CHAPTER 21

ログによるシステム アクティビティのモニタ

- ログ の概要（21-1 ページ）
- ログの共通タスク（21-2 ページ）
- ログのベスト プラクティス（21-2 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（21-2 ページ）
- ログ ファイルのタイプ（21-3 ページ）
- ログ サブスクリプションの追加と編集（21-8 ページ）
- 別のサーバへのログ ファイルのプッシュ（21-12 ページ）
- ログ ファイルのアーカイブ（21-13 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（21-14 ページ）
- ログ ファイルの表示（21-15 ページ）
- アクセス ログ ファイル内の Web プロキシ情報（21-15 ページ）
- アクセス ログのスキャン判定エントリの解釈（21-25 ページ）
- W3C 準拠のアクセス ログ ファイル（21-30 ページ）
- アクセス ログのカスタマイズ（21-32 ページ）
- トラフィック モニタのログ ファイル（21-36 ページ）
- ログ ファイルのフィールドとタグ（21-36 ページ）
- ロギングのトラブルシューティング（21-48 ページ）

ログ の概要

Web セキュリティ アプライアンスでは、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。多くのロギング タイプはデフォルトでイネーブルなりますが、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 ログ。**すべての L4 トラフィック モニタ 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

- ログの共通タスク（21-2 ページ）
- ログ ファイルのタイプ（21-3 ページ）

ログの共通タスク

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	ログによる Web プロキシのトラブルシューティング（21-2 ページ）
ログ サブスクリプションを追加および編集する	ログ サブスクリプションの追加と編集（21-8 ページ）
ログ ファイルを表示する	ログ ファイルの表示（21-15 ページ）
ログ ファイルを解釈する	アクセス ログのスキャン判定エントリの解釈（21-25 ページ）
ログ ファイルをカスタマイズする	アクセス ログのカスタマイズ（21-32 ページ）
別のサーバにログ ファイルをプッシュする	別のサーバへのログ ファイルのプッシュ（21-12 ページ）
ログ ファイルをアーカイブする	ログ ファイルのアーカイブ（21-13 ページ）

ログのベスト 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

Web セキュリティ アプライアンスでは、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。

手順 1　デフォルト プロキシ ログを読みます。

手順 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
AVC 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
設定ログ	メモリ マネージャ ログ
接続管理ログ	その他のプロキシ モジュール ログ
データ セキュリティ モジュール ログ	リクエスト デバッグ ログ
DCA エンジン フレームワーク ログ	SNMP モジュール ログ
ディスク マネージャ ログ	Sophos 統合フレームワーク ログ
FireAMP	WBRS フレームワーク ログ
FTP プロキシ ログ	WCCP モジュール ログ
HTTPS ログ	Webcat 統合フレームワーク ログ
ライセンス モジュール ログ	Webroot 統合フレームワーク ログ

手順 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。

手順 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。

手順 5　不要になったサブスクリプションを削除します。

関連項目

- ログ ファイルのタイプ（21-3 ページ）
- ログ サブスクリプションの追加と編集（21-8 ページ）

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、Web セキュリティ アプライアンスのログ 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。	×	×
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（高度なマルウェア防御）を記録します。 ログ ファイル（14-20 ページ）も参照してください。	○	○
監査ログ	認証、許可、アカウンティングのイベント（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。	○	○
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。	○	○
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。	×	○
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。	×	×
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。	○	○
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。	○	○
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。	×	×
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。	×	×
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。	×	×
DCA エンジン フレームワーク ログ（動的コンテンツ分析）	Web プロキシと Cisco Web Usage Controls 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。	×	×
DCA エンジン ログ（動的コンテンツ分析）	Cisco Web Usage Controls 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。	○	○

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	Web プロキシに関連するエラーを記録します。 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。	○	○
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。	×	×
外部認証ログ	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。 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。	×	○
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。	○	○
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。	×	×
FTP サーバ ログ	FTP を使用して、Web セキュリティ アプライアンス 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。	○	○
GUI ログ (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も記録されます。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などが記録されます。	○	○
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。	○	○
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)。	×	×
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。	○	○
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。	×	×
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。	×	×
ロギング ログ	ログ管理に関連するエラーを記録します。	○	○

