セキュリティ プロファイル（Security Profiles）

セキュリティプロファイルは、通常、セキュリティポリシーを適用するためにネットワークトラフィックに適用されるルールのセットと設定を指します。これらのプロファイルには、次の保護対策が含まれています。

- ファイアウォール ルール
- 侵入防御システム（IPS）
- ウイルス対策/マルウェア対策
- Web フィルタリング
- データ漏洩防止（DLP）
- アプリケーション制御

これらの特定のプロファイルは、通常、ポリシールール、ポリシールールセット、またはポリシールールセットグループに追加され、優先度に従って順序付けされます。

復号プロファイル

復号プロファイルは、リバースプロキシまたは転送プロキシのシナリオで Multicloud Defense Gateway によって使用されます。接続がプロキシされると、フロントエンドセッションがゲー

トウェイで終了し、サーバーへの新しいバックエンドセッションが確立されます。この終了は、トラフィックを復号して検査し、悪意のあるアクティビティから保護することを目的としています。暗号化されたトラフィックを復号するには、復号プロファイルが必要です。

復号プロファイルの TLS バージョン

Multicloud Defense Gateway は、すべての TLS バージョン（TLS 1.3、TLS 1.2、TLS 1.1、TLS 1.0）をサポートします。ユーザーは使用する最小TLSバージョンを指定できます。Multicloud Defense Gateway は、指定された最小 TLS バージョン以降の TLS バージョンをネゴシエートします。ゲートウェイは、TLS ネゴシエーション中に、可能な限り最大の TLS バージョンと最も強力な暗号スイートを常に使用します。Multicloud Defense Gateway が指定された最小 TLS バージョンを満たすバージョンをネゴシエートできない場合、ゲートウェイはセッションをドロップし、`TLS_ERROR` イベントをログに記録します。

（注） 1 つのゲートウェイに適用できる最小 TLS バージョンは 1 つだけです。ポリシールールセットまたはポリシー ルールセット グループ内で使用されるすべてのサービスオブジェクトが参照するすべての復号プロファイル全体で、一貫した最小 TLS バージョンを使用する必要があります。異なる最小 TLS バージョンが指定されている場合、適用される最小 TLS バージョンを事前に決定することはできません。

暗号スイート

Multicloud Defense Gateway は、デフォルトの暗号スイートおよびユーザーが選択可能な暗号スイートのセットをサポートします。デフォルトのセットはPFS暗号スイートであり、これは常に選択されます。ユーザーが選択可能なセットは Diffie-Hellman および PKCS（RSA）暗号スイートであり、これはユーザーが選択できます。暗号スイートの組み合わせセット（デフォルトおよびユーザー選択）は、セキュアなフロントエンド暗号化セッションを確立するために、ゲートウェイによって使用されます。クライアントは、優先暗号スイートの順序付きリストを送信します。ゲートウェイは、クライアントによって送信された順序付きセットとゲートウェイで使用可能なセットから選択された暗号スイートで応答します。クライアントが順序付けの定義をサーバーに許可する場合、選択される暗号スイートは、ゲートウェイで使用可能な順序付きセットと、クライアントによって送信されたセットから選択されます。

次に、ゲートウェイでサポートされ、復号プロファイルで使用可能な暗号スイートの順序付きリストを示します。

カテゴリ	暗号スイート	Key Exchange	暗号化方式	Hash	デフォルト
PFS	ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA	AES256-GCM	SHA384	□
PFS	ECDHE-RSA-AES256-CBC-SHA384	ECDHE-RSA	AES256-CBC	SHA384	□
Diffie-Hellman	DH-RSA-AES256-GCM-SHA384	DH-RSA	AES256-GCM	SHA384	
PFS	DHE-RSA-AES256-GCM-SHA384	DHE-RSA	AES256-GCM	SHA384	□

カテゴリ	暗号スイート	Key Exchange	暗号化方式	Hash	デフォルト
PFS	DHE-RSA-AES256-CBC-SHA256	DHE-RSA	AES256-CBC	SHA384	□
PFS	DHE-RSA-AES256-CBC-SHA	DHE-RSA	AES256-CBC	[SHA]	□
Diffie-Hellman	DH-RSA-AES256-SHA256	DH-RSA	AES256-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES256-SHA	DH-RSA	AES256-CBC	SHA160	
PKCS（RSA）	AES256-GCM-SHA384	PKCS-RSA	AES256-GCM	SHA384	
PKCS（RSA）	AES256-SHA256	PKCS-RSA	AES256-CBC	SHA256	
PKCS（RSA）	AES256-SHA	PKCS-RSA	AES256-CBC	SHA160	
PFS	ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA	AES128-GCM	SHA256	□
PFS	ECDHE-RSA-AES128-CBC-SHA256	ECDHE-RSA	AES128-CBC	SHA256	□
Diffie-Hellman	DH-RSA-AES128-GCM-SHA256	DH-RSA	AES128-GCM	SHA256	
PFS	DHE-RSA-AES128-GCM-SHA256	DHE-RSA	AES128-GCM	SHA256	□
PFS	DHE-RSA-AES128-CBC-SHA256	DHE-RSA	AES128-CBC	SHA256	□
Diffie-Hellman	DH-RSA-AES128-SHA256	DH-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-SHA	DH-RSA	AES128-CBC	SHA160	
PKCS（RSA）	AES128-GCM-SHA256	PKCS-RSA	AES128-GCM	SHA256	
PKCS（RSA）	AES128-SHA256	PKCS-RSA	AES128-CBC	SHA256	
PKCS（RSA）	AES128-SHA	PKCS-RSA	AES128-CBC	SHA160	
PFS	ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA	DES-CBC3	[SHA]	□
PFS	ECDHE-RSA-RC4-SHA	ECDHE-RSA	RC4	[SHA]	□
PKCS（RSA）	RC4-SHA	PKCS-RSA	RC4	SHA160	
PKCS（RSA）	RC4-MD5	PKCS-RSA	RC4	SHA160	

復号プロファイルの作成

復号プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [復号（Decryption）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）] と [説明（Description）] を入力します。

