



システム ポリシーの管理

システム ポリシーを使用して、ASA FirePOWER モジュールで次のものを管理できます。

- 監査ログ設定
- メール リレー ホストおよび通知アドレス
- SNMP ポーリング設定
- STIG コンプライアンス

詳細については、次の各項を参照してください。

- システム ポリシーの作成(43-1 ページ)
- システム ポリシーの編集(43-2 ページ)
- システム ポリシーの適用(43-3 ページ)
- システム ポリシーの削除(43-3 ページ)

システム ポリシーの作成

ライセンス:任意(Any)

システム ポリシーを作成したら、それに名前と説明を割り当てます。次に、ポリシーのさまざまな側面(それぞれの項の説明を参照)を設定します。

新しいポリシーを作成する代わりに、別のASA FirePOWER モジュールからシステム ポリシーをエクスポートして、それを対象のASA FirePOWER モジュールにインポートできます。ニーズに合わせて、インポートされたポリシーを編集してから適用することができます。詳細については、[設定のインポートおよびエクスポート\(B-1 ページ\)](#)を参照してください。

システム ポリシーを作成するには、次の手順を実行します。

- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ローカル(Local)] > [システム ポリシー(System Policy)] の順に選択します。
[システム ポリシー(System Policy)] ページが表示されます。
- 手順 2 [ポリシーの作成(Create Policy)] をクリックします。
[ポリシーの作成(Create Policy)] ページが表示されます。
- 手順 3 ドロップダウン リストから、新しいシステム ポリシーのテンプレートとして使用する既存のポリシーを選択します。

■ システム ポリシーの編集

手順 4 新規ポリシーの名前を [新しいポリシー名 (New Policy Name)] フィールドに入力します。

手順 5 新規ポリシーの説明を [新しいポリシーの説明 (New Policy Description)] フィールドに入力します。

手順 6 [作成(Create)] をクリックします。

システム ポリシーが保存され、[システム ポリシーの編集 (Edit System Policy)] ページが表示されます。システム ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- 監査ログの設定(43-5 ページ)
- メール リレー ホストおよび通知アドレスの設定(43-7 ページ)
- SNMP ポーリングの設定(43-8 ページ)
- STIG コンプライアンスの有効化(43-10 ページ)

システム ポリシーの編集

ライセンス:任意(Any)

既存のシステム ポリシーを編集できます。ASA FirePOWER モジュールに現在適用されているシステム ポリシーを編集する場合、変更を保存した後にポリシーを再適用してください。詳細については、[システム ポリシーの適用 \(43-3 ページ\)](#) を参照してください。

既存のシステム ポリシーを編集するには、次の手順を実行します。

手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ローカル (Local)] > [システム ポリシー(System Policy)] の順に選択します。

既存のシステム ポリシーのリストを含む、[システム ポリシー(System Policy)] ページが表示されます。

手順 2 編集するシステム ポリシーの横にある編集アイコン()をクリックします。

[ポリシーの編集(Edit Policy)] ページが表示されます。ポリシー名とポリシーの説明を変更できます。システム ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- 監査ログの設定(43-5 ページ)
- メール リレー ホストおよび通知アドレスの設定(43-7 ページ)
- SNMP ポーリングの設定(43-8 ページ)
- STIG コンプライアンスの有効化(43-10 ページ)



(注) ASA FirePOWER モジュールに適用されているシステム ポリシーを編集する場合、編集が完了したら、更新されたポリシーを再適用してください。[システム ポリシーの適用 \(43-3 ページ\)](#) を参照してください。

手順 3 [ポリシーを保存して終了(Save Policy and Exit)] をクリックして変更を保存します。変更が保存され、[システム ポリシー(System Policy)] ページが表示されます。

システム ポリシーの適用

ライセンス:任意(Any)

ASA FirePOWER モジュールにシステム ポリシーを適用できます。システム ポリシーがすでに適用されている場合、再適用するまで、ポリシーに加えた変更は有効になりません。

システム ポリシーを適用するには、次の手順を実行します。

手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ローカル(Local)] > [システム ポリシー(System Policy)] の順に選択します。

[システム ポリシー(System Policy)] ページが表示されます。

手順 2 適用するシステム ポリシーの横にある適用アイコン()をクリックします。

手順 3 [適用(Apply)] をクリックします。

[システム ポリシー(System Policy)] ページが表示されます。メッセージはシステム ポリシーの適用のステータスを示します。

システム ポリシーの削除

ライセンス:任意(Any)

システム ポリシーは、使用中でも削除できます。使用中の場合は、新しいポリシーが適用されるまで現在のポリシーが使用されます。デフォルトのシステム ポリシーは削除できません。

