Firepower との統合に関する重要な情報：SecureX

- Firepower と SecureX について （1 ページ）
- SecureX 地域クラウド （2 ページ）
- サポートされるイベント タイプ （3 ページ）
- クラウドへのイベント送信方法の比較 （3 ページ）
- ベスト プラクティス （4 ページ）

Firepower と SecureX について

シスコセキュリティ製品の購入に含まれる統合ポータルである SecureX を使用して、すべてのシスコセキュリティ製品のデータを表示します。

SecureX は簡素化されたプラットフォーム エクスペリエンスです。シスコの統合型セキュリティポートフォリオをお客様の既存のインフラストラクチャとつなぎ、可視性の統合、自動化の有効化、そしてネットワーク、エンドポイント、クラウド、およびアプリケーション全体のセキュリティの強化を実現します。

SecureX の詳細については、https://www.cisco.com/c/en/us/products/security/securex/index.htmlを参照してください。

SecureX ポータルで Firepower データを表示して操作するには、このドキュメントの手順に従います。

SecureX 地域クラウド

地域	クラウドへのリンク	サポートされている Firepower 統合方式
北米	https://securex.us.security.cisco.com	• 直接統合： Firepower リリース 6.4 以降 • syslog 経由での統合： Firepower リリース 6.3 以降
欧州	https://securex.eu.security.cisco.com	• 直接統合： Firepower リリース 6.5 以降 • syslog 経由での統合： Firepower リリース 6.3 以降
アジア（APJC）	https://securex.apjc.security.cisco.com	• 直接統合： Firepower リリース 6.5 以降 • syslog 経由での統合： Firepower リリース 6.3 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。

- Firepower のバージョンと統合方法（syslog または直接）が選択内容に影響を及ぼします。

  詳細については、SecureX 地域クラウド （2 ページ）を参照してください。
- 可能な場合は、Firepower の導入環境に最も近い地域クラウドを使用してください。
- 異なるクラウド内のデータを集約またはマージ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。
- 各地域のクラウド上にアカウントを作成できます。各クラウドのデータは区分されます。
- Firepower 製品で選択した地域は、シスコ サポート診断およびシスコ サポートネットワーク機能にも使用されます（該当し有効にしている場合）。これらの詳細については、ご使用の Firepower 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

Firepower と SecureX 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 *Firepower* バージョンのサポート

機能	FMC バージョンによって管理されているデバイス （直接統合）	FDM バージョンによって管理されている FTD デバイス （直接統合）	Syslog
侵入（IPS）イベント	6.3 以降（syslog 経由） 6.4 以降（直接接続経由）	6.3 以降（syslog 経由） 6.4 以降（直接接続経由）	サポートあり
セキュリティ インテリジェンスの接続イベント	6.5 以降	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	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

Firepower 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。

直接送信	プロキシを使用した syslog 経由での送信
サポートされているバージョンの Firepower ソフトウェアを実行している Firepower Threat Defense（NGFW）デバイスのみをサポート	サポートされているバージョンの Firepower 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
Firepower 6.4 以降をサポート	Firepower 6.3 以降をサポート
サポートされるイベント タイプ （3 ページ）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。

直接送信	プロキシを使用した syslog 経由での送信
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。
Firepower Threat Defense デバイスのインターネットへの接続が必要	Firepower デバイスのインターネットへの接続は不要
Firepower の展開では、Smart Software Manager オンプレミスサーバー（旧称 Smart Software Satellite Server）は使用できません。	導入では、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	オンプレミス仮想 Cisco Security Services Proxy（CSSP）サーバーが必要 このプロキシサーバーの詳細については、Security Services Exchange（SSE）のオンラインヘルプを参照 SSE にアクセスするには、Security Services Exchange へのアクセスを参照

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し、SecureX と統合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。