Security Cloud Control の新機能

最終更新：2026 年 9 月 15 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 –2026 Cisco Systems, Inc. All rights reserved.

目 次

第 I 部 : Security Cloud Control：新機能 7

第 1 章 2026 年の新機能 1

2026 年 6 月 1

2026 年 6 月 4 日 1

2026 年 5 月 1

2026 年 5 月 7 日 1

2026 年 4 月 2

2026 年 4 月 23 日 2

2026 年 3 月 2

2026 年 3 月 26 日 2

2026 年 3 月 19 日 3

2026 年 3 月 12 日 3

2026 年 2 月 4

2026 年 2 月 19 日 4

2026 年 2 月 5 日 4

2026 年 1 月 4

2026 年 1 月 29 日 4

第 2 章 2025 年の新機能 5

2025 年 12 月 5

クラウド提供型 Firewall Management Center に対する更新 5

2025 年 12 月 4 日 6

2025 年 11 月 6

2025 年 11 月 20 日 6
2025 年 11 月 13 日 6
2025 年 11 月 6 日 6
2025 年 10 月 7
2025 年 10 月 23 日 7
2025 年 9 月 7
2025 年 9 月 18 日 7
2025 年 8 月 8
2025 年 8 月 28 日 8
2025 年 8 月 21 日 9
クラウド提供型 Firewall Management Center に対する更新 9
2025 年 7 月 9
2025 年 7 月 24 日 9
2025 年 7 月 3 日 10
2025 年 6 月 11
2025 年 6 月 12 日 11
2025 年 4 月 12
2025 年 4 月 23 日 12
2025 年 4 月 10 日 12
2025 年 3 月 12
2025 年 3 月 13 日 12
2025 年 3 月 6 日 13

第 3 章 **2024 の新機能** 15
2024 年 12 月 15
2024 年 12 月 12 日 15
2024 年 12 月 5 日 16
2024 年 11 月 16
Security Cloud Control の概要 16
2024 年 11 月 21 日 17
2024 年 11 月 7 日 17

2024 年 10 月 18
2024 年 10 月 17 日 18
2024 年 9 月 18
2024 年 9 月 13 日 18
2024 年 9 月 5 日 18
2024 年 8 月 19
2024 年 8 月 23 日 19
2024 年 8 月 8 日 20
2024 年 6 月 21
2024 年 6 月 27 日 21
2024 年 6 月 20 日 21
2024 年 6 月 13 日 21
2024 年 6 月 6 日 22
2024 年 5 月 23
2024 年 5 月 30 日 23
2024 年 5 月 23 日 23
2024 年 5 月 16 日 24
2024 年 4 月 25
2024 年 4 月 25 日 25
2024 年 4 月 18 日 25
2024 年 3 月 25
2024 年 3 月 7 日 25
2024 年 2 月 26
2024 年 2 月 13 日 26
2024 年 1 月 26
2024 年 1 月 25 日 26

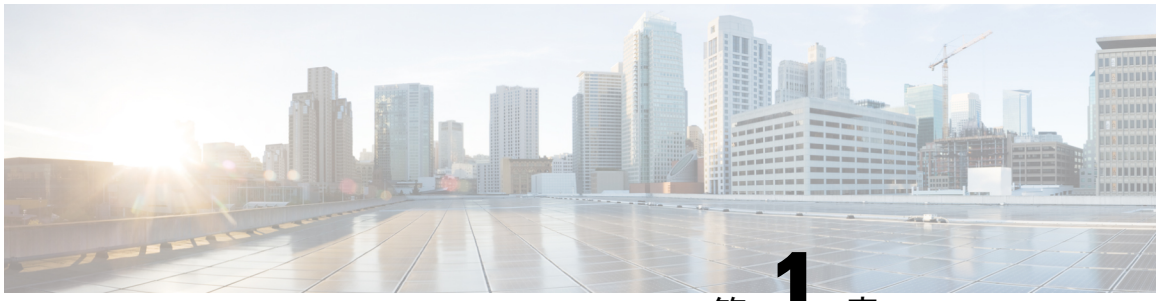
第 4 章 2023 の機能概要 27
2023 年 12 月 27
2023 年 12 月 14 日 27
2023 年 12 月 7 日 28

2023 年 11 月 28
2023 年 11 月 30 日 28
2023 年 11 月 14 日 28
2023 年 11 月 2 日 29
2023 年 10 月 30
2023 年 10 月 26 日 30
2023 年 10 月 19 日 30
2023 年 10 月 12 日 30
2023 年 10 月 5 日 31
2023 年 9 月 32
2023 年 9 月 14 日 32
2023 年 9 月 7 日 32
2023 年 8 月 34
2023 年 8 月 31 日 34
2023 年 8 月 17 日 34
2023 年 8 月 3 日 35
2023 年 7 月 35
2023 年 7 月 20 日 35
2023 年 7 月 13 日 36
2023 年 6 月 36
2023 年 6 月 29 日 36
2023 年 6 月 15 日 36
2023 年 6 月 8 日 37
2023 年 6 月 5 日 37
2023 年 6 月 1 日 37
2023 年 4 月 38
2023 年 4 月 27 日 38
2023 年 3 月 38
2023 年 3 月 23 日 38
2023 年 1 月 38
2023 年 1 月 18 日 38

第 I 部

Security Cloud Control：新機能

- 2026 年の新機能 （1 ページ）
- 2025 年の新機能 （5 ページ）
- 2024 の新機能 （15 ページ）
- 2023 の機能概要 （27 ページ）



第 1 章

2026 年の新機能

これらは、2026 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。

- 2026 年 6 月 （1 ページ）
- 2026 年 5 月 （1 ページ）
- 2026 年 4 月 （2 ページ）
- 2026 年 3 月 （2 ページ）
- 2026 年 2 月 （4 ページ）
- 2026 年 1 月 （4 ページ）

2026 年 6 月

2026 年 6 月 4 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。

2026 年 5 月

2026 年 5 月 7 日

ASA でマルチテナントデバイスのアップグレードを利用可能

クラウド提供型 Firewall Management Center 管理対象 Cisco Secure Firewall Threat Defense デバイスの一括アップグレードに加えて、複数のテナントの ASA を一括アップグレードできるようになりました。

詳細については、「MSSP ポータルでのマルチテナントデバイスのアップグレードについて」を参照してください。

2026 年 4 月

2026 年 4 月 23 日

クラウド展開によるマルチクラウド セキュリティ セットアップの簡素化

新しいクラウド導入機能により、Amazon Web Services（AWS）、Azure、および Google Cloud Platform（GCP）全体での Cisco Secure Firewall Threat Defense Virtual（FTDv）および Multicloud Defense の設定が合理化されます。なお、このリリースにおける Oracle Cloud Infrastructure（OCI）は、Multicloud Defense ゲートウェイでのみサポートされています。このガイド付き設定ツールは、特定のユースケースに最適な適用ポイントを選択して起動するために役立ち、複雑なマルチクラウド環境で高いパフォーマンスと拡張性に優れたネットワークセキュリティを実現できます。クラウド導入では、簡素化されたステップバイステップのセットアップにより、アカウント設定、トラフィックフロー、およびアーキテクチャ要件を簡単に定義できます。

詳細については、「クラウドの導入」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。

2026 年 3 月

2026 年 3 月 26 日

ファイアウォール MSP ポータルが Security Cloud Control に統合

マネージド サービス プロバイダー（MSP）ポータルが Security Cloud Control の Multi-Org 機能に完全に統合されました。この統合プラットフォームにより、マネージド サービス プロバイダーは、単一の一元管理インターフェイスから複数の顧客組織を効率的に管理できます。

主な機能は次のとおりです。

- 一元管理：単一ポータル内の複数の顧客組織をシームレスに管理できます。
- 包括的なモニタリング：すべての管理対象環境におけるデバイスの正常性、設定、および接続ステータスをモニターできます。

- 一括アップグレード：すべてのテナントで クラウド提供型 Firewall Management Center（cdFMC）によって管理される Cisco Secure Firewall Threat Defense デバイスでアップグレードを実行できます。
- 強化された可視性：管理対象のすべてのファイアウォール組織に関する統合された詳細情報にアクセスできます。

あなたへの影響

- アクセス：security.cisco.com から直接新しいポータルを使用します。
- レガシーポータルの廃止：以前の MSP ポータルはまもなく廃止されます。
- サポート：今後のサポートは、統合された Security Cloud Control プラットフォームについてのみ提供されます。

詳細については、「マネージド サービス プロバイダー向け Security Cloud Control ファイアウォール管理の概要」を参照してください。

2026 年 3 月 19 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。

2026 年 3 月 12 日

新しいスマート ライセンシング ダッシュボード

Cisco Secure Firewallにスマート ライセンシング ダッシュボードが導入されました。このダッシュボードには、ライセンスの使用状況、ライセンスタイプ、および規則遵守ステータスが統合されたビューが表示されるため、デバイスがライセンスを取得しており、規則遵守を維持していることを確認できます。この機能は現在、限定リリースで利用可能です。この限定リリース機能へのアクセスをリクエストするには、アカウントチームまたはシスコ営業担当者にお問い合わせください。