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
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。	×	×
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。	○	○
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。	×	×
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。	×	×
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、Web セキュリティ アプライアンスと AnyConnect クライアント間の相互作用を記録します。	○	○
NTP ログ (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。	○	○
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。	○	○
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。	×	○
レポーティング ログ	レポート生成履歴を記録します。	○	○
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。	○	○
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。 **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。	×	×
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。	○	○
SHD ログ (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。	○	○
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。	○	○

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
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。	×	×
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。	×	×
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。	○	○
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。	○	○
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。	○	○
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。	○	○
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。	×	○
UDS ログ (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。Secure Mobility 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。	○	○
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。	○	○
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。 詳細については、W3C 準拠のアクセス ログ ファイル (21-30 ページ) を参照してください。	○	×
WBNP ログ (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。	×	○
WBRS フレームワーク ログ (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。	×	×
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。	×	×
Webcat 統合フレームワーク ログ	Web プロキシと Cisco Web Usage Controls 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。	×	×
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。	×	×

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
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。	○	○
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。	○	○

ログ サブスクリプションの追加と編集

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。

手順 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。

手順 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。

手順 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）	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。 **（注）**　[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。
ログ名（Log Name）	Web セキュリティ アプライアンス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。
ファイルサイズ別ロールオーバー（Rollover by File Size）	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。

オプション	説明
時刻によりロール オーバー（Rollover by Time）	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。 • [なし（None）]。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。 • [カスタム時間間隔（Custom Time Interval）]。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。 • [日次ロールオーバー（Daily Rollover）]。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。 • [週次ロールオーバー（Weekly Rollover）]。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。
ログ スタイル（Log Style） （アクセス ログのみ）	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。

カスタム フィールド（Custom Fields）
（アクセス ログのみ）
	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。
	[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）。

ファイル名（File Name）	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。

オプション	説明
ログ フィールド(Log Fields) (W3C アクセス ログのみ)	W3C アクセス ログに含めるフィールドを選択できます。 [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。 [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。
ログ圧縮(Log Compression)	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。
ログ除外(Log Exclusions)(任意) (アクセス ログのみ)	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。 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。
ログ レベル(Log Level)	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。 • [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。 • [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。 • [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。 • [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。 • [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。 (注)　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。

オプション	説明
取得方法（Retrieval Method）	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。
取得方法: アプライアンス上の FTP（FTP on Appliance）	[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フレーズを使用して、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。 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。 これは、デフォルトの取得方法です。
取得方法: リモート サーバでの FTP（FTP on Remote Server）	[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。 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。 • FTP サーバのホスト名 • ログ ファイルを保存する FTP サーバのディレクトリ • 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 （注）　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。
取得方法: リモート サーバでの SCP（SCP on Remote Server）	[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。 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。 • SCP サーバのホスト名 • ログ ファイルを保存する SCP サーバのディレクトリ • SCP サーバに接続する権限を持つユーザのユーザ名

オプション	説明
取得方法: Syslog 送信（Syslog Push）	テキスト ベースのログの syslog のみを選択できます。 [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。 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。 • Syslog サーバのホスト名 • 転送に使用するプロトコル（UDP または TCP） • 最大メッセージ サイズ（Maximum message size） UDP で有効な値は 1024 ～ 9216 です。 TCP で有効な値は 1024 ～ 65535 です。 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。 • ログで使用するファシリティ

手順 4　変更を送信し、保存します。

次の作業

- 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（21-12 ページ）を参照してください。

関連項目

- ログ ファイルのタイプ（21-3 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（21-14 ページ）

別のサーバへのログ ファイルのプッシュ

はじめる前に

- 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と編集（21-8 ページ）

手順 1　リモート システムにキーを追加します。

a. CLI にアクセスします。

b. `logconfig -> hostkeyconfig` コマンドを入力します。

c. 以下のコマンドを使用してキーを表示します。

コマンド（Command）	説明
ホスト	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。
ユーザ（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。

手順 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（Command）	説明
新規作成（New）	新しいキーを追加します。
フィンガープリント（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。

e. 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（Rollover by File Size）
- 時刻によりロールオーバー（Rollover by Time）
- ログ圧縮（Log Compression）
- 取得方法（Retrieval Method）

