



2025 年の新機能

これらは、2025 年に Security Cloud Control に展開された新しいファイアウォール機能です。

- [2025 年 12 月](#) (1 ページ)
- [2025 年 11 月](#) (2 ページ)
- [2025 年 10 月](#) (3 ページ)
- [2025 年 9 月](#) (3 ページ)
- [2025 年 8 月](#) (4 ページ)
- [2025 年 7 月](#) (5 ページ)
- [2025 年 6 月](#) (7 ページ)
- [2025 年 4 月](#) (8 ページ)
- [2025 年 3 月](#) (8 ページ)

2025 年 12 月

クラウド提供型 Firewall Management Center に対する更新

Security Cloud Control がクラウド提供型 Firewall Management Center の更新をリリースしました。詳細については、[クラウド提供型 Firewall Management Center のリリースノート \[英語\]](#) を参照してください。

AIOps におけるセキュリティインサイトの導入

このリリースでは、組織全体の不審なアクティビティの可視化するために、**セキュリティインサイト**が導入されました。信頼レベルの上昇やその他の不審なユーザーの動作を示す**ユーザーリスクスパイク**など、進化しつづけるセキュリティリスクを特定して対応できるようになりました。

[セキュリティに関するインサイト](#)を参照してください。

2025 年 12 月 4 日

MSSPポータル新しい正常性ダッシュボード

このリリースでは、Cisco Secure Firewall ASA デバイスに正常性ダッシュボードが導入されています。

このダッシュボードには、CPU、メモリ、ディスク使用率、インターフェイス統計などの重要なパフォーマンス指標が表示されます。最適な運用を維持するために、パフォーマンスのボトルネックを早期に検出して能動的なアクションを実行できるようになりました。

詳細については、「[MSSP Portal](#)」の「[About Health Dashboard](#)」を参照してください。

2025 年 11 月

2025 年 11 月 20 日

クラウド提供型 Firewall Management Center に対する更新

Security Cloud Control がクラウド提供型 Firewall Management Center の更新をリリースしました。詳細については、[クラウド提供型 Firewall Management Center のリリースノート](#) [英語] を参照してください。

2025 年 11 月 13 日

パブリック API を使用した MSSP デバイスのアップグレード

Security Cloud Control ファイアウォール管理では、MSSP がテナント全体で Cisco Secure Firewall Threat Defense デバイスをアップグレードするための新しい API エンドポイントが提供されるようになりました。これには、MSSP ポータルが必要です。

詳細については、『[Security Cloud Control Firewall Management API Documentation](#)』を参照してください。

2025 年 11 月 6 日

Security Cloud Control が Catalyst SD-WAN NGFW 機能を管理

Security Cloud Control が Catalyst SD-WAN Manager と統合されるようになりました。これにより、Catalyst SD-WAN Manager によって管理されるセキュリティポリシーやオブジェクトなど、次世代ファイアウォール（NGFW）機能を一元管理できます。

Cisco Security Analytics and Logging を使用すると、ネットワークアクティビティが可視化されます。これにより、セキュリティイベントのモニター、分析、および対応が容易になります。

また、ネットワークで検出された、許可またはブロックされた侵入およびマルウェアイベントも表示できます。

詳細については、「[Managing Cisco Catalyst SD-WAN Firewall Capabilities with Security Cloud Control](#)」を参照してください。

シスコのセキュリティ分析とロギングの階層型サブスクリプションモデルの導入

このリリースでは、新しい階層型サブスクリプションモデルを提供するためにシスコのセキュリティ分析とロギングライセンスが更新されました。この新しい体系では、デフォルトの保持期間が延長され（1 年以上）、ストレージオプションも最大 10 TB に増加しています。固有のニーズに合わせて、Essentials、Advantage、または Premier 階層から選択できます。この更新により、価格設定が簡素化され、ファイアウォールログを管理する際の柔軟性と価値が向上します。

詳細については、「[Cisco Security Analytics and Logging Licenses](#)」を参照してください。

2025 年 10 月

2025 年 10 月 23 日

クラウド提供型 Firewall Management Center によって管理される Firewall Threat Defense デバイスの CLI サポート

