システム ポリシーの管理

システム ポリシーを使用して、FireSIGHT システム アプライアンスで次のものを管理できます。

- アクセス コントロールの設定
- アプライアンスのアクセス リスト
- 監査ログ設定
- 認証プロファイル
- ダッシュボードの設定
- データベース イベント制限
- DNS キャッシュのプロパティ
- メール リレー ホストおよび通知アドレス
- 侵入ポリシーの変更のトラッキング
- 別の言語の指定
- カスタム ログイン バナー
- SNMP ポーリング設定
- 時刻の同期
- STIG コンプライアンス
- 防御センターからの時間の提供
- ユーザ インターフェイスとコマンド ライン インターフェイスのタイムアウト設定
- サーバのマッピングの脆弱性

システム ポリシーを使用して、展開内の他のアプライアンスで同じ可能性が高い防御センターの側面を制御できます。たとえば、ユーザがログインしたときに、アプライアンスで「No Unauthorized Use」メッセージを表示することが、組織のセキュリティ ポリシーで求められる場合があります。システム ポリシーを使用すると、防御センターのシステム ポリシーでログイン バナーを一度設定すれば、管理するすべてのデバイスにそのポリシーを適用できます。

また、防御センターで複数のシステム ポリシーを活用することもできます。たとえば、さまざまな状況で別々のメール リレー ホストを使用する場合や、さまざまなデータベース制限をテストする場合は、単一のポリシーを編集するのではなく、いくつかのシステム ポリシーを作成し、それらを切り替えることができます。

システム ポリシー（展開内で同じ可能性が高いアプライアンスの側面を制御する）をシステム設定（単一のアプライアンスに固有である可能性が高い）と比較します。詳細については、「アプライアンス設定の構成」（P.51-1）を参照してください。

注　システム ポリシーは Sourcefire Software for X-Series には適用**できません**。

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」（P.50-2）
- 「システム ポリシーの編集」（P.50-3）
- 「システム ポリシーの適用」（P.50-4）
- 「システム ポリシーの比較」（P.50-5）
- 「システム ポリシーの削除」（P.50-7）

システム ポリシーの作成

ライセンス：任意

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、別のアプライアンスからシステム ポリシーをエクスポートし、アプライアンスにインポートすることができます。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」（P.A-1）を参照してください。

システム ポリシーを作成する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

[Policy Name] 列には、システム ポリシーの説明が含まれます。[Applied to] 列は、そのポリシーが適用されているアプライアンスの数と、以前に適用されたポリシーが変更されており、再適用が必要な **out-of-date** アプライアンスの数を示します。

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。

- 「アプライアンスのアクセス リストの設定」（P.50-9）
- 「監査ログの設定」（P.50-11）
- 「認証プロファイルの設定」（P.50-12）
- 「ダッシュボードの設定」（P.50-14）

システム ポリシーの編集

ライセンス：任意

既存のシステム ポリシーを編集できます。アプライアンス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」（P.50-4）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：

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

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。

- 「アクセス コントロール ポリシー設定の構成」（P.50-8）
- 「アプライアンスのアクセス リストの設定」（P.50-9）
- 「監査ログの設定」（P.50-11）
- 「認証プロファイルの設定」（P.50-12）
- 「ダッシュボードの設定」（P.50-14）
- 「データベース イベント制限の設定」（P.50-15）
- 「DNS キャッシュ プロパティの設定」（P.50-17）
- 「メール リレー ホストおよび通知アドレスの設定」（P.50-19）
- 「侵入ポリシー設定の構成」（P.50-20）

- 「別の言語の指定」（P.50-21）
- 「カスタム ログイン バナーの追加」（P.50-22）
- 「SNMP ポーリングの設定」（P.50-23）
- 「時刻の同期」（P.50-26）
- 「防御センターからの時刻の提供」（P.50-28）
- 「ユーザ インターフェイスの設定」（P.50-29）
- 「サーバの脆弱性のマッピング」（P.50-30）

注　アプライアンス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」（P.50-4）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：任意

アプライアンスにシステム 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。

注　システム ポリシーは Sourcefire Software for X-Series には適用**できません**。

システム ポリシーを適用する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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。

[Apply] ページが表示されます。

ステップ 3　システム ポリシーを適用するアプライアンスを選択します。

ヒント　グループ、モデル、ヘルス ポリシー、または適用済みのシステム ポリシーごとにアプライアンスをソートできます。個々のアプライアンスまたはグループ全体を選択できます。

ステップ 4　[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 ポリシーの比較

ライセンス：任意

ユーザがアクセスできるシステム ポリシーに応じて、2 つのシステム ポリシーまたは同じシステム ポリシーの 2 つのリビジョンを比較できます。これにより、組織の規格のコンプライアンスや、システム パフォーマンスの最適化を目的として、ポリシー変更を確認することができます。アクティブなシステム ポリシーを別のポリシーと素早く比較する場合は、[Running Configuration] オプションを選択できます。比較後に PDF レポートを生成して、システム ポリシー間またはシステム ポリシーのリビジョン間の相違点を記録することもできます。

システム ポリシーまたはシステム ポリシーのリビジョンを比較するために使用できる 2 つのツールがあります。

- 比較ビューには、2 つのシステム ポリシー間またはシステム ポリシーのリビジョン間の相違点がサイドバイサイド形式で表示されます。各ポリシーまたはポリシー リビジョンの名前は、比較ビューの左右のタイトル バーに表示されます。