システム ポリシーを削除するには、次の手順を実行します。

手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ローカル(Local)] > [システム ポリシー(System Policy)] の順に選択します。

[システム ポリシー(System Policy)] ページが表示されます。

手順 2 削除するシステム ポリシーの横にある削除アイコン()をクリックします。ポリシーを削除するには、[OK] をクリックします。

[システム ポリシー(System Policy)] ページが表示されます。ポリシーの削除について確認を求めるポップアップ メッセージが表示されます。

システム ポリシーの設定

ライセンス:任意(Any)

さまざまなシステム ポリシーの設定を行うことができます。システム ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- アプライアンスのアクセス リストの設定(43-4 ページ)
- 監査ログの設定(43-5 ページ)

- メール リレー ホストおよび通知アドレスの設定(43-7 ページ)
- SNMP ポーリングの設定(43-8 ページ)
- STIG コンプライアンスの有効化(43-10 ページ)

アプライアンスのアクセス リストの設定

ライセンス:任意(Any)

[アクセスリスト(Access List)] ページを使用して、特定ポートのアプライアンスにどのコンピュータがアクセス可能かを制御できます。デフォルトでは、Web インターフェイスへのアクセスに使用されるポート 443(Hypertext Transfer Protocol Secure(HTTPS))と、コマンドラインへのアクセスに使用されるポート 22(Secure Shell(SSH))は、あらゆる IP アドレスに対して有効です。ポート 161 を介した SNMP アクセスを追加することもできます。SNMP 情報をポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があることに注意してください。



注意

デフォルトでは、アプライアンスへのアクセスは制限されません。よりセキュアな環境でアプライアンスを稼動させるために、特定の IP アドレスに対してアプライアンスへのアクセスを追加してから、デフォルトの任意のオプションを削除することを検討してください。

アクセスリストは、システム ポリシーの一部です。新しいシステム ポリシーを作成するか、既存のシステム ポリシーを編集することによって、アクセスリストを指定できます。いずれの場合も、システム ポリシーを適用するまでアクセスリストは有効になりません。

このアクセスリストは、外部データベース アクセスを制御しないので注意してください。外部データベースのアクセスリストの詳細については、[クラウド通信の有効化\(44-2 ページ\)](#)を参照してください。

アクセスリストを設定するには、次の手順を実行します。

Access: Admin

手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ローカル(Local)] > [システム ポリシー(System Policy)] の順に選択します。

[システム ポリシー(System Policy)] ページが表示されます。

手順 2 次の選択肢があります。

- 既存のシステム ポリシーのアクセスリストを変更するには、システム ポリシーの横にある編集アイコン()をクリックします。
- 新しいシステム ポリシーの一部としてアクセスリストを設定するには、[ポリシーの作成(Create Policy)] をクリックします。

[システム ポリシーの作成\(43-1 ページ\)](#) で説明されているように、システム ポリシーの名前および説明を入力し、[保存(Save)] をクリックします。

いずれの場合も、[アクセスリスト(Access List)] ページが表示されます。

手順 3 現在の設定の 1 つを削除するために、削除アイコン()をクリックすることもできます。設定が削除されます。



注意

アプライアンスのインターフェイスへの接続に現在使用されている IP アドレスへのアクセスを削除し、「IP=any port=443」のエントリが存在しない場合、ポリシーを適用した時点ではシステムへのアクセスは失われます。

手順 4 1つ以上の IP アドレスへのアクセスを追加するために、[ルールの追加(Add Rules)] をクリックすることもできます。

[IP アドレスの追加(Add IP Address)] ページが表示されます。

手順 5 [IP アドレス(IP Address)] フィールドでは、追加する IP アドレスに応じて次のオプションがあります。

- 厳密な IP アドレス(192.168.1.101 など)
 - CIDR 表記を使用した IP アドレス ブロック(192.168.1.1/24 など)
- Firepower system での CIDR の使用方法については、[IP アドレスの規則\(1-5 ページ\)](#) を参照してください。
- any(任意の IP アドレスを指定)

手順 6 [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

手順 7 [追加(Add)] をクリックします。

[アクセスリスト(Access List)] ページが再度表示され、ユーザが行った変更が反映されます。

手順 8 [ポリシーを保存して終了(Save Policy and Exit)] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、[システム ポリシーの適用\(43-3 ページ\)](#) を参照してください。

監査ログの設定

ライセンス:任意(Any)

ASA FirePOWER モジュールが外部ホストに監査ログをストリーミングするように、システム ポリシーを設定できます。



(注)