クラウド提供型 Firewall Management Center によって管理される Firewall Threat Defense デバイスの CLI に Security Cloud Control インターフェイスを介してアクセスできるようになりました。[セキュリティデバイス (Security Devices)] > [FTD] に移動し、FTD を選択して、右側のペインで [コマンドラインインターフェイス (Command Line Interface)] を選択します。

詳細については、「[Use the Security Cloud Control Command Line Interface Tool](#)」を参照してください。

2025 年 9 月

2025 年 9 月 18 日

新しい AI Ops 機能の概要

AI Ops は、ファイアウォール管理に AI 主導のインテリジェンスをもたらし、能動的インサイトと実用的ガイダンスを提供して、運用を簡素化し、セキュリティを強化します。

次のような新機能があります。

- **AIOps概要ダッシュボード**: インサイトを統合した統合ビュー。デバイスのパフォーマンスの明確なスナップショットが表示されます。
- **ベストプラクティスと推奨事項**: ベストプラクティスからの逸脱を明らかにし、修復のガイダンスを提供する詳細な評価。
- **機能の活用**: ライセンスごとに分類された、アクティブに使用されている機能の可視化、テナント全体での活用率、および使用率を向上させるためのガイダンス。
- **ソフトウェア アップグレード プランナー**: アップグレードの決定を合理化するための、Cisco Secure Firewall Threat Defense デバイスに最適なアップグレードバージョンの提案（修正済みのバグやセキュリティ脆弱性の可視性を含む）。

これらの機能拡張は、**ポリシーアナライザ**と**オプティマイザ**などの既存の機能に追加され、AIOps を能動的で効率的なファイアウォール管理のための中央ハブとして位置付けます。

Secure Firewall ASA デバイスのデバイス正常性メトリックの導入

このリリースでは、Secure Firewall ASA デバイスのデバイス正常性メトリックが導入されました。このダッシュボードには、CPU、メモリ、ディスク使用率、ファンの状態、インターフェイス統計などの重要なパフォーマンス指標が表示されます。この可視性によって、最適な運用を維持するために、パフォーマンスのボトルネックを検出して能動的なアクションを実行できるようになりました。

詳細については、「[デバイス正常性メトリック](#)」を参照してください。

2025 年 8 月

2025 年 8 月 28 日

Security Cloud Control で CLI テンプレートを利用可能

新しいデバイスを設定するための CLI テンプレートを .txt ファイルとして管理およびエクスポートできるようになりました。CLI テンプレートにアクセスするには、左側のペインで [管理 (Administration)] をクリックし、[統合 (Integrations)] > [CLI テンプレート (CLI Templates)] の順に選択します。

詳細については、「[Manage CLI Templates](#)」を参照してください。

ハードウェアのサポート終了フィルタ

[セキュリティデバイス (Security Devices)] ページでデバイスをフィルタ処理して、サポート終了日が近づいている、またはサポート終了日が過ぎているハードウェアを特定できるようになりました。詳細ビューには、ライフサイクル計画に役立つ推奨交換デバイスも表示されます。

詳細については、「[Security Devices](#)」を参照してください。

2025 年 8 月 21 日

Microsoft Teams での Security Cloud Control の通知

Microsoft Teams で Security Cloud Control の通知を受信するには、Teams で着信ウェブフックを生成し、Security Cloud Control ([管理 (Administration)] > [通知設定 (Notification Settings)]) にウェブフックの URL を入力します。

詳細については、「[Incoming Webhooks for Microsoft Teams](#)」を参照してください。

クラウド提供型 Firewall Management Center に対する更新

Security Cloud Control がクラウド提供型 Firewall Management Center の更新をリリースしました。詳細については、[クラウド提供型 Firewall Management Center のリリースノート \[英語\]](#) を参照してください。

ユニバーサル ゼロトラスト ネットワーク アクセス (ユニバーサル ZTNA)