  これを使用して、Web インターフェイスで相違点を強調表示したまま、両方のポリシーのリビジョンを表示し移動することができます。

- 比較レポートでは、2 つのシステム ポリシー間またはシステム ポリシーのリビジョン間の相違点のレコードがシステム ポリシーと同様の形式（ただし、PDF 形式）で作成されます。

  これを使用して、ポリシーの比較の保存、コピー、出力、共有を行って、さらに検証することができます。

システム ポリシーの比較ビューの使用

ライセンス：任意

比較ビューには、両方のシステム ポリシーまたはポリシー リビジョンがサイドバイサイド形式で表示され、各ポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトル バーにある名前で識別されます。すべてのリビジョンについては、システム ポリシーの比較ビューのポリシー名の右側に、最後に修正が行われた時間と最後のユーザが表示されます。

2 つのシステム ポリシーまたはシステム ポリシーのリビジョンの相違点は次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーまたはポリシー リビジョンで違うことを意味します。違いは赤色のテキストで表示されます。
- 緑は、強調表示されている設定が一方のポリシーまたはポリシー リビジョンにあるものの、もう一方の設定にはないことを示します。

次の表に、実行できる操作を記載します。

表 50-1　システム ポリシーの比較ビューの操作

目的	操作
変更に個別にナビゲートする	タイトル バーの上の [Previous] または [Next] を選択します。 左側と右側の間にある二重矢印アイコン（ ）が移動し、表示している違いを示す [Difference] 番号が変わります。
新しいシステム ポリシーの比較ビューを生成する	[New Comparison] を選択します。 [Select Comparison] ウィンドウが表示されます。詳細については、システム ポリシーの比較レポートの使用を参照してください。
システム ポリシーの比較レポートを生成する	[Comparison Report] を選択します。 システム ポリシーの比較レポートは、システム ポリシーの比較ビューと同じ情報を含む PDF です。

システム ポリシーの比較レポートの使用

ライセンス：任意

システム ポリシーの比較レポートは、システム ポリシーの比較ビューで特定された、2 つのシステム ポリシー間または同じシステム ポリシーの 2 つのリビジョン間の相違点をすべて記録したものであり、PDF 形式で提供されます。このレポートを使用して、2 つのシステム ポリシーの設定の間の相違点をさらに調べ、その結果を保存して配信することができます。

システム ポリシーの比較レポートは、ユーザがアクセスできる任意のシステム ポリシーの比較ビューから生成できます。ユーザがシステム ポリシーに加えた変更は、変更を保存するまではシステム ポリシーの比較レポートに表示されません。

設定によっては、システム ポリシーの比較レポートに 1 つ以上のセクションを含めることができます。次のサンプル グラフィックには、システム ポリシーの比較レポートの [Policy Information]、[User Detection Settings]、[Time Synchronization] セクションが表示されており、両方のシステム ポリシー設定の各規則の設定がリストされています。それぞれのセクションで、同じ形式が使用され、同じレベルの詳細が提供されます。[Value A] 列と [Value B] 列は、比較ビューで設定したポリシーまたはポリシーのリビジョンであることに注意してください。

FireSIGHT システム上で同様の手順を使用して他のポリシー タイプを比較します。詳細については、以下を参照してください。

- 「2 つの侵入ポリシーの比較」（P.20-13）
- 「正常性ポリシーの比較」（P.55-35）

2 つのシステム ポリシーまたは同じポリシーの 2 つのリビジョンを比較する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[System Policy] ページが表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ポップアップ ウィンドウが表示されます。

ステップ 3　[Compare Against] ドロップダウン リストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。
- 同じポリシーの 2 つのリビジョンを比較するには、[Other Revision] を選択します。
- 別のポリシーと現在アクティブなポリシーを比較するには、[Running Configuration] を選択します。

ステップ 4　選択した比較タイプによっては、次の選択肢もあります。

- 異なる 2 つのポリシーを比較する場合、[Policy A] および [Policy B] ドロップダウン リストから比較するポリシーを選択します。
- 同じポリシーの 2 つのリビジョンを比較する場合は、[Policy] ドロップダウン リストからポリシーを選択してから、[Revision A] および [Revision B] ドロップダウン リストから比較するリビジョンを選択します。
- 実行中の設定を別のポリシーと比較する場合は、[Target/Running Configuration A] ドロップダウン リストから実行中の設定を選択し、[Policy B] ドロップダウン リストから他のポリシーを選択します。

ステップ 5　システム ポリシーの比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　システム ポリシーの比較レポートを生成するには、[Comparison Report] をクリックします。

システム ポリシーの比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

システム ポリシーの削除

ライセンス：任意

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：

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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：任意

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。

アクセス コントロール ポリシー設定の構成

ライセンス：Protection

ユーザがアクセス コントロール ポリシーでルールを追加または変更する場合、ルールのコメントの入力を要求するようにシステムを設定できます。これを使用して、ユーザのポリシーの変更の理由を追跡できます。アクセス コントロール ルールの変更に関するコメントを有効にした場合、ルールのコメントをオプションまたは必須に設定できます。システムは、ルールに対する新しい変更が保存されるたびに、ユーザにコメントを入力するようプロンプトを出します。

ユーザがルールを保存したときに、システムはルールのコメントの履歴にコメントを追加します。詳細については、「ルール コメントの追加」（P.21-38）を参照してください。

