セキュリティ、インターネットアクセス、および通信ポート

以下のトピックでは、システム セキュリティ、インターネット アクセス、および通信ポートに関する情報を提供します。

セキュリティと強化

Firewall Management Centerを保護するには、保護された内部ネットワークにそれをインストールしてください。Firewall Management Centerは必要なサービスとポートだけを使用するよう設定されますが、ファイアウォール外部からの攻撃がそこまで（または管理対象デバイスまで）決して到達できないようにする必要があります。

Firewall Management Center とその管理対象デバイスが同じネットワーク上に存在する場合は、デバイス上の管理インターフェイスを、Firewall Management Center と同じ保護された内部ネットワークに接続できます。これにより、Firewall Management Centerからデバイスを安全に制御することができます。また、他のネットワーク上のデバイスからのトラフィックを Firewall Management Center で管理および分離できるように、複数の管理インターフェイスを設定することもできます。

アプライアンスの展開方法に関係なく、アプライアンス間通信は暗号化されます。それでも、分散型サービス拒否（DDoS）や中間者攻撃などの手段でアプライアンス間の通信が中断、ブロック、または改ざんされないよう何らかの対策を講じる必要があります。

通信ポート

エッジ ファイアウォールなどのネットワーク バリアの背後にある展開の場合は、必要なポートでトラフィックを許可してください。本質的な動作またはデフォルトの動作に不要なポートは、構成または機能で必要になるまで閉じたままにすることに注意してください。

Firewall Management Center のポート

管理センターはこれらのポートを使用して通信します。

表 *1 : Firewall Management Center* の着信ポート

インバウンドポート	プロトコル/機能	詳細
22/tcp	SSH	アプライアンスへのリモート接続を保護します。
161/udp	SNMP	SNMP ポーリング経由で MIB にアクセスできるようにします。
443/tcp	HTTPS	**必須です。** 管理センターの Web インターフェイスへアクセスします。
443/tcp	HTTPS	Secure Device Connector（オンプレミス）を使用して、オンプレミスの Firewall Management Center を Security Cloud Control に導入準備します。
443/tcp	HTTPS	Firepower REST API を使用して、統合およびサードパーティ製品と通信します。
443/tcp	HTTPS	Secure Endpoint と統合します。
623/udp	SOL/LOM	Serial Over LAN（SOL）接続を使用した Lights-Out Management（LOM）。
1500/tcp 2000/tcp	データベースアクセス	サードパーティ クライアントによるイベント データベースへの読み取り専用アクセスを可能にします。
8302/tcp	eStreamer	eStreamer クライアントと通信します。
8305/tcp	アプライアンス通信	**必須です。** 管理対象デバイスとのセキュアな通信。また、このポートで接続を開始します。 設定可能。このポートを変更する場合は、展開内のすべてのアプライアンスについて変更する必要があります。デフォルトを維持することをお勧めします。
8307/tcp	ホスト入力クライアント	ホスト入力クライアントと通信します。

インバウンドポート	プロトコル/機能	詳細
8989/tcp	Cisco Support Diagnostics	許可された要求を受け入れ、使用状況の情報と統計情報を送信します。また、このポートで接続を開始します。

