザー アカウントの ID。<br><b>\$ip</b> : ログインが試行された IP アドレス。 |
| Tech support: Service tunnel has been enabled, port \$port                                                                                                                                                              | 情報 (Information)。  | <b>\$port</b> : サービス トンネルに使用されるポート番号。                                                                                              |
| Tech support: Service tunnel has been disabled.                                                                                                                                                                         | 情報 (Information)。  | 適用なし                                                                                                                               |

| メッセージ                                                                                                                                                                                                                                                                               | アラートの重大度         | パラメータ                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>The host at \$ip has been added to the blocked list because of an SSH DOS attack.</li> <li>The host at \$ip has been permanently added to the ssh allowed list.</li> <li>The host at \$ip has been removed from the blocked list.</li> </ul> | 警告<br>(Warning)。 | <p><b>\$ip</b> : ログインが試行された IP アドレス。</p> <p><b>説明 :</b></p> <p>SSH を介してアプライアンスへの接続を試みているが、有効なクレデンシャルを提示しない IP アドレスは、2 分以内に 11 回以上試行に失敗した場合、SSH のブロックリストに追加されます。</p> <p>同じ IP アドレスからユーザが正常にログインすると、その IP アドレスは許可リストに追加されます。</p> <p>許可リストのアドレスは、それらがブロックリストに含まれていてもアクセスが許可されます。</p> <p>エントリは約 1 日後にブロックリストから自動的に削除されます。</p> |



**Note** システムアラートには、機能キーアラート、ロギングアラート、レポートアラートが含まれます。これらのアラートは、システムアラートの一部として設定した後に受信します。

## 機能キー アラート

以下の表は、AsyncOS で生成されるさまざまな機能キー アラートのリストです。アラートの説明と重大度が記載されています。

| メッセージ                                                                                                            | アラートの重大度             | パラメータ                     |
|------------------------------------------------------------------------------------------------------------------|----------------------|---------------------------|
| A “\$feature” key was downloaded from the key server and placed into the pending area. EULA acceptance required. | 情報<br>(Information)。 | <b>\$feature</b> : 機能の名前。 |
| Your “\$feature” evaluation key has expired. Please contact your authorized sales representative.                | 警告<br>(Warning)。     | <b>\$feature</b> : 機能の名前。 |

| メッセージ                                                                                                                    | アラートの重大度         | パラメータ                                                          |
|--------------------------------------------------------------------------------------------------------------------------|------------------|----------------------------------------------------------------|
| Your “\$feature” evaluation key will expire in under \$days day(s). Please contact your authorized sales representative. | 警告<br>(Warning)。 | <b>\$feature</b> : 機能の名前。<br><b>\$days</b> : 機能キーの期限が切れるまでの日数。 |

## ロギングアラート

以下の表は、AsyncOS で生成されるさまざまなロギングアラートのリストです。アラートの説明と重大度が記載されています。

| メッセージ                                                                                            | アラートの重大度              | パラメータ                                                                                                                                  |
|--------------------------------------------------------------------------------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| \$error.                                                                                         | 情報<br>(Information)。  | <b>\$error</b> : エラーのトレースバック文字列。                                                                                                       |
| Log Error: Subscription \$name: Log partition is full.                                           | クリティカル<br>(Critical)。 | <b>\$name</b> : ログサブスクリプション名。                                                                                                          |
| Log Error: Push error for subscription \$name: Failed to connect to \$ip: \$reason.              | クリティカル<br>(Critical)。 | <b>\$name</b> : ログサブスクリプション名。<br><b>\$ip</b> : リモートホストのIPアドレス。<br><b>\$reason</b> : 接続エラーについて説明するテキスト。                                 |
| Log Error: Push error for subscription \$name: An FTP command failed to \$ip: \$reason.          | クリティカル<br>(Critical)。 | <b>\$name</b> : ログサブスクリプション名。<br><b>\$ip</b> : リモートホストのIPアドレス。<br><b>\$reason</b> : 問題点について説明するテキスト。                                   |
| Log Error: Push error for subscription \$name: SCP failed to transfer to \$ip:\$port: \$reason', | クリティカル<br>(Critical)。 | <b>\$name</b> : ログサブスクリプション名。<br><b>\$ip</b> : リモートホストのIPアドレス。<br><b>\$port</b> : リモートホストのポート番号。<br><b>\$reason</b> : 問題点について説明するテキスト。 |

| メッセージ                                                                                                            | アラートの重大度           | パラメータ                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Error: 'Subscription \$name: Failed to connect to \$hostname (\$ip): \$error.                                | クリティカル (Critical)。 | <b>\$name</b> : ログサブスクリプション名。<br><b>\$hostname</b> : Syslog サーバーのホスト名。<br><b>\$ip</b> : Syslog サーバーの IP アドレス。<br><b>\$error</b> : エラーメッセージのテキスト。 |
| Log Error: Subscription \$name: Network error while sending log data to syslog server \$hostname (\$ip): \$error | クリティカル (Critical)。 | <b>\$name</b> : ログサブスクリプション名。<br><b>\$hostname</b> : Syslog サーバーのホスト名。<br><b>\$ip</b> : Syslog サーバーの IP アドレス。<br><b>\$error</b> : エラーメッセージのテキスト。 |
| Subscription \$name: Timed out after \$timeout seconds sending data to syslog server \$hostname (\$ip).          | クリティカル (Critical)。 | <b>\$name</b> : ログサブスクリプション名。<br><b>\$timeout</b> : 秒単位のタイムアウト。<br><b>\$hostname</b> : Syslog サーバーのホスト名。<br><b>\$ip</b> : Syslog サーバーの IP アドレス。  |
| Subscription \$name: Syslog server \$hostname (\$ip) is not accepting data fast enough.                          | クリティカル (Critical)。 | <b>\$name</b> : ログサブスクリプション名。<br><b>\$hostname</b> : Syslog サーバーのホスト名。<br><b>\$ip</b> : Syslog サーバーの IP アドレス。                                    |

| メッセージ                                                                                                                                                         | アラートの重大度          | パラメータ                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Subscription \$name: Oldest log file(s) were removed because log files reached the maximum number of \$max_num_files. Files removed include: \$files_removed. | 情報 (Information)。 | <b>\$name</b> : ログサブスクリプション名。<br><b>\$max_num_files</b> : ログサブスクリプションごとに許可されるファイルの最大数。<br><b>\$files_removed</b> : 削除されたファイルのリスト。 |

## レポートアラート

以下の表は、AsyncOS で生成されるさまざまなレポートアラートのリストです。アラートの説明と重大度が記載されています。

| メッセージ                                                                                                                                                                                                                                                                                                                                                                                                            | アラートの重大度           | パラメータ                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------------------|
| The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.                                                                                                                                                                                                                                                                                                | クリティカル (Critical)。 | 適用なし                               |
| The reporting system is now able to handle new data.                                                                                                                                                                                                                                                                                                                                                             | 情報 (Information)。  | 適用なし                               |
| A failure occurred while building periodic report '\$report_title'.<br><br>This subscription should be examined and deleted if its configuration details are no longer valid.                                                                                                                                                                                                                                    | クリティカル (Critical)。 | <b>\$report_title</b> : レポートのタイトル。 |
| A failure occurred while emailing periodic report '\$report_title'.<br><br>This subscription has been removed from the scheduler.                                                                                                                                                                                                                                                                                | クリティカル (Critical)。 | <b>\$report_title</b> : レポートのタイトル。 |
| Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above \$threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc).<br><br>Once disk usage drops below \$threshold percent, full processing of reporting data will be restarted automatically. | 警告 (Warning)。      | <b>\$threshold</b> : しきい値。         |



| メッセージ                                                                                                                                                                                                                                                                                                                                                                                                            | アラートの重大度           | パラメータ                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------|
| PERIODIC REPORTS: While building periodic report \$report_title' the expected domain specification file could not be found at '\$file_name'. No reports were sent.                                                                                                                                                                                                                                               | クリティカル (Critical)。 | <b>\$report_title</b> : レポートのタイトル。<br><b>\$file_name</b> : ファイルの名前。                                       |
| Counter group "\$counter_group" does not exist.                                                                                                                                                                                                                                                                                                                                                                  | クリティカル (Critical)。 | <b>\$counter_group</b> : counter_group の名前。                                                               |
| PERIODIC REPORTS: While building periodic report \$report_title' the domain specification file '\$file_name' was empty. No reports were sent.                                                                                                                                                                                                                                                                    | クリティカル (Critical)。 | <b>\$report_title</b> : レポートのタイトル。<br><b>\$file_name</b> : ファイルの名前。                                       |
| PERIODIC REPORTS: Errors were encountered while processing the domain specification file '\$file_name' for the periodic report '\$report_title'. Any line which has any reported problem had no report sent.<br><br>\$error_text                                                                                                                                                                                 | クリティカル (Critical)。 | <b>\$report_title</b> : レポートのタイトル。<br><b>\$file_name</b> : ファイルの名前。<br><b>\$error_text</b> : 発生したエラーのリスト。 |
| Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above \$threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc).<br><br>Once disk usage drops below \$threshold percent, full processing of reporting data will be restarted automatically. | 警告 (Warning)。      | <b>\$threshold</b> : しきい値。                                                                                |
| The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled.<br><br>The error message is:<br><br>\$err_msg                                                                                                                        | クリティカル (Critical)。 | <b>\$err_msg</b> : エラー メッセージ テキスト。                                                                        |

## アップデータ アラート

以下の表は、AsyncOS で生成されるさまざまなアップデータ アラートのリストです。アラートの説明と重大度が記載されています。

| メッセージ                                                                                                                                                             | アラートの重大度           | パラメータ                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------|
| The \$app application tried and failed \$attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage. | 警告 (Warning)。      | <b>\$app</b> : Secure Web Appliance セキュリティ サービス名。<br><b>\$attempts</b> : 試行回数。 |
| The updater has been unable to communicate with the update server for at least \$threshold.                                                                       | 警告 (Warning)。      | <b>\$threshold</b> : しきい値の時間。                                                  |
| Unknown error occurred: \$traceback.                                                                                                                              | クリティカル (Critical)。 | <b>\$traceback</b> : トレースバック情報。                                                |
| Certificate Revoke: OCSP validation failed for the UPDATER Server Certificate (\$host:\$port). Ensure the certificate is valid.                                   | クリティカル (Critical)  | <b>\$host</b> : UPDATER サーバーのホスト名。<br><b>\$port</b> : UPDATER サーバーのポート。        |

## マルウェア対策アラート

Advanced Malware Protection に関連するアラートについては、[Advanced Malware Protection の問題に関するアラートの確実な受信, on page 498](#)を参照してください。

## ポリシーの期限切れアラート

次の表は、AsyncOS で生成されるさまざまなポリシー アラートのリストです。アラートの説明と重大度が記載されています。

| メッセージ                                                     | アラートの重大度 | パラメータ                                                                                               |
|-----------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------|
| '\$PolicyType': '\$GroupName' は、有効期限の設定のため、ディセーブルにされています。 | 情報       | <b>\$PolicyType</b> : は、Web ポリシー タイプに基づくアクセスポリシー/復号ポリシーです。<br><b>\$GroupName</b> : は、ポリシーグループの名前です。 |
| '\$PolicyType': '\$GroupName' は、3 日後に期限切れとなります。           | 情報       | <b>\$PolicyType</b> : は、Web ポリシー タイプに基づくアクセスポリシー/復号ポリシーです。<br><b>\$GroupName</b> : は、ポリシーグループの名前です。 |

## FIPS Compliance

Federal Information Processing Standard (FIPS) は、機密情報であるが機密扱いされていない情報を保護するために、すべての政府機関で使用する暗号化モジュールの要件を規定しています。FIPS は、連邦政府のセキュリティとデータ プライバシー要件の遵守を確実にするために役立ちます。国立標準技術研究所 (NIST) によって開発された FIPS は、連邦政府の要件を満たす任意の規格がない場合に使用されます。

Secure Web Appliance は Cisco Common Cryptographic Module (C3M) を使用して FIPS モードの FIPS 140-2 準拠を実現します。デフォルトでは、FIPS モードはディセーブルです。

### 関連項目

- [FIPS モードの問題, on page 740](#)

## FIPS 証明書の要件

FIPS モードでは、Secure Web Appliance でイネーブルになっているすべての暗号化サービスについて FIPS 準拠の証明書を使用する必要があります。これは、以下の暗号化サービスに適用されます。

- HTTPS プロキシ
- 認証
- SaaS のアイデンティティ プロバイダー
- アプライアンス管理 HTTPS サービス
- セキュア ICAP 外部 DLP 設定
- Identity Services Engine
- カスタムの信頼できるルート CA
- SSL の設定
- SSH の設定
- NTP の設定



### Note

FIPS モードをイネーブルにする前に、FIPS 準拠証明書を使用してアプライアンス管理 HTTPS サービスを設定する必要があります。他の暗号化サービスはイネーブルにする必要はありません。

FIPS 準拠の証明書は以下の要件を満たす必要があります。

| 証明書  | アルゴリズム | 署名アルゴリズム                                         | 注記                                                                                                   |
|------|--------|--------------------------------------------------|------------------------------------------------------------------------------------------------------|
| X509 | RSA    | sha1WithRSAEncryption<br>sha256WithRSAEncryption | 最適な復号パフォーマンスと十分なセキュリティを実現するために、1024 ビットのキーサイズを推奨します。ビットサイズをさらに大きくすると、セキュリティは向上しますが、復号のパフォーマンスに影響します。 |

## FIPS 証明書の検証

FIPS モードがイネーブルの場合、アプライアンスは次の証明書チェックを実行します。

- Secure Web Applianceにアップロードされたすべての証明書は、UI によってアップロードされたのか、それとも `certconfig` CLI コマンドによってアップロードされたのかに関係なく、CC 標準に厳格に従うように検証されます。Secure Web Applianceの信頼ストア内の適切な信頼パスが設定されていない証明書は、アップロードできません。
- 信頼できるパス検証によって証明書の署名が検証され、すべての署名者証明書に対して検証済みの `basicConstraints` および `CAFlag` のセットによって証明書/公開キーの改ざんが検証されます。
- 失効リストに対して証明書を検証するために OCSP 検証を使用できます。これは、`certconfig` CLI コマンドを使用して設定できます。



(注) 新しいサブコマンド `OCSPVALIDATION_FOR_SERVER_CERT` がメインの CLI コマンド `certconfig` の下に追加されました。新しいサブコマンドを使用すると、LDAP サーバ証明書およびアップデータサーバ証明書の OCSP 検証を有効にできます。証明書の検証が有効になっている場合、通信に関係する証明書が失効するとアラートが表示されます。

厳格な証明書検証について (200 ページ) も参照してください。

## FIPS モードの有効化または無効化

### Before you begin

- アプライアンス設定のバックアップ コピーを作成します (以下を参照)。[アプライアンス設定ファイルの保存, on page 133](#)
- FIPS モードで使用される証明書で、FIPS 140-3 認定の公開キーアルゴリズムが使用されていることを確認します ([FIPS 証明書の要件, on page 194](#)を参照)。

**Note**

- FIPS モードを変更すると、アプライアンスが再起動されます。
- FIPS モードを無効にした場合、SSL および SSH 設定（FIPS モードが有効にされている場合は、自動的に FIPS 対応になるようにする設定）はデフォルト値にリセットされません。接続する際、厳格でない SSH/SSL 設定を使用してクライアントが接続できるようにする必要があります場合は、明示的にこれらの設定を変更する必要があります。詳細については、[SSL の設定](#) , on page 197 を参照してください。

**Procedure**

- ステップ 1** [システム管理（System Administration）]>[FIPS モード（FIPS Mode）] を選択します。
- ステップ 2** [設定の編集（Edit Settings）] をクリックします。
- ステップ 3** [FIPS コンプライアンスの有効化（Enable FIPS Compliance）] をオンにして、FIPS コンプライアンスを有効にします。
- [FIPS コンプライアンスの有効化（Enable FIPS Compliance）] をオンにすると、[重大な機密性パラメータ（CSP）の暗号化を有効にする（Enable encryption of Critical Sensitive Parameters (CSP)）] チェックボックスが有効になります。
- ステップ 4** パスワード、認証情報、証明書、共有キーなどの設定データの暗号化を有効にする場合は、[重大な機密性パラメータ（CSP）の暗号化を有効にする（Enable encryption of Critical Sensitive Parameters (CSP)）] をオンにします。
- ステップ 5** [送信（Submit）] をクリックします。
- ステップ 6** [続行（Continue）] をクリックして、アプライアンスの再起動を許可します。

## システムの日時の管理

- [タイムゾーンの設定](#), on page 196
- [NTP サーバーによるシステムクロックの同期](#) , on page 197

### タイムゾーンの設定

**Procedure**

- ステップ 1** [システム管理（System Administration）]>[タイムゾーン（Time Zone）] を選択します。
- ステップ 2** [設定の編集（Edit Settings）] をクリックします。
- ステップ 3** 地域、国、およびタイムゾーンを選択するか、GMT オフセットを選択します。

ステップ 4 変更を送信し、保存します。

## NTP サーバーによるシステム クロックの同期

アプライアンスで手動で時間を設定するのではなく、ネットワーク タイムプロトコル (NTP) サーバーに照会して現在の日時を追跡できるように **Secure Web Appliance**を設定することをお勧めします。これは、特にアプライアンスが他のデバイスと統合されている場合に該当します。統合されたすべてのデバイスが同じ NTP サーバーを使用する必要があります。

Secure Web Appliance は NTPv4 をサポートします。

### Procedure

ステップ 1 [システム管理 (System Administration)] > [時間の設定 (Time Settings)] を選択します。

ステップ 2 [設定の編集 (Edit Settings)] をクリックします。

ステップ 3 [時刻の設定方法 (Time Keeping Method)] として [NTP (Network Time Protocol)] を使用 (Use Network Time Protocol) ] を選択します。

ステップ 4 NTP サーバの完全修飾ホスト名または IP アドレスを入力し、以下を実行します：

- [キー タイプ (Key Type)] ドロップダウン リストから [MD5]、[SHA-1] または [AES-CMAC] を選択します。
- 指定された NTP サーバから、対応する MD5、SHA-1、または AES-CMAC キー番号およびキー値を入力します。
- [行の追加 (Add Row)] をクリックします。

#### Note

FIPS が有効な場合、[キー タイプ (Key Type)] ドロップダウン リストに MD5 暗号化方式が表示されません。これは、MD5 暗号化方式が FIPS に準拠していないために予想される動作です。

ステップ 5 (任意) NTP クエリーに使用するアプライアンスのネットワーク インターフェイス タイプ (管理またはデータのいずれか) に関連付けられている、ルーティングテーブルを選択します。これは、NTP クエリーが発信される IP アドレスになります。

#### Note

このオプションは、アプライアンスがデータ トラフィック用と管理トラフィック用に分割ルーティングを使用している場合にのみ変更できます。

ステップ 6 変更を送信し、保存します。

## SSL の設定

セキュリティを向上させるために、いくつかのサービスで SSL v3 とさまざまなバージョンの TLS をイネーブルまたはディセーブルにできます。最善のセキュリティを実現するために、す

すべてのサービスで SSL v3 をディセーブルにすることをお勧めします。デフォルトでは、すべてのバージョンの TLS がイネーブルに設定され、SSL がディセーブルに設定されます。

**Note**

これらの機能は、`sslconfig` CLI コマンドを使用してイネーブルまたはディセーブルにすることもできます。 [Secure Web Appliance CLI コマンド, on page 780](#)を参照してください。

**Note**

- TLSv1.0 と TLSv1.1 は、プロキシ構成以外の SSL 構成ではサポートされなくなりました。AsyncOS をアップグレードする前に、TLS バージョンを TLSv1.2 以降に変更する必要があります。
- SSL 設定ページおよび CLI から、ポート 6443、アプライアンス管理 Web ユーザーインターフェイス、および NGUI の TLS バージョンと暗号をカスタマイズできるようになりました。  
CLI から暗号をカスタマイズする場合は、`sslconfig` コマンドを使用できます。
- TLS 暗号が無効になる SSL 構成を修正または変更した場合は、アプリケーションを再起動します。

**Procedure**

**ステップ 1** [システム管理 (System Administration)] > [SSL 設定 (SSL Configuration)] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** これらのサービスで SSL v3 と TLS v1.x をイネーブルにするには、対応するチェックボックスをオンにします。

- [アプライアンス管理 Web ユーザー インターフェイス (Appliance Management Web User Interface)] : この設定を変更すると、すべてのアクティブ ユーザーの接続が切断されます。

**Note**

- プロトコルバージョンの場合、TLSv1.2 はデフォルトで有効になっています。[TLSv1.3] チェックボックスをオンにするか、`sslconfig` コマンドを使用して、TLSv1.3 を選択できるようになりました。このコマンドの詳細については、[Secure Web Appliance CLI コマンド, on page 780](#)を参照してください。プロトコルバージョンとして TLSv1.3 を選択する場合は、TLSv1.3 を使用する暗号を提供する必要があります。
- [プロキシサービス (Proxy Services)] : セキュアクライアント用の HTTPS プロキシとクレデンシャル暗号化が含まれます。このセクションには以下も含まれています。
  - [使用する暗号 (Cipher(s) to Use)] : プロキシサービスとの通信に使用する追加の暗号スイートを入力できます。スイートの区切りにはコロン (:) を使用します。特定の暗号の使用を防止するに

は、その文字列の先頭に感嘆符 (!) を追加します。たとえば !EXP-DHE-RSA-DES-CBC-SHA と入力します。

確認済みの TLS/SSL バージョンに適切なスイートのみを入力するようにしてください。詳細および暗号リストについては、<https://www.openssl.org/docs/manmaster/man1/ciphers.html> を参照してください。

アプライアンスは TLSv1.3 バージョンをサポートしています。暗号 TLS\_AES\_256\_GCM\_SHA384 がデフォルトの暗号リストに追加されました。デフォルトでは、TLSv1.3 はアプライアンス上で有効になります。

AsyncOS バージョン 14.0 では、暗号 TLS\_AES\_128\_GCM\_SHA256 および TLS\_CHACHA20\_POLY1305\_SHA256 がデフォルトの暗号リストに追加されます。

AsyncOS バージョン 9.0 以前のデフォルトの暗号は、DEFAULT:+kEDH です。

AsyncOS バージョン 9.1 ~ 11.8 のデフォルトの暗号は、次のとおりです。

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

この場合、デフォルトの暗号は ECDHE 暗号の選択によって変わる場合があります。

AsyncOS バージョン 12.0 以降のデフォルトの暗号は、次のとおりです。

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384

EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

#### Note

新しい AsyncOS バージョンにアップグレードする際に、デフォルトの暗号スイートを更新します。暗号スイートは自動的に更新されません。以前のバージョンから AsyncOS 12.0 以降にアップグレードする場合は、暗号スイートを次のように更新することを推奨します。

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384

EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

- [TLS 圧縮の無効化 (推奨) (Disable TLS Compression (Recommended))] : TLS 圧縮を無効にするには、このチェックボックスをオンにします。最善のセキュリティを実現するには、この設定が推奨されます。
- [セキュア LDAP サービス (Secure LDAP Services)] : 認証、外部認証、およびセキュア モビリティが含まれます。
- [セキュア ICAP サービス (外部 DLP) (Secure ICAP Services (External DLP))] : アプライアンスと外部 DLP (データ漏洩防止) サーバー間の ICAP 通信の保護に使用するプロトコルを選択します。詳細については、[外部 DLP サーバーの設定, on page 528](#) を参照してください。



- [サービスの更新 (Update Service)] : アプライアンスと利用可能なアップデート サーバー間の通信に使用するプロトコルを選択します。サービスの更新の詳細については、[AsyncOS for Web のアップグレードとアップデート, on page 206](#)を参照してください。

**Note**

シスコのアップデートサーバーはSSL v3をサポートしていません。したがって、TLS 1.0 以上をCisco アップデート サービスでイネーブルにしておく必要があります。ただし、ローカル アップデート サーバーでは現在も SSL v3 を使用することができます（そのように設定されている場合）。それらのサーバーでサポートされている SSL/TLS のバージョンを確認してください。

**ステップ 4** [Submit] をクリックします。

## 証明書の管理

アプライアンスでは、デジタル証明書を使用してさまざまな接続を確立、確認、保護します。[証明書の管理 (Certificate Management)] ページでは、現在の証明書リストの表示や更新、信頼できるルート証明書の管理、およびブロックされた証明書の表示を行うことができます。

**Note**

アプライアンスがインターネットに接続されていない場合、[証明書管理 (Certificate Management)] ページのロードに時間がかかり、タイムアウトエラーが発生します。さらに、証明書をロードした後、[マニフェストを取得できませんでした (Failed to fetch manifest)] ネットワークエラーが[証明書の更新 (Certificate Updates)] リストに表示されます。

**関連項目**

- 証明書およびキーについて, [on page 201](#)
- 証明書の更新, [on page 202](#)
- 信頼できるルート証明書の管理, [on page 201](#)
- ブロックされた証明書の表示, [on page 202](#)

## 厳格な証明書検証について

AsyncOS 10.5 での FIPS モード更新のリリースに伴い、提示される証明書はすべて、アップロード前にコモン クライテリア (CC) 標準に準拠していることを確認するため厳格に検証されます。証明書を証明書失効リストと照合して検証するには、OCSP 検証を使用できます。

適切で有効な証明書が Secure Web Appliance にアップロードされていることと、すべての関連サーバーで円滑な SSL ハンドシェイクを実行できるように、有効でセキュアな証明書がすべての関連サーバーで設定されていることを確認する必要があります。

厳格な証明書検証は、次の証明書のアップロードに適用されます。

- HTTPS プロキシ ([セキュリティサービス (Security Services)] > [HTTPS プロキシ (HTTPS Proxy)])

- ファイル分析サーバー ([セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] > [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] > [ファイル分析サーバー (File Analysis Server)] : [プライベートクラウドおよび認証局 (Private Cloud & Certificate Authority)] : [アップロードされた認証局の使用 (Use Uploaded Certificate Authority)] )
- 信頼できるルート証明書 ([ネットワーク (Network)] > [証明書の管理 (Certificate Management)] )
- グローバル認証の設定 ([ネットワーク (Network)] > [認証 (Authentication)] > [グローバル認証の設定 (Global Authentication Settings)] )
- SaaS の ID プロバイダ ([ネットワーク (Network)] > [SaaS の ID プロバイダ (Identity Provider for SaaS)] )
- Identity Services Engine ([ネットワーク (Network)] > [Identity Services Engine])
- 外部 DLP サーバー ([ネットワーク (Network)] > [外部DLPサーバー (External DLP Servers)] )
- LDAP およびセキュア LDAP ([ネットワーク (Network)] > [認証 (Authentication)] > [レルム (Realm)] )

[FIPS Compliance \(194 ページ\)](#) も参照してください。

## 証明書およびキーについて

ユーザーに認証を要求するときに、ブラウザはセキュア HTTPS 接続を使用して Web プロキシに認証クレデンシャルを送信します。Secure Web Applianceは、デフォルトで付属の「Cisco Web セキュリティ アプライアンス デモ証明書 (Cisco Web Security Appliance Demo Certificate)」を使用して、クライアントとの HTTPS 接続を確立します。多くのブラウザでは、証明書が無効であるという内容の警告が表示されます。無効な証明書に関するメッセージをユーザーに表示しないようにするには、アプリケーションで自動的に認識される証明書とキーのペアをアップロードします。

### 関連項目

- [証明書とキーのアップロードまたは生成, on page 203](#)
- [証明書署名要求, on page 204](#)
- [中間証明書, on page 205](#)

## 信頼できるルート証明書の管理

Secure Web Applianceには、信頼できるルート証明書のリストが付属し、これが維持されます。信頼できる証明書を持つ Web サイトでは、復号は必要ありません。

信頼できる証明書のリストに証明書を追加し、機能的に証明書を削除すると、信頼できる証明書のリストを管理できます。Secure Web Applianceでは、プライマリリストから証明書は削除

されませんが、ユーザーが証明書の信頼を無効化できます。これで、信頼できるリストから証明書が機能的に削除されます。

信頼できるルート証明書を追加、上書き、ダウンロードするには、以下の手順を実行します。

### Procedure

- 
- ステップ 1** [ネットワーク (Network)] > [証明書の管理 (Certificate Management)] の順に選択します。
- ステップ 2** [証明書の管理 (Certificate Management)] ページの [信頼できるルート証明書の管理 (Manage Trusted Root Certificates)] をクリックします。
- ステップ 3** シスコ認識済みリストに記載されていない認証局の署名が付いたカスタムの信頼できるルート証明書を追加するには、以下の手順を実行します。
- [インポート (Import)] をクリックし、証明書ファイルを参照して選択し、[送信 (Submit)] します。
- ステップ 4** 1 つ以上のシスコ認識済み証明書の信頼を上書きするには、以下の手順を実行します。
- 上書きする各エントリの [信頼を上書き (Override Trust)] チェックボックスをオンにします。
  - [送信 (Submit)] をクリックします。
- ステップ 5** 特定の証明書のコピーをダウンロードするには、以下の手順を実行します。
- シスコの信頼できるルート証明書リストで証明書の名前をクリックし、エントリを展開します。
  - [証明書をダウンロード (Download Certificate)] をクリックします。
- 

## 証明書の更新

[更新 (Updates)] セクションには、アプライアンス上のシスコの信頼できるルート証明書とブロックリストのバンドルについて、バージョン情報と最終更新情報が一覧表示されます。これらのバンドルは定期的に更新されます。

### Procedure

---

[証明書の管理 (Certificate Management)] ページで [今すぐ更新 (Update Now)] をクリックし、アップデート可能なすべてのバンドルを更新します。

---

## ブロックされた証明書の表示

シスコにより無効であると判定されてブロックされた証明書のリストを表示するには、以下の手順を実行します。

## Procedure

[ブロック済み証明書を表示 (View Blocked Certificates)] をクリックします。

## 証明書とキーのアップロードまたは生成

一部の AsyncOS 機能では、接続の確立、確認、または保護のために証明書とキーが必要です。たとえば、Identity Services Engine (ISE) などの機能がこれに該当します。既存の証明書とキーをアップロードしたり、機能を設定するときに新しい証明書とキーを生成したりできます。

### 証明書およびキーのアップロード

アプライアンスにアップロードする証明書は、以下の要件を満たしている必要があります。

- X.509 標準を使用していること。
- 一致する秘密キーが PEM 形式で含まれていること。DER 形式はサポートされていません。

## Procedure

**ステップ 1** [アップロードされた証明書とキーを使用 (Use Uploaded Certificate and Key)] を選択します。

**ステップ 2** [証明書 (Certificate)] フィールドで [参照 (Browse)] をクリックし、アップロードするファイルを検索します。

### Note

Web プロキシは、ファイル内の最初の証明書またはキーを使用します。証明書ファイルは PEM 形式にする必要があります。DER 形式はサポートされていません。

**ステップ 3** [キー (Key)] フィールドで [参照 (Browse)] をクリックし、アップロードするファイルを指定します。

### Note

キーの長さは 512、1024、または 2048 ビットである必要があります。秘密キー ファイルは PEM 形式でなければなりません。DER 形式はサポートされていません。

**ステップ 4** キーが暗号化されている場合は、[キーは暗号化されています (Key is Encrypted)] を選択します。

**ステップ 5** [ファイルのアップロード (Upload File)] をクリックします。

## 証明書およびキーの生成

## Procedure

**ステップ 1** [生成された証明書とキーを使用 (Use Generated Certificate and Key)] を選択します。

**ステップ 2** [新しい証明書とキーを生成 (Generate New Certificate and Key)] をクリックします。

- a) [証明書とキーを生成 (Generate Certificate and Key)] ダイアログボックスで、必要な生成情報を入力します。

**Note**

[共通名 (Common Name)] フィールドには、スラッシュ (/) を除く任意の ASCII 文字を入力できます。

- b) [証明書とキーを生成 (Generate Certificate and Key)] ダイアログボックスで、[生成 (Generate)] をクリックします。

生成が完了すると、[証明書 (Certificate)] セクションに、証明書の情報と 2 つのリンク ([証明書をダウンロード Download Certificate] と [証明書署名要求のダウンロード (Download Certificate Signing Request)]) が表示されます。また、認証局 (CA) から署名付き証明書を受信したときに、それをアップロードするために使用する [署名付き証明書 (Signed Certificate)] オプションも表示されます。

**ステップ 3** [証明書をダウンロード Download Certificate] をクリックして、アプライアンスにアップロードする新しい証明書をダウンロードします。

**ステップ 4** [証明書署名要求のダウンロード (Download Certificate Signing Request)] をクリックして、署名のために認証局 (CA) に送信する新しい証明書ファイルをダウンロードします。この処理の詳細については、[証明書署名要求, on page 204](#)を参照してください。

- a) CA から署名付き証明書が返送されたら、[証明書 (Certificate)] フィールドの [署名付き証明書 (Signed Certificate)] で [参照 (Browse)] をクリックして、署名付き証明書ファイルを指定し、[ファイルのアップロード (Upload File)] をクリックしてアプライアンスにアップロードします。
- b) CA のルート証明書がアプライアンスの信頼できるルート証明書リストに含まれていることを確認します。リストにない場合は追加します。詳細については、[信頼できるルート証明書の管理, on page 201](#)を参照してください。

## 証明書署名要求

Secure Web Appliance は、アプライアンスにアップロードされた証明書の証明書署名要求 (CSR) を生成することはできません。そのため、アプライアンス用に作成された証明書を使用するには、別のシステムから署名要求を発行する必要があります。後でアプライアンスにインストールする必要があるため、このシステムから PEM 形式のキーを保存します。

最新バージョンの OpenSSL がインストールされた、任意の UNIX マシンを使用できます。CSR にアプライアンスのホスト名があることを確認してください。OpenSSL を使用した CSR の生成の詳細については、以下の場所にあるガイドラインを参照してください。

[http://www.modssl.org/docs/2.8/ssl\\_faq.html#ToC28](http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28)

CSR が生成されたら、認証局（CA）に送信します。CA は、証明書を PEM 形式で返します。

初めて証明書を取得する場合は、インターネットで「certificate authority services SSL server certificates（SSL サーバー証明書を提供している認証局）」を検索して、環境のニーズに最も適したサービスを選択します。サービスの手順に従って、SSL 証明書を取得します。



**Note** 独自の証明書を生成して署名することもできます。そのためのツールは <http://www.openssl.org> の無料のソフトウェア OpenSSL に含まれています。

## 中間証明書

ルート認証局(CA)の証明書検証に加えて、AsyncOS では、中間証明書の検証の使用もサポートされます。中間証明書とは信頼できるルート認証局によって発行された証明書であり、追加の証明書を作成するために使用されます。これは、信頼の連鎖を作成します。たとえば、信頼できるルート認証局によって証明書を発行する権利が与えられた **example.com** によって証明書が発行されたとします。**example.com** によって発行された証明書は、**example.com** の秘密キーおよび信頼できるルート認証局の秘密キーと照合して検証する必要があります。

サーバーは、SSL ハンドシェイクで「証明書チェーン」を送信し、クライアント（ブラウザなど。この場合は HTTPS プロキシである **Secure Web Appliance**）がサーバーを認証できるようにします。通常、サーバー証明書は中間証明書により署名され、中間証明書は信頼できるルート証明書により署名され、ハンドシェイク中にサーバー証明書と全体の証明書チェーンがクライアントに表示されます。通常、ルート証明書は **Secure Web Appliance** の信頼できる証明書ストアに存在するため、証明書チェーンの検証は成功します。

ただし、サーバーでエンドポイントエンティティ証明書が変更された場合、新しいチェーンに必要な更新が実行されません。その結果、サーバーは SSL ハンドシェイク中にサーバー証明書のみを表示し、**Secure Web Appliance** プロキシは中間証明書が存在しないため証明書チェーンを検証できません。

以前のソリューションでは、**Secure Web Appliance** 管理者が手動で介入し、信頼できる証明書ストアに必要な中間証明書をアップロードしていました。現在は、CLI コマンド `advancedproxyconfig > HTTPS > Do you want to enable automatic discovery and download of missing Intermediate Certificates?` を使用して、「中間証明書の検出」を有効にできます。これは、**Secure Web Appliance** がこれらの状況で手動手順を排除しようとするために使用するプロセスです。

中間証明書の検出では、「AIA 追跡」という方法を使用します。この方法では、信頼できない証明書が存在する場合、**Secure Web Appliance** はその証明書の「Authority Information Access」という拡張情報があるか検証します。この拡張情報には、オプションの CA 発行者の URI フィールドが含まれています。このフィールドには、問題のサーバー証明書の署名に使用される発行者証明書を照会することができます。これが使用可能になると、**Secure Web Appliance** はルートの CA 証明書が取得されるまで発行者の証明書を再帰的に取得し、チェーンを再度検証しようとしています。

## AsyncOS for Web のアップグレードとアップデート

シスコでは、AsyncOS for Web とそのコンポーネント向けに、アップグレード（新しいソフトウェア バージョン）とアップデート（現在のソフトウェア バージョンの変更）を定期的にリリースしています。



**Note** TLSv1.0 と TLSv1.1 は、プロキシ構成以外の SSL 構成ではサポートされなくなりました。AsyncOS をアップグレードする前に、TLS バージョンを TLSv1.2 以降に変更する必要があります。

### AsyncOS for Web をアップグレードするためのベスト プラクティス

- アップグレードを開始する前に、[システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページまたは `saveconfig` コマンドを使用して、Secure Web Appliance から XML コンフィギュレーション ファイルを保存します。
- PAC ファイルやカスタマイズしたエンドユーザー通知ページなど、アプライアンスに格納されている他のファイルを保存します。
- アップグレード時には、さまざまなプロンプトで長い時間作業を中断しないでください。TCP セッションがダウンロード中にタイムアウトしてしまった場合、アップグレードが失敗する可能性があります。
- アップグレードが完了したら、XML ファイルに設定情報を保存します。

#### 関連項目

- [アプライアンス設定の保存、ロード、およびリセット, on page 132](#)

## AsyncOS およびセキュリティ サービス コンポーネントのアップグレードとアップデート

### アップグレードのダウンロードとインストール

#### 始める前に

アプライアンスのコンフィギュレーション ファイルを保存します ([アプライアンス設定の保存、ロード、およびリセット \(132 ページ\)](#) を参照)。



(注) AsyncOS を Cisco サーバーからではなくローカル サーバーから 1 回の操作でダウンロードとアップグレードする場合は、アップグレードはダウンロード中に即座に実行されます。アップグレードプロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレードプロセスを終了できます。



- (注) アップグレードの実行中、セキュア認証の証明書が FIPS 準拠でない場合は、アプライアンスがアップグレードされる最新パスのデフォルトの証明書で置き換えられます。これは、お客様がアップグレードの前にデフォルトの証明書を使用した場合にのみ起こります。

1 回の操作でダウンロードとインストールを行うか、またはバックグラウンドでダウンロードし後でインストールできます。

varstore ファイルに保存されている設定値に ASCII 以外の文字が含まれていると、アップグレードが失敗します。

## 手順

**ステップ 1** [システム管理 (System Administration)] > [システム アップグレード (System Upgrade)] を選択します。

**ステップ 2** [アップグレードオプション (Upgrade Options)] をクリックします。

アップグレード オプションとアップグレード イメージを選択します。

| 設定               | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アップグレード オプションの選択 | <ul style="list-style-type: none"> <li>• [ダウンロードとインストール (Download and install)] : 1 回の操作でアップグレードをダウンロードしてインストールします。<br/>すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。</li> <li>• [ダウンロードのみ (Download only)] : アップグレードインストーラをダウンロードしますが、インストールは行いません。<br/>すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。インストーラはサービスを中断することなく、バックグラウンドでダウンロードします。<br/>ダウンロードが完了すると、[インストール (Install)] ボタンが表示されます。このボタンをクリックして、ダウンロードしたアップグレードをインストールします。</li> </ul> |
|                  | [アップグレード サーバーで使用可能なアップグレード イメージ ファイルのリスト (List of available upgrade images files at upgrade server)] から、ダウンロードするアップグレード イメージを選択するか、ダウンロードしてインストールしたアップグレード イメージを選択します。                                                                                                                                                                                                                                                                               |



| 設定         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アップグレードの準備 | <ul style="list-style-type: none"> <li>現在の設定のバックアップコピーをアプライアンス上の <b>configuration</b> ディレクトリに保存するには、[アップグレードする前に、現在の設定を configuration ディレクトリに保存 (Save the current configuration to the configuration directory before upgrading)] をオンにします。</li> <li>[現在の設定を保存 (Save current configuration)] オプションがオンになっている場合、[設定ファイル内のパスワードを隠す (Mask passwords in the configuration file)] をオンにしてバックアップコピー内の現在のすべての構成パスワードをマスクすることができます。ただし、パスワードがマスクされた構成ファイルは、[設定をロード (Load Configuration)] コマンドでも、CLI <b>loadconfig</b> コマンドでもロードすることができません。</li> </ul> <p>FIPS モードが有効にされている場合、[設定ファイル内のパスワードを暗号化する (Encrypt passphrases in the Configuration Files)] をオンにすることができます。これらのファイルは、リロードすることができます。</p> <ul style="list-style-type: none"> <li>[現在の設定を保存 (Save current configuration)] オプションがオンになっている場合、[ファイルをメールで送信 (Email file to)] フィールドに 1 つ以上の電子メールアドレスを入力できます。入力した各アドレスに、バックアップ設定ファイルのコピーが電子メールで送信されます。カンマで複数のアドレスを区切ります。</li> </ul> |

**ステップ 3** [続行 (Proceed)] をクリックします。

インストール中の場合、次に従います。

- プロセス中のプロンプトに応答できるようにしてください。
- 完了を求めるプロンプトで、[今すぐ再起動 (Reboot Now)] をクリックします。
- 約 10 分後、アプライアンスにアクセスしてログインします。

アップグレードの問題を修正するためにアプライアンスの電源を再投入する必要があると思われる場合は、再起動後 20 分以上が経過してから再投入してください。

## バックグラウンドダウンロードのキャンセルまたは削除ステータスの表示

### 手順

**ステップ 1** [システム管理 (System Administration)] > [システム アップグレード (System Upgrade)] を選択します。

**ステップ 2** [アップグレードオプション (Upgrade Options)] をクリックします。

**ステップ 3** 次のオプションを選択します。

| 目的                 | 操作手順                                                                                                    |
|--------------------|---------------------------------------------------------------------------------------------------------|
| ダウンロードステータスの表示     | <p>ページの中央を確認してください。</p> <p>進行中のダウンロードおよびダウンロードが完了してインストールされるのを待っているものがない場合は、ダウンロードのステータス情報は表示されません。</p> |
| ダウンロードのキャンセル       | <p>ページの中央にある、[ダウンロードをキャンセル (Cancel Download)] ボタンをクリックします。</p> <p>このオプションは、ダウンロード進行中にのみ表示されます。</p>      |
| ダウンロードされたインストーラの削除 | <p>ページの中央にある、[ファイルを削除 (Delete File)] ボタンをクリックします。</p> <p>このオプションは、インストーラがダウンロードされている場合にのみ表示されます。</p>    |

**ステップ 4** (オプション) アップグレード ログを確認します。

#### 次のタスク

#### 関連項目

- [ローカルおよびリモート アップデート サーバ \(210 ページ\)](#)

## 自動および手動によるアップデート/アップグレードのクエリー

AsyncOS は、新しい AsyncOS アップグレードを除く、すべてのセキュリティ サービス コンポーネントへの新しいアップデートがないか、定期的にアップデート サーバに問い合わせます。AsyncOS をアップグレードするには、AsyncOS が使用可能なアップグレードを問い合わせるよう、手動で要求する必要があります。AsyncOS が使用可能なセキュリティ サービス アップデートを問い合わせるよう、手動で要求することもできます。詳細については、[以前のバージョンの AsyncOS for Web への復元, on page 215](#)を参照してください。

AsyncOS がアップデートまたはアップグレードのアップデート サーバを照会する場合は、以下の手順を実行します。

1. アップデート サーバに問い合わせます。

シスコでは、アップデート サーバに以下のソースを使用できます。

- **Cisco アップデート サーバ。** 詳細については、[Cisco アップデート サーバからのアップデートとアップグレード, on page 211](#)を参照してください。
- **ローカル サーバ。** 詳細については、[ローカル サーバからのアップグレード, on page 212](#)を参照してください。

2. 入手可能なアップデートまたは AsyncOS のアップグレードバージョンを一覧表示する XML ファイルを受信します。この XML ファイルは「マニフェスト」と呼ばれます。

3. アップデートまたはアップグレードイメージ ファイルをダウンロードします。

## セキュリティ サービスのコンポーネントの手動による更新

デフォルトでは、各セキュリティ サービス コンポーネントは、Cisco アップデート サーバからデータベーステーブルに定期的にアップデートを受信します。ただし、手動でデータベーステーブルを更新できます。



**Note** 一部のアップデートは、機能に関連する GUI ページからオンデマンドで利用できます。



**Tip** アップデータ ログ ファイルのアップデート アクティビティの記録を表示してください。[システム管理 (System Administration)] > [ログ サブスクリプション (Log Subscriptions)] ページのアップデータ ログ ファイルに登録します。



**Note** 処理中のアップデートは中断できません。すべての処理中のアップデートは、新しい変更が適用される前に完了する必要があります。

## Procedure

**ステップ 1** [システム管理 (System Administration)] > [アップグレードとアップデートの設定 (Upgrade and Update Settings)] を選択します。

**ステップ 2** [更新設定を編集 (Edit Update Settings)] をクリックします。

**ステップ 3** アップデート ファイルの場所を指定します。

**ステップ 4** [セキュリティ サービス (Security Services)] タブにあるコンポーネント ページの [今すぐ更新 (Update Now)] 機能キーを使用してアップデートを開始します。たとえば、[セキュリティ サービス (Security Services)] > [Web レピュテーション フィルタ (Web Reputation Filters)] ページです。

更新プロセス中、CLI および Web アプリケーション インターフェイスは、応答が遅くなったり、使用できなくなったりする場合があります。

## ローカルおよびリモート アップデート サーバ

デフォルトでは、AsyncOS は、アップデート イメージとアップグレード イメージおよびマニフェスト XML ファイルについて、Cisco アップデート サーバに問い合わせます。ただし、アップグレード イメージ、アップデート イメージおよびマニフェスト ファイルをダウンロードする場所を選択できます。以下の理由から、イメージ ファイルまたはマニフェスト ファイルにローカル アップデート サーバを使用します。

- 同時にアップグレードするアプライアンスが複数あります。ネットワーク内の Web サーバにアップグレードイメージをダウンロードして、ネットワーク内のすべてのアプライアンスに使用できます。
- ファイアウォールの設定には、Cisco アップデート サーバのスタティック IP アドレスが必要です。Cisco アップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。詳細については、[Cisco アップデート サーバのスタティック アドレスの設定, on page 211](#)を参照してください。

**Note**

ローカル アップデート サーバはセキュリティ サービスのアップデートを自動的に受信しません。AsyncOS のアップグレードのみを受信します。AsyncOS のアップグレードにローカル アップデート サーバを使用した後は、アップデートとアップグレードの設定を変更して、再び Cisco アップデート サーバを使用するようにします。これにより、セキュリティ サービスが再び自動的にアップデートされるようになります。

## Cisco アップデート サーバからのアップデートとアップグレード

Secure Web Applianceは、Cisco アップデート サーバに直接接続して、アップグレードイメージとセキュリティ サービス アップデートをダウンロードできます。各アプライアンスは、個別にアップデートとアップグレードをダウンロードします。

### Cisco アップデート サーバのスタティック アドレスの設定

Cisco アップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。

## Procedure

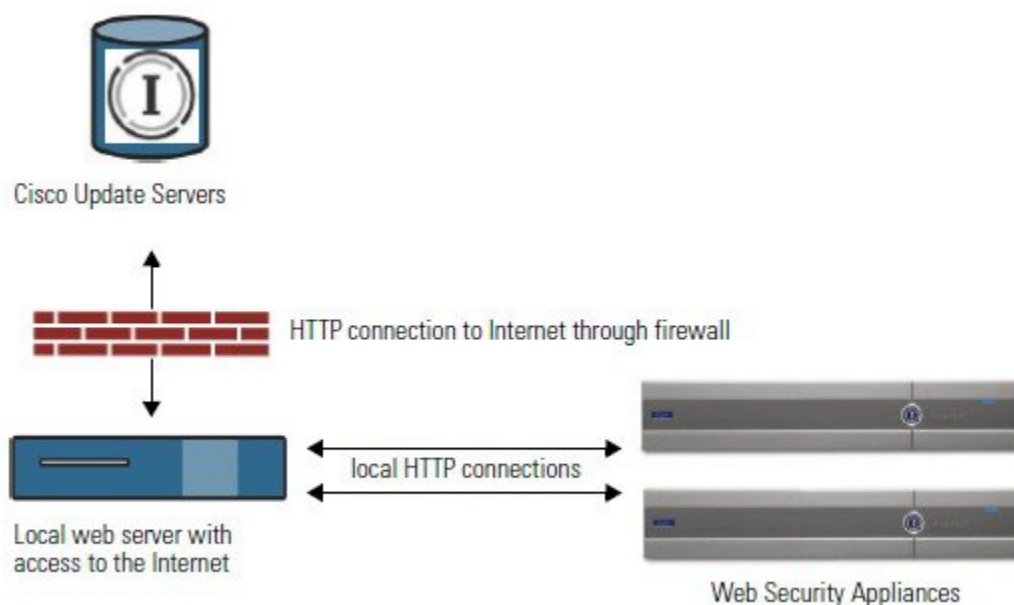
- ステップ 1** シスコ カスタマー サポートに問い合わせ、スタティック URL アドレスを取得します。
- ステップ 2** [システム管理 (System Administration)] > [アップグレードとアップデートの設定 (Upgrade and Update Settings)] ページの順に進み、[更新設定を編集 (Edit Update Settings)] をクリックします。
- ステップ 3** [アップデート設定を編集 (Edit Update Settings)] ページの [アップデートサーバ (イメージ) (Update Servers(images))] セクションで、[ローカルアップデートサーバ (Local Update Servers)] を選択し、ステップ 1 で取得したスタティック URL アドレスを入力します。
- ステップ 4** [アップデートサーバ (リスト) (Update Servers(list))] セクションで Cisco アップデート サーバが選択されていることを確認します。
- ステップ 5** 変更を送信し、保存します。

## ローカルサーバからのアップグレード

Secure Web Applianceは、Cisco アップデート サーバからアップグレードを直接取得する代わりに、ネットワーク内のサーバから AsyncOS のアップグレードをダウンロードできます。この機能を使用すると、シスコから1回だけアップグレードイメージをダウンロードして、ネットワーク内のすべての Secure Web Applianceでそれを使用することができます。

次の図に、Secure Web Applianceでローカルサーバからアップグレードイメージをダウンロードする方法を示します。

Figure 1: ローカルサーバからのアップグレード



### ローカルアップグレードサーバのハードウェアおよびソフトウェア要件

AsyncOS アップグレードファイルのダウンロードでは、Web ブラウザを備えた内部ネットワークにシステムを構築する必要があり、Cisco アップデートサーバへのインターネットアクセスが必要になります。



**Note** このアドレスへの HTTP アクセスを許可するファイアウォール設定値を設定する必要がある場合、特定の IP アドレスではなく DNS 名を使用して設定する必要があります。

AsyncOS アップグレードファイルのホスティングでは、内部ネットワーク上のサーバは、以下の機能を持つ Microsoft IIS (Internet Information Services) などの Web サーバまたは Apache のオープンソースサーバを持つ必要があります。

- 24 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
- ディレクトリの参照ができること

- 匿名（認証なし）または基本（「簡易」）認証用に設定されている
- 各 AsyncOS アップデート イメージ用に最低 350 MB 以上の空きディスク領域が存在すること

## ローカル サーバーからのアップグレードの設定



### Note

アップグレードの完了後にセキュリティ サービス コンポーネントが引き続き自動更新されるように、アップデートとアップグレードの設定を変更して、Cisco アップデート サーバー（ダイナミックまたはスタティック アドレスを使用）を使用することを推奨します。

## Procedure

**ステップ 1** アップグレード ファイルを取得および供給するようにローカル サーバーを設定します。

**ステップ 2** アップグレード zip ファイルをダウンロードします。

ローカル サーバー上のブラウザを使用して、[http://updates.ironport.com/fetch\\_manifest.html](http://updates.ironport.com/fetch_manifest.html) にアクセスしてアップグレード イメージの zip ファイルをダウンロードします。イメージをダウンロードするには、シリアル番号（物理アプライアンス用）または VLN（仮想アプライアンス用）およびアプライアンスのバージョン番号を入力します。利用可能なアップグレードのリストが表示されます。ダウンロードするアップグレード バージョンをクリックします。

**ステップ 3** ディレクトリ構造を変更せずにローカル サーバーのルート ディレクトリにある ZIP ファイルを解凍します。

**ステップ 4** [システム管理 (System Administration)] > [アップグレードとアップデートの設定 (Upgrade and Update Settings)] ページまたは **updateconfig** コマンドを使用して、ローカル サーバーを使用するようにアプライアンスを設定します。

**ステップ 5** [システム管理 (System Administration)] > [システム アップグレード (System Upgrade)] ページで、[使用可能なアップグレード (Available Upgrades)] をクリックするか、**upgrade** コマンドを実行します。

## ローカルとリモートにおけるアップグレード方法の相違

以下の相違点は、Cisco アップデート サーバーからではなく、ローカルサーバーから AsyncOS をアップグレードする場合に該当します。

- ダウンロード中に、アップグレードによるインストールがすぐに実行されます。
- アップグレード プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Control を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

## アップグレードおよびサービス アップデートの設定

Secure Web Applianceがセキュリティ サービス アップデートや AsyncOS for Web のアップグレードをダウンロードする方法を設定できます。たとえば、ファイルをダウンロードするときに使用するネットワーク インターフェイスを選択したり、アップデート間隔を設定したり、自動アップデートをディセーブルにしたりできます。

### Procedure

**ステップ 1** [システム管理 (System Administration)] > [アップグレードとアップデートの設定 (Upgrade and Update Settings)] を選択します。

**ステップ 2** [更新設定を編集 (Edit Update Settings)] をクリックします。

**ステップ 3** 以下の情報を参考にして、設定値を設定します。

| 設定                                         | 説明                                                                                                                                                                                                                                                                   |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 自動更新                                       | セキュリティ コンポーネントの自動アップデートをイネーブルにするかどうかを選択します。自動更新を選択する場合、時間間隔を入力します。デフォルトはイネーブルで、更新間隔は 5 分です。                                                                                                                                                                          |
| アップグレードの通知 (Upgrade Notifications)         | AsyncOS への新規のアップグレードが入手可能である場合に、Web インターフェイスの上部に通知を表示するかどうかを選択します。アプライアンスは、管理者に対してのみこの通知を表示します。<br><br>詳細については、 <a href="#">AsyncOS for Web のアップグレードとアップデート, on page 206</a> を参照してください。                                                                              |
| アップデートサーバ (リスト) (Update Servers (list))    | 利用可能なアップグレードとアップデートのリスト (マニフェスト XML ファイル) を、Cisco アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。<br><br>ローカルアップデートサーバを選択した場合、サーバのファイル名およびポート番号を含む、リストのマニフェスト XML ファイルの完全なパスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合は、有効なユーザ名とパスフレーズも入力できます。 |
| アップデートサーバ (イメージ) (Update Servers (images)) | アップグレードイメージやアップデートイメージを、Cisco アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。<br><br>ローカルアップデートサーバを選択した場合は、サーバのベース URL とポート番号を入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合は、有効なユーザ名とパスフレーズも入力できます。                                                |
| 着信サービス一覧 (Routing Table)                   | アップデート サーバに接続するときに、どのネットワーク インターフェイスのルーティング テーブルを使用するかを選択します。                                                                                                                                                                                                        |

| 設定                              | 説明                                                             |
|---------------------------------|----------------------------------------------------------------|
| プロキシ サーバ (Proxy Server) (オプション) | アップストリーム プロキシ サーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパズフレーズをここに入力します。 |

**ステップ 4** 変更を送信し、保存します。

### What to do next

#### 関連項目

- ローカルおよびリモート アップデート サーバ, on page 210
- 自動および手動によるアップデート/アップグレードのクエリー, on page 209
- AsyncOS およびセキュリティ サービス コンポーネントのアップグレードとアップデート, on page 206

## 以前のバージョンの AsyncOS for Web への復元

Web 用 AsyncOS には、緊急時に Web 用オペレーティング システム AsyncOS を以前の認定済みのビルドに戻す機能があります。



**Note** バージョン 7.5 よりも前の Web 用 AsyncOS のバージョンには戻せません。

## 仮想アプライアンスの AsyncOS を復元した場合のライセンスへの影響

AsyncOS 8.0 に復元した場合、アプライアンスがセキュリティ機能なしで Web トランザクションを処理する 180 日の猶予期間はありません。ライセンスの有効期限は影響を受けません。

## 復元プロセスでのコンフィギュレーション ファイルの使用

バージョン 7.5 で有効であり、それ以降のバージョンにアップグレードする場合、アップグレードプロセスは Secure Web Appliance のファイルに現在のシステム設定を自動的に保存します (ただし、バックアップとして、コンフィギュレーション ファイルをローカル マシンに手動で保存することを推奨します)。これによって、以前のバージョンに復元した後、AsyncOS for Web が以前のリリースに関連するコンフィギュレーション ファイルをロードできます。ただし、復元を実行すると、管理インターフェイスに現在のネットワーク設定を使用します。

## SMA によって管理されるアプライアンスの AsyncOS の復元

Secure Web Appliance から Web 用 AsyncOS に復元することができます。ただし Secure Web Appliance がセキュリティ管理アプライアンスで管理されている場合は、以下のルールとガイドラインを考慮してください。



- 中央集中型レポーティングを Secure Web Appliance でイネーブルにすると、Web 用 AsyncOS は復帰を開始する前にセキュリティ管理アプライアンスへのレポートデータの転送を終了します。セキュリティ管理アプライアンスへのファイルの転送に 40 秒以上かかる場合は、Web 用 AsyncOS がファイルの転送をこのまま待機するように促すか、すべてのファイルを転送せずに復帰を続けます。
- 復元後、適切なプライマリ構成に Secure Web Appliance を関連付ける必要があります。それ以外の場合、セキュリティ管理アプライアンスから Secure Web Appliance に設定をプッシュすると失敗する可能性があります。

## 以前のバージョンへの Web 用の AsyncOS の復元



### Caution

Secure Web Appliance のオペレーティング システムの復元は非常に破壊的な操作であり、すべての設定ログとデータベースが削除されます。さらに、アプライアンスが再設定されるまで、復元によって Web トラフィック処理が中断されます。初期の Secure Web Appliance 設定に応じて、この操作がネットワークの設定を破壊する場合があります。このような場合、復元の実行後にアプライアンスへの物理的なローカル アクセスが必要になります。



### Caution

Cisco Secure Web Appliance のオペレーティングシステムをスマートライセンスが有効になっている以前のバージョンに復元する場合、スマートライセンスの設定は保持されません。以前の AsyncOS バージョンに正常に復元したら、スマートライセンスを有効にして CSSM ポータルに登録する必要があります。スマートソフトウェア ライセンシングをアクティブ化したときに [特定/永久ライセンスの予約 (Specific/Permanent License Reservation)] オプションを選択した場合は、操作の復元の前にアプライアンスで使用されているライセンスを解放し、CSSM ポータルからアプライアンスを登録解除することをお勧めします。復元操作の前にライセンスを解放しなかった場合、またはアプライアンスを登録解除しなかった場合は、シスコサポートに連絡してサポートを受けることができます。



### Note

URL カテゴリ セットのアップデートが利用可能な場合は、AsyncOS の復元後にそれらが適用されます。

### Before you begin

- Cisco Quality Assurance に問い合わせ、目的とする復元が実行可能かどうかを確認してください。（BS：これは、元のトピックの「使用可能なバージョン」セクションの要約です。これが正確かどうか質問済みです。）
- Secure Web Appliance から別のマシンに以下の情報をバックアップします。
  - システム コンフィギュレーション ファイル（パスフレーズをマスクしない状態）。
  - 保持するログ ファイル。

- 保持するレポート。
- アプライアンスに保存されるカスタマイズされたエンド ユーザー通知ページ。
- アプライアンス上に格納されている PAC ファイル。

## Procedure

**ステップ 1** バージョンを戻すアプライアンスの CLI にログインします。

### Note

次のステップで `revert` コマンドの実行するときに、いくつかの警告プロンプトが発行されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元に向けた準備手順が完了するまで、復元プロセスを開始しないでください。

**ステップ 2** `revert` コマンドを入力します。

**ステップ 3** 復元で続行するアプライアンスを 2 回確認します。

**ステップ 4** 戻る利用可能なバージョンの 1 つを選択します。

アプライアンスが 2 回リブートします。

### Note

復元プロセスは時間のかかる処理です。復元が完了して、アプライアンスへのコンソールアクセスが再び利用可能になるまでには、15 ～ 20 分かかります。

アプライアンスは、選択された Web バージョンの AsyncOS を使用して稼働します。Web ブラウザから Web インターフェイスにアクセスできます。

## SNMP を使用したシステムの状態のモニタリング

AsyncOS オペレーティング システムは、SNMP（シンプル ネットワーク管理プロトコル）を使用したシステム ステータスのモニタリングをサポートしています。（SNMP の詳細については、RFC 1065、1066、および 1067 を参照してください）。

以下の点に注意してください。

- SNMP は、デフォルトで**オフ**になります。
- SNMP SET 動作（コンフィギュレーション）は実装されません。
- AsyncOS は SNMPv1、v2、および v3 をサポートしています。SNMPv3 の詳細については、RFC 2571-2575 を参照してください。
- SNMPv3 をイネーブルにする場合、メッセージ認証と暗号化は必須です。認証のパスフレーズと暗号は異なっていなければなりません。暗号化アルゴリズムには AES（推奨）または DES を指定できます。認証アルゴリズムには SHA-1（推奨）または MD5 を指定でき

ます。次に `snmpconfig` コマンドを実行するときは、コマンドにこのパスフレーズが「記憶」されています。

- 15.0 より前の AsyncOS リリースの場合：

SNMPv3 ユーザー名は `v3get` です。

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- AsyncOS リリース 15.0 以降の場合：

デフォルトの SNMPv3 ユーザー名は `v3get` です。管理者は、他のユーザー名を選択できます。

```
> snmpwalk -v 3 -l AuthNoPriv -u <username> -a MD5 serv.example.com
```

- SNMPv1 または SNMPv2 のみを使用する場合は、コミュニティ スtring を設定する必要があります。コミュニティ スtring は、`public` にデフォルト設定されません。
- SNMPv1 および SNMPv2 の場合、どのネットワークからの SNMP GET 要求を受け入れるかを指定する必要があります。
- トラップを使用するには、SNMP マネージャ（AsyncOS には含まれていません）が実行中であり、その IP アドレスがトラップ ターゲットとして入力されている必要があります（ホスト名を使用できますが、その場合、トラップは DNS が動作しているときに限り機能します）。

## MIB ファイル

MIB ファイルは

<http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html> から入手できます。

各 MIB ファイルの最新バージョンを使用します。

以下の複数の MIB ファイルがあります。

- `syncoswebsecurityappliance-mib.txt`：Secure Web Appliance 用のエンタープライズ MIB の SNMPv2 互換の説明。
- `ASYN COS-MAIL-MIB.txt`：電子メールセキュリティ アプライアンス用のエンタープライズ MIB の SNMPv2 互換の説明。
- `IRONPORT-SMI.txt`：この「管理情報構造」ファイルは、`syncoswebsecurityappliance-mib` の役割を定義します。

このリリースには、RFC 1213 および 1907 に規定されている MIB-II の読み取り専用のサブセットが実装されています。

SNMP を使用してアプライアンスで CPU 使用率をモニターリングする方法については、<https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.html> を参照してください。

## SNMP モニターリングのイネーブル化と設定

アプライアンスのシステム ステータス情報を収集するように SNMP を設定するには、コマンドラインインターフェイス (CLI) で `snmpconfig` コマンドを使用します。インターフェイスの値を選択し、設定し終わると、アプライアンスは SNMPv3 GET 要求に応答します。

SNMP モニターリングを使用する場合、以下の点に注意してください。

- これらのバージョン 3 要求には、一致するパスフレーズが含まれている必要があります。
- デフォルトでは、バージョン 1 および 2 要求は拒否されます。
- イネーブルにする場合は、バージョン 1 および 2 要求に一致するコミュニティストリングが含まれている必要があります。

## ハードウェア オブジェクト

Intelligent Platform Management Interface Specification (IPMI) 準拠のハードウェア センサーによって、温度、ファン速度、電源モジュール ステータスなどの情報が報告されます。

モニターリング可能なハードウェア関連のオブジェクト（ファンの数や動作温度範囲など）を決定するには、アプライアンス モデルのハードウェア ガイドを参照してください。

### 関連項目

- [ドキュメント セット, on page 805](#)

## SNMP トラップ

SNMP には、1 つまたは複数の条件が合致したときにトラップ（または通知）を送信して管理アプリケーションに知らせる機能が備わっています。トラップとは、トラップを送信するシステムのコンポーネントに関するデータを含むネットワーク パケットです。トラップは、SNMP エージェント（この場合は Cisco Secure Web Appliance）で、ある条件が満たされた場合に生成されます。条件が満たされると、SNMP エージェントは SNMP パケットを形成し、SNMP 管理コンソール ソフトウェアが稼働するホストに送信します。

インターフェイスに対して SNMP をイネーブルにするときに、SNMP トラップを設定（特定のトラップをイネーブル化またはディセーブル化）できます。

複数のトラップ ターゲットの指定方法：トラップ ターゲットの入力を求められたときに、カンマで区切った IP アドレスを 10 個まで入力できます。

### 関連項目

- [SNMP の connectivityFailure トラップについて , on page 219](#)

## SNMP の connectivityFailure トラップについて

connectivityFailure トラップは、インターネットへのアプライアンスの接続をモニターするために使用されます。これは、5〜7 秒ごとに 1 つの外部サーバーに接続して HTTP GET 要求を送信する試みにより実行されます。デフォルトでは、モニターされる URL はポート 80 上の `downloads.ironport.com` です。

モニターする URL またはポートを変更するには、snmpconfig コマンドを実行し、connectivityFailure トラップをイネーブルにします（すでにイネーブルになっている場合も実行します）。URL を変更するプロンプトが表示されます。



**Tip** connectivityFailure トラップをシミュレートするために、dnsconfig CLI コマンドを使用して、未使用の DNS サーバーを入力することができます。downloads.ironport.com の検索は失敗し、5〜7秒ごとにトラップが送信されます。テストが完了したら、DNS サーバを使用中のサーバーに戻してください。

## CLI の例 : snmpconfig

```
Do you want to enable SNMP? [Y]>

Please choose an IP interface for SNMP requests.
1. Management (10.10.192.43/24 on Management: wsa033.cs1)
[1]>

Which port shall the SNMP daemon listen on?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]>

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]>

Enter the SNMPv3 username or press return to leave it unchanged.
[v3get]>

.
.
.
```

## Web トラフィック タップ (Web Traffic Tap)

開始する前に : Web トラフィック タップ機能を有効にすると、アプライアンスがタップインターフェイスにメッセージをコピーするための追加の CPU サイクルとメモリが必要になり、アプライアンスのトランザクション処理容量（1 秒あたりのリクエスト）が低下することになります。



(注) Web トラフィック タップ機能によるパフォーマンスの影響を低減するには、適切な Web トラフィック タップ ポリシーを設定し、タップされるトラフィックの量を減らします。

この機能は、Amazon Web Services (AWS) ではサポートされません。

Web トラフィックタップ機能により、アプライアンスをパススルーする HTTP および HTTPS の Web トラフィックがタップ可能になり、リアルタイムデータトラフィックとともに Secure Web Appliance インターフェイスにインラインでコピーすることができます。タップされたトラフィックデータを送信する Secure Web Appliance インターフェイスを選択することができます。タップされたトラフィックに HTTPS のデータが含まれている場合、タップインターフェイスに送信する前に、アプライアンスによって復号ポリシーに基づいて復号されます。[復号ポリシー \(345 ページ\)](#) を参照してください。

選択されたタップインターフェイスは、分析、調査、およびアーカイブのため、外部のセキュリティデバイスに直接接続する必要があります。または、専用の VLAN 上の L2 スイッチに接続します。



- (注) タップインターフェイスにミラーリングされたトラフィックは、イーサネット層経由でブロードキャストされ、IP ルーティングに対応していません。したがって、L2 スイッチに接続する場合は、専用の VLAN が必要です。

この機能では、Web トラフィック タップ ポリシーを設定することもできます。お客様によって定義されたこれらのポリシー フィルタに基づき、アプライアンスは外部のセキュリティデバイスで使用可能な Web トラフィックをミラーリングします。Web トラフィック タップ機能により、HTTPS トラフィックへの可視性が実現します。

タッピングという用語は、直接接続されたクライアントとサーバー間で発生した場合、完全な TCP (Transmission Control Protocol) ストリームの再構築を指します。

仮想 Secure Web Appliance では、Web トラフィックタップ機能がサポートされます。



- (注) SSL トラフィックの検査アクションは、企業ポリシーのガイドランおよび/または国の法令に従う必要が生じる場合があります。シスコはどのような法的義務も負わず、そのような法的要件またはポリシー要件に従って Secure Web Appliance の Web トラフィックタップ機能を使用することには、使用者が単独で責任を負います。

アプライアンスを使用して Web トラフィックにタップするには、次の手順を実行する必要があります。

1. Web トラフィック タップ機能の有効化
2. Web トラフィック タップ ポリシーの設定

#### 関連項目

- [Web トラフィック タップの有効化 \(222 ページ\)](#)
- [Web トラフィック タップ ポリシーの設定 \(223 ページ\)](#)

## Web トラフィック タップの有効化

### 始める前に

Web トラフィック タップ機能はデフォルトでは無効になっています。Web トラフィック タップ ポリシーを定義する前に、[Web セキュリティ マネージャ (Web Security Manager)] > [Web トラフィック タップ ポリシー (Web Traffic Tap Policies)] を使用して、Web トラフィック タップ機能を有効にする必要があります。



(注) HTTPS トランザクションをタップするには、復号ポリシーを定義する必要があります。[復号ポリシー \(345 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [ネットワーク (Network)] > [Web トラフィック タップ (Web Traffic Tap)] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** [Web トラフィック タップの編集 (Edit Web Traffic Tap)] ページで、[有効 (Enable)] チェックボックスをオンにし、Web トラフィック タップ機能を有効にします。

#### (注)

Web トラフィック タップ機能を無効にするには、[有効化 (Enable)] チェックボックスをオフにします。Web トラフィック タップ機能を無効にすると、Web トラフィック タップ ポリシーの表示や編集ができません。ポリシーの表示や編集を行うには、機能を再び有効にする必要があります。

**ステップ 4** [タップインターフェイス (Tap Interface)] ドロップダウンリストから、タップされたトラフィックデータを送信する Secure Web Appliance インターフェイスを選択します。インターフェイスのオプションは、P1、P2、T1、T2 です。インターフェイスについての詳細は、[アプライアンスの接続 \(18 ページ\)](#) を参照してください。

#### (注)

選択されたタップインターフェイスは、分析、調査、およびアーカイブのため、外部のセキュリティデバイスに直接接続する必要があります。または、専用の VLAN 上の L2 スイッチに接続します。選択されたタップインターフェイスは接続され、ステータスがアクティブである必要があります。そうでない場合は、タップされたトラフィックのミラーリングは失敗します。

**ステップ 5** [送信 (Submit)] をクリックし、変更をコミットします。

## Web トラフィック タップ ポリシーの設定

### 手順

**ステップ 1** [Web セキュリティ マネージャ (Web Security Manager) ] > [Web トラフィック タップ ポリシー (Web Traffic Tap Policies) ] を選択します。

**ステップ 2** [ポリシーを追加 (Add Policy) ] をクリックします。

[ポリシーの作成 \(369 ページ\)](#) の手順に従い、新しい Web トラフィック タップ ポリシーを追加します。

(注)

タッピング設定なしのグローバル トラフィック タップ ポリシーは、[Web トラフィック タップ ポリシー (Web Traffic Tap Policies) ] ページで、デフォルトで使用できます ([Web セキュリティ マネージャ (Web Security Manager) ] > [Web トラフィック タップ ポリシー (Web Traffic Tap Policies) ]) 。

**ステップ 3** [ポリシー メンバの定義 (Policy Member Definition) ] 領域の [詳細設定 (Advanced) ] セクションを展開して、以下の Web トラフィック タップ用の追加のグループ メンバーシップを追加します。

- プロトコル : HTTP または HTTPS プロトコルのいずれか、またはその両方を選択して、Web トラフィック タップ ポリシーを作成します。

(注)

HTTPS トラフィックをタップするには、一致する複合ポリシーを定義する必要があります ([Web セキュリティ マネージャ (Web Security Manager) ] > [複合化ポリシー (Decryption Policies) ]) 。

Web トラフィック タップ ポリシーは、ネイティブの FTP と SOCKS プロトコルをサポートしていません。

- サブネット (Subnets)
- URL カテゴリ : 必要に応じて、URL フィルタリング カテゴリ用に [タップする (Tap) ] または [タップしない (No Tap) ] を設定します。未分類の URL でトラフィック タップを設定するには、未分類の URL のドロップダウンリストから [タップする (Tap) ] を選択して、[送信 (Submit (送信) ) ] をクリックします。
- ユーザー エージェント (User Agents)

追加のグループ メンバーシップの条件の定義について詳細を確認するには、[ポリシーの作成 \(369 ページ\)](#) を参照してください。

(注)

タップするトラフィックは、Web トラフィック タップ ポリシーで定義されたすべてのフィルタ条件を満たしている必要があります。

[Web セキュリティ マネージャ (Web Security Manager) ] > [Web トラフィック タップ ポリシー (Web Traffic Tap Policies) ] を使用して、URL フィルタリングの表から URL カテゴリを追加することもできます。

(注)



すでに [詳細設定 (Advanced)] セクションに URL のカテゴリが追加されている場合、URL フィルタリングの表ではそれらのカテゴリのみが表示されます ([Web セキュリティ マネージャ (Web Security Manager)] > [Web トラフィック タップ ポリシー (Web Traffic Tap Policies)])。

Web トラフィック タップ ポリシーの順序について詳しくは、[ポリシーの順序 \(368 ページ\)](#) を参照してください。

## HTTP 2.0 プロトコルの設定

Cisco AsyncOS 14.0 バージョンは、TLS を介した Web リクエストおよび応答向けに HTTP 2.0 をサポートします。

TLS を介した Web リクエストおよび応答用の HTTP 2.0。HTTP 2.0 サポートには、TLS 1.2 以降のバージョンでのみ使用可能な TLS ALPN ベースのネゴシエーションが必要です。

このリリースでは、HTTPS 2.0 は次の機能ではサポートされていません。

- Web トラフィック タップ (Web Traffic Tap)
- 外部 DLP (External DLP)
- 全体の帯域幅とアプリケーションの帯域幅



(注) デフォルトでは HTTP 2.0 機能が無効になっているため、CLI コマンド `HTTP 2` を使用して機能を有効にします。

HTTP 2.0 機能では、次をサポートします。

- 最大 4,096 の同時セッションと 128 の同時ストリーム
- ALPN にあるすべての HTTP プロトコルとアドバタイズされた ALPN にある最大 7 つのプロトコル。
- 最大サイズが 16k のヘッダー。



(注) 2.0 の明示的なプロキシに対応する `CONNECT` も HTTP 1.1 で開始します

HTTP 2.0 設定を有効または無効にするために、新しい CLI コマンド `HTTP2` が導入されました。「[Secure Web Appliance CLI コマンド](#)」を参照してください。

アプライアンスの Web ユーザインターフェイスを使用して HTTP 2.0 を有効または無効にしたり、ドメインを制限したりすることはできません。HTTP 2.0 設定は、Cisco Secure Email and Web Manager (シスコのコンテンツセキュリティ管理アプライアンス) ではサポートされていません。

- URL が HTTP 2 例外リストとパススルー URL カテゴリの両方で失敗した場合、HTTP 2 がパススルーよりも優先されます。
- ALPN ログは、パススルー URL カテゴリに対して一貫性がありません。

## Cisco クラウド Web セキュリティ プロキシへのアプライアンスの接続

この章で説明する内容は、次のとおりです。

- [クラウド コネクタ モードで機能を設定および使用する方法](#) (225 ページ)
- [クラウド コネクタ モードでの展開](#) (226 ページ)
- [クラウド コネクタの設定](#) (226 ページ)
- [クラウドのディレクトリ グループの使用による Web アクセスの制御](#) (230 ページ)
- [クラウド プロキシ サーバーのバイパス](#) (230 ページ)
- [クラウド コネクタ モードでの FTP および HTTPS の部分的サポート](#) (231 ページ)
- [セキュア データの漏洩防止](#) (231 ページ)
- [グループ名、ユーザー名、IP アドレスの表示](#) (232 ページ)
- [クラウド コネクタ ログへの登録](#) (232 ページ)
- [クラウド Web セキュリティ コネクタの使用による識別プロファイルと認証](#) (232 ページ)

### クラウド コネクタ モードで機能を設定および使用する方法

クラウド コネクタのサブセットに含まれる機能の使用方法は、注記した点を除き、標準モードと同じです。詳細については、[操作モードの比較, on page 12](#)を参照してください。

このトピックは本書のさまざまな個所と関連し、標準モードとクラウド Web セキュリティ コネクタモードの両方に共通する Secure Web Applianceの主要機能の一部は、それらの個所に記載されています。クラウドへのディレクトリ グループの送信に関する情報およびクラウド コネクタの設定情報を除き、関連情報は本書の他の個所に記載されています。

このトピックには、標準モードでは適用できないクラウド Web セキュリティコネクタの設定に関する情報が含まれています。

本書には、Cisco クラウド Web セキュリティ製品に関する情報は記載されていません。Cisco クラウド Web セキュリティのドキュメントは、<http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html> [英語] から入手できます。

## クラウドコネクタ モードでの展開

アプライアンスの初期設定時に、クラウドコネクタモードと標準モードのどちらで展開するかを選択します。必要なライセンスを所有している場合は、現在展開されているアプライアンスでシステムセットアップウィザードを標準モードで実行し、これをクラウドコネクタモードで再展開することもできます。システムセットアップウィザードを実行すると、既存の設定は上書きされ、既存のすべてのデータが削除されます。

アプライアンスの展開は標準モードとクラウドセキュリティモードのどちらにおいても同様ですが、オンサイト Web プロキシサービスおよびレイヤ 4 トラフィック モニター サービスは、クラウド Web セキュリティ コネクタ モードでは使用できません。

クラウド Web セキュリティ コネクタは、明示的な転送モードまたは透過モードで展開できます。

初期設定後にクラウドコネクタの設定を変更するには、[ネットワーク (Network)] > [クラウドコネクタ (Cloud Connector)] を選択します。

### 関連項目

- [接続、インストール、設定, on page 11](#)

## クラウドコネクタの設定

### Before you begin

「[仮想アプライアンスでの Web インターフェイスへのアクセスの有効化](#)」を参照してください。

### Procedure

**ステップ 1** Secure Web Appliance の Web インターフェイスにアクセスします。

インターネットブラウザに Secure Web Appliance の IPv4 アドレスを入力します。

初めてシステムセットアップウィザードを実行するときは、以下のデフォルトの IPv4 アドレスを使用します。

`https://192.168.42.42:8443`

または

`http://192.168.42.42:8080`

ここで、192.168.42.42 はデフォルトの IPv4 アドレス、8080 は、HTTP のデフォルトの管理ポート設定、8443 は HTTPS のデフォルトの管理ポートです。

**ステップ 2** [システム管理 (System Administration)] > [システムセットアップウィザード (System Setup Wizard)] を選択します。

**ステップ 3** ライセンス契約の条項に同意します。

**ステップ 4** [セットアップの開始 (Begin Setup)] をクリックします。

**ステップ 5** システム設定項目を設定します。

| 設定                                             | 説明                                                                                        |
|------------------------------------------------|-------------------------------------------------------------------------------------------|
| デフォルトシステム<br>ホスト名 (Default<br>System Hostname) | Secure Web Applianceの完全修飾ホスト名。                                                            |
| DNS サーバー (DNS<br>Server(s))                    | ドメイン名サービス ルックアップ用のインターネット ルート DNS サーバー。<br><a href="#">DNS の設定, on page 71</a> も参照してください。 |
| NTP サーバー (NTP<br>Server)                       | システム クロックと同期させるサーバー。デフォルトは time.ironport.com です。                                          |
| タイム ゾーン                                        | アプライアンス上にタイム ゾーンを設定して、メッセージヘッダーおよびログ<br>ファイルのタイムスタンプが正確に表示されるようにします。                      |

**ステップ 6** アプライアンス モードの [クラウド Web セキュリティ コネクタ (Cloud Web Security Connector)] を選択  
します。

**ステップ 7** クラウドコネクタの設定項目を設定します。

| 設定                                                                               | 説明                                                                                                                                                                                          |
|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| クラウド Web セキュ<br>リティプロキシサー<br>バー (Cloud Web<br>Security Proxy<br>Servers)         | クラウドプロキシサーバー (CPS) のアドレス (例 : proxy1743.scansafe.net) 。                                                                                                                                     |
| 失敗のハンドリング<br>(Failure Handling)                                                  | AsyncOS がクラウド Web セキュリティ プロキシへの接続に失敗した場合、イン<br>ターネットに [直接接続 (Connect directly)] するか、[要求をドロップ (Drop<br>requests)] します。                                                                       |
| Cloud Web Security 認<br>証スキーム (Cloud<br>Web Security<br>Authorization<br>Scheme) | トランザクションを認証する方式 :<br><ul style="list-style-type: none"> <li>Secure Web Applianceの一般向け IPv4 アドレス</li> <li>各トランザクションに含まれている認証キー。Cisco Cloud Web Security Portal<br/>内で認証キーを生成できます。</li> </ul> |

**ステップ 8** ネットワーク インターフェイスおよび配線を設定します。

| 設定                            | 説明                                                                                                                                         |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| イーサネット ポート<br>(Ethernet Port) | M1 インターフェイスを管理トラフィック専用として設定する場合は、データトラフィック用の P1 インターフェイスを設定する必要があります。ただし、管理トラフィックとデータトラフィックの両方を M1 インターフェイスとして使用する場合でも、P1 インターフェイスを設定できます。 |
| IP アドレス (IP Address)          | Secure Web Appliance を管理するために使用する IPv4 アドレス。                                                                                               |
| ネットワーク マスク<br>(Network Mask)  | このネットワーク インターフェイス上の Secure Web Appliance を管理する際に使用するネットワークマスク。                                                                             |
| ホスト名<br>(Hostname)            | このネットワーク インターフェイス上の Secure Web Appliance を管理する際に使用するホスト名。                                                                                  |

### ステップ 9 管理およびデータ トラフィックのルートを設定します。

| 設定                             | 説明                                                                                            |
|--------------------------------|-----------------------------------------------------------------------------------------------|
| デフォルト ゲートウェイ (Default Gateway) | 管理インターフェイスやデータ インターフェイスを通過するトラフィックに使用するデフォルトのゲートウェイの IPv4 アドレス。                               |
| 名前 (Name)                      | スタティック ルートの識別に使用する名前。                                                                         |
| 内部ネットワーク<br>(Internal Network) | このルートのネットワーク上の宛先の IPv4 アドレス。                                                                  |
| 内部ゲートウェイ<br>(Internal Gateway) | このルートのゲートウェイの IPv4 アドレス。ルート ゲートウェイは、それが設定されている管理インターフェイスまたはデータ インターフェイスと同じサブネット上に存在する必要があります。 |

### ステップ 10 透過的接続の設定項目を設定します。

#### Note

デフォルトでは、クラウドコネクタはトランスペアレント モードで展開され、レイヤ4 スイッチまたは WCCP バージョン 2 ルータと接続する必要があります。

| 設定                                                          | 説明                                                                                                                                                                         |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| レイヤ 4 スイッチ<br>(Layer-4 Switch)<br>または<br>デバイスなし (No Device) | <ul style="list-style-type: none"> <li>Secure Web Appliance はレイヤ 4 スイッチに接続されます。</li> </ul> または <ul style="list-style-type: none"> <li>明示的な転送モードでクラウドコネクタを展開します。</li> </ul> |

| 設定                              | 説明                                                                                       |
|---------------------------------|------------------------------------------------------------------------------------------|
| WCCP v2 ルータ<br>(WCCP v2 Router) | Secure Web Applianceは WCCP バージョン 2 対応ルータに接続されます。<br>注：パスフレーズは任意であり、7 文字以内の文字を含めることができます。 |

#### ステップ 11 管理設定項目を設定します。

| 設定                                                                 | 説明                                                                                                                                                 |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 管理者パスフレーズ<br>(Administrator Passphrase)                            | Secure Web Applianceにアクセスするためのパスフレーズ。パスフレーズは 6 文字以上にする必要があります。                                                                                     |
| システム アラート<br>メールの送信先<br>(Email system alerts to)                   | アプライアンスによって送信されるアラートの宛先メールアドレス。                                                                                                                    |
| SMTP リレー ホスト経<br>由で電子メールを送信<br>(Send Email via SMTP<br>Relay Host) | (任意) AsyncOS がシステムによって生成された電子メール メッセージの送信に使用する SMTP リレー ホストのホスト名またはアドレス。<br>デフォルトの SMTP リレー ホストは、MX レコードにリストされているメールサーバーです。<br>デフォルトのポート番号は 25 です。 |
| オートサポート<br>(AutoSupport)                                           | アプライアンスは、シスコ カスタマー サポートにシステム アラートと毎週のステータス レポートを送信できます。                                                                                            |

#### ステップ 12 レビューしてインストールします。

- インストールを確認します。
- 前に戻って変更する場合は、[前へ (Previous)] をクリックします。
- 入力した情報を使って続行する場合は、[この設定をインストール (Install This Configuration)] をクリックします。

#### What to do next

##### 関連項目

- セキュア データの漏洩防止, on page 231
- ネットワーク インターフェイス, on page 35
- TCP/IP トラフィック ルートの設定, on page 55
- トランスペアレント リダイレクションの設定, on page 58
- アラートの管理, on page 183

- [SMTP リレー ホストの設定, on page 70](#)

## クラウドのディレクトリ グループの使用による Web アクセスの制御

Cisco クラウド Web セキュリティを使用して、ディレクトリ グループに基づいてアクセスを制御できます。Cisco クラウド Web セキュリティへのトラフィックがクラウドコネクタモードの Secure Web Appliance を介してルーティングされている場合、Cisco クラウド Web セキュリティは、グループベースのクラウドポリシーを適用できるように、クラウドコネクタからトランザクションと共にディレクトリグループ情報を受け取る必要があります。

### Before you begin

Secure Web Appliance の設定に認証レلمを追加します。

### Procedure

- 
- ステップ 1 [ネットワーク (Network)] > [クラウドコネクタ (Cloud Connector)] に移動します。
  - ステップ 2 [クラウドポリシーディレクトリ グループ (Cloud Policy Directory Groups)] 領域で、[グループの編集 (Edit Groups)] をクリックします。
  - ステップ 3 Cisco クラウド Web セキュリティ内で作成したクラウドポリシーの対象となる [ユーザー グループ (User Groups)] と [マシン グループ (Machine Groups)] を選択します。
  - ステップ 4 [追加 (Add)] をクリックします。
  - ステップ 5 [完了 (Done)] をクリックして、変更を確定します。
- 

### What to do next

#### 関連情報

- [認証レلم, on page 90](#)

## クラウド プロキシ サーバーのバイパス

クラウドルーティング ポリシーを使用すると、以下の特性に基づいて、Web トラフィックを Cisco クラウド Web セキュリティ プロキシにルーティングしたり、インターネットに直接ルーティングできたりします。

- 識別プロファイル
- プロキシ ポート (Proxy Port)
- Subnet
- URL カテゴリ
- ユーザー エージェント

クラウドコネクタ モードでクラウドルーティング ポリシーを作成するプロセスは、標準モードを使用してルーティング ポリシーを作成するプロセスと同じです。

#### 関連項目

- [ポリシーの作成](#), on page 369

## クラウドコネクタ モードでの FTP および HTTPS の部分的サポート

クラウドコネクタモードの Secure Web Applianceでは、FTP および HTTPS が完全にはサポートされていません。

### FTP

FTP はクラウドコネクタではサポートされません。アプライアンスがクラウドコネクタ用に設定されている場合、AsyncOS はネイティブ FTP トラフィックをドロップします。

FTP over HTTP はクラウドコネクタ モードでサポートされます。

### HTTPS

クラウドコネクタは復号をサポートしていません。復号せずに HTTPS トラフィックを渡します。

クラウドコネクタは復号をサポートしていないため、通常、AsyncOS は HTTPS トラフィックのクライアント ヘッダー情報にアクセスできません。したがって、通常、AsyncOS は暗号化されたヘッダー情報に依存するルーティング ポリシーを適用できません。これは、透過的 HTTPS トランザクションでよくあることです。たとえば、透過的 HTTPS トランザクションの場合、AsyncOS は HTTPS クライアント ヘッダー内のポート番号にアクセスできないため、ポート番号に基づいてルーティングポリシーを照合できません。この場合、AsyncOS はデフォルトのルーティング ポリシーを使用します。

明示的な HTTPS トランザクションの場合は2つの例外があります。AsyncOS は、明示的 HTTPS トランザクションの以下の情報にアクセスできます。

- URL
- 宛先ポート番号

明示的 HTTPS トランザクションの場合は、URL またはポート番号に基づいてルーティング ポリシーを照合できます。

## セキュア データの漏洩防止

[ネットワーク (Network)] > [外部 DLP サーバー (External DLP Servers)] で、クラウドコネクタを外部のデータ漏洩防止サーバーと統合できます。



## 関連項目

- [機密データの漏洩防止, on page 518](#)

## グループ名、ユーザー名、IP アドレスの表示

設定したグループ名、ユーザー名、IP アドレスを表示するには、whoami.scansafe.net にアクセスします。

## クラウド コネクタ ログへの登録

クラウド コネクタ ログには、認証されたユーザーやグループ、クラウド ヘッダー、認証キーなど、クラウド コネクタの問題のトラブルシューティングに役立つ情報が含まれています。

### Procedure

- 
- ステップ 1** [システム管理 (System Administration)] > [ログ サブスクリプション (Log Subscriptions)] に移動します。
- ステップ 2** [ログ タイプ (Log Type)] メニューから [クラウド コネクタ ログ (Cloud Connector Logs)] を選択します。
- ステップ 3** [ログ名 (Log Name)] フィールドに名前を入力します。
- ステップ 4** ログ レベルを設定します。
- ステップ 5** 変更を [実行 (Submit)] して [確定する (Commit)] します。
- 

### What to do next

## 関連項目

- [ログによるシステム アクティビティのモニター, on page 665](#)

## クラウド Web セキュリティ コネクタの使用による識別プロファイルと認証

クラウド Web セキュリティ コネクタは、基本認証および NTLM をサポートしています。また、特定の宛先に対して認証をバイパスできます。

クラウド コネクタ モードで Active Directory レルムを使用すると、トランザクション要求を特定のマシンから発信された要求として識別できます。マシン ID サービスは標準モードでは使用できません。

2 つの例外を除き、認証は Secure Web Appliance 全体で同様に機能します。標準構成であるかクラウド コネクタ 構成であるかは問いません。次に例外を示します。

- マシン ID サービスは標準モードでは使用できません。

- アプライアンスがクラウド コネクタ モードに設定されている場合、AsyncOS は Kerberos をサポートしません。



**Note** ユーザー エージェントまたは宛先 URL に基づく識別プロファイルは、HTTPS トラフィックに対応していません。

#### 関連項目

- [ポリシーの適用に対するマシンの識別, on page 233](#)
- [未認証ユーザーのゲスト アクセス, on page 234](#)
- [ポリシーの適用に対するエンドユーザーの分類, on page 265](#)
- [エンドユーザー クレデンシャルの取得の概要, on page 75](#)

## ポリシーの適用に対するマシンの識別

マシン ID サービスを有効にすると、AsyncOS は、認証済みユーザーや IP アドレスなどの識別子ではなく、トランザクション要求を実行したマシンに基づいてポリシーを適用できるようになります。AsyncOS は NetBIOS を使用してマシン ID を取得します。



**Note** マシン ID サービスは Active Directory レルムを介してのみ使用できることに注意してください。Active Directory レルムが設定されていない場合、このサービスはディセーブルになります。

### Procedure

**ステップ 1** [ネットワーク (Network)] > [マシンIDサービス (Machine ID Service)] を選択します。

**ステップ 2** [設定の有効化と編集 (Enable and Edit Settings)] をクリックします。

**ステップ 3** マシン ID の設定項目を設定します。

| 設定                                                                   | 説明                                                           |
|----------------------------------------------------------------------|--------------------------------------------------------------|
| マシン ID の NetBIOS の有効化<br>(Enable NetBIOS for Machine Identification) | マシン ID サービスをイネーブルにする場合に選択します。                                |
| レルム                                                                  | トランザクション要求を開始しているマシンの識別に使用する Active Directory レルム。           |
| 失敗のハンドリング (Failure Handling)                                         | AsyncOS がマシンを識別できない場合に、トランザクションをドロップするか、ポリシーの照合を続行するかを指定します。 |

ステップ 4 変更を [実行 (Submit)] して [確定する (Commit)] します。

## 未認証ユーザーのゲスト アクセス

クラウドコネクタモードで、未認証ユーザーにゲストアクセスを提供するように Secure Web Applianceが設定されている場合、AsyncOS は \_\_GUEST\_GROUP\_\_ グループにゲストユーザーを割り当て、その情報を Cisco クラウド Web セキュリティに送信します。未認証ユーザーにゲストアクセスを提供するには、ID を使用します。これらのゲストユーザーを制御するには、Cisco クラウド Web セキュリティ ポリシーを使用します。

### 関連項目

- [認証失敗後のゲスト アクセスの許可, on page 123](#)

## Web 要求の代行受信

この章で説明する内容は、次のとおりです。

- [Web 要求の代行受信の概要 \(234 ページ\)](#)
- [Web 要求の代行受信のためのタスク \(235 ページ\)](#)
- [Web 要求の代行受信のベストプラクティス \(236 ページ\)](#)
- [Web 要求を代行受信するための Web プロキシ オプション \(236 ページ\)](#)
- [ドメイン マップ \(252 ページ\)](#)
- [Web 要求をリダイレクトするためのクライアント オプション \(254 ページ\)](#)
- [クライアントアプリケーションによる PAC ファイルの使用 \(255 ページ\)](#)
- [FTP プロキシ サービス \(258 ページ\)](#)
- [SOCKS プロキシ サービス \(261 ページ\)](#)
- [要求の代替受信に関するトラブルシューティング \(264 ページ\)](#)

## Web 要求の代行受信の概要

Secure Web Applianceは、ネットワーク上のクライアントまたは他のデバイスから転送された要求を代行受信します。

アプライアンスは他のネットワークデバイスと連携してトラフィックを代行受信します。そのようなデバイスとして、一般的なスイッチ、トランスパアレントリダイレクションデバイス、ネットワークタップ、およびその他のプロキシサーバーまたは Secure Web Applianceなどがあげられます。

## Web 要求の代行受信のためのタスク

| 手順     | タスク                                                                                                                                                                                                                                                                                                    | 関連項目および手順へのリンク                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | ベスト プラクティスを検討します。                                                                                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• <a href="#">Web 要求の代行受信のベスト プラクティス, on page 236</a></li> </ul>                                                                                                                                                                                                                                                                                                                |
| ステップ 2 | <p>(任意) 以下のネットワーク関連のフォローアップ タスクを実行します。</p> <ul style="list-style-type: none"> <li>• アップストリーム プロキシを接続および設定する。</li> <li>• ネットワーク インターフェイス ポリシーを設定する。</li> <li>• 透過リダイレクション デバイスを設定する。</li> <li>• TCP/IP ルートを設定する。</li> <li>• VLAN の設定。</li> </ul>                                                        | <ul style="list-style-type: none"> <li>• <a href="#">アップストリーム プロキシ, on page 33</a></li> <li>• <a href="#">ネットワーク インターフェイス, on page 35</a></li> <li>• <a href="#">トランスペアレント リダイレクションの設定, on page 58</a></li> <li>• <a href="#">TCP/IP トラフィック ルートの設定, on page 55</a></li> <li>• <a href="#">VLAN の使用によるインターフェイス能力の向上, on page 66</a></li> </ul>                                                                          |
| ステップ 3 | <p>(任意) 次の Web プロキシのフォローアップ タスクを実行する。</p> <ul style="list-style-type: none"> <li>• 転送モードまたは透過モードで動作するように Web プロキシを設定する。</li> <li>• 代行受信するプロトコル タイプに追加のサービスが必要かどうかを決定。</li> <li>• IP スプーフィングの設定。</li> <li>• Web プロキシ キャッシュの管理。</li> <li>• カスタム Web 要求ヘッダーの使用。</li> <li>• 一部の要求に対してプロキシをバイパス。</li> </ul> | <ul style="list-style-type: none"> <li>• <a href="#">Web 要求を代行受信するための Web プロキシ オプション, on page 236</a></li> <li>• <a href="#">Web プロキシの設定, on page 237</a></li> <li>• <a href="#">Web 要求を代行受信するための Web プロキシ オプション, on page 236</a></li> <li>• <a href="#">Web プロキシ キャッシュ, on page 241</a></li> <li>• <a href="#">Web プロキシの IP スプーフィング, on page 244</a></li> <li>• <a href="#">Web プロキシのバイパス, on page 247</a></li> </ul> |
| ステップ 4 | <p>以下のクライアント タスクを実行します。</p> <ul style="list-style-type: none"> <li>• クライアントが Web プロキシに要求をリダイレクトする方法を決定。</li> <li>• クライアントとクライアント リソースの設定。</li> </ul>                                                                                                                                                   | <ul style="list-style-type: none"> <li>• <a href="#">Web 要求をリダイレクトするためのクライアント オプション, on page 254</a></li> <li>• <a href="#">クライアント アプリケーションによる PAC ファイルの使用, on page 255</a></li> </ul>                                                                                                                                                                                                                                 |
| ステップ 5 | (任意) FTP プロキシを有効化して設定します。                                                                                                                                                                                                                                                                              | <ul style="list-style-type: none"> <li>• <a href="#">FTP プロキシ サービス, on page 258</a></li> </ul>                                                                                                                                                                                                                                                                                                                         |

## Web 要求の代行受信のベスト プラクティス

- 必要なプロキシ サービスのみをイネーブルにします。
- Secure Web Applianceで定義されているすべての WCCP サービスに対して、同じ転送方式とリターン方式（L2またはGRE）を使用します。これによって、プロキシバイパス リストが確実に機能します。
- ユーザーが企業ネットワークの外部から PAC ファイルにアクセスできないことを確認します。これによって、モバイル ワーカーは、企業ネットワーク上にいるときは Web プロキシを使用し、それ以外の場合は Web サーバーに直接接続できます。
- 信頼できるダウンストリームプロキシまたはロードバランサからの X-Forwarded-For ヘッダーのみが Web プロキシで許可されるようにします。
- 当初は明示的な転送だけを使用していた場合でも、Web プロキシをデフォルトの透過モードのままにしておきます。透過モードでは、明示的な転送要求も許可されます。

## Web 要求を代行受信するための Web プロキシ オプション

単独では、Web プロキシは HTTP（FTP over HTTP を含む）および HTTPS を使用する Web 要求を代行受信できます。プロトコル管理を向上させるために、さらに次のプロキシモジュールを利用できます。

- **FTP プロキシ**。FTP プロキシを使用すると、（HTTP でエンコードされた FTP トラフィックだけでなく）ネイティブ FTP トラフィックを代行受信できます。
- **HTTPS プロキシ**。HTTPS プロキシは HTTPS トラフィックの復号をサポートしているので、Web プロキシは、暗号化されていない HTTPS 要求をコンテンツ分析のためにポリシーに渡すことができます。

**Note**

透過モードでは、HTTPS プロキシがイネーブルでない場合、Web プロキシは透過的にリダイレクトされたすべての HTTPS 要求をドロップします。透過的にリダイレクトされた HTTPS 要求がドロップされた場合、その要求のログ エントリは作成されません。

- **SOCKS プロキシ**。SOCKS プロキシを使用すると、SOCKS トラフィックを代行受信できます。

これらの追加のプロキシのそれぞれが機能するには、Web プロキシが必要です。Web プロキシをディセーブルにすると、これらをイネーブルにできません。

**Note**

Web プロキシはデフォルトでイネーブルになります。デフォルトでは、他のプロキシはすべてディセーブルになります。

### 関連項目

- [FTP プロキシ サービス, on page 258](#)
- [SOCKS プロキシ サービス, on page 261](#)

## Web プロキシの設定

### Before you begin

Web プロキシをイネーブルにします。

### Procedure

**ステップ 1** [セキュリティサービス (Security Services)] > [Web プロキシ (Web Proxy)] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** 必要に応じて基本的な Web プロキシ設定項目を設定します。

| プロパティ                                    | 説明                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プロキシを設定する HTTP ポート (HTTP Ports to Proxy) | Web プロキシが HTTP 接続をリッスンするポート                                                                                                                                                                                                                                                                                               |
| キャッシング (Caching)                         | Web プロキシによるキャッシングをイネーブルにするかディセーブルにするかを指定します。<br><br>Web プロキシは、パフォーマンスを向上させるためにデータをキャッシュします。                                                                                                                                                                                                                               |
| プロキシモード (Proxy Mode)                     | <ul style="list-style-type: none"><li>• [透過 (Transparent)] (推奨) : Web プロキシがインターネット ターゲットを指定できるようにします。このモードでは、Web プロキシは、透過的または明示的に転送された Web 要求を代行受信できます。</li><li>• [転送 (Forward)] : クライアントブラウザがインターネット ターゲットを指定できるようにします。Web プロキシを使用するように各 Web ブラウザを個々に設定する必要があります。このモードでは、Web プロキシは明示的に転送された Web 要求のみを代行受信できます。</li></ul> |

| プロパティ           | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP スプーフィング接続タイプ | <p>[プロキシモード (Proxy Mode)] に [透過的 (Transparent)] を選択した場合は、IP スプーフィング接続タイプのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [透過的な接続に対してのみ (For Transparent Connections Only)] : 透過接続の場合にのみ、IP スプーフィングを設定します。</li> <li>• [すべての接続に対して (For All connections)] : 透過的な接続と明示的な接続に IP スプーフィングを設定します。</li> </ul> <p>[プロキシモード (Proxy Mode)] に [転送 (Forward)] を選択した場合は、[IP スプーフィング接続タイプ (IP Spoofing Connection Type)] は常に [明示的 (Explicit)] になります。</p> <p><b>Note</b><br/>         選択した IP スプーフィング接続タイプは、ネイティブ FTP、HTTP、および HTTPS のすべてのプロトコルに適用されます。</p> <p>ルーティングポリシーに IP スプーフィングプロファイルを追加するには、次を参照してください。 <a href="#">ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加, on page 374</a></p> |

**ステップ 4** 必要に応じて Web プロキシの詳細設定を完了します。

| プロパティ                                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 永続的接続のタイムアウト (Persistent Connection Timeout) | <p>トランザクションが完了し、その他のアクティビティが検出されなかった後に、Web プロキシがクライアントまたはサーバーとの接続を開いたままにしておく最大時間 (秒単位)。</p> <ul style="list-style-type: none"> <li>• [クライアント側 (Client side)]。クライアントとの接続のタイムアウト値。</li> <li>• [サーバー側 (Server side)]。サーバーとの接続のタイムアウト値。</li> </ul> <p>これらの値を大きくすると、接続が開いたままになっている時間が延長され、接続の開閉に費やされるオーバーヘッドが低減します。ただし、永続的な同時接続の数が最大数に達した場合に Web Proxy が新しい接続を開く機能も低下します。</p> <p>接続を確立して SSL ハンドシェイクを実行した後、クライアント要求がプロキシに送信されない場合、プロキシは永続的な接続タイムアウトを待ってから、クライアントとの接続を停止します。</p> <p>シスコは、デフォルト値を維持することを推奨します。</p> |
| 使用中接続タイムアウト (In-Use Connection Timeout)      | <p>現在のトランザクションが完了していないときに、Web プロキシがアイドル状態のクライアントまたはサーバーからのデータをさらに待機する最大時間 (秒単位)。</p> <ul style="list-style-type: none"> <li>• [クライアント側 (Client side)]。クライアントとの接続のタイムアウト値。</li> <li>• [サーバー側 (Server side)]。サーバーとの接続のタイムアウト値。</li> </ul>                                                                                                                                                                                                                                                                     |

| プロパティ                                                                                          | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 同時永続的接続<br>(サーバー最大数)<br>(Simultaneous<br>Persistent Connections<br>(Server Maximum<br>Number)) | Web プロキシサーバーがサーバーに対して開いたままにする接続（ソケット）の最大数。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| クライアントあたりの最大接続数                                                                                | <p>クライアントによって開始される同時接続数を、設定した値に制限します。接続数が設定した制限値を超えると、接続がドロップされ、管理者にアラートが送信されます。</p> <p><b>Note</b></p> <p>デフォルトでは、[クライアントあたりの最大接続数（Maximum Connections Per Client）]は無効になっています。</p> <p>制限値を設定するには、[クライアントあたりの最大接続数（Maximum Connections Per Client）]チェックボックスをオンにして、次の手順を実行します。</p> <ul style="list-style-type: none"><li>• [接続（Connections）]：許可される同時接続数を入力します。</li><li>• [除外対象のダウンストリームプロキシまたはロードバランサ（Exempted Downstream Proxy or Load Balancer）]：ダウンストリームプロキシ、ロードバランサ、またはその他のクライアント IP アドレスの IP アドレスを入力します（サブネットまたはホスト名を設定することはできません）。Web プロキシには、この除外リストに含まれる IP アドレスの同時接続の制限が適用されません。</li></ul> |



| プロパティ                                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ヘッダーの生成<br>(Generate Headers)              | <p>要求に関する情報をエンコードするヘッダーを生成して追加します。</p> <ul style="list-style-type: none"> <li>• <b>X-Forwarded-For</b> ヘッダーは、HTTP 要求を発信したクライアントの IP アドレスをエンコードします。</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• ヘッダーの転送をオン/オフするには、advancedproxyconfig CLI コマンドの Miscellaneous オプション「HTTP X-Forwarded-Forヘッダーを通過させますか? (Do you want to pass HTTP X-Forwarded-For headers?)」を使用します。</li> <li>• 明示的な転送アップストリーム プロキシを使用して、プロキシ認証によりユーザー認証やアクセス制御を管理するには、これらのヘッダーを転送する必要があります。</li> <li>• 透過的 HTTPS 要求の場合、アプライアンスは XFF ヘッダーを復号できません。明示的要求の場合、アプライアンスは接続要求で受信される XFF ヘッダーを使用し、SSL トンネル内の XFF を復号しないため、X-Forwarded-For によるクライアント IP アドレスの識別が HTTPS 透過的要求に適用されることはありません。</li> <li>• <b>Request Side VIA</b> ヘッダーは、クライアントからサーバーへの要求が通過するプロキシをエンコードします。</li> <li>• <b>Response Side VIA</b> ヘッダーは、サーバーからクライアントへの要求が通過するプロキシをエンコードします。</li> </ul> |
| Received ヘッダーの使用<br>(Use Received Headers) | <p>アップストリーム プロキシとして展開された Web プロキシが、ダウンストリーム プロキシから送信された X-Forwarded-For ヘッダーを使用してクライアントを識別できるようにします。Web プロキシは、リストに含まれていない送信元からの X-Forwarded-For ヘッダーの IP アドレスを受け入れません。</p> <p>これをイネーブルにする場合は、ダウンストリーム プロキシまたはロード バランサの IP アドレスが必要です (サブネットやホスト名は入力できません)。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 範囲要求の転送<br>(Range Request Forwarding)      | <p>範囲要求の転送をイネーブルまたはディセーブルにするには、[範囲要求の転送の有効化 (Enable Range Request Forwarding)] チェックボックスを使用します。詳細については、<a href="#">Web アプリケーションへのアクセスの管理, on page 506</a>を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**ステップ 5** 変更を送信し、保存します。

### What to do next

- [Web プロキシ キャッシュ, on page 241](#)

- [トランスペアレント リダイレクションの設定, on page 58](#)

## Web プロキシ キャッシュ

Web プロキシは、パフォーマンスを向上させるためにデータをキャッシュします。AsyncOS には「セーフ」から「アグレッシブ」の範囲の定義済みキャッシュモードがあり、またカスタマイズしたキャッシングも使用できます。キャッシュ対象から特定の URL を除外することもできます。これを行うには、その URL をキャッシュから削除するか、無視するようにキャッシュを設定します。

### Web プロキシ キャッシュのクリア

#### Procedure

**ステップ 1** [セキュリティサービス (Security Services)] > [Web プロキシ (Web Proxy)] を選択します。

**ステップ 2** [キャッシュを消去 (Clear Cache)] をクリックしてアクションを確定します。

### Web プロキシ キャッシュからの URL の削除

#### Procedure

**ステップ 1** CLI にアクセスします。

**ステップ 2** `webcache> evict` コマンドを使用して、必要なキャッシング エリアにアクセスします。

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict
Enter the URL to be removed from the cache.
[]>
```

**ステップ 3** Enter the URL to be removed from the cache.

#### Note

URL にプロトコルが含まれていない場合は、URL に `http://` が追加されます (たとえば、`www.cisco.com` は `http://www.cisco.com` となります)。

## Web プロキシによってキャッシュしないドメインまたは URL の指定

## Procedure

**ステップ 1** CLI にアクセスします。

**ステップ 2** `webcache -> ignore` コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore
Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

**ステップ 3** 管理するアドレス タイプを入力します (DOMAINS または URLS)。

```
[]> urls
Manage url entries:
Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

**ステップ 4** `add` と入力して新しいエントリを追加します。

```
[]> add
Enter new url values; one on each line; an empty line to finish
[]>
```

**ステップ 5** 以下の例のように、1 行に 1 つずつ、ドメインまたは URL を入力します。

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com
Enter new url values; one on each line; an empty line to finish
[]>
```

ドメインまたは URL を指定する際に、特定の正規表現 (regex) 文字を含めることができます。DOMAINS オプションでは、前にピリオドを付けることで、キャッシュ対象からドメインとそのサブドメイン全体を除外できます。たとえば、`google.com` ではなく、`.google.com` と入力すると、`www.google.com`、`docs.google.com` などを除外することができます。

URLS オプションでは、正規表現文字の全一式を使用できます。正規表現の使用方法については、[正規表現, on page 321](#)を参照してください。

**ステップ 6** 値の入力を終了するには、メイン コマンドライン インターフェイスに戻るまで Enter キーを押します。

**ステップ 7** 変更を保存します。

## Web プロキシのキャッシュ モードの選択

### Procedure

**ステップ 1** CLI にアクセスします。

**ステップ 2** `advancedproxyconfig -> caching` コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> caching
Enter values for the caching options:
The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

**ステップ 3** 必要な Web プロキシ キャッシュ設定に対応する番号を入力します。

| 入力 | モード            | 説明                                                                                                                                                      |
|----|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | セーフ            | 他のモードと比較して、キャッシングが最も少なく、RFC #2616 には最大限準拠します。                                                                                                           |
| 2  | 最適化            | キャッシングと RFC #2616 への準拠が適度です。セーフ モードと比較した場合、Last-Modified ヘッダーが存在するときにキャッシング時間が指定されていない場合に、最適化モードでは Web プロキシがオブジェクトをキャッシュします。Web プロキシは、ネガティブ応答をキャッシュします。 |
| 3  | アグレッシブ         | キャッシングが最も多く、RFC #2616 への準拠は最小限です。最適化モードと比較した場合、アグレッシブ モードでは、認証済みコンテンツ、ETag の不一致、および Last-Modified ヘッダーのないコンテンツがキャッシュされます。Web プロキシは非キャッシュ パラメータを無視します。   |
| 4  | カスタマイズド<br>モード | 各パラメータを個々に設定します。                                                                                                                                        |

**ステップ 4** オプション 4（カスタマイズモード）を選択した場合は、各カスタム設定の値を入力します（または、デフォルト値のままにします）。

**ステップ 5** メイン コマンド インターフェイスに戻るまで、Enter キーを押します。

**ステップ 6** 変更を保存します。

---

### What to do next

#### 関連項目

- [Web プロキシ キャッシュ, on page 241](#)。

## Web プロキシの IP スプーフィング

デフォルトでは、Web プロキシは要求を転送する際に、自身のアドレスに合わせて要求の送信元 IP アドレスを変更します。これによってセキュリティは強化されますが、IP スプーフィングを実装してこの動作を変更し、Secure Web Appliance からではなく、要求がクライアント IP やその他のルーティング可能なカスタム IP アドレスから発信されたように見せることができます。Web プロキシ IP スプーフィングを設定するには、カスタム IP アドレスの IP スプーフィングプロファイルを作成し、それらをルーティングポリシーに追加します。

IP スプーフィングは、透過的または明示的に転送されたトラフィックに対して機能します。Web プロキシが透過モードで展開されている場合は、透過的にリダイレクトされた接続のみ、またはすべての接続（透過的にリダイレクトされた接続と明示的に転送された接続）に対して（IP スプーフィング接続タイプを設定できる）ことができます。明示的に転送された接続で IP スプーフィングを使用する場合は、リターンパケットを Secure Web Appliance にルーティングする適切なネットワークデバイスがあることを確認してください。

IP スプーフィングがイネーブルで、アプライアンスが WCCP ルータに接続されている場合は、2 つの WCCP サービス（送信元ポートに基づくサービスと宛先ポートに基づくサービス）を設定する必要があります。

IP スプーフィングプロファイルには、HTTPS トラフィックが透過的にリダイレクトされる場合の制限があります。[URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス, on page 749](#) を参照してください。

#### 関連項目

- [IP スプーフィングプロファイルの作成, on page 245](#)
- [Web プロキシの設定, on page 237](#)
- [WCCP サービスの設定, on page 60](#)

## IP スプーフィングプロファイルの作成

### Before you begin

Web プロキシ設定でプロキシモードと IP スプーフィング接続タイプが選択されていることを確認します。詳細については、[Web プロキシの設定, on page 237](#)を参照してください。

### Procedure

- ステップ 1 [Web Security Manager] > [IP スプーフィングプロファイル (IP Spoofing Profiles)] を選択します。
- ステップ 2 [プロファイルを追加 (Add Profile)] をクリックします。
- ステップ 3 IP スプーフィングプロファイルの名前を入力します。
- ステップ 4 スプーフィングプロファイル名に割り当てる IP アドレスを入力します。
- ステップ 5 変更を送信し、保存します。

### What to do next

IP スプーフィングプロファイルをルーティングポリシーに追加します。詳細については、「[ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加, on page 374](#)」を参照してください。

### Related Topics

- [IP スプーフィングプロファイルの編集 \(245 ページ\)](#)
- [IP スプーフィングプロファイルの削除 \(246 ページ\)](#)

## IP スプーフィングプロファイルの編集



### Note

IP スプーフィングプロファイルを更新すると、そのプロファイルに関連付けられているすべてのルーティングポリシーでそのプロファイルが更新されます。

### Procedure

- ステップ 1 [Web Security Manager] > [IP スプーフィングプロファイル (IP Spoofing Profiles)] を選択します。
- ステップ 2 編集する IP スプーフィングプロファイル名のリンクをクリックします。
- ステップ 3 プロファイルの詳細を変更します。
- ステップ 4 変更を送信し、保存します。

## IP スプーフィングプロファイルの削除

## Procedure

**ステップ 1** [Web Security Manager] > [IP スプーフィングプロファイル (IP Spoofing Profiles)] を選択します。

**ステップ 2** 削除する IP スプーフィングプロファイルに対応するゴミ箱アイコンをクリックします。

**Note**

削除しようとしている IP スプーフィングプロファイルが 1 つ以上のルーティングポリシーに割り当てられている場合は、アプライアンスによって警告が表示されます。この場合は、影響を受けるすべてのルーティングポリシーに割り当てる別の IP スプーフィングプロファイルを選択します。

**ステップ 3** 変更を送信し、保存します。

## Web プロキシのカスタム ヘッダー

特定の発信トランザクションにカスタムヘッダーを追加することにより、宛先サーバーによる特別な処理を要求できます。たとえば、YouTube for Schools と関係がある場合、カスタムヘッダーを使用して、YouTube.com へのトランザクション要求を自身のネットワークから発信された、特別な処理を必要とする要求として識別させることができます。

## Web 要求へのカスタム ヘッダーの追加

## Procedure

**ステップ 1** CLI にアクセスします。

**ステップ 2** `advancedproxyconfig -> customheaders` コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders
Currently defined custom headers:
Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
- EDIT - Edit entries
[]>
```

**ステップ3** 次のように、必要なサブコマンドを入力します。

| オプション          | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [削除 (Delete) ] | 指定するカスタム ヘッダーを削除します。コマンドで返されたリストのヘッダーに関連付けられている番号を使用して削除するヘッダーを指定します。                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| [新規 (New) ]    | <p>指定するドメインの使用に提供するヘッダーを作成します。</p> <p>ヘッダーの例：</p> <p>X-YouTube-Edu-Filter: ABCD1234567890abcdef</p> <p>（この場合の値は、YouTube で提供される固有キーです）。</p> <p>ドメインの例：</p> <p>youtube.com</p> <p>カスタムヘッダーの最大長は 16k で、CR または LF を除く任意の値を含めることができます。</p> <p>カスタムヘッダーの例：</p> <pre>Choose the operation you want to perform: - DELETE - Delete entries - NEW - Add new entries - EDIT - Edit entries []&gt; new Please enter the custom HTTP header (in the form field: value): []&gt; [:characters colon(:) and double quotes(") are not allowed]</pre> |
| [編集 (Edit) ]   | 既存のヘッダーを指定したヘッダーと置き換えます。コマンドで返されたリストのヘッダーに関連付けられている番号を使用して削除するヘッダーを指定します。                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**ステップ4** メイン コマンド インターフェイスに戻るまで、Enter キーを押します。

**ステップ5** 変更を保存します。

## Web プロキシのバイパス

- [Web プロキシのバイパス \(Web 要求の場合\) , on page 247](#)
- [Web プロキシのバイパス設定 \(Web 要求の場合\) , on page 248](#)
- [Web プロキシのバイパス設定 \(アプリケーションの場合\) , on page 248](#)

### Web プロキシのバイパス (Web 要求の場合)

特定のクライアントからの透過的要求や特定の宛先への透過的要求が Web プロキシをバイパスするように、Secure Web Applianceを設定できます。

Web プロキシをバイパスすることによって、以下のことが可能になります。



## Web プロキシのバイパス設定 (Web 要求の場合)

- HTTP ポートを使用しているが、適切に機能しない HTTP 非対応の（または独自の）プロトコルが、プロキシサーバーに接続するときに干渉されないようにします。
- ネットワーク内の特定のマシンからのトラフィックが、マルウェアのテストマシンなど、ネットワークプロキシおよび組み込みのセキュリティ保護をすべてバイパスすることを確認します。

バイパスは、Web プロキシに透過的にリダイレクトされる要求に対してのみ機能します。Web プロキシは、トランスペアレントモードでも転送モードでも、クライアントから明示的に転送されたすべての要求を処理します。

## Web プロキシのバイパス設定 (Web 要求の場合)

## Procedure

**ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] > [バイパス設定 (Bypass Settings)] を選択します。

**ステップ 2** [バイパス設定の編集 (Edit Bypass Settings)] をクリックします。

**ステップ 3** Web プロキシをバイパスするアドレスを入力します。

**Note**

/0 をバイパスリスト内の任意の IP のサブネットマスクとして設定すると、アプライアンスはすべての Web トラフィックをバイパスします。この場合、アプライアンスは設定を 0.0.0.0/0 として解釈します。

**ステップ 4** プロキシバイパスリストに追加するカスタム URL カテゴリを選択します。

**Note**

[正規表現 (Regular Expressions)] に Web プロキシバイパスを設定することはできません。

**Note**

カスタム URL カテゴリをプロキシバイパスリストに追加すると、カスタム URL カテゴリのすべての IP アドレスとドメイン名が、送信元と宛先の両方でバイパスされます。

**ステップ 5** 変更を送信し、保存します。

**Note**

IP スプーフィングが有効になっている場合、バイパスリストに含まれているドメインは明示的な要求をサポートしません。

## Web プロキシのバイパス設定 (アプリケーションの場合)

## Procedure

**ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] > [バイパス設定 (Bypass Settings)] を選択します。

**ステップ 2** [アプリケーションのスキップ設定を編集 (Edit Application Bypass Settings)] をクリックします。

**ステップ 3** スキャンをバイパスするアプリケーションを選択します。

**ステップ 4** 変更を送信し、保存します。

**Note**

- Microsoft Update ByPass 機能は、Application Discovery and Control (ADC) でのみ動作します。アプリケーション制御機能に対して ADC が有効になっていることを確認する必要があります。
- Webex バイパス設定は、HTTPS トラフィックにのみ適用されます。ただし、HTTP トラフィックの場合、アプリケーションはアクセス ポリシーを介して使用してブロックできます。

## ポリシーごとの Web プロキシ カスタム ヘッダー

HTTP リクエストのカスタムヘッダープロファイルを設定し、ヘッダー書き換えプロファイルの下に複数のヘッダーを作成できます。各プロファイルには最大 12 のヘッダーを設定できます。既存のヘッダー プロファイルを変更または削除することもできます。既存のアクセス ポリシーにヘッダー書き換えプロファイルを追加して、特定のアクセス ポリシーが適用されるすべてのトランザクションにヘッダーを含めることができます。

ヘッダー書き換えプロファイル機能を使用すると、認証が成功した後、アプライアンスがユーザとグループの情報を別のアップストリームデバイスに渡すことができます。アップストリームプロキシはユーザを認証済みと見なし、追加の認証をバイパスし、定義されたアクセス ポリシーに基づいてユーザにアクセスを提供します。

- [HTTP Web リクエストのヘッダー書き換えプロファイルの作成 \(249 ページ\)](#)
- [ユーザー名とグループ ヘッダー形式の変更 \(251 ページ\)](#) (オプション)
- [アクセス ポリシーへのヘッダー プロファイルの追加 \(251 ページ\)](#)

AsynOS バージョン 14.0 以降では、CLI コマンド `advancedproxyconfig-> customheader` を使用した Web プロキシ カスタム ヘッダーの作成を避けることを推奨します。

### HTTP Web リクエストのヘッダー書き換えプロファイルの作成

#### 手順

**ステップ 1** [Web Security Manager] > [HTTP 書き換えプロファイル (HTTP Rewrite Profiles)] を選択します

**ステップ 2** [プロファイルを追加 (Add Profile)] をクリックします。

**ステップ 3** 作成するヘッダー書き換えプロファイルに一意の名前を割り当てます。

**ステップ 4** [ヘッダー (Headers)] エリアで、次の情報を入力します。

(注)

[ヘッダー書き換えプロファイル (Header Rewrite Profiles)] には空または Null のヘッダー値を入力できません。ヘッダーを保存して、Null または値なしで送信すると、ヘッダーは発信リクエストに含まれません。

たとえば、アウトバウンドサーバーへのヘッダー `Via` を非表示にする場合は、値「」でHTTP書き換えプロファイルにヘッダー名 `Via` を追加します。

- [ヘッダー名 (HeaderName)] : HTTP リクエストに追加するヘッダー名を入力します。例 : X-Client-IP、X-Authenticated-User、X-Authenticated-Groups など
- [ヘッダー値 (Header Value)] : ヘッダー名に対応するリクエストヘッダーに含める値を入力します。ヘッダー変数のプレフィックス :
  - `$ ReqMeta` : クライアント IP、ユーザー、グループなどの標準 HTTP ヘッダー変数を取得します。たとえば、リクエストヘッダーにユーザー名を含める場合、形式は `($ReqMeta[X-Authenticated-User])` です。
  - `$ReqHeader` : 標準の HTTP ヘッダーの値、または同じヘッダー書き換えプロファイルに定義された他のヘッダーのヘッダーの値を使用します。  
たとえば、  

```
Header1:32
```

```
Header2: 44-($ReqHeader[Header1])-46
```

 ヘッダー 2 の値は `44-32-46` になります
- [テキスト形式 (TextFormat)] : エンコーディングのテキスト形式を選択します。使用可能なオプションは ASCII と UTF-8 です。
- [バイナリ エンコーディング (Binary Encoding)] : リクエストヘッダーにバイナリ エンコーディング (Base64) を使用するかどうかを選択します。

(注)

サーバータイプに基づいて、送信されたリクエストヘッダーフィールドのサイズがサーバーの上限を超えた場合、アプライアンスはエラーメッセージを表示します。たとえば、異なるサーバータイプは異なるヘッダー長をサポートします。

- Apache 2.0、2.2 : 8k
- Nginx : 4k ~ 8k
- IIS (バージョンによって異なります) : 8K ~ 16K
- Tomcat : (バージョンによって異なります) 8K

ISE を使用したユーザー識別の場合、グローバル X-authentication ヘッダー設定 (X-Authenticated-User および X-Authenticated-Groups) は、プレフィックスとしてドメインおよび認証メカニズムを適用しません。

ASCII としてテキスト形式を選択した場合でも、`($ ReqMeta [HTTP_header])` 値として UTF+8 を入力できます。現在、次のヘッダーは `($ReqMeta[HTTP_header])` をサポートしています。

- X-Authenticated-User
- X-Authenticated-Groups
- X-Client-IP

ヘッダーの値が Null の場合、ヘッダーは発信リクエストに含まれません。これは、以下を実行しない場合に発生します。

- プロキシ認証を有効にします。
- アクセスポリシー、復号ポリシー、またはルーティングポリシーのメンバーシップ基準でグループを定義します。

**ステップ 5** 変更を送信し、保存します。

## ユーザー名とグループヘッダー形式の変更

### 手順

**ステップ 1** [Web Security Manager] > [HTTP 書き換えプロファイル (HTTP Rewrite Profiles)] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** 形式を変更します。

許可される形式は次のとおりです。

- ユーザー名 : \$authMechanism://\$domainName/\$userName、\$authMechanism:\\\$domainName\\\$userName、\$domainName/\$userName、\$domainName\\\$userName、\$userName
- グループ : \$authMechanism://\$domainName/\$groupName、\$authMechanism:\\\$domainName\\\$groupName、\$domainName/\$groupName、\$domainName\\\$groupName、\$groupName

カンマ (,) 、コロン (:) 、セミコロン (;) 、バックスラッシュ (\) 、縦棒 (|) などのデリミタも変更できます。

**ステップ 4** 変更を送信し、保存します。

## アクセスポリシーへのヘッダープロファイルの追加

### 始める前に

アクセスポリシーの設定 [ポリシーの作成 \(369 ページ\)](#) を参照してください。

### 手順

**ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] を選択します。

**ステップ 2** [アクセスポリシー (Access Policies)] ページで、[HTTP 書き換えプロファイル (HTTP Rewrite Profile)] のリンクをクリックします。

新しいアクセス ポリシーを作成し、それにヘッダー書き換えプロファイルを追加することもできます。新しいアクセス ポリシーを作成するには、次を参照してください。[ポリシーの作成](#) (369 ページ)

**ステップ 3** ポリシーに追加するヘッダー書き換えプロファイルを選択します。追加すると、特定のアクセス ポリシーが適用される HTTP トランザクションにヘッダーが含まれます。

**ステップ 4** 変更を送信し、保存します。

アクセス ポリシーにリンクされたヘッダー書き換えプロファイルは削除できます。削除する前に、別のプロファイルを選択すると、選択したプロファイルがアクセス ポリシーに自動的に適用されます。

## Web プロキシ使用規約

Secure Web Appliance を設定して、Web アクティビティのフィルタリングとモニタリングが行われていることをユーザに通知できます。アプライアンスは、ユーザーが初めてブラウザにアクセスしたときに、一定時間の経過後、エンドユーザー確認ページを表示します。エンドユーザー確認ページが表示されたら、ユーザーはリンクをクリックして、要求した元のサイトまたは他の Web サイトにアクセスする必要があります。

### 関連項目

- [エンドユーザーへのプロキシ アクションの通知, on page 533](#)

## ドメイン マップ

特定のクライアントからの透過的 HTTPS 要求や特定の宛先への透過的 HTTPS 要求が HTTPS プロキシをバイパスするように、Secure Web Applianceを設定できます。

トラフィックがアプライアンスを通過することを必要とするアプリケーションに関して、変更や宛先サーバーの証明書チェックを行わずに、パススルーを使用することができます。

## 特定アプリケーションのドメインマップ

### 始める前に

特定のサーバーへのパススルートラフィックを必要とするデバイスに関して定義された識別ポリシーがあることを確認してください。詳細については、[ユーザーおよびクライアントソフトウェアの分類](#) (267 ページ) を参照してください。具体的には、次のことを行う必要があります。

- [認証/識別から除外 (Exempt from authentication/identification) ] をオンします。
- この識別プロファイルを適用するアドレスを指定します。IP アドレス、CIDR ブロック、およびサブネットを入力できます。

## 手順

**ステップ 1** HTTPS プロキシを有効にします。詳細については、[HTTPS プロキシのイネーブル化 \(348 ページ\)](#) を参照してください。

**ステップ 2** [Webセキュリティマネージャ (Web Security Manager)] > [ドメインマップ (Domain Map)] を選択します。

- a) [ドメインの追加 (Add Domain)] をクリックします。
- b) [ドメイン名 (Domain Name)] に宛先サーバーのドメイン名を入力します。
- c) 既存のドメインが指定されている場合は、優先順位を選択します。
- d) IP アドレスを入力します。
- e) [送信 (Submit)] をクリックします。

**ステップ 3** [Webセキュリティマネージャ (Web Security Manager)] > [カスタムおよび外部URLカテゴリ (Custom and External URL Categories)] を選択します。

- a) [Add Category] をクリックします。
- b) 次の情報を入力します。

| 設定                          | 説明                                                                                                                                              |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| カテゴリ名<br>(Category Name)    | この URL カテゴリの識別子を入力します。この名前は、ポリシー グループに URL フィルタリングを設定するときに表示されます。                                                                               |
| リスト順 (List Order)           | カスタム URL カテゴリのリストで、このカテゴリの順序を指定します。リスト内の最初の URL カテゴリに「1」を入力します。<br><br>URL フィルタリングエンジンでは、指定した順序でカスタム URL カテゴリに対してクライアント要求が評価されます。               |
| カテゴリ タイプ<br>(Category Type) | [ローカルカスタムカテゴリ (Local Custom Category)] を選択します。                                                                                                  |
| 詳細設定<br>(Advanced)          | このセクションに、追加のアドレスセットを指定する正規表現を入力できます。<br>正規表現を使用して、入力したパターンと一致する複数のアドレスを指定できます。<br><br>正規表現の使用方法については、 <a href="#">正規表現 (321 ページ)</a> を参照してください。 |

- c) 変更を送信し、保存します。

**ステップ 4** [Webセキュリティマネージャ (Web Security Manager)] > [復号ポリシー (Decryption Policies)] を選択します。

- a) 新しい復号ポリシーを作成します。
- b) 特定のアプリケーションの HTTPS トラフィックをバイパスするために作成した識別プロファイルを選択します。

- c) [詳細設定 (Advanced)] パネルで、[URLカテゴリ (URL Categories)] のリンクをクリックします。
- d) [追加 (Add)] カラムをクリックして、手順 3 で作成したカスタム URL カテゴリを追加します。
- e) [完了 (Done)] をクリックします。
- f) [復号ポリシー (Decryption Policies)] ページで、[URLフィルタリング (URL Filtering)] のリンクをクリックします。
- g) [パススルー (Pass Through)] を選択します。
- h) 変更を送信し、保存します。

%(フォーマット指定子を使用してアクセスログ情報を表示することができます。詳細については、[アクセス ログのカスタマイズ \(714 ページ\)](#) を参照してください。

(注)

- ドメインマップ機能は HTTPS 透過モードで動作します。
- この機能は、明示モードでは動作せず、HTTP トラフィックについても動作しません。
- この機能を使用してトラフィックを許可するには、ローカルカスタムカテゴリを設定する必要があります。
- この機能を有効にすると、SNI 情報が利用できる場合でも、ドメインマップで設定されたサーバー名に従ってサーバー名の変更または割り当てが行われます。
- この機能は、ドメイン名に基づくトラフィックがドメインマップと一致し、対応するカスタムカテゴリ、復号ポリシー、パススルーアクションが設定されている場合、そのトラフィックをブロックしません。
- 認証をこのパススルー機能と併用することはできません。認証には復号が必要ですが、この場合、トラフィックは復号されません。
- UDP トラフィックはモニターされません。Secure Web Applianceに到達しないように UDP トラフィックを設定する必要があります。代わりに、WhatsApp、Telegram などのアプリケーションのためにファイアウォールを経由してインターネットに直接アクセスする必要があります。
- WhatsApp、Telegram、および Skype は透過モードで動作します。ただし、WhatsApp などの一部のアプリケーションは、アプリケーションの制限のために、明示モードでは動作しません。

## Web 要求をリダイレクトするためのクライアント オプション

クライアントから Web プロキシに明示的に要求を転送することを選択した場合は、それを実行するためのクライアントの設定方法も指定する必要があります。以下の方法から選択します。

- **明示的な設定を使用してクライアントを設定する。** Web プロキシのホスト名とポート番号を使ってクライアントを設定します。設定方法の詳細については、個々のクライアントのマニュアルを参照してください。



**Note** デフォルトでは、Web プロキシ ポートはポート番号 80 と 3128 を使用します。クライアントはいずれかのポートを使用できます。

- **プロキシ自動設定 (PAC) ファイルを使用してクライアントを設定する。** PAC ファイルは、Web 要求の送信先をクライアントに指示します。このオプションを使用すると、プロキシの詳細に対する以降の変更を一元管理できます。

PAC ファイルを使用する場合は、PAC ファイルの保存場所とクライアントがそれらを検出する方法を選択する必要があります。

#### 関連項目

- [クライアントアプリケーションによる PAC ファイルの使用, on page 255](#)

## クライアントアプリケーションによる PAC ファイルの使用

### プロキシ自動設定 (PAC) ファイルのパブリッシュ オプション

クライアントがアクセスできる場所に PAC ファイルをパブリッシュする必要があります。有効な場所は以下のとおりです。

- **Web サーバー**
- **Secure Web Appliance。** クライアントに対しては Web ブラウザとして表示される Secure Web Appliance に PAC ファイルを配置できます。アプライアンスには、さまざまなホスト名、ポート、ファイル名を使用している要求に対応する機能など、PAC ファイルを管理するための追加オプションもあります。
- **ローカル マシン。** クライアントのハードディスクに PAC ファイルをローカルに配置できます。これを一般的な解決方法として使用することは推奨されません。自動 PAC ファイル検出には適していませんが、テストには役立つ可能性があります。

#### 関連項目

- [Secure Web Appliance での PAC ファイルのホスト, on page 256](#)
- [クライアントアプリケーションでの PAC ファイルの指定, on page 257](#)
- [Secure Web Appliance での PAC ファイルのホスト, on page 256](#)
- [クライアントアプリケーションでの PAC ファイルの指定, on page 257](#)

### プロキシ自動設定 (PAC) ファイルを検索するクライアント オプション

クライアントに対して PAC ファイルを使用する場合は、クライアントが PAC ファイルを検索する方法を選択する必要があります。以下の 2 つの対処法があります。



- PAC ファイルの場所をクライアントに設定する。この PAC ファイルを明確に差し指す URL をクライアントに設定します。
- PAC ファイルの場所を自動的に検出するようにクライアントを設定する。DHCP または DNS とともに WPAD プロトコルを使用して PAC ファイルを自動的に検索するようにクライアントを設定します。

## PAC ファイルの自動検出

WPAD は、DHCP および DNS ルックアップを使用してブラウザが PAC ファイルの場所を判別できるようにするプロトコルです。

- DHCP と共に WPAD を使用するには、DHCP サーバーに PAC ファイルの場所の URL と共にオプション 252 を設定します。ただし、すべてのブラウザが DHCP をサポートしているわけではありません。
- DNS と共に WPAD を使用するには、PAC ファイルのホスト サーバーを指し示すように DNS レコードを設定します。

いずれかまたは両方のオプションを設定できます。WPAD は最初に DHCP を使用して PAC ファイルの検出を試み、検出できなかった場合は DNS を使って試みます。

### 関連項目

- [クライアントでの PAC ファイルの自動検出, on page 258](#)

## Secure Web Applianceでの PAC ファイルのホスト

### Procedure

- ステップ 1** [セキュリティ サービス (Security Services) ] > [PAC ファイル ホスティング (PAC File Hosting) ] を選択します。
- ステップ 2** [設定の有効化と編集 (Enable and Edit Settings) ] をクリックします。
- ステップ 3** (任意) 以下の基本設定項目を設定します。

| オプション                                  | 説明                                              |
|----------------------------------------|-------------------------------------------------|
| PAC サーバー ポート<br>(PAC Server Ports)     | Secure Web Applianceが PAC ファイル要求のリッスンに使用するポート。  |
| PAC ファイルの有効期限<br>(PAC File Expiration) | ブラウザ キャッシュで指定されている分数が経過した後に PAC ファイルを期限切れにできます。 |

- ステップ 4** [PACファイル (PAC Files) ] セクションで [参照 (Browse) ] をクリックし、 Secure Web Applianceにアップロードする PAC ファイルをローカルマシンから選択します。

### Note

選択したファイルの名前が `default.pac` である場合は、ブラウザで場所を設定するときにファイル名を指定する必要がありません。名前が指定されていない場合、Secure Web Applianceは `default.pac` というファイルを検索します。

**ステップ 5** [アップロード (Upload)] をクリックして、ステップ 4 で選択した PAC ファイルを Secure Web Appliance にアップロードします。

**ステップ 6** (任意) [PAC ファイルサービスを直接提供するホスト名 (Hostnames for Serving PAC Files Directly)] セクションで、ポート番号を含まない PAC ファイル要求のホスト名と関連ファイル名を設定します。

| オプション                                                                                            | 説明                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| ホスト名<br>(Hostname)                                                                               | Secure Web Applianceが要求を処理する場合に、PAC ファイル要求に含める必要があるホスト名。要求にはポート番号が含まれていないため、要求は Web プロキシの HTTP ポート (ポート80) を使用して処理され、ホスト名評価から PAC ファイル要求として識別できます。 |
| プロキシポートを通じた「GET」要求に対するデフォルト PAC ファイル<br>(Default PAC File for "Get/" Request through Proxy Port) | 同じ行のホスト名に関連付けられる PAC ファイル名。ホスト名に対する要求は、ここで指定した PAC ファイルを返します。<br>アップロード済みの PAC ファイルのみを選択できます。                                                      |
| 行を追加 (AddRow)                                                                                    | 別の行を追加して、追加のホスト名と PAC ファイル名を指定します。                                                                                                                 |

**ステップ 7** 変更を送信し、保存します。

## クライアントアプリケーションでの PAC ファイルの指定

- ・ [クライアントでの PAC ファイルの場所の手動設定, on page 257](#)
- ・ [クライアントでの PAC ファイルの自動検出, on page 258](#)

### クライアントでの PAC ファイルの場所の手動設定

#### Procedure

**ステップ 1** PAC ファイルを作成してパブリッシュします。

**ステップ 2** ブラウザの PAC ファイル設定領域に PAC ファイルの場所を示す URL を入力します。

Secure Web Applianceが PAC ファイルをホストしている場合、有効な URL 形式は以下のようになります。

`http://server_address[.domain][:port][/filename]` | `http://WSAHostname[/filename]`

`WSAHostname` は、Secure Web Appliance に PAC ファイルをホストするときに設定した [ホスト名 (hostname)] の値です。ホストしていない場合、URL の形式は格納場所と（場合によっては）クライアントに応じて異なります。

---

### What to do next

- [Secure Web Appliance での PAC ファイルのホスト, on page 256](#)

## クライアントでの PAC ファイルの自動検出

### Procedure

---

**ステップ 1** `wpad.dat` という名前の PAC ファイルを作成し、Web サーバーまたは Secure Web Appliance にパブリッシュします（DNS と共に WPAD を使用する場合は、Web サーバーのルートフォルダにファイルを配置する必要があります）。

**ステップ 2** 次の MIME タイプで `.dat` ファイルを設定するように Web サーバーを設定します。

```
application/x-ns-proxy-autoconfig
```

#### Note

Secure Web Appliance はこれを自動的に実行します。

**ステップ 3** DNS ルックアップをサポートするには、「wpad」から始まる、内部的に解決可能な DNS 名を作成して（例：`wpad.example.com`）、`wpad.dat` ファイルをホストしているサーバーの IP アドレスに関連付けます。

**ステップ 4** DHCP ルックアップをサポートするには、DHCP サーバーのオプション 252 に `wpad.dat` ファイルの場所の URL を設定します（例：「`http://wpad.example.com/wpad.dat`」）。URL には、IP アドレスなど、有効な任意のホストアドレスを使用できます。特定の DNS エントリは必要ありません。

---

### What to do next

- [クライアントアプリケーションによる PAC ファイルの使用, on page 255](#)
- [Secure Web Appliance での PAC ファイルのホスト, on page 256](#)
- [Firefox で WPAD を使用できない, on page 744](#)

## FTP プロキシ サービス

- [FTP プロキシ サービスの概要, on page 259](#)
- [FTP プロキシの有効化と設定, on page 259](#)

## FTP プロキシ サービスの概要

Web プロキシは、以下の 2 種類の FTP 要求を代行受信できます。

- **ネイティブ FTP**。ネイティブ FTP 要求は、専用 FTP クライアントによって生成されます（または、ブラウザで組み込みの FTP クライアントを使用して生成されます）。FTP プロキシが必要です。
- **FTP over HTTP**。ブラウザは、ネイティブ FTP を使用する代わりに、HTTP 要求内に FTP 要求をエンコードすることがあります。FTP プロキシは必要ありません。

### 関連項目

- [FTP プロキシの有効化と設定, on page 259](#)
- [FTP 通知メッセージの設定, on page 545](#)

## FTP プロキシの有効化と設定



**Note** FTP over HTTP 接続に適用されるプロキシ設定を設定するには、[Web プロキシの設定, on page 237](#)を参照してください。

### Procedure

**ステップ 1** [セキュリティ サービス (Security Services)] > [FTP プロキシ (FTP Proxy)] を選択します。

**ステップ 2** [設定の有効化と編集 (Enable and Edit Settings)] をクリックします（表示されるオプションが [設定の編集 (Edit Settings)] だけの場合、FTP プロキシは設定済みです。）

**ステップ 3** (オプション) 基本的な FTP プロキシ設定項目を設定します。

| プロパティ                                       | 説明                                                                                                                   |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| プロキシ リスニングポート (Proxy Listening Port)        | FTP プロキシが FTP 制御接続をリスンするポート。クライアントは、(FTP サーバーに接続するためのポート (通常はポート 21 を使用) としてではなく) FTP プロキシを設定するときにこのポートを使用する必要があります。 |
| キャッシング (Caching)                            | 匿名ユーザーからのデータ接続をキャッシュするかどうか。<br><b>Note</b><br>匿名ではないユーザーからのデータはキャッシュされません。                                           |
| サーバー側の IP スプーフィング (Server Side IP Spoofing) | FTP プロキシが FTP サーバーの IP アドレスをシミュレートできるようにします。これによって、IP アドレスが制御接続とデータ接続で異なる場合に、トランザクションを許可しない FTP クライアントに対応できます。       |
| クライアント IP スプーフィング                           | FTP プロキシが FTP クライアントの送信元 IP アドレスを模倣できるようにします。有効にすると、FTP 要求は FTP プロキシではなく FTP クライアントから発信されたように見えます。                   |

| プロパティ                                              | 説明                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 認証形式<br>(Authentication Format)                    | FTP クライアントと通信するときに FTP プロキシが使用する認証形式を選択できるようにします。                                                                                                                                                                                                                                                                                                                                 |
| パッシブモードのデータポート範囲 (Passive Mode Data Port Range)    | パッシブ モード接続で FTP プロキシとのデータ接続を確立するために FTP クライアントが使用する TCP ポートの範囲。                                                                                                                                                                                                                                                                                                                   |
| アクティブモードのデータポート範囲<br>(Active Mode Data Port Range) | <p>アクティブ モード接続で FTP プロキシとのデータ接続を確立するために FTP サーバーが使用する TCP ポートの範囲。この設定は、ネイティブ FTP および FTP over HTTP 接続の両方に適用されます。</p> <p>ポート範囲を大きくすると、同じ FTP サーバーからのさらに多くの要求に対応できます。TCP セッションの TIME-WAIT 遅延（通常数分）によって、ポートは使用された直後に、同じ FTP サーバーで再び使用できるようになりません。その結果、所定の FTP サーバーは短時間アクティブ モードで <math>n</math> 回以上 FTP プロキシに接続できません。ここでは <math>n</math> は、このフィールドに指定されたポート数です。</p>                  |
| ウェルカム バナー<br>(Welcome Banner)                      | <p>接続時に FTP クライアントに表示されるウェルカム バナー。次から選択します。</p> <ul style="list-style-type: none"> <li>• <b>[FTP サーバーメッセージを (FTP server message) ]</b>。メッセージは宛先 FTP サーバーによって表示されます。このオプションは、Web プロキシが透過モードに設定されている場合にのみ利用でき、透過接続にのみ適用されます。</li> <li>• <b>[カスタム メッセージ (Custom message) ]</b>。このオプションをオンにすると、すべてのネイティブ FTP 接続に対してこのカスタム メッセージが表示されます。オフにした場合は、明示的な転送ネイティブ FTP 接続に使用されます。</li> </ul> |

#### ステップ 4 (オプション) FTP プロキシの詳細設定を設定します。

| プロパティ                                     | 説明                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 制御接続のタイムアウト (Control Connection Timeouts) | <p>現在のトランザクションが完了していない場合に、アイドル状態の FTP クライアントまたは FTP サーバーからの制御接続による通信を、FTP プロキシがさらに待機する最大時間（秒単位）。</p> <ul style="list-style-type: none"> <li>• <b>[クライアント側 (Client side) ]</b>。アイドル状態の FTP クライアントとの制御接続のタイムアウト値。</li> <li>• <b>[サーバー側 (Server side) ]</b>。アイドル状態の FTP サーバーとの制御接続のタイムアウト値。</li> </ul> |

| プロパティ                                   | 説明                                                                                                                                                                                                                                                                                            |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| データ接続のタイムアウト (Data Connection Timeouts) | <p>現在のトランザクションが完了していない場合に、アイドル状態の FTP クライアントまたは FTP サーバーからのデータ接続による通信を、FTP プロキシがさらに待機する時間。</p> <ul style="list-style-type: none"> <li>• <b>[クライアント側 (Client side)]</b>。アイドル状態の FTP クライアントとのデータ接続のタイムアウト値。</li> <li>• <b>[サーバー側 (Server side)]</b>。アイドル状態の FTP サーバーとのデータ接続のタイムアウト値。</li> </ul> |

ステップ 5 変更を送信し、保存します。

#### What to do next

- [FTP プロキシ サービスの概要, on page 259](#)

## SOCKS プロキシ サービス

- [SOCKS プロキシ サービスの概要, on page 261](#)
- [SOCKS トラフィックの処理のイネーブル化, on page 262](#)
- [SOCKS プロキシの設定, on page 262](#)
- [SOCKS ポリシーの作成, on page 263](#)

## SOCKS プロキシ サービスの概要

Secure Web Applianceには、SOCKS トラフィックを処理するための SOCKS プロキシが含まれます。SOCKS ポリシーは、SOCKS トラフィックを制御するアクセスポリシーと同等です。アクセスポリシーと同様に、識別プロファイルを使用して、各 SOCKS ポリシーによってどのトランザクションを管理するかを指定できます。SOCKS ポリシーをトランザクションに適用すると、ルーティングポリシーによってトラフィックのルーティングを管理できます。

SOCKS プロキシでは、以下の点に注意してください。

- SOCKS プロトコルは、直接転送接続のみをサポートしています。
- SOCKS プロキシは、アップストリームプロキシをサポートしていません（アップストリームプロキシに転送されません）。
- SOCKS プロキシは、Application Visibility and Control (AVC)、Application Discovery and Control (ADC)、Data Loss Prevention (DLP)、およびマルウェア検出に使用されるスキャンングサービスをサポートしていません。
- SOCKS プロキシは、ポリシー追跡をサポートしていません。
- SOCKS プロキシは、SSL トラフィックを復号できません。これは、クライアントからサーバーにトンネリングします。

## SOCKS トラフィックの処理のイネーブル化

### Before you begin

Web プロキシをイネーブルにします。

### Procedure

**ステップ 1** [セキュリティ サービス (Security Services)] > [SOCKS プロキシ (SOCKS Proxy)] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** [SOCKS プロキシを有効にする (Enable SOCKS Proxy)] を選択します。

**ステップ 4** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## SOCKS プロキシの設定

### Procedure

**ステップ 1** [セキュリティ サービス (Security Services)] > [SOCKS プロキシ (SOCKS Proxy)] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** [SOCKS プロキシを有効にする (Enable SOCKS Proxy)] を選択します。

**ステップ 4** 基本および高度な SOCKS プロキシ設定を設定します。

|                                                   |                                                                 |
|---------------------------------------------------|-----------------------------------------------------------------|
| SOCKS プロキシ<br>(SOCKS Proxy)                       | イネーブル。                                                          |
| SOCKS コントロール ポート (SOCKS Control Ports)            | SOCKS 要求を受け入れるポート。デフォルトは 1080 です。                               |
| UDP リクエスト<br>ポート (UDP Request Ports)              | SOCKS サーバーがリスンする必要がある UDP ポート。デフォルトは 16000 ~ 16100 です。          |
| プロキシネゴシエーションタイムアウト<br>(Proxy Negotiation Timeout) | ネゴシエーション段階で SOCKS クライアントからデータを送受信するのを待機する時間 (秒単位)。デフォルトは 60 です。 |

|                                  |                                                                   |
|----------------------------------|-------------------------------------------------------------------|
| UDP トンネル タイムアウト (Tunnel Timeout) | UDP トンネルを閉じる前に UDP クライアントまたはサーバーからのデータを待機する時間 (秒単位)。デフォルトは 60 です。 |
|----------------------------------|-------------------------------------------------------------------|

## SOCKS ポリシーの作成

### Procedure

**ステップ 1** [Web セキュリティ マネージャ (Web Security Manager) ] > [SOCKS ポリシー (SOCKS Policies) ] を選択します。

**ステップ 2** [ポリシーを追加 (Add Policy) ] をクリックします。

**ステップ 3** [ポリシー名 (Policy Name) ] フィールドに名前を割り当てます。

#### Note

各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

**ステップ 4** (オプション) 説明を追加します。

**ステップ 5** [上記ポリシーを挿入 (Insert Above Policy) ] フィールドで、この SOCKS ポリシーに挿入する SOCKS ポリシーの場所を選択します。

#### Note

複数の SOCKS ポリシーを設定する場合、各ポリシーの論理的な順序を決定します。照合が適切に行われるように、ポリシーの順序を指定してください。

**ステップ 6** [アイデンティティとユーザー (Identities and Users) ] セクションで、このグループ ポリシーに適用する 1 つ以上の ID を選択します。

**ステップ 7** (オプション) [詳細 (Advanced) ] セクションを拡張して、追加のメンバーシップ要件を定義します。

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プロキシ ポート (Proxy Ports) | <p>ブラウザに設定されたポート。</p> <p>(オプション) Web プロキシへのアクセスに使用するプロキシ ポートによってポリシー グループのメンバーシップを定義します。[プロキシ ポート (Proxy Ports) ] フィールドに、1 つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。</p> <p>あるポート上に要求を明示的に転送するように設定されたクライアントのセットがあり、別のポート上に要求を明示的に転送するように設定された別のクライアントのセットがある場合、プロキシ ポート上でポリシー グループのメンバーシップを定義することがあります。</p> <p><b>Note</b><br/>このポリシー グループに関連付けられている ID が この詳細設定によって ID メンバーシップを定義している場合、SOCKS ポリシー グループ レベルではこの設定項目を設定できません。</p> |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



|                      |                                                                                                                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サブネット<br>(Subnets)   | <p>(オプション) サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義します。</p> <p>関連付けられた <b>ID</b> で定義できるアドレスを使用するか、または<b>特定のアドレス</b>をここに入力できます。</p> <p><b>Note</b><br/>ポリシー グループに関連付けられている ID が、アドレスによってグループのメンバーシップを定義している場合は、このポリシー グループに、ID のアドレスのサブセットであるアドレスを入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込みます。</p> |
| 時間範囲<br>(Time Range) | <p>(オプション) 時間範囲別にポリシー グループのメンバーシップを定義します。</p> <p>a. [時間範囲 (Time Range)] から時間範囲を選択します。</p> <p>b. このポリシー グループが選択した時間範囲内または範囲外の時間に適用されるかどうかを指定します。</p>                                                                                                                                                                       |

**ステップ 8** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

#### What to do next

- (オプション) SOCKS ポリシーで使用するための ID を追加します。
- SOCKS トラフィックを管理する 1 つ以上の SOCKS ポリシーを追加します。

## 要求の代替受信に関するトラブルシューティング

- URL カテゴリが一部の FTP サイトをブロックしない, [on page 746](#)
- 大規模 FTP 転送の切断, [on page 746](#)
- ファイルのアップロード後に FTP サーバーにゼロ バイト ファイルが表示される, [on page 746](#)
- アップストリーム プロキシ経由で FTP 要求をルーティングできない, [on page 768](#)
- HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する, [on page 759](#)
- HTTPS 要求および FTP over HTTP 要求の場合にユーザーがグローバル ポリシーに一致, [on page 760](#)



## 第 5 章

# アクセス制御

この章で説明する内容は、次のとおりです。

- [ポリシーの適用に対するエンドユーザーの分類 \(265 ページ\)](#)
- [ポリシーの適用に対する URL の分類 \(280 ページ\)](#)
- [HTTPS トラフィックを制御する復号ポリシーの作成 \(343 ページ\)](#)
- [インターネット要求を制御するポリシーの作成 \(362 ページ\)](#)
- [SaaS アクセス コントロール \(399 ページ\)](#)
- [発信トラフィックでの既存の感染のスキャン \(407 ページ\)](#)

## ポリシーの適用に対するエンドユーザーの分類

この章で説明する内容は、次のとおりです。

- [ユーザーおよびクライアント ソフトウェアの分類：概要 \(265 ページ\)](#)
- [ユーザーおよびクライアント ソフトウェアの分類：ベスト プラクティス \(266 ページ\)](#)
- [識別プロファイルの条件 \(267 ページ\)](#)
- [ユーザーおよびクライアント ソフトウェアの分類 \(267 ページ\)](#)
- [識別プロファイルと認証 \(277 ページ\)](#)
- [識別プロファイルのトラブルシューティング \(279 ページ\)](#)
- [識別プロファイルでのサロゲートタイプのトラブルシューティング \(280 ページ\)](#)

## ユーザーおよびクライアント ソフトウェアの分類：概要

識別プロファイルによるユーザーおよびユーザーエージェント（クライアントソフトウェア）の分類は、以下の目的のために行われます。

- ポリシーの適用に対するトランザクション要求をグループ化します（SaaS を除く）。
- 識別および認証の要件の指定

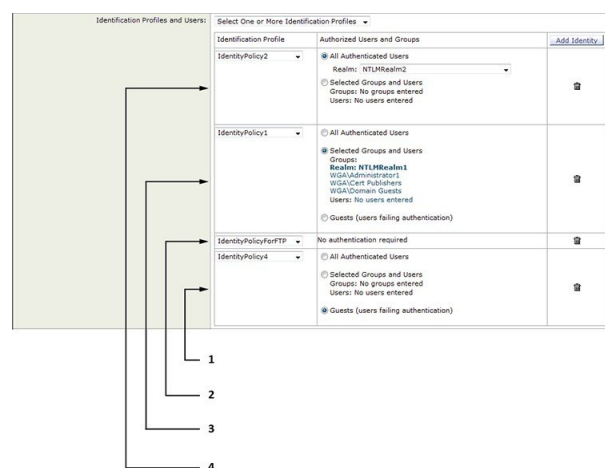
AsyncOS はすべてのトランザクションに識別プロファイルを割り当てます。

- カスタム識別プロファイル：AsyncOS は、そのアイデンティティの条件に基づいてカスタムプロファイルを割り当てます。
- グローバル識別プロファイル：AsyncOS は、カスタムプロファイルの条件を満たさないトランザクションにグローバルプロファイルを割り当てます。デフォルトでは、グローバルプロファイルには認証がありません。

