フレームワークマッピング：Cisco Secure Firewall および Firewall Management Center + Center for Internet Security（CIS）Controls v8.1

© 2026 Cisco and/or its affiliates. All rights reserved.

目次

バックグラウンド	3
CIS Controls v8.1 の概要	3
シスコ製品の概要	5
CIS Controls の詳細なマッピングテーブル	6
主な所見	19
要約	20
関連資料	20

© 2026 Cisco and/or its affiliates. All rights reserved.

バックグラウンド

Cisco Secure Firewall と Firewall Management Center（FMC）は、CIS Critical Security Controls v8.1 の要件を、展開、運用、モニタリング、および文書化が可能なセキュリティ管理に結び付ける実用的な方法を組織に提供します。Secure Firewall は、境界の保護、セグメンテーション、セキュアアクセス、アプリケーション制御、URL フィルタリング、侵入防御、マルウェアおよびファイル検査、暗号化通信の可視性、ならびに詳細なセキュリティイベント テレメトリといった、適用と検査のレイヤを提供します。FMC により、分散型のファイアウォール展開全体にわたって、一元化されたポリシー管理、モニタリング、レポート、デバイスの正常性に関する可視性、ワークフローの証拠、運用の一貫性が追加されます。

CIS をセキュリティフレームワークのロードマップとして使用する組織にとって、この統合プラットフォームは、保護策がネットワーク インフラストラクチャ管理、ネットワークのモニタリングと防御、監査ログ管理、マルウェア防御、電子メールおよび Web の保護、アクセス制御管理、セグメンテーション、ならびに選択されたデータ保護の成果に依存する場合に特に有用です。これらの領域では、ファイアウォールの適用、通信検査、ポリシー制御、ロギング、イベント分析により、運用上の保護と、コンプライアンスに関する議論を支える証拠の両方が得られます。

このマッピングの範囲は、Cisco Firewall と FMC が合理的に提供できる内容に意図的に限定されています。一部の CIS 保護策では、企業ガバナンス、端末管理、アイデンティティ管理、ユーザートレーニング、サービスプロバイダーの監督、バックアップ運用、またはソフトウェア開発セキュリティプログラムが必要とされます。これらの領域でも、Cisco Firewall および FMC は、裏付けとなる有意義な証拠や、技術的な代替コントロールとしての価値を引き続き提供できますが、お客様はその証拠を適切なプロセスオーナーや隣接するセキュリティプラットフォームと組み合わせる必要があります。

CIS Controls v8.1 の概要

CIS Critical Security Controls v8.1 は、一般的なサイバー攻撃からシステムとネットワークを防御するための優先順位付けされた一連の保護策です。シスコのお客様にとってこのフレームワークが有用なのは、セキュリティに関する広範な成果が具体的な保護策に変わり、テクノロジー機能、運用上のオーナーシップ、および証拠にマッピングできるからです。

CIS Controls v8.1 は、現行の業界標準およびフレームワークとの整合性、資産クラスと保護策に関する文言の改訂、および NIST Cybersecurity Framework 2.0 で導入された Govern セキュリティ機能によって v8 を更新したものです。CIS はマッピングリソースと CIS Controls Navigator を公開しているため、チームは CIS の保護策が他のセキュリティ標準や、すでに管理しているより広範なプログラムとどのように関連しているかを確認できます。

この対応表としての価値は、複数のフレームワークが存在する環境で重要です。CIS は、NIST CSF 2.0、NIST SP 800-53 Rev. 5、NIST SP 800-171、ISO/IEC 27001、PCI DSS、SOC 2 などのフレームワークや、その他の規制または業界フレームワークへの個別のマッピングを公開しています。そのため CIS マッピングは、コンプライアンスに関する複数の議論がファイアウォールの適用、モニタリング、ロギング、セグメンテーション、およびポリシー管理の証拠によってどのように支えられるかを、シスコのお客様が説明する際に役立ちます。

© 2026 Cisco and/or its affiliates. All rights reserved.

実装グループ

実装グループ（IG）は、CIS が推奨する優先順位付けモデルです。IG1 は必須のサイバーハイジーンであり、実用的かつ基本的なコントロールによって一般的な攻撃に対処するため、すべての企業が最初に検討すべき保護策の一連の基準です。IG2 は、より複雑な環境、より大きな規制上のリスク、またはより高い運用リスクを抱える組織向けに、IG1 を基盤として構築されたものです。IG3 には CIS コントロールの保護策全体が含まれており、成熟したセキュリティプログラムを備えた組織、重大なリスクにさらされている組織、または最も包括的なカバレッジを必要とする組織向けに設計されています。