Security Cloud Control では、ユニバーサル ゼロトラスト ネットワーク アクセス (ユニバーサル ZTNA) 機能がリリースされました。ユニバーサル ZTNA は、ユーザーアイデンティティ、信頼、およびポスチャに基づいて、内部ネットワークリソースへのセキュアなアクセスを提供する包括的なソリューションです。これにより、リモートアクセス VPN のように、1 つのアプリケーションへのアクセスが暗黙的にネットワーク全体へのアクセス権を付与することがなくなります。[ポリシー (Policies)] > [Zero Trust アプリケーション (Zero Trust Application)] を使用してユニバーサル ZTNA を有効にします。詳細については、[Security Cloud Control のクラウド提供型 Firewall Management Center による Firewall Threat Defense の管理](#)を参照してください。

2025 年 7 月

2025 年 7 月 24 日

MSSP ポータル: セキュリティデバイスのページネーションとソートの強化

MSSP ポータルの [セキュリティデバイス (Security Devices)] ページに、[デバイス (Devices)]、[クラウドサービス (Cloud Services)]、[テンプレート (Templates)]、および [ファイアウォールマネージャ (Firewall Managers)] の専用タブが含まれるようになりました。この機能拡張により、ページのパフォーマンスが向上し、ページネーションとフィルタリングが合理化されます。これにより、セキュリティアセットのより効率的な管理が可能になります。

詳細については、「[Security Devices Details](#)」を参照してください。

Security Cloud Control ファイアウォールマネージャ API の更新

Security Cloud Control ファイアウォールマネージャ API が更新され、ASA デバイスの正常性メトリックを収集して表示し、MSSP ポータルインベントリを表示するための新しい API エンドポイントが追加されました。

イベントログ検索機能の更新

[イベントロギング (Event Logging)] ページの [バックグラウンド検索 (Background Search)] ボタンの名前が [レポート (Reports)] に変更されました。ボタンの機能に変更はありませんが、バックグラウンドでイベントログ検索を実行したり、生成されたレポートを管理したりすることができます。

詳細については、「[Search Historical Events in the Background](#)」を参照してください。

クラウド提供型 Firewall Management Center デバイスバックアップの更新

クラウド提供型 Firewall Management Center の次のアップグレードからは、最新の 5 つの Firewall Threat Defense バックアップのみが保持されます。古いバックアップはすべて自動的に削除されます。

2025 年 5 月 1 日のシスコの発表に従って必要なバックアップをプライベート環境にダウンロードしていない場合は、データへの継続的なアクセスを確保するために、2025 年 7 月 31 日までに必要なバックアップをダウンロードしてください。

デバイスのバックアップをダウンロードする方法については、「[Restore a Firewall Firewall Threat Defense device](#)」を参照してください。

2025 年 7 月 3 日

クラウド提供型 Firewall Management Center に対する更新

Security Cloud Control がクラウド提供型 Firewall Management Center の更新をリリースしました。詳細については、[クラウド提供型 Firewall Management Center のリリースノート \[英語\]](#)を参照してください。

サンプルフィルタを使用した拡張イベント検索

このリリースでは、検索エクスペリエンスを向上させるために、[イベントロギング (Event Logging)] ページにサンプルフィルタが導入されました。これらのフィルタでは、一般的な検索クエリが検索バーに即座に入力されます。これにより、検索クエリを手動で入力する必要性が減少します。サンプルフィルタを選択し、特定のニーズに合わせて検索パラメータを編集するだけで検索できます。

詳細については、「[Use Sample Filters to Search Events](#)」を参照してください。

Firewall 移行ツールの更新

Security Cloud Control は、Secure Firewall 移行ツールの更新バージョンをリリースしました。主な更新には、Azure ファイアウォールの Firewall Threat Defense への移行、Checkpoint および Fortinet ファイアウォールの Multicloud Defense への移行、ポリシー管理の簡素化などが含まれます。詳細については、『[Cisco Secure Firewall 移行ツールリリースノート](#)』を参照してください。