外部ホストが機能しており、監査ログを送信する ASA FirePOWER モジュールからアクセス可能であることを確認する必要があります。

送信元ホスト名は送信される情報の一部です。ファシリティ、重大度、およびオプションのタグを使用して監査ログストリームをより詳細に識別できます。ASA FirePOWER モジュールは、システム ポリシーが適用されるまで監査ログを送信しません。

この機能を有効にしてポリシーを適用し、監査ログを受け入れるように宛先ホストを設定した後で、syslog メッセージが送信されます。次に、出力構造の例を示します。

Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]

現地の日付、時刻、およびホスト名の後に、角括弧で囲まれたオプションタグが続き、送信側デバイス名の後に監査ログメッセージが続きます。

■ システム ポリシーの設定

次に例を示します。

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3000: admin@10.1.1.2, Operations > Monitoring, Page View
```

監査ログの設定を行うには、次の手順を実行します。

手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ローカル(Local)] > [システム ポリシー(System Policy)] の順に選択します。

[システム ポリシー(System Policy)] ページが表示されます。

手順 2 次の選択肢があります。

- 既存のシステム ポリシーの監査ログの設定を変更するには、システム ポリシーの横にある編集アイコン()をクリックします。
- 新しいシステム ポリシーの一部として監査ログ設定を設定するには、[ポリシーの作成(Create Policy)] をクリックします。

[システム ポリシーの作成\(43-1 ページ\)](#) で説明されているように、システム ポリシーの名前および説明を入力し、[保存(Save)] をクリックします。

手順 3 [監査ログ設定(Audit Log Settings)] をクリックします。

[監査ログ設定(Audit Log Settings)] ページが表示されます。

手順 4 [監査ログを Syslog に送信(Send Audit Log to Syslog)] ドロップダウンメニューから、[有効(Enabled)] を選択します。(デフォルト設定では [無効(Disabled)] になっています。)

手順 5 [ホスト(Host)] フィールドにあるホストの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。デフォルト ポート(514)が使用されます。



注意 監査ログを受け入れるように設定しているコンピュータが、リモート メッセージを受け入れるようにセットアップされていない場合、ホストは監査ログを受け入れません。

手順 6 [ファシリティ(Facility)] フィールドから syslog ファシリティを選択します。

手順 7 [重大度(Severity)] フィールドから重大度を選択します。

手順 8 必要に応じて、[タグ(オプション)(Tag (optional))] フィールドで参照タグを挿入します。

手順 9 定期的な監査ログの更新を外部 HTTP サーバに送信するには、[監査ログを HTTP サーバに送信(Send Audit Log to HTTP Server)] ドロップダウンリストから [有効(Enabled)] を選択します。デフォルト設定では [無効(Disabled)] になっています。

手順 10 [監査情報を送信する URL(URL to Post Audit)] フィールドに、監査情報の送信先 URL を指定します。次にリストされている HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力する必要があります。

- subsystem
- actor
- event_type
- message
- action_source_ip
- action_destination_ip
- 結果
- 時刻
- tag(上記のように定義されている場合)



注意

暗号化されたポストを許可するには、HTTPS URL を使用する必要があります。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

手順 11 [ポリシーを保存して終了(Save Policy and Exit)] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、[システム ポリシーの適用\(43-3 ページ\)](#)を参照してください。

メール リレー ホストおよび通知アドレスの設定

ライセンス:任意(Any)

次の処理を行う場合、メール ホストを設定する必要があります。

- イベントベースのレポートの電子メール送信
- スケジュールされたタスクのステータス レポートの電子メール送信
- 変更調整レポートの電子メール送信
- データ切り捨て通知の電子メール送信
- 侵入イベント アラートについての電子メールの使用

アプライアンスとメール リレー ホスト間の通信に使用する暗号化方式を選択し、必要に応じて、メール サーバの認証資格情報を指定できます。設定を行った後、指定された設定を使用してアプライアンスとメール サーバとの間の接続をテストできます。

メール リレー ホストを設定するには、次の手順を実行します。

手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ローカル(Local)] > [システム ポリシー(System Policy)] の順に選択します。

[システム ポリシー(System Policy)] ページが表示されます。

手順 2 次の選択肢があります。

- 既存のシステム ポリシーの電子メールの設定を変更するには、システム ポリシーの横にある編集アイコン()をクリックします。
