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、次の項を参照してください。

システム ポリシーの作成

ライセンス: すべて

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。必要に合わせて、インポートされたポリシーを編集してから、それを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方法:

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy]の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 [Create Policy]をクリックします。

[Create Policy] ページが表示されます。

ステップ 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。

ステップ 4 新規ポリシーの名前を [New Policy Name]フィールドに入力します。

ステップ 5　新規ポリシーの説明を [New Policy Description]フィールドに入力します。

ステップ 6　[Create]をクリックします。

システム ポリシーが保存され、[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（42-5 ページ）
- メール リレー ホストおよび通知アドレスの設定（42-7 ページ）
- SNMP ポーリングの設定（42-8 ページ）
- STIG コンプライアンスの有効化（42-9 ページ）

システム ポリシーの編集

ライセンス: すべて

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（42-3 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方法:

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Local] > [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、[System Policy] ページが表示されます。

ステップ 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。

[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（42-5 ページ）
- メール リレー ホストおよび通知アドレスの設定（42-7 ページ）
- SNMP ポーリングの設定（42-8 ページ）
- STIG コンプライアンスの有効化（42-9 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（42-3 ページ）を参照してください。

ステップ 3　[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、[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:すべて

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方法:

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy]の順に選択します。

[System Policy] ページが表示されます。

ステップ 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。

ステップ 3　[Apply]をクリックします。

[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:すべて

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、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方法:

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy]の順に選択します。

[System Policy] ページが表示されます。

ステップ 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。

[System Policy] ページが表示されます。ポリシーを削除するかどうか確認するポップアップ 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:すべて

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(42-4 ページ)
- 監査ログの設定(42-5 ページ)
- メール リレー ホストおよび通知アドレスの設定(42-7 ページ)
- SNMP ポーリングの設定(42-8 ページ)
- STIG コンプライアンスの有効化(42-9 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：いずれか

[Access List] ページを使用して、特定のポートのアプライアンスにコンピュータがアクセスできるかを制御できます。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するポート 443（Hypertext Transfer Protocol Secure（HTTPS））、コマンドラインへのアクセスに使用するポート 22（Secure Shell（SSH））が任意の 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、デフォルトのオプション**すべて**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ことに注意してください。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（43-2 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。

アクセス： Admin

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy]の順に選択します。

[System Policy] ページが表示されます。

ステップ 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、[Create Policy]をクリックします。

  システム ポリシーの作成（42-1 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、[Save] をクリックします。

いずれの場合も、[Access List] ページが表示されます。

ステップ 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システムへのアクセスは失われます。

ステップ 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、[Add Rules]をクリックすることもできます。

[Add IP Address] ページが表示されます。

ステップ 5　[IP Address]フィールドでは、追加する IP アドレスに応じて以下の選択肢があります。

- 正確な 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 システムでの CIDR の使用方法の詳細については、IP アドレスの規則（1-4 ページ）を参照してください。
- `any`（任意の IP アドレスを指定）

ステップ 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。

ステップ 7　[Add]をクリックします。

[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。

ステップ 8　[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（42-3 ページ）」を参照してください。

監査ログの設定

ライセンス:すべて

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。

この機能が有効になっている状態でポリシーが適用され、宛先ホストが監査ログを受け入れるように設定された後で、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。

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。

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy]の順に選択します。

[System Policy] ページが表示されます。

ステップ 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、[Create Policy]をクリックします。

  システム ポリシーの作成（42-1 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、[Save] をクリックします。

ステップ 3　[Audit Log Settings]をクリックします。

[Audit Log Settings] ページが表示されます。

ステップ 4　[Send Audit Log to Syslog]ドロップダウン メニューから、[Enabled]を選択します。（デフォルト設定では [Disabled]になっています）。

ステップ 5　[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。

ステップ 6　[Facility]フィールドから syslog ファシリティを選択します。

ステップ 7　[Severity]フィールドから重大度を選択します。

ステップ 8　必要に応じて、[Tag (optional)]フィールドで参照タグを挿入します。

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

ステップ 10　[URL to Post Audit]フィールドに、監査情報を送信する 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`
- `result`
- `time`
- `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。

ステップ 11　[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（42-3 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:すべて

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 ホストとの間の通信に使用する暗号化方式を選択し、メール サーバの認証資格情報を指定できます(必要な場合)。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。

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy]の順に選択します。

[System Policy] ページが表示されます。

ステップ 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、[Create Policy]をクリックします。

  システム ポリシーの作成(42-1 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、[Save] をクリックします。

ステップ 3　[Email Notification]をクリックします。

[Configure Email Notification] ページが表示されます。

ステップ 4　[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。

ステップ 5　[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。

ステップ 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 サーバとの間の通信を暗号化するには、[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 サーバとの間の通信を暗号化するには、[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 サーバとの間の非暗号化通信を許可するには、[Encryption Method] ドロップダウン リストから [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。

ステップ 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、[From Address]フィールドに入力します。

ステップ 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ために、[Use Authentication]を選択します。[Username]フィールドにユーザ名を入力します。パスワードを[Password]フィールドに入力します。

ステップ 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、[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。

ステップ 10　[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（42-3 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：すべて

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）ポーリングを有効にできます。SNMP 機能では、SNMP プロトコルのバージョン 1、2、および 3 の使用がサポートされます。

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（42-4 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のある情報も含まれることに注意してください。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。

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy]の順に選択します。

[System Policy] ページが表示されます。

ステップ 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、[Create Policy]をクリックします。

  システム ポリシーの作成（42-1 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、[Create] をクリックします。

ステップ 3　アプライアンスをポーリングするために使用するコンピュータごとに SNMP アクセスをまだ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（42-4 ページ）を参照してください。

ステップ 4　[SNMP]をクリックします。

[SNMP] ページが表示されます。

ステップ 5　[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。

ステップ 6　次の選択肢があります。

- [Version 1]または [Version 2] を選択した場合、[Community String]フィールドに SNMP コミュニティ名を入力します。15に進みます。
- [Version 3]を選択した場合、[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。

ステップ 7　[Username]フィールドにユーザ名を入力します。

ステップ 8　[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。

ステップ 9　[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。

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

ステップ 11　使用するプライバシー プロトコルを [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 [None] を選択します。

ステップ 12　[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。

ステップ 13　[Privacy Password] フィールドのすぐ下にある [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。

ステップ 14　[Add] をクリックします。

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

ステップ 15　[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（42-3 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:すべて

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 に対する厳格なコンプライアンスは保証されません。

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、アプライアンスは強制的にリブートされることに注意してください。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、アプライアンスはリブートしません。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。シスコでは、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。

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy]の順に選択します。

[System Policy] ページが表示されます。

ステップ 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、[Create Policy]をクリックします。

  システム ポリシーの作成（42-1 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、[Save] をクリックします。

ステップ 3　[STIG Compliance]をクリックします。

[STIG Compliance] ページが表示されます。

ステップ 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、[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に、STIG コンプライアンスをアプライアンスで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。

ステップ 5　[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（42-3 ページ）」を参照してください。

アプライアンスに対して STIG コンプライアンスを有効にするシステム ポリシーを適用した場合、アプライアンスがリブートすることに注意してください。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。