2025 年 6 月

2025 年 6 月 12 日

Cisco Security Cloud Control 統合プラットフォームを利用可能

APJ、AUS、EU、インド、および米国の Cisco Security Cloud Control テナントの Cisco Security Cloud Control 統合プラットフォームへの移行が発表されました。

Security Cloud Control 統合プラットフォームにアクセスするには、<https://security.cisco.com/> に移動し、ホームページから **[製品 (Products)]** > **[ファイアウォール (Firewall)]** の順に選択します。

なお、Security Cloud Control 統合プラットフォームの **[ファイアウォール (Firewall)]** ダッシュボードから、現在のすべてのファイアウォール設定および構成に引き続きアクセス可能です。

簡素化されたサイト間 VPN ウィザード

Security Cloud Control は、サイト間 VPN トンネルの作成を簡素化および迅速化するための拡張された統合ウィザードを備えています。この直感的なステップバイステップのガイド付きウィザードを使用すると、数回クリックするだけで複数の VPN 接続をシームレスに設定および管理できます。VPN トンネルの作成は Secure Firewall ASA、クラウド提供型 Firewall Management Center 管理対象 Firewall Threat Defense、Multicloud Defense、およびエクストラネットデバイスでサポートされており、VPN 管理に対する一元化され、合理化されたアプローチが提供されます。

詳細については、「[Introduction to Site-to-Site Virtual Private Network](#)」を参照してください。

ストレージ使用率ダッシュボードの新しいウィジェット

ロギングの傾向を特定し、ストレージを効果的に管理するための新しいウィジェットが導入されました。これらのウィジェットは最適化されたバージョンの SAL イベントロギングを使用している場合にのみ利用できることに注意してください。

- イベントの取り込み率を追跡するための EPS の傾向。
- ストレージの使用パターンをモニタリングするためのイベントタイプ別およびデバイスタイプ別の使用率の傾向。
- 上位デバイスのストレージ使用率を示すデバイス別の使用率の傾向。

詳細については、「[View Security Analytics and Logging Storage Usage and Event Ingest Rate](#)」を参照してください。

2025 年 4 月

2025 年 4 月 23 日

クラウド提供型 Firewall Management Center によって管理される Cisco Secure Firewall Threat Defense バージョン 7.0.x デバイスのサポート終了のお知らせ

2025 年 10 月 22 日以降、クラウド提供型 Firewall Management Center は、バージョン 7.0.x を実行している Cisco Secure Firewall Threat Defense デバイスの管理をサポートしません。継続的な保護と最新の機能へのアクセスを確保するには、2025 年 10 月 22 日までにバージョン 7.2.x 以降（シスコ推奨バージョンは 7.4.2）にアップグレードする必要があります。

2025 年 10 月 22 日以降、バージョン 7.0.x を実行している Cisco Secure Firewall Threat Defense デバイスに変更を加えたり展開したりすることはできません（アップグレードまたは登録解除を除く）。

詳細については、「[よくある質問 \(FAQ\)](#)」を参照してください。

2025 年 4 月 10 日

AIOps のベストプラクティスと推奨事項

「ベストプラクティスと推奨事項」機能は、デバイスの評価を実行し、失敗したチェック項目を強調表示し、詳細レポートを生成します。Cisco Secure Firewall のベストプラクティスに沿って全体的なパフォーマンスを向上させるための是正措置を推奨します。

詳細については、「[Implement Best Practices and Recommendations](#)」を参照してください。

2025 年 3 月

2025 年 3 月 13 日

クラウド提供型 Firewall Management Center に対する更新

Security Cloud Control がクラウド提供型 Firewall Management Center の更新をリリースしました。詳細については、[クラウド提供型 Firewall Management Center のリリースノート \[英語\]](#)を参照してください。

2025 年 3 月 6 日

Firewall 移行ツールの更新

Security Cloud Control は、Firewall 移行ツールの更新バージョンをリリースしました。新機能には、Secure Firewall ASA および Palo Alto Networks ファイアウォールから Multicloud Defense への設定の移行が含まれます。

詳細については、『[Cisco Secure Firewall 移行ツール リリースノート](#)』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。