



ファイアウォール情報

この章は、次の項で構成されています。

- [ファイアウォール情報 \(1 ページ\)](#)
- [ネットワーク攻撃からの電子メールゲートウェイの保護 \(7 ページ\)](#)

ファイアウォール情報

次の表に示すポートは、Cisco Secure Email Gateway を正常に動作させるために開く必要がある場合があります (デフォルト値を示す)。

表 1: ファイアウォールポート

| デフォルトポート | プロトコル | 内外 (In/Out) | ホストネーム | 目的 |
|----------|-------|-------------|--------------------|---|
| 20/21 | TCP | 入力または出力 | AsyncOS IP、FTP サーバ | ログファイルのアグリゲーション用 FTP。 データポート TCP 1024 以上はすべて開いている必要があります。 詳細については、ナレッジベースの FTP ポート情報を検索してください。 ナレッジベース を参照してください。 |
| 22 | TCP | 入力 | AsyncOS IP | CLI への SSH アクセス、ログファイルのアグリゲーション。 |
| 22 | TCP | 発信 | SSH サーバ | ログファイルの SSH アグリゲーション。 |

| | | | | |
|-----|---------|---------|------------------------|---|
| 22 | TCP | 発信 | SCP サーバ | ログ サーバへの SCP 配信。 |
| 25 | TCP | 発信 | 任意 (Any) | 電子メール送信用 SMTP。 |
| 25 | TCP | 入力 | AsyncOS IP | バウンスされた電子メールを受信する SMTP または外部のファイアウォールから電子メールをインジェクトする場合。 |
| 53 | UDP/TCP | 発信 | DNS サーバ | インターネットルートサーバまたはファイアウォール外部の DNS サーバを使用するように設定されている場合の DNS。また、SenderBase クエリの場合。 |
| 80 | HTTP | 入力 | AsyncOS IP | システム モニタリングのための GUI への HTTP アクセス。 |
| 80 | HTTP | 発信 | downloads.ironport.com | McAfee 定義を除くサービス更新。 |
| 80 | HTTP | 発信 | updates.ironport.com | AsyncOS アップグレードおよび McAfee の定義。 |
| 80 | HTTP | 発信 | TAXII サーバ | Eメールゲートウェイで外部脅威フィードを使用できるようにします。 |
| 82 | HTTP | 入力 | AsyncOS IP | スパム隔離の表示に使用されます。 |
| 83 | HTTPS | 入力 | AsyncOS IP | スパム隔離の表示に使用されます。 |
| 110 | TCP | 発信 | POP サーバ | スパム隔離のためのエンドユーザの POP 認証。 |
| 123 | UDP | 入力および出力 | NTP サーバ | タイム サーバがファイアウォールの外側にある場合の NTP。 |
| 143 | TCP | 発信 | IMAP サーバ | スパム隔離のためのエンドユーザの IMAP 認証。 |
| 161 | UDP | 入力 | AsyncOS IP | SNMP クエリ。 |

| | | | | |
|-----------------|-------|----|--|--|
| 162 | UDP | 発信 | 管理ステーション | SNMP トラップ。 |
| 389 または 3268 | LDAP | 発信 | LDAP サーバ | LDAP ディレクトリ サーバがファイアウォールの外側にある場合の LDAP。Cisco スпам隔離のための LDAP 認証。 |
| 636 または 3269 | LDAPS | 発信 | LDAPS | LDAPS — ActiveDirectory のグローバル カタログ サーバ (SSL 使用) |
| 443 | TCP | 入力 | AsyncOS IP | システム モニタリングのための GUI への Secure HTTP (https) アクセス。 |
| 443 | TCP | 発信 | res.cisco.com | アップデート サーバの最新のファイルを確認します。 |
| 443 | TCP | 発信 | update-manifests.ironport.com | アップデートサーバから最新のファイルのリストを取得します (物理ハードウェア E メール ゲートウェイの場合)。 |
| 443 | TCP | 発信 | update-manifests.sco.cisco.com | アップデートサーバから最新のファイルのリストを取得します (仮想 E メール ゲートウェイの場合)。 |
| 443 | TCP | 発信 | serviceconfig.talos.cisco.com grpc.talos.cisco.com email-sender-ip-rep-grpc.talos.cisco.com IP ベースのファイアウォールの場合： 146.112.62.0/24 146.112.63.0/24 146.112.255.0/24 146.112.59.0/24 2a04:e4c7:ffff::/48 2a04:e4c7:ffe::/48 | Cisco Talos インテリジェンスサービス：IP の評価、URL の評価およびカテゴリの取得とサービスログの詳細の送信を行います。 |

| | | | | |
|-----|-----|----|---|--|
| 443 | TCP | 発信 | kinesis.us-west-2.amazonaws.com sensor-provisioner.ep.prod .agari.com houston.sensor.prod.agari.com | Cisco Advanced Phishing Protection クラウドサービスに登録し、ヘッダーの詳細を送信します。 |
| 443 | TCP | 発信 | [セキュリティサービス (Security Services)] > [ファイルレピュテーションと分析 (File Reputation and Analysis)] の [ファイルレピュテーションの詳細設定 (Advanced Settings for File Reputation)] セクションの [クラウドサーバープール (Cloud Server Pool)] で設定されているとおりです。 | 設定されている場合、これはファイルレピュテーションを取得するためにクラウドサービスにアクセスするためのポートです。デフォルトポートは 32137 です。ファイル分析サービスの場合はポート 443 を参照してください。 |
| 443 | TCP | 発信 | [セキュリティサービス (Security Services)] > [ファイルレピュテーションと分析 (File Reputation and Analysis)] の [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクションで設定されているとおりです。 | ファイル分析のためのクラウドサービスへのアクセス。ファイルレピュテーションサービスの場合は、ポート 443 または 32137 を参照してください。 |