ステップ 4 [証明書方式（Certificate Method）] で、[既存のものを選択（Select Existing）] を選択します。

ステップ 5 [証明書（Certificate）] では、希望する証明書を選択します。

ステップ 6 [最小TLSバージョン（Min TLS Version）] で、復号プロファイルで受け入れられる TLS の最低バージョンを選択します。デフォルトは TLS 1.0 です。

ステップ 7 デフォルト以外（非 PFS）の暗号スイートを使用する場合は、Diffie-Hellman または PKCS（RSA）メニューから目的の暗号スイートのセットを選択します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

ネットワーク侵入（IDS/IPS）プロファイル

ネットワーク侵入プロファイルは、トラフィックが悪意のあるものではないことを確認するためにトランザクションを評価する際に使用できる、侵入検知および保護（IDS/IPS）ルールのコレクションです。

侵入検知システム（IDS）は、ネットワークイベントを監視し、それらを分析してセキュリティインシデントや差し迫った脅威、特に悪意のあるトランザクションなどの不審または異常なアクティビティを検出し、観察されたら即時にアラートを送信するソリューションとして定義されます。IDS は、ホストとネットワークを検索します。

侵入防御システム（IPS）は、ネットワークトラフィックをアクティブに分析し、既知の攻撃パターンおよびシグニチャと比較します。システムが不審なトラフィックを検出すると、そのトラフィックがネットワークに侵入しないようブロックします。IPS ルールは、ネットワークベースの IP とホストベースの IP の両方をカバーします。

Multicloud Defense は、これら両方のシステムを単一のプロファイル内で組み合わせて、簡単に設定できるネットワーク侵入プロファイルを作成します。これは、侵害を受けたシステムからの悪意のあるプローブまたは新しいネットワークパターンを検出し、不審なトラフィックを検出、拒否、および報告します。プリエンプティブなブロッキングとレポートにより、ネット

ワークのダウンタイムを軽減し、将来のブロッキングアクティビティをさらに改善できます。Multicloud Defense 内のネットワーク侵入プロファイルは、次のルールセットでコンパイルされています。

表 *1 : Multicloud Defense* は次の *IDS/IPS* ルールセットをサポートします。

ルールセット	説明
Talos ルール	Talos ルールは、実際の調査、侵入テスト、および調査から収集されたインテリジェンスに基づく Cisco のプレミアムルールセットであり、アプリケーションとフレームワークに対して高度なレベルの保護を提供します。

IDS/IPS プロファイルには、悪意のある可能性のある Web アプリケーションは含まれないことに注意してください。詳細については、Web アプリケーション ファイアウォール（WAF）プロファイル （9 ページ）を参照してください。

IPS/IDS プロファイルの作成

IPS/IDS プロファイルを作成してルールセットに追加するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [IPS/IDS]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [全般設定（General Settings）] タブをクリックします。

ステップ 4 [プロファイル名（Profile Name）] に一意のプロファイル名を入力します。

ステップ 5 （任意）[説明（Description）] に説明を入力します。これは、似た名前の他のプロファイルを区別するのに役立ちます。

ステップ 6 IDS/IPS プロファイルが悪意のあるアクティビティを検出した場合は、脅威 PCAP オプションファイルに切り替えます。このオプションを**オン**に切り替える場合は、PCAP プロファイルをゲートウェイにアタッチする必要があります。

ステップ 7 全般設定の [ルールセット（Rule Set）] セクションで、ルールライブラリ（Talos、カスタム）の少なくとも 1 つのルールセットを、IDS/IPS プロファイルで指定する必要があることに注意してください。Talos ルールとカスタムルールセットを使用する場合は、2 つのうち少なくとも 1 つを有効にする必要があります。IDS/IPS プロファイル全体を無効化する場合は、IDS/IPS プロファイルが評価されないように、ポリシールールセットから IDS/IPS プロファイルを削除します。ドロップダウンメニューを使用して、次の設定のいずれかを選択します。これは、このプロファイル内のすべてのルールセットに適用されます。

- [無効（Disabled）] : Talos ルールの使用を無効化するかどうかを指定します。
- [手動（Manual）] : Talos ルールのバージョンを指定します。
- [自動（Automatic）] : Talos ルールの最新バージョンへの自動更新を何日遅延させるかを、公開日からの日数で指定します。

他のドロップダウンメニューを使用して、このプロファイル内のルールをいつ更新するかを選択します。ルールセットの更新は、Talos が更新を送信した**直後**、または更新後の任意の日数とすることができます。

ステップ 8 [Talosルール：ポリシー（Talos Rules: Policy）] をクリックし、ベースとして使用するポリシープロファイルをテーブルから選択します。選択できるプロファイルは 1 つだけです。

ウィンドウ表示が最大化されていない場合は、ウィンドウの右側にスクロールして、選択したプロファイルに**アクション**を割り当てます。

- [ルールのデフォルト（Rule Default）]：トリガーされた各ルールで指定されているアクションに基づいて要求を許可または拒否し、イベントをログに記録します。
- [許可/ログ（Allow Log）]：要求を許可し、イベントをログに記録します。
- [許可/ログなし（Allow No Log）]：要求を許可し、イベントをログに記録しません。
- [拒否/ログ（Deny Log）]：要求を拒否し、イベントをログに記録します。
- [拒否/ログなし（Deny No Log）]：要求を拒否し、イベントをログに記録しません。

ステップ 9 [Talosルール：カテゴリ（Talos Rules: Category）] タブをクリックし、テーブルの少なくとも 1 つのカテゴリをプロファイルに選択します。

ステップ 10 [Talosルール：クラス（Talos Rules: Class）] タブをクリックし、テーブルの少なくとも 1 つのクラスをプロファイルに選択します。

ステップ 11 画面の上部にある [詳細設定（Advanced Settings）] タブをクリックします。

ステップ 12 [ルールの抑制（Rule Suppression）] で [追加（Add）] をクリックし、IP アドレスの有効な [送信元IP/ CIDR リスト（Source IP/CIDR List）] および対応する [ルールIDリスト（Rule ID List）] を入力します。リストの行を削除するには、行の右側にあるマイナスアイコンをクリックします。