詳細については、「スマート ライセンシング ダッシュボードの概要」を参照してください。

MSSP ポータルの新しいスマート ライセンシング ダッシュボード

Cisco Secure Firewall の MSSP ポータルにスマート ライセンシング ダッシュボードが導入されました。このダッシュボードには、ライセンスの使用状況、ライセンスタイプ、および規則遵守ステータスが統合されたビューが表示されるため、デバイスがライセンスを取得しており、規則遵守を維持していることを確認できます。この機能は現在、限定リリースで利用可能で

す。この限定リリース機能へのアクセスをリクエストするには、アカウントチームまたはシスコ営業担当者にお問い合わせください。

詳細については、「スマート ライセンシング ダッシュボードの概要」を参照してください。

2026 年 2 月

2026 年 2 月 19 日

新しいスマート ライセンシング ダッシュボード

Cisco Secure Firewallにスマート ライセンシング ダッシュボードが導入されました。このダッシュボードには、ライセンスの使用状況、ライセンスタイプ、および規則遵守ステータスが統合されたビューが表示されるため、デバイスがライセンスを取得しており、規則遵守を維持していることを確認できます。この機能は現在、限定リリースで利用可能です。この限定リリース機能へのアクセスをリクエストするには、アカウントチームまたはシスコ営業担当者にお問い合わせください。

詳細については、「スマート ライセンシング ダッシュボードの概要」を参照してください。

2026 年 2 月 5 日

アプリケーションインサイトの導入

AIOpsに**アプリケーションインサイト**機能が追加されました。これにより、ThousandEyes Internet Insights を使用してクラウドアプリケーションの障害をプロアクティブに検出できます。監視対象アプリケーションについて、影響を受けたアプリケーション、影響を受けたドメイン、障害の継続時間、および影響を受けたリージョンが示されます。

詳細については、「Detect Application Outages」を参照してください。

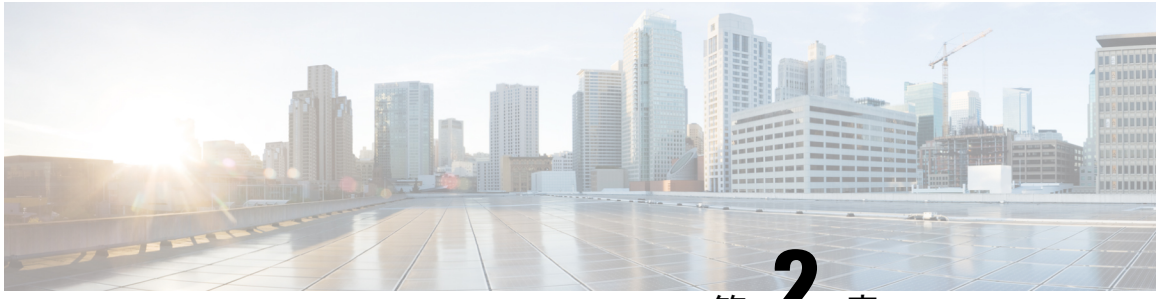
2026 年 1 月

2026 年 1 月 29 日

MSSPポータルでのマルチテナントデバイスのアップグレード

MSSPポータルの新しいアップグレードビューを使用して、クラウド提供型Firewall Management Center (cdFMC)で管理される、複数のテナントにわたるCisco Secure Firewall Threat Defenseデバイスを一括アップグレードできるようになりました。

詳細については、「MSSP ポータルでのマルチテナントデバイスのアップグレードについて」を参照してください。



第 2 章

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 （5 ページ）
- 2025 年 11 月 （6 ページ）
- 2025 年 10 月 （7 ページ）
- 2025 年 9 月 （7 ページ）
- 2025 年 8 月 （8 ページ）
- 2025 年 7 月 （9 ページ）
- 2025 年 6 月 （11 ページ）
- 2025 年 4 月 （12 ページ）
- 2025 年 3 月 （12 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ポータルの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AIOps機能の概要

AIOps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 の次回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。

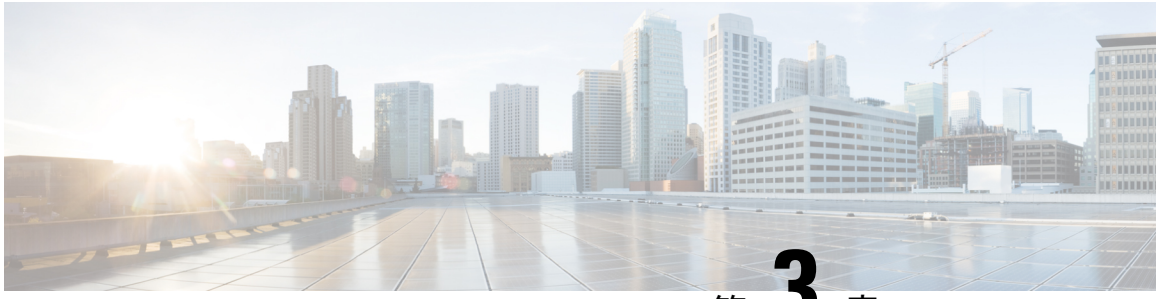
2025 年 3 月 6 日

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。

2025 年 3 月 6 日



第 3 章

2024 の新機能

この章では、2024 年に Cisco Defense Orchestrator に追加された機能の一部について説明します。

- 2024 年 12 月 （15 ページ）
- 2024 年 11 月 （16 ページ）
- 2024 年 10 月 （18 ページ）
- 2024 年 9 月 （18 ページ）
- 2024 年 8 月 （19 ページ）
- 2024 年 6 月 （21 ページ）
- 2024 年 5 月 （23 ページ）
- 2024 年 4 月 （25 ページ）
- 2024 年 3 月 （25 ページ）
- 2024 年 2 月 （26 ページ）
- 2024 年 1 月 （26 ページ）

2024 年 12 月

2024 年 12 月 12 日

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

Security Cloud Control は、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。

クラウド提供型 Firewall Management Center 評価ライセンスの更新

クラウド提供型 Firewall Management Center で 90 日間の評価ライセンスが提供されるようになりました。この期間が経過した後も、Firewall Threat Defenseデバイスをオンボーディングできますが、クラウド提供型 Firewall Management Center が Cisco Smart Software Manager に登録さ

れるまで展開はブロックされます。評価期間の有効期限が近づくと、Security Cloud Control でアラート通知を受信します。

詳細については、「Cloud-Delivered Firewall Management Center Licenses」を参照してください。

2024 年 12 月 5 日

Secure Device Connector と Secure Event Connector を Ubuntu VM 上で管理

CentOS 7 がサポート終了ステータスに達したため、Security Cloud Control では、オンプレミスの Secure Device Connector（SDC）および Secure Event Connector（SEC）での CentOS 7 の使用が非推奨になりました。SDC および SEC が、Ubuntu VM にインストールおよび維持されるようになりました。SDC および SEC を Ubuntu に移行すると、それらのアプリケーションの更新を確実に受け取ることができます。

移行プロセスの詳細については、「Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine」を参照してください。

2024 年 11 月

Security Cloud Control の概要

Cisco Defense Orchestrator は「Security Cloud Control」になりました。

Security Cloud Control は、ネットワークセキュリティから始めて、Cisco Security Cloud を統合するように設計された新しい人工知能組み込みの管理機能ソリューションであり、更新されたユーザーインターフェイス、共通サービス、およびセキュリティクラウド全体の設定、ログやアラートを接続するサービスメッシュを備えた最新のマイクロアプリ アーキテクチャです。

Cisco Secure Firewall Threat Defense と ASA ファイアウォール、Multicloud Defense、および Hypershield を管理し、それらの管理機能を追加のセキュリティ製品に拡張します。さらに、Cisco AI Assistant はポリシーと設定をプロアクティブに最適化し、問題を検出してトラブルシューティングします。

次の Security Cloud Control の新機能を確認してください。

- ネットワーク セキュリティ ソリューションの一元管理エクスペリエンス
- Firewall Threat Defense のデバイスを迅速にオンボーディングし、新機能を発見するのに役立つガイド付きの「Day 0」エクスペリエンス
- すべての管理対象デバイスをエンドツーエンドで可視性化する統合ダッシュボード
- アップグレードされたメニューナビゲーションと簡単なネットワークおよびセキュリティアプリケーションへのアクセスにより、合理化されたソリューションのユーザビリティ
- ファイアウォールルールの作成と管理を容易にする 人工知能アシスタント