マッピングテーブルの IG1/IG2/IG3 列には、各保護策がその導入パスのどこに位置付けられるかが示されています。これにより、お客様は同じシスコファイアウォールおよび FMC のマッピングを段階的なロードマップに使用できます。これは IG1 の優先事項から始まり、プログラムの成熟に従って IG2 に拡張し、組織が完全な CIS カバレッジを必要とする場合は IG3 を使用します。

主要なコントロールの概要

CIS Controls v8.1 は、組織によるセキュリティ態勢の強化、サイバーリスクの軽減、および最新の脅威に対するレジリエンスの向上を支援するように設計された、18 のサイバーセキュリティ ベストプラクティスから成る優先順位付きのセットを提供します。これらのコントロールは、セキュリティガバナンス、資産管理、脆弱性管理、アクセス制御、モニタリング、およびインシデント対応の主要領域を中心に構成されています。これらを総合することで、組織が基盤となるセキュリティ機能を確立し、最も効果的な防御策に合わせてセキュリティリソースを配分するのに役立つ、実用的なリスクベースのフレームワークを提供します。次の表に、18 の CIS コントロールの概要を示します。各コントロールの詳細な説明は、このドキュメントの後続のセクションに記載されています。

表 1. CIS Controls v8.1

コントロール番号	コントロールのタイトル
コントロール 1	企業資産の一覧と管理
コントロール 2	ソフトウェア資産の一覧と管理
コントロール 3	データ保護
コントロール 4	企業資産とソフトウェアの安全な設定
コントロール 5	アカウント管理
コントロール 6	アクセス制御管理
コントロール 7	継続的な脆弱性管理
コントロール 8	監査ログ管理
コントロール 9	電子メールと Web ブラウザの保護
コントロール 10	マルウェア防御
コントロール 11	データ復旧

© 2026 Cisco and/or its affiliates. All rights reserved.

コントロール番号	コントロールのタイトル
コントロール 12	ネットワーク インフラストラクチャ管理
コントロール 13	ネットワークのモニタリングと防御
コントロール 14	セキュリティに関する意識向上とスキルトレーニング
コントロール 15	サービスプロバイダー管理
コントロール 16	アプリケーション ソフトウェアのセキュリティ
コントロール 17	インシデント対応管理
コントロール 18	ペネトレーションテスト

シスコ製品の概要

Cisco Secure Firewall

Cisco Secure Firewall は、オンプレミス、クラウド、ハイブリッド、ブランチ、産業、IoT の各環境全体で、組織によるユーザー、アプリケーション、データ、および重要インフラストラクチャの保護を支援します。Secure Firewall はネットワーク通信に対する幅広い可視性とコントロールを提供することで、セキュリティ チームがリスクを軽減し、セキュリティポリシーを一貫して適用し、全体的なセキュリティ態勢を強化できるようサポートします。

CIS Controls v8.1 のコンテキストにおいて、Cisco Secure Firewall はネットワークのセグメンテーション、アクセス制御の適用、アプリケーションの可視性と制御、侵入防御、マルウェアおよびファイル検査、URL フィルタリング、暗号化通信の分析、リモートアクセスのセキュリティ、およびセキュリティイベントのロギングなどの機能を通じて、組織によるネットワーク セキュリティ プラクティスの導入を支援するうえで重要な役割を果たします。これらの機能により、組織は攻撃対象領域を制限し、悪意のあるアクティビティを検出してブロックし、ネットワーク通信の可視性を高めることができます。

Cisco Talos の脅威インテリジェンスと高度な Snort® 検出テクノロジーを搭載した Cisco Secure Firewall は、お客様が新たな脅威を特定し、セキュリティイベントにより効果的に対応できるよう支援します。アイデンティティ、分析、ロギング、セキュリティ運用、および Extended Detection and Response（XDR）プラットフォームとの統合により、組織はネットワーク管理、脅威検出、マルウェア防御、アクセス制御、監査ログ、継続的なモニタリングに関連する CIS Controls をさらにサポートできます。

Firewall Management Center（FMC）

Cisco Firewall Management Center（FMC）は、企業全体における Cisco Secure Firewall のデプロイメントを管理、モニタリング、最適化するための一元化されたプラットフォームを提供します。FMC は、一貫したポリシー管理、包括的な可視性、シンプルな管理を単一のインターフェイスから可能にすることで、組織によるセキュリティ運用の合理化を支援します。

キャンパス、ブランチ、データセンター、クラウド、またはハイブリッド環境に複数のファイアウォールを展開している組織では、標準化されたセキュリティ制御を維持し、一貫したポリシー適用をサポートするために必要

© 2026 Cisco and/or its affiliates. All rights reserved.