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。

手順 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。

手順 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。

手順 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。

関連項目

- ログ サブスクリプションの追加と編集（21-8 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（21-14 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

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
```

（注）　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

Web セキュリティ アプライアンス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（21-15 ページ）
- アクセス ログ ファイル内の Web プロキシ情報（21-15 ページ）
- W3C アクセス ログの解釈（21-30 ページ）
- トラフィック モニタ ログの解釈（21-36 ページ）
- ログ ファイルのフィールドとタグ（21-36 ページ）

ログ ファイルの表示

はじめる前に

- 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。

手順 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。

手順 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。

手順 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フレーズを入力します。

手順 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。

手順 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。

（注）　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。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報（21-15 ページ）
- W3C アクセス ログの解釈（21-30 ページ）
- トラフィック モニタ ログの解釈（21-36 ページ）

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-DataSecurityPolic
y-ExternalDLPPolicy-RoutingPolicy
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Un
known","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.p
df","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> -
```

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。 **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。 詳細については、W3C 準拠のアクセス ログ ファイル（21-30 ページ）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）。
%1r %2r	GET http://my.site.com/	要求の先頭行。 **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。 以下の文字が符号化された URL に使用されます。 & # % + , : ; = @ ^ { } [ ]
%A	-	認証されたユーザ名。 **注：**advancedproxyconfig > authentication CLI 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。
%H	DIRECT	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。 最も一般的な値は以下のとおりです。 • **NONE。**Web プロキシにコンテンツが含まれていたので、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。 • **DIRECT。**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。 • **DEFAULT_PARENT。**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。
%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。
%D	DEFAULT_CASE_11	ACL デシジョン タグ。 **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。 詳細については、ACL デシジョン タグ（21-19 ページ）を参照してください。

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 タグの一部）	PolicyGroupName	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、復号化ポリシー、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。 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。
N/A（ACL デシジョン タグの一部）	ID（Identity）	ID ポリシー グループの名前。 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。
N/A（ACL デシジョン タグの一部）	OutboundMalwareScanning Policy	Outbound Malware Scanning ポリシー グループの名前。 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。
N/A（ACL デシジョン タグの一部）	DataSecurityPolicy	Cisco データ セキュリティ ポリシー グループの名前。トランザクションがグローバルな Cisco データ セキュリティ ポリシーに一致する場合、この値は「DefaultGroup」になります。このポリシー グループ名は、Cisco データ セキュリティ フィルタが有効な場合にのみ表示されます。データ セキュリティ ポリシーに一致しなかった場合は、「NONE」と表示されます。 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。
N/A（ACL デシジョン タグの一部）	ExternalDLPPolicy	外部 DLP ポリシー グループの名前。トランザクションがグローバル外部 DLP ポリシーに一致する場合、この値は「DefaultGroup」になります。外部 DLP ポリシーに一致しなかった場合は、「NONE」と表示されます。 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。
N/A（ACL デシジョン タグの一部）	RoutingPolicy	ルーティング ポリシー グループ名は *ProxyGroupName/ProxyServerName*。 トランザクションがグローバル ルーティング ポリシーに一致する場合、この値は「DefaultRouting」になります。アップストリーム プロキシ サーバを使用しない場合、この値は「DIRECT」になります。 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。

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,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">	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。 山カッコ内の値の詳細については、アクセス ログのスキャン判定エントリの解釈（21-25 ページ）およびマルウェア スキャンの判定値（21-47 ページ）を参照してください。
%?BLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?% <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。
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。

(注)　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され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。
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	ファイルに対する AMP レピュテーション サーバからの判定を表す値です。 • 1:不明 • 2:正常 • 3:悪意がある • 4:スキャン不可

ACL デシジョン タグ	説明
ARCHIVESCAN_ALLCLEAR ARCHIVESCAN_BLOCKEDFILETYPE ARCHIVESCAN_NESTEDTOODEEP ARCHIVESCAN_UNKNOWNFMT ARCHIVESCAN_UNSCANABLE ARCHIVESCAN_FILETOOBIG	**アーカイブ スキャンの判定** 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。 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。 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。 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。 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。 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。 **アーカイブ スキャン判定の詳細** 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。 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（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。 アーカイブ検査の詳細については、アクセス ポリシー：オブジェクトのブロッキング（10-13 ページ）およびアーカイブ検査の設定（10-15 ページ）を参照してください。
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。