- AIOps Insights による運用のシンプル化と強化されたセキュリティ
- セキュリティ態勢を改善し、不良構成を排除し、ルールを最適化するためのポリシー分析。
- 一貫したポリシーの適用とオブジェクト共有により強化されたハイブリッド環境での保護
- リモートアクセスおよびサイト間 VPN 接続のモニタリングの改善
- 1 つのテナントで最大 1,000 ファイアウォールをサポートするための拡張性の向上

詳細については、Security Cloud Control の製品ページ、Security Cloud Control のドキュメント、および『Cisco Security Cloud Control のよくある質問（FAQ）』を参照してください。

2024 年 11 月 21 日

Cisco Talos とのイベントデータの共有

シスコの脅威インテリジェンスグループである Talos とのイベントデータの共有を有効または無効にできるようになりました。イベントデータを共有することで、Talos は、脅威検出および対応能力が向上し、お客様のネットワークにターゲットを絞ったセキュリティインサイトを提供できるようになります。この機能は、デフォルトでイネーブルにされています。この設定を変更するには、**[管理（Administration）]** > **[一般設定（General Settings）]** をクリックします。

2024 年 11 月 7 日

Firewall 移行ツールの更新

Cisco Security Cloud Control（旧 Cisco Defense Orchestrator）は、Firewall 移行ツールの更新バージョンをリリースしました。サイト間 VPN 設定の事前共有キーの一括更新を実行し、移行対象の設定にエラーを含むパラメータがある場合に移行を続行するか中止するかを選択し、ターゲット Threat Defense デバイスをスポークとして既存のハブやスポーク VPN 設定などに追加できるようになりました。リリースに含まれる機能のリストについては、『Cisco Secure Firewall 移行ツール リリースノート』を参照してください。

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

Cisco Defense Orchestrator は、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。

2024 年 10 月

2024 年 10 月 17 日

マルチテナントポータルでのテナントの作成

テナントを作成し、ユーザーを追加して、プロビジョニングされたテナントでクラウド提供型 Firewall Management Center と Multicloud Defense を有効にできるようになりました。

詳細については、「Manage Multi-Tenant Portal」[英語] を参照してください。

2024 年 9 月

2024 年 9 月 13 日

ポリシーアナライザとオプティマイザを使用したセキュリティポリシーの分析と最適化

新しいポリシーアナライザとオプティマイザを使用して、ポリシーを分析し、異常を検出し、キュレーションされた修復の推奨事項を受信できるようになりました。推奨事項を適用すると、ポリシーが常に最適な状態になり、ファイアウォールのパフォーマンスが向上します。このツールは、クラウド提供型 Firewall Management Center と CDO 管理対象のオンプレミス Firewall Management Center バージョン 7.2 以降の両方のポリシーを分析できます。左側のペインで、**[インサイト（Insights）] > [ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）]** を選択します。

詳細については、「Analyzing, Detecting, and Fixing Policy Anomalies Using Policy Analyzer and Optimizer」[英語] を参照してください。

2024 年 9 月 5 日

Firewall 移行ツールの更新

Cisco Secure Firewall ASA HA ペアから Threat Defense デバイスに設定を移行するときに、移行ツールで Threat Defense の高可用性（HA）ペアを設定できるようになりました。さらに、Cisco Cisco Secure Firewall ASA からサイト間 VPN 設定を移行するときに、サイト間ハブアンドスポーク VPN トポロジを設定できます。

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。

Cisco Defense Orchestrator を使用した Cisco Secure Firewall Threat Defense 3100、4100、4200、または 9300 シャーシのオンボード

Firepower 3100、4100、4200、または 9300 シャーシを Cisco Defense Orchestrator を介して クラウド提供型 Firewall Management Center に追加できるようになりました。

管理センターとシャーシは、シャーシ MGMT インターフェイスを使用して個々の管理接続を共有します。Management Center は、シャーシレベルの正常性アラートを提供します。4100 または 9300 を設定する場合は、引き続き Cisco Secure Firewall Chassis Manager または FXOS CLI を使用する必要があります。3100 または 4200 の場合は、クラウド提供型 Firewall Management Center 内のシャーシ管理インターフェイスを使用できます。詳細については、「Onboard a Chassis」[英語] を参照してください。

2024 年 8 月

2024 年 8 月 23 日

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

Cisco Defense Orchestrator は、クラウド提供型 Firewall Management Center の更新をリリースしました。次に、更新の主要部分を示します。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。

プラットフォーム

- Threat Defense バージョン 7.6.0 のサポート

高可用性/拡張性

- Cisco Secure Firewall 3100 のマルチインスタンスモード

アクセス制御：脅威の検出とアプリケーションの識別

- 機密性の高い、復号できないトラフィックの復号のバイパス

アクセス制御：アイデンティティ

- ユーザー アイデンティティ ソースとしての Microsoft Azure AD

ヘルス モニタリング

- 正常性データの収集（アラートなし）
- Firepower 4100/9300 のシャーシレベルの正常性アラート

管理

- Threat Defense の高可用性は、バックアップから復元した後に自動的に再開されます。

- 変更管理チケットの引き継ぎ、承認ワークフローのその他の機能。

トラブルシューティング

- CPU とルールプロファイラを使用して Snort 3 のパフォーマンスの問題をトラブルシュートします。

Management Center REST API

- Management Center REST API の更新。

2024 年 8 月 8 日

汎用テキスト Dynamic Attributes コネクタのサポート

汎用テキスト Dynamic Attributes コネクタを使用すると、IP アドレスのリストをテキストファイルで維持し、そのリストを使用してアクセス コントロール ポリシーを適用できます。たとえば、アクセス制御ルールの「許可リスト」または「ブロックリスト」の IP アドレスのリストを使用できます。IP アドレスを含むテキストファイルが更新されると、Cisco Secure Dynamic Attributes コネクタは、その IP アドレスリストを使用するアクセス制御ルールを定期的に更新します。テキストファイルごとに最大 10,000 個の IP アドレスを指定できます。詳細については、「Creating a Generic Text」[英語] を参照してください。

Multicloud Defense の VPN トンネルサポート

Multicloud Defense に VPN トンネルを作成し、Multicloud Defense Gateway を 1 つのエンドポイントとし、管理対象デバイスまたは GCP などのクラウド サービス プロバイダーをもう 1 つのエンドポイントとして作成できるようになりました。詳細については、Multicloud Defense ユーザーガイド [英語] を参照してください。

CDO の拡張監査ログ

監査ログに、ユーザーログイン、テナントの関連付けと関連付け解除、ユーザーロールの変更、Active Directory グループの変更など、ユーザー関連およびシステムレベルのアクションが表示されるようになりました。

詳細については、「Audit Logs」[英語] を参照してください。

2024 年 6 月

2024 年 6 月 27 日

アップグレードされた Cisco ASA アクセス コントロール ポリシー インターフェイス

CDO に、強化された共有アクセスリスト、簡素化されたルール管理、および強化された検索結果ナビゲーションを備えた、アップグレードされた Cisco ASA アクセス コントロール ポリシー インターフェイスが導入されました。

詳細については、「Manage ASA Network Security Policy」[英語] を参照してください。

2024 年 6 月 20 日

CDO の [イベントロギング（Event Logging）] ページに UTC とローカルタイムゾーンのトグルボタンが追加されました。この更新により、デバイスによって生成されたイベントは、ユーザーの選択に応じて、ローカルタイムゾーンまたは UTC のタイムスタンプで表示されるようになりました。デフォルトでは、イベントタイムスタンプはローカルタイムゾーンで表示されます。

詳細については、「Change the Time Zone for the Event Timestamps」[英語] を参照してください。

2024 年 6 月 13 日

アプリケーションモニタリング用の新しい Firewall Threat Defense ダッシュボードウィジェット

CDO には、[上位のWebアプリケーション（Top Web Applications）]、[上位のクライアントアプリケーション（Top Client Applications）]、[上位のブロックされたWebアプリケーション（Top Blocked Web Applications）]、[ブロックされた接続別の上位のユーザー（Top Users by Blocked Connections）] の 4 つの新しいダッシュボードウィジェットが追加されました。これらの新しいウィジェットでは、最も使用されている Web アプリケーションとクライアントアプリケーション、および最もブロックされた接続を持つユーザを一目で確認できます。Firewall Threat Defense ダッシュボードに表示される情報はシステムのライセンス方法、設定方法、デバイスの展開方法によって異なります。**[分析（Analytics）]** > **[FTD ダッシュボード（FTD Dashboard）]** をクリックして、新しいダッシュボードウィジェットを表示します。

詳細については、「About the FTD Dashboard」[英語] を参照してください。

Firewall Threat Defense から クラウド提供型 Firewall Management Center への移行を一時停止して、インポートされた共有ポリシーを確認する

Firewall Threat Defense から クラウド提供型 Firewall Management Center への移行プロセスを一時停止して、インポートされた共有ポリシー設定を確認できるようになりました。この段階では、評価期間は開始されず、Firewall Threat Defense のマネージャも変更されないため、設定を