アクセス コントロール ポリシーのルール コメントの設定を構成する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 コントロール ポリシー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アクセス コントロール ポリシーの設定を行うには、[Create Policy] をクリックします。

  「システム ポリシーの作成」（P.50-2）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　[Access Control Preferences] をクリックします。

[Access Control Preferences] ページが表示されます。

ステップ 4　次の選択肢があります。

- ドロップダウン リストから [Disabled] を選択すると、ユーザはコメントを入力せずにアクセス コントロール ポリシーのルールを追加または変更できます。
- ドロップダウン リストから [Optional] を選択すると、アクセス コントロール ポリシーのルールに対する変更を保存するときに [Description of Changes (Optional)] ウィンドウが表示されます。これにより、ユーザはコメントの変更について記述することができます。
- ドロップダウン リストから [Required] を選択すると、アクセス コントロール ポリシーのルールに対する変更を保存するときに [Description of Changes (Required)] ウィンドウが表示されます。この場合、ユーザは変更を保存する前にコメントの変更について記述する必要があります。

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」（P.50-4）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

ライセンス：任意

[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、「データベースへのアクセスの有効化」（P.51-7）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　[System] > [Local] > [System Policy] を選択します。

[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」（P.50-2）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）

  FireSIGHT システムでの CIDR の使用方法の詳細については、「IP アドレスの表記法」（P.1-19）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」（P.50-4）を参照してください。

監査ログの設定

ライセンス：任意

アプライアンス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アプライアンス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。アプライアンスは、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。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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」（P.50-2）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　[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 ポリシーを防御センターと管理対象デバイスに適用するまで、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」（P.50-4）を参照してください。

認証プロファイルの設定

ライセンス：任意

通常、ユーザがアプライアンスにログインする際に、アプライアンスは、アプライアンスのローカル データベースに保存されているユーザ アカウントとユーザの資格情報を比較することによって、資格情報を検証します。ただし、外部認証サーバを参照する認証オブジェクトを作成する場合、システム ポリシーで適用することにより、ローカル データベースを使用せずに、防御センターまたは管理対象デバイスにログインしているユーザーをそのサーバに認証させることができます。

認証が有効になっているシステム ポリシーをアプライアンスに適用した場合、アプライアンスはユーザ資格情報を LDAP または RADIUS サーバ上のユーザに対して検証します。さらに、ユーザがローカルの内部認証を有効にしており、ユーザ資格情報が内部データベースにない場合、アプライアンスは一致する資格情報のセットがないか外部サーバを検査します。ユーザが複数のシステムで同じユーザ名を持っている場合、すべてのサーバですべてのパスワードが動作します。ただし、使用可能な外部認証サーバで認証が失敗した場合、アプライアンスはローカル データベースの検査に戻らないので注意してください。

認証を有効にすると、アカウントが外部で認証されている任意のユーザのデフォルトのユーザ ロールを設定できます。これらのロールを組み合わせることができる場合は、複数のロールを選択できます。たとえば、自社の [Network Security] グループのユーザのみを取得する認証プロファイルをセットアップした場合、デフォルトのユーザ ロールを設定して [Security Analyst] ロールを組み込み、ユーザが自分で追加のユーザ設定を行わなくても収集されたイベント データにアクセスできるようにすることが可能です。ただし、認証プロファイルがセキュリティ グループに加えて他のユーザのレコードを取得する場合、デフォルトのロールを未選択のままにしておきたい場合もあります。使用可能なユーザ ロールの詳細については、「ユーザ特権について」（P.48-4）を参照してください。

防御センターで LDAP 認証オブジェクトを作成する場合、フィルタ検索属性を設定して、LDAP サーバに対して正常に認証できるユーザのセットを指定できることに注意してください。詳細については、「LDAP 固有パラメータの設定」（P.48-18）を参照してください。

アクセス ロールが選択されていない場合、ユーザはログインできますが、どの機能にもアクセスできません。ユーザがログインを試行すると、アカウントが [User Management] ページに表示されます。ここで、追加の権限を付与するアカウント設定を編集できます。ユーザ アカウントの変更の詳細については、「ユーザ特権とオプションの変更」（P.48-58）を参照してください。外部で認証されたユーザとして初めてログインする場合の完全な手順については、「アカウントを設定するためのアプライアンスへのログイン」（P.2-4）を参照してください。

1 つのユーザ ロールを使用するようにシステム ポリシーを設定してそのポリシーを適用し、後でポリシーを変更して別のデフォルトのユーザ ロールを使用し再適用する場合、アカウントを変更するか、削除して再作成するまで、変更前に作成されたユーザ アカウントはすべて、最初のユーザ ロールを保持します。

ユーザは認証を防御センターのシステム ポリシーで有効にしてから、そのポリシーを管理対象デバイスにプッシュする必要があります。デバイスにポリシーを適用した後、外部で認証された対象ユーザはそのデバイスにログインできます。認証プロファイルの設定を変更するには、防御センターでシステム ポリシーを変更してから、そのポリシーをデバイスに再度適用する必要があります。管理対象デバイスでの認証を無効にするには、防御センターのシステム ポリシーでそれを無効にし、デバイスにプッシュすることができます。

外部認証を有効にできるのは、物理および外部防御センターおよび管理対象デバイスのみであることに注意してください。システム ポリシーの適用による外部認証の有効化は、X-Series ベースのソフトウェア デバイスではサポートされません。