ステップ 13 [イベントフィルタリング：ロファイルイベントのフィルタリング（Event Filtering: Profile Event Filtering）] で、次の情報を入力します。

- [タイプ（Type）]：[レート（Rate）] または [サンプル（Sample）] を選択できます。生成されたイベントは、[時間（Time）]評価間隔（秒単位）でトリガーされた指定の [イベント数（Number of Events）] に基づいてレート制限またはサンプル制限されます。
- [イベント数（Number of Events）]：許容されるイベント数の値を手動で入力します。
- （[レート（Rate）] タイプで使用可能）[時間（秒単位）（Time (Seconds)）]：数値を秒単位で入力します。

ステップ 14 [イベントフィルタリング：ルールイベントフィルタリング（Event Filtering: Rule Event Filtering）] で、[追加（Add）] をクリックします。次の情報を入力します。

- [ルールIDリスト（Rule ID List）]：ルール ID のカンマ区切りリストを指定します。
- [イベント数（Number of Events）]：許容されるイベント数の値を手動で入力します。
- （[レート（Rate）] タイプで使用可能）[時間（秒単位）（Time (Sec)）]：数値を秒単位で入力します。

- [タイプ（Type）]：[レート（Rate）]または[サンプル（Sample）]を選択します。生成されたイベントは、[時間（Time）]評価間隔（秒単位）でトリガーされた指定の[イベント数（Number of Events）]に基づいてレート制限またはサンプル制限されます。

ステップ 15 詳細設定の[ルール設定リスト（Rule Setting List）]セクションで、[追加（Add）]をクリックし、次の情報を入力します。

- [送信元IP/CIDRリスト（Source IP/ CIDR List）]：IP または CIDR のカンマ区切りリストを指定します。
- [ルールIDリスト（Rule ID List）]：ルール ID のカンマ区切りリストを指定します。多数のルールがある場合、ルール ID のみが必要であることに注意してください。少数のルールの場合、GID と ID を「GID:ID」としてルール ID に指定する必要があります。例：119:3。
- [アクション（Action）]：送信元 IP/ CIDR リストまたはルール ID リストがトリガーされた場合のアクションを選択します。ルールが抑制されている場合、アクションは実行されず、ログが送信またはキャプチャされることもないことに注意してください。
  - [許可/ログ（Allow Log）]：要求を許可し、イベントをログに記録します。
  - [許可/ログなし（Allow No Log）]：要求を許可し、イベントをログに記録しません。
  - [拒否/ログ（Deny Log）]：要求を拒否し、イベントをログに記録します。
  - [拒否/ログなし（Deny No Log）]：要求を拒否し、イベントをログに記録しません。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

データ損失防止（DLP）プロファイル

DLP（データ損失防止）プロファイルを使用すると、Multicloud Defense のお客様は、Multicloud Defense ソリューションが転送プロキシ（出力）モードで展開されている場合に、データ内のデータ漏えいパターンを探し、検出したらアクションを実行するためのポリシールールを指定できます。

Multicloud Defense では、カスタム PCRE ベースの正規表現パターンに加えて、ソーシャルセキュリティ番号（SSN）、AWS シークレット、クレジットカード番号などの事前にパッケージ化された一般的なデータパターンを指定できます。これにより、PCI、PII、および PHI データの保護を簡単に適用して、コンプライアンス要件を満たすことができます。この機能は、個別の DLP サービスを必要としない既存の Multicloud Defense 機能セットと統合されています。

データ損失防止プロファイルの作成

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [ネットワークの脅威（Network Threats）]**に移動します。

ステップ 2 [侵入プロファイルの作成（Create Intrusion Profile）] をクリックします。

ステップ 3 [データ損失防止（Data Loss Prevention）] をクリックします。

ステップ 4 [名前（Name）] にプロファイルの一意の名前を入力し、説明を入力します。

ステップ 5 テーブルの [DLPフィルタリスト（DLP FIlter List）] に入力します。

ステップ 6 必要に応じて、[追加（Add）] をクリックしてさらに行を挿入します。

ステップ 7 フィルタ処理の [説明（Description）] を入力します。

ステップ 8 ドロップダウンリストから定義済みの静的パターン（CVE 番号など）を選択するか、カスタム正規表現を指定します。

ステップ 9 トラフィックでパターンが表示される必要がある回数を、**数**を指定して定義します。

ステップ 10 パターンが回数に一致した場合に実行する**アクション**を選択します。

（注）
AWS アクセスキーと AWS 秘密キーの事前定義されたパターンは、パターンの制限が厳しいため、DLP インスペクションで一致しない場合があります。AWS アクセスキーと AWS 秘密キーを検出するには、DLP プロファイルで次の緩和されたカスタムパターンを使用します。これにより、誤検出のログイベントが生成される可能性があることに注意してください。

```
AWS アクセスキー：(?<![A-Z0-9])[A-Z0-9]{20}(?![A-Z0-9])

AWS 秘密キー：(?<![AZa-z0-9/+=])[A-Za-z0-9/+=]{40}(?![A-Za-z0-9/+=])
```

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

マルウェア対策プロファイル

マルウェア対策プロファイルは、すべての着信データをスキャンして、マルウェアのインストールやコンピュータへの感染を防ぐことで、マルウェア攻撃を防ぎます。マルウェア対策プログラムは、高度な形式のマルウェアを検出し、ランサムウェア攻撃から保護することもできます。現在、プロファイルの大部分は Talos ClamAV ウイルス検出エンジンです。ClamAV® は、トロイの木馬、ウイルス、マルウェア、およびその他の悪意のある脅威を検出するためのウイルス対策エンジンです。

マルウェア対策プロファイルを作成する場合は、ルールに設定することで、プロファイルをすぐにポリシーに追加することを**強く**お勧めします。

マルウェア対策プロファイルの作成

手順

ステップ 1 **[管理（Manage）]**>**[プロファイル（Profiles）]**>**[ネットワークの脅威（Network Threats）]**に移動します。