な運用フレームワークが FMC によって得られます。セキュリティチームは、セキュリティイベントとネットワークアクティビティの可視性を維持しながら、アクセス制御、侵入防御、マルウェア保護、URL フィルタリング、アプリケーション制御、およびセグメンテーションポリシーを一元管理できます。

CIS Controls の観点から見ると、FMC は一元化されたポリシー管理、ネットワーク検出、デバイスのヘルスモニタリング、イベントの関連付け、レポート、アラート通知、調査ワークフローを提供することで、組織がセキュリティ制御を実装して運用する能力を強化します。これらの機能により、継続的なモニタリング、監査対応の準備、脅威検出、インシデント調査、セキュリティ運用の効率化が可能になります。物理、仮想、クラウド提供型の各導入モデルで利用できる FMC により、組織は進化するビジネス要件とセキュリティ要件に合わせて拡張しつつ、多様な環境全体で一貫したセキュリティ管理プラクティスを展開できます。

マッピングの解釈方法

このドキュメントの CIS Controls マッピングでは、Cisco Secure Firewall と Firewall Management Center（FMC）を組み合わせた場合の寄与を評価します。Secure Firewall がネットワーク層でセキュリティ施行機能と脅威防御機能を提供する一方で、FMC は環境全体にわたって一貫した形でそれらのコントロールを導入、モニタリング、維持するために必要な、中央管理、可視性、レポート、および運用ワークフローを提供します。

次の機能領域は、各ソリューションが CIS Controls の実装にどのように寄与するかを理解する上で有用なフレームワークを提供します。

表 2. CIS との連動における価値

機能領域	Cisco Secure Firewall の利点	Cisco Firewall Management Center（FMC）の利点
ネットワークセキュリティの施行	ネットワーク セグメンテーション、アクセス制御、VPN サービス、アプリケーションの可視性と制御、ネットワーク境界全体でのポリシー施行。	ファイアウォールのデプロイメント全体にわたる、ポリシーの作成、導入、検証、変更管理の一元化、およびポリシーの一貫性。
脅威の防御と検出	侵入防御、Snort ベースの脅威検知、マルウェアとファイルの検査、URL フィルタリング、暗号化通信の可視性。	侵入、マルウェア、ファイル、URL、アプリケーションの各ポリシー、およびイベントの集約と関連付けの中央管理。
可視性、モニタリング、レポート	運用に関するセキュリティの可視性を提供する、接続、侵入、マルウェア、URL、VPN、およびポリシーイベントの収集。	ダッシュボード、レポート、イベント分析、デバイスのヘルスモニタリング、監査データ、および SIEM、ロギング、セキュリティ運用の各プラットフォームとの統合。
インシデント対応と運用	ポリシーの適用、通信のブロック、セキュリティの統合を通じて、封じ込めと緩和措置をサポートします。	調査ワークフロー、運用コンテキスト、ポリシー展開機能、レポート、および統合型の対応支援を提供します。

CIS Controls の詳細なマッピングテーブル

次のセクションでは、Cisco Secure Firewall と Firewall Management Center（FMC）の機能を CIS Controls v8.1 にマッピングします。各コントロールとその保護策を評価することで、Secure Firewall と FMC がコントロール要件をどのように満たすか、またはサポートするかが示されます。組織はこれにより、多層防御セキュリティ戦略の中で CIS Controls の目標達成を支援するうえでそれらが果たす役割を理解できます。マッピング

© 2026 Cisco and/or its affiliates. All rights reserved.

テーブルには、該当する実装グループ（IG1、IG2、および IG3）、資産のタイプ、およびセキュリティ機能（識別、防御、検出、対応、および復旧）が示されています。保護策は次のいずれかに分類されます。

- **適合**：Cisco Secure Firewall または FMC は、保護策の意図を満たす機能を直接提供します。
- **サポート**：Cisco Secure Firewall または FMC は保護策の実装に寄与しますが、要件に完全に対応するには、補完的なテクノロジー、プロセス、または組織的なコントロールが必要になる場合があります。

すべての CIS Controls および保護策が、ネットワーク セキュリティ テクノロジーによって直接対処されるわけではありません。コントロールが主にガバナンス、ポリシー、リスク管理、または従業員トレーニングなどの領域に焦点を当てている場合、マッピングテーブルが含まれない場合があります。それでもこれらのコントロールは、包括的なサイバーセキュリティ プログラムの重要コンポーネントであるため、網羅性を保つために、CIS Controls フレームワーク内での目的と関連性の説明とともに含めています。