表 *2 : Firewall Management Center* のアウトバウンドポート

アウトバウンドポート	プロトコル/機能	詳細
7/UDP 514/udp 6514/tcp	Syslog（監査ロギング）	監査ロギングの設定時の syslog サーバーとの接続を確認します（7/udp）。 TLS が設定されていないときにリモート syslog サーバーに監査ログを送信します（514/udp）。 TLS の設定時にリモート syslog サーバーに監査ログを送信します（6514/tcp）。
25/tcp	SMTP	電子メール通知とアラートを送信。
53/tcp 53/udp	DNS	**必須です。** DNS
67/udp 68/udp	DHCP	DHCP
80/tcp	HTTP	インターネットからデータを送受信します。「インターネットリソースへのアクセス （6 ページ）」を参照してください。
80/tcp	HTTP	HTTP 経由でカスタム セキュリティ インテリジェンス フィードをダウンロードします。
80/tcp	HTTP	URL カテゴリとレピュテーションデータをダウンロードおよびクエリします。この機能も 443/tcp を使用します。
80/tcp	HTTP	RSS フィードをダッシュ ボードに表示します。
123/udp	NTP	時刻を同期します。
162/udp	SNMP	リモート トラップ サーバーに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP	外部認証用に LDAP サーバーと通信します。 検出された LDAP ユーザーに関するメタデータを取得します。 設定可能。
443/tcp	HTTPS	インターネットからデータを送受信します。「インターネットリソースへのアクセス （6 ページ）」を参照してください。

アウトバウンドポート	プロトコル/機能	詳細
443/tcp	HTTPS	Secure Malware Analytics Cloud と通信します（パブリックまたはプライベート）
443/tcp	HTTPS	Secure Endpoint と統合します。このポートの接続も受け入れます。
443/tcp	HTTPS	Cisco Security Cloud または Secure Device Connector（クラウド）を使用して、オンプレミスの Firewall Management Center を Security Cloud Control に導入準備します。
1812/udp 1813/udp	RADIUS	外部認証とアカウンティングのために RADIUS サーバーと通信します。 設定可能。
5222/tcp	ISE	ISE アイデンティティ ソースと通信します。
8305/tcp	アプライアンス通信	**必須です。** 管理対象デバイスとのセキュアな通信。このポートの接続も受け入れます。 設定可能。このポートを変更する場合は、展開内のすべてのアプライアンスについて変更する必要があります。デフォルトを維持することをお勧めします。
8989/tcp	Cisco Support Diagnostics	許可された要求を受け入れ、使用状況の情報と統計情報を送信します。このポートの接続も受け入れます。
8989/tcp	Cisco Success Network	使用状況情報および統計情報を送信します。

管理対象デバイスのポート

管理対象デバイスは、これらのポートを使用して通信します。

表 *3:* 管理対象デバイスのインバウンドポート

インバウンドポート	プロトコル/機能	詳細
22/tcp	SSH	アプライアンスへのリモート接続を保護します。
161/udp	SNMP	SNMP ポーリング経由で MIB にアクセスできるようにします。
443/tcp	HTTPS	Firepower REST API を使用して、統合およびサードパーティ製品と通信します。
443/tcp	リモート アクセス VPN（SSL/IPSec）	リモート ユーザーからネットワークへのセキュアな VPN 接続を許可します。

インバウンドポート	プロトコル/機能	詳細
500/udp 4500/udp	リモート アクセス VPN（IKEv2）	リモート ユーザーからネットワークへのセキュアな VPN 接続を許可します。
885/tcp	キャプティブポータル	キャプティブ ポータルのアイデンティティ ソースと通信します。
8305/tcp	アプライアンス通信	**必須です。** Firewall Management Center とセキュアに通信します。また、このポートで接続を開始します。 設定可能。このポートを変更する場合は、展開内のすべてのアプライアンスについて変更する必要があります。デフォルトを維持することをお勧めします。
8989/tcp	Cisco Support Diagnostics	許可された要求を受け入れます。また、このポートで接続を開始します。

表 *4*: 管理対象デバイスのアウトバウンドポート

アウトバウンドポート	プロトコル/機能	詳細
53/tcp 53/udp	DNS	DNS
67/udp 68/udp	DHCP	DHCP
123/udp	NTP	時刻を同期します。
162/udp	SNMP	リモート トラップ サーバーに SNMP アラートを送信します。
1812/udp 1813/udp	RADIUS	外部認証とアカウンティングのために RADIUS サーバーと通信します。 設定可能。
389/tcp 636/tcp	LDAP	外部認証用に LDAP サーバーと通信します。 設定可能。
443/tcp	HTTPS	インターネットからデータを送受信します。インターネットリソースへのアクセス （6 ページ） を参照してください。
514/udp	Syslog（監査ロギング）	TLS が設定されていないときにリモート syslog サーバーに監査ログを送信します。

