



その他の設定

次のトピックでは、アプライアンスで設定できるいくつかの追加機能について説明します。詳細については、ご使用のリリースの AsyncOS のオンラインヘルプまたはユーザーガイドを参照してください。

- [ユーザーポリシー \(1 ページ\)](#)
- [レポート \(2 ページ\)](#)
- [詳細情報 \(2 ページ\)](#)

ユーザーポリシー

Web インターフェイスを使用し、必要に応じて、どのユーザーがどの Web リソースにアクセスできるかを定義するポリシーを作成します。

- ユーザーの識別：インターネットにアクセスできるユーザーグループを定義するには、[Web セキュリティマネージャ (Web Security Manager)] > [アイデンティティ (Identities)] を選択します。
- アクセスポリシーの定義：許可または拒否するオブジェクトおよびアプリケーション、モニターまたは拒否する URL カテゴリ、Web レピュテーションおよびマルウェア対策を設定してユーザーのアクセスを制御するには、[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。

また、その他複数のポリシータイプを定義して、インターネットへのアクセスを制御することにより、組織の許容可能な使用ポリシーを実施できます。たとえば、HTTPS トランザクションを復号化するためのポリシーや、アップロード要求を制御するその他のポリシーを定義できます。

Cisco Web セキュリティアプライアンスの設定ポリシーについては、『[AsyncOS for Cisco Web Security Appliances User Guide](#)』の「Working with Policies」の章を参照してください。

レポート

Web インターフェイスで使用できるレポートを表示することにより、ネットワーク上でブロックおよびモニターされる Web トラフィックの統計情報を表示できます。ブロックされた上位の URL カテゴリ、クライアントアクティビティ、システムステータスなどに関するレポートを表示できます。

詳細情報

その他にも、Cisco Web セキュリティアプライアンスに設定できる機能があります。機能キーの設定、エンドユーザーの通知、ロギングに関する詳細と、その他の使用可能な Web セキュリティアプライアンス機能の詳細については、マニュアル『Cisco Web Security Appliance S196, S396, S696, and S696F』を参照してください。

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。