コントロール 1：企業資産の一覧と管理

インフラストラクチャに物理的、仮想的、リモートで接続されているすべての企業資産（ポータブルデバイスやモバイルデバイスを含むエンドユーザーデバイス、ネットワークデバイス、非コンピューティング/モノのインターネット（IoT）デバイス、サーバー）、およびクラウド環境内のすべての企業資産を積極的に管理（一覧作成、追跡、修正）し、企業内で監視および保護する必要がある資産の全体像を正確に把握します。これは、承認されていない資産や管理されていない資産を特定し、それらを除去または修復する上でも役立ちます。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
1.1	詳細な企業資産一覧の作成と維持	デバイス	特定	X	X	X		サポート		サポート
1.2	承認されていない資産への対処	デバイス	対応	X	X	X		サポート		サポート
1.3	アクティブ検出ツールの利用	デバイス	検出		X	X		サポート		サポート
1.4	Dynamic Host Configuration Protocol（DHCP）ロギングを使用した企業資産一覧の更新	デバイス	特定		X	X		サポート		サポート
1.5	パッシブ資産検出ツールの使用	デバイス	検出			X		サポート	適合	

コントロール 2：ソフトウェア資産の一覧と管理

ネットワーク上のすべてのソフトウェア（オペレーティングシステム（OS）およびアプリケーション）を積極的に管理（一覧作成、追跡、修正）し、承認されたソフトウェアのみがインストールされて実行できるようにするとともに、承認されていないソフトウェアや管理されていないソフトウェアを検出してインストールまたは実行を防止します。

© 2026 Cisco and/or its affiliates. All rights reserved.

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
2.1	ソフトウェアの一覧の作成と維持	ソフトウェア	特定	X	X	X		サポート		サポート
2.2	承認済みのソフトウェアが現在サポートされていることの確認	ソフトウェア	特定	X	X	X		サポート		サポート
2.3	承認されていないソフトウェアへの対処	ソフトウェア	対応	X	X	X		サポート		サポート
2.4	自動ソフトウェア一覧ツールの利用	ソフトウェア	検出		X	X		サポート		サポート
2.5	承認済みソフトウェアの許可リストへの登録	ソフトウェア	保護		X	X		サポート		サポート
2.6	承認済みライブラリの許可リストへの登録	ソフトウェア	保護		X	X		サポート		サポート
2.7	承認済みスクリプトの許可リストへの登録	ソフトウェア	保護			X		サポート		サポート

コントロール 3：データ保護

データの特定、分類、安全な取り扱い、保持、および廃棄のためのプロセスと技術的コントロールを策定します。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
3.1	データ管理プロセスの確立と維持	データ（Data）	ガバナンス	X	X	X		サポート		サポート
3.2	データの一覧の確立と維持	データ（Data）	特定	X	X	X		サポート		サポート
3.3	データアクセス制御リストの設定	データ（Data）	保護	X	X	X	適合			サポート
3.4	データ保持の施行	データ（Data）	保護	X	X	X		サポート		サポート
3.7	データ分類スキームの確立と維持	デバイス	特定		X	X		サポート		サポート
3.8	データフローの文書化	データ（Data）	特定		X	X		サポート		サポート
3.10	転送中の機密データの暗号化	データ（Data）	保護		X	X		サポート		サポート

© 2026 Cisco and/or its affiliates. All rights reserved.

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
3.12	機密性に基づくデータ処理およびストレージのセグメント化	データ（Data）	保護		X	X		サポート		サポート

© 2026 Cisco and/or its affiliates. All rights reserved.

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
3.13	データ損失防止ソリューションの展開	データ（Data）	保護			X		サポート		サポート
3.13	データ損失防止ソリューションの展開	データ（Data）	保護			X		サポート		サポート
3.14	機密データアクセスのログ記録	データ（Data）	検出			X		サポート		サポート

コントロール 4：企業資産とソフトウェアの安全な設定

企業資産（ポータブルデバイスやモバイルデバイスを含むエンドユーザーデバイス、ネットワークデバイス、非コンピューティング/IoT デバイス、およびサーバー）とソフトウェア（オペレーティングシステム（OS）およびアプリケーション）の安全な設定を確立して維持します。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
4.1	安全な設定プロセスの確立と維持	資料	ガバナンス	X	X	X		サポート		サポート
4.2	ネットワーク インフラストラクチャの安全な設定プロセスの確立と維持	資料	ガバナンス	X	X	X		サポート		サポート
4.3	企業資産に対する自動セッションロックの設定	デバイス	保護	X	X	X		サポート		サポート
4.6	企業資産とソフトウェアの安全な管理	デバイス	保護	X	X	X		サポート		サポート
4.7	企業資産とソフトウェアのデフォルトアカウントの管理	Users	保護	X	X	X		サポート		サポート
4.8	企業資産とソフトウェアの不要なサービスのアンインストールまたは無効化	デバイス	保護		X	X		サポート		サポート
4.9	企業資産に対する信頼できる DNS サーバーの設定	デバイス	保護		X	X		サポート		サポート

コントロール 5：アカウント管理

プロセスとツールを使用して、管理者アカウントを含むユーザーアカウントとサービスアカウントのログイン情報に対して企業資産とソフトウェアへの権限を割り当て、それらの権限を管理します。

© 2026 Cisco and/or its affiliates. All rights reserved.