確認する時間ができます。設定を確認後、移行プロセスを再開して、スケジュールされた移行期間中に クラウド提供型 Firewall Management Center にデバイス固有の設定をインポートできます。[ツールとサービス（Tools & Services）] > [cdFMCへのFTDの移行（Migrate FTD to cdFMC）] の順にクリックします。

詳細については、「Firewall Threat Defense から クラウド提供型 Firewall Management Center への移行」を参照してください。

2024 年 6 月 6 日

Cisco AI Assistant を使用したファイアウォール管理

CDO 管理者は、Cisco Defense Orchestrator（CDO）の Cisco AI Assistant とクラウド提供型 Firewall Management Center の統合により、Cisco Secure Firewall Threat Defense ポリシーをより効率的に管理し、ドキュメントにアクセスできるようになりました。Cisco AI Assistant には、いくつかの主要な機能があります。

- [事前有効化アシスタント（Pre-Enabled Assistant）]：Cisco AI Assistant は、すべての CDO テナントでデフォルトで有効になっています。必要に応じて、テナントの[一般設定（General Settings）] ページで無効化できます。
- [容易なアクセス（Easy Access）]：CDO のネットワーク管理者と管理者は、ロギング後にテナントのダッシュボードの上部にあるメニューバーから Cisco AI Assistant に直接アクセスできます。

- [ユーザーオリエンテーション（User Orientation）]：Cisco AI Assistant ウィジェットを初めて開くとカルーセルウィンドウが表示され、Cisco AI Assistant の紹介、データプライバシー保護に関する説明、効果的な使用に関するヒントが提供されます。
- [ポリシールールアシスタンス（Policy Rule Assistance）]：Cisco AI Assistant は、Cisco Secure Firewall Threat Defense デバイスでポリシールールの作成プロセスを簡素化します。管理者は、簡単なプロンプトを使用してアクセス制御ルールを迅速に作成できます。
- [製品ナレッジリソース（Product Knowledge Resource）]：Cisco AI Assistant には、CDO とクラウド提供型のファイアウォール管理のドキュメントが取り込まれており、サポートが必要な場合は、質問できます。
- **ユーザーフレンドリーなインターフェイス**：
  - [シンプルテキスト入力ボックス（Simple Text Input Box）]：ウィンドウの下部にあり、Cisco AI Assistant を簡単に操作できます。
  - [スレッド履歴（Thread History）]：Cisco AI Assistant に尋ねる質問や一連の質問は、スレッドと呼ばれます。Cisco AI Assistant にはスレッド履歴が保持されるため、自分の過去の質問を参照できます。

- [フィードバック（Feedback）]：Cisco AI Assistant の応答に対する高評価または低評価のフィードバックを提供します。

詳細については、『Cisco AI Assistant ユーザーガイド』を参照してください。

2024 年 5 月

2024 年 5 月 30 日

インドの CDO

CDO は現在、インドの https://in.cdo.cisco.com で入手できます。https://www.getcdo.com にアクセスして、インドでテナントを作成できます。

クラウド提供型 Firewall Management Center の更新

Cisco Defense Orchestrator は、クラウド提供型 Firewall Management Center の更新をリリースしました。この更新に含まれる多くの新機能については、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。

2024 年 5 月 23 日

オーストラリアの CDO

CDO は現在、オーストラリアの https://aus.cdo.cisco.com で入手できます。https://www.getcdo.com にアクセスして、オーストラリアでテナントを作成できます。

CDO API

CDO は、プログラムで CDO と対話できる RESTful API を提供するようになりました。API は、デバイス管理と展開、オブジェクト管理、検索、変更ログのモニタリング、ユーザー管理など、広範な CDO 機能へのアクセスを提供します。詳細については、Cisco Defense Orchestrator API Documentation [英語] を参照してください。また、CDO テナントの右上隅にあるユーザーメニューから移動して、CDO API ドキュメントにアクセスできます。

（注） CDO GraphQL API はサポート対象外、または使用不可となりました。

Firewall 移行ツールの更新

CDO は、Firewall 移行ツールの更新バージョンをホストするようになりました。Secure Firewall ASA デバイスから Firewall Threat Defense デバイスに移行する前に、ネットワークおよびポー

トオブジェクトを最適化でき、さらに、FDM による管理デバイスから Firewall Threat Defense デバイスに DHCP、DDNS、および SNMPv3 の設定を移行できます。

その他の新機能の詳細については、『Cisco Secure Firewall 移行ツール リリースノート』を参照してください。

CDO テナント通知とユーザー通知設定の再配置

通知とユーザー設定のタブが移動しました。[通知（Notifications）] は、**[設定（Settings）]** > **[通知設定（Notification Settings）]** の左側にあるナビゲーションバーに配置されており、電子メールサブスクリプションとサードパーティサービスの統合を管理できます。[ユーザー設定（User Preferences）] は、**[ユーザー名ID（Username ID）]** > **[設定（Preferences）]** > **[通知設定（Notification Preferences）]** に配置されており、テナントに関連付けられているデバイスで特定のアクションが発生したとき、デバイス証明書の期限が近いときや期限切れになったとき、またはバックグラウンドログ検索が開始、終了、または失敗したときにトリガーできます。[ユーザー通知設定（User Notification Preferences）] は個人ユーザーに固有の設定ですが、[テナント通知（Tenant Notifications）] はテナントに関係しているすべてのユーザーに適用されます。詳細については、「Tenant Management」[英語] を参照してください。

デバイス証明書の有効期限通知

CDO は、Cisco Secure Client（旧 AnyConnect）証明書の有効期限ステータスと、Cisco ASA、FDM による管理、および FTD デバイスの管理証明書を監視するようになりました。CDO は、各証明書の期限日が近づくか、期限切れになるとユーザーに通知します。

「Device Certificate Expiry Notification」[英語] を参照してください。

2024 年 5 月 16 日

Multicloud Defense の Cisco Security Cloud Control のサポート

Cisco Security Cloud Control Enterprise は、既存の Multicloud Defense アカウントの追加をサポートするようになりました。 Multicloud Defense タイルを Cisco Security Cloud Enterprise ダッシュボードに追加して、他のシスコ製品インスタンス、ユーザーアイデンティティの管理、および Cisco Security Cloud ポートフォリオ全体のユーザーアクセス管理を監視して一元化できます。詳細については、Multicloud Defense ユーザーガイド [英語] の「Multicloud Defense in Cisco Security Cloud Control」を参照してください。

2024 年 4 月

2024 年 4 月 25 日

CDO のダークテーマ

CDOは、よりカスタマイズ可能なユーザーインターフェイスの外観用にダークテーマオプションを提供するようになりました。右上隅にある[管理（admin）]ドロップダウンをクリックし、**[設定（Preferences）]**>**[一般設定（General Preferences）]**に移動し、[テーマ（Theme）]フィールドで[ダーク（Dark）]をクリックします。デフォルトのテーマは、[ライト（Light）]テーマです。

詳細については、「User Settings」[英語] を参照してください。

2024 年 4 月 18 日

オンプレミスの Cisco Secure Firewall Management Center へのネットワークオブジェクトの自動同期

CDO 内のネットワークオブジェクトを、CDO によって管理されるオンプレミス FMC に自動的かつ継続的に同期できるようになりました。この機能はデフォルトで無効になっています。この機能を有効にするには、[ツールとサービス（Tools & Services）] > [Firewall Management Center] に移動し、オンプレミス FMC を選択し、[アクション（Actions）] ペインで [設定（Settings）] を選択します。続いて、[ネットワークオブジェクトの検出と管理（Discover and Manage Network Objects）] をクリックし、[ネットワークオブジェクトの自動同期を有効にする（Enable automatic sync of network objects）] をクリックします。[ネットワークオブジェクトの検出と管理（Discover and Manage Network Objects）] トグルが有効になっていることを確認します。

詳細については、「Discover and Manage On-Prem Firewall Management Center Network Objects」[英語] を参照してください。

2024 年 3 月

2024 年 3 月 7 日

CDO テナントプロビジョニングの改善

強化された高速なプロビジョニングプロセスを使用して CDO テナントを作成できるようになりました。すでにテナントがある場合でも、新しい CDO テナントを作成できます。さらに、SecureX に対応していない オンプレミス Firewall Management Center がある場合、CDO を介し

て Cisco Security Cloud に登録できるようになりました。CDO アカウントがない場合は、登録プロセス時に作成できます。詳細については、「CDO テナントの作成」を参照してください。

