Firepower システムへのログイン

以下のトピックでは、Firepower システムにログインする方法を示します。

Firepower システムのユーザ アカウント

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、シェル、または CLI へのローカル アクセスを取得する必要があります。ユーザがログイン時にアクセスできる機能は、ユーザ アカウントに許可されている権限によって制御されます。一部のアプライアンスは、外部 LDAP や RADIUS サーバでユーザ クレデンシャルを保存する外部認証を使用するように設定できる場合があります。

（注） システムはユーザ 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が保証されます。

注意 すべてのデバイスで、シェル アクセス権を持つユーザには、（外部認証または CLI `expert` コマンドのどちらを使用して取得されたかにかかわらず）シェルの `sudoers` 権限があるため、セキュリティ リスクが生じる可能性があります。システム セキュリティ上の理由から、次の点を強くお勧めします。

- 外部認証を確立した場合は、シェルアクセスが付与されるユーザのリストを適切に制限してください。
- 7000 および 8000 シリーズの CLI アクセス権限を付与する場合は、**構成**レベルのアクセス権を持つユーザのリストを制限してください。
- いかなる Firepower デバイスでも、事前定義された `admin` に加えてシェル ユーザを確立することはできません。

注意 Cisco TAC の指示に従って操作する場合を除き、シェルや CLI エキスパート モードを使用して FirePOWER デバイスにアクセスしないよう強くお勧めします。

デバイスが異なれば、サポートするユーザアカウントのタイプは異なり、搭載される機能もさまざまです。

Firepower Management Center

Firepower Management Center では、次のユーザ アカウント タイプをサポートします。

- Web インターフェイス アクセス用に事前定義された `admin` アカウント。このアカウントは管理者ロールを保有し、Web インターフェイスから管理できます。
- シェル アクセス用に事前適宜された `admin` アカウント。このアカウントには `sudoers` 権限があります。
- カスタムユーザアカウント。このアカウントは、`admin`ユーザおよび管理者ロールのユーザが作成、管理できます。

注意 システム セキュリティ上の理由から、シスコは、追加のシェル ユーザを Firepower Management Center で確立しないようにすることを推奨します。そのようなリスクを受け入れる場合は、外部認証を使用して、ユーザに Firepower Management Center へのシェル アクセス権を付与できます。内部ユーザのシェル アクセスを有効にすることはできません。

7000 & 8000 シリーズ デバイス

7000 & 8000 シリーズ デバイスでは、次のユーザ アカウント タイプをサポートします。

- 事前定義された `admin` アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。

- カスタム ユーザ アカウント。このアカウントは、admin ユーザおよび管理者ロールのユーザが作成、管理できます。

7000 & 8000 シリーズは、ユーザの外部認証をサポートしています。

NGIPSv デバイス

NGIPSv デバイスでは、次のユーザ アカウント タイプをサポートします。

- 事前定義された admin アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタム ユーザ アカウント。このアカウントは、admin ユーザおよび Configuration アクセス権をもつユーザが作成、管理できます。

NGIPSv は、ユーザの外部認証をサポートしていません。

Firepower Threat Defense および Firepower Threat Defense Virtual デバイス

Firepower Threat Defense および Firepower Threat Defense Virtual デバイスでは、次のユーザ アカウント タイプをサポートします。

- 事前定義された admin アカウント。このアカウントはデバイスにアクセスするすべての形態で使用できます。
- カスタム ユーザ アカウント。このアカウントは、admin ユーザおよび Configuration アクセス権をもつユーザが作成、管理できます。

Firepower Threat Defense は、SSH または HTTP ユーザの外部認証をサポートしていません。

ASA FirePOWER デバイス

ASA FirePOWER モジュールは、次のユーザ アカウント タイプをサポートしています。

- 事前定義された admin アカウント。
- カスタム ユーザ アカウント。このアカウントは、admin ユーザおよび Configuration アクセス権をもつユーザが作成、管理できます。