- 新しいシステム ポリシーの一部として電子メールの設定を行うには、[ポリシーの作成(Create Policy)] をクリックします。

[システム ポリシーの作成\(43-1 ページ\)](#)で説明されているように、システム ポリシーの名前および説明を入力し、[保存(Save)] をクリックします。

手順 3 [電子メール通知>Email Notification] をクリックします。

[電子メール通知の設定(Configure Email Notification)] ページが表示されます。

手順 4 [メール リレー ホスト(Mail Relay Host)] フィールドで、使用するメール サーバのホスト名または IP アドレスを入力します。



(注) 入力したメール ホストはアプライアンスからのアクセスを許可している必要があります。

■ システム ポリシーの設定

手順 5 [ポート番号(Port Number)] フィールドに、電子メールサーバで使用するポート番号を入力します。ポートは通常、暗号化を使用しない場合は 25、SSLv3 を使用する場合は 465、TLS を使用する場合は 587 です。

手順 6 暗号化方式を選択するには、次のオプションがあります。

- Transport Layer Security を使用してアプライアンスとメールサーバ間の通信を暗号化するには、[暗号化方式(Encryption Method)] ドロップダウンリストから [TLS] を選択します。
- セキュアソケットレイヤを使用してアプライアンスとメールサーバ間の通信を暗号化するには、[暗号化方式(Encryption Method)] ドロップダウンリストから [SSLv3] を選択します。
- アプライアンスとメールサーバ間の非暗号化通信を許可するには、[暗号化方式(Encryption Method)] ドロップダウンリストから [なし(None)] を選択します。

アプライアンスとメールサーバとの間の暗号化された通信では、証明書の検証は不要であることに注意してください。

手順 7 アプライアンスによって送信されるメッセージの送信元の電子メールアドレスとして使用する有効な電子メールアドレスを、[送信元アドレス(From Address)] フィールドに入力します。

手順 8 必要に応じて、メールサーバに接続する際にユーザ名とパスワードを指定するには、[認証を使用(Use Authentication)] を選択します。[ユーザ名.Username] フィールドにユーザ名を入力します。パスワードを [パスワード>Password] フィールドに入力します。

手順 9 設定したメールサーバを使用してテストメールを送信するには、[テストメールのサーバ設定(Test Mail Server Settings)] をクリックします。

テストの成功または失敗を示すメッセージがボタンの横に表示されます。

手順 10 [ポリシーを保存して終了(Save Policy and Exit)] をクリックします。

システムポリシーが更新されます。システムポリシーを適用するまで変更は有効になりません。詳細については、[システムポリシーの適用\(43-3 ページ\)](#)を参照してください。

SNMP ポーリングの設定

ライセンス:任意(Any)

システムポリシーを使用して、アプライアンスの Simple Network Management Protocol (SNMP) ポーリングを有効化できます。SNMP 機能は、SNMP プロトコルのバージョン 1、2、および 3 をサポートします。

システムポリシー SNMP 機能を有効にすると、アプライアンスで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になることに注意してください。



(注)

アプライアンスをポーリングするには、使用的する任意のコンピュータで SNMP アクセスを追加する必要があります。詳細については、[アプライアンスのアクセスリストの設定\(43-4 ページ\)](#)を参照してください。SNMP MIB にはアプライアンスの攻撃に使用される可能性がある情報も含まれているので注意してください。シスコでは、SNMP アクセスのアクセスリストを MIB のポーリングに使用される特定のホストに制限することを推奨しています。シスコでは、SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することも推奨しています。

SNMP ポーリングを設定するには、次の手順を実行します。

手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ローカル(Local)] > [システム ポリシー(System Policy)] の順に選択します。

[システム ポリシー(System Policy)] ページが表示されます。

手順 2 次の選択肢があります。

- 既存のシステム ポリシーの SNMP ポーリングの設定を変更するには、システム ポリシーの横にある編集アイコン()をクリックします。
- 新しいシステム ポリシーの一部として SNMP ポーリングの設定を行うには、[ポリシーの作成(Create Policy)] をクリックします。

[システム ポリシーの作成\(43-1 ページ\)](#) で説明されているように、システム ポリシーの名前および説明を入力し、[作成(Create)] をクリックします。

手順 3 アプライアンスのポーリングに使用する各コンピュータに SNMP アクセスを追加していない場合は、ここで追加してください。詳細については、[アプライアンスのアクセスリストの設定\(43-4 ページ\)](#) を参照してください。

手順 4 [SNMP] をクリックします。

[SNMP] ページが表示されます。

手順 5 [SNMP バージョン(SNMP Version)] ドロップダウンリストから、使用する SNMP バージョンを選択します。

ドロップダウンリストに選択したバージョンが表示されます。

手順 6 次の選択肢があります。

- [バージョン 1(Version 1)] または [バージョン 2(Version 2)] を選択した場合は、[コミュニティストリング(Community String)] フィールドに SNMP コミュニティ名を入力します。ステップ 15 に進みます。