個々の Firewall Threat Defense デバイスによる Cisco Cloud へのイベントログの送信の無効化

個々の クラウド提供型 Firewall Management Center管理対象 Firewall Threat Defense デバイス（バージョン 7.4.1 以降）で Cisco Cloud へのイベントログの送信を無効化できるようになりました。このデバイスレベルの制御を使用すると、必要に応じて、Firewall Threat Defense デバイスから Cisco Cloud に送信されるイベントログを一時的に停止できます。Cisco Cloud へのイベントログの送信を無効にする Firewall Threat Defense デバイスを指定するには、[インベントリ（Inventory）] をクリックし、対応する Firewall Threat Defense デバイスを選択して、[デバイス管理（Device Management）] ペインで [クラウドイベント（Cloud Events）] をクリックします。

Ubuntu での Secure Device Connector および Secure Event Connector のインストールの簡素化

Cisco DevNet サイトで利用可能な GitHub プロジェクト を使用して、Secure Device Connector と Secure Event Connector を Ubuntu サーバーに簡単に展開できるようになりました。詳細については、ドキュメントを参照するか、YouTube でビデオをご覧ください。

2024 年 2 月

2024 年 2 月 13 日

クラウド提供型 Firewall Management Center の更新

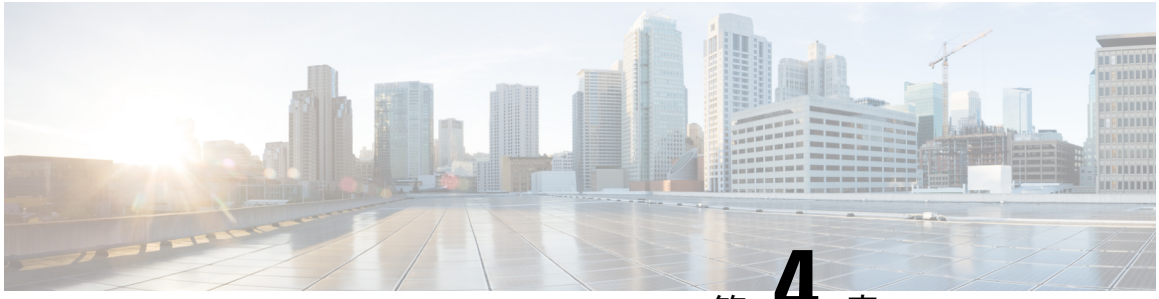
Cisco Defense Orchestrator は、クラウド提供型 Firewall Management Center の更新をリリースしました。この更新に含まれる多くの新機能については、クラウド提供型 Firewall Management Center のリリースノート [英語] を参照してください。

2024 年 1 月

2024 年 1 月 25 日

Firewall 移行ツールの更新

CDO は、Firewall 移行ツールの更新バージョンをホストするようになりました。Cisco Secure Firewall ASA の WebVPN 設定を、クラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスの Zero Trust Access Policy 設定に移行できるようになりました。また、マルチコンテキスト Cisco ASA デバイスからシングルインスタンスの Threat Defense デバイスに移行する場合は、SNMP、DHCP、DVTI 設定を Cisco ASA から Threat Defense デバイスに移行して、ECMP ルーティング設定を移行できます。リリースに含まれるその他の新機能については、『Cisco Secure Firewall 移行ツール リリースノート』を参照してください。



第 4 章

2023 の機能概要

この章では、2023 年に Cisco Defense Orchestrator に追加された機能の一部について説明します。

- 2023 年 12 月 （27 ページ）
- 2023 年 11 月 （28 ページ）
- 2023 年 10 月 （30 ページ）
- 2023 年 9 月 （32 ページ）
- 2023 年 8 月 （34 ページ）
- 2023 年 7 月 （35 ページ）
- 2023 年 6 月 （36 ページ）
- 2023 年 4 月 （38 ページ）
- 2023 年 3 月 （38 ページ）
- 2023 年 1 月 （38 ページ）

2023 年 12 月

2023 年 12 月 14 日

Threat Defense デバイスの追加イベントタイプの監視

CDO は、Threat Defense デバイス用の AAA 、BotNet、フェールオーバー、SSL VPN などの新しいファイアウォールイベントのタイプをサポートするようになりました。

[分析（Analytics）] > [イベントロギング（Event Logging）] に移動し、[FTDイベント（FTD Events）] で使用可能なイベントの新しいリストからフィルタ処理します。詳細については、「Event Types in CDO」[英語] を参照してください。

2023 年 12 月 7 日

CDO を使用したオンプレミス Firewall Management Center ネットワークオブジェクトの管理

CDO 管理対象オンプレミス Firewall Management Center から、他の オンプレミス Firewall Management Center や クラウド提供型 Firewall Management Center によって管理される Threat Defense デバイス、および CDO 管理対象 ASA や Firewall Threat Defense デバイスに対するのネットワークオブジェクトを管理および共有できるようになりました。その結果、CDO の管理対象プラットフォーム間でネットワークオブジェクトの定義の一貫性が促進されます。

オンプレミス Firewall Management Center をオンボーディング後、**[ツールとサービス（Tools & Services）] > [Firewall Management Center]** に移動し、デバイスを選択して [設定（Settings）] を選択し、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] トグルボタンを有効にします。

詳細については、「Discover and Manage On-Prem Firewall Management Center Network Objects」[英語] を参照してください。

2023 年 11 月

2023 年 11 月 30 日

クラウド提供型 Firewall Management Center での Cisco Secure Firewall Threat Defense デバイスバックアップのスケジュール

クラウド提供型 Firewall Management Center を使用して、管理する Cisco Secure Firewall Threat Defense デバイスのスケジュール済みバックアップを実行します。

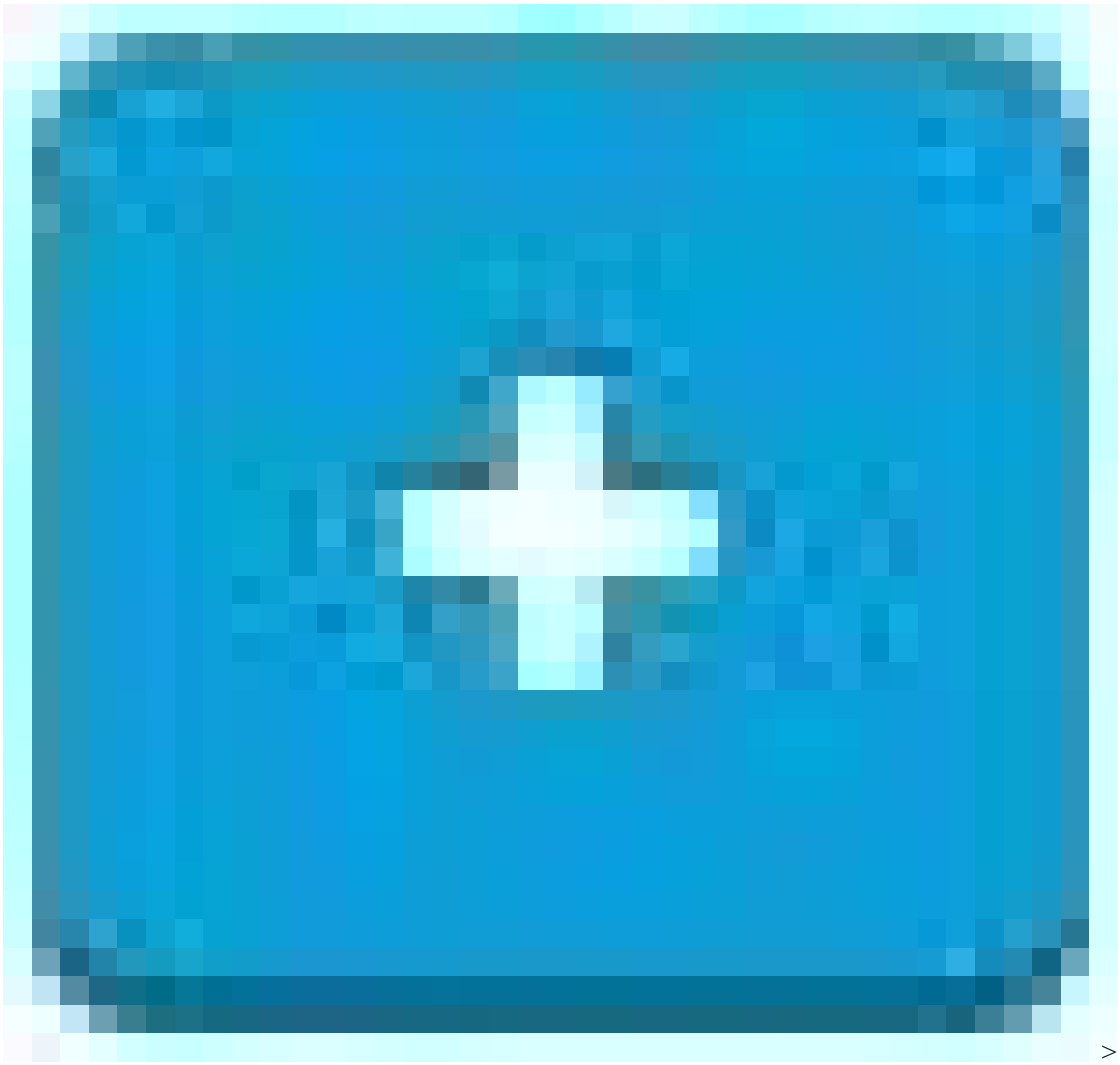
詳細については、「Schedule Remote Device Backups」[英語] を参照してください。