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
5.1	アカウントの一覧の作成と維持	Users	特定	X	X	X		サポート		サポート
5.2	一意のパスワードの使用	Users	保護	X	X	X		サポート		サポート
5.3	休眠アカウントの無効化	Users	保護	X	X	X		サポート		サポート
5.4	管理者権限を専用の管理者アカウントに制限	Users	保護	X	X	X		サポート		サポート
5.5	サービスアカウントの一覧の作成と維持	Users	特定		X	X		サポート		サポート
5.6	アカウント管理の一元化	Users	保護		X	X		サポート	適合	

コントロール 6：アクセス制御管理

プロセスとツールを使用して、企業資産とソフトウェアのユーザーアカウント、管理者アカウント、およびサービスアカウントのログイン情報と権限の作成、割り当て、管理、ならびに取り消しを行います。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
6.1	アクセス付与プロセスの確立	資料	ガバナンス	X	X	X		サポート		サポート
6.2	アクセス取り消しプロセスの確立	資料	ガバナンス	X	X	X		サポート		サポート
6.3	外部公開アプリケーションにおける MFA の要求	Users	保護	X	X	X		サポート		サポート
6.4	リモートネットワーク アクセスにおける MFA の要求	Users	保護	X	X	X		サポート		サポート
6.5	管理アクセスにおける MFA の要求	Users	保護	X	X	X		サポート		サポート
6.6	認証および承認システムの一覧の作成と維持、ならびにアクセス制御の一元管理	ソフトウェア	特定		X	X		サポート		サポート

© 2026 Cisco and/or its affiliates. All rights reserved.

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
6. [6]	役割別のアクセス制御の定義と維持	Users	保護		X	X		サポート		サポート
6.7	アクセス付与プロセスの確立	Users	ガバナンス			X		サポート	適合	

コントロール 7：継続的な脆弱性管理

攻撃者に攻撃の機会を与える要素を修復して最小限に抑えるために、企業のインフラストラクチャ内に存在するすべての企業資産の脆弱性を継続的に評価および追跡する計画を策定します。公開および非公開の業界情報源をモニターし、脅威と脆弱性に関する最新情報を入手します。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
7.1	脆弱性管理プロセスの確立と維持	資料	ガバナンス	X	X	X		サポート		サポート
7.2	修復プロセスの確立と維持	資料	ガバナンス	X	X	X		サポート		サポート
7.5	内部企業資産の自動脆弱性スキャンの実行	ソフトウェア	特定		X	X		サポート		サポート
7.6	外部に公開される企業資産の自動脆弱性スキャンの実行	ソフトウェア	特定		X	X		サポート		サポート
7.7	検出された脆弱性の修復	ソフトウェア	対応		X	X		サポート		サポート

コントロール 8：監査ログ管理

攻撃の検出、把握、または攻撃からの復旧に役立つ可能性があるイベントの監査ログを収集、アラート生成、確認、および保持します。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
8.1	監査ログ管理プロセスの確立と維持	資料	ガバナンス	X	X	X		サポート		サポート
8.2	監査ログの収集	データ（Data）	検出	X	X	X		サポート	適合	
8.3	適切な監査ログストレージの確保	データ（Data）	保護	X	X	X		サポート		サポート

© 2026 Cisco and/or its affiliates. All rights reserved.

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
8.4	時刻の同期の標準化	ネットワーク	保護		X	X		サポート		サポート
8.5	詳細な監査ログの収集	データ（Data）	検出		X	X		サポート	適合	
8.6	DNS クエリ監査ログの収集	データ（Data）	検出		X	X		サポート		サポート
8.7	URL リクエスト監査ログの収集	データ（Data）	検出		X	X	適合			サポート
8.8	コマンドライン監査ログの収集	データ（Data）	検出		X	X		サポート		サポート
8.9	監査ログの一元管理	データ（Data）	検出		X	X		サポート	適合	
8.10	監査ログの保持	データ（Data）	保護		X	X		サポート		サポート
8.11	監査ログレビューの実施	データ（Data）	検出		X	X		サポート		サポート
8.12	サービスプロバイダーログの収集	データ（Data）	検出			X		サポート		サポート

コントロール 9：電子メールと Web ブラウザの保護

電子メールや Web を媒介とする脅威は、攻撃者が直接的な関与によって人間の行動を操作する機会となるため、それらに対する保護と検出を強化します。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
9.2	DNS フィルタリングサービスの使用	デバイス	保護	X	X	X		サポート		サポート
9.3	ネットワークベース URL フィルタの維持と適用	ネットワーク	保護		X	X	適合			サポート
9.6	不要なファイルタイプのブロック	ネットワーク	保護		X	X		サポート		サポート

コントロール 10：マルウェア防御

企業資産における悪意のあるアプリケーション、コード、またはスクリプトのインストール、拡散、実行を防止制御します。

© 2026 Cisco and/or its affiliates. All rights reserved.

