



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 \(1 ページ\)](#)

ファイアウォール情報

次の表は、Cisco コンテンツセキュリティアプライアンスを正常に動作させるために開けなければならないことがあるポートのリストです（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	In または Out	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 (Out)	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。

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 (Out)	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 (Out)	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 (Out)	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 (Out)	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 (Out)	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 (Out)	管理ステーション	SNMP トラップ。
389 または 3268	LDAP	発信 (Out)	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 (Out)	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 (Out)	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 (Out)	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 アプライアンスの場合)。
443	[TCP]	発信 (Out)	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 (仮想アプライアンスの場合)。
443	[TCP]	発信 (Out)	phonehome.senderbase.org	アウトブレイク フィルタの受信/送信。

443	[TCP]	発信 (Out)	<p>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。</p> <p>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。</p>	<p>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。</p> <ul style="list-style-type: none"> • Web セキュリティレポート : (クラウドファイル分析) 管理アプリケーション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 にアプリケーション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 にアプリケーション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 に登録するときに確認済みのサイトにアプリケーション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 (Out)	Syslog サーバ	Syslog ロギング。

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	この機能を集中化する場合、Eメールセキュリティアプライアンスとセキュリティ管理アプライアンス間でポリシー、ウイルス、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

