GLOSSARY

C

CIDR の表記

Classless Inter-Domain Routing。任意のビット数でネットワーク コンテキスト内の IP アドレス範囲を説明するのに便利な省略表現。この表記を使用して、スラッシュ（/）の後に続けて、ネットワーク部分に使用するビット数を追加することで、アドレスのネットワーク プレフィクス部分を記述します。したがって、クラス C ネットワークは、プレフィクス表記で 192.168.0.1/24 と記述できます。CIDR 仕様による 206.13.1.48/25 は、アドレスの先頭 25 ビットが、206.13.1.48 の先頭 25 ビットと一致する任意のアドレスを含みます。

D

DLP

Data Loss Prevention（データ消失防止）。RSA Security の DLP スキャン エンジンを使用して、ユーザによる機密データの電子メールでの誤送信を防ぐことにより、組織の情報および知的財産を守り、規制および組織的なコンプライアンスを順守させます。

DLP 違反

一例として、メッセージ内で検出された、組織の DLP ルールに違反するデータ。

DLP インシデント

データ消失防止インシデントは、DLP ポリシーにより発信メッセージ内に留意すべき 1 つ以上の DLP 違反を検出すると発生します。

DLP ポリシー

データ消失防止ポリシーは、発信メッセージに機密データが含まれているかかどうかを判断し、そのようなデータを含むメッセージに対して AsyncOS が実行するアクションの決定に使用される条件のセットです。

DLP リスク要因

発信メッセージで検出される DLP 違反のセキュリティ リスクを表す 0 ～ 100 のスコア。リスク要因に基づいて、DLP ポリシーによってメッセージに対して実行するアクションが決まります。

DNS Domain Name System（ドメイン ネーム システム）。「RFC 1045」および「RFC 1035」を参照してください。ネットワーク上の DNS サーバは IP アドレスをホスト名に、ホスト名を IP アドレスに解決します。

DoS 攻撃 Denial of Service（サービス拒絶）攻撃。Distributed Denial of Service（DDos; 分散型サービス拒絶）攻撃にもなり得ます。ネットワークまたはコンピュータ上での攻撃。特定のサービスへのアクセスを中断させることを主な目的とします。

DSN Delivery Status Notification（配信ステータス通知）。バウンスされるメッセージ。

F

False Negative スパム メッセージ、またはウイルスや DLP 違反を含むメッセージであるが、検出されなかったメッセージ。

False Positive スパムとして、またはウイルスや DLP 違反を含むメッセージとして誤って分類されたメッセージ。

H

HAT Host Access Table（ホスト アクセス テーブル）。HAT は、リモート ホストからの着信接続を制御するリスナー用のルール セットを保持しています。いずれの*リスナー*にも独自の HAT があります。HAT は、パブリックおよびプライベートのリスナー用に定義され、*メール フロー ポリシー*および*送信者グループ*を含みます。

I

IDE ファイル ウイルス定義ファイル。IDE ファイルには、ウイルスを検出するアンチウイルス ソフトウェアによって使用されるシグニチャまたは定義が格納されています。

L

LDAP Lightweight Directory Access Protocol。インターネット ディレクトリまたはイントラネット ディレクトリのユーザ（電子メール アドレスを含む）、組織などのリソースに関する情報へのアクセスに使用されるプロトコルです。

M

MAIL FROM 「*エンベロープ送信者*」を参照してください。

MTA Mail Transfer Agent または Messaging Transfer Agent。電子メール メッセージの受け入れ、ルーティング、配信を担当するプログラム。Mail User Agent または他の MTA からのメッセージの受信時、MTA はメッセージを一時的にローカルに保存し、受信者を分析し、他の MTA にメッセージをルーティングします。メッセージ ヘッダーを編集したり、追加したりする場合もあります。IronPort アプライアンスは、ハードウェア、セキュリティの強化されたオペレーティング システム、アプリケーション、およびサポート サービスを組み合わせ、目的に合わせて構築された、企業のメッセージング専用のラックマウント サーバ アプライアンスを提供する MTA です。

MUA Mail User Agent。ユーザが電子メール メッセージを作成および読むことができるプログラム。MUA は、ユーザと Message Transfer Agent 間のインターフェイスを提供します。発信メールは、最終的に MTA に渡されて配信されます。

MX レコード 特定のドメインのメールの受け入れを担当するインターネット上の MTA を指定します。Mail Exchange レコードは、ドメイン名のメール ルートを作成します。1 つのドメイン名には、複数のメール ルートを作成でき、それぞれにプライオリティ番号が割り当てられます。最も小さい番号のメール ルートは、そのドメインを担当するプライマリ サーバになります。リストされる他のメール サーバは、バックアップとして使用されます。

N

NTP Network Time Protocol（ネットワーク タイム プロトコル）。`ntpconfig` コマンドでは、Network Time Protocol（NTP; ネットワーク タイム プロトコル）を使用してシステム クロックを他のコンピュータと同期するように、IronPort AsyncOS を設定します。