内部認証によってユーザがログインしようとすると、アプライアンスは最初にそのユーザがローカル ユーザ データベースに存在するかどうか検査します。ユーザが存在する場合、アプライアンスは次にユーザ名とパスワードをローカル データベースに対して検査します。一致が検出されると、ユーザは正常にログインします。ただし、ログインが失敗し、外部認証が有効になっている場合、アプライアンスはそれぞれの外部認証サーバに対して、ユーザをシステム ポリシーに表示される認証順序で検査します。ユーザ名およびパスワードが外部サーバからの結果と一致した場合、アプライアンスはユーザを、その認証オブジェクトに対してデフォルトの権限を持つ外部ユーザに変更します。

外部ユーザがログインしようとすると、アプライアンスは外部認証サーバに対してユーザ名およびパスワードを検査します。一致が検出されると、ユーザは正常にログインします。ログインが失敗した場合、ユーザのログイン試行は拒否されます。外部ユーザは、ローカル データベース内のユーザ リストに対して認証できません。ユーザが新しい外部ユーザの場合、外部認証オブジェクトのデフォルト権限を持つ外部ユーザ アカウントがローカル データベースに作成されます。

外部サーバでのユーザ認証を有効にする方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 ポリシーの認証プロファイ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。
- 新規のシステム ポリシーの認証プロファイ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」（P.50-2）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　[Authentication Profiles] をクリックします。

[Authentication Profiles] ページが表示されます。

ステップ 4　[Status] ドロップダウン リストから [Enabled] を選択します。

ステップ 5　[Default User Role] ドロップダウン リストから、ユーザ ロールを選択して、外部認証済みユーザに付与するデフォルト権限を定義します。

ヒント　ロールを選択する前に Ctrl キーを押すと、複数のデフォルト ユーザ ロールを選択できます。[Security Analyst] ロールと対応する [Security Analyst（Read Only）] ロールの両方を選択した場合でも、適用されるのは [Security Analyst] ロールだけであることに注意してください。

ステップ 6　外部サーバを使用してシェル アクセス アカウントも認証する場合、[Shell Authentication] ドロップダウン リストから [Enabled] を選択します。

ステップ 7　[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 ポリシーを防御センターと管理対象デバイスに適用するまで、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」（P.50-4）を参照してください。

ダッシュボードの設定

ライセンス：任意

[Custom Analysis] ウィジェットがダッシュボードで有効になるように、システム ポリシーを設定できます。ダッシュボードでは、ウィジェットを使用することにより、現在のシステム ステータスが一目でわかります。ウィジェットは小さな内蔵コンポーネントであり、FireSIGHT システムのさまざまな側面に関するインサイトを提供します。

[Custom Analysis] ウィジェットを使用して、柔軟でユーザが設定可能なイベントのクエリに基づいて、アプライアンスのデータベースにイベントを視覚的に作成することができます。カスタム ウィジェットの使用方法の詳細については、「Custom Analysis ウィジェットについて」（P.3-12）を参照してください。

[Custom Analysis] ウィジェットを有効にする方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 ポリシーのダッシュボード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ダッシュボードの設定を行うには、[Create Policy] をクリックします。「システム ポリシーの作成」（P.50-2）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　[Dashboard] をクリックします。

[Dashboard Settings] ページが表示されます。

ステップ 4　ユーザが [Custom Analysis] ウィジェットをダッシュボードに追加できるようにするには、[Enable Custom Analysis Widgets] チェック ボックスを選択します。ユーザがこれらのウィジェットを使用できないようにする場合は、このチェック ボックスをオフにします。

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」（P.50-4）を参照してください。

データベース イベント制限の設定

ライセンス：任意

[Database] ページを使用して、防御センターが保存できる各イベント タイプの最大数を指定します。監査レコードの設定は、管理対象デバイスにも適用されることに注意してください。パフォーマンスを向上させるには、定期的に処理するイベント数に合わせてイベント制限を調整する必要があります。一部のイベント タイプでは、ストレージを無効にすることができます。次の表は、各イベント タイプを保存できる最小および最大レコード数を示しています。

表 50-2　データベース イベントの制限

イベント タイプ	イベントの上限	イベントの下限
侵入イベント	250 万（DC500） 1,000 万（DC1000、仮想 防御センター） 2,000 万（DC750） 3,000 万（DC1500） 1 億（DC3000） 1 億 5,000 万（DC3500）	10,000
検出イベント	1,000 万	ゼロ（ストレージを無効にする）

表 50-2　データベース イベントの制限（続き）

イベント タイプ	イベントの上限	イベントの下限
接続イベント/セキュリティ インテリジェンス イベント	1,000 万（DC500、DC1000、仮想防御センター） 5,000 万（DC750） 1 億（DC1500、DC3000） 5 億（DC3500） イベントの上限は、接続イベントとセキュリティ インテリジェンス イベントとの間で共有されます。2 つのイベントの設定済み最大数の合計はイベントの上限数を超えてはなりません。	ゼロ（ストレージを無効にする）
接続の要約（集約された接続イベント）	1,000 万（DC500、DC1000、仮想防御センター） 5,000 万（DC750） 1 億（DC1500、DC3000） 5 億（DC3500）	ゼロ（ストレージを無効にする）
相関およびコンプライアンスのホワイト リスト イベント	100 万	1
マルウェア イベント	1,000 万	10,000
ファイル イベント	1,000 万	ゼロ（ストレージを無効にする）
ヘルス イベント	100 万	ゼロ（ストレージを無効にする）
監査レコード	100,000	1
修復ステータス イベント	1,000 万	1
ネットワーク上のホストのホワイト リスト違反履歴	30 日間の違反履歴	1 日の履歴
ユーザ アクティビティ（ユーザ イベント）	1,000 万	1
ユーザ ログイン（ユーザ履歴）	1,000 万	1
ルール更新のインポート ログ レコード	100 万	1