AsyncOS は最初から順番に識別プロファイル进行处理します。グローバルプロファイルは最後のプロファイルです。

識別プロファイルには 1 つの条件だけを含めることができます。複数の条件を含む識別プロファイルはすべての条件を満たす必要があります。

1 つのポリシーによって複数の識別プロファイルを要求できます。



|   |                                                         |
|---|---------------------------------------------------------|
| 1 | この識別プロファイルは、認証に失敗したユーザーにゲストアクセスを許可し、それらのユーザーに適用されます。    |
| 2 | この識別プロファイルには、認証は使用されません。                                |
| 3 | この識別プロファイルで指定されたユーザーグループは、このポリシーで認証されます。                |
| 4 | この識別プロファイルでは認証シーケンスが使用され、このポリシーがシーケンス内の 1 つのレールに適用されます。 |

## ユーザーおよびクライアントソフトウェアの分類：ベストプラクティス

- 一般的な識別プロファイルを少数作成して、すべてのユーザーまたは少数の大きなユーザーグループに適用します。より詳細に管理する場合は、プロファイルではなくポリシーを使用します。

- 一意の条件で識別プロファイルを作成します。
- 透過モードで展開する場合は、認証をサポートしていないサイトの識別プロファイルを作成します。「[認証のバイパス, on page 122](#)」を参照してください。

## 識別プロファイルの条件

これらのトランザクションの特性は、以下の識別プロファイルの定義に使用できます。

| オプション                              | 説明                                                                                                                                                                                                                                  |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サブネット (Subnet)                     | クライアントサブネットは、ポリシーのサブネットリストに一致している必要があります。                                                                                                                                                                                           |
| プロトコル (Protocol)                   | トランザクションで使用されるプロトコル (HTTP、HTTPS、SOCKS、またはネイティブ FTP)                                                                                                                                                                                 |
| ポート (Port)                         | 要求のプロキシポートは、識別プロファイルのポートリストに記載されている必要があります (リストに記載がある場合)。明示的な転送接続のために、ブラウザに設定されたポートです。透過接続の場合は、宛先ポートと同じです。                                                                                                                          |
| ユーザー エージェント (User Agent)           | 要求を行うユーザー エージェント (クライアントアプリケーション) は、識別プロファイルのユーザー エージェント リストに記載されている必要があります (リストに記載がある場合)。一部のユーザー エージェントは認証を処理できないため、認証を必要としないプロファイルを作成する必要があります。ユーザー エージェントには、アップデータやブラウザ (Internet Explorer、Mozilla Firefox など) などのプログラムが含まれています。 |
| URL カテゴリ (URL Category)            | 要求 URL の URL カテゴリは、識別プロファイルの URL カテゴリ リストに記載されている必要があります (リストに記載がある場合)。                                                                                                                                                             |
| 認証要件 (Authentication requirements) | 識別プロファイルが認証を必要とする場合は、クライアントの認証クレデンシャルが識別プロファイルの認証要件と一致する必要があります。                                                                                                                                                                    |

## ユーザーおよびクライアント ソフトウェアの分類

始める前に

- 認証レルムを作成します。[Active Directory 認証レルムの作成 \(NTLMSSP および基本\) \(97 ページ\)](#) または [LDAP 認証レルムの作成 \(100 ページ\)](#) を参照してください。
- 識別プロファイルへの変更を確定するときに、エンドユーザーを再認証する必要があるのに注意してください。

- クラウドコネクタモードの場合は、追加の識別プロファイルオプション（マシンID）を使用できます。[ポリシーの適用に対するマシンの識別（233ページ）](#)を参照してください。
- （オプション）認証シーケンスを作成します。[認証シーケンスの作成（118ページ）](#)を参照してください
- （オプション）識別プロファイルにモバイルユーザーを含める場合は、セキュアモビリティをイネーブルにします。
- （オプション）認証サロゲートについて理解しておきます。[識別済みユーザーの追跡（125ページ）](#)を参照してください。

## 手順

- ステップ1** [Web セキュリティ マネージャ（Web Security Manager）]>[識別プロファイル（Identification Profiles）]を選択します。
- ステップ2** [プロファイルの追加（Add Profile）]をクリックしてプロファイルを追加します。
- ステップ3** [識別プロファイルの有効化（Enable Identification Profile）]チェックボックスを使用して、このプロファイルをイネーブルにするか、プロファイルを削除せずにただちにディセーブルにします。
- ステップ4** [名前（Name）]に一意のプロファイル名を割り当てます。
- ステップ5** [説明（Description）]は任意です。
- ステップ6** [上に挿入（Insert Above）]ドロップダウンリストから、このプロファイルを配置するポリシーテーブル内の位置を選択します。

（注）

認証を必要とする最初の識別プロファイルの上に、認証を必要としない識別プロファイルを配置します。

- ステップ7** [ユーザー識別方式（User Identification Method）]セクションで、識別方式を選択して関連パラメータを指定します。表示されるオプションは、選択した方法によって異なります。
- a) [ユーザー識別方式（User Identification Method）]ドロップダウン リストから識別方式を選択します。

| オプション                                                   | 説明                                          |
|---------------------------------------------------------|---------------------------------------------|
| 認証/識別を免除<br>(Exempt from authentication/identification) | ユーザーは基本的に IP アドレスによって識別されます。追加のパラメータはありません。 |
| 認証済みユーザー<br>(Authenticate users)                        | ユーザーは入力した認証クレデンシャルによって識別されます。               |

| オプション                                                                            | 説明                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISEによってユーザーを透過的に識別<br>(Transparently identify users with ISE)                    | ISEサービスがイネブルの場合に使用できます ([ネットワーク (Network)] > [Identity Services Engine])。これらのトランザクションの場合、ユーザー名および関連するセキュリティグループタグは Identity Services Engine から取得されます。ISE-PIC 展開では、ISE グループとユーザー情報が受信されます。詳細については、 <a href="#">ISE/ISE-PIC サービスを統合するためのタスク (420 ページ)</a> を参照してください。 |
| 認証レルムによってユーザーを透過的に識別<br>(Transparently identify users with authentication realm) | このオプションは、1つ以上の認証レルムが透過的識別をサポートするように定義されている場合に使用できます。                                                                                                                                                                                                               |

(注)

少なくとも 1 つの識別プロファイルに認証または透過的識別が設定されている場合、ポリシー テーブルでは、ユーザー名、ディレクトリ グループ、セキュリティ グループ タグを使用してポリシー メンバーシップを定義できます。

(注)

Context Directory Agent (CDA) はサポートされなくなりました。同じ機能を実現するために、透過的なユーザー識別のために ISE/ISE-PIC を設定することをお勧めします。

将来のリリースでは CDA を設定するオプションは使用できなくなります。

詳細については、<https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/bulletin-c25-2428601.html>を参照してください。

- b) 選択した方式に適したパラメータを指定します。この表に示したすべてのセクションが選択ごとに表示されるわけではありません。

|                                                                               |                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 認証レルムまたはゲスト特権へのフォールバック (Fallback to Authentication Realm or Guest Privileges) | <p>ユーザー認証を ISE から取得できない場合：</p> <ul style="list-style-type: none"> <li>• [ゲスト権限をサポート (Support Guest Privileges)]：トランザクションは続行を許可され、すべての識別プロファイルのゲストユーザーと後続のポリシーを照合します。</li> <li>• [トランザクションをブロック (Block Transactions)]：ISE で識別できないユーザーにインターネット アクセスを許可しません。</li> <li>• [ゲスト特権をサポート (Support Guest privileges)]：無効なクレデンシャルにより認証に失敗したユーザーにゲストアクセスを許可する場合、このチェックボックスをオンにします。</li> </ul> |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                 |  |
|---------------------------------|--|
| 認証レルム<br>(Authentication Realm) |  |
|---------------------------------|--|

[レルムまたはシーケンスを選択 (Select a Realm or Sequence)] : 定義済みの認証レルムまたはシーケンスを選択します。

[スキームの選択 (Select a Scheme)] : 認証スキームを選択します。

- [Kerberos] : クライアントは Kerberos チケットによって透過的に認証されます。
- [基本 (Basic)] : クライアントは常にユーザーにクレデンシャルを要求します。ユーザーがクレデンシャルを入力すると、通常は、入力したクレデンシャルの保存について指定するチェックボックスがブラウザに表示されます。ユーザーがブラウザを開くたびに、クライアントはクレデンシャルの入力を要求するか、または以前に保存したクレデンシャルを再送信します。

クレデンシャルは、保護されていないクリアテキスト (Base64) として送信されます。クライアントと Secure Web Appliance 間でのパケットキャプチャにより、ユーザー名やパスワードが開示される可能性があります。

- [NTLMSSP] : クライアントは、Windows のログイン クレデンシャルを使用して透過的に認証します。ユーザーはクレデンシャルの入力を要求されません。

ただし、以下の場合、クライアントはユーザーにクレデンシャルの入力を求めます。

- Windows クレデンシャルによる認証が失敗した。
- ブラウザのセキュリティ設定が原因で、クライアントが Secure Web Appliance を信頼しない。

クレデンシャルは、3 ウェイ ハンドシェイク (ダイジェスト形式の認証) により安全に送信されます。パスワードが接続を介して送信されることはありません。

- [ヘッダーベースの認証 (Header Based Authentication)] : クライアントおよび Secure Web Appliance は、ユーザーを認証済みと見なし、認証またはユーザークレデンシャルの再入力を求めません。X-Authenticated 機能は、Secure Web Appliance がアップストリームデバイスとして動作する場合に機能します。

認証が成功すると、ダウンストリームデバイスは、X-Authenticated-User および X-Authenticated-Groups (オプション) 拡張 HTTP ヘッダーを介して、ユーザー名とユーザーグループ (オプション) を Secure Web Appliance に送信します。

X-Authenticated-Groups ヘッダーは、アプライアンスで [アクセス ポリシーの照合に X-Authenticate-Groups ヘッダー/カスタム ヘッダー内のグループを使用 (Custom Header for matching Access Policies Use Groups in X-Authenticate-Groups Header/Custom Header for matching Access Policies)]



|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                | <p>オプション（[ネットワーク認証（Network Authentication）]&gt;[グローバル設定の編集（Edit Global Settings）]&gt;）を設定している場合にのみ考慮されます。</p> <p>（注）</p> <p>X-Authenticated ヘッダーは、アクセス ポリシーまたはルーティング ポリシーにのみ適用できます。ただし、[ヘッダー ベースの認証（Header Based Authentication）] が有効になっている識別プロファイルの復号ポリシーへの関連付けは照合されません。</p> <ul style="list-style-type: none"> <li>• [ゲスト特権をサポート（Support Guest privileges）]：無効なクレデンシャルにより認証に失敗したユーザーにゲストアクセスを許可する場合、このチェックボックスをオンにします。</li> </ul> |
| グループ認証のレルム<br>（Realm for Group Authentication） | <ul style="list-style-type: none"> <li>• [レルムまたはシーケンスを選択（Select a Realm or Sequence）]：定義済みの認証レルムまたはシーケンスを選択します。</li> </ul>                                                                                                                                                                                                                                                                                                          |

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>認証サロゲート<br/>(Authentication<br/>Surrogates)</p> | <p>認証の成功後にトランザクションをユーザーに関連付ける方法を指定します (オプションは Web プロキシの展開モードにより異なります)。</p> <ul style="list-style-type: none"> <li>• [IP アドレス (IP Address)] : Web プロキシは、特定の IP アドレスの認証済みユーザーを追跡します。透過的ユーザー識別の場合は、このオプションを選択します。</li> <li>• [永続的なクッキー (Persistent Cookie)] : Web プロキシは、アプリケーションごとに各ユーザー用に永続的クッキーを生成することにより、特定のアプリケーション上の認証済みユーザーを追跡します。アプリケーションを終了してもクッキーは削除されません。</li> <li>• [セッションクッキー (Session Cookie)] : Web プロキシは、アプリケーションごとに各ドメインの各ユーザー用に永続的クッキーを生成することにより、特定のアプリケーション上の認証済みユーザーを追跡します。(ただし、ユーザーが同じアプリケーションから同じドメインに対して異なるクレデンシャルを指定した場合、クッキーは上書きされます)。アプリケーションを終了するとクッキーは削除されます。</li> <li>• [サロゲートなし (No Surrogate)] : Web プロキシは、サロゲートを使用してクレデンシャルをキャッシュせず、新しい TCP 接続ごとに認証済みユーザーを追跡します。このオプションを選択すると、Web インターフェイスは適用されなくなったその他の設定をディセーブルにします。このオプションは、明示的な転送モードに設定し、[ネットワーク (Network)] &gt; [認証 (Authentication)] ページでクレデンシャルの暗号化をディセーブルにしたときにのみ使用できます。</li> <li>• [明示的フォワード要求に同じサロゲート設定を適用 (Apply same surrogate settings to explicit forward requests)] : 透過的要求に使用するサロゲートを明示的要求に適用する場合にオンにします (クレデンシャルの暗号化が自動的にイネーブルになります。) このオプションは、Web プロキシがトランスペアレント モードで展開されている場合にのみ表示されます。</li> </ul> <p>(注)</p> <ul style="list-style-type: none"> <li>• [グローバル認証設定 (Global Authentication Settings)] で、すべての要求に対する認証サロゲートのタイムアウト値を定義できます。</li> <li>• 異なる認証サロゲート (IP アドレス、永続的 Cookie、セッション Cookie など) を使用するように識別プロファイルを設定した場合、アクセスは、他のサロゲートと識別プロファイルが一致しても、IP アドレスサロゲートを使用して認証されます。</li> </ul> |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**ステップ 8** [メンバーシップの定義 (Membership Definition)] セクションで、選択した識別方式に適したメンバーシップパラメータを指定します。以下の表に示すオプションは、すべてのユーザー識別方式で使用できるわけではありません。

| メンバーシップの定義 (Membership Definition)                |                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ユーザーの場所別メンバーの定義 (Define Members by User Location) | この識別プロファイルの適用対象として、 <b>[ローカルユーザーのみ (Local Users Only)]</b> 、 <b>[リモートユーザーのみ (Remote Users Only)]</b> 、または <b>[両方 (Both)]</b> を設定します。ここでの選択は、この識別プロファイルで使用可能な認証設定に影響します。                                                                                                                                                                                                   |
| サブネット別メンバーの定義 (Define Members by Subnet)          | この識別プロファイルを適用するアドレスを入力します。IP アドレス、CIDR ブロック、およびサブネットを入力できます。<br><br>(注)<br>何も入力しない場合は、すべての IP アドレスにこの識別プロファイルが適用されます。                                                                                                                                                                                                                                                     |
| プロトコル別メンバーの定義 (Define Members by Protocol)        | この識別プロファイルを適用するプロトコルを選択します。適用するすべてのプロトコルを選択してください。<br><br><ul style="list-style-type: none"> <li>• <b>[HTTP/HTTPS]</b> : 基礎のプロトコルとして HTTP または HTTPS を使用するすべての要求に適用されます。これには、FTP over HTTP、および HTTP CONNECT を使用してトンネリングされるその他のプロトコルも含まれます。</li> <li>• <b>[ネイティブ FTP (Native FTP)]</b> : ネイティブ FTP 要求にのみ適用されます。</li> <li>• <b>[SOCKS]</b> : SOCKS ポリシーにのみ適用されます。</li> </ul> |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>マシン ID によるメンバーの定義 (Define Members by Machine ID)</b> | <ul style="list-style-type: none"><li>• [このポリシーではマシンIDを使用しないでください (Do Not Use Machine ID in This Policy)] : ユーザーはマシン ID によって識別されません。</li><li>• [マシンIDをベースにしたユーザー認証ポリシーの定義 (Define User Authentication Policy Based on Machine ID)] : ユーザーは基本的にマシン ID によって識別されます。</li></ul> <p>[マシングループ (Machine Groups)] 領域をクリックして、[認証済みマシングループ (Authorized Machine Groups)] ページを表示します。</p> <p>追加する各グループごとに、[ディレクトリ検索 (Directory Search)] フィールドに追加するグループの名前を入力し、[追加 (Add)] をクリックします。リストからグループを削除するには、グループを選択して [削除 (Remove)] をクリックします。</p> <p>[完了 (Done)] をクリックして前のページに戻ります。</p> <p>[マシンID (Machine IDs)] 領域をクリックして、[認証済みマシン (Authorized Machines)] ページを表示します。</p> <p>[認証済みマシン (Authorized Machines)] フィールドで、ポリシーに関連付けるマシン ID を入力し、[完了 (Done)] をクリックします。</p> <p>(注)<br/>マシン ID による認証はコネクタ モードのみでサポートされ、Active Directory が必要です。</p> |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>詳細設定</b> | <p>このセクションを展開して、追加のメンバーシップ要件を定義します。</p> <ul style="list-style-type: none"> <li>• <b>[プロキシポート (Proxy Ports)]</b> : Web プロキシへのアクセスに使用する 1 つ以上のプロキシポートを指定します。ポート番号をカンマで区切って入力します。明示的な転送接続の場合、プロキシポートはブラウザで設定されます。</li> </ul> <p>透過接続の場合は、宛先ポートと同じです。</p> <p>ポート別の ID の定義は、アプライアンスが明示的な転送モードで展開されている場合、またはクライアントがアプライアンスに明示的に要求を転送する場合に最もよく機能します。クライアント要求が透過的にアプライアンスにリダイレクトされる場合は、ポート別の ID の定義によって一部の要求が拒否されることがあります。</p> <ul style="list-style-type: none"> <li>• <b>[URL カテゴリ (URL Categories)]</b> : ユーザー定義または定義済みの URL カテゴリを選択します。デフォルトでは、両方のメンバーシップが除外されます。つまり、[追加 (Add)] 列で選択されていない限り、Web プロキシはすべてのカテゴリを無視します。</li> </ul> <p>URL カテゴリによってメンバーシップを定義する必要がある場合、そのカテゴリに対する認証要求から除外する必要があるときは ID グループにのみ定義します。</p> <ul style="list-style-type: none"> <li>• <b>[ユーザーエージェント (User Agents)]</b> : クライアント要求で見つかったユーザーエージェントごとにポリシーグループメンバーシップを定義します。一般的に定義されているエージェントを選択するか、正規表現を使用して独自のブラウザを定義できます。</li> </ul> <p>また、これらのユーザーエージェントの指定を含めるか除外するかも指定します。つまり、メンバーシップの定義に選択したユーザーエージェントのみを含めるか、選択したユーザーエージェントを明確に除外するかどうかを指定します。</p> |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**ステップ 9** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

#### 次のタスク

- [エンドユーザー クレデンシャルの取得の概要 \(75 ページ\)](#)
- [ポリシー タスクによる Web 要求の管理 : 概要 \(364 ページ\)](#)

## ID の有効化/無効化

### Before you begin

- 識別プロファイルをディセーブルにすると、関連するポリシーからその識別プロファイルが削除されるので注意してください。
- 識別プロファイルを再度イネーブルにしても、その識別プロファイルはポリシーに再び関連付けられません。

### Procedure

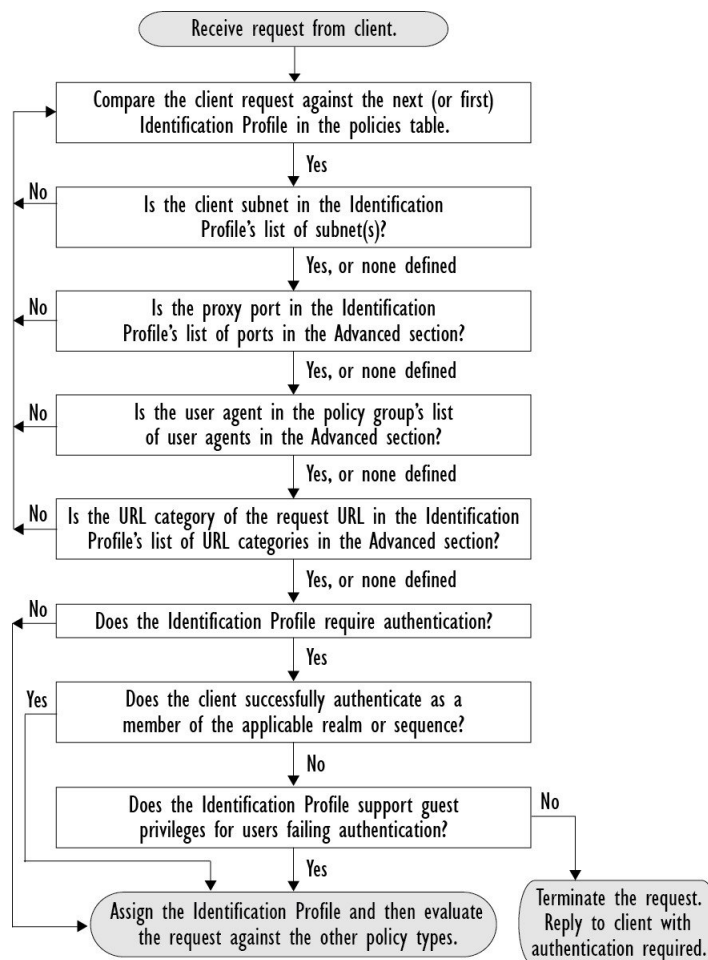
- 
- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager) ] > [識別プロファイル (Identification Profiles) ] を選択します。
  - ステップ 2** 識別プロファイル テーブルのプロファイルをクリックして、そのプロファイルの [識別プロファイル (Identification Profile) ] ページを開きます。
  - ステップ 3** [クライアント/ユーザー識別プロファイルの設定 (Client/User Identification Profile Settings) ] の真下にある [識別プロファイルの有効化 (Enable identification IProfile) ] をオンまたはオフにします。
  - ステップ 4** 変更を送信して確定します ([送信 (Submit) ] と [変更を確定 (Commit Changes) ] ) 。
- 

## 識別プロファイルと認証

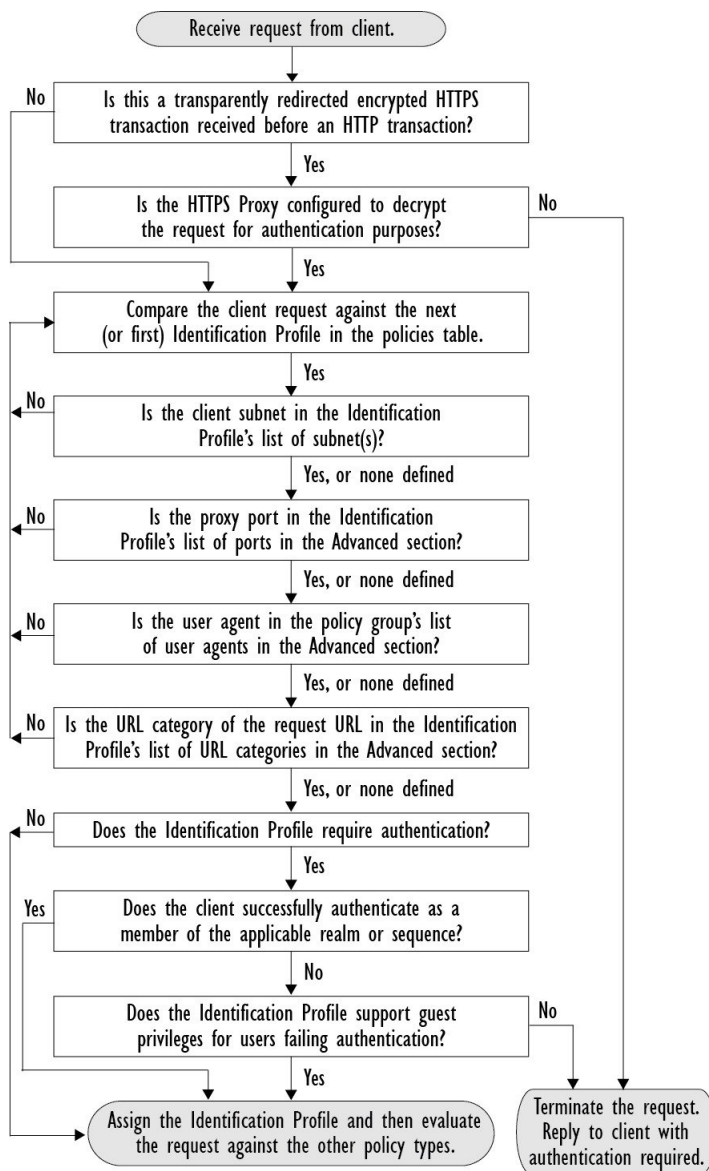
次の図に、識別プロファイルが次を使用するように設定されているときに、Web プロキシがクライアント要求を識別プロファイルに対して評価する方法を示します。

- 認証サロゲートなし
- 認証サロゲートとしての IP アドレス
- 透過的要求を使用する認証サロゲートとしてのクッキー
- 明示的要求を使用する認証サロゲートとしてのクッキー (クレデンシャルの暗号化がイネーブルになっている場合)

Figure 2: 識別プロフィールと認証プロセス：サロゲートおよび IP ベースのサロゲートなし



次の図に、識別プロフィールが認証サロゲートとして Cookie を使用し、クレデンシャルの暗号化を有効にして、要求が明示的に転送されるように設定されているときに、Web プロキシがクライアント要求を識別プロフィールに対して評価する方法を示します。

Figure 3: 識別プロファイルと認証プロセス : **Cookie** ベースのサロゲート

## 識別プロファイルのトラブルシューティング

- 基本認証に関する問題, [on page 742](#)
- ポリシーに関する問題, [on page 758](#)
- ポリシーが適用されない, [on page 759](#)
- ポリシーのトラブルシューティング ツール : ポリシー トレース, [on page 761](#)
- アップストリーム プロキシに関する問題, [on page 767](#)



## 識別プロファイルでのサロゲートタイプのトラブルシューティング

Cisco Web セキュリティアプライアンスが IP アドレスと Cookie ベースの認証サロゲートの両方を使用するように設定されていて、エンドユーザーからのアクセスが両方のアイデンティティに一致する場合、IP アドレスは Cookie ベースの認証サロゲートをオーバーライドします。

共有および個別コンピューターの両方を使用するネットワークでは、IP アドレスとサブネットに基づいて2つの異なる識別プロファイルを作成することをお勧めします。これにより、IP または Cookie 認証サロゲートが使用されるかどうかが決まります。

## ポリシーの適用に対する URL の分類

この章で説明する内容は、次のとおりです。

- [URL トランザクションの分類の概要 \(280 ページ\)](#)
- [URL フィルタリング エンジンの設定 \(284 ページ\)](#)
- [URL カテゴリ セットの更新の管理 \(285 ページ\)](#)
- [URL カテゴリによるトランザクションのフィルタリング \(293 ページ\)](#)
- [YouTube の分類 \(301 ページ\)](#)
- [カスタム URL カテゴリの作成および編集 \(305 ページ\)](#)
- [アダルト コンテンツのフィルタリング \(314 ページ\)](#)
- [アクセス ポリシーでのトラフィックのリダイレクト \(317 ページ\)](#)
- [ユーザーへの警告と続行の許可 \(318 ページ\)](#)
- [時間ベースの URL フィルタの作成 \(319 ページ\)](#)
- [URL フィルタリング アクティビティの表示 \(320 ページ\)](#)
- [正規表現 \(321 ページ\)](#)
- [URL カテゴリについて \(325 ページ\)](#)

## URL トランザクションの分類の概要

グループ ポリシーを使用して、疑わしいコンテンツが含まれている Web サイトへのアクセスを制御するセキュリティポリシーを作成できます。ブロック、許可、または復号されるサイトは、各グループ ポリシーのカテゴリ ブロッキングを設定する際に選択するカテゴリに応じて決まります。URL カテゴリに基づいてユーザー アクセスを制御するには、Cisco Web Usage Controls を有効にする必要があります。これは、ドメインプレフィックスとキーワード分析を使用して URL を分類するマルチレイヤ URL フィルタリング エンジンです。

以下のタスクを実行するときに、URL カテゴリを使用できます。

| オプション                                         | 方法                                                       |
|-----------------------------------------------|----------------------------------------------------------|
| ポリシー グループ メンバーシップの定義                          | <a href="#">URL と URL カテゴリの照合, on page 283</a>           |
| HTTP、HTTPS、および FTP 要求へのアクセスの制御                | <a href="#">URL カテゴリによるトランザクションのフィルタリング, on page 293</a> |
| 特定のホスト名と IP アドレスを指定する、ユーザー定義のカスタム URL カテゴリの作成 | <a href="#">カスタム URL カテゴリの作成および編集, on page 305</a>       |

## 失敗した URL トランザクションの分類

動的コンテンツ分析エンジンは、アクセス ポリシーのみを使用して Web サイトへのアクセスを制御する場合に URL を分類します。ポリシー グループ メンバーシップを判別する場合や、復号ポリシーまたはシスコデータセキュリティ ポリシーを使用して Web サイトへのアクセスを制御する場合は、URL を分類しません。その理由は、このエンジンが宛先サーバーからの応答コンテンツを分析することによって機能するからです。そのため、サーバーから応答をダウンロードする前の要求時に行う必要がある決定では、このエンジンを使用できません。

未分類 URL の Web レピュテーション スコアが WBSR の許可範囲内にある場合、AsyncOS は動的コンテンツ分析を行わずに要求を許可します。

動的コンテンツ分析エンジンは URL を分類した後、カテゴリの評価と URL を一時キャッシュに格納します。これによって、以降のトランザクションで以前の応答のスキャンを利用することができ、応答時ではなく要求時にトランザクションを分類できます。

動的コンテンツ分析エンジンをイネーブルにすると、トランザクションのパフォーマンスに影響することがあります。ただし、ほとんどのトランザクションは Cisco Web 利用の制御 URL カテゴリ データベースを使用して分類されるので、動的コンテンツ分析エンジンは通常、トランザクションのごく一部に対してのみ呼び出されます。

## 動的コンテンツ分析エンジンのイネーブル化

**Note**

- ダイナミック コンテンツ分析 (DCA) はデフォルトで無効になり、AsyncOS 15.2.x 以降のバージョンではサポートされなくなりました。DCA の機能は、Talos Web フィルタリング サービスに置き換えられます。Talos Web フィルタリング サービスは、年間 50 億を超える悪意のあるドメインと URL をブロックし、新しいドメインと URL の検出と分類の速度と精度を向上させます。これにより、SWA アプライアンスに対する Talos の頻繁な更新とともに DCA の必要性をなくし、未分類の Web サイト情報を最小限に抑えることができ、WSA ユーザーによりパフォーマンスの高いソリューションを提供します。
- 定義済みの URL カテゴリを使用して、アクセス ポリシー（またはアクセス ポリシーで使用する ID）でポリシー メンバーシップを定義できます。また、アクセス ポリシーにより同じ URL カテゴリに対してアクションを実行できます。ID とアクセス ポリシーグループ メンバーシップを判別するときに、要求の URL を未分類にすることも可能です。ただし、サーバーから応答を受信した後で動的コンテンツ分析エンジンで分類する必要があります。Cisco Web Usage Controls は動的コンテンツ分析によるカテゴリ評価を無視し、残りのトランザクションに対する URL の評価は「未分類」のままになります。ただし、それ以降のトランザクションは引き続き、新しいカテゴリ評価を利用できます。

**Procedure**

- ステップ 1** [セキュリティ サービス (Security Services)] > [使用許可コントロール (Acceptable Use Controls)] を選択します。
- ステップ 2** Cisco Web Usage Controls を有効にします。
- ステップ 3** 動的コンテンツ分析エンジンを**クリック**してイネーブルにします。
- ステップ 4** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

**未分類の URL**

未分類の URL とは、定義済みの URL カテゴリにも付属のカスタム URL カテゴリにも一致しない URL です。

**Note**

ポリシー グループのメンバーシップを判別するときに、カスタム URL カテゴリは、ポリシー グループのメンバーシップに対して選択されている場合にのみグループに含まれていると見なされます。

一致しないカテゴリと見なされたトランザクションはすべて、[レポート (Reporting)] > [URL カテゴリ (URL Categories)] ページで [分類されてない URL (Uncategorized URL)] として報告されます。未分類 URL の多くは、内部ネットワーク内の Web サイトへの要求から生じま

す。カスタム URL カテゴリを使用して内部 URL をグループ化し、内部 Web サイトに対するすべての要求を許可することを推奨します。これによって、[分類されてないURL (Uncategorized URL)] として報告される Web トランザクションの数が減少し、内部トランザクションが [バイパスされたURLフィルタリング (URL Filtering Bypassed)] 統計情報の一部として報告されるようになります。

#### 関連項目

- フィルタリングされない未分類のデータについて, on page 320。
- カスタム URL カテゴリの作成および編集, on page 305。

## URL と URL カテゴリの照合

URL フィルタリングエンジンはクライアント要求の URL と URL カテゴリを照合するときに、まず、ポリシー グループに含まれているカスタム URL カテゴリと照合して URL を評価します。要求の URL がグループに含まれているカスタム カテゴリと一致しない場合、URL フィルタリングエンジンはその URL を定義済みの URL カテゴリと比較します。URL がカスタム URL カテゴリにも定義済みの URL カテゴリにも一致しない場合、要求は未分類になります。



#### Note

ポリシー グループのメンバーシップを判別するときに、カスタム URL カテゴリは、ポリシー グループのメンバーシップに対して選択されている場合にのみグループに含まれていると見なされます。

特定の Web サイトが割り当てられているカテゴリを確認するには、[未分類の URL と誤って分類された URL の報告](#), on page 283 の URL に移動します。

#### 関連項目

- [未分類の URL](#), on page 282。

## 未分類の URL と誤って分類された URL の報告

未分類の URL および誤分類された URL をシスコに報告できます。シスコでは、複数の URL を同時に送信できる URL 送信ツールをシスコの Web サイトで提供しています。

- <https://talosintelligence.com/tickets>
  - 送信された URL のステータスを確認するには、このページの [送信された URL のステータス (Status on Submitted URLs)] タブをクリックします。
  - また、URL 送信ツールを使用して、URL に割り当てられている URL カテゴリを検索できます。
- [https://www.talosintelligence.com/reputation\\_center/support](https://www.talosintelligence.com/reputation_center/support)
  - クレームを送信するには、シスコアカウントにログインする必要があります。URL、IP、またはドメインに関するクレームを送信できます。

- Web レピュテーション情報を検索するには、[レピュテーションセンター検索 (Reputation Center Search)] ボックスを使用します。

## URL カテゴリ データベース

URL が分類されるカテゴリは、フィルタリングカテゴリデータベースによって決定されます。Secure Web Appliance は各 URL フィルタリング エンジンごとに情報を収集し、個別のデータベースに保持します。フィルタリングカテゴリデータベースは、Cisco アップデートサーバーから定期的にアップデートを受信します。

URL カテゴリ データベースには、シスコ内部およびインターネットのさまざまなデータ要素とデータ ソースが格納されています。要素の 1 つであるオープンディレクトリプロジェクトからの情報は、時々検討されて当初のものから大幅に変更されます。

特定の Web サイトが割り当てられているカテゴリを確認するには、[未分類の URL と誤って分類された URL の報告, on page 283](#)の URL に移動します。

### 関連項目

- [手動による URL カテゴリ セットの更新, on page 292](#)

## URL フィルタリング エンジンの設定

デフォルトでは、Cisco Web 利用の制御 URL フィルタリング エンジン はシステム セットアップ ウィザードでイネーブルになります。

### Procedure

- ステップ 1 [セキュリティサービス (Security Services)] > [使用許可コントロール (Acceptable Use Controls)] を選択します。
- ステップ 2 [グローバル設定を編集 (Edit Global Settings)] をクリックします。
- ステップ 3 [使用許可コントロールを有効にする (Enable Acceptable Use Controls)] プロパティがイネーブルになっていることを確認します。
- ステップ 4 次の Cisco Web Usage Controls のいずれかを選択します。
  - a. アプリケーション制御を有効にする

#### Note

AsyncOS 15.0 以降では、AVC または ADC エンジンを使用して Web トラフィックを監視できます。デフォルトでは、AVC は有効になっています。

- [アプリケーションの表示およびコントロールを有効にする (Enable Application Visibility and Control (AVC)) を有効にする : 300 以上のアプリケーションがあります
- [アプリケーションの検出およびコントロールを有効にする (Application Discovery and Control (ADC)) ] : 3000 以上のアプリケーションがあります

- b. ダイナミックコンテンツ分析エンジンを有効にする
- c. 複数の URL カテゴリの有効化

**Note**

複数の URL カテゴリ機能は、アクセスポリシーのみに適用されます。複数の URL カテゴリ機能を復号ポリシーおよび識別プロファイルに適用することはできません。

**ステップ 5** URL フィルタリングエンジンを利用できない場合に、Web プロキシが使用すべきデフォルトのアクション ([モニター (Monitor) ] または [ブロック (Block) ]) を選択します。デフォルトは [モニター (Monitor) ] です。

**ステップ 6** 変更を送信して確定します ([送信 (Submit) ] と [変更を確定 (Commit Changes) ]) 。

## URL カテゴリ セットの更新の管理

事前定義された URL カテゴリのセットは、新しい Web のトレンドと進化する使用パターンに合わせて時々更新されます。URL カテゴリ セットの更新は、新規 URL の追加や誤分類 URL の再マッピングによる変更とは異なります。カテゴリセットの更新によって既存のポリシーの設定が変更されることがあるため、対処が必要になります。URL カテゴリ セットの更新は製品のリリース間で行われ、AsyncOS のアップグレードは必要ありません。

これらに関する情報は、以下の URL から入手できます：

[http://www.cisco.com/en/US/products/ps10164/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html)。

以下のアクションを実行します。

| 実行する時期                                 | 方法                                                                                                                                                                                                                            |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 更新が実行される前<br>(初期設定の一部としてこれらのタスクを実行します) | <a href="#">URL カテゴリ セットの更新による影響について , on page 285</a><br><a href="#">URL カテゴリ セットの更新の制御 , on page 291</a><br><a href="#">新規および変更されたカテゴリのデフォルト設定 , on page 292</a><br><a href="#">カテゴリおよびポリシーの変更に関するアラートの受信 , on page 293</a> |
| 更新が実行された後                              | <a href="#">URL カテゴリ セットの更新に関するアラートへの応答 , on page 293</a>                                                                                                                                                                     |

## URL カテゴリ セットの更新による影響について

URL カテゴリ セットの更新は、既存のアクセス ポリシー、復号ポリシー、シスコ データ セキュリティ ポリシー、および ID に以下のような影響を与えます。

- [URL カテゴリ セットの変更によるポリシーグループメンバーシップへの影響 , on page 286](#)
- [URL カテゴリ セットの更新によるポリシーのフィルタリングアクションへの影響 , on page 286](#)

## URL カテゴリ セットの変更によるポリシー グループ メンバーシップへの影響

このセクションの内容は、URL カテゴリによって定義できるメンバーシップを含んでいるすべてのポリシー タイプ、および ID に該当します。ポリシー グループ メンバーシップが URL カテゴリによって定義されている場合、カテゴリセットへの変更は以下のような影響を及ぼす可能性があります。

- メンバーシップの唯一の条件であったカテゴリが削除された場合、ポリシーまたは ID はディセーブルになります。

ポリシーのメンバーシップを定義していた URL カテゴリが変更され、それに伴って ACL リストも変更された場合は、Web プロキシが再起動します。

## URL カテゴリ セットの更新によるポリシーのフィルタリングアクションへの影響

URL カテゴリ セットの更新により、ポリシーの動作が以下のように変更される可能性があります。

| 変更内容            | ポリシーおよび ID への影響                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 新しいカテゴリが追加された場合 | <p>新しい URL カテゴリでは、[ポリシー設定 (Policy Configuration)] ページの [更新カテゴリのデフォルトアクション (Default Action for Update Categories)] オプションから次のいずれかのアクションが選択されます。</p> <ul style="list-style-type: none"> <li>• [最小の制限 (Least Restrictive)]</li> <li>• [最大の制限 (Most Restrictive)]</li> </ul> <p>アクションは、新しいカテゴリに対してデフォルトで設定されます。[アクセスポリシー (Access Policies)] および [シスコデータセキュリティポリシー (Cisco Data Security Policies)] で、次の手順を実行します。</p> <ul style="list-style-type: none"> <li>• [最大の制限 (Most Restrictive)] は [ブロック (Block)]</li> <li>• [最小の制限 (Least Restrictive)] は [モニタ (Monitor)]</li> </ul> <p>Web トラフィックタップ (WTT) ポリシー：</p> <ul style="list-style-type: none"> <li>• [最大の制限 (Most Restrictive)] は [タップ (Tap)]</li> <li>• [最小の制限 (Least Restrictive)] は [タップなし (No Tap)]</li> </ul> <p>[復号ポリシー (Decryption Policies)]：</p> <ul style="list-style-type: none"> <li>• [最大の制限 (Most Restrictive)] は [ブロック (Block)]</li> <li>• [最小の制限 (Least Restrictive)] は [パススルー (Pass Through)]</li> </ul> |

| 変更内容            | ポリシーおよび ID への影響                                                                                                                                              |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| カテゴリが削除された場合    | <p>削除されたカテゴリに関連付けられていたアクションは削除されます。</p> <p>ポリシーが削除されたカテゴリにのみ依存していた場合、そのポリシーはディセーブルになります。</p> <p>ポリシーが依存している ID が削除されたカテゴリにのみ依存していた場合、そのポリシーはディセーブルになります。</p> |
| カテゴリの名称が変更された場合 | 既存のポリシーの動作に対する変更はありません。                                                                                                                                      |
| カテゴリが分割された場合    | 1 つのカテゴリが複数の新規カテゴリとなることがあります。新しいカテゴリアクションは、[更新カテゴリのデフォルトアクション (Default Action for Update Categories) ] から選択されます。                                             |



| 変更内容                    | ポリシーおよび ID への影響 |
|-------------------------|-----------------|
| 複数の既存のカテゴリ<br>がマージされた場合 |                 |

| 変更内容 | ポリシーおよび ID への影響                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>ポリシーの元のカテゴリすべてに同じアクションが割り当てられている場合、マージされたカテゴリには元のカテゴリと同じアクションが含まれます。元のカテゴリすべてが [グローバル設定を使用 (Use Global Setting)] に設定されていた場合、マージされたカテゴリも [グローバル設定を使用 (Use Global Setting)] に設定されます。</p> <p>ポリシーの元のカテゴリにさまざまなアクションが割り当てられている場合、マージされたカテゴリに割り当てられるアクションは、そのポリシーの [分類されていないURL (Uncategorized URLs)] の設定によって決まります。</p> <ul style="list-style-type: none"> <li>• [分類されていないURL (Uncategorized URLs)] が [ブロック (Block)] (または [グローバル設定を使用 (Use Global Settings)] (グローバル設定が [ブロック (Block)] のとき)) に設定されている場合は、元のカテゴリにおいて最も制限が厳しいアクションがマージされたカテゴリに適用されます。</li> <li>• [分類されていないURL (Uncategorized URLs)] が [ブロック (Block)] 以外 (または [グローバル設定を使用 (Use Global Settings)] 以外 (グローバル設定が [ブロック (Block)] 以外のとき)) に設定されている場合は、元のカテゴリにおいて最も制限が緩いアクションがマージされたカテゴリに適用されます。</li> </ul> <p>この場合、以前ブロックされていたサイトにユーザがアクセスできるようになる可能性があります。</p> <p>ポリシー メンバーシップが URL カテゴリによって定義されており、マージに関連する一部のカテゴリ、または [分類されていないURL (Uncategorized URLs)] のアクションがポリシー メンバーシップの定義に含まれていない場合は、欠落している項目に対してグローバルポリシーの値が使用されます。</p> <p>制限の厳しさの順位は以下のとおりです (すべてのアクションをすべてのポリシー タイプで利用できるわけではありません)。</p> <ul style="list-style-type: none"> <li>• ブロック (Block)</li> <li>• ドロップ (Drop)</li> <li>• 復号 (Decrypt)</li> <li>• 警告 (Warn)</li> <li>• 時間ベース (Time-based)</li> <li>• モニター (Monitor)</li> <li>• パススルー (Pass Through)</li> </ul> <p><b>Note</b></p> |

| 変更内容 | ポリシーおよび ID への影響                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------|
|      | マージされたカテゴリに基づいている時間ベースのポリシーでは、元のカテゴリのいずれかに関連付けられているアクションが選択されます。（時間ベースのポリシーでは、制限が最も厳しいまたは最も緩いアクションが明確ではないことがあります）。 |

## 関連項目

- [マージされたカテゴリ：例](#), on page 290.

## マージされたカテゴリ：例

以下の例は、ポリシーの [URLフィルタリング (URL Filtering)] ページの設定に基づいてマージされたカテゴリを示しています。

| 元のカテゴリ 1                         | 元のカテゴリ 2                                                                                                                                            | 分類されてない URL                                                                                                                                                                | マージされたカテゴリ                       |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| モニター (Monitor)                   | モニター (Monitor)                                                                                                                                      | (N/A)                                                                                                                                                                      | モニター (Monitor)                   |
| ブロック (Block)                     | ブロック (Block)                                                                                                                                        | (N/A)                                                                                                                                                                      | ブロック (Block)                     |
| グローバル設定を使用 (Use Global Settings) | グローバル設定を使用 (Use Global Settings)                                                                                                                    | (N/A)                                                                                                                                                                      | グローバル設定を使用 (Use Global Settings) |
| 警告 (Warn)                        | ブロック (Block)                                                                                                                                        | モニター (Monitor)<br>元のカテゴリにおいて最も制限が緩いアクションを使用。                                                                                                                               | 警告 (Warn)                        |
| モニター (Monitor)                   | <ul style="list-style-type: none"> <li>• ブロック (Block) または</li> <li>• グローバル設定を使用 (Use Global Settings) (グローバルが [ブロック (Block)] に設定されている場合)</li> </ul> | <ul style="list-style-type: none"> <li>• ブロック (Block) または</li> <li>• グローバル設定を使用 (Use Global Settings) (グローバル設定が [ブロック (Block)] の場合)</li> </ul> 元のカテゴリにおいて最も制限が厳しいアクションを使用。 | ブロック (Block)                     |

| 元のカテゴリ 1                                               | 元のカテゴリ 2                                                                                                                                              | 分類されてない URL                                                                                                                                                                        | マージされたカテゴリ     |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| ブロック (Block)                                           | <ul style="list-style-type: none"> <li>• モニタ (Monitor) または</li> <li>• グローバル設定を使用 (Use Global Settings) (グローバルが [モニタ (Monitor)] に設定されている場合)</li> </ul> | <ul style="list-style-type: none"> <li>• モニタ (Monitor) または</li> <li>• グローバル設定を使用 (Use Global Settings) (グローバル設定が [モニタ (Monitor)] の場合)</li> </ul> <p>元のカテゴリにおいて最も制限が緩いアクションを使用。</p> | モニター (Monitor) |
| メンバーシップが URL カテゴリによって定義されているポリシーの場合：<br>モニター (Monitor) | カテゴリのアクションがポリシーで指定されておらず、カテゴリのグローバルポリシーの値が [ブロック (Block)]。                                                                                            | 未分類の URL のアクションがポリシーで指定されておらず、未分類の URL のグローバル ポリシーの値が [モニタ (Monitor)]。                                                                                                             | モニター (Monitor) |

## URL カテゴリ セットの更新の制御

デフォルトでは、URL カテゴリ セットの更新は自動的に行われます。ただし、これらの更新によって既存のポリシー設定が変更される可能性があるため、すべての自動更新をディセーブルにすることを推奨します。

| オプション                                                                                                                                                                                      | 方法                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| 更新をディセーブルにした場合は、[システム管理 (System Administration)] > [アップグレードとアップデートの設定 (Upgrade and Update Settings)] ページの [アップデートサーバ (リスト) (Update Servers (list))] セクションで、記載されているすべてのサービスを手動で更新する必要があります。 | <p>手動による URL カテゴリ セットの更新, <a href="#">on page 292</a></p> <p>および</p> <p>セキュリティ サービスのコンポーネントの手動による更新, <a href="#">on page 210</a></p> |
| すべての自動更新をディセーブルにします                                                                                                                                                                        | アップグレードおよびサービス アップデートの設定, <a href="#">on page 214</a> 。                                                                              |



**Note** CLI を使用する場合は、更新間隔をゼロ (0) に設定して更新をディセーブルにします。

## 手動による URL カテゴリ セットの更新



## Note

- 進行中の更新を中断しないでください。
- 自動更新をディセーブルにした場合は、必要に応じて手動で URL カテゴリ セットを更新できます。

## Procedure

**ステップ 1** [セキュリティサービス (Security Services)] > [使用許可コントロール (Acceptable Use Controls)] を選択します。

**ステップ 2** アップデートが利用可能かどうかを確認します。

[使用許可コントロールエンジンの更新 (Acceptable Use Controls Engine Updates)] テーブルの [Cisco Web 利用の制御 - Web カテゴリのカテゴリリスト (Cisco Web Usage Controls - Web Categorization Categories List)] を参照してください。

**ステップ 3** 更新するには、[今すぐ更新 (Update Now)] をクリックします。

## 新規および変更されたカテゴリのデフォルト設定

URL カテゴリ セットの更新によって、既存のポリシーの動作が変更されることがあります。URL カテゴリ セットが更新された場合に対応できるように、ポリシーを設定する際は、特定の変更に対してデフォルトの設定を指定しておく必要があります。新しいカテゴリが追加された場合や既存のカテゴリが新しいカテゴリにマージされた場合、それらのカテゴリに対する各ポリシーのデフォルトアクションは、そのポリシーの **[更新カテゴリのデフォルトアクション (Default Action for Update Categories)]** の設定に影響されます。

## 既存の設定の確認または変更の実行

## Procedure

**ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] を選択します。

**ステップ 2** 各アクセスポリシー、復号ポリシー、シスコデータセキュリティポリシーに対して、[URL フィルタリング (URL Filtering)] リンクをクリックします。

**ステップ 3** [分類されてない URL (Uncategorized URLs)] に対して選択されている設定を確認します。

## What to do next

## 関連項目

- [URL カテゴリ セットの更新によるポリシーのフィルタリングアクションへの影響, on page 286。](#)

## カテゴリおよびポリシーの変更に関するアラートの受信

カテゴリ セットの更新によって、以下の 2 種類のアラートがトリガーされます。

- カテゴリの変更についてのアラート
- カテゴリ セットの変更によって変更またはディセーブル化されたポリシーに関するアラート

### Procedure

- 
- ステップ 1** [システム管理 (System Administration)] > [アラート (Alerts)] を選択します。
  - ステップ 2** [受信者の追加 (Add Recipient)] をクリックして電子メール アドレス (または、複数の電子メール アドレス) を追加します。
  - ステップ 3** 受信するアラートの [アラートタイプ (Alert Types)] と [アラートの重大度 (Alert Severities)] を決定します。
  - ステップ 4** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。
- 

## URL カテゴリ セットの更新に関するアラートへの応答

カテゴリ セットの変更に関するアラートを受信した場合は、以下を実行する必要があります。

- カテゴリがマージ、追加、削除された後、ポリシーと ID が引き続きポリシーの目的に合致していることを確認します。さらに
- 新しいカテゴリや分割によるカテゴリの細分化を活用できるように、ポリシーと ID を変更することを検討します。

### 関連項目

- [URL カテゴリ セットの更新による影響について, on page 285](#)

## URL カテゴリによるトランザクションのフィルタリング

URL フィルタリング エンジンを使用して、アクセス ポリシー、復号ポリシー、データ セキュリティ ポリシーのトランザクションをフィルタリングできます。ポリシー グループの URL カテゴリを設定する際は、カスタム URL カテゴリ (定義されている場合) と定義済み URL カテゴリのアクションを設定できます。

設定できる URL フィルタリングアクションは、ポリシー グループのタイプに応じて異なります。

| オプション                                              | 方法                                                            |
|----------------------------------------------------|---------------------------------------------------------------|
| アクセス ポリシー<br>(Access Policies)                     | <a href="#">アクセス ポリシー グループの URL フィルタの設定, on page 294</a>      |
| 復号ポリシー (Decryption Policies)                       | <a href="#">復号ポリシー グループの URL フィルタの設定, on page 298</a>         |
| シスコ データ セキュリティ ポリシー (Cisco Data Security Policies) | <a href="#">データセキュリティ ポリシー グループの URL フィルタの設定, on page 299</a> |

#### 関連項目

- [アクセス ポリシーでのトラフィックのリダイレクト, on page 317](#)
- [ユーザーへの警告と続行の許可, on page 318](#)
- [カスタム URL カテゴリの作成および編集, on page 305](#)
- [URL カテゴリセットの更新によるポリシーのフィルタリングアクションへの影響, on page 286](#)

## アクセス ポリシー グループの URL フィルタの設定

ユーザー定義のアクセス ポリシー グループおよびグローバル ポリシー グループに対して URL フィルタリングを設定できます。

### Procedure

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] > [アクセス ポリシー (Access Policies)] を選択します。
- ステップ 2** ポリシー テーブルで、編集するポリシー グループの [URL フィルタ (URL Filtering)] 列にあるリンクをクリックします。
- ステップ 3** (任意) [カスタム URL カテゴリのフィルタリング (Custom URL Category Filtering)] セクションで、このポリシーのアクションの実行対象となるカスタム URL カテゴリを追加できます。
  - a) [カスタムカテゴリの選択 (Select Custom Categories)] をクリックします。
  - b) このポリシーに含めるカスタム URL カテゴリを選択して、[適用 (Apply)] をクリックします。

URL フィルタリング エンジンでクライアント要求と照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンでは、クライアント要求と含まれているカスタム URL カテゴリを比較します。除外されたカスタム URL カテゴリは無視されます。URL フィルタリング エンジンでは、定義済みの URL カテゴリよりも前に、含まれているカスタム URL カテゴリとクライアント要求の URL を比較します。

ポリシーに含まれているカスタム URL カテゴリは、[カスタム URL カテゴリのフィルタリング (Custom URL Category Filtering)] セクションに表示されます。

**ステップ 4** [カスタム URL カテゴリのフィルタリング (Custom URL Category Filtering)] セクションで、含まれている各カスタム URL カテゴリのアクションを選択します。

| アクション                            | 説明                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| グローバル設定を使用 (Use Global Settings) | <p>グローバル ポリシー グループで設定されているこのカテゴリ用のアクションを使用します。これは、ユーザー定義のポリシー グループのデフォルトアクションです。ユーザー定義のポリシー グループにのみ適用されます。</p> <p><b>Note</b><br/>           カスタム URL カテゴリがグローバル アクセス ポリシーから除外されている場合、ユーザー定義のアクセス ポリシーに含まれているカスタム URL カテゴリのデフォルトアクションは、[グローバル設定を使用 (Use Global Settings)]ではなく、[モニター (Monitor)]になります。カスタム URL カテゴリがグローバル アクセス ポリシーで除外されている場合は、[グローバル設定を使用 (Use Global Settings)]を選択できません。</p> |
| ブロック (Block)                     | Web プロキシは、この設定に一致するトランザクションを拒否します。                                                                                                                                                                                                                                                                                                                                                           |
| リダイレクト (Redirect)                | 当初の宛先がこのカテゴリの URL であるトラフィックを、指定された場所にリダイレクトします。このオプションを選択すると、[リダイレクト先 (Redirect To)] フィールドが表示されます。すべてのトラフィックをリダイレクトする URL を入力します。                                                                                                                                                                                                                                                            |
| 許可 (Allow)                       | <p>このカテゴリの Web サイトに対してクライアント要求を常に許可します。</p> <p>許可された要求は、以降のすべてのフィルタリングとマルウェア スキャンをバイパスします。</p> <p>この設定は信頼できる Web サイトに対してのみ使用してください。この設定は内部サイトに対して使用することをお勧めします。</p>                                                                                                                                                                                                                          |
| モニター (Monitor)                   | Web プロキシは、要求を許可せず、ブロックもしません。代わりに、他のポリシー グループ制御設定 (Web レピュテーション フィルタリングなど) と照合して、クライアント要求の評価を続行します。                                                                                                                                                                                                                                                                                           |
| 警告 (Warn)                        | <p>当初、Web プロキシは要求をブロックして警告ページを表示しますが、ユーザーは警告ページのハイパーテキスト リンクをクリックすることで続行できます。</p> <p><b>Note</b><br/>           YouTube カテゴリフィルタリングでは、どのカテゴリの警告アクションを選択しても、警告メッセージなしでそのカテゴリのビデオを表示できます。これは想定された動作です。</p>                                                                                                                                                                                     |
| クォータベース (Quota-Based)            | 個々のユーザーが、指定されたボリュームまたは時間クォータに達すると、警告が表示されます。クォータに達すると、ブロック ページが表示されます。 <a href="#">時間範囲およびクォータ, on page 389</a> を参照してください。                                                                                                                                                                                                                                                                   |



| アクション                 | 説明                                                                                             |
|-----------------------|------------------------------------------------------------------------------------------------|
| 時間ベース<br>(Time-Based) | Web プロキシは、指定された時間範囲内で要求をブロックまたはモニターします。<br><a href="#">時間範囲およびクォータ, on page 389</a> を参照してください。 |

**ステップ 5** [事前定義された URL カテゴリのフィルタリング (Predefined URL Category Filtering)] セクションで、各カテゴリに対して以下のいずれかのアクションを選択します。

- グローバル設定を使用 (Use Global Settings)
- モニター (Monitor)
- 警告 (Warn)
- ブロック (Block)
- 時間ベース (Time-Based)
- クォータベース (Quota-Based)

**ステップ 6** [分類されていない URL (Uncategorized URLs)] セクションで、定義済みまたはカスタムの URL カテゴリに分類されない Web サイトへのクライアント要求に対して実行するアクションを選択します。この設定により、URL カテゴリ セットの更新で生じた新規カテゴリとマージ カテゴリのデフォルト アクションも決まります。

**ステップ 7** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

### What to do next

- [埋め込み/参照コンテンツのブロックの例外, on page 296](#)

### 埋め込み/参照コンテンツのブロックの例外

Web サイトに、別のカテゴリに分類されているコンテンツまたはアプリケーションとみなされるコンテンツが埋め込まれているか、参照している可能性があります。たとえば、ニュース Web サイトには、ストリーミングビデオとして分類され、アプリケーション YouTube と識別されるコンテンツが含まれることがあります。デフォルトでは、埋め込まれたコンテンツは、埋め込まれている Web サイトに関係なく、独自のカテゴリまたはアプリケーションに対して選択されたアクションに基づいてブロックまたは監視されます。この表を使用して、例外を設定します（たとえば、ニュース Web サイトまたはイントラネットを表すカスタムカテゴリから参照されるすべてのコンテンツを許可する場合）。



**Note** アプリケーション参照コンテンツの設定は、利用可能な Application Control Engine によって異なります。Application Control Engine が変更された場合は、アプリケーション参照コンテンツを確認してください。



**Note** 埋め込みコンテンツに対する要求には、通常、要求が発信されるサイトのアドレスが含まれます（要求の HTTP ヘッダーの「referer」フィールドとして知られています）。このヘッダー情報を使用して、参照コンテンツの分類が決定されます。

この機能を使用して、埋め込み/参照コンテンツのデフォルト アクションに対する例外を定義できます。たとえば、ニュース Web サイトまたはイントラネットを表すカスタム カテゴリのすべての埋め込み/参照コンテンツを許可することができます。



**Note** Referer ベースの例外は、アクセス ポリシーでのみサポートされます。HTTPS トラフィックでこの機能を使用するには、アクセス ポリシーで例外を定義する前に、例外用に選択する URL カテゴリの HTTPS 復号を設定する必要があります。HTTPS 復号の設定については、[復号ポリシー グループの URL フィルタの設定, on page 298](#)を参照してください。この機能と HTTPS 復号の使用に関する詳細については、[埋め込み/参照コンテンツのブロックの例外に対する条件および制約事項, on page 750](#)を参照してください。

## Procedure

- ステップ 1** 特定のアクセス ポリシーの [URL フィルタリング (URL Filtering)] ページ ([アクセス ポリシー グループの URL フィルタの設定, on page 294](#)を参照) で、[埋め込みおよび参照コンテンツのブロックの例外 (Exceptions to Blocking for Embedded/Referred Content)] セクションの [例外の有効化 (Enable Except)] をクリックします。
- ステップ 2** [これらのカテゴリごとに参照コンテンツの例外を設定 (Set Exception for Content Referred by These Categories)] 列の [クリックしてカテゴリを選択 (Click to select categories)] リンクをクリックして、URL フィルタリング カテゴリの参照の例外の選択ページを開きます。
- ステップ 3** [定義済みおよびカスタム URL カテゴリ (Predefined and Custom URL Categories)] リストから、この参照の例外を定義するカテゴリを選択し、[完了 (Done)] をクリックしてこのアクセス ポリシーの [URL フィルタリング (URL Filtering)] ページに戻ります。
- ステップ 4** [この参照コンテンツの例外を設定 (Set Exception for this Referred Content)] ドロップダウン リストから例外のタイプを選択します。
  - [すべての埋め込み/参照コンテンツ (All embedded/referred content)] : コンテンツのカテゴリに関係なく、指定したカテゴリ タイプのサイトのすべての埋め込み/参照コンテンツはブロックされません。
  - [選択した埋め込み/参照コンテンツ (Selected embedded/referred content)] : このオプションを選択した後、指定した URL カテゴリから発信された場合はブロックしない特定のカテゴリおよびアプリケーションを選択します。
  - [すべての埋め込み/参照コンテンツの例外 (All embedded/referred content except)] : このオプションを選択すると、ここで指定する URL カテゴリおよびアプリケーションを除いて、指定したカテゴリ タイプのサイトのすべての埋め込み/参照コンテンツはブロックされません。つまり、ここで指定するタイプはブロックされたままになります。

**Note**

[参照元の例外 (Referrer Exception)] オプションは、カスタム URL カテゴリがアクセスポリシーに含まれていない場合でもデフォルトで有効になっています。

**ステップ 5** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

**What to do next**

[レポート (Reporting)] ページ ([URL カテゴリ (URL Categories)], [ユーザー (Users)], および [Web サイト (Web Sites)] ) や [概要 (Overview)] ページの関連チャートに表示される表およびチャートに、「Referrer によって許可される」トランザクションデータを表示するように選択できます。チャート表示オプションの選択の詳細については、[チャート化するデータの選択](#), on page 583を参照してください。

## 復号ポリシー グループの URL フィルタの設定

ユーザー定義の復号ポリシー グループおよびグローバル復号ポリシー グループに対して URL フィルタリングを設定できます。

**Procedure**

**ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] > [復号ポリシー (Decryption Policies)] を選択します。

**ステップ 2** ポリシーテーブルで、編集するポリシー グループの [URL フィルタ (URL Filtering)] 列にあるリンクをクリックします。

**ステップ 3** (任意) [カスタム URL カテゴリのフィルタリング (Custom URL Category Filtering)] セクションで、このポリシーのアクションの実行対象となるカスタム URL カテゴリを追加できます。

- a) [カスタムカテゴリの選択 (Select Custom Categories)] をクリックします。
- b) このポリシーに含めるカスタム URL カテゴリを選択して、[適用 (Apply)] をクリックします。

URL フィルタリング エンジンでクライアント要求と照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンでは、クライアント要求と含まれているカスタム URL カテゴリを比較します。除外されたカスタム URL カテゴリは無視されます。URL フィルタリング エンジンでは、定義済みの URL カテゴリよりも前に、含まれているカスタム URL カテゴリとクライアント要求の URL を比較します。

ポリシーに含まれているカスタム URL カテゴリは、[カスタム URL カテゴリのフィルタリング (Custom URL Category Filtering)] セクションに表示されます。

**ステップ 4** カスタムおよび定義済みの各 URL カテゴリのアクションを選択します。

| アクション                              | 説明                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| グローバル設定を使用<br>(Use Global Setting) | <p>グローバル復号ポリシー グループで設定されているこのカテゴリ用のアクションを使用します。これは、ユーザー定義のポリシー グループのデフォルトアクションです。</p> <p>ユーザー定義のポリシー グループにのみ適用されます。</p> <p>カスタム URL カテゴリがグローバル復号ポリシーから除外されている場合、ユーザー定義の復号ポリシーに含まれているカスタム URL カテゴリのデフォルトアクションは、[グローバル設定を使用 (Use Global Settings)] でなく、[モニター (Monitor)] になります。カスタム URL カテゴリがグローバル復号ポリシーから除外されている場合は、[グローバル設定を使用 (Use Global Settings)] を選択できません。</p> |
| パススルー (Pass Through)               | トラフィック コンテンツを検査せずに、クライアントとサーバー間の接続をパススルーします。                                                                                                                                                                                                                                                                                                                       |
| モニター (Monitor)                     | Web プロキシは、要求を許可せず、ブロックもしません。代わりに、他のポリシー グループ制御設定 (Web レピュテーション フィルタリングなど) と照合して、クライアント要求の評価を続行します。                                                                                                                                                                                                                                                                 |
| 復号 (Decrypt)                       | 接続を許可しますが、トラフィック コンテンツを検査します。アプライアンスはトラフィックを復号し、プレーンテキスト HTTP 接続であるかのように、復号したトラフィックにアクセスポリシーを適用します。接続を復号し、アクセスポリシーを適用することにより、トラフィックをスキャンしてマルウェアを検出できます。                                                                                                                                                                                                            |
| ドロップ (Drop)                        | 接続をドロップし、サーバーに接続要求を渡しません。アプライアンスは接続をドロップしたことをユーザーに通知しません。                                                                                                                                                                                                                                                                                                          |

**Note**

HTTPS 要求の特定の URL カテゴリをブロックする場合は、復号ポリシー グループのその URL カテゴリを復号することを選択し、次に、アクセス ポリシー グループの同じ URL カテゴリをブロックすることを選択します。

**ステップ 5** [分類されてない URL (Uncategorized URLs)] セクションで、定義済みまたはカスタムの URL カテゴリに分類されない Web サイトへのクライアント要求に対して実行するアクションを選択します。

この設定により、URL カテゴリ セットの更新で生じた新規カテゴリとマージカテゴリのデフォルトアクションも決まります。

**ステップ 6** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## データ セキュリティ ポリシー グループの URL フィルタの設定

ユーザー定義のデータセキュリティポリシー グループおよびグローバルポリシー グループに対して URL フィルタリングを設定できます。

## Procedure

**ステップ 1** [Webセキュリティマネージャ (Web Security Manager) ]>[シスコデータセキュリティ (Cisco Data Security) ]を選択します。

**ステップ 2** ポリシーテーブルで、編集するポリシー グループの [URL フィルタ (URL Filtering) ]列にあるリンクをクリックします。

**ステップ 3** (任意) [カスタムURLカテゴリのフィルタリング (Custom URL Category Filtering) ]セクションで、このポリシーのアクションの実行対象となるカスタム URL カテゴリを追加できます。

- a) [カスタムカテゴリの選択 (Select Custom Categories) ]をクリックします。
- b) このポリシーに含めるカスタム URL カテゴリを選択して、[適用 (Apply) ]をクリックします。

URL フィルタリング エンジンでクライアント要求と照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンは、クライアント要求と含まれているカスタム URL カテゴリを比較します。除外されたカスタム URL カテゴリは無視されます。URL フィルタリング エンジンは、定義済みの URL カテゴリよりも前に、含まれているカスタム URL カテゴリとクライアント要求の URL を比較します。

ポリシーに含まれているカスタム URL カテゴリは、[カスタムURLカテゴリのフィルタリング (Custom URL Category Filtering) ]セクションに表示されます。

**ステップ 4** [カスタムURLカテゴリのフィルタリング (Custom URL Category Filtering) ]セクションで、各カスタム URL カテゴリのアクションを選択します。

| アクション                           | 説明                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| グローバル設定を使用 (Use Global Setting) | <p>グローバル ポリシー グループで設定されているこのカテゴリ用のアクションを使用します。これは、ユーザー定義のポリシー グループのデフォルト アクションです。</p> <p>ユーザー定義のポリシー グループにのみ適用されます。</p> <p>カスタム URL カテゴリがグローバルシスコデータセキュリティ ポリシーから除外されている場合、ユーザー定義のシスコ データセキュリティ ポリシーに含まれているカスタム URL カテゴリのデフォルト アクションは、[グローバル設定を使用 (Use Global Settings) ]でなく、[モニター (Monitor) ]になります。カスタム URL カテゴリがグローバルなシスコ データ セキュリティ ポリシーから除外されている場合は、[グローバル設定を使用 (Use Global Settings) ]を選択できません。</p> |
| 許可 (Allow)                      | <p>このカテゴリの Web サイトに対してアップロード要求を常に許可します。カスタム URL カテゴリにのみ適用されます</p> <p>許可された要求は以降のすべてのデータ セキュリティ スキャンをバイパスし、アクセス ポリシーに対して評価されます。</p> <p>この設定は信頼できる Web サイトに対してのみ使用してください。この設定は内部サイトに対して使用することをお勧めします。</p>                                                                                                                                                                                                  |

| アクション          | 説明                                                                                               |
|----------------|--------------------------------------------------------------------------------------------------|
| モニター (Monitor) | Web プロキシは、要求を許可せず、ブロックもしません。代わりに、他のポリシーグループ制御設定 (Web レピュテーションフィルタリングなど) と照合して、アップロード要求の評価を続行します。 |
| ブロック (Block)   | Web プロキシは、この設定に一致するトランザクションを拒否します。                                                               |

**Note**

ファイルサイズの上限を無効にしない場合、URL フィルタリングで [許可 (Allow)] または [モニター (Monitor)] オプションが選択されているときに、Secure Web Appliance で最大ファイルサイズの検証が続行されます。

**ステップ 5** [事前定義された URL カテゴリのフィルタリング (Predefined URL Category Filtering)] セクションで、各カテゴリに対して以下のいずれかのアクションを選択します。

- グローバル設定を使用 (Use Global Settings)
- モニター (Monitor)
- ブロック (Block)

**ステップ 6** [分類されてない URL (Uncategorized URLs)] セクションで、定義済み URL カテゴリにもカスタム URL カテゴリにも該当しない Web サイトへのアップロード要求に対して実行するアクションを選択します。この設定により、URL カテゴリ セットの更新で生じた新規カテゴリとマージカテゴリのデフォルト アクションも決まります。

**ステップ 7** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

**What to do next****関連項目**

- [URL カテゴリ セットの更新によるポリシーのフィルタリングアクションへの影響](#), on page 286。

## YouTube の分類

YouTube 分類機能により、YouTube のカスタム URL カテゴリを作成し、YouTube カスタムカテゴリに関するポリシーを設定することで、アクセスを保護および制御することができます。



(注) 特定の YouTube カテゴリをブロックする時間ベースのアクセスポリシールールを設定する場合：

- 設定した時間ベースのルールは、アクセスポリシーの設定時にすでに開かれて再生されているビデオには適用されません。
- ルールは、ルールを設定した後に新しく開いたビデオにのみ適用されます。



- (注)
- [googleapis.com](https://googleapis.com) がアップストリームプロキシまたはアップストリーム ファイアウォールでブロックされていないことを確認します。Cisco アップデートサーバーと WBNP テレメトリサーバーに例外を設定している場合は、[googleapis.com](https://googleapis.com) にも同様に設定します。
  - 次のビデオは、ブロックされる YouTube のカテゴリに属する場合でもブロックされません。
    - チャンネルの [studio.youtube.com](https://studio.youtube.com) ページに表示されるビデオサムネイル。
    - Google の検索結果に表示されるビデオサムネイル。
    - YouTube ショート ビデオ カテゴリが断続的に機能しなくなる場合があります。

YouTube 分類機能を設定するには、次の作業を実行します。

| 手順 | タスク                                                                                                                                                | トピックおよび手順へのリンク                                       |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| 1. | <a href="https://www.youtube.com">www.youtube.com</a> と <a href="https://m.youtube.com">m.youtube.com</a> を使用して、YouTube のカスタムおよび外部 URL カテゴリを作成します。 | <a href="#">カスタム URL カテゴリの作成および編集 (305 ページ)</a> 。    |
| 2. | YouTube のカスタムおよび外部 URL カテゴリを復号ポリシーに追加します。                                                                                                          | <a href="#">復号ポリシー グループの URL フィルタの設定 (298 ページ)</a> 。 |
| 3. | YouTube 分類機能を有効にします。                                                                                                                               | <a href="#">YouTube 分類機能の有効化 (303 ページ)</a> 。         |

| 手順 | タスク                                         | トピックおよび手順へのリンク                                                                                                                                                                                                                       |
|----|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4. | YouTube のカスタムおよび外部 URL カテゴリにアクセスポリシーを適用します。 | <a href="#">アクセス ポリシー グループの URL フィルタの設定 (294 ページ)</a> 。<br><br>(注)<br>[アクセスポリシー (Access Policies)] > [URLフィルタリング (URL Filtering)] ページの [YouTubeカテゴリのフィルタリング (YouTube Category Filtering)] セクションで、「ブロック、モニター、または警告」アクションを設定する必要があります。 |

## YouTube 分類機能の有効化

### 始める前に

- HTTPS プロキシを有効にします ([セキュリティサービス (Security Services)] > [HTTPS プロキシ (HTTPS Proxy)])。
- [使用許可コントロール (Acceptable Use Controls)] を有効にします ([セキュリティサービス (Security Services)] > [使用許可コントロール (Acceptable Use Controls)])。
- www.youtube.com と m.youtube.com を使用してカスタムおよび外部 URL カテゴリを設定します ([Webセキュリティマネージャ (Web Security Manager)] > [カスタムおよび外部URL カテゴリ (Custom and External URL Categories)])。
- YouTube のカスタム URL カテゴリと外部 URL カテゴリを使用し、アクションを [復号 (decrypt)] にして復号ポリシーを設定します。
- YouTube 用の Google API サービスを使用して Google API キーを生成します。Google API キーを生成するには、次の手順を実行します。
  1. Google アカウントのクレデンシャルを使用して <https://console.developers.google.com/> にログインします (個人の Google アカウントの使用は推奨されません)。
  2. プロジェクトを作成します。
  3. [API とサービスの有効化 (Enable APIs and Services)] で、[YouTube Data API v3] を有効にします。
  4. ウィザードを使用して API キーを生成するか、または [API とサービス (APIs & Services)] の下にある [クレデンシャル (Credentials)] オプションを使用します。





- (注) ウィザードを使用して API キーを生成するには、[YouTube Data API v3] で次の手順を実行します。
1. [APIの呼び出し元 (Where will you be calling the API from?) ] ドロップダウンリストから、[その他の非UI (Other non-UI) ] (cron job、daemon など) を選択します。
  2. [アクセスするデータ (What data will you be accessing) ] セクションで、[パブリックデータ (Public data) ] を選択します。
  3. [必要なクレデンシヤル (What credentials do I need?) ] をクリックし、次に [完了 (Done) ] をクリックします。

## 手順

**ステップ 1** [セキュリティ サービス (Security Services) ] > [使用許可コントロール (Acceptable Use Controls) ] を選択します。

**ステップ 2** [グローバル設定を編集 (Edit Global Settings) ] をクリックします。

**ステップ 3** YouTube の分類の横にある [有効化 (Enable) ] チェックボックスをオンにします。

**ステップ 4** Google API サービスを使用して生成した API キーを入力します。

YouTube 分類機能を有効にする前に、Google API サービスを使用して API キーを生成する必要があります。

**ステップ 5** クエリタイムアウトを入力して、アプライアンスと YouTube API サーバー間のタイムアウト期間を設定します。

**ステップ 6** YouTube カテゴリトラフィックが通過するルーティングテーブルを選択します。

- データ (Data) : P1 および P2 インターフェイス用
- 管理 (Management) : M1 インターフェイス用

(注)

デフォルトのルーティングテーブルはデータです。上記の 2 つのオプションは、データと管理サービス用に 2 つの個別のルーティングテーブルを設定した場合にのみ使用できます ([ネットワーク (Network) ] > [インターフェイス (Interfaces) ]) 。

**ステップ 7** 変更を送信し、保存します。

## カスタム URL カテゴリの作成および編集

特定のホスト名と IP アドレスを指定する、カスタムおよび外部のライブフィード URL カテゴリを作成できます。また、既存の URL カテゴリを編集したり削除することができます。これらのカスタム URL カテゴリを同じアクセスポリシーグループ、復号ポリシーグループ、またはシスコデータセキュリティポリシーグループに含めて、各カテゴリに異なるアクションを割り当てると、より上位のカスタム URL カテゴリのアクションが優先されます。

**Note**

これらの URL カテゴリ定義で利用できる外部ライブフィードファイルは 30 までに制限されており、各ファイルに格納できるエントリ数は最大 5000 です。外部フィードエントリを増やしたり、正規表現エントリの数が膨大になったりすると、パフォーマンスの低下につながります。

Secure Web Appliance では、先頭に文字「c\_」が付加されたカスタム URL カテゴリ名の最初の 4 文字が、アクセスログで使用されます。Sawmill を使用してアクセスログを解析する場合は、カスタム URL カテゴリの名前に注意してください。カスタム URL カテゴリの最初の 4 文字にスペースが含まれていると、Sawmill はアクセスログエントリを正しく解析できません。代わりに、最初の 4 文字にはサポートされる文字のみを使用します。カスタム URL カテゴリの完全な名前をアクセスログに記録する場合は、%XF フォーマット指定子をアクセスログに追加します。

**Note**

DNS が複数の IP を Web サイトに解決し、それらの IP の 1 つがカスタムブロックリストに登録されている場合、Secure Web Appliance はカスタムブロックリストへの登録の有無にかかわらずすべての IP の Web サイトをブロックします。

**Before you begin**

[セキュリティ サービス (Security Services)] > [使用許可コントロール (Acceptable Use Controls)] に移動し、使用許可コントロールをイネーブルにします。

**Procedure**

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] > [カスタムおよび外部 URL カテゴリ (Custom and External URL Categories)] を選択します。
- ステップ 2** カスタム URL カテゴリを作成するには、[カテゴリを追加 (Add Category)] をクリックします。既存のカスタム URL カテゴリを編集するには、URL カテゴリの名前をクリックします。
- ステップ 3** 次の情報を入力します。

| 設定                          | 説明                                                                                                                                                                                                  |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| カテゴリ名<br>(Category Name)    | この URL カテゴリの識別子を入力します。この名前は、ポリシー グループに URL フィルタリングを設定するときに表示されます。                                                                                                                                   |
| リスト順 (List Order)           | カスタム URL カテゴリのリストで、このカテゴリの順序を指定します。リスト内の最初の URL カテゴリに「1」を入力します。<br><br>URL フィルタリング エンジンでは、指定した順序でカスタム URL カテゴリに対してクライアント要求が評価されます。                                                                  |
| カテゴリ タイプ<br>(Category Type) | [ローカル カスタム カテゴリ (Local Custom Category)] または [外部ライブフィード カテゴリ (External Live Feed Category)] を選択します。                                                                                                 |
| 着信サービス一覧<br>(Routing Table) | [管理 (Management)] または [データ (Data)] を選択します。この選択は、「分割ルーティング」が有効にされている場合にのみ行うことができます。つまり、ローカル カスタム カテゴリでは選択できません。分割ルーティングの有効化については、 <a href="#">ネットワーク インターフェイスのイネーブル化または変更, on page 37</a> を参照してください。 |

| 設定                                                     | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サイト/フィード<br>ファイルの場所<br>(Sites / Feed File<br>Location) | <p>[カテゴリ タイプ (Category Type)] で [ローカル カスタム カテゴリ (Local Custom Category)] を選択した場合、カスタム [サイト (Sites)] を指定します。</p> <ul style="list-style-type: none"> <li>• このカスタム カテゴリのサイトアドレスを1つまたは複数入力します。複数のアドレスは、改行またはカンマで区切って入力します。これらのアドレスの形式は、次のいずれかにします。 <ul style="list-style-type: none"> <li>• IPv4 アドレス。10.1.1.0 など</li> <li>• IPv6 アドレス。2001:0db8:: など</li> <li>• IPv4 CIDR アドレス。10.1.1.0/24 など</li> <li>• IPv6 CIDR アドレス。2001:0db8::/32 など</li> <li>• ドメイン名。example.com など</li> <li>• ホスト名。crm.example.com など</li> </ul> </li> <li>• .example.com などのドットで始まる部分的なホスト名は、ドメインのすべてのサブドメイン (www.example.com、mail.example.com など) と一致しますが、ルートドメイン自体 (example.com) とは一致しません。ルートドメインとそのサブドメインの両方を含めるには、example.com と .example.com の両方を指定します。</li> <li>• 正規表現は、次に示すように [詳細設定 (Advanced)] セクションで入力できます。</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Cisco Secure Web Appliance では、サイトのアドレスに非 ASCII 文字を使用できません。</li> <li>• 複数のカスタム URL カテゴリで同じアドレスを使用することは可能ですが、カテゴリがリストされる順序は相互関係によります。同じポリシーにこれらのカテゴリを含めて、それぞれに異なるアクションを定義する場合、カスタム URL カテゴリ テーブルの1番上にリストされるカテゴリに定義されたアクションが適用されます。</li> </ul> <ul style="list-style-type: none"> <li>• (オプション) [URLのソート (Sort URLs)] をクリックして、[サイト (Sites)] フィールド内のすべてのアドレスをソートします。</li> </ul> <p><b>Note</b><br/>アドレスをソートした後は、元の順序に戻すことができません。</p> |

| 設定    | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 除外サイト | <p>[カテゴリタイプ (Category Type)] に [外部ライブフィードカテゴリ (External Live Feed Category)] を選択した場合は、既存のフィードファイルから除外するサイトを入力します。複数のアドレスは、改行またはカンマで区切って入力します。これらのアドレスの形式は、次のいずれかにします。</p> <ul style="list-style-type: none"><li>• IPv6 アドレス (2001:0db8::/32 など)</li><li>• IPv4 アドレス (10.1.1.0 など)</li><li>• CIDR IPv6 アドレス (2001:0db8::/32 など)</li><li>• CIDR IPv4 アドレス (10.1.1.0/24 など)</li><li>• ドメイン名。example.com など</li><li>• ホスト名。crm.example.com など</li><li>• .example.com などのドットで始まる部分的なホスト名は、ドメインのすべてのサブドメイン (www.example.com、mail.example.com など) と一致しますが、ルートドメイン自体 (example.com) とは一致しません。ルートドメインとそのサブドメインの両方を含めるには、example.com と .example.com の両方を指定します。</li></ul> |

| 設定                                 | 説明 |
|------------------------------------|----|
| フィードの場所<br>(Feed Location)<br>(続き) |    |

| 設定 | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>[カテゴリ タイプ (Category Type)] に [外部ライブフィードカテゴリ (External Live Feed Category)] を選択した場合、[フィードファイルの場所 (Feed File Location)] 情報を入力します。つまり、このカスタムカテゴリのアドレスが含まれるファイルの場所を指定して、そのファイルをダウンロードします。</p> <p>a. [シスコのフィード形式 (Cisco Feed Format)] または [Office 365のフィード形式 (Office 365 Feed Format)]、または [Office 365 Webサービス (Office 365 Web Service)] を選択してから、適切なフィードファイルの情報を入力します。</p> <ul style="list-style-type: none"> <li>• [シスコのフィード形式 (Cisco Feed Format)] : <ul style="list-style-type: none"> <li>• 使用するトランスポート プロトコル (HTTPS または HTTP) を選択してから、ライブフィードファイルの URL を入力します。このファイルはカンマ区切り値 (.csv) 形式のファイルでなければなりません。このファイルの詳細については、<a href="#">外部フィードファイルの形式, on page 313</a>を参照してください。</li> <li>• 必要に応じて、[詳細設定 (Advanced)] セクションの [認証 (Authentication)] にクレデンシャルを入力します。指定したフィードサーバに接続するために使用するユーザ名とパスワードを入力します。</li> </ul> </li> <li>• [Office 365 のフィード形式 (Office 365 Feed Format)] : <ul style="list-style-type: none"> <li>• [Office 365 フィードの場所 (Office 365 Feed Location)] に、ライブフィードファイルの場所 (URL) を入力します。</li> </ul> <p>このファイルは、XML ファイル形式でなければなりません。このファイルの詳細については、<a href="#">外部フィードファイルの形式, on page 313</a>を参照してください。</p> </li> <li>• <b>Office 365 Webサービス (Office 365 Web Service)</b> <p>Web サービスの URL を入力します。ClientRequestId が含まれておらず、JSON 形式である必要があります。アプライアンスは ClientRequestId を自動的に生成します。</p> </li> </ul> <p>b. [シスコのフィード形式 (Cisco Feed Format)] および [Office 365のフィード形式 (Office 365 Feed Format)] の場合は、[ファイルの取得 (Get File)] をクリックして、フィードサーバとの接続をテストし、フィードファイルを解析してサーバからダウンロードします。</p> <p>[ファイルの取得 (Get File)] ボタンの下にあるテキスト ボックスに、進捗状況が表示されます。エラーが発生した場合は、その問題が示されるので、問題を修正してから再試行します。発生する可能性のあるエラーについては、<a href="#">外部ライブフィードファイルのダウンロードに関する問題, on page 755</a>を参照してください。</p> <p>[Office 365 Webサービス (Office 365 Web Service)] の場合は、[テスト開始 (Start Test)] をクリックし、サービスを開始して URL および IP をダウンロードします。</p> |

| 設定                 | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <p><b>Note</b><br/>これらの URL カテゴリ定義で利用できる外部ライブフィードは最大 30 です。また、各ファイルに格納できるエントリ数は最大 5000 に制限されています。外部フィードエントリを増やすと、パフォーマンスの低下につながります。</p> <p><b>Tip</b><br/>ライブフィード カテゴリの変更を保存した後、[カスタムおよび外部 URL カテゴリ (Custom and External URL Categories) ] ページ ([Web セキュリティ マネージャ (Web Security Manager) ] &gt; [カスタムおよび外部 URL カテゴリ (Custom and External URL Categories) ]) の [フィードの内容 (Feed Content) ] 列でこのエントリに対応する [表示 (View) ] をクリックすると、ダウンロードしたシスコ フィード形式または Office 365 フィード形式のファイルに含まれているアドレスを表示するウィンドウが開きます。</p>                                                                                                                       |
| 詳細設定<br>(Advanced) | <p>[カテゴリ タイプ (Category Type) ] に [ローカル カスタム カテゴリ (Local Custom Category) ] を選択した場合、このセクションに、追加のアドレスセットを指定する正規表現を入力できます。</p> <p>正規表現を使用して、入力したパターンと一致する複数のアドレスを指定できます。</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• URL フィルタリング エンジンでは、まず [サイト (Sites) ] フィールドに入力したアドレスと URL が比較されます。トランザクションの URL が [サイト (Sites) ] フィールドの入力値と一致した場合は、ここで入力した式との比較は行われません。</li> <li>• URL パスを正規表現として追加するときは、スペース文字の代わりに「%20」を使用します。正規表現として使用する場合、URL パスにスペース文字を含めることはできません。</li> <li>• Cisco Secure Web Appliance では、正規表現に非 ASCII 文字を使用できません。</li> </ul> <p>正規表現の使用方法については、<a href="#">正規表現, on page 321</a> を参照してください。</p> |
| 詳細設定 (正規表現の除外)     | <p>[カテゴリタイプ (Category Type) ] に [外部ライブフィードカテゴリ (External Live Feed Category) ] を選択した場合は、既存のフィード ファイルから除外する正規表現を入力します。エントリは、フィードファイルの既存の正規表現と正確に一致する必要があります。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



| 設定                               | 説明                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フィードの自動更新 (Auto Update the Feed) | <p>フィードの更新オプションを選択します。</p> <ul style="list-style-type: none"> <li>• <b>[自動更新しない (Do not auto update) ]</b></li> <li>• <b>[n HH:MM 間隔 (Every n HH:MM) ]</b>。たとえば、5 分間隔の場合は <b>00:05</b> と入力します。ただし、頻繁に更新すると <b>Secure Web Appliance</b> のパフォーマンスに影響することに注意してください。</li> </ul> <p><b>Note</b><br/>リロードして再公開するたびに、使用可能なフィードファイルが現在ダウンロードされているファイルと同じであっても、アプライアンスは使用可能なフィードファイルをダウンロードし、ダウンロード時間を更新します。</p> |

**ステップ 4** 変更を送信して確定します ([送信 (Submit) ] と [変更を確定 (Commit Changes) ])。

### What to do next

#### 関連項目

- [正規表現, on page 321](#)。
- [アクセス ログのカスタマイズ, on page 714](#)。
- [カスタム URL カテゴリおよび外部 URL カテゴリに関する問題, on page 755](#)

## カスタムおよび外部 URL カテゴリのアドレス形式とフィード ファイル形式

カスタムおよび外部 URL カテゴリを作成および編集する場合は、1 つ以上のネットワーク アドレスを指定する必要があります。ローカル カスタム カテゴリのアドレスを指定するのか、それとも外部ライブフィードカテゴリのフィードファイル形式で指定するのかは問いません。各インスタンスでは、複数のアドレスを改行またはカンマで区切って入力することがあります。これらのアドレスの形式は、次のいずれかにします。

- IPv4 アドレス。10.1.1.0 など
- IPv6 アドレス。2001:0db8:: など
- IPv4 CIDR アドレス。10.1.1.0/24 など
- IPv6 CIDR アドレス。2001:0db8::/32 など
- ドメイン名。example.com など
- ホスト名。crm.example.com など
- .example.com などのドットで始まる部分的なホスト名は、ドメインのすべてのサブドメイン (www.example.com、mail.example.com など) と一致しますが、ルートドメイン自体

(example.com) とは一致しません。ルートドメインとそのサブドメインの両方を含めるには、example.com と .example.com の両方を指定します。

- 指定したパターンと一致する複数のアドレスを指定する正規表現（正規表現の仕様の詳細については、[正規表現](#)（321 ページ）を参照）



- (注) 複数のカスタム URL カテゴリで同じアドレスを使用することは可能ですが、カテゴリがリストされる順序は相互関係によります。同じポリシーにこれらのカテゴリを含めて、それぞれに異なるアクションを定義する場合、カスタム URL カテゴリ テーブルの 1 番上にリストされるカテゴリに定義されたアクションが適用されます。

## 外部フィードファイルの形式

カスタム カテゴリおよび外部の URL カテゴリを作成および編集する場合に、[カテゴリタイプ (Category Type)] で [外部ライブ フィード カテゴリ (External Live Feed Category)] を選択する場合は、フィード形式 ([シスコフィード形式 (Cisco Feed Format)] または [Office 365 フィード形式 (Office 365 Feed Format)]) を選択して、該当するフィードファイル サーバの URL を指定する必要があります。

フィードファイルごとに予測される形式は、次のとおりです。

- シスコフィード形式 (Cisco Feed Format) : カンマ区切り値 (.csv) ファイル (.csv 拡張子の付いたテキストファイル) を指定する必要があります。 .csv ファイルの各エントリは、アドレス/カンマ/アドレスタイプの形式で、独立した行に記述する必要があります (www.cisco.com,site や ad2.\*\com,regex など)。有効なアドレスタイプは site と regex です。次に、シスコ フィード形式の .csv ファイルの一部を示します。

```
www.cisco.com,site
\ .xyz,regex
ad2.*\com,regex
www.trafficholder.com,site
2000:1:1:11:1:1::200,site
```



- (注) ファイル内の site エントリの一部として http:// または https:// を含めないでください。エラーが発生します。つまり、www.example.com は正しく解析されますが、http://www.example.com ではエラーが発生します。

- Office 365 フィード形式 (Office 365 Feed Format) : Microsoft Office 365 サーバ、または保存先のローカル サーバに配置された XML ファイルです。Office 365 サービスが提供するもので、変更することはできません。ファイル内のネットワーク アドレスは、products > product > addresslist > address の構造に従う XML タグで囲まれます。現在の実装では

addresslist 型には IPv6、IPv4、または URL（ドメインや正規表現を含むことも可）を指定できます。次に、Office 365 フィード ファイルのスニペットを示します。

```
<products updated="4/15/2016">

 <product name="o365">

 <addresslist type="IPv6">

 <address>2603:1040:401::d:80</address>

 <address>2603:1040:401::a</address>

 <address>2603:1040:401::9</address>

 </addresslist>

 <addresslist type="IPv4">

 <address>13.71.145.72</address>

 <address>13.71.148.74</address>

 <address>13.71.145.114</address>

 </addresslist>

 <addresslist type="URL">

 <address>*.aadrm.com</address>

 <address>*.azurerms.com</address>

 <address>*.cloudapp.net2</address>

 </addresslist>

 </product>

 <product name="LYO">

 <addresslist type="URL">

 <address>*.broadcast.skype.com</address>

 <address>*.Lync.com</address>

 </addresslist>

 </product>

</products>
```

## アダルトコンテンツのフィルタリング

一部の Web 検索や Web サイトからアダルトコンテンツをフィルタリングするように、Secure Web Applianceを設定できます。AVC エンジン、URL や Web クッキーを書き換えてセーフモードを有効化することで、特定の Web サイトに実装されているセーフモード機能を利用し、セーフサーチやサイトコンテンツレーティングを適用します。

以下の機能によってアダルトコンテンツをフィルタリングします。

| オプション                                            | 説明                                                                                                                                             |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| セーフサーチの適用 (Enforce safe searches)                | 発信検索要求がセーフサーチ要求として検索エンジンに表示されるように、Secure Web Applianceを設定することができます。これにより、ユーザーが検索エンジンを使用して使用許可ポリシーを回避するのを防止できます。                                |
| サイトコンテンツレーティングの適用 (Enforce site content ratings) | 一部のコンテンツ共有サイトでは、独自のセーフサーチ機能を適用するか、アダルトコンテンツへのアクセスをブロックするか、または両方を実行することによって、サイトのアダルトコンテンツへのユーザーによるアクセスを制限しています。この分類機能は、一般的にコンテンツレーティングと呼ばれています。 |



**Note** セーフサーチ機能またはサイトコンテンツレーティング機能がイネーブルになっているアクセスポリシーは、安全なブラウジングアクセスポリシーと見なされます。

## セーフサーチおよびサイトコンテンツレーティングの適用



**Note** セーフサーチおよびサイトコンテンツレーティングを有効にすると、安全に参照するために、AVCエンジンがアプリケーションを識別する役割を果たすようになります。条件の1つとして、AVCエンジンは応答本文をスキャンし、検索アプリケーションを検出します。その結果、アプライアンスは範囲ヘッダーを転送しません。

### Procedure

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] > [アクセス ポリシー (Access Policies)] を選択します。
- ステップ 2** [URL フィルタリング (URL Filtering)] 列にある、アクセス ポリシー グループまたはグローバル ポリシー グループのリンクをクリックします。
- ステップ 3** ユーザー定義のアクセス ポリシーを編集する場合、[コンテンツ フィルタ (Content Filtering)] セクションの [コンテンツ フィルタ カスタム設定を定義 (Define Content Filtering Custom Settings)] を選択します。
- ステップ 4** [セーフサーチを有効にする (Enable Safe Search)] チェックボックスをオンにして、セーフサーチ機能をイネーブルにします。
- ステップ 5** Secure Web Applianceのセーフサーチ機能で現在サポートされていない検索エンジンからユーザをブロックするかどうかを選択します。

**ステップ 6** [サイトコンテンツ評価を有効にする (Enable Site Content Rating)] チェックボックスをオンにして、サイト コンテンツ レーティング機能をイネーブルにします。

**ステップ 7** サポート対象のコンテンツ レーティング Web サイトからのアダルトコンテンツをすべてブロックするか、エンドユーザー URL フィルタリング警告ページを表示するかを選択します。

**Note**

サポート対象のいずれかの検索エンジンの URL、またはサポート対象のいずれかのコンテンツ レーティング Web サイトの URL が、[許可 (Allow)] アクションが適用されているカスタム URL カテゴリに含まれている場合、検索結果はブロックされず、すべてのコンテンツが表示されます。

**ステップ 8** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## What to do next

### 関連項目

- [ユーザーへの警告と続行の許可, on page 318.](#)

## アダルト コンテンツ アクセスのロギング

デフォルトでは、アクセス ログには安全なブラウジング スキャンの判定が含まれており、判定は各エントリの山カッコ内に記載されています。安全なブラウジング スキャンの判定は、セーフ サーチまたはサイト コンテンツ レーティング機能がトランザクションに適用されているかどうかを示します。安全なブラウジング スキャンの判定変数をアクセス ログや W3C アクセス ログに追加することもできます。

- アクセス ログ : %XS
- W3C アクセス ログ : x-request-rewrite

| 値      | 説明                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------|
| ensrch | 元のクライアント要求が安全ではなく、セーフ サーチ機能が適用されました。                                                                                               |
| enrt   | 元のクライアント要求が安全ではなく、サイト コンテンツ レーティング機能が適用されました。                                                                                      |
| unsupp | 元のクライアント要求がサポートされていない検索エンジン向けでした。                                                                                                  |
| err    | 元のクライアント要求は安全ではありませんが、エラーのためにセーフ サーチ機能もサイト コンテンツ レーティング機能も適用されませんでした。                                                              |
| -      | 機能がバイパスされたため (トランザクションがカスタム URL カテゴリで許可された場合など)、またはサポートされていないアプリケーションで要求が実行されたため、セーフ サーチ機能もサイト コンテンツ レーティング機能もクライアント要求に適用されませんでした。 |

セーフ サーチまたはサイト コンテンツ レーティング機能によってブロックされた要求には、アクセス ログで以下のいずれかの ACL デシジョン タグが使用されます。

- BLOCK\_SEARCH\_UNSAFE
- BLOCK\_CONTENT\_UNSAFE
- BLOCK\_UNSUPPORTED\_SEARCH\_APP
- BLOCK\_CONTINUE\_CONTENT\_UNSAFE

#### 関連項目

- [ACL デシジョン タグ, on page 692。](#)

## アクセス ポリシーでのトラフィックのリダイレクト

最初の宛先がカスタム URL カテゴリの URL であるトラフィックを指定する場所にリダイレクトするように Secure Web Applianceを設定できます。これにより、宛先サーバーではなく、アプライアンスでトラフィックをリダイレクトできます。カスタム アクセス ポリシー グループまたはグローバル ポリシー グループのトラフィックをリダイレクトできます。

#### Before you begin

トラフィックをリダイレクトするには、少なくとも 1 つのカスタム URL カテゴリを定義する必要があります。

#### Procedure

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager) ] > [アクセス ポリシー (Access Policies) ] を選択します。
- ステップ 2** [URL フィルタリング (URL Filtering) ] 列にある、アクセス ポリシー グループまたはグローバル ポリシー グループのリンクをクリックします。
- ステップ 3** [カスタム URL カテゴリのフィルタリング (Custom URL Category Filtering) ] セクションで、[カスタム カテゴリの選択 (Select Custom Categories) ] をクリックします。
- ステップ 4** [このポリシーのカスタムカテゴリを選択 (Select Custom Categories for this Policy) ] ダイアログボックスで、リダイレクトするカスタム URL カテゴリに対して [ポリシーに含める (Include in policy) ] を選択します。
- ステップ 5** [適用 (Apply) ] をクリックします。
- ステップ 6** リダイレクトするカスタム カテゴリの [リダイレクト (Redirect) ] 列をクリックします。
- ステップ 7** [リダイレクト先 (Redirect to) ] フィールドにトラフィックのリダイレクト先の URL を入力します。
- ステップ 8** 変更を送信して確定します ([送信 (Submit) ] と [変更を確定 (Commit Changes) ]) 。

#### Note

トラフィックをリダイレクトするようにアプライアンスを設定する場合は、無限ループにならないように注意してください。

#### What to do next

#### 関連項目

- [カスタム URL カテゴリの作成および編集, on page 305](#)

## ロギングとレポート

トラフィックをリダイレクトすると、本来の要求対象である Web サイトのアクセス ログ エントリに REDIRECT\_CUSTOMCAT から始まる ACL タグが付けられます。以降、アクセス ログ（通常は次の行）にリダイレクト先の Web サイトのエントリが表示されます。

[レポート (Reporting)] タブに表示されるレポートでは、リダイレクトされたトランザクションは [許可 (Allowed)] と示されます。

## ユーザーへの警告と続行の許可

サイトが組織の利用規定を満たしていないことをユーザーに警告できます。認証によりユーザー名が使用可能になっている場合、アクセスログではユーザー名によってユーザーが追跡され、ユーザー名が使用できない場合は IP アドレスによって追跡されます。

以下のいずれかの方法を使用して、ユーザーに警告したり、続行を許可することができます。

- アクセス ポリシー グループの URL カテゴリに対して [警告 (Warn)] アクションを選択します。または
- サイト コンテンツ レーティング機能をイネーブルにして、アダルト コンテンツにアクセスするユーザーをブロックする代わりに、ユーザーに警告します。

## [エンドユーザー フィルタリング警告 (End-User Filtering Warning)] ページの設定



### Note

- 「警告して継続」機能は、HTTP トランザクションと復号された HTTPS トランザクションに対してのみ機能します。ネイティブ FTP トランザクションでは機能しません。
- URL フィルタリング エンジン、特定の要求についてユーザーに警告する場合に、Web プロキシがエンドユーザーに送信する警告ページを提供します。ただし、すべての Web サイトでエンドユーザーに警告ページが表示されるわけではありません。表示されない場合、ユーザーは [警告 (Warn)] オプションが割り当てられている URL からブロックされます。引き続きそのサイトにアクセスするチャンスは与えられません。

## Procedure

**ステップ 1** [セキュリティ サービス (Security Services)] > [ユーザー通知 (End-User Notification)] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** [エンドユーザー フィルタリング警告 (End-User Filtering Warning)] ページで以下の設定項目を設定します。

| オプション                          | 方法                                                                                                                                                                                                                                                                            |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 警告の時間間隔 (Time Between Warning) | <p>[警告の時間間隔 (Time Between Warning)] では、Web プロキシが、ユーザーごとに各 URL カテゴリに対して、[エンドユーザー フィルタリング警告 (End-User Filtering Warning)] ページを表示する頻度を指定します。</p> <p>この設定は、ユーザー名によって追跡されるユーザーと IP アドレスによって追跡されるユーザーに適用されます。</p> <p>30 ～ 2678400 秒 (1 か月) の任意の値を指定します。デフォルトは 1 時間 (3600 秒) です。</p> |
| カスタム メッセージ (Custom Message)    | <p>カスタムメッセージは、ユーザーによって入力されるテキストであり、すべての [エンドユーザーフィルタリング警告 (End-User Filtering Warning)] ページに表示されます。</p> <p>いくつかの単純な HTML タグを組み込み、テキストを書式設定できます。</p>                                                                                                                           |

**ステップ 4** [送信 (Submit)] をクリックします。

#### What to do next

##### 関連項目

- [アダルト コンテンツのフィルタリング, on page 314](#)
- [通知ページ上のカスタム メッセージ, on page 545](#)
- [エンドユーザー URL フィルタリング警告ページの設定, on page 544](#)

## 時間ベースの URL フィルタの作成

Secure Web Applianceが特定のカテゴリの URL の要求を日時別に処理する方法を設定できます。

#### Before you begin

[Web セキュリティ マネージャ (Web Security Manager)] > [定義済み時間範囲 (Defined Time Range)] に移動し、1 つ以上の時間範囲を定義します。

#### Procedure

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] > [アクセス ポリシー (Access Policies)] を選択します。
- ステップ 2** ポリシー テーブルで、編集するポリシー グループの [URL フィルタ (URL Filtering)] 列にあるリンクをクリックします。
- ステップ 3** 時間範囲に基づいて設定する URL カテゴリ (カスタムまたは定義済み) に対して、[時間ベース (Time-Based)] を選択します。



- ステップ 4** [時間範囲内 (In Time Range)] フィールドで、URL カテゴリに使用する定義済みの時間範囲を選択します。
- ステップ 5** [アクション (Action)] フィールドで、定義した時間範囲内でこの URL カテゴリのトランザクションに割り当てるアクションを選択します。
- ステップ 6** [それ以外の場合 (Otherwise)] フィールドで、定義した時間範囲外でこの URL カテゴリのトランザクションに割り当てるアクションを選択します。
- ステップ 7** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

### What to do next

#### 関連項目

- [時間範囲およびクォータ, on page 389](#)

## URL フィルタリング アクティビティの表示

[レポート (Reporting)] > [URL カテゴリ (URL Categories)] ページには、一致した上位の URL カテゴリとブロックされた上位の URL カテゴリに関する情報を含む、総合的な URL 統計情報が表示されます。また、帯域幅の節約と Web トランザクションに関するカテゴリ固有のデータも表示されます。

#### 関連項目

- [エンドユーザーのアクティビティをモニターするレポートの生成, on page 579](#)

## フィルタリングされない未分類のデータについて

[レポート (Reporting)] > [URL カテゴリ (URL Categories)] ページで URL 統計情報を検討する際は、以下のデータの解釈方法を理解しておくことが大切です。

| データ タイプ                                   | 説明                                                      |
|-------------------------------------------|---------------------------------------------------------|
| URL フィルタリングのバイパス (URL Filtering Bypassed) | URL フィルタリングの前に実行されるポリシー、ポートおよび管理ユーザ エージェントのブロッキングを示します。 |
| 分類されてないURL (Uncategorized URL)            | URL フィルタリングエンジンに照会したが、カテゴリが一致しなかったすべてのトランザクションを表しています。  |

## アクセス ログへの URL カテゴリの記録

アクセス ログ ファイルでは、各エントリのスキャン判定情報セクションにトランザクションの URL カテゴリが記録されます。

#### 関連項目

- [ログによるシステム アクティビティのモニター, on page 665。](#)

- [URL カテゴリについて, on page 325。](#)

## 正規表現

Secure Web Applianceで使用される正規表現構文は、他の Velocity パターン マッチング エンジンの実装で使用する正規表現構文とはやや異なっています。また、アプライアンスは、バックスラッシュによるスラッシュのエスケープはサポートしていません。正規表現でスラッシュを使用する必要がある場合は、バックスラッシュなしでスラッシュを入力します。



**Note** 技術的には、AsyncOS for Web では Flex 正規表現アナライザが使用されています。

正規表現は以下の個所で使用できます。

- **アクセス ポリシーのカスタム URL カテゴリ。**アクセス ポリシー グループで使用するカスタム URL カテゴリを作成する際は、正規表現を使用して、入力パターンと一致する複数の Web サーバを指定できます。正規表現で使用する最大文字数は、Web セキュリティの脆弱性を制限するため、2048 文字に設定されています。
- **ブロックするカスタム ユーザ エージェント。**アクセス ポリシー グループをブロックするようにアプリケーションを編集する際は、ブロックする特定のユーザエージェントを正規表現を使用して入力できます。



**Note** 広範な文字照合を実行する正規表現はリソースを消費し、システムパフォーマンスに影響を与える可能性があります。したがって、正規表現は慎重に適用する必要があります。

### 関連項目

- [カスタム URL カテゴリの作成および編集, on page 305](#)

## 正規表現の形成

正規表現は、一般的に、表現における「一致」を利用するルールです。これらを適用することで、特定の URL 宛先や Web サーバーに一致させることができます。たとえば、以下の正規表現は blocksite.com を含むパターンに一致します。

```
\.blocksite\.com
```

以下の正規表現の例を考えてください。

```
server[0-9]\.example\.com
```

この例では、`server[0-9]` は `example.com` ドメインの `server0`、`server1`、`server2`、...、`server9` と一致します。

以下の例では、正規表現は `downloads` ディレクトリ内の `.exe`、`.zip`、`bin` で終わるファイルに一致します。

```
/downloads/.*\.(exe|zip|bin)
```



**Note** 空白または英数字以外の文字を含む正規表現は、ASCII 引用符で囲む必要があります。

## 検証エラーを回避するための注意事項

**重要：**63 文字以上を返す正規表現は失敗し、無効なエントリのエラーが生成されます。必ず、63 文字以上を返す可能性がない正規表現を作成してください。

検証エラーを最小限に抑えるため、以下の注意事項に従ってください。

- 可能な限り、ワイルドカードやカッコで囲んだ式ではなく、リテラル式を使用してください。リテラル式とは、「It's as easy as ABC123」のような基本的に加工されていないテキストです。この式は、「It's as easy as [A-C]{3}[1-3]{3}」を使用するよりも失敗する可能性が低くなります。後者の式では、結果として非決定性有限オートマトン（NFA）エントリが生じるため、処理時間が大幅に長くなる可能性があります。
- エスケープしていないピリオドの使用は可能な限り避けてください。ピリオドは特別な正規表現文字であり、改行文字以外のあらゆる文字に一致します。たとえば、「`url.com`」などの実際のピリオドと一致させたい場合は、「`url\.com`」のように `\` 文字を使用してピリオドをエスケープします。エスケープされたピリオドはリテラル入力と見なされるので、問題が生じません。
- ピリオドの後に 63 文字以上を返すパターン内のエスケープされていないピリオドは、パターンマッチングエンジンによって無効化されます。その影響についてのアラートがユーザーに送信され、パターンを修正または置換するまで更新のたびにアラートを受信し続けます。

可能な限り、エスケープしていないピリオドではなく、より具体的な一致パターンを使用してください。たとえば、後ろに 1 つの数字が続く URL に一致させるには、「`url.`」ではなく、「`url[0-9]`」を使用します。

- 長い正規表現内でエスケープしていないピリオドを使用することは、特に問題を引き起こすので、避ける必要があります。たとえば、「Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created .qual」はエラーを引き起こす可能性があります。ピリオドを含む「`.qual`」をリテラルの「`equal`」に置き換えると問題が解決します。

また、パターン内でエスケープしていないピリオドを使用し、パターンマッチングエンジンでそのピリオドが無効化されると、63 文字以上が返されます。パターンを修正するか、置き換えてください。

- 正規表現を終了または開始する場合は「\*」は使用できません。また、URL に一致させるために正規表現で「./」を使用したり、その式の最後にドットを使用することはできません。
- ワイルドカードとカッコの組み合わせは、問題を引き起こす可能性があります。この組み合わせをできる限り使用しないようにしてください。たとえば、  
「id:[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{12}\\) Gecko/20100101 Firefox/9\\.0\\.1\\\$」はエラーになる可能性があります、  
「Gecko/20100101 Firefox/9\\.0\\.1\\\$」はエラーになりません。後者の式にはワイルドカードやカッコで囲まれた式が含まれておらず、また、どちらの式でもエスケープされたピリオドが使用されています。

ワイルドカードやカッコで囲まれた式を排除できない場合は、式のサイズと複雑さを減らすようにしてください。たとえば、「[0-9a-z]{64}」ではエラーが発生する可能性があります。「[0-9]{64}」や「[0-9a-z]{40}」のように、より短いまたはより単純な表現に変更すると、問題が解決します。

エラーが発生した場合は、ワイルドカード（「\*」、「+」、「.」など）やカッコで囲まれた式に前述のルールを適用して、問題を解決してください。



#### Note

CLI オプション `advancedproxyconfig>miscellaneous>Do you want to enable URL lower case conversion for velocity regex?` を使用して、大文字と小文字を区別しないマッチングの場合に小文字に変換するデフォルトの正規表現変換をイネーブルまたはディセーブルにすることができます。このオプションは、大文字と小文字の区別が重要な状況で問題が発生する場合に使用します。このオプションの詳細については、[Secure Web Appliance CLI コマンド, on page 780](#) を参照してください。

## 正規表現の文字テーブル

| メタ文字 | 説明                                                                                                                                                                                                                                                                                 |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| .    | 改行文字（0x0A）を除く任意の文字と一致します。たとえば、正規表現 <code>rt</code> は文字列 <code>rat</code> 、 <code>rut</code> 、 <code>rt</code> と一致しますが、 <code>root</code> とは一致しません。<br><br>長いパターン内、特に長いパターンの途中でエスケープしていないピリオドを使用する場合は、慎重に行ってください。詳細については、 <a href="#">検証エラーを回避するための注意事項, on page 322</a> を参照してください。 |
| *    | 直前の正規表現の 0 回または複数回の出現と一致します。たとえば、 <code>.*</code> は任意の文字列と一致し、「 <code>[0-9]*</code> 」は任意の数字と一致します。<br><br>このメタ文字を使用する場合（特にピリオドと一緒に使用する場合は、慎重に使用してください。エスケープされていないピリオドを含むパターンは、ピリオドが無効になると 63 文字以上を返します。詳細については、 <a href="#">検証エラーを回避するための注意事項, on page 322</a> を参照してください。          |

| メタ文字 | 説明                                                                                                                                                                                                                                                                                                   |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \    | エスケープ文字。以下のメタ文字を通常の文字として扱うための文字です。たとえば、\ は、行の先頭ではなく、キャレット記号 (^) と一致させる場合に使用します。同様に、\. は、任意の 1 文字ではなく、実際のピリオドと一致させる場合に使用します。                                                                                                                                                                          |
| ^    | 行の先頭と一致します。たとえば、正規表現 ^When in matches は、「When in the course of human events」の先頭と一致しますが、「What and when in the」とは一致しません。                                                                                                                                                                               |
| \$   | 行または文字列の末尾と一致します。たとえば、b\$. は末尾が「b.」のあらゆる行または文字列と一致します。                                                                                                                                                                                                                                               |
| +    | 直前の正規表現の 1 回以上の出現と一致します。たとえば、正規表現 9+ は 9、99、および 999 と一致します。                                                                                                                                                                                                                                          |
| ?    | 直前の正規表現の 0 回または 1 回の出現と一致します。たとえば、colou?r は、「u」が任意であるため、「colour」と「color」のどちらとも一致します。                                                                                                                                                                                                                 |
| ()   | 左右のカッコの間の式を 1 つのグループとして扱い、他のメタ文字の範囲を制限します。たとえば、(abc)+ は文字列「abc」の 1 回以上の出現と一致します。「abcabcabc」や「abc123」とは一致しますが、「abab」や「ab123」とは一致しません。                                                                                                                                                                 |
|      | 論理和 (OR) : 前のパターンまたは後ろのパターンと一致します。たとえば、(him her) は、行「it belongs to him」や「it belongs to her」と一致し、「it belongs to them」とは一致しません。                                                                                                                                                                        |
| []   | <p>カッコで囲まれた文字列の 1 文字に一致します。たとえば、正規表現 r[aou]t は、「rat」、「rot」、「rut」と一致し、「ret」とは一致しません。</p> <p>文字の範囲は先頭文字、ハイフン、および終了文字で指定します。たとえば、パターン [0-9] は任意の数字と一致します。複数の範囲も指定できます。パターン [A-Za-z] は大文字または小文字を示しています。範囲外 (補集合) の文字を照合するには、左角カッコの後に先頭文字を示すキャレット記号を使用します。たとえば、式 [^269A-Z] は 2、6、9、および大文字以外の文字と一致します。</p> |

| メタ文字  | 説明                                                                                                                                                                                                                                                        |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| { }   | <p>前のパターンと一致する回数を指定します。</p> <p>次に例を示します。</p> <p>D{1,3} は、文字 D が 1 ～ 3 回出現する場合に一致します。</p> <p>前のパターンが特定の回数（{n}）または特定回数以上（{n,}）出現する場合に一致します。たとえば、式 A[0-9]{3} は後ろに 3 桁の数字が続く「A」と一致します。つまり、「A123」とは一致しますが、「A1234」とは一致しません。式 [0-9]{4,} は 4 桁以上の任意の数字と一致します。</p> |
| "..." | 引用符で囲まれた文字を文字どおりに解釈します。                                                                                                                                                                                                                                   |

## URL カテゴリについて

ここでは、Cisco Web Usage Controls の URL カテゴリのリストを示します。表には URL カテゴリ名の省略形も記載されています。これらの省略形は、アクセス ログ ファイル エントリの [Web レピュテーション フィルタリング (Web Reputation Filtering)] や [マルウェア対策スキャン (Anti-malware Scanning)] セクションに表示されることがあります。



**Note** アクセス ログでは、Cisco Web Usage Controls の URL カテゴリの各省略形の前にプレフィックス「IW\_」が付いています。つまり、「art」カテゴリは「IW\_art」となります。

| URL カテゴリ     | 省略形  | コード  | 説明                                                                                                                                                                  | URL の例                                             |
|--------------|------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| アダルト (Adult) | adlt | 1006 | アダルト コンテンツを指しますが、ポルノではありません。アダルト向けのナイトクラブ（ストリップクラブ、スワッピングクラブ、同伴サービス、ストリッパーなど）、セックスに関する全般情報（ポルノとは限らない）、性器ピアス、アダルト向けの製品やグリーティングカード、健康や疾病関連以外の性行為に関する情報なども含まれることがあります。 | www.adultentertainment.com<br>www.sincerelynot.com |

| URL カテゴリ                      | 省略形  | コード  | 説明                                                                                                                                                                          | URL の例                                 |
|-------------------------------|------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| アドバタイズメント<br>(Advertisements) | adv  | 1027 | Web ページに表示されることの多いバナー広告やポップアップ広告。広告コンテンツを提供しているその他の広告関連 Web サイト。広告サービスおよび広告営業は、[事業および産業 (Business and Industry) ] カテゴリに分類されます。                                              | www.adforce.com<br>www.doubleclick.com |
| アルコール<br>(Alcohol)            | alc  | 1077 | 嗜好品としてのお酒、ビールやワインの醸造、カクテルのレシピ、リキュール販売、ワイナリー、ブドウ園、ビール工場、アルコール類の販売元など。アルコール中毒は [健康と薬 (Health and Medicine) ] カテゴリに分類されます。バーおよびレストランは [飲食 (Dining and Drinking) ] カテゴリに分類されます。 | www.samueladams.com<br>www.whisky.com  |
| 動物とペット                        | ペット  | 1107 | 国内の動物、家畜、介助動物、ペット、およびそれらの世話に関する情報。獣医サービス、医療、および動物の健康。ペットと動物のトレーニング、水族館、動物園、および動物のショー。保護施設、人道支援団体、動物中心のチャリティー、保護区域、ハチの管理、トレーニング、および牧畜。恐竜や絶滅した動物。                             | www.petmd.com<br>www.wheatenorg.uk     |
| 芸術 (Arts)                     | art  | 1002 | 画廊および展示会、芸術家および芸術作品、写真、文学および書籍、舞台芸術および劇場、ミュージカル、バレエ、美術館、デザイン、建築。映画およびテレビは [エンターテインメント (Entertainment) ] に分類されます。                                                            | www.moma.org<br>www.nga.gov            |
| 占星術<br>(Astrology)            | astr | 1074 | 占星術、ホロスコープ、占い、数霊術、霊能者による助言、タロット。                                                                                                                                            | www.astro.com<br>www.astrology.com     |

| URL カテゴリ                                                      | 省略形  | コード  | 説明                                                                                                                                                                                                                                                           | URL の例                                       |
|---------------------------------------------------------------|------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| オークション<br>(Auctions)                                          | auct | 1088 | オンラインまたはオフラインのオークション、オークション会社、オークション案内広告など。                                                                                                                                                                                                                  | www.craigslist.com<br>www.ebay.com           |
| ビジネスおよび<br>産業 (Business<br>and Industry)                      | busi | 1019 | マーケティング、商業、企業、ビジネス手法、労働力、人材、運輸、給与、セキュリティとベンチャーキャピタル、オフィス用品、産業機器（プロセス用機器）、機械と機械系、加熱装置、冷却装置、資材運搬機器、包装装置、製造、立体処理、金属製作、建築と建築物、旅客輸送、商業、工業デザイン、建築、建築資材、出荷と貨物（貨物取扱業務、トラック輸送、運送会社、トラック輸送業者、貨物ブローカーと輸送ブローカー、優先サービス、荷高と貨物のマッチング、追跡とトレース、鉄道輸送、海上輸送、ロードフィーダーサービス、移動と保管）。 | www.freightcenter.com<br>www.ge.com          |
| 大麻                                                            | cann | 1109 | 大麻の快楽的および医療的消費に重点を置いた Web サイト。サイトには、マーケティング、法律および規制の問題に関する議論、成長と生産、道具、研究、大麻産業への投資が含まれる場合があります。ディスペンサリー、カンナビノイド（CBD油、THC など）ベースの製品も含まれています。                                                                                                                   | www.localproduct.co<br>www.oregonbc.com      |
| チャットおよび<br>インスタント<br>メッセージ<br>(Chat and Instant<br>Messaging) | chat | 1040 | Web ベースのインスタントメッセージングおよびチャットルーム。                                                                                                                                                                                                                             | www.icq.com<br>www.e-chat.co                 |
| 不正および盗用<br>(Cheating and<br>Plagiarism)                       | plag | 1051 | 不正行為を助長し、学期末論文（盗用したもの）などの書物を販売したりします。                                                                                                                                                                                                                        | www.bestessays.com<br>www.superiorpapers.com |
| 児童虐待コン<br>テンツ (Child<br>Abuse Content)                        | cprn | 1064 | 世界中の違法な児童性的虐待コンテンツ。                                                                                                                                                                                                                                          | —                                            |



| URL カテゴリ                                     | 省略形  | コード  | 説明                                                                                                                                                                                                                  | URL の例                                        |
|----------------------------------------------|------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| クラウドおよびデータセンター                               | serv | 1118 | 組織のアプリケーション、サービス、またはデータ処理をサポートするためにクラウドインフラストラクチャまたはデータセンターホスティングを提供するために使用されるプラットフォーム。これらのドメインと IP アドレスの分散型という性質のため、コンテンツや所有権に基づいてより具体的なカテゴリを適用することはできません。                                                         | www.azurewebsites.net<br>www.s3.amazonaws.com |
| コンピュータセキュリティ<br>(Computer Security)          | csec | 1065 | 企業ユーザおよび家庭ユーザ向けのセキュリティ製品およびセキュリティサービス。                                                                                                                                                                              | www.computersecurity.com<br>www.symantec.com  |
| コンピュータおよびインターネット<br>(Computers and Internet) | comp | 1003 | コンピュータおよびソフトウェアに関する情報（ハードウェア、ソフトウェア、ソフトウェアサポートなど）、ソフトウェアエンジニア向けの情報、プログラミング、ネットワーク、Web サイト設計、Web およびインターネット全般、コンピュータ科学、コンピュータグラフィック、クリップアートなど。フリーウェアとシェアウェアは、[フリーウェアおよびシェアウェア (Freeware and Shareware)] カテゴリに分類されます。 | www.xml.com<br>www.w3.org                     |

| URL カテゴリ                        | 省略形  | コード  | 説明                                                                                                                                                                                                                                      | URL の例                                                                                                                                     |
|---------------------------------|------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 表記法、会議および見本市                    | expo | 1110 | 特定の業界、市場、または共通の関心をテーマにしたセミナー、見本市、大会、会議。チケットの取得、登録、要約またはプレゼンテーションの提案ガイドライン、ワークショップ、スポンサーの詳細、ベンダーまたは出展者の情報、およびその他のマーケティングまたは販促資料に関する情報が含まれる場合があります。このカテゴリには、アカデミック イベント、プロフェッショナル イベント、ポップカルチャー イベントが含まれます。すべて、一時的または毎年恒例のイベントである傾向があります。 | <a href="http://www.thsmallbusinessexpo.com">www.thsmallbusinessexpo.com</a><br><a href="http://www.makerfaire.com">www.makerfaire.com</a> |
| 暗号通貨                            | Cryp | 1111 | ユーザが暗号通貨を取引できるオンラインブローカー業者および Web サイト。分析、解説、アドバイス、業績指標、価格チャートなどの暗号通貨に関する情報。仮想通貨マイニングおよびマイニングビジネスに関する一般的な情報はこのカテゴリに含まれますが、マイニング アクティビティに直接関係するドメインと IP アドレスは仮想通貨マイニングとして分類されます。                                                          | <a href="http://www.coinbase.com">www.coinbase.com</a><br><a href="http://www.coinsutra.com">www.coinsutra.com</a>                         |
| 仮想通貨マイニング                       | mine | 1112 | 暗号通貨マイニングプールにアクティブに参加しているホスト。                                                                                                                                                                                                           | <a href="http://www.give-me-coins.com">www.give-me-coins.com</a><br><a href="http://www.slushpool.com">www.slushpool.com</a>               |
| 出会い系 (Dating)                   | date | 1055 | 出会い系サイト、結婚紹介所など。                                                                                                                                                                                                                        | <a href="http://www.eharmony.com">www.eharmony.com</a><br><a href="http://www.match.com">www.match.com</a>                                 |
| デジタル ポストカード (Digital Postcards) | card | 1082 | デジタルはがきおよび電子カードの送信。                                                                                                                                                                                                                     | <a href="http://www.hallmarkcards.com">www.hallmarkcards.com</a><br><a href="http://www.bluemountain.com">www.bluemountain.com</a>         |
| 飲食 (Dining and Drinking)        | food | 1061 | 飲食店、レストラン、バー、居酒屋、パブ、レストラン ガイド、レストラン レビューなど。                                                                                                                                                                                             | <a href="http://www.zagat.com">www.zagat.com</a><br><a href="http://www.experiencethepub.com">www.experiencethepub.com</a>                 |

| URL カテゴリ                                   | 省略形  | コード  | 説明                                                                                                                                                          | URL の例                                        |
|--------------------------------------------|------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| DIY プロジェクト (DIY Projects)                  | diy  | 1097 | エキスパートや専門家の支援を受けずに、物品を作成、改善、変更、装飾、修復するためのガイダンスおよび情報。                                                                                                        | www.diy-tips.co.uk<br>www.thisoldhouse.com    |
| DNS トンネリング                                 | tunn | 1122 | サービスとして DNS トンネリングを提供するサイト。これらのサービスは、PC またはモバイル向けのものであり、企業のポリシーおよびインスペクションをバイパスする可能性のあるトラフィックを送信するために、DNS を介して特別に VPN 接続を作成します。                             |                                               |
| 暗号化された DNS                                 | doht | 1113 | DNS over HTTPS (DoH) プロトコルまたは DNS over TLS プロトコルを使用した暗号化 DNS リクエスト。これらのプロトコルは通常、エンドユーザによってセキュリティとプライバシーの層として使用されますが、暗号化によってリクエストの宛先が非表示にされ、サードパーティ経由で渡されます。 | www.cloudflare-dns.com<br>www.dns. google.com |
| ダイナミックおよびレジデンシャル (Dynamic and Residential) | dyn  | 1091 | ブロードバンドリンクの IP アドレス。通常は、ホーム ネットワークへのアクセスを試みているユーザを指します。たとえば、ホーム コンピュータへのリモートセッションの場合などです。                                                                   | http://109.60.192.55                          |
| ダイナミック DNS プロバイダー (Dynamic DNS Provider)   | ddns | 1114 | ダイナミック DNS サービスを使用して、動的に割り当てられた IP アドレスでホストされているエンドポイントから特定のアプリケーションまたはコンテンツに Web 経由でアクセス可能にすることができます。アクセス権は、ダイナミック DNS サービスが所有するドメインのホスト名を介して付与されます。       | www.noip.com<br>www.afraid.org                |

| URL カテゴリ                            | 省略形  | コード  | 説明                                                                                                             | URL の例                                              |
|-------------------------------------|------|------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| 教育<br>(Education)                   | edu  | 1001 | 教育関連の Web サイト。たとえば、学校、短大、大学、教材、教師用資料、技術訓練、職業訓練、オンライントレーニング、教育問題、教育政策、学資援助、学校助成金、規範、試験など。                       | www.education.com<br>www.greatschools.org           |
| エンターテインメント<br>(Entertainment)       | ent  | 1093 | 映画、音楽、バンド、テレビ、芸能人、ファンサイト、エンターテインメントニュース、芸能界のゴシップ、エンターテインメントの会場などに関する詳細や批評など。<br>[芸術 (Arts)] カテゴリとの違いを確認してください。 | www.eonline.com<br>www.ew.com                       |
| 過激 (Extreme)                        | extr | 1075 | 性的暴力または犯罪性のあるもの、暴力および暴力的行為、悪趣味な写真や血まみれの写真（解剖写真など）、犯行現場、犯罪被害者、事故被害者の写真、過度にわいせつな文章や写真、衝撃的な内容の Web サイトなど。         | www.car-accidents.com<br>www.crime-scene-photos.com |
| ファッション<br>(Fashion)                 | fash | 1076 | 衣料、服飾、美容室、化粧品、アクセサリ、宝飾品、香水、身体改造に関連する図表や文章、タトゥー、ピアス、モデル事務所など。皮膚科関連製品は [健康と薬 (Health and Medicine)] カテゴリに分類されます。 | www.fashion.net<br>www.styleseat.com                |
| ファイル転送サービス (File Transfer Services) | fts  | 1071 | ダウンロードサービスおよびホスティングによるファイル共有を主目的とするファイル転送サービス                                                                  | www.sharefile.com<br>www.wetransfer.com             |
| フィルタリング回避 (Filter Avoidance)        | filt | 1025 | 検出されない匿名の Web 利用を促進および支援する Web サイト。<br>例：cgi、php、および glype を使用した匿名プロキシサービス。                                    | www.bypassschoolfilter.com<br>www.filterbypass.com  |

| URL カテゴリ                                 | 省略形  | コード  | 説明                                                                                                                                                                                                   | URL の例                                         |
|------------------------------------------|------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| 金融 (Finance)                             | fnnc | 1015 | 会計実務、会計士、課税、税、銀行、保険、投資、国家経済、個人資産管理（各種保険、クレジットカード、個人退職金積立計画、遺産相続計画、ローン、住宅ローン）などの金融や財務関連のもの。株は[オンライントレード (Online Trading)] に分類されます。                                                                    | www.finance.yahoo.com<br>www.bankofamerica.com |
| フリーウェアおよびシェアウェア (Freeware and Shareware) | free | 1068 | フリー ソフトウェアおよびシェアウェア ソフトウェアのダウンロードを提供します。                                                                                                                                                             | www.freewarehome.com<br>www.filehippo.com      |
| ギャンブル (Gambling)                         | gamb | 1049 | カジノ、オンライン ギャンブル、ブックメーカー、オッズ、ギャンブルに関する助言、ギャンブルの対象となっているレース、スポーツブックキング、スポーツギャンブル、株式スプレッドベッティングサービス。ギャンブル中毒に関する Web サイトは、[健康と薬 (Health and Medicine)] カテゴリに分類されます。国営宝くじは、[宝くじ (Lotteries)] カテゴリに分類されます。 | www.888.com<br>www.gambling.com                |
| ゲーム (Games)                              | game | 1007 | さまざまなカード ゲーム、ボードゲーム、ワードゲーム、ビデオゲーム、戦闘ゲーム、スポーツゲーム、ダウンロード型ゲーム、ゲーム批評、攻略本、コンピュータゲーム、インターネットゲーム（ロールプレイング ゲームなど）。                                                                                           | www.games.com<br>www.shockwave.com             |

| URL カテゴリ                        | 省略形  | コード  | 説明                                                                                                                                                                                   | URL の例                                                                                                                     |
|---------------------------------|------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| 生成 AI                           | gnai | 1128 | 生成 AI とは、人工知能モデルを使用して、ユーザーから提供されたプロンプトに基づき文章、音声、動画、画像などの出力を生成することを主な目的とするサイトを指します。この定義は、より広範なサービス提供の一環として生成 AI を間接的に組み込むだけのテクノロジーを除外します。                                             | <a href="https://www.deepseek.com/">https://www.deepseek.com/</a>                                                          |
| 政府および法律<br>(Government and Law) | gov  | 1011 | 政府 Web サイト、外交関係、政府および選挙に関するニュースや情報、法律家、法律事務所、法律関連の出版物、法律関連の参考資料、裁判所、訴訟事件一覧表、法律関連の協会などの法律分野に関する情報、立法および判例、市民権問題、移民関連、特許、著作権、法執行制度および矯正制度に関する情報、犯罪報道、法的措置、犯罪統計、軍事（軍隊、軍事基地、軍組織）/テロ対策など。 | <a href="http://www.usa.gov">www.usa.gov</a><br><a href="http://www.law.com">www.law.com</a>                               |
| ハッキング<br>(Hacking)              | hack | 1050 | Web サイト、ソフトウェア、およびコンピュータのセキュリティを回避する方法に関する議論。                                                                                                                                        | <a href="http://www.hackthissite.org">www.hackthissite.org</a><br><a href="http://www.gohacking.com">www.gohacking.com</a> |
| ヘイトスピーチ<br>(Hate Speech)        | hate | 1016 | 社会集団、肌の色、宗教、性的指向、障がい、階級、民族、国籍、年齢、性別、性同一性を基に、憎悪、不寛容、差別を助長する Web サイト。人種差別を扇動するサイト、性差別、人種差別の神学、人種差別の音楽、ネオナチ組織、特定民族至上主義、ホロコースト否定論。                                                       | <a href="http://www.kkk.com">www.kkk.com</a><br><a href="http://www.aryanunity.com">www.aryanunity.com</a>                 |

| URL カテゴリ                     | 省略形  | コード  | 説明                                                                                                                                      | URL の例                                    |
|------------------------------|------|------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| 健康と薬                         | hmed | 1104 | 健康管理、疾病および障がい、医療、病院、医師、医薬品、精神衛生、精神医学、薬理学、エクササイズおよびフィットネス、身体障がい、ビタミン剤およびサプリメント、健康にかかわる性行為（疾病および健康管理）、喫煙、飲酒、薬物使用、健康にかかわるギャンブル（疾病および健康管理）。 | www.webmd.com<br>www.health.com           |
| ユーモア<br>(Humor)              | lol  | 1079 | ジョーク、スケッチ、コミック、その他のユーモラスなコンテンツ。不快感を与える可能性のあるアダルト ユーモアは [アダルト (Adult) ] に分類されます。                                                         | www.pun.me<br>www.jokes.com               |
| ハンティング                       | hunt | 1022 | 職業としての狩猟または魚釣り、またはスポーツとしての狩猟：ガンクラブ、およびその他の狩猟関連のサイト。                                                                                     | www.bulletsafaris.com<br>www.mfha.org     |
| 違法行為 (Illegal Activities)    | ilac | 1022 | 窃盗、不正行為、電話ネットワークへの不法アクセスなどの犯罪を助長するサイト、コンピュータウイルス、テロリズム、爆弾、無秩序、殺人や自殺を描写したものやその実行方法を記述した Web サイト。                                         | www.ekran.no<br>www.pyrobin.com           |
| 違法ダウンロード (Illegal Downloads) | ildl | 1084 | 著作権契約に違反してソフトウェア保護を回避するための、ソフトウェア、シリアル番号、キー生成ツールなどをダウンロードできる Web サイト。Torrent は [ピアファイル転送 (Peer File Transfer) ] に分類されます。                | www.keygenninja.com<br>www.rootscrack.com |
| 違法ドラッグ<br>(Illegal Drugs)    | drug | 1047 | 気晴らしのためのドラッグ、ドラッグ摂取の道具、ドラッグの購入と製造に関する情報。                                                                                                | www.shroomery.org<br>www.hightimes.com    |

| URL カテゴリ                                                                     | 省略形   | コード  | 説明                                                                                                                                                                                                                                                     | URL の例                                       |
|------------------------------------------------------------------------------|-------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| インフラストラクチャおよびコンテンツ配信ネットワーク<br>(Infrastructure and Content Delivery Networks) | infr  | 1018 | コンテンツ配信インフラおよび動的に生成されるコンテンツ、セキュリティで保護されているか、または分類が困難なために細かく分類できない Web サイトなど。                                                                                                                                                                           | www.akamai.net<br>www.webstat.net            |
| Internet of Things (IoT)                                                     | iot   | 1116 | Internet of Things (IoT) およびその他のネットワーク認識型電子機器の設定で、全般的な正常性、アクティビティ、または支援をモニターするために使用されるドメイン。また、これらのサイトでは、ソフトウェアまたはファームウェアの更新を提供したり、デバイスを管理するためのリモートアクセスを許可したりできます。IoTは、プリンタ、テレビ、サーモスタット、システム モニタリング、自動化、スマート アプライアンスなどの製品の消費者とプロフェッショナルの両方のセグメントに存在します。 | www.samsungotn.net<br>www.transport.nest.com |
| インターネット電話 (Internet Telephony)                                               | v oip | 1067 | インターネットを利用した電話サービス。                                                                                                                                                                                                                                    | www.skype.com<br>www.getvoca.com             |
| 求職 (Job Search)                                                              | job   | 1004 | 職業に関する助言、履歴書の書き方、面接に関するスキル、就職斡旋サービス、求人データベース、職業紹介所、人材派遣会社、雇用主の Web サイトなど。                                                                                                                                                                              | www.careerbuilder.com<br>www.monster.com     |
| 下着および水着 (Lingerie and Swimsuits)                                             | ling  | 1031 | 下着および水着。特にモデルが着用している Web サイト。                                                                                                                                                                                                                          | www.swimsuits.com<br>www.victoriassecret.com |
| 宝くじ (Lotteries)                                                              | lotr  | 1034 | 宝くじ、コンテストおよび国が運営する宝くじ。                                                                                                                                                                                                                                 | www.calottery.com<br>www.flalottery.com      |
| [軍 (Military) ]                                                              | mil   | 1099 | 武装部隊などの軍隊：軍事基地：軍事組織：テロ対策。                                                                                                                                                                                                                              | www.goarmy.com<br>www.todaysmilitary.com     |



| URL カテゴリ                                  | 省略形  | コード  | 説明                                                                                                                                                                     | URL の例                                                |
|-------------------------------------------|------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| 携帯電話<br>(Mobile Phones)                   | cell | 1070 | ショート メッセージ サービス (SMS)、着信音などの携帯電話用ダウンロード サービス。携帯電話会社の Web サイトは、[ビジネス および産業 (Business and Industry) ] カテゴリに分類されます。                                                       | www.cbfsms.com<br>www.zedge.net                       |
| 博物館                                       | muse | 1117 | 一般的な関心を集めたり、または高い専門性を備えたりするテーマに関する情報を保持することを専門とする、オンラインおよび物理的な博物館と展示品。テーマは、芸術、歴史、科学、または文化的に重要なものです。                                                                    | www.ushmm.org<br><del>www.museumofmodernart.org</del> |
| 自然と保護                                     | ncon | 1106 | 天然資源、生態学および自然保護、森林、原生地、植物、草花、森林保護、森林、原生林および林業、森林管理（再生、保護、保全、伐採、森林状態、間伐、計画的火入れ）、農作業（農業、ガーデニング、園芸、造園、種まき、除草、灌漑、剪定、収穫）、環境汚染問題（大気質、有害廃棄物、汚染防止、リサイクル、廃棄物処理、水質、環境産業）に関するサイト。 | www.nature.org<br>www.thepottedgarden.co.uk           |
| ニュース<br>(News)                            | news | 1058 | ニュース、ヘッドライン、新聞、テレビ局、雑誌、天気、スキー場の状態。                                                                                                                                     | www.cnn.com<br>www.news.bbc.co.uk                     |
| 非政府組織<br>(Non-Governmental Organizations) | ngo  | 1087 | クラブ、圧力団体、コミュニティ、非営利組織および労働組合などの非政府組織。                                                                                                                                  | www.panda.org<br>www.unions.org                       |
| 性的でないヌード<br>(Non-Sexual Nudity)           | nsn  | 1060 | ヌーディズム、ヌード、自然主義、ヌーディスト キャンプ、芸術的ヌードなど。                                                                                                                                  | www.1001fessesproject.com<br>www.naturistsociety.com  |
| 非実用的                                      | nact | 1103 | 検査されたが、到達不能またはカテゴリに割り当てられるコンテンツが不足しているサイト。                                                                                                                             | —                                                     |

| URL カテゴリ                                            | 省略形  | コード  | 説明                                                                                                                                                                                                     | URL の例                                  |
|-----------------------------------------------------|------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| オンライン コミュニティ<br>(Online Communities)                | comm | 1024 | アフィニティ グループ、Special Interest Group (SIG; 同じ興味を持つ人々の集まり)、Web ニュースグループ、Web 掲示板など。[プロフェッショナルネットワーキング (Professional Networking)] カテゴリまたは[ソーシャルネットワーキング (Social Networking)] カテゴリに分類される Web サイトはここには含まれません。 | www.reddit.com<br>www.stackexchange.com |
| オンライン ドキュメントの共有とコラボレーション                            | docs | 1115 | ドキュメントの作成、変換、編集に使用されるクラウドベースのソフトウェア。コラボレーションおよび共有機能は、通常は作成者が設定したアクセス権限で使用できます。ドキュメントはオンラインで保存することも、ダウンロードして使用することもできます。                                                                                | www.pastebin.com<br>www.docs.google.com |
| オンライン会議<br>(Online Meetings)                        | meet | 1100 | オンライン会議、デスクトップ共有、リモートアクセス、および複数の場所のコラボレーションを容易にするその他のツール。                                                                                                                                              | www.join.me<br>www.teamviewer.com       |
| オンライン ストレージおよびバックアップ<br>(Online Storage and Backup) | osb  | 1066 | バックアップ、共有、およびホスティングを目的とした、オフサイトストレージおよびピアツーピア型ストレージ                                                                                                                                                    | www.adrive.com<br>www.dropbox.com       |
| オンライン トレード (Online Trading)                         | trad | 1028 | オンライン証券会社、ユーザがオンラインで株取引できる Web サイト、株式市場、株式、債券、投資信託会社、ブローカー、株式市場の分析と解説、株式審査、株価チャート、IPO、株式分割に関する情報。株式スプレッドベッティング サービスは[ギャンブル (Gambling)] に分類されます。その他の金融サービスは[財務 (Finance)] に分類されます。                      | www.tdameritrade.com<br>www.etrade.com  |

| URL カテゴリ                              | 省略形  | コード  | 説明                                                                                                                                                                | URL の例                                        |
|---------------------------------------|------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| 業務用電子メール<br>(Organizational Email)    | pem  | 1085 | Outlook Web Access (OWA) など<br>で業務用のメールを利用する際に<br>使用する Web サイト。                                                                                                   | www.mail.zoho.com<br>www.webmail.edmc.edu     |
| 超常現象<br>(Paranormal)                  | prnm | 1101 | UFO、幽霊、未確認動物、テレキ<br>ネシス、都市伝説、神話。                                                                                                                                  | www.ghoststudy.com<br>www.ufocasebook.com     |
| パーク ドメイン<br>(Parked Domains)          | park | 1092 | 広告ネットワークの有料リスティ<br>ングサービスを利用してそのドメ<br>インのトラフィックから収益を得<br>ようとする Web サイト、またはド<br>メイン名を販売して収益を得よう<br>と考えている「不正占拠者」が所<br>有する Web サイト。有料広告リン<br>クを返す偽の検索サイトも含まれ<br>ます。 | www.domainzaar.com<br>www.cricketbuzz.com     |
| ピア ファイル転<br>送 (Peer File<br>Transfer) | p2p  | 1056 | ピアツーピア型のファイル要求<br>Web サイト。ファイル転送自体の<br>トラッキングは行いません。                                                                                                              | www.bittorrent.com<br>www.torrentdownloads.me |
| 個人サイト<br>(Personal Sites)             | pers | 1081 | 個人が運営している個人関連の<br>Web サイト、個人用ホーム ページ<br>サーバ、個人的コンテンツが公開<br>されている Web サイト、特定の<br>テーマがない個人ブログなど。                                                                    | www.blogmaverick.com<br>www.stallman.org      |
| パーソナル VPN<br>(Personal VPN)           | pvpn | 1102 | バーチャル プライベート ネット<br>ワーク (VPN) サイト、または一<br>般的に個人使用向けのツール (法<br>人による使用の可否は場合によ<br>る)。                                                                               | www.openvpn.net<br>www.torvpn.com             |
| 写真検索と画像                               | img  | 1090 | 画像、写真、クリップ アートの保<br>存と検索を促進します。                                                                                                                                   | www.flickr.com<br>www.photobucket.com         |
| 政治 (Politics)                         | pol  | 1083 | 政治家、政党、政治、選挙、民主<br>主義、投票などに関連するニュー<br>スや情報の Web サイト。                                                                                                              | www.politics.com<br>www.gp.org                |

| URL カテゴリ                                        | 省略形  | コード  | 説明                                                                                                                              | URL の例                                     |
|-------------------------------------------------|------|------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| ポルノ<br>(Pornography)                            | porn | 1054 | 性的表現が露骨な文章または画像。性的表現が露骨なアニメや漫画、性的表現が露骨な描写全般、フェチ志向の文章や画像、性的表現が露骨なチャットルーム、セックスシミュレータ、ストリップポーカー、アダルト映画、わいせつな芸術、性的表現が露骨な Web メールなど。 | www.redtube.com<br>www.youporn.com         |
| ホストとしての<br>プライベート IP<br>アドレス                    | piah | 1121 | URL のホスト部分として使用されるプライベート IP アドレス。プライベート IP アドレスは、境界ルータの背後での内部使用専用であるため、パブリックにルーティングできません。                                       |                                            |
| プロフェッショナル ネットワーキング<br>(Professional Networking) | pnet | 1089 | キャリア開発や専門性開発を目的としたソーシャル ネットワーキング。[ ソーシャル ネットワーキング (Social Networking) ] も参照してください。                                              | www.linkedin.com<br>www.europeanpwn.net    |
| 不動産 (Real Estate)                               | rest | 1045 | 不動産の検索に役立つ情報、事務所および商業区画、賃貸、アパート、戸建てなどの不動産物件一覧、住宅建築など。                                                                           | www.realtor.com<br>www.zillow.com          |
| レシピと食品                                          | reci | 1105 | 料理、レシピ、および食品やノンアルコール飲料に関する情報、料理と食品の文化的側面、食生活の説明と守るべきヒント、食品に関する一般的な栄養情報を共有または議論する専門サイト。調理機器および用具の使用および説明。フードセレブ、ライフスタイル、マニアのブログ。 | www.allrecipes.com<br>www.seriousseats.com |
| 参照                                              | ref  | 1017 | 都道府県および市区町村の案内情報、地図、時刻、参考文献、辞書、図書館など                                                                                            | www.wikipedia.org<br>www.yellowpages.com   |
| 地域の制限付き<br>サイト (ドイツ)                            | xdeu | 1125 | 地方政府の判断により違法である可能性のあるコンテンツが原因でドイツで制限されている URL。                                                                                  |                                            |

| URL カテゴリ                                             | 省略形  | コード  | 説明                                                                                                   | URL の例                                              |
|------------------------------------------------------|------|------|------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| 地域の制限付き<br>サイト（英国）                                   | xgbr | 1123 | 地方政府の判断により違法である<br>可能性があるコンテンツが原因で<br>英国で制限されている URL。                                                |                                                     |
| 地域の制限付き<br>サイト（イタリ<br>ア）                             | xita | 1124 | 地方政府の判断により違法である<br>可能性があるコンテンツが原因で<br>イタリアで制限されている URL。                                              |                                                     |
| 地域の制限付き<br>サイト（ポーラ<br>ンド）                            | xpol | 1126 | 地方政府の判断により違法である<br>可能性があるコンテンツが原因で<br>ポーランドで制限されている<br>URL。                                          | www.betsafe62.com<br>www.tornadobet69.com           |
| 宗教（Religion）                                         | rel  | 1086 | 宗教に関するコンテンツ、宗教に<br>関する情報、宗教団体。                                                                       | www.religionfacts.com<br>www.religioustolerance.org |
| SaaS および B2B<br>（SaaS and<br>B2B）                    | saas | 1080 | オンライン ビジネス サービス用<br>Web ポータル、オンライン会議な<br>ど。                                                          | www.netsuite.com<br>www.salesforce.com              |
| 子供向け（Safe<br>for Kids）                               | kids | 1057 | 幼児や児童向けに作成されている<br>か、明示的に幼児や児童向けと認<br>められている Web サイト。                                                | www.discoverykids.com<br>www.nickjr.com             |
| 科学技術<br>（Science and<br>Technology）                  | sci  | 1012 | 科学技術（航空宇宙、電子工学、<br>工学、数学など）、宇宙探査、気<br>象学、地理学、環境、エネルギー<br>（化石燃料、原子力、再生可能エ<br>ネルギー）、通信（電話、電気通<br>信）など。 | www.physorg.com<br>www.science.gov                  |
| 検索エンジンお<br>よびポータル<br>（Search Engines<br>and Portals） | srch | 1020 | 検索エンジンなど、インターネッ<br>ト上の情報にアクセスするための<br>起点となるサイト。                                                      | www.bing.com<br>www.google.com                      |
| 性教育（Sex<br>Education）                                | sxed | 1052 | 事実に基づいて性的情報を扱う<br>Web サイト、性的健康、避妊、妊<br>娠など                                                           | www.avert.org<br>www.scarleteen.com                 |
| ショッピング<br>（Shopping）                                 | shop | 1005 | 物々交換、オンライン購入、クー<br>ポン、無料提供、事務用品、オン<br>ラインカタログ、オンラインモー<br>ルなど。                                        | www.amazon.com<br>www.shopping.com                  |

| URL カテゴリ                                   | 省略形  | コード  | 説明                                                                                              | URL の例                                         |
|--------------------------------------------|------|------|-------------------------------------------------------------------------------------------------|------------------------------------------------|
| ソーシャル ネットワーキング<br>(Social Networking)      | snet | 1069 | ソーシャル ネットワーキング関連。[プロフェッショナル ネットワーキング (Professional Networking)] も参照してください。                      | www.facebook.com<br>www.twitter.com            |
| 社会科学 (Social Science)                      | socs | 1014 | 社会に関係する科学と歴史、考古学、文化人類学、カルチュラル スタディーズ、歴史学、言語学、地理学、哲学、心理学、女性学。                                    | www.archaeology.org<br>www.anthropology.net    |
| 社会および文化<br>(Society and Culture)           | scty | 1010 | 家族および家族関係、民族性、社会組織、家系、高齢者、保育など。                                                                 | www.childcareaware.org<br>www.familysearch.org |
| ソフトウェア アップデート<br>(Software Updates)        | swup | 1053 | ソフトウェア パッケージに対する更新プログラムを提供している Web サイト。                                                         | www.softwarepatch.com<br>www.windowsupdate.com |
| スポーツおよびレクリエーション<br>(Sports and Recreation) | sprt | 1008 | すべてのプロ スポーツおよびアマチュア スポーツ、レクリエーション活動、釣り、ファンタジー スポーツ (ゲーム)、公園、遊園地、レジャープール、テーマ パーク、動物園、水族館、温泉施設など。 | www.espn.com<br>www.recreation.gov             |
| ストリーミング オーディオ<br>(Streaming Audio)         | aud  | 1073 | リアルタイム ストリーミング オーディオ コンテンツ (インターネット ラジオやオーディオフィードなど)。                                           | www.live-radio.net<br>www.shoutcast.com        |
| ストリーミング ビデオ<br>(Streaming Video)           | vid  | 1072 | リアルタイム ストリーミング ビデオ (インターネット テレビ、Web キャスト、動画共有など)。                                               | www.hulu.com<br>www.youtube.com                |

| URL カテゴリ                | 省略形  | コード  | 説明                                                                                                                                            | URL の例                                  |
|-------------------------|------|------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| テロリズムと暴力的な過激主義          | terr | 1119 | イデオロギーの一環として、死または暴力を助長するテロリストまたは過激派の Web サイト。サイトには、グラフィックや不穏な画像、ビデオおよびテキストが含まれていることがあります。一部のサイトは、テロを支持していないが、暴力的な資料を直接共有している場合もあります。          |                                         |
| タバコ<br>(Tobacco)        | tob  | 1078 | 愛煙家の Web サイト、タバコ製造会社、パイプ、喫煙製品（違法薬物吸引用でないもの）など。タバコ中毒は [健康と薬 (Health and Medicine)] カテゴリに分類されます。                                                | www.bat.com<br>www.tobacco.org          |
| 乗り物<br>(Transportation) | trns | 1044 | 個人用の乗り物、自動車およびバイクに関する情報、新車、中古車、オートバイの購入、自動車愛好会、小型船舶、航空機、レジャー用自動車 (RV) など。自動車レースおよびバイク レースは [スポーツおよびレクリエーション (Sports and Recreation)] に分類されます。 | www.cars.com<br>www.motorcycles.com     |
| 旅行 (Travel)             | trvl | 1046 | ビジネス旅行と個人旅行、旅行情報、トラベル リソース、旅行代理店、休暇利用のパック旅行、船旅、宿泊施設、交通手段、航空便の予約、航空運賃、レンタカー、別荘など。                                                              | www.expedia.com<br>www.lonelyplanet.com |
| URL 短縮サービス              | shrt | 1120 | 長い URL を短縮したり、URL をブランディングしたり、ハイパーリンクの最終的な宛先を隠したりするために使用されるドメイン。                                                                              | www.bit.ly<br>www.tinyurl.com           |

| URL カテゴリ                         | 省略形         | コード  | 説明                                                                                                                                                                   | URL の例                                        |
|----------------------------------|-------------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| 武器<br>(Weapons)                  | weap        | 1036 | 一般的な武器の購入および使用に関する情報（銃販売店、銃オークション、銃の案内広告、銃の付属品、銃の展示会、銃の訓練など）、銃に関する全般情報、その他の武器や狩猟関連画像のサイトなども含まれる場合があります。政府の軍に関する Web サイトは、[政府および法律 (Government and Law)] カテゴリに分類されます。 | www.coldsteel.com<br>www.gunbroker.com        |
| Web キャッシュとアーカイブ                  | cach        | 1108 | 通常、保存またはロード時間の短縮のために格納されるキャッシュまたはアーカイブされた Web コンテンツ。                                                                                                                 | www.archive.org<br>www.webcitation.org        |
| Web ホスティング (Web Hosting)         | whst        | 1037 | Web サイトのホスティング、帯域幅サービスなど。                                                                                                                                            | www.bluehost.com<br>www.godaddy.com           |
| Web ページ翻訳 (Web Page Translation) | tran        | 1063 | Web ページの翻訳。                                                                                                                                                          | www.babelfish.com<br>www.translate.google.com |
| Web-based Email                  | メール<br>アドレス | 1038 | Web メール サービス。個人が自分の会社の電子メール サービスを利用するための Web サイトは、[業務用電子メール (Organizational Email)] カテゴリに分類されます。                                                                     | www.mail.yahoo.com<br>www.outlook.com         |

#### 関連項目

- [URL カテゴリ セットの更新の管理, on page 285](#)
- [未分類の URL と誤って分類された URL の報告, on page 283](#)

## HTTPS トラフィックを制御する復号ポリシーの作成

この章で説明する内容は、次のとおりです。

- [HTTPS トラフィックを制御する復号ポリシーの作成：概要 \(344 ページ\)](#)
- [復号ポリシーによる HTTPS トラフィックの管理：ベストプラクティス \(345 ページ\)](#)
- [復号ポリシー \(345 ページ\)](#)



- [ルート証明書 \(353 ページ\)](#)
- [HTTPS トラフィックのルーティング \(361 ページ\)](#)
- [暗号化/HTTPS/証明書のトラブルシューティング \(362 ページ\)](#)

## HTTPS トラフィックを制御する復号ポリシーの作成：概要

復号ポリシーで、Web プロキシ内の HTTPS トラフィックの処理が定義されます。

- HTTPS トラフィックを復号するタイミング。
- 無効な、または失効したセキュリティ証明書を使用する要求の処理方法。

HTTPS トラフィックを以下のように処理する復号ポリシーを作成できます。

- 暗号化されたトラフィックをパススルーする。
- トラフィックを復号し、HTTP トラフィック用に定義されたコンテンツベースのアクセスポリシーを適用する。これによって、マルウェアスキャンも可能になります
- HTTPS 接続をドロップする。
- Web プロキシがポリシーに対して要求を評価しているときに、要求をモニターする（最終アクションは実行されない）。この評価によって、最終的にドロップ、パススルー、または復号のアクションが実行されます。



### Caution

個人識別情報の取り扱いに注意してください。エンドユーザの HTTPS セッションを復号することを選択した場合は、Secure Web Applianceのアクセスログとレポートに個人識別情報が含まれることがあります。管理者は `advancedproxyconfig CLI` コマンドと HTTPS サブコマンドを使用して、ログに保存する URI テキストの量を設定できます。URI 全体、またはクエリーの部分が除外された URI の部分的な形式をログに保存できます。ただし、URI からクエリーを削除することを選択した場合でも、個人を特定できる情報は残されたままになる可能性があります。

## 復号ポリシー タスクによる HTTPS トラフィックの管理の概要

| 手順 | 復号ポリシーによる HTTPS トラフィック管理のためのタスク リスト | 関連項目および手順へのリンク                                 |
|----|-------------------------------------|------------------------------------------------|
| 1  | HTTPS プロキシをイネーブルにする                 | <a href="#">HTTPS プロキシのイネーブル化, on page 348</a> |

| 手順 | 復号ポリシーによる HTTPS トラフィック管理のためのタスク リスト | 関連項目および手順へのリンク                                                                                                                                                  |
|----|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2  | 証明書とキーをアップロードまたは生成する                | <ul style="list-style-type: none"> <li>ルート証明書およびキーのアップロード, <a href="#">on page 356</a></li> <li>HTTPS プロキシ用の証明書およびキーの生成, <a href="#">on page 356</a></li> </ul> |
| 3  | 復号オプションを設定する                        | <a href="#">復号オプションの設定, on page 352</a>                                                                                                                         |
| 5  | (任意) 無効な証明書の処理を設定する                 | <a href="#">無効な証明書の処理の設定, on page 357</a>                                                                                                                       |
| 6  | (任意) リアルタイムの失効ステータス チェックをイネーブルにする   | <a href="#">リアルタイムの失効ステータス チェックの有効化, on page 359</a>                                                                                                            |
| 7  | (任意) 信頼された証明書とブロックされた証明書を管理する       | <a href="#">信頼できるルート証明書, on page 360</a>                                                                                                                        |

## 復号ポリシーによる HTTPS トラフィックの管理 : ベスト プラクティス

一般的な復号ポリシー グループを少数作成して、ネットワーク上のすべてのユーザーまたは少数の大きなユーザー グループに適用します。その後、復号された HTTPS トラフィックにきめ細かい管理を適用する必要がある場合は、より具体的なアクセス グループを使用します。

### 復号ポリシー

アプライアンスは、HTTPS 接続要求に対して、以下のアクションを実行できます。

| オプション          | 説明                                                                                                |
|----------------|---------------------------------------------------------------------------------------------------|
| モニター (Monitor) | モニター (Monitor) は、最終的に適用される最終アクションを決定するために Web プロキシが他の管理設定に対してトランザクションを評価し続ける必要があることを示す中間のアクションです。 |
| 削除 (Drop)      | アプライアンスは接続をドロップします。サーバーに接続要求を渡しません。アプライアンスは接続をドロップしたことをユーザーに通知しません。                               |

| オプション                | 説明                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| パススルー (Pass through) | <p>アプライアンスは、トラフィックの内容を検査せずに、クライアントとサーバー間の接続をパススルーします。</p> <p>ただし、標準のパススルーポリシーを使用している場合、Secure Web Applianceは要求されたサーバーとのHTTPSハンドシェイクを開始して、このサーバーの有効性をチェックします。有効性チェックでは、サーバー証明書が検証されます。サーバーのチェックが失敗した場合、トランザクションはブロックされます。</p> <p>特定のサイトの検証チェックをスキップするには、これらのサイトを含むカスタム カテゴリが組み込まれたポリシーを設定して、これらのサイトが信頼できることを示します。これらのサイトは、有効性チェックを受けないでパススルーされます。有効性チェックのスキップを許可するポリシーを設定する場合は、注意してください。</p> |
| 復号 (Decrypt)         | <p>アプライアンスは、接続を許可しますが、トラフィックの内容を検査します。トラフィックを復号、プレーンテキスト HTTP 接続であるかのように、復号されたトラフィックにアクセス ポリシーを適用します。接続を復号し、アクセス ポリシーを適用することにより、トラフィックをスキャンしてマルウェアを検出できます。</p>                                                                                                                                                                                                                              |

モニター以外のすべての操作は、Webプロキシがトランザクションに適用する「最終アクション」です。最終アクションは、Webプロキシが他の管理設定に対してトランザクションを評価することを停止する操作です。たとえば、復号ポリシーが、無効なサーバー証明書をモニターするように設定されている場合、Webプロキシは、サーバーにある証明書が無効である場合のHTTPS トランザクションの処理方法についての最終決定を行いません。復号ポリシーが、Webレピュテーション スコアが低いサーバーをブロックするように設定されている場合、レピュテーション スコアが低いサーバーに対するすべての要求が URL カテゴリ操作を考慮せずにドロップされます。

次の図に、Webプロキシが復号ポリシー グループに対してクライアント要求を評価する方法を示します。「[復号ポリシーアクションの適用](#)」に、復号ポリシーの制御設定を評価するときに Webプロキシで使用する順序が表示されます。[Figure 9: アクセス ポリシーのアクションの適用, on page 387](#)には、アクセスポリシーの制御設定を評価するときに Webプロキシで使用する順序が表示されます。

Figure 4: 復号ポリシーアクションの適用

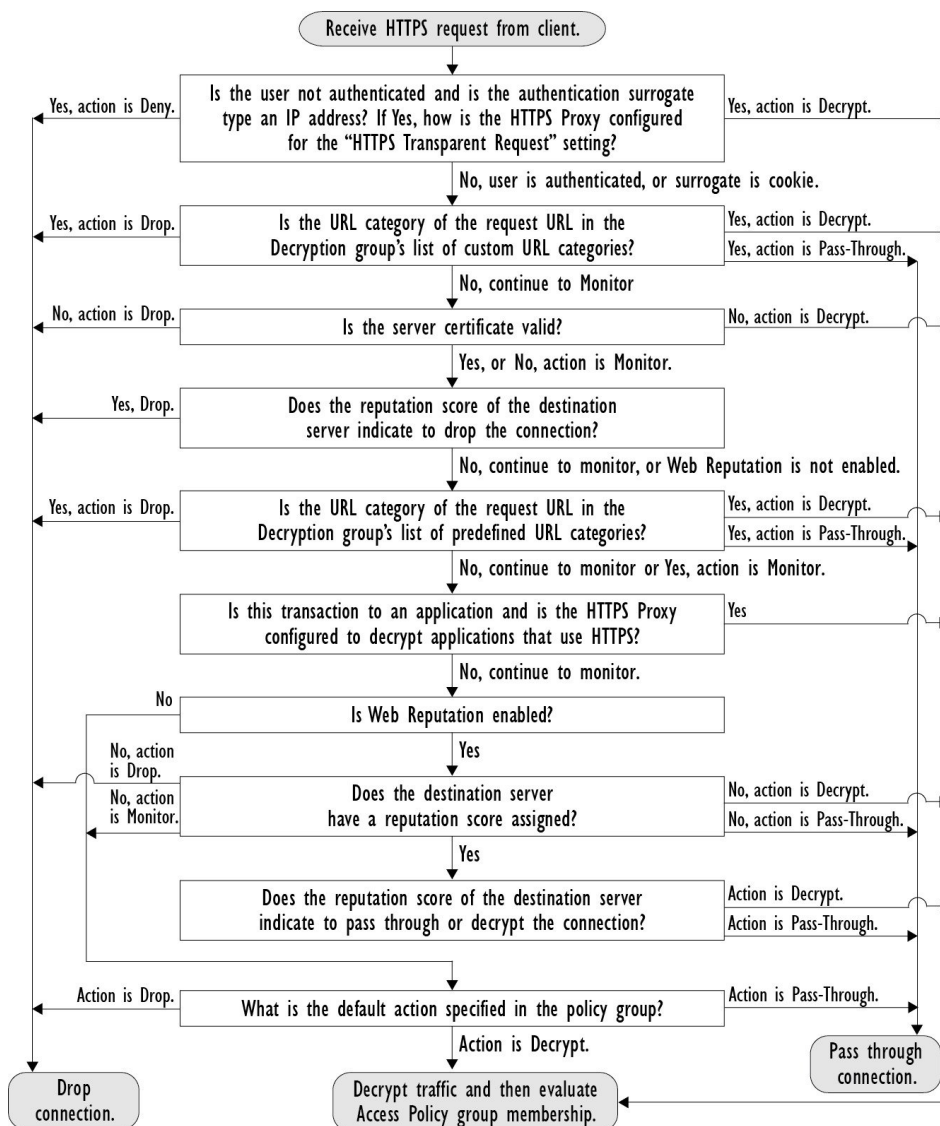
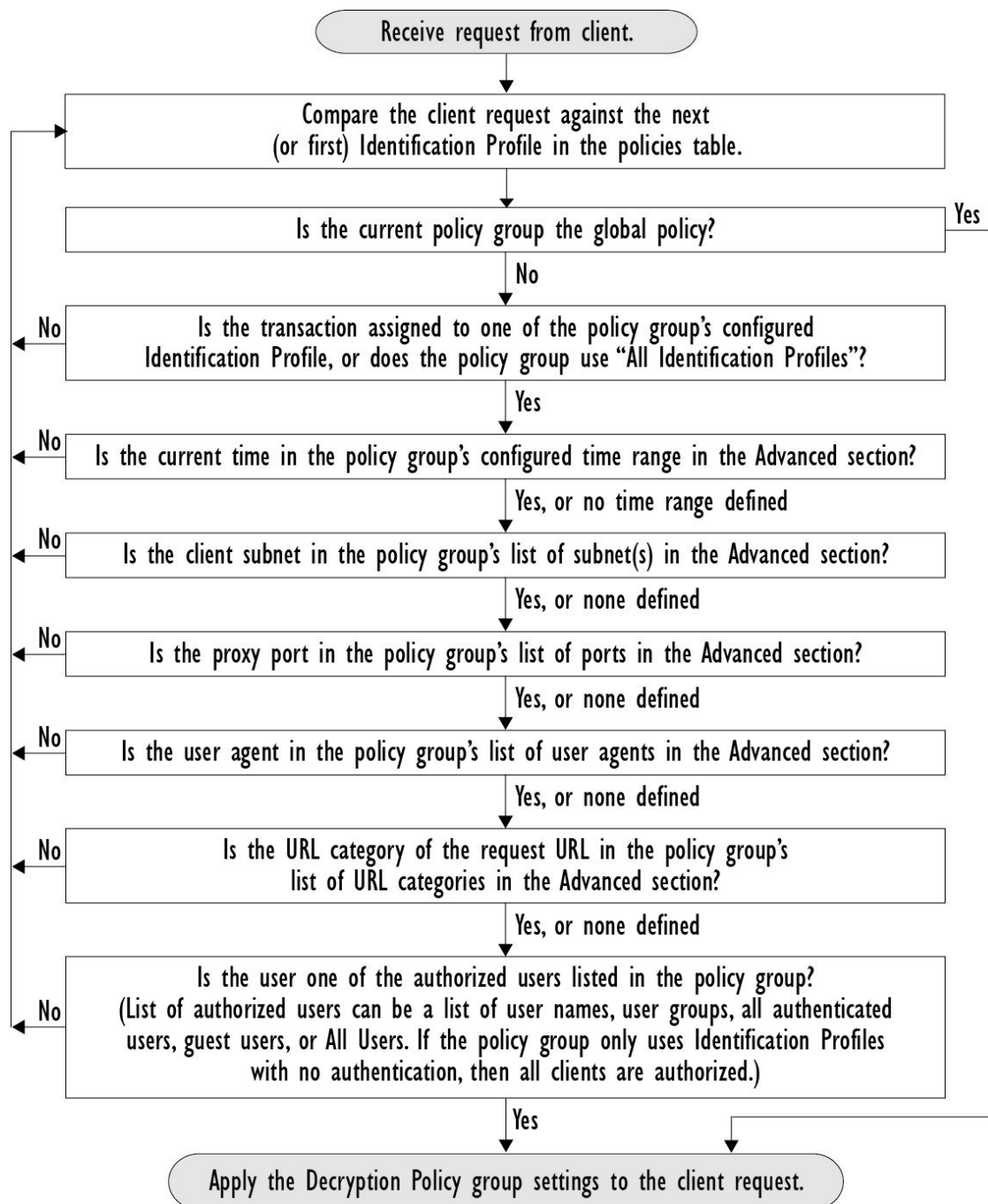


Figure 5: 復号ポリシーのポリシー グループ トランザクション フロー



## HTTPS プロキシのイネーブル化

HTTPS トラフィックをモニターして復号するには、HTTPS プロキシをイネーブルにする必要があります。HTTPS プロキシをイネーブルにする場合は、アプライアンスが、ネットワークのクライアント アプリケーションに自己署名済みサーバー証明書を送信するときに使用する

ルート証明書を設定します。組織の既存のルート証明書およびキーをアップロードするか、ユーザーが入力した情報で証明書およびキーを生成するようにアプライアンスを設定することができます。

HTTPS プロキシをイネーブルした後は、すべての HTTPS ポリシー決定が復号ポリシーによって処理されます。また、このページで、サーバー証明書が無効な場合の、アプライアンスによる HTTPS トラフィックの処理も設定できます。

### Before you begin

HTTPS プロキシをイネーブルにすると、アクセス ポリシー内の HTTPS 専用のルールがディセーブルになり、Web プロキシは HTTP 用のルールを使用して、復号された HTTPS トラフィックを処理します。

## Procedure

**ステップ 1** [セキュリティ サービス (Security Services)] > [HTTPS プロキシ (HTTPS Proxy)] に移動し、[設定の有効化と編集 (Enable and Edit Settings)] をクリックします。

HTTPS プロキシ ライセンス契約書が表示されます。

**ステップ 2** HTTPS プロキシ ライセンス契約書の条項を読み、[同意する (Accept)] をクリックします。

**ステップ 3** [HTTPS プロキシを有効にする (Enable HTTPS Proxy)] フィールドがイネーブルであることを確認します。

**ステップ 4** [HTTPS ポートからプロキシへ (HTTPS Ports to Proxy)] フィールドに、アプライアンスが HTTPS トラフィックをチェックするポートを入力します。ポート 443 がデフォルト ポートです。

### Note

Secure Web Appliance はプロキシとして最大 30 ポートを使用できます。3 ポートは常に FTP プロキシ用に予約されており、27 ポートは HTTP および HTTPS プロキシとして構成できます。

**ステップ 5** 復号に使用するルート/署名証明書をアップロードまたは生成します。

### Note

アップロードされた証明書とキーのペアと、生成された証明書とキーのペアの両方がアプライアンスにある場合は、[署名用ルート証明書 (Root Certificate for Signing)] セクションで選択されている証明書とキーのペアのみを使用します。

**ステップ 6** [HTTPS 透過的要求 (HTTPS Transparent Request)] セクションで、以下のオプションのいずれかを選択します。

- Decrypt the HTTPS request and redirect for authentication (HTTPS 要求を復号して、認証のためにリダイレクトする)
- Deny the HTTPS request (HTTPS 要求を拒否する)

この設定は、認証サロゲートとして IP アドレスを使用するトランザクションだけに、ユーザーがまだ認証されていない場合に適用されます。

### Note

このフィールドは、アプライアンスが透過モードで展開されている場合にだけ表示されます。

**ステップ 7** [HTTPSを使用するアプリケーション（Applications that Use HTTPS）] セクションで、アプリケーションの可視性とコントロール、およびアプリケーションの検出と制御を向上させるために復号をイネーブルにするかどうか選択します。

**Note**

署名用ルート証明書がクライアントにインストールされていない場合は、復号により、アプリケーションでエラーが発生することがあります。アプライアンス ルート証明書の詳細については、[証明書の検証と HTTPS の復号の管理](#), on page 355 を参照してください。

**ステップ 8** 変更を送信し、保存します。

### What to do next

#### 関連項目

- [証明書の検証と HTTPS の復号の管理](#), on page 355

## HTTPS トラフィックの制御

Secure Web Applianceが復号ポリシー グループに HTTPS 接続要求を割り当てた後、接続要求は、そのポリシー グループの管理設定を継承します。復号ポリシー グループの管理設定で、アプライアンスが接続を復号するか、ドロップするか、またはパススルーするかが決定されます。

| オプション                               | 説明                                                                                                                                                                                                                                                                                               |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URL カテゴリ（URL Categories）</b>     | <p>定義済みおよびカスタムの各 URL カテゴリについて、HTTPS 要求で実行するアクションを設定できます。[URL フィルタリング（URL Filtering）] 列にある、設定するポリシー グループのリンクをクリックします。</p> <p><b>Note</b><br/>HTTPS 要求の特定の URL カテゴリをドロップ（エンドユーザー通知なし）するのではなく、ブロック（エンドユーザー通知あり）する場合は、復号ポリシー グループのその URL カテゴリの復号を選択し、その後に、アクセス ポリシー グループの同じ URL カテゴリのブロックを選択します。</p> |
| <b>Web レピュテーション（Web Reputation）</b> | <p>要求されたサーバーの Web レピュテーション スコアに基づいて、HTTPS 要求に対して実行するアクションを設定できます。[Web レピュテーション（Web Reputation）] 列にある、設定するポリシー グループのリンクをクリックします。</p>                                                                                                                                                              |

| オプション                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| デフォルト アクション (Default Action) | <p>他に該当する設定がない場合にアプライアンスが実行する必要があるアクションを設定できます。[デフォルト アクション (Default Action) ] 列にある、設定するポリシー グループのリンクをクリックします。</p> <p><b>Note</b><br/>設定されたデフォルトアクションは、下される決定が、URL カテゴリと Web レピュテーション スコアのどちらにも基づいていない場合にのみ、トランザクションに影響します。Web レピュテーション フィルタリングがディセーブルの場合は、デフォルト アクションが、URL カテゴリの Monitor アクションに一致するすべてのトランザクションに適用されます。Web レピュテーション フィルタリングがイネーブルの場合は、スコアなしのサイトに Monitor アクションが選択されている場合にのみ、デフォルト アクションが使用されます。</p> |

Web レピュテーション スコアが高い暗号化トラフィックをバイパスするには、[HTTPS プロキシ設定 (HTTPS Proxy Settings) ] ページの [復号オプション (Decryption Options) ] セクションにある [アプリケーション検出のための復号 (Decrypt for Application Detection) ] オプションをオフにしてください。

次の図に、アプライアンスが特定の復号ポリシーを HTTPS 要求に割り当てた後に、その要求で実行するアクションを決定する方法を示します。宛先サーバーの Web レピュテーション スコアが評価されるのは1回だけですが、その結果は、決定フローの2つのポイントで適用されます。たとえば、Web レピュテーション スコアのドロップアクションは、定義済みの URL カテゴリに指定されているあらゆるアクションに優先することに注意してください。



```

graph TD
 Start([Receive HTTPS request from client]) --> Q1{Is the user not authenticated and is the authentication surrogate type an IP address? If Yes, how is the HTTPS Proxy configured for the "HTTPS Transparent Request" setting?}

 Q1 -- "Yes, action is Deny." --> Drop1([Drop connection.])
 Q1 -- "No, user is authenticated, or surrogate is cookie." --> Q2{Is the URL category of the request URL in the Decryption group's list of custom URL categories?}

 Q2 -- "Yes, action is Drop." --> Drop1
 Q2 -- "No, continue to Monitor" --> Q3{Is the server certificate valid?}
 Q2 -- "Yes, action is Decrypt.
Yes, action is Pass-Through." --> End([Pass through connection.])

 Q3 -- "No, action is Decrypt." --> End
 Q3 -- "Yes, or No, action is Monitor." --> Q4{Does the reputation score of the destination server indicate to drop the connection?}

 Q4 -- "Yes, Drop." --> Drop1
 Q4 -- "No, continue to monitor, or Web Reputation is not enabled." --> Q5{Is the URL category of the request URL in the Decryption group's list of predefined URL categories?}

 Q5 -- "Yes, action is Drop." --> Drop1
 Q5 -- "Yes, action is Decrypt.
Yes, action is Pass-Through." --> End
 Q5 -- "No, continue to monitor or Yes, action is Monitor." --> Q6{Is this transaction to an application and is the HTTPS Proxy configured to decrypt applications that use HTTPS?}

 Q6 -- "Yes" --> End
 Q6 -- "No, continue to monitor." --> Q7{Is Web Reputation enabled?}

 Q7 -- "No" --> Drop1
 Q7 -- "Yes" --> Q8{Does the destination server have a reputation score assigned?}

 Q8 -- "No, action is Drop."
"No, action is Monitor." --> Drop1
 Q8 -- "Yes" --> Q9{Does the reputation score of the destination server indicate to pass through or decrypt the connection?}

 Q9 -- "Action is Decrypt."
"Action is Pass-Through." --> End
 Q9 -- "Action is Drop." --> Drop1

 Drop1 --> Drop1
 End --> End

```

The flowchart illustrates the decryption process flow, starting with receiving an HTTPS request from a client. It proceeds through several decision points based on authentication, URL categories, server certificates, reputation scores, and policy configurations. The final outcome is either dropping the connection, decrypting traffic and evaluating Access Policy group membership, or passing through the connection.

