



## FireSIGHT システムへのログイン

この章では、FireSIGHT システムへのログインおよびログアウトのために、アプライアンスベースの Web インターフェイスおよびコマンドライン インターフェイス (CLI) を使用して実行する必要のある手順について詳細を示します。また、LDAP または RADIUS クレデンシャルを使用する外部で認証されるユーザ アカウントを設定することもできます。

Web インターフェイスにログインした後、特定の領域の上にポインタを置くと、コンテキストメニューの機能によって追加情報および有益なナビゲーションリンクが提供されます。

詳細については、次の項を参照してください。

- 「アプライアンスへのログイン」 (P.2-1)
- 「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)
- 「アプライアンスからのログアウト」 (P.2-5)
- 「コンテキストメニューの使用」 (P.2-6)

## アプライアンスへのログイン

ライセンス：任意

FireSIGHT システム防御センターには、管理および分析タスクを実行するために使用できる Web インターフェイスがあります。物理管理対象デバイスにも、初期セットアップ、基本的な分析と設定タスクを実行するために使用できる Web インターフェイスがあります。ブラウザ要件の詳細については、このバージョンの FireSIGHT システムのリリース ノートを参照してください。

仮想管理対象デバイスには、Web インターフェイスがありません。これらのデバイス（シリーズ 3 デバイスも同様）では、デバイスの管理防御センターを使用して完了できないすべてのタスクを実行するために使用できるインタラクティブ CLI が FireSIGHT システムによって提供されます。

Sourcefire Software for X-Series にも Web インターフェイスはありません。ただし、X-Series プラットフォームに固有の CLI があります。この CLI を使用して、システムをインストールしたり、その他のプラットフォーム固有の管理タスクを実行したりします。X-Series プラットフォーム CLI へのログイン方法を含む詳細については、『*Sourcefire Software for X-Series Installation and Configuration Guide*』を参照してください。

ASA FirePOWER デバイスには、独自の管理アプリケーション (ASDM と CSM) と ASA デバイスを設定するための CLI があります。また、FireSIGHT システムでは、デバイスの管理防御センターで実行できないタスクを実行するために使用できるインタラクティブ CLI が提供されます。ASA 固有のツールを使用して、システムをインストールしたり、その他のプラットフォーム固有の管理タスクを実行したりします。詳細については、ASA のマニュアルを参照してください。



注

FirePOWER アプライアンスはユーザ アカウントに基づいてユーザ アクティビティを監査するため、ユーザが正しいアカウントでシステムにログインしていることを確認してください。



注意

ユーザ名とパスワードを入力して、アプライアンスの Web インターフェイス、CLI、またはシェルへのアクセスを取得する必要があります。アプライアンスにログインすると、アクセスできる機能はユーザ アカウントに付与されている特権によって制御されます。クレデンシャルを間違えて複数回指定すると、シェル アクセス アカウントがロックされることがあります。正しいクレデンシャルを入力してもログインが拒否される場合、ログインを繰り返し試行せずに、システム管理者に連絡してください。

Web セッション中に初めてアプライアンスのホーム ページにアクセスする際、そのアプライアンスでの前回のログインセッションに関する情報を表示できます。前回のログインに関する以下の情報を表示できます。

- ログインの曜日、月、日、年
- 24 時間表記でのログインのアプライアンス ローカル時刻
- アプライアンスにアクセスするため最後に使用されたホストおよびドメイン名

セッション タイムアウトが適用されないように設定しない限り、デフォルトでは、非アクティブな状態が 1 時間続くとセッションは自動的にログアウトします。管理者ロールを持つユーザは、システム ポリシーのセッション タイムアウト間隔を変更できます。詳細については、「[ユーザ ログイン設定の管理](#)」(P.48-50) および「[ユーザ インターフェイスの設定](#)」(P.50-29) を参照してください。

かなり多くの時間がかかる一部のプロセスでは、Web ブラウザに、スクリプトが応答不能になったことを示すメッセージが表示されることがあります。このメッセージが表示された場合は、スクリプトが完了するまで続行させます。



注

アプライアンスにシステムを新規インストール (新規または再イメージング) する場合、管理 (admin) ユーザ アカウントを使用してログインし、初期セットアップ プロセスを完了する必要があります。『[FireSIGHT System Installation Guide](#)』を参照してください。「[新しいユーザ アカウントの追加](#)」(P.48-46) の説明に従って他のユーザ アカウントを作成した後は、そのユーザも他のユーザもそれらのアカウントを使用して Web インターフェイスにログインする必要があります。