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
10.1	マルウェア対策ソフトウェアの展開と維持	デバイス	検出	X	X	X		サポート		サポート
10.2	マルウェア対策シグネチャの自動更新の設定	デバイス	保護	X	X	X		サポート		サポート
10.5	エクスプロイト防止機能の有効化	デバイス	保護		X	X		サポート		サポート
10.6	マルウェア対策ソフトウェアの一元管理	デバイス	保護		X	X		サポート		サポート
10.7	行動ベースのマルウェア対策ソフトウェアの使用	デバイス	検出		X	X		サポート		サポート

コントロール 11：データ復旧

対象範囲の企業資産をインシデント発生前の信頼できる状態に復元するのに十分なデータ復旧プラクティスを確立して維持します。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
11.2	自動バックアップの実行	データ（Data）	Recover	X	X	X				サポート
11.3	復旧データの保護	データ（Data）	保護	X	X	X				サポート
11.5	データ復旧のテスト	データ（Data）	Recover		X	X				サポート

コントロール 12：ネットワーク インフラストラクチャ管理

攻撃者が脆弱なネットワークサービスやアクセスポイントを悪用することを防ぐために、ネットワークデバイスの整備、実装、および積極的な管理（追跡、報告、修正）を行います。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
12.1	ネットワーク インフラストラクチャを最新の状態に保つ	ネットワーク	保護	X	X	X		サポート		サポート
12.2	安全なネットワークアーキテクチャの確立と維持	ネットワーク	保護		X	X		サポート		サポート

© 2026 Cisco and/or its affiliates. All rights reserved.

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
12.3	ネットワーク インフラストラクチャの安全な管理	ネットワーク	保護		X	X		サポート		サポート
12.4	アーキテクチャ図の確立と維持	資料	ガバナンス		X	X		サポート		サポート
12.5	ネットワークの認証、承認、および監査（AAA）の一元管理	ネットワーク	保護		X	X		サポート		サポート
12.6	ネットワーク インフラストラクチャを最新の状態に保つ	ネットワーク	保護		X	X		サポート		サポート
12.7	安全なネットワークアーキテクチャの確立と維持	デバイス	保護		X	X	適合			サポート
12.8	ネットワーク インフラストラクチャの安全な管理	デバイス	保護			X		サポート		サポート

コントロール 13：ネットワークのモニタリングと防御

企業のネットワーク インフラストラクチャおよびユーザーベース全体で、セキュリティ脅威に対する包括的なネットワークモニタリングと防御を確立して維持するためのプロセスとツールを運用します。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
13.1	セキュリティイベント アラートの一元管理	ネットワーク	検出		X	X		サポート	適合	
13.2	ホストベースの侵入検出ソリューションの展開	デバイス	検出		X	X		サポート		サポート
13.3	ネットワーク侵入検出ソリューションの展開	ネットワーク	検出		X	X	適合			サポート
13.4	ネットワークセグメント間での通信フィルタリングの実行	ネットワーク	保護		X	X	適合			サポート
13.5	リモート資産のアクセス制御の管理	デバイス	保護		X	X		サポート		サポート
13.6	ネットワーク通信フローログの収集	ネットワーク	検出		X	X	適合		適合	

© 2026 Cisco and/or its affiliates. All rights reserved.

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
13.7	ホストベースの侵入防御ソリューションの展開	デバイス	保護			X		サポート		サポート
13.8	ネットワーク侵入防御ソリューションの展開	ネットワーク	保護			X	適合			サポート
13.9	ポートレベルのアクセス制御の展開	ネットワーク	保護			X		サポート		サポート
13.10	アプリケーションレイヤ フィルタリングの実行	ネットワーク	保護			X	適合			サポート
13.11	セキュリティイベント アラートのしきい値の調整	ネットワーク	検出			X		サポート	適合	

コントロール 14：セキュリティに関する意識向上とスキルトレーニング

従業員がセキュリティを意識し、企業のサイバーセキュリティリスクの軽減に向けて適切なスキルを備えるよう、その行動に影響を与えるための、セキュリティ意識向上プログラムを確立して維持します。