ACL デシジョン タグ	説明
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エージェント（Block Custom User Agents）] 設定で定義されたユーザ 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_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ました。これを防ぐために、SSL 接続が WSA 自体に向けられている場合、実際の WSA 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。
BLOCK_AMP_RESP	Web プロキシが、アクセス ポリシー グループの高度なマルウェア防御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、Outbound Malware Scanning ポリシー グループの Anti-Malware 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 Anti-Malware 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 Anti-Malware 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。

ACL デシジョン タグ	説明
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。
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。
DECRYPT_ADMIN	Web プロキシが、復号化ポリシー 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化しました。

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 プロキシががトランザクションを復号化しました。
DECRYPT_WEBCAT	Web プロキシが、復号化ポリシー 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化しました。
DECRYPT_WBRS	Web プロキシが、復号化ポリシー 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化しました。
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。
DROP_ADMIN	Web プロキシが、復号化ポリシー 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、復号化ポリシー 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、復号化ポリシー 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_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 グループの高度なマルウェア防御設定に基づいてサーバの応答をモニタしました。
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_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 エンジンは要求をブロックしませんでした。
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、ある認証レル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ル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、復号化ポリシー 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、復号化ポリシー 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、復号化ポリシー 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。

ACL デシジョン タグ	説明
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ル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。
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","fd5ef49d4213e05f448f11ed9c98253d
85829614fba368a421d14e64c426da5e",-,ARCHIVESCAN_BLOCKEDFILETYPE,"BlockedFileType:
application/x-rpm, BlockedFile: allfiles/linuxpackage.rp">
```

(注)　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（21-15 ページ）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。
2	ns	%XW	Web レピュテーション フィルタリング 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。 詳細については、マルウェア スキャンの判定値（21-47 ページ）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。

位置	フィールド値	フォーマット指定子	説明
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。 詳細については、マルウェア スキャンの判定値（21-47 ページ）を参照してください。
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。
14	-	%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。 詳細については、マルウェア スキャンの判定値（21-47 ページ）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。
16	"-"	“%Xy”	Sophos によって好ましくないコンテンツが検出されたファイルの名前。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。

位置	フィールド値	フォーマット指定子	説明
18	-	%Xl	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。 • **0.** 許可(Allow) • **1.** ブロック(Block) • **-(ハイフン)** 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 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。
19	-	%Xp	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、このフィールドで使用できる値を示します。 • **0.** 許可(Allow) • **1.** ブロック(Block) • **-(ハイフン)** 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)] > [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。
20	`IW_infr`	%XQ	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。 URL カテゴリの省略形の一覧については、URL カテゴリについて(9-30 ページ)を参照してください。
21	-	%XA	応答側のスキャン時に動的コンテンツ分析エンジンによって決定された URL カテゴリの判定(省略形)。Cisco Web Usage Controls 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)。 URL カテゴリの省略形の一覧については、URL カテゴリについて(9-30 ページ)を参照してください。
22	`"Trojan Phisher"`	“%XZ”	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。
23	`"-"`	“%Xk”	Web レピュテーション フィルタによって返された脅威タイプ。これは、ターゲット Web サイトのレピュテーションを低下させます。通常、このフィールドにはレピュテーションが -4 以下のサイトが入力されます。
24	`"Unknown"`	“%XO”	AVC 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 エンジンがイネーブルの場合にのみ適用されます。

位置	フィールド値	フォーマット指定子	説明
25	"Unknown"	“%Xu”	AVC 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 エンジンがイネーブルの場合にのみ適用されます。
26	"-"	“%Xb”	AVC 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 エンジンがイネーブルの場合にのみ適用されます。
27	"-"	“%XS”	安全なブラウジング スキャンの判定。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。 可能な値のリストについては、アダルト コンテンツ アクセスのロギング (9-23 ページ) を参照してください。
36	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）。
29	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。
30	[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。
31	"-"	“%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。
32	"-"	“%X4”	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。 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。
33	37	%X#1#	高度なマルウェア防御ファイル スキャンの判定: • 0:悪意のないファイル • 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 • 2:ファイル スキャンがタイムアウト • 3:スキャン エラー • 3 よりも大きい値:悪意のあるファイル
34	"W32.CiscoTestVector"	%X#2#	高度なマルウェア防御ファイル 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。

位置	フィールド値	フォーマット指定子	説明
35	33	%X#3#	高度なマルウェア防御ファイル 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。 詳細については、第 14 章「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「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。
36	0	%X#4#	アップロードおよび分析要求のインジケータ： 「0」は、高度なマルウェア防御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。 「1」は、高度なマルウェア防御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。
37	"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。
38	"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e	%X#6#	このファイルの SHA-256 ID。
39	-	%X#7#	次のファイルの AMP レピュテーション サーバの判定。 • 1：不明 • 2：正常 • 3：悪意がある • 4：スキャン不可
40	ARCHIVESCAN_BLOCKEDFILETYPE	%X#8#	アーカイブ スキャン判定。
41	"BlockedFileType: application/x-rpm, BlockedFile: allfiles/linuxpackage.rp"	%X#9#	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（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。

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（21-36 ページ）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（21-15 ページ）
- アクセス ログのカスタマイズ（21-32 ページ）
- W3C 準拠のアクセス ログ ファイル（21-30 ページ）
- ログ ファイルの表示（21-15 ページ）
- ログ ファイルのフィールドとタグ（21-36 ページ）

W3C 準拠のアクセス ログ ファイル

Web セキュリティ アプライアンスには、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（21-30 ページ）
- W3C アクセス ログの解釈（21-30 ページ）

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（21-30 ページ）
- W3C フィールドのプレフィックス（21-31 ページ）

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 Web セキュリティ アプライアンス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（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（System）	ログ ファイルを生成した Web セキュリティ アプライアンス（「Management_IP - Management_hostname」形式）。
[ソフトウェア（Software）]	これらのログを生成したソフトウェア
フィールド	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
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（21-15 ページ）
- アクセス ログのカスタマイズ（21-32 ページ）

- トラフィック モニタのログ ファイル（21-36 ページ）
- ログ ファイルのフィールドとタグ（21-36 ページ）
- ログ ファイルの表示（21-15 ページ）

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（21-36 ページ）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（21-32 ページ）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（21-33 ページ）。
- W3C アクセス ログのカスタマイズ（21-33 ページ）

標準アクセス ログのカスタマイズ

手順 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。

手順 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。

手順 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。例:

```
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)。

(注)　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。

手順 4　変更を送信し、保存します。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報(21-15 ページ)。
- ログ ファイルのフィールドとタグ(21-36 ページ)
- アクセス ログのユーザ定義フィールド(21-32 ページ)

W3C アクセス ログのカスタマイズ

手順 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。

手順 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。

手順 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。

(注)　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。

手順 4　変更を送信し、保存します。

関連項目

- W3C 準拠のアクセス ログ ファイル（21-30 ページ）
- ログ ファイルのフィールドとタグ（21-36 ページ）
- アクセス ログのユーザ定義フィールド（21-32 ページ）
- CTA 固有のカスタム W3C ログの設定（21-34 ページ）

CTA 固有のカスタム W3C ログの設定

WSA 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。

はじめる前に

- **SCP** を自動アップロード プロトコルとして選択して WSA の Cisco ScanCenter にデバイスのアカウントを作成します（詳細については、『*Cisco ScanCenter Administrator Guide*』の「プロキシ デバイスのアップロード」のセクションを参照してください）。SCP（セキュア コピー プロトコル）のホスト名と生成された WSA のユーザ名（大文字小文字を区別、デバイスごと異なる）をメモします。

手順 1　W3C アクセス ログのカスタマイズ（21-33 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追加し、[ログタイプ（Log Type）] として [W3C ログ（W3C Logs）] を選択します。

手順 2　[ログ名（Log Name）] は説明的な名前にします。

手順 3　[選択されたログフィールド（Selected Log Fields）] リストのエントリをすべて削除します（[すべて（All）] を選択し、[削除（Remove）] をクリックします）。