侵入イベント データベース内のイベント数が最大数を超えると、データベースがイベントの制限内に戻るまで、最も古いイベントおよびパケット ファイルがプルーニングされます。イベントが自動的にプルーニングされたときに自動電子メール通知を生成する方法については、「メール リレー ホストおよび通知アドレスの設定」（P.50-19）を参照してください。

検出およびユーザ データベースを手動でプルーニングする方法の詳細については、「データベースからの検出データの消去」（P.B-1）を参照してください。

さらに、侵入イベントおよび監査レコードがデータベースからプルーニングされたときに通知を受け取る電子メール アドレスを設定できます。

データベース内のレコードの最大数を設定する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 ポリシーのデータベース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データベースの設定を行うには、[Create Policy] をクリックします。

  「システム ポリシーの作成」（P.50-2）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 Control Preferences] ページが表示されます。

ステップ 3　[Database] をクリックします。

[Database] ページが表示されます。

ステップ 4　各データベースについて、保存するレコードの数を入力します。

各データベースが保持できるレコード数の詳細については、「データベース イベントの制限」を参照してください。

ステップ 5　必要に応じて、[Data Pruning Notification Address] フィールドで、侵入イベント、検出イベント、監査レコード、セキュリティ インテリジェンス データ、または URL フィルタリング データがアプライアンスのデータベースからプルーニングされたときに通知を受け取る電子メール アドレスを入力します。

また、電子メール サーバを設定する必要があることにも注意してください。詳細については、「メール リレー ホストおよび通知アドレスの設定」（P.50-19）を参照してください。

ステップ 6　[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」（P.50-4）を参照してください。

DNS キャッシュ プロパティの設定

ライセンス：任意

DNS サーバが [Network] ページで設定されている場合、イベント ビュー ページで IP アドレスを自動的に解決するようにアプライアンスを設定できます。[Administrator] ロールが割り当てられたユーザは、アプライアンスによって実行される DNS キャッシングの基本プロパティも設定できます。DNS キャッシングを設定すると、追加のルックアップを実行せずに、以前に解決した IP アドレスを識別できます。これにより、IP アドレスの解決が有効になっている場合に、ネットワーク上のトラフィックの量を減らし、イベント ページの表示速度を早めることができます。

DNS キャッシュ プロパティを構成するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 DNS キャッシュ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 DNS キャッシュの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」（P.50-2）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　[DNS Cache] をクリックします。

[DNS Cache] ページが表示されます。

ステップ 4　キャッシングを有効にするには、[DNS Resolution Caching] ドロップダウン リストから [Enabled] を選択します。これを無効にするには、[Disabled] を選択します。

注　DNS 解決のキャッシングは、以前に解決された DNS ルックアップのキャッシングを許可するシステム全体の設定です。ユーザ アカウントごとに IP アドレス解決を設定するには、ユーザは [User Preferences] メニューから [Event View Settings] も選択し、[Resolve IP Addresses] を有効にしてから [Save] をクリックする必要があります。DNS サーバの設定の詳細については、「ネットワーク設定の構成」（P.51-9）を参照してください。イベント ビューの設定については、「イベント ビュー設定の設定」（P.58-3）を参照してください。

ステップ 5　[DNS Cache Timeout（in minutes）] フィールドで、非アクティブのために削除されるまで DNS エントリがメモリ内にキャッシュされる時間（分単位）を入力します。

デフォルトは 300 分（5 時間）です。

ステップ 6　[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」（P.50-4）を参照してください。

注意　DNS キャッシングがアプライアンスで有効になっている場合でも、[User Preferences] メニューからアクセスできる [Events] ページで設定されていなければ、ユーザごとの IP アドレス解決は有効になりません。

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

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
- ディスカバリ イベント、影響フラグ、および相関イベント アラートについての電子メールの使用
- 侵入イベント アラートについての電子メールの使用
- ヘルス 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。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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」（P.50-2）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　[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」（P.50-4）を参照してください。

侵入ポリシー設定の構成

ライセンス：Protection

侵入ポリシーを変更する場合に、コメントの入力を要求するようシステムを設定できます。これを使用して、ユーザのポリシーの変更の理由を追跡できます。侵入ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。変更に関する説明が監査ログに書き込まれます。

侵入ポリシーのすべての変更を監査ログに書き込むこともできます。監査ログの詳細については、「監査レコードの管理」（P.56-1）を参照してください。

侵入ポリシーのコメントの設定を行うには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 ポリシーの侵入ポリシー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侵入ポリシーの設定を行うには、[Create Policy] をクリックします。

「システム ポリシーの作成」（P.50-2）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　[Intrusion Policy Preferences] をクリックします。