ASA FirePOWER モジュールは、ユーザの外部認証をサポートしていません。ASA CLI および ASDM を介した ASA デバイスへのアクセスについては、『*Cisco ASA Series General Operations CLI Configuration Guide*』および『*Cisco ASA Series General Operations ASDM Configuration Guide*』に記載されています。

Firepower Management Center 展開のユーザ インターフェイス

タイプに応じて、Webベースの GUI、補助的な CLI、または Linux シェルを使用して FirePOWER アプライアンスにアクセスできます。Firepower Management Center 展開では、ほとんどの設定タスクを Firepower Management Center の GUI から実行します。デバイスに直接アクセスする必要があるタスクはごくわずかです。

ブラウザの要件については、「Firepower Release Notes」を参照してください。

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
Firepower Management Center	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • アドミニストレーティブ タスク、管理タスク、分析タスクに使用することができます	なし	• 事前定義された admin ユーザとカスタム外部ユーザ アカウントでサポートされます • • SSH シリアル、またはキーボードとモニタ接続を使用してアクセス可能 • Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
7000 & 8000 シリーズ デバイス	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • 初期設定、基本的な分析、および設定タスクにのみ使用することができます	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • SSH シリアル、またはキーボードとモニタ接続を使用してアクセス可能 • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • **Configuration** アクセス権を持つ CLI ユーザが expert コマンドを使用してアクセスできます • Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください
Firepower Threat Defense Firepower Threat Defense Virtual	なし	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • SSH 接続を使用してアクセスできます • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • **Configuration** アクセス権を持つ CLI ユーザが expert コマンドを使用してアクセスできます • Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください

アプライアンス	Web ベースの GUI	補助的な CLI	Linux シェル
NGIPSv	なし	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • SSH 接続を使用してアクセスできます • Cisco TAC の指示に従って設定およびトラブルシューティングを行う場合にのみ、使用できます	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • **Configuration** アクセス権を持つ CLI ユーザが expert コマンドを使用してアクセスできます • Cisco TAC の指示に従って管理およびトラブルシューティングを行う場合にのみ、使用してください
ASA FirePOWERモジュール	なし	• 事前定義された admin ユーザとカスタム ユーザ アカウントでサポートされます • SSH 接続を使用してアクセスできます • 設定タスクおよび管理タスクに使用することができます	なし

関連トピック

ユーザ アカウントの管理

Web インターフェイスに関する考慮事項

- 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ができます。

- Web セッション時にアプライアンスのホーム ページに初めてアクセスした際に、そのアプライアンスに対する最後のログインセッションに関する情報を表示できます。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
- デフォルトのホーム 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、システムから警告メッセージが表示され、そのアクティビティがログに記録されます。
- 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スクリプトの続行を許可してください。

関連トピック

ホームページの指定

セッションのタイムアウト（Session Timeout）

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、Firepower システムが自動的にセッションからユーザをログアウトします。

管理者ロールを割り当てられたユーザは、以下の設定を使用して、アプライアンスのセッション タイムアウト間隔を変更できます。

アプライアンス	設定
Firepower Management Center	**[システム（System）] > [設定（Configuration）] > [シェル タイムアウト（Shell Timeout）]**
7000 & 8000 シリーズ デバイス	**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [シェル タイムアウト（Shell Timeout）]**

関連トピック

セッション タイムアウトの設定

Firepower Management Center Web インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	Management Center	任意（Any）	任意（Any）

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

始める前に

- 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としてログインし、アカウントの特権を変更します。
- ユーザ アカウントの作成の説明に従って、ユーザ アカウントを作成します。

手順

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 Firepower Management Center のホスト名に対応します。

ステップ 2 [ユーザ名（Username）] および [パスワード（Password）] フィールドに、ユーザ名とパスワードを入力します。次の注意事項に注意を払ってください。

- ユーザ名は大文字/小文字を区別しません。
- マルチドメイン導入環境では、ユーザアカウントが作成されたドメインをユーザ名の前に付加します。先祖ドメインを前に付加する必要はありません。たとえばユーザアカウントを SubdomainB で作成し、そのドメインの先祖ドメインが DomainA である場合、次の形式でユーザ名を入力します。

  ```
  SubdomainB\username
  ```