**Web インターフェイスを介して、アプライアンスにログインする方法：**

アクセス：Any

- 
- ステップ 1** ブラウザで `https://hostname/` にアクセスします。ここで、`hostname` はアプライアンスのホスト名です。
- [Login] ページが表示されます。
- ステップ 2** [Username] および [Password] フィールドにユーザ名とパスワードを入力します。ユーザ名は、大文字と小文字が区別されます。
- ログイン時に SecurID® トークンが使用される場合、SecurID PIN にトークンを付加し、ログインするためのパスワードとして使用します。たとえば、PIN が 1111 で、SecurID トークンが 222222 である場合、1111222222 と入力します。FireSIGHT システムにログインする前に、SecurID PIN を生成しておく必要があります。
- ステップ 3** [Login] をクリックします。
- デフォルトの開始ページが表示されます。ユーザアカウントにカスタム ホーム ページを選択した場合、そのページが代わりに表示されます。詳細については、「[ホーム ページの指定](#)」(P.58-3) を参照してください。
- ページの上部に表示されるメニューおよびメニュー オプションは、自分のユーザアカウントの特権に基づきます。ただし、デフォルト ホーム ページのリンクには、ユーザアカウントの特権の範囲全体にわたるオプションが含まれます。アカウントに付与された特権とは異なる特権を必要とするリンクをクリックした場合、次の警告メッセージが表示されます。
- You are attempting to view an unauthorized page.This activity has been logged.  
選択可能なメニューから別のオプションを選択するか、またはブラウザ ウィンドウで [Back] をクリックして。
- 

**コマンドライン経由でシリーズ 3、仮想デバイス、または ASA FirePOWER にログインする方法：**

アクセス：CLI 基本設定

- 
- ステップ 1** シリーズ 3 および仮想デバイスの場合、`hostname` でアプライアンスへの SSH 接続を開きます。ここで、`hostname` はアプライアンスのホスト名です。ASA FirePOWER デバイスの場合、管理アドレスで ASA FirePOWER モジュールへの SSH 接続を開きます。
- [login as:] コマンド プロンプトが表示されます。
- ステップ 2** ユーザー名を入力し、Enter キーを押します。
- [Password:] プロンプトが表示されます。
- ステップ 3** パスワードを入力し、Enter キーを押します。
- ログイン時に SecurID® トークンが使用される場合、SecurID PIN にトークンを付加し、ログインするためのパスワードとして使用します。たとえば、PIN が 1111 で、SecurID トークンが 222222 である場合、1111222222 と入力します。FireSIGHT システムにログインする前に、SecurID PIN を生成しておく必要があります。
- ログイン バナーが表示され、その後、> プロンプトが表示されます。
- コマンドラインアクセスのレベルによって許可されるコマンドを使用できます。使用可能な CLI 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。
-

# 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

## ライセンス：任意

一部のユーザアカウントは、外部認証サーバによって認証されることがあります。組織によってLDAPまたはRADIUSクレデンシャルを使用してFireSIGHTシステムにログインすることが許可されている場合、外部ユーザクレデンシャルを使用してアプライアンスに初めてログインする時に、アプライアンスは、ローカルユーザレコードを作成して、それらのクレデンシャルを一連のアクセス許可と関連付けます。ローカルユーザレコードのアクセス許可は、グループやリストメンバーシップを使用して付与されていない限り、以下のように変更することができます。

- 外部認証されたユーザアカウントのデフォルトロールが特定のアクセスロールに設定されている場合、システム管理者による追加設定なしで、外部アカウントクレデンシャルを使用してアプライアンスにログインできます。
- アカウントが外部で認証され、デフォルトでは何もアクセス権限を付与されない場合、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（またはシステム管理者）はアクセス許可を変更して、ユーザ機能への適切なアクセスを付与できます。

シェルアクセスユーザの場合、アプライアンスでのローカルユーザアカウントは作成されません。シェルへのアクセスは、LDAPサーバのシェルアクセスフィルタまたはPAMログイン属性セット、あるいはRADIUSサーバのシェルアクセスリストのいずれかによって完全に制御されます。

シェルユーザは、大文字、小文字、または大文字小文字が混在するユーザ名を使用してログインできます。シェルのログイン認証では、大文字と小文字が区別されます。LDAPユーザ名には、アンダースコア（\_）、ピリオド（.）、ハイフン（-）を含めることができますが、それ以外は英数字のみのユーザ名しかサポートされません。