2023 年 11 月 14 日

クラウド提供型 Firewall Management Center のプロビジョニングの改善

CDO は、クラウド提供型 Firewall Management Center 用の拡張された高速なプロビジョニングプロセスを提供するようになりました。テナントでクラウド提供型 Firewall Management Center を有効にすると、CDO は自動的にプロビジョニングし、CDO 通知センター、および着信ウェブフックを設定したアプリケーションを介して通知します。有効にするには、**[ツールとサー**

ビス（**Tools & Services**）] > **[Firewall Management Center]** >



> **[FMC]** > **[クラウド提供型 FMCの有効化（Enable Cloud-Delivered FMC）]** の順に選択します。

詳細については、「Enable Cloud-delivered Firewall Management Center on Your CDO Tenant」[英語] および「Notification Settings」[英語] を参照してください。

2023 年 11 月 2 日

ゼロ タッチ プロビジョニング を使用したオンプレミス Management Center への Firewall Threat Defense デバイスのオンボード

ゼロタッチプロビジョニング メソッドを使用して Threat Defense デバイスをオンボードするときに、管理プラットフォームとして オンプレミス Firewall Management Center を選択できるようになりました。その結果、新しいデバイス、または以前に設定または管理されていないデバイスのオンプレミス管理がサポートされます。詳細については、「Onboard a Secure Firewall Threat Defense Device With Zero-Touch Provisioning」[英語] を参照してください。

2023 年 10 月

2023 年 10 月 26 日

Firewall 移行ツールの更新

CDO は、Firewall 移行ツールの更新バージョンをホストします。CDO を使用して、Cisco Secure Firewall ASA デバイスにある複数のトランスペアレント ファイアウォール モードのコンテキストをトランスペアレントモードのインスタンスにマージして移行できます。

さらに、サイト間およびリモートアクセス VPN 設定を Fortinet および Palo Alto Networks ファイアウォールから、シスコのクラウド提供型 Firewall Management Center で管理されている Threat Defense に移行できます。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。

2023 年 10 月 19 日

クラウド提供型 Firewall Management Center の更新

Cisco Defense Orchestrator は、クラウド提供型 Firewall Management Center の更新をリリースしました。更新に含まれる多くの新機能については、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。新機能の完全なリストについては、『クラウド提供型 Firewall Management Center のリリースノート：Cisco Defense Orchestrator の機能』を参照してください。

サイト間 VPN 接続を使用したオンプレミスからクラウド提供型 Firewall Management Center への Cisco Secure Firewall Threat Defense デバイスの移行

Cisco Secure Firewall Threat Defense デバイスのサイト間 VPN 設定は、デバイスがオンプレミスの Firewall Management Center からクラウド提供型 Firewall Management Center に移行されるときに、残りの設定とともに移行されるようになりました。詳細については、「Migrate On-Prem Management Center managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center」[英語] を参照してください。

2023 年 10 月 12 日

Cisco ASA システム設定ポリシー

CDO には、システム設定ポリシーを作成して、ドメインネームサービス、HTTP、セキュアコピーサーバーの有効化、メッセージロギング、アクセス制御リストをチェックしない VPN トラフィックの許可など、Cisco ASA デバイスの重要な設定を簡単に管理する機能があります。システム設定ポリシーは複数の Cisco ASA デバイスに適用でき、ポリシーに加えられた変更は、このポリシーを使用するすべてのデバイスに影響します。さらに、単一の Cisco ASA デバ

イスのデバイス固有の設定を個別に編集し、デバイス固有の値で共有システム設定をオーバーライドできます。

詳細については、「ASA System Settings」[英語] を参照してください。

[ポリシー（Policies）] > [Cisco ASAシステム設定（ASA System Settings）] の順に選択します。

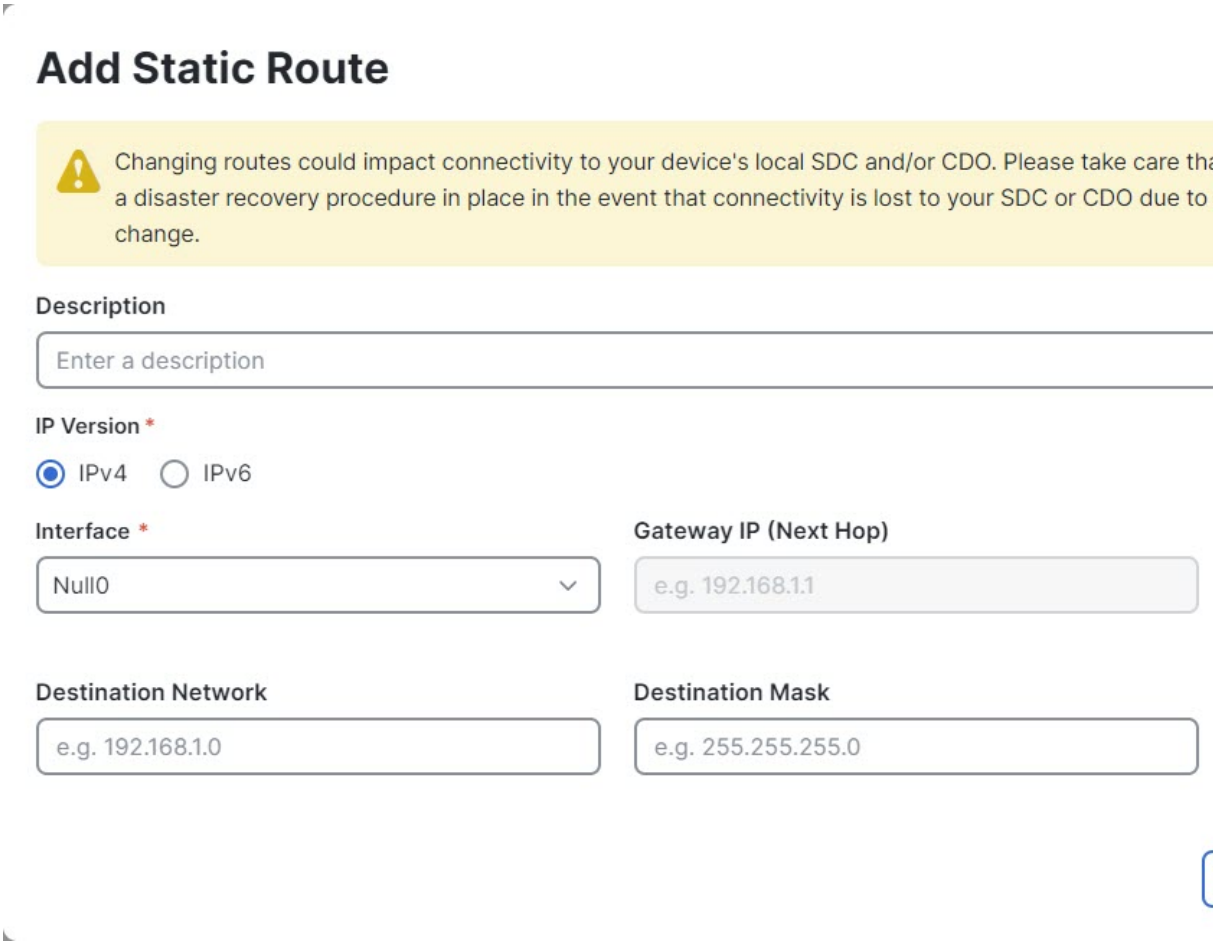
2023 年 10 月 5 日

Cisco ASA スタティックルーティングの CDO サポート

CDOユーザーインターフェイスを使用して、Cisco ASAのスタティックルートを設定できるようになりました。この機能を使用すると、CLIを使用せずに、特定のIPv4またはIPv6宛先ネットワークのトラフィックの送信先を指定できます。

詳細については、「ASA Static Routing」[英語] を参照してください。

[インベントリ（Inventory）] > [Cisco ASA（ASA）] タブ > [ルーティング（Routing）] の順に選択します。



Terraform を使用した CDO の管理

Terraform を使用し、Infrastructure as Code（IaC）の原則を使用して CDO インフラストラクチャの管理を自動化するできるようになりました。CDO は、セキュアなデバイスコネクタとセキュアなイベントコネクタを迅速に展開するための Terraform プロバイダーと Terraform モジュールを提供します。詳細については、「Terraform」[英語] を参照してください。