ステップ 2 [マルウェア対策（Anti-malware）] を選択します。

ステップ 3 [名前（Name）] に一意の名前を入力し、説明を入力します。

ステップ 4 Talos ルールセットに次のいずれかのモードを選択します。

- [手動モード（Manual Mode）]：ドロップダウンから Talos ルールセットバージョンを選択します。選択したルールセットバージョンは、このプロファイルを使用するすべてのゲートウェイの Multicloud Defense データパスエンジンによって使用されます。新しいルールセットバージョンに自動的に更新されることはありません。
- [自動モード（Automatic Mode）]： Multicloud Defense によってルールセットバージョンが公開された後で、展開を何日遅延させるかを選択します。新しいルールセットは Multicloud Defense によって毎日公開され、このプロファイルを使用するゲートウェイは、**N** 日以上前の最新のルールセットバージョンに自動的に更新されます。ここで **N** はドロップダウンから選択された「遅延日数」の引数です。たとえば、2024 年 1 月 10 日に展開を 5 日間遅延させることを選択した場合、 Multicloud Defense Controller は 1 月 5 日以前に公開されたルールセットバージョンを選択します。そのルールセットバージョンを使用した社内テストが何らかの理由で失敗した場合、Multicloud Defense は数日間公開を行わない場合があることにご注意ください。

ステップ 5 ウイルス署名の一致が見つかった場合に実行する **アクション** を選択します。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

Web アプリケーション ファイアウォール（WAF）プロファイル

Web 保護プロファイルは、既知の Web アプリケーション攻撃を検出してブロックできる Web アプリケーション ファイアウォール（WAF）ルールの集合です。署名と制約を使用して Web トラフィックを調べるように WAF プロファイルを設定できます。また、指定したパターンに一致する HTTP メソッドを制御する HTTP メソッドポリシーを適用することもできます。通

常、クロスサイトフォージェリ、クロスサイト スクリプティング（XSS）、ファイルインクルージョン、SQL インジェクションなどの攻撃から Web アプリケーションを保護します。

表 *2:* サポートされる *WAF* ルールセット

ルール セット	説明
コアルール	コアルールは、ModSecurity CRS（コアルールセット）の標準のルールセットであり、任意の Web アプリケーションに対して基本レベルの保護を提供します。
Trustwave ルール	Trustwave ルールは、実際の調査、侵入テスト、および調査から収集されたインテリジェンスに基づく ModSecurity のプレミアムルールセットであり、特定の Web アプリケーションとフレームワークに対して高度なレベルの保護を提供します。
シスコの規則	カスタムルールは、顧客が作成した特定のルールセットであり、カスタム Web アプリケーションに特別なレベルの保護を提供します。

WAF プロファイルには悪意のある IP が含まれないことに注意してください。詳細については、「悪意のある IP プロファイル （22 ページ）」と「ネットワーク侵入（IDS/IPS）プロファイル （4 ページ）」を参照してください。

WAF プロファイルの作成

WAF プロファイルを作成するには、次の手順を実行します。

（注） コアルールセットが指定されている場合、コアルールを無効にすることはできません。コアルールを無効化するには、WAF プロファイルからすべてのコアルールセットを削除して、評価されないようにします。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [WAF]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 次の一般設定を指定します。

a) [プロファイル名（Profile Name）] に一意のプロファイル名を入力します。

b) （任意）[説明（Description）] に説明を入力します。これは、似た名前のプロファイルを区別するのに役立ちます。

c) アクションを指定します。

- [ルールのデフォルト（Rule Default）]：トリガーされた各ルールで指定されているアクションに基づいて要求を許可または拒否し、イベントをログに記録します。
- [許可/ログ（Allow Log）]：要求を許可し、イベントをログに記録します。
- [拒否/ログ（Deny Log）]：要求を拒否し、イベントをログに記録します。

d) WAFプロファイルが悪意のあるアクティビティを検出した場合に、脅威HARファイルを生成するかどうかを指定します。これを動作させるには、ゲートウェイにPcapプロファイルがアタッチされている必要があります。

e) WAFプロファイルが悪意のあるアクティビティを検出した場合に、HTTP要求HARファイルを生成するかどうかを指定します。

f) [ルールセット（RULE SETS）]セクションの左側にある垂直タブで、[コアルール（Core Rules）]をクリックします。ルールライブラリ（コア、Trustwave、カスタム）から少なくとも1つのルールセットを指定する必要があります。

- 次を指定します。
  - [手動（Manual）]：使用するコアルールのバージョンを指定します。
  - [自動（Automatic）]：コアルールの最新バージョンへの自動更新を何日遅延させるかを、公開日からの日数で指定します。
- プロファイルに追加するルールを特定し、[プロファイルに追加（Add to Profile）]をクリックします。右側のテーブルに選択内容が表示されます。

g) 左側にある垂直タブで、[Trustwaveルール（Trustwave Rules）]をクリックします。

- 次を指定します。
  - [無効（Disabled）]：Trustwaveルールの使用を無効化するかどうかを指定します。
  - [手動（Manual）]：使用するTrustwaveルールのバージョンを指定します。
  - [自動（Automatic）]：Trustwaveルールの最新バージョンへの自動更新を何日遅延させるかを、公開日からの日数で指定します。
- プロファイルに追加するルールを特定し、[プロファイルに追加（Add to Profile）]をクリックします。選択内容は、右側の[プロファイルの選択（Profile Selections）]テーブルに表示されます。

h) 左側にある垂直タブで、[カスタムルール（Custom Rules）]をクリックします。

- 次のいずれかのオプションを指定します。
  - [無効（Disabled）]：カスタムルールの使用を無効化するかどうかを指定します。
  - [手動（Manual）]：使用するカスタムルールのバージョンを指定します。
  - [自動（Automatic）]：カスタムルールの最新バージョンへの自動更新を何日遅延させるかを、公開日からの日数で指定します。

- プロファイルに追加するルールを特定し、[プロファイルに追加（Add to Profile）] をクリックします。選択内容は、右側の [プロファイルの選択（Profile Selections）] テーブルに表示されます。