HTTPS プロキシのイネーブル化, on page 348で説明したように、HTTPS プロキシがイネーブルであることを確認します。

**ステップ1** 「セキュリティサービス (Security Services)」 > 「HTTPSプロキシ (HTTPS Proxy)」に移動します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** 復号オプションをイネーブルにします。

**Note**

このオプションを有効化すると、一部の HTTPS アプリケーションの検出効率が向上します。ただし、署名用ルート証明書がクライアントにインストールされていない場合は、復号によりその他の HTTPS アプリケーションでエラーが発生することがあります。使用許可コントロールで ADC または AVC を選択すると、アプリケーション識別のために復号されます。

| 復号オプション           | 説明                                                                                                                                           |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 認証のための復号          | この HTTPS トランザクションの前に認証されていないユーザーに復号を許可して、認証されるようにします。                                                                                        |
| エンドユーザー通知のための復号   | AsyncOS がエンドユーザー通知を表示できるように復号を許可します。<br><b>Note</b><br>証明書が無効であり、無効な証明書をドロップするように設定されている場合は、最初にロギングされたトランザクションのアクションがポリシー トレースの実行時に「復号」されます。 |
| エンドユーザー確認応答のための復号 | この HTTPS トランザクションの前に Web のプロキシに確認応答していないユーザーに復号を許可し、AsyncOS がエンドユーザーの確認応答を表示できるようにします。                                                       |
| アプリケーション検出のための復号  | AsyncOS が HTTPS アプリケーションを検出する機能を強化します。                                                                                                       |

## 認証および HTTPS 接続

HTTPS 接続レイヤでの認証は、以下のタイプの要求で使用できます。

| オプション                           | 説明                                                                                                                                      |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 明示的要求<br>(Explicit requests)    | <ul style="list-style-type: none"> <li>セキュア クライアント認証がディセーブルである、または</li> <li>セキュア クライアント認証がイネーブルで、サロゲートが IP ベースである</li> </ul>            |
| 透過的要求<br>(Transparent requests) | <ul style="list-style-type: none"> <li>サロゲートが IP ベースで、認証の復号がイネーブル、または</li> <li>サロゲートが IP ベースで、クライアントが以前に HTTP 要求を使用して認証されている</li> </ul> |

## ルート証明書

HTTPS プロキシは、アプライアンスにアップロードした秘密キー ファイルとルート証明書を使用して、トラフィックを復号します。アプライアンスにアップロードするルート証明書ファ

イルと秘密キー ファイルは、PEM 形式である必要があります。DER 形式はサポートされていません。

ルート証明書の情報は、以下のように入力できます。

- **生成する。**基本的な設定情報を入力してから、ボタンをクリックすると、アプライアンスが、残りの証明書と秘密キーを生成します。
- **アップロードする。**アプライアンスの外部で作成された証明書ファイルと、それに一致する秘密キー ファイルをアップロードできます。

**Note**

また、ルート認証局によって署名された中間証明書をアップロードすることもできます。Web プロキシがサーバー証明書を模倣すると、アップロードされた証明書とともに、模倣された証明書がクライアントアプリケーションに送信されます。このように、クライアントアプリケーションが信頼するルート認証局によって中間証明書が署名されている限り、アプリケーションは模倣されたサーバー証明書も信頼します。詳細については、[証明書およびキーについて, on page 201](#)を参照してください。

Secure Web Applianceが作成したルート証明書を処理する場合は、以下のいずれかを選択できます。

- **ルート証明書を受け入れるようにユーザーに通知します。**組織内のユーザーに、企業の新しいポリシーについて通知し、組織が提供したルート証明書を、信頼できる認証局として受け入れるように指示できます。
- **クライアントマシンにルート証明書を追加します。**ネットワーク上のすべてのクライアントマシンに、信頼できるルート認証局としてルート証明書を追加できます。そうすれば、クライアントアプリケーションは自動的にルート証明書を持つトランザクションを受け入れるようになります。

**Procedure**

**ステップ 1** [セキュリティサービス (Security Services) ] > [HTTPSプロキシ (HTTPS Proxy) ] に移動します。

**ステップ 2** [設定の編集 (Edit Settings) ] をクリックします。

**ステップ 3** 生成またはアップロードされた証明書の [証明書のダウンロード (Download Certificate) ] リンクをクリックします。

**Note**

クライアントマシンで証明書エラーが表示される可能性を減らすには、Secure Web Applianceにルート証明書を生成またはアップロードした後に変更を送信してから、クライアントマシンに証明書を配布し、その後にアプライアンスへの変更をコミットします。

## 証明書の検証と HTTPS の復号の管理

Secure Web Applianceは証明書を検証してから、コンテンツを検査して復号します。

### 有効な証明書

有効な証明書の条件：

- 有効期限が切れていない。現在の日付が証明書の有効期間内です。
- 公認の認証局である。発行認証局は、Secure Web Applianceに保存されている、信頼できる認証局のリストに含まれています。
- 有効な署名がある。デジタル署名が、暗号規格に基づいて適切に実装されています。
- 名前が一貫している。通常名が、HTTP ヘッダーで指定されたホスト名に一致します。
- 失効していない。発行認証局が証明書を無効にしません。

### 関連項目

- [リアルタイムの失効ステータス チェックの有効化, on page 359](#)
- [無効な証明書の処理の設定, on page 357](#)
- [証明書失効ステータスのチェックのオプション, on page 358](#)

### 無効な証明書の処理

アプライアンスは、無効なサーバー証明書に対して、以下のアクションの 1 つを実行できます。

- 切断。
- 復号。
- モニタ。

### 複数の理由で無効となる証明書

認識できないルート認証局と期限切れ証明書の両方の理由により無効なサーバー証明書に対して、HTTPS プロキシは、認識できないルート認証局に適用されるアクションを実行します。

それ以外のすべての場合は、同時に複数の理由により無効なサーバー証明書に対して HTTPS プロキシは、制限レベルが最高のアクションから最低のアクションへの順にアクションを実行します。

### 復号された接続の、信頼できない証明書の警告

Secure Web Applianceが無効な証明書を検出し、接続を復号するように設定されている場合、AsyncOS は、信頼できない証明書を作成します。エンドユーザは、これを受け入れるか、拒否する必要があります。証明書の一般名は「Untrusted Certificate Warning」です。

この信頼できない証明書を信頼できる証明書のリストに追加すると、エンドユーザーは接続を受け入れるか拒否するかを選択できなくなります。

AsyncOS は、これらの証明書のいずれかを生成するときに、「Signing untrusted key」または「Signing untrusted cert」というテキストのプロキシ ログ エントリを作成します。

## ルート証明書およびキーのアップロード

### Before you begin

HTTPS プロキシをイネーブルにします。 [HTTPS プロキシのイネーブル化, on page 348](#)。

### Procedure

**ステップ 1** [セキュリティサービス (Security Services)] > [HTTPS プロキシ (HTTPS Proxy)] に移動します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** [アップロードされた証明書とキーを使用 (Use Uploaded Certificate and Key)] を選択します。

**ステップ 4** [証明書 (Certificate)] フィールドで [参照 (Browse)] をクリックし、ローカルマシンに保存されている証明書ファイルに移動します。

アップロードするファイルに複数の証明書またはキーが含まれている場合、Web プロキシはファイル内の先頭の証明書またはキーを使用します。

**ステップ 5** [キー (Key)] フィールドで [参照 (Browse)] をクリックし、秘密キー ファイルに移動します。

#### Note

キーの長さは 512、1024、または 2048 ビットである必要があります。

**ステップ 6** キーが暗号化されている場合は、[キーは暗号化されています (Key is Encrypted)] を選択します。

**ステップ 7** [ファイルのアップロード (Upload Files)] をクリックして、証明書およびキーのファイルを Secure Web Appliance に転送します。

アップロードされた証明書の情報が [HTTPS プロキシ設定を編集 (Edit HTTPS Proxy Settings)] ページに表示されます。

**ステップ 8** (任意) [証明書のダウンロード (Download Certificate)] をクリックすると、ネットワーク上のクライアント アプリケーションに証明書を転送できます。

**ステップ 9** 変更を送信し、保存します。

## HTTPS プロキシ用の証明書およびキーの生成

### Before you begin

HTTPS プロキシをイネーブルにします。 [HTTPS プロキシのイネーブル化, on page 348](#)。

## Procedure

- ステップ 1** [セキュリティサービス (Security Services)] > [HTTPSプロキシ (HTTPS Proxy)] に移動します。
- ステップ 2** [設定の編集 (Edit Settings)] をクリックします。
- ステップ 3** [生成された証明書とキーを使用 (Use Generated Certificate and Key)] を選択します。
- ステップ 4** [新しい証明書とキーを生成 (Generate New Certificate and Key)] をクリックします。
- ステップ 5** [証明書とキーを生成 (Generate Certificate and Key)] ダイアログボックスで、ルート証明書に表示する情報を入力します。
- [共通名 (Common Name)] フィールドには、スラッシュ (/) を除く任意の ASCII 文字を入力できます。
- ステップ 6** [生成 (Generate)] をクリックします。
- ステップ 7** 生成された証明書の情報が [HTTPS プロキシ設定を編集 (Edit HTTPS Proxy Settings)] ページに表示されます。
- ステップ 8** (任意) [証明書のダウンロード (Download Certificate)] をクリックすると、ネットワーク上のクライアントアプリケーションに証明書を転送できます。
- ステップ 9** (任意) [証明書署名要求のダウンロード (Download Certificate Signing Request)] リンクをクリックすると、証明書署名要求 (CSR) を認証局 (CA) に送信できます。
- ステップ 10** (任意) CA から署名付き証明書を受信した後、それを Secure Web Appliance にアップロードします。この操作は、アプライアンスで証明書を生成した後はいつでも実行できます。
- ステップ 11** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## 無効な証明書の処理の設定

### Before you begin

[HTTPS プロキシのイネーブル化, on page 348](#)で説明したように、HTTPS プロキシがイネーブルであることを確認します。

## Procedure

- ステップ 1** [セキュリティサービス (Security Services)] > [HTTPSプロキシ (HTTPS Proxy)] に移動します。
- ステップ 2** [設定の編集 (Edit Settings)] をクリックします。
- ステップ 3** 証明書エラーのタイプごとに、プロキシの応答 (ドロップ、復号、モニター) を定義します。

| 証明書エラーのタイプ | 説明                     |
|------------|------------------------|
| 期限切れ       | 現在の日付が、証明書の有効範囲外にあります。 |

| 証明書エラーのタイプ       | 説明                                                                                                                                                                                                                 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ホスト名の不一致         | 証明書にあるホスト名が、クライアントがアクセスしようとしたホスト名に一致しません。<br><br><b>Note</b><br>明示的な転送モードで展開されている場合にのみ、Web プロキシはホスト名の照合を実行できます。透過モードで展開されている場合は、宛先サーバーのホスト名がわからない（わかっているのは IP アドレスのみです）ため、ホスト名をサーバー証明書のホスト名と比較できません。               |
| 認識できないルート認証局/発行元 | ルート認証局または中間認証局が認識されません。                                                                                                                                                                                            |
| 無効な署名証明書         | 署名証明書に問題があります。                                                                                                                                                                                                     |
| 無効なリーフ証明書        | リーフ証明書に、拒否、でコード、または不一致などの問題が発生しました。                                                                                                                                                                                |
| その他のエラー タイプ      | 他のほとんどのエラー タイプは、アプライアンスが HTTPS サーバーとの SSL ハンドシェイクを完了できないことが原因です。サーバー証明書の詳細なエラー シナリオに関する情報については、 <a href="http://www.openssl.org/docs/apps/verify.html">http://www.openssl.org/docs/apps/verify.html</a> を参照してください。 |

**ステップ 4** 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

## 証明書失効ステータスのチェックのオプション

発行認証局が証明書を失効させたかどうかを特定するために、Secure Web Applianceでは、次の方法で発行認証局をチェックできます。

- **証明書失効リスト（Comodo 証明書のみ）**。Secure Web Applianceは Comodo の証明書失効リストをチェックします。Comodo は、このリストを独自のポリシーに従って更新して維持します。最後に更新された日時によっては、Secure Web Applianceがチェックした時点では、証明書失効リストが古くなっている可能性があります。
- **オンライン証明書ステータス プロトコル（OCSP）**。Secure Web Applianceが、発行認証局で失効ステータスをリアルタイムでチェックします。発行認証局が OCSP をサポートしている場合は、リアルタイム ステータス チェック用の URL が証明書に含まれています。この機能は、新規インストールではデフォルトでイネーブルになり、更新ではデフォルトでディセーブルになります。



### Note

Secure Web Applianceは、他のすべての点で有効であることを特定し、OCSP URL を含んでいる証明書の OCSP クエリーのみを実行します。

## 関連項目

- [リアルタイムの失効ステータス チェックの有効化, on page 359](#)
- [無効な証明書の処理の設定, on page 357](#)

## リアルタイムの失効ステータス チェックの有効化

## Before you begin

HTTPS プロキシがイネーブルであることを確認します。 [HTTPS プロキシのイネーブル化, on page 348](#)を参照してください。

## Procedure

**ステップ 1** [セキュリティ サービス (Security Services)] > [HTTPS プロキシ (HTTPS Proxy)] に移動します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** [オンライン証明書ステータス プロトコル (OCSP) を有効にする (Enable Online Certificate Status Protocol (OCSP))] を選択します。

**ステップ 4** [OCSP結果処理 (Result Handling)] の各プロパティを設定します。

シスコでは、OCSP 結果処理のオプションを、無効な証明書の処理のオプションと同じアクションに設定することを推奨します。たとえば、[モニターする期限切れ証明書 (Expired Certificate to Monitor)] を設定する場合は、モニターする失効証明書を設定します。

**ステップ 5** (任意) [詳細 (Advanced)] 設定セクションを展開し、以下の設定項目を設定します。

| フィールド名                                                         | 説明                                                                                      |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| OCSP 有効応答キャッシュ タイムアウト (OCSP Valid Response Cache Timeout)      | 有効な OCSP 応答を再確認する前に待機する時間。単位は秒 (s)、分 (m)、時間 (h)、または日 (d)。デフォルトの単位は秒です。有効な範囲は 1 秒～7 日です。 |
| OCSP 無効応答キャッシュ タイムアウト (OCSP Invalid Response Cache Timeout)    | 無効な OCSP 応答を再確認する前に待機する時間。単位は秒 (s)、分 (m)、時間 (h)、または日 (d)。デフォルトの単位は秒です。有効な範囲は 1 秒～7 日です。 |
| OCSP ネットワーク エラーキャッシュ タイムアウト (OCSP Network Error Cache Timeout) | 応答がなかった後に、OCSP 応答側に連絡を再度試みる前に待機する時間。単位は秒 (s)、分 (m)、時間 (h)、または日 (d)。有効な範囲は 1 秒～24 時間です。  |



| フィールド名                                                           | 説明                                                                                                           |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 許容されるクロックスキュー (Allowed Clock Skew)                               | Secure Web Applianceと OCSP 応答側の間で許容される設定時間の差の最大値。単位は秒 (s) または分 (m)。有効な範囲は 1 秒～ 60 分です。                       |
| OCSP 応答待機最大時間 (Maximum Time to Wait for OCSP Response)           | OCSP 応答側からの応答を待機する時間の最大値。有効な範囲は 1 秒～ 10 分です。OCSP レスポンダを使用できない場合に、HTTPS 要求へのエンドユーザーアクセスの遅延を短縮するには、短い期間を指定します。 |
| OCSP チェックにアップストリームプロキシを使用 (Use upstream proxy for OCSP checking) | アップストリームプロキシのグループ名。                                                                                          |
| アップストリームプロキシから除外するサーバー (Servers exempt from upstream proxy)      | 除外するサーバーの IP アドレスまたはホスト名。空白のままにすることもできます。                                                                    |

**ステップ 6** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## 信頼できるルート証明書

Secure Web Applianceには、信頼できるルート証明書のリストが付属し、これが維持されます。信頼できる証明書を持つ Web サイトでは、復号は必要ありません。

信頼できる証明書のリストに証明書を追加し、機能的に証明書を削除すると、信頼できる証明書のリストを管理できます。Secure Web Applianceでは、プライマリリストから証明書は削除されませんが、ユーザーが証明書の信頼を無効化できます。これで、信頼できるリストから証明書が機能的に削除されます。

### 信頼できるリストへの証明書の追加

#### Before you begin

HTTPS プロキシがイネーブルであることを確認します。[HTTPS プロキシのイネーブル化, on page 348](#)を参照してください。

#### Procedure

**ステップ 1** [セキュリティサービス (Security Services)] > [HTTPSプロキシ (HTTPS Proxy)] に移動します。

**ステップ 2** [信頼できるルート証明書の管理 (Manage Trusted Root Certificates)] をクリックします。

**ステップ3** [インポート (Import)] をクリックします。

**ステップ4** [参照 (Browse)] をクリックして証明書ファイルに移動します。

**ステップ5** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

[カスタム信頼済みルート証明書 (Custom Trusted Root Certificates)] リストで、アップロードした証明書を探します。

## 信頼できるリストからの証明書の削除

### Procedure

**ステップ1** [セキュリティ サービス (Security Services)] > [HTTPS プロキシ (HTTPS Proxy)] を選択します。

**ステップ2** [信頼できるルート証明書の管理 (Manage Trusted Root Certificates)] をクリックします。

**ステップ3** リストから削除する証明書に対応する [信頼をオーバーライド (Override Trust)] チェックボックスを選択します。

**ステップ4** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## HTTPS トラフィックのルーティング

クライアントのヘッダーに保存されている情報に基づいて HTTPS トランザクションをルーティングする AsyncOS の機能は限定的であり、透過 HTTPS と明示 HTTPS で異なります。

| オプション    | 説明                                                                                                                                                                                                         |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 透過 HTTPS | 透過 HTTPS の場合は、AsyncOS がクライアントのヘッダー情報にアクセスできません。したがって、ルーティングポリシーまたは識別プロファイルがクライアントヘッダー内の情報に依存している場合、AsyncOS はルーティングポリシーを適用できません。                                                                            |
| 明示 HTTPS | <p>明示 HTTPS の場合、AsyncOS は、クライアントヘッダー内の以下の情報にアクセスできます。</p> <ul style="list-style-type: none"> <li>• URL</li> <li>• 宛先ポート番号</li> </ul> <p>したがって、明示 HTTPS トランザクションでは、URL またはポート番号に基づいてルーティング ポリシーを照合できます。</p> |

## 暗号化/HTTPS/証明書のトラブルシューティング

- URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス, on page 749
- IP ベースのサロゲートと透過的要求を含む HTTPS, on page 749
- 特定 Web サイトの復号のバイパス, on page 750
- アラート：セキュリティ証明書に関する問題（Problem with Security Certificate）, on page 751

## インターネット要求を制御するポリシーの作成

この章で説明する内容は、次のとおりです。

- ポリシーの概要：代行受信されたインターネット要求の制御（362 ページ）
- ポリシー タスクによる Web 要求の管理：概要（364 ページ）
- ポリシーによる Web 要求の管理：ベスト プラクティス（364 ページ）
- ポリシー（364 ページ）
- ポリシーの設定（376 ページ）
- トランザクション要求のブロック、許可、リダイレクト（385 ページ）
- クライアント アプリケーション（388 ページ）
- 時間範囲およびクォータ（389 ページ）
- URL カテゴリによるアクセス制御（394 ページ）
- リモートユーザー（396 ページ）
- ポリシーに関するトラブルシューティング（399 ページ）

## ポリシーの概要：代行受信されたインターネット要求の制御

ユーザーが Web 要求を作成すると、設定されている Secure Web Applianceが要求を代行受信し、最終結果を得るまでに要求が通過するプロセスを管理します。最終結果は特定の Web サイトや電子メールにアクセスすることであったり、さらにはオンラインアプリケーションにアクセスすることであったりします。Secure Web Applianceのポリシーを設定する際に、ユーザーからの要求の基準とアクションを定義するためにポリシーが作成されます。

ポリシーは、Secure Web Applianceが Web 要求を識別および制御する手段です。クライアントが Web 要求をサーバーに送信すると、Web プロキシはその要求を受信して評価し、要求が属しているポリシーグループを判定します。その後、ポリシーで定義されているアクションが要求に適用されます。

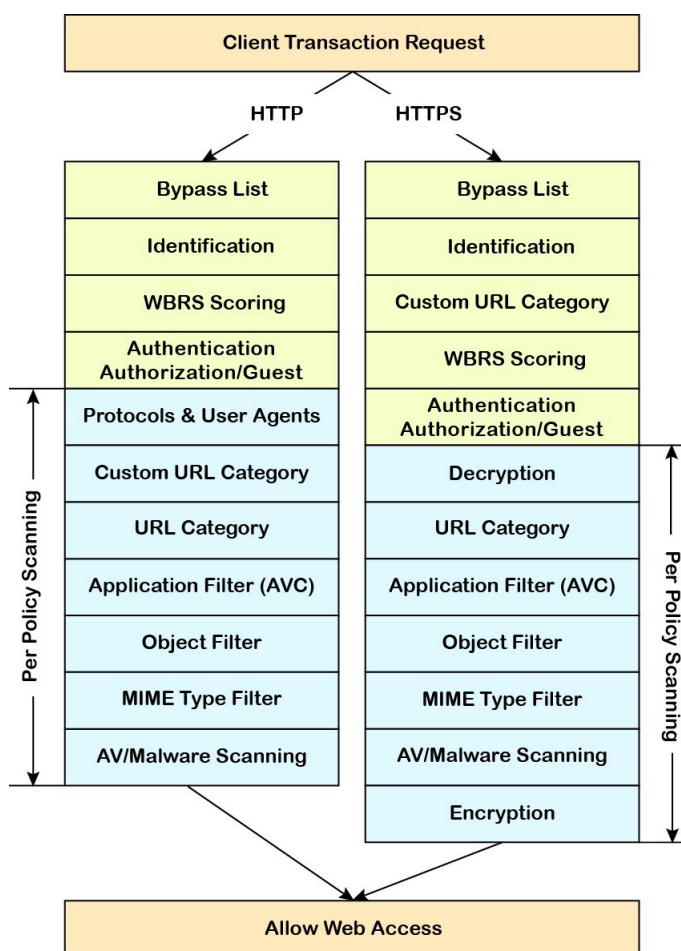
Secure Web Applianceは複数のポリシータイプを使用して、Web 要求のさまざまな側面を管理します。ポリシータイプは独自にトランザクションを全面管理するか、追加の処理のために他のポリシータイプにトランザクションを渡します。ポリシータイプは、実行する機能（アクセス、ルーティング、セキュリティなど）によってグループ化できます。

AsyncOSは、アプライアンスからの不要な外部通信を避けるために、外部の依存関係を評価する前にポリシーに基づいてトランザクションを評価します。たとえば、未分類のURLをブロックするポリシーによってトランザクションがブロックされた場合、そのトランザクションがDNS エラーによって失敗することはありません。

## 代行受信された HTTP/HTTPS 要求の処理

次の図に、代行受信された Web 要求がアプライアンスによって処理される場合のフローを示します。

Figure 7: HTTP/HTTPS トランザクション フロー



さまざまなトランザクション処理フローを示した次の図も参照してください。

- [Figure 2: 識別プロファイルと認証プロセス：サロゲートおよび IP ベースのサロゲートなし, on page 278](#)

- [Figure 3: 識別プロファイルと認証プロセス : Cookie ベースのサロゲート, on page 279](#)
- [Figure 8: アクセス ポリシーのポリシー グループ トランザクション フロー, on page 369](#)
- [Figure 5: 復号ポリシーのポリシー グループ トランザクション フロー, on page 348](#)
- [HTTPS トラフィックの制御, on page 350](#)

## ポリシー タスクによる Web 要求の管理 : 概要

| 手順  | ポリシーによる Web 要求管理のタスク リスト          | 関連項目および手順へのリンク                                                                                                                           |
|-----|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | 認証レールを設定して一定の順序に配置する              | <a href="#">認証レール, on page 90</a>                                                                                                        |
| 2   | (アップストリーム プロキシの場合) プロキシ グループを作成する | <a href="#">アップストリーム プロキシのプロキシ グループの作成, on page 34</a>                                                                                   |
| 2   | (オプション) カスタムクライアントアプリケーションを作成する   | <a href="#">クライアントアプリケーション, on page 388</a>                                                                                              |
| 3   | (オプション) カスタム URL カテゴリを作成する        | <a href="#">カスタム URL カテゴリの作成および編集, on page 305</a>                                                                                       |
| 4   | 識別プロファイルを作成する                     | <a href="#">ユーザーおよびクライアント ソフトウェアの分類, on page 267</a>                                                                                     |
| 5   | (オプション) 時間範囲を作成し、時間帯によってアクセスを制限する | <a href="#">時間範囲およびクォータ, on page 389</a>                                                                                                 |
| [6] | ポリシーを作成して順序付ける                    | <ul style="list-style-type: none"> <li>• <a href="#">ポリシーの作成, on page 369</a></li> <li>• <a href="#">ポリシーの順序, on page 368</a></li> </ul> |

## ポリシーによる Web 要求の管理 : ベスト プラクティス

Active Directory ユーザー オブジェクトを使用して Web 要求を管理する場合は、基準としてプライマリ グループを使用しないでください。Active Directory ユーザー オブジェクトにはプライマリ グループは含まれません。

## ポリシー

- [ポリシー タイプ, on page 365](#)
- [ポリシーの順序, on page 368](#)
- [ポリシーの作成, on page 369](#)

## ポリシータイプ

| ポリシータイプ                                         | 要求タイプ                                                                                          | 説明                                                                                                                                                                                                                                                     | タスクへのリンク                                            |
|-------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| アクセス                                            | <ul style="list-style-type: none"> <li>• HTTP</li> <li>• 復号された HTTPS</li> <li>• FTP</li> </ul> | <p>HTTP、FTP、復号 HTTPS の着信トラフィックをブロック、許可、またはリダイレクトします。</p> <p>HTTPS プロキシがディセーブルの場合、アクセス ポリシーは暗号化された着信 HTTPS トラフィックも管理します。</p>                                                                                                                            | <a href="#">ポリシーの作成, on page 369</a>                |
| SOCKS                                           | <ul style="list-style-type: none"> <li>• SOCKS</li> </ul>                                      | Socks 通信要求を許可またはブロックします。                                                                                                                                                                                                                               | <a href="#">ポリシーの作成, on page 369</a>                |
| アプリケーション認証<br>(Application Authentication)      | <ul style="list-style-type: none"> <li>• アプリケーション</li> </ul>                                   | <p>Software as a Service (SaaS) アプリケーションへのアクセスを許可または拒否します。</p> <p>シングルサインオンを使用してユーザーを認証し、アプリケーションへのアクセスをただちにディセーブルにすることによってセキュリティを向上させます。</p> <p>ポリシーのシングルサインオン機能を使用するには、Secure Web Appliance を ID プロバイダーとして設定し、SaaS の証明書とキーをアップロードまたは作成する必要があります。</p> | <a href="#">SaaS アプリケーション認証ポリシーの作成, on page 404</a> |
| 暗号化<br>HTTPS 管理<br>(Encrypted HTTPS Management) | <ul style="list-style-type: none"> <li>• HTTPS</li> </ul>                                      | <p>HTTPS 接続を復号、パズル、またはドロップします。</p> <p>AsyncOS は、その後の処理のために、復号したトラフィックをアクセス ポリシーに渡します。</p>                                                                                                                                                              | <a href="#">ポリシーの作成, on page 369</a>                |

| ポリシータイプ                                                      | 要求タイプ                                                                                          | 説明                                                                                                                                                                                                                                                                | タスクへのリンク                              |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| データセキュリティ<br>(Data Security)                                 | <ul style="list-style-type: none"> <li>• HTTP</li> <li>• 復号された HTTPS</li> <li>• FTP</li> </ul> | Web へのデータのアップロードを管理します。データセキュリティポリシーは発信トラフィックをスキャンし、宛先とコンテンツに基づいて、トラフィックがデータアップロードの社内規則に準じていることを確認します。スキャンのために外部サーバーに発信トラフィックをリダイレクトする外部 DLP ポリシーとは異なり、データセキュリティポリシーは、Secure Web Applianceを使用してトラフィックをスキャンし、評価します。                                                | <a href="#">ポリシーの作成 , on page 369</a> |
| 外部 DLP<br>(データ漏洩防止)<br>(External DLP (Data Loss Prevention)) | <ul style="list-style-type: none"> <li>• HTTP</li> <li>• 復号された HTTPS</li> <li>• FTP</li> </ul> | サードパーティの DLP システムを実行しているサーバーに発信トラフィックを送信します。DLP システムはトラフィックをスキャンし、トラフィックがデータアップロードに関する社内規則に準拠していることを確認します。データのアップロードも管理するデータセキュリティポリシーとは異なり、外部 DLP ポリシーは Secure Web Appliance をスキャン作業から解放します。これによって、アプライアンスのリソースが解放され、サードパーティ製ソフトウェアによって提供されるその他の機能を活用できるようになります。 | <a href="#">ポリシーの作成 , on page 369</a> |
| 発信マルウェアスキャン<br>(Outbound Malware Scanning)                   | <ul style="list-style-type: none"> <li>• HTTP</li> <li>• 復号された HTTPS</li> <li>• FTP</li> </ul> | <p>悪意のあるデータを含んでいる可能性があるデータのアップロード要求をブロック、モニター、または許可します。</p> <p>ネットワークにすでに存在しているマルウェアが外部ネットワークに送信されるのを防止します。</p>                                                                                                                                                   | <a href="#">ポリシーの作成 , on page 369</a> |

| ポリシータイプ             | 要求タイプ                                                                                    | 説明                                                                                                                                                                                                                                                                                                                                                                          | タスクへのリンク                             |
|---------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| ルーティング<br>(Routing) | <ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> <li>• FTP</li> </ul> | <p>Web トラフィックをアップストリーム プロキシを介して送信するか、または宛先サーバーに送信します。既存のネットワーク設計を保護したり、Secure Web Applianceからの処理をオフロードしたり、サードパーティのプロキシシステムから提供される追加機能を活用したりするために、アップストリームプロキシを介してトラフィックをリダイレクトできます。</p> <p>複数のアップストリームプロキシが使用可能な場合、Secure Web Applianceはロードバランシング技術を使用して、それらのプロキシにデータを分散できます。</p> <p>クライアントの送信元 IP アドレスを保持するか、あるいは Web プロキシ IP または IP スプーフィングプロファイルを使用してカスタム IP に変更します。</p> | <a href="#">ポリシーの作成, on page 369</a> |

各ポリシータイプはポリシーテーブルを使用して、ポリシーを保存および管理します。各ポリシーテーブルには、ポリシータイプのデフォルトアクションを保守管理する、定義済みのグローバルポリシーが用意されています。必要に応じて、追加のユーザー定義ポリシーが作成され、ポリシーテーブルに追加されます。ポリシーは、ポリシーテーブルのリストに記載されている順序で処理されます。

個々のポリシーには、ポリシーが管理するユーザー要求のタイプおよび要求に対して実行するアクションが定義されています。各ポリシー定義には2つのメインセクションがあります。

- **[識別プロファイルとユーザー (Identification Profiles and Users)]** : 識別プロファイルは、ポリシーのメンバーシップ基準で使用されます。Web トランザクションを識別するためのさまざまなオプションが含まれているので特に重要です。また、ポリシーと多くのプロパティを共有します。
- **[詳細設定 (Advanced)]** : ポリシーの適用対象となるユーザーの識別に使用される基準。1つ以上の基準をポリシーで指定でき、基準を満たすにはすべてが一致する必要があります。



- [プロトコル (Protocols)] : さまざまなネットワーク デバイス間でデータを転送できるようにします (http、https、ftp など)。
- [プロキシポート (Proxy Ports)] : 要求が Web プロキシへのアクセスに使用する番号付きのポート。
- [サブネット (Subnets)] : 要求が発信された、接続ネットワーク デバイスの論理グループ (地理的な場所、ローカル エリア ネットワーク (LAN) など)。
- [時間範囲 (Time Range)] : 時間範囲を作成すると、ポリシーでそれを使用し、要求が行われた時間帯に基づいて Web 要求を識別したり、Web 要求にアクションを適用できます。時間範囲は、個々のユニットとして作成されます。
- [URLカテゴリ (URL Categories)] : URL カテゴリは Web サイトの定義済みまたはカスタムのカテゴリです (ニュース、ビジネス、ソーシャルメディアなど)。これらを使用して、Web 要求を識別したり、Web 要求にアクションを適用できます。
- [ユーザーエージェント (User Agents)] : 要求の作成に使用されるクライアントアプリケーション (アップデータや Web ブラウザなど) があります。ユーザー エージェントに基づいてポリシーの基準を定義したり、制御設定を指定できます。認証からユーザーエージェントを除外することもできます。これは、クレデンシャルの入力を求めることができないアプリケーションで役立ちます。カスタム ユーザー エージェントを定義できますが、これらの定義を他のポリシーで再利用することはできません。

**Note**

複数のメンバーシップ基準を定義した場合、クライアント要求は、ポリシーに一致するために、すべての基準を満たす必要があります。

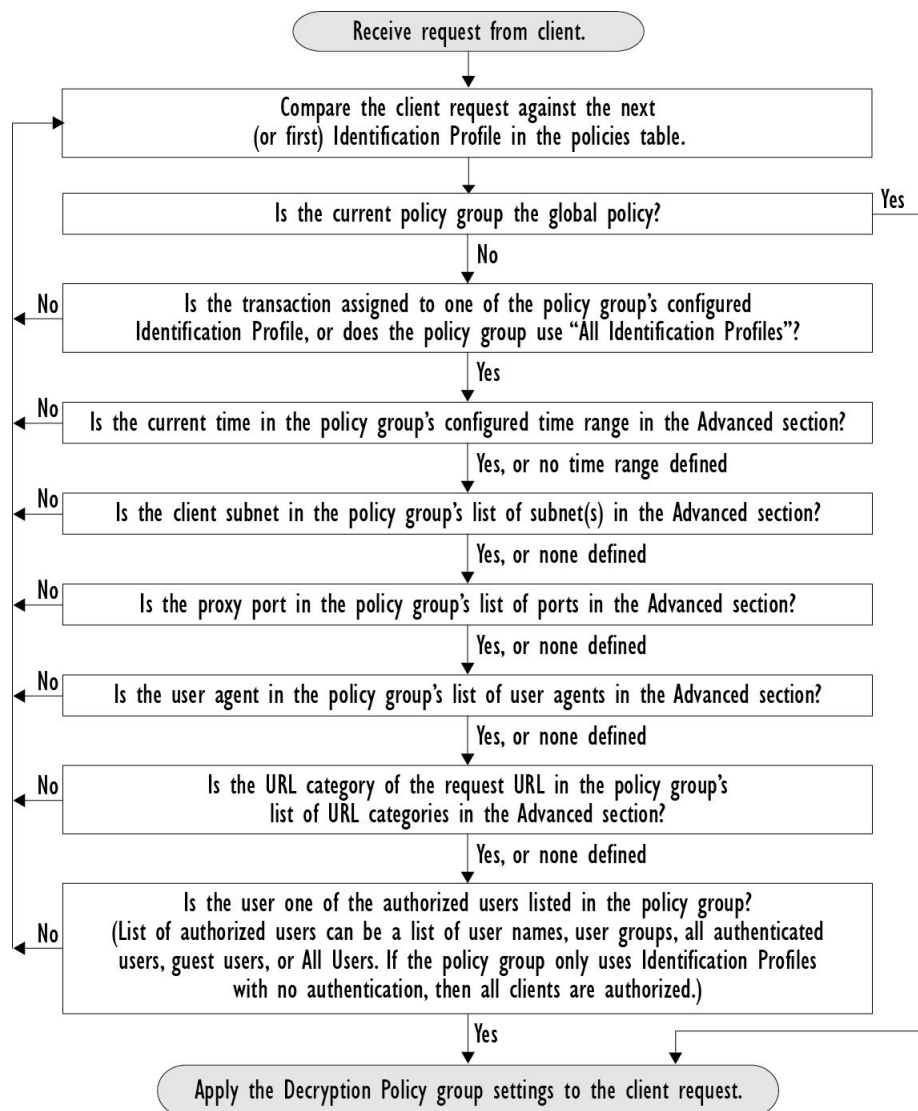
## ポリシーの順序

ポリシー テーブルにポリシーを記載する順序によって、Web 要求に適用されるポリシーの優先順位が決まります。Web 要求との照合はテーブルの最上位のポリシーから順に行われ、要求がポリシーに一致した時点で照合は終了します。テーブル内のそれ以降のポリシーは処理されません。

ユーザ定義のポリシーが Web 要求と一致しない場合、そのポリシー タイプのグローバル ポリシーが適用されます。グローバル ポリシーは常にポリシー テーブルの最後に配置され、順序変更できません。

次の図に、アクセス ポリシー テーブルを介したクライアント要求のフローを示します。

Figure 8: アクセス ポリシーのポリシー グループ トランザクション フロー



## ポリシーの作成

### Before you begin

- 該当するプロキシをイネーブルにします。
  - Web プロキシ (HTTP、復号されたHTTPS、および FTP 用)
  - HTTPS プロキシ (HTTPS Proxy)
  - SOCKS プロキシ (SOCKS Proxy)
- 関連する識別プロファイルを作成します。

- [ポリシーの順序, on page 368](#)について理解しておきます。
- (暗号化された HTTPS のみ) 証明書とキーをアップロードまたは作成します。
- (データセキュリティのみ) Cisco データセキュリティフィルタの設定をイネーブルにします。
- (外部 DLP のみ) 外部 DLP サーバを定義します。
- (ルーティングのみ) Secure Web Appliance に対して関連するアップストリームプロキシを定義します。
- (オプション) 関連するクライアント アプリケーションを作成します。
- (オプション) 関連する時間範囲を作成します。 [時間範囲およびクォータ, on page 389](#)を参照してください。
- (オプション) 関連する URL カテゴリを作成します。 [カスタム URL カテゴリの作成および編集, on page 305](#)を参照してください。

## Procedure

**ステップ 1** [ポリシー設定 (Policy Settings)] セクションで、[アイデンティティを有効化 (Enable Identity)] チェックボックスを使用してこのポリシーをイネーブルにするか、ポリシーを削除せずにただちにディセーブルにします。

**ステップ 2** [名前 (Name)] に一意のポリシー名を割り当てます。

**ステップ 3** [説明 (Description)] は任意です。

**ステップ 4** [上に挿入 (Insert Above)] ドロップダウンリストで、このポリシーを表示するテーブル内の位置を選択します。

### Note

ポリシーを配置します。最上位のものが最も制限が厳しく、最下位のものが最も緩くなります。詳細については、[ポリシーの順序, on page 368](#)を参照してください。

**ステップ 5** [ポリシーの有効期限 (Policy Expires)] エリアで、[ポリシーの有効期限の設定 (Set Expiration for Policy)] チェックボックスをオンにして、ポリシーの有効期限を設定します。設定するポリシーの有効期限の日時を入力します。設定期限を越えると、ポリシーは自動的に無効になります。

### Note

システムは 1 分ごとにポリシーをチェックして、1 分間に有効期限が切れるポリシーを無効にします。たとえば、ポリシーが 11:00 に期限が切れるように設定されている場合、ポリシーは最大で 11:01 までに無効になります。

ポリシーの有効期限機能は、アクセスポリシー、復号ポリシー、および Web トラフィック タップ ポリシーにのみ適用されます。

ポリシーの有効期限の 3 日前にメールが届き、有効期限にもう一度メールが届きます。

### Note

アラートを受信するには、[システム管理 (System Administration)] > [アラート (Alerts)] を使用して、ポリシーの有効期限アラートを有効にする必要があります。[ポリシーの期限切れアラート, on page 193](#)を参照してください

Cisco コンテンツ セキュリティ管理アプライアンスを使用してポリシーの有効期限を設定することもできます。設定された有効期限が過ぎるとポリシーは失効しますが、Cisco コンテンツ セキュリティ管理アプライアンスの GUI では無効と表示されません。

ポリシーの有効期限機能を設定した後、有効期限はアプライアンスのローカル時間の設定に基づいて期限切れとなります。

**ステップ 6** [ポリシーメンバの定義 (Policy Member Definition)] セクションで、ユーザおよびグループのメンバーシップの定義方法を選択します。[識別プロファイルとユーザ (Identification Profiles and Users)] リストから、以下のいずれかを選択します。

- [すべての識別プロファイル (All Identification Profiles)] : このポリシーを既存のすべてのプロファイルに適用します。少なくとも 1 つの [詳細設定 (Advanced)] オプションを定義する必要があります。
- [1つ以上の識別プロファイルを選択 (Select One or More Identification Profiles)] : 個々の識別プロファイルを指定するためのテーブルが表示されます。1 行ごとに 1 つのプロファイル メンバーシップ定義が含まれています。

**ステップ 7** [すべての識別プロファイル (All Identification Profiles)] を選択した場合 :

a) 以下のいずれか 1 つのオプションを選択して、このポリシーを適用する承認済みユーザとグループを指定します。

- [すべての承認済みユーザ (All Authenticated Users)] : 認証または透過的 ID によって識別されたすべてのユーザ。
- [選択されたグループとユーザ (Selected Groups and Users)] : 指定したユーザとグループが使用されます。

指定した **ISE セキュリティ グループ タグ (SGT)** や指定したユーザを追加または編集するには、次の適切なラベルのリンクをクリックします。たとえば、現在指定しているユーザのリストを編集するには、そのリストをクリックします。詳細については、[ポリシーのセキュリティ グループ タグの追加と編集, on page 374](#)を参照してください。

ISE を使用する場合、ISE セキュリティ グループ タグを追加または編集できます。これは ISE-PIC 導入ではサポートされていません。指定した **ISE グループ** を追加または編集するには、次のラベルのリンクをクリックします。このオプションは、ISE-PIC に固有です。

- [ゲスト (Guests)] : ゲストとして接続されているユーザと認証に失敗したユーザ。
- [すべてのユーザ (All Users)] : すべてのクライアント。承認済みかどうかは問いません。このオプションを選択する場合は、少なくとも 1 つの [詳細設定 (Advanced)] オプションを設定する必要があります。

**ステップ 8** [1つ以上の識別プロファイルを選択 (Select One or More Identification Profiles)] を選択すると、プロファイル選択テーブルが表示されます。

- a) [識別プロファイル (Identity Profiles)] 列の [識別プロファイルの選択 (Select Identification Profile)] ドロップダウン リストから、識別プロファイルを選択します。
- b) このポリシーを適用する承認済みユーザとグループを指定します。

- [すべての承認済みユーザ (All Authenticated Users)] : 認証または透過的 ID によって識別されたすべてのユーザ。
- [選択されたグループとユーザ (Selected Groups and Users)] : 指定したユーザとグループが使用されます。

指定した ISE セキュリティ グループ タグ (SGT) や指定したユーザを追加または編集するには、適切なラベルのリンクをクリックします。たとえば、現在指定しているユーザのリストを編集するには、そのリストをクリックします。詳細については、[ポリシーのセキュリティ グループ タグの追加と編集, on page 374](#)を参照してください。

- [ゲスト (Guests)] : ゲストとして接続されているユーザと認証に失敗したユーザ。

- c) プロファイル選択テーブルに行を追加するには、[識別プロファイルの追加 (Add Identification Profile)] をクリックします。行を削除するには、その行のゴミ箱アイコンをクリックします。

必要に応じて、ステップ (a) から (c) を繰り返して必要な識別プロファイルを追加します。

**ステップ 9** [詳細設定 (Advanced)] セクションを展開し、追加のグループ メンバーシップ基準を定義します ([ポリシーメンバの定義 (Policy Member Definition)] セクションで選択したオプションによっては、このステップは任意になります。また、設定するポリシーのタイプによっては、以下のオプションの一部を使用できません)。

| 高度なオプション               | 説明                                                                                                                                                                                                                                                  |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プロトコル (Protocols)      | このポリシーを適用するプロトコルを選択します。[その他のすべて (All others)] は、選択されていないすべてのプロトコルを意味します。関連付けられている識別プロファイルを特定のプロトコルに適用すると、このポリシーもそれらのプロトコルに適用されます                                                                                                                    |
| プロキシ ポート (Proxy Ports) | <p>特定のポートを使用して Web プロキシにアクセスするトラフィックにのみ、このポリシーが適用されます。1 つ以上のポート番号を入力します。複数のポートはカンマで区切ります。</p> <p>明示的な転送接続のために、ブラウザに設定されたポートです。</p> <p>透過接続の場合は、宛先ポートと同じです。</p> <p><b>Note</b><br/>関連付けられている識別プロファイルを特定のプロキシポートにのみ適用している場合は、ここにプロキシ ポートを入力できません。</p> |

| 高度なオプション                  | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サブネット (Subnets)           | <p>特定のサブネットのトラフィックにのみこのポリシーが適用されます。[サブネット指定 (Specify subnets)] を選択し、サブネットをカンマで区切って入力します。</p> <p>サブネットによってさらにフィルタリングしない場合は、[選択したアイデンティティからのサブネットを使用 (Use subnets from selected Identities)] をオンのままにしておきます。</p> <p><b>Note</b><br/>関連する ID を特定のサブネットに適用すると、このポリシーの適用を ID が適用されるアドレスのサブセットに限定できます。</p>                                                                                                                                                                                                                                                                                                                                                 |
| 時間範囲 (Time Range)         | <p>ポリシー メンバーシップに時間範囲を適用できます。</p> <ul style="list-style-type: none"> <li>• [時間範囲 (Time Range)] : 前に定義した時間範囲を選択します (<a href="#">時間範囲およびクォータ, on page 389</a>) 。</li> <li>• [時間範囲の一致 (Match Time Range)] : このオプションを使用して、この時間範囲を含めるか除外するかを指定します。つまり、指定した範囲内のみを照合するか、指定した範囲を除くすべての時間について照合するかを指定します。</li> </ul>                                                                                                                                                                                                                                                                                                                                          |
| URL カテゴリ (URL Categories) | <p>特定の宛先 (URL) と URL カテゴリによってポリシー メンバーシップを制限できます。すべての必要なカスタム カテゴリと定義済みカテゴリを選択します。カスタム カテゴリの詳細については、<a href="#">カスタム URL カテゴリの作成および編集, on page 305</a>を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ユーザ エージェント (User Agents)  | <p>特定のユーザエージェントを選択し、このポリシーのユーザ定義の一部として、正規表現を使用してカスタム エージェントを定義できます。</p> <ul style="list-style-type: none"> <li>• <b>[共通ユーザ エージェント (Common User Agents)]</b> <ul style="list-style-type: none"> <li>• [ブラウザ (Browsers)] : このセクションを展開して、さまざまな Web ブラウザを選択します。</li> <li>• [その他 (Others)] : このセクションを展開して、アプリケーションアップデートなどの特定の非ブラウザ エージェントを選択します。</li> </ul> </li> <li>• [カスタム ユーザ エージェント (Custom User Agents)] : 1 つ以上の正規表現を (1 行に 1 つずつ) 入力して、カスタム ユーザ エージェントを定義できます。</li> <li>• [ユーザ エージェントの一致 (Match User Agents)] : このオプションを使用して、これらのユーザエージェントの指定を含めるか除外するかを指定します。つまり、メンバーシップの定義に選択したユーザ エージェントのみを含めるか、選択したユーザ エージェントを明確に除外するかどうかを指定します。</li> </ul> |

## ポリシーのセキュリティ グループ タグの追加と編集

ポリシーの特定の識別プロファイルに割り当てられているセキュリティグループタグ (SGT) のリストを変更するには、[ポリシーの追加または編集 (Add/Edit Policy)] ページの [選択されたグループとユーザ (Selected Groups and Users)] リストで、[ISEセキュリティグループタグ (ISE Secure Group Tags)] ラベルの後ろのリンクをクリックします。( [ポリシーの作成](#), on [page 369](#) を参照。) このリンクは、[タグが未入力 (No tags entered)] または現在割り当てられているタグのリストです。リンクをクリックすると [セキュリティグループタグの追加または編集 (Add/Edit Group)] ページが開きます。

現在このポリシーに割り当てられている SGT が [承認済みセキュリティグループタグ (Authorized Secure Group Tags)] セクションに表示されます。接続されている ISE サーバから使用可能なすべての SGT が、[セキュリティグループタグの検索 (Secure Group Tag Search)] セクションに表示されます。

### Procedure

**ステップ 1** [承認済みセキュリティグループタグ (Authorized Secure Group Tags)] リストに 1 つ以上の SGT を追加するには、[セキュリティグループタグの検索 (Secure Group Tag Search)] セクションに必要な事項を入力し、[追加 (Add)] をクリックします。

#### Note

- すでに追加されている SGT が緑色で強調表示されます。この利用可能な SGT のリストから特定の SGT を検索するには、[検索 (Search)] フィールドにテキスト文字列を入力します。
- Secure Web Appliance が ISE/ISE-PIC に接続されている場合、ISE/ISE-PIC からのデフォルト SGT も表示されます。これらの SGT には割り当てられたユーザがありません。正しい SGT を選択したことを確認してください。

**ステップ 2** [承認済みセキュリティグループタグ (Authorized Secure Group Tags)] リストから 1 つ以上の SGT を削除するには、削除するエントリを選択し、[削除 (Delete)] をクリックします。

**ステップ 3** [完了 (Done)] をクリックして、[グループの追加または編集 (Add/Edit Group)] ページに戻ります。

### What to do next

#### 関連項目

- [時間範囲およびクォータ](#), on [page 389](#)
- [ポリシーでのクライアントアプリケーションの使用](#), on [page 388](#)

## ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加

ルーティングポリシーにルーティング先と IP スプーフィングプロファイルを設定することによって、Web プロキシが Web トラフィックを転送し、送信元 IP アドレスを要求する方法を設定できます。



**Note**

- デフォルトでは、アップストリーム プロキシ グループがアプライアンス上に設定されていない場合でも、グローバル ルーティング ポリシーは有効になります。
- IP スプーフィングプロファイルはルーティング先とは関連がないため、個別に設定できません。
- ルーティングポリシーは、アップストリームプロキシを設定せずに有効にすることができます。

**Note**

セキュリティ管理アプライアンスでルーティングポリシーのアップストリームプロキシグループを設定するには、**Secure Web Appliance**のコンフィギュレーションファイルを保存し、セキュリティ管理アプライアンスにインポートします。それ以外の場合は、セキュリティ管理アプライアンスはアップストリームプロキシを「見つかりませんでした (Not Found)」として表示し、設定のプッシュ後にルーティングポリシーを無効にします。

**Procedure**

- ステップ 1** [Web Security Manager] > [ルーティングポリシー (Routing Policies)] を選択します。
- ステップ 2** [ルーティングポリシー (Routing Policies)] ページで、アップストリームプロキシグループを設定するルーティングポリシーの [ルーティング先 (Routing Destination)] 列の下にあるリンクをクリックします。
- ステップ 3** 選択したポリシーに適したアップストリームプロキシグループを次から選択します。

| アクション                                                | 説明                                                                                                                                                                            |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [グローバルポリシー設定を使用する (Use Global Policy Settings)]      | Web プロキシは、グローバルポリシーで定義されている設定を使用します。これは、ユーザー定義のポリシー グループのデフォルトアクションです。デフォルトでは、グローバルルーティングポリシーのルーティング先は[直接接続 (Direct Connection)] として設定されます。<br><br>ユーザー定義のポリシー グループにのみ適用されます。 |
| [直接接続 (Direct Connection)]                           | Web プロキシは、Web トラフィックを宛先 Web サーバーに直接転送します。                                                                                                                                     |
| [カスタムアップストリームプロキシグループ (Custom upstream proxy group)] | Web プロキシは、Web トラフィックを外部のアップストリームプロキシグループにリダイレクトします。アップストリームプロキシグループの作成の詳細については、 <a href="#">アップストリームプロキシ</a> , on page 33 を参照してください。                                          |



**ステップ 4** [ルーティングポリシー (Routing Policies)] ページで、IP スプーフィングプロファイルを設定するルーティングポリシーの [IP スプーフィング (IP Spoofing)] 列の下にあるリンクをクリックします。

**ステップ 5** 選択したポリシーに適した IP スプーフィングプロファイルを次から選択します。

| アクション                                                 | 説明                                                                                                                                                |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| [グローバルポリシー設定を使用する (Use Global Policy Settings)]       | Web プロキシは、グローバルポリシーで定義されている設定を使用します。これは、ユーザー定義のポリシー グループのデフォルト アクションです。グローバル ルーティング ポリシーの場合、IP スプーフィングはデフォルトで無効になっています。ユーザー定義のポリシー グループにのみ適用されます。 |
| [IP スプーフィングを使用しない (Do Not Use IP Spoofing)]           | Web プロキシは、要求送信元の IP アドレスを変更し、それ自体のアドレスと一致させてセキュリティを強化します。                                                                                         |
| [クライアント IP を使用する (Use Client IP)]                     | Web プロキシは送信元アドレスを保持するため、Secure Web Applianceからではなく、送信元クライアントから発信されたように見えます。                                                                       |
| [カスタム スプーフィング プロファイル名 (Custom spoofing profile name)] | Web プロキシは、要求の送信元 IP アドレスを選択したカスタム IP スプーフィング プロファイル名に定義されているカスタム IP に変更します。                                                                       |

**ステップ 6** 変更を [実行 (Submit)] して [確定する (Commit)] します。

### What to do next

#### 関連項目

- [アップストリーム プロキシ, on page 33](#)
- [Web プロキシの IP スプーフィング, on page 244](#)

## ポリシーの設定

ポリシーテーブルの各行はポリシー定義を表し、各列にはそのポリシー要素の設定ページへのリンクが含まれています。



#### Note

以下のポリシー設定コンポーネントについて、URL フィルタリングのみを使用して「警告」オプションを指定できます。

| オプション                                           | 説明                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プロトコルとユーザーエージェント<br>(Protocols and User Agents) | プロトコルへのポリシー アクセスの制御、および特定のクライアントアプリケーション（インスタント メッセージクライアント、Web ブラウザ、インターネット電話サービスなど）のブロック設定に使用されます。また、特定のポートの HTTP CONNECT 要求をトンネルするようにアプライアンスを設定することもできます。トンネリングがイネーブルの場合、アプライアンスは HTTP トラフィックを、評価せずに、指定されたポート経由で渡します。                                                                                                                                                                                                  |
| URL フィルタリング<br>(URL Filtering)                  | <p>AsyncOS for Web では、アプライアンスが、特定の HTTP 要求または HTTPS 要求の URL カテゴリに基づいてトランザクションを処理する方法を設定できます。定義済みのカテゴリリストを使用して、クォータ ベースまたは時間ベースのフィルタをモニター、ブロック、警告または設定するかを選択できます。</p> <p>また、カスタム URL カテゴリを作成して、カスタム カテゴリ内の Web サイト用のクォータベースまたは時間ベースのフィルタをブロック、リダイレクト、許可、モニター、警告、または適用するかを選択することもできます。カスタム URL カテゴリの作成については、<a href="#">カスタム URL カテゴリの作成および編集, on page 305</a> を参照してください。</p> <p>また、組み込みまたは参照コンテンツのブロックの例外を追加することもできます。</p> |

| オプション                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アプリケーション<br>(Applications) | <p>AVC または ADC エンジン、アクセプタブルユース ポリシーのコンポーネントであり、アプリケーションで使用する Web トラフィックを深く理解し、管理できるように、Web トラフィックを検査します。アプリケーションタイプまたは個々のアプリケーションごとにアプリケーションをブロックまたは許可するように、Web プロキシを設定できます。</p> <p>AsyncOS 15.0 以降では、AVC または ADC エンジンを使用して Web トラフィックを監視できます。デフォルトでは、AVC は有効になっています。</p> <p>AVC エンジンは ADC エンジンと同じように動作しますが、AVC エンジンは限られた数のアプリケーションをサポートします。また、AVC エンジンでは特定のアプリケーション内の特定のアプリケーション動作（ファイル転送など）に制御を適用できます。設定の詳細については、<a href="#">Web アプリケーションへのアクセスの管理, on page 506</a>を参照してください</p> <p><b>Note</b><br/>ADC アクティビティの設定後に、ADC アプリケーションエンジンは特定のトラフィックのアクティビティ情報を検索または評価します。</p> <p>ADC 署名データベースの更新により、カテゴリ全体が [ブロック (Block)] に設定されている場合でも、追加された新しいアプリケーションはすべてデフォルトで [モニタ (Monitor)] に設定されます。</p> |
| オブジェクト<br>(Objects)        | <p>これらのオプションを使用して、Web プロキシがファイルの特性（ファイルのサイズ、ファイルのタイプ、および MIME タイプなど）に基づいてファイルのダウンロードをブロックできるように設定します。一般的に、オブジェクトとは、個々に選択、アップロード、ダウンロード、および処理できる項目です。次に示すような</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| オプション                                             | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| マルウェア対策とレピュテーション<br>(Anti-Malware and Reputation) | <p>Web レピュテーション フィルタを使用すると、Web ベースのレピュテーション スコアを URL に割り当て、URL ベースのマルウェアが含まれている可能性を判定できます。マルウェア対策スキャンにより、Web ベースのマルウェアの脅威を識別して阻止します。Advanced Malware Protection はダウンロードしたファイル内のマルウェアを識別します。</p> <p>マルウェア対策とレピュテーション ポリシーは、各コンポーネントごとにグローバル設定から継承されます。[セキュリティ サービス (Security Services)] &gt; [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] では、マルウェア スキャンの判定に基づいてモニターまたはブロックするようにマルウェア カテゴリをカスタマイズしたり、Web レピュテーション スコアのしきい値をカスタマイズすることができます。マルウェア カテゴリはポリシー内でさらにカスタマイズできます。また、ファイル レピュテーション サービスと分析サービス用のグローバル設定項目もあります。</p> <p>詳細については、<a href="#">アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定, on page 466</a>および<a href="#">ファイル レピュテーションと分析機能の設定, on page 483</a>を参照してください。</p> |
| HTTP ReWrite プロファイル                               | <p>HTTP リクエストのカスタム ヘッダー プロファイルを設定し、ヘッダー書き換えプロファイルの下に複数のヘッダーを作成できます。ヘッダー書き換えプロファイル機能を使用すると、認証が成功した後、アプライアンスがユーザとグループの情報を別のアップストリームデバイスに渡すことができます。アップストリームプロキシはユーザを認証済みと見なし、追加の認証をバイパスし、定義されたアクセス ポリシーに基づいてユーザにアクセスを提供します。</p> <p><a href="#">ポリシーごとの Web プロキシカスタム ヘッダー, on page 249</a>を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                        |

| オプション       | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ポリシーの複製     | <p>既存のポリシーに、新しいポリシーに必要な設定のほとんどが含まれている場合は、既存のポリシーを複製してから変更することで時間を節約できます。複製されたポリシーは同じグループ化属性を共有しますが、表示名、IP アドレス、ホスト、ドメイン名などの独自の ID を持っています。</p> <p>Cisco Secure Web Appliance のクローンオプションを含む次のポリシーは、Cisco Secure Email and Web Manager (SMA) でも管理できます。</p> <ul style="list-style-type: none"> <li>• アクセス</li> <li>• 復号</li> <li>• ID</li> <li>• ルーティング (Routing)</li> <li>• 外部 DLP (External DLP)</li> <li>• 発信マルウェア スキャン (Outbound Malware Scanning)</li> <li>• HTTP ReWrite プロファイル</li> <li>• Cisco データ セキュリティ</li> </ul> <p><b>Note</b><br/>インスタンスで複製できるポリシーは 1 つだけです。</p> |
| 削除 (Delete) | 作成したポリシーを削除します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## アクセス ポリシー : オブジェクトのブロッキング

[アクセス ポリシー : オブジェクト (Access Policies: Objects)] ページのオプションを使用して、ファイルサイズ、ファイルタイプ、MIME タイプなどのファイル特性に基づきファイルのダウンロードをブロックできます。オブジェクトとは一般的に、個々に選択、アップロード、ダウンロード、および処理できる項目を指します。

個々のアクセス ポリシー、およびグローバル ポリシーによって、さまざまなオブジェクトタイプをブロック対象に指定できます。これらのオブジェクトタイプには、アーカイブ、ドキュメントタイプ、実行可能コード、Web ページ コンテンツなどが含まれます。

### 手順

**ステップ 1** [アクセス ポリシー (Access Policies)] ページ ([Web セキュリティ マネージャ (Web Security Manager)] > [アクセス ポリシー (Access Policies)]) で、編集対象のポリシーを表す行の [オブジェクト (Objects)] 列にあるリンクをクリックします。

**ステップ 2** このアクセス ポリシーでブロックするオブジェクトのタイプを選択します。

- [グローバルポリシー オブジェクトブロック設定を使用 (Use Global Policy Objects Blocking Settings)] : このポリシーでは、グローバルポリシーに対して定義されているオブジェクトブロック設定を使用します。これらの設定は、読み取り専用モードで表示されます。設定を変更するには、グローバルポリシーの設定を編集します。
- [カスタムオブジェクトブロック設定の定義 (Define Custom Objects Blocking Settings)] : このポリシーのすべてのオブジェクトブロック設定を編集できます。
- [このポリシーのオブジェクトブロックを無効にする (Disable Object Blocking for this Policy)] : このポリシーのオブジェクトブロックを無効にします。オブジェクトブロックのオプションは表示されません。

**ステップ 3** 前のステップで [カスタムオブジェクトブロック設定の定義 (Define Custom Objects Blocking Settings)] を選択した場合、[アクセス ポリシー : オブジェクト (Access Policies: Objects)] ページで、必要に応じてオブジェクトブロックのオプションをオフにします。

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| オブジェクトのサイズ       | <p>ダウンロードサイズに基づいて、オブジェクトをブロックできます。</p> <ul style="list-style-type: none"> <li>• [HTTP/HTTPS 最大ダウンロードサイズ (HTTP/HTTPS Max Download Size)] : HTTP/HTTPS ダウンロードの最大オブジェクト サイズを指定するか (指定したサイズより大きいオブジェクトはブロックされます)、HTTP/HTTPS でダウンロードするオブジェクトに最大サイズの制限を設けないことを指定します。</li> <li>• [FTP 最大ダウンロードサイズ (FTP Max Download Size)] : FTP ダウンロードの最大オブジェクトサイズを指定するか (指定したサイズより大きいオブジェクトはブロックされます)、FTP でダウンロードするオブジェクトに最大サイズの制限を設けないことを指定します。</li> </ul> |
| ブロックするオブジェクトタイプ  |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| アーカイブ (Archives) | このセクションを展開して、ブロックするアーカイブファイルのタイプを選択します。このリストには、ARC、BinHex、StuffIt などのアーカイブタイプが含まれます。                                                                                                                                                                                                                                                                                                                                                   |

|                                      |  |
|--------------------------------------|--|
| 検査可能なアーカイブ<br>(Inspectable Archives) |  |
|--------------------------------------|--|

このセクションを展開して、検査可能なアーカイブファイルの特定のタイプを [許可 (Allow)]、[ブロック (Block)]、または [検査 (Inspect)] します。検査可能なアーカイブとは、Secure Web Appliance により各ファイルのコンテンツを検査し、ファイルタイプブロック ポリシーを適用できるアーカイブファイル (圧縮ファイル) のことです。検査可能なアーカイブタイプには、7zip、Microsoft CAB、RAR、TAR などが含まれます。

アーカイブの検査には、以下のことが適用されます。

- [検査 (Inspect)] とマークされたアーカイブタイプだけが展開されて検査されます。
- 一度に検査できるアーカイブは1つだけです。同時に検査可能なアーカイブが他にある場合でも、それらのアーカイブは検査されません。
- 検査されるアーカイブに、現在のポリシーで [ブロック (Block)] アクションが割り当てられているファイルタイプが含まれる場合、許可されるファイルタイプが含まれているとしても、アーカイブ全体がブロックされます。
- サポートされないアーカイブタイプが含まれる検査対象アーカイブは、「スキャン不可 (unscannable)」としてマークされます。ブロック対象のアーカイブタイプが含まれている場合、アーカイブはブロックされます。
- パスワード保護された暗号化アーカイブはサポートされないため、「スキャン不可 (unscannable)」としてマークされます。
- 検査可能なアーカイブが不完全であるか破損している場合、「スキャン不可 (unscannable)」としてマークされます。
- [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] グローバル設定に指定された [DVS エンジン オブジェクト スキャンの制限 (DVS Engine Object Scanning Limits)] の値は、検査可能なアーカイブのサイズにも適用されます。指定されたサイズを超えているオブジェクトは、「スキャン不可 (unscannable)」としてマークされます。このオブジェクトサイズ制限については、[マルウェア対策とレピュテーションフィルタの有効化 \(463 ページ\)](#) を参照してください。
- 「スキャン不可 (unscannable)」としてマークされた検査可能なアーカイブは、アーカイブ全体がブロックされるか、許可されるかのいずれかです。
- カスタムの MIME タイプをブロックするようにアクセス ポリシーが設定されており、アーカイブ検査が有効になっている場合。
  - アプライアンスがカスタム MIME タイプのファイルを Content-Type ヘッダーの一部として直接ダウンロードしようすると、アクセスがブロックされます。
  - 同じファイルが ZIP/アーカイブファイルの一部である場合、アプライアンスはアーカイブを検査し、独自の MIME 評価に基づいて MIME



|                                         |                                                                                                                                                                                                                                                                                            |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         | <p>タイプを決定します。アプライアンスのエンジンによって評価される MIME が設定済みのカスタム MIME タイプと一致しない場合、コンテンツはブロックされません。</p> <ul style="list-style-type: none"> <li>• アプライアンスは設定されたアーカイブを検査できますが、RAR や 7-Zip などの特定のアーカイブを検査することには制限があります。</li> </ul> <p>アーカイブ検査の設定について詳しくは、<a href="#">アーカイブ検査の設定 (384 ページ)</a> を参照してください。</p> |
| <b>ドキュメント タイプ (Document Types)</b>      | このセクションを展開して、ブロックするテキストドキュメントのタイプを選択します。このリストには、FrameMaker、Microsoft Office、PDF などのドキュメント タイプが含まれます。                                                                                                                                                                                       |
| <b>実行可能コード (Executable Code)</b>        | このセクションを展開して、ブロックする実行可能コードのタイプを選択します。このリストには、Java アプレット、UNIX 実行可能ファイル、Windows 実行可能ファイルが含まれます。                                                                                                                                                                                              |
| <b>インストーラ (Installers)</b>              | ブロックするインストーラのタイプを選択します。このリストには、UNIX/LINUX パッケージが含まれます。                                                                                                                                                                                                                                     |
| <b>メディア (Media)</b>                     | ブロックするメディア ファイルのタイプを選択します。このリストには、音声、ビデオ、および写真画像処理フォーマット (TIFF/PSD) が含まれます。                                                                                                                                                                                                                |
| <b>P2P メタファイル (P2P Metafiles)</b>       | このリストには BitTorrent リンク (.torrent) が含まれます。                                                                                                                                                                                                                                                  |
| <b>Web ページ コンテンツ (Web Page Content)</b> | このリストには、フラッシュおよびイメージが含まれます。                                                                                                                                                                                                                                                                |
| <b>その他 (Miscellaneous)</b>              | このリストには、カレンダー データが含まれます。                                                                                                                                                                                                                                                                   |
| <b>カスタム MIME タイプ</b>                    | <p>MIME タイプに基づいてブロックする追加のオブジェクト/ファイルを定義できます。</p> <p>[ブロックする MIME タイプ(Block Custom MIME Types)] フィールドに、1 つ以上の MIME タイプを入力します。</p>                                                                                                                                                           |

**ステップ 4** [Submit] をクリックします。

## アーカイブ検査の設定

個々のアクセスポリシーで、特定のタイプの検査可能なアーカイブを許可、ブロック、または検査することができます。検査可能なアーカイブとは、Secure Web Appliance により各ファイルのコンテンツを検査し、ファイル タイプ ブロック ポリシーを適用できるアーカイブファイル（圧縮ファイル）のことです。個々のアクセスポリシーでアーカイブ検査を設定する方法について詳しくは、[アクセスポリシー：オブジェクトのブロッキング \(380 ページ\)](#) を参照してください。



- (注) アーカイブ検査では、ネストされたオブジェクトがディスクに書き込まれて検査されます。ファイルの検査で使用可能なディスク容量は、随時 1 GB です。このディスク使用量の最大サイズを超えるアーカイブ ファイルは、「スキャン不可 (unscannable)」としてマークされます。

Secure Web Appliance の [使用許可コントロール (Acceptable Use Controls)] ページには、システム全体の検査可能なアーカイブ設定が表示されます。これらの設定は、アクセスポリシーでアーカイブの抽出と検査が有効にされている場合は常にアーカイブに適用されます。

## 手順

**ステップ 1** [セキュリティ サービス (Security Services)] > [使用許可コントロール (Acceptable Use Controls)] を選択します。

**ステップ 2** [アーカイブ設定の編集 (Edit Archives Settings)] ボタンをクリックします。

**ステップ 3** 必要に応じて、検査可能なアーカイブ設定を編集します。

- [カプセル化されたアーカイブの最大抽出数 (Maximum Encapsulated Archive Extractions)] : 抽出して検査する「カプセル化」されたアーカイブの最大数。つまり、他の検査可能なアーカイブが含まれるアーカイブを検査する最大深さです。カプセル化されたアーカイブとは別のアーカイブファイルに含まれるアーカイブのことです。有効な値は 0 ~ 5 です。深さは、最初にネストされているファイルを 1 としてカウントされます。

外部アーカイブファイルは値ゼロのファイルと見なされます。このネストの最大値を超えるファイルがアーカイブに含まれている場合、アーカイブは「スキャン不可 (unscannable)」としてマークされます。この設定はパフォーマンスに影響を与えることに注意してください。

- [検査できないアーカイブをブロック (Block Uninspectable Archives)] : このオプションをオンにすると、Secure Web Appliance は展開して検査できなかったアーカイブをブロックします。

**ステップ 4** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## トランザクション要求のブロック、許可、リダイレクト

Web プロキシは、トランザクション要求のグループ用に作成されたポリシーに基づいて、Web トラフィックを制御します。

- [許可 (Allow)]。Web プロキシは、中断のない接続を許可します。許可された接続は、DVS エンジンによってスキャンされていない可能性があります。
- [ブロック (Block)]。Web プロキシは、接続を許可せず、ブロックの理由を説明するエンド ユーザー通知ページを表示します。

- **リダイレクト**。Web プロキシは、最初に要求された宛先サーバーへの接続を許可せず、指定された別の URL に接続します（[アクセスポリシーでのトラフィックのリダイレクト](#), on [page 317](#) を参照）。



**Note** 上記のアクションは、Web プロキシがクライアント要求に対して実行する最終アクションです。アクセスポリシーに対して設定できるモニターアクションは最終アクションではありません。

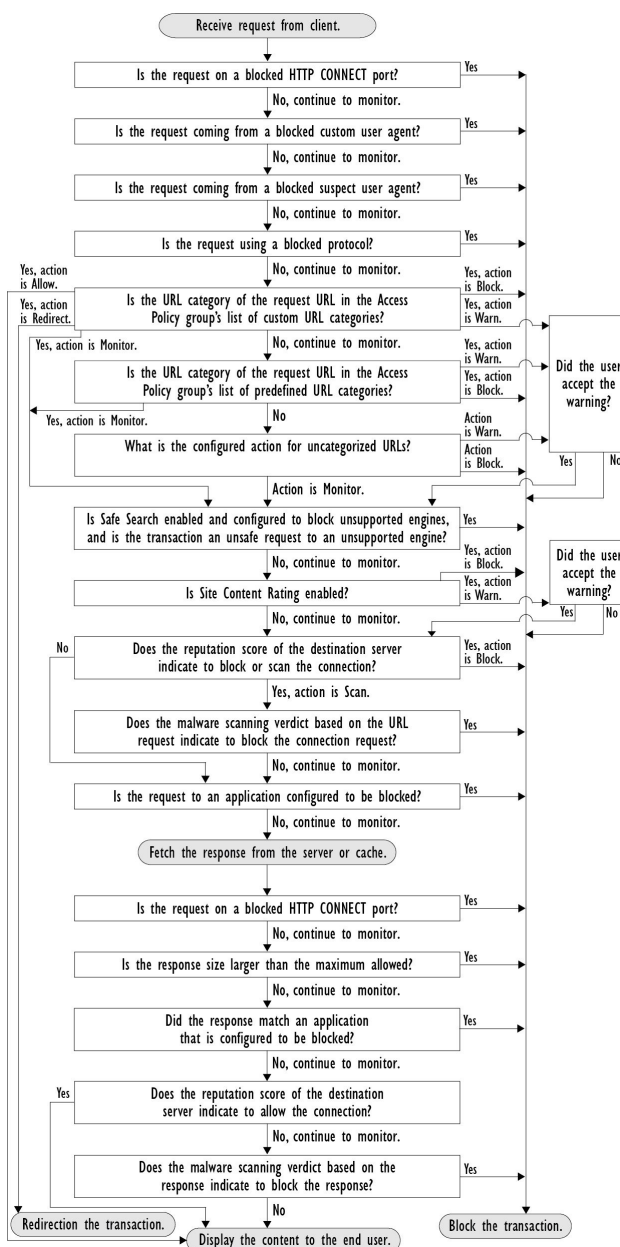
通常、トラフィックは、トランスポートプロトコルに基づいて、さまざまなタイプのポリシーにより制御されます。

| ポリシータイプ                                 | プロトコル (Protocols) |       |     |       | サポートされるアクション |            |                   |                |
|-----------------------------------------|-------------------|-------|-----|-------|--------------|------------|-------------------|----------------|
|                                         | HTTP              | HTTPS | FTP | SOCKS | ブロック (Block) | 許可 (Allow) | リダイレクト (Redirect) | モニター (Monitor) |
| アクセス (Access)                           | x                 | x     | x   |       | x            | x          | x                 | x              |
| SOCKS                                   |                   |       |     | x     | x            | x          |                   |                |
| SAAS                                    | x                 | x     |     |       |              |            |                   |                |
| 復号 (Decryption)                         | x                 | x     |     |       |              |            |                   | x              |
| データセキュリティ (Data Security)               | x                 | x     | x   |       | x            |            |                   | x              |
| 外部 DLP (External DLP)                   | x                 | x     | x   |       |              |            | x                 |                |
| 発信マルウェアスキャン (Outbound Malware Scanning) | x                 | x     | x   |       | x            |            |                   | x              |
| ルーティング (Routing)                        | x                 | x     | x   |       |              |            | x                 |                |



次の図に、Web プロキシが特定のアクセス ポリシーを要求に割り当てた後に、その要求で実行するアクションを決定する方法を示します。宛先サーバーの Web レピュテーション スコアが評価されるのは 1 回だけですが、その結果は、決定フローの 2 つのポイントで適用されます。

**Figure 9: アクセスポリシーのアクションの適用**



# クライアント アプリケーション

## クライアント アプリケーションについて

クライアント アプリケーション（Web ブラウザなど）は要求を行うために使用されます。クライアント アプリケーションに基づいてポリシー メンバーシップを定義し、制御設定を指定してクライアント アプリケーションの認証を免除することができます。これは、アプリケーションがクレデンシャルの入力を要求できない場合に役立ちます。

## ポリシーでのクライアント アプリケーションの使用

### クライアント アプリケーションによるポリシー メンバーシップの定義

#### Procedure

- ステップ 1** [Web セキュリティ マネージャ（Web Security Manager）] メニューからポリシー タイプを選択します。
- ステップ 2** ポリシー テーブル内のポリシー名をクリックします。
- ステップ 3** [詳細設定（Advanced）] セクションを展開して、[クライアントアプリケーション（Client Applications）] フィールド内のリンクをクリックします。
- ステップ 4** クライアント アプリケーションを 1 つ以上定義します。

| オプション                    | 方法                                                                                                                                                                                                               |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 定義済みクライアント アプリケーションを選択する | <p>[ブラウザ（Browser）] と [その他（Other）] セクションを展開して、必要なクライアント アプリケーションのチェックボックスをオンにします。</p> <p><b>Tip</b><br/>可能な場合は [すべてのバージョン（Any Version）] オプションだけを選択します。これによって、複数のオプションを選択するよりもパフォーマンスが向上します。</p>                   |
| カスタムクライアント アプリケーションを定義する | <p>[カスタムクライアントアプリケーション（Custom Client Applications）] フィールドに適切な正規表現を入力します。必要に応じて、新規行に追加の正規表現を入力します。</p> <p><b>Tip</b><br/>正規表現の例を参照するには、[クライアントアプリケーションのパターン例（Example Client Applications Patterns）] をクリックします。</p> |

- ステップ 5** （任意）定義したクライアント アプリケーション以外のすべてのクライアント アプリケーションにポリシー メンバーシップを基づかせるには、[選択したクライアント アプリケーション以外にすべてに一致（Match All Except The Selected Client Applications Definitions）] オプション ボタンをクリックします。
- ステップ 6** [完了（Done）] をクリックします。

## クライアントアプリケーションによるポリシー制御設定の定義

### Procedure

- ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] メニューからポリシー タイプを選択します。
- ステップ 2** ポリシー テーブルで必要なポリシー名を検索します。
- ステップ 3** 同じ行の [プロトコルとクライアントアプリケーション (Protocols and Client Applications)] 列のセル リンクをクリックします。
- ステップ 4** [プロトコルおよびクライアントアプリケーション設定の編集 (Edit Protocols and Client Applications Settings)] ペインのドロップダウン リストから、[カスタム設定を定義 (Define Custom Settings)] を選択します (まだ設定していない場合)。
- ステップ 5** 定義するクライアントアプリケーションに対応する [カスタムクライアントアプリケーション (Custom Client Applications)] フィールドに正規表現を入力します。必要に応じて、新規行に追加の正規表現を入力します。

#### Tip

正規表現の例を参照するには、[クライアント アプリケーションのパターン例 (Example Client Application Patterns)] をクリックします。

- ステップ 6** 変更を送信し、保存します。

## 認証からのクライアント アプリケーションの除外

### Procedure

|        | Command or Action                                   | Purpose                                              |
|--------|-----------------------------------------------------|------------------------------------------------------|
| ステップ 1 | 認証が不要の識別プロファイルを作成する。                                | ユーザーおよびクライアント ソフトウェアの分類, <a href="#">on page 267</a> |
| ステップ 2 | 除外するクライアントアプリケーションとして識別プロファイルのメンバーシップを設定する。         | ポリシーでのクライアントアプリケーションの使用, <a href="#">on page 388</a> |
| ステップ 3 | 上記の識別プロファイル以外の他のすべての識別プロファイルを、認証が必要なポリシーのテーブルに配置する。 | ポリシーの順序, <a href="#">on page 368</a>                 |

## 時間範囲およびクォータ

ユーザがアクセスできる時間、ユーザの最大接続時間またはデータ量（「帯域幅クォータ」）を制限するために、アクセスポリシーおよび復号ポリシーに時間範囲、時間クォータ、ボリュームクォータを適用できます。

- [ポリシーおよび使用許可コントロールの時間範囲, on page 390](#)

- [時間およびボリューム クォータ, on page 391](#)

## ポリシーおよび使用許可コントロールの時間範囲

時間範囲によって、ポリシーおよび使用許可コントロールを適用する期間を定義します。



**Note** 時間範囲を使用して、ユーザ認証が必要な時間帯を定義することはできません。認証要件は識別プロファイルで定義されますが、時間範囲はサポートされません。

- [時間範囲の作成, on page 390](#)

### 時間範囲の作成

#### Procedure

**ステップ 1** [Web セキュリティマネージャ (Web Security Manager) ] > [時間範囲およびクォータの定義 (Define Time Ranges and Quotas) ] を選択します。

**ステップ 2** [時間範囲の追加 (Add Time Range) ] をクリックします。

**ステップ 3** 時間範囲の名前を入力します。

**ステップ 4** [タイムゾーン (Time Zone) ] のオプションを選択します。

- [アプライアンスのタイムゾーン設定を使用 (Use Time Zone Setting from Appliance) ] - Secure Web Appliance と同じタイムゾーンを使用します。
- [この時間範囲のタイムゾーンを指定 (Specify Time Zone for this Time Range) ] - [GMT オフセット (GMT Offset) ] として、またはその国の地域、国、および特定のタイムゾーンとして、異なるタイムゾーンを定義します。

**ステップ 5** 1 つ以上の [曜日 (Day of Week) ] チェックボックスをオンにします。

**ステップ 6** [時刻 (Time of Day) ] のオプションを選択します。

- [終日 (All Day) ] - 24 時間中使用できます。
- [開始 (From) ] と [終了 (To) ] - 特定の時間範囲を定義します。HH:MM (24 時間形式) で開始時刻と終了時刻を入力します。

#### Tip

各時間範囲は、開始時刻と終了時刻の境界を定義します。たとえば、8:00 ~ 17:00 を入力する場合、8:00:00 ~ 16:59:59 に一致しますが 17:00:00 には一致しません。深夜は、開始時刻が 00:00、終了時刻が 24:00 として指定する必要があります。

**ステップ 7** 変更を送信し、保存します。

## 時間およびボリューム クォータ

クォータを使用すると、与えられたデータ量と時間を使い切るまで、個々のユーザはインターネット リソース（またはインターネット リソース クラス）にアクセスできます。AsyncOS は、HTTP、HTTPS、FTP トラフィックに定義されたクォータを適用します。

ユーザが時間またはボリューム クォータに達すると、AsyncOS は最初に警告を表示し、次にブロック ページを表示します。

時間およびボリューム クォータの使用について、以下の点に注意してください。

- AsyncOS が透過モードで展開され、HTTPS プロキシがディセーブルの場合、ポート 443 ではリッスンされず、要求はドロップされます。これは標準の動作です。AsyncOS が明示モードで展開されている場合は、アクセス ポリシーにクォータを設定できます。

HTTPS プロキシがイネーブルの場合、要求に対して実行可能なアクションは、パススルー、復号、ドロップ、またはモニタとなります。全般的に、復号ポリシーのクォータはパススルー カテゴリにのみ適用されます。

パススルーの場合は、トンネル トラフィックのクォータを設定するオプションもあります。アクセスポリシーで設定したクォータは復号トラフィックに適用されるため、復号ではこのオプションは使用できません。

- URL フィルタリングがディセーブルの場合やキーが使用できない場合、AsyncOS は URL のカテゴリを識別できず、[アクセス ポリシー (Access Policy)] > [URL フィルタリング (URL Filtering)] ページは無効になります。したがって、クォータを設定するには、機能キーが存在し、アクセプタブル ユース ポリシーがイネーブルになっている必要があります。
- Facebook や Gmail など、多くの Web サイトでは自動アップデートが頻繁に起こります。使用していないブラウザ ウィンドウやタブでこのような Web サイトを開いたままにしておくと、ユーザの時間およびボリューム クォータが消費され続けます。
- プロキシを再起動すると、ハイパフォーマンスモードは次のようになります。
  - [有効 (Enabled)] - 時間とボリュームのクォータはリセットされません。クォータは、設定された時間に基づいて 24 時間以内に自動的に 1 回リセットされます。
  - [無効 (Disabled)] - 時間とボリュームのクォータがリセットされます。クォータは自動的に 24 時間以内にリセットされるため、リセットの影響が残るのは現在時刻から 24 時間のみです。設定の変更またはプロキシプロセスのクラッシュが原因でプロキシが再起動する場合があります。
- decrypt-for-EUN オプションがイネーブルの場合でも、HTTPS に対して EUN ページ（警告とブロックの両方）を表示できません。



### Note

複数のクォータを特定のユーザに適用した場合は、常に最も制限が厳しいクォータが適用されます。

- [ボリューム クォータの計算, on page 392](#)
- [時間クォータの計算, on page 392](#)



- [時間、ボリウム、および帯域幅のクォータの定義, on page 392](#)

## ボリウム クォータの計算

ボリウム クォータの計算方法は次のとおりです。

- HTTP および復号された HTTPS トラフィック：HTTP 要求と応答の本文がクォータの上限に対してカウントされます。要求ヘッダーと応答ヘッダーは上限に対してカウントされません。
- トンネルトラフィック（トンネル化 HTTPS を含む）：AsyncOS は、トンネル化トラフィックをクライアントからサーバに（およびその逆に）移動するだけです。トンネル化トラフィックのデータ量全体が、クォータの上限に対してカウントされます。
- FTP：制御接続トラフィックはカウントされません。アップロードおよびダウンロードされたファイルのサイズは、クォータの上限に対してカウントされます。



### Note

クライアント側のトラフィックのみがクォータの上限に対してカウントされます。応答がキャッシュから送信された場合でもクライアント側のトラフィックが生成されるため、キャッシュされたコンテンツも上限に対してカウントされます。

## 時間クォータの計算

時間クォータの計算方法は次のとおりです。

- HTTP および復号された HTTPS トラフィック：同じ URL カテゴリへの各接続時間（確立から切断まで）に 1 分を加えた時間が、時間クォータの上限に対してカウントされます。1 分以内に同じ URL カテゴリに対して複数の要求が行われた場合、それらは 1 つの連続セッションとしてカウントされ、セッションの最後（つまり、少なくとも 1 分の「沈黙」の後）にのみ 1 分が追加されます。
- トンネルトラフィック（トンネル化 HTTPS を含む）：トンネルの実際の期間（確立から切断まで）が、クォータの上限に対してカウントされます。複数の要求に対する上記の計算は、トンネル化トラフィックにも適用されます。
- FTP：FTP 制御セッションの実際の期間（確立から切断まで）が、クォータの上限に対してカウントされます。複数の要求に対する上記の計算は、FTP トラフィックにも適用されます。

## 時間、ボリウム、および帯域幅のクォータの定義

### Before you begin

- [セキュリティサービス (Security Services)] > [使用許可コントロール (Acceptable Use Controls)] に移動し、使用許可コントロールをイネーブルにします。
- 毎日の制限としてクォータを適用しない場合は、時間範囲を定義します。

## Procedure

- ステップ 1** [Web セキュリティマネージャ (Web Security Manager)] > [時間範囲およびクォータの定義 (Define Time Ranges and Quotas)] に移動します。
- ステップ 2** [クォータの追加 (Add Quota)] をクリックします。
- ステップ 3** [クォータ名 (Quota Name)] に一意のクォータ名を入力します。
- ステップ 4** 時間とボリュームのクォータを毎日リセットするには、[毎日このクォータをリセットする時刻 (Reset this quota daily at)]、および [毎日時間とボリュームのクォータをリセットする時刻 (Reset Time and Volume quota daily at)] を選択し、フィールドに 12 時間形式で時刻を入力し、メニューから [AM] または [PM] を選択します。または、[事前定義された時間範囲プロファイルを選択します (Select a predefined time range profile)] を選択します。

### Note

リセットクォータオプションを使用しても、設定した帯域幅クォータ値はリセットされません。

- ステップ 5** 時間クォータを設定するには、[時間クォータ Time Quota] チェックボックスをオンにして、[時間 (hrs)] メニューから時間数を、[分 (mins)] メニューから分数を選択し、0 分 (常にブロック) から 23 時間 59 分までの時間数を設定します。
- ステップ 6** ボリューム クォータを設定するには、フィールドに数字を入力し、メニューから [KB] (キロバイト)、[MB] (メガバイト)、または [GB] (ギガバイト) を選択します。
- ステップ 7** 帯域幅クォータを設定するには、フィールドに数値を入力し、メニューから [Kbps] (キロバイト/秒)、または [Mbps] (メガバイト/秒) を選択します。
- ただし、同じアクセスポリシーや復号ポリシーに、URL 帯域幅クォータと全体的な Web アクティビティクォータの両方を設定することはできません。
  - 全体的な帯域幅制限または AVC 帯域幅制限が有効になっている場合、またはその逆の場合、帯域幅クォータは設定できません。
  - キャッシュされたコンテンツも帯域幅クォータで考慮されます。
  - クォータプロファイルの編集では、CDS ポリシーにマッピングされている既存の時間またはボリュームクォータのプロファイルに帯域幅クォータを追加しないでください。
  - 復号ポリシーで Web アクティビティ全体の帯域幅クォータを使用して URL を調整するには、URL をパススルーに設定する必要があります。
  - 未分類の URL の場合、詳細な帯域幅制御を介してスロットルするには、次の設定が必要です。
    - アクセスポリシー：復号ポリシー内の未分類の URL は、アクセスポリシーおよび全体的な Web アクティビティ帯域幅クォータでそれぞれ[復号/監視 (Decrypt/Monitor)] および[監視 (Monitor)] に設定されています。
    - 復号ポリシー：復号ポリシーの未分類の URL は、パススルーおよび全体的な Web アクティビティの帯域幅クォータに設定されています。

### Note

AsyncOS リリース 15.0 にアップグレードする前に帯域幅クォータが設定されたすべてのクォータプロファイルを削除します。

**ステップ 8** [送信 (Submit)] をクリックし、次に [変更を確定 (Commit Changes)] をクリックして変更を適用します。または、[キャンセル (Cancel)] をクリックして変更を破棄します。

### What to do next

(オプション) [セキュリティ サービス (Security Services)] > [エンドユーザ通知 (End-User Notification)] に移動し、クォータ用のエンドユーザ通知を設定します。

## URL カテゴリによるアクセス制御

対応する Web サイトのカテゴリに基づいて、Web 要求を識別してアクションを実行できます。Secure Web Appliance には、多数の定義済み URL カテゴリ (Web ベースの電子メールなど) が用意されています。

定義済みのカテゴリおよびそれらに関連付けられている Web サイトは、Secure Web Appliance に搭載されているフィルタリングデータベースで定義されます。これらのデータベースは、Cisco によって自動的に最新の状態に維持されます。指定したホスト名と IP アドレスに対してカスタム URL カテゴリを作成することもできます。

URL カテゴリは、要求を識別するポリシーを除くすべてのポリシーで使用できます。また、要求にアクションを適用するポリシー (アクセス、暗号化 HTTPS 管理、データ セキュリティ) でも使用できます。

カスタム URL カテゴリの作成については、[カスタム URL カテゴリの作成および編集, on page 305](#) を参照してください。

## URL カテゴリによる Web 要求の識別

### Before you begin

- 使用許可コントロールを有効にします ([URL フィルタリング エンジンの設定, on page 284](#) を参照)。
- (任意) カスタム URL カテゴリを作成します ([カスタム URL カテゴリの作成および編集, on page 305](#) を参照)。

### Procedure

**ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] メニューからポリシー タイプ (SaaS 以外) を選択します。

**ステップ 2** ポリシー テーブル内のポリシー名をクリックします (または新しいポリシーを追加します)。

- ステップ 3** [詳細設定 (Advanced)] セクションを展開して、[URL カテゴリ (URL Categories)] フィールド内のリンクをクリックします。
- ステップ 4** Web 要求の識別に使用する URL カテゴリに対応する [追加 (Add)] 列のセルをクリックします。この操作を、カスタム URL カテゴリと定義済み URL カテゴリのリストに対して実行します。
- ステップ 5** [完了 (Done)] をクリックします。
- ステップ 6** 変更を送信し、保存します。

## URL カテゴリによる Web 要求へのアクション

### Before you begin

- 使用許可コントロールを有効にします ([URL フィルタリング エンジン の設定](#), on page 284 を参照)。
- (任意) カスタム URL カテゴリを作成します ([カスタム URL カテゴリ の作成および編集](#), on page 305 を参照)。



#### Note

ポリシー内で基準として URL カテゴリを使用している場合、同じポリシー内にアクションを指定する際には、それらのカテゴリだけを使用できます。そのため、下記のオプションの一部が異なっていたり、使用できないことがあります。

### Procedure

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] メニューから [アクセス ポリシー (Access Policies)]、[Cisco データ セキュリティ ポリシー (Cisco Data Security Policies)]、または [暗号化 HTTPS 管理 (Encrypted HTTPS Management)] のいずれかを選択します。
- ステップ 2** ポリシー テーブルで必要なポリシー名を検索します。
- ステップ 3** 同じ行の [URL フィルタリング (URL Filtering)] 列のセル リンクをクリックします。
- ステップ 4** (任意) カスタム URL カテゴリを追加します。

- a) [カスタムカテゴリの選択 (Select Custom Categories)] をクリックします。
- b) このポリシーに含めるカスタム URL カテゴリを選択して、[適用 (Apply)] をクリックします。

URL フィルタリング エンジンでクライアント要求と照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンは、クライアント要求と含まれているカスタム URL カテゴリを比較します。除外されたカスタム URL カテゴリは無視されます。URL フィルタリング エンジンは、定義済みの URL カテゴリよりも前に、含まれているカスタム URL カテゴリとクライアント要求の URL を比較します。

ポリシーに含まれているカスタム URL カテゴリは、[カスタム URL カテゴリのフィルタリング (Custom URL Category Filtering)] セクションに表示されます。

**ステップ5** カスタムおよび定義済みの各 URL カテゴリのアクションを選択します。

**Note**

使用可能なアクションは、カスタムカテゴリと定義済みカテゴリとは異なり、ポリシータイプによっても異なります。

**ステップ6** [分類されてないURL (Uncategorized URLs)] セクションで、定義済み URL カテゴリにもカスタム URL カテゴリにも該当しない Web サイトへのクライアント要求に対して実行するアクションを選択します。

**ステップ7** 変更を送信し、保存します。

## リモートユーザー

- [リモートユーザーについて, on page 396](#)
- [リモートユーザーの ID を設定する方法, on page 397](#)
- [ASA のリモートユーザー ステータスと統計情報の表示, on page 399](#)

### リモートユーザーについて

Cisco AnyConnect セキュアモビリティはネットワーク境界をリモートエンドポイントまで拡張し、Secure Web Applianceにより提供される Web フィルタリングサービスの統合を実現します。

リモートユーザーおよびモバイルユーザーは Cisco AnyConnect Secure VPN（仮想プライベートネットワーク）クライアントを使用して、適応型セキュリティ アプライアンス（ASA）との VPN セッションを確立します。ASA は、IP アドレスとユーザー名によるユーザー識別情報とともに、Web トラフィックを Secure Web Applianceに送信します。Secure Web Applianceは、トラフィックをスキャンしてアクセプタブルユース ポリシーを適用し、セキュリティ上の脅威からユーザを保護します。セキュリティアプライアンスは、安全と判断された、ユーザーが受け入れ可能なすべてのトラフィックを返します。

セキュアモビリティがイネーブルの場合は、ID とポリシーを設定し、ユーザーの場所に応じてユーザーに適用できます。

- **リモートユーザー。**これらのユーザーは、VPNを使用してリモートロケーションからネットワークに接続されます。Cisco ASA と Cisco AnyConnect クライアントの両方が VPN アクセスに使用されている場合、Secure Web Applianceはリモートユーザを自動的に識別します。それ以外の場合は、Secure Web Applianceの管理者が IP アドレスの範囲を設定して、リモートユーザを指定する必要があります。
- **ローカルユーザー。**これらのユーザーは、有線またはワイヤレスでネットワークに接続されます。

Secure Web Applianceを Cisco ASA と統合すると、認証されたユーザ名によりユーザを透過的に識別するように設定して、リモートユーザのシングルサインオンを実現できます。

## リモートユーザーの ID を設定する方法

| タスク                    | 解説場所                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. リモートユーザーの ID を設定する。 | <a href="#">リモートユーザーの ID の設定, on page 397</a>                                                                                                                                                                                                                                                                                                                                       |
| 2. リモートユーザーの ID を作成する。 | <a href="#">ユーザーおよびクライアントソフトウェアの分類, on page 267</a> <ol style="list-style-type: none"> <li>1. [ユーザーの場所別メンバーの定義 (Define Members by User Location)] セクションで、[ローカルユーザーのみ (Local Users Only)] を選択します。</li> <li>2. [認証ごとにメンバを定義 (Define Members by Authentication)] セクションで、[Cisco ASA統合を通じてユーザーを透過的に識別する (Identify Users Transparently through Cisco ASA Integration)] を選択します。</li> </ol> |
| 3. リモートユーザーのポリシーを作成する。 | <a href="#">ポリシーの作成, on page 369</a>                                                                                                                                                                                                                                                                                                                                                |

### リモートユーザーの ID の設定

#### Procedure

- ステップ 1** [セキュリティサービス (Security Services)] > [AnyConnectセキュアモビリティ (AnyConnect Secure Mobility)] で、[有効 (Enable)] をクリックします。
- ステップ 2** AnyConnect セキュア モビリティのライセンス契約書の条項を読み、[同意する (Accept)] をクリックします。
- ステップ 3** リモートユーザーの識別方法を設定します。

| オプション               | 説明                                               | この他の手順                                                                                                                     |
|---------------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| IPアドレス (IP Address) | リモートデバイスに割り当てられているとアプライアンスが見なす IP アドレスの範囲を指定します。 | <ol style="list-style-type: none"> <li>a. [IP 範囲 (IP Range)] フィールドに IP アドレスの範囲を入力します。</li> <li>b. ステップ 4 に進みます。</li> </ol> |

| オプション                                      | 説明                                                                                                                                                                                                                                                        | この他の手順                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco ASA 統合<br>(Cisco ASA<br>Integration) | Secure Web Applianceが通信する 1 つ以上の Cisco ASA を指定します。Cisco ASA は IP アドレスとユーザーのマッピングを保持し、その情報を Secure Web Appliance に伝達します。Web プロキシはトランザクションを受信すると、IP アドレスを取得し、IP アドレスとユーザーのマッピングをチェックしてユーザーを特定します。Cisco ASA と統合してユーザーを特定する場合は、リモートユーザーのシングルサインオンをイネーブルにできます。 | <p>a. Cisco ASA のホスト名または IP アドレスを入力します。</p> <p>b. ASA へのアクセスに使用するポート番号を入力します。Cisco ASA のデフォルトポート番号は 11999 です。</p> <p>c. クラスタ内に複数の Cisco ASA が設定されている場合は、[ 行の追加 (Add Row) ] をクリックし、クラスタ内の各 ASA を設定します。</p> <p><b>Note</b><br/>2 つの Cisco ASA が高可用性に設定されている場合は、アクティブな Cisco ASA の 1 つのホスト名または IP アドレスのみを入力します。</p> <p>d. Cisco ASA のアクセス パスフレーズを入力します。</p> <p><b>Note</b><br/>ここで入力するパスフレーズは、指定した Cisco ASA 用に設定されているアクセス パスフレーズと一致する必要があります。</p> <p>e. (オプション) [ テスト開始 (Start Test) ] をクリックして、Secure Web Appliance が設定されている Cisco ASA に接続できることを確認します。</p> |

**ステップ 4** 変更を送信して確定します ([送信 (Submit) ] と [変更を確定 (Commit Changes) ] )。

**Note**

Secure Web Appliance で [ユーザーの場所別メンバーの定義 (Define Members by User Location) ] オプションを有効にするには、AnyConnect セキュリティモビリティを有効にします ([セキュリティサービス (Security Services) ] > [AnyConnect Security Mobility] )。デフォルトでは、このオプションは Cisco Content Security Management Appliance ([Web] > [設定マスター (Configuration Master) ] > [識別プロファイル (Identification Profiles) ]) で使用できます。[ユーザーの場所別メンバーの定義 (Define Members by User Location) ] オプションを使用してセキュリティ管理アプライアンスで識別プロファイルを設定し、その設定を AnyConnect セキュリティモビリティが有効になっていない Secure Web Appliance に公開すると、その識別プロファイルは無効になります。

## ASA のリモート ユーザー ステータスと統計情報の表示

Secure Web Applianceが ASA と統合されている場合は、以下のコマンドを使用してセキュアモビリティに関連する情報を表示します。

| コマンド                   | 説明                                                                                                                                                                                                                                                                                                                          |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>musstatus</code> | <p>このコマンドにより、以下の情報が表示されます。</p> <ul style="list-style-type: none"> <li>Secure Web Applianceと各 ASA との接続ステータス。</li> <li>Secure Web Applianceと各 ASA との接続時間（分単位）。</li> <li>各 ASA からのリモート クライアントの数。</li> <li>サービス対象のリモート クライアントの数。これは、Secure Web Applianceを介してトラフィックの受け渡しを行ったリモートクライアントの数です。</li> <li>リモート クライアントの合計数。</li> </ul> |

## ポリシーに関するトラブルシューティング

- [HTTPS に対してアクセス ポリシーを設定できない, on page 758](#)
- [一部の Microsoft Office ファイルがブロックされない, on page 743](#)
- [DOS の実行可能オブジェクト タイプをブロックすると、Windows OneCare のアップデートがブロックされる, on page 743](#)
- [識別プロファイルがポリシーから削除される, on page 759](#)
- [ポリシーが適用されない, on page 759](#)
- [HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する, on page 759](#)
- [HTTPS 要求および FTP over HTTP 要求の場合にユーザーがグローバル ポリシーに一致, on page 760](#)
- [ユーザーに誤ったアクセス ポリシーが割り当てられる , on page 760](#)
- [ポリシーのトラブルシューティング ツール：ポリシー トレース, on page 761](#)

## SaaS アクセス コントロール

この章で説明する内容は、次のとおりです。

- [SaaS アクセス コントロールの概要（400 ページ）](#)



- [ID プロバイダとしてのアプライアンスの設定 \(401 ページ\)](#)
- [SaaS アクセス コントロールと複数のアプライアンスの使用 \(404 ページ\)](#)
- [SaaS アプリケーション認証ポリシーの作成 \(404 ページ\)](#)
- [シングル サイン オン URL へのエンドユーザー アクセスの設定 \(407 ページ\)](#)

## SaaS アクセス コントロールの概要

Secure Web Applianceは、セキュリティ アサーションマークアップ言語 (SAML) を使用して、SaaS アプリケーションへのアクセスを許可します。SAML バージョン 2.0 に厳密に準拠している SaaS アプリケーションで動作します。

Cisco SaaS アクセス コントロールによって、以下のことが可能になります。

- SaaS アプリケーションにアクセスできるユーザーおよび場所を制御する。
- ユーザーが組織を退職した時点で、すべての SaaS アプリケーションへのアクセスをただちに無効にする。
- ユーザーに SaaS ユーザー クレデンシャルの入力を求めるフィッシング攻撃のリスクを軽減する。
- ユーザーを透過的にサインインさせるか (シングル サイン オン機能)、ユーザーに認証ユーザー名とパスワードの入力を求めるかを選択する。

SaaS アクセスコントロールは、Secure Web Applianceがサポートしている認証メカニズムを必要とする SaaS アプリケーションでのみ動作します。現在、Web プロキシは「PasswordProtectedTransport」認証メカニズムを使用しています。

SaaS アクセスコントロールをイネーブルにするには、Secure Web Applianceと SaaS アプリケーションの両方の設定を行う必要があります。

### Procedure

|        | Command or Action                       | Purpose                                                       |
|--------|-----------------------------------------|---------------------------------------------------------------|
| ステップ 1 | Secure Web Applianceを ID プロバイダーとして設定する。 | <a href="#">ID プロバイダとしてのアプライアンスの設定, on page 401</a>           |
| ステップ 2 | SaaS アプリケーションの認証ポリシーを作成します。             | <a href="#">SaaS アプリケーション認証ポリシーの作成, on page 404</a>           |
| ステップ 3 | SaaS アプリケーションをシングル サイン オン用に設定します。       | <a href="#">シングルサイン オン URL へのエンドユーザー アクセスの設定, on page 407</a> |
| ステップ 4 | (任意) 複数の Secure Web Applianceを設定する。     | <a href="#">SaaS アクセス コントロールと複数のアプライアンスの使用, on page 404</a>   |

## ID プロバイダとしてのアプライアンスの設定

Secure Web Applianceを ID プロバイダーとして設定する場合、定義する設定は通信するすべての SaaS アプリケーションに適用されます。Secure Web Applianceは、作成する各 SAML アサーションに署名するために証明書とキーを使用します。

### Before you begin

- (オプション) SAML アサーションに署名するための証明書 (PEM 形式) とキーを検索します。
- 各 SaaS アプリケーションに証明書をアップロードします。

### Procedure

- 
- ステップ 1 [ネットワーク (Network) ] > [SaaS の ID プロバイダ (Identity Provider for SaaS) ] を選択します。
  - ステップ 2 [設定の編集 (Edit Settings) ] をクリックします。
  - ステップ 3 [SaaS シングルサインオンサービスを有効にする (Enable SaaS Single Sign-on Service) ] をオンにします。
  - ステップ 4 [アイデンティティ プロバイダのドメイン名 (Identity Provider Domain Name) ] フィールドに仮想ドメイン名を入力します。
  - ステップ 5 [アイデンティティ プロバイダのエンティティ ID (Identity Provider Entity ID) ] フィールドに、一意のテキスト識別子を入力します (URI 形式の文字列を推奨) 。
  - ステップ 6 証明書とキーをアップロードまたは生成します。

| 方法              | その他の手順                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 証明書およびキーのアップロード | <p>a. [アップロードされた証明書とキーを使用 (Use Uploaded Certificate and Key)] を選択します。</p> <p>b. [証明書 (Certificate)] フィールドで [参照 (Browse)] をクリックし、アップロードするファイルを検索します。</p> <p><b>Note</b><br/>Web プロキシは、ファイル内の最初の証明書またはキーを使用します。証明書ファイルは PEM 形式にする必要があります。DER 形式はサポートされていません。</p> <p>c. [キー (Key)] フィールドで [参照 (Browse)] をクリックし、アップロードするファイルを指定します。</p> <p>キーが暗号化されている場合は、[キーは暗号化されています (Key is Encrypted)] を選択します。</p> <p><b>Note</b><br/>キーの長さは 512、1024、または 2048 ビットである必要があります。秘密キーファイルは PEM 形式でなければなりません。DER 形式はサポートされていません。</p> <p>d. [ファイルのアップロード (Upload File)] をクリックします。</p> <p>e. [証明書をダウンロード (Download Certificate)] をクリックして、Secure Web Appliance が通信する SaaS アプリケーションに転送する証明書のコピーをダウンロードします。</p> |

| 方法          | この他の手順                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 証明書およびキーの生成 | <p>a. [生成された証明書とキーを使用 (Use Generated Certificate and Key)] を選択します。</p> <p>b. [新しい証明書とキーを生成 (Generate New Certificate and Key)] をクリックします。</p> <p>1. [証明書とキーを生成 (Generate Certificate and Key)] ダイアログボックスで、署名付き証明書に表示する情報を入力します。</p> <p><b>Note</b><br/>[共通名 (Common Name)] フィールドには、スラッシュ (/) を除く任意の ASCII 文字を入力できます。</p> <p>2. [生成 (Generate)] をクリックします。</p> <p>c. [証明書をダウンロード (Download Certificate)] をクリックして、Secure Web Applianceが通信する SaaS アプリケーションに証明書を転送します。</p> <p>d. (オプション) 署名付き証明書を使用するには、[証明書署名要求のダウンロード (Download Certificate Signing Request)] (DCSR) リンクをクリックして、認証局 (CA) に要求を送信します。CA から署名付き証明書を受信したら、[参照 (Browse)] をクリックし、署名付き証明書の場所に移動します。[ファイルのアップロード (Upload File)] をクリックします。(バグ 37984)</p> |

**Note**

アップロードされた証明書とキーのペアと、生成された証明書とキーのペアの両方がアプライアンスにある場合、アプライアンスは、[署名証明書 (Signing Certificate)] セクションで現在選択されている証明書とキーのペアのみを使用します。

**ステップ 7** アプライアンスを ID プロバイダとして設定する場合は、設定を書き留めておきます。これらの設定の一部は、SaaS アプリケーションをシングルサインオン用に設定する際に使用する必要があります。

**ステップ 8** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

**What to do next**

SAML アサーションの署名に使用する証明書とキーを指定したら、各 SaaS アプリケーションに証明書をアップロードします。

**関連項目**

- [シングルサインオン URL へのエンドユーザー アクセスの設定, on page 407](#)

## SaaS アクセス コントロールと複数のアプライアンスの使用

### Before you begin

[ID プロバイダとしてのアプライアンスの設定, on page 401](#)

### Procedure

- 
- ステップ 1** 各 Secure Web Applianceに対して同じ ID プロバイダーのドメイン名を設定します。
- ステップ 2** 各 Secure Web Applianceに対して同じ ID プロバイダーのエンティティ ID を設定します。
- ステップ 3** [ネットワーク (Network) ] > [SaaS の ID プロバイダ (Identity Provider for SaaS) ] ページで、各アプライアンスに同じ証明書と秘密キーをアップロードします。
- ステップ 4** 設定する各 SaaS アプリケーションにこの証明書をアップロードします。
- 

## SaaS アプリケーション認証ポリシーの作成

### Before you begin

- 関連付けられた ID を作成します。
- ID プロバイダを設定します ([ID プロバイダとしてのアプライアンスの設定, on page 401](#) を参照)。
- ID プロバイダの署名証明書とキーを入力します ([ネットワーク (Network) ] > [SaaS の ID プロバイダ (Identity Provider for SaaS) ] > [設定の有効化と編集 (Enable and Edit Settings) ])。
- 認証レルムを作成します。 [認証レルム, on page 90](#)

### Procedure

- 
- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager) ] > [SaaS ポリシー (SaaS Policies) ] を選択します。
- ステップ 2** [アプリケーションの追加 (Add Application) ] をクリックします。
- ステップ 3** 以下の設定項目を設定します。

| プロパティ                           | 説明                                                                                                                        |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| アプリケーション名<br>(Application Name) | このポリシーの SaaS アプリケーションを識別する名前を入力します。各アプリケーション名は一意である必要があります。 Secure Web Appliance は、アプリケーション名を使用して、シングル サインオン URL を生成できます。 |
| 説明                              | (オプション) この SaaS ポリシーの説明を入力します。                                                                                            |

| プロパティ                                              | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サービスプロバイダのメタデータ<br>(Metadata for Service Provider) | <p>このポリシーで参照されるサービスプロバイダを示すメタデータを設定します。サービスプロバイダのプロパティを手動で記述するか、または SaaS アプリケーションによって提供されるメタデータ ファイルをアップロードできます。</p> <p>Secure Web Applianceは、SAML を使用して SaaS アプリケーション（サービスプロバイダー）と通信する方法を決定するために、メタデータを使用します。メタデータの適切な設定については、SaaS アプリケーションを参照してください。</p> <p>キーの手動設定（Configure Keys Manually）：このオプションを選択した場合は、以下を入力します。</p> <ul style="list-style-type: none"> <li>• [サービスプロバイダのエンティティ ID（Service Provider Entity ID）]。SaaS アプリケーションが自身をサービス プロバイダとして識別するために使用するテキスト（通常は URI 形式）を入力します。</li> <li>• [名前IDの形式（Name ID Format）]。サービス プロバイダに送信する SAML アサーションでアプライアンスがユーザーを識別するために使用する形式を、ドロップダウン リストから選択します。ここで入力する値は、SaaS アプリケーションの対応する設定と一致している必要があります。</li> <li>• [Assertion Consumer ServiceのURL（Assertion Consumer Service URL）]。Secure Web Applianceが作成した SAML アサーションの送信先 URL を入力します。SaaS アプリケーションのマニュアルを参照して、使用する適切な URL（ログイン URL）を決定してください。</li> </ul> <p>[ハードディスクからファイルをインポート（Import File from Hard Disk）]：このオプションを選択した場合は、[参照（Browse）] をクリックしてファイルを検索し、[インポート（Import）] をクリックします。</p> <p><b>Note</b><br/>このメタデータ ファイルは、サービスプロバイダのインスタンスを説明する SAML 標準に準拠した XML ドキュメントです。すべての SaaS アプリケーションがメタデータ ファイルを使用するわけではありませんが、使用する場合は、ファイルについて SaaS アプリケーションのプロバイダにお問い合わせください。</p> |

| プロパティ                                                                   | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ユーザー識別/SaaS SSO の認証 (User Identification / Authentication for SaaS SSO) | <p>SaaS シングル サインオンに対してユーザーを識別または認証する方法を指定します。</p> <ul style="list-style-type: none"> <li>• ユーザーに対して、常にローカル認証クレデンシャルの入力を求める。</li> <li>• Web プロキシが透過的にユーザー名を取得した場合に、ユーザーに対してローカル認証クレデンシャルの入力を求める。</li> <li>• SaaS ユーザーのローカル認証クレデンシャルを使用して、ユーザーを自動的にサインインさせる。</li> </ul> <p>この SaaS アプリケーションにアクセスするユーザーを認証するために、Web プロキシが使用する認証レルムまたはシーケンスを選択します。SaaS アプリケーションに正常にアクセスするには、ユーザーは認証レルムまたは認証シーケンスのメンバーである必要があります。Identity Services Engine を認証に使用しており、LDAP を選択した場合は、SAML ユーザー名と属性のマッピングにレルムが使用されます。</p>                                                                                                                 |
| SAML ユーザー名のマッピング (SAML User Name Mapping)                               | <p>Web プロキシが SAML アサーションでサービス プロバイダにユーザー名を示す方法を指定します。ネットワーク内で使用されているユーザー名を渡すか ([マッピングなし (No mapping) ])、または以下のいずれかの方法で内部ユーザー名を別の形式に変更できます。</p> <ul style="list-style-type: none"> <li>• [LDAP クエリー (LDAP query) ]。サービス プロバイダに送信されるユーザー名は、1 つ以上の LDAP クエリー属性に基づきます。LDAP 属性フィールドと任意のカスタム テキストを含む式を入力します。属性名は山カッコで囲む必要があります。任意の数の属性を含めることができます。たとえば、LDAP 属性が「user」と「domain」の場合は、&lt;user&gt;@&lt;domain&gt;.com と入力できます。</li> <li>• [固定ルールマッピング (Fixed Rule Mapping) ]。サービス プロバイダに送信されるユーザー名は、前または後ろに固定文字列を追加した内部ユーザー名に基づきます。[式名 (Expression Name) ] フィールドに固定文字列を入力し、その前または後ろに %s を付けて内部ユーザー名における位置を示します。</li> </ul> |
| SAML 属性マッピング (SAML Attribute Mapping)                                   | <p>(オプション) SaaS アプリケーションから要求された場合は、LDAP 認証サーバーから内部ユーザーに関する追加情報を SaaS アプリケーションに提供できます。各 LDAP サーバー属性を SAML 属性にマッピングします。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 認証コンテキスト (Authentication Context)                                       | <p>Web プロキシが内部ユーザーを認証するために使用する認証メカニズムを選択します。</p> <p><b>Note</b><br/>           認証コンテキストは、ID プロバイダが内部ユーザーの認証に使用した認証メカニズムをサービス プロバイダに通知します。一部のサービス プロバイダでは、ユーザーに SaaS アプリケーションへのアクセスを許可するために特定の認証メカニズムが必要です。サービス プロバイダが ID プロバイダでサポートされていない認証コンテキストを必要とする場合、ユーザーはシングル サインオンを使用して ID プロバイダからサービス プロバイダにアクセスできません。</p>                                                                                                                                                                                                                                                                                                |

**ステップ 4** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

#### What to do next

アプリケーションを設定したのと同じパラメータを使用して、SaaS アプリケーション側にシングルサインオンを設定します。

## シングルサインオン URL へのエンドユーザー アクセスの設定

Secure Web Appliance を ID プロバイダーとして設定し、SaaS アプリケーション用に SaaS アプリケーション認証ポリシーを作成すると、アプライアンスによってシングルサインオン URL (SSO URL) が作成されます。Secure Web Appliance は SaaS アプリケーション認証ポリシーで設定されたアプリケーション名を使用して、シングルサインオン URL を生成します。SSO URL の形式は以下のとおりです。

`http://IdentityProviderDomainName /SSOURL/ApplicationName`

#### Procedure

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] > [SaaS ポリシー (SaaS Policies)] ページで、シングルサインオン URL を取得します。
- ステップ 2** フロー タイプに応じてエンドユーザーが URL を使用できるようにします。
- ステップ 3** ID プロバイダによって開始されるフローを選択すると、アプライアンスはユーザーを SaaS アプリケーションにリダイレクトします。
- ステップ 4** サービス プロバイダによって開始されるフローを選択する場合は、この URL を SaaS アプリケーションで設定する必要があります。
- 常に SaaS ユーザーにプロキシ認証を要求する。ユーザーは有効なクレデンシャルを入力した後、SaaS アプリケーションにログインします。
  - SaaS ユーザーを透過的にサインインさせる。ユーザーは SaaS アプリケーションに自動的にログインします。

#### Note

アプライアンスが透過モードで展開されている場合に、明示的な転送要求を使用して、すべての認証済みユーザーに対するシングルサインオン動作を実現するには、ID グループを設定する際に、[明示的転送要求に同じサロゲート設定を適用 (Apply same surrogate settings to explicit forward requests)] 設定を選択します。

## 発信トラフィックでの既存の感染のスキャン

この章で説明する内容は、次のとおりです。



- [発信トラフィックのスキャンの概要 \(408 ページ\)](#)
- [アップロード要求について \(408 ページ\)](#)
- [アウトバウンド マルウェア スキャン ポリシーの設定 \(410 ページ\)](#)
- [アップロード要求の制御 \(412 ページ\)](#)
- [DVS スキャンのロギング \(413 ページ\)](#)

## 発信トラフィックのスキャンの概要

悪意のあるデータがネットワークから発信されないようにするため、Secure Web Applianceには発信マルウェアスキャン機能があります。ポリシー グループを使用して、マルウェアのスキャン対象となるアップロード、スキャンに使用するマルウェア対策スキャン エンジン、ブロックするマルウェアのタイプを定義できます。

Cisco Dynamic Vectoring and Streaming (DVS) エンジンは、トランザクション要求がネットワークから発信されるときにそれをスキャンします。Cisco DVS エンジンとの連携により、Secure Web Applianceでは無意識のうちに悪意のあるデータがアップロードされるのを防止できます。

次の作業を実行できます。

| タスク                              | タスクへのリンク                                                |
|----------------------------------|---------------------------------------------------------|
| マルウェアをブロックするポリシーを作成する            | <a href="#">アウトバウンド マルウェア スキャン ポリシーの設定, on page 410</a> |
| 発信マルウェア ポリシー グループにアップロード要求を割り当てる | <a href="#">アップロード要求の制御, on page 412</a>                |

## 要求が DVS エンジンによってブロックされた場合のユーザー エクスペリエンス

Cisco DVS エンジンがアップロード要求をブロックすると、Web プロキシはエンドユーザーにブロック ページを送信します。ただし、すべての Web サイトでエンドユーザーにブロック ページが表示されるわけではありません。一部の Web 2.0 Web サイトでは、静的 Web ページの代わりに JavaScript を使用して動的コンテンツが表示され、ブロック ページが表示されることはありません。そのような場合でも、ユーザーは適切にブロックされているので悪意のあるデータをアップロードすることはありませんが、そのことが Web サイトから通知されない場合もあります。

## アップロード要求について

発信マルウェア スキャン ポリシーは、サーバーにデータをアップロードするトランザクション（アップロード要求）に対して、Web プロキシが HTTP 要求と復号 HTTPS 接続をブロックするかどうかを定義します。アップロード要求は、要求本文にコンテンツが含まれている HTTP または復号 HTTPS 要求です。

アップロード要求を受信すると、Web プロキシは要求を発信マルウェア スキャン ポリシー グループと比較して、適用するポリシー グループを決定します。ポリシー グループに要求を割り当てた後、ポリシー グループの設定済み制御設定と要求を比較し、要求をモニターするかブロックするかを決定します。発信マルウェア スキャン ポリシーによる判定で要求をモニターすることが決定されると、要求はアクセス ポリシーに対して評価され、Web プロキシが実行する最終アクションが該当するアクセス ポリシーによって決定されます。



**Note** サイズがゼロ (0) バイトのファイルのアップロードを試みているアップロード要求は、発信マルウェア スキャン ポリシーに対して評価されません。

## グループメンバーシップの基準

各クライアント要求に ID が割り当てられ、次に、それらの要求が他のポリシー タイプと照合して評価され、タイプごとに要求が属するポリシー グループが判定されます。Web プロキシは、要求のポリシー グループメンバーシップに基づいて、設定されているポリシー制御設定をクライアント要求に適用します。

Web プロキシは、特定のプロセスを実行してグループメンバーシップの基準と照合します。グループメンバーシップの以下の要素が考慮されます。

| 基準                                   | 説明                                                                                                                                                                                  |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 識別プロファイル<br>(Identification Profile) | 各クライアント要求は、識別プロファイルに一致するか、認証に失敗するか、ゲストアクセスが許可されるか、または認証に失敗して終了します。                                                                                                                  |
| 権限を持つユーザー                            | 割り当てられた識別プロファイルが認証を必要とする場合に、そのユーザーが発信マルウェア スキャン ポリシー グループの承認済みユーザーのリストに含まれており、ポリシー グループに一致している必要があります。承認済みユーザーのリストには、任意のグループまたはユーザーを指定でき、識別プロファイルがゲストアクセスを許可している場合はゲスト ユーザーを指定できます。 |
| 詳細オプション<br>(Advanced options)        | 発信マルウェア スキャン ポリシー グループメンバーシップの複数の高度なオプションを設定できます。一部のオプション（プロキシポート、URL カテゴリなど）は、識別プロファイル内に定義することもできます。高度なオプションを識別プロファイル内で設定すると、発信マルウェア スキャン ポリシー グループ レベルでは設定できなくなります。               |

## クライアント要求と発信マルウェア スキャン ポリシー グループの照合

Web プロキシは、アップロード要求のステータスを最初のポリシー グループのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合は、その以下のポリシー グループとアップロード要求を比較します。アップロード要求をユーザー定義のポリシー グループと照合するまで、Web プロキシはこのプロセスを続行します。ユーザー定義のポリシー グループに一致しない場合は、グローバルポリシー グループと照合します。Web プロキシは、アップロード要求をポリシー グループまたはグローバル ポリシー グループと照合するときに、そのポリシー グループのポリシー設定を適用します。

## アウトバウンド マルウェア スキャン ポリシーの設定

宛先サイトの 1 つ以上のアイデンティティや URL カテゴリなど、複数の条件の組み合わせに基づいてアウトバウンドマルウェア スキャンポリシー グループを作成できます。ポリシー グループのメンバーシップには、少なくとも 1 つの条件を定義する必要があります。複数の条件が定義されている場合、アップロード要求がポリシー グループと一致するには、すべての条件を満たしていなければなりません。ただし、アップロード要求は設定された ID の 1 つのみと一致する必要があります。

### Procedure

**ステップ 1** [Webセキュリティマネージャ (Web Security Manager) ] > [発信マルウェア スキャン (Outbound Malware Scanning) ] を選択します。

**ステップ 2** [ポリシーを追加 (Add Policy) ] をクリックします。

**ステップ 3** ポリシー グループの名前と説明 (オプション) を入力します。

#### Note

各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

**ステップ 4** [上記ポリシーを挿入 (Insert Above Policy) ] フィールドで、ポリシー テーブル内のポリシー グループを配置する場所を選択します。

複数のポリシー グループを設定する場合は、各グループに論理的な順序を指定します。

**ステップ 5** [識別プロファイルおよびユーザー (Identification Profiles And Users) ] セクションで、このポリシー グループに適用する 1 つまたは複数の ID グループを選択します。

**ステップ 6** (オプション) [詳細 (Advanced) ] セクションを拡張して、追加のメンバーシップ要件を定義します。

**ステップ 7** いずれかの拡張オプションを使用してポリシーグループのメンバーシップを定義するには、拡張オプションのリンクをクリックし、表示されるページでオプションを設定します。

| 高度なオプション                     | 説明                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プロトコル                        | <p>クライアント要求で使用するプロトコルによってポリシー グループのメンバーシップを定義するかどうかを選択します。含めるプロトコルを選択します。</p> <p>[その他のすべて (All others)] は、このオプションの上に一覧表示されていないプロトコルを意味します。</p> <p><b>Note</b><br/>HTTPS プロキシをイネーブルにすると、復号ポリシーのみが HTTPS トランザクションに適用されます。アクセス、ルーティング、アウトバウンドマルウェア スキャン、データセキュリティ、外部 DLP のポリシーの場合は、HTTPS プロトコルによってポリシー メンバーシップを定義できません。</p>                                                                                                |
| プロキシ ポート<br>(Proxy Ports)    | <p>Web プロキシへのアクセスに使用するプロキシポートで、ポリシー グループ メンバーシップを定義するかどうかを選択します。[プロキシポート (Proxy Ports)] フィールドに、1 つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。</p> <p>明示的な転送接続のために、ブラウザに設定されたポートです。透過接続の場合は、宛先ポートと同じです。</p> <p>クライアント要求がアプライアンスに透過的にリダイレクトされるときにプロキシポートでポリシー グループのメンバーシップを定義すると、一部の要求が拒否される場合があります。</p> <p><b>Note</b><br/>このポリシー グループに関連付けられている ID がこの詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。</p> |
| サブネット<br>(Subnets)           | <p>サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義するかどうかを選択します。</p> <p>関連 ID で定義されている可能性のあるアドレスを使用するか、またはここで特定のアドレスを入力することができます。</p> <p><b>Note</b><br/>ポリシー グループに関連付けられている ID がアドレスによってメンバーシップを定義している場合は、ID で定義されているアドレスのサブセットであるアドレスを、このポリシー グループに入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込めます。</p>                                                                                                   |
| URL カテゴリ<br>(URL Categories) | <p>URL カテゴリでポリシー グループのメンバーシップを定義するかどうかを選択します。ユーザー定義または定義済みの URL カテゴリを選択します。</p> <p><b>Note</b><br/>このポリシー グループに関連付けられている ID がこの詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。</p>                                                                                                                                                                                                                     |

| 高度なオプション                  | 説明                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ユーザー エージェント (User Agents) | <p>クライアント要求で使用するユーザー エージェント (アップデータや Web ブラウザなどのクライアント アプリケーション) ごとにポリシー グループ メンバーシップを定義するかどうかを選択します。一般的に定義されているユーザー エージェントを選択するか、正規表現を使用して独自に定義できます。メンバーシップの定義に選択したユーザー エージェントのみを含めるか、選択したユーザー エージェントを明確に除外するかどうかを指定します。</p> <p><b>Note</b><br/>このポリシー グループに関連付けられている<b>識別プロファイル</b>が、この詳細設定によって<b>識別プロファイル</b> メンバーシップを定義している場合、<b>非識別プロファイル</b> ポリシー グループ レベルではこの設定項目を設定できません。</p> |
| ユーザーの場所 (User Location)   | ユーザーのリモートまたはローカルの場所でポリシー グループのメンバーシップを定義するかどうかを選択します。                                                                                                                                                                                                                                                                                                                                 |

**ステップ 8** 変更を送信します。

**ステップ 9** アウトバウンドマルウェア スキャン ポリシー グループの管理を設定して、Web プロキシがトランザクションを処理する方法を定義します。

新しいアウトバウンドマルウェア スキャン ポリシー グループは、各制御設定のオプションが設定されるまで、グローバル ポリシー グループの設定を自動的に継承します。

**ステップ 10** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## アップロード要求の制御

各アップロード要求は、アウトバウンドマルウェア スキャン ポリシー グループに割り当てられ、そのポリシー グループの制御設定を継承します。Web プロキシは、アップロード要求ヘッダーを受信することにより、要求本文をスキャンする必要があるかどうかを判定するための必要情報を得ます。DVS エンジンが要求をスキャンし、Web プロキシに判定を返します。必要に応じて、エンド ユーザーにブロック ページが表示されます。

### Procedure

- ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] > [発信マルウェア スキャン (Outbound Malware Scanning)] を選択します。
- ステップ 2** [接続先 (Destinations)] 列で、設定するポリシー グループのリンクをクリックします。
- ステップ 3** [接続先設定の編集 (Edit Destination Settings section)] セクションで、ドロップダウン メニューから [接続先スキャンのカスタム設定の定義 (Define Destinations Scanning Custom Settings)] を選択します。
- ステップ 4** [スキャンする接続先 (Destination to Scan)] セクションで、以下のいずれかを選択します。

| オプション                                                                            | 説明                                                                                                                                                                                            |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| どのアップロードもスキャンしない (Do not scan any uploads)                                       | DVS エンジンはアップロード要求をスキャンしません。すべてのアップロード要求がアクセス ポリシーに対して評価されます。                                                                                                                                  |
| すべてのアップロードをスキャンする (Scan all uploads)                                             | DVS エンジンはすべてのアップロード要求をスキャンします。DVS エンジンのスキャン判定に応じて、アップロード要求はブロックされるか、またはアクセス ポリシーに対して評価されます。                                                                                                   |
| 指定したカスタム URL カテゴリへのアップロードをスキャン (Scan uploads to specified custom URL categories) | DVS エンジンは、特定のカスタム URL カテゴリに属するアップロード要求をスキャンします。DVS エンジンのスキャン判定に応じて、アップロード要求はブロックされるか、またはアクセス ポリシーに対して評価されます。<br>[カスタムカテゴリリストを編集 (Edit custom categories list)] をクリックして、スキャンする URL カテゴリを選択します。 |

**ステップ 5** 変更を送信します。

**ステップ 6** [マルウェア対策フィルタリング (Anti-Malware Filtering)] 列で、ポリシー グループのリンクをクリックします。

**ステップ 7** [マルウェア対策設定 (Anti-Malware Settings)] セクションで、[マルウェア対策カスタム設定の定義 (Define Anti-Malware Custom Settings)] を選択します。

**ステップ 8** [Cisco DVS マルウェア対策設定 (Cisco DVS Anti-Malware Settings)] セクションで、このポリシー グループに対してイネーブルにするマルウェア対策スキャン エンジンを選択します。

**ステップ 9** [マルウェア カテゴリ (Malware Categories)] セクションで、さまざまなマルウェア カテゴリをモニターするかブロックするかを選択します。

このセクションに一覧表示されるカテゴリは、イネーブルにするスキャンエンジンによって異なります。

#### Note

設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャンエンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV\_TIMEOUT や SV\_ERROR の場合は、スキャン不可のトランザクションと見なされます。

**ステップ 10** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## DVS スキャンのロギング

アクセス ログは、DVS エンジンがマルウェアについてアップロード要求をスキャンしたかどうかを示します。各アクセス ログ エントリのスキャン判定情報セクションには、スキャンされたアップロードに対する DVS エンジン アクティビティの値が含まれています。フィールドのいずれかを W3C またはアクセス ログに追加すると、この DVS エンジン アクティビティをより簡単に検索できます。

Table 5: W3C ログのログ フィールドおよびアクセス ログのフォーマット指定子

| W3C ログフィールド           | アクセス ログのフォーマット指定子 |
|-----------------------|-------------------|
| x-req-dvs-scanverdict | %X2               |
| x-req-dvs-threat-name | %X4               |
| x-req-dvs-verdictname | %X3               |

DVS エンジンによってアップロード要求がマルウェアと判定され、DVS エンジンがマルウェアのアップロードをブロックするように設定されている場合、アクセス ログの ACL デシジョン タグは BLOCK\_AMW\_REQ になります。

ただし、DVS エンジンによってアップロード要求がマルウェアと判定され、DVS エンジンがマルウェアをモニターするように設定されている場合、アクセス ログの ACL デシジョン タグは、実際にトランザクションに適用されるアクセス ポリシーによって決まります。

DVS エンジンがマルウェアについてアップロード要求をスキャンしたかどうかを判断するには、各アクセス ログ エントリのスキャン判定情報セクションで、DVS エンジン アクティビティの結果を確認します。



## 第 6 章

### 統合

---

この章で説明する内容は、次のとおりです。

- [Cisco Identity Services Engine \(ISE\) / ISE パッシブ ID コントローラ \(ISE-PIC\) の統合 \(415 ページ\)](#)
- [Cisco XDR との統合 \(433 ページ\)](#)
- [Cisco Secure Web Appliance と Cisco Umbrella の統合 \(439 ページ\)](#)

## Cisco Identity Services Engine (ISE) / ISE パッシブ ID コントローラ (ISE-PIC) の統合

この章で説明する内容は、次のとおりです。

- [Identity Services Engine \(ISE\) / ISE パッシブ ID コントローラ \(ISE-PIC\) サービスの概要 \(415 ページ\)](#)
- [ISE/ISE-PIC の証明書 \(419 ページ\)](#)
- [フォールバック認証 \(420 ページ\)](#)
- [ISE/ISE-PIC サービスを統合するためのタスク \(420 ページ\)](#)
- [ISE-SXP 統合の設定 \(430 ページ\)](#)
- [ISE/ISE-PIC 統合での VDI \(仮想デスクトップインフラストラクチャ\) ユーザー認証 \(432 ページ\)](#)
- [Identity Services Engine に関する問題のトラブルシューティング \(433 ページ\)](#)

## Identity Services Engine (ISE) / ISE パッシブ ID コントローラ (ISE-PIC) サービスの概要

Cisco Identity Services Engine (ISE) は、ID 管理を向上させるためにネットワーク上の個々のサーバーで実行されるアプリケーションです。Secure Web Appliance は、ISE または ISE-PIC の



サーバーからユーザーアイデンティティ情報にアクセスできます。ISE または ISE-PIC のいずれかが設定されている場合は、適切に設定された識別プロファイルに対してユーザー名および関連するセキュリティ グループ タグが ISE から、ユーザー名および Active Directory グループが ISE-PIC からそれぞれ取得され、それらのプロファイルを使用するように設定されたポリシーで透過的ユーザー識別が許可されます。

- セキュリティ グループ タグと Active Directory グループを使用してアクセス ポリシーを作成できます。
- ISE/ISE-PIC による透過的な識別に失敗したユーザーの場合、Active Directory ベースのレールムを使用してフォールバック認証を設定できます。「[フォールバック認証, on page 420](#)」を参照してください。
- 仮想デスクトップ環境 (Citrix、Microsoft 共有/リモート デスクトップ サービスなど) でユーザーの認証を設定できます。「[ISE/ISE-PIC 統合での VDI \(仮想デスクトップ インフラストラクチャ\) ユーザー認証, on page 432](#)」を参照してください。

**Note**

- ISE/ISE-PIC サービスはコネクタ モードでは使用できません。
- ISE/ISE-PIC バージョン 2.4、および PxGrid バージョン 2.0 がサポートされます。
- Secure Web Applianceの Web インターフェイスで ISE 設定ページを使用して、ISE または ISE-PIC サーバーの設定、証明書のアップロード、ISE または ISE-PIC のいずれかのサービスへの接続を実行します。ISE または ISE-PIC を設定する手順は似ています。ISE-PIC に固有の詳細が適宜記載されています。

Cisco Secure Web Appliance ISE バージョンのサポートマトリックスの詳細については、『[ISE Compatibility Matrix Information](#)』を参照してください。

**Table 6: Secure Web Appliance-ISE スケール サポート マトリックス**

| モデル             | AD グループが有効になっていないセッションスケール | AD グループが有効になっているセッションスケール |                                                                  |
|-----------------|----------------------------|---------------------------|------------------------------------------------------------------|
| -               | サポートされている最大アクティブセッション数     | サポートされている最大アクティブセッション数    | サポートされている最大エンドポイント数<br>(各ユーザーの AD グループエントリと ISE データベース内のエンドポイント) |
| S695、S696       | 200K                       | 125K                      | 400K                                                             |
| S600V           | 150K                       | 50K                       | 150K                                                             |
| S195、S196、S300V | 50K                        | 50K                       | 75K                                                              |
| S100V           | 50K                        | 40K                       | 50K                                                              |

**Note**

\*S190、S390、および S690 モデルはサポートされていません。

**関連項目**

- [pxGrid について, on page 418](#)
- [ISE/ISE-PIC サーバーの展開とフェールオーバーについて, on page 418](#)

## pxGrid について

シスコの Platform Exchange Grid (pxGrid) を使用すると、セキュリティ モニターリングとネットワーク 検出システム、ID とアクセス管理プラットフォームなど、ネットワーク インフラストラクチャのコンポーネントを連携させることができます。これらのコンポーネントは pxGrid を使用して、パブリッシュまたはサブスクライブ メソッドにより情報を交換します。

以下の 3 つの主要 pxGrid コンポーネントがあります：pxGrid パブリッシャ、pxGrid クライアント、pxGrid コントローラ。

- pxGrid パブリッシャ：pxGrid クライアントの情報を提供します。
- pxGrid クライアント：パブリッシュされた情報をサブスクライブする任意のシステム（Secure Web Appliance など）。パブリッシュされる情報には、セキュリティグループタグ（SGT）、Active Directory グループ、ユーザーグループおよびプロファイルの情報が含まれます。
- pxGrid コントローラ：クライアントの登録/管理およびトピック/サブスクリプションプロセスを制御する ISE/ISE-PIC pxGrid ノードが該当します。

各コンポーネントには信頼できる証明書が必要です。これらの証明書は各ホストプラットフォームにインストールしておく必要があります。

## ISE/ISE-PIC サーバーの展開とフェールオーバーについて

単一の ISE/ISE-PIC ノードのセットアップはスタンドアロン展開と呼ばれ、この 1 つのノードによって、管理およびポリシー サービスが実行されます。フェールオーバーをサポートし、パフォーマンスを向上させるには、複数の ISE/ISE-PIC ノードを分散展開でセットアップする必要があります。Secure Web Appliance で ISE/ISE-PIC フェールオーバーをサポートするために必要な最小限の分散 ISE/ISE-PIC 構成は以下のとおりです。

- 2 つの pxGrid ノード
- 2 つの管理ノード
- 1 つのポリシー サービス ノード

この構成は、『Cisco Identity Services Engine Hardware Installation Guide』では「中規模ネットワーク展開」と呼ばれています。詳細については、『Installation Guide』のネットワーク展開に関する項を参照してください。

### 関連項目

- [ISE/ISE-PIC の証明書, on page 419](#)
- [ISE/ISE-PIC サービスを統合するためのタスク, on page 420](#)
- [ISE/ISE-PIC サービスへの接続, on page 423](#)
- [Identity Services Engine に関する問題のトラブルシューティング, on page 433](#)

## ISE/ISE-PIC の証明書

**Note**

このセクションでは、ISE/ISE-PIC 接続に必要な証明書について説明します。[ISE/ISE-PIC サービスを統合するためのタスク, on page 420](#)では、これらの証明書に関する詳細情報を提供します。[証明書の管理, on page 200](#)は、AsyncOS の証明書の一般的な管理情報を提供します。

