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	入力/出力	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。

ファイアウォール情報

22	TCP	発信	SCP サーバ	ログ サーバへの SCP 配信。
25	TCP	発信	任意	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	。
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	cdn-microupdates.cloudmark.com	Intelligent MultiScan 機能のサードパーティ スパム コンポーネントへの更新に使われます。アプライアンスは、サードパーティの phone home の更新の CIDR 範囲 208.83.136.0/22 に接続する必要があります。
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。

ファイアウォール情報

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。
6363269	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 アプライアンスの場合）。
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（仮想アプライアンスの場合）。
443	TCP	発信	phonehome.senderbase.org	アウトブレイク フィルタの受信/送信。
443	TCP	発信	コマンドライン インターフェイスで websecurityadvancedconfig コマンドを実行し、すべてのデフォルトを受け入れます。Web セキュリティ サービスのホスト名が表示されます。	URL フィルタリングに使用する URL レピュテーションとカテゴリの情報を取得するためのクラウド サービス。

ファイアウォール情報

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	[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す。 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	AMP for Endpoints コンソール サーバにアクセスします。

ファイアウォール情報

443	TCP	入力および出力	outlook.office365.com login.microsoftonline.com。	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	発信	aggregator.cisco.com	Cisco Aggregator サーバにアクセスします。
443	HTTPS	発信	logapi.ces.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。
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）。
7025	TCP	入力および出力	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。

ファイアウォール情報