アウトバウンドポート	プロトコル/機能	詳細
8305/tcp	アプライアンス通信	**必須です。** Firewall Management Center とセキュアに通信します。このポートの接続も受け入れます。 設定可能。このポートを変更する場合は、展開内のすべてのアプライアンスについて変更する必要があります。デフォルトを維持することをお勧めします。
8514/udp	Secure Network Analytics Manager	セキュリティ分析とロギング（オンプレミス） を使用して Secure Network Analytics に syslog メッセージを送信します。
8989/tcp	Cisco Support Diagnostics	使用状況情報および統計情報を送信します。このポートの接続も受け入れます。

インターネットリソースへのアクセス

インターネットにアクセスするシステムに加えて、ブラウザは Amplitude（amplitude.com）の Web 分析サーバーに接続し、個人特定可能でない使用状況データを Cisco に提供することができます。

Firewall Management Center がアクセスするインターネットリソース

Management Center は、ポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに接続します。NTP と whois を除いて、プロキシ サーバを構成できます。一部の機能では、場所によってシステムがアクセスできるリソースが決まります。一部の機能には、デバイスからのアクセスも必要です。次の表を参照してください。

表 *5 : Firewall Management Center* がアクセスするインターネットリソース

機能	理由	ハイ アベイラビリティ	リソース
CA 証明書バンドル	システム定義により毎日決まった時刻に、新しいCA証明書について自動的にクエリを実行するようになりました。ローカルCAバンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。	各ピアが自身の証明書をダウンロードします。	cisco.com/security/pki

機能	理由	ハイ アベイラビリティ	リソース
マルウェア防御	Secure Malware Analytics Cloud のルックアップ。	両方のピアが検索を実行します。	適切な Cisco Secure エンドポイントおよびマルウェア分析操作に必要なサーバー アドレス
	ファイル事前分類とローカルのマルウェア分析のシグニチャ更新をダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	動的分析結果のクエリを実行します。	両方のピアが動的分析レポートのクエリを実行します。	fmc.api.threatgrid.com fmc.api.threatgrid.eu
イベントエンリッチメント	Talos 分類のダウンロード イベントエンリッチメントについて Talos クラウドサービスにクエリを実行します。	両方のピアが通信します。	URL： • *.talos.cisco.com • est.sco.cisco.com IPv4 ブロック： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 ブロック： • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48
セキュリティ インテリジェンス	セキュリティ インテリジェンス フィードをダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	intelligence.sourcefire.com

機能	理由	ハイ アベイラビリティ	リソース
URL フィルタリング	URL カテゴリおよびレピュテーション データをダウンロードします。 URL カテゴリおよびレピュテーション データを手動でクエリ（ルックアップ）します。 未分類 URL のクエリ。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	URL： • *.talos.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com IPv4 ブロック： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 ブロック： • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48
Cisco Secure 動的属性コネクタ	Amazon Elastic Container Registry（Amazon ECR）からパッケージを取得する	各ピアは、独自のパッケージをダウンロードします。	public.ecr.aws csdac-cosign.s3.us-west-1.amazonaws.com
Secure Endpoint	Secure Endpoint によって検出されたマルウェア イベントをクラウドから受信します。 システムによって検出されたマルウェア イベントを Secure Endpoint に表示します。 Secure Endpoint で作成された一元的なファイル ブロックリストと許可リストを使用して、クラウドによる判断をオーバーライドします。	両方のピアがイベントを受信します。 両方のピア（設定が同期されていない）でクラウド接続を設定する必要もあります。	適切な Cisco Secure エンドポイントおよびマルウェア分析操作に必要なサーバー アドレス
Cisco Smart Software Manager	Smart Software Manager と通信します。	アクティブなピアが通信します。	www.cisco.com smartreceiver.cisco.com