このコントロールは、主に組織のポリシー、プロセス、従業員教育プログラムを通じて対処します。Cisco Secure Firewall と Firewall Management Center（FMC）は、セキュリティに関する意識向上活動やトレーニング活動を直接実施するようには設計されていませんが、組織によるセキュリティポリシーの施行、ネットワークアクティビティの監視、および従業員向けの意識向上施策を通じて対処されるサイバー脅威への露出の低減を支援することで、多層防御セキュリティ戦略の重要なコンポーネントとして機能します。

コントロール 15：サービスプロバイダー管理

機密データを保持する、または企業の重要な IT プラットフォームやプロセスを担当するサービスプロバイダーの評価プロセスを策定し、これらのプロバイダーがそうしたプラットフォームやデータを適切に保護していることを確認します。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
15.4	サービスプロバイダー契約にセキュリティ要件が含まれていることの確認	資料	ガバナンス		X	X		サポート		サポート
15.5	サービスプロバイダーの評価	Users	ガバナンス			X		サポート		サポート
15.6	サービスプロバイダーの監視	データ（Data）	ガバナンス			X		サポート		サポート

© 2026 Cisco and/or its affiliates. All rights reserved.

コントロール 16：アプリケーション ソフトウェアのセキュリティ

社内で開発、ホスト、または取得されたソフトウェアのセキュリティライフサイクルを管理して、企業に影響が及ぶ前にセキュリティ上の弱点を防止、検出、および修正します。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
16.7	アプリケーション インフラストラクチャ用の標準的なハードニング設定テンプレートの使用	ソフトウェア	保護		X	X		サポート		サポート
16.8	実稼働システムと非実稼働システムの分離	ネットワーク	保護		X	X		サポート		サポート
16.10	アプリケーション アーキテクチャでのセキュア設計原則の適用	ソフトウェア	保護		X	X		サポート		サポート
16.13	アプリケーションのペネトレーションテストの実施	ソフトウェア	ガバナンス			X		サポート		サポート
16.14	脅威モデリングの実施	ソフトウェア	保護			X		サポート		サポート

コントロール 17：インシデント対応管理

攻撃への準備、検出、および迅速な対応のためのインシデント対応能力（ポリシー、計画、手順、定義されたロール、トレーニング、コミュニケーションなど）を開発して維持するためのプログラムを確立します。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
17.1	インシデント処理を管理する担当者の指名	Users	対応	X	X	X		サポート		サポート
17.2	セキュリティインシデントを報告するための連絡先情報の確立と維持	資料	ガバナンス	X	X	X		サポート		サポート
17.3	インシデントを報告するための企業プロセスの確立と維持	資料	ガバナンス	X	X	X		サポート		サポート
17.3	インシデントを報告するための企業プロセスの確立と維持	資料	ガバナンス		X	X		サポート		サポート

© 2026 Cisco and/or its affiliates. All rights reserved.

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
17.3	インシデントを報告するための企業プロセスの確立と維持	資料	ガバナンス		X	X		サポート		サポート
17.4	インシデント対応プロセスの確立と維持	資料	ガバナンス		X	X		サポート		サポート
17.5	主要なロールと責任の割り当て	Users	対応		X	X		サポート		サポート
17.6	インシデント対応中のコミュニケーション メカニズムの定義	Users	対応		X	X		サポート		サポート
17.7	定期的なインシデント対応演習の実施	Users	Recover		X	X		サポート		サポート
17.8	インシデント後のレビューの実施	Users	Recover		X	X		サポート		サポート
17.9	セキュリティインシデントのしきい値の確立と維持	資料	Recover			X		サポート		サポート

コントロール 18：ペネトレーションテスト

コントロール（人、プロセス、テクノロジー）の弱点を特定して悪用し、攻撃者の目的と行動をシミュレーションすることで、企業資産の有効性とレジリエンシをテストします。

サブコントロール	タイトル	アセットタイプ	セキュリティ機能	IG1	IG2	IG3	Firewall が適合	Firewall がサポート	FMC が適合	FMC がサポート
18.1	ペネトレーションテスト プログラムの確立と維持	資料	ガバナンス		X	X		サポート		サポート
18.2	定期的な外部ペネトレーションテストの実施	ネットワーク	検出		X	X		サポート		サポート
18.3	ペネトレーションテストで判明した事項の修復	ネットワーク	保護		X	X		サポート		サポート
18.4	セキュリティ対策の検証	ネットワーク	保護			X		サポート		サポート
8.5	定期的な内部ペネトレーションテストの実施	ネットワーク	検出			X		サポート		サポート

© 2026 Cisco and/or its affiliates. All rights reserved.