[Intrusion Policy Preferences] ページが表示されます。

ステップ 4　[Comments on policy change] ドロップダウン リストには、次のオプションがあります。

- [Disabled] を選択すると、変更に関する説明を入力せずに侵入ポリシーを変更できます。
- [Optional] を選択すると、侵入ポリシーに対する変更を保存するときに [Description of Changes] ウィンドウが表示されます。これにより、ユーザはコメントの変更について記述することができます。
- [Required] を選択すると、侵入ポリシーに対する変更を保存するときに [Description of Changes] ウィンドウが表示されます。この場合、ユーザは変更を保存する前にコメントの変更について記述する必要があります。

ステップ 5　必要に応じて、侵入ポリシーのすべての変更を監査ログに書き込むには、[Write changes in Intrusion Policy to audit log] を選択します。

ステップ 6　[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」（P.50-4）を参照してください。

別の言語の指定

ライセンス：任意

[Language] ページを使用して、Web インターフェイス用に異なる言語を指定できます。

注意　ここで選択した言語は、アプライアンスにログインしたすべてのユーザの Web インターフェイスに使用されます。

ユーザ インターフェイスに異なる言語を選択する方法：

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 ポリシーの言語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言語の設定を行うには、[Create Policy] をクリックします。

  「システム ポリシーの作成」（P.50-2）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　[Language] をクリックします。

[Language] ページが表示されます。

ステップ 4　使用する言語を選択します。

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」（P.50-4）を参照してください。

カスタム ログイン バナーの追加

ライセンス：任意

SSH を使用してアプライアンスにログインしたときに、Web インターフェイスのログイン ページに表示されるカスタム ログイン バナーを作成できます。バナーには、小なり記号（<）および大なり記号（>）以外の出力可能な文字を含めることができます。

カスタム バナーを追加するには、次の手順に従ってください。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 ポリシーのログイン バナーを変更するには、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ログイン バナーの設定を行うには、[Create Policy] をクリックします。

  「システム ポリシーの作成」（P.50-2）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　[Login Banner] をクリックします。

[Login Banner] ページが表示されます。

ステップ 4　[Custom Login Banner] フィールドに、このシステム ポリシーで使用するログイン バナーを入力します。

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」（P.50-4）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

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。

この機能を使用して、次のものにアクセスできます。

- アプライアンスの標準 Management Information Base（MIB）。これには、連絡先、管理、場所、サービス情報、IP アドレッシングやルーティングの情報、およびトランスミッション プロトコルの使用状況の統計などのシステムの詳細が含まれます。
- 管理対象デバイスの追加の MIB。これには、物理インターフェイス、論理インターフェイス、仮想インターフェイス、ARP、NDP、仮想ブリッジ、および仮想ルータを通して渡されるトラフィックの統計が含まれます。

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」（P.50-9）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。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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」（P.50-2）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。

いずれの場合も、[Access List] ページが表示されます。

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」（P.50-9）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。手順 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」（P.50-4）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

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。

展開内の任意のアプライアンスで STIG コンプライアンスを有効にする場合は、それをすべてのアプライアンスで有効にする必要があります。非準拠の管理対象デバイスを STIG 準拠の防御センターに登録したり、STIG 準拠デバイスを非準拠の防御センターに登録したりすることはできません。

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。製品のこのバージョンでこのモードを使用する場合、FireSIGHT システム STIG コンプライアンスの詳細については、サポートに問い合わせて、バージョン 5.3.1 用の FireSIGHT システム STIG リリース ノートのコピーを入手してください。

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。これらの設定の詳細については、バージョン 5.3.1 用の FireSIGHT システム STIG リリース ノートを参照してください。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。

バージョン 5.2.0 よりも前のバージョンからアップグレードしたアプライアンスの場合、コンプライアンスを有効にしたままポリシーを適用してもアプライアンス証明書が再生成されるため、すでに登録されている管理対象デバイスまたはピアを再登録する必要があります。

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。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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」（P.50-2）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　[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」（P.50-4）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。

また、デバイスがバージョン 5.2.0 よりも前のバージョンからアップグレードされた場合、STIG コンプライアンスを有効にした後でデバイスを再登録する必要があります。

時刻の同期

ライセンス：任意

[Time Synchronization] ページを使用して、アプライアンスで時刻の同期を管理できます。時刻を同期する場合、以下の方法を選択できます。

- 手動
- 1 つまたは複数の NTP サーバを使用（そのうちの 1 つは防御センターに指定できる）

時刻の設定は、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、既存のポリシーを編集することによって、時刻の設定を指定できます。いずれの場合も、システム ポリシーを適用するまで時刻の設定は使用されません。

アプライアンスの大半のページでは、時刻の設定は [Time Zone] ページ（デフォルトでは米国/ニューヨーク）で設定したタイム ゾーンを使用してローカル時刻で表示されますが、アプライアンス自体には UTC 時間を使用して保存されることに注意してください。さらに、現在の時刻は [Time Synchronization] ページの上部に UTC で表示されます（ローカル時刻は手動時計設定オプションで表示されます（有効になっている場合））。

Sourcefire Software for X-Series の時刻設定を管理するには、コマンドライン インターフェイスまたはオペレーティング システム インターフェイスなどのネイティブ アプリケーションを使用する必要があります。Sourcefire Software for X-Series とそれが管理する防御センターの時刻は、同じ物理アプライアンスまたは NTP サーバから同期します。詳細については、シスコ『*Software for X-Series Installation Guide*』を参照してください。