Secure Web Appliance と各 ISE/ISE-PIC サーバー間で相互認証と安全な通信を行うには、一連の 2 つの証明書が必要です。

- **Web Appliance クライアント証明書**： Secure Web Appliance を認証するために ISE/ISE-PIC サーバーで使用されます。
- **ISE pxGrid 証明書**： Secure Web Appliance-ISE/ISE-PIC データサブスクリプション (ISE/ISE-PIC サーバーに対する進行中のパブリッシュ/サブスクライブクエリー) 向けに ISE/ISE-PIC サーバーを認証するためにポート 5222 で Secure Web Appliance によって使用されます。

この 2 つの証明書は、認証局 (CA) による署名でも自己署名でもかまいません。CA 署名付き証明書が必要な場合、AsyncOS には自己署名 Web Appliance クライアント証明書、または証明書署名要求 (CSR) を生成するオプションがあります。同様に ISE/ISE-PIC サーバーにも、CA 署名付き証明書が必要な場合に、自己署名 ISE/ISE-PIC pxGrid 証明書、または CSR を生成するオプションがあります。

### 関連項目

- [自己署名証明書の使用, on page 419](#)
- [CA 署名付き証明書の使用, on page 420](#)
- [Identity Services Engine \(ISE\) / ISE パッシブ ID コントローラ \(ISE-PIC\) サービスの概要, on page 415](#)
- [ISE/ISE-PIC サービスを統合するためのタスク, on page 420](#)
- [ISE/ISE-PIC サービスへの接続, on page 423](#)

## 自己署名証明書の使用

自己署名証明書が ISE/ISE-PIC サーバーで使用される場合は、ISE/ISE-PIC サーバーで開発された ISE/ISE-PIC pxGrid 証明書、Secure Web Appliance で開発された Web Appliance クライアント証明書を、ISE/ISE-PIC サーバー上の信頼できる証明書ストアに追加する必要があります (ISE の場合は [管理 (Administration)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)]、ISE-PIC の場合は [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)] )。

**Caution**

認証に自己署名証明書を使用するのは、他の認証方法ほど安全ではないためお勧めしません。また、自己署名証明書は失効ポリシーをサポートしていません。

## CA 署名付き証明書の使用

CA 署名付き証明書の場合：

- ISE/ISE-PIC サーバーで、Web Appliance クライアント証明書に適した CA ルート証明書が信頼できる証明書ストアにあることを確認します ([管理 (Administration)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] )。
- Secure Web Appliance で、適切な CA ルート証明書が信頼できる証明書リストにあることを確認します ([ネットワーク (Network)] > [証明書管理 (Certificate Management)] > [信頼できるルート証明書の管理 (Manage Trusted Root Certificates)] )。
- [Identity Services Engine] ページ ([ネットワーク (Network)] > [Identity Services Engine]) で、ISE/ISE-PIC pxGrid 証明書用の CA ルート証明書がアップロードされていることを確認します。

## フォールバック認証

ISE/ISE-PIC で利用できないユーザー情報については、フォールバック認証を設定できます。フォールバック認証が成功するには、次のものがが必要です。

- Active Directory ベースのレルムのフォールバックオプションで設定された識別プロファイル。
- フォールバックオプションを含む正しい識別プロファイルを使用したアクセスポリシー。

## ISE/ISE-PIC サービスを統合するためのタスク

**Note**

- ISE/ISE-PIC バージョン 2.4、および PxGrid バージョン 2.0 がサポートされます。
- ISE-PIC で既存のアクセス ポリシーの使用を続行するには、ISE-PIC を使用する各識別プロファイルを編集してユーザーを透過的に識別する必要があります。これは、CDA を使用した識別プロファイルに適用されます。CDA 識別から ISE-PIC ベースの識別に移行している場合は、それぞれの識別プロファイルを編集する必要があります。

**Note**

- AsyncOS 11.5 以前のバージョンから AsyncOS 11.7 以降のバージョンにアップグレードする場合は、Secure Web Appliance で ISE を再設定します。
- 証明書は ISE/ISE-PIC デバイスを介して生成する必要があります、生成された証明書は Secure Web Appliance にアップロードする必要があります。

| 手順 | タスク                                                             | トピックおよび手順へのリンク                                                                                                                                                                               |
|----|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | ISE/ISE-PIC デバイスを介した証明書の生成。                                     | <a href="#">ISE/ISE-PIC を介した証明書の生成, on page 422</a>                                                                                                                                          |
| 2  | Secure Web Appliance にアクセスするために ISE/ISE-PIC を設定する。              | <a href="#">Secure Web Appliance にアクセスするための ISE/ISE-PIC サーバーの設定, on page 422</a>                                                                                                             |
| 3  | Secure Web Appliance で ISE/ISE-PIC サービスを設定および有効にする。             | <a href="#">ISE/ISE-PIC サービスへの接続, on page 423</a>                                                                                                                                            |
| 4  | Secure Web Appliance クライアント証明書が自己署名済みの場合は、ISE/ISE-PIC にインポートする。 | <a href="#">自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC スタンドアロン展開へのインポート, on page 426</a><br><a href="#">自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC 分散型展開へのインポート, on page 426</a> |
| 5  | 必要に応じて、Secure Web Appliance でロギングを設定する。                         | <a href="#">ISE/ISE-PIC へのロギングの設定, on page 428</a>                                                                                                                                           |
| 6  | ISE/ISE-PIC ERS サーバーの詳細を取得します。                                  | <a href="#">ISE/ISE-PIC からの ISE/ISE-PIC ERS サーバー詳細情報の取得, on page 429</a>                                                                                                                     |

**関連項目**

- [Identity Services Engine \(ISE\) / ISE パッシブ ID コントローラ \(ISE-PIC\) サービスの概要, on page 415](#)
- [ISE/ISE-PIC の証明書, on page 419](#)
- [Identity Services Engine に関する問題のトラブルシューティング, on page 433](#)

## ISE/ISE-PIC を介した証明書の生成



(注) ISE/ISE-PIC デバイスを介して生成される証明書は、PKCS12 形式である必要があります。

### • ISE/ISE-PIC :

#### 手順

**ステップ 1** [ワークセンター (Work Centers)] > [PassiveID] > [サブスクライバ (Subscribers)] > [証明書 (Certificates)] を選択します。

**ステップ 2** [証明書のダウンロード形式 (Certificate Download Format)] ドロップダウンリストから [PKCS12形式 (PKCS 12 format)] を選択します。[証明書 (Certificates)] タブでその他の必要な情報を入力し、pxGrid 証明書を生成します。

**ステップ 3** 次の `openssl` コマンドを使用して、生成された XXX.pk12 ファイルからルート CA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを抽出します。

- ルート CA : `openssl pkcs12 -in XXX.p12 -cacerts -nokeys -chain -out RootCA.pem`
- Web Appliance クライアント証明書 : `openssl pkcs12 -in XXX.p12 -clcerts -nokeys -out publicCert.pem`
- Web Appliance クライアントキー : `openssl pkcs12 -in XXX.p12 -nocerts -nodes -out privateKey.pem`

(注)

証明書パスワードは、手順 2 の実行中に ISE Web インターフェイスで入力したものを使用してください。

(注)

セカンダリ/フェールオーバー ISE サーバーを介してセカンダリルート CA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを生成するには、同じ手順を実行します。

## Secure Web Applianceにアクセスするための ISE/ISE-PIC サーバーの設定

### • ISE

- 識別トピックサブスクライバ (Secure Web Appliance など) がリアルタイムでセッションコンテキストを取得できるように、各 ISE サーバーを設定する必要があります。

1. [管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [設定 (Settings)] > [pxGridの設定 (pxGrid Settings)] を選択します。
2. [新しい証明書ベースのアカウントを自動的に承認する (Automatically approve new certificate-based accounts)] がオンになっていることを確認します。

ISE/ISE-PIC での認証に関与しない、設定済みの古い Secure Web Applianceをすべて削除します。

ISE サーバーのフッターが緑で、「**pxGridに接続されました (Connected to pxGrid)**」と表示されていることを確認します。

#### • ISE-PIC

- 識別トピックサブスクリバ（Secure Web Applianceなど）がリアルタイムでセッションコンテキストを取得できるように、各 ISE-PIC サーバーを設定する必要があります。

1. **[サブスクリバ (Subscribers)] > [設定 (Settings)]** を選択します。
2. **[新しい証明書ベースのアカウントを自動的に承認する (Automatically approve new certificate-based accounts)]** がオンになっていることを確認します。

ISE/ISE-PIC での認証に関与しない、設定済みの古い Secure Web Applianceをすべて削除します。

ISE サーバーのフッターが緑で、「**pxGridに接続されました (Connected to pxGrid)**」と表示されていることを確認します。

詳細については、Cisco Identity Services Engine のドキュメントを参照してください。

## ISE/ISE-PIC サービスへの接続



### Note

ISE 管理証明書、pxGrid 証明書、および MNT 証明書がルート CA 証明書によって署名されている場合は、アプライアンスで [ISE pxGrid ノード証明書 (ISE pxGrid Node Certificate)] フィールドにルート CA 証明書自体をアップロードします ([ネットワーク (Network)] > [Identity Services Engine])。

### Before you begin

- 各 ISE/ISE-PIC サーバーが Secure Web Appliance へのアクセス用に正しく設定されていることを確認します ([ISE/ISE-PIC サービスを統合するためのタスク, on page 420](#)を参照)。
- 有効な ISE/ISE-PIC 関連の証明書およびキーを取得します。関連情報については、[ISE/ISE-PIC を介した証明書の生成, on page 422](#)を参照してください。
- 取得した RootCA.pem を Secure Web Appliance にインポートします ([ネットワーク (Network)] > [CertificateManagement] > [TrustedRootCertificate] > [ManageTrustedRootCertificate] 上のクライアント (Client on ManageTrustedRootCertificate))。生成された XXX.pk12 ファイルからルート CA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを抽出するには、[ISE/ISE-PIC を介した証明書の生成, on page 422](#)を参照してください。





**Note** セカンダリ XXXX.pk12 ファイルから抽出された RootCA.pem について同じ手順に実行します（セカンダリ/フェールオーバー ISE サーバーが使用可能な場合）。

- Secure Web Appliance の Web インターフェイスで ISE 設定ページを使用して、ISE または ISE-PIC サーバーの設定、証明書のアップロード、ISE または ISE-PIC のいずれかのサービスへの接続を実行します。ISE と ISE-PIC を設定する手順は同じです。ISE-PIC 設定に固有の詳細が適宜記載されています。
- ISE/ISE-PIC が提供する Active Directory グループを使用してアクセスポリシーを構築する場合は、ERS を有効にします。
- AsyncOS 15.0 リリースの一部として、OpenSSL バージョン 1.1.1 およびライブラリは IP ベースの証明書を受け入れなくなりました。[テスト開始 (Start Test)] が成功し、ISE が期待どおりに機能することを確認するには、SWA ISE 設定でホスト名のみを使用する必要があります。

## Procedure

- ステップ 1** [ネットワーク (Network)] > [Identification Service Engine] を選択します。
- ステップ 2** [設定の編集 (Edit Settings)] をクリックします。
- ISE/ISE-PIC を初めて設定する場合は、[設定の有効化と編集 (Enable and Edit Settings)] をクリックします。
- ステップ 3** [ISE サービスを有効にする (Enable ISE Service)] をオンにします。
- ステップ 4** ホスト名または IPv4 アドレスを使用して **プライマリ管理ノード** を特定し、Secure Web Appliance の [プライマリ ISE pxGrid ノード (Primary ISE pxGrid Node)] タブに次の情報を入力します。
- a) Secure Web Appliance-ISE/ISE-PIC データサブスクリプション (ISE/ISE-PIC サーバーに対して進行中のクエリー) 用の **ISE pxGrid ノード証明書** を指定します。
- プライマリ ISE サーバーからルート CA として生成される証明書（つまり、RootCA.pem）（または、すべての中間証明書を含む証明書チェーン）を参照して選択し、[ISE/ISE-PIC を介した証明書の生成, on page 422](#) を参照して [ファイルのアップロード (Upload File)] をクリックします。詳細については、[証明書およびキーのアップロード, on page 203](#) を参照してください。
- ステップ 5** フェールオーバー用に 2 台目の ISE/ISE-PIC サーバーを使用している場合は、ホスト名または IPv4 アドレスを使用してその **プライマリ管理ノード** を特定し、ホスト名または IPv4 アドレスを使用して Secure Web Appliance の [セカンダリ ISE pxGrid ノード (Secondary ISE pxGrid Node)] タブに次の情報を入力します。
- a) セカンダリ **ISE pxGrid ノード証明書** を入力します。

セカンダリ ISE サーバーからルート CA として生成される証明書（つまり、**RootCA.pem**）（または、すべての中間証明書を含む証明書チェーン）を参照して選択し、[ISE/ISE-PIC を介した証明書の生成, on page 422](#)を参照して [ファイルのアップロード (Upload File)] をクリックします。詳細については、[証明書およびキーのアップロード, on page 203](#)を参照してください。

**Note**

プライマリからセカンダリの ISE サーバーにフェールオーバーするときに、既存の ISE SGT キャッシュに含まれていないユーザーは、Secure Web Appliance の設定に応じて、認証が必要になるか、またはゲスト認証が割り当てられます。ISE フェールオーバーが完了すると、通常の ISE 認証が再開されます。

**ステップ 6** Secure Web Appliance-ISE/ISE-PIC サーバーの相互認証用の **Web Appliance クライアント証明書**を指定します。

- **[アップロードされた証明書とキーを使用 (Use Uploaded Certificate and Key)]**

証明書とキーの両方に対して、[選択 (Choose)] をクリックして各ファイルを参照します。

**Note**

ISE/ISE-PIC デバイスを介して生成された publicCert.pem と privateKey.pem を選択してアップロードします。「[ISE/ISE-PIC を介した証明書の生成, on page 422](#)」を参照してください。

キーが暗号化されている場合は、[キーは暗号化されています (Key is Encrypted)] チェックボックスをオンにします。

[ファイルのアップロード (Upload Files)] をクリックします。（このオプションの詳細については、[証明書およびキーのアップロード, on page 203](#)を参照してください）。

**ステップ 7** ISE SGT eXchange Protocol (SXP) サービスを有効にします。

Secure Web Appliance が ISE サービスから SXP バインディングトピックを取得する方法については、[SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化, on page 431](#)を参照してください。

**ステップ 8** ISE 外部 Restful サービス (ERS) を有効にします。

- ERS 管理者のユーザー名とパスワードを入力します。[ISE/ISE-PIC からの ISE/ISE-PIC ERS サーバー詳細情報の取得, on page 429](#)を参照。
- ERS が同じ ISE または ISE/ISE-PIC pxGrid ノードで使用可能な場合は、[ISE pxGrid ノードと同じサーバー名 (Server name same as ISE pxGrid Node)] チェックボックスを確認します。同じノードで使用できない場合は、プライマリおよびセカンダリ（設定されている場合）サーバーのホスト名または IPv4 アドレスを入力します。

**ステップ 9** **[テスト開始 (Start Test)]** をクリックして、ISE/ISE-PIC の pxGrid ノードと同じ接続をテストします。

**ステップ 10** **[送信 (Submit)]** をクリックします。

---

**What to do next**

- [ユーザーおよびクライアント ソフトウェアの分類, on page 267](#)

- インターネット要求を制御するポリシーの作成, on page 362

#### 関連情報

- <http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html> 特に「How To Integrate Cisco Secure Web Appliance using ISE/ISE-PIC and TrustSec through pxGrid..」。

## 自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC スタンドアロン展開へのインポート

基本的な手順は以下のとおりです。

- ISE 管理ノード
  - [管理 (Administration)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)] の順に選択します。

次のオプションがオンになっていることを確認してください。

- [ISE内の認証用に信頼する (Trust for authentication within ISE)]
- [クライアント認証およびsyslog用に信頼する (Trust for client authentication and Syslog)]
- [シスコサービスの認証用に信頼する (Trust for authentication of Cisco Services)]

- ISE-PIC 管理ノード

- [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)] の順に選択します。

次のオプションがオンになっていることを確認してください。

- [ISE内の認証用に信頼する (Trust for authentication within ISE)]
  - [クライアント認証およびsyslog用に信頼する (Trust for client authentication and Syslog)]
  - [シスコサービスの認証用に信頼する (Trust for authentication of Cisco Services)]

詳細については、Cisco Identity Services Engine のドキュメントを参照してください。

## 自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC 分散型展開へのインポート

基本的な手順は以下のとおりです。

- ISE 管理ノード :

- [管理 (Administration)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)] の順に選択します。

次のオプションがオンになっていることを確認してください。

- [ISE内の認証用に信頼する (Trust for authentication within ISE)]
- [クライアント認証およびsyslog用に信頼する (Trust for client authentication and Syslog)]
- [シスコサービスの認証用に信頼する (Trust for authentication of Cisco Services)]

• ISE-PIC 管理ノード :

- [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)] の順に選択します。

次のオプションがオンになっていることを確認してください。

- [ISE内の認証用に信頼する (Trust for authentication within ISE)]
- [クライアント認証およびsyslog用に信頼する (Trust for client authentication and Syslog)]
- [シスコサービスの認証用に信頼する (Trust for authentication of Cisco Services)]

詳細については、Cisco Identity Services Engine のドキュメントを参照してください。



- (注) 分散型 ISE 展開では、Secure Web Applianceは MNT、PAN、および PxGrid ノードと通信します。この場合、証明書またはすべての証明書の発行者が、「抽出されたルート証明書」（つまり、ISE/ISE-PIC デバイスを介して生成された RootCA）で使用する必要があります。  
「[ISE/ISE-PIC を介した証明書の生成（422 ページ）](#)」を参照してください。

## 手順

- ステップ 1** [ISE/ISE-PIC を介した証明書の生成（422 ページ）](#) の手順に従って、RootCA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを生成します。
- ステップ 2** ISE/ISE-PIC 管理ノードで、[ISE/ISE-PIC] > [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [システム証明書 (System Certificates)] から自己署名証明書を手動でエクスポートします。
1. [pxGrid]、[EAP認証 (EAP Authentication)]、[管理 (Admin)]、[ポータル (Portal)]、[RADIUS DTLS] のいずれかによって使用されている (Used by) 証明書を選択します。
  2. [エクスポート (Export)] をクリックし、生成された .pem ファイルを保存します。

すべての ISE/ISE-PIC 分散ノードについて上記の手順を繰り返します。

**ステップ 3** openssl コマンドを使用して、ダウンロードした証明書ファイルを **RootCA.pem** に手動で追加します。ISE/ISE-PIC デバイスを介して **RootCA.pem** で証明書ファイルを生成および抽出する方法については、[ISE/ISE-PIC を介した証明書の生成 \(422 ページ\)](#) を参照してください。

1. ダウンロードした証明書に対して次のコマンドを実行します。

Example:

```
openssl x509 -in <DownloadCertificate>.pem -text | egrep "Subject:|Issuer:"
```

例 (出力) :

```
Issuer: CN=isehcamnt2.node
Subject: CN=isehcamnt2.node
```

2. 内容を次のように変更します。

Example:

```
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

3. **RootCA.pem** に次の行を追加します。

```
Bag Attributes: <Empty Attributes>
```

4. 手順 (2) のサブジェクトおよび発行者を **RootCA.pem** に (手順 (3) の行とともに) 追加します。

Example:

```
Bag Attributes: <Empty Attributes>
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

5. ダウンロードした証明書ファイルの内容全体をコピーし、**RootCA** の末尾 (手順 (4) のデータの後) に貼り付けます。

ダウンロードされたすべての分散型 ISE/ISE-PIC ノードの証明書について手順 (1) ~ (5) を繰り返し、変更された **RootCA** 証明書を保存します。

**ステップ 4** Secure Web Appliance の ISE 設定ページで、変更された **RootCA.pem** をアップロードします。「[ISE/ISE-PIC サービスへの接続 \(423 ページ\)](#)」を参照してください。

## ISE/ISE-PIC へのロギングの設定

- 認証メカニズムをログ記録するために、アクセスログにカスタムフィールド **%m** を追加します ([アクセス ログのカスタマイズ, on page 714](#))。
- ISE/ISE-PIC サービスログが作成されていることを確認します。作成されていない場合は作成します ([ログ サブスクリプションの追加および編集, on page 676](#))。
- ユーザーの識別と認証のために ISE/ISE-PIC にアクセスする識別プロファイルを定義します (「[ユーザーおよびクライアントソフトウェアの分類](#)」、117 ページ)。
- ISE/ISE-PIC ID を使用して、ユーザー要求の条件とアクションを定義するアクセスポリシーを設定します (「[ポリシーの設定](#)」、191 ページ)。

## ISE/ISE-PIC からの ISE/ISE-PIC ERS サーバー詳細情報の取得

- ISE/ISE-PIC で Cisco ISE の REST API（API で HTTPS ポート 9060 を使用）を有効にします。

**Note**

グループに基づいてセキュリティポリシーを設定するには、Secure Web Applianceで ISE 外部 RESTful サービス（ERS）を有効にする必要があります（[ネットワーク（Network）]>[Identity Services Engine]）。これは、バージョン 11.7 以降に適用されます。

**• ISE**

- [管理（Administration）]>[設定（Settings）]>[ERS設定（ERS Settings）]>[プライマリ管理ノードのERS設定（ERS settings for primary admin node）]>[ERSを有効化する（Enable ERS）]を選択します。

セカンダリノードがある場合は、[その他すべてのノードの読み取り用ERS（ERS for Read for All Other Nodes）]を有効にします。

**• ISE-PIC**

- [設定（Settings）]>[ERS設定（ERS Settings）]>[ERSを有効化する（Enable ERS）]を選択します。

- 正しい外部 RESTful サービスグループで ISE 管理者を作成していることを確認します。外部 RESTful サービス管理者グループには、ERS API へのフルアクセス（GET、POST、DELETE、PUT）が含まれています。このユーザーは、ERS API 要求を作成、読み取り、更新、および削除できます。外部 RESTful サービスオペレータ：読み取り専用アクセス（GET 要求のみ）。

**• ISE**

- [管理（Administration）]>[システム（System）]>[管理者アクセス（Admin Access）]>[管理者（Administrators）]>[管理者ユーザー（Admin Users）]を選択します。

**• ISE-PIC**

- [管理（Administration）]>[管理者アクセス（Admin Access）]>[管理者ユーザー（Admin Users）]を選択します。

ERS サービスが ISE/ISE-PIC pxGrid ノードではなく別のサーバーで使用可能な場合は、プライマリおよびセカンダリ（設定されている場合）サーバーのホスト名または IPv4 アドレスが必要です。

詳細については、Cisco Identity Services Engine のドキュメントを参照してください。

## ISE-SXP 統合の設定

このセクションは、次のトピックで構成されています。

- [SGT から IP へのアドレスマッピングの ISE-SXP プロトコルについて \(430 ページ\)](#)
- [注意事項と制約事項 \(430 ページ\)](#)
- [前提条件 \(431 ページ\)](#)
- [SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化 \(431 ページ\)](#)
- [ISE-SXP プロトコルのコンフィギュレーションの確認 \(432 ページ\)](#)

### SGT から IP へのアドレスマッピングの ISE-SXP プロトコルについて

SGT Exchange Protocol (SXP) は、ネットワークデバイス間で IP-SGT バインディングを伝播するために開発されたプロトコルです。セキュリティグループタグ (SGT) は、信頼ネットワーク内のトラフィックの送信元の権限を指定します。

Cisco Identity Services Engine (ISE) の展開を Cisco Secure Web Appliance と統合して、パッシブ認証に使用できます。Secure Web Appliance は、ISE から SXP マッピングをサブスクライブできます。ISE は SXP を使用して、SGT から IP へのアドレスマッピングデータベースを管理対象デバイスに伝播します。ISE サーバーを使用するように Secure Web Appliance を設定する場合は、ISE から SXP トピックをリッスンするオプションを有効にします。これにより、Secure Web Appliance は ISE から直接 SGT と IP アドレスマッピングについて学習します。

Secure Web Appliance は、ダミーのユーザー認証 IP アドレスを生成します。これには、ISE クラスターの IP アドレスとクライアントの IP アドレスが含まれます。したがって、複数のクライアント IP アドレスをクラスター IP アドレスで認証できます。

### 注意事項と制約事項

SGT から IP アドレスへのマッピングの ISE-SXP プロトコルに関するガイドラインと制限は次のとおりです。

- IPv6 対応のエンドポイントは、Secure Web Appliance リリース 14.5 ではサポートされません。
- Secure Web Appliance リリース 14.5 では、ユーザー名とグループマッピングは、SGT から IP アドレスへのマッピングでは使用できません。したがって、管理者は Secure Web Appliance の ISE ユーザーおよびグループに基づいてポリシーを作成することはできません。ただし、SGT を使用してポリシーを作成できます。
- 一括ダウンロードプロセスの再起動タイムスタンプをスケジュールするには、ised プロセスを再起動する時刻を HH::MM 形式 (24 時間) で設定する必要があります。



(注) ユーザー認証プロセスが示される時刻は 1 日の中で短時間に設定することをお勧めします。たとえば、00:00 時に設定します。

## 前提条件

SGT から IP アドレスへのマッピングの ISE-SXP プロトコルに関する前提条件は次のとおりです。

- 信頼できるルート証明書が必要です。信頼できるルート証明書を追加するには、「[信頼できるルート証明書の管理](#)」を参照してください。

## SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化

SGT から IP アドレスへのマッピングを含む、ISE で定義されているすべてのマッピングは、SXP を介して公開できます。次のメカニズムを使用して、ISE-SXP 情報を取得できます。

- 一括ダウンロード：ised プロセスの再起動後、Secure Web Appliance は、集約ノードで使用可能なすべての ISE-SXP エントリの情報を取得するために、一括ダウンロード要求を ISE アグリゲータノードに送信します。AsyncOS コマンドラインインターフェイス (CLI) を使用して、再起動のタイムスタンプをスケジュールできます。
- 差分更新：Secure Web Appliance は、WebSocket を介して登録し、差分更新メッセージを取得します。メッセージには次の 2 つのタイプがあります。
  - 作成：新しく作成されたすべてのエントリ
  - 削除：すべての SXP 更新エントリ



(注) Secure Web Appliance は、更新されたエントリごとに 2 つのメッセージ（「削除 (Delete)」の後に「作成 (Create)」）を受信します。

再起動をスケジュールすることができます。

## 手順

**ステップ 1** [ネットワーク (Network)] > [Identification Service Engine] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** [ISE サービスを有効にする (Enable ISE Service)] をオンにします。

**ステップ 4** Secure Web Appliance で ISE サービスから SXP バインディングトピックを取得できるようにするには、[有効 (Enable)] をオンにします。

デフォルトでは、ISE SGT eXchange Protocol (SXP) サービスは無効になっています。

**ステップ 5** [テスト開始 (Start Test)] をクリックして接続をテストします。

(注)

SXP 情報は、ISE-SGT eXchange Protocol (SXP) サービスが有効になっている場合にのみ表示されます。



ステップ 6 [Submit] をクリックします。

## ISE-SXP プロトコルのコンフィギュレーションの確認

次のいずれかの方法を使用して、ISE-SXP プロトコルのコンフィギュレーションを確認できます。

- [SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化 \(431 ページ\)](#) で [テスト開始 (Start Test)] をクリックして、表示された情報を確認します。
- AsyncOS コマンドライン インターフェイス (CLI) の **ISEDATA** コマンドの下で **STATISTICS** コマンドを使用します。

**STATISTICS** コマンドを使用すると、次の情報が表示されます。

- ERS ホスト名
- ERS 接続時間
- セッション一括ダウンロード
- グループ一括ダウンロード
- SGT 一括ダウンロード
- SXP 一括ダウンロード
- セッションの更新
- グループの更新
- SXP の更新
- メモリの割り当て
- メモリの割り当て解除
- 合計セッション数

ユーザー名は次の形式で生成されます。

```
isesxp_<ISE-node-ip>_sgt<SGT number>_<Client IP address>
```

例 : isesxp\_10.10.2.68\_sgt18\_10.10.10.10

## ISE/ISE-PIC 統合での VDI（仮想デスクトップ インフラストラクチャ）ユーザー認証

使用される送信元ポートに基づいて VDI 環境のユーザーの ISE/ISE-PIC による透過的な識別を設定できます。

Cisco Terminal Services (TS) エージェントを VDI サーバーにインストールする必要があります。Cisco TS エージェントは、ISE/ISE-PIC にアイデンティティ情報を提供します。アイデンティティ情報には、ドメイン、ユーザー名、および各ユーザーが使用するポート範囲が含まれます。

- サポートサイト (<https://www.cisco.com/c/en/us/support/index.html>) から Cisco TS エージェントをダウンロードします。
- 詳細については、『Cisco Terminal Services (TS) Agent Guide』 (<https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html>) を参照してください。
- Cisco TS エージェントと連携するように ISE/ISE-PIC API プロバイダを設定します。API コールの送信については、Cisco TS エージェントのドキュメントを参照してください。



(注)

- VDI 環境ユーザーのフォールバック認証はサポートされていません。
- シスコ ターミナル サービス エージェントと Microsoft サーバー設定で、リモートデスクトップセッションの最大数が同じであることを確認します。これにより、誤ったセッション情報が ISE から Secure Web Appliance に送信されないようにし、新しいセッションの誤認証が回避されます。

## Identity Services Engine に関する問題のトラブルシューティング

- Identity Services Engine に関する問題, on page 751
  - ISE 問題のトラブルシューティング ツール, on page 751
  - ISE サーバーの接続に関する問題, on page 752
  - ISE 関連の重要なログ メッセージ, on page 754

## Cisco XDR との統合

この章で説明する内容は、次のとおりです。

- アプライアンスと Cisco XDR の統合 (434 ページ)
- アプライアンスと Cisco XDR の統合方法 (435 ページ)
- Cisco XDR プラグインを使用した脅威分析の実行 (438 ページ)

## アプライアンスと Cisco XDR の統合

Cisco Extended Detection and Response (XDR) は、すべてのシスコセキュリティ製品に組み込まれたセキュリティプラットフォームです。これは新しいテクノロジーを導入する必要のないクラウドネイティブです。Cisco XDR は、可視性を統合し、自動化を可能にして、ネットワーク、エンドポイント、クラウド、およびアプリケーション全体のセキュリティを強化するプラットフォームを提供することで、脅威からの保護の要求を簡素化します。統合プラットフォームで技術を連携することで、Cisco XDR は測定可能な分析情報、望ましい成果、比類のないチーム間のコラボレーションを実現します。Cisco XDR では、セキュリティインフラストラクチャを連携させて機能を拡張できます。

アプライアンスと Cisco XDR の統合には、次のセクションが含まれています。

- [アプライアンスと Cisco XDR の統合方法 \(435 ページ\)](#)
- [Cisco XDR プラグインを使用した脅威分析の実行 \(438 ページ\)](#)

アプライアンスを Cisco XDR と統合し、Cisco XDR で以下のアクションを実行できます。

- 組織内の複数のアプライアンスから Web データを表示および送信します。
- Web レポートおよびトラッキングで検出された脅威を特定、調査、修正します。
- 侵害された URL または Web トラフィックをブロックします。
- 特定した脅威を迅速に解決し、特定した脅威に対して推奨されるアクションを実行します。
- 脅威をドキュメント化して調査内容を保存し、他のデバイスと情報を共有します。
- 悪意のあるドメインのブロック、不審な観測対象の追跡、承認ワークフローの開始、または Web ポリシーを更新するための IT チケットの作成を行います。

Cisco XDR には、次の URL を使用してアクセスできます。

- <https://xdr.us.security.cisco.com/> (北米)
- <https://xdr.eu.security.cisco.com/> (欧州)
- <https://xdr.apjc.security.cisco.com/> (アジア太平洋地域、日本、中国)

Cisco Secure Web Appliance は高度な脅威防御機能を備え、脅威を迅速に検出、ブロック、修復します。また、データの損失を防ぎ、送信中の重要情報をエンドツーエンドの暗号化によって保護します。Secure Web Appliance モジュールで強化できる観測可能量の詳細については、地理的位置に基づいたそれぞれの URL を使用して **Cisco XDR のログインページ** に移動してください。

- <https://xdr.us.security.cisco.com/administration/integrations> (北米)
- <https://xdr.eu.security.cisco.com/administration/integrations> (欧州)
- <https://xdr.apjc.security.cisco.com/administration/integrations> (アジア太平洋地域、日本、中国)

Cisco XDR と統合するモジュールに移動し、**【始める（Get Started）】**をクリックします。

Cisco Secure Web Appliance を XDR と統合すると、Cisco Secure Web Appliance の Web トラッキングデータが検証されます。トランザクションタイムアウト（60 秒）は、Cisco Secure Web Appliance での処理遅延が原因で発生し、統合が失敗します。正常に統合するには、統合の時間制限をデフォルトの 30 日から 1 日または 2 日に短縮します。ただし、この短縮を行うと Cisco Secure Web Appliance のモニタリングの有効性に影響します。

## アプライアンスと Cisco XDR の統合方法

表 7: アプライアンスと Cisco XDR の統合方法

|        | 操作内容                                             | 詳細                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | 前提条件を確認します。                                      | <a href="#">前提条件（436 ページ）</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ステップ 2 | Secure Web Appliance で、Cisco XDR 統合を有効にします。      | <a href="#">Cisco Secure Web Appliance での Cisco XDR の有効化（436 ページ）</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| ステップ 3 | 登録が成功したかどうかを確認します。                               | <a href="#">登録が成功したかどうかの確認（437 ページ）</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ステップ 4 | Cisco XDR で、Cisco Web セキュリティアプライアンス モジュールを追加します。 | <p>詳細については、地域に基づいて、それぞれの URL にアクセスしてください。</p> <ul style="list-style-type: none"><li>• <a href="https://xdr.us.security.cisco.com/administration/integrations">https://xdr.us.security.cisco.com/administration/integrations</a>（北米）</li><li>• <a href="https://xdr.eu.security.cisco.com/administration/integrations">https://xdr.eu.security.cisco.com/administration/integrations</a>（欧州）</li><li>• <a href="https://xdr.apjc.security.cisco.com/administration/integrations">https://xdr.apjc.security.cisco.com/administration/integrations</a>（アジア太平洋地域、日本、中国）</li></ul> <p>Cisco XDR と統合するために必要な Cisco Web セキュリティアプライアンス モジュール（Cisco Secure Web Appliance）に移動し、<b>【始める（Get Started）】</b>をクリックして、そのページに記載されている手順を参照してください。</p> |

## 前提条件



(注) すでに Cisco Threat Response のユーザーアカウントをお持ちの場合は、Cisco XDR のユーザーアカウントを作成する必要はありません。Cisco Threat Response ユーザーアカウントのログイン情報を使用して Cisco XDR にログインできます。

- Cisco XDR でユーザーアカウントを作成する際には、必ず管理者アクセス権を使用してください。新しいユーザーアカウントを作成するには、地域に基づいたそれぞれの URL を使用して、**Cisco XDR のログインページ**に移動します。

- <https://xdr.us.security.cisco.com/> (北米)
- <https://xdr.eu.security.cisco.com/> (欧州)
- <https://xdr.apjc.security.cisco.com/> (アジア太平洋地域、日本、中国)

ログインページで **[SecureX サインオンアカウントの作成 (Create a SecureX Sign-on Account)]** をクリックし、ログインプロセスに進みます。新しいユーザーアカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。

- (プロキシサーバーを使用していない場合のみ。) ファイアウォールで HTTPS (インおよびアウト) 443 ポートが次の FQDN に対してオープンになっていることを確認して、アプライアンスを XDR に登録できるようにしてください。
  - api-sse.cisco.com (NAM ユーザのみに対応)
  - api.eu.sse.itd.cisco.com (欧州連合 (EU) のユーザのみに対応)
  - api.apj.sse.itd.cisco.com (APJC ユーザのみに対応)

## Cisco Secure Web Appliance での Cisco XDR の有効化

### 手順

- ステップ 1 アプライアンスにログインします。
- ステップ 2 **[システム管理 (System Administration)]** > **[スマート ソフトウェア ライセンシング (Smart Software Licensing)]** を選択し、スマートライセンス登録プロセスを完了します。手順の詳細については、[Cisco Smart Software Manager でのアプライアンスの登録 \(140 ページ\)](#) を参照してください。
- ステップ 3 登録プロセスが正常に完了した後、ライセンスを要求する必要があります。手順の詳細については、[ライセンスの要求 \(143 ページ\)](#) を参照してください。
- ステップ 4 **[管理 (Administration)]** > **[システム セットアップ ウィザード (System Setup Wizard)]** を選択し、システムセットアッププロセスを完了します。手順の詳細については、[システム セットアップ ウィザード \(24 ページ\)](#) を参照してください。

このステップを完了すると、Cisco Secure Web Appliance の XDR ページにリダイレクトされ ([ネットワーク (Network)] > [クラウドサービス設定 (Cloud Services Settings)]、Cisco Cloud Service が自動的に有効になります。これで、デバイスが Cisco Security Services Exchange に登録されます。

**ステップ 5** [クラウドサービスの設定 (Cloud Services Settings)] ページから、次の手順を実行します。

- a) [設定の編集 (Edit Settings)] をクリックします。
- b) ドロップダウンリストから、リージョンを選択します。
- c) [XDR] チェックボックスをオンにして、[変更の送信 (submit Changes)] をクリックします。

---

### 次のタスク

アプライアンスを Cisco XDR に登録します。詳細については、地理的位置に基づいたそれぞれの URL を使用して、**Cisco XDR のログインページ**にアクセスしてください。

- <https://xdr.us.security.cisco.com/> (北米)
- <https://xdr.eu.security.cisco.com/> (欧州)
- <https://xdr.apjc.security.cisco.com/> (アジア太平洋地域、日本、中国)

Cisco XDR と統合するモジュールに移動し、**[始める (Get Started)]** をクリックして、そのページに記載されている手順を参照してください。

## 登録が成功したかどうかの確認

- Security Services Exchange で、Security Services Exchange のステータスを確認して、正常に登録されたことを確認します。
- Cisco XDR で、**[管理 (Administration)]** > **[オンプレミスアプライアンス (On-Prem Appliances)]** に移動し、Security Services Exchange に登録されている Secure Web Appliance を表示します。

登録済みのアプライアンスを表示するには、地域に基づいてそれぞれの URL に移動します。

- <https://xdr.us.security.cisco.com/administration/on-premise-appliances> (北米)
- <https://xdr.eu.security.cisco.com/administration/on-premise-appliances> (欧州)
- <https://xdr.apjc.security.cisco.com/administration/on-premise-appliances> (アジア太平洋地域、日本、中国)



(注) 別の Cisco XDR サーバー（例：欧州 - [api.eu.sse.itd.cisco.com](https://api.eu.sse.itd.cisco.com)）に切り替える場合は、**[ネットワーク (Network)] > [クラウドサービスの設定 (Cloud Services Settings)] > [設定の編集 (Edit Settings)] > [任意のサーバーに変更 (Change to any server)]** に移動して、サーバーを変更する必要があります。SSE 接続は、以前のサーバーバージョンから新しく選択されたリージョンに自動的に移行されます。

Security Services Exchange にアプライアンスが正常に登録されたら、Cisco XDR に Secure Web Appliance Web モジュールを追加します。詳細については、地域に基づいて、それぞれの URL にアクセスしてください。

- <https://xdr.us.security.cisco.com/>（北米）
- <https://xdr.eu.security.cisco.com/>（欧州）
- <https://xdr.apjc.security.cisco.com/>（アジア太平洋地域、日本、中国）

Cisco XDR と統合するモジュールに移動し、**[始める (Get Started)]** をクリックして、そのページに記載されている手順を参照してください。

## Cisco XDR プラグインを使用した脅威分析の実行

Cisco SecureXXDR は、可視性の統合、自動化の実現、インシデント対応ワークフローの迅速化、脅威ハンティングの改善を行う一連の分散型機能をサポートします。これらの分散型機能は、Cisco XDR プラグインでアプリケーションやツールの形式で利用できます。

この章で説明する内容は、次のとおりです。

- [Cisco XDR プラグインのインストール（438 ページ）](#)
- [例：NGUI を介して Cisco XDR プラグインを使用 Secure Web Appliance（439 ページ）](#)

## Cisco XDR プラグインのインストール

### 始める前に

[前提条件（436 ページ）](#) に記載されているすべての前提条件を満たしていることを確認してください。

Cisco XDR プラグインまたは拡張機能は、Google Chrome、Microsoft Edge、および Mozilla で利用できます。それぞれのブラウザの拡張機能ストアのページから、拡張機能をダウンロードできます。

### 手順

**ステップ 1** ブラウザの拡張機能ストアから Cisco XDR プラグインをダウンロードしてインストールします。

ステップ2 Cisco XDR の機能拡張ボタンをクリックします。

ステップ3 リージョンを選択し、[認証 (Authenticate)] をクリックします。

ステップ4 Cisco XDR アカウントの詳細を入力し、シングルサインオン手順を完了します。

## 例：NGUI を介して Cisco XDR プラグインを使用 Secure Web Appliance

### 手順

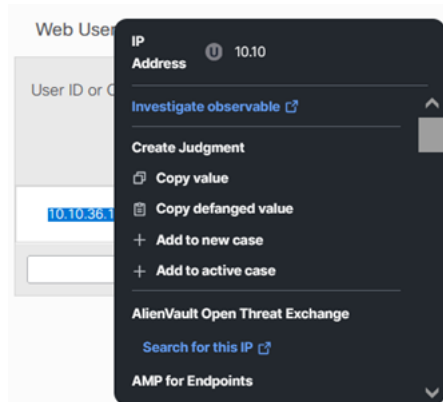
ステップ1 アプライアンスの新しい Web インターフェイスにログインします。

ステップ2 [レポート (Reports)] > [概要 (Overview)] に移動します。

ステップ3 調査の対象とするレポートカテゴリを選択します。

ステップ4 IP アドレスまたはドメインを選択し、右クリックして [Cisco XDR] を選択します。

XDR プラグインで使用可能なすべてのアプリケーションを使用して、強調表示されたデータを調査することも可能です（例：AMP for Endpoints）。



## Cisco Secure Web Appliance と Cisco Umbrella の統合

この章で説明する内容は、次のとおりです。

- [Cisco Secure Web Appliance \(SWA\) と Cisco Umbrella について](#) (440 ページ)
- [統合のためのガイドライン](#) (440 ページ)
- [エンドツーエンドの手順](#) (440 ページ)
- [Cisco Secure Web Appliance と Cisco Umbrella を統合する方法](#) (441 ページ)
- [Web ポリシーと接続先リストの設定](#) (445 ページ)



- [AD ユーザーまたは AD グループの設定 \(449 ページ\)](#)
- [Microsoft 365 の互換性の設定 \(450 ページ\)](#)
- [ポリシーの競合管理とポリシーの順序付け \(450 ページ\)](#)
- [ブロックされているページの管理 \(451 ページ\)](#)
- [Cisco Umbrella シームレス ID \(451 ページ\)](#)

## Cisco Secure Web Appliance (SWA) と Cisco Umbrella について

Umbrella は、シスコのクラウドベース Secure Internet Gateway (SIG) プラットフォームです。インターネットベースの脅威に対する防御を複数のレベルで提供します。Umbrella は、セキュア Web ゲートウェイ、ファイアウォール、DNS レイヤセキュリティ、およびクラウドアクセスセキュリティブローカ (CASB) 機能を統合して、システムを脅威から保護します。

Cisco Umbrella と Cisco Secure Web Appliance の統合により、Cisco Umbrella から Cisco Secure Web Appliance への共通 Web ポリシーの展開が容易になります。Cisco Umbrella ダッシュボードを使用してポリシーを設定したり、ログを表示したりできます。

Cisco Umbrella ダッシュボードで共通 Web ポリシーを設定すると、ポリシーは Cisco Secure Web Appliance にプッシュされます。これらの設定された Web ポリシーのレポートデータは Cisco Umbrella に送り返され、Cisco Umbrella ダッシュボードで使用できます。レポートデータには、参照された URL、その IP アドレス、URL が許可されたかブロックされたかなどの情報が含まれます。

次の URL を使用して Cisco Umbrella にアクセスできます。

<https://login.umbrella.com/umbrella>

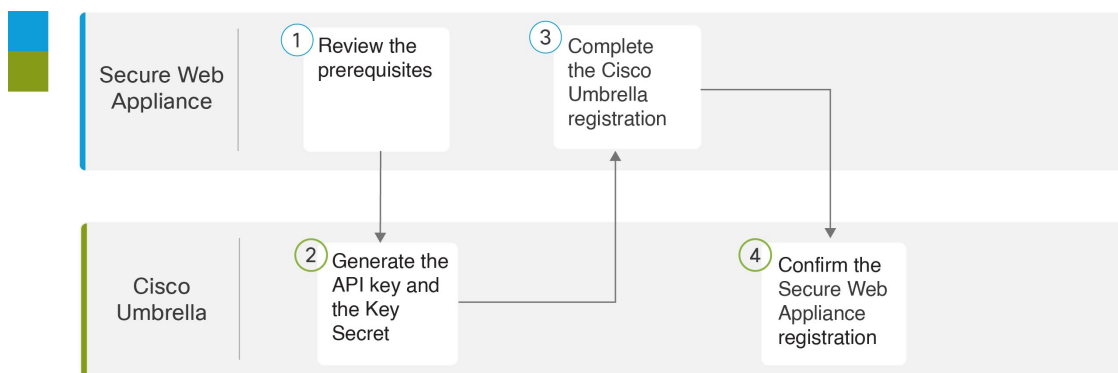
詳細については、『[Umbrella Integration with Secure Web Appliance](#)』を参照してください。

## 統合のためのガイドライン

- Cisco Umbrella でデバイスの登録を正常に完了するには、Cisco Umbrella 組織で有効な範囲の API キーとキーシークレットを取得します。
- Web ポリシーを正しく変換するには、証明書バンドルとカテゴリを Cisco Secure Web Appliance の最新のカテゴリに更新します。

## エンドツーエンドの手順

次のフローチャートは、Cisco Secure Web Appliance と Cisco Umbrella を統合するためのワークフローを示しています。



## Cisco Secure Web Appliance と Cisco Umbrella を統合する方法

表 8 : Cisco Secure Web Appliance と Cisco Umbrella を統合する方法

|        | 操作内容                                                   | 詳細                                                                    |
|--------|--------------------------------------------------------|-----------------------------------------------------------------------|
| ステップ 1 | Cisco Secure Web Appliance で、前提条件を確認します。               | <a href="#">前提条件 (441 ページ)</a>                                        |
| ステップ 2 | Cisco Umbrella で、API キーとキーシークレットを生成します。                | 「 <a href="#">Generate API Keys and Key Secret</a> 」                  |
| ステップ 3 | Cisco Secure Web Appliance で、シスコ登録を完了します。              | 「 <a href="#">Cisco Secure Web Appliance を Cisco Umbrella に登録する</a> 」 |
| ステップ 4 | Cisco Umbrella で、Cisco Secure Web Appliance の登録を確認します。 | 「 <a href="#">登録が成功したかどうかの確認</a> 」                                    |

### 前提条件

Cisco Secure Web Appliance で以下を実行します。

- Cisco Umbrella に正しく接続するには、Cert バンドル（シスコの信頼できるルート証明書バンドル：2.2）を更新します。
- Cisco Umbrella からの変換されたポリシーを正常に設定するには、コンテンツカテゴリ（107）を更新します。
- Cisco Umbrella のルールセットで HTTPS インスペクションが有効になっている場合は、Cisco Secure Web Appliance で HTTPS プロキシを手動で有効にします。
- Cisco Umbrella のルールで選択したアプリケーション設定を正常に変換するには、Cisco Secure Web Appliance で[セキュリティサービス（Security Services）] > [使用許可コントロール（Acceptable Use Controls）]に移動し、[アプリケーションの検出と制御（ADC）（Application Discovery and Control (ADC)）]を有効にします。

- AD が Cisco Umbrella に統合されている場合は、Cisco Secure Web Appliance で Active Directory (AD) レルムを設定します。正常な AD コネクタとドメインコントローラを使用することをお勧めします。
- AsyncOS バージョン 15.1 にアップグレードするには、スマートライセンスをアクティブにする必要があります。
- 内部ネットワークがパブリックネットワークに関連付けられていること、または Active Directory が Cisco Umbrella と統合されていることを確認します。

Cisco Umbrella で以下を実行します。

Cisco Umbrella の [キースコープ (Key Scopes)] を使用して、[APIキー (API Key)] と [キーシークレット (Key Secret)] を生成します。キーの生成手順については『[Cisco Umbrella SIG User Guide](#)』を参照してください。



- (注)
- [APIキー (API Key)] と [キーシークレット (Key Secret)] ([管理 (Admin)] > [APIキー (API Keys)]) を生成する際に、特定の組織について、[認証 (Auth)] (読み取り専用) として [キースコープ (Key Scope)] を選択し、[展開または登録済みアプライアンス (Deployments/Registered Appliances)] (読み取りまたは書き込み) として [登録済みアプライアンス (Registered Appliances)] を選択していることを確認します。
  - [登録済みアプライアンス (Registered Appliance)] ページは、有効なサブスクリプションでのみ表示できます。

Cisco Umbrella から Cisco Secure Web Appliance ポリシーを設定および管理できます。

## Cisco Secure Web Appliance を Cisco Umbrella に登録する

### 手順

**ステップ 1** Cisco Secure Web Appliance にログインします。

**ステップ 2** [ネットワーク (Network)] > [Umbrella設定 (Umbrella Settings)] を選択します。

**ステップ 3** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 4** [Umbrella設定 (Umbrella Settings)] で、[APIキー (API Key)]、[APIシークレット (API Secret)] を入力し、[登録 (Register)] をクリックします。

Cisco Secure Web Appliance が登録されると、成功メッセージが表示されます。

(注)

M1 インターフェイスを介してインターネットにアクセスできない場合、パブリック ドメイン (api.umbrella.com) へのアクセスはブロックされ、Umbrella への登録も失敗します。

**ステップ 5** Cisco Secure Web Appliance と Cisco Umbrella 間の接続を開始するには、ハイブリッドポリシーを有効にする必要があります。有効にするには、[ハイブリッドポリシー (Hybrid Policy)] チェックボックスをオンにします。

**ステップ 6** Cisco Umbrella で設定された Web ポリシーレポートデータを Cisco Secure Web Appliance から Cisco Umbrella レポートダッシュボードに送信するには、[ハイブリッドレポート (Hybrid Reporting)] チェックボックスをオンにします。Cisco Umbrella ダッシュボードは、外部クライアントの IP アドレスに基づいて Cisco Secure Web Appliance レポートデータをフィルタ処理します。

(注)

ハイブリッドポリシーを無効にすると、ハイブリッドレポートも無効になります。

**ステップ 7** [ソースインターフェイス (Source Interface)] ドロップダウンリストから [管理 (Management)] または [データ (Data)] を選択します。Cisco Secure Web Appliance は、[データポート (Data Port)] がインターフェイスとして設定されている場合にのみ、[データ (Data)] インターフェイスを表示します。

**ステップ 8** 変更を送信し、保存します。

---

### 次のタスク

[登録が成功したかどうかの確認 \(443 ページ\)](#)



(注)

- [ハイブリッドポリシー (Hybrid Policy)] チェックボックスを有効にすると、ポリシーが変換され、Cisco Umbrella から Cisco Secure Web Appliance にプッシュされます。ポリシーのプッシュが失敗すると、ユーザーは電子メールで通知を受けることができます。この通知は、[システム管理 (System Administration)] > [アラート (Alerts)] で [システム (System)] アラートとして設定できます。
- ハイブリッドレポートを有効にすると、Cisco Umbrella で設定されたポリシーの Cisco Secure Web Appliance レポートデータのみが Cisco Umbrella レポートに送信されます。レポートデータが Cisco Secure Web Appliance によって送信されない場合、ユーザーは電子メールで通知を受けることができます。この通知は、[システム管理 (System Administration)] > [アラート (Alerts)] で [システム (System)] アラートとして設定できます。

---

## 登録が成功したかどうかの確認

Cisco Umbrella で、[展開 (Deployments)] > [コアアイデンティティ (Core Identities)] > [登録済みのアプライアンス (Registered Appliances)] ページに移動し、Cisco Umbrella に登録されている Cisco Secure Web Appliance デバイスを表示します。



(注)

- 登録済みの Cisco Secure Web Appliance のステータスは、Cisco Secure Web Appliance の [Umbrella設定 (Umbrella Settings)] ページで [ハイブリッドポリシー (Hybrid Policy)] チェックボックスをオンにした場合にのみ、アクティブになります。それ以外の場合、Cisco Secure Web Appliance デバイスのステータスはオフラインです。
- Cisco Secure Web Appliance の [Umbrella設定 (Umbrella Settings)] ページで [ハイブリッドポリシー (Hybrid Policy)] と [ハイブリッドレポート (Hybrid Reporting)] のチェックボックスをオンにした場合、Cisco Umbrella のハイブリッドレポートのステータスは**アクティブ**になります。
- ポリシー同期のステータスが**失敗**の場合、ステータスにカーソルを合わせるとエラーメッセージが表示されます。
- ポリシー同期のステータスが警告アイコンの付いた**成功**である場合、ステータスにカーソルを合わせると次の警告メッセージが表示されます：「一部のユーザー/グループが正常な状態でないADコネクタまたはドメインコントローラのルール/ルールセットで選択されている場合は、[展開 (Deployments)] > [設定 (Configuration)] > [サイトとActive Directory (Sites and Active Directory)] に移動してエラーの詳細を確認し、修正してください。(If a few users/groups have been selected in rules/rulesets from AD Connectors or Domain Controllers which are not in a healthy state, navigate to Deployments > Configuration > Sites and Active Directory to see the error details and fix it.)」ADの詳細と選択されたユーザー/グループの情報も、警告メッセージで確認できます。

Cisco Umbrella UI の [登録済みアプライアンス (Registered Appliances)] ページにある [ポリシーのプッシュ (Policy Push)] オプションを使用すると、設定した Web ポリシーを選択した Cisco Secure Web Appliance にプッシュできます。

## Cisco Umbrella からの Cisco Secure Web Appliance の登録解除

### 手順

- ステップ 1 Cisco Secure Web Appliance にログインします。
- ステップ 2 [ネットワーク (Network)] > [Umbrella設定 (Umbrella Settings)] を選択します。
- ステップ 3 [設定の編集 (Edit Settings)] をクリックします。
- ステップ 4 [ハイブリッドポリシー (Hybrid Policy)] および [ハイブリッドレポート (Hybrid Reporting)] チェックボックスをオンにして無効にします。
- ステップ 5 変更を保存します。
- ステップ 6 [APIキー (API Key)], [APIシークレット (API Secret)] を入力し、[登録解除 (Deregister)] をクリックします。

Cisco Umbrella がプッシュしたポリシーを保持するか削除するかを尋ねられます。[はい (Yes)] を選択すると、Cisco Umbrella がプッシュしたポリシーは、変更がコミットされた後に Cisco Secure Web Appliance から削除されます。

## Cisco Umbrella レポートینگ ダッシュボードの表示

Cisco Secure Web Appliance は、Cisco Umbrella が設定したポリシー レポートینگ データを Cisco Umbrella ダッシュボードに送信します。このレポートینگデータを Cisco Umbrella で表示するには、[レポートینگ (Reporting)] > [アクティビティ検索 (Activity Search)] に移動し、[IDタイプ (Identity Type)] として [Cisco Secure Web Appliance (Secure Web Appliance)] を選択します。

## Web ポリシーと接続先リストの設定

統合が成功すると、Web ポリシーが変換され、Cisco Umbrella から Cisco Secure Web Appliance にプッシュされます。

統合してハイブリッドレポートを有効にしている場合、Cisco Secure Web Appliance は Cisco Umbrella ポリシーに基づいて生成されたレポートデータを Cisco Umbrella レポートダッシュボードに送信します。

次のプロファイルとポリシーは、Cisco Secure Web Appliance に変換されます。

- 識別プロファイルの設定 (445 ページ)
- カスタムおよび外部 URL カテゴリの設定 (446 ページ)
- アクセスポリシーの設定 (446 ページ)
- 復号ポリシーの設定 (447 ページ)
- アクセスポリシーでのアプリケーションの設定 (448 ページ)

## 識別プロファイルの設定

認証オプション (AD が Cisco Umbrella に統合されている場合) または認証を免除オプション (AD が Cisco Umbrella に統合されていない場合) を持つグローバル識別プロファイルは 1 つだけです。

Cisco Umbrella でルールセットアイデンティティを作成するには、[Webポリシー (Web Policy)] に移動し、ルールセットアイデンティティとして[ネットワーク (Networks)] または[ADユーザー (AD Users)] または[ADグループ (AD Groups)] を選択します。詳細については、<https://docs.umbrella.com/umbrella-user-guide/docs/add-a-rules-based-policy#setup>を参照してください。



(注) ネットワークアイデンティティに関連付けられた内部ネットワークがあることを確認してください。

Cisco Umbrella で内部ネットワークを作成し ([展開 (Deployments)] > [設定 (Configuration)] > [内部ネットワーク (Internal Networks)] )、パブリックネットワークに関連付けることができます。内部ネットワークは、Cisco Secure Web Appliance のアクセスポリシーおよび復号ポリシーでサブネットとして変換されます。

## カスタムおよび外部 URL カテゴリの設定

Cisco Umbrella の接続先リストは、Cisco Secure Web Appliance のカスタムおよび外部 URL カテゴリとして変換されます ([Webセキュリティマネージャ (Web Security Manager)] > [カスタムおよび外部URLカテゴリ (Custom and External URL Categories)] )。

Cisco Umbrella で接続先リストを作成し ([ポリシー (Policy)] > [ポリシーコンポーネント (Policy Components)] > [接続先リスト (Destination Lists)] )、Web ポリシーに関連付けます。詳細については、「<https://docs.umbrella.com/umbrella-user-guide/docs/add-a-destination-list>」を参照してください。

## アクセスポリシーの設定

Cisco Umbrella の Web ポリシー (規則) は、Cisco Secure Web Appliance のアクセスポリシーとして変換されます。

パブリックネットワーク (内部ネットワークが関連付けられている)、内部ネットワーク、AD ユーザー、およびルールアイデンティティとして設定された AD グループを使用して、Cisco Umbrella でルールを作成します。[コンテンツカテゴリ (Content Categories)] または [接続先リスト (Destination Lists)] を使用して接続先を設定します。

詳細については、<https://docs.umbrella.com/umbrella-user-guide/docs/add-rules-to-a-ruleset#procedure> を参照してください。

変換されたルールを Cisco Secure Web Appliance で表示できます ([Webセキュリティマネージャ (Web Security Manager)] > [アクセスポリシー] > [URLフィルタリング (URL Filtering)] )。

アクセスポリシーについて、[Umbrellaルール (Umbrella Rules)] から選択した [コンテンツカテゴリ (Content Categories)] を [URLフィルタリング (URL Filtering)] > [定義済みURLカテゴリフィルタリング (Predefined URL Category Filtering)] で表示できます。また、[接続先リスト (Destination lists)] を [URLフィルタリング (URL Filtering)] > [カスタムおよび外部URLカテゴリフィルタリング (Custom and External URL Category Filtering)] で表示できます。

ルールセットで選択したアイデンティティに基づいて、すべての接続先をモニターする追加のアクセスポリシーが作成されます。



- (注)
- 変換するアイデンティティの選択に基づいて、Cisco Umbrella ルールから Cisco Secure Web Appliance アクセスポリシーへの 1 対 1 のマッピングまたは 1 対多のマッピングが作成されます。
  - ルールセットで選択したアイデンティティに基づいて、すべての接続先をモニターする追加のアクセスポリシーが作成されます。

## 復号ポリシーの設定

Cisco Umbrella の [HTTPS インスペクション (HTTPS Inspection) ] ポリシーは、アイデンティティとともに使用できるように、Cisco Secure Web Appliance の [復号ポリシー (Decryption policies) ] として変換されます。



- (注) Cisco Secure Web Appliance で [HTTPS プロキシ (HTTPS Proxy) ] が有効になっている場合にのみ、Cisco Umbrella から復号ポリシーを設定できます。

Cisco Umbrella で HTTPS インスペクションを有効にします ([ポリシー (Policies) ] > [管理 (Management) ] > [Web ポリシー (Web Policy) ] > [ルールセット設定 (Ruleset Settings) ] > [HTTPS インスペクション設定 (HTTPS Inspection Settings) ] )。

[選択的復号リスト (Selective Decryption List) ] で [なし (None) ] を選択すると、すべての事前定義されたコンテンツカテゴリが復号されます。ドロップダウンから選択的復号リストを選択して、HTTPS インスペクションをバイパスします。

Cisco Umbrella の [選択的復号リスト (Selective Decryption List) ] からの変換されたコンテンツカテゴリは、[URL フィルタリング (URL Filtering) ] > [事前定義された URL カテゴリフィルタリング (Predefined URL Category Filtering) ] に表示され、Cisco Umbrella の [選択的復号リスト (Selective Decryption List) ] からのドメインは、復号ポリシーの [URL フィルタリング (URL Filtering) ] > [カスタムおよび外部 URL カテゴリフィルタリング (Category Filtering) ] に表示されます。

Cisco Umbrella の HTTPS インスペクション設定は、次のように Cisco Secure Web Appliance に変換されます。

- 有効にすると、[ドメイン (Domains) ] と、[選択的復号リスト (Selective Decryption List) ] の [コンテンツカテゴリ (Content Categories) ] は、Cisco Secure Web Appliance で [パススルー (Passthrough) ] に設定され、残りのカテゴリは [復号する (Decrypt) ] に設定されます。
- 無効にすると、[復号ポリシー (Decryption Policies) ] は、すべての事前定義された URL カテゴリフィルタリングが [モニター (Monitor) ] として、Cisco Secure Web Appliance に表示されます。
- [HTTPS 経由でブロックされているページを表示 (Display Block Page Over HTTPS) ] が選択されている場合、[復号ポリシー (Decryption Policies) ] は、すべての事前定義された



URL カテゴリフィルタリングが[モニター (Monitor)]として、Cisco Secure Web Appliance に表示されます。

詳細については、「[Add a Ruleset to the WebPolicy](#)」を参照してください。



- (注)
- Cisco Umbrella の [選択的復号リスト (Selective Decryption List)] の [アプリケーション (Applications)] を Cisco Secure Web Appliance の [復号ポリシー (Decryption Policies)] に変換することはサポートされていません。
  - ルールセットアイデンティティでネットワークとともに AD ユーザーまたは AD グループが選択されると、追加の復号ポリシーが作成されます。
  - Cisco Umbrella から変換された復号ポリシーのデフォルトアクションは、[復号する (Decrypt)] に設定されます。
  - Cisco Secure Web Appliance では、Cisco Umbrella から変換された [復号ポリシー (Decryption Policies)] に対して WBRs が無効になっています。

## アクセスポリシーでのアプリケーションの設定

Cisco Umbrella で CASI と呼ばれる [アプリケーション設定 (Application Settings)] は、Cisco Secure Web Appliance のアクセスポリシーで [ADCアプリケーション (ADC Applications)] として変換されます。

Cisco Umbrella ルールでアプリケーションカテゴリまたは特定のアプリケーションを選択でき、Cisco Secure Web Appliance でアクセスポリシーのアプリケーションに同じルールアクションが適用されます。ルール内で選択されていないアプリケーションはグローバル設定を継承します。

選択したアプリケーションのドメインで構成されるカスタム URL カテゴリが作成され、Cisco Secure Web Appliance にプッシュされます。これを表示するには、**[URL フィルタリング (URL Filtering)]** > **[カスタムおよび外部 URL カテゴリのフィルタリング (Custom and External URL Category Filtering)]** に移動し、アクセスポリシーの **[URL フィルタリング (URL Filtering)]** セクションで **[アクション (Action)]** を **[モニター (Monitor)]** として選択します。

詳細については、「[Manage Application Settings on Umbrella](#)」を参照してください。

これらのルールは、Cisco Secure Web Appliance に変換されると、**[Web セキュリティマネージャ (Web Security Manager)]** > **[アクセスポリシー (Access Policies)]** > **[アプリケーション (Applications)]** に移動して表示できます。

重要 選択したアプリケーションを含むアプリケーションルールを Cisco Umbrella から Cisco Secure Web Appliance に正常に変換するには、**[アプリケーションの検出および制御 (ADC) (Application Discovery and Control (ADC))]** を有効にする必要があります。

詳細については、「[AVC または ADC エンジン を有効にする](#)」を参照してください。



- (注) Cisco Umbrella のアプリケーションポリシーは、Cisco Secure Web Appliance で復号ポリシーとして変換されません。

## AD ユーザーまたは AD グループの設定

Cisco Umbrella Web ポリシーの AD ユーザーまたは AD グループは、ポリシーメンバー定義セクションの [選択されたグループおよびユーザー (Selected Groups and Users)] として Cisco Secure Web Appliance ポリシーで設定する必要があります。

Cisco Umbrella では、AD が統合されている場合 ([展開 (Deployments)] > [構成 (Configuration)] > [サイトおよびアクティブディレクトリ (Sites and Active Directory)] )、レルムを [すべてのレルム (All Realms)] として、[ケルベロス、NTLMSSPまたは基本を使用する (Use Kerberos or NTLMSSP or Basic)] をスキーマとして、[IPアドレス (IP Address)] を認証サロゲートとして作成するグローバル ID プロファイルは 1 つだけです。[セキュリティサービス (Security Services)] > [プロキシ設定 (Proxy Settings)] > [Webプロキシ設定 (Web Proxy Settings)] > [基本設定 (Basic Settings)] > [プロキシモード (Proxy Mode)] で、[Webプロキシモード (Web Proxy Mode)] が [透過的 (Transparent)] である場合、Cisco Secure Web Appliance で [同じサロゲート設定を明示的な転送要求に適用する (Apply same surrogate settings to explicit forward requests)] チェックボックスが有効になります。



- (注) Cisco Umbrella に統合されているアクティブディレクトリは、Cisco Secure Web Appliance で手動で設定し、到達可能である必要があります。

Cisco Umbrella ([ポリシー (Policies)] > [管理 (Management)] > [Webポリシー (Web Policy)] > [ルールセットアイデンティティ (Ruleset Identities)] ) で、Cisco Umbrella の統合 AD から [ADユーザー (AD Users)] または [ADグループ (AD Group)] を選択します。ルールセットアイデンティティで選択した [ADユーザー (AD Users)] または [ADグループ (AD Groups)] は、Cisco Secure Web Appliance の復号ポリシーのメンバーシップセクション ([Webセキュリティマネージャ (Web Security Manager)] > [復号ポリシー (Decryption Policies)] > [ポリシーメンバー定義 (Policy Member Definition)] ) にマップする必要があります。

Cisco Umbrella ([ポリシー (Policies)] > [管理 (Management)] > [Webポリシー (Web Policy)] > [ルールセット (Ruleset)] > [ルール (Rules)] ) で、[ADユーザー (AD Users)] として選択されたアイデンティティまたは選択されたルールアクションおよび接続先で [ADグループ (AD Groups)] でルールを作成します。ルールで選択された [ADユーザー (AD Users)] または [ADグループ (AD Groups)] は、Cisco Secure Web Appliance のアクセスポリシーのメンバーシップセクション ([Webセキュリティマネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] > [ポリシーメンバー定義 (Policy Member Definition)] ) にマップされます。

ルールセットアイデンティティの選択された [ADユーザー (AD Users)] または [ADグループ (AD Groups)] を使用して追加のポリシーが作成され、すべての事前定義されたコンテンツカテゴリが許可されます。

## Microsoft 365 の互換性の設定

[Microsoft 365互換性 (Microsoft 365 Compatibility)] 設定を Cisco Umbrella から Cisco Secure Web Appliance の [カスタムおよび外部URLカテゴリ (Custom and External URL Categories)] に変換できます。

Cisco Umbrella では、[Microsoft 365互換性 (Microsoft 365 Compatibility)] が有効になっている場合 ([ポリシー (Policies)] > [管理 (Management)] > [Webポリシー (Web Policy)] > [グローバル設定 (Global Settings)] )、Cisco Secure Web Appliance の [カスタムおよび外部URLカテゴリ (Custom and External URL Categories)] は、[カテゴリタイプ (Category Type)] が [外部ライブフィードカテゴリ (External Live Feed Category)] として、[フィードファイルの場所 (Feed File Location)] が [Office 365 Webサービス (Office 365 Web Service)] として作成されます。このカテゴリは、Cisco Secure Web Appliance の [URLフィルタリング (URL Filtering)] セクションで、[アクション (Action)] を [パススルー (Passthrough)] として Cisco Umbrella から設定された復号ポリシーに対して選択されます。



(注) 復号ポリシーは、Cisco Secure Web Appliance で [HTTPSプロキシ (HTTPS Proxy)] が有効になっている場合にのみ設定されます。

## ポリシーの競合管理とポリシーの順序付け

Cisco Umbrella の管理対象プロファイル、または識別プロファイル、アクセスポリシー、復号ポリシー、および Cisco Umbrella から Cisco Secure Web Appliance に設定されたカスタムおよび外部 URL カテゴリなどのポリシーを編集または削除することはできません。名前の先頭に「umbrella<space>」が付いたプロファイルまたはポリシーを作成することはできません (例: umbrella abc)。



- (注)
- Cisco Secure Web Appliance で設定された Cisco Umbrella ポリシーをクローンすることはできません。
  - Cisco Secure Web Appliance では、Cisco Umbrella から変換されたポリシーの順序を変更できません。
  - Cisco Secure Web Appliance の [ネットワーク (Network)] > [Umbrella設定 (Umbrella Settings)] でハイブリッドポリシー オプションを無効化した後、Cisco Umbrella からプッシュされたポリシーを編集または削除できます。
  - REST API を使用して、Cisco Umbrella からプッシュされたポリシーを編集および削除できます。

Cisco Umbrella のポリシー規則のシーケンスは、Cisco Secure Web Appliance へのポリシー変換中に保持されます。したがって、Cisco Secure Web Appliance 管理者が設定したポリシーまたはプロファイルは、Cisco Umbrella から変換されたポリシーよりも優先されます。

## ブロックされているページの管理

最初のルールセットに関連付けられている Cisco Umbrella の [ブロックされているページ (Block Page) ] 設定 ([ポリシー (Policies) ] > [管理 (Management) ] > [ポリシーコンポーネント (Policy Components) ] > [ブロックされているページの外観 (Block Page Appearance) ]) を、Cisco Secure Web Appliance の [エンドユーザー通知 (End-User Notification) ] ページ ([セキュリティサービス (Security Services) ] > [エンドユーザー通知 (End-User Notification) ]) に変換できます。

Cisco Umbrella で、Cisco Umbrella の [ブロックされているページ (Block Page) ] 設定を変換するには、ブロックされているページを設定し、最初のルールセットでブロックされているページを選択します ([ポリシー (Policies) ] > [Webポリシー]) 。



- (注) 最初のルールセットの選択された [ブロックされているページ (Block Page) ] の変更は、3 時間ごとに Cisco Secure Web Appliance にプッシュされます。

詳細については、「<https://docs.umbrella.com/umbrella-user-guide/docs/create-a-custom-block-page>」を参照してください。

## Cisco Umbrella シームレス ID

Cisco Umbrella シームレス ID 機能を使用すると、正常に認証された後に、アプライアンスからユーザ識別情報を Cisco Umbrella セキュア Web ゲートウェイ (SWG) にパスすることができます。Cisco Umbrella SWG は、Secure Web Appliance から受信した認証済み識別情報に基づいて、Active Directory のユーザー情報をチェックします。Cisco Umbrella SWG は、ユーザを認証済みと見なし、定義されたセキュリティポリシーに基づいてユーザにアクセスを提供します。

Secure Web Appliance は、X-USWG-PKH、X-USWG-SK、および X-USWG-Data を含む HTTP ヘッダーを使用して Cisco Umbrella SWG にユーザー識別情報を渡します。



- (注)
- Cisco Umbrella シームレス ID ヘッダーは、Secure Web Appliance 上の同じ名前のヘッダーを上書きします。
  - Cisco Umbrella シームレス ID 機能は、Active Directory でのみ認証方式をサポートします。この機能は、LDAP、Cisco Identity Services Engine (ISE)、および Cisco Context Directory Agent (CDA) をサポートしていません。
  - Cisco Umbrella SWG は FTP および SOCKS トラフィックをサポートしていません。

表 9: HTTPS トラフィックの動作

| 構成モード    | サロゲート                  | 認証のための復号 | Secure Web Appliance 認証 | Cisco Umbrella シームレス ID の共有 |
|----------|------------------------|----------|-------------------------|-----------------------------|
| Explicit | IP サロゲート               | はい/いいえ   | 対応                      | 対応                          |
| 透過       | IP サロゲート               | 対応       | 対応                      | 対応                          |
| 透過       | IP サロゲート               | 非対応      | 認証をスキップ                 | 非対応                         |
| Explicit | Cookie、クレデンシャルの暗号化なし   | はい/いいえ   | 対応                      | 対応                          |
| Explicit | Cookie、クレデンシャルの暗号化あり   | はい/いいえ   | 対応                      | 非対応                         |
| 透過       | Cookie、クレデンシャル暗号化あり/なし | はい/いいえ   | 認証をスキップ                 | 非対応                         |



(注) Secure Web Applianceは、認証されたユーザーの UPN 値を Active Directory から取得し、Cisco Umbrella シームレス ID でユーザーに正しい Web ポリシーを適用できるようにします。この機能を利用するには、すべての Active Directory ユーザーにデフォルトまたはカスタマイズされた UPN 値を割り当てる必要があります。

ここでは、次の内容について説明します。

- [Cisco Umbrella シームレス ID の設定](#)
- [Cisco Umbrella SWG のルーティング先の設定](#)

## Cisco Umbrella シームレス ID の設定

始める前に

- [ネットワーク (Network)] > [証明書の管理 (Certificate Management)] > [信頼できるルート証明書の管理 (Manage Trusted Root Certificates)]を選択して、ルートまたはカスタムの Umbrella 証明書をアプライアンスに手動でアップロードします。「[証明書の管理](#)」を参照してください。
- 認証用の識別プロファイルが設定されていることを確認します。
- 設定済みの識別プロファイルを使用してルーティングポリシーを定義します。

## 手順

- 
- ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] > [Cisco Umbrella シームレス ID (Cisco Umbrella Seamless ID)] を選択します。
- ステップ 2** [設定の編集 (Edit Settings)] をクリックします。
- ステップ 3** Cisco Umbrella SWG ホスト名または IP アドレスを入力します。
- ステップ 4** HTTP および HTTPS トラフィック用の SWG のポート番号を入力します。
- 最大 6 つのポート番号を入力できます。
- ステップ 5** (オプション) [接続テスト (Connectivity Test)] をクリックして、ポートを介した Cisco Umbrella SWG の接続と証明書の検証が正常に行われていることを確認します。
- ステップ 6** Cisco Umbrella SWG の一意のカスタマー組織 ID を入力します。
- ステップ 7** 送信して確定します。
- 

## Cisco Umbrella SWG のルーティング先の設定

新しいルーティングポリシーを作成するには、「[ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加](#)」を参照してください。

。

## 手順

- 
- ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] > [ルーティングポリシー (Routing Policies)] を選択します。
- ステップ 2** [ルーティングポリシー (Routing Policies)] ページで、必要なポートを含む Cisco Umbrella シームレス ID を設定するルーティングポリシーの [ルーティング先 (Routing Destination)] 列の下にあるリンクをクリックします。
- ステップ 3** ポリシーのアップストリームプロキシグループとして、ポートを含む適切な Cisco Umbrella シームレス ID を選択します。[アップストリームプロキシグループ (Upstream Proxy Group)] ドロップダウンリストには、[Cisco Umbrella シームレス ID (Cisco Umbrella Seamless ID)] ページ ([Webセキュリティマネージャ (Web Security Manager)] > [Cisco Umbrella シームレス ID (Cisco Umbrella Seamless ID)]) で設定したすべての Cisco Umbrella シームレス ID とポートが表示されます。
- (注)  
ルーティングポリシーにすでにリンクされているポート番号を持つ Cisco Umbrella シームレス ID を削除すると ([Webセキュリティマネージャ (Web Security Manager)] > [Cisco Umbrella シームレス ID (Cisco Umbrella Seamless ID)])、ルーティング先が [直接接続 (Direct Connection)] に変わります。
- ステップ 4** 変更を送信し、保存します。
-





## 第 7 章

# ネットワーク セキュリティ

---

この章で説明する内容は、次のとおりです。

- [セキュリティ サービスの設定 \(455 ページ\)](#)
- [ファイル レピュテーション フィルタリングとファイル分析 \(477 ページ\)](#)
- [Web アプリケーションへのアクセスの管理 \(506 ページ\)](#)
- [機密データの漏洩防止 \(518 ページ\)](#)
- [エンドユーザーへのプロキシアクションの通知 \(533 ページ\)](#)
- [非標準ポートでの不正トラフィックの検出 \(572 ページ\)](#)

## セキュリティ サービスの設定

この章で説明する内容は、次のとおりです。

- [セキュリティ サービスの設定の概要 \(456 ページ\)](#)
- [Web レピュテーション フィルタの概要 \(456 ページ\)](#)
- [マルウェア対策スキャンの概要 \(459 ページ\)](#)
- [適応型スキャンについて \(462 ページ\)](#)
- [マルウェア対策とレピュテーション フィルタの有効化 \(463 ページ\)](#)
- [ポリシーにおけるマルウェア対策およびレピュテーションの設定 \(465 ページ\)](#)
- [AMP for Endpoints コンソールとアプライアンスの統合 \(471 ページ\)](#)
- [データベース テーブルの保持 \(474 ページ\)](#)
- [Web レピュテーション フィルタリング アクティビティおよび DVS スキャンのロギング \(474 ページ\)](#)
- [キャッシング \(475 ページ\)](#)
- [マルウェアのカテゴリについて \(475 ページ\)](#)



## セキュリティ サービスの設定の概要

Secure Web Applianceは、セキュリティ コンポーネントを使用してさまざまなマルウェアの脅威からエンドユーザを保護します。グループ ポリシーごとにマルウェア対策と Web レピュテーション設定値を設定できます。アクセス ポリシーを設定すると、AsyncOS for Web はブロックするコンテンツを判定するときに、マルウェア対策スキャンと Web レピュテーションスコアの組み合わせを使用することを選択できるようになります。

マルウェアからエンドユーザーを保護するには、アプライアンスでこれらの機能をイネーブルにしてから、ポリシーごとにマルウェア対策と Web レピュテーションの設定値を設定します。

| オプション                                      | 説明                                                          | リンク                                                        |
|--------------------------------------------|-------------------------------------------------------------|------------------------------------------------------------|
| マルウェア対策スキャン (Anti-malware scanning)        | アプライアンスに統合された複数のマルウェア対策スキャンエンジンを使用して、マルウェアの脅威をブロックします。      | <a href="#">マルウェア対策スキャンの概要, on page 459</a>                |
| Web レピュテーション フィルタ (Web Reputation Filters) | Web サーバーの動作を分析し、URL に URL ベースのマルウェアが含まれているかどうかを判定します。       | <a href="#">Web レピュテーションフィルタの概要, on page 456</a>           |
| Advanced Malware Protection                | ファイルレピュテーションを評価し、ファイルの特性を分析することによって、ダウンロードファイルに潜む脅威から保護します。 | <a href="#">ファイルレピュテーションフィルタリングとファイル分析の概要, on page 477</a> |

### 関連項目

- [マルウェア対策とレピュテーション フィルタの有効化, on page 463](#)
- [適応型スキャンについて, on page 462](#)

## Web レピュテーション フィルタの概要

Web レピュテーション フィルタは、Web ベースのレピュテーション スコア (WBRs) を URL に割り当て、URL ベースのマルウェアが含まれている可能性を判断します。Secure Web Appliance は、Web レピュテーション スコアを使用して、未然にマルウェア攻撃を特定して防ぎます。Web レピュテーション フィルタは、アクセス、復号、および Cisco データ セキュリティの各ポリシーで使用できます。

### Web レピュテーション スコア

Web レピュテーション フィルタでは、データを使用してインターネット ドメインの信頼性が評価され、URL のレピュテーションにスコアが付けられます。Web レピュテーションの計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定さ

れます。マルウェアが存在する可能性の累計が、-10 ～ +10 の Web レピュテーション スコアにマッピングされます（+10 がマルウェアを含む可能性が最も低い）。

パラメータには、たとえば以下のものがあります。

- URL 分類データ
- ダウンロード可能なコードの存在
- 長く不明瞭なエンドユーザ ライセンス契約書（EULA）の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク オーナー情報
- URL の履歴
- URL の経過時間
- ブロック リストに存在
- 許可リストに存在
- 人気のあるドメインの URL タイプミス
- ドメインのレジストラ情報
- IP アドレス情報


**Note**

シスコは、ユーザー名、パスワード、クライアント IP アドレスなどの識別情報を収集しません。

## Web レピュテーション フィルタの動作のしくみについて

Web レピュテーション スコアは URL 要求に対して実行されるアクションに関連付けられます。各ポリシー グループを設定して、特定の Web レピュテーション スコアにアクションを関連付けることができます。使用可能なアクションは、URL 要求に割り当てられているポリシー グループのタイプによって異なります。

| ポリシー タイプ                                          | 操作                        |
|---------------------------------------------------|---------------------------|
| アクセス ポリシー（Access Policies）                        | ブロック、スキャン、または許可から選択できます。  |
| 復号ポリシー（Decryption Policies）                       | ドロップ、復号、またはパススルーから選択できます。 |
| シスコ データ セキュリティ ポリシー（Cisco Data Security Policies） | ブロックまたはモニターから選択できます。      |

### アクセス ポリシーの Web レピュテーション

アクセス ポリシーに Web レピュテーションを設定する場合は、手動で設定するか、AsyncOS for Web で適応型スキャンを使用して最適なオプションを選択することができます。適応型スキャンがイネーブルの場合は、各アクセス ポリシーで Web レピュテーション フィルタリング

をイネーブルまたはディセーブルにできますが、Web レピュテーション スコアは編集できません。

| スコア        | アクション           | 説明                                                                                | 例                                                                                                                                                                              |
|------------|-----------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -10 ～ -6.0 | ブロック<br>(Block) | 不正なサイト。要求はブロックされ、以降のマルウェア スキャンは実行されません。                                           | <ul style="list-style-type: none"> <li>• URL がユーザーの許可なしに情報をダウンロード。</li> <li>• URL ボリュームが急上昇。</li> <li>• URL が人気のあるドメインの誤入力。</li> </ul>                                         |
| -5.9 ～ 5.9 | スキャン<br>(Scan)  | 判別不能なサイト。さらにマルウェア スキャンを行うために、DVS エンジンに要求が渡されます。DVS エンジンは、要求とサーバー応答のコンテンツをスキャンします。 | <ul style="list-style-type: none"> <li>• 動的 IP アドレスを持ち、ダウンロード可能なコンテンツを含む最近作成された URL。</li> <li>• Web レピュテーション スコアがプラスのネットワーク オーナーの IP アドレス。</li> </ul>                          |
| 6.0 ～ 10.0 | 許可<br>(Allow)   | 正常なサイト。要求は許可されます。マルウェア スキャンは必要ありません。                                              | <ul style="list-style-type: none"> <li>• URL にダウンロード可能なコンテンツが含まれていない。</li> <li>• 歴史が長く信頼できる大規模ドメイン。</li> <li>• 複数の許可リストに記載されているドメイン。</li> <li>• 評価が低い URL へのリンクがない。</li> </ul> |

デフォルトでは、+7 の Web レピュテーション スコアが割り当てられている HTTP 要求の URL は許可され、さらなるスキャンは必要ありません。しかし、+3 などの低いスコアの HTTP 要求は、マルウェアをスキャンする Cisco DVS エンジンに自動的に転送されます。レピュテーションが非常に低い HTTP 要求の URL はブロックされます。

#### 関連項目

- [適応型スキャンについて, on page 462](#)

#### 復号ポリシーの Web レピュテーション

| スコア        | アクション           | 説明                                                       |
|------------|-----------------|----------------------------------------------------------|
| -10 ～ -9.0 | ドロップ<br>(Drop)  | 不正なサイト。要求は、エンドユーザーへの通知なしでドロップされます。この設定の使用には注意が必要です。      |
| -8.9 ～ 5.9 | 復号<br>(Decrypt) | 判別不能なサイト。要求は許可されますが、接続が復号され、アクセスポリシーが復号されたトラフィックに適用されます。 |

| スコア        | アクション                   | 説明                        |
|------------|-------------------------|---------------------------|
| 6.0 ～ 10.0 | パススルー<br>(Pass through) | 正常なサイト。要求は、検査や復号なしで渡されます。 |

### Cisco データ セキュリティ ポリシーの Web レピュテーション

| スコア        | アクション             | 説明                                                                                                            |
|------------|-------------------|---------------------------------------------------------------------------------------------------------------|
| -10 ～ -6.0 | ブロック<br>(Block)   | 不正なサイト。トランザクションはブロックされ、以降のスキューン実行されません。                                                                       |
| -5.9 ～ 0.0 | モニター<br>(Monitor) | トランザクションは Web レピュテーションに基づいてブロックされず、引き続きコンテンツ（ファイルタイプとサイズ）の検査が行われます。<br><br><b>Note</b><br>スコアがないサイトはモニターされます。 |

## マルウェア対策スキューンの概要

Secure Web Applianceのマルウェア対策機能は、Cisco DVS™ エンジンとマルウェア対策スキューンエンジンを用いて、Web ベースのマルウェアの脅威を阻止します。DVS エンジン、Webroot™、McAfee、Sophos マルウェア対策スキューン エンジンと連携します。

スキューン エンジンはトランザクションを検査して、DVS エンジンに渡すマルウェア スキューンの判定を行います。DVS エンジンは、マルウェア スキューンの判定に基づいて、要求をモニターするかブロックするかを決定します。アプライアンスのアンチマルウェア コンポーネントを使用するには、マルウェア対策スキューンをイネーブルにして、グローバル設定値を設定してから、各種のポリシーに特定の設定を適用する必要があります。

#### 関連項目

- マルウェア対策とレピュテーション フィルタの有効化, on page 463
- 適応型スキューンについて, on page 462
- McAfee スキューン, on page 461

## DVS エンジンの動作のしくみについて

DVS エンジンは、Web レピュテーション フィルタから転送された URL のトランザクションに対してマルウェア対策スキューンを実行します。Web レピュテーション フィルタは、特定の URL にマルウェアが含まれている可能性を計算し、URL スコアを割り当てます。このスコアは、トランザクションをブロック、スキューンまたは許可するアクションに関連付けられています。

割り当てられた Web レピュテーション スコアがトランザクションをスキューンすることを示している場合、DVS エンジンは URL 要求とサーバー応答のコンテンツを受信します。DVS エン

ジンはスキャン エンジン（Webroot および（または）Sophos、または McAfee）と連携して、マルウェア スキャンの判定を返します。DVS エンジンは、マルウェア スキャンの判定およびアクセスポリシーの設定情報を使用して、クライアントへのコンテンツをブロックするか配信するかを判定します。

## 複数のマルウェア判定の使用

DVS エンジンは、1 つの URL に対して複数のマルウェア判定を下すことがあります。イネーブルなスキャン エンジンの一方または両方から複数の判定が返される場合もあります。

- **異なるスキャン エンジンによるさまざまな判定。** Sophos または McAfee のどちらか一方と Webroot を同時にイネーブルにすると、それぞれのスキャン エンジンが同じオブジェクトに対して異なるマルウェア判定を返すことがあります。イネーブルな両方のスキャン エンジンから 1 つの URL に対して複数の判定が返された場合、アプライアンスは最も制限が厳しいアクションを実行します。たとえば、一方のスキャン エンジンがブロックの判定を返し、他方のスキャン エンジンがモニターの判定を返した場合、DVS エンジンは常に要求をブロックします。
- **同じスキャン エンジンからの異なる判定。** オブジェクトに複数の感染が含まれている場合、1 つのスキャン エンジンが 1 つのオブジェクトに対して複数の判定を返すことがあります。同じスキャン エンジンが 1 つの URL に対して複数の判定を返した場合、アプライアンスは最も優先順位の高い判定に従ってアクションを実行します。以下のリストは、可能性があるマルウェア スキャンの判定を優先順位が高いものから順に示しています。
  - ウィルス
  - トロイのダウンロード
  - トロイの木馬
  - トロイのフィッシャ
  - ハイジャッカー
  - システム モニター
  - 商用システム モニター
  - ダイアラ
  - ワーム
  - ブラウザ ヘルパー オブジェクト
  - フィッシング URL
  - アドウェア
  - 暗号化ファイル
  - スキャン不可
  - その他のマルウェア

## Webroot スキャン

Webroot スキャンエンジンはオブジェクトを検査してマルウェア スキャンの判定を行い、判定を DVS エンジンに送信します。Webroot スキャン エンジンは、以下のオブジェクトを検査します。

- **URL 要求。**Webroot は URL 要求を評価して、URL にマルウェアの疑いがあるかどうかを判別します。この URL からの応答にマルウェアが含まれている可能性があるとして Webroot が判断した場合、アプライアンスは、アプライアンス独自の設定に応じて、要求をモニターまたはブロックします。Webroot によって要求が正常である評価された場合、アプライアンスは URL を取得し、サーバーの応答をスキャンします。
- **サーバー応答。**アプライアンスが URL を取得すると、Webroot はサーバー応答のコンテンツをスキャンし、Webroot シグニチャ データベースと照合します。

## McAfee スキャン

McAfee スキャン エンジン は、HTTP 応答内の Web サーバからダウンロードされたオブジェクトを検査します。オブジェクトの検査後、マルウェア スキャンの判定を DVS エンジンに渡し、DVS エンジンが要求をモニターするかブロックするかを決定できるようにします。

McAfee スキャン エンジン は以下の方法を使用して、マルウェア スキャンの判定を行います。

- ウィルス シグニチャ パターンの照合
- ヒューリスティック分析

### ウィルス シグニチャ パターンの照合

McAfee は、そのデータベース内のウィルス定義をスキャン エンジンに使用し、特定のウィルスや各種のウィルスなどの潜在的に望ましくないソフトウェアを検出します。ファイル内のウィルス シグニチャを検索します。McAfee をイネーブルにした場合、McAfee スキャン エンジンはこの方法を使用して、サーバー応答のコンテンツをスキャンします。

### ヒューリスティック分析

ヒューリスティック分析は、特定のルールではなく、一般的なルールを使用して新しいウィルスとマルウェアを検出する手法です。ヒューリスティック分析を使用する場合、McAfee スキャン エンジン は、オブジェクトのコードを確認して一般的なルールを適用し、オブジェクトがどの程度ウィルスに類似しているかを判断します。

ヒューリスティック分析を使用すると、偽陽性（ウィルスと指摘された正常なコンテンツ）の報告が増加し、アプライアンスのパフォーマンスが影響を受ける可能性があります。McAfee をイネーブルにするときに、オブジェクトのスキャンでヒューリスティック分析をイネーブルにするかどうかを選択できます。

### McAfee カテゴリ

| McAfee の判定 | マルウェア スキャン判定カテゴリ |
|------------|------------------|
| 既知のウィルス    | ウィルス             |
| トロイの木馬     | トロイの木馬           |
| ジョーク ファイル  | アドウェア            |
| テスト ファイル   | ウィルス             |

| McAfee の判定        | マルウェアスキャン判定カテゴリ |
|-------------------|-----------------|
| ワナビ               | ウィルス            |
| 不活化               | ウィルス            |
| 商用アプリケーション        | 商用システム モニター     |
| 望ましくないオブジェクト      | アドウェア           |
| 望ましくないソフトウェアパッケージ | アドウェア           |
| 暗号化ファイル           | 暗号化ファイル         |

## Sophos スキャン

Sophos スキャン エンジンとは、HTTP 応答内の Web サーバーからダウンロードされたオブジェクトを検査します。オブジェクトの検査後、マルウェア スキャンの判定を DVS エンジンに渡し、DVS エンジンが要求をモニターするかブロックするかを決定できるようにします。McAfee アンチマルウェア ソフトウェアがインストールされているときに、McAfee スキャン エンジンではなく、Sophos スキャン エンジンをイネーブルにする必要がある場合があります。

## 適応型スキャンについて

アダプティブスキャン機能は、どのマルウェア対策スキャンエンジン（ダウンロードファイルの Advanced Malware Protection スキャンを含む）によって Web 要求を処理するかを決定します。

適応型スキャン機能は、スキャンエンジンを実行する前に、マルウェアとして特定するトランザクションに「アウトブレイク ヒューリスティック（Outbreak Heuristics）」マルウェア対策カテゴリを適用します。アプライアンスでマルウェア対策設定を行うときに、これらのトランザクションをブロックするかどうかを選択できます。

## 適応型スキャンとアクセス ポリシー

適応型スキャンをイネーブルにした場合は、アクセス ポリシーに設定できる Web レピュテーションとマルウェア対策の設定項目の一部がやや異なります。

- 各アクセス ポリシーでは Web レピュテーション フィルタリングをイネーブルまたはディセーブルにできますが、Web レピュテーション スコアは編集できません。
- 各アクセス ポリシーではマルウェア対策スキャンをイネーブルにできますが、どのマルウェア対策スキャンエンジンをイネーブルにするかは選択できません。適応型スキャンによって、各 Web 要求に最適なエンジンが選択されます。



**Note** 適応型スキャンがイネーブルになっておらず、アクセス ポリシーに **Web** レピュテーションとマルウェア対策の特定の設定項目が設定されている場合に、適応型スキャンをイネーブルにすると、既存の Web レピュテーションとマルウェア対策の設定が上書きされます。

ポリシーごとの Advanced Malware Protection の設定は、適応型スキャンがイネーブルかどうかに関わらず同じです。

## マルウェア対策とレピュテーション フィルタの有効化

### Before you begin

Web レピュテーションフィルタ、DVS エンジン、およびスキャンエンジン (Webroot、McAfee、Sophos) がイネーブルになっていることを確認します。デフォルトでは、システムのセットアップ時にこれらがイネーブルになります。

### Procedure

- ステップ 1** [セキュリティサービス (Security Services) ] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] を選択します。
- ステップ 2** [グローバル設定を編集 (Edit Global Settings) ] をクリックします。
- ステップ 3** 必要に応じて、以下の項目を設定します。

| 設定                                                                                      | 説明                                                                                     |
|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Web レピュテーション<br>フィルタリング (Web<br>Reputation Filtering)                                   | Web レピュテーション フィルタリングをイネーブルにするかどうかを選択します。                                               |
| 適応型スキャン<br>(Adaptive Scanning)                                                          | 適応型スキャンをイネーブルにするかどうかを選択します。Web レピュテーション<br>フィルタリングがイネーブルの場合にのみ、適応型スキャンをイネーブルに<br>できます。 |
| ファイル レピュテー<br>ションフィルタリング<br>とファイル分析 (File<br>Reputation Filtering and<br>File Analysis) | 『 <a href="#">ファイルレピュテーションと分析サービスの有効化と設定, on page 488</a> 』を参<br>照してください。              |



| 設定                                                                                                           | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AMP for Endpoints コンソールの統合 ([詳細設定 (Advanced)] > [ファイルレピュテーションの詳細設定 (Advanced Settings for File Reputation)]) | お使いのアプライアンスを AMP for Endpoints コンソールと統合するには、[AMP for Endpoints コンソールでのアプライアンスの登録 (Register the Appliance with Secure Endpoint AMP for Endpoints console)] をクリックします。詳細な手順については、 <a href="#">AMP for Endpoints コンソールとアプライアンスの統合, on page 471</a> を参照してください。                                                                                                                                                                                                        |
| DVS エンジン オブジェクト スキャンの制限 (DVS Engine Object Scanning Limits)                                                  | <p>スキャン対象オブジェクト サイズの最大値を指定します。</p> <p>指定した [最大オブジェクトサイズ (Maximum Object Size)] の値は、すべてのマルウェア対策とウイルス対策スキャン エンジンおよび Advanced Malware Protection 機能によってスキャンされる、要求と応答のサイズ全体に適用されます。これは、アーカイブ検査で検査可能なアーカイブの最大サイズも指定します。アーカイブ検査について詳しくは、<a href="#">アクセス ポリシー：オブジェクトのブロッキング, on page 380</a>を参照してください。</p> <p>アップロードまたはダウンロードのサイズがこのサイズを超えると、セキュリティ コンポーネントは、進行中のスキャンを中断し、Web プロキシにスキャンの判定を提供しない可能性があります。検査可能なアーカイブがこのサイズを上回ると、[スキャンされていません (Not Scanned)] と示されます。</p> |
| Sophos                                                                                                       | Sophos スキャン エンジンをイネーブルにするかどうかを選択します。                                                                                                                                                                                                                                                                                                                                                                                                                             |
| McAfee                                                                                                       | <p>McAfee スキャン エンジンをイネーブルにするかどうかを選択します。</p> <p>McAfee をイネーブルにするときに、ヒューリスティック スキャンをイネーブルにするかどうかを選択できます。</p> <p><b>Note</b><br/>ヒューリスティック分析はセキュリティ保護を向上させますが、偽陽性が生じてパフォーマンスが低下する可能性があります。</p>                                                                                                                                                                                                                                                                      |
| Webroot                                                                                                      | <p>Webroot スキャン エンジンをイネーブルにするかどうかを選択します。</p> <p>Webroot スキャン エンジンをイネーブルにするときに、脅威リスクしきい値 (TRT) を設定できます。TRT はマルウェアが存在する確率に対して数値を割り当てます。</p> <p>独自のアルゴリズムによって URL 照合シーケンスの結果を評価し、脅威リスクレーティング (TRR) を割り当てます。この値は、TRT 設定に関連付けられます。TRR 値が TRT 以上の場合、URL はマルウェアと見なされ、さらなる処理に渡されます。</p> <p><b>Note</b><br/>脅威リスクしきい値に 90 よりも低い値を設定すると、URL ブロッキング レートが劇的に増加し、正当な要求が拒否されてしまいます。TRT のデフォルト値 90 を維持することを強く推奨します。TRT 設定の最小値は 51 です。</p>                                       |

ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

#### What to do next

- [適応型スキャンについて, on page 462](#)
- [McAfee スキャン, on page 461](#)

## Advanced Malware Protection サービスのキャッシュのクリア

AMP キャッシュ消去機能は、クリーンなファイル、悪意のあるファイル、不明なファイルについて、ファイルレピュテーションの判定結果を消去します。



（注） AMP キャッシュはパフォーマンス向上のために使用されます。**Clear Cache** コマンドを使用すると、キャッシュの再投入中に一時的にパフォーマンスが低下する可能性があります。

#### 手順

ステップ 1 [セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。

ステップ 2 [セキュアエンドポイントサービス（Advanced Malware Protection Services）] セクションで、[キャッシュ消去（Clear Cache）] をクリックし、動作を確認します。

## ポリシーにおけるマルウェア対策およびレピュテーションの設定

[マルウェア対策およびレピュテーションフィルタ（Anti-Malware and Reputation Filters）] がアプライアンスでイネーブルの場合は、ポリシー グループでさまざまな設定値を設定できます。マルウェア スキャンの判定に基づいて、マルウェア カテゴリのモニターまたはブロックをイネーブルにできます。

以下のポリシー グループにマルウェア対策を設定できます。

| ポリシー タイプ                                              | タスクへのリンク                                                        |
|-------------------------------------------------------|-----------------------------------------------------------------|
| アクセス ポリシー（Access Policies）                            | <a href="#">アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定, on page 466</a> |
| 発信マルウェア スキャン ポリシー（Outbound Malware Scanning Policies） | 発信マルウェア スキャンポリシーによるアップロード要求の制御                                  |

以下のポリシー グループに Web レピュテーションを設定できます。

| ポリシー タイプ                                           | タスクへのリンク                                                        |
|----------------------------------------------------|-----------------------------------------------------------------|
| アクセス ポリシー (Access Policies)                        | アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定, <a href="#">on page 466</a> |
| 復号ポリシー (Decryption Policies)                       | 復号ポリシー グループの Web レピュテーション フィルタの設定, <a href="#">on page 470</a>  |
| シスコ データ セキュリティ ポリシー (Cisco Data Security Policies) | 復号ポリシー グループの Web レピュテーション フィルタの設定, <a href="#">on page 470</a>  |

アクセスポリシーでのみ Advanced Malware Protection 設定を構成できます。「[ファイル レピュテーションと分析機能の設定, on page 483](#)」を参照してください。

## アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定

適応型スキャンがイネーブルの場合、アクセス ポリシーに設定できる Web レピュテーションとマルウェア対策の設定項目は、適応型スキャンがオフの場合とやや異なります。



### Note

展開にセキュリティ管理アプライアンスが含まれており、この機能をプライマリ構成で設定する場合、このページのオプションは、関連するプライマリ構成で適応型セキュリティが有効になっているかどうかに応じて異なります。[Web]>[ユーティリティ (Utilities)]>[セキュリティ サービス表示 (Security Services Display)] ページで、セキュリティ管理アプライアンスの設定を確認します。

- [適応型スキャンについて, on page 462](#)

### マルウェア対策およびレピュテーションの設定 (適応型スキャンがイネーブルの場合)

#### Procedure

- ステップ 1** [Webセキュリティマネージャ (Web Security Manager)]>[アクセスポリシー (Access Policies)] を選択します。
- ステップ 2** 設定するアクセス ポリシーの [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] リンクをクリックします。
- ステップ 3** [Webレピュテーションとマルウェア対策の設定 (Web Reputation and Anti-Malware Settings)] セクションで [Webレピュテーションとマルウェア対策のカスタム設定の定義 (Define Web Reputation and Anti-Malware Custom Settings)] を選択します。  
  
これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。
- ステップ 4** [Web レピュテーション設定 (Web Reputation Settings)] セクションで、Web レピュテーション フィルタリングをイネーブルにするかどうかを選択します。適応型スキャンによって、各 Web 要求に最適な Web レピュテーション スコアのしきい値が選択されます。

- ステップ 5** [セキュアエンドポイント設定（Advanced Malware Protection Settings）] セクションで設定項目を設定します。
- ステップ 6** [Cisco IronPort DVSマルウェア防御設定（Cisco IronPort DVS Anti-Malware Settings）] セクションまでスクロールします。
- ステップ 7** 必要に応じて、ポリシーのマルウェア対策設定を指定します。

|                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 疑わしいユーザー エージェント スキャンを有効にする（Enable Suspect User Agent Scanning） | <p>HTTP 要求ヘッダーで指定されているユーザー エージェント フィールドに基づいて、トラフィックをスキャンするかどうかを選択します。</p> <p>このチェックボックスをオンにした場合は、ページ下部の [追加スキャン（Additional Scanning）] セクションで、疑わしいユーザー エージェントをモニターするかブロックするかを選択できます。</p> <p><b>Note</b><br/>FTP-over-HTTP 要求では、Chrome ブラウザはユーザー エージェント文字列を含まないためユーザー エージェントとして検出されません。</p>                                                                                                                              |
| マルウェア対策スキャンを有効にする（Enable Anti-Malware Scanning）                | <p>マルウェアのトラフィックをスキャンするために、DVS エンジンを使用するかどうかを選択します。適応型スキャンによって、各 Web 要求に最適なエンジンが選択されます。</p>                                                                                                                                                                                                                                                                                                                             |
| マルウェア カテゴリ（Malware Categories）                                 | <p>マルウェア スキャンの判定に基づいて各種のマルウェア カテゴリをモニターするかブロックするかを選択します。</p>                                                                                                                                                                                                                                                                                                                                                           |
| その他カテゴリ（Other Categories）                                      | <p>このセクションに表示されたオブジェクトおよび応答のタイプを、モニターするかブロックするかを選択します。</p> <p><b>Note</b><br/>[アウトブレイクヒューリスティクス（Outbreak Heuristics）] カテゴリは、スキャン エンジンの実行前に適応型スキャンによってマルウェアとして識別されたトランザクションに適用されます。</p> <p><b>Note</b><br/>設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャン エンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。</p> |

- ステップ 8** 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

### What to do next

- [適応型スキャンについて, on page 462](#)

## マルウェア対策およびレピュテーションの設定（適応型スキャンがディセーブルの場合）

## Procedure

- ステップ 1** [Webセキュリティマネージャ（Web Security Manager）]>[アクセスポリシー（Access Policies）]を選択します。
- ステップ 2** 設定するアクセス ポリシーの[マルウェア対策とレピュテーション（Anti-Malware and Reputation）]リンクをクリックします。
- ステップ 3** [Webレピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）]セクションで[Webレピュテーションとマルウェア対策のカスタム設定の定義（Define Web Reputation and Anti-Malware Custom Settings）]を選択します。
- これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。
- ステップ 4** [Web レピュテーション設定（Web Reputation Settings）]セクションで設定項目を設定します。
- ステップ 5** [セキュアエンドポイント設定（Advanced Malware Protection Settings）]セクションで設定項目を設定します。
- ステップ 6** [Cisco IronPort DVSマルウェア防御設定（Cisco IronPort DVS Anti-Malware Settings）]セクションまでスクロールします。
- ステップ 7** 必要に応じて、ポリシーのマルウェア対策設定を指定します。

## Note

Webroot、Sophos、または McAfee スキャンをイネーブルにすると、このページの[マルウェアカテゴリ（Malware Categories）]で、追加のカテゴリをモニターするかブロックするかを選択できます。

| 設定                                                                 | 説明                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 疑わしいユーザー エージェント スキャンを有効にする<br>(Enable Suspect User Agent Scanning) | <p>HTTP 要求ヘッダーで指定されているユーザー エージェント フィールドに基づいて、アプライアンスがトラフィックをスキャンできるようにするかどうかを選択します。</p> <p>このチェックボックスをオンにした場合は、ページ下部の[追加スキャン（Additional Scanning）]セクションで、疑わしいユーザー エージェントをモニターするかブロックするかを選択できます。</p> <p><b>Note</b><br/>FTP-over-HTTP 要求では、Chrome ブラウザはユーザー エージェント文字列を含まないためユーザー エージェントとして検出されません。</p> |
| Webroot を有効にする<br>(Enable Webroot)                                 | アプライアンスがトラフィックをスキャンする際に、Webroot スキャン エンジンを使用できるようにするかどうかを選択します。                                                                                                                                                                                                                                       |
| Sophos または McAfee を有効にする (Enable Sophos or McAfee)                 | アプライアンスがトラフィックをスキャンする際に、Sophos または McAfee スキャン エンジンを使用できるようにするかどうかを選択します。                                                                                                                                                                                                                             |

| 設定                                 | 説明                                                                                                                                                                                                                                                                                 |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| マルウェア カテゴリ<br>(Malware Categories) | マルウェア スキャンの判定に基づいて各種のマルウェア カテゴリをモニターするかブロックするかを選択します。このセクションに表示されるカテゴリは、上記でイネーブルにするスキャン エンジンによって異なります。                                                                                                                                                                             |
| その他カテゴリ<br>(Other Categories)      | このセクションに表示されたオブジェクトおよび応答のタイプを、モニターするかブロックするかを選択します。<br><br><b>Note</b><br>設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャン エンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。 |

**ステップ 8** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

#### What to do next

- [アクセス ポリシーの Web レピュテーション スコアのしきい値の設定, on page 469](#)
- [マルウェアのカテゴリについて, on page 475](#)

## Web レピュテーション スコアの設定

Secure Web Applianceをインストールして設定すると、Web レピュテーション スコアのデフォルト設定が指定されます。ただし、Web レピュテーション スコアのしきい値の設定は組織のニーズに合わせて変更できます。各ポリシー グループに応じた Web レピュテーション フィルタを設定してください。

### アクセス ポリシーの Web レピュテーション スコアのしきい値の設定

#### Procedure

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] > [アクセス ポリシー (Access Policies)] を選択します。
- ステップ 2** [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] 列で、編集するアクセス ポリシー グループのリンクをクリックします。
- ステップ 3** [Webレピュテーションとマルウェア対策の設定 (Web Reputation and Anti-Malware Settings)] セクションで [Webレピュテーションとマルウェア対策のカスタム設定の定義 (Define Web Reputation and Anti-Malware Custom Settings)] を選択します。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。

## 復号ポリシー グループの Web レピュテーション フィルタの設定

- ステップ 4** [Web レピュテーション フィルタを有効にする (Enable Web Reputation Filtering)] フィールドがイネーブルになっていることを確認します。
- ステップ 5** マーカーを動かして、URL のブロック、スキャン、許可の各アクションの範囲を変更します。
- ステップ 6** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

### Note

適応型スキャンがディセーブルの場合は、アクセス ポリシーの Web レピュテーション スコアのしきい値を編集できます。

## 復号ポリシー グループの Web レピュテーション フィルタの設定

### Procedure

- ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] > [復号ポリシー (Decryption Policies)] を選択します。
- ステップ 2** [Web レピュテーション (Web Reputation)] 列で、編集する復号ポリシー グループのリンクをクリックします。
- ステップ 3** [Web レピュテーション設定 (Web Reputation Settings)] セクションで、[Web レピュテーションのカスタム設定の定義 (Define Web Reputation Custom Settings)] を選択します。これにより、グローバル ポリシー グループによる Web レピュテーション設定を上書きすることができます。
- ステップ 4** [Web レピュテーション フィルタを有効にする (Enable Web Reputation Filtering)] フィールドがオンになっていることを確認します。
- ステップ 5** マーカーを動かして、URL のドロップ、復号、およびパススルー アクションの範囲を変更します。
- ステップ 6** [スコアを持たないサイト (Sites with No Score)] フィールドで、Web レピュテーション スコアが割り当てられていないサイトの要求に対して実行するアクションを選択します。
- ステップ 7** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## データ セキュリティ ポリシー グループの Web レピュテーション フィルタの設定

### Procedure

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] > [シスコ データ セキュリティ (Cisco Data Security)] を選択します。
- ステップ 2** [Web レピュテーション (Web Reputation)] 列で、編集するデータ セキュリティ ポリシー グループのリンクをクリックします。
- ステップ 3** [Web レピュテーション設定 (Web Reputation Settings)] セクションで、[Web レピュテーションのカスタム設定の定義 (Define Web Reputation Custom Settings)] を選択します。
- これにより、グローバル ポリシー グループによる Web レピュテーション設定を上書きすることができます。

**ステップ 4** マーカーを動かして、URL のブロックおよびモニター アクションの範囲を変更します。

**ステップ 5** 変更を送信して確定します ([送信 (Submit) ] と [変更を確定 (Commit Changes) ] )。

**Note**

Cisco データ セキュリティ ポリシーの Web レピュテーションのしきい値には、負またはゼロの値のみ設定できます。定義では、すべての正のスコアがモニターされます。

## AMP for Endpoints コンソールとアプライアンスの統合

お使いのアプライアンスを AMP for Endpoints コンソールと統合すると、AMP for Endpoints コンソールで以下の操作を実行できます。

- シンプル カスタム検出リストを作成する。
- シンプル カスタム検出リストに新しい悪意のあるファイル SHA を追加する。
- アプリケーション許可リストを作成する。
- アプリケーション許可リストに新しいファイル SHA を追加する。
- カスタム ポリシーを作成する。
- カスタムポリシーにシンプルカスタム検出リストおよびアプリケーション許可リストを関連付ける。
- カスタム グループを作成する。
- カスタム グループにカスタム ポリシーを関連付ける。
- 登録済みのアプライアンスをデフォルトのグループからカスタム グループに移動する。
- 特定のファイル SHA のファイル トラジェクトリの詳細を表示する。

アプライアンスを AMP for Endpoints コンソールと統合するには、アプライアンスをコンソールに登録する必要があります。

統合後に、ファイル SHA がファイル レピュテーション サーバに送信されると、ファイル SHA に対してファイル レピュテーション サーバーから得られた判定は、AMP for Endpoints コンソールの同じファイル SHA に対してすでに利用可能な判定により上書きされます。

ファイル SHA がすでにグローバルに悪意のあるものとしてマークされている場合、AMP for Endpoints コンソールで同じファイル SHA をブロックリストに追加すると、ファイルの判定結果は「悪意のあるもの」になります。

[高度なマルウェア防御 (Advanced Malware Protection) ] レポートページには、新しいセクション、[カテゴリ別受信マルウェアファイル (Incoming Malware Files by Category) ] があります。このセクションには、AMP for Endpoints コンソールから受信されたブロックリストに登録されているファイル SHA の割合が、[カスタム検出 (Custom Detection) ] として表示されます。ブロックリストに登録されているファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル (Incoming Malware Threat Files) ] セクションに [シンプルカスタム検出 (Simple



Custom Detection) ] として表示されます。レポートの [詳細 (More Details) ] セクションのリンクをクリックすると、AMP for Endpoints コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリ詳細を表示できます。

[高度なマルウェア防御 (Advanced Malware Protection) ] レポートページには、新しいセクション、[カテゴリ別受信悪意のあるファイル (Incoming Malicious Files by Category) ] があります。このセクションには、AMP for Endpoints コンソールから受信されたブロックリストに登録されているファイル SHA の割合が、[カスタム検出 (Custom Detection) ] として表示されます。ブロックリストのファイル SHA の脅威名は、レポートの [悪意のある脅威ファイル (Malicious Threat Files) ] セクションに [カスタム検出 (Custom Detection) ] として表示されます。AMP for Endpoints コンソールでブロックリストに登録されたファイル SHA のファイルトラジェクトリの詳細を表示するには、[#unique\\_643](#)を参照してください。

### 始める前に

AMP for Endpoints コンソールの管理アクセス権を伴うユーザーアカウントがあることを確認してください。AMP for Endpoints コンソールのユーザーアカウントを作成する方法の詳細については、Cisco TAC にお問い合わせください。

(クラスタ化された設定の場合) クラスタ化された設定では、ログインしているアプライアンスを AMP for Endpoints コンソールにのみ登録できます。アプライアンスを AMP for Endpoints コンソールにスタンドアロンモードですでに登録している場合は、アプライアンスをクラスタに参加させる前に手動で登録を解除してください。

ファイル レピュテーション フィルタリングが有効化され、設定されていることを確認してください。ファイル レピュテーション フィルタリングを有効にして設定する方法については、「[ファイルレピュテーションと分析サービスの有効化と設定 \(488 ページ\)](#)」を参照してください。

### 手順

- 
- ステップ 1** [セキュリティサービス (Security Services) ] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] を選択します。
- ステップ 2** [グローバル設定を編集 (Edit Global Settings) ] をクリックします。
- ステップ 3** Web インターフェイスの [ファイルレピュテーションとファイル分析 (File Reputation and File Analysis) ] ページで、[ファイルレピュテーション (File Reputation) ] の [詳細設定 (Advanced Settings) ] パネルにある [AMP for Endpoints へのアプライアンスの登録 (Register Appliance with Secure Endpoint AMP for Endpoints) ] をクリックします。
- [ AMP for Endpoints へのアプライアンスの登録 (Register Appliance with Secure Endpoint AMP for Endpoints) ] をクリックすると、AMP for Endpoints コンソールのログインページが表示されます。
- ステップ 4** Web インターフェイスの [マルウェア対策レピュテーション (Anti-Malware Reputation) ] ページで、[ファイルレピュテーション (File Reputation) ] の [詳細設定 (Advanced Settings) ] パネルにある [AMP for Endpoints へのアプライアンスの登録 (Register Appliance with Secure Endpoint AMP for Endpoints) ] をクリックします。

[ AMP for Endpoints へのアプライアンスの登録 (Register Appliance with Secure Endpoint AMP for Endpoints) ] をクリックすると、AMP for Endpoints コンソールのログインページが表示されます。

(注)

アプライアンスを AMP for Endpoints コンソールと統合するには、アプライアンスをコンソールに登録する必要があります。コンソールへのアプライアンスの登録は 1 時間に 1 回に制限することを推奨します。

(注)

AMP for Endpoints にアプライアンスを登録する前に、ファイルレピュテーションフィルタリングを有効にし、設定する必要があります。ファイルレピュテーションフィルタリングを有効にして設定する方法については、「[ファイルレピュテーションと分析サービスの有効化と設定 \(488 ページ\)](#)」を参照してください。

**ステップ 5** ご使用のユーザーログイン情報で、AMP for Endpoints コンソールにログインします。

**ステップ 6** AMP for Endpoints の認証ページで [許可 (Allow) ] をクリックして、アプライアンスを登録します。

[許可 (Allow) ] をクリックすると登録が完了し、アプライアンスの [マルウェア対策レピュテーション (Anti-Malware Reputation) ] ページにリダイレクトされます。[ AMP for Endpoints コンソールの統合 (Secure Endpoint AMP for Endpoints Console Integration) ] フィールドに、お使いのアプライアンスの名前が表示されます。アプライアンス名は、AMP for Endpoints のコンソールページでアプライアンス設定をカスタマイズする際に使用できます。

## 次のタスク

次の手順：

- AMP for Endpoints コンソールページの [アカウント (Accounts) ] > [アプリケーション (Applications) ] セクションに移動すると、アプライアンスが AMP for Endpoints コンソールに登録されているかどうかを確認できます。アプライアンス名は、AMP for Endpoints コンソールページの [アプリケーション (Applications) ] セクションに表示されます。
- 登録されたアプライアンスは、デフォルトのポリシー (ネットワークポリシー) が関連付けられたデフォルトのグループ (監査グループ) に追加されます。デフォルトポリシーには、ブロックリストまたは許可リストに追加されるファイル SHA が含まれています。AMP for Endpoints の設定をお使いのアプライアンス用にカスタマイズして、ブロックリストまたは許可リストに追加されている独自のファイル SHA を追加する場合は、<https://console.amp.cisco.com/docs> で AMP for Endpoints のユーザーマニュアルを参照してください。
- アプライアンス接続を AMP for Endpoints コンソールから登録解除するには、アプライアンスの [ファイルレピュテーション (File Reputation) ] セクションの [詳細設定 (Advanced Settings) ] で [登録解除 (Deregister) ] をクリックするか、または AMP for Endpoints のコンソールページ (<https://console.amp.cisco.com/>) にアクセスする必要があります。詳細については、<https://console.amp.cisco.com/docs> で AMP for Endpoints のユーザーマニュアルを参照してください。



- (注) ファイル レピュテーション サーバーを別のデータセンターに変更すると、アプライアンスは AMP for Endpoints コンソールから自動的に登録解除されます。ファイルレピュテーションサーバーに選択された同じデータセンターを使用して、アプライアンスを AMP for Endpoints コンソールに再登録する必要があります。



- (注) 悪意のあるファイル SHA がクリーンと判定される場合、そのファイル SHA が AMP for Endpoints コンソールで許可リストに追加されていないか確認する必要があります。

## データベース テーブルの保持

Web レピュテーション、Webroot、Sophos、および McAfee のデータベースは、Cisco アップデートサーバーから定期的にアップデートを受信します。サーバーのアップデートは自動化されており、アップデート間隔はサーバーによって設定されます。

### Web レピュテーション データベース

Secure Web Applianceが保持しているフィルタリング データベースには、統計情報およびさまざまなタイプの要求の処理方法に関する情報が含まれています。また、Cisco SensorBase ネットワーク サーバーに Web レピュテーション統計情報を送信するようにアプライアンスを設定することもできます。SensorBase サーバー情報は SensorBase ネットワークからのデータフィールドに活用され、Web レピュテーション スコアの作成に使用されます。

## Web レピュテーション フィルタリング アクティビティおよび DVS スキャンのロギング

アクセス ログ ファイルには、Web レピュテーション フィルタと DVS エンジンから返された各トランザクションの情報が記録されます。アクセス ログのスキャン判定情報セクションには、トランザクションに適用されたアクションの原因を把握するのに役立つ多くのフィールドがあります。たとえば、あるフィールドには、Sopho から DVS エンジンに渡された Web レピュテーション スコアやマルウェア スキャン判定が表示されます。

## 適応型スキャンのロギング

| アクセス<br>ログのカ<br>スタム<br>フィール<br>ド | W3C ログのカスタム フィールド        | 説明                                                                                                                 |
|----------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------|
| %X6                              | x-as-malware-threat-name | 適応型スキャンから返されたマルウェア対策名。トランザクションがブロックされていない場合、このフィールドはハイフン（「-」）を返します。この変数は、スキャン判定情報（各アクセス ログ エントリの末尾の山カッコ内）に含まれています。 |

適応型スキャンエンジンによってブロックおよびモニターされるトランザクションは、以下の ACL デシジョン タグを使用します。

- BLOCK\_AMW\_RESP
- MONITOR\_AMW\_RESP

## キャッシング

以下のガイドラインは、AsyncOS がマルウェアのスキャン中にキャッシュを使用する仕組みを示しています。

- AsyncOS は、オブジェクト全体がダウンロードされたときにだけオブジェクトをキャッシュします。スキャン中にマルウェアがブロックされた場合、オブジェクト全体はダウンロードされないで、キャッシュされません。
- AsyncOS は、コンテンツの取得元がサーバーであるか Web キャッシュであるかにかかわらず、コンテンツをスキャンします。
- コンテンツがキャッシュされる時間はさまざまな要因によって異なります。デフォルト値はありません。
- AsyncOS は、シグニチャが更新されるとコンテンツを再スキャンします。

## マルウェアのカテゴリについて

| マルウェアのタイプ        | 説明                                                                                                                    |
|------------------|-----------------------------------------------------------------------------------------------------------------------|
| アドウェア            | アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザーがシステム設定を変更できなくなる場合もあります。 |
| ブラウザ ヘルパー オブジェクト | ブラウザヘルパー オブジェクトは、広告の表示やユーザー設定の乗っ取りに関連するさまざまな機能を実行する可能性があるブラウザ プラグインです。                                                |

| マルウェアのタイプ        | 説明                                                                                                                                                           |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 商用システム モニタ       | 商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。                                                                                                 |
| ダイヤラ             | ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザーの完全な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザーを接続するプログラムです。                                                                    |
| 一般的なスパイウェア       | スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。                                                                                                  |
| ハイジャッカー          | ハイジャッカーは、ユーザーの承諾なしにユーザーを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザーのシステムに不要な変更を加えたりします。                                                                |
| 悪意のある既知の高リスクファイル | これらは、Advanced Malware Protection ファイルレピュテーション サービスによって脅威と判定されたファイルです。                                                                                        |
| その他のマルウェア        | このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。                                                                                                             |
| フィッシング URL       | フィッシング URL は、ブラウザのアドレスバーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。                                                                                            |
| PUA              | 望ましくないアプリケーションのこと。PUA は、悪質ではないが望ましくないと見なされるアプリケーションです。                                                                                                       |
| システム モニター        | システム モニターには、以下のいずれかを実行するソフトウェアが含まれます。 <ul style="list-style-type: none"> <li>公然と、または密かに、システムプロセスやユーザアクションを記録する。</li> <li>これらの記録を後で取得して確認できるようにする。</li> </ul> |
| トロイのダウンロード       | トロイのダウンロードは、インストール後にリモートホスト/サイトにアクセスして、リモートホストからパッケージやアフィリエイトをインストールするトロイの木馬です。                                                                              |
| トロイの木馬           | トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。                                                                                                  |
| トロイのフィッシャ        | トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待ったり、感染したマシンをスキャンしてユーザー名とパスワードを探したりします。                                                                        |

| マルウェアのタイプ | 説明                                                        |
|-----------|-----------------------------------------------------------|
| ウイルス      | ウイルスは、ユーザーが気付かない間にコンピュータにロードされるプログラムまたはコードです。             |
| ワーム       | ワームは、コンピュータ ネットワーク上で自己を複製し、悪質なアクションを実行するプログラムまたはアルゴリズムです。 |

## ファイルレピュテーションフィルタリングとファイル分析

この章で説明する内容は、次のとおりです。

- [ファイル レピュテーション フィルタリングとファイル分析の概要 \(477 ページ\)](#)
- [ファイル レピュテーションと分析機能の設定 \(483 ページ\)](#)
- [ファイルレピュテーションおよびファイル分析のレポートとトラッキング \(499 ページ\)](#)
- [ファイルの脅威判定の変更時のアクションの実行 \(503 ページ\)](#)
- [ファイル レピュテーションと分析のトラブルシューティング \(503 ページ\)](#)

### ファイル レピュテーション フィルタリングとファイル分析の概要

Advanced Malware Protection は、次によりゼロデイやファイルベースの標的型の脅威から保護します。

- 既知のファイルのレピュテーションを取得する。
- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を常に評価し、脅威と判定されているファイルがネットワークに侵入するとユーザに通知する。

この機能はファイルのダウンロードに使用できます。アップロードされたファイル。

ファイル レピュテーションおよびファイル分析サービスでは、パブリック クラウドまたはプライベート クラウド（オンプレミス）を選択できます。

- プライベートクラウドファイルレピュテーションサービスは Cisco AMP 仮想プライベートクラウドアプライアンスにより提供され、「プロキシ」モードまたは「エアギャップ」（オンプレミス）モードで動作します。「[オンプレミスのファイルレピュテーションサーバの設定, on page 486](#)」を参照してください。
- プライベートクラウドファイル分析サービスは、オンプレミス Cisco AMP マルウェア分析アプライアンスにより提供されます。「[オンプレミスのファイル分析サーバの設定, on page 487](#)」を参照してください。

## ファイル脅威判定のアップデート

新しい情報の出現に伴い、脅威の判定は変化します。最初にファイルが不明または正常として評価されると、ユーザがこのファイルにアクセスできます。新しい情報が利用可能になるのに伴い脅威判定が変更されると、アラートが送信され、ファイルとその新しい判定が[AMP 判定のアップデート (AMP Verdict Updates)] レポートに示されます。脅威の影響に対処する最初の作業として、侵入のきっかけとなったトランザクションを調査できます。

判定が「悪意がある」から「正常」に変更されることもあります。

アプライアンスが同じファイルの後続インスタンスを処理するときに、更新された結果がただちに適用されます。

判定アップデートのタイミングに関する情報は、ファイル基準のドキュメント（[ファイル レピュテーションおよび分析サービスでサポートされるファイル](#), on page 480を参照）に記載されています。

### 関連項目

- [ファイル レピュテーションおよびファイル分析のレポートとトラッキング](#), on page 499
- [ファイルの脅威判定の変更時のアクションの実行](#), on page 503

## ファイル処理の概要

最初に、ファイルのダウンロード元の Web サイトが Web ベース レピュテーション サービス (WBRs) に対して評価されます。

サイトの Web レピュテーション スコアが「スキャン (Scan)」に設定されている範囲内である場合、アプライアンスはトランザクションをスキャンしてマルウェアがあるかどうかを確認し、同時にクラウドベースサービスに対してファイルのレピュテーションを照会します。（サイトのレピュテーション スコアが「ブロック (Block)」範囲内である場合、トランザクションはブロックされるため、ファイルをさらに処理する必要はありません。）スキャン中にマルウェアが検出されると、ファイルのレピュテーションに関係なくトランザクションはブロックされます。

適応型スキャンもイネーブルになっている場合は、ファイルレピュテーション評価とファイル分析は適応型スキャンに含まれます。

アプライアンスとファイル レピュテーション サービス間の通信は暗号化され、改ざんされないように保護されます。

ファイル レピュテーションの評価後：

- ファイルがファイル レピュテーション サービスに対して既知であり、正常であると判断された場合、ファイルはエンドユーザに対して解放されます。
- ファイル レピュテーション サービスから悪意があるという判定が返されると、このようなファイルに対して指定したアクションが、アプライアンスにより適用されます。
- レピュテーションサービスがファイルを認識しているが、決定的な判定を下すための十分な情報がない場合、レピュテーションサービスはファイルの特性（脅威のフィンガープリ

ントや動作分析など)に基づき、レピュテーションスコアを戻します。このスコアが設定されたレピュテーションしきい値を満たすか、または超過した場合、悪意がある、またはリスクの高いファイルに関するアクセスポリシーで設定したアクションがアプライアンスによって適用されます。レピュテーションサーバーは、分析スコアに関係なく、分析用にファイルを送信します（ファイルが分析用の条件を満たす場合）。で生成されたテクニカルサポート コレクションに組み込まれます。

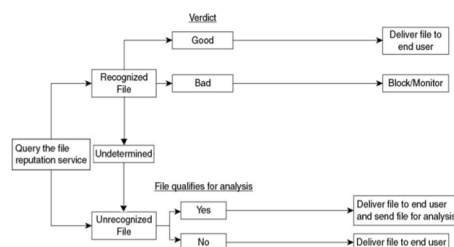
ファイル分析スコアに関係なく、AMP クラウドの判定結果が **MALICIOUS** の場合、ファイルはブロックされます。

- レピュテーションサービスにそのファイルに関する情報がなく、そのファイルが分析の基準を満たしていない場合（[ファイルレピュテーションおよび分析サービスでサポートされるファイル](#), on page 480を参照）、そのファイルは正常と見なされ、エンドユーザに解放されます。
- クラウドベースのファイル分析サービスを有効にしており、レピュテーションサービスにそのファイルの情報がなく、そのファイルが分析できるファイルの基準を満たしている場合（[ファイルレピュテーションおよび分析サービスでサポートされるファイル](#), on page 480を参照）は、ファイルは正常と見なされ、任意で分析用に送信されます。
- オンプレミスのファイル分析での展開では、レピュテーション評価とファイル分析は同時に実行されます。レピュテーションサービスから判定が返された場合は、その判定が使用されます。これは、レピュテーションサービスにはさまざまなソースからの情報が含まれているためです。レピュテーションサービスがファイルを認識していない場合、そのファイルはユーザに解放されますが、ファイル分析の結果がローカルキャッシュで更新され、そのファイルのインスタンスの以降の評価に使用されます。
- サーバとの接続がタイムアウトしたためにファイルレピュテーションの判定の情報が利用できない場合、そのファイルはスキャン不可と見なされ、設定されたアクションが適用されます。

## 低リスク ファイル

当初ファイルが不明で動的コンテンツを含まないと評価された場合、アプライアンスはそのファイルを事前分類エンジンに送信し、事前分類エンジンで低リスクに指定されます。このファイルは分析用にアップロードされません。キャッシュの有効期限内に同じファイルにアクセスした場合、改めて低リスクと評価され、分析用にアップロードされることはありません。キャッシュタイムアウトの後、同じファイルにもう一度アクセスすると、不明、低リスクと順を追って評価されます。このプロセスは低リスクファイルに対して繰り返されます。これらの低リスクファイルはアップロードされないため、ファイル分析レポートには含められません。

Figure 10: クラウドファイル分析の展開における **Advanced Malware Protection** ワークフロー





ファイルが分析のために送信される場合：

- 分析用にクラウドに送信される場合、ファイルは HTTPS 経由で送信されます。
- 分析には通常、数分かかりますが、さらに時間がかかることもあります。
- ファイル分析で悪意があるとしてフラグ付けされたファイルが、レピュテーションサービスでは悪意があると識別されない場合があります。ファイルレピュテーションは、1回のファイル分析結果でなく、さまざまな要因によって経時的に決定されます。
- オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用して分析されたファイルの結果は、ローカルにキャッシュされます。



#### Note

- ファイルレピュテーションサーバーから unknown、File\_unknown、unscannable の判定が返された場合、分析スコアはチェックされなくなります。これは、スコアに関係なく、AMP クラウドの判定結果に基づいて AMP がアクションを実行できるように不明またはスキャンできないファイルに対して AsyncOS 15.2.4 で導入された動作の変更に従います。
- 判定が unknown、File\_unknown、unscannable の場合は、詳細な分析のためにファイルが送信されます。その後、ファイルはそのままクライアントに配信され、TG サーバーからの結果が SWA キャッシュに保存され、レポートに表示されます。

判別のアップデートの詳細については、[ファイル脅威判定のアップデート](#) , on page 478 を参照してください。

## ファイルレピュテーションおよび分析サービスでサポートされるファイル

レピュテーションサービスはほとんどのタイプのファイルを評価します。ファイルタイプの識別はファイルコンテンツによって行われ、ファイル拡張子には依存していません。

レピュテーションが不明な一部のファイルは、分析して脅威の特性を調べることができます。ファイル分析機能を設定すると、分析するファイルタイプを選択できます。新しいタイプを動的に追加できます。アップロード可能なファイルタイプのリストが変更された場合はアラートを受け取るので、追加されたファイルタイプを選択してアップロードできます。

ファイルレピュテーションおよび分析サービスでサポートされているファイルの詳細は、登録済みのお客様に限り提供しています。評価と分析の対象となるファイルについて詳しくは、『*File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*』を参照してください。このドキュメントは、<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html> から入手できます。ファイルレピュテーションの評価基準、および分析用ファイルの送信基準はいつでも変更できます。

このドキュメントにアクセスするには、シスコの顧客アカウントとサポート契約が必要です。登録するには、<https://www.cisco.com/c/en/us/about/help/login-account-help.html> にアクセスしてください。

[セキュリティサービス (Security Services)] > [マルウェア対策およびレピュテーション (Anti-Malware and Reputation)] ページの [DVSエンジンオブジェクトスキャンの制限 (DVS Engine Object Scanning Limits)] の設定も、ファイル レピュテーションと分析の最大ファイル サイズを決定します。

Advanced Malware Protectionが対応しないファイルのダウンロードをブロックするには、ポリシーを設定する必要があります。



**Note** どこかのソースからすでに分析用にアップロードしたことがあるファイルは、再度アップロードされません。このようなファイルの分析結果を表示するには、[ファイル分析 (File Analysis)] レポート ページから SHA-256 を検索します。

#### 関連項目

- [ファイル レピュテーションと分析サービスの有効化と設定, on page 488](#)
- [Advanced Malware Protection の問題に関するアラートの確実な受信, on page 498](#)
- [アーカイブ ファイルまたは圧縮ファイルの処理, on page 481](#)

### アーカイブ ファイルまたは圧縮ファイルの処理

ファイルが圧縮またはアーカイブされている場合：

- 圧縮ファイルまたはアーカイブ ファイルのレピュテーションが評価されます。
- 選択されたファイルの種類によっては、圧縮ファイルまたはアーカイブファイルは圧縮解除され、すべての抽出されたファイルのレピュテーションが評価されます。

ファイル形式を含めて、検査対象となるアーカイブ ファイルや圧縮ファイルについて詳しくは、[ファイルレピュテーションおよび分析サービスでサポートされるファイル, on page 480](#) の情報を参照してください。

このシナリオでは、次のようになります。

- 抽出されたファイルのいずれかが悪意のあるファイルである場合、ファイル レピュテーション サービスは、その圧縮/アーカイブ ファイルに対して「悪意がある (Malicious)」という判定を返します。
- 圧縮/アーカイブ ファイルが悪意のあるファイルであり、抽出されたすべてのファイルが正常である場合、ファイルレピュテーション サービスは、圧縮/アーカイブ ファイルに対して「悪意がある (Malicious)」という判定を返します。
- 抽出されたファイルのいくつかの判定が「不明 (unknown)」である場合、それらの抽出ファイルは、状況に応じて、分析のために送信されます（そのように設定されており、ファイル タイプがファイル分析でサポートされている場合）。
- 圧縮/アーカイブ ファイルの圧縮解除中にファイルの抽出に失敗した場合、ファイル レピュテーション サービスは、圧縮/アーカイブ ファイルに対して「スキャン不可

(Unscannable)」という判定を返します。ただし、抽出されたファイルの1つが悪意のあるファイルである場合、ファイルレピュテーションサービスは、圧縮/アーカイブファイルに対して「悪意がある (Malicious)」という判定を返します（「悪意がある (Malicious)」という判定は「スキャン不可 (Unscannable)」よりも順位が高くなります）。

- 圧縮ファイルやアーカイブファイルは、次のシナリオではスキャン不可として処理されません。
  - データ圧縮率が 20 を超える。
  - アーカイブ ファイルに 5 を超えるレベルのネストが含まれる。
  - アーカイブ ファイルに 200 を超える子ファイルが含まれる。
  - アーカイブ ファイルのサイズが 50 MB を超える。
  - アーカイブ ファイルがパスワードで保護されているか、または読み取り不可である。



**Note** 1 つ以上の構成ファイルがファイル分析の対象となる場合、Cisco Secure Web Appliance はアーカイブファイル全体を Cisco Secure Malware Analytics に送信します。構成ファイルに悪意のあるものが見つかった場合、アーカイブファイル全体がマルウェアとしてマークされます。

Cisco Secure Web Appliance が圧縮ファイルまたはアーカイブファイルの抽出に失敗した場合、ファイルは分析のために Cisco Secure Malware Analytics にアップロードされます。



**Note** セキュア MIME タイプの抽出ファイル（テキストやプレーンテキストなど）のレピュテーションは、評価されません。

## クラウドに送信される情報のプライバシー

- クラウド内のレピュテーション サービスには、ファイルを一意に識別する SHA のみが送信されます。ファイル自体は送信されません。
- クラウド内のファイル分析サービスを使用している場合、ファイルが分析の要件を満たしていれば、ファイル自体がクラウドに送信されます。
- 分析用にクラウドに送信されて「悪意がある」と判定されたすべてのファイルに関する情報は、レピュテーション データベースに追加されます。この情報は他のデータと共にレピュテーション スコアを決定するために使用されます。

オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスで分析されたファイルの情報は、レピュテーションサービスと共有されません。

## ファイルレピュテーションと分析機能の設定

- [ファイルレピュテーションと分析サービスとの通信の要件](#) , on page 483
- [オンプレミスのファイルレピュテーションサーバの設定](#) , on page 486
- [オンプレミスのファイル分析サーバの設定](#) , on page 487
- [ファイルレピュテーションと分析サービスの有効化と設定](#) , on page 488
- [\(パブリッククラウドファイル分析サービスのみ\) アプライアンスグループの設定](#) , on page 495
- [アクセスポリシーごとのファイルレピュテーションおよび分析サービスのアクションの設定](#) , on page 497
- [Advanced Malware Protection の問題に関するアラートの確実な受信](#) , on page 498
- [Advanced Malware Protection 機能の集約管理レポートの設定](#) , on page 499

## ファイルレピュテーションと分析サービスとの通信の要件

- これらのサービスを使用する Secure Web Appliance はすべて（オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用するよう設定されたファイル分析サービスは除く）、インターネット経由で直接サービスに接続する必要があります。
- デフォルトでは、ファイルレピュテーションおよび分析サービスとの通信は、アプライアンスの管理ポート（M1）経由でルーティングされます。アプライアンスが管理ポートを使用してデータをルーティングしていない場合は、[データインターフェイス経由でのファイルレピュテーションサーバおよびファイル分析サーバへのトラフィックのルーティング](#) , on page 484 を参照してください。
- ファイルレピュテーションとファイル分析にパブリッククラウドサーバーとプライベート/オンプレミスの組み合わせを使用することはできません。オンプレミスデバイスを使用している場合は、ファイル分析とファイルレピュテーションの両方にオンプレミスのクラウドサーバーが必要です。パブリッククラウドサーバーを使用している場合は、ファイルレピュテーションとファイル分析の両方にパブリッククラウドサーバーが必要です。
- デフォルトでは、ファイルレピュテーションとクラウドベースの分析サービスとの通信は、デフォルトゲートウェイに関連付けられているインターフェイス経由でルーティングされます。トラフィックを異なるインターフェイス経由でルーティングするには、[セキュリティサービス (Security Services)] > [ファイルレピュテーションと分析 (File Reputation and Analysis)] ページの [詳細設定 (Advanced)] セクションで、各アドレスにスタティックルートを作成します。
- 以下のファイアウォールポートが開いている必要があります。

| ファイ<br>ア<br>ウォー<br>ル ポー<br>ト | 説明                                            | プロ<br>トコ<br>ル | 入力<br>/ 出<br>力 | ホスト名 (Hostname)                                                                                                                                                                                              | アプライアンス イン<br>ターフェイス                                                               |
|------------------------------|-----------------------------------------------|---------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 443                          | ファイル分<br>析のための<br>クラウド<br>サービスへ<br>のアクセ<br>ス。 | TCP           | 発信             | [セキュリティサービス<br>(Security Services)] > [マ<br>ルウェア対策とレピュテー<br>ション (Anti-Malware and<br>Reputation)] の [詳細設定<br>(Advanced)] セクショ<br>ン: [ファイル分析の詳細<br>設定 (Advanced Settings for<br>File Analysis)] で設定され<br>た名前。 | 管理 (データポート<br>経由でこのトラ<br>フィックをルーティ<br>ングするようにスタ<br>ティック ルートが設<br>定されている場合を<br>除く)。 |

- ファイル レピュテーション機能を設定するときに、ポート 443 で SSL を使用するかどうかを選択します。

#### 関連項目

- [ファイル レピュテーションと分析サービスの有効化と設定, on page 488](#)

#### データ インターフェイス経由でのファイル レピュテーション サーバおよびファイル分析サーバへのトラフィックのルーティング

([ネットワーク (Network)] > [インターフェイス (Interfaces)] ページで) アプライアンスの管理ポートがアプライアンス管理サービス専用に設定されている場合は、代わりに、データポートを介してファイルレピュテーションおよび分析のトラフィックをルーティングするように、アプライアンスを設定します。

[ネットワーク (Network)] > [ルート (Routes)] ページでデータトラフィックのルートを追加します。全般的な要件と手順については、次を参照してください。 [TCP/IP トラフィック ルートの設定, on page 55](#)

| 接続先                | 宛先ネットワーク                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | ゲートウェイ                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| ファイル レピュテーション サービス | <p>[セキュリティ サービス (Security Services) ]<br/> &gt; [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] の [詳細設定 (Advanced) ] セクション &gt; [ファイル レピュテーションの詳細設定 (Advanced Settings for File Reputation) ] セクションで、[ファイル レピュテーション サーバ (File Reputation Server) ] にファイル レピュテーション サーバの名前 (URL) を指定し、[クラウド ドメイン (Cloud Domain) ] にクラウド サーバ プールのクラウド ドメインを指定します。</p> <p>ファイル レピュテーション サーバのプライベートクラウドを選択する場合は、サーバのホスト名または IP アドレスを入力し、有効な公開キー指定します。これは、プライベートクラウドアプライアンスで使用されるキーと同じである必要があります。</p> <p>[セキュリティ サービス (Security Services) ]<br/> &gt; [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] の [詳細設定 (Advanced) ] セクション : [ファイル レピュテーションの詳細設定 (Advanced Settings for File Reputation) ] で設定されているクラウド サーバ プールのホスト名。</p> | データ ポートのゲートウェイの IP アドレス。 |

| 接続先        | 宛先ネットワーク                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | ゲートウェイ                   |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| ファイル分析サービス | <ul style="list-style-type: none"> <li>• [セキュリティサービス (Security Services)] &gt; [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] の [詳細設定 (Advanced)] セクション &gt; [ファイル レピュテーションの詳細設定 (Advanced Settings for File Reputation)] セクションの [ファイル分析サーバ (File Analysis Server)] に、ファイル分析サーバの名前 (URL) を指定します。</li> <li>ファイル分析サーバのプライベートクラウドを選択する場合は、サーバ URL と有効な認証局を指定します。</li> <li>• ファイル分析クライアント ID は、ファイル分析サーバでのこのアプライアンスのクライアント ID です (読み取り専用)。</li> </ul> <p>[セキュリティサービス (Security Services)]、[マルウェア対策とレピュテーション (Anti-Malware and Reputation)] の [詳細設定 (Advanced)] セクション: [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] で設定されているファイル分析サーバのホスト名。</p> | データ ポートのゲートウェイの IP アドレス。 |

#### 関連項目

- [TCP/IP トラフィック ルートの設定, on page 55](#)

## オンプレミスのファイル レピュテーション サーバの設定

プライベートクラウドのファイル分析サーバーとして Cisco AMP 仮想プライベート クラウド アプライアンスを使用する場合は、以下のように設定します。

- FireAMP プライベートクラウドのインストールおよび設定に関するガイドを含む、Cisco Advanced Malware Protection 仮想プライベート クラウド アプライアンスのドキュメントは、  
<http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html> から取得できます。

この項目に記載されているタスクはこのドキュメントを参照して実行します。

AMP 仮想プライベート クラウド アプライアンスのヘルプリンクを使用して、その他のドキュメントも入手できます。

- 「プロキシ」モードまたは「エアギャップ」（オンプレミス）モードでの Cisco AMP 仮想プライベート クラウド アプライアンスを設定および構成します。
- Cisco AMP 仮想プライベート クラウド アプライアンスのソフトウェアバージョンが、Cisco Secure Web Appliance との統合を可能にするバージョン 2.2 であることを確認します。
- AMP 仮想プライベートクラウドの証明書およびキーをそのアプライアンスにダウンロードして、この Secure Web Appliance にアップロードします。



(注) オンプレミスのファイル レピュテーション サーバーを設定した後に、この からこのサーバーへの接続を設定します。Secure Web Appliance [ファイル レピュテーションと分析サービスの有効化と設定 \(488 ページ\)](#) のステップ 6 を参照してください。

## オンプレミスのファイル分析サーバの設定

Cisco Secure Endpoint マルウェア分析アプライアンスをプライベートクラウドのファイル分析サーバーとして使用する場合：

- 『Cisco Secure Endpoint Malware Analytics Appliance Setup and Configuration Guide』 および 『Cisco Secure Endpoint Malware Analytics Appliance Administration Guide』を入手してください。Cisco Secure Endpoint マルウェア分析アプライアンスのドキュメントは、<https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html> から入手できます。

この項目に記載されているタスクはこのドキュメントを参照して実行します。

追加のドキュメントは、Cisco Secure Endpoint マルウェア分析アプライアンスのヘルプリンクから入手できます。

Administration Guide で、次のすべての情報を検索します：他の Cisco アプライアンス（CSA、Cisco Sandbox API Secure Web Appliance）との統合。

- Cisco Secure Endpoint マルウェア分析アプライアンスを設定および構成します。
- 必要に応じて、Cisco Secure Endpoint マルウェア分析アプライアンスのソフトウェアバージョンをバージョン 1.2.1 に更新します。これにより、Cisco Secure Web Appliance との統合がサポートされます。  
バージョン番号を確認し更新を実行する方法については、AMP マルウェア分析のドキュメントを参照してください。
- アプライアンスがネットワーク上で相互に通信できることを確認します。Cisco Secure Web Appliance は、Cisco Secure Endpoint マルウェア分析アプライアンスの正常な（CLEAN）インターフェイスに接続可能である必要があります。
- 自己署名証明書を展開する場合は、Secure Web Appliance で使用される Cisco Secure Endpoint マルウェア分析アプライアンスから自己署名 SSL 証明書を生成します。SSL 証明書とキーをダウンロードする手順については、Cisco Secure Endpoint マルウェア分析アプライアンス



スの管理者ガイドを参照してください。CN として Cisco Secure Endpoint マルウェア分析アプライアンスのホスト名がある証明書を生成してください。Cisco Secure Endpoint マルウェア分析アプライアンスからのデフォルトの証明書は機能しません。

- マルウェア分析アプライアンスへの Secure Web Appliance の登録は、「[ファイルレピュテーションと分析サービスの有効化と設定, on page 488](#)」で説明したように、ファイル分析の設定を送信したときに自動的に実行されます。ただし、同じ手順に記載されているように、登録をアクティブ化する必要があります。



#### Note

オンプレミスのファイル分析サーバーを設定した後に、この Secure Web Appliance からこのサーバーへの接続を設定します。『[ファイルレピュテーションと分析サービスの有効化と設定, on page 488](#)』のステップ 7 を参照してください。

## ファイルレピュテーションと分析サービスの有効化と設定

### Before you begin

- [ファイルレピュテーションと分析サービスとの通信の要件, on page 483](#)を満たします。
- ファイルレピュテーションと分析サービスにデータ ネットワーク インターフェイスを使用する場合は、アプライアンスでデータ ネットワーク インターフェイスがイネーブルになっていることを確認します。[ネットワーク インターフェイスのイネーブル化または変更, on page 37](#)を参照してください。
- [アップグレードおよびサービス アップデートの設定, on page 214](#)で設定したアップデートサーバーへの接続を確認します。
- Cisco AMP 仮想プライベート クラウド アプライアンスをプライベートクラウドのファイルレピュテーションサーバーとして使用する場合は、[オンプレミスのファイルレピュテーション サーバの設定, on page 486](#)を参照してください。
- Cisco Secure Endpoint マルウェア分析アプライアンスをプライベートクラウドのファイル分析サーバーとして使用する場合は、[オンプレミスのファイル分析サーバの設定, on page 487](#)を参照してください。

### Procedure

- ステップ 1 [セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] を選択します。
- ステップ 2 [グローバル設定を編集 (Edit Global Settings)] をクリックします。
- ステップ 3 [ファイルレピュテーションフィルタを有効にする (Enable File Reputation Filtering)] をクリックし、必要に応じて [ファイル分析を有効にする (Enable File Analysis)] をクリックします。

- [ファイルレピュテーションフィルタを有効にする (Enable File Reputation Filtering)] をオンにする場合、[ファイルレピュテーションサーバ (File Reputation Server)] セクションを設定するために (ステップ 6)、外部パブリックレピュテーションクラウドサーバの URL を入力するか、プライベートレピュテーションクラウドサーバの接続情報を入力する必要があります。
- 同様に、[ファイル分析を有効にする (Enable File Analysis)] をオンにする場合、[ファイル分析サーバの URL (File Analysis Server URL)] セクションを設定するために (ステップ 7)、外部クラウドサーバの URL を入力するか、プライベート分析クラウドの接続情報を入力する必要があります。

**Note**

新しいファイルタイプがアップグレード後に追加される場合がありますが、デフォルトでは有効になっていません。ファイル分析を有効にしており、新しいファイルタイプを分析に含めることが必要な場合には、それらを有効にする必要があります。

**ステップ 4** ライセンス契約が表示された場合は、それに同意します。

**ステップ 5** [ファイル分析 (File Analysis)] セクションで、適切なファイルグループ (たとえば、「Microsoft Documents」) からファイル分析のために送信する必要があるファイルタイプを選択します。

サポートされるファイルタイプについては、次のドキュメントの説明を参照してください。 [ファイルレピュテーションおよび分析サービスでサポートされるファイル](#), on page 480

**ステップ 6** [ファイルレピュテーションの詳細設定 (Advanced Settings for File Reputation)] パネルを展開し、必要に応じて以下のオプションを調整します。

| オプション                   | 説明                            |
|-------------------------|-------------------------------|
| クラウドドメイン (Cloud Domain) | ファイルレピュテーションクエリーに使用するドメインの名前。 |

| オプション                                    | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ファイルレピュテーションサーバ (File Reputation Server) | <p>パブリックレピュテーションクラウドサーバまたはプライベートレピュテーションクラウドクラウドのホスト名を選択します。</p> <p>プライベートレピュテーションクラウドを選択する場合は、次の情報を入力します。</p> <ul style="list-style-type: none"> <li>• [コンソールのホスト名 (Console Hostname)] - Cisco Secure Endpoint プライベートクラウドアプライアンスのコンソールのホスト名。</li> <li>• [アクティベーションコード (Activation Code)] - Cisco Secure Endpoint プライベートクラウドアプライアンスのアクティベーションコード。</li> <li>• [認証局 (Certificate Authority)] : ドロップダウンリストから認証局を選択します。 <ul style="list-style-type: none"> <li>• [シスコのデフォルト認証局を使用する (Use Cisco Default Certificate Authority)] : サーバーのデフォルト認証局を使用する場合は、このオプションを選択します。</li> <li>• [アップロードした認証局を使用する (Use Uploaded Certificate Authority)] : サーバーのカスタム認証局を使用する場合は、このオプションを選択します。</li> </ul> </li> </ul> <p>コンソールのホスト名とアクティベーションコードを取得する方法の詳細については、<a href="#">Cisco Secure Endpoint プライベートクラウドのドキュメント</a>を参照してください。</p> <p><b>Note</b><br/> ファイルレピュテーションのSSL通信を実行するには、CLI コマンド <code>certconfig &gt; CERTAUTHORITY &gt; CUSTOM</code>、または Web インターフェイスの [ネットワーク (Network)] &gt; [証明書 (カスタム認証局) (Certificates (Custom Certificate Authorities))] を使用して、AMP オンプレミスレピュテーションサーバ CA 証明書をこのアプライアンスの証明書ストアに追加する必要があります。この証明書は、Cisco Secure Endpoint プライベートクラウドアプライアンスから取得します ([統合 (Integrations)] &gt; [Cisco Secure Web Appliance] &gt; [バージョン15.2.4以降 (Version 15.2.4 and above)] &gt; [SSL 構成 (SSL Configuration)] &gt; [ダウンロード (download)] )。</p> |
| AMP for Endpoints コンソールの統合               | <p>お使いのアプライアンスを AMP for Endpoints コンソールと統合するには、[AMP for Endpoints コンソールでのアプライアンスの登録 (Register the Appliance with Secure Endpoint AMP for Endpoints console)] をクリックします。詳細な手順については、<a href="#">AMP for Endpoints コンソールとアプライアンスの統合, on page 471</a>を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ファイルレピュテーションのプロキシ設定                      | <p>アップストリームプロキシを設定するには、適切な [サーバー (Server)]、[ポート (Port)]、[ユーザー名 (Username)]、および [パスフレーズ (Passphrase)] の情報を入力します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| オプション                                               | 説明                                             |
|-----------------------------------------------------|------------------------------------------------|
| ハートビート間隔<br>(Heartbeat Interval)                    | レトロスペクティブなイベントを確認するための ping の送信頻度（分単位）。        |
| クエリー タイムアウト<br>(Query Timeout)                      | レピュテーション クエリーがタイムアウトになるまでの経過秒数。                |
| ファイル レピュテーション クライアント ID (File Reputation Client ID) | ファイル レピュテーション サーバ上のこのアプライアンスのクライアント ID（読み取り専用） |

**Note**

このセクションの他の設定は、シスコのサポートのガイダンスなしに変更しないでください。

- ステップ 7** ファイル分析にクラウドサービスを使用する場合は、[ファイル分析の詳細設定（Advanced Settings for File Analysis）] パネルを展開し、必要に応じて次のオプションを調整します。

| オプション                                           | 説明 |
|-------------------------------------------------|----|
| ファイル分析サーバの<br>URL (File Analysis Server<br>URL) |    |

| オプション | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>外部クラウド サーバの名前（URL）、または [プライベート分析クラウド（Private analysis cloud）] を選択します。</p> <p>外部クラウド サーバを指定する場合、アプライアンスに物理的に近いサーバを選択します。新たに使用可能になったサーバは、標準の更新プロセスを使用して、このリストに定期的に追加されます。</p> <p>ファイル分析にオンプレミス Cisco Secure Endpoint マルウェア分析アプライアンスを使用するプライベート分析クラウドを選択し、次の情報を入力します。</p> <ul style="list-style-type: none"> <li>• [TG サーバー（TG Servers）]：スタンドアロンの、またはクラスタ化された Cisco Secure Endpoint マルウェア分析アプライアンスの IPv4 アドレスまたはホスト名を入力します。最大 7 つの Cisco Secure Endpoint マルウェア分析アプライアンスを追加できます。</li> </ul> <p><b>Note</b><br/>シリアル番号は、スタンドアロンまたはクラスタ化された Cisco Secure Endpoint マルウェア分析アプライアンスの追加順序を示しています。アプライアンスの優先順位を示すものではありません。</p> <p><b>Note</b><br/>1 つのインスタンスにスタンドアロンサーバーとクラスタサーバーを追加することはできません。スタンドアロンまたはクラスタのいずれかである必要があります。</p> <p>1 つのインスタンスに追加できるスタンドアロンサーバーは 1 つだけです。クラスタモードの場合、最大 7 台まで複数のサーバーを追加でき、すべてのサーバーが同じクラスタに属している必要があります。複数のクラスタを追加することはできません。</p> <ul style="list-style-type: none"> <li>• [認証局（Certificate Authority）]：[シスコのデフォルト認証局を使用する（Use Cisco Default Certificate Authority）] または [アップロードした認証局を使用する（Use Uploaded Certificate Authority）] を選択します。</li> </ul> <p>[アップロードした認証局を使用する（Use Uploaded Certificate Authority）] を選択する場合、[参照（Browse）] をクリックし、このアプライアンスとプライベート クラウド アプライアンスとの間の暗号化通信に使用する有効な証明書ファイルをアップロードします。これは、プライベートクラウド サーバで使用される証明書と同じである必要があります。</p> <p><b>Note</b><br/>ファイル分析のためにアプライアンスで Cisco Secure Endpoint マルウェア分析ポータルを設定している場合は、Cisco Secure Endpoint マルウェア分析ポータル (<a href="https://panacea.threatgrid.eu">https://panacea.threatgrid.eu</a> など) にアクセスし、ファイル分析用に送信されたファイルを表示および追跡できます。Cisco Secure Endpoint マルウェア分析ポータルにアクセスする方法については、Cisco TAC にお問い合わせ</p> |

| オプション                                     | 説明                                                                                                                                                                                |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | 合わせください。                                                                                                                                                                          |
| プロキシの設定 (Proxy Settings)                  | 別のアップストリームプロキシを設定するには、[ファイルレピュテーションプロキシを使用する (Use File Reputation Proxy)] チェックボックスをオフにして、適切な [サーバー (Server)]、[ポート (Port)]、[ユーザー名 (Username)]、および [パスフレーズ (Passphrase)] の情報を入力します。 |
| ファイル分析クライアント ID (File Analysis Client ID) | ファイル分析サーバ上のこのアプライアンスのクライアント ID (読み取り専用)                                                                                                                                           |

