Secure Firewall Management Center と SecureX の統合について

Secure Firewall Management Center と SecureX について

Cisco SecureX プラットフォームは、広範なシスコの統合型セキュリティポートフォリオとお客様のインフラストラクチャをつなぐことで、一貫した操作性を提供します。これにより可視性が統一され、自動化が実現し、ネットワーク、エンドポイント、クラウド、およびアプリケーションの全体でセキュリティが強化されます。

SecureX の詳細については、Cisco SecureX 製品のページを参照してください。

SecureX と Management Center の統合により、Management Center の全データの概要が提供されます。

このドキュメントの指示に従い、SecureX ポータルを使用して、Management Center バージョン 7.0.2 および 7.2 で管理されているデバイスのファイアウォール イベント データを表示および操作します。Management Center のバージョンが 7.1 以下の場合（7.0.2 を除く）、Management Center と SecureX の統合については『Cisco Secure Firewall Threat Defence and SecureX Integration Guide』[英語] の指示に従ってください。

SecureX 地域クラウド

地域	クラウドへのリンク	サポートされる統合方法と管理対象デバイスのバージョン	サポートされる Management Center バージョン
北米	https://securex.us.security.cisco.com	• 直接統合： バージョン 6.4 以降 • syslog を使用した統合： バージョン 6.3 以降	バージョン 7.0.2、バージョン 7.2 以降
欧州	https://securex.eu.security.cisco.com	• 直接統合： バージョン 6.5 以降 • syslog を使用した統合： バージョン 6.3 以降	バージョン 7.0.2、バージョン 7.2 以降
アジア（APJC）	https://securex.apjc.security.cisco.com	• 直接統合： バージョン 6.5 以降 • syslog を使用した統合： バージョン 6.3 以降	バージョン 7.0.2、バージョン 7.2 以降

地域クラウドの選択に関する注意事項と制約事項

地域クラウドを選択する前に、次の重要な点を考慮してください。

- 地域クラウドの選択は、バージョンと統合方法（syslog または直接）によって異なります。

  詳細については「SecureX 地域クラウド」を参照してください。

- 可能な場合は、導入環境に最も近い地域クラウドを使用してください。
- 複数の地域クラウドのデータをマージまたは集約することはできません。
- 複数の地域からデータを集約する必要がある場合は、すべての地域のデバイスが同じ地域のクラウドにデータを送信する必要があります。
- 地域クラウドごとにアカウントを作成でき、各クラウドのデータは個別に維持されます。

- ご使用の製品で選択した地域は、 Cisco Support Diagnostics および Cisco Support Network 機能にも使用されます（該当し有効にしている場合）。これらの機能の詳細については、ご使用の製品のオンラインヘルプを参照してください。

サポートされるイベント タイプ

Secure Firewall Management Center と SecureX の統合では、次のイベントタイプがサポートされています。

表 *1 : Cisco Cloud* にイベントを送信するためのバージョンのサポート

イベントタイプ	**Threat Defense** のデバイスバージョン（直接統合）	**Syslog**
侵入（IPS）イベント	6.4 以降	6.3 以降
セキュリティ接続イベント	6.5 以降	未サポート
ファイルおよびマルウェアのイベント	6.5 以降	サポート対象外

クラウドへのイベント送信方法の比較

デバイスは、syslog を使用して、または直接的に Security Services Exchange ポータルを経由することで SecureX でイベントを利用可能にします。

イベントの直接送信	**Syslog** を使用したプロキシサーバー経由のイベント送信
サポートされているバージョンのソフトウェアを実行している Threat Defense （NGFW）デバイスのみをサポートします。	サポートされているバージョンのソフトウェアを実行しているすべてのデバイスをサポートします。
バージョン 6.4 以降をサポートします。	バージョン 6.3 以降をサポートします。
に示されているすべてのイベントタイプをサポートします。	侵入イベントのみをサポートします。

イベントの直接送信	Syslog を使用したプロキシサーバー経由のイベント送信
アプライアンスおよびデバイスで最適なソフトウェアバージョンが実行されているかどうかなど、システムステータス情報を表示する SecureX タイルをサポートします。	システムステータス機能は、syslog ベースの統合ではサポートされていません。
Threat defense デバイスはインターネットに接続する必要があります。	デバイスをインターネットに接続する必要はありません。
展開時に Smart Software Manager オンプレミスサーバー（旧称 Smart Software Satellite Server）を使用できません。	展開時に、Smart Software Manager オンプレミスサーバーを使用できます。
オンプレミスのプロキシサーバーのセットアップとメンテナンスは不要です。	オンプレミス仮想 Cisco Security Service Proxy（CSSP）サーバーが必要です。 このプロキシ サーバーの詳細については、Security Services Exchange のオンライン ヘルプを参照 Security Services Exchange にアクセスするには、「Security Services Exchange へのアクセス」を参照してください。

ベスト プラクティス

参照先の手順に関するトピックの「要件」に関するトピックや「始める前に」のセクションを含め、次のトピックのガイドラインとセットアップ手順に厳密に従います。

- すべての統合：

  地域クラウドの選択に関する注意事項と制約事項 （2 ページ）を参照してください。

- 直接統合の場合：

  Cisco Cloud にイベントを直接送信する方法を参照してください。

- syslog を使用した統合の場合：

  『syslog を使用した Cisco Cloud へのイベントの送信方法』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。