データの消去とストレージ

Firewall Management Center に保管されたデータ

対象	参照先
Firewall Management Center のデータストレージに関する一般情報	[ディスク使用量（Disk Usage）] ウィジェット
古いデータの消去	Firewall Management Center データベースからのデータの消去 （2 ページ）
Firewall Management Center 上のデータへの外部アクセス許可（高度な機能）	外部データベース アクセス
バックアップ	バックアップとリモートストレージの管理 およびサブトピック
レポート	ローカル ストレージの設定
イベント	接続ロギング データベース およびサブトピック
ネットワーク検出データ	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Discovery Data Storage Settings*」およびそれ以降のトピック

対象	参照先
ファイル（Files）	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Malware Protection and File Policies*」の章にあるファイルの保存に関する情報（ベストプラクティスを含む）。 Cisco Secure Firewall Management Center デバイス構成ガイドの「*Tuning File and Malware Inspection Performance and Storage*」
パケット データ	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Edit General Settings*」
ユーザーおよびユーザーアクティビティ	Cisco Secure Firewall Management Center デバイス構成ガイドの「*The Users Database*」 Cisco Secure Firewall Management Center デバイス構成ガイドの「*The User Activity Database*」

Firewall Management Center データベースからのデータの消去

データベース消去ページを使用すると、検出、アイデンティティ、接続、およびセキュリティ関連の接続のデータ ファイルを Firewall Management Center データベースから消去できます。データベースを消去すると、該当するプロセスが再起動される点に注意してください。

⚠

注意 データベースを消去すると、Firewall Management Center から指定したデータが削除されます。削除されたデータは復元できません。

始める前に

データを消去するには、管理者権限またはセキュリティアナリスト権限が必要です。このタスクを実行するには、グローバルドメインに属している必要があります。

手順

ステップ 1 [システム（System）]（⚙） > **[ツール（Tools）]** > **[データの削除（Data Purge）]**を選択します。

ステップ 2 [Discovery and Identity] の下で、次のいずれかまたはすべてを実行します。

- [ネットワーク検出イベント（Network Discovery Events）]チェックボックスをオンにして、データベースからすべてのネットワーク検出イベントを削除します。

- [ホスト（Hosts）]チェックボックスをオンにして、データベースからすべてのホストとホストの侵害の兆候フラグを削除します。
- [ユーザー アクティビティ（User Activity）] チェックボックスをオンにして、データベースからすべてのユーザー アクティビティ イベントを削除します。
- [ユーザー アイデンティティ（User Identities）] チェックボックスをオンにして、データベースからすべてのユーザー ログインとユーザー履歴データ、およびユーザーの侵害の兆候フラグを削除します。

（注）
Microsoft Azure AD レルムのユーザー アクティビティ イベント、ユーザーログイン、およびユーザー履歴データは削除「されません」。

ステップ 3 [接続（Connections）] で、次のいずれかまたはすべてを実行します。

- [接続イベント（Connection Events）] チェックボックスをオンにして、データベースからすべての接続データを削除します。
- [接続の概要イベント（Connection Summary Events）]チェックボックスをオンにして、データベースからすべての接続の概要データを削除します。
- **[セキュリティ関連の接続イベント（Security-Related Connection Events）]**チェックボックスをクリックして、データベースからすべてのセキュリティ関連の接続データをデータベースから削除します。

（注）
[接続イベント（Connection Events）] チェックボックスをオンにしても、セキュリティ インテリジェンス イベントは削除されません。セキュリティ インテリジェンス データとの接続は、[セキュリティ インテリジェンス イベント（Security Intelligence Events）] ページに引き続き表示されます（[分析（Analysis）] > [接続（Connections）] メニューの下に表示）。同様に、**[セキュリティ関連の接続イベント（Security-Related Connection Events）]** チェックボックスをオンにしても、セキュリティ関連の接続データに関連する接続イベントは削除されません。

ステップ 4 [選択したイベントの消去（Purge Selected Events）] をクリックします。
項目が消去され、該当するプロセスが再起動されます。

外部データストレージ

オプションで、特定のタイプのデータを保存するためにリモートデータストレージを使用できます。

対象	参照先
バックアップ	バックアップとリモートストレージの管理 およびサブトピック リモート ストレージ デバイス およびサブトピック
レポート	リモート ストレージ デバイス およびサブトピック リモート ストレージへのレポートの移動
イベント	外部ツールを使用したイベントの分析 の syslog およびその他のリソースに関する情報 Cisco Secure Cloud Analytics でのリモートデータストレージ （5 ページ） Secure Network Analytics アプライアンスでのリモートデータストレージ（6 ページ） 接続イベントをリモートで保存する場合は、FMC での接続イベントの保存を無効にすることを検討してください。詳細については、データベース およびサブトピックを参照してください。

重要 syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。

セキュリティ分析とロギング リモート イベント ストレージ オプションの比較

イベントデータを Firewall Management Center の外部に保存するための類似しているが異なるオプション：

オンプレミス	SaaS
ファイアウォールの背後に設置するストレージシステムを購入し、ライセンスを取得してセットアップします。	ライセンスとデータストレージプランを購入し、データをシスコのクラウドに送信します。