ステップ 4 ウィンドウの上部までスクロールし、[詳細設定（Advanced Settings）] タブをクリックします。

a) [ルールの抑制（Rule Suppression）] で、[追加（Add）] をクリックしてルールに 1 つ以上の行を追加します。ルールの抑制は、特定の IP または CIDR のリストに対して行えます。

- [送信元IP/CIDRリスト（Source IP/ CIDR List）] には、IP または CIDR のカンマ区切りリストを指定します。
- [ルールIDリスト（Rule ID List）] には、ルール ID のカンマ区切りリストを指定します。

b) [イベントフィルタリング（Event Filtering）] で、次の情報を入力します。

- [タイプ（Type）] : [レート（Rate）] または [サンプル（Sample）]
- **イベント数**
- [時間(秒)（Time (Seconds)）]

c) [ルールイベントフィルタリング（Rule Event Filtering）] で、[追加（Add）] をクリックしてルールに 1 つ以上の行を追加します。新しい行を作成するごとに、有効な [ルールIDリスト（Rule ID List）]、[イベント数（Number of Events）]、[時間（秒）（Time (Sec)）]を入力し、[タイプ（Type）] として [タイプ（Type）] または [サンプル（Sample）] を選択します。

d) [コアルールセット（Core Rule Set）] で、[要求異常（Request Anomaly）] と [応答異常（Response Anomaly）] の両方に対して値を選択します。[要求異常（Request Anomaly）] に 3 未満の値を使用すると、大量のアラートが生成されることに注意してください。

e) [パラノイアレベル（Paranoia Level）] を選択します。オプションの範囲は 1 ～ 4 です。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

イベントのフィルタリング

WAF プロファイルがトリガーされたときに生成されるセキュリティイベントの数を減らすために、[詳細設定（Advanced Settings）] の [イベントフィルタリング（Event Filtering）] を設定して、イベントのレート制限またはサンプリングを行うことができます。この設定により、検出や保護の動作が変わることはありません。

[タイプ（Type）] を [レート（Rate）] に指定すると、生成されるイベントは、[時間（Time）] 評価間隔（秒単位）でトリガーされた指定のイベント数に基づいてレート制限されます。たとえば、[イベント数（Number of Events）] が 50 に指定され、[時間（Time）] が 5 秒に指定されている場合、1 秒あたり 10 個イベントのみが生成されます。

[タイプ（Type）] を [サンプル（Sample）] に指定すると、生成されるイベントは、指定のイベント数に基づいてサンプリングされます。たとえば、[イベント数（Number of Events）] が 10 に指定されている場合、イベントが10個トリガーされるごとに1つのイベントのみが生成されます。

プロファイルイベントのフィルタリング

プロファイルイベントのフィルタリングは、WAFプロファイルで設定されているすべてのルールに適用されます。

- [タイプ（Type）] を [レート（Rate）] または [サンプル（Sample）] に指定します。
  - [レート（Rate）] : [イベント数（Number of Events）] と [時間（Time）] 評価間隔（秒単位）を指定します。
  - [サンプル（Sample）] : [イベント数（Number of Events）] を指定します。

ルール イベント フィルタリング

WAF プロファイルがトリガーされたときに生成されるセキュリティイベントの数を減らすために、イベントフィルタリングを設定して、イベントのレート制限またはサンプリングを行うことができます。この設定により、検出や保護の動作が変わることはありません。

ルール イベント フィルタリングは、WAF プロファイルで設定されている特定のルールに適用されます。

手順

ステップ 1 [ルールイベントフィルタリング（Rule Event Filtering）] で [追加（Add）] をクリックします。

ステップ 2 [ルールIDリスト（Rule ID List）] には、ルール ID のカンマ区切りリストを指定します。

ステップ 3 [タイプ（Type）] を [レート（Rate）] または [サンプル（Sample）] に指定します。

- [レート（Rate）] : [イベント数（Number of Events）] と [時間（Time）] 評価間隔（秒単位）を指定します。
- [サンプル（Sample）] : [イベント数（Number of Events）] を指定します。

次のタスク

WAF プロファイルとポリシールールの関連付け

L7 DoS プロファイルの作成

Multicloud Defense Gateway には、バックエンド Web サーバーへのクライアント要求を継続的にモニタリングすることで、アプリケーションレイヤへの攻撃をモニター、検出、および修復する機能があります。レイヤ 7 DoS 攻撃は、 Web サーバーのリソースを枯渇させることを目

的としており、多数のHTTP要求を送信することでサービスの可用性に影響を与えます。この機能は、Webベースのアプリケーションの可用性を維持するために、ゲートウェイを有効にしてバックエンド Web サービスへのインバウンド接続にプロキシを使用する場合に有効になります。また、この機能を有効にすると、フロントエンド ロード バランサがアプリケーション DoS 攻撃の検出と修復をサポートしていない、またはそれに最適化されていない場合に、ゲートウェイが追加のセキュリティを提供できます。

この機能は、API サービスをホストしているバックエンド Web サーバーを DoS から保護するためにも使用できます。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）]**に移動します。

ステップ 2 [レイヤ7 DOS（Layer 7 DOS）]を選択します。

ステップ 3 [プロファイル名（Profile Name）] に一意のプロファイル名を入力します。

ステップ 4 （任意）[説明（Description）]に説明を入力します。これは、同様の名前を持つ他のプロファイルを区別するのに役立ちます。

ステップ 5 [要求レート制限（Request Rate Limits）] を追加します。

リソースへの過剰な要求の制限は、次のパラメータに基づいて行います。これらのパラメータの値は、レイヤ 7 DoS オプションで保護する Web サービスのトラフィックパターンを測定し、理解した上で指定してください。

表 *3:* パラメータ

パラメータ	説明
URI	リソース要求を制限するためのパスを示すために使用される相対URI。たとえば、https://www.example.com/login.html でサービスリソースをモニターして保護する場合は、[要求レート制限（Request Rate Limits）] テーブルの URI パラメータとして /login.html を入力します。