R

RAT Recipient Access Table（受信者アクセス テーブル）。受信者アクセス テーブルでは、パブリック リスナーが受け入れる受信者を定義します。テーブルは、アドレス（場合により、部分的なアドレスまたはホスト名）およびそのアドレスを受け入れるか拒否するかを指定します。その受信者に対する RCPT TO コマンドへの SMTP 応答を任意に含めることができます。RAT には通常、ローカル ドメインを含めます。

RCPT TO 「*エンベロープ受信者*」を参照してください。

S

STARTTLS Transport Layer Security（TLS）は、Secure Socket Layer（SSL）テクノロジーの改良版です。これは、インターネット上での SMTP カンバセーションの暗号化に広く使用されているメカニズムです。IronPort AsyncOS オペレーティング システムは、RFC 2487 に記述されている、SMTP の STARTTLS 拡張（Secure SMTP over TLS）をサポートします。

T

TOC Threat Operations Center。これは、ウイルス拡散の検出と対応にかかわる、すべてのスタッフ、ツール、データ、およびファシリティを指します。

あ

アンチウイルス

Sophos および McAfee のアンチウイルス スキャン エンジンは、ファイルをスキャンしてウイルス、トロイの木馬、およびワームを見つけるウイルス検出エンジンを使用して、クロスプラットフォームのアンチウイルスの保護、検出、およびウイルス除去を行います。これらのプログラムは、「悪意のあるソフトウェア」を意味する *マルウェア*と総称されます。アンチウイルス スキャナは、すべてのタイプのマルウェアに共通する相似点を利用して、ウイルスだけでなく、すべてのタイプの悪意のあるソフトウェアを検出および削除します。

う

ウイルス感染フィルタ

IronPort のウイルス感染フィルタ機能は、ウイルスから保護するための追加の層を提供します。ウイルス感染フィルタ機能は、疑わしい電子メール メッセージを検疫し、更新されたウイルス IDE が使用可能になるまで、または脅威なしと判断されるまでの間、そのメッセージを保持します。

え

エンベロープ受信者

RCPT TO: SMTP コマンドで定義される電子メール メッセージの受信者。「Recipient To」または「Envelope To」アドレスと呼ばれることもあります。

エンベロープ送信者

MAIL FROM: SMTP コマンドで定義される電子メール メッセージの送信者。「Mail From」または「Envelope From」アドレスと呼ばれることもあります。

お

オープン リレー

オープン リレー（「セキュアでないリレー」または「サード パーティ」リレーともいう）は、電子メール メッセージの検査なしのサード パーティ リレーを許可する SMTP 電子メール サーバです。オープン リレーは、ローカル ユーザ以外が送受信する電子メールを処理することで、不明な送信者が大量の電子メール（典型的には*スパム*）をご使用の*ゲートウェイ*を通過してルーティングできるようにします。`listenerconfig` コマンドおよび `systemsetup` コマンドは、ユーザが気付かずにシステムをオープン リレーとして設定することを防止します。

か

完全修飾ドメイン名（FQDN）

ドメイン名でよりレベルの高いドメイン名からトップレベル ドメイン名までを含めたドメイン名。たとえば、`mail3.example.com` は、192.168.42.42 の *ホスト*の完全修飾ドメイン名であり、`example.com` は、example.com *ドメイン*の完全修飾ドメイン名です。完全修飾ドメイン名は、インターネット内で一意である必要があります。

カンバセーション型バウンス

SMTP カンバセーション内で発生するバウンス。カンバセーション型バウンスには、*ハード バウンス*と*ソフト バウンス*の 2 種類があります。

き

キュー

IronPort アプライアンスでは、電子メール キュー内のメッセージを削除、バウンス、保留、またはリダイレクトできます。宛先ドメインへのメッセージのこの電子メール キューは、*配信*キューとも呼ばれます。IronPort Anti-Spam またはメッセージ フィルタ アクションによる処理を待機しているメッセージのキューは、*ワーク* キューとも呼ばれます。`status detail` コマンドを使用して、両方のキューのステータスを表示できます。

キューの最大時間

*ハード バウンス*される前に、*配信*用の電子メール キューに*ソフト バウンス*メッセージがとどまる最大時間。

許可ホスト

プライベート リスナー経由で IronPort アプライアンスを使用した電子メールのリレーが許可されたコンピュータ。許可ホストは、そのホスト名または IP アドレスによって定義されます。

こ

コンテンツ フィルタ 電子メール パイプラインのワーク キューの受信者単位のスキャン フェーズ中にメッセージを処理するために使用されるコンテンツ ベースのフィルタ。コンテンツ フィルタはメッセージ フィルタの後に呼び出され、個々の分裂されたメッセージに対して実行されます。

コンテンツ照合分類子 RSA データ消失防止スキャン エンジンの検出コンポーネント。分類子には、裏付けデータを検索するコンテキスト ルールとともに、機密データを検出するためのいくつかのルールが含まれます。たとえば、クレジット カードの分類子には、メッセージにクレジット カード番号と一致するストリングが含まれているだけでなく、期限データ、クレジット カード会社名、住所などの裏付け情報も含まれる必要があります。