2023 年 9 月

2023 年 9 月 14 日

Secure Event Connector のナビゲーションの変更

右上の管理メニューを展開して [セキュアコネクタ（Secure Connectors）] ページにアクセスできなくなりました。セキュアコネクタを管理するには、**[ツールとサービス（Tools & Services）]** > **[セキュアコネクタ（Secure Connectors）]** の順に選択します。詳細については、「Secure Event Connectors」[英語] を参照してください。

2023 年 9 月 7 日

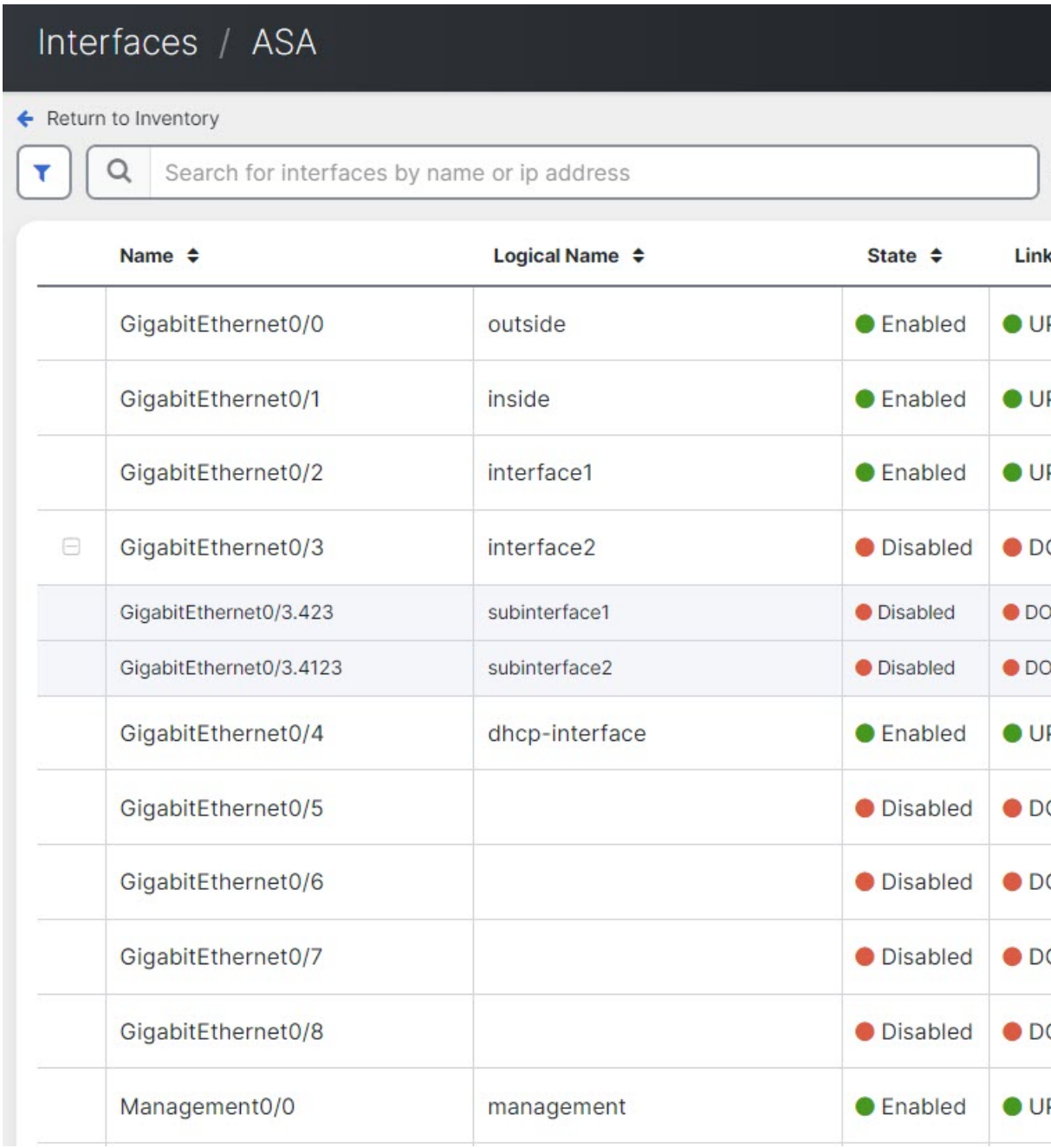
CDO ユーザーインターフェイスを使用した Cisco ASA インターフェイスの設定

CDO のグラフィカル ユーザー インターフェイスを使用して、Cisco ASA の物理ネットワークインターフェイス、論理的なサブインターフェイス、VLAN、および EtherChannel を設定できるようになりました。ルートベースのサイト間 VPN で作成された仮想トンネルインターフェイスも表示できます。

（注） VLAN では 110 デバイスのみサポートされます。

詳細については、「Configure ASA Interfaces」[英語] 参照してください。

[インベントリ（Inventory）]、[Cisco ASA（ASA）]、[管理（Management）]、[インターフェイス（Interfaces）] の順に選択します。

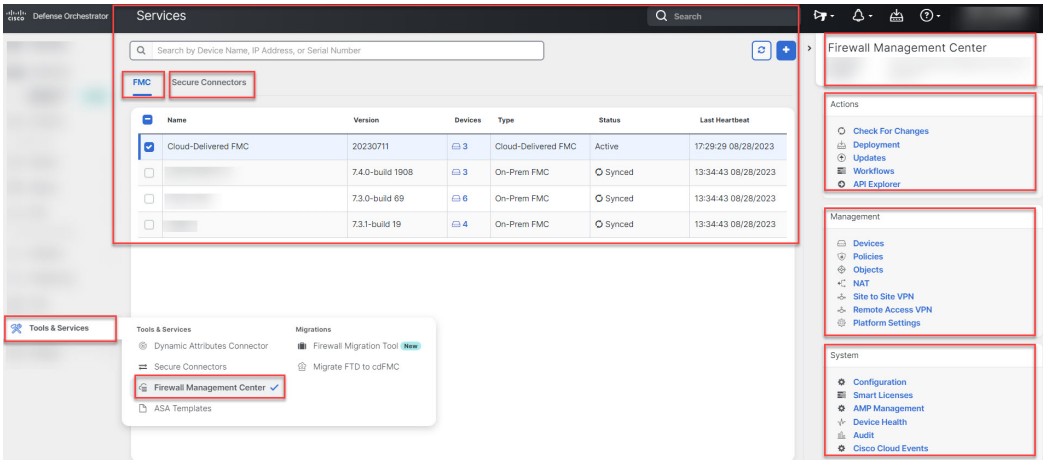

Interfaces / ASA
Return to Inventory
Search for interfaces by name or ip address
Name
Logical Name
State
Link
GigabitEthernet0/0
outside
Enabled
GigabitEthernet0/1
inside
Enabled
GigabitEthernet0/2
interface1
Enabled
GigabitEthernet0/3
interface2
Disabled
GigabitEthernet0/3.423
subinterface1
Disabled
GigabitEthernet0/3.4123
subinterface2
Disabled
GigabitEthernet0/4
dhcp-interface
Enabled
GigabitEthernet0/5
Disabled
GigabitEthernet0/6
Disabled
GigabitEthernet0/7
Disabled
GigabitEthernet0/8
Disabled
Management0/0
management
Enabled

2023 年 8 月

2023 年 8 月 31 日

[サービス（Services）] ページからのクラウド提供型 FMC、オンプレミス FMC、およびセキュアコネクタの管理

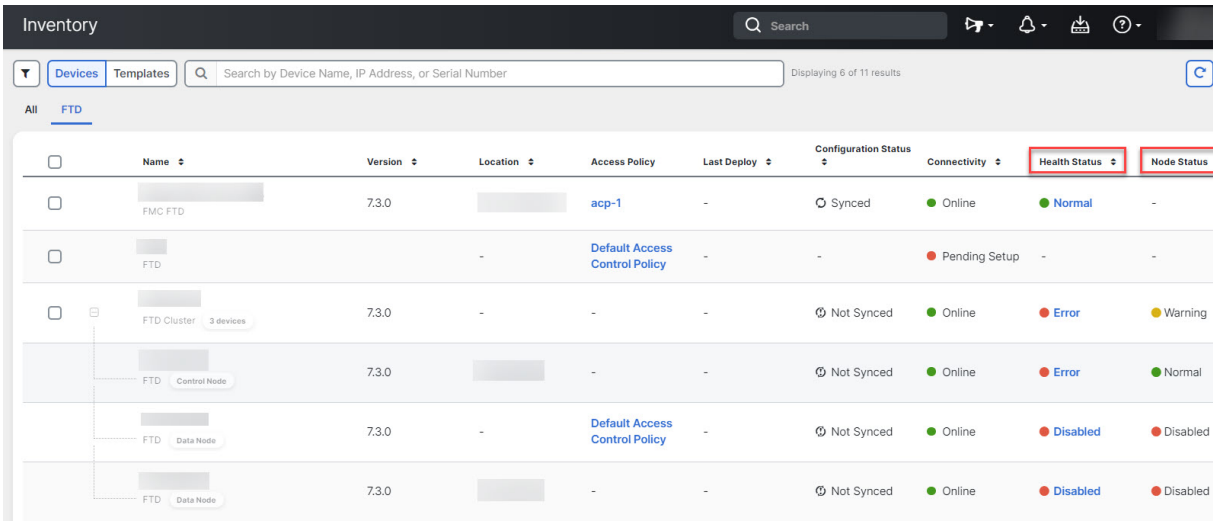
新しい [サービス（Services）] ページから、クラウド提供型 Firewall Management Center、オンプレミス Firewall Management Center、およびセキュアコネクタを管理できるようになりました。**[ツールとサービス（Tools & Services）]** > **[Firewall Management Center]** または [セキュアコネクタ（Secure Connectors）] を選択します。詳細については、「View Services Page Information」[英語] を参照してください。