手順 4　[選択されたログフィールド（Selected Log Fields）] リストに以下のフィールドを追加します。

a.　以下をコピーして [カスタム フィールド（Custom Field）] ボックス内に貼り付け、[追加（Add）] をクリックします。

```
timestamp
x-elapsed-time
c-ip
cs-username
c-port
s-ip
s-port
cs-url
cs-bytes
sc-bytes
cs(User-Agent)
```

```
cs-mime-type
cs-method
sc-http-status
cs(Referer)
sc(Location)
x-amp-sha
x-amp-verdict
x-amp-malware-name
x-amp-score
```

手順 5　[ファイルサイズによりロールオーバー(Rollover by File Size)] を指定します。この場合、`500M` が推奨されます。

手順 6　[時刻によりロールオーバー(Rollover by Time)] オプションを選択します。

[以下の間隔でロールオーバー:(Rollover every)] を以下のガイドラインに基づく間隔に指定した、[カスタム時間間隔(Custom Time Interval)] を推奨します。

プロキシの背後のユーザ数	推奨ロールオーバー期間
不明または 2000 未満	55 分
2000 ～ 4000	30 分
4000 ～ 6000	20 分
6000 超	10 分

手順 7　[検索方法(Retrieval Method)] には、[リモート SCP サーバ(SCP on Remote Server)] を選択して CWS のアカウントからの CTA サーバ情報を入力します。

a. [SCP ホスト(SCP Host)] フィールドに、Cisco ScanCenter で指定した SCP ホスト(たとえば `etr.cloudsec.sco.cisco.com`)を入力します。

b. [SCP ポート(SCP Port)] フィールドに `22` と入力します。

c. [ディレクトリ(Directory)] フィールドに `/upload` と入力します。

d. [ユーザ名(Username)] フィールドに、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。

e. [ホストキーチェックを有効化(Enable Host Key Checking)] をオンにし、[自動スキャン(Automatically Scan)] を選択します。

手順 8　WSA で、[送信(Submit)] をクリックします。

公開 SSH キーが WSA によって生成され、管理コンソールに表示されます。

手順 9　WSA によって生成された公開 SSH キーをクリップボードにコピーします。

手順 10　Cisco ScanCenter ポータルに切り替え、適切なデバイス アカウントを選択し、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。(詳細については、『*Cisco ScanCenter Administrator Guide*』の「プロキシ デバイスの アップロード」のセクションを参照してください。

プロキシ デバイスと CTA システム間の認証が成功すると、ログ ファイルをプロキシ デバイスから CTA システムにアップロードし、分析できるようになります。

Cisco ScanCenter は、Cisco Cloud Web Security の管理ポータルです。
http://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。

手順 11　WSA に戻り、[変更を確定(Commit Changes)] をクリックします。

(注)　設定の変更を確定すると WSA は再起動します。したがって、接続されたユーザは一時的に切断される場合があります。

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 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（21-15 ページ）

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（21-37 ページ）
- トランザクション結果コード（21-18 ページ）
- ACL デシジョン タグ（21-19 ページ）
- マルウェア スキャンの判定値（21-47 ページ）

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（21-32 ページ）、および ログ サブスクリプションの追加と編集（21-8 ページ）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
%:<1	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した後、Web レピュテーション フィルタから応答を受信するまでの待機時間。
%:<s	x-p2p-asw-req-wait-time	Web プロキシが要求を送信した後、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までの待機時間。
%:>1	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	ヘッダーの受信後、応答本文全体を待機する時間
%:>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。
%:>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。
%: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-s2p-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）。

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>	x-p2p-mcafee-resp-wait-時刻	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-時刻	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-時刻	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-時刻	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。
%?BLOCK_SUSPECT_USER_AGENT,MONITOR_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と Web プロキシが判定した場合、そのユーザ エージェントがこのフィールドに記録されます。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。
%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。
%D	x-acltag	ACL デシジョン タグ。