パラメータ	説明
HTTP メソッド（HTTP Methods）	HTTP メソッドをリソース URI ごとに指定すると、どの HTTPメソッドがクライアント要求のレート制限の対象となり、どれが対象とならないかを制御できます。テーブルの各行のドロップダウンから複数のメソッドを選択できます。HTTP メソッドリストが空の場合、メソッドは無視され、リソースへのすべてのコールにレートが適用されることを意味します。 （注） レートはリソースごとに適用されます。したがって、複数のメソッドがある場合、その行の [要求レート（Request Rate）] で指定されたレート制限が共有されます。たとえば、レートが1秒あたり 3 リクエストであり、GET、POST、および PUT が HTTP メソッドで指定され、2 つの GET と 1 つの POST が単一のクライアント IP からその URI に対して同じ秒内で発生した場合、同じ秒内で PUT は許可されません。
要求レート（Request Rate）	1秒あたりの要求数。これは、単一のクライアントがルールのURI部分で指定されたURIリソースに要求を送信できるレートを決定します。
バースト サイズ	ルールの URI 部分で指定された URI リソースにクライアントが同時に送信できる要求の最大数を指定します。このしきい値を超える要求が同時にプロキシに到着した場合、バックエンドサーバーには送信されません。

ステップ 6 完了したら、[保存（Save）] をクリックします。ルールは上から順にチェックされ、最初に一致したものから適用されるため、URI に基づいてルールの順序を決定することが重要です。リストの上位に追加された URI に、その下位のルールのリソースを含むリソースパスが含まれている場合は、最初に一致したルールが適用されます。

次のタスク

- プロファイルの詳細の表示
- L7 DoS プロファイルを**サービスオブジェクト**に追加します。その後、プロファイルへのゲートウェイ関連付けの追加を実行します。ルールセットを更新しても、変更がすぐに展開されない場合があることに注意してください。

URL（Uniform Resource Locator）フィルタプロファイル

URL フィルタリングプロファイルは、 HTTP リクエストの URL を評価し、トラフィックを許可または拒否するアクションを適用します。URL を評価するには、トラフィックを [転送プロ

キシ（Forward Proxy）]ルールで処理する必要があります。プロファイル内の一連のURLは、フルパスを表す文字列として、またはPerl互換正規表現（PCRE）で表される文字列として指定できます。ドメインフィルタリングのみが必要な場合は、FQDNフィルタリングプロファイルを使用することをお勧めします。FQDNフィルタリングプロファイルは、URLフィルタリングと組み合わせて使用することもできます。この場合、ドメインはFQDNフィルタリングプロファイルを使用して評価され、URLはURLフィルタリングプロファイルを使用して評価されます。

URLフィルタリングプロファイルでは、一連の定義済みカテゴリを使用できます。カテゴリの詳細については、「FQDN / URL フィルタリングカテゴリ」を参照してください。

（注） URLフィルタリングは、ユーザー指定の行（URLとカテゴリ）および2つのデフォルト行（[未分類（Uncategorized）]と[任意（ANY）]）を含むテーブルとして構成されます。必要に応じて、カテゴリとURLを各行内で組み合わせることができます。

各URLフィルタリングプロファイルの制限は次のとおりです。

- ユーザー指定の行の最大数：254（スタンドアロンまたはスタンドアロンのグループ）
- 1行あたりのカテゴリとURLの最大数：60
- URL文字の最大長：2048文字

マルチレベルドメイン（「www.example.com」など）を指定する場合は、「.」文字をエスケープ処理することが重要です（「www\.example\.com」など）。そうしないと、任意の1文字を表すワイルドカードとして扱われます。

未分類

- URLフィルタリングプロファイルの最後から2番目の行であり、[未分類（Uncategorized）]として表されます。
- ユーザー指定のURLと一致しないURL、またはカテゴリを持たないURLに対して実行するポリシーアクションを指定します。
- スタンドアロンプロファイルがグループプロファイルで使用され、グループプロファイルがポリシールールセットに適用されている場合、[未分類（Uncategorized）]行はグループプロファイルから取得されます。スタンドアロンプロファイルの[未分類（Uncategorized）]行は、スタンドアロンプロファイルがポリシールールセットに直接適用されている場合にのみ適用されます。

デフォルト（任意）

- [任意（ANY）]として表される、URLフィルタリングプロファイルの最終行。
- ユーザー指定のURLまたはカテゴリに一致しないURL、または[未分類（Uncategorized）]ではないURLに対して実行するポリシーアクションを指定します。

- スタンドアロンプロファイルがグループプロファイルで使用され、グループプロファイルがポリシールールセットに適用されている場合、[任意（ANY）]行はグループプロファイルから取得されます。スタンドアロンプロファイルの [任意（ANY）] 行は、スタンドアロンプロファイルがポリシールールセットに直接適用されている場合にのみ適用されます。

URL フィルタリングプロファイルの作成

スタンドアロン URL フィルタリングプロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）]**>**[プロファイル（Profiles）]**>**[URLフィルタリング（URL Filtering）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力します。

ステップ 4 （任意）[説明（Description）] に説明を入力します。これは、同様の名前を持つ他のプロファイルを区別する場合に役立ちます。

ステップ 5 [追加（Add）] をクリックして新しい行を作成します。

ステップ 6 個々の URL を指定します（例：https://www.google.com）。

- 各 URL は PCRE（Perl 互換正規表現）として指定されます。
- 各 URL はフルパスとして指定する必要があります。
- 小数点「.」はエスケープ処理することを検討してください。そうしないと、一文字を表すワイルドカードとして扱われます。

ステップ 7 [カテゴリ（Categories）] を指定します（例：ギャンブル、スポーツ、ソーシャルネットワーキング）。

ステップ 8 ポリシーを適用する HTTP メソッドを指定します。

ステップ 9 メソッドのサブセットとして次のいずれかを選択します。

- 消去
- get
- Head
- Options
- パッチ
- 投稿
- Put

ステップ 10 すべてのメソッドに対して [すべて（All）] を指定します。

ステップ 11 ユーザー指定の [URL/カテゴリ（URLs/Categories）]、[未分類（Uncategorized）]、および [任意（ANY）] の行に対してポリシーの [アクション（Action）] を指定します。