2023 年 8 月 17 日

Threat Defense デバイスの正常性ステータスの把握

CDO の [インベントリ（Inventory）] ページに、Threat Defense デバイスの正常性とノードステータスが表示されるようになりました。デバイスの正常性の詳細については、デバイスの正常性ステータスをクリックし、クラウド提供型 Firewall Management Center またはオンプレミス Firewall Management Center のユーザーインターフェイスのデバイスの [正常性モニタリング（Health Monitoring）] ページに移動して、確認できます。ノードステータスは、クラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスに対してのみ表示されることに注意してください。



詳細については、「Cisco Defense Orchestrator を使用したオンプレミス FMC の管理」および「Managing Cisco Secure Firewall Threat Defense Devices with Cloud-delivered Firewall Management Center」[英語] を参照してください。

2023 年 8 月 3 日

Firewall 移行ツールの更新

CDO は、Firewall 移行ツールの更新バージョンをホストするようになりました。Cisco Secure Firewall ASA デバイスの複数のコンテキストをルーテッドモードインスタンスにマージし、クラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスに移行できるようになりました。さらに、移行ツールは、Virtual Routing and Forwarding（VRF）機能を活用して、マルチコンテキストの Cisco ASA 環境で観察される分離されたトラフィックフローを複製できるようになりました。複製されたフローは新たにマージされた設定の一部になります。

詳細については、Cisco Defense Orchestrator の Firewall 移行ツールを使用したファイアウォールの移行ガイド [英語] の「Migrating Secure Firewall ASA Managed by CDO」を参照してください。

2023 年 7 月

2023 年 7 月 20 日

GCP によって管理される仮想 Firewall Threat Defense デバイスの EasyDeploy

仮想 Firewall Threat Defense デバイスを作成し、Google Cloud Platform（GCP）プロジェクトに同時に展開できるようになりました。EasyDeploy メソッドでは、新しい仮想デバイスを作成

し、デバイスをクラウド環境に関連付けるために必要な手順を組み合わせることで、手順が合理化され、セットアップに必要な時間が最小限に抑えられます。

オンボーディングフローでは、クラウド提供型 Firewall Management Center を有効にする**必要があります**。詳細については、「Deploy a Threat Defense Device to Google Cloud Platform」[英語] を参照してください。

2023 年 7 月 13 日

異なるブラウザタブで CDO と クラウド提供型 Firewall Management Center ポータルを開く

CDO と クラウド提供型 Firewall Management Center ポータルページを異なるブラウザタブで開き、CDO と クラウド提供型 Firewall Management Centerの両方で同時に作業できるようになりました。

詳細については、「Support to Open CDO and Cloud-delivered Firewall Management Center Applications on Different Tabs」[英語] を参照してください。

2023 年 6 月

2023 年 6 月 29 日

イベントビューアでのバックグラウンド検索のスケジュール設定

定期的なスケジュールでイベントビューアを使用してバックグラウンド検索を実行できるようになりました。スケジュールは、絶対時間（例：5 月 1 日から 5 月 5 日）またはスライディングウィンドウ（例：「最終日」）に対応しています。

詳細については、「Schedule a Background Search in the Event Viewer」[英語] を参照してください。

新しいイベント属性のサポート

現在、セキュリティグループ、暗号化された可視性プロセスの確実性スコア、暗号化された可視性脅威の信頼性、暗号化された可視性脅威の確実性スコア、暗号化された可視性フィンガープリントは、CDO のイベントビューアでサポートされている syslog イベント属性です。イベントロギングビューをカスタマイズすると、新たにサポートされた属性の列を作成できます。

2023 年 6 月 15 日

CDO の Firewall 移行ツールを使用したファイアウォールの移行

Cisco Defense Orchestrator の Firewall 移行ツールを使用して、Secure Firewall ASA デバイス、FDM による管理 Threat Defense デバイス、および Check Point、Palo Alto Networks、Fortinet ファ

イアウォールなどのサードパーティ製ファイアウォールからクラウド提供型Firewall Management Center に設定を移行できるようになりました。詳細については、Cisco Defense Orchestrator の Firewall 移行ツールを使用したファイアウォールの移行ガイド [英語] を参照してください。

2023 年 6 月 8 日

AWS および Azure によって管理される仮想 Firewall Threat Defense デバイスの EasyDeploy

仮想 Firewall Threat Defense デバイスを作成し、Amazon Web Services（AWS）または Azure 環境に同時に展開できるようになりました。EasyDeploy メソッドでは、新しい仮想デバイスを作成し、デバイスをクラウド環境に関連付けるために必要な手順を組み合わせることで、手順が合理化され、セットアップに必要な時間が最小限に抑えられます。

オンボーディングフローでは、クラウド提供型Firewall Management Centerを有効にする**必要があります**。詳細については、「Deploy a Threat Defense Device with AWS」[英語] および「Deploy a Threat Defense Device with an Azure VNet」[英語] をそれぞれ参照してください。

2023 年 6 月 5 日

CDO に導入された Multicloud Defense ソリューション

Multicloud Defense ソリューション は、クラウド ネットワーク トラフィック、およびクラウド アプリケーションとワークロードのセキュリティ ポリシー オーケストレーションと保護に特化したソリューションです。複数のクラウドタイプに対して統合されたセキュリティポリシーと Web 保護を提供し、クラウド資産に対するネットワークの可視性を提供し、脅威インテリジェンスや外部ロギングなどのサービスを統合します。クラウドアカウントとの間の入出力トラフィックと、クラウドアカウントの「East-West」ネットワークトラフィックを適用します。

Multicloud Defense ソリューション は現在、AWS、Azure、Google Cloud Platform（GCP）、および Oracle OCI クラウドアカウントをサポートしています。

詳細 については、「About Multicloud Defense」[英語] を参照してください。Multicloud Defense ソリューションを試す場合は、「Multicloud Defense 90 日間無料トライアル」を参照してください。

2023 年 6 月 1 日

SecureX の統合によるオンプレミスの Cisco Secure Firewall Management Center の自動検出

CDO は、CDO アカウントにリンクされている SecureX テナントに関連付けられているすべての オンプレミス Firewall Management Center をオンボードできるようになりました。また、それらの オンプレミス Firewall Management Center にリンクされている Cisco Secure Firewall Threat Defense のデバイスがオンボードされます。詳細については、「Auto Onboard an On-Prem Firewall Management Center with SecureX」[英語] を参照してください。

2023 年 4 月

2023 年 4 月 27 日

イベントフィルタリングの改善

相対時間範囲を使用して、イベントをさらにフィルタ処理できるようになりました。絶対時間範囲は、明示的に指定された時間フレームです。相対時間範囲の例は、過去 3 日間または過去 3 時間です。相対時間範囲は、絶対時間範囲に必ずしも含まれていない可能性があるトラフィックとイベントをターゲットにするのに役立ちます。詳細については、「Search for Events in the Events Logging Page」[英語] を参照してください。

2023 年 3 月

2023 年 3 月 23 日

イベントロギングのバックグラウンド検索

CDO では、検索条件を定義し、定義された検索条件に基づいてイベントログ内のイベントを検索できます。バックグラウンド検索機能を使用すると、バックグラウンドでイベントログの検索を実行して、バックグラウンド検索が完了した後に検索結果を表示できます。

設定したサブスクリプションアラートとサービス統合に基づいて、バックグラウンド検索が完了すると通知されます。「Learn more about background searches used with event logging」[英語] を参照してください。

2023 年 1 月

2023 年 1 月 18 日

FTD のリモートアクセス VPN セッションの監視

CDO は、CDO の クラウド提供型 Firewall Management Center を使用して管理される FTD のリモートアクセス VPN セッションを監視できるようになりました。

[RA VPNモニタリング（RA VPN Monitoring）] ページには次の情報が表示されます。

- アクティブなセッションと履歴セッションのリスト。
- 各セッションに関連付けられているデバイスとユーザーの詳細。

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。