**ステップ 8** (オプション) ファイルレピュテーション判定結果の値にキャッシュ有効期限を設定する場合は、[キャッシュ設定 (Cache Settings)] パネルを展開します。

**ステップ 9** 許容されるファイル分析スコアの上限を設定するには、[しきい値の設定 (Threshold Settings)] パネルを展開します。スコアがこのしきい値を超えた場合は、ファイルが感染していることを示しています。次のいずれかのオプションを選択します。

- クラウドサービスの値を使用 (95) (Use value from Cloud Service (60))
- [カスタム値の入力 (Enter Custom Value)] : デフォルトでは 95 に設定されます。

#### Note

- [しきい値設定 (Threshold Settings)] オプションは、[レピュテーションしきい値 (Reputation Threshold)] ではなく [ファイル分析しきい値 (File Analysis Threshold)] として分類されるようになりました。
- AsyncOS 15.2.4 リリース以降、[しきい値設定 (Threshold Settings)] パネルは無効になっています。したがって、AMP しきい値設定を構成することはできません。詳細については、[ファイル処理の概要](#), on page 478 を参照してください。

**ステップ 10** 変更を送信し、保存します。

**ステップ 11** オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用している場合は、Cisco Secure Endpoint マルウェア分析アプライアンスでこのアプライアンスのアカウントをアクティブ化します。

「ユーザー」アカウントをアクティブ化するための詳細な手順は、Cisco Secure Endpoint マルウェア分析のドキュメントで説明しています。

- ページセクションの下部に表示されたファイル分析クライアント ID を書き留めます。ここにはアクティブ化する「ユーザ」が表示されます。
- Cisco Secure Endpoint マルウェア分析アプライアンスにサインインします。
- [ようこそ... (Welcome...)] > [ユーザの管理 (Manage Users)] を選択し、[ユーザの詳細 (User Details)] に移動します。
- Secure Web Appliance のファイル分析クライアント ID に基づいて「ユーザー」アカウントを見つけます。

- e) アプライアンスの「ユーザ」アカウントをアクティブにします。

## 重要：ファイル分析設定に必要な変更

新しいパブリック クラウド ファイル分析サービスを使用する場合は、次の説明を読み、データセンターの分離を維持するようにしてください。

- 既存のアプライアンスのグループ化情報は、新しいファイル分析サーバには保存されません。新しいファイル分析サーバでアプライアンスを再グループ化する必要があります。
- ファイル分析隔離エリアに隔離されたメッセージは、保存期間が経過するまで保存されます。隔離エリアでの保存期間が経過すると、メッセージはファイル分析隔離エリアから解放され、AMP エンジンによって再スキャンされます。その後、ファイルは分析のために新しいファイル分析サーバにアップロードされますが、メッセージがもう一度ファイル分析隔離エリアに送信されることはありません。

詳細については、<https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html> から Cisco AMP マルウェア分析のドキュメントを参照してください。

## (パブリック クラウド ファイル分析サービスのみ) アプライアンス グループの設定

組織のすべてのコンテンツ セキュリティ アプライアンスで、組織内の任意のアプライアンスから分析用に送信されるファイルに関するクラウド内の分析結果の詳細が表示されるようにするには、すべてのアプライアンスを同じアプライアンスグループに結合する必要があります。



### Note

マシンレベルでアプライアンスのグループを設定できます。アプライアンスのグループは、クラスタ レベルで設定することはできません。

## Procedure

**ステップ 1** [セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] を選択します。

**ステップ 2** (電子メールゲートウェイでスマートライセンスが無効になっている場合に適用) [アプライアンスID/名前 (Appliance ID/Name)] フィールドにグループ ID を手動で入力し、[今すぐグループ化 (Group Now)] をクリックします。

または

(電子メールゲートウェイでスマートライセンスが有効になっている場合に適用) システムによりスマートアカウント ID がグループ ID として自動的に登録され、[アプライアンスグループID/名前 (Appliance Group ID/Name)] フィールドに表示されます。

注：



- アプライアンスは1つのグループだけに属することができます。
- マシンはいつでもグループに追加できます。
- マシンレベルまたはクラスタレベルでアプライアンスのグループを設定できます。
- これがグループに追加されている最初のアプライアンスである場合、グループにわかりやすいIDを指定します。このIDは大文字と小文字が区別され、スペースを含めることはできません。
- アプライアンスグループIDは、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。ただし、IDはグループ内の以降のアプライアンスでは検証されません。
- アプライアンスグループIDを更新すると、変更はすぐに有効になります。確定は必要ありません。
- グループ内のすべてのアプライアンスがクラウド内の同じファイル分析サーバーを使用するように設定する必要があります。
- スマートライセンシングが有効になっている場合、アプライアンスはスマートアカウントIDを使用してグループ化されます。

**ステップ3** [ファイル分析クラウドレポートのためのアプライアンスのグループ化 (Appliance Grouping for File Analysis Cloud Reporting)] セクションで、ファイル分析クラウドレポートグループIDを入力します。

- これがグループに追加されている最初のアプライアンスである場合、グループにわかりやすいIDを指定します。
- このIDは大文字と小文字が区別され、スペースを含めることはできません。
- 指定したIDは、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。ただし、IDは以降のグループアプライアンスでは検証されません。
- 不正なグループIDを入力したか、または他の何らかの理由でグループIDを変更する必要がある場合は、Cisco TAC に問い合わせる必要があります。
- この変更はすぐに反映されます。コミットする必要はありません。
- グループ内のすべてのアプライアンスがクラウド内の同じファイル分析サーバを使用するように設定する必要があります。
- アプライアンスは1つのグループだけに属することができます。
- いつでもグループにマシンを追加できますが、追加できるのは一度のみです。

**ステップ4** [アプライアンスをグループに追加 (Add Appliance to Group)] をクリックします。

## 分析グループ内のアプライアンスの確認

### Procedure

**ステップ1** [セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] を選択します。

**ステップ 2** [ファイル分析クラウド レポートの用のアプライアンスのグループ化 (Appliance Grouping for File Analysis Cloud Reporting)] セクションで、[グループ内のアプライアンスの表示 (View Appliances in Group)] をクリックします。

**ステップ 3** 特定のアプライアンスのファイル分析クライアント ID を表示するには、以下の場所を参照します。

| アプライアンス              | ファイル分析クライアント ID の場所                                                                                                                                  |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| E メール セキュリティ アプライアンス | [セキュリティ サービス (Security Services)] > [ファイル レピュテーションと分析 (File Reputation and Analysis)] ページの [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクション |
| Secure Web Appliance | [セキュリティ サービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] ページの [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクション  |
| セキュリティ管理アプライアンス      | [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] ページの下部                                |

## アクセス ポリシーごとのファイル レピュテーションおよび分析サービスのアクションの設定

### Procedure

**ステップ 1** [Web セキュリティ マネージャ (Web Security Manager)] > [アクセス ポリシー (Access Policies)] を選択します。

**ステップ 2** テーブルの [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] 列にあるポリシーのリンクをクリックします。

**ステップ 3** [高度なマルウェア防御設定 (Advanced Malware Protection Settings)] セクションで、[ファイル レピュテーション フィルタリングとファイル分析を有効にする (Enable File Reputation Filtering and File Analysis)] を選択します。

ファイル分析がグローバルにイネーブルになっていない場合、ファイルレピュテーションフィルタだけが提供されます。

**ステップ 4** [悪意のある既知の高リスク ファイル (Known Malicious and High-Risk Files)] に対してアクション ([モニタ (Monitor)] または [ブロック (Block)]) を選択します。

デフォルトは [モニタリング (Monitor)] です。

**ステップ 5** 変更を送信し、保存します。

## Advanced Malware Protection の問題に関するアラートの確実な受信

Advanced Malware Protectionに関連するアラートを送信するようにアプライアンスが設定されていることを確認します。

以下の場合にアラートを受信します。

| アラートの説明                                                                                                                                              | タイプ            | 重大度         |
|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------|
| オンプレミス（プライベートクラウド）の Cisco Secure Endpoint マルウェア分析アプライアンスへの接続をセットアップし、「 <a href="#">ファイルレピュテーションと分析サービスの有効化と設定</a> 」に説明されているようにアカウントをアクティブ化する必要があります。 | マルウェア対策        | 警告（Warning） |
| 機能キーが期限切れになりました                                                                                                                                      | （すべての機能に対する標準） |             |
| ファイル レピュテーションまたはファイル分析サービスに到達できません。                                                                                                                  | マルウェア対策        | 警告（Warning） |
| クラウドサービスとの通信が確立されました。                                                                                                                                | マルウェア対策        | 情報（Info）    |
|                                                                                                                                                      |                | 情報（Info）    |
| ファイル レピュテーションの判定が変更されました。                                                                                                                            | マルウェア対策        | 情報（Info）    |
| 分析用に送信できるファイル タイプが変更された。新しいファイル タイプのアップロードをイネーブルにできます。                                                                                               | マルウェア対策        | 情報（Info）    |
| 一部のファイル タイプの分析が一時的に利用できません。                                                                                                                          | マルウェア対策        | 警告（Warning） |
| サポートされているすべてのファイル タイプの分析が一時停止後に復旧されます。                                                                                                               | マルウェア対策        | 情報（Info）    |
| 無効なファイル分析サービスキーです。このエラーを修正するには、Cisco TAC にファイル分析IDの詳細を連絡する必要があります。                                                                                   | AMP            | エラー（Error）  |

### 関連項目

- [ファイル レピュテーション サーバまたはファイル分析サーバへの接続失敗に関する各種アラート](#) , on page 504
- [ファイルの脅威判定の変更時のアクションの実行](#) , on page 503

## Advanced Malware Protection 機能の集約管理レポートの設定

セキュリティ管理アプライアンスでレポートを集約管理する場合は、管理アプライアンスに関するオンラインヘルプまたはユーザーガイドの Web レポーティングのトピックの「Advanced Malware Protection」セクションで、重要な設定要件を確認してください。

## ファイルレピュテーションおよびファイル分析のレポートとトラッキング

- [SHA-256 ハッシュによるファイルの識別](#) , on page 499
- [ファイルレピュテーションとファイル分析レポートのページ](#) , on page 500
- [その他のレポートでのファイルレピュテーションフィルタデータの表示](#) , on page 501
- [Web トラッキング機能と Advanced Malware Protection 機能について](#) , on page 502

### SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム (SHA-256) を使用して各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイル进行处理する場合、すべてのインスタンスが同じ SHA-256 として認識されます。複数のアプライアンスが同じファイル进行处理する場合、ファイルのすべてのインスタンスには同じ SHA-256 ID があります。

ほとんどのレポートでは、ファイルはその SHA-256 値でリストされます (短縮形式)。組織のマルウェアインスタンスに関連付けられたファイル名を特定するには、[レポート (Reporting)] > [高度なマルウェア防御 (Advanced Malware Protection)] を選択し、テーブルの SHA-256 リンクをクリックします。関連付けられたファイル名が詳細ページに表示されます。

## ファイルレピュテーションとファイル分析レポートのページ

| レポート                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advanced Malware Protection | <p>ファイルレピュテーションサービスによって特定されたファイルベースの脅威を示します。</p> <p>判定が変更されたファイルについては、[AMP 判定のアップデート (AMP Verdict Updates)] レポートを参照してください。これらの判定は、[高度なマルウェア防御 (Advanced Malware Protection)] レポートに反映されません。</p> <p>圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御 (Advanced Malware Protection)] レポートに含まれます。</p> <p>[カテゴリ別受信マルウェアファイル (Incoming Malware Files by Category)] セクションは、[カスタム検出 (Custom Detection)] に分類される、AMP for Endpoints コンソールから受信したブロックリストに登録されたファイル SHA の割合を示しています。</p> <p>AMP for Endpoints コンソールから取得されるブロックリストに登録されているファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル (Incoming Malware Threat Files)] セクションで [シンプルカスタム検出 (Simple Custom Detection)] として表示されます。</p> <p>レポートの [詳細 (More Details)] セクションでリンクをクリックすると、AMP for Endpoints コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリ詳細を表示できます。</p> <p>[リスク低 (Low Risk)] 判定の詳細をレポートの [AMP により渡された受信ファイル (Incoming Files Handed by AMP)] セクションに表示できます。</p> |

| レポート                                                 | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advanced Malware Protection [ファイル分析 (File Analysis)] | <p>分析用に送信された各ファイルの時間と判定（または中間判定）を表示します。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。</p> <p>1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。</p> <p>ドリルダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。</p> <p>SHA に関するその他の情報を検索するか、またはファイル分析詳細ページの下部のリンクをクリックして、ファイルを分析したサーバに関する追加の詳細を表示することもできます。</p> <p>(注)<br/>圧縮/アーカイブ ファイルから抽出したファイルが分析用に送信される場合は、それらの抽出ファイルの SHA 値だけが [ファイル分析 (File Analysis)] レポートに含まれます。</p>                                                                                           |
| Advanced Malware Protection レピュテーション                 | <p>Advanced Malware Protection は対象を絞ったゼロデイ脅威に焦点を当てるため、集約データでより詳細な情報が提供されると、脅威の判定が変わる可能性があります。</p> <p>[ AMP レピュテーション (AMP Reputation) ] レポートには、このアプライアンスで処理され、メッセージ受信後に判定が変わったファイルが表示されます。この状況の詳細については、<a href="#">ファイル脅威判定のアップデート (478 ページ)</a> を参照してください。</p> <p>1000 を超える判定アップデートを表示するには、データを .csv ファイルとしてエクスポートします。</p> <p>1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。</p> <p>使用可能な最大時間範囲内（レポートに選択された時間範囲に関係なく）に特定の SHA-256 の影響を受けるすべてのメッセージを表示するには、SHA-256 リンクをクリックします。</p> |

## その他のレポートでのファイル レピュテーション フィルタ データの表示

該当する場合は、ファイルレピュテーションおよびファイル分析のデータを他のレポートでも使用できます。デフォルトでは、[高度なマルウェア防御でブロック (Blocked by Advanced

Malware Protection) ] 列は適用可能なレポートに表示されません。追加列を表示するには、テーブルの下 [列 (Columns) ] リンクをクリックします。

[ユーザーの場所別のレポート (Report by User Location) ] には [高度なマルウェア防御 (Advanced Malware Protection) ] タブがあります。

## Web トラッキング機能と Advanced Malware Protection 機能について

Web トラッキングでファイル脅威情報を検索するときには、以下の点に注意してください。

- ファイル レピュテーション サービスにより検出された悪意のあるファイルを検索するには、Web メッセージトラッキングの [詳細設定 (Advanced) ] セクションの [マルウェア脅威 (Malware Threat) ] エリアの [マルウェア カテゴリでフィルタ (Filter by Malware Category) ] オプションで [既知の悪意のある、リスクが高いファイル (Known Malicious and High-Risk Files) ] を選択します。
- Web トラッキングには、ファイルレピュテーション処理に関する情報と、トランザクションメッセージの処理時点で戻された元のファイル レピュテーション判定だけが含まれます。たとえば最初にファイルがクリーンであると判断され、その後、判定のアップデートでそのファイルが悪質であると判断された場合、クリーンの判定のみがトラッキング結果に表示されます。

クリーンな添付ファイルおよびスキャンできない添付ファイルの情報は表示されません。

検索結果の [ブロック - AMP (Block - AMP) ] は、ファイルのレピュテーション判定が原因でトランザクションがブロックされたことを意味します。

トラッキングの詳細に表示される [AMP 脅威スコア (AMP Threat Score) ] は、ファイルを明確に判定できないときにクラウドレピュテーションサービスが提示するベストエフォート型のスコアです。この場合、スコアは1~100です。(AMP判定が返された場合、またはスコアがゼロの場合は[AMP脅威スコア (AMP Threat Score) ] を無視してください)。アプライアンスはこのスコアをしきい値スコア ([セキュリティサービス (Security Services) ] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] ページで設定) と比較して、実行するアクションを決定します。デフォルトでは、スコアが 60 ~ 100 の場合に悪意のあるファイルと見なされます。デフォルトのしきい値スコアの変更は推奨されません。WBRSスコアは、ファイルのダウンロード元サイトのレピュテーションであり、ファイル レピュテーションとは関係ありません。



**Note** AsyncOS 15.2.4以降、[セキュリティサービス (Security Services) ] > [マルウェア対策とレピュテーション設定 (Anti Malware and Reputation Settings) ] > [ファイル分析 (File Analysis) ] > [詳細 (Advanced) ] にあるしきい値の設定は無効になっています。アプライアンスは、AMP 脅威スコアをしきい値スコア ([セキュリティサービス (Security Services) ] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] ページで設定) と比較して、実行するアクションを決定しなくなります。詳細については、[ファイル処理の概要](#) , on page 478を参照してください。

- 判定の更新は [ AMP 判定の更新 (AMP Verdict Updates) ] レポートだけに表示されます。Web トラッキングの元のトランザクションの詳細は、判定の変更によって更新されません。特定のファイルに関連するトランザクションを確認するには、判定アップデートレポートで SHA-256 リンクをクリックします。
- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析 (File Analysis) ] レポートにのみ表示されます。

分析済みファイルのその他の情報は、クラウドまたはオンプレミスのファイル分析サーバーから入手できます。ファイルについて使用可能なすべてのファイル分析情報を確認するには、[レポート (Reporting) ] > [ファイル分析 (File Analysis) ] を選択し、ファイルで検索する SHA-256 を入力するか、または Web トラッキングの詳細で SHA-256 リンクをクリックします。ファイル分析サービスによってソースのファイルが分析されると、その詳細を表示できます。分析されたファイルの結果だけが表示されます。

分析目的で送信されたファイルの後続インスタンスがアプライアンスにより処理される場合、これらのインスタンスは、Web トラッキング検索結果に表示されます。

## ファイルの脅威判定の変更時のアクションの実行

### Procedure

- ステップ 1 [ AMP 判定の更新 (AMP Verdict updates) ] レポートを表示します。
- ステップ 2 該当する SHA-256 リンクをクリックします。エンドユーザーに対してアクセスが許可されていたファイルに関連するすべてのトランザクションの Web トラッキング データが表示されます。
- ステップ 3 トラッキング データを使用して、侵害された可能性があるユーザーと、違反に関連するファイルの名前やファイルのダウンロード元 Web サイトなどの情報を特定します。
- ステップ 4 ファイルの脅威の動作を詳細に把握するために、[ファイル分析 (File Analysis) ] レポートを検証して、この SHA-256 が分析用に送信されたかどうかを確認します。

### What to do next

#### 関連項目

[ファイル脅威判定のアップデート](#) , on page 478

## ファイル レピュテーションと分析のトラブルシューティング

- [ログ ファイル](#) , on page 504
- [ファイル レピュテーション サーバまたはファイル分析サーバへの接続失敗に関する各種アラート](#) , on page 504
- [API キーのエラー \(オンプレミスのファイル分析\)](#) , on page 505
- [ファイルが予想どおりにアップロードされない](#) , on page 505



- クラウド内のファイル分析の詳細が完全でない, [on page 506](#)
- 分析のために送信できるファイル タイプに関するアラート, [on page 506](#)

## ログ ファイル

ログの説明：

- AMP と amp は、ファイル レピュテーション サービスまたはエンジンを示しています。
- Retrospective は判定のアップデートを示しています。
- VRT と sandboxing はファイル分析サービスを示しています。

ファイル分析を含む Advanced Malware Protectionに関する情報は、アクセスログまたは AMP エンジンのログに記録されます。詳細については、ログによるシステムアクティビティのモニタリングに関するトピックを参照してください。

ログ メッセージ「ファイル レピュテーション クエリーに対する受信応答 (Response received for file reputation query)」の「アップロードアクション (upload action)」の値は以下のようになります。

- 1：送信。(1: SEND.) この場合、ファイル分析のためにファイルを送信する必要があります。
- 2：送信しない。(2: DON'T SEND.) この場合は、ファイル分析用にファイルを送信しません。
- 3：メタデータのみを送信。(3: SEND ONLY METADATA.) この場合、ファイル分析のためにファイル全体ではなく、メタデータのみを送信します。
- 0：アクションなし。(0: NO ACTION.) この場合、他のアクションは不要です。

## ファイル レピュテーション サーバまたはファイル分析サーバへの接続失敗に関する各種アラート

### 問題

ファイル レピュテーション サービスまたは分析サービスへの接続の失敗に関するアラートをいくつか受信した。(単一のアラートは一時的な問題のみを示していることがあります。)

### 解決方法

- [ファイル レピュテーションと分析サービスとの通信の要件, on page 483](#)に記載されている要件を満たしていることを確認します。
- アプライアンスとクラウドサービスとの通信を妨げている可能性があるネットワークの問題を確認します。
- [クエリー タイムアウト (Query Timeout)] の値を大きくします。  
[セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] を選択します。[高度なマルウェア防御サービス (Advanced

Malware Protection Services) ] セクションの [詳細設定 (Advanced settings) ] エリアの [クエリタイムアウト (Query Timeout) ] の値。

## API キーのエラー（オンプレミスのファイル分析）

### 問題

ファイル分析レポートの詳細を表示しようとした場合や、分析用ファイルをアップロードするのに Secure Web Appliance が AMP マルウェア分析サーバーに接続できない場合、API キーのアラートを受信します。

### 解決方法

このエラーは、AMP マルウェア分析サーバーのホスト名を変更し、AMP マルウェア分析サーバーの自己署名証明書を使用する場合に発生します。また、他の状況でも発生する可能性があります。この問題を解決するには、次の手順を実行します。

- 新しいホスト名がある AMP マルウェア分析アプライアンスから新しい証明書を生成します。
- Secure Web Appliance に新しい証明書をアップロードします。
- AMP マルウェア分析アプライアンスの API キーをリセットします。手順については、AMP マルウェア分析アプライアンスのオンラインヘルプを参照してください。

### 関連項目

- [ファイル レピュテーションと分析サービスの有効化と設定, on page 488](#)

## ファイルが予想どおりにアップロードされない

### 問題

ファイルが予想どおりに評価または分析されていません。アラートまたは明らかなエラーはありません。

### 解決方法

以下の点に注意してください。

- ファイルが他のアプライアンスによる分析用に送信されているために、すでにファイル分析サーバー、またはそのファイルを処理するアプライアンスのキャッシュに存在している可能性があります。
- [セキュリティ サービス (Security Services) ] > [マルチウェア対策とレピュテーション (Anti-Malware and Reputation) ] ページの [DVS エンジン オブジェクト スキャンの制限 (DVS Engine Object Scanning Limits) ] ページで設定した最大ファイルサイズの制限を確認します。この制限は Advanced Malware Protection 機能に適用されます。

## クラウド内のファイル分析の詳細が完全でない

### 問題

パブリック クラウド内の完全なファイル分析結果は、組織のその他の Secure Web Appliance からアップロードされたファイルでは取得できません。

### 解決方法

ファイルの分析結果データを共有するすべてのアプライアンスをグループ化してください。  
(パブリック クラウド ファイル分析サービスのみ) [アプライアンス グループの設定](#), on page 495を参照してください。この設定は、グループの各アプライアンスで実行する必要があります。

## 分析のために送信できるファイル タイプに関するアラート

### 問題

ファイル分析のために送信できるファイルタイプに関する重大度情報のアラートを受け取れます。

### 解決方法

このアラートは、サポート対象のファイル タイプが変更された場合や、アプライアンスがサポート対象のファイルタイプを確認した場合に送信されます。これは、以下の場合に発生する可能性があります。

- 自分または別の管理者が分析用に選択されているファイル タイプを変更した。
- サポート対象のファイル タイプがクラウド サービスでの可用性に基づいて一時的に変更された。この場合、アプライアンスで選択されたファイルタイプのサポートは可能な限り迅速に復旧されます。どちらのプロセスも動的であり、ユーザによる操作は必要ありません。
- アプライアンスが再起動した（たとえば、AsyncOS のアップグレードの一環として）。

## Web アプリケーションへのアクセスの管理

この章で説明する内容は、次のとおりです。

- [Web アプリケーションへのアクセスの管理：概要](#)（507 ページ）
- [AVC または ADC エンジン](#)を有効にする（508 ページ）
- [アプリケーション制御のポリシー設定](#)（509 ページ）
- [帯域幅の制御](#)（513 ページ）
- [インスタント メッセージ トラフィックの制御](#)（516 ページ）
- [AVC または ADC アクティビティの表示](#)（517 ページ）

## Web アプリケーションへのアクセスの管理：概要

Application Visibility and Control (AVC) または、Application Discovery and Control (ADC) エンジンを使用すると、各アプリケーションの基盤技術を完全に理解していなくても、ネットワーク上のアプリケーション アクティビティを制御するポリシーを作成できます。アクセス ポリシーグループのアプリケーション制御を設定できます。個々に、またはアプリケーションのタイプに応じて、アプリケーションをブロックまたは許可することができます。また、特定のアプリケーション タイプに制御を適用することも可能です。

アクセス ポリシーを使用して、以下の操作を実行できます。

- アプリケーションの動作やアクティビティ、またはきめ細かいゲインコントロールを制御します。

ADC には、きめ細かいゲインコントロール (FGC) または動作構成があります。複数のアプリケーションに対して FGC を設定できます。

- 特定のアプリケーション タイプで使用する帯域幅の量を制御する



**Note** これは、AVC にのみ適用されます。

- アプリケーションがブロックされたときにエンドユーザーに通知する
- インスタント メッセージ、ブログ、ソーシャル メディアのアプリケーションに制御を割り当てる
- 範囲要求の設定を指定する



**Note** これは、AVC にのみ適用されます。

AVC または ADC エンジンを使用してアプリケーションを制御するには、以下のタスクを実行します。

| タスク                               | タスクへのリンク                                                 |
|-----------------------------------|----------------------------------------------------------|
| AVC または ADC エンジンを実効にする            | <a href="#">AVC または ADC エンジンを実効にする, on page 508</a>      |
| アクセス ポリシー グループに制御を設定する            | <a href="#">アクセス ポリシー グループのアプリケーション管理設定, on page 512</a> |
| アプリケーションタイプが消費する帯域幅を制限して輻輳を制御する   | <a href="#">帯域幅の制御, on page 513</a>                      |
| <b>Note</b><br>これは、AVC にのみ適用されます。 |                                                          |

| タスク                                                  | タスクへのリンク                                            |
|------------------------------------------------------|-----------------------------------------------------|
| インスタント メッセージ トラフィックを許可し、インスタント メッセージングによるファイル共有を禁止する | <a href="#">インスタント メッセージ トラフィックの制御, on page 516</a> |

## AVC または ADC エンジン を有効にする

[使用許可コントロール (Acceptable Use Controls)] を有効にする場合は、AVC または ADC エンジン を有効にします。



**Note** [レポート (Reporting)] > [アプリケーションの表示 (Application Visibility)] ページの [アプリケーションの表示 (Application Visibility)] レポートで、AVC または ADC エンジンのスキャンアクティビティを確認できます。

### What to do next

#### 関連項目

- [アプリケーション エンジンとデフォルトのアクション, on page 508](#)
- [要求が AVC または ADC エンジンによりブロックされた場合のユーザー体験, on page 509](#)

## アプリケーション エンジンとデフォルトのアクション

AsyncOS は定期的にアップデート サーバーに問い合わせ、AVC エンジンを含めたすべてのセキュリティ サービス コンポーネントについて新しいアップデートの有無を確認します。AVC エンジンのアップデートには、新しいアプリケーションタイプやアプリケーションに対するサポートが含まれることがあります。また、アプリケーションの動作が変更された場合は、既存のアプリケーションに対するサポートも更新されます。AsyncOS バージョンの更新に合わせて AVC エンジンを更新することにより、サーバをアップグレードすることなく、Secure Web Applianceの柔軟性が保たれます。

AsyncOS for Web は、グローバル アクセス ポリシーに以下のデフォルト アクションを割り当てます。

- 新しいアプリケーションタイプのデフォルトアクションは、[モニター (Monitor)] です。
- 特定アプリケーション内のブロック ファイル転送などの新しいアプリケーション動作のデフォルト設定は、[モニター (Monitor)] です。
- 既存のアプリケーションタイプの新しいアプリケーションのデフォルトアクションは、そのアプリケーション タイプのデフォルト アクションです。



**Note** グローバルアクセスポリシーでは、各アプリケーションタイプのデフォルトアクションを設定できます。これによって、AVC または ADC エンジンのアップデートにより導入された新しいアプリケーションは、指定されたデフォルトアクションを自動的に継承します。「[アクセスポリシー グループのアプリケーション管理設定, on page 512](#)」を参照してください。

## 要求が AVC または ADC エンジンによりブロックされた場合のユーザー体験

AVC または ADC エンジンによってトランザクションがブロックされると、Web プロキシはエンドユーザーにブロックページを送信します。ただし、すべての Web サイトでブロック ページが表示されるわけではありません。多くの Web サイトでは、静的 Web ページの代わりに JavaScript を使用して動的コンテンツが表示され、ブロック ページが表示されることはありません。そのような場合でも、ユーザーは適切にブロックされているので悪意のあるデータをダウンロードすることはありませんが、ブロックされていることが Web サイトから通知されない場合もあります。



**Note** HTTPS プロキシが無効で、Webroot が次の場合：

- [有効 (Enabled)] : AVC または ADC エンジンは起動する場合と起動しない場合があり、判定が返されます。トランザクションは、スキャナの判定に従って処理されます。
- [無効 (Disabled)] : AVC または ADC エンジンが起動し、判定が返されます。トランザクションは、AVC または ADC の判定に従って処理されます。

## アプリケーション制御のポリシー設定

アプリケーションを制御するには、以下の要素を設定する必要があります。

| オプション                              | 説明                                                                               |
|------------------------------------|----------------------------------------------------------------------------------|
| アプリケーション タイプ (Application Types)   | 1 つまたは複数のアプリケーションを含むカテゴリです。                                                      |
| アプリケーション (Applications)            | あるアプリケーションタイプに属している特定のアプリケーション。                                                  |
| アプリケーション動作 (Application behaviors) | 管理者が制御できるアプリケーション内でユーザーが実行できる特定のアクションまたは動作。すべてのアプリケーションに設定可能な動作が含まれているわけではありません。 |

アクセス ポリシー グループのアプリケーション制御を設定できます。[Web セキュリティ マネージャ (Web Security Manager)] > [アクセス ポリシー (Access Policies)] ページで、設定す

るポリシー グループの [アプリケーション (Applications)] リンクをクリックします。アプリケーションの設定時には、以下のアクションを選択できます。

| オプション                   | 説明                                                                                                                                                                                                                                              |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ブロック (Block)            | このアクションは、最終アクションです。ユーザーは Web ページを閲覧できなくなり、代わりにエンドユーザー通知ページが表示されます。<br><br><b>Note</b><br>アプリケーションがADC/AVCでブロックされるように設定されている場合、アプリケーションのすべてのサブカテゴリもブロックされます。特定のサブカテゴリは詳細なゲイン制御機能を使用してブロックできますが、この機能は smugmug、Facebook、LinkedIn などの特定のアプリに限定されます。 |
| モニター (Monitor)          | このアクションは、中間アクションです。Web プロキシは引き続きトランザクションを他の制御設定と比較して、適用する最終アクション決定します。                                                                                                                                                                          |
| 制限 (Restrict)           | このアクションは、アプリケーションの動作がブロックされることを示します。たとえば、特定のインスタントメッセージアプリケーションのファイル転送をブロックすると、そのアプリケーションのアクションは制限されます。                                                                                                                                         |
| 帯域幅制限 (Bandwidth Limit) | Media や Facebook などの特定のアプリケーションに対して、Web トラフィックで使用可能な帯域幅を制限できます。アプリケーション自体やそのアプリケーション ユーザーの帯域幅を制限できます。                                                                                                                                           |

#### 関連項目

- [範囲要求の設定 \(Range Request Settings\)](#) , on page 510
- [アプリケーション制御の設定のためのルールとガイドライン](#) , on page 511

## 範囲要求の設定 (Range Request Settings)

HTTP の範囲要求がディセーブルのときに大きなファイルが複数のストリームでダウンロードされる場合、統合されたパッケージがスキャンされます。これにより、大きなオブジェクトのダウンロードで使用するダウンロード管理ユーティリティやアプリケーションから、パフォーマンス上のメリットが得られなくなります。

代わりに、[範囲要求の転送 (Range Request Forwarding)] をイネーブルにすると ([Web プロキシの設定](#), on page 237 を参照)、着信する範囲要求の処理方法をポリシーごとに制御できます。このプロセスは「バイトサービング」と呼ばれ、大きなファイルの要求時に帯域幅を最適化するための方法です。

ただし、範囲要求の転送のイネーブル化は、ポリシーベースの Application Visibility and Control (AVC) の効率を妨げ、セキュリティを侵害する可能性があります。セキュリティ上の影響よ

りもメリットの方が重要な場合にのみ、十分に注意して HTTP の [範囲要求の転送 (Range Request Forwarding)] をイネーブルにしてください。



**Note** 範囲要求設定は、範囲要求転送が有効で、少なくとも 1 つのアプリケーションが [ブロック (Block)]、[制限 (Restrict)]、または [スロットル (Throttle)] に設定されている場合に使用できます。

| ポリシーの範囲要求の設定                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 範囲要求の設定<br>(Range Request Settings) | <ul style="list-style-type: none"> <li>• <b>範囲要求を転送しない</b>：クライアントは特定の範囲の要求を送信します。ただし、Secure Web Applianceは、ターゲットサーバーに送信する前に要求から範囲ヘッダーを削除します。次に Secure Web Applianceは、ファイル全体をスキャンし、バイト範囲をクライアントに送信します。</li> </ul> <p><b>Note</b><br/>クライアントが初めて範囲要求を送信すると、Secure Web Applianceはクライアントからの後続の範囲要求を想定して、ファイル全体を送信します。同じクライアントまたは別のクライアントからの後続の要求では、Secure Web Applianceは部分的なコンテンツのみをクライアントに配信します。</p> <ul style="list-style-type: none"> <li>• <b>範囲要求を転送する</b>：クライアントは特定の範囲の要求を送信します。Secure Web Applianceは、同じ要求をターゲットサーバーに送信し、部分的なコンテンツを受信してクライアントに返します。Secure Web Applianceは、スキャン結果が正確でない可能性がある部分的なコンテンツのみをスキャンします。</li> </ul> |
| 例外リスト<br>(Exception list)           | 現在の転送先の選択肢から除外する、トラフィックの宛先を指定できます。つまり、[範囲要求を転送しない (Do not forward range requests)] を選択した場合は、要求を転送する宛先を指定できます。同様に、[範囲要求を転送する (Forward range requests)] を選択した場合は、要求を転送しない宛先を指定できます。                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## アプリケーション制御の設定のためのルールとガイドライン

アプリケーション制御を設定する際は、以下のルールとガイドラインを考慮してください。

- サポートされるアプリケーションタイプ、アプリケーション、およびアプリケーション動作は、AsyncOS for Web のアップグレード間で、または AVC または ADC エンジンのアップデート後に変化する可能性があります。
- セーフサーチまたはサイトコンテンツレーティングを有効にすると、AVC エンジンが、安全なブラウジングのためのアプリケーションを特定する必要があります。条件の1つとして、AVC エンジン は応答本文をスキャンし、検索アプリケーションを検出します。その結果、アプライアンスは範囲ヘッダーを転送しません。



- [アプリケーションタイプ (Application Type)] リストでは、各アプリケーションタイプの要約にアプリケーションの最終アクションが一覧表示されますが、それらのアクションがグローバル ポリシーから継承されたものか、現在のアクセス ポリシーで設定されたものかについては示されません。特定のアプリケーションのアクションについて詳細を調べるには、そのアプリケーション タイプを展開します。
- グローバルアクセスポリシーでは、各アプリケーションタイプのデフォルトアクションを設定できます。これによって、AVC または ADC エンジンのアップデートにより導入された新しいアプリケーションは、デフォルトアクションを自動的に継承します。
- [参照 (Browse)] ビューでアプリケーションタイプの [すべてを編集 (edit all)] リンクをクリックすると、そのアプリケーションタイプに属するすべてのアプリケーションに同じアクションを簡単に設定できます。ただし、設定できるのは、アプリケーション動作のアクションではなく、アプリケーションのアクションだけです。アプリケーション動作を設定するには、アプリケーションを個別に編集する必要があります。
- [検索 (Search)] ビューでは、テーブルをアクション列でソートすると、最終アクションに基づいてテーブルが並べ替えられます。たとえば、[グローバル (ブロック) を使用 (Use Global (Block))] は [ブロック (Block)] の後に配置されます。
- 署名用ルート証明書がクライアントにインストールされていない場合は、復号により、アプリケーションでエラーが発生することがあります。

#### 関連項目

- [アクセス ポリシー グループのアプリケーション管理設定, on page 512](#)
- [全体の帯域幅制限の設定, on page 514](#)
- [AVC または ADC アクティビティの表示, on page 517](#)

## アクセス ポリシー グループのアプリケーション管理設定

### Procedure

- ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] を選択します。
- ステップ 2** ポリシー テーブルで、編集するポリシー グループの [アプリケーション (Applications)] 列にあるリンクをクリックします。
- ステップ 3** グローバル アクセス ポリシーを設定する場合：
  - a) [アプリケーションタイプのデフォルトアクション (Default Actions for Application Types)] セクションで、各アプリケーションタイプのデフォルトアクションを定義します。
  - b) ページの [アプリケーション設定を編集 (Edit Applications Settings)] セクションで、各アプリケーションタイプの各メンバーのデフォルトアクションを一括して、または個々に編集できます。個々のアプリケーションのデフォルトアクションを編集する手順は、以下のとおりです。

- ステップ 4** ユーザー定義のアクセス ポリシーを設定する場合は、[アプリケーション設定を編集 (Edit Applications Settings)] セクションで [アプリケーションのカスタム設定を定義 (Define Applications Custom Settings)] を選択します。
- ステップ 5** [アプリケーションの設定 (Application Settings)] 領域で、ドロップダウンメニューから [参照ビュー (Browse view)] または [検索ビュー (Search view)] を選択します。
- **[参照ビュー (Browse view)]**。アプリケーションタイプを参照できます。[参照ビュー (Browse view)] を使用すると、特定タイプのすべてのアプリケーションを同時に設定できます。[参照ビュー (Browse view)] でアプリケーションタイプが折りたたまれている場合は、アプリケーションタイプの要約にアプリケーションの最終アクションが一覧表示されます。ただし、それらのアクションがグローバルポリシーから継承されたものか、現在のアクセスポリシーで設定されたものかについては示されません。
  - **[検索ビュー (Search view)]**。名前によってアプリケーションを検索できます。すべてのアプリケーションのリストが長く、特定のアプリケーションをすばやく見つけて設定する必要がある場合は、[検索ビュー (Search view)] を使用します。
- ステップ 6** 各アプリケーションとアプリケーション動作のアクションを設定します。
- ステップ 7** 該当する各アプリケーションの帯域幅制御を設定します。
- ステップ 8** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## What to do next

### 関連項目

- [帯域幅の制御, on page 513](#)

## 帯域幅の制御

全体的な制限とユーザーの制限の両方をトランザクションに適用した場合は、最も制限の厳しいオプションが適用されます。URL カテゴリの ID グループを定義し、帯域幅を制限するアクセス ポリシーでそのグループを使用することにより、特定の URL カテゴリに対して帯域幅制限を定義できます。

以下の帯域幅制限を定義できます。

| 帯域幅制限 | 説明                                                                                                                                              | タスクへのリンク                                 |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| 全体    | サポートされるアプリケーションタイプに対して、ネットワーク上の全ユーザー向けの全体的制限を定義します。全体的な帯域幅制限は、Cisco Secure Web Appliance と Web サーバー間のトラフィックに影響を与えます。Web キャッシュからのトラフィックは制限されません。 | <a href="#">全体の帯域幅制限の設定, on page 514</a> |

| 帯域幅制限 | 説明                                                                                                     | タスクへのリンク                                   |
|-------|--------------------------------------------------------------------------------------------------------|--------------------------------------------|
| ユーザー  | アプリケーションタイプごとに、ネットワーク上の特定ユーザーに対する制限を定義します。ユーザーの帯域幅制限は、Web サーバーからのトラフィックだけでなく、Web キャッシュからのトラフィックも制限します。 | <a href="#">ユーザーの帯域幅制限の設定, on page 514</a> |



**Note** 帯域幅制限を定義しても、ユーザーへのデータ転送が遅くなるだけです。クォータに達したかどうかに基づいてデータがブロックされるわけではありません。Web プロキシによって各アプリケーションのトランザクションに遅延が生じ、サーバーへのリンクが減速したように見えます。

## 全体の帯域幅制限の設定

### Procedure

- ステップ 1 [Web セキュリティ マネージャ (Web Security Manager)] > [全体の帯域幅制限 (Overall Bandwidth Limits)] を選択します。
- ステップ 2 [設定の編集 (Edit Settings)] をクリックします。
- ステップ 3 [制限値 (Limit to)] オプションを選択します。
- ステップ 4 メガビット/秒 (Mbps) またはキロビット/秒 (kbps) 単位で、制限するトラフィック量を入力します。
- ステップ 5 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## ユーザーの帯域幅制限の設定

ユーザーの帯域幅制限を定義するには、アクセス ポリシーの Applications Visibility and Control ページで帯域幅制御を設定します。アクセスポリシーで、ユーザーに対して以下のタイプの帯域幅制御を定義できます。

| オプション                                                                      | 説明                                                                  | タスクへのリンク                                                 |
|----------------------------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------------------------|
| アプリケーション タイプのデフォルトの帯域幅制限 (Default bandwidth limit for an application type) | グローバルアクセスポリシーで、あるアプリケーションタイプに属するすべてのアプリケーションに対してデフォルトの帯域幅制限を定義できます。 | <a href="#">アプリケーション タイプのデフォルトの帯域幅制限の設定, on page 515</a> |

| オプション                                                        | 説明                                                                                             | タスクへのリンク                                                  |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| アプリケーション タイプの帯域幅制限 (Bandwidth limit for an application type) | ユーザー定義のアクセス ポリシーで、グローバルアクセス ポリシーで定義されたアプリケーション タイプのデフォルトの帯域幅制限を上書きすることができます。                   | <a href="#">アプリケーション タイプのデフォルトの帯域幅制限の無効化, on page 515</a> |
| アプリケーションの帯域幅制限 (Bandwidth limit for an application)          | ユーザー定義のアクセス ポリシーまたはグローバルアクセス ポリシーで、アプリケーション タイプの帯域幅制限を適用するか、制限しないか（アプリケーション タイプの制限を免除）を選択できます。 | <a href="#">アプリケーションの帯域幅制御の設定, on page 516</a>            |

## アプリケーション タイプのデフォルトの帯域幅制限の設定

### Procedure

- ステップ 1 [Webセキュリティマネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] を選択します。
- ステップ 2 ポリシー テーブルで、グローバル アクセス ポリシーの [アプリケーション (Applications)] 列にあるリンクをクリックします。
- ステップ 3 [アプリケーションタイプのデフォルトアクション (Default Actions for Application Types)] セクションで、編集するアプリケーション タイプの [帯域幅制限 (Bandwidth Limit)] の横にあるリンクをクリックします。
- ステップ 4 [帯域幅制限を設定 (Set Bandwidth Limit)] を選択し、制限するトラフィック量を、メガビット/秒 (Mbps) またはキロビット/秒 (kbps) 単位で入力します。
- ステップ 5 [適用 (Apply)] をクリックします。
- ステップ 6 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## アプリケーション タイプのデフォルトの帯域幅制限の無効化

ユーザー定義のアクセス ポリシーで、グローバルアクセス ポリシー グループで定義されたデフォルトの帯域幅制限を上書きすることができます。これは [参照ビュー (Browse view)] でのみ実行できます。

### Procedure

- ステップ 1 [Webセキュリティマネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] を選択します。

- ステップ 2** ポリシー テーブルで、編集するユーザー定義ポリシー グループの [アプリケーション (Applications)] 列にあるリンクをクリックします。
- ステップ 3** [アプリケーション設定を編集 (Edit Applications Settings)] セクションで [アプリケーションのカスタム設定を定義 (Define Applications Custom Settings)] を選択します。
- ステップ 4** 編集するアプリケーション タイプの [帯域幅制限 (Bandwidth Limit)] の横にあるリンクをクリックします。
- ステップ 5** 別の帯域幅制限値を選択するには、[帯域幅制限を設定 (Set Bandwidth Limit)] を選択し、制限するトラフィック量を、メガビット/秒 (Mbps) またはキロビット/秒 (kbps) 単位で入力します。帯域幅を制限しないことを指定するには、[アプリケーションタイプに対する帯域幅制限なし (No Bandwidth Limit for Application Type)] を選択します。
- ステップ 6** [適用 (Apply)] をクリックします。
- ステップ 7** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## アプリケーションの帯域幅制御の設定

### Procedure

- ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] を選択します。
- ステップ 2** ポリシー テーブルで、編集するポリシー グループの [アプリケーション (Applications)] 列にあるリンクをクリックします。
- ステップ 3** 定義するアプリケーションが含まれているアプリケーション タイプを展開します。
- ステップ 4** 設定するアプリケーションのリンクをクリックします。
- ステップ 5** [モニター (Monitor)] を選択し、次に、アプリケーションタイプに対して定義されている帯域幅制限を使用するか、制限しないかを選択します。

### Note

帯域幅制限の設定は、アプリケーションがブロックされている場合や、アプリケーションタイプに対して帯域幅制限が定義されていない場合は適用できません。

- ステップ 6** [完了 (Done)] をクリックします。
- ステップ 7** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## インスタント メッセージ トラフィックの制御

IM トラフィックをブロックまたはモニターすることができます。また、IM サービスによっては、IM セッションの特定のアクティビティ (アプリケーション動作) をブロックすることもできます。

## Procedure

- ステップ 1 [Webセキュリティマネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] を選択します。
- ステップ 2 ポリシー テーブルで、編集するポリシー グループの [アプリケーション (Applications)] 列にあるリンクをクリックします。
- ステップ 3 [アプリケーションのカスタム設定を定義 (Define Applications Custom Settings)] をクリックします。
- ステップ 4 [インスタントメッセージ (Instant Messaging)] アプリケーション タイプを展開します。
- ステップ 5 設定する IM アプリケーションの横にあるリンクをクリックします。
- ステップ 6 この IM アプリケーションのすべてのトラフィックをブロックするには、[ブロック (Block)] を選択します。
- ステップ 7 IM アプリケーションをモニターしながら、アプリケーション内の特定のアクティビティをブロックするには、[モニター (Monitor)] を選択してから、アプリケーション動作として [ブロック (Block)] を選択します。
- ステップ 8 [完了 (Done)] をクリックします。
- ステップ 9 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## AVC または ADC アクティビティの表示

[レポート (Reporting)] > [アプリケーションの表示 (Application Visibility)] ページには、使用されている上位のアプリケーションとアプリケーション タイプに関する情報が表示されます。また、ブロックされている上位のアプリケーションとアプリケーションタイプも表示されます。

### アクセスログファイルの AVC または ADC 情報

アクセスログファイルには、トランザクションごとに AVC または ADC エンジンから返された情報が記録されます。アクセスログのスキャン判定情報セクションには、以下のようなフィールドがあります。

| 説明                                | アクセス ログのカスタム フィールド | W3C ログのカスタムフィールド |
|-----------------------------------|--------------------|------------------|
| アプリケーション名<br>(Application name)   | %XO                | xAPP             |
| アプリケーションタイプ<br>(Application type) | %Xu                | x-type           |

|                                      |     |                |
|--------------------------------------|-----|----------------|
| アプリケーション動作<br>(Application behavior) | %Xb | x-avc-behavior |
|--------------------------------------|-----|----------------|



**Note** 特定のアプリケーションに対してADCアプリケーションの動作を設定すると、そのアプリケーションのみを検索できます。それ以外の場合、カスタム動作は[不明 (Unknown)]になります。

## 機密データの漏洩防止

この章で説明する内容は、次のとおりです。

- [機密データの漏洩防止の概要 \(518 ページ\)](#)
- [アップロード要求の管理 \(520 ページ\)](#)
- [外部 DLP システムにおけるアップロード要求の管理 \(521 ページ\)](#)
- [データセキュリティおよび外部 DLP ポリシー グループのメンバーシップの評価 \(522 ページ\)](#)
- [データ セキュリティ ポリシーおよび外部 DLP ポリシーの作成 \(523 ページ\)](#)
- [アップロード要求の設定の管理 \(526 ページ\)](#)
- [外部 DLP システムの定義 \(528 ページ\)](#)
- [外部 DLP ポリシーによるアップロード要求の制御 \(531 ページ\)](#)
- [データ損失防止スキンのロギング \(532 ページ\)](#)

## 機密データの漏洩防止の概要

Secure Web Applianceは以下の機能によってデータの安全を確保します。

| オプション                     | 説明                                                                                                                                                                            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco データ セキュリティ フィルタ     | Secure Web Applianceの Cisco データ セキュリティ フィルタは、HTTP、HTTPS、FTPを介してネットワークから発信されるデータを評価します。                                                                                        |
| サードパーティ製データ漏洩防止 (DLP) の統合 | Secure Web Applianceは、機密データを識別して保護する代表的なサードパーティ製コンテンツ対応 DLP システムを統合します。Web プロキシは Internet Content Adaptation Protocol (ICAP) を使用して、プロキシサーバーが外部システムにコンテンツ スキャンをオフロードできるようにします。 |

アップロード要求を受信すると、Web プロキシは要求をデータ セキュリティ ポリシー グループや外部 DLP ポリシー グループと比較して、適用するポリシー グループを決定します。両方のタイプのポリシーが設定されている場合は、外部 DLP ポリシーと比較する前に、Cisco データ セキュリティ ポリシーと要求を比較します。ポリシー グループに要求を割り当てた後、その要求をポリシー グループの設定済み制御設定と比較し、要求に対して実行するアクションを決定します。アップロード要求を処理するためのアプライアンスの設定方法は、ポリシー グループのタイプによって異なります。



**Note** サイズがゼロ (0) バイトのファイルのアップロードを試みているアップロード要求は、Cisco データ セキュリティ ポリシーまたは外部 DLP ポリシーに対して評価されません。

ネットワークから発信されるデータを制限したり制御するには、以下のタスクを実行します。

| タスク                                     | タスクへのリンク                                                      |
|-----------------------------------------|---------------------------------------------------------------|
| Cisco データ セキュリティ ポリシーを作成する              | <a href="#">アップロード要求の管理, on page 520</a>                      |
| 外部 DLP ポリシーを作成する                        | <a href="#">外部 DLP システムにおけるアップロード要求の管理, on page 521</a>       |
| データセキュリティ ポリシーおよび外部 DLP ポリシーを作成する       | <a href="#">データ セキュリティ ポリシーおよび外部 DLP ポリシーの作成, on page 523</a> |
| Cisco データ セキュリティ ポリシーを使用してアップロード要求を制御する | <a href="#">アップロード要求の設定の管理, on page 526</a>                   |
| 外部 DLP ポリシーを使用してアップロード要求を制御する           | <a href="#">外部 DLP ポリシーによるアップロード要求の制御, on page 531</a>        |

## 最小サイズ以下のアップロード要求のバイパス

ログファイルに記録されるアップロード要求の数を減らすために、最小要求サイズを定義できます。このサイズを下回る場合、アップロード要求は Cisco データセキュリティ フィルタや外部 DLP サーバーによってスキャンされません。

これを実行するには、以下の CLI コマンドを使用します。

- **datasecurityconfig**. Cisco データ セキュリティ フィルタに適用します。
- **externaldlpconfig**. 設定されている外部 DLP サーバーに適用します。

デフォルトでは、どちらの CLI コマンドでも要求本文の最小サイズは 4 KB (4096 バイト) です。有効な値は 1 ~ 64 KB です。指定したサイズは、アップロード要求の本文全体のサイズに適用されます。



**Note**

すべてのチャンク エンコードされたアップロードとすべてのネイティブ FTP トランザクションは、Cisco データ セキュリティ フィルタまたは外部 DLP サーバーによってスキャンされます（有効な場合）。ただし、カスタム URL カテゴリに基づいてこれらをバイパスできます。

## 要求が機密データとしてブロックされた場合のユーザー エクスペリエンス

Cisco データセキュリティフィルタや外部 DLP サーバーは、アップロード要求をブロックするときに、Web プロキシがエンド ユーザーに送信するブロック ページを提供します。すべての Web サイトでエンドユーザーにブロック ページが表示されるわけではありません。たとえば、一部の Web 2.0 Web サイトは静的な Web ページの代わりに JavaScript を使用して動的なコンテンツを表示し、ブロック ページを表示しない場合があります。そのような場合でも、データセキュリティ違反が発生しないようにユーザーは適切にブロックされていますが、そのことが Web サイトから通知されない場合もあります。

## アップロード要求の管理

### Before you begin

[セキュリティ サービス (Security Services)] > [データ セキュリティ フィルタ (Data Security Filters)] に移動し、Cisco データ セキュリティ フィルタを有効にします。

### Procedure

データ セキュリティ ポリシー グループを作成して設定します。

Cisco データ セキュリティ ポリシーは、アップロード要求を評価する際に、URL フィルタリング、Web レピュテーション、およびアップロードコンテンツ情報を使用します。これらのセキュリティコンポーネントを個々に設定し、アップロード要求をブロックするかどうかを決定します。

Web プロキシはアップロード要求を制御設定と比較する際に、順番に設定を評価します。各制御設定は、Cisco データ セキュリティ ポリシーの次のアクションのいずれかを実行するように設定できます。

| アクション           | 説明                                                 |
|-----------------|----------------------------------------------------|
| ブロック<br>(Block) | Web プロキシは、接続を許可せず、ブロックの理由を説明するエンド ユーザー通知ページを表示します。 |

| アクション             | 説明                                                                                                                                                                                                                                                                                 |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 許可<br>(Allow)     | <p>Web プロキシは、データ セキュリティ ポリシーの残りのセキュリティ サービス スキャンをバイパスし、最終アクションを実行する前にアクセス ポリシーに対して要求を評価します。</p> <p>Cisco データ セキュリティ ポリシーでは、残りのデータ セキュリティ スキャンをバイパスできますが、外部 DLP やアクセス ポリシーのスキャンはバイパスしません。Web プロキシが要求に対して実行する最終アクションは、該当するアクセス ポリシー（または、要求をブロックする可能性がある適切な外部 DLP ポリシー）によって決まります。</p> |
| モニター<br>(Monitor) | <p>Web プロキシは、引き続き、トランザクションと他のデータ セキュリティ ポリシー グループの制御設定を比較し、トランザクションをブロックするか、またはアクセス ポリシーに対して評価するかを決定します。</p>                                                                                                                                                                       |

Cisco データ セキュリティ ポリシーの場合、Web プロキシがクライアント要求に対して実行する最終アクションは「ブロック」アクションだけです。「モニター」および「許可」アクションは中間アクションです。いずれの場合も、Web プロキシは、トランザクションを外部 DLP ポリシー（設定されている場合）およびアクセス ポリシーに対して評価します。Web プロキシは、アクセス ポリシー グループの制御設定（または、要求をブロックする可能性がある適切な外部 DLP ポリシー）に基づいて適用する最終アクションを決定します。

### What to do next

#### 関連項目

- [外部 DLP システムにおけるアップロード要求の管理, on page 521](#)
- [アップロード要求の設定の管理, on page 526](#)

## 外部 DLP システムにおけるアップロード要求の管理

外部 DLP システムでアップロード要求を処理するように Secure Web Applianceを設定するには、以下のタスクを実行します。

### Procedure

- ステップ 1** [ネットワーク (Network) ] > [外部 DLP サーバー (External DLP Servers) ] を選択します。外部 DLP システムを定義します。スキャンのためにアップロード要求を外部 DLP システムに渡すには、少なくとも 1 つの ICAP 準拠 DLP システムを Secure Web Appliance で定義する必要があります。
- ステップ 2** 外部 DLP ポリシー グループを作成して設定します。外部 DLP システムを定義したら、外部 DLP ポリシー グループを作成して設定し、スキャンのために DLP システムに送信するアップロード要求を決定します。

**ステップ 3** アップロード要求が外部 DLP ポリシーに一致した場合、Web プロキシは、Internet Content Adaptation Protocol (ICAP) を使用して、スキャンのためにアップロード要求を DLP システムに送信します。DLP システムは、要求本文のコンテンツをスキャンし、Web プロキシにブロックまたは許可の判定を返します。許可の判定は、アップロード要求がアクセス ポリシーと比較される Cisco データ セキュリティ ポリシーの許可アクションに似ています。Web プロキシが要求に対して実行する最終アクションは、適用されるアクセス ポリシーによって決まります。

### What to do next

#### 関連項目

- [外部 DLP ポリシーによるアップロード要求の制御, on page 531](#)
- [外部 DLP システムの定義, on page 528](#)

## データ セキュリティおよび外部 DLP ポリシーグループのメンバーシップの評価

各クライアント要求に ID が割り当てられ、次に、それらの要求が他のポリシー タイプと照合して評価され、タイプごとに要求が属するポリシー グループが判定されます。Web プロキシは、データ セキュリティおよび外部 DLP ポリシーに対してアップロード要求を評価します。Web プロキシは、クライアント要求のポリシー グループ メンバーシップに基づいて、設定されているポリシー制御設定をクライアント要求に適用します。

## クライアント要求とデータ セキュリティおよび外部 DLP ポリシー グループとの照合

クライアント要求と一致するポリシー グループを判定するために、Web プロキシは、特定のプロセスを実行してグループ メンバーシップの基準と照合します。グループ メンバーシップの以下の要素が考慮されます。

- **ID。**各クライアント要求は、識別プロファイルに一致するか、認証に失敗するか、ゲスト アクセスが許可されるか、または認証に失敗して終了します。
- **権限を持つユーザー。**割り当てられた識別プロファイルが認証を必要とする場合は、そのユーザーがデータ セキュリティまたは外部 DLP ポリシー グループの承認済みユーザーのリストに含まれており、ポリシーグループに一致する必要があります。承認済みユーザーのリストには、任意のグループまたはユーザーを指定でき、識別プロファイルがゲスト アクセスを許可している場合はゲスト ユーザーを指定できます。
- **高度なオプション。**データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップに対して複数の詳細オプションを設定できます。一部のオプション（プロキシポート、URL カテゴリなど）は、ID 内に定義することもできます。ID 内に詳細オプションを設定する場合、データ セキュリティまたは外部 DLP ポリシー グループ レベルでは設定できません。

この項では、Web プロキシがアップロード要求をデータ セキュリティおよび外部 DLP の両方のポリシー グループと照合する方法について概要を説明します。

Web プロキシは、ポリシーテーブルの各ポリシーグループを順番に読み取ります。次に、アップロード要求のステータスを最初のポリシーグループのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシーグループのポリシー設定を適用します。

一致しない場合は、その以下のポリシーグループとアップロード要求を比較します。アップロード要求をユーザー定義のポリシーグループと照合するまで、Web プロキシはこのプロセスを続行します。ユーザー定義のポリシーグループに一致しない場合は、グローバルポリシーグループと照合します。Web プロキシは、アップロード要求をポリシーグループまたはグローバルポリシーグループと照合するときに、そのポリシーグループのポリシー設定を適用します。

## データ セキュリティ ポリシーおよび外部 DLP ポリシーの作成

宛先サイトの URL カテゴリや 1 つ以上の識別プロファイルなど、複数の条件の組み合わせに基づいてデータセキュリティおよび外部 DLP ポリシーグループを作成できます。ポリシーグループのメンバーシップには、少なくとも 1 つの条件を定義する必要があります。複数の条件が定義されている場合、アップロード要求がポリシーグループと一致するには、すべての条件を満たしていなければなりません。ただし、アップロード要求は設定された識別プロファイルの 1 つとのみ一致する必要があります。

### Procedure

**ステップ 1** [Web セキュリティ マネージャ (Web Security Manager) ] > [Cisco データ セキュリティ (Cisco Data Security) ] (データセキュリティ ポリシー グループ メンバーシップを定義する場合) 、または [Web セキュリティ マネージャ (Web Security Manager) ] > [外部データ漏洩防止 (External Data Loss Prevention) ] (外部 DLP ポリシー グループ メンバーシップを定義する場合) を選択します。

**ステップ 2** [ポリシーを追加 (Add Policy) ] をクリックします。

**ステップ 3** [ポリシー名 (Policy Name) ] フィールドにポリシーグループの名前を入力し、[説明 (Description) ] フィールドに説明を追加します。

#### Note

各ポリシーグループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

**ステップ 4** [上記ポリシーを挿入 (Insert Above Policy) ] フィールドで、ポリシーテーブル内でポリシーグループを配置する場所を選択します。

複数のポリシーグループを設定する場合は、各グループに論理的な順序を指定します。正しく照合されるようにポリシーグループの順序を指定してください。

**ステップ 5** [アイデンティティとユーザー (Identities and Users) ] セクションで、このポリシーグループに適用する 1 つ以上の識別プロファイルグループを選択します。

**ステップ 6** (任意) [詳細設定 (Advanced) ] セクションを展開して、追加のメンバーシップ要件を定義します。

**ステップ 7** いずれかの拡張オプションを使用してポリシーグループのメンバーシップを定義するには、拡張オプションのリンクをクリックし、表示されるページでオプションを設定します。

| 高度なオプション                  | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プロトコル<br>(Protocols)      | <p>クライアント要求で使用するプロトコルによってポリシー グループのメンバーシップを定義するかどうかを選択します。含めるプロトコルを選択します。</p> <p>[その他のすべて (All others)] は、このオプションの上に一覧表示されていないプロトコルを意味します。</p> <p><b>Note</b><br/>HTTPS プロキシをイネーブルにすると、復号ポリシーのみが HTTPS トランザクションに適用されます。アクセス、ルーティング、アウトバウンドマルウェア スキャン、データ セキュリティ、外部 DLP のポリシーの場合は、HTTPS プロトコルによってポリシー メンバーシップを定義できません。</p>                                                                                                                                                                                                                                                                                                                                    |
| プロキシ ポート<br>(Proxy Ports) | <p>Web プロキシへのアクセスに使用するプロキシポートで、ポリシー グループメンバーシップを定義するかどうかを選択します。[プロキシポート (Proxy Ports)] フィールドに、1つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。</p> <p>明示的な転送接続のために、ブラウザに設定されたポートです。透過接続の場合は、宛先ポートと同じです。あるポート上に要求を明示的に転送するように設定されたクライアントのセットがあり、別のポート上に要求を明示的に転送するように設定された別のクライアントのセットがある場合、プロキシポート上でポリシー グループのメンバーシップを定義することがあります。</p> <p>シスコでは、アプライアンスが明示的な転送モードで配置されている場合、またはクライアントがアプライアンスに要求を明示的に転送する場合にだけ、プロキシポートでポリシー グループのメンバーシップを定義することを推奨します。クライアント要求がアプライアンスに透過的にリダイレクトされるときにプロキシポートでポリシー グループのメンバーシップを定義すると、一部の要求が拒否される場合があります。</p> <p><b>Note</b><br/>このポリシー グループに関連付けられている ID がこの詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。</p> |
| サブネット<br>(Subnets)        | <p>サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義するかどうかを選択します。</p> <p>関連付けられた識別プロファイルで定義できるアドレスを使用するか、または特定のアドレスをここに入力できます。</p> <p><b>Note</b><br/>ポリシー グループに関連付けられている識別プロファイルがアドレスによってグループのメンバーシップを定義している場合は、識別プロファイルで定義されているアドレスのサブセットであるアドレスを、このポリシー グループに入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込みます。</p>                                                                                                                                                                                                                                                                                                                              |

| 高度なオプション                     | 説明                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL カテゴリ<br>(URL Categories) | <p>URL カテゴリでポリシー グループのメンバーシップを定義するかどうかを選択します。ユーザー定義または定義済みの URL カテゴリを選択します。</p> <p><b>Note</b><br/>このポリシー グループに関連付けられている ID がこの詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。</p>                                                                                                                                                            |
| ユーザー エージェント<br>(User Agents) | <p>クライアント要求で使用されるユーザー エージェント（アップデータや Web ブラウザなどのクライアント アプリケーション）ごとにポリシー グループ メンバーシップを定義するかどうかを選択します。一般的に定義されているユーザー エージェントを選択するか、正規表現を使用して独自に定義できます。メンバーシップの定義に選択したユーザー エージェントのみを含めるか、選択したユーザー エージェントを明確に除外するかどうかを指定します。</p> <p><b>Note</b><br/>このポリシー グループに関連付けられている識別プロファイルが、この詳細設定によって識別プロファイルメンバーシップを定義している場合、非識別プロファイル ポリシー グループ レベルではこの設定項目を設定できません。</p> |
| ユーザーの場所<br>(User Location)   | <p>ユーザーのリモートまたはローカルでポリシー グループのメンバーシップを定義するかどうかを選択します。</p> <p>このオプションは、セキュアモビリティがイネーブルの場合にのみ表示されます。</p>                                                                                                                                                                                                                                                         |

**ステップ 8** 変更を送信します。

**ステップ 9** データ セキュリティ ポリシー グループを作成する場合は、その制御設定を設定して、Web プロキシがアップロード要求を処理する方法を定義します。

新しいデータセキュリティポリシーグループは、各制御設定のオプションが設定されるまで、グローバルポリシーグループの設定を自動的に継承します。

外部 DLP ポリシー グループを作成する場合は、その制御設定を設定して、Web プロキシがアップロード要求を処理する方法を定義します。

新しい外部 DLP ポリシー グループは、カスタム設定が設定されるまで、グローバルポリシーグループの設定を自動的に継承します。

**ステップ 10** 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

## What to do next

### 関連項目

- データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップの評価, on page 522

- クライアント要求とデータ セキュリティおよび外部 DLP ポリシー グループとの照合, on page 522
- アップロード要求の設定の管理, on page 526
- 外部 DLP ポリシーによるアップロード要求の制御, on page 531

## アップロード要求の設定の管理

各アップロード要求は、データセキュリティ ポリシーグループに割り当てられ、そのポリシーグループの制御設定を継承します。データ セキュリティ ポリシー グループの制御設定によって、アプライアンスが接続をブロックするか、またはアクセスポリシーに対して接続を評価するかが決まります。

[Web セキュリティ マネージャ (Web Security Manager) ] > [Cisco データ セキュリティ (Cisco Data Security) ] ページで、データ セキュリティ ポリシー グループの制御設定を設定します。

以下の設定項目を設定して、アップロード要求で実行するアクションを決定できます。

| オプション                     | リンク                                       |
|---------------------------|-------------------------------------------|
| URL カテゴリ (URL Categories) | <a href="#">URL カテゴリ, on page 526</a>     |
| Web レピュテーション              | <a href="#">Web レピュテーション, on page 526</a> |
| 目次                        | <a href="#">コンテンツのブロック, on page 527</a>   |

データセキュリティ ポリシー グループがアップロード要求に割り当てられた後、ポリシーグループの制御設定が評価され、要求をブロックするかアクセスポリシーに対して評価するかが決定されます。

### URL カテゴリ

AsyncOS for Web では、アプライアンスが特定の要求の URL カテゴリに基づいてトランザクションを処理する方法を設定できます。定義済みのカテゴリリストを使用して、カテゴリ別にコンテンツをモニターするかブロックするかを選択できます。カスタム URL カテゴリを作成し、カスタム カテゴリの Web サイトに対してトラフィックを許可、モニター、またはブロックするかを選択することもできます。

### Web レピュテーション

Web レピュテーションの設定はグローバル設定を継承します。特定のポリシー グループ用に Web レピュテーション フィルタリングをカスタマイズするには、[Web レピュテーション設定 (Web Reputation Settings) ] プルダウン メニューを使用して Web レピュテーション スコアのしきい値をカスタマイズします。

Cisco データ セキュリティ ポリシーの Web レピュテーションのしきい値には、負またはゼロの値のみ設定できます。定義では、すべての正のスコアがモニターされます。

## コンテンツのブロック

[Cisco データ セキュリティ (Cisco Data Security)] > [コンテンツ (Content)] ページの設定項目を使用し、Web プロキシが次のファイル特性に基づいてデータのアップロードをブロックするように設定できます。

- **[ファイルサイズ (File size)]**。許容される最大アップロード サイズを指定できます。指定した最大値以上のサイズのアップロード はすべてブロックされます。HTTP/HTTPS およびネイティブ FTP 要求に対して異なる最大ファイル サイズを指定できます。

アップロード要求サイズが最大アップロード サイズと最大スキャン サイズ ([セキュリティ サービス (Security Services)] > [マルウェア対策 (Anti-Malware)] ページの [DVS エンジン オブジェクト スキャンの制限 (DVS Engine Object Scanning Limits)] フィールドで設定) のどちらよりも大きい場合、アップロード要求はブロックされますが、ファイル名とコンテンツ タイプはデータ セキュリティ ログに記録されません。アクセス ログのエントリは変更されません。

- **[ファイルタイプ (Filetype)]**。定義済みのファイルタイプまたは入力したカスタム MIME タイプをブロックできます。定義済みファイルタイプをブロックする場合は、そのタイプのすべてのファイルまたは指定したサイズよりも大きいファイルをブロックできます。ファイル タイプをサイズによってブロックする場合は、最大ファイル サイズとして、[セキュリティ サービス (Security Services)] > [マルウェア対策 (Anti-Malware)] ページの [DVS エンジン オブジェクト スキャンの制限 (DVS Engine Object Scanning Limits)] フィールドの値と同じ値を指定できます。デフォルトでは、この値は 32 MB です。

Cisco データセキュリティフィルタは、ファイルタイプによってブロックする場合にアーカイブ ファイルのコンテンツを検査しません。アーカイブ ファイルは、ファイルタイプまたはファイル名によってブロックできます。コンテンツによってブロックすることはありません。

**Note**

一部の MIME タイプのグループでは、1 つのタイプをブロックすると、グループ内のすべての MIME タイプがブロックされます。たとえば、application/x-java-applet をブロックすると、application/java や application/javascript など、すべての MIME タイプがブロックされます。

- **[ファイル名 (File name)]**。指定した名前のファイルをブロックできます。ブロックするファイル名を指定する場合は、リテラル文字列または正規表現をテキストとして使用できます。

**Note**

8 ビット ASCII 文字のファイル名のみを入力してください。Web プロキシは、8 ビット ASCII 文字のファイル名のみを照合します。



## 外部 DLP システムの定義

Secure Web Applianceでは、アプライアンスに複数の DLP サーバを定義することにより、同じベンダーの複数の外部 DLP サーバを統合できます。Web プロキシが DLP システムに接続する際に使用するロード バランシング技術を定義できます。これは、複数の DLP システムを定義する場合に役立ちます。外部 DLP サーバとのセキュアな通信に使用されるプロトコルの指定については、[SSL の設定](#) , on page 197を参照してください。



### Note

外部 DLP サーバが Web プロキシによって変更されたコンテンツを送信しないことを確認します。AsyncOS for Web は、アップロード要求をブロックまたは許可する機能のみをサポートしています。外部 DLP サーバによって変更されたコンテンツのアップロードはサポートしません。

## 外部 DLP サーバの設定

### Procedure

**ステップ 1** [ネットワーク (Network) ] > [外部 DLP サーバ (External DLP Servers) ] を選択します。

**ステップ 2** [設定の編集 (Edit Settings) ] をクリックします。

| 設定                                                                | 説明                                                                                                                                                                                                                     |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 外部 DLP サーバの<br>プロトコル<br>(Protocol for<br>External DLP<br>Servers) | <p>以下のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [ICAP] : DLPクライアント/サーバの ICAP 通信は暗号化されません。</li> <li>• [セキュアICAP (Secure ICAP) ] : DLP クライアント/サーバの ICAP 通信は暗号化トンネルを介して行われます。追加の関連オプションが表示されます。</li> </ul> |

| 設定                                    | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 外部 DLP サーバー<br>(External DLP Servers) | <p>以下の情報を入力して、ICAP 準拠 DLP システムにアクセスします。</p> <ul style="list-style-type: none"><li>• [サーバー アドレス (Server address)] と [ポート (Port)] : DLP システムにアクセスするホスト名/IP アドレスと TCP ポート。</li><li>• [再接続の試行 (Reconnection attempts)] : 失敗するまでに Web プロキシが DLP システムへの接続を試行する回数。</li><li>• [サービス URL (Service URL)] : 特定の DLP サーバーに固有の ICAP クエリー URL。Web プロキシは、ここに入力された情報を外部 DLP サーバーに送信する ICAP 要求に含めます。URL は、ICAP プロトコル (icap://) から始める必要があります。</li><li>• [証明書 (Certificate)] (オプション) : 各外部 DLP サーバー接続を保護するために提供する証明書は、認証局 (CA) の署名付き証明書でも自己署名証明書でもかまいません。指定されたサーバーから証明書を取得し、アプライアンスにアップロードします。<ul style="list-style-type: none"><li>• 証明書ファイルを参照して選択し、[ファイルのアップロード (Upload File)] をクリックします。</li></ul></li></ul> <p><b>Note</b><br/>この単一ファイルには、暗号化されていない形式でクライアント証明書と秘密キーを含める必要があります。</p> <ul style="list-style-type: none"><li>• [セキュア ICAP を使用するすべての DLP サーバーにこの証明書を使用する (Use this certificate for all DLP servers using Secure ICAP)] : ここで定義するすべての外部 DLP サーバーに同じ証明書を使用する場合は、このチェックボックスをオンにします。サーバーごとに異なる証明書を入力するには、このオプションをオフのままにします。</li><li>• [テスト開始 (Start Test)] : このチェックボックスをオンにすると、Secure Web Appliance と定義済み外部 DLP サーバ間の接続をテストできます。</li></ul> |

| 設定                                         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ロード バランシング (Load Balancing)                | <p>複数の DLP サーバーを定義する場合は、Web プロキシがさまざまな DLP サーバーにアップロード要求を分散する際に使用するロードバランシング技術を選択します。以下のロードバランシング技術を選択できます。</p> <ul style="list-style-type: none"> <li>• <b>[なし (フェールオーバー) (None(failover)) ]</b>。Web プロキシは、1 つの DLP サーバーにアップロード要求を送信します。一覧表示されている順序で DLP サーバーへの接続を試みます。ある DLP サーバーに到達できない場合、Web プロキシはリストの以下のサーバーへの接続を試みます。</li> <li>• <b>[最少接続 (Fewest connections) ]</b>。Web プロキシは、各 DLP サーバーが扱っているアクティブな要求の数を追跡し、その時点で接続数が最も少ない DLP サーバーにアップロード要求を送信します。</li> <li>• <b>[ハッシュベース (Hash based) ]</b>。Web プロキシは、ハッシュ関数を使用して、DLP サーバーに要求を分散します。ハッシュ関数はプロキシ ID と URL を入力として使用し、同じ URL の要求が常に同じ DLP サーバーに送信されるようにします。</li> <li>• <b>[ラウンド ロビン (Round robin) ]</b>。Web プロキシは、リストされた順序ですべての DLP サーバー間にアップロード要求を均等に分散します。</li> </ul> |
| サービス要求タイムアウト (Service Request Timeout)     | <p>Web プロキシが DLP サーバーからの応答を待機する時間を入力します。この時間が経過すると、ICAP 要求は失敗し、[失敗のハンドリング (Failure Handling) ] の設定に応じて、アップロード要求はブロックまたは許可されます。</p> <p>デフォルトは 60 秒です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 最大同時接続数 (Maximum Simultaneous Connections) | <p>Secure Web Appliance から設定されている各外部 DLP サーバへの同時 ICAP 要求接続の最大数を指定します。このページの [失敗のハンドリング (Failure Handling) ] 設定は、この制限を超えるすべての要求に適用されます。</p> <p>デフォルトは 25 です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 失敗のハンドリング (Failure Handling)               | <p>DLP サーバーがタイムリーに応答できなかった場合に、アップロード要求をブロックするか許可するか (評価のためにアクセス ポリシーに渡される) を選択します。</p> <p>デフォルトは、許可 ([すべてのデータ転送をスキャンなしで許可する (Permit all data transfers to proceed without scanning) ]) です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 信頼できるルート証明書 (Trusted Root Certificate)     | <p>外部 DLP サーバーによって提供された証明書に対して、信頼できるルート証明書を参照して選択し、[ファイルのアップロード (Upload File) ] をクリックします。詳細については、<a href="#">証明書の管理, on page 200</a>を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 無効な証明書オプション (Invalid Certificate Options)  | <p>さまざまな無効な証明書の処理方法 ([ドロップ (Drop) ] または [モニター (Monitor) ]) を指定します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| 設定                                  | 説明                                                |
|-------------------------------------|---------------------------------------------------|
| サーバー証明書<br>(Server<br>Certificates) | このセクションには、アプライアンスで現在使用可能なすべての DLP サーバー証明書が表示されます。 |

**ステップ 3** (オプション) [行を追加 (Add Row)] をクリックし、表示される新しいフィールドに DLP サーバー情報を入力することによって、別の DLP サーバーを追加できます。

**ステップ 4** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## 外部 DLP ポリシーによるアップロード要求の制御

Web プロキシは、アップロード要求ヘッダーを受信することにより、スキャン用に要求を外部 DLP システムに送信する必要があるかどうかを判定するための必要情報を得ます。DLP システムは要求をスキャンし、Web プロキシに判定 (ブロックまたはモニター) を返します (要求はアクセス ポリシーに対して評価されます)。

### Procedure

**ステップ 1** [Webセキュリティマネージャ (Web Security Manager)] > [外部データ漏洩防止 (External Data Loss Prevention)] を選択します。

**ステップ 2** [接続先 (Destinations)] 列で、設定するポリシー グループのリンクをクリックします。

**ステップ 3** [接続先設定の編集 (Edit Destination Settings section)] セクションで、[接続先スキャンのカスタム設定の定義 (Define Destinations Scanning Custom Settings)] を選択します。

**ステップ 4** [スキャンする接続先 (Destination to Scan)] セクションで、以下のオプションのいずれかを選択します。

- **[どのアップロードもスキャンしない (Do not scan any uploads)]**。アップロード要求は、スキャンのために設定済み DLP システムに送信されません。すべてのアップロード要求がアクセス ポリシーに対して評価されます。
- **[すべてのアップロードをスキャンする (Scan all uploads)]**。すべてのアップロード要求が、スキャンのために設定済み DLP システムに送信されます。アップロード要求は、DLP システムのスキャン判定に応じて、ブロックされるか、アクセス ポリシーに対して評価されます。
- **[指定したカスタムおよび外部 URL カテゴリ以外へのアップロードをスキャン (Scan uploads except to specified custom and external URL categories)]**。特定のカスタム URL カテゴリに該当するアップロードの要求が、DLP スキャン ポリシーから除外されます。[カスタムカテゴリリストを編集 (Edit custom categories list)] をクリックして、スキャンする URL カテゴリを選択します。

**ステップ 5** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## データ損失防止スキンのロギング

アクセス ログは、アップロード要求が Cisco データ セキュリティ フィルタまたは外部 DLP サーバーのいずれかによってスキャン済みかどうかを示します。アクセス ログ エントリには、Cisco データ セキュリティ ポリシーのスキャン判定用のフィールド、および外部 DLP スキャン判定に基づく別のフィールドが含まれています。

アクセス ログに加えて、Secure Web Applianceには、Cisco データ セキュリティ ポリシーや外部 DLP ポリシーをトラブルシューティングするための次のようなログ ファイルが用意されています。

- **データ セキュリティ ログ。** Cisco データ セキュリティ フィルタで評価されたアップロード要求のクライアント履歴を記録します。
- **データ セキュリティ モジュール ログ。** Cisco データ セキュリティ フィルタに関するメッセージを記録します。
- **デフォルト プロキシ ログ。** Web プロキシに関連するエラーの記録に加えて、デフォルト プロキシ ログには外部 DLP サーバーへの接続に関連するメッセージが含まれています。これにより、外部 DLP サーバーとの接続や統合に関する問題をトラブルシューティングできます。

以下のテキストは、データ セキュリティ ログのエントリのサンプルを示しています。

```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com
nc
```

| フィールド値                                       | 説明                                                                                                                                    |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Mon Mar 30 03:02:13 2009<br>Info:            | タイムスタンプおよびトレース レベル                                                                                                                    |
| 303                                          | トランザクション ID                                                                                                                           |
| 10.1.1.1                                     | ソース IP アドレス                                                                                                                           |
| -                                            | ユーザー名 (User name)                                                                                                                     |
| -                                            | 承認されたグループ名。                                                                                                                           |
| <<bar,text/plain,5120><foo,text/plain,5120>> | 一度にアップロードされる各ファイルのファイル名、ファイルタイプ、ファイルサイズ<br><br><b>Note</b><br>このフィールドには、設定されている最小の要求本文サイズ（デフォルトは 4096 バイト）よりも小さいテキスト/プレーンファイルは含まれません。 |

| フィールド値                                                                  | 説明                            |
|-------------------------------------------------------------------------|-------------------------------|
| BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting | Cisco データ セキュリティ ポリシーおよびアクション |
| ns                                                                      | Web レピュテーション スコア              |
| server.com                                                              | 発信 URL                        |
| nc                                                                      | URL カテゴリ                      |

**Note**

サイトへのデータ転送（POST 要求など）がいつ外部 DLP サーバーによってブロックされたかを確認するには、アクセス ログの DLP サーバーの IP アドレスまたはホスト名を検索します。

## エンドユーザーへのプロキシ アクションの通知

この章で説明する内容は、次のとおりです。

- [エンドユーザー通知の概要](#)（533 ページ）
- [通知ページの一般設定項目の設定](#)（534 ページ）
- [エンドユーザー確認応答ページ](#)（535 ページ）
- [エンドユーザー通知ページ](#)（539 ページ）
- [エンドユーザー URL フィルタリング警告ページの設定](#)（544 ページ）
- [FTP 通知メッセージの設定](#)（545 ページ）
- [通知ページ上のカスタム メッセージ](#)（545 ページ）
- [通知ページ HTML ファイルの直接編集](#)（547 ページ）
- [通知ページのタイプ](#)（552 ページ）

## エンドユーザー通知の概要

以下のタイプのエンドユーザーへの通知を設定できます。

| オプション                                             | 説明                                                                                                        | 解説場所                                                                                                                                                                                                                                 |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エンドユーザー<br>確認応答ページ                                | エンドユーザーに、自分の Web アクティビティがフィルタリングおよびモニターされていることを通知します。エンドユーザー確認応答ページは、ユーザーが初めてブラウザにアクセスしてから一定時間経過後に表示されます。 | <a href="#">エンドユーザー確認応答ページ, on page 535</a>                                                                                                                                                                                          |
| エンドユーザー<br>通知ページ                                  | エンドユーザーに、特定のブロック理由のために特定のページへのアクセスがブロックされていることを通知します。                                                     | <a href="#">エンドユーザー通知ページ, on page 539</a>                                                                                                                                                                                            |
| エンドユーザー<br>URL フィルタ<br>リング警告ページ                   | エンドユーザーに、ユーザーがアクセスしようとしているサイトが組織のアクセプタブルユースポリシーに一致しないことを警告し、ユーザーが選択すればアクセスの続行を許可します。                      | <a href="#">エンドユーザー URL フィルタリング警告ページの設定, on page 544</a>                                                                                                                                                                             |
| FTP 通知メッ<br>セージ (FTP<br>notification<br>messages) | エンドユーザーに、ネイティブ FTP トランザクションがブロックされた理由を知らせます。                                                              | <a href="#">FTP 通知メッセージの設定, on page 545</a> 。                                                                                                                                                                                        |
| 時間およびボ<br>リューム クォ<br>ータの有効期<br>限警告ページ             | エンドユーザーに、設定されたデータ量または時間制限に達したため、アクセスがブロックされることを通知します。                                                     | これらの設定は、[セキュリティ サービス (Security Services)] > [エンドユーザー通知 (End-User Notification)] ページの [時間およびボリューム クォータの有効期限警告ページ (Time and Volume Quotas Expiry Warning Page)] セクションで行います。<br><br><a href="#">時間範囲およびクォータ, on page 389</a> も参照してください。 |

## 通知ページの一般設定項目の設定

通知ページの表示言語とロゴを指定します。制限についてはこの手順で説明します。

### Procedure

**ステップ 1** [セキュリティ サービス (Security Services)] > [エンドユーザー通知 (End-User Notification)] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** [全般設定 (General Settings)] セクションで、Web プロキシが通知ページを表示する際に使用する言語を選択します。

- HTTP の言語設定は、すべての HTTP 通知ページ（確認通知、オンボックスのエンドユーザー通知、カスタマイズしたエンドユーザー通知、エンドユーザー URL フィルタリング警告）に適用されます。
- FTP の言語は、すべての FTP 通知メッセージに適用されます。

**ステップ 4** 各通知ページでロゴを使用するかどうかを選択します。Cisco ロゴを指定したり、[カスタム ロゴを使用 (Use Custom Logo)] フィールドに入力した URL で参照される任意のグラフィック ファイルを指定することができます。

この設定は、IPv4 を介して提供されるすべての HTTP 通知ページに適用されます。AsyncOS では IPv6 を介したイメージはサポートされません。

**ステップ 5** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

---

### What to do next

#### 関連項目

- [通知ページの URL とロゴに関する注意事項, on page 546](#)

## エンドユーザー確認応答ページ

Secure Web Appliance を設定して、Web アクティビティのフィルタリングとモニタリングが行われていることをユーザに通知できます。（そのように設定されている場合）アプライアンスは、HTTP または HTTPS を使用して Web にアクセスしているすべてのユーザーに、エンドユーザー確認応答ページを表示します。ユーザーが初めて Web サイトにアクセスを試みたとき、または設定された時間間隔の後にエンドユーザー確認応答ページが表示されます。

認証でユーザー名を使用可能な場合、Web プロキシはユーザー名によってユーザーを追跡します。ユーザー名を使用できない場合は、ユーザーを追跡する方法（IP アドレスまたは Web ブラウザのセッション Cookie のいずれか）を選択できます。



---

**Note** ネイティブ FTP トランザクションは、エンドユーザー確認ページから除外されます。

---

- [エンドユーザー確認ページによる HTTPS および FTP サイトへのアクセス, on page 536](#)
- [エンドユーザー確認応答ページについて, on page 536](#)
- [エンドユーザー確認応答ページの設定, on page 537](#)



## エンドユーザー確認ページによる HTTPS および FTP サイトへのアクセス

エンドユーザー確認応答ページは、アクセプタブルユースポリシー契約をクリックすることを求める HTML ページをエンドユーザーに表示することにより動作します。ユーザーがリンクをクリックすると、Web プロキシは、最初に要求された Web サイトにクライアントをリダイレクトします。ユーザーに対して使用可能なユーザー名がない場合は、ユーザーがサロゲート（IP アドレスまたは Web ブラウザセッション Cookie のいずれか）を使用してエンドユーザー確認応答ページを受け入れた時期を記録します。

- **HTTPS。** Web プロキシは、ユーザーが Cookie を使用してエンドユーザー確認応答ページを確認したかどうかを追跡しますが、トランザクションを復号しない限り Cookie を取得できません。エンドユーザー確認応答ページがイネーブルになっており、セッション Cookie を使用してユーザーを追跡する場合は、HTTPS 要求をバイパス（パススルー）するかドロップするかを選択できます。advancedproxyconfig>EUN CLI コマンドを使用してこの操作を実行し、「セッションベースの EUA により HTTPS 要求に対して実行されるアクション（「bypass」または「drop」）」コマンドをバイパスすることを選択します。
- **FTP over HTTP。** Web ブラウザは、FTP over HTTP トランザクションに Cookie を送信することはないので、Web プロキシは Cookie を取得できません。このような状況を回避するために、FTP over HTTP トランザクションに対してエンドユーザー確認応答ページの要求が適用されないようにできます。正規表現として「ftp://」（引用符なし）を使用してカスタム URL カテゴリを作成し、このカスタム URL カテゴリに対してユーザーにエンドユーザー確認ページを表示しないようにする ID ポリシー定義します。

## エンドユーザー確認応答ページについて

- ユーザーが IP アドレスによって追跡される場合、アプライアンスは最大時間間隔の最短の値と IP アドレスの最長アイドルタイムアウトを使用して、エンドユーザー確認応答ページを再表示する時点を指定します。
- ユーザーがセッション Cookie を使用して追跡される場合、Web プロキシは、ユーザーが Web ブラウザを閉じて再起動したときや、別の Web ブラウザアプリケーションを開いたときに、エンドユーザー確認応答ページを再表示します。
- クライアントが FTP over HTTP を使用して HTTPS サイトまたは FTP サーバーにアクセスする場合、セッション Cookie によるユーザーの追跡は動作しません。
- アプライアンスが明示的転送モードで展開され、ユーザーが HTTPS のサイトに移動する場合、エンドユーザー確認応答ページでは、最初に要求された URL にユーザーをリダイレクトするリンクにドメイン名のみが含まれます。最初に要求された URL のドメイン名の後にテキストが含まれている場合、このテキストは切り捨てられます。
- エンドユーザー確認ページがユーザーに表示されると、そのトランザクションのアクセスログエントリには ACL デシジョンタグとして OTHER が表示されます。これは、最初に要求した URL がブロックされ、代わりにユーザーにはエンドユーザー確認ページが表示されたためです。

## エンドユーザー確認応答ページの設定

### Before you begin

- 表示言語の設定、および表示されるロゴのカスタマイズについては、[通知ページの一般設定項目の設定, on page 534](#) を参照してください。
- エンドユーザーに表示されるメッセージをカスタマイズする場合は、[通知ページ上のカスタムメッセージ, on page 545](#) を参照してください。[カスタムメッセージ (Custom Message) ] ボックスでできること以上のカスタマイズが必要な場合は、[通知ページ HTML ファイルの直接編集, on page 547](#) を参照してください。

Web インターフェイスまたはコマンドライン インターフェイスで、エンドユーザー確認応答ページをイネーブルにしたり、設定することができます。Web インターフェイスでエンドユーザー確認応答ページを設定する場合は、各ページに表示するカスタムメッセージを含めることができます。

CLI で、`advancedproxyconfig> eun` を使用します。

### Procedure

- ステップ 1** [セキュリティ サービス (Security Services) ] > [ユーザー通知 (End-User Notification) ] を選択します。
- ステップ 2** [設定の編集 (Edit Settings) ] をクリックします。
- ステップ 3** [確認ページからクリックすることをエンドユーザーに要求 (Require end-user to click through acknowledgment page) ] フィールドをイネーブルにします。
- ステップ 4** オプションを入力します。

| 設定                                           | 説明                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 確認応答の時間間隔<br>(Time Between Acknowledgements) | <p>[確認応答の時間間隔 (Time Between Acknowledgements) ] では、Web プロキシがユーザーごとにエンドユーザー確認ページを表示する頻度を指定します。この設定は、ユーザー名で追跡されるユーザー、および IP アドレスまたはセッション Cookie で追跡されるユーザーに適用されます。30 ～ 2678400 秒 (1 か月) の任意の値を指定できます。デフォルトは 1 日 (86400 秒) です。</p> <p>[確認応答の時間間隔 (Time Between Acknowledgements) ] を変更して確定すると、Web プロキシは、Web プロキシに確認応答済みのユーザーにも新しい値を使用します。</p> |
| 無活動タイムアウト<br>(Inactivity Timeout)            | <p>[無活動タイムアウト (Inactivity Timeout) ] では、IP アドレスまたはセッション Cookie (未認証ユーザーのみ) によって追跡され確認されたユーザーが、アクセプタブルユースポリシーに同意していないと見なされるまでに、アイドル状態を維持できる時間を指定します。30 ～ 2678400 (1 か月) 秒の任意の値を指定できます。デフォルトは 4 時間 (14400 秒) です。</p>                                                                                                                         |

| 設定                             | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サロゲート タイプ<br>(Surrogate Type)  | <p>Web プロキシがユーザーの追跡に使用する方式を指定します。</p> <ul style="list-style-type: none"> <li>• <b>[IP アドレス (IP Address)]</b>。Web プロキシは、その IP アドレスのユーザーがエンドユーザー確認応答ページ上のリンクをクリックしたときに、任意の Web ブラウザまたはブラウザ以外の HTTP プロセスを使用して Web にアクセスできるようにします。IP アドレスによるユーザーの追跡では、ユーザーが非アクティブであったり設定された時間間隔が経過したために、新たな確認が必要になり、Web プロキシが新しいエンドユーザー確認応答ページを表示するまで、ユーザーは Web アクセスできます。セッション Cookie による追跡とは異なり、IP アドレスによる追跡では、設定された時間間隔が経過しない限り、ユーザーは複数の Web ブラウザアプリケーションを開くことができ、エンドユーザー確認に合意する必要はありません。</li> </ul> <p><b>Note</b><br/>IP アドレスが設定され、ユーザーが認証されると、Web プロキシは、IP アドレスではなく、ユーザー名によってユーザーを追跡します。</p> <ul style="list-style-type: none"> <li>• <b>[セッション Cookie (Session Cookie)]</b>。ユーザーがエンドユーザー確認応答ページ上のリンクをクリックすると、Web プロキシはユーザーの Web ブラウザに Cookie を送信し、Cookie を使用してユーザーのセッションを追跡します。[確認応答の時間間隔 (Time Between Acknowledgements)] の値が失効するまで、または、ユーザーが割り当てられた時間よりも長時間非アクティブであったり Web ブラウザを閉じるまで、ユーザーは Web ブラウザを使用して Web にアクセスできます。</li> </ul> <p>ブラウザ以外の HTTP クライアント アプリケーションを使用している場合、ユーザーが Web にアクセスするには、エンドユーザー確認応答ページ上のリンクをクリックできなければなりません。別の Web ブラウザ アプリケーションを開く場合は、Web プロキシが別の Web ブラウザにセッション Cookie を送信できるように、ユーザーは再度エンドユーザー確認プロセスを実行する必要があります。</p> <p><b>Note</b><br/>クライアントが FTP over HTTP を使用して HTTPS サイトや FTP サーバーにアクセスする場合、セッション Cookie を使用したユーザーの追跡はサポートされません。</p> |
| カスタム メッセージ<br>(Custom message) | <p>各エンドユーザー確認応答ページに表示するテキストをカスタマイズします。いくつかの単純な HTML タグを組み込んでテキストを書式設定できます。</p> <p><b>Note</b><br/>Web インターフェイスでエンドユーザー確認応答ページを設定する場合にのみカスタム メッセージを組み込むことができます。これは CLI では実行できません。</p> <p><a href="#">通知ページ上のカスタム メッセージ, on page 545</a>も参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**ステップ 5** (オプション) [確認応答ページのカスタマイズをプレビュー (Preview Acknowledgment Page Customization)] をクリックして、別のブラウザ ウィンドウに現在のエンドユーザー確認応答ページを表示します。

**Note**

HTML 通知ファイルを編集した場合、このプレビュー機能は使用できなくなります。

**ステップ 6** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## エンドユーザー通知ページ

ポリシーが Web サイトからユーザーをブロックする場合、URL 要求をブロックした理由をユーザーに通知するようにアプライアンスを設定できます。これは、以下のようないくつかの方法で実行できます。

| 目的                                                       | 参照先                                                  |
|----------------------------------------------------------|------------------------------------------------------|
| Secure Web Applianceでホストされている、事前定義され、カスタマイズ可能なページを表示します。 | <a href="#">オンボックス エンド ユーザー通知ページの設定, on page 539</a> |
| 特定の URL にある HTTP エンドユーザー通知ページにユーザーをリダイレクトします。            | <a href="#">オフボックスエンドユーザー通知ページ, on page 540</a>      |

## オンボックス エンド ユーザー通知ページの設定

**Before you begin**

- 表示言語の設定、および表示されるロゴのカスタマイズについては、[通知ページの一般設定項目の設定, on page 534](#) を参照してください。
- オンボックス通知を使用して表示されるメッセージをカスタマイズする場合は、[通知ページ上のカスタム メッセージ, on page 545](#) 以下のトピックを参照してください。[カスタム メッセージ (Custom Message)] ボックスでできること以上のカスタマイズが必要な場合は、[通知ページ HTML ファイルの直接編集, on page 547](#) を参照してください。

オンボックス ページは、アプライアンス上にある、事前定義されたカスタマイズ可能な通知ページです。

**Procedure**

- ステップ 1** [セキュリティ サービス (Security Services)] > [エンドユーザー通知 (End-User Notification)] を選択します。
- ステップ 2** [設定の編集 (Edit Settings)] をクリックします。
- ステップ 3** [通知タイプ (Notification Type)] フィールドで、[オンボックス エンド ユーザー通知を使用 (Use On Box End User Notification)] を選択します。

**ステップ 4** オンボックス エンドユーザー通知ページの設定項目を設定します。

| 設定                                                              | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| カスタム メッセージ<br>(Custom Message)                                  | 各通知ページに必要なテキストを追加します。カスタムメッセージを入力すると、AsyncOS は、連絡先情報を含む通知ページの末尾の文の前にメッセージを配置します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| コンタクト情報<br>(Contact Information)                                | 各通知ページに表示される連絡先情報をカスタマイズします。<br>AsyncOS は、ユーザーがネットワーク管理者に提供できる通知コードを表示する前に、連絡先情報の文をページの末尾の文として表示します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| エンドユーザー誤分類<br>レポート (End-User<br>Misclassification<br>Reporting) | 有効になっている場合、誤分類要求は、HTTPS プロキシが有効の場合はHTTPS 経由で送信され、それ以外の場合はHTTP 経由で送信されます。セキュリティアラート通知は受信しません。<br><br>イネーブルにすると、ユーザーは誤分類された URL をシスコに報告できます。マルウェアの疑いがあるため、または URL フィルタによってブロックされたサイトのオンボックス エンドユーザー通知ページには、追加のボタンが表示されます。このボタンを使用して、ユーザーは誤分類されていると思われるページをレポートできます。その他のポリシー設定によってブロックされたページには表示されません。<br><br><b>Note</b> <ul style="list-style-type: none"> <li>• [SensorBase ネットワークに参加 (SensorBase Network Participation) ] を有効にする必要があります。詳細については、「<a href="#">Cisco SensorBase ネットワークへの参加の有効化</a>」を参照してください。</li> <li>• アプライアンスのシリアル番号にリンクされている有効なシスコアカウントが必要です。</li> <li>• 誤分類された URL のレポートは、仮想 Secure Web Appliance では機能しません。</li> </ul> |

**ステップ 5** (オプション) [通知ページのカスタマイズをプレビュー (Preview Notification Page Customization) ] リンクをクリックして、別のブラウザ ウィンドウで現在のエンド ユーザー通知ページを表示します。

**Note**

HTML 通知ファイルを編集した場合、このプレビュー機能は使用できなくなります。

**ステップ 6** 変更を送信して確定します ([送信 (Submit) ] と [変更を確定 (Commit Changes) ]) 。

## オフボックス エンドユーザー通知ページ

すべての HTTP エンドユーザー通知ページを指定した特定の URL にリダイレクトするように Web プロキシを設定できます。

- [アクセスをブロックする理由に基づく適切なオフボックス ページの表示, on page 541](#)

- ## アクセスをブロックする理由に基づく適切なオフボックス ページの表示

Web サイトがブロックされた理由ごとに異なるページをユーザーに表示する場合は、リダイレクト URL のクエリー文字列を解析できる CGI スクリプトを Web サーバーに作成します。これによって、サーバーは適切なページに別のリダイレクトを実行できます。

以下の表は、AsyncOS がクエリ文字列に含めるパラメータを示しています。

| パラメータ名         | 説明                                                                                                                                                               |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time           | トランザクションの日付と時刻。                                                                                                                                                  |
| ID             | トランザクション ID。                                                                                                                                                     |
| Client_IP      | クライアントの IP アドレス。                                                                                                                                                 |
| User           | 要求を行うクライアントのユーザー名（該当する場合）。                                                                                                                                       |
| Site           | HTTP 要求の宛先ホスト名。                                                                                                                                                  |
| URI            | HTTP 要求で指定された URL パス。                                                                                                                                            |
| Status_Code    | 要求の HTTP ステータス コード。                                                                                                                                              |
| Decision_Tag   | DVS エンジンがトランザクションを処理した方法を示す、アクセス ログ エントリで定義されている ACL デシジョン タグ。                                                                                                   |
| URL_Cat        | URL フィルタリングエンジンがトランザクション要求に割り当てた URL カテゴリ。<br><br>注：AsyncOS for Web は、定義済みとユーザー定義の両方の URL カテゴリの URL カテゴリ名全体を送信します。カテゴリ名に対して URL エンコードが行われるため、スペースは「%20」と書き込まれます。 |
| WBRS           | Web レピュテーションフィルタが要求の URL に割り当てた WBRS スコア。                                                                                                                        |
| DVS_Verdict    | DVS エンジンがトランザクションに割り当てるマルウェア カテゴリ。                                                                                                                               |
| DVS_ThreatName | DVS エンジンによって検出されたマルウェアの名前。                                                                                                                                       |

| パラメータ名     | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reauth_URL | <p>制限付き URL フィルタリング ポリシーによって Web サイトからブロックされた場合、ユーザーはこの URL をクリックして再度認証を受けることができます。このパラメータは、[URLカテゴリまたはユーザー セッションの制限によりエンドユーザーがブロックされた場合に再認証プロンプトをイネーブルにする（Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction）] グローバル認証設定がイネーブルになっているときに、URL カテゴリがブロックされたため、ユーザーが Web サイトからブロックされた場合に使用します。</p> <p>このパラメータを使用するには、CGI スクリプトで以下の手順が実行されるようにします。</p> <ol style="list-style-type: none"> <li>1.Reauth_Url パラメータの値を取得する。</li> <li>2. URL エンコードされた値をデコードする。</li> <li>3. 値を Base64 でデコードし、実際の再認証 URL を取得する。</li> <li>4. デコードした URL を何らかの方法で（リンクまたはボタンとして）エンドユーザー通知ページに組み込み、「リンクをクリックすると、より広範なアクセスが可能になる新しい認証クレデンシャルを入力できること」をユーザーに示す使用説明を含める。</li> </ol> |



**Note** AsyncOS は、リダイレクトされた各 URL に、常にすべてのパラメータを組み込みます。特定のパラメータの値が存在しない場合、AsyncOS はハイフン (-) を渡します。

## カスタム URL へのエンドユーザー通知ページのリダイレクト（オフボックス）

### Procedure

- ステップ 1** [セキュリティ サービス（Security Services）] > [エンドユーザー通知（End-User Notification）] を選択します。
- ステップ 2** [設定の編集（Edit Settings）] をクリックします。
- ステップ 3** [エンドユーザー通知ページ（End-User Notification Pages）] セクションで、[カスタム URL へのリダイレクト（Redirect to Custom URL）] を選択します。
- ステップ 4** [通知ページの URL（Notification Page URL）] フィールドに、ブロックされた Web サイトをリダイレクトする URL を入力します。
- ステップ 5** （オプション）[カスタム URL のプレビュー（Preview Custom URL）] をクリックします。
- ステップ 6** 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。



## エンドユーザー URL フィルタリング警告ページの設定

### Before you begin

- オンボックス通知を使用して表示されるメッセージをカスタマイズする場合は、[通知ページ上のカスタム メッセージ, on page 545](#) 以下のトピックを参照してください。[カスタム メッセージ (Custom Message)] ボックスでできること以上のカスタマイズが必要な場合は、[通知ページ HTML ファイルの直接編集, on page 547](#) を参照してください。

エンドユーザー URL フィルタリング警告ページは、ユーザーが特定の URL カテゴリの Web サイトに初めてアクセスしてから一定時間経過後に表示されます。サイトコンテンツレーティング機能がイネーブルのときに、ユーザーがアダルト コンテンツにアクセスした場合の警告ページを設定することもできます。

### Procedure

- ステップ 1** [セキュリティ サービス (Security Services)] > [エンドユーザー通知 (End-User Notification)] を選択します。
- ステップ 2** [設定の編集 (Edit Settings)] をクリックします。
- ステップ 3** [エンドユーザーフィルタリング警告ページ (End-User URL Filtering Warning Page)] セクションまでスクロール ダウンします。
- ステップ 4** [確認応答の時間間隔 (Time Between Warning)] フィールドで、Web プロキシがユーザーごとに各 URL カテゴリに対してエンドユーザー URL フィルタリング警告ページを表示する時間間隔を入力します。  
30 ～ 2678400 秒 (1 か月) の任意の値を指定できます。デフォルトは 1 時間 (3600 秒) です。秒、分、または日単位で値を入力できます。秒には「s」、分には「m」、日には「d」を使用します。
- ステップ 5** [カスタム メッセージ (Custom Message)] フィールドで、すべてのエンドユーザー URL フィルタリング警告ページに表示するテキストを入力します。
- ステップ 6** [URL カテゴリ警告ページのカスタマイズをプレビュー (Preview URL Category Warning Page Customization)] をクリックして、別のブラウザ ウィンドウでエンドユーザー URL フィルタリング警告ページを表示します。

### Note

HTML 通知ファイルを編集した場合、このプレビュー機能は使用できなくなります。

- ステップ 7** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## FTP 通知メッセージの設定

### Before you begin

オンボックス通知を使用して表示されるメッセージをカスタマイズする場合は、[通知ページ上のカスタムメッセージ, on page 545](#)以下のトピックを参照してください。[カスタムメッセージ (Custom Message)] ボックスでできること以上のカスタマイズが必要な場合は、[通知ページ HTML ファイルの直接編集, on page 547](#)を参照してください。

FTP サーバーの認証エラーやサーバー ドメイン名に対する低いレピュテーションなど、何らかの理由により FTP プロキシが FTP サーバーとの接続を確立できない場合、FTP プロキシはネイティブ FTP クライアントに定義済みのカスタマイズ可能な通知メッセージを表示します。通知は、接続がブロックされる理由によって固有なものになります。

### Procedure

- ステップ 1 [セキュリティ サービス (Security Services)] > [エンドユーザー通知 (End-User Notification)] を選択します。
- ステップ 2 [設定の編集 (Edit Settings)] をクリックします。
- ステップ 3 [ネイティブ FTP (Native FTP)] セクションまでスクロール ダウンします。
- ステップ 4 [言語 (Language)] フィールドで、ネイティブ FTP 通知メッセージを表示する際に使用する言語を選択します。
- ステップ 5 [カスタム メッセージ (Custom Message)] フィールドで、すべてのネイティブ FTP 通知メッセージに表示するテキストを入力します。
- ステップ 6 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## 通知ページ上のカスタム メッセージ

以下のセクションの説明は、[エンドユーザー通知の編集 (Edit End-User Notification)] ページで設定した任意の通知タイプの [カスタム メッセージ (Custom Message)] ボックスに入力するテキストに適用されます。

- [通知ページのカスタム メッセージでサポートされる HTML タグ, on page 545](#)
- [通知ページの URL とロゴに関する注意事項, on page 546](#)

## 通知ページのカスタム メッセージでサポートされる HTML タグ

[カスタム メッセージ (Custom Message)] ボックスが用意された [エンドユーザー通知の編集 (Edit End-User Notification)] ページでは、HTML タグを使用して、任意の通知のテキストを書式設定することができます。タグは小文字で入力し、標準 HTML 構文 (終了タグなど) に従う必要があります。

以下の HTML タグを使用できます。

- `<a></a>`
- `<span></span>`
- `<b></b>`
- `<big></big>`
- `<br>`
- `<code></code>`
- `<em></em>`
- `<i></i>`
- `<small></small>`
- `<strong></strong>`

たとえば、一部のテキストを斜体にすることができます。

Please acknowledge the following statements `<i>before</i>` accessing the Internet.

`<span>` タグにより、CSS スタイルを使用してテキストを書式設定できます。たとえば、一部のテキストを赤色にすることができます。

`<span style="color: red">Warning:</span>` You must acknowledge the following statements `<i>before</i>` accessing the Internet.



#### Note

通知ページをさらに柔軟にする必要がある場合や、JavaScript を追加したい場合は、HTML 通知ファイルを直接編集します。通知の [カスタム メッセージ (Custom Message)] ボックスに入力した JavaScript は、Web ユーザーのインターフェイスでは削除されます。「[通知ページ HTML ファイルの直接編集](#), on page 547」を参照してください。

## 通知ページの URL とロゴに関する注意事項

この項は以下のいずれかのカスタマイズを行う場合に適用されます。

- [エンドユーザー通知の編集 (Edit End-User Notification)] ページで、任意の通知の [カスタム メッセージ (Custom Message)] ボックスにテキストを入力する。
- オンボックス通知の HTML ファイルを直接編集する。
- カスタム ロゴを使用する。

オンボックス通知の場合、カスタム テキストにリンクが埋め込まれた URL パスとドメイン名の新組み合わせとカスタム ロゴのあらゆる組み合わせが、以下のものから免除されます。

- ユーザー認証
- エンドユーザー確認応答
- マルウェア スキャンおよび Web レピュテーション スコアなどのすべてのスキャン

たとえば、以下の URL がカスタム テキストに埋め込まれている場合、

`http://www.example.com/index.html`

`http://www.mycompany.com/logo.jpg`

以下の URL すべてがあらゆるスキャンの対象外として扱われます。

```
http://www.example.com/index.html
http://www.mycompany.com/logo.jpg
http://www.example.com/logo.jpg
http://www.mycompany.com/index.html
```

また、埋め込まれた URL の形式が `<protocol>://<domain-name>/<directory path>/` である場合、ホスト上のそのディレクトリパスにあるすべてのサブファイルとサブディレクトリもすべてのスキャンから除外されます。

たとえば、`http://www.example.com/gallery2/` という URL が埋め込まれている場合は、`http://www.example.com/gallery2/main.php` などの URL も対象外として扱われます。

これにより、埋め込まれたコンテンツが最初の URL に関連している限り、埋め込まれたコンテンツを使用してより高度なページを作成することができます。ただし、リンクやカスタムロゴとして含めるパスを決定する際に注意を払う必要があります。

## 通知ページ HTML ファイルの直接編集

各通知ページは、Secure Web Applianceに HTML ファイルとして保存されます。Web ベース インターフェイスの [カスタム メッセージ (Custom Message)] ボックスでできること以上のカスタマイズが必要な場合は、これらの HTML ファイルを直接編集できます。たとえば、標準 JavaScript を含めるか、または各ページの全体的なルック アンド フィールを編集できます。

以下の各項の情報は、エンドユーザー確認ページなど、アプライアンスの任意の種類のエンドユーザー通知 HTML ファイルに適用されます。

- [通知 HTML ファイルを直接編集するための要件](#), on page 547
- [通知ページ HTML ファイルの直接編集](#), on page 547
- [通知 HTML ファイルでの変数の使用](#), on page 548
- [通知 HTML ファイルのカスタマイズのための変数](#), on page 549

### 通知 HTML ファイルを直接編集するための要件

- 個々の通知ページ ファイルは、有効な HTML ファイルである必要があります。組み込むことができる HTML タグのリストについては、[通知ページのカスタム メッセージでサポートされる HTML タグ](#), on page 545を参照してください。
- カスタマイズした通知ページ ファイルの名前は、Secure Web Applianceに同梱されているファイルの名前と正確に一致する必要があります。

configuration\eun ディレクトリに必要な名前を持つ特定のファイルが含まれていない場合、アプライアンスは標準のオンボックス エンドユーザー通知ページを表示します。

- HTML ファイルに URL へのリンクを含めないでください。通知ページに含まれるリンクは、アクセス ポリシーで定義されたアクセス制御ルールの対象となり、ユーザーは再帰ループで終了する場合があります。

- 特に JavaScript が含まれている場合は、期待どおりに動作することを確認するために、サポートされているクライアントのブラウザで HTML ファイルをテストします。
- カスタマイズしたページが効果を表すようにするには、`advancedproxyconfig > EUN > Refresh EUN Pages` CLI コマンドを使用して、カスタマイズしたファイルを有効化する必要があります。

## 通知 HTML ファイルの直接編集

### Before you begin

- [通知 HTML ファイルを直接編集するための要件](#) , [on page 547](#) の要件を確認します。
- [通知 HTML ファイルのカスタマイズのための変数](#) , [on page 549](#) および [通知 HTML ファイルでの変数の使用](#) , [on page 548](#) を参照してください。

### Procedure

- 
- ステップ 1** FTP クライアントを使用して、Secure Web Appliance に接続します。
- ステップ 2** `configuration\eun` ディレクトリに移動します。
- ステップ 3** 編集する通知ページの言語ディレクトリ ファイルをダウンロードします。
- ステップ 4** ローカルマシンで、テキストエディタまたは HTML エディタを使用して HTML ファイルを編集します。
- ステップ 5** FTP クライアントを使用して、ステップ 3 でこれらのファイルをダウンロードした同じディレクトリに、カスタマイズした HTML ファイルをアップロードします。
- ステップ 6** SSH クライアントを開き、Secure Web Appliance に接続します。
- ステップ 7** `advancedproxyconfig > EUN` CLI コマンドを実行します。
- ステップ 8** 2 を入力して、カスタム エンド ユーザー通知ページを使用します。
- ステップ 9** HTML ファイルを更新する際にカスタム エンド ユーザー通知ページ オプションがイネーブルになっている場合は、1 を入力して、カスタム エンド ユーザー通知ページを更新します。
- これを実行しないと、Web プロキシを再起動するまで新しいファイルが有効になりません。
- ステップ 10** 変更を保存します。
- ステップ 11** SSH クライアントを閉じます。
- 

## 通知 HTML ファイルでの変数の使用

通知 HTML ファイルを編集する際に、条件変数を含めると、実行時点のステータスに応じて異なるアクションを実行する if-then ステートメントを作成できます。

以下の表は、さまざまな条件変数の形式を示しています。

| 条件変数の形式          | 説明                                                                               |
|------------------|----------------------------------------------------------------------------------|
| <code>??V</code> | 変数 <code>%V</code> の出力が空でない場合、この条件変数は TRUE に評価されます。                              |
| <code>!V</code>  | 以下の条件を表します。<br><br><code>else</code><br><br>これを <code>??V</code> 条件変数とともに使用します。  |
| <code>##V</code> | 以下の条件を表します。<br><br><code>endif</code><br><br>これを <code>??V</code> 条件変数とともに使用します。 |

たとえば、以下の HTML コードの一部であるテキストでは、再認証が提供されるかどうかをチェックする条件変数として `%R` が使用され、再認証 URL を提供する標準変数として `%r` が使用されています。

```

??R
<div align="left">
 <form name="ReauthInput" action="%r" method="GET">
 <input name="Reauth" type="button" OnClick="document.location='%r'" id="Reauth"
 value="Login as different user...">
 </form>
</div>
##R

```

[通知 HTML ファイルのカスタマイズのための変数, on page 549](#)に記載されている任意の変数を条件変数として使用できます。ただし、条件文での使用に最も適した変数は、サーバー応答ではなく、クライアント要求に関連する変数であり、常に TRUE に評価される変数ではなく、状況に応じて TRUE に評価される（または評価されない）変数です。

## 通知 HTML ファイルのカスタマイズのための変数

通知 HTML ファイルで変数を使用して、ユーザー固有の情報を表示できます。また、各変数を条件変数に変換して、if-then ステートメントを作成することもできます。詳細については、[通知 HTML ファイルでの変数の使用, on page 548](#)を参照してください。

| 変数              | 説明                                    | 条件変数として使用する場合、常に TRUE に評価 |
|-----------------|---------------------------------------|---------------------------|
| <code>%a</code> | FTP の認証レلم                            | 非対応                       |
| <code>%A</code> | ARP アドレス                              | 対応                        |
| <code>%b</code> | ユーザーエージェント名                           | 非対応                       |
| <code>%B</code> | ブロックした理由（BLOCK-SRC または BLOCK-TYPE など） | 非対応                       |
| <code>%c</code> | エラー ページの担当者                           | 対応                        |

| 変数 | 説明                                                      | 条件変数として使用する<br>場合、常に <b>TRUE</b> に評価 |
|----|---------------------------------------------------------|--------------------------------------|
| %C | Set-Cookie: ヘッダー行全体、または空の文字列                            | 非対応                                  |
| %d | クライアント IP アドレス                                          | 対応                                   |
| %D | ユーザー名                                                   | 非対応                                  |
| %e | エラー ページの電子メール アドレス                                      | 対応                                   |
| %E | エラー ページのロゴの URL                                         | 非対応                                  |
| %f | ユーザー フィードバック セクション                                      | 非対応                                  |
| %F | ユーザー フィードバックの URL                                       | 非対応                                  |
| %g | Web カテゴリ名（使用可能な場合）                                      | 対応                                   |
| %G | 許可される最大ファイル サイズ（MB 単位）                                  | 非対応                                  |
| %h | プロキシのホスト名                                               | 対応                                   |
| %H | URL のサーバー名                                              | 対応                                   |
| %i | トランザクション ID（16 進数値）                                     | 対応                                   |
| %I | 管理 IP アドレス                                              | 対応                                   |
| %j | URL カテゴリ 警告ページのカスタム テキスト                                | 非対応                                  |
| %k | エンドユーザー 確認応答ページおよびエンドユーザー URL フィルタリング警告ページのリダイレクション リンク | 非対応                                  |
| %K | レスポンス ファイル タイプ                                          | 非対応                                  |
| %l | WWW-Authenticate: ヘッダー行                                 | 非対応                                  |
| %L | Proxy-Authenticate: ヘッダー行                               | 非対応                                  |
| %M | 要求方式（「GET」、「POST」など）                                    | 対応                                   |
| %n | マルウェア カテゴリ名（使用可能な場合）                                    | 非対応                                  |
| %N | マルウェア 脅威名（使用可能な場合）                                      | 非対応                                  |
| %o | Web レピュテーションの脅威タイプ（使用可能な場合）                             | 非対応                                  |
| %O | Web レピュテーションの脅威の理由（使用可能な場合）                             | 非対応                                  |
| %p | Proxy-Connection HTTP ヘッダーの文字列                          | 対応                                   |

| 変数 | 説明                                                                                                          | 条件変数として使用する場合、常に <b>TRUE</b> に評価 |
|----|-------------------------------------------------------------------------------------------------------------|----------------------------------|
| %P | Protocol                                                                                                    | 対応                               |
| %q | ID ポリシー グループの名前                                                                                             | 対応                               |
| %Q | 非 ID ポリシーのポリシー グループ名                                                                                        | 対応                               |
| %r | リダイレクト URL                                                                                                  | 非対応                              |
| %R | 再認証が提供されます。この変数は、 <b>false</b> の場合に空の文字列を出力し、 <b>true</b> の場合にスペースを出力するので、単独で使用しても役立ちません。代わりに、条件変数として使用します。 | 非対応                              |
| %S | プロキシの署名                                                                                                     | なし。常に <b>FALSE</b> に評価           |
| %t | UNIX のタイムスタンプ (秒 + ミリ秒)                                                                                     | 対応                               |
| %T | 日付                                                                                                          | 対応                               |
| %u | URI の一部を構成する URL (サーバー名を除く URL)                                                                             | 対応                               |
| %U | 要求の完全な URL                                                                                                  | 対応                               |
| %v | HTTP プロトコルのバージョン                                                                                            | 対応                               |
| %W | 管理 WebUI ポート                                                                                                | 対応                               |
| %X | 拡張ブロック コード。ACL デシジョン タグや WBRs スコアなど、アクセス ログに記録された大部分の Web レピュテーションやアンチマルウェア情報をエンコードする 16 バイトの Base64 値です。   | 対応                               |
| %Y | 設定されている場合は、管理者のカスタム テキスト文字列。設定されていない場合は空の文字列                                                                | 非対応                              |
| %y | エンドユーザー確認応答ページのカスタム テキスト                                                                                    | 対応                               |
| %z | Web レピュテーション スコア                                                                                            | 対応                               |
| %Z | DLP メタデータ                                                                                                   | 対応                               |
| %% | 通知ページにパーセント記号 (%) を出力します                                                                                    | N/A                              |



## 通知ページのタイプ

デフォルトでは、Web プロキシは、ユーザーがブロックされたことおよびその理由をユーザーに知らせる通知ページを表示します。

ほとんどの通知ページは、管理者または Cisco カスタマー サポートが潜在的な問題をトラブルシューティングするのに役立つ可能性のあるさまざまなコードのセットを表示します。一部のコードはシスコ内部でのみ使用されます。通知ページに表示されるさまざまなコードは、カスタマイズした通知ページに含めることができる変数と同じです（[通知 HTML ファイルのカスタマイズのための変数](#), on page 549 を参照）。

以下の表は、ユーザーに表示される可能性があるさまざまな通知ページを示しています。

| ファイル名および<br>通知タイトル                                                           | 通知の説明                                                                | 通知テキスト                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_ACCEPTED<br>フィードバックを受信しました。ありがとうございます。<br>(Feedback Accepted, Thank You) | ユーザーが [誤分類をレポート (Report Misclassification) ] オプションを使用した後に表示される通知ページ。 | 誤分類のレポートが送信されました。（The misclassification report has been sent.）フィードバックいただき、ありがとうございます。（Thank you for your feedback.）                                                                                                               |
| ERR_ADAPTIVE_SECURITY<br>ポリシー：全般<br>(Policy: General)                        | ユーザーが適応型スキャン機能によってブロックされた場合に表示されるブロック ページ。                           | この Web サイト <URL> は、コンテンツがセキュリティ リスクであると判定されたため、組織のセキュリティ ポリシーに基づいてブロックされました。（Based on your organization's security policies, this web site <URL> has been blocked because its content has been determined to be a security risk.） |

| ファイル名および<br>通知タイトル                                         | 通知の説明                                                                                  | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_ADULT_CONTENT<br>ポリシーの確認<br>(Policy<br>Acknowledgment) | エンドユーザーがアダルトコンテンツに分類されるページにアクセスしたときに表示される警告ページ。ユーザーは確認リンクをクリックして、最初に要求したサイトに進むことができます。 | 明示的にアダルト向けとレーティングされたコンテンツを含む Web ページにアクセスしようとしています。（You are trying to visit a web page whose content are rated as explicit or adult.）下記のリンクをクリックし、このコンテンツタイプに対するインターネットの使用を管理している組織のポリシーを讀了して同意済みであることを確認してください。（By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content.）ブラウジング動作に関するデータがモニターされ、記録される場合があります。（Data about your browsing behavior may be monitored and recorded.）この種の Web ページに引き続きアクセスした場合は、このメッセージが定期的に提示され、確認を求められます。（You will be periodically asked to acknowledge this statement for continued access to this kind of web page.）<br><br>このステートメントに同意してインターネットにアクセスするには、ここをクリックしてください。（Click here to accept this statement and access the Internet.） |
| ERR_AVC<br>ポリシー：アプリケーションの制御 (Policy: Application Controls) | ユーザーが Application Visibility and Control エンジンによってブロックされた場合に表示されるブロックページ。               | 組織のアクセス ポリシーに基づき、タイプ %2 のアプリケーション %1 へのアクセスがブロックされました。（Based on your organization's access policies, access to application %1 of type %2 has been blocked.）                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| ファイル名および<br>通知タイトル                                   | 通知の説明                                                 | 通知テキスト                                                                                                                                                                                                                                                                             |
|------------------------------------------------------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_BAD_REQUEST<br>不正な要求 (Bad Request)               | 無効なトランザクション要求によって生じるエラー ページ。                          | システムはこの要求を処理できません。 (The system cannot process this request.) 非標準のブラウザによって無効な HTTP 要求が生成された可能性があります。 (A non-standard browser may have generated an invalid HTTP request.)<br><br>標準ブラウザを使用している場合は、要求を再試行してください。<br>(If you are using a standard browser, please retry the request.) |
| ERR_BLOCK_DEST<br>ポリシー : 宛先<br>(Policy: Destination) | ブロックされている Web サイトのアドレスにユーザーがアクセスを試みた場合に表示されるブロック ページ。 | 組織のアクセス ポリシーに基づき、この Web サイト <URL> へのアクセスがブロックされました。<br>(Based on your organization's Access Policies, access to this web site <URL> has been blocked.)                                                                                                                             |

| ファイル名および<br>通知タイトル                                | 通知の説明                                                                      | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_BROWSER<br>セキュリティ：ブラウザ<br>(Security: Browser) | マルウェアまたはスパイウェアによって侵害されていると識別されたアプリケーションからトランザクション要求が発信された場合に表示されるブロック ページ。 | <p>組織のネットワークに対するセキュリティ上の脅威であると判定されたため、組織のアクセスポリシーに基づき、コンピュータからの要求がブロックされました。</p> <p>(Based on your organization's Access Policies, requests from your computer have been blocked because it has been determined to be a security threat to the organization's network.)</p> <p>「&lt;マルウェア名&gt;」として識別されたマルウェア/スパイウェアエージェントによってブラウザが侵害されている可能性があります。</p> <p>(Your browser may have been compromised by a malware/spyware agent identified as "&lt;malware name&gt;".)</p> <p>&lt;担当者名&gt;&lt;電子メールアドレス&gt;に連絡し、以下に示すコードを提出してください。(Please contact &lt;contact name&gt; &lt;email address&gt; and provide the codes shown below.)</p> <p>非標準のブラウザを使用しており、誤って分類されたと思われる場合は、以下のボタンを使用してこの誤分類をレポートしてください。(If you are using a non-standard browser and believe it has been misclassified, use the button below to report this misclassification.)</p> |

| ファイル名および<br>通知タイトル                                   | 通知の説明                                                 | 通知テキスト                                                                                                                                                                                                                                                            |
|------------------------------------------------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_BROWSER_CUSTOM<br>ポリシー：ブラウザ<br>(Policy: Browser) | ブロックされたユーザー エージェントからトランザクション要求が発信されたときに表示されるブロック ページ。 | 組織のアクセス ポリシーに基づき、ブラウザからの要求がブロックされました。(Based on your organization's Access Policies, requests from your browser have been blocked.) このブラウザ「<ブラウザ タイプ>」は、潜在的なセキュリティ リスクのため許可されません。(This browser "<browser type>" is not permitted due to potential security risks.) |
| ERR_CERT_INVALID<br>無効な証明書 (Invalid Certificate)     | 要求された HTTPS サイトが無効な証明書を使用している場合に表示されるブロック ページ。        | サイト <ホスト名> が無効な証明書を提示したため、セキュアセッションを確立できません。(A secure session cannot be established because the site <hostname> provided an invalid certificate.)                                                                                                                 |

| ファイル名および<br>通知タイトル                                                           | 通知の説明                                                                                             | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_CONTINUE_<br>UNACKNOWLEDGED<br><br>ポリシーの確認<br>(Policy<br>Acknowledgment) | 警告アクションが割り当てられているカスタム URL カテゴリのサイトをユーザーが要求した場合に表示される警告ページ。ユーザーは確認リンクをクリックして、最初に要求したサイトに進むことができます。 | URL カテゴリ <URL カテゴリ> に分類される Web ページにアクセスしようとしています。（You are trying to visit a web page that falls under the URL Category <URL category>。）下記のリンクをクリックし、このコンテンツタイプに対するインターネットの使用を管理している組織のポリシーを読了して同意済みであることを確認してください。（By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content.）ブラウジング動作に関するデータがモニターされ、記録される場合があります。（Data about your browsing behavior may be monitored and recorded.）この種の Web ページに引き続きアクセスした場合は、このメッセージが定期的に提示され、確認を求められます。（You will be periodically asked to acknowledge this statement for continued access to this kind of web page.）<br><br>このステートメントに同意してインターネットにアクセスするには、ここをクリックしてください。（Click here to accept this statement and access the Internet.） |

| ファイル名および<br>通知タイトル                                      | 通知の説明                                                               | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_DNS_FAIL<br>DNS の障害 (DNS Failure)                   | 要求された URL に無効なドメイン名が含まれている場合に表示されるエラー ページ。                          | <p>このホスト名 &lt;ホスト名&gt; のホスト名解決 (DNS ルックアップ) に失敗しました。 (The hostname resolution (DNS lookup) for this hostname &lt;hostname&gt; has failed.) インターネットアドレスのスペルが誤っているか、インターネットアドレスが廃止されているか、ホスト &lt;ホスト名&gt; が一時的に利用できないか、または DNS サーバーが無応答状態になっている可能性があります。 (The Internet address may be misspelled or obsolete, the host &lt;hostname&gt; may be temporarily unavailable, or the DNS server may be unresponsive.)</p> <p>入力したインターネットアドレスのスペルを確認してください。<br/>(Please check the spelling of the Internet address entered.) スペルが正しい場合は、後でこの要求を試行してください。 (If it is correct, try this request later.)</p> |
| ERR_EXPECTATION_FAILED<br>予測の失敗<br>(Expectation Failed) | トランザクション要求が HTTP 417 「Expectation Failed」 応答をトリガーしたときに表示されるエラー ページ。 | <p>システムはこのサイト &lt;URL&gt; に対する要求を処理できません。<br/>(The system cannot process the request for this site &lt;URL&gt;.) 非標準のブラウザによって無効な HTTP 要求が生成された可能性があります。 (A non-standard browser may have generated an invalid HTTP request.)</p> <p>標準ブラウザを使用している場合は、要求を再試行してください。<br/>(If using a standard browser, please retry the request.)</p>                                                                                                                                                                                                                                                             |

| ファイル名および<br>通知タイトル                                | 通知の説明                                                                                                                                                      | 通知テキスト                                                                                                                                                                                                                                                   |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_FILE_SIZE<br>ポリシー：ファイルサイズ (Policy: File Size) | 要求されたファイルが許容される最大ファイルサイズよりも大きい場合に表示されるブロック ページ。                                                                                                            | ダウンロードサイズが許容限度を超えているため、組織のアクセス ポリシーに基づき、この Web サイトまたはダウンロード<URL>へのアクセスがブロックされました。<br>(Based on your organization's Access Policies, access to this web site or download <URL> has been blocked because the download size exceeds the allowed limit.)     |
| ERR_FILE_TYPE<br>ポリシー：ファイルタイプ (Policy: File Type) | 要求したファイルがブロックされているファイルタイプである場合に表示されるブロック ページ。                                                                                                              | ファイル タイプ「<ファイル タイプ>」は許可されていないため、組織のアクセス ポリシーに基づき、この Web サイトまたはダウンロード<URL>へのアクセスがブロックされました。(Based on your organization's Access Policies, access to this web site or download <URL> has been blocked because the file type "<file type>" is not allowed.) |
| ERR_FILTER_FAILURE<br>フィルタの障害 (Filter Failure)    | URL フィルタリングエンジンが一時的に URL フィルタリング応答を配信できず、[到達不能サービスに対するデフォルトアクション (Default Action for Unreachable Service) ] オプションが[ブロック (Block) ] に設定されている場合に表示されるエラー ページ。 | 内部サーバーが到達不能または過負荷になっているため、ページ<URL>の要求が拒否されました。<br>(The request for page <URL> has been denied because an internal server is currently unreachable or overloaded.)<br>後で要求を再試行してください。<br>(Please retry the request later.)                                |
| ERR_FOUND<br>検出 (Found)                           | 一部のエラー用の内部リダイレクション ページ。                                                                                                                                    | ページ<URL>は<リダイレクト先 URL> にリダイレクトされます。<br>(The page <URL> is being redirected to <redirected URL>.)                                                                                                                                                         |



| ファイル名および<br>通知タイトル                                                        | 通知の説明                                                                                                         | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_FTP_ABORTED<br>FTP 中断 (FTP<br>Aborted)                                | FTP over HTTP トランザクション<br>要求が HTTP 416 「Requested Range<br>Not Satisfiable」 応答をトリガーし<br>たときに表示されるエラー ペー<br>ジ。 | ファイル<URL>に対する要求が成<br>功しませんでした。 (The request<br>for the file <URL> did not succeed.)<br>FTP サーバー <ホスト名> が突然<br>接続を終了しました。 (The FTP<br>server <hostname> unexpectedly<br>terminated the connection.)<br><br>後で要求を再試行してください。<br>(Please retry the request later.)                                                                                                                                                                                                                                                |
| ERR_FTP_AUTH_<br>REQUIRED<br>FTP 認可が必要 (FTP<br>Authorization<br>Required) | FTP over HTTP トランザクション<br>要求が FTP 530 「Not Logged In」<br>応答をトリガーしたときに表示さ<br>れるエラー ページ。                        | FTP サーバー <ホスト名> には認<br>証が必要です。 (Authentication is<br>required by the FTP server<br><hostname>.) プロンプトに従って<br>有効なユーザー ID とパスフレーズ<br>を入力してください。 (A valid<br>user ID and passphrase must be<br>entered when prompted.)<br><br>場合により、FTP サーバーが匿名<br>接続の数を制限する可能性があり<br>ます。 (In some cases, the FTP<br>server may limit the number of<br>anonymous connections.) 通常、匿<br>名ユーザーとしてこのサーバーに<br>接続している場合は、後で再試行<br>してください。 (If you usually<br>connect to this server as an anonymous<br>user, please try again later.) |

| ファイル名および<br>通知タイトル                                             | 通知の説明                                                                                    | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_FTP_CONNECTION_FAILED<br>FTP 接続の失敗 (FTP Connection Failed) | FTP over HTTP トランザクション要求が FTP 425 「Can't open data connection」 応答をトリガーしたときに表示されるエラー ページ。 | システムが FTP サーバー <ホスト名> と通信できません。 (The system cannot communicate with the FTP server <hostname>.) FTP サーバーが一時的または恒久的にダウンしているか、ネットワークの問題により到達不能になっている可能性があります。 (The FTP server may be temporarily or permanently down, or may be unreachable because of network problems.)<br><br>入力したアドレスのスペルを確認してください。 (Please check the spelling of the address entered.) スペルが正しい場合は、後でこの要求を試行してください。 (If it is correct, try this request later.) |
| ERR_FTP_FORBIDDEN<br>FTP の禁止 (FTP Forbidden)                   | FTP over HTTP トランザクション要求が、ユーザーアクセスが許可されないオブジェクトに対して行われた場合に表示されるエラー ページ。                  | FTP サーバー <ホスト名> によってアクセスが拒否されました。 (Access was denied by the FTP server <hostname>.) ご使用の ID にはこのドキュメントへのアクセス権がありません。 (Your user ID does not have permission to access this document.)                                                                                                                                                                                                                                             |
| ERR_FTP_NOT_FOUND<br>FTP が検出されない (FTP Not Found)               | FTP over HTTP トランザクション要求が、サーバー上に存在しないオブジェクトに対して行われた場合に表示されるエラー ページ。                      | ファイル<URL>が見つかりませんでした。 (The file <URL> could not be found.) アドレスが間違っているか、または廃止されています。 (The address is either incorrect or obsolete.)                                                                                                                                                                                                                                                                                               |

| ファイル名および<br>通知タイトル                                                   | 通知の説明                                                                                                            | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_FTP_SERVER_ERR<br>FTP サーバー エラー<br>(FTP Server Error)             | FTP をサポートしていないサーバーにアクセスを試みている FTP over HTTP トランザクションに対して表示されるエラーページ。通常、サーバーは HTTP 501 「Not Implemented」 応答を返します。 | システムが FTP サーバー <ホスト名> と通信できません。 (The system cannot communicate with the FTP server <hostname>.) FTP サーバーが一時的または恒久的にダウンしているか、このサービスを提供していない可能性があります。<br>(The FTP server may be temporarily or permanently down, or may not provide this service.)<br><br>有効なアドレスであることを確認してください。 (Please confirm that this is a valid address.) スペルが正しい場合は、後でこの要求を試行してください。 (If it is correct, try this request later.)   |
| ERR_FTP_SERVICE_UNAVAIL<br>FTP サービス使用不可<br>(FTP Service Unavailable) | 使用できないFTPサーバーにアクセスを試みている FTP over HTTP トランザクションに対して表示されるエラー ページ。                                                 | システムが FTP サーバー <ホスト名> と通信できません。 (The system cannot communicate with the FTP server <hostname>.) FTP サーバーがビジー状態であるか、恒久的にダウンしているか、またはこのサービスを提供していない可能性があります。 (The FTP server may be busy, may be permanently down, or may not provide this service.)<br><br>有効なアドレスであることを確認してください。 (Please confirm that this is a valid address.) スペルが正しい場合は、後でこの要求を試行してください。 (If it is correct, try this request later.) |

| ファイル名および<br>通知タイトル                                                           | 通知の説明                                                                                          | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_GATEWAY_TIMEOUT<br>ゲートウェイのタイム<br>アウト (Gateway<br>Timeout)                | 要求されたサーバーがタイムリー<br>に応答しなかったときに表示され<br>るエラー ページ。                                                | システムが外部サーバー <ホスト<br>名> と通信できません。 (The<br>system cannot communicate with the<br>external server <hostname>.) イン<br>ターネットサーバーがビジー状態<br>か、恒久的にダウンしているか、<br>またはネットワークの問題により<br>到達不能になっている可能性があ<br>ります。 (The Internet server may<br>be busy, may be permanently down,<br>or may be unreachable because of<br>network problems.)<br><br>入力したインターネットアドレス<br>のスペルを確認してください。<br>(Please check the spelling of the<br>Internet address entered.) スペルが<br>正しい場合は、後でこの要求を試<br>行してください。 (If it is correct,<br>try this request later.) |
| ERR_IDS_ACCESS_<br>FORBIDDEN<br><br>IDS アクセスの禁止<br>(IDS Access<br>Forbidden) | 設定済みの Cisco データ セキュリ<br>ティポリシーによってブロックさ<br>れているファイルを、ユーザーが<br>アップロードしようとした場合に<br>表示されるエラー ページ。 | 組織のデータ転送ポリシーに基づ<br>き、アップロード要求がブロック<br>されました。 (Based on your<br>organization's data transfer policies,<br>your upload request has been<br>blocked.) ファイルの詳細 (File<br>details) :<br><br><ファイルの詳細>                                                                                                                                                                                                                                                                                                                           |

| ファイル名および<br>通知タイトル                                                        | 通知の説明                                     | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_INTERNAL_ERROR<br>内部エラー (Internal Error)                              | 内部エラーが発生した場合に表示されるエラー ページ。                | <p>ページ&lt;URL&gt;に対する要求を処理中に内部システムエラーが発生しました。(Internal system error when processing the request for the page &lt;URL&gt;.)</p> <p>この要求を再試行してください。<br/>(Please retry this request.)</p> <p>この状態が続く場合は、&lt;担当者名&gt;&lt;電子メールアドレス&gt;に連絡し、以下に示すコードを提出してください。(If this condition persists, please contact &lt;contact name&gt; &lt;email address&gt; and provide the code shown below.)</p>                                                                                             |
| ERR_MALWARE_SPECIFIC<br>セキュリティ : マルウェアの検出<br>(Security: Malware Detected) | ファイルのダウンロード時にマルウェアが検出された場合に表示されるブロック ページ。 | <p>この Web サイト &lt;URL&gt; は、コンピュータまたは組織のネットワークに対するセキュリティ上の脅威と判定されたため、組織のアクセスポリシーに基づいてブロックされました。(Based on your organization's Access Policies, this web site &lt;URL&gt; has been blocked because it has been determined to be a security threat to your computer or the organization's network.)</p> <p>カテゴリ &lt;マルウェア カテゴリ&gt; のマルウェア &lt;マルウェア名&gt; がこのサイトで検出されました。<br/>(Malware &lt;malware name&gt; in the category &lt;malware category&gt; has been found on this site.)</p> |

| ファイル名および<br>通知タイトル                                                                   | 通知の説明                                                                                                      | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_MALWARE_SPECIFIC_OUTGOING<br><br>セキュリティ：マルウェアの検出<br>(Security: Malware Detected) | ファイルのアップロード時にマルウェアが検出された場合に表示されるブロック ページ。                                                                  | 受信側端末のネットワークセキュリティにとって有害なマルウェアがこのファイルから検出されたため、組織のポリシーに基づいてこのファイルの URL (<URL>) へのアップロードがブロックされました。(Based on your organization's policy, the upload of the file to URL (<URL>) has been blocked because the file was detected to contain malware that will be harmful to the receiving end's network security.)<br><br>マルウェア名 (Malware Name) : <マルウェア名><br><br>マルウェア カテゴリ (Malware Category) : <マルウェアのカテゴリ> |
| ERR_NATIVE_FTP_DENIED                                                                | ネイティブFTP トランザクションがブロックされたときに、ネイティブFTP クライアントで表示されるブロック メッセージ。                                              | 530 ログインが拒否されました<br>(530 Login denied)                                                                                                                                                                                                                                                                                                                                                                     |
| ERR_NO_MORE_FORWARDS<br><br>これ以上転送なし (No More Forwards)                              | Web プロキシとネットワーク上の他のプロキシ サーバー間に転送ループがあることをアプライアンスが検出した場合に表示されるエラーページ。Web プロキシはループを切断し、クライアントにこのメッセージを表示します。 | ページ<URL>に対する要求が失敗しました。(The request for the page <URL> failed.)<br><br>サーバー アドレス <ホスト名> が無効であるか、またはこのサーバーにアクセスするにはポート番号を指定する必要があります。<br>(The server address <hostname> may be invalid, or you may need to specify a port number to access this server.)                                                                                                                                                     |
| ERR_POLICY<br><br>ポリシー：全般<br>(Policy: General)                                       | 要求が何らかのポリシー設定によってブロックされた場合に表示されるブロック ページ。                                                                  | 組織のアクセス ポリシーに基づき、この Web サイト<URL> へのアクセスがブロックされました。<br>(Based on your organization's Access Policies, access to this web site <URL> has been blocked.)                                                                                                                                                                                                                                                      |

| ファイル名および<br>通知タイトル                                                                         | 通知の説明                                                                                                                                                     | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_PROTOCOL<br>ポリシー：プロトコル<br>(Policy: Protocol)                                           | 使用しているプロトコルに基づいて要求がブロックされた場合に表示されるブロック ページ。                                                                                                               | データ転送プロトコル「<プロトコル タイプ>」が許可されていないため、組織のアクセスポリシーに基づき、この要求はブロックされました。(Based on your organization's Access Policies, this request has been blocked because the data transfer protocol "<protocol type>" is not allowed.)                                                                                                                                                                                                                 |
| ERR_PROXY_AUTH_REQUIRED<br>プロキシ認可が必要<br>(Proxy Authorization Required)                     | 続行するために認証クレデンシャルを入力する必要がある場合に表示される通知ページ。これは明示的なトランザクション要求に使用されます。                                                                                         | このシステムを使用してインターネットにアクセスするには、認証が必要です。(Authentication is required to access the Internet using this system.) プロンプトに従って有効なユーザー ID とパスフレーズを入力してください。(A valid user ID and passphrase must be entered when prompted.)                                                                                                                                                                                                                      |
| ERR_PROXY_PREVENT_MULTIPLE_LOGIN<br>別のマシンからログイン済み (Already Logged In From Another Machine) | 別のマシンの Web プロキシですでに認証されているユーザー名と同じユーザー名を使用して Web へのアクセスが試みられた場合に表示されるブロック ページ。これは、[ユーザーセッション制限 (User Session Restrictions)] グローバル認証オプションがイネーブルの場合に使用されます。 | このユーザー ID には別の IP アドレスからのアクティブセッションが存在するため、組織のポリシーに基づき、インターネットへのアクセス要求が拒否されました。<br>(Based on your organization's policies, the request to access the Internet was denied because this user ID has an active session from another IP address.)<br><br>別のユーザーとしてログインする場合は、下のボタンをクリックして、別のユーザー名とパスフレーズを入力してください。(If you want to login as a different user, click on the button below and enter a different a user name and passphrase.) |

| ファイル名および<br>通知タイトル                         | 通知の説明         | 通知テキスト                                                                                                                                                                                         |
|--------------------------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_PROXY_REDIRECT<br>リダイレクト<br>(Redirect) | リダイレクション ページ。 | この要求は、リダイレクトされます。<br>(This request is being<br>redirected.) このページが自動的に<br>リダイレクトされない場合は、こ<br>こをクリックして続行してくださ<br>い。(If this page does not<br>automatically redirect, click here to<br>proceed.) |



| ファイル名および<br>通知タイトル                                                        | 通知の説明                                                                                      | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_PROXY_<br>UNACKNOWLEDGED<br><br>ポリシーの確認<br>(Policy<br>Acknowledgment) | エンドユーザー確認ページ<br><br>詳細については、 <a href="#">エンドユーザー<br/>通知ページ</a> , on page 539を参照して<br>ください。 | <p>インターネットにアクセスする前に、以下のステートメントを確認してください。（Please acknowledge the following statements before accessing the Internet.）</p> <p>危険なコンテンツを検出して組織のポリシーを適用するために、Web トランザクションは自動的にモニターされ処理されます。</p> <p>（Your web transactions will be automatically monitored and processed to detect dangerous content and to enforce organization's policies.） 下記のリンクをクリックすると、モニターリングに同意し、訪問したサイトに関するデータが記録される可能性について承認したものと見なされます。（By clicking the link below, you acknowledge this monitoring and accept that data about the sites you visit may be recorded.）</p> <p>モニターリングシステムの存在について、定期的に承認を求められます。（You will be periodically asked to acknowledge the presence of the monitoring system.） ユーザーには、インターネットアクセスに関する組織のポリシーに従う責任があります。（You are responsible for following organization's policies on Internet access.）</p> <p>このステートメントに同意してインターネットにアクセスするには、ここをクリックしてください。（Click here to accept this statement and access the Internet.）</p> |

| ファイル名および<br>通知タイトル                                                   | 通知の説明                                                             | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_PROXY_UNLICENSED<br><br>プロキシのライセンス<br>なし (Proxy Not<br>Licensed) | Secure Web Appliance Web プロキシの有効なライセンス キーがない場合に<br>表示されるブロック ページ。 | セキュリティ デバイスの適切な<br>ライセンスがないため、インター<br>ネットにアクセスできません。<br>(Internet access is not available<br>without proper licensing of the security<br>device.)<br><br><担当者名><電子メール アドレス<br>>に連絡し、以下に示すコードを<br>提出してください。 (Please contact<br><contact name> <email address> and<br>provide the codes shown below.)<br><br><b>Note</b><br>セキュリティ デバイスの管理イン<br>ターフェイスにアクセスするに<br>は、ポートに設定されている IP<br>アドレスを入力します。 |
| ERR_RANGE_NOT_SATISFIABLE<br><br>範囲が不適切 (Range<br>Not Satisfiable)   | Web サーバーが要求されたバイト<br>範囲に対応できない場合に<br>表示されるエラー ページ。                | システムはこの要求を処理でき<br>ません。 (The system cannot process<br>this request.) 非標準のブラウザに<br>よって無効な HTTP 要求が生成さ<br>れた可能性があります。 (A<br>non-standard browser may have<br>generated an invalid HTTP request.)<br><br>標準ブラウザを使用している場合<br>は、要求を再試行してください。<br>(If you are using a standard browser,<br>please retry the request.)                                                                                  |
| ERR_REDIRECT_PERMANENT<br><br>永続的リダイレクト<br>(Redirect Permanent)      | 内部リダイレクション ページ。                                                   | ページ<URL>は<リダイレクト先<br>URL>にリダイレクトされます。<br>(The page <URL> is being redirected<br>to <redirected URL>.)                                                                                                                                                                                                                                                                                           |
| ERR_REDIRECT_REPEAT_REQUEST<br><br>リダイレクト<br>(Redirect)              | 内部リダイレクション ページ。                                                   | 要求を繰り返してください。<br>(Please repeat your request.)                                                                                                                                                                                                                                                                                                                                                  |

| ファイル名および<br>通知タイトル                                             | 通知の説明                                                             | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_SAAS_AUTHENTICATION<br>ポリシー：アクセス拒否 (Policy: Access Denied) | 続行するために認証クレデンシャルを入力する必要がある場合に表示される通知ページ。これはアプリケーションへのアクセスに使用されます。 | 組織のポリシーに基づき、<URL>へのアクセス要求は、ログインクレデンシャルの入力が必要なページにリダイレクトされました。<br>(Based on your organization's policy, the request to access <URL> was redirected to a page where you must enter the login credentials.) 認証に成功し、適切な権限が付与されている場合は、アプリケーションへのアクセスが許可されます。 (You will be allowed to access the application if authentication succeeds and you have the proper privileges.)                                         |
| ERR_SAAS_AUTHORIZATION<br>ポリシー：アクセス拒否 (Policy: Access Denied)  | ユーザーがアクセス権限のないアプリケーションにアクセスを試みた場合に表示されるブロックページ。                   | 承認されたユーザーではないため、組織のポリシーに基づき、アプリケーション<URL>へのアクセスがブロックされました。 (Based on your organization's policy, the access to the application <URL> is blocked because you are not an authorized user.) 別のユーザーとしてログインする場合は、このアプリケーションへのアクセスを認可されているユーザーのユーザー名とパスワードを入力してください。 (If you want to login as a different user, enter a different username and passphrase for a user that is authorized to access this application.) |
| ERR_SAML_PROCESSING<br>ポリシー：アクセス拒否 (Policy: Access Denied)     | アプリケーションにアクセスするためのシングルサインオン URL の処理に内部プロセスが失敗した場合に表示されるエラーページ。    | シングルサインオン要求の処理中にエラーが検出されたため、<ユーザー名>へのアクセス要求が完了しませんでした。 (The request to access <user name> did not go through because errors were found during the process of the single sign on request.)                                                                                                                                                                                                                      |

| ファイル名および<br>通知タイトル                                               | 通知の説明                                                                 | 通知テキスト                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_SERVER_NAME_EXPANSION<br>サーバー名の拡張<br>(Server Name Expansion) | 自動的に URL を展開し、その更新した URL にユーザーをリダイレクトする内部リダイレクションページ。                 | サーバー名 <ホスト名> は省略形と見なされ、<リダイレクト先 URL> にリダイレクトされます。<br>(The server name <hostname> appears to be an abbreviation, and is being redirected to <redirected URL>.)                                                                                                                                                                                                                                                                                                                                            |
| ERR_URI_TOO_LONG<br>URI が長すぎる (URI Too Long)                     | URL が長すぎる場合に表示されるブロック ページ。                                            | 要求された URL が長すぎるため、処理できませんでした。(The requested URL was too long and could not be processed.) これはネットワークへの攻撃を示している可能性があります。(This may represent an attack on your network.)<br><br><担当者名><電子メールアドレス>に連絡し、以下に示すコードを提出してください。(Please contact <contact name> <email address> and provide the codes shown below.)                                                                                                                                                                                                  |
| ERR_WBRS<br>セキュリティ：マルウェアのリスク<br>(Security: Malware Risk)         | Web レピュテーションスコアが低いため、Web レピュテーションフィルタによってサイトがブロックされた場合に表示されるブロック ページ。 | この Web サイト <URL> は、Web レピュテーションフィルタによって、コンピュータまたは組織のネットワークに対するセキュリティ上の脅威であると判定されたため、組織のアクセスポリシーに基づいてブロックされました。<br>(Based on your organization's access policies, this web site <URL> has been blocked because it has been determined by Web Reputation Filters to be a security threat to your computer or the organization's network.) この Web サイトは、マルウェア/スパイウェアと関連付けられています。<br>(This web site has been associated with malware/spyware.)<br><br>脅威のタイプ (Threat Type) : %o<br>脅威の理由 (Threat Reason) : %O |

| ファイル名および<br>通知タイトル                                              | 通知の説明                                                    | 通知テキスト                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_WEBCAT<br>ポリシー：URL フィルタリング (Policy: URL Filtering)          | ブロックされた URL カテゴリの Web サイトにユーザーがアクセスを試みた場合に表示されるブロック ページ。 | Web カテゴリ「<カテゴリ タイプ>」は許可されていないため、組織のアクセスポリシーに基づき、この Web サイト<URL> へのアクセスはブロックされました。<br>(Based on your organization's Access Policies, access to this web site <URL> has been blocked because the web category "<category type>" is not allowed.) |
| ERR_WWW_AUTH_REQUIRED<br>WWW 認可が必要 (WWW Authorization Required) | 要求されたサーバーが続行するために認証クレデンシャルの入力が必要とする場合に表示される通知 ページ。       | 要求した Web サイト<ホスト名>にアクセスするには認証が必要です。(Authentication is required to access the requested web site <hostname>.) プロンプトに従って有効なユーザー ID とパスフレーズを入力してください。(A valid user ID and passphrase must be entered when prompted.)                              |

## 非標準ポートでの不正トラフィックの検出

この章で説明する内容は、次のとおりです。

- [不正トラフィックの検出の概要 \(572 ページ\)](#)
- [L4 トラフィック モニターの設定 \(573 ページ\)](#)
- [既知のサイトのリスト \(573 ページ\)](#)
- [L4 トラフィック モニターのグローバル設定 \(574 ページ\)](#)
- [L4 トラフィック モニター アンチマルウェア ルールのアップデート \(575 ページ\)](#)
- [不正トラフィック検出ポリシーの作成 \(575 ページ\)](#)
- [L4 トラフィック モニターのアクティビティの表示 \(577 ページ\)](#)

## 不正トラフィックの検出の概要

Secure Web Applianceは、すべてのネットワーク ポート全体にわたって不正なトラフィックを検出し、マルウェアがポート 80 をバイパスしようとするのを阻止する統合レイヤ4 トラフィック モニタを備えています。内部クライアントがマルウェアに感染し、標準以外のポートとプロ

トコルを介して Phone Home を試みた場合、L4 トラフィック モニターは Phone Home アクティビティが企業ネットワークから外部に発信されるのを阻止します。デフォルトでは、L4 トラフィック モニターがイネーブルになり、すべてのポートでトラフィックをモニターするように設定されます。これには、DNS やその他のサービスが含まれます。

L4 トラフィック モニターは、独自の内部データベースを使用し、保持します。このデータベースは、IP アドレスおよびドメイン名の照合によって継続的に更新されます。

## L4 トラフィック モニターの設定

### Procedure

**ステップ 1** ファイアウォールの内側に L4 トラフィック モニターを設定します。

**ステップ 2** L4 トラフィック モニターが、プロキシポートの後ろ、かつクライアント IP アドレスのネットワークアドレス変換 (NAT) を実行する任意のデバイスの前に、「論理的に」接続されていることを確認します。

**ステップ 3** グローバル設定項目を設定する

[L4 トラフィック モニターのグローバル設定, on page 574](#)を参照してください。

**ステップ 4** L4 トラフィック モニターのポリシーを作成する

「[不正トラフィック検出ポリシーの作成, on page 575](#)」を参照してください。

## 既知のサイトのリスト

| アドレス                      | 説明                                                                                                                                                                                                        |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 既知の許可アドレス (Known allowed) | [許可リスト (Allow List)] プロパティに記載されている IP アドレスまたはホスト名。これらのアドレスは、「許可リスト」アドレスとしてログファイルに表示されます。                                                                                                                  |
| 未記載 (Unlisted)            | マルウェア サイトであるか既知の許可アドレスであるかが不明な IP アドレス。これらは、[許可リスト (Allow List)] や [追加するサスペクトマルウェアアドレス (Additional Suspected Malware Addresses)] プロパティに記載されておらず、L4 トラフィック モニター データベースにも含まれていません。これらのアドレスはログ ファイルに表示されません。 |

| アドレス                     | 説明                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 不明瞭なアドレス<br>(Ambiguous)  | <p>これらは「グレーリスト」アドレスとしてログ ファイルに表示され、以下のアドレスが該当します。</p> <ul style="list-style-type: none"> <li>リストに記載されていないホスト名と既知のマルウェアのホスト名の両方に関連付けられている <i>IP</i> アドレス。</li> <li>リストに記載されていないホスト名と [追加するサスペクト マルウェア アドレス (Additional Suspected Malware Addresses) ] プロパティに含まれるホスト名の両方に関連付けられている <i>IP</i> アドレス。</li> </ul>                                          |
| 既知のマルウェア (Known malware) | <p>これらは「ブロックリスト」アドレスとしてログファイルに表示され、以下のアドレスが該当します。</p> <ul style="list-style-type: none"> <li>L4 トラフィック モニター データベースで既知のマルウェア サイトと判定され、[許可リスト (Allow List) ] に記載されていない <i>IP</i> アドレスまたはホスト名。</li> <li>[追加するサスペクトマルウェアアドレス (Additional Suspected Malware Addresses) ] プロパティに記載され、[許可リスト (Allow List) ] リストに記載されていない、不明瞭ではない <i>IP</i> アドレス。</li> </ul> |

## L4 トラフィック モニターのグローバル設定

### Procedure

**ステップ 1** [セキュリティサービス (Security Services) ] > [L4 トラフィック モニター (L4 Traffic Monitor) ] を選択します。

**ステップ 2** [グローバル設定を編集 (Edit Global Settings) ] をクリックします。

**ステップ 3** L4 トラフィック モニターをイネーブルにするかどうかを選択します。

**ステップ 4** L4 トラフィック モニターをイネーブルにする場合は、モニター対象のポートを選択します。

- **[すべてのポート (All ports) ]**。不正なアクティビティに対して TCP ポート 65535 をすべてモニターします。
- **[プロキシ ポートを除くすべてのポート (All ports except proxy ports) ]**。不正なアクティビティに対して、以下のポートを除くすべての TCP ポートをモニターします。
  - [セキュリティ サービス (Security Services) ] > [Web プロキシ (Web Proxy) ] ページの [プロキシを設定する HTTP ポート (HTTP Ports to Proxy) ] プロパティで設定したポート (通常はポート 80) 。
  - [セキュリティ サービス (Security Services) ] > [HTTPS プロキシ (HTTPS Proxy) ] ページの [プロキシを設定する透過 HTTPS ポート (Transparent HTTPS Ports to Proxy) ] プロパティで設定したポート (通常はポート 443) 。

