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

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 ベースの記事を参照してください。
22	SSH	発信	AsyncOS IP	中央集中型コンフィギュレーション マネージャのコンフィギュレーションの配信。 バックアップにも使用されます。

ファイアウォール情報

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	SCP サーバ	ログ サーバへの SCP 配信。
23	Telnet	入力	AsyncOS IP	CLI への Telnet アクセス。
23	Telnet	発信	Telnet サーバ	Telnet アップグレード
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	AsyncOS アップグレードおよび。
80	HTTP	発信	upgrades.ironport.com	AsyncOS アップグレード。
801	HTTP	入力および出力	AsyncOS IP	`trailblazerconfig` CLI コマンドを使用した、GUI への HTTP アクセス。
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。

ファイアウォール情報

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 スパム隔離のための 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	update-static.ironport.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	phonehome.senderbase.org	アウトブレイク フィルタの受信/送信。

ファイアウォール情報

443	TCP	発信	Web Security Appliances の [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] ページの [詳細設定（Advanced）] セクション > [ファイル分析の詳細設定（Advanced Settings for File Analysis）] で設定されているファイル分析サーバ URL。 Email Security Appliance の [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）] ページの [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ファイル分析サーバ URL。	ファイル分析サーバに詳細なファイル分析結果を表示します。 • Web セキュリティ レポート：（クラウドファイル分析）管理アプライアンスがファイル分析サーバに到達できることを確認する
443	HTTPS	入力および出力	api sse.cisco.com	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 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 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。

ファイアウォール情報

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。
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。
32137	TCP			
6080	HTTP	入力または出力		HTTP サーバの API ポートへのアクセス
6443	HTTPS	入力または出力		HTTPS サーバの API ポートへのアクセス

ファイアウォール情報

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。