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

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、その後に `>` 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うか、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。
