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がある手順について説明します。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(2-1 ページ)
- アプライアンスからのログアウト(2-5 ページ)
- コンテキスト メニューの使用(2-5 ページ)

アプライアンスへのログイン

ライセンス: 任意(Any)

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、リリース ノートで FireSIGHT システム のこのバージョンについて参照してください。

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。

Blue Coat X-Series 向け Cisco NGIPS にも Web インターフェイスはありません。ただし、X-シリーズ 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-シリーズ 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、『*Blue Coat X-Series 向け Cisco NGIPS 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 の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。

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権限によって制御されます。詳細については、ユーザ アカウントの管理（61-47 ページ）を参照してください。

組織が認証に共通アクセス カード（CAC）を使用している場合は、CAC クレデンシャルを使用してアプライアンスの Web インターフェイスにアクセスすることもできます。CAC 認証および許可の詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

注意　誤ったクレデンシャルを複数回指定すると、シェルのアクセス 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いるのにログインが拒否される場合は、ログインを繰り返さずに、システム管理者に連絡してください。

Web セッションでアプライアンスのホームページに初めてアクセスするユーザは、そのアプライアンスの最後のログイン セッション情報を表示することができます。最後のログインについて、次の情報を表示できます。

- ログインの曜日、月、日、年
- ログイン時のアプライアンスのローカル時間（24 時間表記）
- アプライアンスにアクセスするために最後に使用されたホストとドメイン名

デフォルトでは、ユーザがセッションからタイムアウトされないと設定されていない限り、非活動の状態が 1 時間経過した後で、自動的にセッションからユーザがログアウトされます。管理者ロールを持つユーザは、システム ポリシーでセッション 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（61-52 ページ）およびユーザ インターフェイスの設定（63-32 ページ）を参照してください。

プロセスの中には長時間かかるものがあります。このため、Web ブラウザで、スクリプトが応答しなくなっていることを示すメッセージが表示されることがあります。このような場合は、プロセスが完了してからスクリプトを続行するようにしてください。

(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 システム 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（61-48 ページ）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。

ヒント　ネットワークのユーザが CAC クレデンシャルを使用して [CAC ログイン（CAC Login）] ページにログインできるようにするには、CAC 認証および許可を設定する**必要があります**。詳細については、CAC を使用した LDAP 認証について（61-10 ページ）を参照してください。

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: 任意（Any）

手順 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を表します。

[ログイン（Login）]ページが表示されます。

手順 2　[ユーザ名（Username）] および [パスワード（Password）] フィールドで、ユーザ名とパスワードを入力します。ユーザ名では、大文字と小文字が区別されます。

組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加して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` の場合は、`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。

手順 3　[ログイン（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（71-3 ページ）を参照してください。

ヒント　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権限を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、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（61-60 ページ）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、ユーザ アカウントの権限によって異なります。ただし、デフォルト ホームページのリンクには、ユーザ アカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、次の警告メッセージが表示されます。

> 認証されていないページを表示しようとしています。（`You are attempting to view an unauthorized page.`）このアクティビティはログに記録されています。（`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 [戻る（Back）] をクリックして前のページに戻ります。

CAC クレデンシャルを使用して 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: 任意（Any）

手順 1　組織の指示に従って CAC を挿入します。

手順 2　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を表します。

手順 3　プロンプトが表示されたら、ステップ 1 で挿入した CAC に関連付けられた PIN を入力します。

PIN が受け入れられます。

手順 4　プロンプトが表示されたら、ドロップダウン リストから適切な証明書を選択します。

ブラウザが選択内容を受け入れると、[CAC ログイン（CAC Login）] ページが表示されます。

手順 5　CAC クレデンシャルを使用して認証するには、[続行（Continue）] をクリックします。

ユーザ名とパスワードを使用して認証するには、[ユーザ名（Username）] と [パスワード（Password）] フィールドにそれらを入力します。ユーザ名では、大文字と小文字が区別されます。

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（71-3 ページ）を参照してください。

ヒント　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権限を変更してもらうか、管理者アクセス権を持つユーザとしてログインし、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（61-60 ページ）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、ユーザ アカウントの権限によって異なります。ただし、デフォルト ホームページのリンクには、ユーザ アカウントの権限の範囲に対応するオプションが含まれています。アカウントに付与されている権限とは異なる権限が必要なリンクをクリックすると、次の警告メッセージが表示されます。

> 認証されていないページを表示しようとしています。（You are attempting to view an unauthorized page.）このアクティビティはログに記録されています。（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 [戻る（Back）] をクリックして前のページに戻ります。

（注）　ブラウズ セッションがアクティブな間は、CAC を削除**しない**でください。セッション中に CAC を削除または交換すると、Web ブラウザでセッションが終了し、システムにより Web インターフェイスから強制的にログアウトされます。