アプライアンスの時刻は、外部タイム サーバと同期できます。リモート NTP サーバを指定した場合、アプライアンスはそれに対するネットワーク アクセス権限を持っている必要があります。信頼できない NTP サーバを指定しないでください。NTP サーバへの接続では、構成されたプロキシ設定は使用されません。NTP サーバとして防御センターを使用するには、「防御センターからの時刻の提供」（P.50-28）を参照してください。

シスコでは、仮想アプライアンスを物理 NTP サーバと同期することを推奨します。管理対象デバイス（仮想または物理）と仮想防御センターを同期しないでください。

注　時刻の同期後に、防御センターと管理対象デバイスの時刻が一致していることを確認します。そうしないと、管理対象デバイスが防御センターと通信する場合に意図しない結果が発生することがあります。

時刻を同期する手順は、防御センターか管理対象デバイスのどちらの Web インターフェイスを使用するかによって若干異なります。各手順については後で個別に説明します。

時刻を同期するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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」（P.50-2）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　[Time Synchronization] をクリックします。

[Time Synchronization] ページが表示されます。

ステップ 4　防御センターから管理対象デバイスに時刻を提供する場合は、[Serve time via NTP] ドロップダウン リストで [Enabled] を選択します。

ステップ 5　防御センターで時刻を同期する方法を指定するには、次のオプションがあります。

- 時刻を手動で設定するには、[Manually in Local Configuration] を選択します。システム ポリシーを適用した後の時刻の設定については、「手動での時間の設定」（P.51-13）を参照してください。
- NTP を介して別のサーバから時刻を受信するには、[Via NTP from] を選択し、使用する NTP サーバの IP アドレスのコンマ区切りリストをテキスト ボックスに入力するか、DNS が無効になっている場合は、完全修飾ホストおよびドメインの名前を入力します。

注意　アプライアンスがリブートされ、ここで指定したものとは異なる NTP サーバ レコードを DHCP サーバが設定した場合、DHCP 提供の NTP サーバが代わりに使用されます。この状況を回避するには、同じ NTP サーバを設定するように DHCP サーバを設定します。

ステップ 6　任意の管理対象デバイスで時刻を同期する方法を指定するには、次のオプションがあります。

- 時刻を手動で設定するには、[Manually in Local Configuration] を選択します。システム ポリシーを適用した後の時刻の設定については、「手動での時間の設定」（P.51-13）を参照してください。
- NTP を介して防御センターから時刻を受信するには、[Via NTP from Defense Center] を選択します。詳細については、「防御センターからの時刻の提供」（P.50-28）を参照してください。
- NTP を介して別のサーバから時刻を受信するには、[Via NTP from] を選択します。。テキスト ボックスで、NTP サーバの IP アドレスのコンマ区切りリストを入力するか、DNS が無効になっている場合は、完全修飾ホストおよびドメインの名前を入力します。

注　管理対象デバイスを設定された NTP サーバと同期するには、数分かかる場合があります。さらに、管理対象デバイスを NTP サーバとして設定されている防御センターと同期する場合、防御センター自体が NTP サーバを使用するように設定されていると、時刻を同期するのにいくらか時間がかかることがあります。これは、管理対象デバイスに時刻を提供するために、防御センターは設定された NTP サーバとまず同期する必要があるためです。

ステップ 7　[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」（P.50-4）を参照してください。

防御センターからの時刻の提供

ライセンス：任意

NTP を使用して防御センターをタイム サーバとして設定してから、それを使用して防御センターと管理対象デバイスの間で時刻を同期することができます。

NTP を使用して時刻を提供するように防御センターを設定した後は、時刻を手動で設定できないことに注意してください。時刻を手動で変更する必要がある場合は、NTP を使用して時刻を提供するよう防御センターを設定する**前に**、その変更を行う必要があります。防御センターを NTP サーバとして設定した**後に**、時刻を手動で変更する必要がある場合は、[Via NTP] オプションを無効にして [Save] をクリックし、時刻を手動で変更して [Save] をクリックしてから、[Via NTP] を有効にして [Save] をクリックします。

注　NTP を使用して時刻を提供するよう防御センターを設定してから、後でそれを無効にした場合、管理対象デバイスの NTP サービスは引き続き防御センターと時刻を同期しようとします。同期の試行を停止するには、NTP を管理対象デバイスの Web インターフェイスから無効にする必要があります。

NTP サーバとして防御センターを設定するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 NTP サーバ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 NTP サーバの設定を行うには、[Create Policy] をクリックします。

  「システム ポリシーの作成」（P.50-2）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　[Time Synchronization] をクリックします。

[Time Synchronization] ページが表示されます。

ステップ 4　[Serve Time via NTP] ドロップダウン リストから [Enabled] を選択します。

ステップ 5　管理対象デバイスの [Set My Clock] オプションで、[Via NTP from Defense Center] を選択します。

ステップ 6　[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 ポリシーを防御センターと管理対象デバイスに適用するまで、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」（P.50-4）を参照してください。

注　防御センターを管理対象デバイスと同期するには、数分かかる場合があります。

ユーザ インターフェイスの設定

ライセンス：任意

FireSIGHT システムの Web インターフェイスまたはコマンドライン インターフェイスの無人ログイン セッションは、セキュリティ上のリスクを生じさせる場合があります。非アクティブが原因でユーザのログイン セッションがタイムアウトになるまでのアイドル時間を分単位で設定できます。シェル（コマンドライン）セッションでも同様のタイムアウトを設定できます。

