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 （1 ページ）
- 復号化ポリシーによる HTTPS トラフィックの管理：ベスト プラクティス （2 ページ）
- 復号化ポリシー （3 ページ）
- ルート証明書 （10 ページ）
- HTTPS トラフィックのルーティング （18 ページ）
- 暗号化/HTTPS/証明書のトラブルシューティング （18 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

復号化ポリシーで、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化するタイミング。
- 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化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化し、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、または復号化のアクションが実行されます。

注意 **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 セッションを復号化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。

復号化ポリシー タスクによる HTTPS トラフィックの管理の概要

手順	復号化ポリシーによる 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	HTTPS プロキシのイネーブル化 （5 ページ）
2	証明書とキーをアップロードまたは生成する	• ルート証明書およびキーのアップロード （13 ページ） • HTTPS プロキシ用の証明書およびキーの生成 （13 ページ）
3	復号化オプションを設定する	復号化オプションの設定 （9 ページ）
5	（任意）無効な証明書の処理を設定する	無効な証明書の処理の設定 （14 ページ）
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	リアルタイムの失効ステータス チェックの有効化 （15 ページ）
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	信頼できるルート証明書 （17 ページ）

復号化ポリシーによる HTTPS トラフィックの管理：ベスト プラクティス

一般的な復号化ポリシー 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、復号化された 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。

復号化ポリシー

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）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。
パススルー（Pass through）	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。 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。 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。
復号化（Decrypt）	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化、プレーン テキスト HTTP 接続であるかのように、復号化されたトラフィックにアクセス ポリシーを適用します。接続を復号化し、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。

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、復号化ポリシーが、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。復号化ポリシーが、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 プロキシが復号化ポリシー 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。「HTTPS トラフィックの制御」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。アクセスポリシーのアクションの適用には、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。