ログイン時にSecurIDトークンが使用される場合、SecurID PINにトークンを付加し、ログインするためのパスワードとして使用します。たとえば、PINが1111で、SecurIDトークンが222222である場合、1111222222と入力します。



注

Webインターフェイスにアクセスできない場合は、システム管理者に連絡してアカウントの特権を変更してもらるか、管理者アクセス権を持つユーザーとしてログインし、アカウントの特権を変更します。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。

## アプライアンスの外部認証アカウントを作成する方法：

アクセス：Any

**ステップ 1** ブラウザで `https://hostname/` にアクセスします。ここで、`hostname` はアプライアンスのホスト名です。

[Login] ページが表示されます。

**ステップ 2** [Username] と [Password] のフィールドに値を入力します。



注

企業でSecurIDトークンが使用される場合、SecurID PINにSecurIDトークンを付加し、ログイン時のパスワードとして使用します。

**ステップ 3** [Login] をクリックします。

表示されるページは、外部認証のデフォルトのアクセス ロールによって異なります。

- 認証オブジェクトまたはシステム ポリシーでデフォルトのアクセス ロールが選択された場合、デフォルトの開始ページが表示されます。ユーザ アカウントに新規ホーム ページを選択した場合、そのページが代わりに表示されます。詳細については、「[ホーム ページの指定](#)」(P.58-3) を参照してください。

ページの上部で選択できるメニューおよびメニュー オプションは、自分のユーザ アカウントの特権に基づきます。ただし、デフォルト ホーム ページのリンクには、ユーザ アカウントの特権の範囲全体にわたるオプションが含まれます。アカウントに付与された特権とは異なる特権を必要とするリンクをクリックした場合、次の警告メッセージが表示されます。

You are attempting to view an unauthorized page.This activity has been logged.

選択可能なメニューから別のオプションを選択するか、またはブラウザ ウィンドウで [Back] をクリックします。

- デフォルトのアクセス ロールが選択されていない場合、[Login] ページが以下のエラーとともに再表示されます。

Unable to authorize access.If you continue to have difficulty accessing this device, please contact the system administrator.

認証方式として属性マッチングを使用する RADIUS サーバを使用する場合、ユーザ アカウントは作成されますが、初回のログインの試行は拒否されることに注意してください。再度ログインする必要があります。

## アプライアンスからのログアウト

ライセンス：任意

シスコは、もう Web インターフェイスを使用しなくなったときにはログアウトすることを推奨します。これは、短時間 Web ブラウザから離れる場合でもです。ログアウトすることによって Web セッションは終了し、誰もそのクレデンシャルでアプライアンスを使用できなくなります。

セッション タイムアウトが適用されないように設定しない限り、デフォルトでは、非アクティブな状態が 1 時間続くとセッションは自動的にログアウトします。管理者ロールを持つユーザは、システム ポリシーのセッション タイムアウト間隔を変更できます。詳細については、「[ユーザ ログイン設定の管理](#)」(P.48-50) および「[ユーザ インターフェイスの設定](#)」(P.50-29) を参照してください。

アプライアンスからログアウトする方法：

アクセス：Any

**ステップ 1** ツールバーの [Logout] をクリックします。

# コンテキストメニューの使用

## ライセンス：機能に応じて異なる

便宜上、Web インターフェイスの特定のページでは、FireSIGHT システムのその他の機能にアクセスするためのショートカットとして使用できるポップアップ コンテキストメニューがサポートされています。メニューの内容は、ホットスポット（アクセスする場所で、ページだけでなく特定のデータも含まれます）によって異なります。

たとえば、イベント ビュー、侵入イベントのパケット ビュー、ダッシュボード、および Context Explorer における IP アドレスのホットスポットでは、追加オプションが提供されます。ホットスポットを右クリックして IP アドレスのコンテキストメニューを使用し、そのアドレスに関連付けられたホストについて詳細を調べます。これには、使用可能な whois およびホストプロファイル情報も含まれます。セキュリティ インテリジェンス フィルタリングをサポートしていない DC500 防御センター以外では、個々の IP アドレスをセキュリティ インテリジェンスのグローバル ホワイトリストまたはブラックリストに追加することもできます。

別の例として、イベント ビューおよびダッシュボードの SHA-256 値のホットスポットによって、ファイルの SHA-256 ハッシュ値をクリーン リストまたはカスタム検出リストに追加するか、コピーするためにハッシュ値全体を表示することができます。この機能も、DC500 防御センターではサポートされないことに注意してください。