- [許可/ログ（Allow Log）]：要求を許可し、イベントをログに記録します。
- [許可/ログなし（Allow No Log）]：要求を許可し、イベントをログに記録しません。
- [拒否/ログ（Deny Log）]：要求を拒否し、イベントをログに記録します。
- [拒否/ログなし（Deny No Log）]：要求を拒否し、イベントをログに記録しません。

ステップ 12 [リターンステータスコード（Return Status Code）] を指定します。

ステップ 13 **100 以上 600 未満**の整数値を指定します。この値は、要求を行ったクライアントに返される HTTP ステータスを表します。一般的なリターンコードは **503** です。

ステップ 14 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

完全修飾ドメイン名のフィルタプロファイル

完全修飾ドメイン名（FQDN）フィルタリングプロファイルは、トラフィックに関連付けられたFQDNを評価し、トラフィックを許可または拒否するアクションを適用します。FQDNを評価するには、トラフィックを TLS で暗号化し、 TLS hello ヘッダーの SNI フィールドに FQDN を含める必要があります。FQDNは、[転送（Forwarding）]ルールまたは[転送プロキシ（Forward Proxy）]ルールのいずれかによって処理されるトラフィックについて評価できます。プロファイル内の一連の FQDN は、完全なドメインを表す文字列として、またはPerl 互換正規表現（PCRE）で表される文字列として指定できます。ドメイン許可リストのみが必要な場合は、FQDNフィルタリングプロファイルを使用することをお勧めします。FQDNフィルタリングプロファイルは、URLフィルタリングプロファイルと組み合わせて使用することもできます。この場合、ドメインはFQDN フィルタリングプロファイルを使用して評価され、URL は URL フィルタリングプロファイルを使用して評価されます。

FQDNフィルタリングは、ルールの一致後に、条件に基づいて許可または拒否するカテゴリをフィルタ処理するために使用します。フィルタは詳細に設定できます。FQDN フィルタ行には、拒否や許可など、使用できるログ関連のアクションが含まれます。

FQDN フィルタリングプロファイルでは、一連の定義済みカテゴリを使用することもできます。カテゴリの詳細については、「FQDN / URL フィルタリングカテゴリ」を参照してください。

（注） FQDN フィルタリングプロファイルは、ユーザー指定の行（FQDN とカテゴリ）および 2 つのデフォルト行（[未分類（Uncategorized）] と [任意（ANY）]）を含むテーブルとして整理されます。必要に応じて、カテゴリと FQDN を各行内で組み合わせることができます。

各 FQDNフィルタプロファイルの制限は次のとおりです。

- ユーザー指定の行の最大数：254（スタンドアロンまたはスタンドアロンのグループ）
- 1 行あたりのカテゴリと FQDN の最大数：60
- FQDN 文字の最大長：255 文字

マルチレベルドメイン（「www.example.com」など）を指定する場合は、「.」文字をエスケープ処理することが重要です（「www\.example\.com」など）。そうしないと、任意の 1 文字を表すワイルドカードとして扱われます。

スタンドアロンとグループ

FQDN フィルタプロファイルは、スタンドアロンまたはグループとして指定できます。

スタンドアロンのFQDNフィルタプロファイルには、FQDNとカテゴリが含まれています。プロファイルは、1つ以上のポリシールールセットに直接適用されるか、FQDNグループプロファイルに関連付けられます。

FQDN フィルタ グループ プロファイルには、さまざまな目的で定義したり、組み合わせてグループプロファイルを作成したりできる、スタンドアロンプロファイルの番号付きリストが含まれます。グループプロファイルは、1 つ以上のポリシールールセットに直接適用できます。各チームは、特定のスタンドアロンプロファイルを作成および管理できます。これらのスタンドアロンプロファイルは、グループプロファイルにまとめて階層を作成したり、ユースケースに基づいてさまざまな組み合わせを作成したりできます。組み合わせの例としては、すべてに適用されるグローバル FQDN リスト、異なる CSP ごとに適用される CSP 固有のリスト、および異なるアプリケーションごとに適用されるアプリケーション固有のリストなどがあります。

未分類

- [未分類（Uncategorized）] として表される、FQDN フィルタプロファイルの最後から 2 番目の行。
- ユーザー指定の FQDN と一致しない FQDN、またはカテゴリを持たない FQDN に対して実行するポリシーアクションを指定します。
- スタンドアロンプロファイルがグループプロファイルで使用され、グループプロファイルがポリシールールセットに適用されている場合、[未分類（Uncategorized）] 行はグループプロファイルから取得されます。スタンドアロンプロファイルの [未分類（Uncategorized）] 行は、スタンドアロンプロファイルがポリシールールセットに直接適用されている場合にのみ適用されます。

デフォルト（任意）

- [任意（ANY）] として表される、FQDN フィルタプロファイルの最終行。
- ユーザー指定の FQDN またはカテゴリに一致しない FQDN、または [未分類（Uncategorized）] ではない FQDN に対して実行するポリシーアクションを指定します。
- スタンドアロンプロファイルがグループプロファイルで使用され、グループプロファイルがポリシールールセットに適用されている場合、[任意（ANY）]行はグループプロファイルから取得されます。スタンドアロンプロファイルの [任意（ANY）] 行は、スタンドアロンプロファイルがポリシールールセットに直接適用されている場合にのみ適用されます。

スタンドアロン FQDN フィルタプロファイルの作成

スタンドアロン FQDNフィルタプロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [FQDNフィルタリング（FQDN Filtering）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力します。