- 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。Firepower 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 [ログイン（Login）] をクリックします。

関連トピック

セッションのタイムアウト（Session Timeout） （7 ページ）

7000 または 8000 シリーズ デバイスの Web インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	7000 & 8000 シリーズ	該当なし	任意（Any）

ユーザは単一のアクティブなセッションに制限されます。すでにアクティブセッションがあるユーザアカウントにログインしようとすると、もう一方のセッションを終了するか、または別のユーザとしてログインするように求められます。

始める前に

- 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としてログインし、アカウントの特権を変更します。
- デバイスに該当する Firepower クイック スタート ガイドおよびユーザ アカウントの作成の説明に従って、初期設定プロセスを完了し、ユーザ アカウントを作成します。

手順

ステップ 1 ブラウザで `https://hostname/` にアクセスします。ここで、*hostname* はアクセスする管理対象デバイスのホスト名に対応します。

ステップ 2 [ユーザ名（Username）] および [パスワード（Password）] フィールドに、ユーザ名とパスワードを入力します。次の注意事項に注意を払ってください。

- ユーザ名は大文字/小文字を区別しません。
- 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。Firepower 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 [ログイン（Login）] をクリックします。

関連トピック

セッションのタイムアウト（Session Timeout） （7 ページ）

CAC クレデンシャルを使用した Firepower Management Center へのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	Management Center	任意（Any）	任意（Any）

ユーザは単一のアクティブなセッションに制限されます。

注意 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。

始める前に

- 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としてログインし、アカウントの特権を変更します。
- ユーザ アカウントの作成の説明に従ってユーザ アカウントを作成します。
- CAC 認証の設定の説明に従って、CAC の認証と認可を設定します。

手順

ステップ 1 組織の指示に従って CAC を挿入します。

ステップ 2 ブラウザで `https://hostname/` にアクセスします。ここで、*hostname* は Firepower Management Center のホスト名に対応します。

ステップ 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。

ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ステップ 5 [続行（Continue）] をクリックします。

関連トピック

CAC 認証

セッションのタイムアウト（Session Timeout） （7 ページ）

CAC クレデンシャルを使用した 7000 または 8000 シリーズ デバイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	7000 & 8000 シリーズ	該当なし	任意（Any）

ユーザは単一のアクティブなセッションに制限されます。

注意 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。

始める前に

- 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としてログインし、アカウントの特権を変更します。
- ユーザ アカウントの作成の説明に従って、ユーザ アカウントを作成します。
- CAC 認証の設定の説明に従って、CAC の認証と認可を設定します。

手順

ステップ 1 組織の指示に従って CAC を挿入します。

ステップ 2 ブラウザで `https://hostname/` にアクセスします。ここで、*hostname* はアクセスするアプライアンスのホスト名に対応します。

ステップ 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。

ステップ 4 プロンプトが表示されたら、ドロップダウン リストから該当する証明書を選択します。

ステップ 5 [続行（Continue）] をクリックします。

関連トピック

CAC 認証

セッションのタイムアウト（Session Timeout） （7 ページ）

従来型デバイスでのコマンドラインインターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	該当なし	CLI の基本設定

従来型管理対象デバイス（7000 & 8000 シリーズ、NGIPSv、および ASA FirePOWER）のコマンドライン インターフェイスに直接ログインできます。

始める前に

最初のログインにデフォルトの **admin** ユーザを使用して初期設定プロセスを完了します。

- 7000 & 8000 シリーズ デバイスでは、ユーザ アカウントの作成の説明に従って、Web インターフェイスでユーザ アカウントを作成します。
- すべてのデバイスで、CLI にログインできる追加のユーザ アカウントを **configure user add** コマンドを使用して作成します。

手順

ステップ 1 SSH を使用して、管理インターフェイスのホスト名または IP アドレスに接続します。または、コンソール ポートに接続することもできます。

ステップ 2 「`log in as:`」コマンド プロンプトに対してユーザ名を入力し、Enter を押します。

ステップ 3 「`Password:`」プロンプトに対してパスワードを入力し、Enter 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。Firepower 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 4 CLI プロンプトで、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します。