ステップ5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

## L4 トラフィック モニター アンチマルウェア ルールのアップデート

### Procedure

ステップ1 [セキュリティサービス（Security Services）] > [L4 トラフィック モニター（L4 Traffic Monitor）] を選択します。

ステップ2 [今すぐ更新（Update Now）] をクリックします。

## 不正トラフィック検出ポリシーの作成

L4 トラフィック モニターがとるアクションは、設定する L4 トラフィック モニターのポリシーによって異なります。

### Procedure

ステップ1 [Webセキュリティマネージャ（Web Security Manager）] > [L4 トラフィック モニター（L4 Traffic Monitor）] を選択します。

ステップ2 [設定の編集（Edit Settings）] をクリックします。

ステップ3 [L4 トラフィック モニターのポリシーの編集（Edit L4 Traffic Monitor Policies）] ページで、L4 トラフィック モニターのポリシーを設定します。

- a) [許可リスト（Allow List）] を定義します。
- b) [許可リスト（Allow List）] に既知の安全なサイトを追加します。

#### Note

Secure Web Appliance の IP アドレスやホスト名を許可されたリストに含めないでください。さもないと、L4 トラフィック モニターは、どんなトラフィック もブロックしません。

- c) 不審なマルウェア アドレスに対して実行するアクションを決定します。

| アクション     | 説明                                             |
|-----------|------------------------------------------------|
| 許可（Allow） | 既知の許可されたアドレスおよびリストに未記載のアドレスの発着信トラフィックを常に許可します。 |



| アクション             | 説明                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| モニター<br>(Monitor) | <p>以下のような状況の下で、トラフィックをモニターします。</p> <ul style="list-style-type: none"> <li>• [サスペクトマルウェアアドレスに対するアクション (Action for Suspected Malware Addresses)] オプションが [モニター (Monitor)] に設定されている場合、既知の許可されたアドレス以外のすべての着発信トラフィックを常にモニターします。</li> <li>• [サスペクトマルウェアアドレスに対するアクション (Action for Suspected Malware Addresses)] オプションが [ブロック (Block)] に設定されている場合、不明瞭なアドレスの着発信トラフィックをモニターします。</li> </ul> |
| ブロック<br>(Block)   | [サスペクトマルウェアアドレスに対するアクション (Action for Suspected Malware Addresses)] オプションが [ブロック (Block)] に設定されている場合、既知のマルウェア アドレスの着発信トラフィックをブロックします。                                                                                                                                                                                                                                            |

**Note**

：不審なマルウェア トラフィックをブロックすることを選択した場合は、不明瞭なアドレスを常にブロックするかどうかを選択できます。デフォルトでは、不明瞭なアドレスはモニターされます。

：ブロックを実行するように L4 トラフィック モニターを設定する場合は、L4 トラフィック モニターと Web プロキシを同じネットワーク上に設定する必要があります。すべてのクライアントがデータ トラフィック用に設定されたルートでアクセスできることを確認するには、[ネットワーク (Network)] > [ルート (Routes)] ページを使用します。

- VM のセットアップでは、透過モードの要求が断続的な時間差で P1 インターフェイスと T1 インターフェイスを通過する間に、それらの要求が複製されます。そのため、一部の IP は、ブロックした後でもアプライアンスを通過する可能性があります。

- d) [追加するサスペクトマルウェアアドレス (Additional Suspected Malware Addresses)] プロパティを定義します。

**Note**

[追加するサスペクトマルウェアアドレス (Additional Suspected Malware Addresses)] のリストに内部 IP アドレスを追加すると、正当な宛先 URL が L4 トラフィック モニターのレポートにマルウェアとして表示されます。このような誤りを回避するために、[Web セキュリティ マネージャ (Web Security Manager)] > [L4 トラフィック モニター ポリシー (L4 Traffic Monitor Policies)] ページの [追加するサスペクトマルウェアアドレス (Additional Suspected Malware Addresses)] フィールドに内部 IP アドレスを入力しないでください。

**ステップ 4** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

**What to do next****関連項目**

- [不正トラフィックの検出の概要, on page 572](#)

- 有効な形式, on page 577。

## 有効な形式

[許可リスト (AllowList)] または [追加するサスペクトマルウェアアドレス (Additional Suspected Malware Addresses)] プロパティにアドレスを追加する場合は、空白またはカンマを使用して複数のエントリを区切ります。以下のいずれかの形式でアドレスを入力できます。

- **IPv4 IP アドレス**。例：IPv4 形式：10.1.1.0。IPv6 形式：2002:4559:1FE2::4559:1FE2
- **CIDR アドレス**。例：10.1.1.0:24。
- **ドメイン名**。例：example.com
- **ホスト名**。例：crm.example.com

## L4 トラフィック モニターのアクティビティの表示

Sシリーズアプライアンスは、サマリー統計情報の機能固有のレポートおよびインタラクティブな表示を生成するために、複数のオプションをサポートしています。

### モニターリング アクティビティとサマリー統計情報の表示

[レポート (Reporting)] > [L4 トラフィック モニター (L4 Traffic Monitor)] ページには、モニターリング アクティビティの統計的なサマリーが表示されます。以下の表示とレポート ツールを使用して、L4 トラフィック モニターのアクティビティの結果を表示できます。

| 表示対象                       | 参照先                                                                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| クライアントの統計                  | [レポート (Reporting)] > [クライアント アクティビティ (Client Activity)]                                                                                                         |
| マルウェアの統計情報<br>ポートの統計情報     | [レポート (Reporting)] > [L4 トラフィック モニター (L4 Traffic Monitor)]                                                                                                      |
| L4 トラフィック モニターの<br>ログ ファイル | [システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] <ul style="list-style-type: none"> <li>• trafmon_errlogs</li> <li>• trafmonlogs</li> </ul> |



#### Note

Web プロキシが転送プロキシとして設定され、L4 トラフィック モニターがすべてのポートをモニターするように設定されている場合は、プロキシのデータ ポートの IP アドレスが記録され、[レポート (Reporting)] > [クライアントアクティビティ (Client Activity)] ページのクライアントアクティビティ レポートにクライアント IP アドレスとして表示されます。Web プロキシが透過プロキシとして設定されている場合は、クライアントの IP アドレスが正しく記録され、表示されるように IP スプーフィングをイネーブルにします。

## L4 トラフィック モニターのログ ファイルのエントリ

L4 トラフィック モニター ログ ファイルはモニターリング アクティビティの詳細を記録します。



## 第 8 章

# レポートとアラート

この章で説明する内容は、次のとおりです。

- [エンドユーザーのアクティビティをモニターするレポートの生成 \(579 ページ\)](#)
- [セキュア アプライアンス レポート \(592 ページ\)](#)
- [新しい Web インターフェイスでのセキュア アプライアンス レポート \(611 ページ\)](#)

## エンドユーザーのアクティビティをモニターするレポートの生成

この章で説明する内容は、次のとおりです。

- [レポートの概要 \(579 ページ\)](#)
- [レポート ページの使用 \(581 ページ\)](#)
- [新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#)
- [レポートの有効化 \(588 ページ\)](#)
- [レポートのスケジュール設定 \(588 ページ\)](#)
- [オンデマンドでのレポートの生成 \(590 ページ\)](#)
- [アーカイブ レポート \(591 ページ\)](#)
- [L4 トラフィック モニタ レポートのトラブルシューティング \(591 ページ\)](#)

## レポートの概要

Secure Web Applianceでは概要レポートが生成されるので、ネットワークで起きていることを把握したり、特定のドメイン、ユーザ、カテゴリのトラフィックの詳細を表示することができます。レポートを実行して特定の期間内のシステムアクティビティをインタラクティブに表示したり、レポートをスケジュールして定期的に行うことができます。

## 関連項目

- [レポート ページからのレポートの印刷とエクスポート, on page 586](#)

## レポートでのユーザー名の使用

認証をイネーブルにすると、Web プロキシで認証される際に、ユーザーはユーザー名でレポートに一覧表示されます。デフォルトでは、ユーザー名は認証サーバーに表示されるとおりに書き込まれます。ただし、すべてのレポートでユーザー名を識別できないようにすることができます。



## Note

管理者の場合は、常にレポートにユーザー名が表示されます。

## Procedure

- ステップ 1 [セキュリティサービス (Security Services)] > [レポート (Reporting)] を選択し、[設定を編集 (Edit Settings)] をクリックします。
- ステップ 2 [ローカルレポート (Local Reporting)] で、[レポートでユーザー名を匿名にする (Anonymize usernames in reports)] を選択します。
- ステップ 3 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

## レポート ページ

Secure Web Applianceには以下のレポートがあります。

- マイ ダッシュボード (My Dashboard) (レポートの「ホームページ」。メニュー バーの左端にある [ホーム (Home)] アイコンをクリックしてアクセスすることもできます。)
- 概要 (Overview)
- ユーザー (Users)
- ユーザー数 (User Count)
- Web サイト (Web Sites)
- URL カテゴリ (URL Categories)
- アプリケーションの表示 (Application Visibility)
- マルウェア対策 (Anti-Malware)
- Advanced Malware Protection
- ファイル分析 (File Analysis)

- AMP 判定の更新
- クライアント マルウェア リスク (Client Malware Risk)
- Web レピュテーション フィルタ (Web Reputation Filters)
- L4 トラフィック モニター (L4 Traffic Monitor)
- SOCKS プロキシ (SOCKS Proxy)
- ユーザの場所別レポート (Reports by User Location)
- Web トラッキング (Web Tracking)
- システム容量 (System Capacity)
- システム ステータス (System Status)
- スケジュール設定されたレポート (Scheduled Reports)
- アーカイブ レポート (Archived Reports)

## レポート ページの使用

さまざまなレポート ページにシステム アクティビティの概要が表示され、システム データを表示するための複数のオプションがあります。Web サイトおよびクライアント固有のデータをページごとに検索することもできます。

レポート ページでは、以下のタスクが実行できます。

| オプション                | タスクへのリンク                                               |
|----------------------|--------------------------------------------------------|
| レポートで表示する時間範囲を変更する   | <a href="#">時間範囲の変更, on page 581</a>                   |
| 特定のクライアントとドメインを検索する  | <a href="#">データの検索, on page 583</a>                    |
| チャートに表示するデータを選択する    | <a href="#">チャート化するデータの選択, on page 583</a>             |
| レポートを外部ファイルにエクスポートする | <a href="#">レポート ページからのレポートの印刷とエクスポート, on page 586</a> |

## 時間範囲の変更

[時間範囲 (Time Range)] フィールドを使用して、各セキュリティ コンポーネントの表示データを更新できます。このオプションを使用して、定義済みの時間範囲のアップデートを生成できます。また、開始時刻と終了時刻を指定してカスタム時間範囲を定義することもできます。



### Note

選択した時間範囲は、[時間範囲 (Time Range)] メニューで異なる値を選択するまで、すべてのレポート ページ全体で使用されます。

|                               |                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------|
| 時間範囲<br>(Time Range)          | 返されるデータ                                                                           |
| 時間<br>(Hour)                  | 60 分間と、追加で最大 5 分間                                                                 |
| 日 (Day)                       | 直近の 24 時間とその時点の 1 時間未満の時間を含めた時間に対して 1 時間間隔                                        |
| 週 (Week)                      | 直近の 7 日間にその時点の日を足した日数に対して 1 日間隔                                                   |
| 月 (30 日)<br>(Month (30 days)) | 直近の 30 日間にその時点の日を足した日数に対して 1 日間隔                                                  |
| 昨日<br>(Yesterday)             | Secure Web Applianceに定義されているタイムゾーンを使用した直近の 24 時間 (00:00 から 23:59)                 |
| カスタム範囲 (Custom Range)         | 定義済みのカスタム時間範囲。<br>[カスタム範囲 (Custom Range)] を選択すると、開始時刻と終了時刻を入力できるダイアログボックスが表示されます。 |



**Note** すべてのレポートで、システム設定のタイムゾーンに基づき、グリニッジ標準時 (GMT) オフセットで日付および時刻情報が表示されます。ただし、データエクスポートでは、世界の複数のタイムゾーンの複数のシステムに対応するためにのみ、GMT で時刻が表示されます。

## レポートの時間範囲の選択

ほとんどの事前定義レポートページでは、含まれるデータの時間範囲を選択できます。選択した時間範囲は、[時間範囲 (Time Range)] メニューで異なる値を選択するまで、すべてのレポートページに対して使用されます。

使用可能な時間範囲オプションは、アプライアンスごとに異なり、またセキュリティ管理アプライアンス上の電子メール レポーティングおよび Web レポーティングによって異なります。



**Note** レポート ページの時間範囲は、グリニッジ標準時 (GMT) オフセットで表示されます。たとえば、太平洋標準時は、GMT + 7 時間 (GMT + 07:00) です。



**Note** すべてのレポートで、システム設定の時間帯に基づき、グリニッジ標準時 (GMT) オフセットで日付および時刻情報が表示されます。ただし、データエクスポートでは、世界の複数のタイムゾーンの複数のシステムに対応するために、GMT で時刻が表示されます。

## データの検索

一部のレポートには、特定のデータポイントを検索するために使用できるフィールドがあります。データを検索するときに、レポートは検索する特定のデータセットのレポートデータを調整します。入力する文字列に完全に一致する値や入力する文字列で始まる値を検索できます。以下のレポート ページには検索フィールドがあります。

| 検索フィールド                              | 説明                                            |
|--------------------------------------|-----------------------------------------------|
| ユーザー (Users)                         | ユーザー名またはクライアント IP アドレスでユーザーを検索します。            |
| Web サイト (Web Sites)                  | ドメインまたはサーバーの IP アドレスでサーバーを検索します。              |
| URL カテゴリ (URL Categories)            | URL カテゴリを検索します。                               |
| アプリケーションの表示 (Application Visibility) | AVC または ADC エンジンがモニターし、ブロックするアプリケーション名を検索します。 |
| クライアントマルウェアリスク (Client Malware Risk) | ユーザー名またはクライアント IP アドレスでユーザーを検索します。            |



### Note

クライアント IP アドレスおよびクライアント ユーザー ID を表示するには、認証を設定する必要があります。

## チャート化するデータの選択

各 Web レポーティング ページのデフォルト チャートには、一般に参照されるデータが表示されますが、代わりに異なるデータをチャート化するように選択できます。ページに複数のチャートがある場合は、チャートごとに変更できます。チャートのオプションは、レポートのテーブルの列見出しと同じです。

### Procedure

**ステップ 1** チャートの下に [チャートオプション (Chart Options)] をクリックします。

**ステップ 2** 表示するデータを選択します。

**ステップ 3** [完了 (Done)] をクリックします。



## カスタム レポート

既存のレポートのページからチャート（グラフ）とテーブルを組み合わせてカスタム レポートのページを作成できます。

| 目的                                   | 操作手順                                                                                                                                                                                                                                                                                                    |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| カスタム レポート ページにモジュールを追加               | 参照先： <ul style="list-style-type: none"> <li>• <a href="#">カスタム レポートに追加できないモジュール</a> , on page 584。</li> <li>• <a href="#">カスタム レポート ページの作成</a> , on page 584</li> </ul>                                                                                                                                 |
| カスタム レポート ページの表示                     | <ol style="list-style-type: none"> <li>1. [モニター（Monitor）]&gt;[メール（Email）]または[Web]&gt;[レポート（Reporting）]&gt;[レポート（Reporting）]&gt;[マイレポート（My Reports）]を選択します。</li> <li>2. 表示する時間範囲を選択します選択した時間範囲は[マイレポート（My Reports）]ページのすべてのモジュールを含むすべてのレポートに適用されます。</li> </ol> <p>新しく追加されたモジュールは関連するセクションの上部に表示されます。</p> |
| カスタム レポート ページでのモジュールの再配置             | 目的の場所にモジュールをドラッグ アンド ドロップします。                                                                                                                                                                                                                                                                           |
| カスタム レポート ページからのモジュールの削除             | モジュールの右上にある [X] をクリックします。                                                                                                                                                                                                                                                                               |
| カスタム レポート の PDF または CSV バージョンの生成     | [レポート（Reporting）]>[アーカイブ レポート（Archived Reports）]を選択し、[今すぐレポートを生成（Generate Report Now）]をクリックします。                                                                                                                                                                                                         |
| カスタム レポート の PDF または CSV バージョンの定期的な生成 | [レポート（Reporting）]>[スケジュールされたレポート（Scheduled Reports）]を選択します。                                                                                                                                                                                                                                             |

### カスタム レポートに追加できないモジュール

- 検索結果（Web トラッキングの検索結果を含む）

### カスタム レポート ページの作成

#### Before you begin

- 追加するモジュールが追加可能であることを確認します。[カスタム レポートに追加できないモジュール](#) , on page 584を参照してください。

- モジュールの右上の [X] をクリックして、不要なデフォルト モジュールを削除します。

## Procedure

**ステップ 1** 以下のいずれかの方法でカスタム レポート ページにモジュールを追加します。

### Note

一部のモジュールは、以下のいずれかの方法を使用した場合のみ利用できます。ある方式を使用してモジュールを追加できない場合は、別の方法を試してください。

- 追加するモジュールがある [メール (Email)] タブまたは [Web] タブのレポート ページに移動し、モジュールの上部にある [+] ボタンをクリックします。
- [レポート (Reporting)] > [マイレポート (My Reports)] に移動し、[+] ボタン (いずれかのセクションの上部にあります) をクリックして、追加するレポート モジュールを選択します。目的のモジュールを見つけるには、[マイレポート (My Reports)] ページの各セクションにある [+] ボタンをクリックしなければならない場合があります。

各モジュールは一度だけ追加できます。すでに特定のモジュールをレポートに追加している場合は、追加オプションが利用できなくなっています。

**ステップ 2** カスタマイズした (たとえば、カラムの追加、削除、または順序変更をした、あるいはチャートにデフォルト以外のデータを表示した) モジュールを追加する場合は、これらのモジュールを [マイレポート (My Reports)] ページでカスタマイズします。

モジュールがデフォルト設定に追加されます。元のモジュールの時間範囲は保持されません。

**ステップ 3** 別に凡例を持つチャート (たとえば、[概要 (Overview)] ページからのグラフ) を追加する場合は、別途凡例を追加します。必要に応じて、説明するデータの隣にドラッグアンドドロップします。

## レポートおよびトラッキングにおけるサブドメインとセカンドレベルドメインの比較

レポーティングおよびトラッキングの検索では、セカンドレベルのドメイン

(<http://george.surbl.org/two-level-tlds>に表示されている地域ドメイン) は、ドメインタイプがサブドメインと同じように見えますが、サブドメインとは別の方法で処理されます。次に例を示します。

- レポートには、co.uk などの 2 レベルのドメインの結果は含まれませんが、foo.co.uk の結果は含まれます。レポートには、cisco.com などの主要な企業ドメインの下にサブドメインが含まれます。
- 地域ドメイン co.uk に対するトラッキング検索結果には、foo.co.uk などのドメインは含まれませんが、cisco.com に対する検索結果には subdomain.cisco.com などのサブドメインが含まれます。

## レポート ページからのレポートの印刷とエクスポート

ページ右上隅の [印刷可能 (PDF) (Printable (PDF))] リンクをクリックすると、すべてのレポート ページを印刷形式の PDF 版で生成できます。また、[エクスポート (Export)] リンクをクリックして、未処理データをカンマ区切り形式 (CSV) ファイルとしてエクスポートすることもできます。

CSV エクスポートには未処理データのみが含まれるため、Web ベースのレポート ページからエクスポートされたデータには、パーセンテージなどの計算データが含まれていない場合があります (そのデータが Web ベースのレポートで表示される場合でも、含まれていない場合があります)。

### レポート データのエクスポート

ほとんどのレポートには、未処理データをカンマ区切り形式 (CSV) のファイルにエクスポートできる [エクスポート (Export)] リンクが用意されています。CSV ファイルにデータをエクスポートすると、Microsoft Excel などのアプリケーションを使用し、データにアクセスして処理することができます。

エクスポートされた CSV データは、Secure Web Applianceでのタイムゾーン設定にかかわらず、すべてのメッセージトラッキングおよびレポーティングデータをグリニッジ標準時 (GMT) で示します。GMT 時間への変換の目的は、アプライアンスに依存せずにデータを使用したり、複数のタイムゾーンにあるアプライアンスからのデータを参照する際にデータを使用したりできるようにするためです。

以下の例は、Anti-Malware カテゴリ レポートの raw データ エクスポートのエントリであり、太平洋夏時間 (PDT) が GMT 7 時間で表示されています。

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name,
Transactions Monitored, Transactions Blocked, Transactions Detected
1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525,
2100, 2625
```

| カテゴリ ヘッダー                      | 値                    | 説明                     |
|--------------------------------|----------------------|------------------------|
| タイムスタンプ開始<br>(Begin Timestamp) | 1159772400.0         | エポックからの秒数で表されたクエリ開始時刻。 |
| タイムスタンプ終了 (End Timestamp)      | 1159858799.0         | エポックからの秒数で表されたクエリ終了時刻。 |
| 開始日 (Begin Date)               | 2006-10-02 07:00 GMT | クエリの開始日。               |
| End Date                       | 2006-10-03 06:59 GMT | クエリの終了日。               |
| 名前 (Name)                      | Adware               | マルウェア カテゴリの名前。         |
| Transactions Monitored         | 525                  | モニタリングされたトランザクション数。    |
| Transactions Blocked           | 2100                 | ブロックされたトランザクション数。      |

| カテゴリ ヘッダー                             | 値    | 説明                                                     |
|---------------------------------------|------|--------------------------------------------------------|
| 検出されたトランザクション (Transactions Detected) | 2625 | トランザクションの総数 = (検出されたトランザクションの数) + (ブロックされたトランザクションの数)。 |



**Note** カテゴリ ヘッダーは、レポートのタイプごとに異なります。

ローカライズされた CSV データをエクスポートすると、ブラウザによっては見出しが正しく表示されない場合があります。これは、ブラウザによっては、ローカライズされたテキストに対して適切な文字セットが使用されない場合があることから発生します。この問題の回避策として、ローカル マシンにファイルを保存し、[ファイル (File)] > [開く (Open)] を使用して任意の Web ブラウザでファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

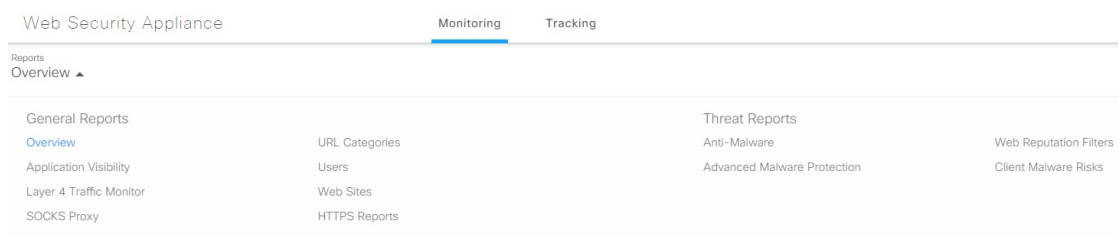
## 新しい Web インターフェイスでのインタラクティブ レポート ページの使用

次の図に示す [レポート (Reports)] ドロップダウンを使用すると、Secure Web Applianceのレポートを表示することができます。



(注) [概要 (Overview)] レポートページは、ランディングページ (ログイン後に表示されるページ) です。レポートまたはトラッキングページから新しい Web インターフェイスをリロードすると、デフォルトのランディングページ ([概要 (Overview)] レポートページ) がロードされます。

図 11: レポートドロップダウン



Web レポートは、一般的なレポートと脅威レポートに分類されます。

新しい Web インターフェイスにアクセスするには、「[新しい Web インターフェイスでのセキュア アプライアンス レポート](#)」を参照してください。

## 関連項目

- [\(Web レポートのみ\) チャート化するデータの選択 \(644 ページ\)](#)

## レポートの有効化

組織に複数の Secure Web Applianceがあり、Cisco コンテンツ セキュリティ管理アプライアンスを使用して集約レポートのデータを管理および表示する場合、各 Secure Web Applianceで集約管理レポートを有効にする必要があります。

アプライアンスの設定に基づいてレポートのタイプを選択できます。すべてのレポートをローカルで保存できます。。組織に複数の Secure Web Applianceがあり、Cisco コンテンツセキュリティ管理アプライアンスを1つ使用している場合は、集約管理レポートを選択して集約したレポートデータを管理および表示できます。集約管理レポート、またはローカルレポートを選択すると、各 Secure Web Applianceにこれらの設定が適用されます。

### Procedure

**ステップ 1** [セキュリティサービス (Security Services)] > [レポート (Reporting)] を選択し、[設定を編集 (Edit Settings)] をクリックします。

- a) アプライアンスでレポートを有効にする場合は、[ローカルレポート (Local Reporting)] をオンにします。アプライアンス ポータルにログインした後、レポートにアクセス可能になります。
- b) Cisco コンテンツ セキュリティ管理アプライアンスを介してレポートを使用可能にする場合は、[集中管理レポート (Centralized Reporting)] をオンにします。

Secure Web Applianceのみが、ローカル レポートについて収集されたすべてのデータを保存します。集約管理レポートがアプライアンスで有効な場合、Secure Web Applianceはシステム容量データとシステムステータスデータのみを保持します。これらは Secure Web Applianceでローカルに使用できる唯一のレポートです。

管理アプライアンスでのこの機能の設定については、Cisco コンテンツセキュリティ管理アプライアンス ユーザー ガイドの集約管理 Web レポートの使用とトラッキングに関するトピックを参照してください。

**ステップ 2** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)] )。

## レポートのスケジュール設定

日単位、週単位、または月単位で実行されるようにレポートをスケジュール設定することができます。スケジュール化したレポートは、前日、過去7日間、前月のデータを含めるように設定できます。

レポートをスケジュール設定できるレポート タイプは以下のとおりです。

- 概要 (Overview)

- ユーザー (Users)
- Web サイト (Web Sites)
- URL カテゴリ (URL Categories)
- アプリケーションの表示 (Application Visibility)
- マルウェア対策 (Anti-Malware)
- Advanced Malware Protection
- Advanced Malware Protection 判定の更新
- クライアント マルウェア リスク (Client Malware Risk)
- Web レピュテーション フィルタ (Web Reputation Filters)
- L4 トラフィック モニター (L4 Traffic Monitor)
- SOCKS プロキシ (SOCKS Proxy)
- ユーザの場所別レポート (Reports by User Location)
- システム容量 (System Capacity)
- マイ ダッシュボード (My Dashboard)

## スケジュール設定されたレポートの追加

### Procedure

- ステップ 1** [レポート (Reporting)] > [スケジュールされたレポート (Scheduled Reports)] を選択し、[定期レポートの追加 (Add Scheduled Report)] をクリックします。
- ステップ 2** レポート [タイプ (Type)] を選択します。
- ステップ 3** レポートのわかりやすい [タイトル (Title)] を入力します。  
同じ名前のレポートを複数作成しないでください。
- ステップ 4** レポートに含めるデータの時間範囲を選択します。
- ステップ 5** 生成されるレポートの [形式 (Format)] を選択します。  
デフォルト形式は PDF です。ほとんどのレポートで、raw データを CSV ファイルとして保存することもできます。
- ステップ 6** 設定するレポートのタイプに応じて、含める行数やデータをソートする列など、さまざまなレポート オプションを指定できます。必要に応じて、これらのオプションを設定します。
- ステップ 7** [スケジュール (Schedule)] セクションで、レポートを実行する周期 (毎日、毎週、または毎月) と時間を選択します。

**ステップ 8** [メールの送信先 (Email to)] フィールドに、生成されたレポートを送信する相手の電子メールアドレスを入力します。

電子メールアドレスを指定しなかった場合は、レポートのアーカイブのみが行われます。

**ステップ 9** データの [レポート言語 (Report Language)] を選択します。

**ステップ 10** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

---

## スケジュール設定されたレポートの編集

### Procedure

---

**ステップ 1** [レポート (Reporting)] > [スケジュールされたレポート (Scheduled Reports)] を選択します。

**ステップ 2** リストからレポートのタイトルを選択します。

**ステップ 3** 設定を変更します。

**ステップ 4** 変更を送信して確定します ([送信 (Submit)] と [変更を確定 (Commit Changes)])。

---

## スケジュール設定されたレポートの削除

### Procedure

---

**ステップ 1** [レポート (Reporting)] > [スケジュールされたレポート (Scheduled Reports)] を選択します。

**ステップ 2** 削除するレポートに対応するチェックボックスをオンにします。

**ステップ 3** スケジュール設定されたすべてのレポートを削除するには、[すべて (All)] チェックボックスを選択します。

**ステップ 4** 削除して変更を確定します ([削除 (Delete)] と [変更を確定 (Commit Changes)])。

### Note

削除されたレポートのアーカイブ版は削除されません。

---

## オンデマンドでのレポートの生成

### Procedure

---

**ステップ 1** [レポート (Reporting)] > [アーカイブ レポート (Archived Reports)] を選択します。

**ステップ 2** [今すぐレポートを生成 (Generate Report Now)] をクリックします。

- ステップ 3** レポート [タイプ (Type)] を選択します。
- ステップ 4** レポートのわかりやすい [タイトル (Title)] を入力します。  
同じ名前のレポートを複数作成しないでください。
- ステップ 5** レポートに含めるデータの時間範囲を選択します。
- ステップ 6** 生成されるレポートの [形式 (Format)] を選択します。  
デフォルト形式は PDF です。ほとんどのレポートで、raw データを CSV ファイルとして保存することもできます。
- ステップ 7** 設定するレポートのタイプに応じて、含める行数やデータをソートする列など、さまざまなレポート オプションを指定できます。必要に応じて、これらのオプションを設定します。
- ステップ 8** [配信オプション (Delivery Options)] のいずれかを選択します。
- レポートの [アーカイブ (Archive)] (レポートが [アーカイブ レポート (Archived Reports)] ページに表示されます)。
  - [今すぐ受信者にメールを送信 (Email now to recipients)] (1 つまたは複数の電子メール アドレスを指定します)。
- ステップ 9** データの [レポート言語 (Report Language)] を選択します。
- ステップ 10** [このレポートを配信 (Deliver This Report)] をクリックして、レポートを生成します。
- ステップ 11** 変更を確定します。

## アーカイブ レポート

[レポート (Reporting)] > [アーカイブ レポート (Archived Reports)] ページには、使用可能なアーカイブ済みのレポートが一覧表示されます。[レポートのタイトル (Report Title)] 列のそれぞれの名前は、そのレポートのビューにリンクしています。[表示 (Show)] メニューは、一覧表示されたレポートのタイプをフィルタリングします。列見出しをクリックして、各列のデータをソートすることができます。

アプライアンスでは、スケジュール設定されたレポートごとに最大 12 のインスタンスが保存されます (最大で合計 1000 レポート)。アーカイブ済みのレポートは、アプライアンスの /periodic\_reports ディレクトリに保管されます。アーカイブ済みのレポートは自動的に削除されます。新しいレポートが追加されると、古いレポートが削除され、常に 1000 という数が維持されます。12 インスタンスという制限は、同じ名前と時間範囲のスケジュール設定された各レポートに適用されます。

## L4 トラフィック モニタ レポートのトラブルシューティング

Web プロキシが転送プロキシとして設定され、L4 トラフィック モニタがすべてのポートをモニタするように設定されている場合、プロキシのデータ ポートの IP アドレスが記録され、クライアント IP アドレスとしてレポートに表示されます。Web プロキシがトランスペアレントプロキシとして設定されている場合は、クライアント IP アドレスが正しく記録され、表示さ



れるように IP スプーフィングを有効にします。これを行うには、『IronPort AsyncOS for Web User Guide』を参照してください。

#### 関連項目

- [\[クライアント マルウェア リスク \(Client Malware Risk\)\] ページ, on page 600](#)
- [L4 トラフィック モニタによって処理されたトランザクションの検索, on page 608](#)

## セキュア アプライアンス レポート

この章で説明する内容は、次のとおりです。

- [\[概要 \(Overview\)\] ページ \(593 ページ\)](#)
- [\[ユーザ \(Users\)\] ページ \(595 ページ\)](#)
- [\[ユーザー数 \(User Count\)\] ページ \(596 ページ\)](#)
- [\[Webサイト \(Web Sites\)\] ページ \(596 ページ\)](#)
- [\[URLカテゴリ \(URL Categories\)\] ページ \(597 ページ\)](#)
- [\[アプリケーションの表示 \(Application Visibility\)\] ページ \(598 ページ\)](#)
- [\[マルウェア対策 \(Anti-Malware\)\] ページ \(599 ページ\)](#)
- [Advanced Malware Protection ページ \(600 ページ\)](#)
- [\[ファイル分析 \(File Analysis\)\] ページ \(600 ページ\)](#)
- [\[セキュアエンドポイント判定のアップデート \(AMP Verdict Updates\)\] ページ \(600 ページ\)](#)
- [\[クライアント マルウェア リスク \(Client Malware Risk\)\] ページ \(600 ページ\)](#)
- [\[Web レピュテーション フィルタ \(Web Reputation Filters\)\] ページ \(602 ページ\)](#)
- [\[L4 トラフィック モニター \(L4 Traffic Monitor\)\] ページ \(602 ページ\)](#)
- [\[SOCKS プロキシ \(SOCKS Proxy\)\] ページ \(603 ページ\)](#)
- [\[ユーザー ロケーション別のレポート \(Reports by User Location\)\] ページ \(603 ページ\)](#)
- [\[Web トラッキング \(Web Tracking\)\] ページ \(604 ページ\)](#)
- [\[システム容量 \(System Capacity\)\] ページ \(609 ページ\)](#)
- [\[システムステータス \(System Status\)\] ページ \(609 ページ\)](#)

## [概要 (Overview)] ページ

[レポート (Reporting)] > [概要 (Overview)] ページには、Secure Web Applianceでのアクティビティの概要が表示されます。このページには、Secure Web Applianceで処理される Web トラフィックに関するグラフおよびサマリー テーブルが含まれています。

Table 10: システム概要

| セクション                                                  | 説明                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web プロキシ トラフィックの特徴 (Web Proxy Traffic Characteristics) | 過去 1 分間における 1 秒あたりの平均トランザクション数、過去 1 分間の平均帯域 (bps)、過去 1 分間の平均応答時間 (ms)、および現在の接続総数のリスト。                                                                                                                                                                                                                                                                        |
| システム リソースの使用率 (System Resource Utilization)            | 現在の全体的な CPU 負荷、RAM およびレポート/ログディスク使用率のリスト。[システム ステータス (System Status)] ページに切り替えるには、 <b>[システム ステータス詳細 (System Status Details)]</b> をクリックします (詳細は <a href="#">新しい Web インターフェイスの [システムステータス (System Status)] ページ, on page 656</a> を参照)。<br><br><b>Note</b><br>このページに表示される CPU 使用率値はさまざまな瞬間に個別に読み取られるため、[システムステータス (System Status)] ページに表示される CPU 値と若干異なる場合があります。 |

Table 11: 時間範囲ベースのカテゴリと概要

| セクション                                                                                                                                  | 説明                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| 時間範囲：以下のセクションに表示されるデータの時間範囲を選択します。オプションは、[時間 (Hour)]、[日 (Day)]、[週 (Week)]、[30日 (30 Days)]、[前日 (Yesterday)]、[カスタム範囲 (Custom Range)] です。 |                                                                                                                   |
| Web プロキシアクティビティ総数 (Total Web Proxy Activity)                                                                                           | トランザクションの実際の数 (縦の目盛り)、および (Web プロキシ) アクティビティが発生したおよその日付 (横の時間軸) が表示されます。                                          |
| Web プロキシの概要 (Web Proxy Summary)                                                                                                        | 疑わしいまたは正常な Web プロキシ アクティビティの比率を表示できます。                                                                            |
| L4 トラフィック モニターの概要 (L4 Traffic Monitor Summary)                                                                                         | L4 トラフィック モニターによってモニターされ、ブロックされたトラフィックをレポートします。                                                                   |
| 疑わしいトランザクション (Suspect Transactions)                                                                                                    | さまざまなセキュリティ コンポーネントによって疑わしいトランザクションと分類された Web トランザクションを表示できます。<br><br>トランザクションの実際の数、およびアクティビティが発生したおよその日付が表示されます。 |

| セクション                                                                     | 説明                                                                                                                                |
|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 疑わしいトランザクションの概要 (Suspect Transactions Summary)                            | ブロックまたは警告された疑わしいトランザクションの比率を表示できます。                                                                                               |
| 上位 URL カテゴリ : 総トランザクション数 (Top URL Categories: Total Transactions)         | ブロックされた上位 10 の URL カテゴリが表示されます。                                                                                                   |
| 上位アプリケーション タイプ : 総トランザクション数 (Top Application Types: Total Transactions)   | AVC または ADC エンジンによってブロックされた上位アプリケーションタイプが表示されます。                                                                                  |
| 上位マルウェア カテゴリ : モニターまたはブロック (Top Malware Categories: Monitored or Blocked) | 検出されたすべてのマルウェア カテゴリが表示されます。                                                                                                       |
| ブロックまたは警告されたトランザクション数の上位ユーザー (Top Users Blocked or Warned Transactions)   | ブロックされたトランザクションまたは警告されたトランザクションを生成しているユーザーが表示されます。認証されたユーザーはユーザー名で表示され、認証されていないユーザーは IP アドレスで表示されます。                              |
| Web トラフィック タップ ステータス                                                      | タップされていないトラフィック トランザクションおよびタップされたトラフィック トランザクションがグラフ形式で表示されます。                                                                    |
| Web トラフィック タップ サマリ                                                        | タップされたトラフィック トランザクションおよびタップされていないトラフィック トランザクションの概要が、トラフィック トランザクションの合計とともに表示されます。                                                |
| タップされた HTTP/HTTPS トラフィック                                                  | タップされた HTTP および HTTPS トラフィック トランザクションがグラフ形式で表示されます。                                                                               |
| タップされたトラフィック サマリ                                                          | HTTP および HTTPS トラフィック トランザクションの概要が、HTTP および HTTPS トラフィック トランザクションの合計とともに表示されます。                                                   |
| EUP トランザクション                                                              | カプセル化された URL のトランザクションが表示されます。これらは、 <a href="https://translate.google.com">translate.google.com</a> などの Web サイトから実行されたトランザクションです。 |
| EUP トランザクションの概要                                                           | カプセル化された URL のトランザクションの概要が表示されます。                                                                                                 |
| 疑わしい EUP トランザクション                                                         | 疑わしいと検出された、カプセル化された URL のトランザクションが表示されます。                                                                                         |
| 疑わしい EUP トランザクションの概要                                                      | 疑わしいと検出された、カプセル化された URL のトランザクションの概要が表示されます。                                                                                      |

## [ユーザ (Users) ] ページ

[レポート (Reporting) ]>[ユーザ (Users) ] ページには、個々のユーザーの Web トラフィック情報を表示するためのリンクが提供されています。ネットワーク上のユーザーがインターネット、特定の Web サイト、または特定の URL で費やした時間と、ユーザーが使用した帯域幅の量を表示できます。

| セクション                                                       | 説明                                                             |
|-------------------------------------------------------------|----------------------------------------------------------------|
| [時間範囲 (Time Range) ] (ドロップダウン リスト)                          | レポートに含めるデータの時間範囲を選択できるメニュー。                                    |
| ブロックされたトランザクション数別上位ユーザー (Top Users by Transactions Blocked) | ブロックされたトランザクションの数 (横の目盛り) が最大のユーザー (縦の目盛り) が表示されます。            |
| 使用した帯域幅別上位ユーザー (Top Users by Bandwidth Used)                | システム上で最も帯域幅 (ギガバイト単位の使用量を示す横の目盛り) を使用しているユーザー (縦の目盛り) が表示されます。 |
| ユーザー テーブル (Users Table)                                     | 個々のユーザーを一覧表示し、ユーザーごとに複数の統計情報を表示します。                            |

## [ユーザーの詳細 (User Details) ] ページ

[ユーザーの詳細 (User Details) ] ページには、[レポート (Reporting) ]>[ユーザ (Users) ] ページの [ユーザー テーブル (Users Table) ] で選択した特定のユーザーに関する情報が表示されます。

| セクション                                                       | 説明                                     |
|-------------------------------------------------------------|----------------------------------------|
| [時間範囲 (Time Range) ] (ドロップダウン リスト)                          | レポートに含めるデータの時間範囲を選択できるメニュー。            |
| 総トランザクション数別 URL カテゴリ (URL Categories by Total Transactions) | 特定のユーザーが使用している特定の URL カテゴリのリストが表示されます。 |
| 総トランザクション数別トレンド (Trend by Total Transaction)                | ユーザーが Web にいつアクセスしたかが表示されます。           |

| セクション                                   | 説明                                                                                                                                                   |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 一致した URL カテゴリ (URL Categories Matched)  | 完了したトランザクションとブロックされたトランザクションの両方について、指定した時間範囲内で一致したすべての URL カテゴリが表示されます。                                                                              |
| 一致したドメイン (Domains Matched)              | このユーザーがアクセスした特定のドメインまたは IP アドレスに関する情報が表示されます。<br><br><b>Note</b><br>このドメインのデータを CSV ファイルにエクスポートする場合は、先頭から 300,000 件のエントリのみがファイルにエクスポートされるので注意してください。 |
| 一致したアプリケーション (Applications Matched)     | AVC または ADC エンジンによって検出された、特定のユーザーが使用している特定のアプリケーションが表示されます。                                                                                          |
| 検出されたマルウェア脅威 (Malware Threats Detected) | 特定のユーザーによって引き起こされているマルウェアの脅威の内、上位のものが表示されます。                                                                                                         |
| 一致したポリシー (Policies Matched)             | この特定のユーザーに適用されている特定のポリシーが表示されます。                                                                                                                     |

## [ユーザー数 (User Count) ] ページ

[レポート (Reporting) ] > [ユーザー数 (User Count) ] ページには、アプライアンスの認証されたユーザーと認証されていないユーザーの合計に関する情報が表示されます。このページには、直近の過去 30 日間、90 日間、および 180 日間のユニーク ユーザー数が表示されます。



(注) システムは、認証されたユーザーと認証されていないユーザーの合計を、1 日に 1 回計算します。

たとえば、5 月 22 日 23 時 59 分にユーザー数レポートを表示すると、システムは 5 月 22 日 0 時までの合計ユーザー数を表示します。

## [Web サイト (Web Sites) ] ページ

[レポート (Reporting) ] > [Web サイト (Web Sites) ] ページは、Secure Web Appliance で発生しているアクティビティ全体を集約したものです。

| セクション                                                         | 説明                                                                                                                                                    |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)                             | このメニューからレポートに含めるデータの時間範囲を選択できます。                                                                                                                      |
| 総トランザクション数別上位ドメイン (Top Domains by Total Transactions)         | サイト上のアクセス上位ドメインがグラフ形式で表示されます。                                                                                                                         |
| ブロックされたトランザクション数別上位ドメイン (Top Domains by Transactions Blocked) | トランザクションごとに発生するブロック アクションをトリガーした上位ドメインが、グラフ形式で表示されます。                                                                                                 |
| 一致したドメイン (Domains Matched)                                    | <p>サイト上のアクセスされたドメインがインタラクティブなテーブルに表示されます。</p> <p><b>Note</b><br/>このドメインのデータを CSV ファイルにエクスポートする場合は、先頭から 300,000 件のエントリのみがファイルにエクスポートされるので注意してください。</p> |

## [URLカテゴリ (URL Categories)] ページ

[レポート (Reporting)] > [URL カテゴリ (URL Categories)] ページでは、ネットワーク上のユーザーがアクセスしている URL カテゴリを表示できます。[URL カテゴリ (URL Categories)] ページを [アプリケーションの表示 (Application Visibility)] ページおよび [ユーザー (Users)] ページと併用すると、特定のユーザーとそのユーザーがアクセスを試みているアプリケーションや Web サイトのタイプを調べることができます。



**Note** すでに定義されている一連の URL カテゴリは更新されることがあります。

| セクション                                                             | 説明                                              |
|-------------------------------------------------------------------|-------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)                                 | レポートの時間範囲を選択します。                                |
| 総トランザクション数別上位 URL カテゴリ (Top URL Categories by Total Transactions) | このセクションには、サイト上でアクセスされた上位 URL カテゴリがグラフ形式で表示されます。 |

| セクション                                                                                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ブロックまたは警告を受けたトランザクション数別上位 URL カテゴリ (Top URL Categories by Blocked and Warned Transactions) | トランザクションごとに発生するブロックまたは警告アクションをトリガーした上位 URL がグラフ形式で表示されます。                                                                                                                                                                                                                                                                                                                                             |
| 一致した URL カテゴリ (URL Categories Matched)                                                     | <p>指定した時間範囲における URL カテゴリ別のトランザクションの傾向、および各カテゴリで使用された帯域幅と費やされた時間が表示されます。</p> <p>未分類の URL の比率が 15 ～ 20 % を上回る場合は、次のオプションを検討してください。</p> <ul style="list-style-type: none"> <li>• 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループポリシーに適用できます。</li> <li>• 評価およびデータベース更新用に、未分類の URL と誤って分類された URL をシスコにレポートできます。</li> <li>• Web レピュテーション フィルタリングと、アンチマルウェア フィルタリングがイネーブルになっていることを確認してください。</li> </ul> |

## URL カテゴリ セットの更新とレポート

Secure Web Applianceでは、一連の定義済み URL カテゴリが定期的に自動更新される場合があります。

これらの更新が行われると、古いカテゴリに関連づけられたデータが古すぎてレポートに含まれなくなるまで、古いカテゴリ名は引き続きレポートに表示されます。URL カテゴリ セットの更新後に生成されたレポートデータには新しいカテゴリが使用されるので、同じレポートに新旧両方のカテゴリが表示される場合があります。

## [アプリケーションの表示 (Application Visibility)] ページ

[レポート (Reporting)] > [アプリケーションの表示 (Application Visibility)] ページには、Application Visibility and Control または Application Discovery and Control エンジンで検出されたアプリケーションと、使用されているアプリケーションのタイプ、およびブロックされているアプリケーションのタイプが表示されます。

| セクション                             | 説明                          |
|-----------------------------------|-----------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト) | レポートに含めるデータの時間範囲を選択できるメニュー。 |

| セクション                                                                    | 説明                                                                                                                     |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| [総トランザクション数の上位アプリケーションタイプ (Top Application Types by Total Transactions)] | このセクションには、サイト上でアクセスされた上位アプリケーション タイプがグラフ形式で表示されます。                                                                     |
| ブロックされたトランザクション数別上位アプリケーション (Top Applications by Blocked Transactions)   | トランザクションごとに発生するブロック アクションをトリガーした上位アプリケーション タイプが、グラフ形式で表示されます。                                                          |
| 一致したアプリケーション タイプ (Application Types Matched)                             | [総トランザクション数別上位アプリケーション タイプ (Top Applications Type by Total Transactions)] グラフに表示されているアプリケーション タイプについて、さらに詳しい情報を表示できます。 |
| 一致したアプリケーション (Applications Matched)                                      | 指定した時間範囲内のすべてのアプリケーションが表示されます。                                                                                         |

## [マルウェア対策 (Anti-Malware)] ページ

[レポート (Reporting)] > [マルウェア対策 (Anti-Malware)] ページでは、Cisco DVS エンジンによって検出されたマルウェアをモニターおよび識別することができます。

| セクション                                               | 説明                                                                                             |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)                   | レポートに含めるデータの時間範囲を選択できるメニュー。                                                                    |
| 検出された上位マルウェア カテゴリ (Top Malware Categories Detected) | DVS エンジンによって検出された上位のマルウェア カテゴリが表示されます。                                                         |
| 検出された上位マルウェア 脅威 (Top Malware Threats Detected)      | DVS エンジンによって検出された上位のマルウェア 脅威が表示されます。                                                           |
| マルウェア カテゴリ (Malware Categories)                     | [検出された上位マルウェア カテゴリ (Top Malware Categories Detected)] セクションに表示されている特定のマルウェア カテゴリに関する情報が表示されます。 |
| マルウェア 脅威 (Malware Threats)                          | [上位マルウェア 脅威 (Top Malware Threats)] セクションに表示されている特定のマルウェア の脅威に関する情報が表示されます。                     |



## [マルウェア カテゴリ (Malware Category)] レポート ページ

### Procedure

ステップ 1 [レポート (Reports)] > [マルウェア対策 (Anti-Malware)] を選択します。

ステップ 2 [マルウェア カテゴリ (Malware Categories)] インタラクティブテーブルで、[マルウェア カテゴリ (Malware Category)] カラム内のカテゴリをクリックします。

## [マルウェア脅威 (Malware Threats)] レポート ページ

### Procedure

ステップ 1 [レポート (Reports)] > [マルウェア対策 (Anti-Malware)] を選択します。

ステップ 2 [マルウェア脅威 (Malware Threats)] テーブルで、[マルウェア カテゴリ (Malware Category)] カラム内のカテゴリをクリックします。

## Advanced Malware Protection ページ

「[ファイルレピュテーションフィルタリングとファイル分析, on page 477](#)」を参照してください。

## [ファイル分析 (File Analysis)] ページ

「[ファイルレピュテーションおよびファイル分析のレポートとトラッキング, on page 499](#)」を参照してください。

## [セキュアエンドポイント判定のアップデート (AMPVerdictUpdates)] ページ

「[ファイルレピュテーションフィルタリングとファイル分析, on page 477](#)」を参照してください。

## [クライアント マルウェア リスク (Client Malware Risk)] ページ

[レポート (Reporting)] > [クライアントマルウェアリスク (Client Malware Risk)] ページは、クライアントマルウェアリスクアクティビティをモニターするために使用できるセキュリティ関連のレポートページです。[クライアントマルウェアリスク (Client Malware Risk)]

ページには、L4トラフィックモニター (L4TM) によって特定された、頻度の高いマルウェア接続に関与しているクライアント IP アドレスが表示されます。

| セクション                                                                          | 説明                                                                                                                                                                                    |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)                                              | レポートに含めるデータの時間範囲を選択できるメニュー。                                                                                                                                                           |
| Web プロキシ：マルウェア リスク別上位クライアント (Web Proxy: Top Clients by Malware Risk)           | このチャートには、マルウェアのリスクが発生した上位 10 人のユーザが表示されます。                                                                                                                                            |
| [L4トラフィックモニター:検出されたマルウェア接続 (L4 Traffic Monitor: Malware Connections Detected)] | このチャートには、組織内で最も頻繁にマルウェア サイトに接続しているコンピュータの IP アドレスが表示されます。                                                                                                                             |
| Web プロキシ：マルウェア リスク別クライアント (Web Proxy: Clients by Malware Risk)                 | [Web プロキシ：マルウェア リスク別クライアント (Web Proxy: Clients by Malware Risk)] テーブルには、[Web プロキシ：マルウェア リスク別上位クライアント (Web Proxy: Top Clients by Malware Risk)] セクションに表示されている個々のクライアントに関する詳細情報が表示されます。 |
| [L4トラフィックモニター:マルウェアリスク別クライアント (L4 Traffic Monitor: Clients by Malware Risk)]   | このテーブルには、組織内でマルウェア サイトに頻繁にアクセスしているコンピュータの IP アドレスが表示されます。                                                                                                                             |

## [Web プロキシ：マルウェア リスク別クライアント (Web Proxy: Clients by Malware Risk)] の [クライアントの詳細 (Client Detail)] ページ

[クライアントの詳細 (Client Detail)] ページには、指定した時間範囲における特定クライアントの Web アクティビティとマルウェア リスクの全データが表示されます。

### Procedure

- 
- ステップ 1** [レポート (Reporting)] > [クライアント マルウェア リスク (Client Malware Risk)] を選択します。
- ステップ 2** [Web プロキシ：クライアントマルウェアのリスク (Web Proxy-Client Malware Risk)] セクションで、[ユーザー ID/クライアント IP アドレス (User ID / Client IP Address)] 列のユーザー名をクリックします。
- 

### What to do next

[\[ユーザーの詳細 \(User Details\)\] ページ, on page 595](#)

## [Web レピュテーション フィルタ (Web Reputation Filters) ] ページ

[レポート (Reporting) ] > [Web レピュテーション フィルタ (Web Reputation Filters) ] ページは、指定した時間範囲内のトランザクションに対する Web レピュテーション フィルタ (ユーザーが設定) の結果を表示する、セキュリティ関連のレポート ページです。

| セクション                                                                                                | 説明                                                                    |
|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| [時間範囲 (Time Range) ] (ドロップダウン リスト)                                                                   | レポートに含めるデータの時間範囲を選択できるメニュー。                                           |
| Web レピュテーション アクション (トレンド) (Web Reputation Actions (Trend))                                           | 指定した時間 (横方向の時間軸) に対する Web レピュテーション アクションの総数 (縦方向の目盛り) が、グラフ形式で表示されます。 |
| Web レピュテーション アクション (ボリューム) (Web Reputation Actions (Volume))                                         | Web レピュテーション アクションのボリュームがトランザクション数との対比で表示されます。                        |
| ブロックされたトランザクション別 Web レピュテーション 脅威タイプ (Web Reputation Threat Types by Blocked Transactions)            | レピュテーション スコアが低いためブロックされた脅威タイプが表示されます。                                 |
| 詳細にスキャンされたトランザクション別 Web レピュテーション 脅威タイプ (Web Reputation Threat Types by Scanned Further Transactions) | トランザクションのスキャンを指示するレピュテーション スコアが生じた、脅威タイプが表示されます。                      |
| Web レピュテーション アクション (スコアによる内訳) (Web Reputation Actions (Breakdown by Score))                          | 各アクションの Web レピュテーション スコアの内訳が表示されます。                                   |

## [L4 トラフィック モニター (L4 Traffic Monitor) ] ページ

[レポート (Reporting) ] > [L4 トラフィック モニター (L4 Traffic Monitor) ] ページは、指定した時間範囲内に L4 トラフィック モニターが検出したマルウェア ポートとマルウェア サイトに関する情報を表示する、セキュリティ関連のレポート ページです。マルウェア サイトに頻繁にアクセスしているクライアントの IP アドレスも表示されます。

L4 トラフィック モニターは、アプライアンスのすべてのポートに着信するネットワーク トラフィックをリッスンし、ドメイン名と IP アドレスを独自のデータベース テーブルのエントリと照合して、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

| セクション                                   | 説明                                                     |
|-----------------------------------------|--------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)       | レポート対象の時間範囲を選択できるメニュー。                                 |
| 上位クライアント IP (Top Client IPs)            | 組織内で最も頻繁にマルウェア サイトに接続しているコンピュータの IP アドレスがグラフ形式で表示されます。 |
| 上位マルウェア サイト (Top Malware Sites)         | L4 トラフィック モニターによって検出された上位のマルウェア ドメインがグラフ形式で表示されます。     |
| クライアント ソース IP (Client Source IPs)       | 頻繁にマルウェア サイトに接続している組織内のコンピュータの IP アドレスが表示されます。         |
| マルウェア ポート (Malware Ports)               | L4 トラフィック モニターによって最も頻繁にマルウェア が検出されたポートが表示されます。         |
| 検出されたマルウェア サイト (Malware Sites Detected) | L4 トラフィック モニターによって最も頻繁にマルウェア が検出されたドメインが表示されます。        |

## [SOCKS プロキシ (SOCKS Proxy)] ページ

[レポート (Reporting)] > [SOCKS プロキシ (SOCKS Proxy)] ページでは、上位宛先およびユーザーに関する情報を含む、SOCKS プロキシを介して処理されたトランザクションのデータとトレンドを表示できます。

## [ユーザー ロケーション別のレポート (Reports by User Location)] ページ

[レポート (Reporting)] > [ユーザーの場所別レポート (Reports by User Location)] ページで、ローカルおよびリモート ユーザーが実行しているアクティビティを確認できます。

対象となるアクティビティは以下のとおりです。

- ローカル ユーザーおよびリモート ユーザーがアクセスしている URL カテゴリ。
- ローカル ユーザーおよびリモート ユーザーがアクセスしているサイトによってトリガーされているアンチマルウェア アクティビティ。
- ローカル ユーザーおよびリモート ユーザーがアクセスしているサイトの Web レピュテーション。
- ローカル ユーザーおよびリモート ユーザーがアクセスしているアプリケーション。
- ユーザー (ローカルおよびリモート)。
- ローカル ユーザーおよびリモート ユーザーがアクセスしているドメイン。

| セクション                                                                           | 説明                                                                              |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| [時間範囲 (Time Range) ] (ドロップダウン リスト)                                              | レポートに含めるデータの時間範囲を選択できるメニュー。                                                     |
| Web プロキシ アクティビティ<br>総数：リモート ユーザー<br>(Total Web Proxy Activity:<br>Remote Users) | 指定した時間 (横方向) におけるリモート ユーザーのアクティビティ (縦方向) が表示されます。                               |
| Web プロキシの概要 (Web Proxy Summary)                                                 | ネットワーク上のローカルユーザーとリモートユーザーのアクティビティの要約が表示されます。                                    |
| Web プロキシ アクティビティ<br>総数：ローカル ユーザー<br>(Total Web Proxy Activity:<br>Local Users)  | 指定した時間 (横方向) におけるリモート ユーザーのアクティビティ (縦方向) が表示されます。                               |
| 検出された疑わしいトランザクション：リモート ユーザー<br>(Suspect Transactions Detected:<br>Remote Users) | 指定した時間内 (横方向) に、リモート ユーザー向けに定義されたアクセス ポリシーによって検出された、疑わしいトランザクション (縦方向) が表示されます。 |
| 疑わしいトランザクションの要約 (Suspect Transactions Summary)                                  | ネットワーク上のリモート ユーザーの疑わしいトランザクションの要約が表示されます。                                       |
| 検出された疑わしいトランザクション：ローカル ユーザー<br>(Suspect Transactions Detected:<br>Local Users)  | 指定した時間内 (横方向) に、リモート ユーザー向けに定義されたアクセス ポリシーによって検出された、疑わしいトランザクション (縦方向) が表示されます。 |
| 疑わしいトランザクションの要約 (Suspect Transactions Summary)                                  | ネットワーク上のローカル ユーザーの疑わしいトランザクションの要約が表示されます。                                       |

## [Web トラッキング (Web Tracking) ] ページ

[Web トラッキング (Web Tracking) ] ページを使用して、個々のトランザクションまたは疑わしいトランザクションのパターンを検索し、その詳細を取得します。必要に応じて、以下のタブのいずれかで検索を行います。

|                                                                                    |                                                                 |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| <b>[Web トラッキング (Web Tracking) ]</b> ページ                                            | タスクへのリンク                                                        |
| Web プロキシによって処理されたトランザクション (Transactions processed by the Web Proxy)                | <a href="#">Web プロキシによって処理されるトランザクションの検索 , on page 605</a>      |
| L4 トラフィック モニターによって処理されたトランザクション (Transactions processed by the L4 Traffic Monitor) | <a href="#">L4 トラフィック モニタによって処理されたトランザクションの検索 , on page 608</a> |
| SOCKS プロキシによって処理されたトランザクション (Transactions processed by the SOCKS Proxy)            | <a href="#">SOCKS プロキシによって処理されるトランザクションの検索 , on page 609</a>    |

または、透過的なパススルーなどの場合に、FQDN を使用して [Web トラッキング (Web Tracking) ] ページで Web サイトデータを検索します。



**Note** 透過的なリクエストでは、ドメインまたはサーバーの名前がトラッキングページに表示されません。ただし、透過的なパススルーを含む透過的な要求が SNI なしで送信されると、IP アドレスが表示されます。

## Web プロキシによって処理されるトランザクションの検索

[レポート (Reporting) ] > [Web トラッキング (Web Tracking) ] ページの [プロキシ サービス (Proxy Services) ] タブを使用して、特定のユーザーまたはすべてのユーザーの Web の使用状況を追跡し、レポートできます。

所定の期間内に記録されたトランザクションのタイプ (ブロック、モニターリング、および警告されたトランザクション、完了したトランザクションなど) の検索結果を表示できます。URL カテゴリ、マルウェアの脅威、アプリケーションなど、複数の条件を使用してデータ結果をフィルタリングすることもできます。



**Note** Web プロキシは、「OTHER-NONE」以外の ACL デシジョン タグを含むトランザクションのみレポートします。

### Procedure

**ステップ 1** [レポート (Reporting) ] > [Web トラッキング (Web Tracking) ] を選択します。

**ステップ 2** [プロキシ サービス (Proxy Services) ] タブをクリックします。

**ステップ 3** 設定項目を設定します。

| 設定                              | 説明                                                                                                                                                                                                                                                      |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 時間範囲 (Time Range)               | レポート対象の時間範囲を選択します。                                                                                                                                                                                                                                      |
| ユーザー/クライアント IP (User/Client IP) | (任意) レポートに表示される認証ユーザー名、または追跡対象のクライアント IP アドレスを入力します。IP 範囲を CIDR 形式で入力することもできます。<br>このフィールドを空にしておくと、すべてのユーザーに関する検索結果が返されます。                                                                                                                              |
| Web サイト (Website)               | (任意) 追跡対象の Web サイトを入力します。このフィールドを空にしておくと、すべての Web サイトに関する検索結果が返されます。<br><br><b>Note</b><br>SNI (サーバー名指定) で検索できます。SNI、TLS プロトコルの拡張子を使用して、クライアントは Web トランザクションの実行中に安全にホスト名を指定できます。単語全体を指定する必要があります。<br><br>SNI を有効にするには、AMP、およびレピュテーションサービスを有効にする必要があります。 |
| トランザクション タイプ (Transaction Type) | 追跡対象のトランザクションのタイプを [すべてのトランザクション (All Transactions) ]、[完了 (Completed) ]、[ブロックされた (Blocked) ]、[モニタ対象 (Monitored) ]、または [警告対象 (Warned) ] から選択します。                                                                                                         |

**ステップ 4** (任意) [詳細設定 (Advanced) ] セクションを展開してフィールドを設定し、より詳細な条件で Web トラッキングの結果をフィルタリングします。

| 設定                      | 説明                                                                                                                                                                                                                                                              |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL カテゴリ (URL Category) | URL カテゴリでフィルタリングするには、[URL カテゴリ別フィルタ (Filter by URL Category) ] を選択し、フィルタリング対象とする URL カテゴリの先頭文字を入力します。表示されたリストからカテゴリを選択します。                                                                                                                                      |
| アプリケーション (Application)  | アプリケーションでフィルタリングするには、[アプリケーションによるフィルタ (Filter by Application) ] を選択し、フィルタリングに使用するアプリケーションを選択します。<br><br>アプリケーションタイプでフィルタリングするには、[アプリケーションタイプによるフィルタ (Filter by Application Type) ] を選択し、フィルタリングに使用するアプリケーションタイプを選択します。                                          |
| ポリシー                    | このトランザクションに対して最終決定を行うポリシーの名前でフィルタするには、[アクションポリシーによってフィルタ (Filter by Action Policy) ] を選択し、フィルタリングに使用するポリシー グループ名 (アクセス ポリシー、復号ポリシー、またはデータセキュリティ ポリシー) を入力します。詳細については、 <a href="#">アクセス ログ ファイル内の Web プロキシ情報, on page 686</a> の PolicyGroupName に関する説明を参照してください。 |

| 設定                          | 説明                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advanced Malware Protection | <a href="#">Web トラッキング機能と Advanced Malware Protection 機能について</a> , on page 502を参照してください。                                                                                                                                                                                                                                                                                                                             |
| マルウェアの脅威                    | <p>特定のマルウェアの脅威でフィルタリングするには、[マルウェア脅威によるフィルタ (Filter by Malware Threat)] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。</p> <p>マルウェア カテゴリでフィルタリングするには、[マルウェアカテゴリによるフィルタ (Filter by Malware Category)] を選択し、フィルタリングに使用するマルウェア カテゴリを選択します。</p>                                                                                                                                                                                        |
| WBRs                        | <p>[WBRs] セクションでは、Web レピュテーション スコアによるフィルタリングと、特定の Web レピュテーションの脅威によるフィルタリングが可能です。</p> <ul style="list-style-type: none"> <li>Web レピュテーション スコアでフィルタリングするには、[スコア範囲 (Score Range)] を選択し、フィルタリングに使用する上限値と下限値を選択します。あるいは、[スコアなし (No Score)] を選択すると、スコアがない Web サイトをフィルタリングできます。</li> <li>Web レピュテーションの脅威でフィルタリングするには、[レピュテーション脅威によるフィルタ (Filter by Reputation Threat)] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。</li> </ul> |
| AnyConnect セキュア モビリティ       | ユーザーの場所 (リモートまたはローカル) によってフィルタリングするには、[ユーザーの場所でフィルタ (Filter by User Location)] を選択し、フィルタリングするユーザー タイプを選択します。                                                                                                                                                                                                                                                                                                         |
| ユーザー リクエスト                  | <p>クライアントによって開始されたトランザクションでフィルタリングするには、[ユーザーが要求したトランザクションによるフィルタ (Filter by User-Requested Transactions)] を選択します。</p> <p><b>Note</b><br/>このフィルタをイネーブルにすると、検索結果に「最も想定される」トランザクションが含まれることがあります。</p>                                                                                                                                                                                                                    |
| カプセル化された URL の保護            | <p>カプセル化された URL トランザクションでこのフィルタを有効にします。</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>HTTPS プロキシを有効にする必要があります。 <a href="#">HTTPS プロキシのイネーブル化</a>, on page 348を参照してください</li> <li><a href="https://translate.google.com">https://translate.google.com</a> の Web レピュテーション スコアの範囲が復号する設定になっていることを確認します。 <a href="#">復号ポリシー グループの Web レピュテーション フィルタの設定</a>, on page 470を参照してください</li> </ul>               |

ステップ 5 [検索 (Search)] をクリックします。



結果はタイム スタンプでソートされ、最新の結果が最上部に表示されます。

[詳細の表示 (Display Details)] リンクの下のカッコ内の数値は、ロードされたイメージ、実行された JavaScript、アクセスされたセカンダリ サイトなど、ユーザーが開始したトランザクションによって発生した関連トランザクションの数を示します。

**ステップ 6** (任意) [トランザクション (Transactions)] 列の [詳細の表示 (Display Details)] をクリックし、各トランザクションに関する詳細情報を表示します。

#### Note

1000 件を超える結果を表示する必要がある場合は、[印刷可能なダウンロード (Printable Download)] リンクをクリックすると、関連するトランザクションの詳細を除く raw データ一式が含まれた CSV ファイルを取得できます。

#### Tip

結果内の URL が切り詰められている場合、アクセス ログで完全な URL を確認できます。

500 件までの関連トランザクションの詳細を表示するには、[関連トランザクション (Related Transactions)] リンクをクリックします。

### What to do next

- [URL カテゴリ セットの更新とレポート , on page 598](#)
- [マルウェアのカテゴリについて, on page 475](#)
- [Web トラッキング機能と Advanced Malware Protection 機能について , on page 502](#)

## L4 トラフィック モニタによって処理されたトランザクションの検索

[レポート (Reporting)] > [Web トラッキング (Web Tracking)] ページの [L4 トラフィック モニター (L4 Traffic Monitor)] タブには、マルウェア サイトおよびポートへの接続に関する詳細情報が表示されます。マルウェア サイトへの接続は、次のタイプの情報によって検索できます。

- 時間範囲
- サイト、使用された IP アドレスまたはドメイン
- ポート (Port)
- 組織内のコンピュータに関連付けられた IP アドレス
- 接続タイプ

一致した検索結果のうち最初の 1000 件が表示されます。

## SOCKS プロキシによって処理されるトランザクションの検索

ブロックまたは完了したトランザクション、ユーザー、および宛先ドメイン、IP アドレス、またはポートなど含む、さまざまな基準を満たすトランザクションを検索できます。

### Procedure

**ステップ 1** [ウェブ (Web)] > [レポート (Reporting)] > [Web トラッキング (Web Tracking)] を選択します。

**ステップ 2** [SOCKS プロキシ (SOCKS Proxy)] タブをクリックします。

**ステップ 3** 結果をフィルタリングするには、[詳細設定 (Advanced)] をクリックします。

**ステップ 4** 検索条件を入力します。

**ステップ 5** [検索] をクリックします。

### What to do next

[\[SOCKS プロキシ \(SOCKS Proxy\)\] ページ](#), on page 603

## [システム容量 (System Capacity)] ページ

[レポート (Reporting)] > [システム容量 (System Capacity)] ページには、Secure Web Appliance のリソース使用率に関する現在および履歴情報が表示されます。

[システム容量 (System Capacity)] ページにデータを表示する時間範囲を選択する場合、以下のことに留意することが重要です。

- **Hour レポート。** Hour レポートは、分テーブルに照会して、60 分間を超える分単位で、1 分間にアプライアンスに記録されたアイテム（バイトや接続など）の正確な数を表示します。
- **Day レポート。** Day レポートは、時間テーブルに照会して、24 分間を超える時間単位で、1 時間にアプライアンスに記録されたアイテム（バイトや接続など）の正確な数を表示します。この情報は時間テーブルから収集されます。

Week レポートおよび 30 Days レポートは、Hour レポートおよび Day レポートと同じように動作します。

## [システムステータス (System Status)] ページ

システム ステータスをモニターするには、[レポート (Reporting)] > [システム ステータス (System Status)] ページを使用します。このページは、Secure Web Appliance の現在のステータスと設定を表示します。

| セクション                                                                | 表示内容                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Web Appliance<br>のステータス (Web<br>Security Appliance<br>Status) | <ul style="list-style-type: none"> <li>• システムの動作期間</li> <li>• システム リソースの使用率：レポーティングおよびロギングに使用される CPU 使用率、RAM 使用率、およびディスク領域の使用率。</li> </ul> <p>このページに表示される CPU 使用率値はさまざまな瞬間に個別に読み取られるため、システムの [概要 (Overview) ] ページ (<a href="#">[概要 (Overview) ] ページ, on page 593</a>) に表示される CPU 値と若干異なる場合があります。</p> <p>システムによって使用されない RAM は Web オブジェクトキャッシュによって使用されるので、効率的に動作する RAM 使用率は 90% を超える場合があります。システムで重大なパフォーマンス問題が発生していない場合で、この値が 100% に固定されない場合、システムは正常に動作しています。</p> <p><b>Note</b><br/>プロキシバッファ メモリは、この RAM を使用する 1 つのコンポーネントです。</p> |
| プロキシトラフィック<br>の特性 (Proxy Traffic<br>Characteristics)                 | <ul style="list-style-type: none"> <li>• 1 秒あたりのトランザクション</li> <li>• 帯域幅</li> <li>• 応答時間</li> <li>• キャッシュ ヒット率</li> <li>• 接続</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                           |
| Web トラフィック<br>タップ (Web Traffic<br>Tap)                               | Web トラフィック タップ CPU 使用率。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 高可用性 (High<br>Availability)                                          | 高可用性サービスのステータス。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 外部サービス<br>(External Services)                                        | <ul style="list-style-type: none"> <li>• Identity Services Engine</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| セクション                         | 表示内容                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 現在の設定 (Current Configuration) | <p>Web プロキシ設定：</p> <ul style="list-style-type: none"><li>• Web プロキシのステータス：イネーブルまたはディセーブル。</li><li>• 展開トポロジ</li><li>• Web プロキシ モード：フォワードまたは透過。</li><li>• IP スプーフィング：イネーブルまたはディセーブル。</li></ul> <p>L4 トラフィック モニター設定：</p> <ul style="list-style-type: none"><li>• L4 トラフィック モニターのステータス：イネーブルまたはディセーブル。</li><li>• L4 トラフィック モニターの配線。</li><li>• L4 トラフィック モニターのアクション：モニターまたはブロック。</li></ul> <p>Web トラフィック タップ設定：</p> <ul style="list-style-type: none"><li>• Web トラフィック タップのステータス：イネーブルまたはディセーブル。</li><li>• Web トラフィック タップ インターフェイス：P1、P2、TI、T2</li></ul> <p>Secure Web Appliance バージョン情報</p> <p>ハードウェア情報</p> |

#### 関連項目

[\[システム容量 \(System Capacity\) \] ページ, on page 609](#)

## 新しい Web インターフェイスでのセキュア アプライアンス レポート

この章で説明する内容は、次のとおりです。

- [新しい Web インターフェイスの Web レポート ページの概要 \(612 ページ\)](#)
- [\(Web レポートのみ\) チャート化するデータの選択 \(644 ページ\)](#)
- [新しい Web インターフェイスでの Web トラッキング \(645 ページ\)](#)
- [Web トラッキングの検索結果の使用 \(651 ページ\)](#)

- [新しい Web インターフェイスでの Web レポートのスケジューリングとアーカイブ](#) (653 ページ)
- [新しい Web インターフェイスの \[システムステータス \(System Status\)\] ページ](#) (656 ページ)

## 新しい Web インターフェイスの Web レポート ページの概要

次の表は、Secure Web Appliance 用 AsyncOS のサポートされている最新リリースで、Web インターフェイスの [レポート (Reports)] ドロップダウンから利用できるレポートを示します。詳細については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用](#) (587 ページ) を参照してください。Secure Web Appliance でこれ以前のリリースの AsyncOS を実行している場合は、これらのレポートの一部を利用できません。

表 12: [Web レポート (Web Reports)] ドロップダウンのオプション

| [レポート (Reports)] ドロップダウンのオプション                | 操作                                                                                                                                                                                                                      |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 一般的なレポート                                      |                                                                                                                                                                                                                         |
| [概要 (Overview)] ページ                           | [概要 (Overview)] ページには、Secure Web Appliance でのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフおよび要約テーブルが含まれます。詳細については、 <a href="#">[概要 (Overview)] ページ</a> (616 ページ) を参照してください。                                             |
| [アプリケーションの表示 (Application Visibility)] ページ    | [アプリケーションの表示 (Application Visibility)] ページでは、セキュリティ管理アプライアンスおよび Secure Web Appliance 内で特定のアプリケーションタイプに適用されているコントロールを適用し、表示できます。詳細については、 <a href="#">[アプリケーションの表示 (Application Visibility)] ページ</a> (618 ページ) を参照してください。 |
| [レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor)] ページ | 指定した時間範囲内に L4 トラフィック モニタで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。詳細については、 <a href="#">[レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor)] ページ</a> (620 ページ) を参照してください。                                                             |
| [SOCKS プロキシ (SOCKS Proxy)] ページ                | 宛先、ユーザなど、SOCKS プロキシ トランザクションのデータを表示できます。詳細については、 <a href="#">[SOCKS プロキシ (SOCKS Proxy)] ページ</a> (623 ページ) を参照してください。                                                                                                    |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [レポート (Reports) ] ドロップダウンのオプション | 操作                                                                                                                                                                                                                                                                                                                                                                                                      |
| [URLカテゴリ (URL Categories) ] ページ | <p>[URLカテゴリ (URL Categories) ] ページでは、アクセスされている次の上位 URL カテゴリを表示できます。</p> <ul style="list-style-type: none"><li>• トランザクションごとに発生するブロック アクションまたは警告アクションをトリガーした上位 URL。</li><li>• 完了したトランザクションと、警告とブロックが行われたトランザクションの両方を対象とした、指定した時間範囲内のすべての URL カテゴリ。これはインタラクティブな列見出しのあるインタラクティブ テーブルとなっていて、必要に応じてデータをソートできます。</li></ul> <p>詳細については、<a href="#">[URLカテゴリ (URL Categories) ] ページ (625 ページ)</a> を参照してください。</p> |

| [レポート (Reports) ] ドロップダウンのオプション | 操作                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ユーザ (Users) ] ページ              | <p>[ユーザ (Users) ] ページには複数の Web トラッキング リンクが表示され、各ユーザの Web トラッキング情報を確認できます。</p> <p>[ユーザ (Users) ] ページでは、システム上のユーザ (1 人または複数) がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。</p> <p>[ユーザ (Users) ] ページのインタラクティブな [ユーザ (Users) ] テーブルで個々のユーザをクリックすると、その特定のユーザの詳細情報が [ユーザの詳細 (User Details) ] ページに表示されます。</p> <p>[ユーザの詳細 (User Details) ] ページでは、[ユーザ (Users) ] ページの [ユーザ (Users) ] テーブルで指定したユーザに関する具体的な情報を確認できます。このページから、お使いのシステムでの各ユーザのアクティビティを調査できます。特に、ユーザ レベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。</p> <p>詳細については、<a href="#">[ユーザ (Users) ] ページ (629 ページ)</a> を参照してください。</p> <p>システムにおける各ユーザの情報については、<a href="#">[ユーザの詳細 (User Details) ] ページ (Web レポートینگ) (631 ページ)</a> を参照してください。</p> |
| [Web サイト (Web Sites) ] ページ      | <p>[Web サイト (Web Sites) ] ページでは、管理対象アプライアンスで発生しているアクティビティ全体を集約して表示できます。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。詳細については、<a href="#">[Web サイト (Web Sites) ] ページ (634 ページ)</a> を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| [HTTPS レポート (HTTPS Reports) ]   | <p>[HTTPS レポート (HTTPS Reports) ] レポート ページでは、管理対象のアプライアンスの HTTP/HTTPS トラフィック サマリー (トランザクションまたは帯域幅の使用量) のすべてを集約しています。詳細については、<a href="#">[HTTPS レポート (HTTPS Reports) ] ページ (627 ページ)</a> を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                                                  |                                                                                                                                                                                                                                                                             |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [レポート (Reports)] ドロップダウンのオプション                   | 操作                                                                                                                                                                                                                                                                          |
| 脅威レポート                                           |                                                                                                                                                                                                                                                                             |
| [マルウェア対策 (Anti-Malware)] ページ                     | [マルウェア対策 (Anti-Malware)] ページでは、指定した時間範囲内にアンチマルウェア スキャン エンジンで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。レポートの上部には、上位の各マルウェア ポートおよび各マルウェア Web サイトの接続数が表示されます。レポートの下部には、検出されたマルウェア ポートとマルウェア サイトが表示されます。詳細については、 <a href="#">[マルウェア対策 (Anti-Malware)] ページ (637 ページ)</a> を参照してください。 |
| Advanced Malware Protection ページ                  | Advanced Malware Protection では、既知のファイルレピュテーションを取得し、レピュテーションサービスには未知である特定のファイルの動作を分析し、新しい情報が利用可能になったときに新たな脅威を継続的に評価し、ネットワークに侵入した後に脅威と判断されたファイルについて通知することによって、ゼロデイの脅威や標的型のファイルベースの脅威から保護します。詳細については、 <a href="#">Advanced Malware Protection ページ (635 ページ)</a> を参照してください。     |
| [クライアント マルウェア リスク (Client Malware Risk)] ページ     | [クライアントマルウェアリスク (Client Malware Risk)] ページは、セキュリティ関連のレポートページです。このページを使用して、著しく頻繁にマルウェア サイトへ接続している可能性がある個々のクライアント コンピュータを特定できます。<br><br>詳細については、 <a href="#">[クライアントマルウェアリスク (Client Malware Risks)] ページ (641 ページ)</a> を参照してください。                                             |
| [Web レピュテーション フィルタ (Web Reputation Filters)] ページ | 指定した時間範囲内のトランザクションに対する、Web レピュテーション フィルタリングに関するレポートを表示できます。詳細については、「 <a href="#">[Web レピュテーション フィルタ (Web Reputation Filters)] ページ (642 ページ)</a> 」を参照してください。                                                                                                                 |

## [滞留時間 (Time Spent)] について

さまざまなテーブルの [滞留時間 (Time Spent)] 列は、Web ページでユーザーが費やした時間を表します。各 URL カテゴリでユーザーが費やした時間。ユーザーを調査する目的で使われます。URL のトラッキング時には、その特定の URL に各ユーザーが費やした時間。



トランザクションイベントに「viewed」のタグが付けられる（ユーザーが特定の URL に進む）と、[滞留時間 (Time Spent)] の値の計算が開始され、Web レポート テーブルのフィールドとして追加されます。

費やされた時間を計算するため、AsyncOS はアクティブ ユーザーごとに、1 分間のアクティビティに対して 60 秒という時間を割り当てます。この 1 分間の終わりに、各ユーザーが費やした時間は、そのユーザーが訪れた各ドメイン間で均等に配分されます。たとえば、あるユーザーがアクティブな 1 分間に 4 つの異なるドメインに進んだ場合、そのユーザーは各ドメインで 15 分ずつ費やしたと見なされます。

経過時間の値に関して、以下の注意事項を考慮してください。

- アクティブ ユーザーは、アプライアンスを介して HTTP トラフィックを送信し、Web サイトにアクセスした、すなわち AsyncOS が「ページ ビュー」と見なす動作を行ったユーザー名または IP アドレスとして定義されています。
- AsyncOS では、クライアント アプリケーションが開始する要求とは逆に、ユーザーが開始する HTTP 要求としてページ ビューを定義します。AsyncOS はヒューリスティック アルゴリズムを使用して、可能な限り効果的にユーザー ページ ビューを識別します。

単位は時間：分形式で表示されます。

## [概要 (Overview)] ページ

[概要 (Overview)] レポート ページには、Secure Web Appliance でのアクティビティの概要が表示されます。これには、着信および発信 トランザクションに関するグラフおよび要約 テーブルが含まれます。

[概要 (Overview)] レポート ページを表示するには、[レポート (Reports)] ドロップダウンから [モニタリング (Monitoring)] > [概要 (Overview)] を選択します。詳細については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#) を参照してください。

[概要 (Overview)] レポート ページの上部には、URL とユーザの使用量に関する統計情報、Web プロキシ アクティビティ、および各種 トランザクション サマリーが表示されます。トランザクション サマリーには、さらに詳細なトレンド情報が示されます。たとえば、疑わしい トランザクションと、そのグラフの隣にそれらの トランザクション がブロックされた数、およびブロックされた方法が表示されます。

[概要 (Overview)] レポート ページの下半分は、使用状況に関する情報に使用されます。つまり、表示されている上位 URL カテゴリ、ブロックされている上位 アプリケーション タイプ および カテゴリ、これらのブロックまたは警告を生成している上位 ユーザが表示されます。

表 13: [概要 (Overview)] ページの詳細

| セクション                             | 説明                                                                         |
|-----------------------------------|----------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト) | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。 |

| セクション                                                                     | 説明                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Webプロキシアクティビティ総数 (Total Web Proxy Activity) ]                            | <p>現在セキュリティ管理アプライアンスで管理されている Secure Web Applianceによって報告される Web プロキシアクティビティを表示できます。</p> <p>このセクションには、トランザクションの実際の数、およびアクティビティが発生したおよその日付がグラフ形式で表示されます。</p> <p>疑わしいWebプロキシアクティビティまたは正常なプロキシアクティビティの比率を、トランザクションの総数も含めて表示できます。</p>     |
| [疑わしいトランザクション (Suspect Transactions) ]                                    | <p>管理者が疑わしいトランザクションと分類した Web トランザクションをグラフ形式で表示できます。</p> <p>このセクションには、トランザクションの実際の数、およびアクティビティが発生したおよその日付がグラフ形式で表示されます。</p> <p>ブロックまたは警告された疑わしいトランザクションの比率も表示できます。また、検出されてブロックされたトランザクションのタイプ、およびそのトランザクションが実際にブロックされた回数を確認できます。</p> |
| [L4トラフィックモニタの概要 (L4 Traffic Monitor Summary) ]                            | <p>現在セキュリティ管理アプライアンスで管理されている Secure Web Applianceによって報告される L4 トラフィックをグラフ形式で表示できます。</p>                                                                                                                                              |
| 上位 URL カテゴリ : 総トランザクション数 (Top URL Categories: Total Transactions)         | <p>ブロックされている上位の URL カテゴリが、URL カテゴリのタイプおよび特定タイプのカテゴリが実際にブロックされた回数を含め、グラフ形式で表示されます。</p> <p>すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、<a href="#">URL カテゴリ セットの更新とレポート (626 ページ)</a> を参照してください。</p>                 |
| 上位アプリケーション タイプ : 総トランザクション数 (Top Application Types: Total Transactions)   | <p>ブロックされている上位アプリケーションタイプが、実際のアプリケーションタイプ名および特定のアプリケーションがブロックされた回数を含め、グラフ形式で表示されます。</p>                                                                                                                                             |
| 上位マルウェアカテゴリ : モニタまたはブロック済み (Top Malware Categories: Monitored or Blocked) | <p>検出されたすべてのマルウェア カテゴリをグラフ形式で表示できます。</p>                                                                                                                                                                                            |

| セクション                                                                  | 説明                                                                         |
|------------------------------------------------------------------------|----------------------------------------------------------------------------|
| ブロックまたは警告されたトランザクション数の上位ユーザ (Top Users Blocked or Warned Transactions) | ブロックまたは警告されたトランザクションを生成している実際のユーザをグラフ形式で表示できます。ユーザは IP アドレスまたはユーザ名で表示できます。 |
| [上位の脅威カテゴリ : WBRsによりブロック (Top Threat Categories: Blocked) ]            | ブロックされたすべての脅威カテゴリを表示できます (グラフ形式)。                                          |

## [アプリケーションの表示 (Application Visibility) ] ページ



(注) [アプリケーションの表示 (Application Visibility) ] の詳細については、『User Guide for AsyncOS for Cisco Secure Web Appliance』の「Understanding Application Visibility and Control」のトピックを参照してください。

[アプリケーションの表示 (Application Visibility) ] レポートページでは、セキュリティ管理アプライアンスおよび Secure Web Appliance 内の特定のアプリケーションタイプに制御を適用することができます。

[アプリケーションの表示 (Application Visibility) ] レポートページを表示するには、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [アプリケーションの表示 (Application Visibility) ] を選択します。詳細については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#) を参照してください。

アプリケーション制御を使用すると、たとえば URL フィルタリングのみを使用する場合よりも Web トラフィックをきめ細かく制御できるだけでなく、次のタイプのアプリケーションおよびアプリケーションタイプに対する制御を強化できます。

- 回避アプリケーション (アノニマイザや暗号化トンネルなど)。
- コラボレーション アプリケーション (Cisco Webex、Facebook、インスタント メッセージングなど)。
- リソースを大量消費するアプリケーション (ストリーミング メディアなど)。

### アプリケーションとアプリケーションタイプの違いについて

レポートに関連するアプリケーションを制御するには、アプリケーションとアプリケーションタイプの違いを理解することが非常に重要です。

- **アプリケーションタイプ。** 1つまたは複数のアプリケーションを含むカテゴリです。たとえば検索エンジンは、Google Search や Craigslist などの検索エンジンを含むアプリケーションタイプです。インスタント メッセージングは、Yahoo Instant Messenger や Cisco Webex などを含む別のアプリケーションタイプです。Facebook もアプリケーションタイプです。



(注) AVC のすべてのアプリケーション タイプが ADC に適用できるわけではありません。

- **アプリケーション。** アプリケーションタイプに属している特定のアプリケーションです。たとえば、YouTube はメディア アプリケーション タイプに含まれるアプリケーションです。
- **アプリケーション動作。** アプリケーション内でユーザが実行できる特定のアクションまたは動作です。たとえば、ユーザは Yahoo Messenger などのアプリケーションの使用中にファイルを転送できます。すべてのアプリケーションに、設定可能なアプリケーション動作が含まれているわけではありません。

[アプリケーションの表示 (Application Visibility)] ページには次の情報が表示されます。

表 14: [アプリケーションの表示 (Application Visibility)] ページの詳細

| セクション                                                                    | 説明                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)                                        | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                   |
| [総トランザクション数の上位アプリケーションタイプ (Top Application Types by Total Transactions)] | <p>サイト上でアクセスされた上位のアプリケーションタイプがグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p> <p>たとえば、Yahoo Instant Messenger などのインスタントメッセージング ツール、Facebook、Presentation というアプリケーション タイプが表示されます。</p> |

| セクション                                                                     | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ブロックされたトランザクション数の上位アプリケーション (Top Applications by Blocked Transactions) ] | <p>トランザクションごとに発生するブロックアクションをトリガーした上位アプリケーションタイプが、グラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p> <p>たとえば、ユーザが Google Talk や Yahoo Instant Messenger などの特定のアプリケーションタイプを起動しようとしたが、特定のポリシーが適用されているために、ブロックアクションがトリガーされたとします。このアプリケーションは、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。</p> |
| [一致したアプリケーションタイプ (Application Types Matched) ]                            | <p>[一致したアプリケーションタイプ (Application Types Matched) ] インタラクティブ テーブルでは、[総トランザクション数の上位アプリケーションタイプ (Top Applications Type by Total Transactions) ] テーブルに表示されているアプリケーションタイプに関するさらに詳しい情報を表示できます。</p> <p>[アプリケーション (Applications) ] カラムで、詳細を表示するアプリケーションをクリックできます。</p>                                                                                                                                                                                        |
| [一致したアプリケーション (Applications Matched) ]                                    | <p>[一致したアプリケーション (Applications Matched) ] インタラクティブ テーブルには、指定した時間範囲内のすべてのアプリケーションが表示されます。</p> <p>さらに、[一致したアプリケーション (Application Matched) ] セクション内で特定のアプリケーションを検索できます。このセクション下部のテキストフィールドに特定のアプリケーション名を入力し、[アプリケーションの検索 (Find Application) ] をクリックします。</p>                                                                                                                                                                                            |

## [レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ] ページ

[レイヤ4トラフィックモニター (Layer 4 Traffic Monitor Page) ] レポートページには、指定した時間範囲内にレイヤ4トラフィックモニターによってお使いの Secure Web Appliance 上で検出されたマルウェアポートとマルウェアサイトに関する情報が表示されます。マルウェアサイトに頻繁にアクセスしているクライアントの IP アドレスも表示されます。

[Web サイト (Web Sites) ] レポートページを表示するには、[レポート (Reports) ] ドロップダウンから [モニターリング (Monitoring) ] > [Web サイト (Web Sites) ] を選択します。詳細に

については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#) を参照してください。

レイヤ 4 トラフィックモニターは、各 Secure Web Applianceのすべてのポートに着信するネットワークトラフィックをリッスンし、ドメイン名と IP アドレスを独自のデータベーステーブルのエントリと照合して、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

このレポートのデータを使用して、ポートまたはサイトをブロックするかどうかを判断したり、特定のクライアント IP アドレスが著しく頻繁にマルウェアサイトに接続している理由（たとえば、その IP アドレスに関連付けられたコンピュータが、中央のコマンド/コントロールサーバに接続しようとするマルウェアに感染しているなど）を調査したりできます。

表 15:[レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor)] ページの詳細

| セクション                                                                     | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)                                         | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                                                                                                     |
| 上位クライアントIP：検出されたマルウェア接続 (Top Client IPs: Malware Connections Detected)    | <p>組織内で最も頻繁にマルウェアサイトに接続している上位のコンピュータの IP アドレスがグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">チャート化するデータの選択 (583 ページ)</a> を参照してください。</p> <p>このグラフは、<a href="#">[クライアント マルウェア リスク (Client Malware Risks)] ページ (641 ページ)</a> の[レイヤ4トラフィックモニタ：検出されたマルウェア接続 (Layer 4 Traffic Monitor: Malware Connections Detected)] グラフと同じです。</p> |
| 上位マルウェアサイト：検出されたマルウェア接続 (Top Malware Sites: Malware Connections Detected) | <p>レイヤ 4 トラフィック モニタによって検出された上位のマルウェア ドメインがグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">チャート化するデータの選択 (583 ページ)</a> を参照してください。</p>                                                                                                                                                                                           |

| セクション                              | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [クライアントソースIP (Client Source Ips) ] | <p>このインタラクティブテーブルを使用すると、組織内でマルウェア サイトに頻繁に接続しているコンピュータの IP アドレスを表示できます。</p> <p>特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[クライアントIPによるフィルタ (Filter by Client IP) ] をクリックします。この機能を使用して、マルウェアがどのポートを使用してマルウェア サイトへ「誘導」しているかを判断できます。</p> <p>各接続のポートや宛先ドメインなどの詳細情報を表示するには、テーブル内のエントリをクリックします。たとえば、ある特定のクライアント IP アドレスの [ブロックされたマルウェア接続 (Malware Connections Blocked) ] が高い数値を示している場合、その列の数値をクリックすると、ブロックされた各接続のリストが表示されます。このリストは、[Webトラッキング検索 (Web Tracking Search) ] ページの [レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ] タブに検索結果として表示されます。リストの詳細については、<a href="#">レイヤ4トラフィック モニターによって処理されたトランザクションの検索 (650ページ)</a> を参照してください。</p> <p>このグラフは、[クライアントマルウェア リスク (Client Malware Risks) ] ページ (641 ページ) の [レイヤ4トラフィックモニタ : 検出されたマルウェア接続 (Layer 4 Traffic Monitor: Malware Connections Detected) ] グラフと同じです。</p> |
| [マルウェアポート (Malware Ports) ]        | <p>このインタラクティブテーブルを使用すると、レイヤ4トラフィック モニタによって最も頻繁にマルウェアが検出されたポートを表示できます。</p> <p>詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[検出されたマルウェア接続の総数 (Total Malware Connections Detected) ] の数値をクリックすると、そのポートの各接続の詳細情報が表示されます。このリストは、[Webトラッキング検索 (Web Tracking Search) ] ページの [レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ] タブに検索結果として表示されます。リストの詳細については、<a href="#">レイヤ4トラフィック モニターによって処理されたトランザクションの検索 (650 ページ)</a> を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                                    |



| セクション                                    | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [検出されたマルウェアサイト (Malware Sites Detected)] | <p>このインタラクティブテーブルを使用すると、レイヤ4トラフィック モニタが最も頻繁にマルウェアを検出したドメインを表示できます。</p> <p>特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[ポート別にフィルタ (Filter by Port)] をクリックします。この機能を使用して、サイトまたはポートをブロックするかどうかを判断できます。</p> <p>詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[ブロックされたマルウェア接続 (Malware Connections Blocked)] の数値をクリックすると、特定のサイトに対してブロックされた各接続のリストが表示されます。このリストは、[Webトラッキング検索 (Web Tracking Search)] ページの [レイヤ4トラフィック モニタ (Layer 4 Traffic Monitor)] タブに検索結果として表示されます。リストの詳細については、<a href="#">レイヤ4トラフィック モニターによって処理されたトランザクションの検索 (650 ページ)</a> を参照してください。</p> |

#### 関連項目

[L4 トラフィック モニタ レポートのトラブルシューティング \(591 ページ\)](#)

## [SOCKS プロキシ (SOCKS Proxy)] ページ

[SOCKS プロキシ (SOCKS Proxy)] レポート ページでは、SOCKS プロキシを通じて処理されたトランザクションを、宛先およびユーザに関する情報を含めてグラフおよび表の形式で表示できます。

[SOCKS プロキシ (SOCKS Proxy)] レポートページを表示するには、[レポート (Reports)] ドロップダウンから [モニターリング (Monitoring)] > [SOCKS プロキシ (SOCKS Proxy)] を選択します。詳細については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#) を参照してください。



(注) レポートに表示される宛先は、SOCKS クライアント (通常はブラウザ) が SOCKS プロキシに送信するアドレスです。

SOCKS ポリシー設定を変更するには、『*User Guide for AsyncOS for Cisco Secure Web Appliances*』を参照してください。



表 16: [SOCKS プロキシ (SOCKS Proxy)] ページの詳細

| セクション                                                                 | 説明                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)                                     | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。                                                                                                                                                                   |
| 上位SOCKS宛先：トランザクション合計 (Top Destinations for SOCKS: Total Transactions) | SOCKS プロキシによって検出された上位の宛先をグラフ形式で表示できます。<br><br>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、 <a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。  |
| 上位SOCKSユーザ：マルウェアトランザクション (Top Users for SOCKS: Malware Transactions)  | SOCKS プロキシによって検出された上位のユーザをグラフ形式で表示できます。<br><br>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、 <a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。 |
| 宛先 (Destinations)                                                     | このインタラクティブ テーブルでは、SOCKS プロキシを通じて処理された宛先ドメインまたはIPアドレスのリストを表示できます。<br><br>特定の宛先のデータのみを含めるには、テーブルの下部のボックスにドメイン名またはIPアドレスを入力し、[ドメインまたはIPの検索 (Find Domain or IP)] をクリックします。                                                                       |
| ユーザー (Users)                                                          | このインタラクティブ テーブルでは、SOCKS プロキシを通じて処理されたユーザまたはIPアドレスのリストを表示できます。<br><br>特定のユーザのデータのみを含めるには、テーブルの下部のボックスにユーザ名またはIPアドレスを入力し、[ユーザID/クライアントIPアドレスの検索 (Find User ID / Client IP Address)] をクリックします。                                                  |

## 関連項目

[SOCKS プロキシによって処理されるトランザクションの検索 \(651 ページ\)](#)

## [URLカテゴリ (URL Categories)] ページ

[URLカテゴリ (URL Categories)] レポート ページを使用して、システム上のユーザがアクセスしているサイトの URL カテゴリを表示できます。

[URL カテゴリ (URL Categories)] レポートページを表示するには、[レポート (Reports)] ドロップダウンから [モニターリング (Monitoring)] > [URL カテゴリ (URL Categories)] を選択します。詳細については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#) を参照してください。

[URL カテゴリ (URL Categories)] ページには次の情報が表示されます。

表 17: [URLカテゴリ (URL Categories)] ページの詳細

| セクション                                                                                    | 説明                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)                                                        | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                                                 |
| 上位 URL カテゴリ : 総トランザクション数 (Top URL Categories: Total Transactions)                        | <p>サイト上でアクセスされた上位 URL カテゴリがグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p>                                                                                                                                           |
| 上位 URL カテゴリ : ブロックおよび警告されたトランザクション (Top URL Categories: Blocked and Warned Transactions) | <p>トランザクションごとに発生するブロックまたは警告アクションをトリガーした上位 URL がグラフ形式で表示されます。たとえば、ユーザがある URL にアクセスしたが、特定のポリシーが適用されているために、ブロックアクションまたは警告がトリガーされたとします。この URL は、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p> |
| [上位 YouTube カテゴリ (Top Youtube Categories)] : [トランザクションの合計数 (Total Transactions)]         | <p>サイト上でアクセスされている上位の YouTube カテゴリを表示できます (グラフ形式)。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p>                                                                                                                                |

| セクション                                                                                                            | 説明                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [上位 YouTube カテゴリ (Top Youtube Categories) ] : [ブロックされたトランザクションと警告されたトランザクション (Blocked and Warned Transactions) ] | <p>トランザクションごとに発生するブロックアクションまたは警告アクションをトリガーした上位の YouTube URL を表示できます (グラフ形式)。たとえば、ユーザが特定の YouTube URL にリダイレクトされ、特定のポリシーが適用されている場合は、ブロックアクションまたは警告がトリガーされました。この YouTube URL は、ブロックまたは警告されたトランザクションとしてこのグラフに一覧表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p> |
| [一致した URL カテゴリ (URL Categories Matched) ]                                                                        | <p>[一致した URL カテゴリ (URL Categories Matched) ] インタラクティブ テーブルには、指定した時間範囲内における URL カテゴリ別のトランザクションの処理、使用された帯域幅、各カテゴリで費やされた時間が表示されます。</p> <p>未分類の URL が多数ある場合は、<a href="#">未分類の URL の削減 (626 ページ)</a> を参照してください。</p>                                                                                                                                                                                                             |

## 未分類の URL の削減

未分類の URL の比率が 15 ～ 20 % を上回る場合は、次のオプションを検討してください。

- 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループポリシーに適用できます。これらのトランザクションは、代わりに [URL フィルタリングバイパス (URL Filtering Bypassed) ] 統計情報に含まれるようになります。これを行うには、『AsyncOS for Cisco Secure Web Appliance User Guide』でカスタム URL カテゴリについて参照してください。
- 既存またはその他のカテゴリに含めるべきサイトについては、[誤って分類された URL と未分類の URL のレポート, on page 627](#)を参照してください。

## URL カテゴリ セットの更新とレポート

Secure Web Applianceでは、一連の定義済み URL カテゴリが定期的に自動更新される場合があります。

これらの更新が行われると、古いカテゴリに関連づけられたデータが古すぎてレポートに含まれなくなるまで、古いカテゴリ名は引き続きレポートに表示されます。URL カテゴリ セットの更新後に生成されたレポートデータには新しいカテゴリが使用されるので、同じレポートに新旧両方のカテゴリが表示される場合があります。

## [URL カテゴリ (URL Categories)] ページとその他のレポート ページの併用

[URL カテゴリ (URL Categories)] ページを [アプリケーションの表示 (Application Visibility)] ページ, on page 618、[ユーザの詳細 (User Details)] ページ (Web レポート) , on page 631、および [ユーザ (Users)] ページ, on page 629 と併用して、特定のユーザーや特定のユーザーがアクセスしようとしているアプリケーションまたは Web サイトのタイプを調査できます。

たとえば、[URL カテゴリ (URL Categories)] ページ, on page 625 からは、サイトでアクセスしたすべての URL カテゴリの詳細を示す人事リソース向けの高レベルレポートを生成できます。同じページの [URL カテゴリ (URL Categories)] インタラクティブ テーブルでは、URL カテゴリ「Streaming Media」に関するさらに詳しい情報を収集できます。[ストリーミングメディア (Streaming Media)] カテゴリ リンクをクリックすると、特定の [URL カテゴリ (URL Categories)] レポート ページが表示されます。このページには、ストリーミング メディア サイトにアクセスしている上位ユーザが表示されるだけでなく ([カテゴリ別の総トランザクション上位ユーザ (Top Users by Category for Total Transactions)] セクション)、YouTube.com や QuickPlay.com などのアクセスされたドメインも表示されます ([一致したドメイン (Domains Matched)] インタラクティブ テーブル)。

この時点で、特定のユーザに関するさらに詳しい情報を得られます。たとえば、特定のユーザによる使用が突出しているの、そのユーザのアクセス先を正確に確認する必要があります。ここから、[ユーザ (Users)] インタラクティブ テーブルのユーザをクリックすることができます。このアクションにより [ユーザ (Users)] ページ, on page 629が表示され、そのユーザのトレンドを確認し、そのユーザの Web での行動を正確に把握できます。

さらに詳しい情報が必要な場合は、インタラクティブ テーブルで [完了したトランザクション (Transactions Completed)] リンクをクリックして、Web トラッキングの詳細を表示できます。これにより、[Web トラッキング (Web Tracking)] ページに Web プロキシ サービスによって処理されたトランザクションの検索, on page 645が表示され、ユーザがサイトにアクセスした日付、完全な URL、その URL で費やされた時間などについて、実際の詳細情報を確認できます。

## 誤って分類された URL と未分類の URL のレポート

誤って分類された URL と未分類の URL について、次の URL で報告できます。

<https://talosintelligence.com/tickets>。

送信内容は評価され、今後のルール更新への組み込みに活用されます。

送信された URL のステータスを確認するには、このページの [送信した URL のステータス (Status on Submitted URLs)] タブをクリックします。

## [HTTPS レポート (HTTPS Reports)] ページ

[HTTPS レポート (HTTPS Reports)] レポート ページでは、管理対象のアプライアンスの HTTP/HTTPS トラフィック サマリー (トランザクションまたは帯域幅の使用量) のすべてを集約しています。

また、管理対象のアプライアンスを通過する個々の HTTP/HTTPS Web トラフィックの場合、クライアント側接続またはサーバ側接続のいずれかに基づいてサポート対象の暗号のサマリーを確認することもできます。

[HTTPS レポート (HTTPS Reports)] レポートページを表示するには、[レポート (Reports)] ドロップダウンから[モニタリング (Monitoring)] > [HTTPS レポート (HTTPS Reports)] を選択します。詳細については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#) を参照してください。

表 18: [HTTPSレポート (HTTPS Reports)] ページの詳細

| セクション                                 | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)     | レポートの時間範囲を選択します。詳細については、 <a href="#">時間範囲の変更 (581 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                                                                                                                             |
| [Webトラフィックサマリー (Web Traffic Summary)] | <p>アプライアンスの Web トラフィック サマリーは、次のいずれかの方法で表示できます。</p> <ul style="list-style-type: none"> <li>• <b>トランザクション</b>：グラフ形式の HTTP または HTTPS Web トランザクションの数と表形式の HTTP または HTTPS Web トランザクションの割合に基づいて Web トラフィック サマリーを表示するには、ドロップダウン リストからこのオプションを選択します。</li> <li>• <b>帯域幅の使用量</b>：グラフ形式の HTTP または HTTPS Web トラフィックで消費される帯域幅の大きさと表形式の HTTP または HTTPS 帯域幅の使用量の割合に基づいて Web トラフィック サマリーを表示するには、ドロップダウン リストからこのオプションを選択します。</li> </ul>                                            |
| トレンド：Web トラフィック                       | <p>次のいずれかの方法で必要な時間範囲に基づいてアプライアンスの Web トラフィックのトレンドグラフを表示することができます。</p> <ul style="list-style-type: none"> <li>• <b>Web トラフィックトレンド</b>：トランザクションまたは帯域幅の使用量に基づいて HTTP と HTTPS Web トラフィックの累積トレンドを表示するには、ドロップダウン リストからこのオプションを選択します。</li> <li>• <b>HTTPSトレンド</b>：トランザクションまたは帯域幅の使用量に基づいて HTTPS Web トラフィックのトレンドを表示するには、ドロップダウン リストからこのオプションを選択します。</li> <li>• <b>HTTPトレンド</b>：トランザクションまたは帯域幅の使用量に基づいて HTTP Web トラフィックのトレンドを表示するには、ドロップダウン リストからこのオプションを選択します。</li> </ul> |

| セクション | 説明                                                                                                                                                                                                                                                                                           |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 暗号    | <p>暗号のサマリーは、次のいずれかの方法で表示できます。</p> <ul style="list-style-type: none"> <li>クライアント側接続別：グラフ形式で HTTP または HTTPS Web トラフィックのクライアント側で使用される暗号のサマリーを表示するには、ドロップダウンリストからこのオプションを選択します。</li> <li>サーバ側接続別：グラフ形式で HTTP または HTTPS Web トラフィックのサーバ側で使用される暗号のサマリーを表示するには、ドロップダウンリストからこのオプションを選択します。</li> </ul> |

## [ユーザ (Users)] ページ

[ユーザ (Users)] レポート ページには、各ユーザの Web レポート情報を表示できる複数のリンクが表示されます。

[ユーザー (Users)] レポートページを表示するには、[レポート (Reports)] ドロップダウンから [モニターリング (Monitoring)] > [ユーザー (Users)] を選択します。詳細については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#) を参照してください。

[ユーザ (Users)] ページでは、システム上のユーザ（1 人または複数）がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。



(注) セキュリティ管理アプライアンスがサポートできる Secure Web Appliance 上のユーザーの最大数は 500 です。

[ユーザ (Users)] ページには、システム上のユーザに関する次の情報が表示されます。

表 19: [ユーザ (Users)] ページの詳細

| セクション                             | 説明                                                                         |
|-----------------------------------|----------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト) | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。 |

| セクション                                                   | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 上位ユーザ：ブロックされたトランザクション (Top Users: Transactions Blocked) | <p>上位ユーザ (IP アドレスまたはユーザ名で表示) と、そのユーザがブロックされたトランザクションの数がグラフ形式で表示されます。レポーティングを目的として、ユーザ名または IP アドレスを認識できないようにすることができます。このページやスケジュール済みのレポートでユーザ名を認識できないようにする方法の詳細については、『<i>User Guide for AsyncOS for Cisco Content Security Management Appliances</i>』を参照してください。デフォルト設定では、すべてのユーザ名が表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p> |
| 上位ユーザ：使用帯域幅 (Top Users: Bandwidth Used)                 | <p>システム上で最も多くの帯域幅を使用している上位ユーザ (IP アドレスまたはユーザ名で表示) がグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p>                                                                                                                                                                                                                        |
| ユーザー (Users)                                            | <p>このインタラクティブテーブルを使用すると、特定のユーザ ID またはクライアント IP アドレスを検索できます。[ ユーザ (User) ] テーブル下部のテキストフィールドに特定のユーザ ID またはクライアント IP アドレスを入力し、[ ユーザ ID / クライアント IP アドレスの検索 (Find User ID / Client IP Address) ] をクリックします。IP アドレスが正確に一致していなくても結果は返されます。</p> <p>特定のユーザをクリックすると、さらに具体的な情報を得ることができます。詳細については、<a href="#">[ ユーザの詳細 (User Details) ] ページ (Web レポーティング) (631 ページ)</a> を参照してください。</p>                                                                                                                       |



(注) クライアント IP アドレスの代わりにユーザ ID を表示するには、セキュリティ管理アプライアンスを設定し、LDAP サーバからユーザ情報を取得する必要があります。



## 【ユーザの詳細 (User Details)】ページ (Web レポーティング)

【ユーザの詳細 (User Details)】ページでは、【ユーザ (Users)】レポート ページのインタラクティブ テーブルで指定したユーザに関する具体的な情報を確認できます。

【ユーザの詳細 (User Details)】ページでは、システムでの個々のユーザのアクティビティを調査できます。特に、ユーザレベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。

特定のユーザの【ユーザの詳細 (User Details)】ページを表示するには、【ユーザ (Users)】レポート ページの【ユーザ (Users)】インタラクティブ テーブルでそのユーザをクリックします。

【ユーザの詳細 (User Details)】ページには、システム上の個々のユーザに関する次の情報が表示されます。

表 20: 【ユーザの詳細 (User Details)】ページの詳細

| セクション                                                     | 説明                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 【時間範囲 (Time Range)】(ドロップダウン リスト)                          | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                        |
| URL カテゴリ: トランザクション合計 (URL Categories: Total Transactions) | <p>特定のユーザが使用している特定の URL カテゴリがグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。</p> <p>すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、<a href="#">URL カテゴリ セットの更新とレポート (598 ページ)</a> を参照してください。</p>                                                       |
| トレンド: トランザクション合計 (Trend: Total Transactions)              | <p>このトレンドグラフを使用すると、特定のユーザのすべての Web トランザクションを表示できます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。</p> <p>たとえば、1 日の特定の時刻に Web トラフィックに大きなスパイクが存在するかどうか、また、それらのスパイクがいつ発生したかが、このグラフからわかります。【時間範囲 (Time Range)】ドロップダウン リストを使用すると、このグラフを拡張し、このユーザが Web を閲覧していた時間を表示するきめ細かさを増減できます。</p> |



| セクション                                   | 説明                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [一致したURLカテゴリ (URL Categories Matched) ] | <p>[一致したURLカテゴリ (URL Categories Matched) ] インタラクティブ テーブルは、完了したトランザクションとブロックされたトランザクションの両方について、一致したカテゴリが表示されます。</p> <p>テーブル下部のテキストフィールドに入力して[URLカテゴリの検索 (Find URL Category) ]をクリックすると、特定の URL カテゴリを検索できます。カテゴリは正確に一致している必要はありません。</p> <p>すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、<a href="#">URL カテゴリ セットの更新とレポート (598 ページ)</a> を参照してください。</p> |
| [一致したドメイン (Domains Matched) ]           | <p>[一致したドメイン (Domains Matched) ] インタラクティブ テーブルは、ユーザがアクセスしたドメインまたは IP アドレスを示します。また、ユーザがこれらのカテゴリで費やした時間、およびカラム ビューで設定したその他のさまざまな情報も参照できます。</p> <p>テーブル下部のテキストフィールドに入力して[ドメインまたはIPの検索 (Find Domain or IP) ]をクリックすると、特定のドメインまたは IP アドレスを検索できます。ドメインまたは IP アドレスは正確に一致している必要はありません。</p>                                                                                  |
| [一致したアプリケーション (Applications Matched) ]  | <p>[一致したアプリケーション (Applications Matched) ] インタラクティブ テーブルには、特定のユーザが使用しているアプリケーションが表示されます。たとえば、Flash ビデオを多用するサイトにユーザがアクセスしている場合は、[アプリケーション (Application) ] 列にそのアプリケーション タイプが表示されます。</p> <p>テーブル下部のテキスト フィールドに入力して[アプリケーションの検索 (Find Application) ]をクリックすると、特定のアプリケーション名を検索できます。アプリケーションの名前は正確に一致している必要はありません。</p>                                                     |

| セクション                                                                                  | 説明                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Advanced Malware Protection で検出された脅威 (Advanced Malware Protection Threats Detected) ] | <p>[セキュアエンドポイントで検出された脅威 (Advanced Malware Protection Threats Detected) ] インタラクティブテーブルには、Advanced Malware Protectionエンジンによって検出されたマルウェア脅威ファイルが表示されます。</p> <p>テーブル下部のテキストフィールドに入力して[マルウェア脅威ファイルSHA 256の検索 (Find malware Threat File SHA 256) ]をクリックすると、マルウェア脅威ファイルの特定の SHA 値に関するデータを検索できます。アプリケーションの名前は正確に一致している必要はありません。</p> |
| [検出されたマルウェア脅威 (Malware Threats Detected) ]                                             | <p>[検出されたマルウェア脅威 (Malware Threats Detected) ] インタラクティブテーブルには、特定のユーザによってトリガーされた上位のマルウェア脅威が表示されます。</p> <p>テーブル下部のテキストフィールドに入力して[マルウェア脅威の検索 (Find Malware Threat) ]をクリックすると、特定のマルウェア脅威名に関するデータを検索できます。マルウェア脅威の名前は正確に一致している必要はありません。</p>                                                                                       |
| [一致したポリシー (Policies Matched) ]                                                         | <p>[一致したポリシー (Policies Matched) ] インタラクティブテーブルには、Web へのアクセス時にこのユーザに適用されたポリシー グループが表示されます。</p> <p>テーブル下部のテキストフィールドに入力して[ポリシー検索 (Find Policy) ]をクリックすると、特定のポリシー名を検索できます。ポリシーの名前は正確に一致している必要はありません。</p>                                                                                                                       |



- (注) [クライアントマルウェアリスクの詳細 (Client Malware Risk Details) ] テーブルのクライアント レポートでは、ユーザ名の末尾にアスタリスク (\*) が付いていることがあります。たとえば、クライアント レポートに「jsmith」と「jsmith\*」の両方のエントリが表示される場合があります。アスタリスク (\*) が付いているユーザ名は、ユーザの指定したユーザ名が認証サーバで確認されていないことを示しています。この状況は、認証サーバがその時点で使用できず、かつ認証サービスを使用できないときもトラフィックを許可するようにアプライアンスが設定されている場合に発生します。

## [Webサイト (Web Sites)] ページ

[Webサイト (Web Sites)] レポートページは、管理対象のアプライアンスで発生しているアクティビティ全体を集約したものです。このレポートページを使用すると、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタすることができます。

[Web サイト (Web Sites)] レポートページを表示するには、[レポート (Reports)] ドロップダウンから [モニターリング (Monitoring)] > [Web サイト (Web Sites)] を選択します。詳細については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#) を参照してください。

[Webサイト (Web Sites)] ページには次の情報が表示されます。

表 21 : [Webサイト (Web Sites)] ページの詳細

| セクション                                                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト)                          | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                                                                     |
| 上位ドメイン：トランザクション合計 (Top Domains: Total Transactions)        | <p>Web サイト上でアクセスされた上位のドメインがグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p>                                                                                                                                                              |
| 上位ドメイン：ブロックされたトランザクション (Top Domains: Transactions Blocked) | <p>トランザクションごとに発生するブロックアクションをトリガーした上位ドメインが、グラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p> <p>たとえば、ユーザがあるドメインにアクセスしたが、特定のポリシーが適用されていたために、ブロックアクションがトリガーされたとします。このドメインはブロックされたトランザクションとしてこのグラフに追加され、ブロックアクションをトリガーしたドメイン サイトが表示されます。</p> |

| セクション                         | 説明                                                                                                                                                                                                                                                                                              |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [一致したドメイン (Domains Matched) ] | <p>このインタラクティブ テーブルでは、Web サイト上でアクセスされたドメインを検索できます。特定のドメインをクリックすると、より詳細な情報を得ることができます。[Web トラッキング (Web Tracking) ] ページに [プロキシサービス (Proxy Services) ] タブが表示され、トラッキング情報と、特定のドメインがブロックされた理由を確認できます。</p> <p>特定のドメインをクリックすると、そのドメインの上位ユーザ、そのドメインでの上位トランザクション、一致した URL カテゴリ、および検出されたマルウェアの脅威が表示されます。</p> |

## Advanced Malware Protection ページ

Advanced Malware Protection は、次によりゼロデイやファイルベースの標的型の脅威から保護します。

- 既知のファイルのレピュテーションを取得する。
- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を評価し、脅威と判定されているファイルがネットワークに侵入するとユーザに通知する。

ファイル レピュテーション フィルタリングとファイル分析の詳細については、ユーザーガイドまたは *Secure Web Appliance* の AsyncOS のオンラインヘルプを参照してください。

Advanced Malware Protection レポートページには、次のレポートビューが表示されます。

- [\[セキュアエンドポイントサマリー \(Advanced Malware Protection Summary\) \] ページ](#)
- [Advanced Malware Protection – \[ファイル分析 \(File Analysis\) \] ページ](#)

Advanced Malware Protection レポートページを表示するには、[レポート (Reports) ] ドロップダウンから [モニターリング (Monitoring) ] > Advanced Malware Protection を選択します。詳細については、「[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#)」を参照してください。

### Advanced Malware Protection – [セキュアエンドポイントサマリー (AMP Summary) ] ページ

[セキュアエンドポイント (Advanced Malware Protection) ] レポートページの [セキュアエンドポイントサマリー (AMP Summary) ] セクションには、ファイル レピュテーション サービスによって識別された、ファイルベースの脅威が表示されます。

各 SHA にアクセスしようとしたユーザー、およびその SHA-256 に関連付けられたファイル名を表示するには、テーブルの SHA-256 リンクをクリックします。

[マルウェア脅威ファイル (Malware Threat File) ] インタラクティブ テーブルのリンクをクリックすると、レポートに対して選択された時間範囲に関係なく、設定可能な最大時間範囲内で検

出されたそのファイルのすべてのインスタンスが [Web トラッキング (Web Tracking)] に表示されます。

圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御 (Advanced Malware Protection)] レポートに含まれます。

[セキュアエンドポイント (Advanced Malware Protection)] ページの [セキュアエンドポイント サマリー (AMP Summary)] セクションには、次の情報を表示できます。

- Advanced Malware Protection エンジンのファイル レピュテーション サービスによって識別されたファイルの概要 (グラフ形式)。
- 上位のマルウェア脅威ファイル (グラフ形式)。
- ファイル タイプに基づいた上位の脅威ファイル (グラフ形式)。
- 選択した時間範囲のすべてのマルウェア脅威ファイルに関するトレンド グラフ。
- 上位のマルウェア脅威ファイルを一覧表示する [マルウェア脅威ファイル (Malware Threat Files)] インタラクティブ テーブル。
- このアプライアンスで処理され、トランザクションの処理後に判定が変わったファイルを一覧表示する [レトロスペクティブ判定変更 (Retrospective Verdict Change)] インタラクティブ テーブルを含むファイル。この状況の詳細については、お使いの Secure Web Appliance のマニュアルを参照してください。

1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。

同一ファイルの複数の Secure Web Appliance で判定のアップデートが異なる場合は、最も新しいタイムスタンプの結果が表示されます。

SHA-256 リンクをクリックすると、レポート用に選択された時間範囲に関係なく使用可能な最大時間範囲内にこの SHA-256 が含まれた、すべてのトランザクションの Web トラッキング結果が表示されます。

## Advanced Malware Protection – [ファイル分析 (File Analysis)] ページ

[セキュアエンドポイント (Advanced Malware Protection)] レポートページの [ファイル分析 (File Analysis)] セクションには、分析のために送信された各ファイルについて、時刻と判定 (または中間判定) が表示されます。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。

オンプレミスの AMP Malware Analytics アプライアンスでの導入の場合: AMP Malware Analytics アプライアンスで許可リストに含まれているファイルは、「クリーン」として表示されます。許可リストについては、AMP Malware Analytics のオンラインヘルプを参照してください。

ドリルダウンすると、各ファイルの脅威の特性およびスコアを含む詳細な分析結果が表示されます。

また、分析を実行したサーバーで SHA に関する追加の詳細を直接表示するには、SHA を検索するか、またはファイル分析の詳細ページ下部にある AMP Malware Analytics リンクをクリックします。

圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析 (File Analysis)] レポートに含まれます。

[セキュアエンドポイント (Advanced Malware Protection)] レポートページの [ファイル分析 (File Analysis)] セクションを使用すると、次の情報を表示できます。

- Advanced Malware Protection エンジンのファイル分析サービスによってファイル分析のためにアップロードされたファイルの数。
- ファイル分析要求が完了しているファイルのリスト。
- ファイル分析要求の処理待ちとなっているファイルのリスト。

## [マルウェア対策 (Anti-Malware)] ページ

[マルウェア対策 (Anti-Malware)] レポートページはセキュリティ関連のレポートページであり、イネーブルなスキャンエンジン (Webroot、Sophos、McAfee、または Adaptive Scanning) によるスキャン結果が反映されます。

[マルウェア対策 (Anti-Malware)] レポートページを表示するには、[レポート (Reports)] ドロップダウンから [モニターリング (Monitoring)] > [マルウェア対策 (Anti-Malware)] を選択します。詳細については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#) を参照してください。

このページを使用して、Web ベースのマルウェアの脅威を特定およびモニタすることができます。



(注) L4 トラフィック モニタリングで検出されたマルウェアのデータを表示するには、次を参照してください。[レイヤ4トラフィックモニタ \(Layer 4 Traffic Monitor\)\] ページ \(620 ページ\)](#)

[マルウェア対策 (Anti-Malware)] ページには次の情報が表示されます。

表 22: [マルウェア対策 (Anti-Malware)] ページの詳細

| セクション                             | 説明                                                                         |
|-----------------------------------|----------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウン リスト) | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。 |

| セクション                                | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 上位マルウェアカテゴリ (Top Malware Categories) | <p>特定のカテゴリタイプによって検出された上位のマルウェアカテゴリをグラフ形式で表示できます。有効なマルウェアカテゴリの詳細については、<a href="#">マルウェアのカテゴリについて (639 ページ)</a> を参照してください。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p>                                                                                                                           |
| 上位マルウェア脅威 (Top Malware Threats)      | <p>上位のマルウェア脅威をグラフ形式で表示できます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p>                                                                                                                                                                                                                        |
| [マルウェアカテゴリ (Malware Categories) ]    | <p>[マルウェアカテゴリ (Malware Categories) ] インタラクティブ テーブルには、[上位マルウェアカテゴリ (Top Malware Categories) ] チャートに表示されている個々のマルウェアカテゴリに関する詳細情報が表示されます。</p> <p>[マルウェアカテゴリ (Malware Categories) ] インタラクティブ テーブル内のリンクをクリックすると、個々のマルウェアカテゴリおよびネットワークでの検出場所に関するさらに詳しい情報が表示されます。</p> <p>例外：このテーブルの [アウトブレイクヒューリスティック (Outbreak Heuristics) ] リンクを使用すると、そのカテゴリでいつトランザクションが発生したかを示すチャートが表示されます。</p> <p>有効なマルウェアカテゴリの詳細については、<a href="#">マルウェアのカテゴリについて (639 ページ)</a> を参照してください。</p> |
| [マルウェア脅威 (Malware Threats) ]         | <p>[マルウェアの脅威 (Malware Threats) ] インタラクティブ テーブルには、[上位マルウェア脅威 (Top Malware Threats) ] セクションに表示されている個々のマルウェアの脅威に関する詳細情報が表示されます。</p> <p>「アウトブレイク (Outbreak) 」のラベルと番号が付いている脅威は、他のスキャンエンジンとは別に、Adaptive Scanning 機能によって特定された脅威です。</p>                                                                                                                                                                                                                            |

## [マルウェア カテゴリ (Malware Category)] レポート ページ

## Procedure

**ステップ 1** [レポート (Reports)] > [マルウェア対策 (Anti-Malware)] を選択します。

**ステップ 2** [マルウェア カテゴリ (Malware Categories)] インタラクティブテーブルで、[マルウェア カテゴリ (Malware Category)] カラム内のカテゴリをクリックします。

## [マルウェアの脅威 (Malware Threat)] レポート

[マルウェア脅威 (Malware Threats)] レポート ページには、特定の脅威にさらされているクライアント、および感染した可能性があるクライアントのリストが表示され、[クライアントの詳細 (Client Detail)] ページへのリンクがあります。レポート上部のトレンドグラフには、指定した時間範囲内で脅威に関してモニターされたトランザクションおよびブロックされたトランザクションが表示されます。下部のテーブルには、指定した時間範囲内で脅威に関してモニターされたトランザクションおよびブロックされたトランザクションの実際の数が表示されます。

このレポートを表示するには、[マルウェア対策 (Anti-Malware)] レポート ページの [マルウェアのカテゴリ (Malware Category)] 列でカテゴリをクリックします。

詳細については、テーブルの下に [サポートポータルマルウェア詳細 (Support Portal Malware Details)] リンクをクリックしてください。

## マルウェアのカテゴリについて

Secure Web Appliance は、次のタイプのマルウェアをブロックできます。

| マルウェアのタイプ        | 説明                                                                                                                                                                                                                                                 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アドウェア            | アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。アドウェアアプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。 |
| ブラウザ ヘルパー オブジェクト | ブラウザヘルパーオブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザプラグインです。                                                                                                                                                                                |
| 商用システム モニタ       | 商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。                                                                                                                                                                                       |



| マルウェアのタイプ            | 説明                                                                                                                                                                                       |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ダイヤラ                 | ダイヤラは、モデムあるいは別のタイプのインターネットアクセスを利用して、ユーザの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。                                                                                                |
| 一般的なスパイウェア           | スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。                                                                                                                              |
| ハイジャッカー              | ハイジャッカーは、ユーザの完全で有効な承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。                                                                                         |
| その他のマルウェア            | このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。                                                                                                                                         |
| アウトブレイク<br>ヒューリスティック | このカテゴリは、他のアンチマルウェア エンジンとは別に、 <b>Adaptive Scanning</b> によって検出されたマルウェアを示しています。                                                                                                             |
| フィッシング URL           | フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャルエンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。                                              |
| PUA                  | 望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。                                                                                                                                   |
| システム モニタ             | システム モニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。<br><br>公然と、または密かに、システムプロセスやユーザアクションを記録する。<br><br>これらの記録を後で取得して確認できるようにする。                                                                      |
| トロイのダウンロード           | トロイのダウンロードは、インストール後にリモートホスト/サイトにアクセスして、リモートホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンロードはリモートホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。 |
| トロイの木馬               | トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。                                                                                                                              |

| マルウェアのタイプ | 説明                                                                                                                     |
|-----------|------------------------------------------------------------------------------------------------------------------------|
| トロイのフィッシャ | トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークションサイト、あるいはオンライン支払サイトに関係するユーザ名とパスワードを探します。 |
| ウイルス      | ウイルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行されるプログラムまたはコードです。                                                            |
| ワーム       | ワームは、コンピュータ ネットワーク上で自己を複製し、通常は悪質なアクションを実行するプログラムまたはアルゴリズムです。                                                           |

## [クライアントマルウェアリスク (Client Malware Risks)] ページ

[レポート (Reporting)] > [クライアントマルウェアリスク (Client Malware Risk)] ページは、クライアントマルウェアリスクアクティビティをモニターするために使用できるセキュリティ関連のレポートページです。[クライアントマルウェアリスク (Client Malware Risk)] ページには、L4 トラフィックモニター (L4TM) によって特定された、頻度の高いマルウェア接続に参与しているクライアント IP アドレスが表示されます。

表 23: [クライアントマルウェアリスク (Client Malware Risks)] ページの詳細情報

| セクション                                                                            | 説明                                                                                                                                                                                     |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range)] (ドロップダウンリスト)                                                 | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。                                                                                                             |
| [Webプロキシ: モニタまたはブロックされた上位クライアント (Web Proxy: Top Clients Monitored or Blocked)]   | このチャートには、マルウェアのリスクが発生した上位 10 人のユーザが表示されます。                                                                                                                                             |
| [L4 トラフィックモニター: 検出されたマルウェア接続 (L4 Traffic Monitor: Malware Connections Detected)] | このチャートには、組織内で最も頻繁にマルウェアサイトに接続しているコンピュータの IP アドレスが表示されます。                                                                                                                               |
| [Webプロキシ: クライアントマルウェアリスク (Web Proxy: Client Malware Risk)]                       | [Webプロキシ: クライアントマルウェアリスク (Web Proxy: Client Malware Risk)] インタラクティブテーブルには、[Webプロキシ: マルウェアリスク別上位クライアント (Web Proxy: Top Clients by Malware Risk)] セクションに表示されている個々のクライアントに関する詳細情報が表示されます。 |
| L4 トラフィックモニター: マルウェアリスク別クライアント (L4 Traffic Monitor: Clients by Malware Risk)     | [L4 トラフィックモニター: マルウェアリスク別クライアント (L4 Traffic Monitor: Clients by Malware Risk)] インタラクティブテーブルには、組織内でマルウェアサイトに頻繁にアクセスしているコンピュータの IP アドレスが表示されます。                                          |

## [Web レピュテーション フィルタ (Web Reputation Filters) ] ページ

[Web レピュテーション フィルタ (Web Reputation Filters) ] レポート ページでは、指定した時間範囲内のトランザクションに対する Web レピュテーション フィルタ (ユーザが設定) の結果を確認できます。

[Web レピュテーション フィルタ (Web Reputation Filters) ] レポート ページを表示するには、[レポート (Reports) ] ドロップダウンから、[モニターリング (Monitoring) ] > [Web レピュテーション フィルタ (Web Reputation Filters) ] を選択します。詳細については、[新しい Web インターフェイスでのインタラクティブ レポート ページの使用 \(587 ページ\)](#) を参照してください。

### Web レピュテーション フィルタとは

Web レピュテーション フィルタは、Web サーバの動作を分析し、URL ベースのマルウェアが含まれている可能性を判断するためのレピュテーション スコアを URL に割り当てます。この機能は、エンドユーザのプライバシーや企業の機密情報を危険にさらす URL ベースのマルウェアを防ぐために役立ちます。Secure Web Appliance は、URL レピュテーション スコアを使用して、疑わしいアクティビティを特定するとともに、マルウェア攻撃を未然に防ぎます。Web レピュテーション フィルタは、アクセス ポリシーと復号ポリシーの両方と組み合わせて使用できます。

Web レピュテーション フィルタでは、統計データを使用してインターネット ドメインの信頼性が評価され、URL のレピュテーション にスコアが付けられます。特定のドメインが登録されていた期間、Web サイトがホストされている場所、Web サーバがダイナミック IP アドレスを使用しているかどうかなどのデータを使用して、特定の URL の信頼性が判定されます。

Web レピュテーション の計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定されます。マルウェアが存在する可能性の累計が、-10 ~ +10 の Web レピュテーション スコアにマッピングされます (+10 がマルウェアを含む可能性が最も低い)。

パラメータには、たとえば以下のものがあります。

- URL 分類データ
- ダウンロード可能なコードの存在
- 長く不明瞭なエンドユーザ ライセンス契約書 (EULA) の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク オーナー情報
- URL の履歴
- URL の経過時間
- ブロック リストに存在
- 許可リストに存在
- 人気のあるドメインの URL タイプミス

- ドメインのレジストラ情報
- IP アドレス情報

Web レピュテーションフィルタの詳細については、『*User Guide for AsyncOS for Secure Web Appliances*』の「Web Reputation Filters」を参照してください。

[Webレピュテーションフィルタ (Web Reputation Filters) ] ページには次の情報が表示されます。

表 24: [Webレピュテーションフィルタ (Web Reputation Filters) ] ページの詳細

| セクション                                                                             | 説明                                                                                                              |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| [時間範囲 (Time Range) ] (ドロップダウン リスト)                                                | レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。                                      |
| [Webレピュテーションアクション(トレンド) (Web Reputation Actions (Trend)) ]                        | 指定した時間における Web レピュテーション アクションの合計数をグラフ形式で表示できます。このセクションでは、時間の経過に伴う Web レピュテーション アクションの潜在的なトレンドを確認できます。           |
| [Webレピュテーションアクション(ボリューム) (Web Reputation Actions (Volume)) ]                      | Web レピュテーション アクションのボリュームをトランザクション数の比率で表示できます。                                                                   |
| [WBRsによってブロックされるWebレピュテーションの脅威タイプ (Web Reputation Threat Types Blocked by WBRs) ] | Web レピュテーションフィルタリングによってブロックされたトランザクションで発生した脅威のタイプをグラフ形式で表示できます。<br><br>(注)<br>WBRs では、常に、脅威のタイプを識別できるわけではありません。 |

| セクション                                                                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [他のトランザクションで脅威タイプが検知されました<br>(Threat Types Detected in Other Transactions) ] | <p>Web レピュテーションフィルタリングによってブロックされなかったトランザクションで発生した脅威のタイプをグラフ形式で表示できます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (644 ページ)</a> を参照してください。</p> <p>これらの脅威がブロックされなかった理由には、次のようなものがあります。</p> <ul style="list-style-type: none"> <li>すべての脅威に、ブロッキングのしきい値を満たすスコアがあるわけではありません。ただし、アプライアンスのその他の機能は、これらの脅威を検出する可能性があります。</li> <li>ポリシーが、脅威を許可するよう設定されている可能性があります。</li> </ul> <p>(注)<br/>WBRs では、常に、脅威のタイプを識別できるわけではありません。</p> |
| Web レピュテーションアクション (スコアによる内訳) (Web Reputation Actions (Breakdown by Score))   | Adaptive Scanning がイネーブルでない場合、このインタラクティブ テーブルには各アクションの Web レピュテーションスコアの内訳が表示されます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 一致した脅威カテゴリ                                                                   | 一致した脅威カテゴリを表示できます (グラフ形式)。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### Web レピュテーション設定の調整

指定済みの Web レピュテーションの設定は、レポート結果に基づいて調整することができます。たとえば、しきい値スコアを調整したり、Adaptive Scanning をイネーブルまたはディセーブルにしたりできます。Web レピュテーション設定の詳細については、『*User Guide for AsyncOS for Cisco Secure Web Appliances*』を参照してください。

## (Web レポートのみ) チャート化するデータの選択

各 Web レポーティング ページのデフォルト チャートには、一般に参照されるデータが表示されますが、代わりに異なるデータをチャート化するように選択できます。ページに複数のチャートがある場合は、チャートごとに変更できます。

通常、チャートのオプションは、レポート内のテーブルのカラムと同じです。ただし、チャート化できない列もあります。

チャートには、関連付けられたテーブルに表示するように選択した項目（行）数に関係なく、テーブルの列の使用可能なすべてのデータが反映されます。

## 手順

**ステップ 1** 特定のチャートで  をクリックします。

**ステップ 2** 表示する必要があるデータを選択します。チャートのプレビューは、選択したオプションに従って表示されます。

**ステップ 3** [適用 (Apply)] をクリックします。

## 新しい Web インターフェイスでの Web トラッキング

[Web トラッキング検索 (Web Tracking Search)] ページでは、個々のトランザクションまたは疑わしいトランザクションのパターンを検索し、その詳細を表示することができます。展開で使用するサービスに基づき、関連するタブで検索を行います。

- [Web プロキシ サービスによって処理されたトランザクションの検索 \(645 ページ\)](#)
- [レイヤ 4 トラフィック モニターによって処理されたトランザクションの検索 \(650 ページ\)](#)
- [SOCKS プロキシによって処理されるトランザクションの検索 \(651 ページ\)](#)
- [Web トラッキングの検索結果の使用 \(651 ページ\)](#)
- [Web トラッキング検索結果のトランザクションの詳細の表示 \(652 ページ\)](#)

Web プロキシと レイヤ 4 トラフィック モニターの違いについては、『*User Guide for AsyncOS for Cisco Secure Web Appliances*』の「Understanding How the Secure Web Appliance Works」セクションを参照してください。

## Web プロキシ サービスによって処理されたトランザクションの検索

[Web トラッキング検索 (Web Tracking Search)] ページの [プロキシサービス (Proxy Services)] タブを使用して、個々のセキュリティ コンポーネント、およびアクセプタブル ユース適用コンポーネントから収集された Web トラッキング データを検索できます。このデータには、レイヤ 4 トラフィック モニタリング データまたは SOCKS プロキシによって処理されたトランザクションは含まれません。

このデータを使用して、次の役割を補助することができます。

- **人事または法律マネージャ。** 所定の期間内の従業員に関するレポートを調査します。

たとえば、[プロキシサービス (Proxy Services)] タブを使用して、ユーザがアクセスしている特定の URL について、ユーザがアクセスした時刻や、それが許可された URL であるかどうか、といった情報を取得できます。

- **ネットワークセキュリティ管理者。** 会社のネットワークが従業員のスマートフォンを介してマルウェアの脅威にさらされていないかどうかを調査します。

所定の期間内に記録されたトランザクション（ブロック、モニタリング、および警告されたトランザクション、完了したトランザクションなど）の検索結果を表示できます。URL カテゴリ、マルウェアの脅威、アプリケーションなど、複数の条件を使用してデータ結果をフィルタリングすることもできます。



(注) Web プロキシは、「OTHER-NONE」以外の ACL デシジョン タグを含むトランザクションのみレポートします。

[プロキシサービス (Proxy Services)] タブと他の Web レポート ページの併用例については、を参照してください。

## 手順

- ステップ 1** セキュリティ管理アプライアンスで、ドロップダウン リストから [Web] を選択します。
- ステップ 2** [URL カテゴリ (URL Categories)] ページとその他のレポート ページの併用 (627 ページ) [トラッキング (Tracking)] > [プロキシサービス (Proxy Services)] を選択します。
- ステップ 3** 検索オプションとフィルタリング オプションをすべて表示するには、[詳細設定 (Advanced)] をクリックします。
- ステップ 4** 検索条件を入力します。

表 25: [プロキシサービス (Proxy Services)] タブの Web トラッキング検索条件

| オプション                    | 説明                                                                                                                                            |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| デフォルトの検索条件               |                                                                                                                                               |
| 時間範囲 (Time Range)        | レポート対象の時間範囲を選択します。セキュリティ管理アプライアンスで利用できる時間範囲については、 <a href="#">レポートの時間範囲の選択 (582 ページ)</a> を参照してください。                                           |
| ユーザ/クライアント IPv4 または IPv6 | レポートに表示される認証ユーザ名、または追跡対象のクライアント IP アドレスを任意で入力します。IP 範囲を 172.16.0.0/16 のような CIDR 形式で入力することもできます。<br><br>このフィールドを空にしておくと、すべてのユーザに関する検索結果が返されます。 |

| オプション                           | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web サイト (Website)               | 追跡対象の Web サイトを任意で入力します。このフィールドを空にしておくと、すべての Web サイトに関する検索結果が返されます。                                                                                                                                                                                                                                                                                                                                                                                                                             |
| トランザクション タイプ (Transaction Type) | 追跡対象のトランザクションのタイプを [すべてのトランザクション (All Transactions) ]、[完了 (Completed) ]、[ブロックされた (Blocked) ]、[モニタ対象 (Monitored) ]、または [警告対象 (Warned) ] から選択します。                                                                                                                                                                                                                                                                                                                                                |
| 高度な検索条件                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| URL カテゴリ                        | <p>URL カテゴリでフィルタリングするには、[URLカテゴリによるフィルタ (Filter by URL Category) ] を選択し、フィルタリング対象とするカスタムまたは定義済み URL カテゴリの先頭文字を入力します。表示されたリストからカテゴリを選択します。</p> <p>ドロップダウン リストに表示されるエンジン名に関係なく、カテゴリ名に一致する最近のトランザクションがすべて含まれます。</p>                                                                                                                                                                                                                                                                               |
| マルウェアの脅威                        | <p>特定のマルウェアの脅威でフィルタリングするには、[マルウェア脅威によるフィルタ (Filter by Malware Threat) ] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。</p> <p>マルウェアカテゴリでフィルタリングするには、[マルウェアカテゴリによるフィルタ (Filter by Malware Category) ] を選択し、フィルタリングに使用するマルウェアカテゴリを選択します。説明については、<a href="#">マルウェアのカテゴリについて (639 ページ)</a> を参照してください。</p>                                                                                                                                                                                                       |
| アプリケーション                        | <p>アプリケーションでフィルタ処理するには、[アプリケーション (Application) ] を選択し、フィルタ処理するアプリケーションを選択します。</p> <p>アプリケーションタイプでフィルタ処理するには、[アプリケーションタイプ (Application Type) ] を選択し、フィルタ処理するアプリケーションタイプを選択します。</p>                                                                                                                                                                                                                                                                                                              |
| WBRs                            | <p>[WBRs] セクションでは、Web ベースのレピュテーション スコアによるフィルタリングと、特定の Web レピュテーションの脅威によるフィルタリングが可能です。</p> <ul style="list-style-type: none"> <li>Web レピュテーションスコアでフィルタリングするには、[スコア範囲 (Score Range) ] を選択し、フィルタリングに使用する上限値と下限値を選択します。あるいは、[スコアなし (No Score) ] を選択すると、スコアがない Web サイトをフィルタリングできます。</li> <li>Web レピュテーションの脅威でフィルタリングするには、[レピュテーション脅威によるフィルタ (Filter by Reputation Threat) ] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。</li> </ul> <p>WBRs スコアの詳細は、『IronPort AsyncOS for Web User Guide』を参照してください。</p> |



| オプション                                                       | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 脅威カテゴリ                                                      | <p>特定の脅威カテゴリでフィルタ処理するには、[脅威カテゴリ (Threat Category)] セクションを展開し、必要な脅威カテゴリを選択します。</p> <p>使用可能なすべての脅威カテゴリを選択するには、[すべて選択 (Select All)] をクリックします。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| YouTube カテゴリ                                                | <p>特定の YouTube カテゴリでフィルタ処理するには、[YouTube カテゴリ (YouTube Category)] セクションを展開し、表示する YouTube カテゴリを選択します。</p> <p>使用可能なすべての YouTube カテゴリを選択するには、[すべて選択 (Select All)] をクリックします。アクティブなカテゴリと非アクティブなカテゴリ別にフィルタ処理することもできます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ポリシー                                                        | <p>ポリシーグループでフィルタ処理するには、[ポリシー (Policy)] を選択し、フィルタ処理するポリシーグループ名を入力します。</p> <p>このポリシーが Secure Web Appliance で宣言済みであることを確認してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| AnyConnect セキュア<br>モビリティ<br>(AnyConnect Secure<br>Mobility) | <p>リモートアクセスまたはローカルアクセスでフィルタ処理するには、[ユーザーの場所 (User Location)] を選択し、アクセスタイプを選択します。すべてのアクセス タイプを含めるには、[フィルタを無効にする (Disable Filter)] を選択します (旧リリースでは、このオプションは Mobile User Security と呼ばれていました。)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Advanced Malware<br>Protection                              | <p>ファイルレピュテーションサービスで識別されたファイルベースの脅威をフィルタ処理するには、[ファイル名 (Filename)] ボックスにファイル名を入力します。</p> <p>SHA-256 ハッシュを使用してファイルをフィルタ処理するには、SHA-256 ハッシュ値を [ファイル SHA-256 (File SHA-256)] ボックスに入力します。</p> <p>ファイル判定に基づいてファイルをフィルタ処理するには、[セキュアエンドポイントファイル判定 (AMP File Verdict)] を選択し、判定タイプを選択します。使用可能なファイル判定タイプは、[クリーン (Clean)]、[悪意のある (Malicious)]、[不明 (Unknown)]、[スキャン不可 (UnScannable)]、および [低リスク (Lowrisk)] です。</p> <p>判定タイプの [悪意のある (Malicious)] には、次の 3 つのサブカテゴリがあります。</p> <ul style="list-style-type: none"> <li>• [マルウェア (Malware)] : [カスタム検出 (Custom Detection)] や [カスタムしきい値 (Custom Threshold)] 以外の理由によりブロックされたファイル。</li> <li>• [カスタム検出 (Custom Detection)] : AMP for Endpoints コンソールから受信したブロックリストに登録されているファイル SHA の割合。</li> <li>• [カスタムしきい値 (Custom Threshold)] : AMP の設定中にしきい値設定が原因でブロックされたファイル。</li> </ul> |

| オプション     | 説明                                                                                                                                                                                |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ユーザ リクエスト | <p>ユーザによって実際に開始されたトランザクションでフィルタリングするには、[Web ユーザが要求したトランザクションによるフィルタ (Filter by Web User-Requested Transactions)] を選択します。</p> <p>注：このフィルタを有効にすると、検索結果には「最良の推測」 トランザクションが含まれます。</p> |

## マルウェアのカテゴリについて

Secure Web Appliance は、次のタイプのマルウェアをブロックできます。

| マルウェアのタイプ         | 説明                                                                                                                                                                                                                                                 |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アドウェア             | アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。アドウェアアプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。 |
| ブラウザ ヘルパー オブジェクト  | ブラウザヘルパー オブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザプラグインです。                                                                                                                                                                               |
| 商用システム モニタ        | 商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。                                                                                                                                                                                       |
| ダイヤラ              | ダイヤラは、モデムあるいは別のタイプのインターネットアクセスを利用して、ユーザの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。                                                                                                                                                          |
| 一般的なスパイウェア        | スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。                                                                                                                                                                                        |
| ハイジャッカー           | ハイジャッカーは、ユーザの完全で有効な承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。                                                                                                                                                   |
| その他のマルウェア         | このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。                                                                                                                                                                                                   |
| アウトブレイク ヒューリスティック | このカテゴリは、他のアンチマルウェア エンジンとは別に、Adaptive Scanning によって検出されたマルウェアを示しています。                                                                                                                                                                               |

| マルウェアのタイプ  | 説明                                                                                                                                                                                       |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フィッシング URL | フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャルエンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンラインID盗難の一種です。                                                |
| PUA        | 望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。                                                                                                                                   |
| システム モニタ   | システム モニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。<br><br>公然と、または密かに、システムプロセスやユーザアクションを記録する。<br><br>これらの記録を後で取得して確認できるようにする。                                                                      |
| トロイのダウンロード | トロイのダウンロードは、インストール後にリモートホスト/サイトにアクセスして、リモートホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンロードはリモートホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。 |
| トロイの木馬     | トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。                                                                                                                              |
| トロイのフィッシャ  | トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークションサイト、あるいはオンライン支払サイトに関するユーザ名とパスワードを探します。                                                                    |
| ウイルス       | ウイルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行されるプログラムまたはコードです。                                                                                                                              |
| ワーム        | ワームは、コンピュータ ネットワーク上で自己を複製し、通常は悪質なアクションを実行するプログラムまたはアルゴリズムです。                                                                                                                             |

## レイヤ4トラフィック モニターによって処理されたトランザクションの検索

[Webトラッキング検索 (Web Tracking Search)] ページの [レイヤ4トラフィックモニター (Layer 4 Traffic Monitor)] タブには、マルウェア サイトおよびポートへの接続に関する詳細情報が表示されます。マルウェア サイトへの接続は、次のタイプの情報によって検索できます。

- 時間範囲
- トランザクションを開始したマシンの IP アドレス (IPv4 または IPv6)

- 接続先 Web サイトのドメインまたは IP アドレス (IPv4 または IPv6)
- ポート (Port)
- 組織内のコンピュータに関連付けられた IP アドレス
- 接続タイプ

疑わしいサイトにあるホスト名、またはトランザクションを処理した Secure Web Appliance を表示するには、[送信先IPアドレス (Destination IP Address)] 列見出しの [詳細を表示 (Display Details)] リンクをクリックします。

この情報の詳細な使用方法については、[レイヤ4トラフィックモニタ \(Layer4 Traffic Monitor\) ページ \(620 ページ\)](#) を参照してください。

## SOCKS プロキシによって処理されるトランザクションの検索

ブロックまたは完了したトランザクション、トランザクションを開始したクライアントマシンの IP アドレス、および宛先ドメイン、IP アドレス、またはポートなど、さまざまな条件に一致するトランザクションを検索できます。カスタム URL カテゴリ、一致ポリシー、およびユーザロケーション (ローカルまたはリモート) により、結果をフィルタリングすることもできます。IPv4 および IPv6 アドレスがサポートされます。

### 手順

**ステップ 1** [トラッキング (Tracking)] > [SOCKS プロキシ (SOCKS Proxy)] を選択します。

**ステップ 2** 検索オプションとフィルタリング オプションをすべて表示するには、[詳細設定 (Advanced)] をクリックします。

**ステップ 3** 検索条件を入力します。

**ステップ 4** [検索 (Search)] をクリックします。

### 次のタスク

#### 関連項目

[\[SOCKS プロキシ \(SOCKS Proxy\)\] ページ \(623 ページ\)](#)

## Web トラッキングの検索結果の使用

- 詳細な Web トラッキング検索結果の表示, [on page 652](#)
- Web トラッキング検索結果について, [on page 652](#)
- Web トラッキング検索結果のトランザクションの詳細の表示, [on page 652](#)
- Web トラッキングおよびアップグレードについて, [on page 653](#)

## 詳細な Web トラッキング検索結果の表示

### Procedure

- ステップ 1** 返された結果のページをすべて確認してください。
- ステップ 2** 現在表示されている数よりも多くの結果を各ページに表示するには、[表示された項目 (Items Displayed)] メニューからオプションを選択します。
- ステップ 3** 条件に一致するトランザクションが、[表示された項目 (Items Displayed)] メニューで選択できる最大トランザクション数より多い場合は、[印刷可能なダウンロード (Printable Download)] リンクをクリックし、一致するすべてのトランザクションを含む CSV ファイルを取得すると、完全な結果を確認できます。
- この CSV ファイルには、関連トランザクションの詳細を除く、raw データ一式が含まれます。

## Web トラッキング検索結果について

デフォルトでは、結果はタイムスタンプでソートされ、最新の結果が最上部に表示されます。

検索結果に表示される情報：

- URL がアクセスされた時刻。
- ロードされたイメージ、実行された JavaScript、アクセスされたセカンダリ サイトなど、ユーザが開始したトランザクションによって発生した関連トランザクションの数。関連トランザクションの数は、列見出しの [すべての詳細を表示(Display All Details)] リンクの下各行に表示されます。
- 処理（トランザクションの結果。該当する場合、トランザクションがブロックまたはモニタされた理由、あるいは警告が発行された理由が表示されます）。

## Web トラッキング検索結果のトランザクションの詳細の表示

| 目的                   | 操作手順                                                                          |
|----------------------|-------------------------------------------------------------------------------|
| リスト内の短縮 URL の完全な URL | トランザクションを処理したホスト Secure Web Appliance をメモして、そのアプライアンスのアクセスログを確認します。           |
| 個々のトランザクションの詳細       | [Web サイト (Website)] 列の URL をクリックします。                                          |
| すべてのトランザクションの詳細      | [Web サイト (Website)] 列見出しの [すべての詳細を表示...(Display All Details...)] リンクをクリックします。 |

| 目的                     | 操作手順                                                                                                                                                                    |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 500 件までの関連トランザクションのリスト | <p>関連トランザクションの数は、検索結果リストの列見出しにある [詳細を表示 (Display Details)] リンクの下のカッコ内に表示されます。</p> <p>トランザクションの [詳細 (Details)] ビューで [関連トランザクション (Related Transactions)] リンクをクリックします。</p> |

## Web トラッキングおよびアップグレードについて

新しい Web トラッキング機能は、アップグレード前に実行されたトランザクションには適用できない場合があります。これは、これらのトランザクションについては、必須データが保持されていない場合があるためです。Web トラッキング データおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートを参照してください。

## 新しい Web インターフェイスでの Web レポートのスケジューリングとアーカイブ

このセクションの内容は次のとおりです。

- [新しい Web インターフェイスでの Web レポートのスケジューリング \(653 ページ\)](#)
- [新しい Web インターフェイスでの Web レポートのアーカイブ \(655 ページ\)](#)

## 新しい Web インターフェイスでの Web レポートのスケジューリング

このセクションの内容は次のとおりです。

- [新しい Web インターフェイスでのスケジュール済み Web レポートの追加 \(654 ページ\)](#)
- [新しい Web インターフェイスでのスケジュール済み Web レポートの編集 \(654 ページ\)](#)
- [新しい Web インターフェイスでのスケジュール済み Web レポートの削除 \(655 ページ\)](#)

日単位、週単位、または月単位で実行されるようにレポートをスケジュール設定することができます。スケジュール設定されたレポートは、前日、過去 7 日間、前月、過去の日（最大 250 日）、過去の月（最大 12 ヶ月）のデータを含めるように設定できます。また、指定した日数（2 ～ 100 日）または指定した月数（2 ～ 12 ヶ月）のデータを含めることもできます。

レポートの実行時間にかかわらず、直前の時間間隔（過去 1 時間、1 日、1 週間、または 1 ヶ月）のデータのみが含まれます。たとえば、日次レポートを午前 1 時に実行するようにスケジュールを設定した場合、レポートには前日の 00:00 から 23:59 までのデータが含まれます。

必要に応じた数（ゼロも含む）のレポート受信者を定義できます。電子メール受信者を指定しない場合でも、レポートはアーカイブされます。レポートを多数のアドレスに送信する必要がある場合、個別に受信者を設定するよりも、メーリングリストを作成するほうが容易です。

## 新しい Web インターフェイスでのスケジュール済み Web レポートの追加

## 手順

- 
- ステップ 1** [モニターリング (Monitoring)] > [スケジュールとアーカイブ (Schedule & Archive)] を選択します。
- ステップ 2** [スケジュール済み/アーカイブ済み (Scheduled / Archived)] タブで、[+] ボタンをクリックします。
- ステップ 3** [レポートタイプ (Report Type)] ドロップダウンメニューからレポートタイプを選択します。
- ステップ 4** [レポートタイトル (Report Title)] フィールドに、レポートのタイトルを入力します。
- 同じ名前の複数のレポートを作成することを防止するため、わかりやすいタイトルを使用することを推奨します。
- ステップ 5** [含める時間範囲 (Time Range to Include)] ドロップダウンメニューからレポートの時間範囲を選択します。
- ステップ 6** 生成されるレポートの形式を選択します。
- デフォルト形式は PDF です。
- ステップ 7** [配信オプション (Delivery Option)] セクションから、次のオプションのいずれかを選択します。
- このオプションを選択すると、レポートが [アーカイブレポート (Archived Reports)] ページに表示されます。
- (注)
- [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] レポートはアーカイブできません。
- レポートをアーカイブするには、[アーカイブのみ (Only Archive)] を選択します。
  - レポートをアーカイブしてメール送信するには、[アーカイブおよび受信者にメール送信 (Archive and Email to Recipients)] をクリックします。
  - レポートを電子メールで送信するには、[受信者への電子メールのみ (Only Email to Recipients)] をクリックします。
- [電子メールID (Email IDs)] フィールドで、受信者の電子メールアドレスを入力します。
- ステップ 8** [スケジュール (Schedule)] 領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。
- ステップ 9** [レポート言語 (Report language)] ドロップダウンリストから、レポートを生成する必要がある言語を選択します。
- ステップ 10** [Submit] をクリックします。
- 

## 新しい Web インターフェイスでのスケジュール済み Web レポートの編集

アプライアンスの新しい Web インターフェイスでレポートを編集するには、[モニターリング (Monitoring)] > [スケジュールとアーカイブ (Schedule & Archive)] ページを選択します。編

集するレポートのレポートタイトルに対応するリンクをクリックします。設定を変更してから、[編集 (Edit)] をクリックしてページで変更を送信します。

### 新しい Web インターフェイスでのスケジュール済み Web レポートの削除

アプライアンスの新しい Web インターフェイスでレポートを削除するには、[モニタリング (Monitoring)] > [スケジュール済み/アーカイブ済み (Scheduled/Archived)] ページを選択します。削除するレポートに対応するチェックボックスをオンにして、ゴミ箱アイコンをクリックします。

スケジュール済みのすべてのレポートを削除するには、レポートタイトルの横にあるチェックボックスをオンにします。削除されたレポートのアーカイブ版は削除されません。

## 新しい Web インターフェイスでの Web レポートのアーカイブ

- [\(新しい Web インターフェイス\) オンデマンドでの Web レポートの生成 \(655 ページ\)](#)
- [新しい Web インターフェイスでのアーカイブ済み Web レポートの表示と管理 \(656 ページ\)](#)

### (新しい Web インターフェイス) オンデマンドでの Web レポートの生成

スケジュールを設定できるレポートのほとんどは、オンデマンドでの生成も可能です。

レポートをオンデマンドで生成するには、次の手順を実行します

#### 手順

- 
- ステップ 1** Secure Web Applianceで、[モニタリング (Monitoring)] > [スケジュールとアーカイブ (Schedule & Archive)] を選択します。
- ステップ 2** [アーカイブの表示 (View Archived)] タブで、[+] ボタンをクリックします。
- ステップ 3** [レポートタイプ (Report Type)] セクションで、ドロップダウンリストからレポートタイプを選択します。  
このページのオプションは変更される場合があります。
- ステップ 4** [レポートタイトル (Report Title)] セクションに、レポートのタイトルの名前を入力します。  
AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前での複数のレポートを作成しないでください。
- ステップ 5** [含める時間範囲 (Time Range to Include)] ドロップダウンリストから、レポートデータの時間範囲を選択します。
- ステップ 6** [添付ファイルの詳細 (Attachment Details)] セクションで、レポートの形式を選択します。  
PDF、配信用、アーカイブ用、またはその両方の用途でPDF形式のドキュメントを作成します。[PDF レポートをプレビュー (Preview PDF Report)] をクリックすると、ただちに PDF ファイルでレポートを表示できます。
- ステップ 7** [配信オプション (Delivery Option)] セクションから、次のオプションのいずれかを選択します。



このオプションを選択すると、レポートが [アーカイブレポート (Archived Reports)] ページに表示されます。

(注)

[ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] レポートはアーカイブできません。

- レポートをアーカイブするには、[アーカイブのみ (Only to Archive)] を選択します。
- レポートをアーカイブしてメール送信するには、[アーカイブおよび受信者にメール送信 (Archive and Email to Recipients)] をクリックします。
- レポートを電子メールで送信するには、[受信者への電子メールのみ (Only Email to Recipients)] をクリックします。

[電子メールID (Email IDs)] フィールドで、受信者の電子メールアドレスを入力します。

**ステップ 8** [レポート言語 (Report language)] ドロップダウンリストから、レポートを生成する必要がある言語を選択します。

**ステップ 9** [このレポートを配信 (Deliver This Report)] をクリックして、レポートを生成します。

## 新しい Web インターフェイスでのアーカイブ済み Web レポートの表示と管理

ここでは、スケジュール設定されたレポートとして生成されたレポートの使用方法について説明します。

### 手順

**ステップ 1** アプライアンスの新しい Web インターフェイスにログインします。

**ステップ 2** [モニタリング (Monitoring)] > [スケジュールとアーカイブ (Schedule & Archive)] を選択します。

**ステップ 3** [アーカイブの表示 (View Archived)] タブを選択します。

**ステップ 4** レポートを表示するには、[レポートタイトル (Report Title)] 列でレポート名をクリックします。[レポートタイプ (Report Type)] ドロップダウンリストでは、[アーカイブ済みレポート (Archived Reports)] タブにリストされているレポートのタイプをフィルタリングします。

**ステップ 5** 検索ボックスで特定のレポートを検索できます。

## 新しい Web インターフェイスの [システムステータス (SystemStatus)] ページ

Secure Web Appliance で、[モニタリング (Monitoring)] > [システムステータス (System Status)] を選択して、システムステータスをモニターします。このページは、Secure Web Appliance の

現在のステータスと設定を表示します。ブラウザの時刻は、右上隅の [システムステータス (System Status)] ページに表示されます。

[システムステータス (System Status)] ページには次のタブがあります。

- [容量](#)

デフォルトでは、[ステータス (Status)] タブが表示されます。

## ステータス

[ステータス (Status)] ページには、次の情報が表示されます。

| セクション                                                                | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Web Appliance<br>のステータス (Web<br>Security Appliance<br>Status) | <ul style="list-style-type: none"> <li>• システムの動作期間</li> <li>• システム リソースの使用率：レポーティングおよびロギングに使用される CPU 使用率、RAM 使用率、およびディスク領域の使用率。</li> </ul> <p>システムによって使用されない RAM は Web オブジェクトキャッシュによって使用されるので、効率的に動作する RAM 使用率は 90% を超える場合があります。システムで重大なパフォーマンス問題が発生していない場合で、この値が 100% に固定されない場合、システムは正常に動作しています。</p> <p>(注)<br/>プロキシバッファ メモリは、この RAM を使用する 1 つのコンポーネントです。</p>                                                                                                                                                               |
| アラート (Alerts)                                                        | <p>発生したアラートの名前と日付と時刻が表示されます。右上隅の上部にある [詳細 (More)] またはアラート名をクリックすると、[すべてのアラート (All Alerts)] ポップアップが表示されます。[すべてのアラート (All Alerts)] ポップアップで、選択したアラート行が強調表示されます。</p> <p>[すべてのアラート (All Alerts)] ポップアップには次の情報が表示されます。</p> <ul style="list-style-type: none"> <li>• アラートの日付と時刻 (Date and Time of Alert)</li> <li>• アラートレベル (Alert Level) : [情報 (Info)]、[警告 (Warning)]、または [クリティカル (Critical)]</li> <li>• アラートクラス (Alert Class)</li> <li>• 問題 (Problem) : アラートの簡単な説明</li> <li>• 受信者 (Recipient) : アラートの詳細が送信される電子メールアドレス</li> </ul> |

| セクション                    | 説明                                                                                                                                                                               |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ディスク使用率 (Disk Usage)     | <p>ディスク使用率の値と RAID ストレージのステータスが表示されます。</p> <p>RAID ストレージのステータスは、アプライアンスの設定によって異なります。仮想アプライアンスの場合、RAID ストレージのステータスには [不明 (Unknown)] と表示され、物理アプライアンスには [Optimal (最適)] と表示されます。</p> |
| プロキシステータス (Proxy Status) | <p>プロキシの CPU 使用率とプロキシディスクの I/O 使用率を表示します。</p> <p>また、プロキシ接続のバックログもポート番号と接続数とともに表示されます。</p>                                                                                        |
| 高可用性 (High Availability) | <p>フェールオーバーグループの名前、優先順位、およびステータスを表示します。</p> <p>また、有効になっている高可用性フェールオーバーグループの数も表示されます。フェールオーバーグループが存在しない場合は、[設定されていません (Not Configured)] というサービスステータスが表示されます。</p>                  |

| セクション                                         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プロキシトラフィックの特性 (Proxy Traffic Characteristics) | <p>次のプロキシトラフィックの特性が表示されます。</p> <ul style="list-style-type: none"> <li>• 1 秒あたりの要求数 (Request Per Second)</li> <li>• 帯域幅</li> <li>• 応答時間 (Response Time)</li> <li>• キャッシュヒット率 (Cache Hit Rate)</li> <li>• 現在の接続数 (Current Connections) : 特定の日時の接続数について次の詳細が表示されます。 <ul style="list-style-type: none"> <li>• アイドル状態のクライアント接続数</li> <li>• アイドル状態のサーバー接続数</li> <li>• クライアントの総接続数</li> <li>• サーバーの総接続数</li> </ul> </li> </ul> <p>これらのデータの平均値と最大値が表示されます。最後の1分間、最後の1時間、およびプロキシの再起動以降についての平均値が表示されます。最大値は、最後の1時間とプロキシの再起動以降について表示されます。</p> <p>(注)</p> <p>[RPSと帯域幅 (RPS and Bandwidth)] の横にあるリンクアイコンをクリックすると、[キャパシティ (Capacity)] タブにリダイレクトされます。同様に、[応答時間 (Response Time)] の横にあるリンクアイコンをクリックすると、[サービス (Services)] タブにリダイレクトされます。</p> |

## 容量 (Capacity)

[キャパシティ (Capacity)] ページには、次の情報が表示されます。

| セクション               | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 時間範囲 (Time Range)   | <p>次の [時間範囲 (Time Range)] オプションを表示します。</p> <ul style="list-style-type: none"> <li>• 時間 (Hour)</li> <li>• 曜日</li> <li>• 週</li> <li>• 30 日</li> <li>• 90 日</li> <li>• 昨日 (Yesterday) (00:00 ~ 23:59)</li> <li>• 先月 (Previous Calendar Month)</li> <li>• [カスタム範囲 (Custom Range)] : 使用可能な最も古いデータ</li> </ul> <p>使用可能な最も古いデータを表示するには [適用 (Apply)] をクリックし、操作をキャンセルするには [キャンセル (Cancel)] をクリックします。</p> <p>(注)<br/>[時間範囲 (Time Range)] オプションは、[キャパシティ (Capacity)] タブのすべての機能に適用されます。</p>                                                                                                         |
| システム CPU およびメモリの使用率 | <p>[システム CPU およびシステムメモリの使用率 (System CPU and System Memory Usage)] では、次の操作を実行できます。</p> <ul style="list-style-type: none"> <li>• しきい値を更新または設定します (例 : 0 ~ 100%) 。</li> <li>• しきい値を変更します。</li> <li>• CPU / メモリ使用率を表示します。カラーコードは次のとおりです。 <ul style="list-style-type: none"> <li>• 赤色 : しきい値を示します。</li> <li>• 緑色 : 平均値を示します。しきい値を変更すると、それに応じて平均値も更新されます。</li> </ul> <p>平均値は、合計値をレコードの長さで割った値です。</p> <li>• 青色 : システムメモリ使用率 (%) を表示します。</li> </li></ul> <p>[システム CPU およびメモリ使用率 (System CPU and Memory Usage)] データは、[時間範囲 (Time Range)] 選択に基づくパーセンテージで表示されます。データとグラフは、現在のデータに基づいて動的に変化します。</p> |

| セクション           | 説明                                                                                                                                                                                                                                                                                    |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 帯域幅および RPS      | <p>次の帯域幅と RPS の詳細をグラフ形式で表示します。</p> <ul style="list-style-type: none"> <li>全体：ダーク ブルーで表示</li> <li>HTTPS 復号：アクア ブルーで表示</li> </ul> <p>凡例ブロックをクリックすると、[全体 (Overall)] 情報と [HTTPS 復号 (HTTPS Decrypted)] 情報を有効または無効にすることができます。</p>                                                           |
| 機能別 CPU 利用率     | <p>各種 CPU 使用率オプションの色分けは次のとおりです。</p> <ul style="list-style-type: none"> <li>薄い緑色：Web プロキシ</li> <li>濃い緑色：ロギング</li> <li>紫色：レポート</li> <li>黄色：WBRs</li> <li>暗い青色：AMP</li> <li>薄い青色：Webroot</li> <li>水色：Sophos</li> <li>灰色：McAfee</li> </ul> <p>凡例ブロックをクリックすると、オプションを有効または無効にすることができます。</p> |
| クライアントまたはサーバー接続 | <p>平均および最大接続数を表示し、次のタスクを実行できます。</p> <ul style="list-style-type: none"> <li>平均および最大接続数の有効化または無効化</li> <li>平均および最大接続の詳細とグラフの表示</li> </ul>                                                                                                                                               |

## サービス

[サービス (Services)] ページには、サービスとそのステータスが表示されます。[サービス (Services)] リボンには、AMP、WCCP、ISE、および CTR のサービスステータスが表示されます。サービス名の横の色は、サービスステータスを示します。

- 赤：サービスの準備ができていません。
- グレー：サービスの準備はできていますが、無効になっています。
- 緑：サービスの準備ができており、有効になっています。

| セクション                       | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 日付                          | 当日のサービスデータがデフォルトで表示されます。最大で過去7日間のデータを表示できます。特定の日のデータを表示するには、カレンダーから日付を選択します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| サービスのステータス (Service Status) | <p>[サービスステータス (Service Status)] テーブルには、サービスのイベントとアラートが表示されます。テーブルには、1時間のスロットに分割された 24 時間の時間間隔が表示されます。各ブロックには 1 時間の時間間隔でアラートが表示されます。</p> <p>ブロックの色が緑の場合は、対応する時間帯にクリティカルなアラートがないことを示します。1 時間に少なくとも 1 つ以上のクリティカルなアラートがある場合は、対応するブロックが赤で表示されます。未来のタイムスロットに対応するブロックは白で表示されます。</p> <p>サービス名の近くの左側にあるアイコンには、最後のブロック（進行中の時間帯）の色が表示されます。</p> <p>赤のブロックをクリックすると、最後の 5 つのアラートが発生した時間を確認できます。また、アラートの合計数も、[「n」 イベント中 5 (5 of 'n' Events)] と表示されます。ここで、「n」は、その時間に発生したアラートの合計数です。[その他 (More)] をクリックすると、[すべてのアラート (All Alerts)] ポップアップが表示されます。</p> <p>[すべてのアラート (All Alerts)] ポップアップには次の情報が表示されます。</p> <ul style="list-style-type: none"> <li>• アラートの日付と時刻 (Date and Time of Alert)</li> <li>• アラートレベル (Alert Level) : [情報 (Info)]、[警告 (Warning)]、または [クリティカル (Critical)]</li> <li>• アラートクラス (Alert Class)</li> <li>• 問題 (Problem) : アラートの簡単な説明</li> <li>• 受信者 (Recipient) : アラートの詳細が送信される電子メールアドレス</li> </ul> |

| セクション                               | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サービス応答時間<br>(Service Response Time) | <p>[サービス応答時間 (Service Response Time)] テーブルには、システムで実行されている各サービスの所要応答時間のパターンが表示されます。次の時間が表示されます。</p> <ul style="list-style-type: none"> <li>• McAfee サービス時間 (McAfee Service Time)</li> <li>• WBRs サービス時間 (WBRs Service Time)</li> <li>• DNS 応答時間 (DNS Response Time)</li> <li>• Webroot サービス時間 (Webroot Service Time)</li> <li>• AMP サービス時間</li> <li>• Sophos サービス時間 (Sophos Service Time)</li> <li>• サーバー応答時間 (Server Response Time)</li> </ul> <p>テーブルには、1 時間のスロットに分割された 24 時間の時間間隔が表示されます。各ブロックは、1 時間のサービス応答パターンを表します。各サービスの応答時間は、次のタイムスロットに分割されます。</p> <ul style="list-style-type: none"> <li>• 0.001 秒～ 0.06 秒</li> <li>• 0.06 秒～ 0.6 秒</li> <li>• 0.6 秒～ 1 秒</li> <li>• 1 秒～ 6 秒</li> <li>• 6 秒以降</li> </ul> <p>デフォルトでは、テーブルにはすべてのサービスの 1 秒～ 6 秒の応答値が表示されます。詳細な分割部分を展開して表示することができます。</p> <p>システムは、すべてのトランザクションの応答時間を計算します。その後で、各タイムスロットで発生したトランザクションボリュームのパーセンテージが表示されます。ブロックの色は、トランザクションボリュームのパーセンテージに基づいています。</p> |



| セクション | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>応答時間が1秒未満の場合、トランザクション量の凡例は次のようになります。</p> <ul style="list-style-type: none"> <li>• 濃い青色：41 ～ 100%</li> <li>• 水色：11 ～ 40%</li> <li>• 薄い青色：1 ～ 10%</li> <li>• 白色：0%</li> </ul> <p>応答時間が1秒以上の場合、トランザクション量の凡例は次のようになります。</p> <ul style="list-style-type: none"> <li>• 赤色：41 ～ 100%</li> <li>• 薄い赤色：26 ～ 40%</li> <li>• 薄い青色：1 ～ 25%</li> <li>• 白色：0%</li> </ul> <p>応答時間のデータが秒単位で使用できない場合、凡例の色オプションは白になり、編集できません。[時間範囲 (Time Range)] オプションをクリックして、サービス応答時間データを取得します。</p> <p>データには、棒グラフと発生回数が含まれます。ただし、次のものは取得できません。</p> <ul style="list-style-type: none"> <li>• 棒グラフ</li> <li>• 以前の日付の凡例データ</li> </ul> <p>時間ブロックをクリックすると、その特定の時間の応答トレンドを棒グラフで表示するポップアップが開きます。</p> <ul style="list-style-type: none"> <li>• 横軸：5 分間隔に分割されたタイムスロット</li> <li>• 垂直軸：タイムスロット内のトランザクション数</li> </ul> <p>ポップアップのブロックにマウスのカーソルを合わせると、その時間間隔のトランザクション数が表示されます。</p> |



## 第 9 章

# モニタリングおよびトラブルシューティング

---

この章で説明する内容は、次のとおりです。

- [ログによるシステム アクティビティのモニター](#) (665 ページ)
- [トラブルシューティング](#) (739 ページ)

## ログによるシステム アクティビティのモニター

この章で説明する内容は、次のとおりです。

- [ロギングの概要](#) (666 ページ)
- [ロギングの共通タスク](#) (666 ページ)
- [ロギングのベストプラクティス](#) (667 ページ)
- [ログによる Web プロキシのトラブルシューティング](#) (667 ページ)
- [ログ ファイルのタイプ](#) (668 ページ)
- [ログ サブスクリプションの追加および編集](#) (676 ページ)
- [別のサーバへのログ ファイルのプッシュ](#) (683 ページ)
- [ログ ファイルのアーカイブ](#) (684 ページ)
- [ログのファイル名とアプライアンスのディレクトリ構造](#) (685 ページ)
- [ログ ファイルの表示](#) (686 ページ)
- [アクセス ログ ファイル内の Web プロキシ情報](#) (686 ページ)
- [W3C 準拠のアクセス ログ ファイル](#) (712 ページ)
- [アクセス ログのカスタマイズ](#) (714 ページ)
- [トラフィック モニタのログ ファイル](#) (720 ページ)

- [ログ ファイルのフィールドとタグ \(721 ページ\)](#)
- [ログギングのトラブルシューティング \(739 ページ\)](#)

## ログギングの概要

Secure Web Applianceでは、システムとトラフィックの管理アクティビティの記録がログファイル上に書き込まれます。管理者はこれらのログ ファイルを参照して、アプライアンスをモニターし、トラブルシューティングできます。

各種アクティビティはいくつかのログギング タイプごとに記録されるため、特定のアクティビティに関する情報の検索が容易です。多くのログギングタイプはデフォルトでイネーブルになりますが、いくつかは、必要に応じて手動でイネーブルにする必要があります。

ログ ファイルをイネーブルにして管理するには、ログ ファイル サブスクリプションを設定します。サブスクリプションにより、ログファイルの作成、カスタマイズ、および管理に関する設定を定義できます。

通常、管理者が主に使用するログ ファイルは、以下の 2 種類です。

- **アクセス ログ。**すべての Web プロキシフィルタリングとスキャンアクティビティが記録されます。
- **トラフィック モニター ログ。**すべての L4 トラフィック モニター アクティビティが記録されます。

これらのログ タイプおよびその他のログ タイプを使用して、アプライアンスの現在と過去のアクティビティを確認できます。ログ ファイル エントリの内容を理解できるように、リファレンス テーブルが用意されています。

### 関連項目

- [ログギングの共通タスク, on page 666](#)
- [ログ ファイルのタイプ, on page 668](#)

## ログギングの共通タスク

| タスク                    | 関連項目および手順へのリンク                                     |
|------------------------|----------------------------------------------------|
| ログ サブスクリプションを追加および編集する | <a href="#">ログ サブスクリプションの追加および編集, on page 676</a>  |
| ログ ファイルを表示する           | <a href="#">ログ ファイルの表示, on page 686</a>            |
| ログ ファイルを解釈する           | <a href="#">アクセス ログのスキャン判定エントリの解釈, on page 703</a> |
| ログ ファイルをカスタマイズする       | <a href="#">アクセス ログのカスタマイズ, on page 714</a>        |

| タスク                   | 関連項目および手順へのリンク                                   |
|-----------------------|--------------------------------------------------|
| 別のサーバーにログ ファイルをプッシュする | <a href="#">別のサーバへのログ ファイルのプッシュ, on page 683</a> |
| ログ ファイルをアーカイブする       | <a href="#">ログ ファイルのアーカイブ, on page 684</a>       |

## ロギングのベスト プラクティス

- ログサブスクリプションの数を最小限にすると、システムパフォーマンスが向上します。
- 記録する詳細を少なくすると、システム パフォーマンスが向上します。

## ログによる Web プロキシのトラブルシューティング

Secure Web Applianceでは、デフォルトで、Web プロキシロギング メッセージ用の 1 つのログサブスクリプションが作成されます（「デフォルトプロキシログ」と呼ばれます）このログには、すべての Web プロキシモジュールに関する基本的な情報が記録されます。アプライアンスには、各 Web プロキシモジュールのログファイルタイプも含まれているので、デフォルトプロキシログを画面いっぱいに散乱させることなく、各モジュールのより詳細なデバッグ情報を読み取ることができます。

使用可能な各種のログを使用して Web プロキシの問題をトラブルシューティングするには、以下の手順に従います。

### Procedure

**ステップ 1** デフォルト プロキシ ログを読みます。

**ステップ 2** 問題を解決するためにより詳細な情報が必要な場合は、その問題に関連する特定の Web プロキシモジュールのログサブスクリプションを作成します。以下の Web プロキシモジュールログ タイプのサブスクリプションを作成できます。

|                     |                      |
|---------------------|----------------------|
| アクセス コントロール エンジン ログ | ロギング フレームワーク ログ      |
| ADC エンジンフレームワークログ   | McAfee 統合フレームワーク ログ  |
| AVC エンジンフレームワークログ   | メモリ マネージャ ログ         |
| 設定ログ                | その他のプロキシ モジュール ログ    |
| 接続管理ログ              | リクエスト デバッグ ログ        |
| データ セキュリティ モジュール ログ | SNMP モジュール ログ        |
| DCA エンジン フレームワーク ログ | Sophos 統合フレームワーク ログ  |
| ディスク マネージャ ログ       | WBRS フレームワーク ログ      |
| FireAMP             | WCCP モジュール ログ        |
| FTP プロキシ ログ         | Webcat 統合フレームワーク ログ  |
| HTTPS ログ            | Webroot 統合フレームワーク ログ |
| ライセンス モジュール ログ      |                      |

**ステップ 3** 問題を再現して、その問題に関する新しい Web プロキシ モジュール ログを確認します。

**ステップ 4** 必要に応じて、他の Web プロキシ モジュール ログを使用して繰り返します。

**ステップ 5** 不要になったサブスクリプションを削除します。

## What to do next

### 関連項目

- [ログ ファイルのタイプ, on page 668](#)
- [ログ サブスクリプションの追加および編集, on page 676](#)

## ログ ファイルのタイプ

Web プロキシ コンポーネントに関するいくつかのログ タイプはイネーブルになっていません。「デフォルト プロキシ ログ」と呼ばれるメインの Web プロキシ ログ タイプはデフォルトでイネーブルになっており、すべての Web プロキシ モジュールの基本的な情報が記録されます。各 Web プロキシ モジュールには、必要に応じてイネーブルにできる独自のログ タイプがあります。

以下の表は、Secure Web Appliance のログ ファイル タイプを示しています。

| ログ ファイル タイプ         | 説明                                                                                                                       | syslog プッシュのサポート | デフォルトのイネーブル設定 |
|---------------------|--------------------------------------------------------------------------------------------------------------------------|------------------|---------------|
| アクセス コントロール エンジン ログ | Web プロキシ ACL（アクセス コントロール リスト）の評価エンジンに関連するメッセージを記録します。                                                                    | 非対応              | 非対応           |
| AMP エンジン ログ         | ファイル レピュテーション スキャンとファイル 分析に関する情報（Advanced Malware Protection）を記録します。<br><a href="#">ログ ファイル</a> , on page 504 も参照してください。 | 対応               | 対応            |

| ログ ファイル タイプ       | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | syslog プッシュのサポート | デフォルトのイネーブル設定 |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------------|
| 監査ログ              | <p>認証、許可、アカウントिंगのイベント（AAA : Authentication、Authorization、および Accounting）を記録します。アプリケーションおよびコマンドライン インターフェイスにおけるすべてのユーザ操作を記録し、変更内容を保存します。</p> <p>監査ログの詳細の一部を次に示します。</p> <ul style="list-style-type: none"> <li>• ユーザ - ログオン</li> <li>• ユーザ - ログオンに失敗しました、パスワードが正しくありません</li> <li>• ユーザ - ログオンに失敗しました、ユーザ名が不明です</li> <li>• ユーザ - ログオンに失敗しました、アカウントの有効期限が切れています</li> <li>• ユーザ - ログオフ</li> <li>• ユーザ - ロックアウト</li> <li>• ユーザ - アクティブ化済み</li> <li>• ユーザ - パスワードの変更</li> <li>• ユーザ - パスワードのリセット</li> <li>• ユーザ - セキュリティ設定/プロファイルの変更</li> <li>• ユーザ - 作成済み</li> <li>• ユーザ - 削除済み/変更済み</li> <li>• グループ/ロール - 削除/変更済み</li> <li>• グループ/ロール - アクセス許可の変更</li> </ul> | 対応               | 対応            |
| アクセス ログ           | Web プロキシのクライアント履歴を記録します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 対応               | 対応            |
| ADC エンジンフレームワークログ | Web プロキシと ADC エンジン間の通信に関連するメッセージを記録します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 非対応              | 非対応           |
| ADC エンジンログ        | AVC エンジンからのデバッグメッセージを記録します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 対応               | 対応            |

| ログ ファイル タイプ                        | 説明                                                          | syslog プッシュのサポート | デフォルトのイネーブル設定 |
|------------------------------------|-------------------------------------------------------------|------------------|---------------|
| 認証フレームワーク ログ                       | 認証履歴とメッセージを記録します。                                           | 非対応              | 対応            |
| AVC エンジン フレームワーク ログ                | Web プロキシと AVC エンジン間の通信に関連するメッセージを記録します。                     | 非対応              | 非対応           |
| AVC エンジン ログ                        | AVC エンジンからのデバッグ メッセージを記録します。                                | 対応               | 対応            |
| CLI 監査ログ                           | コマンドラインインターフェイス アクティビティの監査履歴を記録します。                         | 対応               | 対応            |
| 設定ログ                               | Web プロキシ コンフィギュレーション管理システムに関連するメッセージを記録します。                 | 非対応              | 非対応           |
| 接続管理ログ                             | Web プロキシ接続管理システムに関連するメッセージを記録します。                           | 非対応              | 非対応           |
| データ セキュリティ ログ                      | Cisco データ セキュリティ フィルタで評価されたアップロード要求のクライアント履歴を記録します。         | 対応               | 対応            |
| データ セキュリティ モジュール ログ                | Cisco データ セキュリティ フィルタに関するメッセージを記録します。                       | 非対応              | 非対応           |
| DCA エンジン フレームワーク ログ<br>(動的コンテンツ分析) | Web プロキシと Cisco Web 利用の制御動的コンテンツ分析エンジン間の通信に関連するメッセージを記録します。 | 非対応              | 非対応           |
| DCA エンジン ログ<br>(動的コンテンツ分析)         | Cisco Web 利用の制御動的コンテンツ分析エンジンに関連するメッセージを記録します。               | 対応               | 対応            |



| ログ ファイル タイプ                     | 説明                                                                                                                                                      | syslog プッシュのサポート | デフォルトのイネーブル設定 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------------|
| デフォルト プロキシ ログ                   | <p>Web プロキシに関連するエラーを記録します。</p> <p>これは、Web プロキシに関連するすべてのログの最も基本的なものです。Web プロキシに関連するより具体的な分野のトラブルシューティングを行うには、該当する Web プロキシ モジュールのログ サブスクリプションを作成します。</p> | 対応               | 対応            |
| ディスク マネージャ ログ                   | ディスク上のキャッシュの書き込みに関連する Web プロキシ メッセージを記録します。                                                                                                             | 非対応              | 非対応           |
| 外部認証ログ                          | <p>外部認証サーバによる通信の成功または失敗など、外部認証機能の使用に関連するメッセージを記録します。</p> <p>外部認証がディセーブルされている場合でも、このログにはローカル ユーザのログインの成功または失敗に関するメッセージが記録されています。</p>                     | 非対応              | 対応            |
| フィードバック ログ                      | 誤って分類されたページをレポートする Web ユーザを記録します。                                                                                                                       | 対応               | 対応            |
| FTP プロキシ ログ                     | FTP プロキシに関連するエラーおよび警告メッセージを記録します。                                                                                                                       | 非対応              | 非対応           |
| FTP サーバ ログ                      | FTP を使用して、Secure Web Appliance にアップロードされ、ダウンロードされるすべてのファイルを記録します。                                                                                       | 対応               | 対応            |
| GUI ログ<br>(グラフィカル ユーザ インターフェイス) | Web インターフェイスのページ更新履歴を記録します。GUI ログには、SMTP トランザクションに関する情報（たとえば、アプライアンスから電子メールで送信されるスケジュール済みレポートに関する情報）も記録されます。                                            | 対応               | 対応            |
| Haystack ログ                     | Haystack ログには、データ処理をトラッキングする Web トランザクションが記録されます。                                                                                                       | 対応               | 対応            |

| ログ ファイル タイプ                   | 説明                                                                | syslog プッシュのサポート | デフォルトのイネーブル設定 |
|-------------------------------|-------------------------------------------------------------------|------------------|---------------|
| HTTPS ログ                      | HTTPS プロキシ固有の Web プロキシメッセージを記録します (HTTPS プロキシがイネーブルの場合)。          | 非対応              | 非対応           |
| ISE サーバ ログ                    | ISE サーバの接続および動作情報を記録します。                                          | 対応               | 対応            |
| ライセンス モジュール ログ                | Web プロキシのライセンスおよび機能キー処理システムに関するメッセージを記録します。                       | 非対応              | 非対応           |
| ロギング フレームワーク ログ               | Web プロキシのロギング システムに関するメッセージを記録します。                                | 非対応              | 非対応           |
| ロギング ログ                       | ログ管理に関連するエラーを記録します。                                               | 対応               | 対応            |
| McAfee 統合フレームワーク ログ           | Web プロキシと McAfee スキャン エンジン間の通信に関連するメッセージを記録します。                   | 非対応              | 非対応           |
| McAfee ログ                     | McAfee スキャン エンジンからアンチマルウェア スキャン アクティビティのステータスを記録します。              | 対応               | 対応            |
| メモリ マネージャ ログ                  | Web プロキシ プロセスのメモリ内キャッシュを含むすべてのメモリの管理に関連する Web プロキシメッセージを記録します。    | 非対応              | 非対応           |
| その他のプロキシモジュール ログ              | 主に開発者やカスタマー サポートによって使用される Web プロキシメッセージを記録します。                    | 非対応              | 非対応           |
| AnyConnect セキュア モビリティ デーモン ログ | ステータスチェックなど、Secure Web Appliance と AnyConnect クライアント間の相互作用を記録します。 | 対応               | 対応            |
| NTP ログ<br>(ネットワーク タイム プロトコル)  | ネットワーク タイム プロトコルによって作成されたシステム時刻に変更します。                            | 対応               | 対応            |
| PAC ファイル ホスティング デーモン ログ       | クライアントによるプロキシ自動設定 (PAC) ファイルの使用状況を記録します。                          | 対応               | 対応            |

| ログ ファイル タイプ             | 説明                                                                                                                                                                                                          | syslog プッシュのサポート | デフォルトのイネーブル設定 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------------|
| プロキシバイパスログ              | Webプロキシをバイパスするトランザクションを記録します。                                                                                                                                                                               | 非対応              | 対応            |
| レポーティング ログ              | レポート生成履歴を記録します。                                                                                                                                                                                             | 対応               | 対応            |
| レポーティング クエリー ログ         | レポート生成に関連するエラーを記録します。                                                                                                                                                                                       | 対応               | 対応            |
| リクエスト デバッグ ログ           | すべての Web プロキシ モジュール ログ タイプから、特定の HTTP トランザクションに関する非常に詳細なデバッグ情報を記録します。他のすべてのプロキシログサブスクリプションを作成することなく、特定のトランザクションによるプロキシ問題のトラブルシューティングを行うために、このログサブスクリプションを作成する場合があります。<br><br>注：CLIでのみ、このログサブスクリプションを作成できます。 | 非対応              | 非対応           |
| 認証ログ                    | アクセスコントロール機能に関するメッセージを記録します。                                                                                                                                                                                | 対応               | 対応            |
| SHD ログ<br>(システムヘルスデーモン) | システム サービスの動作状態の履歴および予期しないデーモンの再起動の履歴を記録します。                                                                                                                                                                 | 対応               | 対応            |
| SNMP ログ                 | SNMP管理エンジンに関連するデバッグメッセージを記録します。                                                                                                                                                                             | 対応               | 対応            |
| SNMP モジュール ログ           | SNMP モニタリング システムとの対話に関連する Web プロキシメッセージを記録します。                                                                                                                                                              | 非対応              | 非対応           |
| Sophos 統合フレームワーク ログ     | Web プロキシと Sophos スキャン エンジン間の通信に関連するメッセージを記録します。                                                                                                                                                             | 非対応              | 非対応           |
| Sophos ログ               | Sophos スキャン エンジンからアンチマルウェア スキャン アクティビティのステータスを記録します。                                                                                                                                                        | 対応               | 対応            |

| ログ ファイル タイプ                           | 説明                                                                                                                                         | syslog プッシュのサポート | デフォルトのイネーブル設定 |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------------|
| ステータス ログ                              | 機能キーのダウンロードなど、システムに関連する情報を記録します。                                                                                                           | 対応               | 対応            |
| システム ログ                               | DNS、エラー、およびコミット アクティビティを記録します。                                                                                                             | 対応               | 対応            |
| トラフィック モニタリング エラー ログ                  | L4TM インターフェイスおよびキャプチャ エラーを記録します。                                                                                                           | 対応               | 対応            |
| トラフィック モニタ ログ                         | L4TM ブロックおよび許可リストに追加されたサイトを記録します。                                                                                                          | 非対応              | 対応            |
| UDS ログ<br>(ユーザ検出サービス)                 | Web プロキシが実際の認証を行わずにユーザ名を検出する方法に関するデータを記録します。セキュア モビリティ用の Cisco 適応型セキュリティアプライアンスとの対話、および透過的ユーザ ID 用の Novell eDirectory サーバとの統合に関する情報が含まれます。 | 対応               | 対応            |
| アップデータ ログ                             | WBRS およびその他の更新の履歴を記録します。                                                                                                                   | 対応               | 対応            |
| W3C ログ                                | W3C 準拠の形式で Web プロキシ クライアント履歴を記録します。<br><br>詳細については、 <a href="#">W3C 準拠のアクセス ログ ファイル, on page 712</a> を参照してください。                            | 対応               | 非対応           |
| WBNP ログ<br>(SensorBase ネットワーク参加)      | SensorBase ネットワークへの Cisco SensorBase ネットワーク参加のアップロード履歴を記録します。                                                                              | 非対応              | 対応            |
| WBRS フレームワーク ログ<br>(Web レピュテーション スコア) | Web プロキシと Web レピュテーション フィルタ間の通信に関連するメッセージを記録します。                                                                                           | 非対応              | 非対応           |
| WCCP モジュール ログ                         | WCCP の実装に関連する Web プロキシ メッセージを記録します。                                                                                                        | 非対応              | 非対応           |

| ログ ファイル タイプ          | 説明                                                                     | syslog プッシュのサポート | デフォルトのイネーブル設定 |
|----------------------|------------------------------------------------------------------------|------------------|---------------|
| Webcat 統合フレームワーク ログ  | Web プロキシと Cisco Web 利用の制御に関連付けられた URL フィルタリングエンジン間の通信に関連するメッセージを記録します。 | 非対応              | 非対応           |
| Webroot 統合フレームワーク ログ | Web プロキシと Webroot スキャン エンジン間の通信に関連するメッセージを記録します。                       | 非対応              | 非対応           |
| Webroot ログ           | Webroot スキャン エンジンからアンチマルウェア スキャン アクティビティのステータスを記録します。                  | 対応               | 対応            |
| ウェルカム ページ 確認ログ       | エンド ユーザの確認ページで [同意する (Accept) ] ボタンをクリックする Web クライアントの履歴を記録します。        | 対応               | 対応            |

## ログサブスクリプションの追加および編集

ログ ファイルのタイプごとに複数のログサブスクリプションを作成できます。サブスクリプションには、以下のようなアーカイブおよびストレージに関する設定の詳細が含まれています。

- ロールオーバー設定。ログ ファイルをアーカイブするタイミングを決定します。
- アーカイブ ログの圧縮設定。
- アーカイブ ログの取得の設定。ログをリモート サーバに保存するか、アプライアンスに保存するかを指定します。

### Procedure

- ステップ 1** [システム管理 (System Administration) ] > [ログサブスクリプション (Log Subscriptions) ] を選択します。
- ステップ 2** ログサブスクリプションを追加するには、[ログ設定を追加 (Add Log Subscription) ] をクリックします。あるいは、ログサブスクリプションを編集するには、[ログ名 (Log Name) ] フィールドのログ ファイルの名前をクリックします。
- ステップ 3** サブスクリプションを設定します。

| オプション                                          | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ログタイプ (Log Type)                               | <p>ユーザが登録できる使用可能なログファイルタイプのリスト。このページの他のオプションは、選択したログファイルタイプによって異なります。</p> <p><b>Note</b><br/>[リクエストデバッグログ (Request Debug Logs)] タイプは CLI を使用してのみ登録でき、このリストには表示されません。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ログ名 (Log Name)                                 | <p>Secure Web Applianceでサブスクリプションの参照に使用される名前。この名前は、サブスクリプションのログファイルを保存するログディレクトリにも使用されます。ASCII 文字 ([0-9]、[A-Z]、[a-z]、および _) のみを入力します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| ファイルサイズ別<br>ロールオーバー<br>(Rollover by File Size) | <p>ログファイルの最大ファイルサイズ。このサイズを超えるとそのファイルがアーカイブされ、新しいログファイルが作成されます。100 キロバイトから 10 ギガバイトまでの数値を入力してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 時刻によりロール<br>オーバー<br>(Rollover by Time)         | <p>ログファイルの最大記録時間。この時間を超えるとそのファイルがアーカイブされ、新しいファイルが作成されます。設定可能なオプションは、以下のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>[なし (None)]</b>。AsyncOS は、ログファイルが最大ファイルサイズに達した場合にのみロールオーバーを実行します。</li> <li>• <b>[カスタム時間間隔 (Custom Time Interval)]</b>。AsyncOS は、以前のロールオーバーから指定された時間が経過した後にロールオーバーを実行します。末尾に d、h、m、s を追加して、ロールオーバー間の日数、時間、分、秒を指定します。</li> <li>• <b>[日次ロールオーバー (Daily Rollover)]</b>。AsyncOS は、毎日指定された時刻にロールオーバーを実行します。1 日に複数の時刻を設定するには、カンマを使用して区切ります。1 時間ごとにロールオーバーを実行するように指定するには、時間にアスタリスク (*) を使用します。また、1 分ごとにロールオーバーするためにアスタリスクを使用することもできます。</li> <li>• <b>[週次ロールオーバー (Weekly Rollover)]</b>。AsyncOS は、1 つ以上の曜日の指定された時刻にロールオーバーを実行します。</li> </ul> |
| ログスタイル<br>(Log Style)<br>(アクセスログ)              | <p>使用するログ形式 ([Squid]、[Apache]、または [Squid の詳細 (Squid Details)] のいずれか) を選択します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| オプション                                  | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| カスタムフィールド (Custom Fields)<br>(アクセスログ)  | <p>各アクセス ログ エントリにカスタム情報を含めることができます。</p> <p>[カスタム フィールド (Custom Fields)] にフォーマット指定子を入力する構文は以下のとおりです。</p> <pre>&lt;format_specifier_1&gt; &lt;format_specifier_2&gt; ...</pre> <p>例: %a %b %E</p> <p>フォーマット指定子の前にトークンを追加して、アクセス ログ ファイルの説明テキストを表示できます。次に例を示します。</p> <pre>client_IP %a body_bytes %b error_type %E</pre> <p>この場合、client_IPはログフォーマット指定子%aの説明トークンです (以下同様)。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| ファイル名 (File Name)                      | <p>ログ ファイルの名前。最新のログ ファイルには拡張子 .c が付き、ロール オーバー済みのログには、ファイル作成時のタイムスタンプと拡張子 .s が付きます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ログ フィールド (Log Fields)<br>(W3C アクセス ログ) | <p>W3C アクセス ログに含めるフィールドを選択できます。</p> <p>[使用可能フィールド (Available Fields)] リストでフィールドを選択するか、[カスタム フィールド (Custom Field)] ボックスにフィールドを入力し、[追加 (Add)] をクリックします。</p> <p>[選択されたログ フィールド (Selected Log Fields)] リストに表示されるフィールドの順序によって、W3C アクセス ログ ファイルのフィールドの順序が決まります。[上へ移動 (Move Up)] または [下へ移動 (Move Down)] ボタンを使用してフィールドの順序を変更できます。[選択されたログ フィールド (Selected Log Fields)] リストでフィールドを選択し、[削除 (Remove)] をクリックして、それを削除できます</p> <p>[カスタム フィールド (Custom Field)] ボックスに複数のユーザ定義フィールドを入力し、それらを同時に入力できます。ただし、[追加 (Add)] をクリックする前に、各エントリが改行 (Enter キーを押します) で区切られている必要があります。</p> <p>W3C ログサブスクリプションに含まれるログ フィールドを変更すると、ログサブスクリプションは自動的にロール オーバーします。これにより、ログ ファイルの最新バージョンに適切な新しいフィールド ヘッダーを含めることができます。</p> <p>W3C ログでは、ログ フィールド <i>c-ip</i>、<i>cs-username</i>、または <i>cs-auth-group</i> を必要に応じて匿名化できます。<i>c-ip</i>、<i>cs-username</i>、および <i>cs-auth-group</i> フィールドを匿名化するには、[匿名化 (Anonymization)] チェックボックスをオンにします。チェックボックスをオンにすると、フィールド名は、それぞれ <i>c-a-ip</i>、<i>cs-a-username</i>、および <i>cs-a-auth-group</i> に変更されます。</p> <p><b>Note</b></p> <p>ログ ファイルのプッシュ先である外部サーバが匿名化機能の処理に対応していない場合、匿名化を有効にしないでください。</p> <p>ログの作成後、必要に応じて匿名化したフィールドを非匿名化することができます。<a href="#">W3C ログ フィールドの非匿名化</a>, on page 682を参照してください</p> |

| オプション                                                               | 説明                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 匿名化のためのパスフレーズ<br>(Passphrase for Anonymization)<br><br>(W3C アクセスログ) | <p>フィールドの値を暗号化するためのパスフレーズを作成することができます。このエリアは、ログフィールド <i>c-ip</i>、<i>cs-username</i>、または <i>cs-auth-group</i> を匿名化することを選択している場合のみ有効化されます。</p> <p><b>Note</b><br/>システムは、匿名化のためのパスフレーズの設定中に、パスフレーズのルールを適用します。</p> <p>パスフレーズを自動的に生成するには、[パスフレーズの自動生成 (Auto Generate Passphrase)] の横のチェックボックスをオンにし、[生成する (Generate)] をクリックします。</p> <p><b>Note</b><br/>複数のアプライアンスがある場合は、すべてのアプライアンスに同じパスフレーズを設定する必要があります。</p> |
| ログの圧縮 (Log Compression)                                             | <p>ロールオーバー ファイルを圧縮するかどうかを指定します。AsyncOS は gzip 圧縮形式を使用してログ ファイルを圧縮します。</p>                                                                                                                                                                                                                                                                                                                               |
| ログ除外 (Log Exclusions) (オプション)<br>(アクセスログ)                           | <p>HTTP ステータスコード (4xx または 5xx のみ) を指定して、関連するトランザクションをアクセス ログまたは W3C アクセス ログから除外します。</p> <p>たとえば、401 を入力すると、そのトランザクション番号を持つ、認証に失敗した要求が除外されます。</p>                                                                                                                                                                                                                                                        |



| オプション                                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ログ レベル (Log Level)                         | <p>ログ エントリの詳細のレベルを設定します。次から選択します。</p> <ul style="list-style-type: none"> <li>• [クリティカル (Critical)]。エラーだけが記録されます。これは、最小限の設定であり、syslog レベルの [アラート (Alert)] と同等です。</li> <li>• [警告 (Warning)]。エラーと警告が記録されます。このログレベルは、syslog レベルの [警告 (Warning)] と同等です。</li> <li>• [情報 (Information)]。エラー、警告、および他のシステム操作が記録されます。これはデフォルトの詳細レベルであり、syslog レベルの [情報 (Information)] と同等です。</li> <li>• [デバッグ (Debug)]。システム問題のデバッグに役立つデータが記録されます。エラーの原因を調べるときは、Debug ログレベルを使用します。この設定は一時的に使用し、後でデフォルトレベルに戻します。このログレベルは、syslog レベルの [デバッグ (Debug)] と同等です。</li> <li>• [トレース (Trace)]。これは、詳細レベルの最も高い設定です。このレベルには、システム操作とアクティビティの完全な記録が含まれます。Trace ログレベルは、開発者にのみ推奨されます。このレベルを使用すると、システムのパフォーマンスが大きく低下するので、推奨されません。このログレベルは、syslog レベルの [デバッグ (Debug)] と同等です。</li> </ul> <p><b>Note</b><br/>詳細レベルの設定を高くするほど、作成されるログファイルが大きくなり、システム パフォーマンスに大きな影響を及ぼします。</p> |
| 取得方法 (Retrieval Method)                    | <p>ロール オーバー ログ ファイルを保存する場所と、閲覧用に取得する方法を指定します。利用可能な方法の説明については、下記を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 取得方法 :<br>アプライアンス上の FTP (FTP on Appliance) | <p>[アプライアンス上の FTP (FTP on Appliance)] 方式 (FTP ポーリングと同等) では、ログ ファイルを取得するために、管理者ユーザまたはオペレータ ユーザのユーザ名とパスワードを使用して、リモート FTP クライアントからアプライアンスにアクセスする必要があります。</p> <p>この方法を選択した場合、アプライアンスに保存するログファイルの最大数を入力する必要があります。最大数に達すると、最も古いファイルが削除されます。</p> <p>これは、デフォルトの取得方法です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| オプション                                                 | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>取得方法：<br/>リモートサーバでの FTP (FTP on Remote Server)</p> | <p>[リモートサーバでの FTP (FTP on Remote Server)] 方式 (FTP プッシュと同等) では、リモートコンピュータ上の FTP サーバに定期的にログファイルをプッシュします。</p> <p>この方法を選択した場合、以下の情報を入力する必要があります。</p> <ul style="list-style-type: none"> <li>• FTP サーバのホスト名</li> <li>• ログファイルを保存する FTP サーバのディレクトリ</li> <li>• FTP サーバに接続する権限を持つユーザのユーザ名とパスフレーズ</li> </ul> <p><b>Note</b><br/>AsyncOS for Web は、リモート FTP サーバのパッシブモードのみをサポートします。アクティブモードの FTP サーバにログファイルをプッシュできません。</p>                                                                                                                                        |
| <p>取得方法：<br/>リモートサーバでの SCP (SCP on Remote Server)</p> | <p>[リモートサーバでの SCP (SCP on Remote Server)] 方式 (SCP プッシュと同等) では、セキュアコピープロトコルを使用して、リモート SCP サーバに定期的にログファイルをプッシュします。この方法には、SSH2 プロトコルを使用するリモートコンピュータ上の SSH SCP サーバが必要です。サブスクリプションには、ユーザ名、SSH キー、およびリモートコンピュータ上の宛先ディレクトリが必要です。ログファイルは、ユーザが設定したロールオーバースケジュールに基づいて転送されます。</p> <p>この方法を選択した場合、以下の情報を入力する必要があります。</p> <ul style="list-style-type: none"> <li>• SCP サーバのホスト名</li> <li>• ログファイルを保存する SCP サーバのディレクトリ</li> <li>• SCP サーバに接続する権限を持つユーザのユーザ名</li> </ul> <p><b>Note</b><br/>現在は、非 FIPS モードの SSH-RSA と SSH-DSS、および FIPS モードの SSH-RSA のみがサポートされています。</p> |

| オプション                               | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 取得方法：<br>Syslog 送信<br>(Syslog Push) | <p>テキスト ベースのログの syslog のみを選択できます。</p> <p>[Syslog 送信 (Syslog Push)] 方式では、ポート 514 でリモート Syslog サーバにログ メッセージを送信します。この方法は、RFC 3164 に準拠しています。</p> <p>この方法を選択した場合、以下の情報を入力する必要があります。</p> <ul style="list-style-type: none"> <li>• Syslog サーバのホスト名</li> <li>• 転送に使用するプロトコル (UDP または TCP)</li> <li>• 最大メッセージ サイズ (Maximum message size)</li> </ul> <p>UDP で有効な値は 1024 ～ 9216 です。</p> <p>TCP で有効な値は 1024 ～ 65535 です。</p> <p>最大メッセージ サイズは syslog サーバの設定に応じて異なります。</p> <ul style="list-style-type: none"> <li>• ログで使用するファシリティ</li> </ul> |

**ステップ 4** 変更を送信し、保存します。

#### What to do next

取得方法として SCP を選択した場合は、アプライアンスによって SSH キーが表示されます。このキーを SCP サーバホストに追加します。[別のサーバへのログ ファイルのプッシュ, on page 683](#) を参照してください。

#### 関連項目

- [ログ ファイルのタイプ, on page 668](#)
- [ログのファイル名とアプライアンスのディレクトリ構造, on page 685](#)

## W3C ログ フィールドの非匿名化

ログ サブスクリプションの際にフィールド値 (*c-ip*、*cs-username*、および *cs-auth-group*) の匿名化機能をイネーブルにしていた場合、送信先のログ サーバは、これらのログ フィールドについて、実際の値ではなく匿名化された値 (*c-a-ip*、*cs-a-username*、および *cs-a-auth-group*) を受信します。実際の値を表示したい場合は、ログフィールドを非匿名化する必要があります。

W3C ログのサブスクリプションを追加する際に匿名化されたログ フィールド値 *c-a-ip*、*cs-a-username*、および *cs-a-auth-group* は、非匿名化できます。

## 手順

- 
- ステップ 1** [システム管理 (System Administration)] > [ログ サブスクリプション (Log Subscriptions)] を選択します。
- ステップ 2** 匿名化されたフィールドを非匿名化したいログの [非匿名化 (Deanonymization)] 列で、[非匿名化 (Deanonymization)] をクリックします。
- ステップ 3** [方法 (Method)] エリアで、暗号化されたテキストを非匿名化のために入力する方法として、次のいずれかを選択します。
- 暗号化されたテキストを貼り付ける：[匿名化されたテキスト (Anonymized Text)] フィールドに暗号化されたテキストのみを貼り付けます。このフィールドには、最大 500 エントリを入力できます。複数のエントリはカンマで区切る必要があります。
  - ファイルをアップロードする：暗号化されたテキストを含むファイルを選択します。ファイルには、最大 1000 エントリを含めることができます。ファイル形式は、CSV にする必要があります。システムは、フィールド区切り文字として、スペース、改行、タブ、およびセミコロンをサポートしています。
- (注)  
パスフレーズを変更した場合、それ以前のデータを非匿名化するには、以前のパスフレーズを入力する必要があります。
- ステップ 4** [非匿名化 (Deanonymization)] をクリックすると、非匿名化されたログ フィールド値が [非匿名化結果 (Deanonymization Result)] テーブルに表示されます。
- 

## 別のサーバへのログ ファイルのプッシュ

### Before you begin

必要なログ サブスクリプションを作成または編集し、取得方法として SCP を選択します。 [ログ サブスクリプションの追加および編集, on page 676](#)

### Procedure

- 
- ステップ 1** リモート システムにキーを追加します。
- CLI にアクセスします。
  - `logconfig -> hostkeyconfig` コマンドを入力します。
  - 以下のコマンドを使用してキーを表示します。

| コマンド | 説明                                                                                                                             |
|------|--------------------------------------------------------------------------------------------------------------------------------|
| Host | システム ホスト キーを表示します。これは、リモートシステムの「known_hosts」ファイルに記入される値です。                                                                     |
| User | リモートマシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモートシステムの「authorized_keys」ファイルに記入される値です。 |

d) これらのキーをリモート システムに追加します。

**ステップ 2** CLI で、リモート サーバの SSH 公開ホスト キーをアプライアンスに追加します。

| コマンド        | 説明                           |
|-------------|------------------------------|
| New         | 新しいキーを追加します。                 |
| Fingerprint | システム ホスト キーのフィンガープリントを表示します。 |

**ステップ 3** 変更を保存します。

## ログ ファイルのアーカイブ

AsyncOS は、最新のログ ファイルがユーザー指定の上限（最大ファイル サイズまたは最大時間）に達すると、ログ サブスクリプションをアーカイブ（ロールオーバー）します。

ログ サブスクリプションには以下のアーカイブ設定が含まれます。

- ファイル サイズ別ロールオーバー
- 時刻によりロールオーバー
- ログの圧縮
- 取得方法

また、ログ ファイルを手動でアーカイブ（ロールオーバー）することもできます。

### Procedure

**ステップ 1** [システム管理（System Administration）]>[ログ サブスクリプション（Log Subscriptions）]を選択します。

**ステップ 2** アーカイブするログ サブスクリプションの[ロールオーバー（Rollover）]列のチェックボックスをオンにするか、[すべて（All）]をオンにしてすべてのサブスクリプションを選択します。

**ステップ 3** [今すぐロールオーバー（Rollover Now）]をクリックして、選択したログをアーカイブします。

## What to do next

### 関連項目

- [ログ サブスクリプションの追加および編集, on page 676](#)
- [ログのファイル名とアプライアンスのディレクトリ構造, on page 685](#)

# ログのファイル名とアプライアンスのディレクトリ構造

アプライアンスは、ログサブスクリプション名に基づいてログサブスクリプションごとにディレクトリを作成します。ディレクトリ内のログ ファイル名は、以下の情報で構成されます。

- ログ サブスクリプションで指定されたログ ファイル名
- ログ ファイルが開始された時点のタイムスタンプ
- .c (「current (現在)」を表す)、または .s (「saved (保存済み)」を表す) のいずれかを示す単一文字ステータス コード

ログのファイル名は、以下の形式で作成されます。

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```



**Note** 保存済みのステータスのログ ファイルのみを転送する必要があります。

## ログ ファイルの閲覧と解釈

Secure Web Applianceをモニタしてトラブルシューティングする手段として、現在のログ ファイルのアクティビティを確認できます。これを行うには、アプライアンスのインターフェイスを使用します。

また、過去のアクティビティの記録についてアーカイブファイルを閲覧することもできます。アーカイブ ファイルがアプライアンスに保存されている場合は、アプライアンスのインターフェイスから閲覧できます。それ以外の場合は、適切な方法で外部ストレージの場所から読み取る必要があります。

ログファイルの各情報項目は、フィールド変数によって示されます。どのフィールドがどの情報項目を表しているのかを判別することにより、フィールドの機能を調べて、ログファイルの内容を解釈できます。W3C 準拠のアクセス ログの場合は、ファイルヘッダーに、ログに表示される順でフィールド名がリストされます。しかし、標準のアクセス ログの場合は、このログタイプに関するドキュメントを参照して、フィールドの順序について調べる必要があります。

### 関連項目

- [ログ ファイルの表示, on page 686。](#)
- [アクセス ログ ファイル内の Web プロキシ情報, on page 686。](#)
- [W3C アクセス ログの解釈, on page 712。](#)
- [トラフィック モニタ ログの解釈, on page 720。](#)

- [ログ ファイルのフィールドとタグ, on page 721](#)。

## ログ ファイルの表示

### Before you begin

ここでは、アプライアンス上に保存されているログ ファイルの表示方法について説明します。外部に格納されているファイルの表示方法については、このマニュアルでは説明しません。

### Procedure

- ステップ 1** [システム管理 (System Administration)] > [ログ サブスクリプション (Log Subscriptions)] を選択します。
- ステップ 2** ログ サブスクリプション リストの [ログ ファイル (Log Files)] 列にあるログ サブスクリプション名をクリックします。
- ステップ 3** プロンプトが表示されたら、アプライアンスにアクセスするための管理者のユーザ名とパスワードを入力します。
- ステップ 4** ログインしたら、ログ ファイルのいずれかをクリックして、ブラウザで表示するか、またはディスクに保存します。
- ステップ 5** 最新の結果を表示するには、ブラウザの表示を更新します。

### Note

ログ サブスクリプションが圧縮されている場合は、ダウンロードし、復元してから開きます。

### What to do next

#### 関連項目

- [アクセス ログ ファイル内の Web プロキシ情報, on page 686](#)。
- [W3C アクセス ログの解釈, on page 712](#)。
- [トラフィック モニタ ログの解釈, on page 720](#)。

## アクセス ログ ファイル内の Web プロキシ情報

アクセス ログ ファイルには、すべての Web プロキシフィルタリングとスキャン アクティビティに関する記述が含まれています。アクセス ログ ファイル エントリは、アプライアンスが各トランザクションを処理した方法を表示します。

アクセス ログには 2 つの形式（標準および W3C 準拠）があります。W3C 準拠のログ ファイルは、標準のアクセス ログよりも記録内容とレイアウトをさらにカスタマイズできます。

以下のテキストは、1つのトランザクションに対するアクセス ログ ファイル エントリの例を示します。

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE 11-PolicyGroupName-Identity-
OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy-NONE
<IW_comp,6.9,-,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,-,-,IW_comp,-,-,"-",-,-,
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f1led9c98253d85829614fba368a421d14e64c426da5e">
-
```