図 *1*: 復号化ポリシー アクションの適用

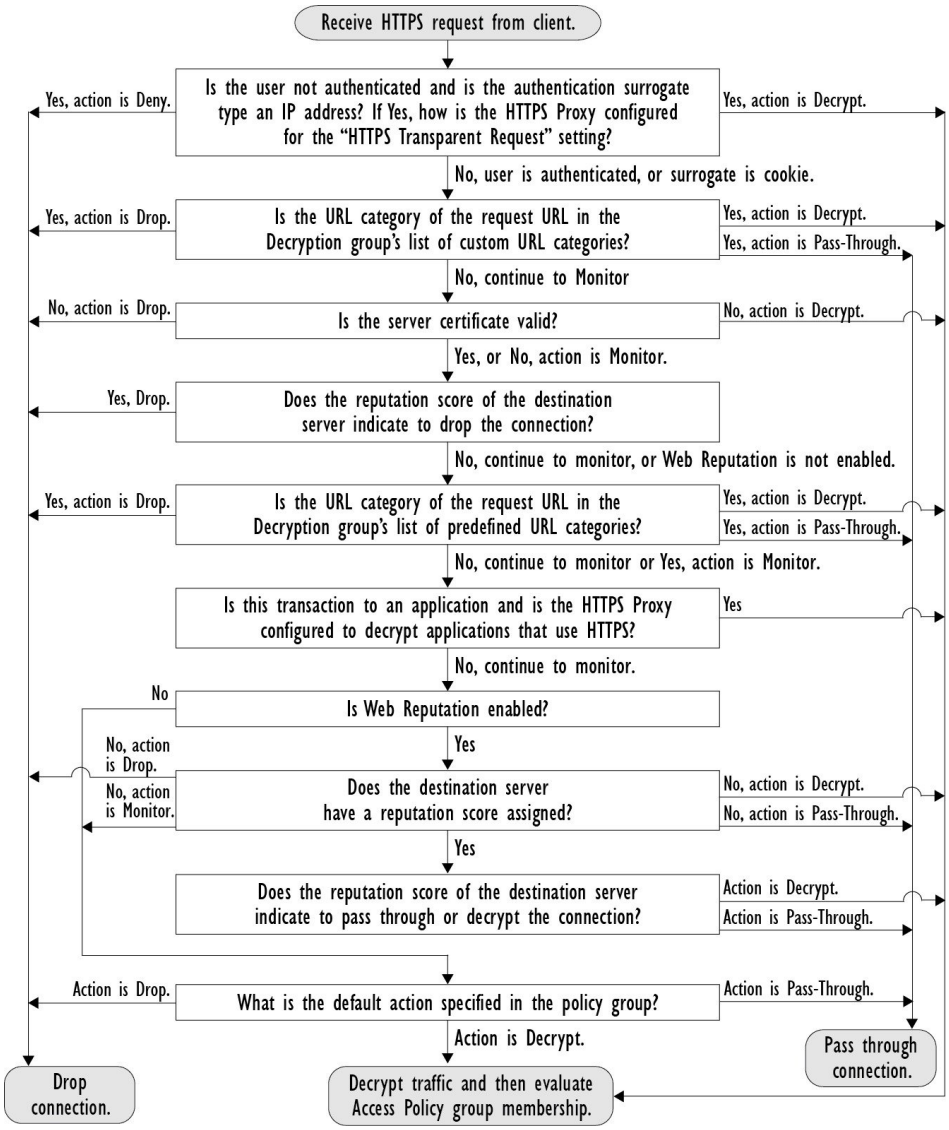
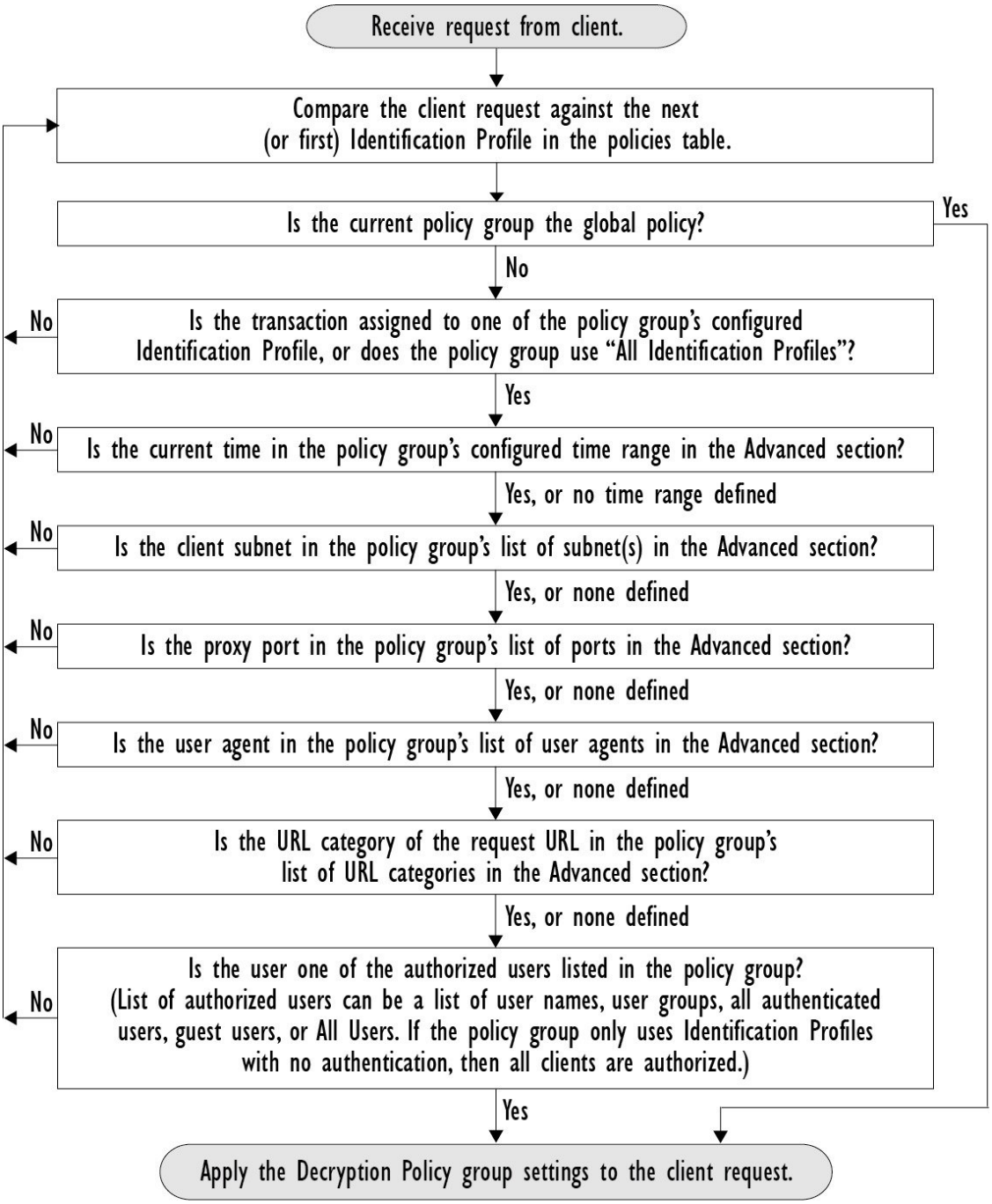