ステップ 4 （任意）[説明（Description）]に説明を入力します。これは、似た名前のプロファイルを区別するのに役立ちます。

ステップ 5 [タイプ（Type）] に [スタンドアロン（Standalone）] を指定します。

ステップ 6 [追加（Add）] をクリックして新しい行を作成します。

ステップ 7 個々の FQDN を指定します（例：google.com）。

a) 各 FQDN は PCRE（Perl 互換正規表現）として指定されます。

b) 「.」文字はエスケープ処理を検討してください。そうしないと、一文字を表すワイルドカードとして扱われます。

ステップ 8 [カテゴリ（Category）] を指定します（例：ギャンブル、スポーツ、ソーシャルネットワーキング）。

ステップ 9 ユーザー指定の [FQDN/カテゴリ（FQDNs/Categories）]、[未分類（Uncategorized）]、および [任意（ANY）] の行に対してポリシーの [アクション（Action）] を指定します。

- [許可/ログ（Allow Log）]：要求を許可し、イベントをログに記録します。
- [許可/ログなし（Allow No Log）]：要求を許可し、イベントをログに記録しません。
- [拒否/ログ（Deny Log）]：要求を拒否し、イベントをログに記録します。
- [拒否/ログなし（Deny No Log）]：要求を拒否し、イベントをログに記録しません。

ステップ 10 （任意）復号が不要または不可能な場合は、任意の FQDN に対して [復号の例外（Decryption Exception）] を指定します。復号の例外を検討する理由としては、次のものが考えられます。

- 暗号化されたトラフィックを検査したくない（金融サービス、防衛、ヘルスケアなど）。
- SSO 認証トラフィックで復号が不可能。
- プロキシ化できない NTLM トラフィック。

ステップ 11 完了したら、[保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

グループ FQDN フィルタプロファイルの作成

少なくとも 2 つのスタンドアロンプロファイルを持つグループ FQDNフィルタプロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [FQDNフィルタリング（FQDN Filtering）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力します。

ステップ 4 （任意）[説明（Description）] に説明を入力します。これは、同様の名前を持つプロファイルを区別するのに役立ちます。

ステップ 5 [タイプ（Type）] に [グループ（Group）] を指定します。

ステップ 6 最初のスタンドアロンプロファイルを選択します（少なくとも 1 つのスタンドアロンプロファイルが必要です）。

ステップ 7 [FQDNプロファイルの追加（Add FQDN Profile）] をクリックして、追加プロファイル用の新しい行を作成します。

ステップ 8 スタンドアロンプロファイルを選択します。

ステップ 9 未分類の FQDN に対するポリシーの [アクション（Action）] を指定します。

ステップ 10 [任意（ANY）] FQDN に対するポリシーの [アクション（Action）] を指定します（デフォルト）。

ステップ 11 （任意）復号が不要または不可能な場合は、未分類または任意に対して [復号の例外（Decryption Exception）] を指定します。復号の例外を検討する理由としては、次のものが考えられます。

- 暗号化されたトラフィックを検査したくない（金融サービス、防衛、ヘルスケアなど）。
- SSO 認証トラフィックで復号が不可能。

- プロキシ化できない NTLM トラフィック。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

悪意のある IP プロファイル

既知の悪意ある IP との通信を防ぐために、追加のセキュリティ保護を有効にすることができます。これらの悪意のある IP は、Trustwave によって定義され、セキュリティプロファイルのルールセットとして Multicloud Defense に統合されます。Trustwave によってアップデートが提供されるのに合わせて、ルールセットは頻繁に更新されます。アップデートは、自動更新設定または手動更新設定を使用して、ポリシールールセットに動的に適用することも、手動で適用することもできます。詳細については、悪意のある IP プロファイルの作成 （22 ページ）を参照してください。

（注） 悪意のある IP は、学習されたさまざまな動作に基づいて Trustwave によって識別されます。

- Web ハニーポットから特定された悪意のある攻撃者
- ボットネット C&C ホスト
- Tor の出口ノード
- その他の学習された動作

悪意のある IP プロファイルの作成

悪意のある IP プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [プロファイル（Profiles）] > [悪意のあるIP（Malicious IPs）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）] に一意のプロファイル名を入力します。

ステップ 4 （任意）[説明（Description）]に説明を入力します。これは、同様の名前を持つ他のプロファイルを区別する場合に役立ちます。

ステップ 5 [IPレピュテーション（IP Reputation）] を有効にするには、このチェックボックスをオンにします。

ステップ 6 [Trustwaveルールセットバージョン（Trustwave Ruleset Version）] ドロップダウンメニューで、次の 2 つのオプションのいずれかを選択します。

- [手動（Manual）]：選択したルールセットバージョンは、このプロファイルを使用するすべてのゲートウェイの Multicloud Defense データパスエンジンによって使用されます。プロファイルは、新しいルールセットバージョンに自動的に更新されません。
- [自動（Automatic）]：Multicloud Defense によってルールセットバージョンが公開された後、更新を何日遅延させるかを選択します。新しいルールセットは Multicloud Defenseによって頻繁に公開されます。このプロファイルを使用するゲートウェイは、**N** 日以上前の最新のルールセットバージョンに自動的に更新されます。ここで **N** はドロップダウンから選択された「遅延日数」の引数です。たとえば、2021 年 1 月 10 日に展開を 5 日間遅延させることを選択した場合、 Multicloud Defense コントローラは 1 月 5 日以前に公開されたルールセットバージョンを選択します。そのルールセットバージョンを使用した社内テストが何らかの理由で失敗した場合、Multicloud Defense は数日間公開を行わない場合があることにご注意ください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットにプロファイルをアタッチします。詳細については、ルールセットとルールセットグループを参照してください。

IP レピュテーション

[IPレピュテーション（IP reputation）]チェックボックスは、プロファイルを[有効化（Enable）]または [無効化（Disable）] する手段として使用されます。チェックボックスがオンで、プロファイルがポリシールールセットにアタッチされている場合、悪意のある IP からの保護が適用されます。チェックボックスがオフで、プロファイルがポリシールールにアタッチされている場合、悪意のある IP からの保護は適用されません。[IPレピュテーション（IP reputation）] チェックボックスは常にオンにすることをお勧めします。悪意のある IP プロファイルを無効化する場合は、チェックボックスをオフにするのではなく、ポリシールールからその関連付けを削除してください。

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。