| | | | | |
|-----|-------|---------|--|--|
| 443 | TCP | 入力および出力 | <p>[セキュリティサービス (Security Services)]> [ファイルレピュテーションと分析 (File Reputation and Analysis)]の [ファイルレピュテーションの詳細設定 (Advanced Settings for File Reputation)]セクションの AMP for Endpoints コンソールの統合のパラメータで設定されているとおりで。</p> <p>api.amp.sourcefire.com api.eu.amp.sourcefire.com api.apjc.amp.sourcefire.com api.amp.cisco.com api.eu.amp.cisco.com api.apjc.amp.cisco.com</p> | AMP for Endpoints コンソール サーバにアクセスします。 |
| 443 | TCP | 入力および出力 | <p>outlook.office365.com login.microsoftonline.com。</p> | メールボックス自動修復のために Office 365 サービスにアクセスします。 |
| 443 | TCP | 入力および出力 | <p>オンプレミス Microsoft Exchange Server のホスト名</p> | メールボックスのメッセージを修復するには、オンプレミス Microsoft Exchange Server にアクセスします。 |
| 443 | TCP | 発信 | <p>aggregator.cisco.com</p> | Cisco Aggregator サーバにアクセスします。 |
| 443 | HTTPS | 発信 | <p>logapi.ces.cisco.com</p> | シスコ TAC によって収集されたデバッグ ログをアップロードするため。 |
| 443 | HTTPS | 発信 | <p>TAXII サーバ</p> | Eメールゲートウェイで外部脅威フィードを使用できるようにします。 |
| 443 | HTTPS | 入力および出力 | <p>api.sse.cisco.com</p> | Cisco SecureX または Cisco Threat Response に Eメールゲートウェイを登録するために使用します。 |

| | | | | |
|---------|---------|------------|---------------------------|---|
| 443 | HTTPS | 入力および出力 | api.eu.sse.itd.cisco.com | Cisco SecureX または Cisco Threat Response に E メールゲートウェイを登録するために使用します。 |
| 443 | HTTPS | 入力および出力 | api.apj.sse.itd.cisco.com | Cisco SecureX または Cisco Threat Response に E メールゲートウェイを登録するために使用します。 |
| 443 | HTTPS | 入力および出力 | est.sco.cisco.com | 証明書をダウンロードする場合に使用し、Cisco SecureX または Cisco Threat Response に登録するときに検証済みのサイトに E メールゲートウェイがアクセスしているかどうかを確認します。 |
| 443 | HTTPS | 入力および出力 | AsyncOS IP | trailblazerconfig CLI コマンドを使用した、GUI への HTTPS アクセス。 |
| 514 | UDP/TCP | 発信 | Syslog サーバ | Syslog ロギング。 |
| 628 | TCP | 入力および入力 | AsyncOS IP | 外部ファイアウォールから電子メールをインジェクトする場合の QMQP。 |
| 990 | TCP/FTP | 発信 | support-ftp.cisco.com | シスコ TAC によって収集されたデバッグ ログをアップロードするため。 |
| 1024 以降 | — | — | — | ポート 21 (FTP) に関する上記の情報を参照してください。 |
| 2222 | CCS | 入力および入力 | AsyncOS IP | クラスタ通信サービス (中央集中管理用)。 |
| | TCP | 発信 | AsyncOS IP | Cisco スпам隔離。 |
| 7025 | TCP | In および Out | AsyncOS IP | この機能が一元化されている場合、Cisco Secure Email Gateway と Cisco Secure Manager Email and Web Gateway 間でポリシー、ウイルス、およびアウトブレイク隔離データを渡します。 |

| | | | | |
|------|-------|---------|------------|--------------------------|
| 6080 | HTTP | 入力または出力 | AsyncOS IP | HTTP サーバの API ポートへのアクセス |
| 6443 | HTTPS | 入力または出力 | AsyncOS IP | HTTPS サーバの API ポートへのアクセス |

ネットワーク攻撃からの電子メールゲートウェイの保護

電子メールゲートウェイをネットワーク攻撃から保護するには、次の前提条件を満たす必要があります。

- ポート 22 (SSH) を電子メールゲートウェイの外部 IP アドレスに公開しないこと。
- Web インターフェイスと CLI 構成設定を使用して電子メールゲートウェイを管理する際、特定の IP アドレスのみを有効にすること。
- (必要な場合) `adminaccessconfig CLI` コマンドを使用して `Host` ヘッダー対策機能を有効にすること。
- `adminaccessconfig CLI` コマンドを使用して、クロスサイトスクリプティング対策機能を有効にすること。
- パブリックリスナーにリレールールを設定しないこと。



(注) 外部リスナーでリレールールが必要な場合は、通常のパブリックリスナーで「SMTP AUTH」を設定します。

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。