図 *2*: 復号化ポリシーのポリシー グループ トランザクション フロー



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化するには、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化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。

始める前に

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、復号化された HTTPS トラフィックを処理します。

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、[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。

（注） 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 復号化に使用するルート/署名証明書をアップロードまたは生成します。

（注） 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 要求を復号化して、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。

（注） 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化をイネーブルにするかどうか選択します。

（注） 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、復号化により、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 の復号化の管理 （11 ページ）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。

次のタスク

関連項目

- 証明書の検証と HTTPS の復号化の管理 （11 ページ）

HTTPS トラフィックの制御

Secure Web Applianceが復号化ポリシー 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。復号化ポリシー グループの管理設定で、アプライアンスが接続を復号化するか、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。

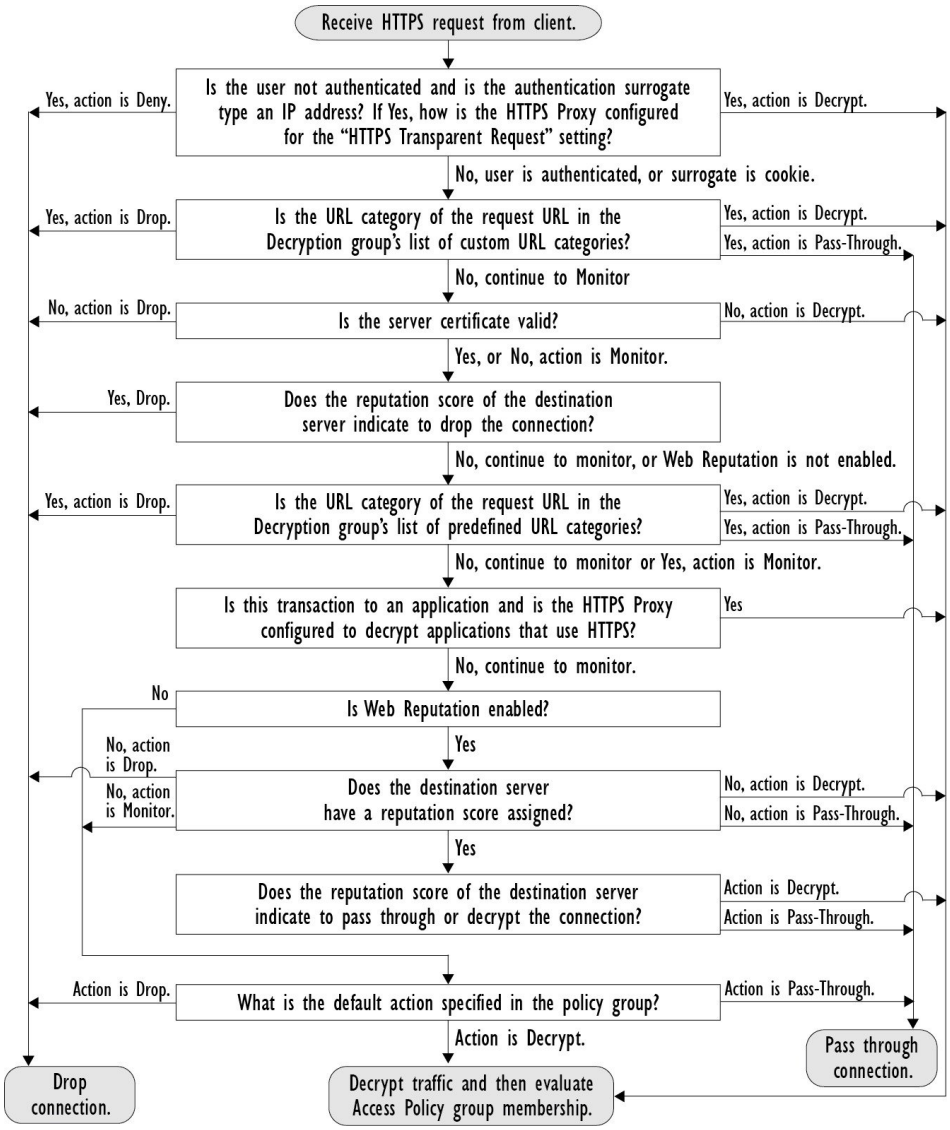
オプション	説明
URL カテゴリ（URL Categories）	定義済みおよびカスタムの各 URL カテゴリについて、HTTPS 要求で実行するアクションを設定できます。[URL フィルタリング（URL Filtering）] 列にある、設定するポリシー グループのリンクをクリックします。 （注） HTTPS 要求の特定の URL カテゴリをドロップ（エンドユーザー通知なし）するのではなく、ブロック（エンドユーザー通知あり）する場合は、復号化ポリシー グループのその URL カテゴリの復号化を選択し、その後に、アクセス ポリシー グループの同じ URL カテゴリのブロックを選択します。
Web レピュテーション（Web Reputation）	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。

