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。

セキュリティ要件

Secure 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。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。

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、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、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 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。

シスコ クラウド

Management Center は次の機能で Cisco Cloud のリソースと通信します。

- **高度なマルウェア防御**

パブリッククラウドはデフォルトで設定されています。変更を加えるには、Cisco Secure Firewall Management Center デバイス構成ガイドの「Change AMP Options」を参照してください。

- **URL フィルタリング**

  詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「URL filtering」の章を参照してください。

- **との統合シスコのセキュリティ分析とロギング（SaaS）**

  Cisco Secure Cloud Analytics でのリモートデータストレージを参照してください。

- **SecureX および SecureX Threat Response** との統合

  詳細については、以下からリンクされている統合ドキュメントを参照してください。

  - シスコ SecureX との統合
  - によるイベントの分析 SecureX Threat Response

- **プロアクティブなサポート機能**

  詳細については、「Cisco Support Diagnostics の登録設定」を参照してください。

- **Cisco Success Network**

  詳細については、Cisco Success Network の登録設定 を参照してください。

- **Cisco Umbrella 接続**

  詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「DNS Policies」を参照してください。

インターネット アクセス要件

デフォルトでは、システムはポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに接続するように設定されています。アプライアンスがインターネットに直接アクセスしないようにするには、プロキシサーバを設定できます。多くの機能では、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。

ほとんどの場合、インターネットにアクセスするのは Management Center です。高可用性ペアの Management Center の両方にインターネット アクセスがある必要があります。機能に応じて、両方のピアがインターネットにアクセスすることも、アクティブ ピアのみがインターネットにアクセスすることもあります。

管理対象デバイスがインターネットにアクセスする場合もあります。たとえば、マルウェア保護設定が動的分析を使用する場合、管理対象デバイスはファイルを直接 Secure Malware Analytics クラウドに送信します。または、外部 NTPサーバーにデバイスを同期することができます。

さらに、Web 分析トラッキングを無効にした場合を除き、ブラウザは Google（google.com）または、Amplitude（amplitude.com） の Web 分析サーバーに連絡し、個人を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。

表 *1*:インターネット アクセス要件

機能	理由	Management Centerハイ アベイラビリティ	リソース
マルウェア防御	マルウェア クラウドルックアップ。	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」を参照してください。
	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（管理対象デバイス）のファイルを送信します。 動的分析結果のクエリ（Management Center）。	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
エンドポイント向け AMP	エンドポイント向け AMP によって検出されたマルウェア イベントを AMP 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 Cisco Advanced Malware Protection for Endpoints で表示します。 AMP クラウドからの性質をオーバーライドするには、AMP for Endpoints で作成された一元的なファイルブロックリストおよび許可リストを使用します。	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」を参照してください。
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	Management Center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： • regsvc.sco.cisco.com • est.sco.cisco.com • updates-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	アクティブピアとスタンバイピアがフィールドイメージを取得します。	https://public.ecr.aws https://csdac-cosign.s3.us-west-1.amazonaws.com
Cisco Smart Licensing	Cisco Smart Software Manager と通信します。	アクティブなピアが通信します。	smartreceiver.cisco.com www.cisco.com
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

機能	理由	Management Centerハイ アベイラビリティ	リソース
システムの更新プログラム	更新プログラムを Cisco から直接 Management Center にダウンロードします。 • システム ソフトウェア • 侵入ルール（SRU/LSP） • 脆弱性データベース（VDB） • 位置情報データベース（GeoDB）	侵入ルール、VDB、および GeoDB をアクティブなピアで更新し、アクティブなピアはその後スタンバイへ同期します。 各ピアで個別にシステム ソフトウェアをアップグレードします。	amazonaws.com cisco.com
SecureX Threat Response 統合	適切なインテグレーションガイドを参照してください。		
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。	外部 NTP サーバを使用するアプライアンスはインターネットにアクセスできる必要があります。	time.cisco.com
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。	RSS フィードを表示するアプライアンスはインターネットにアクセスできる必要があります。	blog.talosintelligence.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

通信ポートの要件

Management Center と管理対象デバイスは、ポート 8305/tcp の双方向型 SSL 暗号化通信チャネルを使用して通信します。このポートは、基本的な通信のためにオープンの状態で保持する必要があります。

他のポートでは、特定の機能に必要な外部リソースへのアクセスとともにセキュアな管理をすることができます。一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。開いたポートを閉じると展開にどのような影響が及ぶか理解するまでは、開いたポートを変更したり閉じたりしないでください。

表 *2:* 通信ポートの要件

ポート	プロトコル/機能	プラットフォーム	方向	詳細
22/tcp	SSH	Management Center Threat Defense	着信	アプライアンスへのリモート接続を保護します。
53/tcp 53/udp	DNS		発信	DNS
67/udp 68/udp	DHCP		発信	DHCP
123/udp	NTP		発信	時刻を同期します。
161/udp	SNMP	Management Center Threat Defense	着信	SNMP ポーリング経由で MIB にアクセスできるようにします。
162/udp	SNMP		発信	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		発信	外部認証用に LDAP サーバーと通信します。 検出された LDAP ユーザに関するメタデータを取得します（Management Center のみ）。 設定可能。
443/tcp	HTTPS	Management Center	着信	Web インターフェイスにアクセスします。
443/tcp	リモート アクセス VPN（SSL/IPSec）	Threat Defense	着信	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。
500/udp 4500/udp	リモート アクセス VPN（IKEv2）	Threat Defense	着信	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。
443/tcp	HTTPS	Management Center Threat Defense	着信	Cisco Terminal Services（TS）エージェントを含め、Firepower REST API を使用して、統合製品やサードパーティ製品と通信します。

ポート	プロトコル/機能	プラットフォーム	方向	詳細
443/tcp	HTTPS		発信	インターネットからデータを送受信します。 詳細については、インターネット アクセス要件 （2 ページ）を参照してください。
443	HTTPS	Management Center	両方	AMP for Endpoints との統合
514/udp	Syslog（アラート）		発信	リモート syslog サーバーにアラートを送信します。
623/udp	SOL/LOM	Management Center	着信	Serial Over LAN（SOL）接続を使用した Lights-Out Management（LOM）。
885/tcp	キャプティブポータル	Threat Defense	着信	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。
1500/tcp 2000/tcp	データベースアクセス	Management Center	着信	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。
1812/udp 1813/udp	RADIUS		発信	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。
8302/tcp	eStreamer	Management Center	着信	eStreamer クライアントと通信します。
8305/tcp	アプライアンス通信		両方	展開におけるアプライアンス間で安全に通信します。 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	Management Center	着信	ホスト入力クライアントと通信します。
8989/tcp	Cisco Support Diagnostics		両方	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。

関連トピック

Management Center 用の LDAP 外部認証オブジェクトの追加
Management Center 用の RADIUS 外部認証オブジェクトの追加

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。