長期にわたり Web インターフェイスに対してセキュアにパッシブな監視を行う予定のユーザが、展開内に存在する可能性があります。ユーザ設定オプションで Web インターフェイスのセッション タイムアウトからユーザを除外することができます。（メニュー オプションへの完全なアクセスを持つ [Administrator] ロールのユーザは、侵害が生じる場合、余分のリスクを生じさせますが、セッション タイムアウトから除外することはできません。）詳細については、「ユーザ ログイン設定の管理」（P.48-50）を参照してください。

システムへのシェル アクセスを制限する必要がある場合、3 番目のオプションによってコマンドラインの expert コマンドを永続的に無効にすることができます。アプライアンスでエキスパート モードを無効にすると、設定シェル アクセスを持つユーザーでも、シェルのエキスパート モードに入ることができなくなります。ユーザがコマンドラインのエキスパート モードに入ると、ユーザはシェルに応じた任意の Linux コマンドを実行できます。エキスパート モードに入っていない場合は、コマンド ライン ユーザはコマンドライン インターフェイスが提供するコマンドだけを実行できます。コマンドライン インターフェイスは、シリーズ 2 アプライアンスではサポートされていないことに注意してください。

コマンドライン インターフェイス コマンドの詳細については、「コマンドライン リファレンス」（P.D-1）を参照してください。コマンドライン アクセス用にユーザを設定する方法の詳細については、「コマンド ライン アクセスの管理」（P.48-48）および 「コマンドライン リファレンス」（P.D-1）（仮想デバイスの CLI ユーザ管理用）を参照してください。

ユーザ インターフェイスの設定を行うには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 ポリシーのユーザ インターフェイス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ユーザ インターフェイスの設定を行うには、[Create Policy] をクリックします。

  「システム ポリシーの作成」（P.50-2）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　[User Interface] をクリックします。

[User Interface] ページが表示されます。

ステップ 4　次の選択肢があります。

- Web インターフェイスのセッション タイムアウトを設定するには、[Browser Session Timeout（Minutes）] フィールドに数値（分数）を入力します。デフォルトの値は 60 で、最大値は 1440（24 時間）です。

  このセッション タイムアウトからユーザを除外する方法については、「ユーザ ログイン設定の管理」（P.48-50）を参照してください。
- コマンドライン インターフェイスのセッション タイムアウトを設定するには、[Shell Timeout（Minutes）] フィールドに数値（分数）を入力します。デフォルトの値は 0 で、最大値は 1440（24 時間）です。
- コマンドライン インターフェイスで expert コマンドを永続的に無効にするには、[Permanently Disable Expert Access] チェック ボックスを選択します。

注意　エキスパート モードが無効になった状態でシステム ポリシーをアプライアンスに適用した場合、Web インターフェイスまたはコマンドラインを介してエキスパート モードにアクセスする機能を復元することはできません。エキスパート モード機能を復元するには、サポートに問い合わせる必要があります。

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 ポリシーを防御センターと管理対象デバイスに適用するまで、変更は有効になりません。セッション タイムアウト間隔の変更は、次回のログイン セッションまでは有効になりません。

サーバの脆弱性のマッピング

ライセンス：Protection

サーバのディスカバリ イベント データベースにアプリケーション ID が含まれており、トラフィックのパケット ヘッダにベンダーおよびバージョンが含まれる場合、FireSIGHT システムは、そのアドレスから送受信されるすべてのアプリケーション プロトコル トラフィックについて、脆弱性をホスト IP アドレスに自動的にマップします。

ただし、多くのサーバには、ベンダーとバージョンの情報が含まれていません。システム ポリシーにリストされているサーバの場合、システムが脆弱性をベンダーとバージョンがないサーバのサーバ トラフィックに関連付けるかどうかを設定できます。

たとえば、ホストが見出しにベンダーまたはバージョンが含まれていない SMTP トラフィックを提供するとします。システム ポリシーの [Vulnerability Mapping] ページで SMTP サーバを有効にしてから、トラフィックを検出するデバイスを管理する防御センターにそのポリシーを適用した場合、SMTP サーバと関連付けられたすべての脆弱性がホストのホスト プロファイルに追加されます。

ディテクタがサーバ情報を収集し、それをホスト プロファイルに追加した場合、アプリケーション プロトコル ディテクタは脆弱性のマッピングに使用されません。これは、カスタム アプリケーション プロトコル ディテクタのベンダーまたはバージョンを指定できず、システム ポリシーで脆弱性のマッピングのためにサーバを選択できないためです。

サーバの脆弱性のマッピングを設定するには、次の手順を実行します。

アクセス：Admin

ステップ 1　[System] > [Local] > [System Policy] を選択します。

[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 ポリシーの脆弱性マッピ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脆弱性マッピ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」（P.50-2）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　[Vulnerability Mapping] をクリックします。

[Vulnerability Mapping] ページが表示されます。

ステップ 4　次の選択肢があります。

- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされないようにするには、そのサーバのチェック ボックスをオフにします。
- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされるようにするには、そのサーバのチェック ボックスをオンにします。

ヒント　[Enabled] の横にあるチェック ボックスを使用して、一度にすべてのチェック ボックスをオンまたはオフにすることができます。

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 ポリシーを防御センターと管理対象デバイスに適用するまで、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」（P.50-4）を参照してください。