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
%e	x-elapsed-time	ミリ秒単位の経過時間。 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。 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
%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。 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	応答コードをキャッシュしません(DCF フラグ)。 応答コードの説明: • クライアント要求に基づく応答コード: – 1 = 要求に「no-cache」ヘッダーがあった。 – 2 = 要求に対してキャッシングが許可されていない。 – 4 = 要求に「Variant」ヘッダーがない。 – 8 = ユーザ要求にユーザ名またはパスフレーズが必要。 – 20 = 指定された HTTP メソッドへの応答。 • アプライアンスで受信された応答に基づく応答コード: – 40 = 応答に「Cache-Control: private」ヘッダーが含まれている。 – 80 = 応答に「Cache-Control: no-store」ヘッダーが含まれている。 – 100 = 応答は、要求がクエリーだったことを示している。 – 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)。 – 400 = 応答に「Last Modified」ヘッダーがない。 – 1000 = 応答がただちに期限切れになる。 – 2000 = 応答ファイルが大きすぎてキャッシュできない。 – 20000 = ファイルの新しいコピーがある。 – 40000 = 応答の「Vary」ヘッダーに不正/無効な値がある。 – 80000 = 応答には Cookie の設定が必要。 – 100000 = キャッシュ不可の HTTP ステータス コード。 – 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)。 – 800000 = 応答トレーラがキャッシュなしを示している。 – 1000000 = 応答のリライトが必要。

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
%k	s-ip	データ ソースの IP アドレス(サーバの IP アドレス) 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: 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。 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。
%m	cs-auth-mechanism	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。 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。 • **BASIC。**ユーザ名が基本認証方式を使用して認証されました。 • **NTLMSSP。**ユーザ名が NTLMSSP 認証方式を使用して認証されました。 • **Kerberos。**ユーザ名は Kerberos 認証方式を使用して認証されました。 • **SSO_TUI。**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。 • **SSO_ISE。**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)。 • **SSO_ASA。**ユーザがリモート ユーザで、ユーザ名は Secure Mobility を使用して Cisco ASA から取得されました。 • **FORM_AUTH。**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。 • **GUEST。**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。
%M	CMF	キャッシュ ミス フラグ(CMF 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
%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。
%P	cs-version	Protocol.
%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	UNIX エポックのタイムスタンプ **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、timestamp 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。
%u	cs(User-Agent)	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。 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。
%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。
%X0	x-resp-dvs-scanverdict	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。 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。
%X1	x-resp-dvs-threat-name	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。 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。

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
%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	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。 • **1.** トランザクションがブロックされました。 • **0.** トランザクションはブロックされませんでした。 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。
%XA	x-webcat-resp-code-abbr	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 Usage Controls URL フィルタリング エンジンにのみ適用されます。
%Xb	x-avc-behavior	AVC 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。

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-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。
%XL	x-webcat-resp-code-full	応答側のスキャン時に決定された URL カテゴリの判定（完全名）。Cisco Web Usage Controls 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	x-avc-app	AVC エンジンによって識別される Web アプリケーション。
%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。 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。
%Xu	x-avc-type	AVC エンジンによって識別される Web アプリケーションのタイプ。
%Xv	x-webroot-scanverdict	Webroot からのマルウェア スキャンの判定。

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
%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	復号化された 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 によって好ましくないコンテンツが検出されたファイルの名前。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	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。 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。
%X#1#	x-amp-verdict	高度なマルウェア防御ファイル スキャンの判定: • 0:悪意のないファイル。 • 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。 • 2:ファイル スキャンがタイムアウト。 • 3:スキャン エラー。 • 3 よりも大きい値:悪意のあるファイル。
%X#2#	x-amp-malware-name	高度なマルウェア防御ファイル 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	高度なマルウェア防御ファイル 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。 詳細については、第 14 章「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「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。

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#4#	x-amp-upload	アップロードおよび分析要求のインジケータ： 「0」は、高度なマルウェア防御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。 「1」は、高度なマルウェア防御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。
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。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報（21-15 ページ）
- W3C アクセス ログの解釈（21-30 ページ）

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 エンジンは、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	Timeout
3	エラー（Error）
4	スキャン不可

マルウェア スキャンの判定値	マルウェア カテゴリ
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（21-15 ページ）
- W3C アクセス ログの解釈（21-30 ページ）

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（A-16 ページ）
- HTTPS トランザクションのロギング（A-16 ページ）
- 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）（A-16 ページ）
- 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（A-17 ページ）