| フォーマット指定子  | フィールド値                  | フィールドの説明                                                                                                                                                                                    |
|------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %t         | 1278096903.150          | UNIX エポック以降のタイムスタンプ。                                                                                                                                                                        |
| %e         | 97                      | 経過時間（遅延）（ミリ秒単位）。                                                                                                                                                                            |
| %a         | 172.xx.xx.xx            | クライアント IP アドレス。<br><br>注：advancedproxyconfig > authentication CLI コマンドを使用して、アクセスログの IP アドレスをマスクするように選択できます。                                                                                 |
| %w         | TCP_MISS                | トランザクション結果コード。<br><br>詳細については、 <a href="#">W3C 準拠のアクセスログファイル, on page 712</a> を参照してください。                                                                                                    |
| %h         | 200                     | HTTP 応答コード。                                                                                                                                                                                 |
| %s         | 8187                    | 応答サイズ（ヘッダー + 本文）。                                                                                                                                                                           |
| %lr<br>%2r | GET http://my.site.com/ | 要求の先頭行。<br><br>注：要求の先頭行がネイティブ FTP トランザクション用の場合、ファイル名の一部の特殊文字はアクセスログでは符号化された URL を表します。たとえば、「@」記号は、アクセスログに「%40」として書き込まれます。<br><br>以下の文字が符号化された URL に使用されます。<br><br>& # % + , ; = @ ^ { } [ ] |



| フォーマット指定子 | フィールド値      | フィールドの説明                                                                                                                                                                                                                                                                                                                                                   |
|-----------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %A        | —           | <p>認証されたユーザ名。</p> <p><b>注：</b> <code>advancedproxyconfig &gt; authentication CLI</code> コマンドを使用して、アクセスログのユーザ名をマスクするように選択できます。</p>                                                                                                                                                                                                                          |
| %H        | DIRECT      | <p>要求コンテンツを取得するために接続されたサーバを説明するコード。</p> <p>最も一般的な値は以下のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>NONE。</b> Web プロキシにコンテンツが含まれていたため、コンテンツを取得するために他のサーバに接続されませんでした。</li> <li>• <b>DIRECT。</b> Web プロキシは、コンテンツを取得するための要求で指定されたサーバに移行しました。</li> <li>• <b>DEFAULT_PARENT。</b> Web プロキシは、コンテンツを取得するためにプライマリペアレントプロキシまたは外部 DLP サーバに移行しました。</li> </ul> |
| %d        | my.site.com | データ ソースまたはサーバの IP アドレス。                                                                                                                                                                                                                                                                                                                                    |
| %c        | text/plain  | 応答本文の MIME タイプ。                                                                                                                                                                                                                                                                                                                                            |

| フォーマット指定子             | フィールド値                        | フィールドの説明                                                                                                                                                                      |
|-----------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %D                    | DEFAULT_CASE_11               | <p>ACL デシジョン タグ。</p> <p>注：ACL デシジョン タグの末尾に、Web プロキシが内部的に使用する動的に生成された数値が含まれます。この数値は無視できます。</p> <p>詳細については、<a href="#">ACL デシジョン タグ, on page 692</a>を参照してください。</p>              |
| N/A (ACL デシジョン タグの一部) | PolicyGroupName               | <p>このトランザクションについて最終決定を行うポリシーグループの名前（アクセスポリシー、復号ポリシー、またはデータセキュリティポリシー）。トランザクションがグローバル ポリシーに一致する場合、この値は「DefaultGroup」になります。</p> <p>ポリシーグループ名のスペースは、アンダースコア ( _ ) に置き換えられます。</p> |
| N/A (ACL デシジョン タグの一部) | ID (Identity)                 | <p>ID ポリシー グループの名前。</p> <p>ポリシーグループ名のスペースは、アンダースコア ( _ ) に置き換えられます。</p>                                                                                                       |
| N/A (ACL デシジョン タグの一部) | OutboundMalwareScanningPolicy | <p>発信マルウェア スキャンポリシー グループの名前。</p> <p>ポリシーグループ名のスペースは、アンダースコア ( _ ) に置き換えられます。</p>                                                                                              |

| フォーマット指定子                | フィールド値             | フィールドの説明                                                                                                                                                                                                                                                                                                                    |
|--------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| N/A (ACL デシジョン<br>タグの一部) | DataSecurityPolicy | <p>Cisco データ セキュリティ ポリ<br/>シー グループの名前。トランザ<br/>クションがグローバルな Cisco<br/>データ セキュリティ ポリシー<br/>に一致する場合、この値は<br/>「DefaultGroup」になります。<br/>このポリシー グループ名は、<br/>Cisco データ セキュリティ フィ<br/>ルタが有効な場合にのみ表示さ<br/>れます。データ セキュリティ<br/>ポリシーに一致しなかった場合<br/>は、「NONE」と表示されま<br/>す。</p> <p>ポリシー グループ名のスペース<br/>は、アンダースコア ( _ ) に置<br/>き換えられます。</p> |
| N/A (ACL デシジョン<br>タグの一部) | ExternalDLPPolicy  | <p>外部 DLP ポリシー グループの<br/>名前。トランザクションがグ<br/>ローバル外部 DLP ポリシーに一<br/>致する場合、この値は<br/>「DefaultGroup」になります。<br/>外部 DLP ポリシーに一致しな<br/>かった場合は、「NONE」と表<br/>示されます。</p> <p>ポリシー グループ名のスペース<br/>は、アンダースコア ( _ ) に置<br/>き換えられます。</p>                                                                                                     |
| N/A (ACL デシジョン<br>タグの一部) | RoutingPolicy      | <p>ルーティング ポリシー グルー<br/>プ名は<br/><i>ProxyGroupName/ProxyServerName</i>。</p> <p>トランザクションがグローバル<br/>ルーティングポリシーに一致す<br/>る場合、この値は<br/>「DefaultRouting」になります。<br/>アップストリームプロキシサー<br/>バを使用しない場合、この値は<br/>「DIRECT」になります。</p> <p>ポリシー グループ名のスペース<br/>は、アンダースコア ( _ ) に置<br/>き換えられます。</p>                                              |

| フォーマット指定子                                                                     | フィールド値                                                                                                                                                                                                                                                                                      | フィールドの説明                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %Xr                                                                           | <IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,<br>"-",-,-,"-","-",-,-,IW_comp,<br>-,"-","-",<br>"Unknown","Unknown","-","-",<br>198.34,0,-,[Local],"-",37,<br>"W32.CiscoTestVector",33,0,<br>"WSA-INFECTED-FILE.pdf",<br>"fd5ef49d4213e05f448f11ed<br>9c98253d85829614fba368a4<br>21d14e64c426da5e"> | <p>スキャン判定情報。アクセスログでは、山カッコ内にさまざまなスキャンエンジンの判定情報が含まれています。</p> <p><b>Note</b><br/>AsyncOS バージョン 11.8 以降では、URL カテゴリ識別子が二重引用符で囲まれて表示されます。たとえば、“IW_comp”と表示されます。</p> <p>山カッコ内の値の詳細については、<a href="#">アクセスログのスキャン判定エントリの解釈, on page 703</a>および<a href="#">マルウェア スキャンの判定値, on page 737</a>を参照してください。</p> |
| %%?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<<br>User-Agent:%!%-% | -                                                                                                                                                                                                                                                                                           | 不審なユーザ エージェント。                                                                                                                                                                                                                                                                                 |

## トランザクション結果コード

アクセス ログ ファイルのトランザクション結果コードは、アプライアンスがクライアント要求を解決する方法を示します。たとえば、オブジェクトの要求がキャッシュから解決可能な場合、結果コードは TCP\_HIT です。ただし、オブジェクトがキャッシュに存在せず、アプライアンスが元のサーバからオブジェクトをプルする場合、結果コードは TCP\_MISS です。以下の表に、トランザクション結果コードを示します。

| 結果コード       | 説明                                                                                     |
|-------------|----------------------------------------------------------------------------------------|
| TCP_HIT     | 要求されたオブジェクトがディスク キャッシュから取得されました。                                                       |
| TCP_IMS_HIT | クライアントがオブジェクトの IMS (If-Modified-Since) 要求を送信し、オブジェクトがキャッシュ内で見つかりました。プロキシは 304 応答を返します。 |
| TCP_MEM_HIT | 要求されたオブジェクトがメモリ キャッシュから取得されました。                                                        |

| 結果コード                   | 説明                                                                                                                                                      |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| TCP_MISS                | オブジェクトがキャッシュ内で見つからなかったため、元のサーバから取得されました。                                                                                                                |
| TCP_REFRESH_HIT         | オブジェクトはキャッシュ内にありましたが、期限切れでした。プロキシが元のサーバに IMS (If-Modified-Since) 要求を送信し、サーバはオブジェクトが変更されていないことを確認しました。そのため、アプライアンスはディスクまたはメモリ キャッシュのいずれかからオブジェクトを取得しました。 |
| TCP_CLIENT_REFRESH_MISS | クライアントが「Pragma: no-cache」ヘッダーを発行して、「don't fetch response from cache」要求を送信しました。クライアントから送信されたこのヘッダーにより、アプライアンスは元のサーバからオブジェクトを取得しました。                      |
| TCP_DENIED              | クライアント要求がアクセスポリシーによって拒否されました。                                                                                                                           |
| UDP_MISS                | オブジェクトは発信サーバから取得されました。                                                                                                                                  |
| NONE                    | トランザクションでエラーが発生しました。DNS 障害やゲートウェイのタイムアウトなど。                                                                                                             |

## ACL デシジョン タグ

ACL デシジョン タグは、Web プロキシがトランザクションを処理した方法を示すアクセス ログ エントリのフィールドです。Web レピュテーション フィルタ、URL カテゴリ、およびスキャン エンジンの情報が含まれます。



**Note** ACL デシジョン タグの末尾に、Web プロキシがパフォーマンスを高めるために内部的に使用する動的に生成された数値が含まれます。この数値は無視できます。

以下の表は、ACL デシジョン タグの値を示しています。

| ACL デシジョン タグ           | 説明                                                                    |
|------------------------|-----------------------------------------------------------------------|
| ALLOW_ADMIN_ERROR_PAGE | Web プロキシが、通知ページとそのページで使用する任意のロゴへのトランザクションを許可しました。                     |
| ALLOW_CUSTOMCAT        | Web プロキシが、アクセス ポリシー グループのカスタム URL カテゴリ フィルタリング設定に基づいてトランザクションを許可しました。 |
| ALLOW_REFERER          | Web プロキシが、埋め込み/参照コンテンツの免除に基づいてトランザクションを許可しました。                        |

| ACL デシジョン タグ     | 説明                                                                                                                                                                   |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ALLOW_WBRS       | Web プロキシが、アクセス ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションを許可しました。                                                                                                   |
| AMP_FILE_VERDICT | <p>ファイルに対する AMP レピュテーションサーバーからの判定を表す値です。</p> <ul style="list-style-type: none"> <li>• 1 : 不明</li> <li>• 2 : 正常</li> <li>• 3 : 悪意がある</li> <li>• 4 : スキャン不可</li> </ul> |

| ACL デシジョン タグ                | 説明 |
|-----------------------------|----|
| ARCHIVESCAN_ALLCLEAR        |    |
| ARCHIVESCAN_BLOCKEDFILETYPE |    |
| ARCHIVESCAN_NESTEDTOODEEP   |    |
| ARCHIVESCAN_UNKNOWNFMT      |    |
| ARCHIVESCAN_UNSCANABLE      |    |
| ARCHIVESCAN_FILETOOBIG      |    |

| ACL デシジョン タグ | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | <p><b>アーカイブ スキャンの判定</b></p> <p>ARCHIVESCAN_ALLCLEAR：検査したアーカイブ内にブロックされたファイル タイプはありません。</p> <p>ARCHIVESCAN_BLOCKEDFILETYPE：検査したアーカイブ内にブロックされたファイル タイプがふくまれています。ログ エントリ ([Verdict Detail]) の次のフィールドに、ブロックされたファイルのタイプ、ブロックされたファイルの名前などの詳細が示されています。</p> <p>ARCHIVESCAN_NESTEDTOODEEP：アーカイブに設定された最大値を超える数の「カプセル化」されたアーカイブまたはネストされたアーカイブが含まれているため、アーカイブはブロックされます。[Verdict Detail] フィールドに「UnScanable Archive-Blocked」が含まれています。</p> <p>ARCHIVESCAN_UNKNOWNFMT：アーカイブに不明な形式のファイル タイプが含まれているため、アーカイブはブロックされます。[Verdict Detail] フィールドの値は「UnScanable Archive-Blocked」です。</p> <p>ARCHIVESCAN_UNSCANABLE：アーカイブにスキャンできないファイルが含まれているため、アーカイブはブロックされます。[Verdict Detail] フィールドの値は「UnScanable Archive-Blocked」です。</p> <p>ARCHIVESCAN_FILETOOBIG：アーカイブのサイズが設定された最大値を超えているため、アーカイブはブロックされます。[Verdict Detail] フィールドの値は「UnScanable Archive-Blocked」です。</p> <p><b>アーカイブ スキャン判定の詳細</b></p> <p>ログ エントリの [Verdict] フィールドの次のフィールドには、ブロックされたファイルのタイプやブロックされたファイルの名前、ブロックされたファイル タイプがアーカイブに含まれていないことを示す「UnScanable Archive-Blocked」や「-」など、判定に関する追加情報が示されています。</p> <p>たとえば、検査可能なアーカイブファイルが「アクセス ポリシー：カスタム オブジェクト ブロック」の設定に基づいてブロックされている場合</p> <p>(ARCHIVESCAN_BLOCKEDFILETYPE)、[Verdict Detail] エントリにはブロックされたファイルのタイプ、およびブロックされたファイルの名前が含まれています。</p> <p>アーカイブ 検査の詳細については、<a href="#">アクセス ポリシー：オブジェクトのブロッキング, on page 380</a>およびアーカイブ 検</p> |



| ACL デシジョン タグ                          | 説明                                                                                                                                                                       |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                       | <a href="#">査の設定, on page 384</a> を参照してください。                                                                                                                             |
| BLOCK_ADC                             | アクセス ポリシー グループの設定されたアプリケーション設定に基づいてトランザクションがブロックされました。                                                                                                                   |
| BLOCK_ADMIN                           | アクセス ポリシー グループのデフォルト設定に基づいてトランザクションがブロックされました。                                                                                                                           |
| BLOCK_ADMIN_CONNECT                   | アクセス ポリシー グループの HTTP CONNECT ポート設定で定義された宛先の TCP ポートに基づいてトランザクションがブロックされました。                                                                                              |
| BLOCK_ADMIN_CUSTOM_USER_AGENT         | アクセス ポリシー グループの [ブロックするユーザーエージェント (Block Custom User Agents) ] 設定で定義されたユーザーエージェントに基づいてトランザクションがブロックされました。                                                                |
| BLOCK_ADMIN_TUNNELING                 | Web プロキシは、アクセス ポリシー グループの HTTP ポート上の非 HTTP トラフィックのトンネリングに基づいてトランザクションをブロックしました。                                                                                          |
| BLOCK_ADMIN_HTTPS_NonLocalDestination | トランザクションがブロックされました。クライアントは、SSL ポートを明示的なプロキシとして使用して認証をバイパスしようとしてしました。これを防ぐために、SSL 接続が Secure Web Appliance 自体に向けられている場合、実際の Secure Web Appliance リダイレクトホスト名への要求だけが許可されます。 |
| BLOCK_ADMIN_IDS                       | データセキュリティポリシーグループで定義された要求本文のコンテンツの MIME タイプに基づいてトランザクションがブロックされました。                                                                                                      |
| BLOCK_ADMIN_FILE_TYPE                 | アクセスポリシーグループで定義されたファイルタイプに基づいてトランザクションがブロックされました。                                                                                                                        |
| BLOCK_ADMIN_PROTOCOL                  | アクセス ポリシー グループの [ブロックするプロトコル (Block Protocols) ] 設定で定義されたプロトコルに基づいてトランザクションがブロックされました。                                                                                   |
| BLOCK_ADMIN_SIZE                      | アクセス ポリシー グループの [オブジェクトサイズ (Object Size) ] 設定で定義された応答のサイズに基づいてトランザクションがブロックされました。                                                                                        |
| BLOCK_ADMIN_SIZE_IDS                  | データセキュリティポリシーグループで定義された要求本文のコンテンツのサイズに基づいてトランザクションがブロックされました。                                                                                                            |

| ACL デシジョン タグ                  | 説明                                                                                                                                                                       |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BLOCK_AMP_RESP                | Web プロキシが、アクセスポリシーグループの <b>Advanced Malware Protection</b> 設定に基づいて応答をブロックしました。                                                                                           |
| BLOCK_AMW_REQ                 | Web プロキシが、発信マルウェア スキャンポリシー グループの <b>Anti-Malware</b> 設定に基づいて要求をブロックしました。要求の本文はポジティブなマルウェアの判定を生成しました。                                                                     |
| BLOCK_AMW_RESP                | Web プロキシが、アクセスポリシーグループの <b>Anti-Malware</b> 設定に基づいて応答をブロックしました。                                                                                                          |
| BLOCK_AMW_REQ_URL             | Web プロキシが HTTP 要求の URL が安全ではないと疑い、アクセス ポリシー グループの <b>Anti-Malware</b> 設定に基づいて要求時にトランザクションをブロックしました。                                                                      |
| BLOCK_AVC                     | アクセス ポリシー グループの設定されたアプリケーション設定に基づいてトランザクションがブロックされました。                                                                                                                   |
| BLOCK_CONTENT_UNSAFE          | アクセス ポリシー グループのサイト コンテンツ レーティング設定に基づいてトランザクションがブロックされました。クライアント要求はアダルト コンテンツに対するものであり、ポリシーはアダルト コンテンツをブロックするように設定されています。                                                 |
| BLOCK_CONTINUE_CONTENT_UNSAFE | アクセス ポリシー グループのサイト コンテンツ レーティング設定に基づいてトランザクションがブロックされ、[警告して継続 (Warn and Continue)] ページが表示されました。クライアント要求はアダルト コンテンツに対するものであり、ポリシーはアダルトコンテンツにアクセスするユーザに警告を表示するように設定されています。 |
| BLOCK_CONTINUE_CUSTOMCAT      | [警告 (Warn)] に設定されているアクセスポリシー グループのカスタム URL カテゴリに基づいてトランザクションがブロックされ、[警告して継続 (Warn and Continue)] ページが表示されました。                                                            |
| BLOCK_CONTINUE_WEBCAT         | [警告 (Warn)] に設定されているアクセスポリシー グループの定義済み URL カテゴリに基づいてトランザクションがブロックされ、[警告して継続 (Warn and Continue)] ページが表示されました。                                                            |
| BLOCK_CUSTOMCAT               | アクセス ポリシー グループのカスタム URL カテゴリ フィルタリング設定に基づいてトランザクションがブロックされました。                                                                                                           |

| ACL デシジョン タグ                 | 説明                                                                                                                         |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| BLOCK_ICAP                   | Web プロキシが、外部 DLP ポリシー グループで定義された外部 DLP システムの判定に基づいて要求をブロックしました。                                                            |
| BLOCK_SEARCH_UNSAFE          | クライアント要求には危険な検索クエリーが含まれており、アクセス ポリシーは安全検索を実行するように設定されているので、元のクライアント要求がブロックされました。                                           |
| BLOCK_SUSPECT_USER_AGENT     | アクセス ポリシー グループの [疑わしいユーザエージェント (Suspect User Agent) ] 設定に基づいてトランザクションがブロックされました。                                           |
| BLOCK_UNSUPPORTED_SEARCH_APP | アクセス ポリシー グループの安全検索設定に基づいてトランザクションがブロックされました。トランザクションはサポートされない検索エンジンに対するものであり、ポリシーはサポートされない検索エンジンをブロックするように設定されています。       |
| BLOCK_WBRS                   | アクセス ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションがブロックされました。                                                                |
| BLOCK_WBRS_IDS               | Web プロキシが、Data Security ポリシー グループの Web レピュテーション フィルタ設定に基づいてアップロード要求をブロックしました。                                              |
| BLOCK_WEBCAT                 | アクセス ポリシー グループの URL カテゴリ フィルタリング設定に基づいてトランザクションがブロックされました。                                                                 |
| BLOCK_WEBCAT_IDS             | Web プロキシが、Data Security ポリシー グループの URL カテゴリ フィルタリング設定に基づいてアップロード要求をブロックしました。                                               |
| BLOCK_YTCAT                  | Web プロキシが、アクセスポリシーグループに事前設定された YouTube カテゴリのフィルタ処理設定に基づいてトランザクションをブロックしました。                                                |
| BLOCK_CONTINUE_YTCAT         | Web プロキシが、[警告 (Warn) ] に設定されているアクセスポリシーグループの定義済み YouTube カテゴリに基づいてトランザクションをブロックし、[警告して継続 (Warn and Continue) ] ページを表示しました。 |
| DECRYPT_ADMIN                | Web プロキシが、復号ポリシー グループのデフォルト設定に基づいてトランザクションを復号しました。                                                                         |

| ACL デシジョン タグ                             | 説明                                                                                                       |
|------------------------------------------|----------------------------------------------------------------------------------------------------------|
| DECRYPT_ADMIN_EXPIRED_CERT               | サーバ証明書が失効していますが、Web プロキシがトランザクションを復号しました。                                                                |
| DECRYPT_EUN_ADMIN_DEFAULT_ACTION         | EUN が有効な場合の復号ポリシーグループのドロップ接続として、デフォルト設定に基づき、Web プロキシがトランザクションを復号しました。                                    |
| DECRYPT_EUN_ADMIN_EXPIRED_CERT           | HTTPS プロキシ設定が、EUN が有効になっている期限切れの証明書をドロップすると、Web プロキシがトランザクションを復号しました。                                    |
| DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT      | HTTPS プロキシ設定が、EUN が有効になっている無効の証明書をドロップすると、Web プロキシがトランザクションを復号しました。                                      |
| DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME    | HTTPS プロキシ設定が、EUN が有効になっている不一致のホスト名をドロップすると、Web プロキシがトランザクションを復号しました。                                    |
| DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR       | HTTPS プロキシ設定が、EUN が有効になっているその他のエラーをもつ OCSP をドロップすると、Web プロキシがトランザクションを復号しました。                            |
| DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT      | HTTPS プロキシ設定が、EUN が有効になっている OCSP が失効した証明書をドロップすると、Web プロキシがトランザクションを復号しました。                              |
| DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT | HTTPS プロキシ設定が、認識できないルート権限または EUN が有効になっている発行者の証明書をドロップすると、Web プロキシがトランザクションを復号しました。                      |
| DECRYPT_EUN_CUSTOMCAT                    | Web プロキシが、復号ポリシーグループの URL カテゴリフィルタリング設定に基づいてトランザクションを復号しました。EUN が有効になっている場合、トラフィックはドロップされます。             |
| DECRYPT_EUN_WBRS                         | Web プロキシが、復号ポリシーグループの Web レピュテーションフィルタ設定に基づいてトランザクションを復号しました。EUN が有効になっている場合、トラフィックはドロップされます。            |
| DECRYPT_EUN_WBRS_NO_SCORE                | Web プロキシが、復号ポリシーグループのスコアなし URL の Web レピュテーションフィルタ設定に基づいてトランザクションを復号しました。EUN が有効になっている場合、トラフィックはドロップされます。 |

| ACL デシジョン タグ               | 説明                                                                                                                         |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| DECRYPT_EUN_WEBCAT         | Web プロキシが、復号ポリシーグループの URL カテゴリ フィルタリング設定に基づいてトランザクションを復号しました。EUN が有効になっている場合、トラフィックはドロップされます。                              |
| DECRYPT_WEBCAT             | Web プロキシが、復号ポリシー グループの URL カテゴリ フィルタリング設定に基づいてトランザクションを復号しました。                                                             |
| DECRYPT_WBRS               | Web プロキシが、復号ポリシーグループの Web レピュテーションフィルタ設定に基づいてトランザクションを復号しました。                                                              |
| DEFAULT_CASE               | AsyncOS サービスが Web レピュテーションやアンチマルウェアスキャンなど、トランザクションで処理を行わなかったため、Web プロキシがクライアントにサーバへのアクセスを許可しました。                           |
| DENY_ADMIN                 | Web プロキシがトランザクションを拒否しました。これは、HTTPS 要求に関して、認証が必要が場合に、HTTPS プロキシ設定で [認証のための復号 (Decrypt for Authentication)] が無効になっていると発生します。 |
| DROP_ADMIN                 | Web プロキシが、復号ポリシー グループのデフォルト設定に基づいてトランザクションをドロップしました。                                                                       |
| DROP_ADMIN_EXPIRED_CERT    | サーバ証明書が失効しているため、Web プロキシがトランザクションをドロップしました。                                                                                |
| DROP_WEBCAT                | Web プロキシが、復号ポリシー グループの URL カテゴリ フィルタリング設定に基づいてトランザクションをドロップしました。                                                           |
| DROP_WBRS                  | Web プロキシが、復号ポリシー グループの Web レピュテーションフィルタ設定に基づいてトランザクションをドロップしました。                                                           |
| MONITOR_ADC                | Web プロキシが、アクセスポリシー グループのアプリケーション設定に基づいてトランザクションをモニタしました。                                                                   |
| MONITOR_ADMIN_EXPIRED_CERT | サーバ証明書が失効しているため、Web プロキシがサーバ応答をモニタしました。                                                                                    |
| MONITOR_AMP_RESP           | Web プロキシが、アクセスポリシーグループの Advanced Malware Protection 設定に基づいてサーバ応答をモニタしました。                                                  |

| ACL デシジョン タグ                    | 説明                                                                                                                                                                                                                                                   |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MONITOR_AMW_RESP                | Web プロキシが、アクセス ポリシー グループの Anti-Malware 設定に基づいてサーバ応答をモニタしました。                                                                                                                                                                                         |
| MONITOR_AMW_RESP_URL            | Web プロキシが HTTP 要求の URL が安全ではないと疑っていますが、アクセス ポリシー グループの Anti-Malware 設定に基づいてトランザクションをモニタしました。                                                                                                                                                         |
| MONITOR_AVC                     | Web プロキシが、アクセス ポリシー グループのアプリケーション設定に基づいてトランザクションをモニタしました。                                                                                                                                                                                            |
| MONITOR_CONTINUE_CONTENT_UNSAFE | 任意で、Web プロキシが、アクセス ポリシー グループのサイト コンテンツ レーティング設定に基づいてトランザクションをブロックし、[警告して継続 (Warn and Continue)] ページを表示しました。クライアント要求はアダルト コンテンツに対するものであり、ポリシーはアダルト コンテンツにアクセスするユーザに警告を表示するように設定されています。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャン エンジンには要求をブロックしませんでした。 |
| MONITOR_CONTINUE_CUSTOMCAT      | 当初、Web プロキシは、[警告 (Warn)] に設定されているアクセス ポリシー グループのカスタム URL カテゴリに基づいて、トランザクションをブロックし、[警告して継続 (Warn and Continue)] ページを表示しました。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャン エンジンには要求をブロックしませんでした。                                                            |
| MONITOR_CONTINUE_WEBCAT         | 当初、Web プロキシは、[警告 (Warn)] に設定されているアクセス ポリシー グループの定義済み URL カテゴリに基づいて、トランザクションをブロックし、[警告して継続 (Warn and Continue)] ページを表示しました。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャン エンジンには要求をブロックしませんでした。                                                            |
| MONITOR_CONTINUE_YTCAT          | 当初、Web プロキシが、[警告 (Warn)] に設定されたアクセスポリシーグループの定義済み YouTube カテゴリに基づいてトランザクションをブロックし、[警告して継続 (Warn and Continue)] ページを表示しました。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャンエンジンは要求をブロックしませんでした。                                                               |

| ACL デシジョン タグ                | 説明                                                                                                                  |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------|
| MONITOR_IDS                 | Web プロキシが、データセキュリティ ポリシーまたは外部 DLP ポリシーのいずれかを使用してアップロード要求をスキャンしましたが、要求をブロックしませんでした。Web プロキシは、アクセス ポリシーに対して要求を評価しました。 |
| MONITOR_SUSPECT_USER_AGENT  | Web プロキシが、アクセス ポリシー グループの Suspect User Agent 設定に基づいてトランザクションをモニタしました。                                               |
| MONITOR_WBRS                | Web プロキシが、アクセス ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションをモニタしました。                                                 |
| NO_AUTHORIZATION            | ユーザが、ある認証レムに対して認証済みであったが、アプリケーション認証ポリシーに設定されている認証レムに対して未認証であったため、Web プロキシはアプリケーションへのユーザ アクセスを許可しませんでした。             |
| NO_PASSWORD                 | ユーザが認証に失敗しました。                                                                                                      |
| PASSTHRU_ADMIN              | Web プロキシが、復号ポリシー グループのデフォルト設定に基づいてトランザクションをパススルーしました。                                                               |
| PASSTHRU_ADMIN_EXPIRED_CERT | サーバ証明書が失効していますが、Web プロキシがトランザクションをパススルーしました。                                                                        |
| PASSTHRU_WEBCAT             | Web プロキシが、復号ポリシー グループの URL カテゴリ フィルタリング設定に基づいてトランザクションをパススルーしました。                                                   |
| PASSTHRU_WBRS               | Web プロキシが、復号ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションをパススルーしました。                                                  |
| REDIRECT_CUSTOMCAT          | Web プロキシが、[リダイレクト (Redirect)] に設定されているアクセス ポリシー グループのカスタム URL カテゴリに基づいて、トランザクションを別の URL にリダイレクトしました。                |
| SAAS_AUTH                   | ユーザが、アプリケーション認証ポリシーに設定されている認証レムに対して透過的に認証されていたため、Web プロキシはそのユーザがアプリケーションにアクセスすることを許可しました。                           |

| ACL デシジョン タグ | 説明                                                        |
|--------------|-----------------------------------------------------------|
| OTHER        | 認可の失敗、サーバの切断、クライアントによる中止などのエラーにより、Web プロキシが要求を完了できませんでした。 |

## アクセス ログのスキャン判定エントリの解釈

アクセス ログ ファイル エントリは、URL フィルタリング、Web レピュテーション フィルタリング、アンチマルウェア スキャンなど、さまざまなスキャン エンジンの結果を集約して表示します。アプライアンスは、各アクセス ログ エントリの末尾の山カッコ内にこの情報を表示します。

以下のテキストは、アクセス ログ ファイル エントリからのスキャン判定情報です。この例では、Webroot スキャン エンジンがマルウェアを検出しました。

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,"-",-,-,-,"-",-,-,"-",-,-,-,-,
IW_infr,-,"Trojan Phisher","-","-","Unknown","Unknown","-","-",489.73,0,

[Local],"-","-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf",

"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e",

ARCHIVESCAN_BLOCKEDFILETYPE,

EXT_ARCHIVESCAN_VERDICT,

EXT_ARCHIVESCAN_THREATDETAIL,

EXT_WTT_BEHAVIOR,
EXT_YTCAT,
"BlockedFileType: application/x-rpm,
BlockedFile: allfiles/linuxpackage.rp">
```



**Note** すべてのアクセス ログ ファイル エントリの例については、[アクセス ログ ファイル内の Web プロキシ情報, on page 686](#)を参照してください。

この例の各要素は、以下の表に示すログ ファイル フォーマット指定子に対応しています。

| 位置 | フィールド値  | フォーマット 指定子 | 説明                                                                        |
|----|---------|------------|---------------------------------------------------------------------------|
| 1  | IW_infr | %XC        | トランザクションに割り当てられたカスタム URL カテゴリ (省略形)。カテゴリが割り当てられない場合、このフィールドには「nc」が表示されます。 |



| 位置 | フィールド値                 | フォーマット<br>指定子 | 説明                                                                                                                                   |
|----|------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------|
| 2  | ns                     | %XW           | Web レピュテーションフィルタ スコア。このフィールドには、スコアの数値、「ns」（スコアがない場合）、または「dns」（DNSルックアップエラーがある場合）が表示されます。                                             |
| 3  | 24                     | %Xv           | Webroot が DVS エンジンに渡したマルウェア スキャンの判定。Webroot でのみ検出された応答に適用します。<br><br>詳細については、 <a href="#">マルウェア スキャンの判定値, on page 737</a> を参照してください。 |
| 4  | "Trojan-Phisher-Gamec" | "%Xn"         | オブジェクトに関連付けられているスパイウェアの名前。Webroot でのみ検出された応答に適用します。                                                                                  |
| 5  | 0                      | %Xt           | マルウェアが存在する可能性を判断する脅威リスク比（TRR）に関連付けられた Webroot 固有の値。Webroot でのみ検出された応答に適用します。                                                         |
| 6  | 354385                 | %Xs           | Webroot が脅威識別子として使用する値。シスコカスタマーサポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Webroot でのみ検出された応答に適用します。                                  |
| 7  | 12559                  | %Xi           | Webroot がトレース識別子として使用する値。シスコカスタマーサポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Webroot でのみ検出された応答に適用します。                                |
| 8  | -                      | %Xd           | McAfee が DVS エンジンに渡したマルウェア スキャンの判定。McAfee でのみ検出された応答に適用します。<br><br>詳細については、 <a href="#">マルウェア スキャンの判定値, on page 737</a> を参照してください。   |

| 位置 | フィールド値 | フォーマット<br>指定子 | 説明                                                                                                                                 |
|----|--------|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| 9  | “-”    | “%Xe”         | McAfee がスキャンしたファイルの名前。McAfee でのみ検出された応答に適用します。                                                                                     |
| 10 | -      | %Xf           | McAfee がスキャン エラーとして使用する値。シスコカスタマーサポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。McAfee でのみ検出された応答に適用します。                               |
| 11 | -      | %Xg           | McAfee が検出タイプとして使用する値。シスコカスタマーサポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。McAfee でのみ検出された応答に適用します。                                  |
| 12 | -      | %Xh           | McAfee がウイルス タイプとして使用する値。シスコカスタマーサポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。McAfee でのみ検出された応答に適用します。                               |
| 13 | “-”    | “%Xj”         | McAfee がスキャンしたウイルスの名前。McAfee でのみ検出された応答に適用します。                                                                                     |
| 18 | -      | %XY           | Sophos が DVS エンジンに渡したマルウェア スキャンの判定。Sophos でのみ検出された応答に適用します。<br><br>詳細については、 <a href="#">マルウェア スキャンの判定値, on page 737</a> を参照してください。 |
| 15 | -      | %Xx           | Sophos がスキャン戻りコードとして使用する値。シスコカスタマーサポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Sophos でのみ検出された応答に適用します。                              |

| 位置 | フィールド値 | フォーマット<br>指定子 | 説明                                                                                                                                                                                                                                                                                                                                                                                         |
|----|--------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16 | "_"    | "%Xy"         | Sophos が好ましくないコンテンツを検出したファイルの名前。Sophos でのみ検出された応答に適用します。                                                                                                                                                                                                                                                                                                                                   |
| 17 | "_"    | "%Xz"         | Sophos が脅威名として使用する値。シスコカスタマーサポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Sophos でのみ検出された応答に適用します。                                                                                                                                                                                                                                                                                            |
| 18 | -      | %Xl           | <p>Cisco データ セキュリティ ポリシーの [コンテンツ (Content) ] 列のアクションに基づく、Cisco データ セキュリティ のスキャン判定。以下のリストは、このフィールドで使用できる値を示します。</p> <ul style="list-style-type: none"> <li>• <b>0.</b> 許可 (Allow)</li> <li>• <b>1.</b> ブロック (Block)</li> <li>• <b>- (ハイフン)</b> Cisco データ セキュリティ フィルタによるスキャンが開始されませんでした。この値は、Cisco データ セキュリティ フィルタがディセーブルの場合、または URL カテゴリ アクションが [許可 (Allow) ] に設定されている場合に表示されます。</li> </ul> |

| 位置 | フィールド値  | フォーマット<br>指定子 | 説明                                                                                                                                                                                                                                                                                                                                                                                        |
|----|---------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19 | -       | %Xp           | <p>ICAP 応答で指定された結果に基づく外部 DLP スキャンの評価。以下のリストは、このフィールドで利用できる値を示します。</p> <ul style="list-style-type: none"> <li>• <b>0.</b> 許可 (Allow)</li> <li>• <b>1.</b> ブロック (Block)</li> <li>• <b>- (ハイフン)</b> 外部 DLP サーバによるスキャンが開始されませんでした。この値は、外部 DLP スキャンがディセーブルの場合、または [外部 DLP ポリシー (External DLP Policies) ] &gt; [接続先 (Destinations) ] ページに除外 URL カテゴリがあるため、コンテンツがスキャンされなかった場合に表示されます。</li> </ul> |
| 20 | IW_infr | %XQ           | <p>要求側のスキャン時に決定された定義済み URL カテゴリの判定 (省略形)。URL フィルタリングがディセーブルの場合、このフィールドにはハイフン (-) が表示されます。</p> <p><b>Note</b><br/>AsyncOS バージョン 11.8 以降では、URL カテゴリ識別子が二重引用符で囲まれて表示されます。たとえば、"IW_infr" などです。</p> <p>URL カテゴリの省略形の一覧については、<a href="#">URL カテゴリについて</a>, on page 325 を参照してください。</p>                                                                                                           |

| 位置 | フィールド値           | フォーマット<br>指定子 | 説明                                                                                                                                                                                                                                                                     |
|----|------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21 | -                | %XA           | <p>応答側のスキャン中に動的コンテンツ分析エンジンによって判定された URL カテゴリの評価（省略形）。Cisco Web 利用の制御の URL フィルタリング エンジンにのみ適用されます。動的コンテンツ分析エンジンがイネーブルになっており、要求時にカテゴリが割り当てられなかった場合にのみ適用されます（値「nc」が要求側のスキャン判定に表示されます）。</p> <p>URL カテゴリの省略形の一覧については、<a href="#">URL カテゴリについて, on page 325</a>を参照してください。</p> |
| 22 | "Trojan Phisher" | "%XZ"         | <p>どのスキャンエンジンがイネーブルになっているかに関係なく、マルウェアカテゴリを提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。</p>                                                                                                                                                 |
| 23 | "_"              | "%Xk"         | <p>カテゴリ名または脅威タイプは、Web レピュテーションフィルタによって返されます。Web レピュテーションが高い場合はカテゴリ名が返され、レピュテーションが低い場合は脅威タイプが返されます。</p>                                                                                                                                                                 |
| 24 | "_"              | %X#10#        | <p>Google 翻訳エンジンの中にカプセル化された URL。カプセル化された URL がない場合、フィールド値は「-」になります。</p>                                                                                                                                                                                                |
| 25 | "Unknown"        | "%XO"         | <p>AVC または ADC エンジンによって返されたアプリケーションの名前（該当する場合）。AVC または ADC エンジンが有効な場合にのみ適用されます。</p>                                                                                                                                                                                    |
| 26 | "Unknown"        | "%Xu"         | <p>AVC または ADC エンジンによって返されたアプリケーションのタイプ（該当する場合）。AVC または ADC エンジンが有効な場合にのみ適用されます。</p>                                                                                                                                                                                   |

| 位置 | フィールド値           | フォーマット<br>指定子 | 説明                                                                                                                                                                 |
|----|------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 27 | "-" or "Unknown" | "%Xb"         | AVC または ADC エンジンによって返されたアプリケーションの動作（該当する場合）。AVC または ADC エンジンが有効な場合にのみ適用されます。<br><br>AVC の場合は「_」、ADC の場合は「Unknown」です。                                               |
| 28 | "_"              | "%XS"         | 安全なブラウジング スキャンの判定。<br>この値は、セーフサーチ機能またはサイトコンテンツレーティング機能がトランザクションに適用されたかどうかを示します。<br><br>可能な値のリストについては、 <a href="#">アダルト コンテンツ アクセスのロギング, on page 316</a> を参照してください。 |
| 29 | 489.73           | %XB           | 要求に対応するために使用された平均帯域幅（KB/秒）。                                                                                                                                        |
| 30 | 0                | %XT           | 帯域幅制限の制御設定によって要求が絞り込まれたかどうかを示す値。「1」は要求が絞り込まれたことを示し、「0」は絞り込まれなかったことを示します。                                                                                           |
| 31 | [Local]          | %l            | 要求を行なっているユーザのタイプ（[ローカル（Local）] または [リモート（Remote）]）。AnyConnect Secure Mobility がイネーブルの場合にのみ適用されます。イネーブルでない場合、値はハイフン（-）です。                                           |
| 32 | "_"              | "%X3"         | どのスキャンエンジンがイネーブルになっているかに依存しない、統合された要求側アンチマルウェア スキャンの判定。発信マルウェア スキャン ポリシーが適用されるときに、クライアント要求のスキャンによってブロックまたはモニタされるトランザクションに適用されます。                                   |

| 位置 | フィールド値                | フォーマット<br>指定子 | 説明                                                                                                                                                                                                                                         |
|----|-----------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 33 | "_"                   | "%X4"         | <p>該当する発信マルウェアスキャンポリシーによってブロックまたはモニタされるクライアント要求に割り当てられた脅威の名前。</p> <p>この脅威の名前は、どのアンチマルウェアスキャンエンジンがイネーブルになっているかには依存しません。</p>                                                                                                                 |
| 34 | 37                    | %X#1#         | <p>Advanced Malware Protection ファイルスキャンからの判定：</p> <ul style="list-style-type: none"> <li>• 0：悪意のないファイル</li> <li>• 1：ファイルタイプが原因で、ファイルがスキャンされなかった</li> <li>• 2：ファイルスキャンがタイムアウト</li> <li>• 3：スキャンエラー</li> <li>• 3よりも大きい値：悪意のあるファイル</li> </ul> |
| 35 | "W32.CiscoTestVector" | %X#2#         | <p>Advanced Malware Protection ファイルスキャンで判定された脅威の名前。「-」は脅威がないことを示します。</p>                                                                                                                                                                   |
| 36 | 33                    | %X#3#         | <p>Advanced Malware Protection ファイルスキャンのレピュテーションスコア。このスコアは、クラウドレピュテーションサービスがファイルを正常と判定できない場合にのみ使用されます。</p> <p>詳細については、<a href="#">ファイルレピュテーションフィルタリングとファイル分析, on page 477</a>の「脅威スコアとレピュテーションしきい値」に関する情報を参照してください。</p> <p>。</p>            |

| 位置 | フィールド値                                                                     | フォーマット<br>指定子 | 説明                                                                                                                                                                     |
|----|----------------------------------------------------------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 37 | 0                                                                          | %X#4#         | アップロードおよび分析要求のインジケータ：<br><br>「0」は、Advanced Malware Protection で分析用にファイルのアップロードが要求されなかったことを示します。<br><br>「1」は、Advanced Malware Protection で分析用にファイルのアップロードが要求されたことを示します。 |
| 38 | "WSA-INFECTED-FILE.pdf"                                                    | %X#5#         | ダウンロードして分析するファイルの名前。                                                                                                                                                   |
| 39 | "fd5ef49d4213e05f448<br>f11ed9c98253d85829614fba<br>368a421d14e64c426da5e" | %X#6#         | このファイルの SHA-256 ID。                                                                                                                                                    |
| 40 | ARCHIVESCAN_BLOCKEDFILETYPE                                                | %X#8#         | アーカイブ スキャン判定。                                                                                                                                                          |
| 41 | EXT_ARCHIVESCAN_VERDICT                                                    | %Xo           | アーカイブ スキャン判定の詳細。検査可能なアーカイブファイルがアクセスポリシーのカスタム オブジェクト ブロック設定に基づいてブロックされている場合<br>(ARCHIVESCAN_BLOCKEDFILETYPE)、この判定の詳細のエントリには、ブロックされたファイルのタイプおよびブロックされたファイルの名前が含まれます。     |
| 54 | EXT_ARCHIVESCAN_THREATDETAIL                                               | %Xm           | アーカイブスキャナによるファイル判定。                                                                                                                                                    |
| 43 | EXT_WTT_BEHAVIOR                                                           | %XU           | Web タップ動作。                                                                                                                                                             |
| 44 | EXT_YTCAT                                                                  | %X#29#        | トランザクションに割り当てられた YouTube URL カテゴリ (省略形)。カテゴリが割り当てられない場合、このフィールドには「nc」が表示されます。                                                                                          |

各フォーマット指定子の機能については、[ログ ファイルのフィールドとタグ, on page 721](#)を参照してください。

#### 関連項目

- [アクセス ログ ファイル内の Web プロキシ情報, on page 686](#)



- [アクセス ログのカスタマイズ, on page 714](#)
- [W3C 準拠のアクセス ログ ファイル, on page 712](#)
- [ログ ファイルの表示, on page 686](#)
- [ログ ファイルのフィールドとタグ, on page 721](#)

## W3C 準拠のアクセス ログ ファイル

Secure Web Applianceには、Web プロキシ トランザクション情報を記録する 2 つの異なるログ タイプ（アクセス ログと W3C 形式のアクセス ログ）が用意されています。W3C アクセス ログは World Wide Web コンソーシアム（W3C）準拠であり、W3C 拡張ログ ファイル（ELF）形式でトランザクション履歴を記録します。

- [W3C フィールド タイプ, on page 712](#)
- [W3C アクセス ログの解釈, on page 712](#)

## W3C フィールド タイプ

W3C アクセス ログ サブスクリプションを定義する場合は、ACL デシジョン タグまたはクライアント IP アドレスなど、含めるログ フィールドを選択します。以下のいずれかのログ フィールドのタイプを含めることができます。

- **定義済み。** Web インターフェイスには、選択できるフィールドのリストが含まれています。
- **ユーザ定義。** 定義済みリストに含まれていないログ フィールドを入力できます。

## W3C アクセス ログの解釈

W3C アクセス ログを解釈するときは、以下のルールとガイドラインを考慮してください。

- 各 W3C アクセス ログ サブスクリプションに記録されるデータは、管理者が指定します。したがって、W3C アクセス ログには設定済みのフィールド形式がありません。
- W3C ログは自己記述型です。ファイル形式（フィールドのリスト）は、各ログ ファイルの先頭のヘッダーで定義されます。
- W3C アクセス ログのフィールドは空白で区切ります。
- フィールドに特定のエントリのデータが含まれていない場合、ログ ファイルには代わりにハイフン (-) が表示されます。
- W3C アクセス ログ ファイルの各行は、1 つのトランザクションに対応し、各行は改行シーケンスで終了します。
- [W3C ログ ファイルのヘッダー, on page 713](#)
- [W3C フィールドのプレフィックス, on page 713](#)

## W3C ログ ファイルのヘッダー

各 W3C ログ ファイルには、ファイルの先頭にヘッダーテキストが含まれています。各行は、# 文字で始まり、ログ ファイルを作成した Secure Web Appliance に関する情報を提供します。W3C ログ ファイルのヘッダーには、ログ ファイルを自己記述型にするファイル形式（フィールドのリスト）が含まれています。

以下の表は、各 W3C ログ ファイルの先頭に配置されているヘッダー フィールドの説明です。

| ヘッダー フィールド           | 説明                                                                          |
|----------------------|-----------------------------------------------------------------------------|
| バージョン<br>(Version)   | 使用される W3C の ELF 形式バージョン                                                     |
| 日付 (Date)            | ヘッダー（およびログ ファイル）が作成された日時。                                                   |
| システム<br>(System)     | ログ ファイルを生成した Secure Web Appliance（「Management_IP - Management_hostname」形式）。 |
| ソフトウェア<br>(Software) | これらのログを生成したソフトウェア                                                           |
| フィールド<br>(Fields)    | ログに記録されたフィールド                                                               |

### W3C ログ ファイルの例：

```
#Version: 1.0
#Date: 2009-06-15 13:55:20
#System: 10.1.1.1 - wsa.qa
#Software: AsyncOS for Web 6.3.0
#Fields: timestamp x-elapsed-time c-ip
x-resultcode-httpstatus sc-bytes cs-method cs-url cs-username
x-hierarchy-origin cs-mime-type x-acltag x-result-code x-suspect-user-agent
```

## W3C フィールドのプレフィックス

ほとんどの W3C ログ フィールドの名前には、クライアントやサーバなど、値を取得したヘッダーを識別するプレフィックスが含まれています。プレフィックスのないログフィールドは、トランザクションに関与するコンピュータに関係ない値を参照します。以下の表は、W3C ログ フィールドのプレフィックスの説明です。

| プレフィックスのヘッダー | 説明           |
|--------------|--------------|
| c            | クライアント       |
| s            | サーバ          |
| cs           | クライアントからサーバへ |

| プレフィックスのヘッダー | 説明              |
|--------------|-----------------|
| sc           | サーバからクライアントへ    |
| x            | アプリケーション固有の識別子。 |

たとえば、W3C ログ フィールド「cs-method」は、クライアントからサーバに送信された要求のメソッドを示し、「c-ip」はクライアントの IP アドレスを示しています。

#### 関連項目

- [アクセス ログ ファイル内の Web プロキシ情報, on page 686。](#)
- [アクセス ログのカスタマイズ, on page 714。](#)
- [トラフィック モニタのログ ファイル, on page 720。](#)
- [ログ ファイルのフィールドとタグ, on page 721。](#)
- [ログ ファイルの表示, on page 686。](#)

## アクセス ログのカスタマイズ

標準アクセス ログや W3C アクセス ログをカスタマイズしてさまざまな定義済みフィールドやユーザ定義フィールドを追加して、ネットワーク内の Web トラフィックに関する包括的な情報を取得できます。

#### 関連項目

- 定義済みフィールドの一覧については、[ログ ファイルのフィールドとタグ, on page 721](#)を参照してください。
- ユーザ定義フィールドの詳細については、[アクセス ログのユーザ定義フィールド, on page 714](#)を参照してください。

## アクセス ログのユーザ定義フィールド

定義済みのフィールドだけではアクセス ログや W3C ログに記録できない HTTP/HTTPS トランザクションのヘッダー情報がある場合は、カスタム ログ フィールドを追加できます。これを行うには、アクセス ログや W3C ログのサブスクリプションを設定するときに、[カスタム フィールド (Custom Fields) ] テキスト ボックスにユーザ定義のログ フィールドを入力します。

カスタム ログ フィールドは、クライアントまたはサーバから送信される任意のヘッダーから任意のデータをとることができます。ログサブスクリプションに追加されるヘッダーが要求または応答に含まれていない場合、ログ ファイルはログ フィールド値としてハイフンを使用します。

以下の表は、アクセス ログおよび W3C ログにカスタム フィールドを追加するときの構文を示しています。

| ヘッダー タイプ              | アクセス ログ フォーマット指定子の構文 | W3C ログ カスタム フィールドの構文  |
|-----------------------|----------------------|-----------------------|
| クライアント アプリケーションからヘッダー | %<ClientHeaderName : | cs(ClientHeaderName ) |
| サーバからヘッダー             | %<ServerHeaderName : | sc(ServerHeaderName ) |

たとえば、クライアント要求の If-Modified-Since ヘッダー値のログを記録する場合、W3C ログサブスクリプションの [カスタム フィールド (Custom Field) ] ボックスに以下のテキストを入力します。

```
cs (If-Modified-Since)
```

#### 関連項目

- [標準アクセス ログのカスタマイズ, on page 715。](#)
- [W3C アクセス ログのカスタマイズ, on page 716。](#)

## 標準アクセス ログのカスタマイズ

### Procedure

**ステップ 1** [システム管理 (System Administration) ] > [ログ サブスクリプション (Log Subscriptions) ] を選択します。

**ステップ 2** アクセス ログ サブスクリプションを編集するには、アクセス ログ ファイル名をクリックします。

**ステップ 3** [カスタム フィールド (Custom Fields) ] に、必要なフォーマット指定子を入力します。

[カスタム フィールド (Custom Fields) ] にフォーマット指定子を入力する構文は以下のとおりです。

```
<format_specifier_1> <format_specifier_2> ...
```

例 : %a %b %E

フォーマット指定子の前にトークンを追加して、アクセス ログ ファイルの説明テキストを表示できます。次に例を示します。

```
client_IP %a body_bytes %b error_type %E
```

この場合、client\_IP はログ フォーマット指定子 %a の説明トークンです (以下同様) 。

#### Note

クライアント要求またはサーバ応答の任意のヘッダーにカスタム フィールドを作成できます。

**ステップ 4** 変更を送信し、保存します。

### What to do next

#### 関連項目

- [アクセス ログ ファイル内の Web プロキシ情報, on page 686。](#)
- [ログ ファイルのフィールドとタグ, on page 721。](#)
- [アクセス ログのユーザ定義フィールド, on page 714。](#)

## W3C アクセス ログのカスタマイズ

### Procedure

- ステップ 1** [システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] を選択します。
- ステップ 2** W3C ログサブスクリプションを編集するには、W3C ログファイル名をクリックします。
- ステップ 3** [カスタム フィールド (Custom Fields)] ボックスにフィールドを入力し、[追加 (Add)] をクリックします。

[選択されたログ フィールド (Selected Log Fields)] リストに表示されるフィールドの順序によって、W3C アクセス ログ ファイルのフィールドの順序が決まります。[上へ移動 (Move Up)] または [下へ移動 (Move Down)] ボタンを使用してフィールドの順序を変更できます。[選択されたログ フィールド (Selected Log Fields)] リストでフィールドを選択し、[削除 (Remove)] をクリックして、それを削除できます。

[カスタム フィールド (Custom Field)] ボックスに複数のユーザ定義フィールドを入力し、それらを同時に入力できます。ただし、[追加 (Add)] をクリックする前に、各エントリが改行 (Enter キーを押します) で区切られている必要があります。

W3C ログサブスクリプションに含まれるログ フィールドを変更すると、ログサブスクリプションは自動的にロールオーバーします。これにより、ログファイルの最新バージョンに適切な新しいフィールドヘッダーを含めることができます。

#### Note

クライアント要求またはサーバ応答の任意のヘッダーにカスタム フィールドを作成できます。

- ステップ 4** 変更を送信し、保存します。

### What to do next

#### 関連項目

- [W3C 準拠のアクセス ログ ファイル, on page 712。](#)
- [ログ ファイルのフィールドとタグ, on page 721。](#)
- [アクセス ログのユーザ定義フィールド, on page 714。](#)
- [Cisco CTA 固有のカスタム W3C ログの設定, on page 716](#)
- [Cisco Cloudlock に固有のカスタム W3C ログの設定, on page 718](#)

### Cisco CTA 固有のカスタム W3C ログの設定

アプライアンスを、Cognitive Threat Analytics (CTA) (分析とレポートのための Cisco Cloud Web Security サービス固有のカスタム W3C アクセス ログ) を「プッシュ」するよう設定する

ことができます。Cisco ScanCenter は Cloud Web Security (CWS) の管理ポータルです。  
<https://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html>を参照してください

### 始める前に

自動アップロードプロトコルとして SCP (Secure Copy Protocol) を選択して、アプライアンス用の Cisco ScanCenter にデバイスのアカウントを作成します。『Cisco ScanCenter Administrator』の「Proxy Device Uploads」のセクションを参照してください ([https://www.cisco.com/c/en/us/td/docs/security/web\\_security/scancenter/administrator/guide/b\\_ScanCenter\\_Administrator\\_Guide.html](https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide.html))。

SCP のホスト名とアプライアンス用の生成されたユーザ名に注意してください。ユーザ名は大文字と小文字が区別され、デバイスごとに異なります。

### 手順

- ステップ 1** [セキュリティサービス (Security Services) ] > [Cisco Cognitive Threat Analytics] を選択します。
- ステップ 2** [設定の編集 (Edit Settings) ] をクリックします。
- ステップ 3** [ログフィールド (Log Fields) ] エリアに、必要に応じて追加のログフィールドを追加します。[ログサブスクリプションの追加および編集 \(676 ページ\)](#) を参照してください。
- ステップ 4** [選択されたログフィールド (Selected Log Fields) ] で、c-ip、cs-username または cs-auth-group の横のチェックボックスを、個別にこれらのフィールドを匿名化する場合は、オンにします。  
  
また、[匿名化 (Anonymization) ] チェックボックスをオンにして、これらのフィールドを同時に匿名化することもできます。[ログサブスクリプションの追加および編集 \(676 ページ\)](#) を参照してください。
- ステップ 5** [検索方法 (Retrieval Method) ] 領域に、Cisco ScanCenter のデバイス用に生成されたユーザ名を入力します。デバイス ユーザ名は大文字と小文字が区別され、プロキシデバイスごとに異なります。
- ステップ 6** 必要に応じて、[詳細オプション (Advanced Options) ] の値を変更します。
- ステップ 7** [送信 (Submit) ] をクリックします。  
  
アプライアンスは公開 SSH キーを生成し、[Cisco Cognitive Threat Analytics] ページにそれらが表示されます。
- ステップ 8** 公開 SSH キーのいずれかをクリップボードにコピーします。
- ステップ 9** [Cisco Cognitive Threat Analytics の表示 (View Cisco Cognitive Threat Analytics) ] ポータルリンクをクリックして、Cisco ScanCenter ポータルに切り替えて、適切なデバイスアカウントを選択してから、公開 SSH キーを [CTA デバイスプロビジョニング (CTA Device Provisioning) ] ページに貼り付けます。(『Cisco ScanCenter Administrator Guide』の「Proxy Device Uploads」のセクションを参照してください)。  
  
プロキシデバイスからのログファイルは、プロキシデバイスと CTA システム間の正常な認証での分析のため CTA システムにアップロードされます。
- ステップ 10** アプライアンスに戻って、変更を確定します。

[システム管理 (System Administration)] > [ログサブスクリプション (Log Subscription)] を使用して、CTA W3C ログを追加することもできます。[W3C アクセス ログのカスタマイズ \(716 ページ\)](#) の手順に従って、新しい W3C アクセス ログ サブスクリプションを次のオプションを指定して追加します。

- ログ タイプとして [W3C ログ (W3C Logs)]
- サブスクリプションとして [Cisco Cognitive Threat Analyticsサブスクリプション (Cisco Cognitive Threat Analytics Subscription)] を選択
- ファイル転送タイプとして [SCP] を選択

カスタム フィールドの詳細については、[ログサブスクリプションの追加および編集 \(676 ページ\)](#) を参照してください。

(注)

CTA ログ サブスクリプションをすでに設定している場合には、アプライアンスの [Cisco Cognitive Threat Analytics] ページで、ログの名前を `cta_log` に変更する必要があります。

ログを作成した後、CTA ログを削除する場合は、[Cisco Cognitive Threat Analytics] ページで [無効化 (Disable)] をクリックします。CTA ログは [ログサブスクリプション (Log Subscriptions)] ページからも削除できます ([システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] )。

匿名の CTA 固有 W3C ログ フィールドを非匿名化するには、[Cisco Cognitive Threat Analytics] ページで [非匿名化 (Cisco Cognitive Threat Analytics)] をクリックします。[W3C ログ フィールドの非匿名化 \(682 ページ\)](#) を参照してください

また、[システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] を使用して、匿名の CTA 固有 W3C ログ フィールドを非匿名化することもできます。「[W3C ログ フィールドの非匿名化 \(682 ページ\)](#)」を参照してください。

## Cisco Cloudlock に固有のカスタム W3C ログの設定

Cisco Cloudlock は、クラウド ネイティブ CASB およびサイバー セキュリティ プラットフォームであり、Software-as-a-Service、Platform-as-a-Service、および Infrastructure-as-a-Service の全体にわたってユーザ、データ、およびアプリケーションを保護します。シスコの Cloudlock ポータルに W3C アクセス ログをプッシュするようお使いのアプライアンスを設定し、分析とレポートに役立てることができます。これらのカスタム W3C ログを使用すると、顧客の SaaS 利用状況がさらに把握しやすくなります。

### 始める前に

お使いのアプライアンスの Cloudlock ポータルにデバイス アカウントを作成し、自動アップロード プロトコルとして SCP を選択します。

Cloudlock ポータルにログオンしてオンライン ヘルプにアクセスし、Cloudlock ポータルにデバイス アカウントを作成するための手順に従ってください。

## 手順

**ステップ 1** [セキュリティ サービス (Security Services)] > [Cisco Cloudlock] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

(注)

ログのフィールドは、[ログフィールド (Log Fields)] エリアでデフォルトで選択されています。デフォルトで選択されている以外のログフィールドをさらに追加することはできません。[ログフィールド (Log Fields)] エリアに表示されているログフィールドの順番を変えることは推奨されません。

Cloudlock ログファイルのログフィールド (*c-ip*、*cs-username*、または *cs-auth-group*) を匿名化することはできません。

**ステップ 3** [取得方法 (Retrieval Method)] エリアで、次の情報を入力します。

- Cloudlock サーバのホスト名とポート番号
- ログ ファイルを保存する Cloudlock サーバのディレクトリ
- Cloudlock サーバに接続する権限を持つユーザのユーザ名

**ステップ 4** 必要に応じ、[詳細オプション (Advanced Options)] の値を変更します。

**ステップ 5** [送信 (Submit)] をクリックします。

アプライアンスによって公開 SSH キーが生成され、Cisco Cloudlock ページに表示されます。

**ステップ 6** 公開 SSH キーのいずれかをクリップボードにコピーします。

**ステップ 7** [Cloudlockポータルを表示 (View Cloudlock Portal)] リンクをクリックして、Cisco Cloudlock ポータルに切り替えます。適切なデバイス アカウントを選択し、公開 SSH キーを [Cloudlock設定 (Cloudlock Setting)] ページに貼り付けます。

お使いのプロキシ デバイスと Cloudlock システムの間で認証が成功すると、プロキシ デバイスからのログ ファイルが、分析のため、Cloudlock システムにアップロードされます。

**ステップ 8** アプライアンスに戻って、変更を確定します。

Cloudlock W3C ログの追加は、[システム管理 (System Administration)] > [ログサブスクリプション (Log Subscription)] を使用して行うこともできます [W3C アクセス ログのカスタマイズ \(716 ページ\)](#) の手順に従って、新しい W3C アクセス ログ サブスクリプションを次のオプションを指定して追加します。

- ログ タイプとして [W3C ログ (W3C Logs)]
- サブスクリプションとして [Cisco Cloudlock] を選択
- ファイル転送タイプとして [SCP] を選択

カスタム フィールドの詳細については、[ログ サブスクリプションの追加および編集 \(676 ページ\)](#) を参照してください。



(注)

Cloudlock ログ サブスクリプションがすでに設定済みの場合、ログ名を **cloudlock\_log** に変更し、それを、アプライアンスの Cisco Cloudlock ページにリストする必要があります。

ログの作成後に Cloudlock ログを削除する場合は、Cisco Cloudlock ページで [無効 (Disable)] をクリックします。Cloudlock ログの削除は、[ログサブスクリプション (Log Subscription)] ページ ([システム管理 (System Administration)] > [ログサブスクリプション (Log subscriptions)]) から行うこともできます。

## トラフィック モニタのログ ファイル

レイヤ 4 トラフィック モニター ログ ファイルには、レイヤ 4 モニタリング アクティビティの詳細が記録されます。レイヤ 4 トラフィック モニタ ログ ファイルのエントリを表示して、ファイアウォールブロック リストやファイアウォール許可リストのアップデートを追跡できます。

### トラフィック モニタ ログの解釈

下記の例では、トラフィック モニタ ログに記録されるさまざまなタイプのエントリの意味について説明します。

#### 例 1

```
172.xx.xx.xx discovered for blocksite.net (blocksite.net) added to firewall block list.
```

この例では、一致する場所がブロック リストのファイアウォール エントリとなります。レイヤ 4 トラフィック モニタにより、アプライアンスを通過した DNS 要求に基づいて、ブロック リストのドメイン名への IP アドレスが検出されました。その後で、その IP アドレスがファイアウォールのブロック リストに追加されました。

#### 例 2

```
172.xx.xx.xx discovered for www.allowsite.com (www.allowsite.com) added to firewall allow list.
```

この例では、一致が許可リストのファイアウォール エントリとなります。レイヤ 4 トラフィック モニタによりドメイン名 エントリが照合され、一致がアプライアンスの許可リストに追加されました。その後で、その IP アドレスがファイアウォールの許可リストに追加されました。

#### 例 3

```
Firewall noted data from 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.
```

この例では、レイヤ 4 トラフィック モニタにより内部 IP アドレスとブロック リストに記載されている外部 IP アドレス間で渡されたデータ レコードが記録されています。この場合、レイヤ 4 トラフィック モニタは、「ブロック」ではなく「モニタ」に設定されています。

#### 関連項目

- [ログ ファイルの表示, on page 686](#)

## ログ ファイルのフィールドとタグ

- [アクセス ログのフォーマット指定子と W3C ログ ファイルのフィールド, on page 721](#)
- [トランザクション結果コード, on page 691](#)
- [ACL デシジョン タグ, on page 692](#)
- [マルウェア スキャンの判定値, on page 737](#)

### アクセス ログのフォーマット指定子と W3C ログ ファイルのフィールド

ログ ファイルでは、各ログ ファイル エントリを構成している情報項目を表すために変数が使用されます。これらの変数は、アクセス ログではフォーマット指定子、W3C ログではログ フィールドと呼ばれ、各フォーマット指定子には対応するログ フィールドがあります。

アクセス ログにこれらの値を表示するよう設定する方法については、[アクセス ログのカスタマイズ, on page 714](#)、および[ログサブスクリプションの追加および編集, on page 676](#)のカスタム フィールドに関する情報を参照してください。

以下の表は、これらの変数に関する説明です。

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド     | 説明                                                                                                                  |
|-------------------|---------------------|---------------------------------------------------------------------------------------------------------------------|
| %:<A              | AcITime             | アクセス制御リストトランザクションにかかった合計時間を出力します。                                                                                   |
| %{                | x-id-shared         | Umbrella と共有する ID のステータスを出力します。<br><br>IDがトランザクションで共有されている場合、対応するフォーマッタの値は「ID_SHARED」です。それ以外の場合は、アクセスログに「-」が表示されます。 |
| %[                | x-spoofed-ip        | プロキシ IP スプーフィングで使用する送信元 IP アドレス。                                                                                    |
| %)                | x-proxy-instance-id | ハイパフォーマンスモードが有効になっている場合のプロキシのインスタンス ID。それ以外の場合は、ハイフンをログに記録します。                                                      |
| %(                | cs-domain-map       | ドメインマップを使用して解決された解決済みのドメイン名。                                                                                        |
| %X#11#            | ext_auth_sgt        | ISE 統合で使用するセキュリティ グループ タグのカスタム フィールド パラメーター。                                                                        |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド             | 説明                                                                                                                                                                                                                       |
|-------------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| '%\$              | cipher information          | トランザクションの両方のログの暗号情報（クライアントプロキシ暗号情報 ## プロキシサーバ暗号情報）。この情報は「<ciphername>, <protocol version>, Kx=<key exchange>, Au=<authentication>, Enc=<symmetric encryption method>, Mac=<message authentication code>」のようなシーケンスで示されます。 |
| '%:<l             | x-p2s-first-byte-time       | Web プロキシがサーバへの接続を開始した時点から最初にサーバに書き込みが行えるようになるまでの時間。Web プロキシが複数のサーバに接続してトランザクションを完了する必要がある場合、これらの時間の合計になります。                                                                                                              |
| '%:<a             | x-p2p-auth-wait-time        | Web プロキシが要求を送信後、Web プロキシの認証プロセスからの応答を受信する待機時間。                                                                                                                                                                           |
| '%:<b             | x-p2s-body-time             | ヘッダーの後、要求本文をサーバに書き込むまでの待機時間。                                                                                                                                                                                             |
| '%:<d             | x-p2p-dns-wait-time         | Web プロキシが Web プロキシ DNS プロセスに DNS 要求を送信するのにかかった時間。                                                                                                                                                                        |
| '%:<h             | x-p2s-header-time           | 最初のバイトの後、要求ヘッダーをサーバに書き込むまでの待機時間。                                                                                                                                                                                         |
| '%:<r             | x-p2p-reputation- wait-time | Web プロキシが要求を送信後、Web レピュテーションフィルタからの応答を受信する待機時間。                                                                                                                                                                          |
| '%:<s             | x-p2p-asw-req- wait-time    | Web プロキシが要求を送信後、Web プロキシのアンチス パイウェア プロセスからの判定を受信する待機時間。                                                                                                                                                                  |
| '%:>l             | x-s2p-first-byte-time       | サーバからの最初の応答バイトの待機時間                                                                                                                                                                                                      |
| '%:>a             | x-p2p-auth-svc-time         | Web プロキシの認証プロセスからの応答を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。                                                                                                                                                               |
| '%:>b             | x-s2p-body-time             | 受信したヘッダーの後の完全な応答本文の待機時間                                                                                                                                                                                                  |
| '%:>c             | x-p2p-fetch-time            | Web プロキシがディスク キャッシュからの応答を読み取るのに必要な時間。                                                                                                                                                                                    |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド            | 説明                                                                                                                       |
|-------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------|
| %:>d              | x-p2p-dns-svc-time         | Web プロキシ DNS プロセスが Web プロキシに DNS 結果を返送するのにかかった時間。                                                                        |
| %:>h              | x-s2p-header-time          | 最初の応答バイト後のサーバヘッダーの待機時間                                                                                                   |
| %:>g              |                            | SSL サーバ ハンドシェイク遅延の情報。                                                                                                    |
| %o                | -                          | 消費された時間クォータ。                                                                                                             |
| %O                | -                          | 消費されたボリュームクォータ。                                                                                                          |
| %X#41#            | x-bw-info                  | 適用される帯域幅クォータ制御レベル、リクエストにマッピングされた帯域幅パイプ番号、設定された帯域幅クォータ制限、および使用される帯域幅クォータプロファイル (level-pipe_no-quota_limit-quota_profile)。 |
| %:>r              | x-p2p-reputation-svc- time | Web レピュテーションフィルタからの判定を受信する待機時間 (Web プロキシが要求を送信するのに必要な時間を含む)。                                                             |
| %:>s              | x-p2p-asw-req-svc- time    | Web プロキシのアンチス パイウェア プロセスからの判定を受信する待機時間 (Web プロキシが要求を送信するのに必要な時間を含む)。                                                     |
| %:1<              | x-c2p-first-byte-time      | 新しいクライアント接続からの最初の要求バイトを待機する時間。                                                                                           |
| %:1>              | x-p2c-first-byte-time      | 最初のバイトがクライアントに書き込まれるまでの待機時間。                                                                                             |
| %:A<              | x-p2p-avc-svc-time         | AVC プロセスからの応答を受信する待機時間 (Web プロキシが要求を送信するのに必要な時間を含む)。                                                                     |
| %:A>              | x-p2p-avc-wait-time        | Web プロキシが要求を送信後、AVC プロセスからの応答を受信する待機時間。                                                                                  |
| %:b<              | x-c2p-body-time            | クライアント本文全体を待機する時間。                                                                                                       |
| %:b>              | x-p2c-body-time            | 本文全体がクライアントに書き込まれるまでの待機時間。                                                                                               |

| アクセス ログのフォーマット指定子                                                       | W3C ログのログ フィールド                 | 説明                                                                                                                                     |
|-------------------------------------------------------------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| %.C<                                                                    | x-p2p-dca-resp- svc-time        | 動的コンテンツ分析からの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。                                                                                   |
| %.C>                                                                    | x-p2p-dca-resp- wait-time       | Web プロキシが要求を送信後、動的コンテンツ分析からの応答を受信する待機時間。                                                                                               |
| %.h<                                                                    | x-c2p-header-time               | 最初のバイトの後の完全なクライアントヘッダーの待機時間                                                                                                            |
| %.h>                                                                    | x-p2c-header-time               | クライアントに書き込まれる完全なヘッダーの待機時間                                                                                                              |
| %.m<                                                                    | x-p2p-mcafee-resp- svc-time     | McAfee スキャン エンジンからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。                                                                            |
| %.m>                                                                    | x-p2p-mcafee-resp- wait-time    | Web プロキシが要求を送信後、McAfee スキャン エンジンからの応答を受信する待機時間。                                                                                        |
| %.p<                                                                    | x-p2p-sophos-resp- svc-time     | Sophos スキャン エンジンからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。                                                                            |
| %.p>                                                                    | x-p2p-sophos-resp- wait-time    | Web プロキシが要求を送信後、Sophos スキャン エンジンからの応答を受信する待機時間。                                                                                        |
| %.w<                                                                    | x-p2p-webroot- resp -svc-time   | Webroot スキャン エンジンからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。                                                                           |
| %.w>                                                                    | x-p2p-webroot- resp- wait- time | Web プロキシが要求を送信後、Webroot スキャン エンジンからの応答を受信する待機時間。                                                                                       |
| %.H0CK_SUSPECT_USER_AGENT, MONICR_SUSPECT_USER_AGENT?%< User-Agent?/%%% | x-suspect-user-agent            | 不審なユーザ エージェント（該当する場合）。ユーザ エージェントが疑わしい Web プロキシが判定した場合、このフィールドにそのユーザ エージェントを記録します。それ以外の場合、ハイフンが表示されます。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。 |
| %<Referer:                                                              | cs(Referer)                     | Referer ヘッダー                                                                                                                           |
| %>Server:                                                               | sc(Server)                      | 応答の Server ヘッダー                                                                                                                        |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド             | 説明                                                                                                                                                                                                                      |
|-------------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %a                | c-ip                        | クライアント IP アドレス。                                                                                                                                                                                                         |
| %A                | cs-username                 | 認証されたユーザ名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。                                                                                                                                                                             |
| %b                | sc-body-size                | 本文のコンテンツ用に Web プロキシからクライアントに送信されたバイト数。                                                                                                                                                                                  |
| %B                | bytes                       | 使用された合計バイト数（要求サイズ+応答サイズ、つまり %q + %s）。                                                                                                                                                                                   |
| %c                | cs-mime-type                | 応答本文の MIME タイプ。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。                                                                                                                                                                        |
| %C                | cs(Cookie)                  | Cookie ヘッダー。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。                                                                                                                                                                           |
| %d                | s-hostname                  | データ ソースまたはサーバの IP アドレス。                                                                                                                                                                                                 |
| %]                | x-http-rewrite-profile-name | HTTP ヘッダー書き換えプロファイル名。                                                                                                                                                                                                   |
| %D                | x-acltag                    | ACL デンジョン タグ。                                                                                                                                                                                                           |
| %e                | x-elapsed-time              | ミリ秒単位の経過時間。<br><br>TCP トラフィックの場合、HTTP 接続の開始から完了までの経過時間です。<br><br>UDP トラフィックの場合、最初のデータグラムを送信してから、最後のデータグラムが許可される時間までの経過時間です。UDP トラフィックの経過時間が大きいと、タイムアウト値が大きくなる可能性があり、存続時間の長い UDP アソシエーションの許容データグラムが必要以上に長く許可される可能性があります。 |
| %E                | x-error-code                | カスタマーサポートが失敗したトランザクションの原因をトラブルシューティングするのに役立つエラー コード番号。                                                                                                                                                                  |
| %f                | cs(X-Forwarded-For)         | X-Forwarded-For ヘッダー                                                                                                                                                                                                    |
| %F                | c-port                      | クライアントの送信元ポート                                                                                                                                                                                                           |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド  | 説明                                                                                                                       |
|-------------------|------------------|--------------------------------------------------------------------------------------------------------------------------|
| %g                | cs-auth-group    | 承認されたグループ名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。<br><br>このフィールドは、ユーザが適切なグループまたはポリシーに一致しているかどうかを判断する、認証問題のトラブルシューティングに使用されます。 |
| %G                |                  | 人間が読み取れる形式のタイムスタンプ。                                                                                                      |
| %h                | sc-http-status   | HTTP 応答コード。                                                                                                              |
| %H                | s-hierarchy      | 階層の取得。                                                                                                                   |
| %i                | x-icap-server    | 要求の処理中に接続した最後の ICAP サーバの IP アドレス。                                                                                        |
| %I                | x-transaction-id | トランザクション ID。                                                                                                             |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド | 説明 |
|-------------------|-----------------|----|
| %j                | DCF             |    |



| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   |                 | <p>応答コードをキャッシュしません（DCF フラグ）。</p> <p>応答コードの説明：</p> <ul style="list-style-type: none"> <li>クライアント要求に基づく応答コード： <ul style="list-style-type: none"> <li>1 = 要求に「no-cache」ヘッダーがあった。</li> <li>2 = 要求に対してキャッシングが許可されていない。</li> <li>4 = 要求に「Variant」ヘッダーがない。</li> <li>8 = ユーザ要求にユーザ名またはパスワードが必要。</li> <li>20 = 指定された HTTP メソッドへの応答。</li> </ul> </li> <li>アプライアンスで受信された応答に基づく応答コード： <ul style="list-style-type: none"> <li>id="li_7443F05D141F4D9FB788FD416697DB65"&gt;40 = 応答に「Cache-Control: private」ヘッダーが含まれている。</li> <li>80 = 応答に「Cache-Control: no-store」ヘッダーが含まれている。</li> <li>100 = 応答は、要求がクエリーだったことを示している。</li> <li>200 = 応答に含まれている「有効期限」の値が小さい（期限切れ間近）。</li> <li>400 = 応答に「Last Modified」ヘッダーがない。</li> <li>1000 = 応答がただちに期限切れになる。</li> <li>2000 = 応答ファイルが大きすぎてキャッシュできない。</li> <li>20000 = ファイルの新しいコピーがある。</li> <li>40000 = 応答の「Vary」ヘッダーに不正/無効な値がある。</li> </ul> </li> </ul> |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド | 説明                                                                                                                                                                                                                                                           |
|-------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   |                 | <ul style="list-style-type: none"> <li>• 80000 = 応答には Cookie の設定が必要。</li> <li>• 100000 = キャッシュ不可の HTTP ステータス コード。</li> <li>• 200000 = アプライアンスが受信したオブジェクトが不完全（サイズに基づく）。</li> <li>• 800000 = 応答トレーラがキャッシュなしを示している。</li> <li>• 1000000 = 応答のリライトが必要。</li> </ul> |
| %k                | s-ip            | データ ソースの IP アドレス（サーバの IP アドレス）<br><br>この値は、ネットワーク上の侵入検知デバイスによって IP アドレスがフラグ付けされたときに、要求元を決定するのに使用されます。これにより、フラグ付けされた IP アドレスを参照したクライアントの検索が可能になります。                                                                                                           |
| %l                | user-type       | ユーザのタイプ（ローカルまたはリモート）。                                                                                                                                                                                                                                        |
| %L                | x-local_time    | 人間が読み取れる形式の要求のローカル時刻：<br>DD/MMM/YYYY : hh:mm:ss +nnnn。このフィールドは、二重引用符付きでアクセスログに書き込まれます。<br><br>このフィールドを有効にすると、各ログエントリのエポックタイムからローカルタイムを計算せずにログを問題に関連付けることができます。                                                                                               |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド   | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %m                | cs-auth-mechanism | <p>認証問題をトラブルシューティングするのに使用されます。</p> <p>トランザクションで使用する認証メカニズム。値は以下のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>BASIC</b>。ユーザ名が基本認証方式を使用して認証されました。</li> <li>• <b>NTLMSSP</b>。ユーザ名が NTLMSSP 認証方式を使用して認証されました。</li> <li>• <b>NEGOTIATE</b>。ユーザ名は Kerberos 認証方式を使用して認証されました。</li> <li>• <b>SSO_TUI</b>。クライアント IP アドレスと透過的ユーザ ID を使用して認証されたユーザ名を照合することによって、ユーザ名が取得されました。</li> <li>• <b>SSO_ISE</b>。ユーザは ISE サーバによって認証されました (ISE 認証のフォールバック メカニズムとして選択されている場合、ログには GUEST と表示されます)。</li> <li>• <b>SSO_ASA</b>。ユーザがリモートユーザで、ユーザ名はセキュア モビリティを使用して Cisco ASA から取得されました。</li> <li>• <b>FORM_AUTH</b>。アプリケーションへのアクセス時に、ユーザが Web ブラウザのフォームに認証クレデンシャルを入力しました。</li> <li>• <b>GUEST</b>。ユーザが認証に失敗し、代わりにゲストアクセスが許可されました。</li> </ul> |
| %M                | CMF               | キャッシュ ミス フラグ (CMF フラグ)。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| %N                | s-computerName    | サーバ名または宛先ホスト名。このフィールドは、二重引用符付きでアクセスログに書き込まれます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| %p                | s-port            | 宛先ポート番号。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド       | 説明                                                                                                                                                                                                                                  |
|-------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %P                | cs-version            | <p>使用されるプロトコル。値は以下のとおりです。</p> <ul style="list-style-type: none"> <li>• 0 = プロトコルの使用なし</li> <li>• 1 = HTTP</li> <li>• 2 = HTTPS</li> <li>• 3 = FTP over HTTP</li> <li>• 4 = FTP</li> <li>• 5 = SOCKS</li> <li>• 6 = HTTP2</li> </ul> |
| %q                | cs-bytes              | 要求サイズ（ヘッダー + 本文）。                                                                                                                                                                                                                   |
| %r                | x-req-first-line      | 要求の先頭行：要求方法（URI）。                                                                                                                                                                                                                   |
| %s                | sc-bytes              | 応答サイズ（ヘッダー + 本文）。                                                                                                                                                                                                                   |
| %t                | timestamp             | <p>UNIX エポックのタイムスタンプ</p> <p>注：サードパーティ製のログ アナライザ ツールを使用して W3C アクセス ログを解析する場合は、<b>timestamp</b> フィールドを含める必要があります。ほとんどのログアナライザは、このフィールドで提供される形式の時間のみ認識します。</p>                                                                         |
| %u                | cs(User-Agent)        | <p>ユーザエージェント。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。</p> <p>このフィールドは、アプリケーションが認証に失敗しているかどうか、および/または別のアクセス権限が必要かどうかを判断するのに役立ちます。</p>                                                                                                       |
| %U                | cs-uri                | 要求 URI。                                                                                                                                                                                                                             |
| %v                | date                  | YYYY-MM-DD 形式の日付。                                                                                                                                                                                                                   |
| %V                | 時刻                    | HH:MM:SS 形式の時刻。                                                                                                                                                                                                                     |
| %w                | sc-result-code        | 結果コード。例：TCP_MISS、TCP_HIT。                                                                                                                                                                                                           |
| %W                | sc-result-code-denial | 結果コードの拒否。                                                                                                                                                                                                                           |
| %x                | x-latency             | 待ち時間。                                                                                                                                                                                                                               |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド          | 説明                                                                                                                                                                                                                                                                        |
|-------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %X0               | x-req-dvs-scanverdict    | <p>どのスキャンエンジンがイネーブルになっているかに関係なく、マルウェアカテゴリ番号を提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。</p> <p>このフィールドは、二重引用符付きでアクセス ログに書き込まれます。</p>                                                                                                         |
| %X1               | x-req-dvs-threat-name    | <p>どのスキャンエンジンがイネーブルになっているかに関係なく、マルウェア脅威の名前を提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。</p> <p>このフィールドは、二重引用符付きでアクセス ログに書き込まれます。</p>                                                                                                          |
| %X2               | x-req-dvs-scanverdict    | 要求側 DVS スキャンの判定                                                                                                                                                                                                                                                           |
| %X3               | x-req-dvs-verdictname    | 要求側 DVS 判定の名前                                                                                                                                                                                                                                                             |
| %X4               | x-req-dvs-threat-name    | 要求側 DVS 脅威の名前                                                                                                                                                                                                                                                             |
| %X6               | x-as-malware-threat-name | <p>マルウェア対策スキャンエンジンを起動することなく、適応型スキャンによってトランザクションがブロックされたかどうかを示します。設定可能な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>1.</b> トランザクションがブロックされました。</li> <li>• <b>0.</b> トランザクションはブロックされませんでした。</li> </ul> <p>この変数は、スキャン判定情報（各アクセス ログ エントリの末尾の山カッコ内）に含まれています。</p> |
| %XA               | x-webcat-resp-code- abbr | <p>応答側のスキャン中に判定された URL カテゴリの評価（省略形）。Cisco Web 利用の制御の URL フィルタリング エンジンにのみ適用されます。</p>                                                                                                                                                                                       |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド            | 説明                                                                                                                                       |
|-------------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| %Xb               | x-avc-behavior             | AVC または ADC エンジンによって識別される Web アプリケーションの動作。                                                                                               |
| %XB               | x-avg-bw                   | 帯域幅制限が AVC エンジンで定義されている場合、ユーザの平均帯域幅。                                                                                                     |
| %XC               | x-webcat-code-abbr         | トランザクションに割り当てられたカスタム URL カテゴリの URL カテゴリの省略形。                                                                                             |
| %Xd               | x-mcafee-scanverdict       | McAfee 固有の ID : (スキャン判定)。                                                                                                                |
| %Xe               | x-mcafee-filename          | McAfee 固有の ID : (判定を生成するファイル名) このフィールドは二重引用符付きでアクセス ログに書き込まれます。                                                                          |
| %Xf               | x-mcafee-av-scanerror      | McAfee 固有の ID : (スキャン エラー)。                                                                                                              |
| %XF               | x-webcat-code-full         | トランザクションに割り当てられた URL カテゴリの完全名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。                                                                          |
| %Xg               | x-mcafee-av-detecttype     | McAfee 固有の ID : (検出タイプ)。                                                                                                                 |
| %XG               | x-avc-reqhead-scanverdict  | AVC 要求ヘッダーの判定。                                                                                                                           |
| %Xh               | x-mcafee-av-virustype      | McAfee 固有の ID : (ウイルス タイプ)。                                                                                                              |
| %XH               | x-avc-reqbody- scanverdict | AVC 要求本文の判定。                                                                                                                             |
| %Xi               | x-webroot-trace-id         | Webroot 固有のスキャン識別子 : (トレース ID)                                                                                                           |
| %Xj               | x-mcafee-virus-name        | McAfee 固有の ID : (ウイルス名) このフィールドは、二重引用符付きでアクセス ログに書き込まれます。                                                                                |
| %Xk               | x-wbrs-threat-type         | Web レピュテーションの脅威タイプ。                                                                                                                      |
| %XK               | x-wbrs-threat-reason       | Web レピュテーションの脅威の理由。                                                                                                                      |
| %Xl               | x-ids-verdict              | Cisco データ セキュリティ ポリシーのスキャン判定。このフィールドが含まれている場合はIDS判定が表示されます。IDS がアクティブでドキュメントが「正常」とスキャン判定された場合は「0」、要求に対する IDS ポリシーがアクティブでない場合は「-」が表示されます。 |

| アクセスログのフォーマット指定子 | W3C ログのログフィールド              | 説明                                                                                                                                             |
|------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| %XL              | x-webcat-resp-code- full    | 応答側のスキャン中に判定された URL カテゴリの評価（完全名）。Cisco Web 利用の制御の URL フィルタリング エンジンにのみ適用されます。                                                                   |
| %XM              | x-avc-resphead- scanverdict | AVC 応答ヘッダーの判定。                                                                                                                                 |
| %Xn              | x-webroot-threat-name       | Webroot 固有の ID：（脅威の名前）このフィールドは二重引用符付きでアクセスログに書き込まれます。                                                                                          |
| %XN              | x-avc-reqbody-scanverdict   | AVC 応答本文の判定。                                                                                                                                   |
| %XO              | xAPP                        | AVC または ADC エンジンによって識別される Web アプリケーションタイプ。                                                                                                     |
| %Xp              | x-icap-verdict              | 外部 DLP サーバのスキャン判定。                                                                                                                             |
| %XP              | x-acl-added-headers         | 認識されないヘッダー。クライアント要求の追加ヘッダーのログを記録するには、このフィールドを使用します。クライアント要求を認証してリダイレクトする方法として要求にヘッダーを追加する、特殊なシステム（YouTube for Schools など）のトラブルシューティングをサポートします。 |
| %XQ              | x-webcat-req-code- abbr     | 要求側のスキャン時に決定された定義済み URL カテゴリの判定（省略形）。                                                                                                          |
| %Xr              | x-result-code               | スキャン判定情報。                                                                                                                                      |
| %XR              | x-webcat-req-code-full      | 要求側のスキャン中に判定された URL カテゴリの評価（完全名）。                                                                                                              |
| %Xs              | x-webroot-spyid             | Webroot 固有の ID：（スパイ ID）。                                                                                                                       |
| %XS              | x-request-rewrite           | 安全なブラウジング スキャンの判定。<br>セーフ サーチ機能またはサイト コンテンツ レーティング機能がトランザクションに適用されたかどうかを示します。                                                                  |
| %Xt              | x-webroot-trr               | Webroot 固有の ID：（脅威リスク比率（TRR））。                                                                                                                 |
| %XT              | x-bw-throttled              | 帯域幅制限がトランザクションに適用されたかどうかを示すフラグ。                                                                                                                |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド        | 説明                                                                                                                                                                                                                                                             |
|-------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %Xu               | xAPP タイプ               | AVC または ADC エンジンによって識別される Web アプリケーション。                                                                                                                                                                                                                        |
| %Xv               | x-webroot-scanverdict  | Webroot からのマルウェア スキャンの判定。                                                                                                                                                                                                                                      |
| %XV               | x-request-source-ip    | Web プロキシ設定で、[X-Forwarded-For を使用したクライアント IP アドレスの識別を有効にする (Enable Identification of Client IP Addresses using X-Forwarded-For) ] チェックボックスをオンにした場合のダウンストリーム IP アドレス。                                                                                            |
| %XW               | x-wbrs-score           | 復号された WBRs スコア <-10.0-10.0>。                                                                                                                                                                                                                                   |
| %Xx               | x-sophos-scanerror     | Sophos 固有の ID : (スキャンの戻りコード) 。                                                                                                                                                                                                                                 |
| %Xy               | x-sophos-file-name     | Sophos が好ましくないコンテンツを検出したファイルの名前。Sophos でのみ検出された応答に適用します。                                                                                                                                                                                                       |
| %XY               | x-sophos-scanverdict   | Sophos 固有の ID : (スキャン判定) 。                                                                                                                                                                                                                                     |
| %Xz               | x-sophos-virus-name    | Sophos 固有の ID : (脅威の名前) 。                                                                                                                                                                                                                                      |
| %XZ               | x-resp-dvs-verdictname | <p>どのスキャンエンジンがイネーブルになっているかに関係なく、マルウェア カテゴリを提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。</p> <p>このフィールドは、二重引用符付きでアクセスログに書き込まれます。</p>                                                                                                |
| %X#1#             | x-amp-verdict          | <p>Advanced Malware Protection ファイルスキャンからの判定 :</p> <ul style="list-style-type: none"> <li>• 0 : 悪意のないファイル。</li> <li>• 1 : ファイル タイプが原因で、ファイルがスキャンされなかった。</li> <li>• 2 : ファイル スキャンがタイムアウト。</li> <li>• 3 : スキャン エラー。</li> <li>• 3 よりも大きい値 : 悪意のあるファイル。</li> </ul> |



| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド     | 説明                                                                                                                                                                                                                          |
|-------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %X#2#             | x-amp-malware-name  | Advanced Malware Protection ファイルスキャンで判定された脅威の名前。「-」は脅威がないことを示します。                                                                                                                                                           |
| %X#3#             | x-amp-score         | Advanced Malware Protection ファイルスキャンのレピュテーションスコア。<br><br>このスコアは、クラウドレピュテーション サービスがファイルを正常と判定できない場合にのみ使用されます。<br><br>詳細については、 <a href="#">ファイルレピュテーションフィルタリングとファイル分析</a> , on page 477 の「脅威スコアとレピュテーションしきい値」に関する情報を参照してください。 |
| %X#4#             | x-amp-upload        | アップロードおよび分析要求のインジケータ：<br><br>「0」は、Advanced Malware Protection で分析用にファイルのアップロードが要求されなかったことを示します。<br><br>「1」は、Advanced Malware Protection で分析用にファイルのアップロードが要求されたことを示します。                                                      |
| %X#5#             | x-amp-filename      | ダウンロードして分析するファイルの名前。                                                                                                                                                                                                        |
| %X#6#             | x-amp-sha           | このファイルの SHA-256 ID。                                                                                                                                                                                                         |
| %y                | cs-method           | 方式。                                                                                                                                                                                                                         |
| %Y                | cs-url              | URL 全体。                                                                                                                                                                                                                     |
| %:>A              | x-p2p-adc-svc-time  | ADC プロセスからの応答を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。                                                                                                                                                                         |
| %:a>              | x-p2p-adc-wait-time | Web プロキシが要求を送信後、ADC プロセスからの応答を受信する待機時間。                                                                                                                                                                                     |
| %:e<              | x-p2p-amp-svc-time  | AMP スキャンエンジンからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。                                                                                                                                                                     |

| アクセス ログのフォーマット指定子 | W3C ログのログ フィールド               | 説明                                                        |
|-------------------|-------------------------------|-----------------------------------------------------------|
| %:e>              | x-p2p-amp-wait-time           | Web プロキシが要求を送信後、AMP スキャンエンジンからの応答を受信する待機時間。               |
| 該当なし              | x-hierarchy-origin            | 要求コンテンツを取得するために接続したサーバを示すコード (DIRECT/www.example.com など)。 |
| 該当なし              | x-resultcode-httpstatus       | 結果コードおよび HTTP 応答コード (間をスラッシュ (/) で区切ります)。                 |
| 該当なし              | x-archivescan-verdict         | アーカイブ検査の判定を表示します。                                         |
| 該当なし              | x-archivescan-verdict- reason | アーカイブスキャンでブロックされるファイルの詳細。                                 |
| %XU               | 該当なし                          | 将来のために予約済み。                                               |

#### 関連項目

- [アクセス ログ ファイル内の Web プロキシ情報, on page 686。](#)
- [W3C アクセス ログの解釈, on page 712。](#)

## マルウェア スキャンの判定値

マルウェア スキャンの判定は、マルウェアを含む可能性を判別する、URL 要求またはサーバ応答に割り当てられた値です。Webroot、McAfee、および Sophos のスキャン エンジン、マルウェア スキャンの判定を DVS エンジンに返し、DVS エンジンが要求をモニタするかブロックするかを決定できるようにします。特定のアクセス ポリシーに対するアンチマルウェア設定を編集した場合、各マルウェア スキャンの判定は、[アクセス ポリシー (Access Policies)] > [レピュテーションおよびマルウェア対策設定 (Reputation and Anti-Malware Settings)] ページにリストされているマルウェア カテゴリに対応します。

以下のリストは、さまざまなマルウェア スキャンの判定値および対応するマルウェア カテゴリを示しています。

| マルウェア スキャンの判定値 | マルウェア カテゴリ |
|----------------|------------|
| -              | 設定しない      |
| 0              | 不明         |
| 1              | スキャンしない    |
| 2              | タイムアウト     |

| マルウェア スキャンの判定値 | マルウェア カテゴリ        |
|----------------|-------------------|
| 3              | エラー               |
| 4              | スキャン不可            |
| 10             | 一般的なスパイウェア        |
| 12             | ブラウザ ヘルパー オブジェクト  |
| 13             | アドウェア             |
| 14             | システム モニタ          |
| 18             | 商用システム モニタ        |
| 19             | ダイヤラ              |
| 20             | ハイジャッカー           |
| 21             | フィッシング URL        |
| 22             | トロイのダウンローダ        |
| 23             | トロイの木馬            |
| 24             | トロイのフィッシャ         |
| 25             | ワーム               |
| 26             | 暗号化ファイル           |
| 27             | ウィルス              |
| 33             | その他のマルウェア         |
| 34             | PUA               |
| 35             | 中断                |
| 36             | アウトブレイク ヒューリスティック |
| 37             | 既知の悪意のある高リスク ファイル |

#### 関連項目

- [アクセス ログ ファイル内の Web プロキシ情報, on page 686。](#)
- [W3C アクセス ログの解釈, on page 712。](#)

## ロギングのトラブルシューティング

- [アクセス ログ エントリにカスタム URL カテゴリが表示されない, on page 757](#)
- [HTTPS トランザクションのロギング, on page 757](#)
- [アラート：生成データのレートを維持できない \(Unable to Maintain the Rate of Data Being Generated\) , on page 757](#)
- [W3C アクセス ログでサードパーティ製ログ アナライザ ツールを使用する場合の問題, on page 758](#)

## トラブルシューティング

この章で説明する内容は、次のとおりです。

- [一般的なトラブルシューティングとベスト プラクティス \(740 ページ\)](#)
- [FIPS モードの問題 \(740 ページ\)](#)
- [認証に関する問題 \(741 ページ\)](#)
- [オブジェクトのブロックに関する問題 \(743 ページ\)](#)
- [ブラウザに関する問題 \(744 ページ\)](#)
- [DNS に関する問題 \(744 ページ\)](#)
- [フェールオーバーの問題 \(744 ページ\)](#)
- [機能キーの期限切れ \(745 ページ\)](#)
- [FTP に関する問題 \(745 ページ\)](#)
- [アップロード/ダウンロード速度の問題 \(746 ページ\)](#)
- [ハードウェアに関する問題 \(748 ページ\)](#)
- [HTTPS/復号/証明書に関する問題 \(748 ページ\)](#)
- [Identity Services Engine に関する問題 \(751 ページ\)](#)
- [カスタム URL カテゴリおよび外部 URL カテゴリに関する問題 \(755 ページ\)](#)
- [ロギングに関する問題 \(756 ページ\)](#)
- [ポリシーに関する問題 \(758 ページ\)](#)
- [ファイル レピュテーションとファイル分析に関する問題 \(764 ページ\)](#)
- [リブートの問題 \(765 ページ\)](#)
- [サイトへのアクセスに関する問題 \(766 ページ\)](#)
- [アップストリーム プロキシに関する問題 \(767 ページ\)](#)

- [仮想アプライアンス](#) (768 ページ)
- [WCCP に関する問題](#) (769 ページ)
- [パケット キャプチャ](#) (769 ページ)
- [サポートの使用](#) (771 ページ)

## 一般的なトラブルシューティングとベスト プラクティス

以下のカスタム フィールドを含むようにアクセス ログを設定します。

%u、%g、%m、%k、%L（これらの値は大文字と小文字が区別されます）。

これらのフィールドの説明については、[アクセス ログのフォーマット指定子と W3C ログ ファイルのフィールド](#), on page 721 を参照してください。

設定の手順については、[アクセス ログのカスタマイズ](#), on page 714 および [ログ サブスクリプションの追加および編集](#), on page 676 を参照してください。

## FIPS モードの問題

Secure Web Applianceを AsyncOS 10.5 にアップグレードして、FIPS モードおよび CSP 暗号化をイネーブルにした後に、暗号化と証明書に関する問題が発生した場合は、次の項目を確認してください。

- [CSP 暗号化](#) (740 ページ)
- [証明書の検証](#) (740 ページ)

## CSP 暗号化

FIPS モードの CSP 暗号化がイネーブルになる前に動作していた機能が、暗号化がイネーブルになった後に動作しなくなった場合は、CSP 暗号化に問題があるかどうかを判別します。CSP 暗号化および FIPS モードをディセーブルにして、機能をテストします。動作する場合は、FIPS モードをイネーブルにして再びテストします。動作する場合は、CSP 暗号化をイネーブルにして再びテストします。「[FIPS モードの有効化または無効化](#) (195 ページ)」を参照してください。

## 証明書の検証

AsyncOS 10.5 にアップグレードする前に Secure Web Applianceで受け入れられた証明書は、再アップロードしたときに、アップロード方法に関係なく拒否される可能性があります。（つまり、[HTTPS プロキシ (HTTPS Proxy)]、[証明書管理 (Certificate Management)]、[SaaS のアイデンティティプロバイダ (Identity Provider for SaaS)]、ISE 設定、認証設定などの UI ページを使用した場合も、certconfig CLI コマンドを使用した場合も）拒否されることがあります。

証明書の署名者 CA が「カスタムの信頼できる証明機関」として [証明書の管理 (Certificate Management)] ページ ([ネットワーク (Network)] > [証明書管理 (Certificate Management)])

ページで追加されていることを確認してください。証明書パス全体を信頼することができない場合は、証明書を Secure Web Appliance にアップロードできません。

また、古い設定をリロードすると、含まれている証明書が信頼されなくなって、リロードに失敗することがあります。保存された設定をロードする間に、これらの証明書を置き換えてください。



(注) すべての証明書検証エラーは、監査ログ (/data/pub/audit\_logs/audit\_log.current) に記録されます。

## 認証に関する問題

- 認証の問題のトラブルシューティング ツール, on page 741
- 認証の失敗による通常動作への影響, on page 741
- LDAP に関する問題, on page 742
- 基本認証に関する問題, on page 742
- シングル サインオンに関する問題, on page 743
- 以下の項も参照してください。
  - 一般的なトラブルシューティングとベスト プラクティス, on page 740
  - HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する, on page 759
  - 認証をサポートしていない URL にアクセスできない, on page 766
  - クライアント要求がアップストリーム プロキシで失敗する, on page 767

## 認証の問題のトラブルシューティング ツール

Kerberos チケットのキャッシュを表示および消去するための KerbTray または klist (どちらも Windows Server Resource Kit に付属)。Active Directory を表示および編集するための Active Directory Explorer。Wireshark は、ネットワークのトラブルシューティングに使用できるパケット アナライザです。

## 認証の失敗による通常動作への影響

一部のユーザーエージェントまたはアプリケーションは、認証に失敗してアクセスを拒否されると、Secure Web Appliance への要求の送信を繰り返します。その結果、マシン クレデンシャルを使用して、Active Directory サーバへの要求の送信が繰り返されるので、運用に悪影響を及ぼすことがあります。

最適な結果を得るには、これらのユーザーエージェントの認証をバイパスします。「[問題のあるユーザー エージェントの認証のバイパス](#), on page 120」を参照してください。

## LDAP に関する問題

- [NTLMSSP に起因する LDAP ユーザーの認証の失敗, on page 742](#)
- [LDAP 参照に起因する LDAP 認証の失敗, on page 742](#)

### NTLMSSP に起因する LDAP ユーザーの認証の失敗

LDAP サーバーは NTLMSSP をサポートしていません。一部のクライアントアプリケーション（Internet Explorer など）は、NTLMSSP と Basic の選択肢が与えられたときに、常に NTLMSSP を選択します。以下の条件がすべて該当する場合は、ユーザーの認証に失敗します。

- ユーザーが LDAP レルムにのみ存在する。
- 識別プロファイルで LDAP レルムと NTLM レルムの両方を含むシーケンスを使用している。
- 識別プロファイルで「基本または NTLMSSP」認証方式を使用している。
- ユーザーが Basic を介して NTLMSSP を選択するアプリケーションから要求を送信する。

上記の条件の少なくとも1つが該当する場合は、認証プロファイル、認証レルム、またはアプリケーションを再設定してください。

### LDAP 参照に起因する LDAP 認証の失敗

以下の条件がすべて該当する場合は、LDAP 認証に失敗します。

- LDAP 認証レルムで Active Directory サーバーを使用している。
- Active Directory サーバーが別の認証サーバーへの LDAP 参照を使用している。
- 参照された認証サーバが Secure Web Appliance で使用できない。

回避策：

- アプライアンスで LDAP 認証レルムを設定するときに、Active Directory フォレストにグローバル カタログ サーバー（デフォルト ポートは 3268）を指定します。
- `advancedproxyconfig > authentication` CLI コマンドを使用して、LDAP 参照をディセーブルにします。デフォルトでは、LDAP 参照はディセーブルになります。

## 基本認証に関する問題

- [基本認証の失敗, on page 743](#)

### 関連する問題

- [アップストリーム プロキシが基本クレデンシャルを受け取らない, on page 767](#)

## 基本認証の失敗

基本認証方式を使用する場合、AsyncOS for Web では 7 ビット ASCII 文字のパスフレーズのみがサポートされます。パスフレーズに 7 ビット ASCII 以外の文字が含まれていると、基本認証は失敗します。

## シングル サインオンに関する問題

- エラーによりユーザーがクレデンシャルを要求される, [on page 743](#)

### エラーによりユーザーがクレデンシャルを要求される

Secure Web Appliance が WCCP v2 対応デバイスに接続されている場合、NTLM 認証が機能しないことがあります。透過 NTLM 認証を適切に実行しない、厳格にロックダウンされた Internet Explorer バージョンを使ってユーザーが要求を行っており、アプライアンスが WCCP v2 対応デバイスに接続されている場合、ブラウザはデフォルトで基本認証を使用します。その結果、認証クレデンシャルが不要な場合でも、ユーザーはクレデンシャルの入力を要求されます。

#### 回避策

Internet Explorer で、[ローカル イン트라ネット] ゾーンの [信頼済みサイト] リストに Secure Web Appliance のリダイレクト ホスト名を追加します ([ツール] > [インターネット オプション] > [セキュリティ] タブ)。

## オブジェクトのブロックに関する問題

- 一部の Microsoft Office ファイルがブロックされない, [on page 743](#)
- DOS の実行可能オブジェクト タイプをブロックすると、Windows OneCare のアップデートがブロックされる, [on page 743](#)

### 一部の Microsoft Office ファイルがブロックされない

[ブロックするオブジェクト タイプ (Block Object Type)] セクションで Microsoft Office ファイルをブロックすると、一部の Microsoft Office ファイルがブロックされない可能性があります。

すべての Microsoft Office ファイルをブロックする必要がある場合は、[ブロックする MIME タイプ (Block Custom MIME Types)] フィールドに **application/x-ole** を追加します。ただし、このカスタム MIME タイプをブロックすると、Visio ファイルや一部のサードパーティ アプリケーションなど、すべての Microsoft 複合オブジェクト フォーマット タイプがブロックされます。

### DOS の実行可能オブジェクト タイプをブロックすると、Windows OneCare のアップデートがブロックされる

DOS の実行可能オブジェクト タイプをブロックするように Secure Web Appliance を設定すると、Windows OneCare のアップデートがブロックされます。



## ブラウザに関する問題

- [Firefox で WPAD を使用できない, on page 744](#)

### Firefox で WPAD を使用できない

Firefox ブラウザが WPAD による DHCP ルックアップをサポートしていない可能性があります。最新の情報については、[https://bugzilla.mozilla.org/show\\_bug.cgi?id=356831](https://bugzilla.mozilla.org/show_bug.cgi?id=356831) を参照してください。

PAC ファイルが Secure Web Appliance にホストされている場合に、Firefox（または、DHCP をサポートしていない他のブラウザ）で WPAD を使用するには、ポート 80 を介して PAC ファイルを使用するようにアプライアンスを設定します。

#### Procedure

- 
- ステップ 1** [セキュリティサービス (Security Services)] > [Web プロキシ (Web Proxy)] を選択し、[プロキシを設定する HTTP ポート (HTTP Ports to Proxy)] フィールドからポート 80 を削除します。
- ステップ 2** アプライアンスにファイルをアップロードする場合、PAC サーバーポートとしてポート 80 を使用します。
- ステップ 3** ポート 80 の Web プロキシを指し示すようにブラウザが手動設定されている場合は、[プロキシを設定する HTTP ポート (HTTP Ports to Proxy)] フィールドで、別のポートを指し示すようにブラウザを再設定します。
- ステップ 4** PAC ファイルのポート 80 への参照を変更します。
- 

## DNS に関する問題

- [アラート : DNS キャッシュのブートに失敗 \(Failed to bootstrap the DNS cache\) , on page 744](#)

### アラート : DNS キャッシュのブートに失敗 (Failed to bootstrap the DNS cache)

アプライアンスのリブート時に、「DNS キャッシュのブートに失敗 (Failed to bootstrap the DNS cache)」というメッセージを含むアラートが生成された場合は、システムがプライマリ DNS サーバーに接続できなかったことを示しています。この事象は、ネットワーク接続が確立される前に DNS サブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

## フェールオーバーの問題

- [フェールオーバーの誤った設定, on page 745](#)
- [仮想アプライアンスでのフェールオーバーに関する問題 , on page 745](#)

## フェールオーバーの誤った設定

フェールオーバーグループを誤って設定すると、複数のプライマリプライアンスをもたらしたり、その他のフェールオーバーの問題が発生したりする可能性があります。failoverconfig CLI コマンドの testfailovergroup サブコマンドを使用して、フェールオーバーの問題を診断します。

例：