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 の基本設定

手順 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。

手順 2　ユーザ名を入力し、Enter キーを押します。

`Password:` プロンプトが表示されます。

手順 3　パスワードを入力して Enter キーを押します。

組織でログイン時に SecurID® トークンが使用されている場合、ログインするには SecurID PIN にトークンを付加して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` の場合は、`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 `>` プロンプトが示されます。

コマンド ライン アクセスのレベルで許可されている任意の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（D-1 ページ）を参照してください。

アプライアンスからのログアウト

ライセンス: 任意（Any）

Web インターフェイスをアクティブに使用しなくなった場合、Cisco では、少しの間 Web ブラウザから離れるだけであっても、ログアウトすることを推奨しています。ログアウトによって Web セッションが終了し、自分のクレデンシャルを使用して他のユーザがアプライアンスを使用できないようになります。

デフォルトでは、ユーザがセッションからタイムアウトされないと設定されていない限り、非活動の状態が 1 時間経過した後で、自動的にセッションからユーザがログアウトされます。管理者ロールを持つユーザは、システム ポリシーでセッション 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（61-52 ページ）およびユーザ インターフェイスの設定（63-32 ページ）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: 任意（Any）

手順 1　ツールバーの [ログアウト（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

操作の利便性を高めるため、Web インターフェイスのいくつかのページではポップアップ コンテキスト メニューをサポートしています。これは、FireSIGHT システムの他の機能にアクセスする際のショートカットとして使用できます。メニューの内容は*ホットスポット*によって異なり、ユーザはページだけでなく特定のデータにアクセスすることもできます。

たとえば、イベント ビューの *IP アドレス ホットスポット*、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 には追加のオプションがあります。アドレスに関連付けられているホストの詳細（使用可能な whois やホスト プロファイルの情報など）を知るには、ホットスポットを右クリックして [IP アドレス（IP address）] コンテキスト メニューを使用します。（セキュリティ インテリジェンスのフィルタリングをサポートしていない）DC500 防御センターを除いては、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個別の IP アドレスを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*では、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したり、コピーするためにハッシュ値全体を表示したりできます。この機能は、DC500 防御センターではサポートされていないことに注意してください。

次の一覧では、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 メニューで使用できるオプションについて説明しています。Cisco 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場所では、ブラウザの標準のコンテキスト メニューが表示されます。

アクセス コントロール、SSL、および NAT ポリシー エディタ

アクセス コントロール、SSL、および NAT ポリシー エディタには、各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。

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）、しきい値と抑制のオプションの設定、およびルールのドキュメンテーションの表示を行うことができます。

イベント ビューア

イベント 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、および特定の検出ファイルの SHA-256 ハッシュ値のホットスポットが含まれます。ほとんどのイベント タイプでは、コンテキスト メニューを使用して、Context Explorer で関連情報を表示したり、イベントの情報について新しいウィンドウでドリルダウンしたりできます。ファイルの SHA-256 ハッシュ値、脆弱性の説明、URL などの、イベント フィールドに含まれているテキストが長すぎて、イベント ビューですべて表示できない場合、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 イベントの場合、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でのファイルの追加または削除、ファイルのコピーのダウンロード、アーカイブ ファイル内にネストされたファイルの表示、ネストされたファイルの親アーカイブ ファイルのダウンロード、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。

侵入イベントに対しても、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で実行できるものと類似のタスクを実行できます。これには、トリガー ルールを編集する、ルール状態を設定する（ルールの無効化を含む）、しきい値と抑制のオプションを設定する、ルールのドキュメンテーションを表示するなどのタスクがあります。

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 メニューではなく、左クリックのコンテキスト 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、関連する情報を Context Explorer で表示するためのホットスポットが含まれます。ダッシュボード ウィジェットには、IP アドレスと SHA-256 値のホットスポットも含めることができます。

Context Explorer

Context Explorer には、図、表、およびグラフのホットスポットが含まれます。Context Explorer よりも詳細なグラフまたはリストのデータを調べたい場合は、関連するデータのテーブル ビューにドリルダウンすることができます。また、関連するホスト、ユーザ、アプリケーション、ファイル、および侵入ルールの情報を表示できます。

Context Explorer でも左クリックのコンテキスト メニューを使用することに注意してください。これには、Context Explorer に特有のフィルタリングおよび他のオプションも含まれています。詳細については、Context Explorer データのドリルダウン（56-41 ページ）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: 任意（Any）

手順 1　Web インターフェイスのホットスポット対応ページで、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、「右クリックでメニューを表示(Right-click for menu)」というメッセージが表示されます。

手順 2　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 ビューでは、ポインティング デバイスを左クリックします。
- ホットスポット対応の他のすべてのページでは、ポインタを合わせたデバイスを右クリックします。

ポップアップ コンテキスト メニューが表示され、ホットスポットに適したオプションが示されます。

手順 3　オプションの名前を左クリックして、いずれかのオプションを選択します。

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。