Firepower Threat Defense デバイスのコマンドライン インターフェイスへのログイン

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	該当なし	Firepower Threat Defense	該当なし	CLI の基本設定

Firepower Threat Defense 管理対象デバイスのコマンドライン インターフェイスに直接ログインできます。

始める前に

最初のログインにデフォルトの **admin** ユーザを使用して初期設定プロセスを完了します。**configure user add** コマンドを使用して、CLI にログインできる追加のユーザ アカウントを作成します。

手順

ステップ 1 コンソール ポートまたは SSH を使用して、Firepower Threat Defense CLI に接続します。

Firepower Threat Defense デバイスの管理インターフェイスに SSH で接続できます。SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。特定のデータ インターフェイスへの SSH 接続を許可する方法については、セキュア シェルの設定を参照してください。

デバイスのコンソール ポートに直接接続できます。デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナルエミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。

コンソール ポートでアクセスする最初の CLI は、デバイス タイプによって異なります。

- ASA シリーズ デバイス：コンソール ポートの CLI は通常の Firepower Threat Defense CLI です。
- Firepower シリーズ デバイス：コンソール ポートの CLI は FXOS です。Firepower Threat Defense CLI には、**connect ftd** コマンドを使用してアクセスできます。FXOS CLI はシャーシ レベルの設定およびトラブルシューティングにのみ使用します。基本設定、モニタリング、および通常のシステムのトラブルシューティングには Firepower Threat Defense CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

ステップ 2 管理者ユーザ名とパスワードでログインします。

ステップ 3 CLI プロンプト（>）で、コマンドライン アクセス レベルで許可されている任意のコマンドを使用します。

ステップ 4 （オプション）診断 CLI にアクセスします。

system support diagnostic-cli

この CLI を使用して、高度なトラブルシューティングを行います。この CLI では、追加の **show** コマンドや、ASA 5506W-X ワイヤレス アクセス ポイントの CLI へのアクセスに必要な **session wlan console** コマンドなど、その他のコマンドが利用できます。

この CLI には 2 つのサブモード、ユーザ EXEC モードと特権 EXEC モードがあります。特権 EXEC モードではより多くのコマンドが利用できます。特権 EXEC モードを開始するには、**enable** コマンドを入力し、プロンプトに対してパスワードを入力せずに Enter を押します。

例：

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

通常の CLI に戻るには、**Ctrl+a**、**d** を入力します。

Web インターフェイスでの基本システム情報の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
該当なし	任意（Any）	任意（Any）	任意（Any）	任意（Any）

[バージョン情報（About）] ページには、Firepower システムのさまざまなコンポーネントのモデル、シリアル番号、バージョン情報など、アプライアンスに関する情報が示されます。また、シスコの著作権情報も示されます。

手順

ステップ 1 ページ上部のツールバーから [ヘルプ（Help）] をクリックします。

ステップ 2 [バージョン情報（About）] を選択します。

Firepower Management Center のドメインの切り替え

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	Management Center	任意（Any）	任意（Any）

マルチドメイン導入環境では、ユーザ ロール権限によって、ユーザがアクセスできるドメインと、そのドメイン内でのユーザの権限が決まります。単一のユーザアカウントを複数のドメインに関連付けて、各ドメインでそのユーザに異なる権限を割り当てることができます。たとえば、あるユーザにグローバル ドメインでは読み取り専用権限を割り当て、子孫ドメインでは管理者権限を割り当てることができます。

複数のドメインに関連付けられているユーザは、同じ Web インターフェイス セッション内でドメインを切り替えることができます。

ツールバーのユーザ名の下に、利用可能なドメインのツリーが表示されます。ツリーの表示は次のようになります。

- 先祖ドメインは表示されますが、使用しているユーザアカウントに割り当てられた権限に応じて、先祖ドメインへのアクセスが無効である場合があります。
- 兄弟ドメインや子孫ドメインを含め、使用しているユーザアカウントでアクセスできない他のドメインは非表示になります。