以下のリストは、Web インターフェイスのさまざまなページのコンテキストメニューで利用できるオプションについて説明します。シスコのコンテキストメニューがサポートされていないページまたはロケーションでは、ブラウザの通常のコンテキストメニューが表示されます。

## アクセス コントロール ポリシー エディタ

アクセス コントロール ポリシー エディタには、各アクセス コントロール ルール上のホットスポットが含まれます。コンテキストメニューを使用して、新しいルールとカテゴリの挿入、ルールの切り取り、コピー、貼り付け、ルール状態の設定、およびルールの編集を実行できます。

## NAT ポリシー エディタ

NAT ポリシー エディタには、各 NAT ルール上のホットスポットが含まれます。コンテキストメニューを使用して、新しいルールの挿入、ルールの切り取り、コピー、貼り付け、ルール状態の設定、およびルールの編集を実行できます。

## 侵入ルール エディタ

侵入ルール エディタには、各侵入ルール上のホットスポットが含まれます。コンテキストメニューを使用して、ルールの編集、ルール状態の設定（ルールの無効化を含む）、しきい値と抑制オプションの設定、およびルール ドキュメントの表示を実行できます。

## イベント ビューア

[Event] ページ（ドリルダウン ページとテーブル ビュー）には、各イベント、IP アドレス、および特定の検出されたファイルの SHA-256 ハッシュ値にホットスポットがあります。ほとんどのイベント タイプについて、コンテキストメニューを使用して、Context Explorer に関連情報を表示したり、新しいウィンドウにイベント情報をドリルダウンしたりできます。イベント フィールドにすべてを表示するには長すぎるテキスト（SHA-256 のハッシュ値、脆弱性に関する説明、URL など）が含まれる場所では、コンテキストメニューを使用してテキスト全体を表示することができます。

キャプチャしたファイル、ファイル イベント、およびマルウェア イベントについて、コンテキストメニューを使用して、クリーン リストまたはカスタム検出リストへのファイルの追加、それらのリストからのファイルの削除、ファイルのコピーのダウンロード、ま

たは動的分析のための Collective Security Intelligence クラウドへのファイルの送信を実行できます。

侵入イベントについて、コンテキストメニューを使用して、侵入ルールエディタまたは侵入ポリシーのタスクに似たタスクを実行することができます。トリガー ルールの編集、ルール状態の設定（ルールの無効化を含む）、しきい値と抑制オプションの設定、およびルールドキュメントの表示を実行できます。

### パケットビュー

侵入イベントのパケットビューには、IP アドレスのホットスポットが含まれます。パケットビューでは、右クリックメニューの代わりに左クリックコンテキストメニューを使用することに注意してください。

### ダッシュボード

多くのダッシュボードウィジェットには、Context Explorer に関連情報を表示するホットスポットが含まれます。ダッシュボードウィジェットは、IP アドレスと SHA-256 値のホットスポットを含む場合があります。

### Context Explorer

Context Explorer には、グラフ、表、およびグラフ上にホットスポットが含まれます。Context Explorer で可能なものよりも詳しくグラフやリストのデータを調べたい場合、関連データのテーブルビューにドリルダウンできます。また、関連するホスト、ユーザ、アプリケーション、ファイル、および侵入ルール情報を表示することもできます。

Context Explorer では、Context Explorer に固有のフィルタリングやその他のオプションを含む左クリックコンテキストメニューを使用することに注意してください。詳細については、「[Context Explorer データのドリルダウン](#)」(P.4-36) を参照してください。

### コンテキストメニューにアクセスする方法：

アクセス：Any

---

**ステップ 1** Web インターフェイスのホットスポットに対応するページで、ポインタをホットスポットの上に置きます。

Context Explorer 以外では、「Right-click for menu」メッセージが表示されます。

**ステップ 2** 以下のようにして、コンテキストメニューを起動します。

- Context Explorer またはパケットビューで、ポインタを合わせたデバイスを左クリックします。
- その他のすべてのホットスポットに対応するページで、ポインティング・デバイスを右クリックします。

ホットスポットに該当するオプションとともにポップアップコンテキストメニューが表示されます。

**ステップ 3** オプションの名前を左クリックして、オプションの1つを選択します。

アクセスコントロールポリシーエディタまたはNATポリシーエディタを使用している場合、ルールが変更されます。それ以外の場合は、選択したオプションに基づいて、新しいブラウザウィンドウが開きます。

---