オプション	説明
デフォルト アクション（Default Action）	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。 （注） 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。

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 [復号化オプション（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化（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化ポリシーを 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。

図 *3 :* 復号化ポリシー アクションの適用



復号化オプションの設定

始める前に

HTTPS プロキシのイネーブル化 （5 ページ）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 復号化オプションをイネーブルにします。

（注） 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、復号化によりその他の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。

復号化オプション	説明
認証のための復号化	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化を許可して、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化	AsyncOS がエンド ユーザー通知を表示できるように復号化を許可します。 （注） 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「復号化」されます。
エンドユーザー確認応答のための復号化	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化を許可し、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化	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（Explicit requests）	• 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 • 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
透過的要求（Transparent requests）	• サロゲートが IP ベースで、認証の復号化がイネーブル、または • 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

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化します。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。

（注） 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。

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。

（注） 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 の復号化の管理

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化します。

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ていません。

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 （15 ページ）
- 無効な証明書の処理の設定 （14 ページ）
- 証明書失効ステータスのチェックのオプション （15 ページ）

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（Decrypt）]。**
- **[モニター]。**

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。

復号化された接続の、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、接続を復号化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

始める前に

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 （5 ページ）。

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。

（注） 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

始める前に

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 （5 ページ）。

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

始める前に

HTTPS プロキシのイネーブル化 （5 ページ）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 証明書エラーのタイプごとに、プロキシの応答（**ドロップ**、**復号化**、**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。
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。 （注） 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。

証明書エラーのタイプ	説明
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、http://www.openssl.org/docs/apps/verify.html 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。

（注） 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 （15 ページ）
- 無効な証明書の処理の設定 （14 ページ）

リアルタイムの失効ステータス チェックの有効化

始める前に

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 （5 ページ）を参照してください。

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
OSCP 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。
OSCP 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。
OSCP 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。
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。
OSCP 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。
OSCP 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、復号化は必要ありません。

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

始める前に

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 （5 ページ）を参照してください。

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

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	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。 • URL • 宛先ポート番号 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。

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
- IP ベースのサロゲートと透過的要求を含む HTTPS
- 特定 Web サイトの復号化のバイパス
- アラート：セキュリティ証明書に関する問題（Problem with Security Certificate）

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。