- [Version 3] を選択した場合、[ユーザを追加(Add User)] をクリックするとユーザ定義ページが表示されます。

手順 7 [ユーザ名(Username)] フィールドにユーザ名を入力します。

手順 8 [認証プロトコル(Authentication Protocol)] ドロップダウンリストから、認証に使用するプロトコルを選択します。

手順 9 [認証パスワード(Authentication Password)] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

手順 10 [認証パスワード(Authentication Password)] フィールドのすぐ下にある [パスワードの確認(Verify Password)] フィールドに認証パスワードを再入力します。

手順 11 使用するプライバシー プロトコルを [プライバシー プロトコル(Privacy Protocol)] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし(None)] を選択します。

手順 12 [プライバシー パスワード(Privacy Password)] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

手順 13 [プライバシー パスワード(Privacy Password)] フィールドのすぐ下にある [パスワードの確認(Verify Password)] フィールドにプライバシー パスワードを再入力します。

手順 14 [追加(Add)] をクリックします。

ユーザが追加されます。ステップ 6 ~ 13 までを繰り返して、さらにユーザを追加できます。ユーザを削除するには、削除アイコン()をクリックします。

■ システム ポリシーの設定

手順 15 [ポリシーを保存して終了(Save Policy and Exit)] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、[システム ポリシーの適用\(43-3 ページ\)](#)を参照してください。

STIG コンプライアンスの有効化

ライセンス:任意(Any)

米国連邦政府内の組織は、Security Technical Implementation Guides(STIG)に示されている一連のセキュリティ チェックリストに準拠しなければならない場合があります。STIG コンプライアンス オプションは、米国国防総省によって定められた特定の要件に準拠することを目的とした設定を有効にします。

STIG コンプライアンスを有効にした場合、適用可能なすべての STIG に厳格なコンプライアンスが保証されるわけではありません。

STIG コンプライアンスを有効にすると、ローカル シェル アクセス アカウントのパスワードの複雑さや維持に関するルールが変わります。さらに、STIG コンプライアンス モードでは、ssh のリモート ストレージを使用できません。

STIG コンプライアンスが有効なシステム ポリシーを適用すると、アプライアンスが強制的に再起動されるので注意してください。すでに STIG が有効になっているアプライアンスに STIG が有効なシステム ポリシーを適用した場合、アプライアンスは再起動しません。STIG が無効なシステム ポリシーを STIG が有効になっているアプライアンスに適用した場合、STIG は引き続き有効であり、アプライアンスはリブートしません。



注意

サポートからの支援なしでこの設定を無効にすることはできません。また、この設定はシステムのパフォーマンスに大きく影響する可能性があります。Cisco では、米国国防総省のセキュリティ要件に準拠する以外の目的で、STIG コンプライアンスを有効化することを推奨しません。

STIG コンプライアンスを有効にするには、次の手順を実行します。

手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ローカル(Local)] > [システム ポリシー(System Policy)] の順に選択します。

[システム ポリシー(System Policy)] ページが表示されます。

手順 2 次の選択肢があります。

- 既存のシステム ポリシーの時間の設定を変更するには、システム ポリシーの横にある編集アイコン()をクリックします。
- 新しいシステム ポリシーの一部として時間の設定を行うには、[ポリシーの作成(Create Policy)] をクリックします。

[システム ポリシーの作成\(43-1 ページ\)](#) で説明されているように、システム ポリシーの名前および説明を入力し、[保存(Save)] をクリックします。

手順 3 [STIG コンプライアンス(STIG Compliance)] をクリックします。

[STIG コンプライアンス(STIG Compliance)] ページが表示されます。

手順 4 STIG コンプライアンスをアプライアンスで永続的に有効にする場合は、[STIG コンプライアンスを有効化(Enable STIG Compliance)] を選択します。

**注意**

STIG コンプライアンスが有効なポリシーを適用した後、アプライアンスで STIG コンプライアンスを無効にすることはできません。コンプライアンスを無効にする必要がある場合は、サポートに連絡してください。

手順 5 [ポリシーを保存して終了(Save Policy and Exit)] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、[システム ポリシーの適用\(43-3 ページ\)](#)を参照してください。

STIG コンプライアンスを有効にするシステム ポリシーをアプライアンスに適用すると、アプライアンスが再起動するので注意してください。STIG が有効なシステム ポリシーをすでに STIG が有効になっているアプライアンスに適用した場合は、アプライアンスはリブートしないことに注意してください。

■ システム ポリシーの設定