```
wsa.wga> failoverconfig
Currently configured failover profiles:
1. Failover Group ID: 61
 Hostname: failoverV4Pl.wga, Virtual IP: 10.4.28.93/28
 Priority: 100, Interval: 3 seconds
 Status: PRIMARY
Choose the operation you want to perform:
- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)
[> testfailovergroup
Failover group ID to test (-1 for all groups):
[> 61
```

## 仮想プライアンスでのフェールオーバーに関する問題

仮想プライアンス上に展開している場合は、ハイパーバイザのインターフェイス/仮想スイッチが無差別モードを使用するように設定されていることを確認してください。

## 機能キーの期限切れ

(Webインターフェイスから) アクセスしようとしている機能の機能キーの有効期限が切れている場合は、シスコの担当者またはサポート組織までご連絡ください。

## FTP に関する問題

- [URL カテゴリが一部の FTP サイトをブロックしない, on page 746](#)
- [大規模 FTP 転送の切断, on page 746](#)
- [ファイルのアップロード後に FTP サーバーにゼロ バイト ファイルが表示される, on page 746](#)
- [Chrome ブラウザが FTP-over-HTTP 要求でユーザー エージェントとして検出されない, on page 746](#)
- 以下の項も参照してください。
  - [アップストリーム プロキシ経由で FTP 要求をルーティングできない, on page 768](#)
  - [HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する, on page 759](#)

## URL カテゴリが一部の FTP サイトをブロックしない

ネイティブ FTP 要求が FTP プロキシに透過的にリダイレクトされる場合、FTP サーバーに対するホスト名情報は含まれず、IP アドレス情報だけが含まれます。そのため、要求の宛先がこれらのサーバーである場合でも、ホスト名情報しか持っていない一部の定義済み URL カテゴリと Web レピュテーションフィルタが、ネイティブ FTP 要求と一致しくなくなります。これらのサイトへのアクセスをブロックする場合は、サイトの IP アドレスを使用してサイト用のカスタム URL カテゴリを作成する必要があります。

## 大規模 FTP 転送の切断

FTP プロキシと FTP サーバーとの接続が遅い場合、特に、Cisco データセキュリティフィルタがイネーブルのときに、大きなファイルのアップロードに時間がかかることがあります。そのため、FTP プロキシがファイル全体をアップロードする前に FTP クライアントがタイムアウトしてしまい、トランザクション失敗の通知を受け取る場合があります。しかし、トランザクションは失敗しておらず、バックグラウンドで続行され、FTP プロキシによって完了されません。

FTP クライアントのアイドルタイムアウト値を適切に増加することにより、この問題を回避できます。

## ファイルのアップロード後に FTP サーバーにゼロ バイト ファイルが表示される

発信マルウェア対策スキャンによって FTP プロキシがアップロードをブロックすると、FTP クライアントは FTP サーバー上にゼロ バイト ファイルを作成します。

## Chrome ブラウザが FTP-over-HTTP 要求でユーザー エージェントとして検出されない

FTP-over-HTTP 要求では、Chrome ブラウザはユーザー エージェント文字列を含まないためユーザー エージェントとして検出されません。

## アップロード/ダウンロード速度の問題

Secure Web Appliance は、数千ものクライアントとサーバーの接続を並行して処理するように設計されています。また、送信/受信バッファのサイズは安定性を犠牲にすることなく、最適なパフォーマンスを実現するように設定されています。通常、実際の用途は、多数の一時的な接続で構成されたブラウザトラフィックです。これには受信パケットステアリング (RPS) データと受信フローステアリング (RFS) データが含まれ、Secure Web Appliance が最適化されています。

ただし、プロキシ経由で大容量ファイルを転送する場合などは、アップロードまたはダウンロード速度が著しく低下することがあります。たとえば、10 Mbps の回線で Secure Web Appliance を通じて 100 MB のファイルをダウンロードすると、サーバーからファイルを直接ダウンロードするよりも約 7 ～ 8 倍の時間がかかる可能性があります。

大容量ファイル転送が多数行われる特異な環境では、この問題を改善するために `networktuning` コマンドを使用して送信/受信バッファのサイズを増やすことができますが、そうするとネットワーク メモリが枯渇してシステムの安定性に影響が生じる可能性もあります。 `networktuning`

コマンドの詳細については、[Secure Web Appliance CLI コマンド, on page 780](#)を参照してください。



**Caution** TCP 受信/送信バッファ制御ポイントとその他の TCP バッファ パラメータを変更する場合は、注意が必要です。副次的な影響を理解している場合にのみ、`networktuning` コマンドを使用してください。

自動送受信バッファは、`networktuning`によってデフォルトで有効になっていますが、他のネットワーク チューニング パラメータは変更できます。送信バッファと受信バッファに高い値を設定すると、高負荷シナリオで不安定になる可能性があることに注意してください。Cisco Secure Web Appliance は、アプライアンスの推奨 RPS の範囲内で、大きなファイルのダウンロードの最大 10% を処理できます。

メモリ負荷が原因で Cisco Secure Web Appliance が不安定になっていることに気付いた場合は、CLI から `networktuning` コマンドを使用して、自動送受信バッファを無効にできます。この調整により、低速のダウンロード速度で多数の並列ダウンロードがサポートされます。

`networktuning` コマンドの使用例を以下に示します。デフォルトの `mbuf` クラスタ値は、SWA モデルに基づいて設定されます。

```
networktuning
sendspace = 8192-2097152
recvspace = 8192-2097152
send-auto = 1 [Remember to disable miscellaneous > advancedproxy > send buf auto tuning]
recv-auto = 1 [Remember to disable miscellaneous > advancedproxy > recv buf auto tuning]
mbuf clusters = 252470-1000000
sendbuf-max = 2097152
recvbuf-max = 2097152
```

## 質問

これらのパラメータは何ですか。

Secure Web Applianceには、固有のニーズに合わせて変更できる複数のバッファと最適化アルゴリズムがあります。バッファサイズは、「最も一般的な」導入シナリオに合わせて初めから最適化されています。ただし、より高速の接続ごとのパフォーマンスが必要な場合に大きいバッファ サイズを使用できますが、全体的なメモリ使用量が増加します。そのため、バッファ サイズの増加は、システムで使用可能なメモリの範囲内にする必要があります。送信/受信スペース変数は、ソケット経由の通信用にデータを保存するために使用できるバッファサイズを制御します。自動送信/受信オプションを使用して、送信/受信 TCP ウィンドウサイズの動的スケールリングを有効および無効にします（これらのパラメータは、FreeBSD カーネルに適用されます）。

これらの例の値はどのように決定されましたか。

この「問題」が発生したお客様のネットワークでさまざまな値のセットをテストして、これらの値に絞りました。その後、シスコのラボで安定性の変化とパフォーマンスの向上についてさらにテストしました。自己責任で、これら以外の値を自由に使用できます。

## ハードウェアに関する問題

- アプライアンスの電源の再投入, on page 748
- アプライアンスの状態およびステータス インジケータ, on page 748
- アラート : 380 または 680 ハードウェアでバッテリー再学習タイムアウト (RAID イベント) (Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware), on page 748

### アプライアンスの電源の再投入

重要x80 または x90 アプライアンスの電源を再投入する場合は、アプライアンスが起動するまで (すべての LED が緑色になるまで) 少なくとも 20 分間待ってから、電源ボタンを押してください。

### アプライアンスの状態およびステータス インジケータ

ハードウェア アプライアンスの前面/背面パネルのライトは、アプライアンスの状態およびステータスを示します。これらのインジケータの説明については、『Cisco x90 Series Content Security Appliances Installation and Maintenance Guide』など、<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html> [英語] から入手可能なハードウェア ガイドを参照してください。

温度範囲など、アプライアンスの仕様についてもこれらのマニュアルで確認できます。

### アラート : 380 または 680 ハードウェアでバッテリー再学習タイムアウト (RAID イベント) (Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware)

このアラートは、問題を示している場合と示していない場合があります。バッテリー再学習タイムアウト自体は、RAID コントローラに問題があることを示すものではありません。コントローラは、後続の再学習で回復します。以降 48 時間他の RAID アラートに関する電子メールを監視して、この問題が他の問題の副作用ではないことを確認してください。システムから他の RAID タイプのアラートが示されない場合は、この警告を無視してかまいません。

## HTTPS/復号/証明書に関する問題

- URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス, on page 749
- HTTPS 要求の失敗, on page 749
- 特定 Web サイトの復号のバイパス, on page 750
- 埋め込み/参照コンテンツのブロックの例外に対する条件および制約事項, on page 750
- アラート : セキュリティ証明書に関する問題 (Problem with Security Certificate), on page 751
- 以下の項も参照してください。
  - HTTPS トランザクションのロギング, on page 757
  - HTTPS に対してアクセス ポリシーを設定できない, on page 758

- [HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する, on page 759](#)

## URL カテゴリ基準を使用しているルーティングポリシーによる HTTPS サイトへのアクセス

透過的にリダイレクトされた HTTPS 要求の場合、Web プロキシは宛先サーバーとやり取りして、サーバー名とサーバーが属する URL カテゴリを判別する必要があります。したがって、Web プロキシがルーティング ポリシー グループのメンバーシップを評価する時点では、まだ宛先サーバーとやり取りしていないので、HTTPS 要求の URL カテゴリが不明です。Web プロキシが URL カテゴリを認識していない場合、情報が不足しているために透過的 HTTPS 要求をユーザー定義のルーティングポリシーと一致させることはできません。

その結果、どのルーティングポリシーグループにも、どの識別プロファイルにもメンバーシップ基準がない場合は、透過的にリダイレクトされる HTTPS トランザクションのみがルーティングポリシーと一致します。ユーザー定義のルーティングポリシーまたは識別プロファイルが URL カテゴリ単位でメンバーシップを定義している場合は、透過的 HTTPS トランザクションはデフォルトのルーティングポリシーグループと一致します。

## HTTPS 要求の失敗

- [IP ベースのサロゲートと透過的要求を含む HTTPS, on page 749](#)
- [カスタムおよびデフォルト カテゴリの異なるクライアントの「Hello」動作, on page 749](#)

### IP ベースのサロゲートと透過的要求を含む HTTPS

HTTPS 要求が、以前の HTTP 要求の認証情報を利用できないクライアントから発信された場合、AsyncOS は HTTPS プロキシの設定に応じて、HTTPS 要求に失敗するか、またはユーザーを認証するために HTTPS 要求を復号します。この動作を定義するには、[セキュリティサービス (Security Services)] > [HTTPS プロキシ (HTTPS Proxy)] ページで [HTTPS 透過的要求 (HTTPS Transparent Request)] 設定を使用します。「復号ポリシー」のトピックの「HTTPS プロキシの有効化」に関する項を参照してください。

### カスタムおよびデフォルト カテゴリの異なるクライアントの「Hello」動作

パケット キャプチャをスキャンすると、カスタム カテゴリおよびデフォルト (Web) カテゴリの HTTPS 復号パススルー ポリシーに対して別々の時間で「Client Hello」ハンドシェイクが送信されます。

デフォルト カテゴリを介した HTTPS ページのパススルーでは、要求元から Client Hello を受信する前に Client Hello が送信され、接続が失敗します。カスタム URL カテゴリを介した HTTPS ページのパススルーでは、要求元から Client Hello を受信した後に Client Hello が送信され、接続が成功します。

対応策として、SSL 3.0 のみと互換性がある Web ページのパススルー アクションを使用して、カスタム URL カテゴリを作成することができます。

## 特定 Web サイトの復号のバイパス

HTTPS サーバーへのトラフィックが、Web プロキシなどのプロキシサーバーによって復号されると、一部の HTTPS サーバーは期待どおりに機能しなくなります。たとえば、セキュリティの高い銀行のサイトなど、一部の Web サイトとそれらに関連する Web アプリケーションおよびアプレットは、オペレーティングシステムの証明書ストアを使用するのではなく、信頼できる証明書のハードコードされたリストを維持します。

すべてのユーザーがこれらのタイプのサイトにアクセスできるようにするには、これらのサーバーへの HTTPS トラフィックの復号をバイパスします。

### Procedure

**ステップ 1** 拡張プロパティを設定して、影響を受ける HTTPS サーバーを含むカスタム URL カテゴリを作成します。

**ステップ 2** メンバーシップの一環としてステップ 1 で作成されたカスタム URL カテゴリを使用する復号ポリシーを作成し、カスタム URL カテゴリに対するアクションを [通過 (Pass Through)] に設定します。

## 埋め込み/参照コンテンツのブロックの例外に対する条件および制約事項

Referer ベースの例外は、アクセス ポリシーでのみサポートされます。HTTPS トラフィックでこの機能を使用するには、アクセス ポリシーで例外を定義する前に、例外用に選択する URL カテゴリの HTTPS 復号を設定する必要があります。ただし、この機能は特定の条件下では機能しません。



**Note** 時間範囲が設定されている場合、最も高い優先順位が割り当てられます。時間範囲クォータに達した場合、リファラは機能しません。

- 接続がトンネル化されていて HTTPS 復号が有効になっていない場合、この機能は HTTPS サイトに発行される要求に対して機能しません。
- RFC 2616 に従って、ブラウザクライアントにはオープンに/匿名で参照するためのトグルスイッチが用意されている場合があります。これによって、Referer および参照元情報の送信をそれぞれ有効/無効にすることができます。この機能は Referer ヘッダーのみに依存しており、それらの送信をオフにするとこの機能は使用できなくなります。
- RFC 2616 に従って、参照元ページがセキュアなプロトコルで転送された場合、クライアントには（セキュアでない）HTTP 要求の Referer ヘッダー フィールドは含まれません。そのため、HTTPS ベースのサイトから HTTP ベースのサイトに対するすべての要求には Referer ヘッダーが含まれず、この機能は期待どおりに動作しません。
- 復号ポリシーが設定されている場合（カスタムカテゴリが復号ポリシーと一致する場合やアクションがドロップに設定されている場合など）、そのカテゴリのすべての着信要求はドロップされ、バイパスは実行されません。



## アラート：セキュリティ証明書に関する問題（Problem with Security Certificate）

通常、アプライアンスで生成またはアップロードされるルート証明書情報は、信頼できるルート認証局としてクライアントアプリケーションで認識されません。ユーザーが HTTPS 要求を送信すると、大部分の Web ブラウザでは、デフォルトで、Web サイトのセキュリティ証明書に問題があることを知らせる警告メッセージがクライアントアプリケーションによって表示されます。通常、エラーメッセージには、Web サイトのセキュリティ証明書が信頼できる認証局によって発行されていないこと、または Web サイトが未知の認証局によって認証されていることが表示されます。クライアントアプリケーションによっては、この警告メッセージがユーザーに示されず、ユーザーは承認されない証明書を受け入れることができません。



### Note

**Mozilla Firefox ブラウザ**：Mozilla Firefox ブラウザで使用するには、アップロードする証明書に「basicConstraints=CA:True」を含める必要があります。この制約により、Firefox は、信頼されたルート認証局としてルート証明書を認識できるようになります。

## Identity Services Engine に関する問題

- [ISE 問題のトラブルシューティング ツール, on page 751](#)
- [ISE サーバーの接続に関する問題, on page 752](#)
- [ISE 関連の重要なログ メッセージ, on page 754](#)

## ISE 問題のトラブルシューティング ツール

以下のツールは、ISE 関連の問題をトラブルシューティングする際に役立ちます。

- ISE テスト ユーティリティ。ISE サーバーへの接続のテストに使用され、貴重な接続関連情報を提供します。これは、[Identity Services Engine] ページの [テスト開始（Start Test）] オプションです（[ISE/ISE-PIC サービスへの接続, on page 423](#)を参照）。
- ISE およびプロキシログ（以下を参照）。[ログによるシステムアクティビティのモニター, on page 665](#)
- ISE 関連の CLI コマンド `iseconfig` および `isedata`。特に `isedata` は、セキュリティ グループ タグ（SGT）のダウンロードを確認するために使用します。詳細については、[Secure Web Appliance CLI コマンド, on page 780](#)を参照してください。
- Web トラッキング機能およびポリシー トレース機能。これらを使用してポリシーの一致に関する問題をデバッグできます。たとえば、許可されるべきユーザーがブロックされた場合（または、その逆の場合）などに使用できます。詳細については、[ポリシーのトラブルシューティング ツール：ポリシー トレース, on page 761](#)を参照してください。
- [パケット キャプチャ, on page 769](#)（サポートの使用, [on page 771](#) する場合）
- 認証ステータスを確認する場合は、openssl Online Certificate Status Protocol（ocsp）ユーティリティを使用できます。これは <https://www.openssl.org/> から入手できます。



## ISE サーバーの接続に関する問題

### 証明書の問題

Secure Web Appliance と ISE サーバーは証明書を使用して正常な接続を相互認証します。したがって、一方のエンティティによって指定された各証明書を、もう一方が認識できなければなりません。たとえば、Secure Web Appliance のクライアント証明書が自己署名の場合、該当する ISE サーバーの信頼できる証明書リストに同じ証明書が含まれている必要があります。同様に、Web Appliance クライアント証明書が CA 署名付きの場合も、該当する ISE サーバーにその CA ルート証明書が存在している必要があります。同様の要件は、ISE サーバー関連の管理証明書および pxGrid 証明書にも該当します。

証明書の要件およびインストールについては、[Identity Services Engine \(ISE\) / ISE パッシブ ID コントローラ \(ISE-PIC\) サービスの概要, on page 415](#) で説明されています。証明書関連の問題が発生した場合は、以下を確認してください。

- CA 署名付き証明書を使用する場合：
  - 管理証明書および pxGrid 証明書のルート CA 署名証明書が Secure Web Appliance に存在していることを確認します。
  - Web Appliance クライアント証明書のルート CA 署名証明書が ISE サーバーの信頼できる証明書リストに含まれていることを確認します。
- 自己署名証明書を使用する場合：
  - (Secure Web Appliance で生成され、ダウンロードされた) Web Appliance クライアント証明書が ISE サーバーにアップロードされていること、および ISE サーバーの信頼できる証明書リストに含まれていることを確認します。
  - (ISE サーバーで生成され、ダウンロードされた) ISE 管理者証明書および pxGrid 証明書が Secure Web Appliance にアップロードされていること、およびこのアプライアンスの証明書リストに含まれていることを確認します。
- 期限切れの証明書：
  - アップロード時に有効だった証明書が、期限切れでないことを確認します。

### 証明書の問題を示すログ出力

以下の ISE サービス ログの抜粋は、証明書の欠落または無効な証明書による接続タイムアウトを示しています。

```
Tue Mar 24 03:56:14 2015 Debug: ISELoggerThread: Logging queue starting
Tue Mar 24 03:56:14 2015 Info: ISEService: Successfully loaded configuration from: /data/ise/ise_se
Tue Mar 24 03:56:14 2015 Debug: Statistics loaded from file
Tue Mar 24 03:56:14 2015 Info: ISEService: RPC Server Socket :/tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: RPCServer: Starting at: /tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: ISEService: Running
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE client attempt 0
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE connection with reconnection True
Tue Mar 24 03:56:14 2015 Info: ISEService: Sending ready signal...
Tue Mar 24 03:56:14 2015 Info: ISEDynamicConfigThread: Started Server..
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Successfully created ISE client
Tue Mar 24 03:56:14 2015 Trace: ISEEngineManager: Waiting for client connection, 0 seconds of 30
Tue Mar 24 03:56:17 2015 Trace: ISEEngineManager: Waiting for client connection, 3 seconds of 30
Tue Mar 24 03:56:20 2015 Trace: ISEEngineManager: Waiting for client connection, 6 seconds of 30
Tue Mar 24 03:56:23 2015 Trace: ISEEngineManager: Waiting for client connection, 9 seconds of 30
Tue Mar 24 03:56:26 2015 Trace: ISEEngineManager: Waiting for client connection, 12 seconds of 30
Tue Mar 24 03:56:29 2015 Trace: ISEEngineManager: Waiting for client connection, 15 seconds of 30
Tue Mar 24 03:56:32 2015 Trace: ISEEngineManager: Waiting for client connection, 18 seconds of 30
Tue Mar 24 03:56:35 2015 Trace: ISEEngineManager: Waiting for client connection, 21 seconds of 30
Tue Mar 24 03:56:38 2015 Trace: ISEEngineManager: Waiting for client connection, 24 seconds of 30
Tue Mar 24 03:56:41 2015 Trace: ISEEngineManager: Waiting for client connection, 27 seconds of 30
Tue Mar 24 03:56:44 2015 Trace: ISEEngineManager: Waiting for client connection, 30 seconds of 30
Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out
Tue Mar 24 03:56:47 2015 Debug: ISEEngineManager: Stopping client...
```

Secure Web Applianceのこれらのトレースレベルログエントリは、30 秒後に ISE サーバーへの接続の試行が終了されることを示しています。

## ネットワークの問題

Identity Services Engine (ISE/ISE-PIC サービスへの接続, [on page 423](#)) で [テスト開始 (Start Test)] を実行中に ISE サーバーへの接続が失敗した場合、ポート 443 と 5222 に設定されている ISE サーバーへの接続を確認します。

ポート 5222 は公式のクライアント/サーバー Extensible Messaging and Presence Protocol (XMPP) ポートであり、ISE サーバーへの接続に使用されます。また、Jabber や Google Talk などのアプリケーションでも使用されます。ただし、一部のファイアウォールはポート 5222 をブロックするように設定されています。

接続の確認に使用できるツールには、tcpdump があります。

## ISE サーバーの接続に関するその他の問題

Secure Web Applianceが ISE サーバーへの接続を試みたときに、以下の問題によって失敗することがあります。

- ISE サーバーのライセンスの期限が切れている。
- ISE サーバーの [管理 (Administration)] > [pxGrid サービス (pxGrid Services)] ページで、pxGrid ノードのステータスが [未接続 (not connected)] になっている。このページで [自動登録の有効化 (Enable Auto-Registration)] がオンになっていることを確認してください。

- 失効した Secure Web Appliance クライアント（特に「test\_client」または「pxgrid\_client」）が、ISE サーバー上に存在する。これらは削除する必要があります。ISE サーバーの [管理 (Administration)] > [pxGrid サービス (pxGrid Services)] > [クライアント (Clients)] を参照してください。
- すべてのサービスが起動して実行される前に、Secure Web Appliance が ISE サーバーへの接続を試みている。  
ISE サーバーに対する一部の變更（証明書のアップデートなど）では、ISE サーバーまたはそこで実行されているサービスの再起動が必要です。この間に ISE サーバーへの接続を試みると失敗しますが、最終的に接続に成功します。

## ISE 関連の重要なログメッセージ

ここでは、Secure Web Appliance における ISE 関連の重要なログメッセージについて説明します。

- Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out

Secure Web Appliance の ISE プロセスが 30 秒以内に ISE サーバーに接続できませんでした。

- Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: WSA Client cert/key missing. Please check ISE config

Web Appliance クライアント証明書とキーが Secure Web Appliance の [Identity Service Engine] 設定ページでアップロードされなかったか、生成されませんでした。

- Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: ISE service exceeded maximum allowable disconnect duration with ISE server

Secure Web Appliance の ISE プロセスが 120 秒以内に ISE サーバーに接続できず、終了しました。

- Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Subscription to updates failed ...

Secure Web Appliance の ISE プロセスが、アップデートのために ISE サーバーに登録できませんでした。

- Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Could not create ISE client: ...

ISE サーバー接続用に Secure Web Appliance の ISE クライアントを作成するときに、内部エラーが発生しました。

- Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Bulk Download thread failed: ...

この内部エラーは、接続または再接続時に SGT の一括ダウンロードに失敗したことを示しています。

- Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to start service. Error: ...

Secure Web Appliance の ISE サービスの起動に失敗しました。

- Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send ready signal ...  
Secure Web Applianceの ISE サービスが heimdall に Ready 信号を送信できませんでした。
- Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send restart signal ...  
Secure Web Applianceの ISE サービスが heimdall に再起動信号を送信できませんでした。

## カスタム URL カテゴリおよび外部 URL カテゴリに関する問題

- [外部ライブ フィード ファイルのダウンロードに関する問題 \(755 ページ\)](#)
- [.CSV ファイルの IIS サーバでの MIME タイプに関する問題 \(756 ページ\)](#)
- [コピー アンド ペーストの後にフィード ファイルの形式が不正になる \(756 ページ\)](#)

### 外部ライブ フィード ファイルのダウンロードに関する問題

カスタムおよび外部 URL カテゴリを作成および編集し、[外部ライブ フィード (External Live Feed) ] ファイル ([シスコ フィード形式 (Cisco Feed Format) ] または [Office 365 フィード形式 (Office 365 Feed Format) ] のいずれか) を提供する場合、[ファイルの取得 (Get File) ] ボタンをクリックして、指定したサーバとの接続を開始し、ファイルをダウンロードして解析する必要があります。このプロセスの進行状況と結果が表示されます。エラーが発生した場合は、進行状況と結果が説明されます。問題を修正し、もう一度ファイルのダウンロードを試します。

次の 4 種類のエラーが発生する可能性があります。

- 接続の例外

Failed to resolve server hostname : フィード ファイルの場所として指定した URL は無効です。この問題を解決するには、正しい URL を指定します。

- プロトコル エラー

Authentication failed due to invalid credentials : サーバ認証が失敗しました。サーバ接続に適切なユーザ名とパスワードを指定します。

The requested file is not found on the server : フィード ファイルに指定した URL が無効なりソースを示しています。指定したサーバで正しいファイルが使用できることを確認します。

- コンテンツ検証エラー

Failed to validate the content of the field : フィード ファイルのコンテンツが無効です。

- 解析エラー

- シスコフィード形式.csv ファイルは、1 つ以上のエントリを含む必要があります。各エントリはサイトのアドレスまたは有効な正規表現文字列で、カンマ、アドレスタイ

**.CSV ファイルの IIS サーバでの MIME タイプに関する問題**

ブ (site または regex のいずれか) が続きます。フィードファイルのエントリに対してこの表記規則に従わない場合、解析エラーがスローされます。

また、http:// または https:// を site エントリの一部としてファイルに含めないでください。エラーが発生します。つまり、www.example.com は正しく解析されますが、http://www.example.com ではエラーが発生します。

- Microsoft サーバから取得した XML ファイルは、標準の XML パーサーによって解析されます。XML タグングの矛盾にも、解析エラーとしてフラグが付きます。

解析エラーの行番号はログに含まれます。次に例を示します。

Line 8: 'www.anyurl.com' - Line is missing address or address-type field. フィードファイルの 8 行目には、有効なアドレスまたは正規表現のパターン、またはアドレスタイプは含まれていません。

Line 12: 'www.test.com' - Unknown address type. 12 行目に無効なアドレスタイプがあります。アドレスタイプは site または regex のいずれかになります。

**.CSV ファイルの IIS サーバでの MIME タイプに関する問題**

カスタムおよび外部 URL カテゴリの作成および編集中に [External Live Feed Category (外部ライブフィードファイルカテゴリ)] > [Cisco Feed Format (シスコフィード形式)] オプションの .csv ファイルを提供すると、シスコフィード形式サーバがインターネットインフォメーションサービス (IIS) のバージョン 7 または 8 ソフトウェアを実行している場合にファイルを取得する際、[406 not acceptable (406 受け入れられません)] エラーが発生する場合があります。同様に、feedsd ログでは次のような内容が報告されます。31 May 2016 16:47:22 (GMT +0200) Warning: Protocol Error: 'HTTP error while fetching file from the server'。

これは、IIS 上の .csv ファイルのデフォルトの MIME タイプが text/csv ではなく application/csv であるためです。この問題は、IIS サーバにログインし、.csv ファイルの MIME タイプのエントリを text/csv に編集することで解決できます。

**コピーアンドペーストの後にフィードファイルの形式が不正になる**

UNIX または OS X システムから Windows システムに .csv (テキスト) フィードファイルのコンテンツをコピーアンドペーストする場合、余分な改行 (\r) が自動的に追加され、フィードファイルの形式が不正になる場合があります。

.csv ファイルを手動で作成する場合や、SCP、FTP、または POST を使用して UNIX または OS X から Windows システムにファイルを転送する場合は、問題はありません。

**ロギングに関する問題**

- [アクセス ログ エントリにカスタム URL カテゴリが表示されない, on page 757](#)
- [HTTPS トランザクションのロギング, on page 757](#)
- [アラート: 生成データのレートを維持できない \(Unable to Maintain the Rate of Data Being Generated\) , on page 757](#)



- [W3C アクセス ログでサードパーティ製ログ アナライザ ツールを使用する場合の問題, on page 758](#)

## アクセス ログ エントリにカスタム URL カテゴリが表示されない

Web アクセス ポリシー グループに、[モニター (Monito)] に設定されたカスタム URL カテゴリ セットとその他のコンポーネント (Web レピュテーション フィルタ、DVS エンジンなど) がある場合に、カスタム URL カテゴリ内の URL に対する要求を許可するかブロックするかについて最終決定が行われると、要求のアクセス ログ エントリには、カスタム URL カテゴリの代わりに、定義済みの URL カテゴリが表示されます。

## HTTPS トランザクションのロギング

アクセス ログでの HTTPS トランザクションの表示は、HTTP トランザクションと似ていますが、特性は少し異なります。記録される内容は、トランザクションが HTTPS プロキシに明示的に送信されるか、または透過的にリダイレクトされるかどうかによって異なります。

- **TUNNEL**。これは、HTTPS 要求が HTTPS プロキシに透過的にリダイレクトされたときにアクセス ログに記録されます。
- **CONNECT**。これは、HTTPS 要求が HTTPS プロキシに明示的に送信されたときにアクセス ログに記録されます。

HTTPS トラフィックが復号されたときは、アクセス ログにトランザクションに対して、以下の 2 つのエントリが含まれます。

- TUNNEL または CONNECT が、処理された要求のタイプに応じて記録されます。
- HTTP 方式および復号された URL。例: 「GET https://ftp.example.com」。

完全な URL は、HTTPS プロキシがトラフィックを復号するときだけ表示されます。

## アラート : 生成データのレートを維持できない (Unable to Maintain the Rate of Data Being Generated)

内部ロギングプロセスがフルバッファにより Web トランザクションイベントをドロップする場合、AsyncOS for Web が設定されたアラート受信者にクリティカルな電子メール メッセージを送信します。

デフォルトでは、Web プロキシが非常に高い負荷を受けたときに、内部ロギングプロセスは Web プロキシの負荷を減らす際にそれらを記録するイベントをバッファします。ロギングバッファ ファイルが完全に満杯になったときに、Web プロキシはトラフィックの処理を続行しますが、ロギングプロセスはイベントの一部をアクセス ログまたは Web トラッキング レポートに記録しません。これは、Web トラフィックのスパイク時に発生する可能性があります。

ただし、アプライアンスが持続的に過剰容量になっている場合にも、ロギングバッファが満杯になることがあります。AsyncOS for Web は、ロギングプロセスがデータをドロップしなくなるまで、数分ごとにクリティカルな電子メール メッセージを送信し続けます。

クリティカルなメッセージは以下のようなテキストが含まれます。

Reporting Client: The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.

AsyncOS for Web が、このクリティカルなメッセージを継続的または頻繁に送信する場合、アプライアンスは過剰容量になっている可能性があります。Secure Web Applianceの容量を追加する必要があるかどうかを確認するには、シスコ カスタマー サポートにお問い合わせください。

## W3C アクセス ログでサードパーティ製ログ アナライザ ツールを使用する場合の問題

サードパーティ製のログアナライザツールを使用して、W3Cアクセスログを閲覧したり解析する場合は、状況に応じて[タイムスタンプ (timestamp)] フィールドを含める必要があります。W3Cの[タイムスタンプ (timestamp)] フィールドには、UNIX エポック以降の時間が表示され、ほとんどのログアナライザはこの形式の時間のみ認識します。

## ポリシーに関する問題

- [HTTPS に対してアクセス ポリシーを設定できない, on page 758](#)
- [オブジェクトのブロックに関する問題, on page 743](#)
- [識別プロファイルがポリシーから削除される, on page 759](#)
- [ポリシーの照合に失敗, on page 759](#)
- [ポリシーのトラブルシューティング ツール: ポリシー トレース, on page 761](#)
- 次のセクションも参照してください。 [URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス, on page 749](#)

## HTTPS に対してアクセス ポリシーを設定できない

HTTPS プロキシをイネーブルにすると、すべての HTTPS ポリシー決定が復号ポリシーによって処理されます。また、アクセスおよびルーティング ポリシー グループ メンバーシップを HTTPS で定義することも、HTTPS トランザクションをブロックするようにアクセス ポリシーを設定することもできなくなります。

アクセスおよびルーティング ポリシー グループの一部のメンバーシップが HTTPS によって定義されており、一部のアクセスポリシーがHTTPSをブロックする場合は、HTTPS プロキシをイネーブルにすると、それらのアクセスおよびルーティング ポリシー グループがディセーブルになります。ポリシーは、いつでもイネーブルにすることができますが、そうすると、HTTPS 関連の設定がすべて削除されます。

## オブジェクトのブロックに関する問題

- [一部の Microsoft Office ファイルがブロックされない, on page 743](#)
- [DOS の実行可能オブジェクト タイプをブロックすると、Windows OneCare のアップデートがブロックされる, on page 743](#)

## 一部の Microsoft Office ファイルがブロックされない

[ブロックするオブジェクトタイプ (Block Object Type)] セクションで Microsoft Office ファイルをブロックすると、一部の Microsoft Office ファイルがブロックされない可能性があります。

すべての Microsoft Office ファイルをブロックする必要がある場合は、[ブロックする MIME タイプ (Block Custom MIME Types)] フィールドに **application/x-ole** を追加します。ただし、このカスタム MIME タイプをブロックすると、Visio ファイルや一部のサードパーティアプリケーションなど、すべての Microsoft 複合オブジェクトフォーマットタイプがブロックされます。

## DOS の実行可能オブジェクトタイプをブロックすると、Windows OneCare のアップデートがブロックされる

DOS の実行可能オブジェクトタイプをブロックするように Secure Web Appliance を設定すると、Windows OneCare のアップデートがブロックされます。

## 識別プロファイルがポリシーから削除される

識別プロファイルをディセーブルにすると、その識別プロファイルは関連するポリシーから削除されます。識別プロファイルがイネーブルになっていることを確認し、再びポリシーに追加します。

## ポリシーの照合に失敗

- [ポリシーが適用されない, on page 759](#)
- [HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する, on page 759](#)
- [HTTPS 要求および FTP over HTTP 要求の場合にユーザーがグローバル ポリシーに一致, on page 760](#)
- [ユーザーに誤ったアクセス ポリシーが割り当てられる, on page 760](#)

## ポリシーが適用されない

複数の識別プロファイルの基準が同じである場合、AsyncOS は一致する最初の識別プロファイルにトランザクションを割り当てます。したがって、トランザクションはその他の同じ基準の識別プロファイルとは照合されず、以降の同じ基準の識別プロファイルに適用されるポリシーは照合も適用もされません。

## HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する

クレデンシャルの暗号化がイネーブルの場合は、サロゲートとして IP アドレスを使用するようにアプライアンスを設定する必要があります。

クレデンシャルの暗号化がイネーブルになっており、サロゲートタイプとして Cookie を使用するように設定されている場合、認証は HTTPS 要求や FTP over HTTP 要求で機能しません。クレデンシャルの暗号化がイネーブルの場合、Web プロキシは HTTPS 接続を使用して、クライアントを認証のために Web プロキシ自体にリダイレクトするからです。認証が成功した後、Web プロキシは元の Web サイトにクライアントをリダイレクトします。ユーザーの識別を続けるために、Web プロキシはサロゲート (IP またはクッキー) を使用する必要があります。



ただし、要求が HTTP または FTP over HTTP を使用している場合、Cookie を使用してユーザーを追跡すると、以下の動作が引き起こされます。

- **HTTPS。** Web プロキシは、復号ポリシーを割り当てる前にユーザーのアイデンティティを解決（したがって、トランザクションを復号）する必要がありますが、トランザクションを復号しない限り、Cookie を取得してユーザーを識別することはできません。
- **FTP over HTTP。** FTP over HTTP を使用して FTP サーバーにアクセスする場合のジレンマは、HTTPS サイトにアクセスする場合と同様です。Web プロキシは、アクセス ポリシーを割り当てる前にユーザーのアイデンティティを解決する必要がありますが、FTP トランザクションから Cookie を設定できません。

したがって、HTTP 要求と FTP over HTTP 要求は、認証を必要としないアクセス ポリシーとのみ一致します。通常、これらの要求は、認証を必要としないグローバル アクセス ポリシーに一致します。

### HTTPS 要求および FTP over HTTP 要求の場合にユーザーがグローバル ポリシーに一致

アプライアンスがクッキーベースの認証を使用する場合、Web プロキシは、HTTP 要求を介した HTTPS および FTP のクライアントからクッキー情報を取得しません。このため、クッキーからユーザー名を取得できません。

HTTPS 要求や FTP over HTTP 要求は、他のメンバーシップ基準に従って識別プロファイルと照合されますが、識別プロファイルで認証が必要な場合でも、Web プロキシはクライアントに認証を要求しません。代わりに、Web プロキシはユーザー名を NULL に設定し、ユーザーを未認証と見なします。

その後、ポリシーと照合して評価される際に、未認証の要求は [すべての ID (All Identities)] を指定しているポリシーとのみ一致し、[すべてのユーザー (All Users)] が適用されます。通常、これはグローバル アクセス ポリシーなどのグローバル ポリシーです。

### ユーザーに誤ったアクセス ポリシーが割り当てられる

- ネットワーク上のクライアントが、ネットワーク接続状態インジケータ (NCSI) を使用している。
- Secure Web Appliance が NTLMSSP 認証を使用している。
- 識別プロファイルが IP ベースのサロゲートを使用している。

ユーザーは自分のクレデンシャルではなく、マシンクレデンシャルを使用して識別され、その結果、誤ったアクセス ポリシーが割り当てられる場合があります。

#### 回避策：

マシン クレデンシャルのサロゲート タイムアウト値を小さくします。

## Procedure

**ステップ 1** `advancedproxyconfig > authentication` CLI コマンドを使用します。

**ステップ 2** マシン クレデンシャルのサロゲート タイムアウトを入力します。

## ポリシーのパラメータを変更した後のポリシー トレースの不一致

[アクセス ポリシー (Access Policy) ]、[識別プロファイルとユーザー (Identification Profiles and Users) ]、[1 つ以上の識別プロファイルを選択 (Select One or More Identification Profiles) ]、[選択されたグループとユーザー (Selected Groups and Users) ] など、ポリシーのパラメータを変更した場合、変更が有効になるまで数分かかります。

## ポリシーのトラブルシューティング ツール : ポリシー トレース

- [ポリシー トレース ツールについて, on page 761](#)
- [クライアント要求のトレース, on page 761](#)
- [詳細設定 : 要求の詳細, on page 763](#)
- [詳細設定 : レスポンスの詳細の上書き, on page 764](#)

### ポリシー トレース ツールについて

ポリシー トレース ツールはクライアント要求をエミュレートし、Web プロキシによる要求の処理方法を詳しく示します。Web プロキシの問題をトラブルシューティングするときに、このツールを使用し、クライアント要求を追跡してポリシー処理をデバッグできます。基本トレースを実行したり、詳細なトレース設定を行ってオプションをオーバーライドしたりできます。



**Note** ポリシー トレース ツールを使用する場合、Web プロキシはアクセス ログまたはレポート データベース内の要求を記録しません。

ポリシー トレース ツールは、要求を Web プロキシだけで使用されるポリシーと照合して評価します。これらのポリシーには、アクセス、暗号化 HTTPS 管理、ルーティング、セキュリティ、発信マルウェア スキャンがあげられます。



**Note** SOCKS および外部 DLP ポリシーは、ポリシー トレース ツールによって評価されません。

### クライアント要求のトレース



**Note** CLI コマンド `maxhttpheadersize` を使用して、プロキシ要求の最大 HTTP ヘッダー サイズを変更できます。この値を大きくすると、指定したユーザーが多数の認証グループに属しているか、または応答ヘッダーが現在の最大ヘッダーサイズよりも大きい場合に発生する可能性のあるポリシー トレースの失敗を軽減できます。このコマンドの詳細については、[Secure Web Appliance CLI コマンド, on page 780](#) を参照してください。

## Procedure

**ステップ 1** [システム管理 (System Administration)] > [ポリシー トレース (Policy Trace)] を選択します。

**ステップ 2** [送信先 URL (Destination URL)] フィールドに、トレースする URL を入力します。

**ステップ 3** (オプション) 追加のエミュレーション パラメータを入力します。

| エミュレート対象                        | 入力                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 要求を行う際に使用されるクライアントの送信元 IP アドレス。 | [クライアント IP アドレス (Client IP Address)] フィールドに IP アドレス。<br><br><b>Note</b><br>IP アドレスを指定しない場合、AsyncOS は localhost を使用します。また、SGT (セキュリティ グループ タグ) は取得できず、SGT に基づくポリシーは照合されません。                                                                                                                                                       |
| 要求を行う際に使用される認証/識別クレデンシャル。       | [ユーザー名 (User Name)] フィールドにユーザー名を入力し、[認証/識別 (Authentication/Identification)] ドロップダウン リストから [Identity Services Engine] または認証レルムを選択します。<br><br><b>Note</b><br>イネーブルになっているオプションのみを使用できます。つまり、認証オプションと ISE オプションは、両方がイネーブルになっている場合にのみ使用できます。<br><br>ここで入力するユーザーに対して認証が機能するためには、ユーザーがあらかじめ Secure Web Appliance を介して正常に認証されている必要があります。 |

**ステップ 4** [一致するポリシーの検索 (Find Policy Match)] をクリックします。

ポリシー トレースの出力が [結果 (Results)] ペインに表示されます。

### Note

[HTTPS を通過 (Pass Through HTTPS)] トランザクションでは、ポリシー トレース ツールはさらにスキャンをバイパスし、トランザクションにアクセス ポリシーは関連付けられません。同様に、[HTTPS を復号 (Decrypt HTTPS)] トランザクションでは、ツールは実際にはトランザクションを復号できず、適用されるアクセス ポリシーを決定することができません。いずれの場合も、[ドロップ (Drop)] トランザクションの場合と同様、トレースの結果には「アクセス ポリシー：適用なし (Access policy: Not Applicable)」が表示されます。

### Note

指定されたクライアント IP アドレスがルーティングできない場合、トレース結果に「接続トレース：発信サーバーへの接続：失敗 (Connection Trace: Connection to Origin Server: Failed)」と表示されます。

## What to do next

### 関連項目

- 詳細設定：要求の詳細, on page 763
- 詳細設定：レスポンスの詳細の上書き, on page 764

## 詳細設定：要求の詳細

[ポリシー トレース (Policy Trace) ] ページの [詳細設定 (Advanced) ] セクションで、[要求の詳細 (Request Details) ] ペインの設定項目を使用し、このポリシー トレース用に発信マルウェア スキャン要求を調整できます。

### Procedure

**ステップ 1** [ポリシー トレース (Policy Trace) ] ページの [詳細設定 (Advanced) ] セクションを展開します。

**ステップ 2** [要求の詳細 (Request Details) ] ペインのフィールドを必要に応じて設定します。

| 設定                                                | 説明                                                                                                       |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| プロキシ ポート (Proxy Port)                             | プロキシポートに基づいてポリシーメンバーシップをテストするトレース要求に対して、使用する特定のプロキシポートを選択します。                                            |
| ユーザー エージェント (User Agent)                          | 要求でシミュレートするユーザー エージェントを指定します。                                                                            |
| 要求の時間帯 (Time of Request)                          | 要求でシミュレートする日付と時間帯を指定します。                                                                                 |
| ファイルのアップロード (Upload File)                         | 要求でアップロードをシミュレートするローカルファイルを選択します。<br>ここでアップロードするファイルを指定する場合、Web プロキシは、GET 要求ではなく HTTP POST 要求をシミュレートします。 |
| オブジェクトのサイズ (Object Size)                          | 要求オブジェクトのサイズ (バイト単位) を入力します。キロバイト、メガバイト、またはギガバイトを表す、K、M、または G を入力できます。                                   |
| MIME タイプ (MIME Type)                              | MIME タイプを入力します。                                                                                          |
| アンチマルウェア スキャンの判定 (Anti-malware Scanning Verdicts) | Webroot、McAfee、Sophos スキャンの判定をオーバーライドするには、オーバーライドする特定タイプの判定を選択します。                                       |

**ステップ 3** [一致するポリシーの検索 (Find Policy Match) ] をクリックします。

ポリシー トレースの出力が [結果 (Results) ] ペインに表示されます。

## 詳細設定：レスポンスの詳細の上書き

[ポリシー トレース (Policy Trace)] ページの [詳細設定 (Advanced)] セクションで、[レスポンスの詳細の上書き (Response Detail Overrides)] ペインの設定項目を使用し、このポリシー トレース用に Web アクセス ポリシー レスポンスの аспек트를「調整」できます。

### Procedure

**ステップ 1** [ポリシー トレース (Policy Trace)] ページの [詳細設定 (Advanced)] セクションを展開します。

**ステップ 2** [レスポンスの詳細の上書き (Response Detail Overrides)] ペインのフィールドを必要に応じて設定します。

| 設定                                                | 説明                                                                                                              |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| URL カテゴリ (URL Category)                           | トレース応答の URL トランザクション カテゴリをオーバーライドするには、この設定を使用します。応答結果の URL カテゴリと置き換えるカテゴリを選択します。                                |
| アプリケーション (Application)                            | 同様に、トレース応答のアプリケーションカテゴリをオーバーライドするには、この設定を使用します。応答結果のアプリケーションカテゴリと置き換えるカテゴリを選択します。                               |
| オブジェクトのサイズ (Object Size)                          | 応答オブジェクトのサイズ (バイト単位) を入力します。キロバイト、メガバイト、またはギガバイトを表す、K、M、または G を入力できます。                                          |
| MIME タイプ (MIME Type)                              | MIME タイプを入力します。                                                                                                 |
| Web レピュテーション スコア (Web Reputation Score)           | Web レピュテーション スコア (-10.0 ~ 10.0) を入力します。<br>Web レピュテーション スコアを 100 にすると、「スコアなし」を意味します。                            |
| アンチマルウェア スキャンの判定 (Anti-malware Scanning Verdicts) | これらのオプションを使用して、トレース応答で提供される特定のマルウェア対策 スキャンの判定をオーバーライドします。応答結果の Webroot、McAfee、または Sophos のスキャン判定と置き換える判定を選択します。 |

**ステップ 3** [一致するポリシーの検索 (Find Policy Match)] をクリックします。

ポリシー トレースの出力が [結果 (Results)] ペインに表示されます。

## ファイル レピュテーションとファイル分析に関する問題

「[ファイル レピュテーションと分析のトラブルシューティング](#) , on page 503」を参照してください。

## リブートの問題

- KVM で動作する仮想アプライアンスがリブート時にハングアップ, on page 765
- ハードウェア アプライアンス : アプライアンスの電源のリモート リセット, on page 765

### KVM で動作する仮想アプライアンスがリブート時にハングアップ



**Note** これは KVM の問題であり、状況によって異なる場合があります。

詳細については、<https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html> および <https://bugs.launchpad.net/qemu/+bug/1329956> を参照してください。

#### Procedure

**ステップ 1** 次の点をチェックします。

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

**ステップ 2** 上記の値が Y に設定されている場合 :

a) 仮想アプライアンスを停止し、KVM カーネル モジュールを再インストールします。

```
rmmod kvm_intel modprobe kvm_intel enable_apicv=N
```

b) 仮想アプライアンスを再起動します。

### ハードウェア アプライアンス : アプライアンスの電源のリモート リセット

#### Before you begin

- IPMI バージョン 2.0 を使用してデバイスを管理できるユーティリティを取得し、設定します。
- サポートされている IPMI コマンドの使用方法を理解します。IPMI ツールのマニュアルを参照してください。

アプライアンスのハード リセットが必要な場合は、サードパーティの Platform Management (IPMI) ツールを使用してアプライアンス シャーシをリモートからリブートできます。

#### 制約事項

- リモート電源管理は、特定のハードウェアでのみ使用できます。詳細については、[リモート電源再投入の有効化](#), on page 170 を参照してください。
- この機能を使用する場合は、使用が必要になる前に、あらかじめ有効にしておく必要があります。詳細は、[リモート電源再投入の有効化](#), on page 170 を参照してください。
- 以下の IPMI コマンドだけがサポートされます : status、on、off、cycle、reset、diag、soft。サポートされていないコマンドを発行すると、「権限不足」エラーが発生します。

## Procedure

**ステップ 1** IPMI を使用して、必要なクレデンシャルと共に、先に設定したリモート電源管理ポートに割り当てられた IP アドレスに、サポートされている電源の再投入コマンドを発行します。

たとえば、IPMI をサポートする UNIX タイプのマシンからは、次のようなコマンドを発行します。

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

S195、S395、および S695 モデルの場合は、次を使用します。

```
ipmitool -I lanplus -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

ここで 192.0.2.1 は、リモート電源管理ポートに割り当てられた IP アドレスであり、remoteresetuser および passphrase は、この機能を有効にしたときに入力したクレデンシャルです。

**ステップ 2** アプライアンスが再起動されるまで、少なくとも 11 分間待ちます。

## サイトへのアクセスに関する問題

- 認証をサポートしていない URL にアクセスできない, [on page 766](#)
- POST 要求を使用してサイトにアクセスできない, [on page 767](#)
- 次のセクションも参照してください。特定 Web サイトの復号のバイパス, [on page 750](#)

### 認証をサポートしていない URL にアクセスできない

以下は、認証をサポートしていないため、Secure Web Applianceが透過モードで展開されている場合に使用できないアプリケーションのリストの一部です。

- Mozilla Thunderbird
- Adobe Acrobat アップデート
- HttpBridge
- CollabNet の Subversion
- Microsoft Windows アップデート
- Microsoft Visual Studio

回避策：認証を必要としない URL のユーザー クラスを作成します。

#### 関連項目

- 認証のバイパス, [on page 122](#)

## POST 要求を使用してサイトにアクセスできない

ユーザーの最初のクライアント要求が POST 要求で、ユーザーの認証が必要な場合、POST 本文のコンテンツは失われます。この問題は、アクセス コントロールのシングル サインオン機能を使用しているアプリケーションに対して POST 要求を行った場合に発生することがあります。

回避策：

- 最初の要求として POST を使用する URL に接続する前に、ブラウザから別の URL を要求して、最初に Web プロキシでユーザーを認証させます。
- 最初の要求として POST を使用する URL の認証をバイパスします。



**Note** アクセス コントロールを使用すると、アプリケーション認証ポリシーで設定された Assertion Consumer Service (ACS) URL の認証をバイパスできます。

関連項目

- [認証のバイパス, on page 122。](#)

## アップストリーム プロキシに関する問題

- [アップストリーム プロキシが基本クレデンシャルを受け取らない, on page 767](#)
- [クライアント要求がアップストリーム プロキシで失敗する, on page 767](#)

### アップストリーム プロキシが基本クレデンシャルを受け取らない

アプライアンスとアップストリームプロキシの両方が NTLMSP による認証を使用している場合、設定によっては、アプライアンスとアップストリームプロキシで、認証クレデンシャルを要求する無限ループが発生する可能性があります。たとえば、アップストリームプロキシでは基本認証が必要だが、アプライアンスでは NTLMSP 認証が必要な場合、アプライアンスはアップストリーム プロキシに正常に基本認証クレデンシャルを渡すことができません。これは、認証プロトコルの制限によるものです。

### クライアント要求がアップストリーム プロキシで失敗する

設定：

- Secure Web Appliance とアップストリーム プロキシ サーバが基本認証を使用している。
- ダウンストリームの Secure Web Appliance でクレデンシャルの暗号化がイネーブルになっている。



Web プロキシはクライアントから「Authorization」HTTP ヘッダーを受信しますが、アップストリーム プロキシ サーバーでは「Proxy-Authorization」HTTP ヘッダーが必要であるため、クライアント要求はアップストリーム プロキシで失敗します。

## アップストリーム プロキシ経由で FTP 要求をルーティングできない

ネットワークにFTP接続をサポートしていないアップストリームプロキシが含まれる場合は、すべてのIDに適用され、かつFTP要求にのみ適用されるルーティングポリシーを作成する必要があります。ルーティングポリシーを設定して、FTPサーバーに直接接続するか、プロキシのすべてがFTP接続をサポートしているプロキシグループに接続します。

## 仮想アプライアンス

- AsyncOS の起動中に強制リセット、電源オフ、リセットのオプションを使用しないでください, on page 768
- KVM 展開でネットワーク接続が最初は機能するが、その後失敗する, on page 768
- KVM 展開におけるパフォーマンスの低下、ウォッチドッグ問題、および高 CPU 使用率, on page 768
- Linux ホスト上で実行されている仮想アプライアンスの一般的なトラブルシューティング, on page 769

## AsyncOS の起動中に強制リセット、電源オフ、リセットのオプションを使用しないでください

仮想ホストにおける以下の操作は、ハードウェアアプライアンスのプラグを抜くことと同等であり、特に AsyncOS の起動中ではサポートされていません。

- KVM の強制リセットオプション。
- VMware の電源オフとリセットオプション。（これらのオプションは、アプライアンスが完全に起動してから安全に使用できます）。

## KVM 展開でネットワーク接続が最初は機能するが、その後失敗する

### 問題

前回の作業後にネットワーク接続が失われる。

### 解決方法

これは KVM の問題です。OpenStack ドキュメントの「KVM: Network connectivity works initially, then fails」の項を参照してください。このドキュメントは、[http://docs.openstack.org/admin-guide-cloud/content/section\\_network-troubleshoot.html](http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html) にあります。

## KVM 展開におけるパフォーマンスの低下、ウォッチドッグ問題、および高 CPU 使用率

### 問題

Ubuntu 仮想マシン上で実行しているときに、アプライアンスのパフォーマンスが低下して、ウォッチドッグの問題が発生し、アプライアンスが異常に高い CPU 使用率を示す。

#### 解決方法

Ubuntu から最新の Host OS アップデートをインストールしてください。

## Linux ホスト上で実行されている仮想アプライアンスの一般的なトラブルシューティング

#### 問題

KVM 展開で実行されている仮想アプライアンスに関する問題は、ホスト OS の設定の問題と関連している可能性があります。

#### 解決方法

『*Virtualization Deployment and Administration Guide*』のトラブルシューティングに関するセクションおよびその他の情報を参照してください。このドキュメントは、

[https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/7/pdf/Virtualization\\_Deployment\\_and\\_Administration\\_Guide/Red\\_Hat\\_Enterprise\\_Linux-7-Virtualization\\_Deployment\\_and\\_Administration\\_Guide-en-US.pdf](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf) [英語] から入手できます。

## WCCP に関する問題

- [最大ポート エントリ数, on page 769](#)

### 最大ポート エントリ数

WCCPを使用している展開では、HTTP、HTTPS、およびFTPの各ポートの合計30が最大ポート エントリ数になります。

## パケット キャプチャ

- [パケット キャプチャの開始, on page 770](#)
- [パケット キャプチャ ファイルの管理, on page 771](#)

アプライアンスでは、アプライアンスが接続されているネットワークで送受信される TCP/IP と他のパケットをキャプチャして表示できます。



**Note** パケット キャプチャ機能は UNIX の tcpdump コマンドに似ています。

Secure Web Appliance は、NIC ペアリングインターフェイスのパケットキャプチャをサポートしていません。パケットキャプチャは、アクティブなインターフェイスにのみ適用されます。たとえば、P1 と P2 の両方がペアになっている場合、P1 と P2 のどちらもユーザーインターフェイスまたは CLI で設定されません。

## パケット キャプチャの開始

### Procedure

**ステップ 1** [ヘルプとサポート (Help and Support)] > [パケット キャプチャ (Packet Capture)] を選択します。

**ステップ 2** (オプション) [設定の編集 (Edit Settings)] をクリックし、パケット キャプチャの設定を変更します。

| オプション                                         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| キャプチャ ファイル サイズ制限<br>(Capture File Size Limit) | キャプチャ ファイル を拡大できる最大サイズを指定します。[キャプチャ 期間 (Capture Duration)] が [ファイル サイズの上限に達するまでキャプチャを実行 (Run Capture Until File Size Limit Reached)] に設定されていない場合は、上限に達すると、データが破棄されて新しいファイルが開始されます。                                                                                                                                                                                                                                                                                                     |
| キャプチャ 期間<br>(Capture Duration)                | <p>キャプチャを自動的に停止するとき (および場合) のオプション。次から選択します。</p> <ul style="list-style-type: none"> <li>• [ファイル サイズの上限に達するまでキャプチャを実行 (Run Capture Until File Size Limit Reached)]。キャプチャはファイル サイズの上限に達するまで実行されます。</li> <li>• [制限時間に達するまでキャプチャを実行 (Run Capture Until Time Elapsed Reaches)]。キャプチャは指定された期間だけ実行されます。単位を指定せずに時間の長さを入力すると、AsyncOS は、デフォルトで秒を使用します。</li> <li>• [制限なしでキャプチャを実行 (Run Capture Indefinitely)]。パケット キャプチャは、手動で停止するまで実行されます。</li> </ul> <p><b>Note</b><br/>キャプチャは手動でいつでも終了できます。</p> |
| インターフェイス<br>(Interfaces)                      | トラフィックがキャプチャされるインターフェイス。                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| フィルタ (Filters)                                | <p>パケットをキャプチャするときに適用するフィルタリング オプション。フィルタリングを使用すると、必要なパケットだけをキャプチャできます。次から選択します。</p> <ul style="list-style-type: none"> <li>• [フィルタなし (No Filters)]。すべてのパケットがキャプチャされます。</li> <li>• [事前定義されたフィルタ (Predefined Filters)]。定義済みのフィルタを使用して、ポートやIPアドレスによりフィルタリングできます。何も指定しなかった場合は、すべてのトラフィックがキャプチャされます。</li> <li>• [カスタムフィルタ (Custom Filter)]。必要なパケット キャプチャ オプションの正確な構文がわかっている場合は、このオプションを使用します。標準の tcpdump 構文を使用します。</li> </ul>                                                               |

(オプション) パケット キャプチャの変更を送信して確定します。

### Note

変更内容をコミットせずにパケット キャプチャ設定を変更し、パケット キャプチャを開始する場合、AsyncOSは新しい設定を使用します。これにより、今後のパケット キャプチャの実行に対する設定を適用せずに現在のセッションで新しい設定を使用することができます。この設定は、クリアするまで有効なままになります。

**ステップ 3** [キャプチャを開始 (Start Capture)] をクリックします。実行中のキャプチャを手動で停止するには、[キャプチャを停止 (Stop Capture)] をクリックします。

## パケット キャプチャ ファイルの管理

アプライアンスは、取り込んだパケット アクティビティをファイルに保存し、そのファイルをローカルに格納します。デバッグやトラブルシューティングのために、FTPを使用してパケット キャプチャ ファイルをシスコ カスタマー サポートに送信できます。

- [パケット キャプチャ ファイルのダウンロードまたは削除, on page 771](#)

### パケット キャプチャ ファイルのダウンロードまたは削除



**Note**

また、FTP を使用してアプライアンスに接続し、captures ディレクトリからパケット キャプチャ ファイルを取り出すこともできます。

### Procedure

- ステップ 1** [ヘルプとサポート (Help and Support)] > [パケットキャプチャ (Packet Capture)] を選択します。
- ステップ 2** [パケットキャプチャファイルの管理 (Manage Packet Capture Files)] ペインから、使用するパケット キャプチャファイルを選択します。このペインが表示されない場合は、アプライアンスにパケット キャプチャ ファイルが保存されていません。
- ステップ 3** 必要に応じて、[ファイルのダウンロード (Download File)] または [選択ファイルの削除 (Delete Selected File)] をクリックします。

## サポートの使用

- [効率的なサービス提供のための情報収集, on page 771](#)
- [テクニカル サポート要請の開始, on page 772](#)
- [仮想アプライアンスのサポートの取得, on page 772](#)
- [アプライアンスへのリモート アクセスのイネーブル化, on page 773](#)

### 効率的なサービス提供のための情報収集

サポートに問い合わせる前に以下の手順を実行してください。

- 一般的なトラブルシューティングとベスト プラクティス, on page 740の説明に従い、カスタム ログのフィールドを有効にします。
- パケット キャプチャを実行することを検討してください。「パケット キャプチャ, on page 769」を参照してください。

## テクニカル サポート要請の開始

### Before you begin

- 自身の Cisco.com ユーザー ID がこのアプライアンスのサービス契約に関連付けられていることを確認します。Cisco.com プロファイルに現在関連付けられているサービス契約の一覧を参照するには、Cisco.com Profile Manager (<https://sso.cisco.com/autho/forms/CDClogin.html>) にアクセスしてください。Cisco.com のユーザー ID がない場合は、登録して ID を取得してください。

緊急ではない場合は、アプライアンスを使用してサポート要請をシスコ カスタマー サポートに送信できます。アプライアンスは要請を送信する際に、アプライアンスの設定も送信します。サポート要求を送信するには、アプライアンスがインターネットに電子メールを送信する必要があります。



**Note** 緊急の問題がある場合は、Cisco Worldwide Support Center に連絡してください。

### Procedure

- ステップ 1 [ヘルプとサポート (Help and Support)] > [テクニカルサポートに問い合わせる (Contact Technical Support)] を選択します。
- ステップ 2 (オプション) 要請のその他の受信者を選択します。デフォルトでは、サポート要請とコンフィギュレーション ファイルがシスコ カスタマー サポートに送信されます。
- ステップ 3 自身の連絡先情報を入力します。
- ステップ 4 問題の詳細を入力します。
  - この問題に関するカスタマー サポート チケットをすでに持っている場合は、それを入力してください。
- ステップ 5 [送信 (Send)] をクリックします。トラブル チケットがシスコで作成されます。

## 仮想アプライアンスのサポートの取得

Cisco Content Security 仮想アプライアンスのサポート ケースを報告する場合は、仮想ライセンス番号 (VLN)、契約番号、および製品 ID コード (PID) を提供する必要があります。

発注書を参照するか以下の表を使用すると、仮想アプライアンスで動作中のソフトウェアライセンスに基づく PID を特定できます。

| 機能                          | PID          | 説明                                                                                                                                                      |
|-----------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web Security Essentials     | WSA-WSE-LIC= | 内容 :<br><ul style="list-style-type: none"> <li>• Web Usage Controls</li> <li>• Web レピュテーション</li> </ul>                                                  |
| Web Security Premium        | WSA-WSP-LIC= | 内容 :<br><ul style="list-style-type: none"> <li>• Web Usage Controls</li> <li>• Web レピュテーション</li> <li>• Sophos および Webroot Anti-Malware シグネチャ</li> </ul> |
| Web Security Anti-Malware   | WSA-WSM-LIC= | Sophos および Webroot Anti-Malware シグネチャが含まれます。                                                                                                            |
| McAfee Anti-Malware         | WSA-AMM-LIC= | —                                                                                                                                                       |
| Advanced Malware Protection | WSA-AMP-LIC= | —                                                                                                                                                       |

## アプライアンスへのリモート アクセスのイネーブル化

[リモートアクセス (Remote Access)] オプションを使用すると、シスコ カスタマー サポート がサポートのためにリモート アプライアンスにアクセスできるようになります。

### Procedure

**ステップ 1** [ヘルプとサポート (Help and Support)] > [リモートアクセス (Remote Access)] を選択します。

**ステップ 2** [有効 (Enable)] をクリックします。

**ステップ 3** [カスタマーサポートのリモートアクセス (Customer Support Remote Access)] オプションを設定します。

| オプション                | 説明                                                                                                                        |
|----------------------|---------------------------------------------------------------------------------------------------------------------------|
| シード文字列 (Seed String) | 文字列を入力する場合は、その文字列が既存または将来のパスフレーズと一致しないようにしてください。<br><br>[送信 (Submit)] をクリックすると、文字列がページの上部に表示されます。<br>この文字列をサポート担当者に提出します。 |

| オプション                                   | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| セキュア トンネル<br>(Secure Tunnel)<br>(推奨)    | <p>リモート アクセス接続にセキュア トンネルを使用するかどうかを指定します。</p> <p>このオプションがイネーブルの場合、アプライアンスは、指定されたポートからサーバー <code>upgrades.ironport.com</code> への SSH トンネルを作成します（デフォルトでは、ポート 443）。接続が確立されると、シスコカスタマーサポートは SSH トンネルを使用してアプライアンスにアクセスできるようになります。</p> <p><code>techsupport</code> トンネルがイネーブルになると、<code>upgrades.ironport.com</code> に 7 日間接続されたままになります。7 日が経過すると、<code>techsupport</code> トンネルを使用して新しい接続を作成できなくなりますが、既存の接続は存続し、機能します。</p> <p>リモートアクセスアカウントは、明確に非アクティブ化されるまでアクティブな状態を維持します。</p> |
| 送信元インターフェイス (Source Interface)          | トンネルとリモートアクセス接続の確立に使用するインターフェイスを選択できます。                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| アプライアンスシリアル番号 (Appliance Serial Number) | アプライアンスのシリアル番号。                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**ステップ 4** 変更を送信し、保存します。

**ステップ 5** ページ上部近くに表示される成功メッセージでシード文字列を検索し、書き留めます。

セキュリティ上の理由から、この文字列はアプライアンスに保存されず、後から文字列を確認する方法はありません。

安全な場所にこのシード文字列を保存します。

**ステップ 6** シード文字列をサポート担当者に提出します。



## 第 10 章

# コマンドラインインターフェイス

この章で説明する内容は、次のとおりです。

- [コマンドラインインターフェイスの概要, on page 775](#)
- [コマンドラインインターフェイスへのアクセス, on page 775](#)
- [汎用 CLI コマンド, on page 779](#)
- [Secure Web Appliance CLI コマンド, on page 780](#)

## コマンドラインインターフェイスの概要

AsyncOS コマンドラインインターフェイス (CLI) を使用して、Secure Web Applianceを設定したりモニタすることができます。コマンドラインインターフェイスには、それらのサービスがイネーブルに設定されている IP インターフェイスで SSH を使用してアクセスするか、シリアルポートで端末エミュレーションソフトウェアを使用してアクセスできます。デフォルトでは、SSH は管理ポートに設定されます。

コマンドは、引数の有無を問わず、コマンド名を入力すると起動されます。引数を指定せずにコマンドを入力した場合は、必要な情報の入力を求めるプロンプトが表示されます。

## コマンドラインインターフェイスへのアクセス

以下のいずれかの方法で接続できます。

- **イーサネット。** Secure Web Applianceの IP アドレスを使用して SSH セッションを開始します。工場出荷時のデフォルト IP アドレスは 192.168.42.42 です。SSH は、ポート 22 を使用するように設定されています。
- **シリアル接続。** シリアル ケーブルが接続されているパーソナル コンピュータの通信ポートを使用して、ターミナルセッションを開始します。



## 初回アクセス

**admin** アカウントを使用して初めて CLI にアクセスした後は、さまざまな許可レベルにより他のユーザーを追加できます。以下のデフォルトの **admin** ユーザー名とパスワードを入力してアプライアンスにログインします。

- ユーザー名 : **admin**
- パスワード : **ironport**

デフォルトのパスワードで初めてログインすると、システム セットアップ ウィザードのプロンプトにより **admin** アカウントのパスワードを変更するよう求められます。

**admin** アカウントのパスワードは、`passwd` コマンドを使用していつでもリセットできます。

## 以降のアクセス

有効なユーザー名とパスワードを使用して、いつでもアプライアンス接続してログインできます。現在のユーザー名での最近のアプライアンスへのアクセス試行（成功、失敗を含む）の一覧が、ログイン時に自動的に表示されることに注意してください。

追加のユーザーの設定については、`userconfig` コマンド、または [ユーザー アカウントの管理, on page 171](#) を参照してください。

## コマンド プロンプトの使用

最上位のコマンド プロンプトは、完全修飾ホスト名に続いて大なり (>) 記号とスペース 1 つで構成されます。次に例を示します。

```
example.com>
```

コマンドを実行すると、CLI によりユーザーの入力が要求されます。CLI が入力を待機しているときは、プロンプトとして、角カッコ ([ ]) で囲まれたデフォルト値の後ろに大なり記号 (>) が表示されます。デフォルト値がない場合、カッコ内は空です。

次に例を示します。

```
example.com> routeconfig
```

```
Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]>
```

デフォルト設定がある場合は、コマンド プロンプトのカッコ内にその設定が表示されます。次に例を示します。

```
example.com> setgateway
```

```
Warning: setting an incorrect default gateway may cause the current connection
```

```
to be interrupted when the changes are committed.
Enter new default gateway:
[172.xx.xx.xx]>
```

デフォルト設定が表示されたときに **Return** キーを押すと、デフォルト値を受け入れたことになります。

## コマンドの構文

インタラクティブモードで操作している場合、CLI コマンド構文は単一のコマンドから構成されます。スペースは含まれず、引数やパラメータ也没有。例：

```
example.com> logconfig
```

## 選択リスト

入力できる複数の選択肢がある場合、コマンドによっては番号付きリストを使用します。プロンプトで選択する番号を入力します。

例：

```
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 3
```

## Yes/No クエリー

yes または no のオプションがある場合、質問はデフォルト値（カッコ内表示）を付けて表示されます。**Y**、**N**、**Yes**、または **No** で返答できます。大文字と小文字の区別はありません。

例：

```
Do you want to enable the proxy? [Y]> Y
```

## サブコマンド

一部のコマンドでは、NEW、EDIT、DELETE などのサブコマンド命令を使用できます。EDIT および DELETE 関数では、設定されている値のリストが表示されます。

次に例を示します。

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (172.xxx.xx.xx/xx: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
```

```
- DELETE - Remove an interface.
[]>
```

サブコマンド内からメイン コマンドに戻るには、空のプロンプトで Enter または Return を押します。

## サブコマンドのエスケープ

サブコマンド内ではいつでも Ctrl+C キーボード ショートカットを使用して、ただちに最上位の CLI に戻ることができます。

## コマンド履歴

CLI は、セッション中に入力されたすべてのコマンドの履歴を保持します。最近使用したコマンドの実行リストをスクロールするには、キーボードの上下矢印キーを使用するか、Ctrl+P キーと Ctrl+N キーを組み合わせ使用します。

## コマンドのオートコンプリート

AsyncOS CLI は、コマンド補完機能をサポートしています。コマンドの先頭の数文字を入力して Tab キーを押すと、CLI によって残りの文字列が補完されます。入力した文字が複数のコマンドに該当する場合、CLI はそのセットをさらに「絞り込み」ます。例：

```
example.com> set (press the Tab key)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (pressing the Tab again completes the entry with sethostname)
example.com> sethostname
```

## CLI を使用した設定変更の確定

- 設定の変更の多くは、確定するまで有効になりません。
- commit コマンドを使用すると、他の操作を通常どおりに実行しながら設定を変更できます。
- 変更を正常に確定するには、最上位のコマンドプロンプトになっている必要があります。コマンドライン階層の 1 つ上のレベルに移動するには、空のプロンプトで Return キーを押します。
- 確定されていない設定の変更は記録されますが、commit コマンドを実行するまで有効になりません。ただし、一部のコマンドは commit コマンドを実行しなくても有効になります。CLI セッションの終了、システムのシャットダウン、再起動、障害、または clear コマンドの発行により、確定されていない変更はクリアされます。
- ユーザーが確認とタイムスタンプを受け取るまで、変更は実際に確定されません。

## 汎用 CLI コマンド

ここでは、変更の確定やクリアなど、一般的なCLIセッションで使用される基本的なコマンドについて説明します。

### CLI の例：設定変更の確定

`commit` コマンドの後のコメントの入力は任意です。

```
example.com> commit

Please enter some comments describing your changes:
[]> Changed "psinet" IP Interface to a different IP address
Changes committed: Wed Jan 01 12:00:01 2007
```

### CLI の例：設定変更のクリア

`clear` コマンドは、`commit` または `clear` コマンドが最後に実行された以降にアプライアンスの設定に対して行われた変更をすべてクリアします。

```
example.com> clear

Are you sure you want to clear all changes since the last commit? [Y]> y
Changes cleared: Wed Jan 01 12:00:01 2007
example.com>
```

### CLI の例：コマンドライン インターフェイス セッションの終了

`exit` コマンドを実行すると、CLI アプリケーションからログアウトされます。確定されていない設定変更はクリアされます。

```
example.com> exit

Configuration changes entered but not committed. Exiting will lose changes.
Type 'commit' at the command prompt to commit changes.

Are you sure you wish to exit? [N]> y
```

### CLI の例：コマンドライン インターフェイスでのヘルプの検索

`help` コマンドを実行すると、使用可能なすべての CLI コマンドが表示され、各コマンドの簡単な説明を参照できます。`help` コマンドは、コマンドプロンプトで `help` と入力するか、疑問符 (?) を 1 つ入力して実行できます。

```
example.com> help
```

さらに、`help commandname` を入力して、特定のコマンドのヘルプにアクセスできます。

## 関連項目

- [Secure Web Appliance CLI コマンド, on page 780](#)

# Secure Web Appliance CLI コマンド

Secure Web Applianceの CLI は、システムへのアクセスおよびシステムのアップグレードと管理を実行する、一連のプロキシコマンドと UNIX コマンドをサポートしています。



**Note** すべての CLI コマンドをすべての動作モード（標準およびクラウド Web セキュリティ コネクタ）で適用/使用できるわけではありません。

## adminaccessconfig

Secure Web Applianceの設定で、アプライアンスにログインする管理者に対して厳しいアクセス要件を設け、非アクティブタイムアウトの値を指定できます。詳細については、[アプライアンスの割り当てに対するセキュリティ設定の追加, on page 179](#)と [ユーザー ネットワーク アクセス, on page 181](#)を参照してください。

## advancedproxyconfig

Web プロキシの詳細オプションを設定します。サブコマンドは以下のとおりです。

**AUTHENTICATION** : 認証設定オプション。

- When would you like to forward authorization request headers to a parent proxy
- Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog
- Would you like to log the username that appears in the request URI
- Should the Group Membership attribute be used for directory lookups in the Web UI (when it is not used, empty groups and groups with different membership attributes will be displayed)
- Would you like to use advanced Active Directory connectivity checks
- Would you like to allow case insensitive username matching in policies
- Would you like to allow wild card matching with the character \* for LDAP group names
- Enter the charset used by the clients for basic authentication [ISO-8859-1/UTF-8]
- Would you like to enable referrals for LDAP
- Would you like to enable secure authentication
- Enter the hostname to redirect clients for authentication
- Enter the surrogate timeout for user credentials

- Enter the surrogate timeout for machine credentials
- Enter the surrogate timeout in the case traffic permitted due to authentication service unavailability
- Enter re-auth on request denied option [disabled / embedlinkinblockpage]
- Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication
- Configure username and IP address masking in logs and reports
- ローカル認証キャッシュを有効/無効にするタイムアウト。

このCLIオプションを使用して、プロキシプロセスの即時認証キャッシュを有効または無効にすることができます。この時間は秒単位で設定されます。デフォルトでは、このオプションが有効になっており、30 秒に設定されています。この時間は、IP サロゲート時間より短くする必要があります。

**CACHING** : プロキシ キャッシュ モード。以下のうち 1 つを選択します。

- Safe Mode
- Optimized Mode
- Aggressive Mode
- Customized Mode

[Web プロキシのキャッシュ モードの選択, on page 243](#)も参照してください。

**DNS** : DNS 設定オプション。

- Enter the URL format for the HTTP 307 redirection on DNS lookup failure
- Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure
- Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive
- Do you want to disable IP address in Host Header
- Find web server by:
  - 0 = Always use DNS answers in order
  - 1 = Use client-supplied address then DNS
  - 2 = Limited DNS usage
  - 3 = Very limited DNS usage

デフォルト値は 0 です。オプション 1 および 2 では、[Webレピュテーション (Web Reputation)] がイネーブルに設定されている場合、DNS が使用されます。オプション 2 および 3 では、DNS は、アップストリーム プロキシがない場合、または設定されたアップストリーム プロキシが失敗するイベントで、明示的なプロキシ要求に使用されます。すべてのオプションで、[宛先 IP アドレス (Destination IP Addresses)] がポリシー メンバーシップで使用されている場合、DNS が使用されます。

**EUN** : エンドユーザー通知パラメータ。

- Choose:
  1. Refresh EUN pages
  2. Use Custom EUN pages
  3. Use Standard EUN pages
- Would you like to turn on presentation of the User Acknowledgement page?

[Web プロキシ使用規約, on page 252](#)と [エンドユーザー通知の概要, on page 533](#)も参照してください。

**NATIVEFTP** : ネイティブ FTP の設定。

- Would you like to enable FTP proxy
- Enter the ports that FTP proxy listens on
- Enter the range of port numbers for the proxy to listen on for passive FTP connections
- Enter the range of port numbers for the proxy to listen on for active FTP connections
- Enter the authentication format:
  1. Check Point
  2. No Proxy Authentication
  3. Raptor
- Would you like to enable caching
- Would you like to enable server IP spoofing
- Would you like to enable client IP spoofing
- Would you like to pass FTP server welcome message to the clients
- Enter the max path size for the ftp server directory

[FTP プロキシ サービスの概要, on page 259](#)も参照してください。

**FTPOVERHTTP** : FTP Over HTTP オプション。

- Enter the login name to be used for anonymous FTP access
- Enter the password to be used for anonymous FTP access

[FTP プロキシ サービスの概要, on page 259](#)も参照してください。

**Highperformance** : ハイパフォーマンスモードを有効化または無効化できます。

**HTTPS** : HTTPS 関連のオプション。

- HTTPS URI Logging Style - fulluri or stripquery
- Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose

- Would you like to decrypt HTTPS requests for End User Notification purpose
- Action to be taken when HTTPS servers ask for client certificate during handshake:
  1. Pass through the transaction
  2. Reply with certificate unavailable
- Do you want to enable server name indication (SNI) extension?
- Do you want to enable automatic discovery and download of missing Intermediate Certificates?
- Do you want to enable session resumption?

[HTTPS トラフィックを制御する復号ポリシーの作成：概要, on page 344](#)も参照してください。

**SCANNING**：スキャン オプション。

- Would you like the proxy to do malware scanning all content regardless of content type
- Enter the time to wait for a response from an anti-malware scanning engine (Sophos, McAfee, or Webroot), in seconds
- Do you want to disable Webroot body scanning

[マルウェア対策スキャンの概要, on page 459](#)と [発信トラフィックのスキャンの概要, on page 408](#)も参照してください。

**SCANNERS**：scanners サブコマンドを使用してスキャナエンジンを設定できます。scanners サブコマンドを使用するには、「Adaptive Scanning」機能を無効にする必要があります。

- Choose the operation you want to perform:

AMP : Secure Endpoint 関連オプション

SOPHOS : Sophos Memory 関連オプション

- **AMP**：このコマンドを使用して、AMP エンジンでスキャンする必要のない MIME タイプを追加し、スキャンのパフォーマンスを向上させることができます。デフォルトの MIME タイプのオプションは、「image/ALL and text/ALL」です。

MIME タイプを追加するには、デフォルトのオプションの後に追加する必要があります。たとえば、ビデオと音声の MIME タイプを追加する場合は、次の形式にする必要があります。

「image/ALL and text/ALL video/ALL audio/ALL」

- **SOPHOS**：大量のトラフィックがエンジンを通過している場合、Sophos エンジンのスキャンがタイムアウトし、メモリが不足する可能性があります。これは malloc メモリの問題によるものです。この問題を解決するには、sophos サブコマンドを使用し、MALLOC\_SETTING を選択します。MALLOC\_SETTING を選択すると、次のメッセージが表示されます。

Changing Sophos Malloc Settings will lead to stoppage of coredumps.  
Do you want to change the sophos malloc settings ? [Y]>



[はい (yes) ] を選択すると、**malloc** 設定が変更され、**Sophos** が再起動されます。デフォルト設定に戻すには、同じコマンドを使用します。



**Note** コマンドを使用する前に、次の点に注意してください。

- **Sophos malloc** 設定の変更中は、トラフィックが実行されないようにします。
- CLI から設定を変更すると、**Sophos** の再起動が必要になるため、変更の更新に時間がかかる場合があります。
- **malloc** 設定は頻繁に変更しないでください。



**Note** TAC 専用です。

- **Windows/Linux** の更新トラフィックが原因で **Sophos** がコアリングしている場合は、必ずコアリングが完了した後に **malloc** 設定を変更する必要があります。
- **Sophos** の再起動後、変更が更新されるまでに時間がかかるため、コアリングが 1 回表示される場合があります。

**PROXYCONN** : プロキシ接続ヘッダーを含むことができないユーザー エージェントのリストを管理します。リストのエントリは、**Flex (Fast Lexical Analyzer)** の正規表現として解釈されます。その文字列の一部がリスト内の正規表現のいずれかに一致するユーザー エージェントは、一致とされます。

- 実行する操作を選択します。

NEW - Add an entry to the list of user agents

DELETE - Remove an entry from the list

**CUSTOMHEADERS** : 特定のドメインのカスタム要求ヘッダーを管理します。

- 実行する操作を選択します。

DELETE - Delete entries

NEW - Add new entries

EDIT - Edit entries

[Web 要求へのカスタム ヘッダーの追加](#), [on page 246](#) も参照してください。

**MISCELLANEOUS** : その他のプロキシ関連パラメータ。

- Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)

- Would you like proxy to perform dynamic adjustment of TCP receive window size
- Would you like proxy to perform dynamic adjustment of TCP send window size
- Do you want to filter non-HTTP responses?  
(HTTP 以外の応答はデフォルトでフィルタされます。プロキシ経由で HTTP 以外の応答を許可する場合は、**N** と入力します。)
- Enable caching of HTTPS responses
- Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds)
- Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)
- Mode of the proxy:
  1. Explicit forward mode only
  2. Transparent mode with L4 Switch or no device for redirection
  3. Transparent mode with WCCP v2 Router for redirection
- Spoofing of the client IP by the proxy:
  1. すべての要求に対してイネーブル
  2. 透過的要求に対してのみイネーブル
- Do you want to pass HTTP X-Forwarded-For headers?
- Do you want to enable server connection sharing?
- Would you like to permit tunneling of non-HTTP requests on HTTP ports?
- Would you like to block tunneling of non-SSL transactions on SSL Ports?
- Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?
- Do you want proxy to throttle content served from cache?
- Would you like the proxy to use client IP addresses from X-Forwarded-For headers
- Do you want to forward TCP RST sent by server to client?
- Do you want to enable WCCP proxy health check?
- Do you want to enable URL lower case conversion for velocity regex?

Web プロキシ データに対する P2 データ インターフェイスの使用 , on page 54 と Web プロキシ の設定, on page 237 も参照してください。

**socks** : SOCKS プロキシのオプション。

- Would you like to enable SOCKS proxy
- プロキシ ネゴシエーション タイムアウト (Proxy Negotiation Timeout)
- UDP トンネル タイムアウト (Tunnel Timeout)
- SOCKS コントロール ポート (SOCKS Control Ports)

- UDP リクエスト ポート (UDP Request Ports)

Web プロキシデータに対する P2 データ インターフェイスの使用, on page 54 と SOCKS プロキシ サービス, on page 261 も参照してください。

**CONTENT-ENCODING** : コンテンツエンコーディング タイプを許可およびブロックします。

現在許可されているコンテンツエンコーディング タイプ : `compress`、`deflate`、`gzip`

現在ブロックされているコンテンツエンコーディング タイプ : 該当なし

特定のコンテンツエンコーディングタイプの設定を変更するには、次のオプションを選択します。

1. `compress`
2. `deflate`
3. `gzip`

[1]>

The encoding type "compress" is currently allowed

Do you want to block it? [N]>



**Note** **centralauthcache** コマンドは、ハイパフォーマンス対応デバイスに適用でき、認証キャッシュのパフォーマンスを向上させます。

### **adminaccessconfig**

アプライアンスにログインする管理者の認証により厳しいアクセス要件を設けるように、Secure Web Applianceを設定できます。

### **alertconfig**

アラートの受信者を指定し、システム アラートを送信するためのパラメータを設定します。

### **authcache**

認証キャッシュから1つまたはすべてのエントリ (ユーザー) を削除できるようにします。また、その時点で認証キャッシュに含まれているすべてのユーザーのリストを表示できます。



**Note** **centralauthcache** が有効な場合、**authcache** コマンドは ISE 認証ユーザー名を表示しません。ISE ユーザー情報を取得するには、**isedata** コマンドを使用します。

### **bwcontrol**

帯域幅制御機能をデバッグします。

- **bwcontrol listpipes** : Secure Web Applianceでアクティブなすべての帯域幅制御パイプのリストが表示されます。
- **bwcontrol monitor <pipe number>** : 5 秒ごとに、指定されたパイプで測定された帯域幅を表示します。

AsyncOS 14.5 以降は、トレースモードのプロキシログがデフォルトで表示されます。

### 用語

- **URLBW** : アクセスポリシー URL カテゴリによって適用される帯域幅制御。
- **OverallBW** : アクセスポリシーの全体的な Web アクティビティクォータによって適用される帯域幅制御。
- **OverallMediaBW** : 全体の帯域幅制限によって適用される帯域幅制御。
- **AVCPerUserBW** : AVC 帯域幅制限によって適用される帯域幅制御。

### certconfig

**SETUP** : セキュリティ証明書とキーを設定します。

**OCSPVALIDATION** : アップロード時に証明書の OCSP 検証を有効/無効にします。

**OCSPVALIDATION\_FOR\_SERVER\_CERT** : サーバー証明書の OCSP 検証を有効にする

### clear

前回の確定以降の保留されている設定変更をクリアします。

### clientconnections

クライアントあたりの最大接続数が有効になっている場合に、接続の詳細を表示します。詳細には、クライアントの IP アドレスと接続数が含まれます。

Choose the operation you want to perform:

- **LIST** : cstat DB からすべてのエントリを一覧表示します
- **SEARCH** : cstat DB からエントリを検索します

### コミット

システム設定に対する保留中の変更を確定します。

### configbackup

バックアップ設定ファイルを保存し、リモート配置されたバックアップサーバーに FTP または SCP を介してファイルを送信します。

**csidconfig**

Security Services Exchange ポータルに対するテレメトリデータの公開に関連するアプライアンス上の Cisco Success Network 機能のさまざまなパラメータを設定できます。

サブコマンドは次のとおりです:

- **CISCO\_SUCCESS\_NETWORK** : 機能を有効にして、アプライアンスの詳細と機能の使用状況を Cisco に送信することを有効または無効にします。
- **CSIDATAPUSHINTERVAL** : テレメトリデータのプッシュの時間間隔を設定します。

**createcomputerobject**

指定された場所にコンピュータ オブジェクトを作成します。

**curl**

cURL 要求を、Web サーバーに直接またはプロキシ経由で送信します。要求および返される応答の HTTP ヘッダーから、Web ページをロードできなかった理由を判別できます。




---

**Note** このコマンドは、TAC の監督のもとで管理者またはオペレータだけが使用できます。

---

サブコマンドは次のとおりです:

- **DIRECT** : 直接 URL アクセス
- **APPLIANCE** : アプライアンス経由での URL アクセス

**datasecurityconfig**

要求の最小本文サイズを定義します。これよりも本文サイズが小さい場合、アップロード要求は Cisco データセキュリティ フィルタによってスキャンされません。

**date**

現在の日付を表示します。例 :

```
Thu Jan 10 23:13:40 2013 GMT
```

**diagnostic**

プロキシおよびレポート関連のサブコマンド :

**NET** : ネットワーク診断ユーティリティ

このコマンドは廃止されました。アプライアンスでネットワークトラフィックをキャプチャするには、**packetcapture** を使用します。

**PROXY** : プロキシデバッグ ユーティリティ

実行する操作を選択します。

- SNAP : プロキシのスナップショットを取得します。
- OFFLINE : プロキシをオフラインにします (WCCP 経由)。
- RESUME : プロキシのトラフィックを再開します (WCCP 経由)。
- CACHE : プロキシのキャッシュをクリアします。

**proxyscannermap** : このコマンドは、各プロキシと対応するスキャナプロセス間の PID マッピングを表示します。

**REPORTING** : レポートユーティリティ

レポートシステムは現在有効になっています。

実行する操作を選択します。

- DELETEDB : レポート データベースを再度初期化します。
- DISABLE : レポート システムを無効にします。
- DBSTATS : DB とエクスポート ファイルをリストします (export\_files および always\_onbox フォルダに含まれる未処理のファイルとフォルダのリストを表示します)。
- DELETEEXPORTDB : エクスポート ファイルを削除します (export\_files および always\_onbox フォルダに含まれる未処理のファイルとフォルダをすべて削除します)。
- DELETEJOURNAL : ジャーナル ファイルを削除します (aclog\_journal\_file をすべて削除します)。

## dnsconfig

DNS サーバーのパラメータを設定します。

Choose the operation you want to perform:

- NEW : 新規サーバーを追加します。
- EDIT : サーバーを編集します。
- DELETE : サーバーを削除します。
- SETUP : 全般的な設定を行います。
- SEARCH : DNS ドメイン検索リストを設定します。

```
[>] setup
```

```
Do you want to enable Secure DNS? [N]> Yes
```

## dnsflush

アプライアンスの DNS エントリをフラッシュします。

### etherconfig

イーサネット ポート接続を設定します。

Choose the operation you want to perform:

- **MEDIA** : イーサネット メディアの設定を表示して編集します。
- **PAIRING** : NIC ペアリングを表示して設定します。
- **VLAN** : VLAN を表示して設定します。
- **MTU** : MTU を表示して設定します。



**Note** M2、Data 1、および Data 2 インターフェイスはサポートされていません。したがって、これらのインターフェイスオプションは CLI では使用できません。

### externaldlpconfig

要求の最小本文サイズを定義します。これよりも本文サイズが小さい場合、アップロード要求は外部 DLP サーバーでスキャンされません。

### externaldlpconfig

要求の最小本文サイズを定義します。これよりも本文サイズが小さい場合、アップロード要求は外部 DLP サーバーでスキャンされません。

### fipsconfig

**SETUP** : FIPS 140-2 準拠と Critical Sensitive Parameter (CSP) の暗号化を有効/無効にします。即時リブートが必要となる点に注意してください。

**FIPSCHECK** : FIPX モードに準拠しているかどうかを確認します。各種証明書とサービスが FIPS に準拠しているかどうかを示します。

詳細については、[FIPS Compliance, on page 194](#)を参照してください。

### grep

指定された入力ファイルを検索して、特定のパターンに一致するものを含む行を見つけます。

### gathererdconfig

アプライアンスと認証サーバーの間にポーリング機能を設定します。

### help

コマンドのリストを返します。

### httppatchconfig

発信 HTTP パッチ要求を有効または無効にします。デフォルト値は **enable** です。

### http2

HTTP 2 設定を有効または無効にします。

### iccm\_message

この Secure Web Applianceがセキュリティ管理アプライアンス（M-Series）によって管理される時期を示すメッセージを、Web インターフェイスと CLI からクリアします。

### ifconfig または interfaceconfig

M1、P1、P2などのネットワークインターフェイスを設定して管理します。現在設定されているインターフェイスを表示し、インターフェイスの作成、編集、削除のための操作メニューを提供します。

### iseconfig

現在の ISE 設定パラメータを表示します。実行する ISE 設定操作を指定できます。

ISE RECONCILIATION TIME SETUP : ISE 調整時間のセットアップを設定します。ised プロセスを自動的に再起動するには、ISE 設定の時間を HH::MM 形式（24 時間）で設定します。再起動後、一括ダウンロードが行われます。

REMOVEISENODEDETAILS : セカンダリ ISE pxGridノードを削除します。セキュリティ Web アプライアンスは、Web アプライアンスのデータサブスクリプション（継続的な更新）をサポートするために ISE pxGrid ノードと通信します。セカンダリ ISE pxGrid ノード（サーバー）の指定はオプションです。セカンダリ ISE pxGridノードを削除するには、REMOVEISENODEDETAILS 操作を選択します。

```
Choose the operation you want to perform:
-ISE RECONCILIATION TIME SETUP - Configure ISE reconciliation time setup.
-REMOVEISENODEDETAILS - remove seconadry ise config details
```

デフォルトでは、オプション 1 の値は深夜 00:00 時です。

### isedata

ISE データ関連の操作を指定します。

statistics : ISE サーバーのステータスと ISE 統計情報を表示します。

cache : ISE キャッシュを表示するか、IP アドレスを確認します。

sgts : ISE セキュア グループ タグ（SGT）テーブルを表示します。

groups : ISE グループ テーブルを表示します。



VDI が実装されている場合、メインコマンド `cache` の下のサブコマンド `show` および `checkip` に詳細が表示されます。`show` サブコマンドはポート範囲に関する詳細を表示し、`checkip` サブコマンドは IP アドレス、名前、ポート範囲などの VDI ユーザーに関する詳細を表示します。

```
[]> cache
```

Choose the operation you want to perform:

- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address

### last

`tty` やホストなどのユーザー固有のユーザー情報を新しい順に並べて一覧表示したり、指定した日時にログインしたユーザーのリストを表示します。

### loadconfig

システム コンフィギュレーション ファイルをロードします。

### logconfig

ログ ファイルへのアクセスを設定します。

### mailconfig

指定されたアドレスに現在のコンフィギュレーション ファイルをメールで送信します。

### maxhttpheadersize

プロキシ要求の最大 HTTP ヘッダー サイズまたは URL サイズを設定します。値をバイト単位で入力するか、キロバイトを表す場合は数値に **K** を付記します。

多数の認証グループに属するユーザーの場合はポリシー トレースが失敗する可能性があります。また、HTTP 応答ヘッダーのサイズまたは URL サイズが現在の「最大ヘッダー サイズ」よりも大きい場合、失敗することがあります。この値を大きくすると、このような障害を軽減できます。最小値は 32 KB、デフォルト値は 32 KB、最大値は 1024 KB です。

### modifyauthhelpers

このコマンドを使用して、BASIC、NTLMSSP、および NEGO の Kerberos 認証ヘルパーを 5 ～ 21 の範囲内の数値で設定します。

### musconfig

このコマンドを使用してセキュア モビリティを有効化し、リモート ユーザーの識別方法を設定します (IP アドレスによって識別するか、1 つ以上の Cisco 適応型セキュリティ アプライアンスと統合することで識別)。



#### Note

このコマンドを使って変更すると、Web プロキシが再起動されます。

### musstatus

Secure Web Applianceを適応型セキュリティアプライアンスと統合したときに、このコマンドを使用してセキュアモビリティに関連する情報を表示します。

このコマンドにより、以下の情報が表示されます。

- Secure Web Applianceと個々の適応型セキュリティ アプライアンスとの接続状態。
- Secure Web Applianceと個々の適応型セキュリティ アプライアンスとの接続時間（分単位）。
- 個々の適応型セキュリティ アプライアンスからのリモート クライアントの数。
- サービス対象のリモート クライアントの数。これは、 Secure Web Applianceを介してトラフィックの受け渡しを行ったリモート クライアントの数です。
- リモート クライアントの合計数。

### networktuning

Secure Web Applianceは、複数のバッファおよび最適化アルゴリズムを使用して何百もの TCP 接続を同時に処理し、一般的な Web トラフィック（つまり、一時的な HTTP 接続）に対して高いパフォーマンスを実現します。

大容量ファイル（100MB 以上）が頻繁にダウンロードされるような特定の状況では、バッファが大きいほど接続ごとのパフォーマンスが向上する可能性があります。ただし、全体的なメモリ使用量が増加するため、システムで使用可能なメモリに応じてバッファを増やす必要があります。

送信および受信スペース変数は、指定の TCP ソケットを介した通信用にデータを保存するために使用されるバッファを表します。自動送信および受信変数は、ウィンドウサイズを動的に制御するためのFreeBSD自動調整アルゴリズムを有効または無効にするために使用されます。これら 2 つのパラメータは、FreeBSD カーネルに直接適用されます。

SEND\_AUTO と RECV\_AUTO が有効な場合、システムの負荷と使用可能なリソースに基づいてウィンドウサイズが動的に調整されます。負荷が小さい Secure Web Applianceでは、トランザクションあたりの遅延を削減するためウィンドウサイズが大きく維持されます。動的に調整されるウィンドウサイズの最大値は、設定されている mbuf クラスタの数に依存します。つまり、システムで使用可能な RAM の合計に応じて異なります。クライアント接続の合計数が増加する場合、または使用可能なネットワーク バッファ リソースが非常に少なくなる場合には、すべてのネットワーク バッファ リソースがプロキシトラフィックにより使用されることを防いでシステムを保護するため、ウィンドウサイズが削減されます。

このコマンドの使用に関する詳細については、[アップロード/ダウンロード速度の問題, on page 746](#)を参照してください。

networktuning サブコマンドは、次のとおりです。

**SENDSPACE** : TCP 送信スペースのバッファサイズ。8192 ～ 2097152 バイトの範囲で、デフォルトは 32768 バイトです。

**RECSPACE** : TCP 受信スペースのバッファサイズ。8192 ～ 2097152 バイトの範囲で、デフォルトは 65536 バイトです。

**SEND-AUTO** : TCP 送信の自動調整を有効または無効にします。1 はオン、0 はオフで、デフォルトはオンです。TCP 送信の自動調整を無効にする場合、必ず `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP send window size? Yes` の順に使用して、送信バッファの自動調整を有効にしてください。

**RECV-AUTO** : TCP 受信の自動調整を有効または無効にします。1 はオン、0 はオフで、デフォルトはオンです。TCP 受信の自動調整を無効にする場合、必ず `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP receive window size? Yes` の順に使用して、受信バッファの自動調整を無効にしてください。

**MBUF CLUSTER COUNT** : 使用可能な mbuf クラスタの数を変更します。許容範囲は 252470 ～ 1000000 です。この値は、インストールされたシステム メモリによって変わります。98304 \* (X/Y) の計算を使用し、X はシステム上の RAM のギガバイトで、Y は 4 GB です。たとえば 4 GB RAM の場合、推奨値は 98304 \* (4/4) = 98304 になります。RAM が増加する場合は、線形スケールリングが推奨されます。

**SENDER-MAX** : 最大送信バッファサイズを指定します。範囲は 131072 ～ 2097152 バイトで、デフォルトは 2 MB (2097152 バイト) です。

**RECVBUF-MAX** : 最大受信バッファサイズを指定します。範囲は 131072 ～ 2097152 バイトで、デフォルトは 2 MB (2097152 バイト) です。

**CLEAN-FIB-1** : データルーティングテーブルからすべての M1/M2 エントリを削除します。基本的には、コントロールプレーン/データプレーンの分離を有効にします。つまり、「分離ルーティング」が有効になっている場合に M1 インターフェイス経由のデータ送信からデータプレーンプロセスを無効にします。データプレーンプロセスは、「データルーティングテーブルの使用」が有効になっているプロセス、または非管理トラフィックを厳密に伝達するプロセスです。コントロールプレーンプロセスでは、依然として M1 または P1 インターフェイスのいずれかを介してデータを送信できます。

これらのパラメータに何らかの変更を行った後は、必ず変更を確定してアプライアンスを再起動してください。



**Caution** 副次的な影響を理解している場合にのみ、このコマンドを使用してください。TAC ガイダンスを受けている場合にのみ使用することを推奨します。

## nslookup

指定されたホストとドメインの情報を取得したり、ドメイン内のホストのリストを印刷するために、インターネット ドメイン ネーム サーバーに照会します。

## ntpconfig

NTP サーバーの設定現在設定されているインターフェイスを表示し、インターフェイスを追加、削除、または設定する操作メニューを提供します。このインターフェイスの IP アドレスから NTP クエリーが発信されます。

**packetcapture**

アプライアンスが接続されているネットワーク上で送受信されている TCP/IP などのパケットを代行受信して表示します。

**passwd**

パスフレーズを設定します。

**pathmtudiscovery**

パス MTU ディスカバリをイネーブルまたはディセーブルにします。

パケットフラグメンテーションが必要な場合は、パス MTU ディスカバリをディセーブルにすることができます。

**ping**

指定されたホストまたはゲートウェイに ICMP エコー要求を送信します。

**process\_status**

アプライアンスのアクティブなプロセスのリストを表示します。



---

**Note** このコマンドは、管理者モードでのみ使用できます。

---

**proxyconfig <enable | disable>**

Web プロキシをイネーブルまたはディセーブルにします。

**proxystat**

Web プロキシの統計情報を表示します。

**quit、q、exit**

アクティブなプロセスまたはセッションを終了します。

**quotaquery**

カテゴリ別にボリュームと使用時間を確認またはリセットするために使用します。

Choose the operation you want to perform:

- RESET：プロキシクォータキャッシュ内にある特定のエントリのクォータをリセットします。
- SEARCH：プロキシクォータキャッシュ内のユーザーエントリのリストを検索します。
- RESETALL：プロキシクォータキャッシュ内のすべてのエントリをリセットします。



**Note** マルチプロキシモードで、CLI から *quotoquery* にアクセスしているときにアプライアンスをリセットする場合、クォータユーザー名が「\」文字で構成されているときは、別の「\」を追加してから、アプライアンスをリセットします。たとえば、クォータユーザー名「vol:W2012-01\administrator@AD1」が見つかった場合、リセットを実行する前に、クォータユーザー名を編集（「\」を追加）して「W2012-01\\administrator@AD1」とします。リセットを実行する場合、プレフィックス「vol:」は必要ありません。

### reboot

ファイルシステム キャッシュをディスクにフラッシュし、実行中のすべてのプロセスを停止して、システムを再起動します。

### reportingconfig

レポートング システムを設定します。

### resetconfig

出荷時の初期状態に設定を復元します。

### revert

Web オペレーティング システム用の AsyncOS を以前の認定済みビルドに復元します。これは非常に危険な操作で、すべての設定ログおよびデータベースを破棄します。このコマンドの使用については、[以前のバージョンの AsyncOS for Web への復元, on page 215](#)を参照してください。

### rollbackconfig

直前に確定した 10 の設定のうち 1 つをロールバックできます。デフォルトでは、ロールバック設定機能が有効になっています。

### rollovernow

ログ ファイルをロール オーバーします。

### routeconfig

トラフィックの宛先 IP アドレスとゲートウェイを設定します。現在設定されているルートを表示し、エントリを作成、編集、削除、クリアするための操作メニューを提供します。

### saveconfig

現在の設定のコピーをファイルに保存します。必要に応じて、このファイルを使用してデフォルトを復元できます。

FIPS モードが有効な場合は、パスフレーズ処理オプション `Mask passphrases` または `Encrypt passphrases` を指定します。

**setgateway**

マシンのデフォルト ゲートウェイを設定します。

**sethostname**

hostname パラメータを設定します。

**setntlmsecuritymode**

NTLM 認証レルムのセキュリティ設定を、「ads」または「domain」に変更します。

- domain : AsyncOS は Active Directory ドメインにドメイン セキュリティ信頼アカウントを結合します。AsyncOS では、Active Directory はこのモードでネストされた Active Directory グループだけを使用する必要があります。
- ads : AsyncOS は、Active Directory のネイティブ メンバーとしてドメインを結合します。

デフォルト設定は ads です。

**settime**

システム時刻を設定します。

**settz**

現在のタイムゾーンとタイムゾーンのバージョンを表示します。ローカルタイムゾーンを設定する操作メニューを提供します。

**showconfig**

すべての設定値を表示します。



---

**Note** ユーザーのパスワードは暗号化されます。

---

**shutdown**

接続を終了してシステムをシャットダウンします。

**smbprotoconfig**

Samba バージョン 4.11.15 の SMB1 プロトコルサポートを有効または無効にします。

Choose the operation you want to perform:

- 有効 (Enable) : SMB1 プロトコルを有効にします
- 無効 (Disable) : SMB1 プロトコルを無効にします

**smtprelay**

内部的に生成された電子メールのSMTPリレーホストを設定します。SMTPリレーホストは、システムで生成された電子メールやアラートを受け取るために必要です。

**smtpconfig**

SNMPクエリーをリッスンしてSNMP要求を受け入れるように、ローカルホストを設定します。

**sshconfig**

信頼できるサーバーのホスト名とホストキーオプションを設定します。



**Note** AsyncOS 14.x から AsyncOS 15.x にアップグレードすると、デフォルトの `sshconfig` 値を確認できます。アップグレード後、SWA で操作を続行する直前に、`sshconfig` 値をサポートされている値に再設定する必要があります。

**sslconfig**

[バージョン (VERSIONS)] : SSL/TLSバージョンを有効/無効にします。このオプションを使用して、次のサービスのSSL/TLSバージョンを有効または無効にできます。

- [LDAPS] : セキュアLDAPサービス（認証、外部認証、SaaS SSO、およびセキュアモビリティを含む）。
- [アップデータ (Updater)] : 更新サービス
- [WebUI] : アプライアンス管理 Web ユーザーインターフェイス
- [RADSEC] : セキュアRADSECサービス（認証、外部認証を含む）
- [SICAP] : セキュアICAPサービス
- [プロキシ (Proxy)] : プロキシサービス（セキュアクライアント用のHTTPSプロキシとログイン情報の暗号化を含む）。

[暗号 (CIPHERS)] : Cisco Secure Web Appliance でサービスの暗号を設定します。

暗号方式は、次のサービスに対して構成できます。

- プロキシ : プロキシ : プロキシサービス（セキュアクライアント用のHTTPSプロキシとログイン情報の暗号化を含む）。
- NextGenUI : 次世代 Web ユーザー インターフェイス

AsyncOS バージョン 9.0 以前のデフォルトの暗号は、`DEFAULT:+kEDH` です。

AsyncOS バージョン 9.1 ~ 11.8 のデフォルトの暗号は、次のとおりです。

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

この場合、デフォルトの暗号は ECDHE 暗号の選択によって変わる場合があります。

AsyncOS バージョン 12.0 以降のデフォルトの暗号は、次のとおりです。

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384

EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```



**Note** 新しい AsyncOS バージョンにアップグレードする際に、デフォルトの暗号スイートを更新します。暗号スイートは自動的に更新されません。以前のバージョンから AsyncOS 12.0 以降にアップグレードする場合は、暗号スイートを次のように更新することを推奨します。

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384

EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

**FALLBACK** : SSL/TLS のフォールバック オプションを有効または無効にします。イネーブルの場合、リモートサーバーとの通信は、ハンドシェイクの失敗後、最も低く設定されているプロトコルにフォールバックします。

プロトコルバージョンがクライアントとサーバーの間でネゴシエートされると、実装の問題が原因でハンドシェイクが失敗する可能性があります。このオプションがイネーブルの場合、プロキシは現在設定されている TLS/SSL プロトコルの最も低いバージョンを使用して接続を試みます。



**Note** AsyncOS 9.x の新規インストール時、フォールバックはデフォルトでディセーブルに設定されています。フォールバック オプションがある以前のバージョンからアップグレードする場合、現在の設定が保持されます。そうでない場合、つまりこのオプションがないバージョンからアップグレードする場合、フォールバックはデフォルトでイネーブルに設定されています。

**ECDHE** : LDAP での ECDHE 暗号の使用を有効または無効にします。

その後のリリースで追加の ECDH 暗号がサポートされていますが、追加の暗号とともに提供された特定の名前付き曲線が原因で、セキュア LDAP 認証と HTTPS トラフィック復号の際中に、アプライアンスが接続をクローズする場合があります。追加の暗号の指定については、[SSL の設定](#) , on page 197 を参照してください。

これらの問題がある場合は、このオプションを使用して、一方または両方の機能で ECDHE 暗号の使用をディセーブルにするか、またはイネーブルにします。



## ssltool

アプライアンスの CLI から別の OPENSSL コマンドを実行し、SSL 接続のトラブルシューティングを行います。ssltool コマンドには、次のサブコマンドが用意されています。

- **scient** : これは openssl s\_client コマンドの CLI バージョンです。アプライアンスを使用せずに直接 SSL/TLS を使用してリモート ホストに接続します。
  - **COMMAND** : openssl s\_client コマンドを実行します。次の openssl s\_client コマンドがサポートされます。
 

```
-connect, -servername, -verify, -cipher, -verify_return_error, -reconnect, -pause,
-showcerts, -prexit, -state, -debug, -msg, -tls1, -tls1_1, -tls1_2, -no_ssl2,
-no_ssl3, -no_tls1, -no_tls1_1, -no_tls1_2, -tlsextdebug, -no_ticket, -status,
-save, -noout
```

サポートされる openssl s\_client コマンドの詳細については、インラインヘルプを参照してください。



### Note

command の実行後、-save オプションを使用して出力をファイルに保存できます。保存されたログファイルにアクセスすることはできません。これらのログ ファイルは、シスコ サポート チームによってデバッグに使用されます。

- **HELP** : ヘルプ情報を提供します。
- **CLEARLOGS** : ssltool によって生成されたすべてのログを削除します。

## status

システム ステータスを表示します。

## supportrequest

サポート要求の電子メールを Cisco カスタマーサポートに送信します。これには、システム情報およびプライマリ設定のコピーが含まれます。

(オプション) サービス要求番号を指定すると、システム情報と設定情報の大きなセットがサービス要求に自動的に追加されます。この情報は ZIP で圧縮され、FTP を使用してサービス要求にアップロードされます。

## tail

ログ ファイルの末尾を表示します。コマンドは、ログ ファイル名をパラメータとして受け入れます。

### 例 1

```
example.com> tail
Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
```

```
2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
...
...
Enter the number of the log you wish to tail.
[]> 9
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 10:03:07 2017 Info: Begin Logfile
~
~
...
...
"CTRL-C" + "q"
```

## 例 2

```
example.com> tail system_logs
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 09:59:10 2017 Info: Begin Logfile
...
...
"CTRL-C" + "q"
```

## tcpservices

開かれている TCP/IP サービスに関する情報を表示します。

## techsupport

Cisco カスタマー サポートがシステムにアクセスしてトラブルシューティングを支援できるように、一時的な接続を提供します。

## testauthconfig

特定の認証レルムで定義された認証サーバーに対して、そのレルムの認証設定をテストします。

### testauthconfig [-d level] [realm name]

オプションを指定せずにコマンドを実行すると、設定されている認証レルムのリストが表示されるので、そのリストから選択できます。

デバッグ フラグ (- d) によってデバッグ情報のレベルが制御されます。指定できるレベルの範囲は 0~10 です。指定しない場合は、レベル 0 が使用されます。レベル 0 の場合は、コマンドによって成功または失敗が返されます。テスト設定が失敗すると、失敗の原因が一覧表示されます。



#### Note

レベル 0 を使用することを推奨します。トラブルシューティングのためにさらに詳細な情報が必要な場合にのみ、別のデバッグ レベルを使用してください。

**tuiconfig tuistatus**

これらの 2 つのコマンドについては、[CLI を使用した透過的ユーザー識別の詳細設定, on page 86](#) で説明しています。

**traceroute**

ゲートウェイを通過し、宛先ホストまでのパスをたどって、IP パケットをトレースします。

**trailblazerconfig**

trailblazerconfig コマンドを使用すると、新しい Web インターフェイスで HTTP と HTTPS のポートを介して受信接続と送信接続をルーティングできます。



**Note** デフォルトで、trailblazerconfig の CLI コマンドはアプライアンスで有効になっています。help trailblazerconfig コマンドを入力すると、インライン ヘルプを参照できます。

構文は次のようになります。

```
trailblazerconfig enable <https_port> <http_port>
trailblazerconfig disable
trailblazerconfig status
```

ここで、

'enable' は、デフォルトのポート（HTTPS: 4431 または HTTP: 801）で trailblazer を実行します。

'disable' は trailblazer を終了します

'status' は trailblazer のステータスをチェックします。



**Note** アプライアンスで trailblazerconfig コマンドを有効にしている場合、リクエスト URL にはホスト名に付加された HTTP/HTTPS ポート番号が含まれます。

ブラウザの操作をシームレスにするために、以下のいずれかのステップを試行できます。

- Web インターフェイスで使用される証明書を承認し、新しいブラウザウィンドウで `https://hostname:<https_api_port>`（例: `https://some.example.com:6443`）の URL 構文を使用して証明書を承認します。ここで、<https\_api\_port> は [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] で設定されている AsyncOS API HTTPS ポートです。また、API ポート (HTTP/HTTPS) がファイアウォールで開かれていることを確認します。
- デフォルトで、trailblazerconfig の CLI コマンドはアプライアンスで有効になっています。HTTP または HTTPS ポートがファイアウォールで開かれていることを確認します。

また、アプライアンスにアクセスするために指定したホスト名を DNS サーバーが解決できることを確認します。

`trailblazerconfig` の CLI コマンドが無効になっている場合、CLI を使用して **trailblazerconfig > enable** コマンドを実行することにより、以下の問題を回避できます。

- 特定のブラウザで API ポートの複数の証明書を追加する必要がある。
- スпам隔離、セーフリスト、またはブロックリストのページを更新するときに、レガシー Web インターフェイスにリダイレクトされる。
- Advanced Malware Protection レポートページのメトリックバーにデータが含まれない。

### updateconfig

アップデートおよびアップグレードを設定します。

### updatenow

すべてのコンポーネントを更新します。

### upgrade

AsyncOS ソフトウェア アップグレードをインストールします。

`downloadinstall` : アップグレードパッケージをダウンロードし、即時にインストールします。

`download` : アップグレードパッケージをダウンロードし、後でインストールできるように保存します。

いずれかのコマンドを入力すると、この Secure Web Appliance に適用可能なアップグレードパッケージのリストが表示されます。使用するパッケージのエントリ番号を入力してそのパッケージを選択し、Enter キーを押します。ダウンロードがバックグラウンドで開始されます。ダウンロード中に、サブコマンド `downloadstatus` と `canceledownload` を使用できます。

最初に `downloadinstall` を入力した場合、ダウンロードが完了するとインストールが即時に開始されます。`download` を入力した場合は、ダウンロード完了時に 2 つのコマンド (`install` と `delete`) が使用可能になります。`install` と入力すると、以前にダウンロードしたパッケージのインストールが開始します。`delete` と入力すると、以前にダウンロードしたパッケージが Secure Web Appliance から削除されます。

### userconfig

システム管理者を設定します。

### version

一般的なシステム情報、インストールされているシステムソフトウェアのバージョン、およびルールの定義を表示します。

**wccpstat**

**all** : すべての WCCP (Web Cache Communication Protocol) サービス グループの詳細を表示します。

**servicegroup** : 特定の WCCP サービス グループの詳細を表示します。

**webcache**

プロキシキャッシュの内容を確認または変更したり、アプライアンスにキャッシュされないドメインと URL を設定します。管理者は特定の URL をプロキシキャッシュから削除したり、プロキシ キャッシュに保存しないドメインや URL を指定できます。

**who**

CLI および Web インターフェイス セッションの両方について、システムにログインしているユーザーを表示します。



---

**Note** 各ユーザーは、最大 10 の同時セッションを持つことができます。

---

**whoami**

ユーザー情報を表示します。



## 付録 A

# その他の情報

この章で説明する内容は、次のとおりです。

- [Cisco 通知サービス](#) , on page 805
- [ドキュメント セット](#) , on page 805
- [トレーニング](#) , on page 806
- [ナレッジ ベースの記事](#) , on page 806
- [シスコサポートコミュニティ](#) , on page 806
- [カスタマー サポート](#) , on page 807
- [リソースにアクセスするためのシスコ アカウントの登録](#) , on page 807
- [マニュアルに関するフィードバック](#) , on page 807
- [サードパーティ コントリビュータ](#) (807 ページ)
- [個人情報の取り扱い](#) (808 ページ)

## Cisco 通知サービス

セキュリティ アドバイザリ、フィールド ノーティス、販売終了とサポート終了の通知、およびソフトウェア アップデートと既知の問題に関する情報などの Cisco コンテンツ セキュリティ アプライアンスに関連する通知が配信されるように署名して参加します。

受信する情報通知の頻度やタイプなどのオプションを指定できます。使用する製品ごとの通知に個別に参加する必要があります。

参加するには、以下の URL に移動します。 <http://www.cisco.com/cisco/support/notifications.html>

Cisco.com アカウントが必要です。ない場合は、 [リソースにアクセスするためのシスコ アカウントの登録](#) , on page 807 を参照してください。

## ドキュメント セット

Cisco Secure Web Appliance の関連資料は、以下の場所から入手できます。

| 製品                                             | リンク                                                                                                                                                                                                                                                               |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Web Applianceについて<br>(ハードウェア マニュアルを含む)。 | <a href="http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html</a>                               |
| コンテンツセキュリティ管理アプライアンス<br>(ハードウェア マニュアルを含む)。     | <a href="http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html</a> |
| Cisco Cloud Web Security<br>(ハードウェア マニュアルを含む)。 | <a href="http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html</a>                                       |

## トレーニング

Cisco 電子メールおよび Web セキュリティ製品のトレーニングは以下で提供しています。

<http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html>

## ナレッジベースの記事

### Procedure

ステップ 1 製品のメイン ページに移動します (<http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html>)。

ステップ 2 名前に **TechNotes** が付くリンクを探します。

## シスコサポートコミュニティ

Web セキュリティと関連管理については、以下の URL からシスコ サポート コミュニティにアクセスしてください。

<https://supportforums.cisco.com/community/5786/web-security>

シスコ サポート コミュニティは、Web セキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。たとえば、投稿にトラブルシューティングのビデオが添えられていることもあります。

## カスタマー サポート

Cisco TAC : [http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html)

従来の IronPort のサポート サイト : <http://www.cisco.com/web/services/acquisitions/ironport.html>

仮想アプライアンスについては、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。

重大ではない問題の場合は、アプライアンスからサポート事例を開くこともできます。

### 関連項目

- サポートの使用 , on page 771

## リソースにアクセスするためのシスコアカウントの登録

Cisco.com の多数のリソースへアクセスするには、シスコのアカウントが必要です。

Cisco.com のユーザ ID をお持ちでない場合は次のリンク先で登録できます。 <https://www.cisco.com/c/en/us/about/help/login-account-help.html>

## マニュアルに関するフィードバック

シスコのテクニカル マニュアル チームは、製品ドキュメントの向上に努めています。コメントおよびご提案をお待ちしています。以下のメール アドレスまでご意見をお寄せください : [contentsecuritydocs@cisco.com](mailto:contentsecuritydocs@cisco.com)

メッセージの件名行に、このマニュアルのタイトルとタイトルページに記載されている発行日をご記入ください。

## サードパーティ コントリビュータ

AsyncOS に含まれている一部のソフトウェアは、FreeBSD Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives Inc.、および他のサードパーティ コントリビュータのソフトウェア使用許諾契約の条項、通知、および条件に基づいて配布されています。これらすべての契約条件はライセンス契約に含まれています。これらの契約内容の全文は次の URL を参照してください。

[https://support.ironport.com/3rdparty/AsyncOS\\_User\\_Guide-1-1.html](https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html)

AsyncOS 内の一部のソフトウェアは、Tobi Oetiker の書面による同意を得て、RRDtool を基にしています。



このマニュアルには、Dell Computer Corporation の許可を得て複製された内容が一部含まれています。このマニュアルには、McAfee の許可を得て複製された内容が一部含まれています。このマニュアルには、Sophos の許可を得て複製された内容が一部含まれています。

## 個人情報の取り扱い

ユーザーエクスペリエンスを向上させるために、また通知やレポートを適時に送信するために、Cisco Secure Web Applianceではユーザーのフルネームと電子メールアドレスが収集されます。

管理者が Cisco Secure Web Applianceを管理するためのユーザーアカウントを作成すると、アプライアンスはこの情報を収集します。この情報には、アカウントの所有者と管理者だけがアクセスできます。この情報を変更できるのは管理者だけです。

この情報はアプライアンス内にローカル保存され、機能、チーム、またはサードパーティアプリケーションと共有されません。

この情報は、ユーザーがアクティブな Cisco Secure Web Appliance アカウントを取得するまで保持され、管理者がユーザーアカウントを削除するとシステムから削除されます。



## 付 録 **B**

# エンド ユーザ ライセンス 契約書

この章で説明する内容は、次のとおりです。

- [Cisco Systems エンド ユーザ ライセンス 契約書](#) , on page 809
- [Cisco コンテンツ セキュリティ ソフトウェア用 エンド ユーザ ライセンス 契約 補則](#) , on page 816

## Cisco Systems エンド ユーザ ライセンス 契約書

**重要：**本エンドユーザライセンス契約書をよくお読みください。お客様がシスコのソフトウェアまたは機器を認定販売元から購入したかどうか、また、お客様ご自身またはお客様が代表する法人（総称して「お客様」）がこのシスコ エンド ユーザ ライセンス 契約におけるエンド ユーザとして登録済みかどうかを確認することは、非常に重要です。エンド ユーザとして登録されていないお客様は本ソフトウェアを使用するライセンスを有しておらず、このエンド ユーザ ライセンス 契約の限定保証は適用されません。お客様が認定販売元から購入されたことを前提として、シスコのソフトウェア、またはシスコが提供するソフトウェアをダウンロード、インストールまたは使用することにより、お客様はこの契約に同意したものと見なされます。

Cisco Systems, Inc. または同社に代わり本ソフトウェアのライセンスを許諾する同社の関連会社（以下、「シスコ」）は、お客様が本ソフトウェアを認定販売元から購入し、かつ本エンド ユーザ ライセンス 契約書に含まれるすべての条件、および本製品に添付され、お客様の発注時に入手可能になる補遺ライセンス契約書に記載の、ライセンスに関する一切の追加制限条件（以下総称して「本契約」）に同意する場合に限り、お客様に対し本ソフトウェアのライセンスを許諾します。本エンド ユーザ ライセンス 契約書内の各規定と補遺ライセンス契約書内の各規定が矛盾する場合、補遺ライセンス契約書内の各規定が優先します。本件ソフトウェアをダウンロード、インストール又は使用することにより、お客様は本件ソフトウェアをご自身が認定販売元から購入したことを表明したこととなり、お客様に本契約の拘束力が及びます。お客様が本契約のすべての規定に同意しない場合、シスコは、お客様による本件ソフトウェアの使用を許諾しません。その場合、（A）お客様は、本件ソフトウェアをダウンロード、インストール、または使用できません、また、（B）お客様は、本件ソフトウェア（あらゆる未開封の CD パッケージや関連文書を含む）を返却して全額払い戻しを受けられます。または、本件ソフトウェアと関連文書が、別の製品の一部として提供されたものである場合には、当該製品全体を返却して全額払い戻しを受けられます。返却および代金払い戻しの有効期限は、認定販売元から本ソフトウェアを購入後 30 日間であり、お客様が最初の登録済みエンド ユーザ購入

者である場合にのみ適用されます。本エンドユーザライセンス契約において、「認定販売元」とは、(A) シスコ、(B) 対象地域内でエンドユーザにシスコの機器、ソフトウェアおよびサービスを配布および/もしくは販売することについてシスコより認定を受けたディストリビュータもしくはシステムインテグレータ、または (C) シスコの機器、ソフトウェアおよびサービスをお客様の地域内でエンドユーザに配布および/もしくは販売することについて、ディストリビュータとシスコとの契約の条件に従い、ディストリビュータもしくはシステムインテグレータにより認定された再販業者を意味します。

本契約の以下の条件は、本ソフトウェア（後に定義）のお客様による使用に適用されます。ただし、(a) 本ソフトウェアのお客様による使用に適用される、お客様とシスコとの間の別段の署名済み契約が存在する場合、または (b) 本ソフトウェアに、導入もしくはダウンロードの手続きの一部として、本ソフトウェアのお客様による使用に適用される別段の「クリック同意」ライセンス契約もしくは第三者ライセンス契約が含まれている場合は、この限りではありません。上記各契約書内の各規定が矛盾する場合、その優先順位は、以下のとおりです。(1) 署名済みの契約、(2) クリック同意契約または第三者のライセンス契約、(3) 本契約。本契約において、「本ソフトウェア」とは、認定販売元からお客様に提供されるシスコ機器に組み込まれたファームウェアおよびコンピュータ プログラムを含むコンピュータ プログラム、ならびに一切のアップグレード、更新、バグ修正またはこれらの修正バージョン（総称して「アップグレード」）であって、*Cisco Software Transfer and Re-licensing Policy*（随時シスコによりなされる修正を含む）に基づいて再許諾されたもの、またはこれらのいずれかのバックアップコピーを意味します。

**本件ライセンス。**本契約の各契約条件に従うことを条件として、シスコはお客様に対し、お客様が必要なライセンス料を認定販売元に支払った本ソフトウェアおよび本文書を社内業務目的で使用するための、非排他的かつ譲渡不能なライセンスを付与します。「本文書」とは、本ソフトウェアに関する情報を文書化したもの（当該情報がユーザマニュアル、技術マニュアル、研修資料、仕様書その他のいずれに含まれているか否かは問わない）であって、認定販売元が何らかの形式（CD-ROMやオンラインを含む）により本ソフトウェアとともに提供するものを意味します。本ソフトウェアを使用するには、登録番号または製品認証キーを入力し、シスコの Web サイトにてお手持ちの本ソフトウェアをオンライン登録した上で、必要なライセンスキーまたはライセンス ファイルを入手する必要があります。

お客様が本ソフトウェアを使用するためのライセンスは、単一のハードウェアシャーシもしくはカード、または該当する補遺ライセンス契約書、もしくは認定販売元が同意済みで、お客様が必要なライセンス料を認定販売元に支払済みの該当する発注書（以下、「本発注書」）に記載されているその他の制限に限定され、お客様はこの制限を超えて本ソフトウェアを使用してはなりません。

本文書または該当する補遺ライセンス契約書に別途明記されていない限り、お客様は、以下のいずれかのみを目的として本ソフトウェアを使用する必要があります。お客様が所有または賃借しており、お客様の社内業務目的に使用されるシスコ機器に本ソフトウェアを組み込んで使用すること。当該シスコ機器上で本ソフトウェアを実行すること。（対応する本文書が、シスコ以外の機器に本ソフトウェアをインストールすることを許可している場合に）当該シスコ機器と通信すること。お客様には上記以外のいかなるライセンス（黙示のライセンス、禁反言の法理が適用されるライセンス、またはその他のライセンス）も付与されません。

シスコがライセンス料を徴収しない評価版またはベータ版については、上記のライセンス料の支払い要件は適用されません。

一般的な各種制限。本契約は、本ソフトウェアおよび本文書の使用許諾であり、これらの権原を移転するものではありません。シスコは、本ソフトウェアおよび本文書のコピーのすべてについて所有権を留保します。お客様は、本件ソフトウェアおよび本文書に、シスコまたはそのサプライヤもしくはライセンサの営業秘密が含まれていることを認識しているものとします。この営業秘密には、各プログラムの固有の内部設計および構造ならびに関連インターフェイス情報が含まれますが、これらのみには限定されません。本契約に明示的に別段の規定がない限り、お客様は、お客様が認定販売元から購入したシスコ機器の使用に関連する場合にのみ本ソフトウェアを使用するものとし、以下のいずれについてもこれを行う権利を有しておらず、またこれを行わないことについて特に同意するものとします。

(i) 他の個人もしくは法人に、ライセンス権を移転もしくは譲渡するか、本ライセンスのサブライセンスを付与すること（その時点で有効な、シスコのライセンスの再許諾および移転に関するポリシーに従って行う場合は除きます）、または、お客様が認定販売元から購入したものではないシスコ機器もしくは中古のシスコ機器上で本ソフトウェアを使用すること。なお、お客様は、計画された移転、譲渡、サブライセンスの付与または使用はいずれも無効となることを了解するものとします。

(ii) 以下のいずれかを行うこと。(a) 本件ソフトウェアのエラーを修正するか、本件ソフトウェアを変更または改変すること、(b) 本件ソフトウェアをもとに派生物を作成するか、第三者による当該行為を許可すること。

(iii) 本ソフトウェアを対象とするリバースエンジニアリング、逆コンパイル、復号、逆アセンブルを行うか、その他の方法で本ソフトウェアを人間の可読形式に変換すること。なお、本制限事項にかかわらず、適用法に基づいて明示的に許可されている場合、または適用されるオープンソースライセンスに基づいて当該特定の行為を許容すべきことがシスコに義務づけられている場合は除きます。

(iv) 本ソフトウェアで実行したベンチマークテストの結果を公表すること。

(v) シスコの書面による許可なく、サービスビューロ、タイムシェアリング、またはその他の方法により、第三者へのサービス提供を目的として本ソフトウェアを使用、または使用を許可すること。

(vi) シスコの書面による事前の同意なしに、本ソフトウェアおよび本文書に含まれる企業秘密を第三者に対して開示、提供、またはその他の何らかの方法により公開すること。お客様は、かかる営業秘密を保護するため、相当のセキュリティ対策を講じる必要があります。

シスコは、準拠法により求められている範囲内で、お客様からの書面による依頼に応じて、本ソフトウェアと独自に開発された他のプログラムとの互換性を実現するために必要なインターフェイス情報を、シスコが妥当とみなす料金が支払われた場合にお客様に提供するものとします。お客様は、上記情報について厳格な秘密保持義務を遵守すると共に、その提供条件としてシスコが提示した準拠規定に従って上記情報を使用する必要があります。

**本件ソフトウェア、本件アップグレード版、および追加コピー版。**本契約のその他の規定にかかわらず、以下の条件が適用されます。(1) お客様は、追加コピー版またはアップグレード版の作成または取得時に、オリジナルのソフトウェアの有効なライセンスを保有しており、アップグレードまたは追加コピー版の適用料金を認定販売元に支払っている場合を除き、かかる追加コピー版またはアップグレード版を作成または使用するライセンスまたは権利を有しません。(2) アップグレードの使用は、お客様が最初のエンドユーザ購入者または賃借者であるか、またはアップグレードされるソフトウェアを使用するための有効なライセンスを保持し

ており、かつ認定販売元から供給されたシスコ機器に限定されます。(3) 追加の複製物の作成および使用は、必要なバックアップ用途のみに限定されます。

所有権表示。お客様は、いかなる形式であれ、本ソフトウェアのすべての複製物について、あらゆる著作権、財産権およびその他の表示を、それらの著作権およびその他の所有権の表示が本ソフトウェアに含まれているのと同じ形式かつ方法で保持し、複製することに同意します。本契約に基づき明示的に許可される場合でなければ、お客様は、シスコから書面による事前の許可を得ることなく本件ソフトウェアのコピー版または複製物を作成してはなりません。

契約の期間および終了。本契約および本契約において供与されるライセンスは、終了時まで有効に存続します。お客様は、本件ソフトウェアおよび本件文書のすべてのコピーを破棄することにより、随時、本契約および本件ライセンスを終了させることができます。お客様が本契約のいずれかの規定に従わなかった場合、本契約に基づくお客様の権利は、シスコからの通知なしにただちに終了します。お客様は、本契約の終了時に、お客様が保有または管理する本ソフトウェアおよび本文書のすべての複製物を破棄する必要があります。お客様のあらゆる守秘義務、「一般的な制限」と題する条項に基づいてお客様に課されたあらゆる制約および制限、あらゆる責任制限、および保証の否認と制限はすべて、本契約終了後も存続するものとします。また「米国政府がエンドユーザ購入者の場合」および「限定保証表明およびエンドユーザライセンス契約書に適用される一般規定」と題された各条項の各規定の効力は、本契約の終了後も存続します。

お客様の記録の検査。お客様は、シスコとその独立会計士に対して、お客様の通常の営業時間中にお客様の帳簿、記録、財務諸表を査察し、本契約の条項に従っていることを確認する権利を認めるものとします。上記監査の結果、本契約に反する行為が発覚した場合、お客様は、相当のライセンス料に上記監査の実施に伴う相当の費用を加えた額を、速やかにシスコへ支払う必要があります。

輸出、再輸出、移転、および使用に関する規制。本契約に基づいてシスコによって供給されるソフトウェア、本文書、および技術、またはそれらの直接的な製品（「本製品および技術」）は、アメリカ合衆国（「米国」）の法令およびその他関連国の法令に基づく輸出規制の対象となっています。お客様は、シスコの本件ソフトウェアと付帯技術の輸出、再輸出、移転、および使用に適用される各種法規に従う必要があるとともに、必要となる米国および現地の各種許可、認可、または許諾をすべて取得するものとします。シスコおよびお客様は互いに、承認の確保またはライセンスに関し、他方当事者から妥当に要求されたその他の情報、裏付け文書および支援を提供することに同意します。コンプライアンス、輸出、再輸出、移転、および使用についての法律に関する情報は、以下の URL に掲載されています。

[https://www.cisco.com/web/about/doing\\_business/legal/global\\_export\\_trade/general\\_export\\_contract\\_compliance.html](https://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export_contract_compliance.html)

米国政府機関がエンドユーザ購入者である場合。本ソフトウェアおよび資料は、連邦調達規則（FAR）（以下「FAR」）(48 C.F.R.) 2.101 で定義される「商用品目」に分類されます。これは、「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア関連資料」で構成されます（当該用語は FAR 12.212 で使用されています）。FAR 12.212 および DoD FAR 補則。227.7202-1 から 227.7202-4 で定められているとおり、また、他の FAR 条項、または本契約の組み込み先である契約書内のこれと矛盾する他の契約条項にかかわらず、お客様は、連邦政府機関エンドユーザに対して、本ソフトウェアおよび本文書とともに本契約に定める権利のみを提供することができ、または、本契約が直接契約である場合は、連邦政府機関エンドユーザは、本ソフトウェアおよび本文書とともに本契約に定める権利のみを取得します。ソフ

トウェアと資料のいずれか、または両方を使用することにより、政府機関は、本ソフトウェアと資料が「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア関連資料」であることに同意し、この契約書に規定されている権利および制限に同意したことになります。

指定コンポーネントおよび追加条件。本件ソフトウェアは、本書に規定されたものとは異なるライセンス契約条件、保証の否認、制限付き保証又は他の条件（総称して「追加条件」）が適用される、第三者のコンポーネントを含んでいる可能性のある単一又は複数のコンポーネントであって、本件文書、`readme.txt` ファイル、第三者のクリック同意又はその他

（<https://www.cisco.com/> 上など）においてシスコにより指定されたもの（「指定コンポーネント」）を含むこと、又は指定コンポーネントと共に提供されることがあります。お客様は、かかる指定コンポーネントについて該当する追加条件に同意するものとします。

### 限定保証

本契約に規定の各種制限および条件を前提として、シスコは、お客様への出荷日（シスコ以外の認定販売元による再販の場合、シスコの初回出荷より 90 日以内の日）を始期として、(a) 90 日間、または (b) 本ソフトウェアを組み込んでいる製品（以下、「本製品」）に添付される保証カード（存在する場合）に明記されている、本ソフトウェアに固有の保証期間（設定されている場合）、のいずれか長い方の期間内で、(a) 通常の使用において、本ソフトウェアの提供媒体に材質上および製造上の欠陥がないこと、ならびに (b) 本ソフトウェアが本文書に実質的に適合していること、を保証します。シスコによる本件製品の出荷日は、本件製品の出荷に用いられる梱包材に記載されています。上記を除き、本ソフトウェアは「現状のまま」で提供されます。この限定保証は、最初の登録済みエンドユーザたるお客様が認定販売元から購入した本ソフトウェアに対してのみ適用されます。この限定保証のもとでは、お客様の唯一の救済、かつシスコおよびそのサプライヤの全責任は、(i) 欠陥のある媒体の交換、および/または (ii) シスコの選択により、本ソフトウェアの修理、交換、もしくは代金の返金に限定されます。いずれの場合も、この限定保証に反するようなエラーまたは欠陥が、保証期間内に、お客様に本ソフトウェアを提供した認定販売元に報告されることを条件とします。シスコ、またはお客様に本ソフトウェアを提供した認定販売元は、救済の条件として、自らの判断で、本ソフトウェアおよび/または本文書の返却を請求できます。シスコはいかなる場合でも以下の 2 点について保証しません。(i) 本件ソフトウェアにエラーが生じないこと、(ii) お客様が、問題または障害なく本件ソフトウェアを使用できること。また、ネットワークへの侵入やネットワークの攻撃を目的とする新技術が日々開発されているため、シスコは、本件ソフトウェアまたは本件ソフトウェアが使用される各種機器、システムもしくはネットワークが、侵入または攻撃に耐えられることについても保証しません。

制約事項。この保証は、本件ソフトウェア、本件製品、または本件ソフトウェアの使用先として許可されているその他の機器が以下のいずれかに該当するものの場合には適用されません。

(a) シスコまたはシスコ認定代理人以外によって改変されたもの、(b) シスコが提示した指示に従ってインストール、運用、メンテナンスされていないもの、(c) 異常な物理的もしくは電氣的負荷、異常な環境条件、誤使用、過失、事故による影響を受けたもの、(d) ベータ版、評価版、テスト版、実演版としてその使用が許諾されているもの。本ソフトウェアの保証は、以下のいずれかに該当するものには適用されません。(e) 一時的に使用される本ソフトウェアの各種モジュール、(f) シスコのソフトウェア センターに掲載されていないあらゆる本ソフトウェア、(g) シスコがシスコのソフトウェア センターにて「現状のまま」で明示的に提供しているあらゆる本ソフトウェア、(h) 認定販売元がライセンス料を受領していない



あらゆる本ソフトウェア、および (i) 認定販売元以外の第三者から供給された本ソフトウェア。

### 保証の否認

保証に関する本条項に明記されているものを除き、あらゆる明示または黙示の条件、表明および保証は、適用法により許される範囲で除外され、シスコ、そのサプライヤおよびライセンサーによって明示的に放棄されます。上記条件、表明および保証は、以下の (i) または (ii) を含みますが、これらに限定されません。(i) 商品性、特定目的への適合性、非侵害、十分な品質、不干渉、情報内容の正確性に関する黙示の保証または条件、(ii) 各種取引、法律、利用、または商慣行に起因する黙示の保証または条件。これらのいずれかが排除できない場合はその範囲において、かかる黙示の条件、表明および/または保証の存続期間は、上記の「限定保証」条項で言及されている明示的な保証期間に限定されます。州または司法管轄区域によっては、黙示保証の有効期間を限定することが許可されていないため、お客様に上記の制限が適用されない場合があります。この保証は、お客様に特定の法的権利を付与するものですが、お客様は、法域によってはその他の権利を有する場合があります。この放棄および除外は、上記の明示保証がその本質的な目的を達成できない場合にも適用されるものとします。

責任の否認-責任の制限。本ソフトウェアの取得地が米国、ラテンアメリカ諸国、カナダ、日本またはカリブ海沿岸諸国の場合、本契約中の別段の規定にかかわらず、お客様に対するシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーの合算での全責任は、契約、不法行為（過失を含む）、保証違反またはその他の原因に基づくかを問わず、当該請求を生じさせた本ソフトウェアについてお客様が認定販売元に支払った価格、または本ソフトウェアが対象外製品の一部である場合には当該製品について支払われた価格を超えないものとします。ソフトウェアの当該責任の制限は累積的なものであり、一件毎のものではありません。(すなわち、複数の請求が行われた場合でも制限が拡大されることはありません)。

本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニアの場合、本契約中の別段の規定にかかわらず、お客様に対するシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーの合算での全責任は、契約、不法行為（過失を含む）、保証違反またはその他の原因に基づくかを問わず、当該請求を生じさせた本ソフトウェアについてお客様がシスコに支払った価格、または本ソフトウェアが対象外製品の一部である場合には当該対象外製品について支払われた価格を超えないものとします。ソフトウェアの当該責任の制限は累積的なものであり、一件毎のものではありません。(すなわち、複数の請求が行われた場合でも制限が拡大されることはありません)。本契約のいかなる規定も、(i) シスコ、ならびにその関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーが、その過失に起因する身体障害または死亡に関してお客様に対して負う責任、(ii) 詐欺的な不実表示に関するシスコの責任、または (iii) 適用法のもとで排除できないシスコの責任を限定するものではありません。

責任の否認-結果的損害および他の損失に関する免責。本ソフトウェアの取得地が米国、ラテンアメリカ諸国、カリブ海沿岸諸国またはカナダの場合、本契約に定められている救済措置が、その本質的な目的を達成できないものであるかどうかにかかわらず、シスコまたはそのサプライヤは、いかなる場合でも、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、発生原因を問わず、責任論の種類、または本ソフトウェアの使用もしくは使用不能によって発生したかどうかにかかわらず、上記損害が発生する可能性についてシスコまたはそのサプライヤもしくはライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。一部

の州または法域では、結果的な損害または偶発的な損害の制限または除外が許可されていないため、上記制限がお客様に適用されない場合があります。

本ソフトウェアの取得地が日本の場合、死亡もしくは人身傷害または詐欺的な不実表示に起因または関連する責任を除き、本契約に定められている救済措置が、その本質的な目的を達成できないものであるかどうかにかかわらず、シスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーは、いかなる場合でも、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、発生原因を問わず、責任論の種類、または本ソフトウェアの使用もしくは使用不能によって発生したかどうかにかかわらず、上記損害が発生する可能性についてシスコもしくは認定販売元またはそれらのサプライヤもしくはライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。

本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニアの場合、シスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーは、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、その発生原因（契約、不法行為（過失を含む）または本ソフトウェアの使用もしくは使用不能に起因するものを含むが、これらに限定されない）にかかわらず、それぞれの場合において、たとえ当該損害が発生する可能性についてシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。州または司法管轄区域によっては、結果的または偶発的な損害の制限または除外が許可されていないため、お客様に上記の制限が完全には適用されない場合があります。上記の排除は、(i) 死亡または人身傷害、(ii) 詐欺的な不実表示、または (iii) 適用法のもとで排除できない条件に関連するシスコの責任、に起因または関連する責任には適用されません。

お客様は以下の3点について認識および同意しているものとします。(i) シスコは、本契約内の保証の放棄および責任の制限に依拠して価格を決定し本契約を結んでいること、(ii) これは、両当事者間のリスク配分（契約上の救済措置が、その本質的な目的を達成できず、結果的に損失を被るというリスクを含む）にも反映されていること、(iii) これは、両当事者間での取引の基幹を成す事項であること。

準拠法、管轄裁判所。本ソフトウェアの取得地が、認定販売元により受諾された発注書上の住所の記載から判断して、米国、ラテンアメリカ諸国またはカリブ海沿岸諸国の場合、本契約および保証（「本保証」）に関する規定は、法の抵触に関する条文にかかわらず米国カリフォルニア州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、カリフォルニア州内の州裁判所および連邦裁判所が専属的に管轄します。本ソフトウェアの取得地がカナダの場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず、カナダのオンタリオ州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、オンタリオ州内の各裁判所が専属的に管轄します。本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニア（オーストラリアを除く）の場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず英国の各法に準拠し、同法に従って解釈されます。本契約または本保証に起因する各種申し立てについては、英国内の各裁判所が専属的に管轄します。また、本契約が英国法に準拠する場合、本契約の当事者ではない者は、本契約のいずれの条項についても、Contracts (Rights of Third Parties) Act 1999（1999年契約（第三者の権利）法）に基づいて権利行使を行ったり、利益を享受した



りする権利を有しません。本ソフトウェアの取得地が日本の場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず日本国の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、日本国内の東京地方裁判所が専属的に管轄します。本ソフトウェアの取得地がオーストラリアの場合、現地法が明示的に禁止していない限り、本契約および本保証に関する規定は、法の抵触に関する条文にかかわらずオーストラリア連邦ニュー サウス ウェールズ州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、ニュー サウス ウェールズ州内の州裁判所および連邦裁判所が専属的に管轄します。本ソフトウェアの取得地がその他の国の場合、現地法が明示的に禁止していない限り、本契約および本保証に関する規定は、法の抵触に関する条文にかかわらず米国カリフォルニア州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、カリフォルニア州内の州裁判所および連邦裁判所が専属的に管轄します。

上記のすべての国について、両当事者は、国際物品売買契約に関する国際連合条約の規定の適用を明示的に否定します。上記にかかわらず、いずれの当事者も、当事者の知的所有権または所有権の侵害の申し立てに対して、適切な司法管轄区域の裁判所において暫定的な差し止めによる救済を求めることができます。本契約のいずれかの規定が無効または施行不能なものとなった場合でも、本契約の残りの規定および本件保証書は有効に存続します。本契約内に別段の明示規定がない限り、本契約は、本件ソフトウェアおよび本件文書の使用許諾に関する両当事者の合意事項をまとめた唯一の文書となり、本件注文書またはその他の文書内の抵触規定または追加規定に優先し、これらの規定はすべて除外されます。本契約書は英語で記述されており、両当事者は、英語版が優先することに同意しているものとします。

各種製品保証規定やシスコ製品に関するその他の情報は、以下の URL でご確認ください。

<http://www.cisco.com/go/warranty>

## Cisco コンテンツ セキュリティ ソフトウェア用エンド ユーザ ライセンス 契約補則

重要（よくお読みください）

本エンド ユーザ ライセンス 契約補則（以下「SEULA」）には、お客様とシスコとの間のエンド ユーザ ライセンス 契約（以下「EULA」）に基づいてライセンスされているソフトウェア製品に対する追加条項（以下、総称して「契約」）が記載されています。Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT TO THE AGREEMENT. お客様が本契約のすべての規定に同意しない場合、シスコは、お客様による本件ソフトウェアの使用を許諾しません。その場合、（A）お客様は、本件ソフトウェアをダウンロード、インストール、または使用できません、また、

(B) お客様は、本件ソフトウェア（あらゆる未開封の CD パッケージや関連文書を含む）を返却して全額払い戻しを受けられます。または、本件ソフトウェアと関連文書が、別の製品の一部として提供されたものである場合には、当該製品全体を返却して全額払い戻しを受けられます。返却および払い戻しに関するお客様の権利は、シスコまたはシスコ認定リセラーからの購入後30日で失効し、お客様が最初のエンドユーザー購入者である場合にのみ適用されます。

本 SEULA が対象とするお客様の製品の名称および詳細は、次の Cisco Systems E メールセキュリティ アプライアンス（「ESA」）、Cisco Systems Secure Web Appliance（「WSA」）、および Cisco Systems セキュリティ管理アプリケーション（「SMA」）（まとめて「コンテンツセキュリティ」と呼ぶ）およびそれらの仮想アプライアンスの同等品（「ソフトウェア」）になります。

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

Cisco Email Anti-Spam, Sophos Anti-Virus

Cisco Email Outbreak Filters

Cloudmark Anti-Spam

Cisco Image Analyzer

McAfee Anti-Virus

Cisco Intelligent Multi-Scan

Cisco Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

Cisco Web Reputation

Sophos Anti-Malware

Webroot Anti-Malware

McAfee Anti-Malware

Cisco Email Reporting

Cisco Email Message Tracking

Cisco Email Centralized Quarantine

Cisco Web Reporting

Cisco Web Policy and Configuration Management

Cisco Advanced Web Security Management with Splunk

Email Encryption for Encryption Appliances

Email Encryption for System Generated Bulk Email

Email Encryption and Public Key Encryption for Encryption Appliances

## Large Attachment Handling for Encryption Appliances

## Secure Mailbox License for Encryption Appliances

### 定義

For purposes of this SEULA, the following definitions apply:

"Company Service" means the Company's email, Internet, security management services provided to End Users for the purposes of conducting Company's internal business.

"End User" means: (1) for the Secure Web Appliance and SMA, the employee, contractor or other agent authorized by Company to access the Internet and the SMA via the Company Service; and (2) for the ESA, the email boxes of the employees, contractors, or other agent authorized by Company to access or use the email services via the Company Service.

"Ordering Document" means the purchase agreement, evaluation agreement, beta, pre-release agreement or similar agreement between the Company and Cisco or the Company and a Cisco reseller, or the valid terms of any purchase order accepted by Cisco in connection therewith, containing the purchase terms for the Software license granted by this Agreement.

"Personally Identifiable Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

"Server" means a single physical computer or devices on a network that manages or provides network resources for multiple users.

"Services" means Cisco Software Subscription Services.

"Service Description" means the description of the Software Subscription Support Services at <https://www.cisco.com/c/en/us/about/legal/service-descriptions.html>

"Telemetry Data" means samples of Company's email and web traffic, including data on email message and web request attributes and information on how different types of email messages and web requests were handled by Company's Cisco hardware products. Email message metadata and web requests included in Telemetry Data are anonymized and obfuscated to remove any Personally Identifiable Information.

"Term" means the length of the Software subscription You purchased, as indicated in your Ordering Document.

"Virtual Appliance" means the virtual version of Cisco's email security appliances, Secure Web Appliance, and security management appliances.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a Server.

### Additional License Terms and Conditions

#### LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

##### License of Software.

By using the Software and the Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, Cisco hereby grants to Company a nonexclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on Cisco's hardware products, or in the case of the Virtual Appliances, on a Virtual Machine, solely in connection with the provision of the Company Service to End Users. The number of End Users licensed for the use of the Software is limited to the number of End Users specified in the Ordering Documents.

In the event that the number of End Users in connection with the provision of the Company Service exceeds the number of End Users specified in the Ordering Documents, Company shall contact an Approved Source to purchase additional licenses for the Software. The duration and scope of this license(s) is further defined in the Ordering Document. The Ordering Document supersedes the EULA with respect to the term of the Software license. Except for the license rights granted herein, no right, title or interest in any Software is granted to the Company by Cisco, Cisco's resellers or their respective licensors. Your entitlement to Upgrades to the Software is subject to the Service Description. This Agreement and the Services are co-terminus.

**Consent and License to Use Data.**

Subject to the Cisco Privacy Statement at <https://www.cisco.com/c/en/us/about/legal/privacy.html>, Company hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Company. Cisco does not collect or use Personally Identifiable Information in the Telemetry Data. Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving your user experience and the Software and other Cisco security products and services. Company may terminate Cisco's right to collect Telemetry Data at any time by disabling SenderBase Network Participation in the Software. Instructions to enable or disable SenderBase Network Participation are available in the Software configuration guide.

**Description of Other Rights and Obligations**

Please refer to the Cisco Systems, Inc. End User License Agreement, Privacy Statement and Service Description of Software Subscription Support Services.



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。