ドメインを切り替えると、以下の項目が表示されます。

- そのドメインのみに関連するデータ。
- そのドメインで割り当てられたユーザ ロールに応じて定められたメニュー オプション。

手順

アクセスするドメインは、ユーザ名の下にあるドロップダウン リストから選択します。

Firepower システム Web インターフェイスからのログアウト

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	任意（Any）	任意（Any）	任意（Any）

Firepower システムの 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、シスコでは、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。ログアウトすることで Web セッションを終了し、別のユーザが自分の資格情報を使用してインターフェイスを使用できないようにします。

手順

ユーザ名の下にあるドロップダウンリストから、[ログアウト（Logout）] を選択します。

関連トピック

セッションのタイムアウト（Session Timeout） （7 ページ）

コンテキスト メニュー

Firepower システム Web インターフェイスの特定のページでは、右クリック（最も一般的）および左クリックでコンテキストメニューを表示できます。コンテキストメニューは、Firepower システム内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ます。コンテキスト メニューの内容はどこでこのメニューにアクセスするか（どのページかだけでなく特定のデータにアクセスしているか）によって異なります。

次に例を示します。

- IP アドレスのホットスポットでは、そのアドレスに関連付けられているホストに関する情報（使用可能な whois とホスト プロファイル情報を含む）が表示されます。
- SHA-256 ハッシュ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。

Firepower システム コンテキスト メニューをサポートしていないページや場所では、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。

ポリシー エディタ

多くのポリシーエディタには、各ルールのホットスポットが含まれています。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、ルールの編集などを行うことができます。

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ています。ルールの編集、ルール状態の設定、しきい値および抑止オプションの設定、ルールのドキュメンテーションの表示などを行うことができます。 ルール ドキュメントを表示するには、[ルールドキュメンテーション（Rule Documentation）] をクリックして、ルールの詳細を表示します。

イベント ビューア

イベントページ（[分析（Analysis）]ページにある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、URL、DNSクエリ、特定のファイルのSHA-256ハッシュ値のホットスポットが含まれています。ほとんどのイベントタイプでは、表示中に以下の操作を行うことができます。

- Context Explorer で関連情報を表示する。
- 新しいウィンドウでイベント情報をドリルダウンする。
- イベント フィールドに含まれているテキスト（ファイルの SHA-256 ハッシュ値、脆弱性の説明、URL など）が長すぎてイベント ビューですべて表示できない場合、テキスト全体を表示する。

接続イベントの表示中は、デフォルトのセキュリティインテリジェンスのホワイトリストとブラックリストに以下の項目を追加できます。

- IP アドレスのホットスポットの場合、IP アドレス。
- URL のホットスポットの場合、URL またはドメイン名。
- DNS クエリのホットスポットの場合、DNS クエリ。

キャプチャ ファイル、ファイル イベント、マルウェア イベントの表示中は、以下の操作を行うことができます。

- クリーン リストまたはカスタム検出リストのファイルを追加または削除する。
- ファイルのコピーをダウンロードする。
- アーカイブ ファイル内のネストされたファイルを表示する。
- ネストされたファイルの親アーカイブ ファイルをダウンロードする。
- ファイルの構成を表示する。
- ローカル マルウェア分析およびダイナミック分析対象のファイルを送信する。

侵入イベントの表示中は、侵入ルールエディタまたは侵入ポリシーで実行できるようなタスクを行うことができます。

- トリガー ルールを編集する。
- ルールの無効化を含め、ルールの状態を設定する。
- しきい値および抑止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。 表示するには、[ルールドキュメンテーション（Rule Documentation）] をクリックして、ルールの詳細を表示します。

侵入イベントのパケット 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ています。パケット ビューでは、左クリックによるコンテキスト メニューを使用します。

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ています。ダッシュボード ウィジェットには、IP アドレスと SHA-256 ハッシュ値のホットスポットが含まれる場合もあります。

Context Explorer

Context Explorer には、図、表、グラフのホットスポットが含まれています。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 メニューを使用します。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。

関連トピック

セキュリティ インテリジェンスのリストとフィード