主な所見

1. **ネットワークセキュリティおよび防御との強力な連携：**

- Cisco Secure Firewall と Firewall Management Center は、ネットワーク インフラストラクチャ管理、ネットワークモニタリング、アクセス制御の施行、侵入防御、および脅威検出に重点を置いた CIS 保護策と強力に連携します。
- これらのプラットフォームを組み合わせることで、お客様は安全なネットワークアーキテクチャ、通信検査、セグメンテーション、ポリシー施行、不審または不正なアクティビティへの対応などの管理領域を強化できます。

2. **一元化されたポリシー管理と運用の一貫性：**

- FMC は、ファイアウォールポリシー、イベント、設定、レポート、および運用監視の中央管理を可能にし、お客様が分散環境全体でセキュリティ管理策を一貫して適用できるようにします。
- これは、反復可能なプロセス、管理策の運用の文書化、監査の可視性、およびネットワークセキュリティ管理策の継続的な管理を必須とする CIS 保護策において特に重要です。

3. **可視性、ロギング、および監査証拠の有効なサポート：**

- Cisco Secure Firewall と FMC は、監査、調査、レポートに使用できるセキュリティイベント、接続データ、侵入イベント、マルウェアイベント、およびポリシーアクティビティを生成して一元化することにより、CIS コンプライアンスをサポートします。
- これらの機能は、監査ログ管理、ネットワークのモニタリングと防御、マルウェア防御、インシデント対応、および継続的なセキュリティ運用に関連する CIS コントロールにおいて特に有効です。

4. **侵入防御と対応の価値：**

- Cisco Secure Firewall は、侵入防御、マルウェア保護、URL フィルタリング、アプリケーションの可視性と制御、暗号化通信の処理、および Cisco Talos から提供される脅威インテリジェンスなどの機能を通じて能動的な防御をサポートします。
- FMC は、お客様によるイベントの関連付け、セキュリティアクティビティの確認、ポリシーの調整、調査または修復中に実行されたアクションの文書化を支援することで、対応ワークフローを強化します。

5. **より広範な CIS コンプライアンスにおける補完的な役割：**

- Cisco Secure Firewall と FMC は、ネットワークを中心とする CIS 保護策に関する技術的なサポートを提供しますが、一部のコントロールでは、ファイアウォール プラットフォーム外の補完的なツール、プロセス、またはオーナーシップが必要とされます。

従業員トレーニング、アイデンティティ ライフサイクル管理、端末設定、バックアップとリカバリ、ソフトウェア開発、サービスプロバイダーのガバナンスなどの領域は、より広範なセキュリティプログラムを通じて対処する必要があり、ファイアウォールと FMC の証拠を使用してそれらの結果をサポートします。

© 2026 Cisco and/or its affiliates. All rights reserved.

要約

Cisco Secure Firewall と FMC は、施行、テレメトリ、一元化されたポリシー、および運用に関する証拠を組み合わせることで、選択したシスコの機能を CIS Controls v8.1 にマッピングするお客様の取り組みをサポートします。Secure Firewall はネットワークセキュリティの施行レイヤを提供し、アクセス制御の施行、通信のセグメント化、アプリケーションの検査、URL のフィルタ処理、ファイルとマルウェアの分析、侵入の検出、安全なリモートアクセスのサポート、および価値の高いセキュリティイベントの生成を実行します。FMC は管理および可視性のプレーンを提供し、一貫性のあるコントロールの展開、ポリシーの調整、デバイスの正常性のモニタリング、イベントの分析、そしてコンプライアンスおよび対応ワークフローに向けた証拠の保存を支援します。

CIS 保護策がネットワークの可視性、境界防御、通信検査、一元化されたロギング、モニタリング、ポリシーの一貫性、および対応のサポートに依拠する場合に、この組み合わせによる価値が最も高くなります。企業全体のガバナンス、端末設定、ユーザートレーニング、サービスプロバイダー管理、ソフトウェア開発ライフサイクル管理、またはデータライフサイクルのオーナーシップを必要とする保護策の場合、Cisco Firewall と FMC は、適切なプロセスオーナーや関連するセキュリティ プラットフォームと組み合わせて使用すべき技術的な支援コントロールとして位置付けられます。

関連資料

詳細については、次を参照してください。

- CIS Critical Security Controls v8.1
- CIS Critical Security Controls Implementation Groups
- CIS Controls Navigator とフレームワークのマッピング
- Cisco Secure Firewall 製品ページ
- Cisco Secure Firewall Management Center 製品ページ
- Framework Mapping: Cisco Secure Firewall + NIST CSF 2.0

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)

米国で印刷　C22-6655244-00　08/26

© 2026 Cisco and/or its affiliates. All rights reserved.