オンプレミス	SaaS
サポートされるイベントタイプ： • 接続 • セキュリティインテリジェンス • 侵入 • ファイルおよびマルウェア • LINA	サポートされるイベントタイプ： • 接続 • セキュリティインテリジェンス • 侵入 • ファイルおよびマルウェア
syslog と直接統合の両方をサポートします。	syslog と直接統合の両方をサポートします。
• Secure Network Analytics Manager ですべてのイベントを表示します。 • FMC イベントビューアから相互起動して、Secure Network Analytics Manager でイベントを表示します。 • FMC でリモートに保存された接続およびセキュリティインテリジェンスイベントを表示します。	ライセンスに応じて Security Cloud Control または Secure Network Analytics でイベントを表示します。FMC イベントビューアから相互起動します。
詳細については、Secure Network Analytics アプライアンスでのリモートデータストレージ（6 ページ）のリンクを参照してください。	詳細については、Cisco Secure Cloud Analytics でのリモートデータストレージ （5 ページ）のリンクを参照してください。

Cisco Secure Cloud Analytics でのリモートデータストレージ

シスコのセキュリティ分析とロギング（SaaS） を使用して、選択した Cisco Secure Firewall イベントデータを Secure Cloud Analytics に送信します。サポートされているイベント：接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェア。

詳細については、『*Cisco Secure Firewall Management Center および Cisco Security Analytics and Logging（SaaS）統合ガイド*』を参照してください。

イベントは直接送信するか、syslog 経由で送信することができます。

重要 syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。

Secure Network Analytics アプライアンスでのリモートデータストレージ

Cisco Secure Firewall アプライアンスが提供できる以上のデータストレージが必要な場合は、セキュリティ分析とロギング（オンプレミス） を使用して Secure Network Analytics アプライアンスに Cisco Secure Firewall データを保存することができます。詳細については、「Cisco Security Analytics and Logging」から入手可能なマニュアルを参照してください。

接続イベントが Secure Network Analytics アプライアンスに保存されている場合でも、Firewall Management Center で接続イベントを確認できます。Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Secure Firewall Management Center での作業を参照してください。

重要 syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。

（注） Secure Network Analytics アプライアンスバージョン 7.5.1 以降では、**マネージャのみ**の展開はサポートされていません。詳細については、「Cisco Security Analytics and Logging」を参照してください。

データストレージの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
イベントレート制限から優先順位の低い接続イベントを除外する	7.0	任意（Any）	接続イベントをリモートボリュームに保存しているために Firewall Management Center に接続イベントを保存しない場合、それらのイベントは Firewall Management Center ハードウェアデバイスのフローレート制限にカウントされません。 新しい 7.0 構成を使用して セキュリティ分析とロギング（オンプレミス） にイベントを送信する場合は、その統合の一環としてこの設定を構成します。 それ以外の場合は、データベースイベント数の制限の接続データベースに関する情報を参照してください。 新規/変更されたページ：なし。動作の変更のみ。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Secure Network Analytics アプライアンスにイベントを送信するプロセスの改善	7.0	任意（Any）	新しいウィザードにより、セキュリティ分析とロギング（オンプレミス）を使用した Secure Network Analytics アプライアンスへのイベントの直接送信が合理化されます。 このウィザードでは、Firewall Management Center でイベントページを表示しながらリモートで保存された接続イベントを表示したり、Firewall Management Center から相互起動して Secure Network Analytics アプライアンスでイベントを表示したりもできます。 syslog を使用してイベントを送信するようにシステムをすでに設定している場合、その設定を無効にしない限り、syslog を使用してイベントが送信され続けます。 詳細については、Secure Network Analytics アプライアンスでのリモートデータストレージ （6 ページ）で参照されているマニュアルを参照してください。 新規/変更されたページ：**[システム（System）] > [ロギング（Logging）] > [セキュリティ分析とロギング（Security Analytics & Logging）]**ページに、相互起動オプションを作成するための設定ではなく、ウィザードが表示されるようになりました。
Secure Network Analytics アプライアンスでのリモートデータストレージ	6.7	いずれか	セキュリティ分析とロギング（オンプレミス）を使用して、大量の Firepower イベントデータをリモートで保存できるようになりました。Firewall Management Center でイベントを表示する場合、リモートデータストレージの場所にあるイベントをすばやく相互起動して表示できます。 サポートされているイベント：接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェア。イベントは、syslog を使用して送信されます。 このソリューションは、Stealthwatch Enterprise（SWE）バージョン 7.3 を実行している Stealthwatch Management Console（SMC）バーチャル エディションの可用性に依存します。 Secure Network Analytics アプライアンスでのリモートデータストレージ （6 ページ）を参照してください。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Cisco Secure Cloud Analytics でのリモートデータストレージ	6.4	任意（Any）	syslog を使用して、選択した Firepower データを シスコのセキュリティ分析とロギング（SaaS） を使用して送信します。サポートされているイベント：接続、セキュリティインテリジェンス、侵入、ファイル、およびマルウェア。 詳細については、https://cisco.com/go/firepower-sal-saas-integration-docs にある『Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide』を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。