機能	理由	ハイ アベイラビリティ	リソース
Cisco Success Network	使用状況情報および統計情報を送信します。	アクティブなピアが通信します。	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
Cisco Support Diagnostics	許可された要求を受け入れ、使用状況の情報と統計情報を送信します。	アクティブなピアが通信します。	api-sse.cisco.com:8989
Cisco XDR 統合	イベントを Cisco Security Cloudに送信するようにデバイスを構成する	アクティブなピアが通信します。	Cisco セキュア ファイア ウォール脅威防御と Cisco XDR 統合ガイド
時刻の同期	展開内で時間を同期します。 プロキシ サーバではサポートされません。	両方のピアが NTP サーバと通信します。	ユーザーによる構成
RSS フィード	ダッシュ ボードで Cisco 脅威調査ブログを表示します。	両方のピアが通信します。	blog.talosintelligence.com
アップグレード	製品（Management Center およびデバイス/シャーシ）のアップグレードをダウンロードします。	一方のピアで Firewall Management Center アップグレード パッケージをダウンロードすると、両方でのダウンロードが試行されます。一方のピアのみがインターネットにアクセスできる場合は、アップグレードプロセス中にパッケージを同期できます。 Firewall Management Center に保存されているデバイス アップグレード パッケージは同期しませんが、これらはその必要がありません。	cdo-ftd-images-us-west-2.amazonaws.com
侵入ルール	侵入ルール（SRU/LSP）をダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	est.sco.cisco.com updates-talos.sco.cisco.com updates-dyn-talos.sco.cisco.com updates.ironport.com
脆弱性データベース	VDB 更新をダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	support.sourcefire.com

機能	理由	ハイ アベイラビリティ	リソース
位置情報データベース	GeoDB 更新をダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	support.sourcefire.com
[Whois]	外部ホストの whois 情報を要求します。 プロキシ サーバではサポートされません。	whois 情報を要求するすべてのアプライアンスがインターネットにアクセスできる必要があります。	whois クライアントは、クエリ対象の適切なサーバの推測を試みます。推測できない場合、次を使用します。 • NIC ハンドル：whois.networksolutions.com • IPv4 アドレスとネットワーク名：whois.arin.net

管理対象デバイスによってアクセスされるインターネット リソース

管理対象デバイスは、ポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに接続します。NTP 以外のプロキシ サーバを構成できます。一部の機能では、場所によってシステムがアクセスできるリソースが決まります。

表 *6:* 管理対象デバイスによってアクセスされるインターネット リソース

機能	理由	高可用性/クラスタリング	Resource
CA 証明書バンドル	システム定義により毎日決まった時刻に、新しいCA証明書について自動的にクエリを実行するようになりました。ローカルCAバンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。	各ユニットが自身の証明書をダウンロードします。	cisco.com/security/pki
マルウェア防御	動的分析のためにファイルを送信します。	すべての装置がファイルを送信します。	fmc.api.threatgrid.com fmc.api.threatgrid.eu
Cisco Support Diagnostics	許可された要求を受け入れ、使用状況の情報と統計情報を送信します。	すべてのユニットが通信します。	api-sse.cisco.com:8989
時刻の同期	展開内で時間を同期します。 プロキシ サーバではサポートされません。	すべてのユニットが NTP サーバーと通信します。	ユーザーによる構成。

機能	理由	高可用性/クラスタリング	Resource
アップグレード	アップグレードを管理対象デバイスに直接ダウンロードします。 週に 1 回接続をテストします。	アップグレードパッケージは同期されません。各ユニットは、インターネット、アクティブな Firewall Management Center、または内部サーバーから独自の情報を取得する必要があります。	cdo-ftd-images.s3-us-west-2.amazonaws.com
Cisco XDR統合	Cisco Security Cloud にイベントを送信します。	すべてのユニットがイベントを送信します。	Cisco セキュア ファイアウォール脅威防御と Cisco XDR 統合ガイド

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。