さ

最大リトライ回数 *ハード バウンス*される前に、*ソフト バウンス* メッセージの再配信を試行する最大回数。

し

受信 IP インターフェイスで設定された特定のリスナーの電子メール メッセージを受信する動作。IronPort アプライアンスは、インターネットからのインバウンドまたはイントラネット システムからのアウトバウンドの電子メール メッセージを受信するようにリスナーを設定します。

す

スパム Unwanted, Unsolicited Commercial Bulk Email（UCE/UBE）。アンチスパム スキャンでは、フィルタリング ルールに従って、スパムの疑いがある電子メール メッセージを識別します。

そ

送信者グループ
送信者グループは、単に、複数の送信者からの電子メールを同じ方法で扱う（つまり、送信者のグループにメール フロー ポリシーを適用する）ために集められた送信者のリストです。送信者グループは、リスナーの Host Access Table（HAT; ホスト アクセス テーブル）でカンマ区切りの送信者（IP アドレス、IP 範囲、ホスト / ドメイン、SenderBase 評価サービスの分類、SenderBase 評価スコア範囲、または DNS リスト クエリー応答により識別）のリストです。*メール フロー ポリシー*と同様に、送信者グループに名前を割り当てます。

ソフト バウンス メッセージ
キューに設定された*最大リトライ回数*または*最大時間*に基づいて、後から配信が再試行されるメッセージ。

ち

遅延型バウンス
SMTP カンバセーション内で発生するバウンス。受信者のホストは、配信用のメッセージを受け入れますが、後でバウンスするだけです。

て

デバウンス タイム アウト
システムがユーザに同一のアラートの送信を控える時間（秒単位）。

電子メール セキュリティ マネージャ
IronPort アプライアンス上ですべての電子メール セキュリティ サービスおよびアプリケーションを管理するための、単一で包括的なダッシュボード。電子メール セキュリティ マネージャにより、ウイルス感染フィルタ、アンチスパム、アンチウイルス、および電子メール コンテンツのポリシーを、受信者単位または送信者単位で、インバウンドとアウトバウンドの独立したポリシーを使用して管理できます。「*コンテンツ フィルタ*」も参照してください。

は

ハード バウンス メッセージ

永続的に配信できないメッセージ。SMTP カンバセーション中またはその後に生じることがあります。

配信

特定の IP インターフェイスから、受信者のドメインまたは IronPort アプライアンスの内部メール ホストに電子メール メッセージを配信する動作。IronPort アプライアンスは、Virtual Gateway テクノロジーを使用して、同じ物理マシン内の複数の IP インターフェイスからメッセージを配信できます。各仮想ゲートウェイには、独立した IP アドレス、ホスト名とドメイン、および電子メール キューがあり、それぞれに異なるメール フロー ポリシーおよびスキャンの方法を設定できます。

リモート ホストへの最大同時接続、仮想ゲートウェイ単位のホストへの最大同時接続の制限、およびリモート ホストへのカンバセーションを暗号化するかどうかなど、IronPort アプライアンスが実行する配信の設定を、調整できます。

ひ

非カンバセーション型バウンス

受信者のホストがメッセージを受け入れて配信した後に、そのメッセージが返されたために発生するバウンス。ソフト（4XX）またはハード（5XX）のバウンスがあります。これらのバウンス応答を分析し、受信者メッセージに対して実行する処理（ソフト バウンスされた受信者メッセージの再送信、ハード バウンスされた受信者のデータベースからの削除など）を判断します。

評価フィルタ

疑わしい送信者を評価に基づいてフィルタリングする方法。SenderBase 評価サービスは、リモート ホストの接続 IP アドレスに基づいて、陽性と疑わしいスパムを拒否または抑制するための、正確で柔軟な方法を提供します。

ふ

ブラックリスト

既知の不適切な送信者のリスト。デフォルトで、パブリック リスナーのブラックリスト送信者グループに含まれる送信者は、$BLOCKED *メール フロー ポリシー*で設定されたパラメータによって拒否されます。

ほ

ホワイトリスト

既知の適切な送信者のリストです。信頼する送信者をホワイトリストの*送信者グループ*に追加します。$TRUSTED メール フロー ポリシーは、信頼する送信者からの電子メールは*レート制限*をイネーブルにせず、これらの送信者のコンテンツはアンチスパム スキャンの対象にならないように設定されます。

め

メール フロー ポリシー

メール フロー ポリシーは、*リスナー*の *Host Access Table*（HAT; ホスト アクセス テーブル）パラメータ（アクセス ルールの後に *rate limiting* パラメータ、カスタム SMTP コード、および応答が続く）のグループを表す方法です。*送信者グループ*およびメール フロー ポリシーは合わせて、リスナーの HAT で定義されます。ご使用の IronPort アプライアンスは、リスナーの事前定義済みメール フロー ポリシーおよび送信者グループが設定された状態で出荷されます。

も

文字セット（2 バイト）

2 バイト文字セットは、各文字の表現に 2 バイト以上の情報を必要とする外国語文字セットです。

り

リスナー

リスナーは、特定の IP インターフェイスで設定される電子メール処理サービスを記述します。リスナーは、ネットワーク内にある内部システムまたはインターネットから IronPort アプライアンスに入る電子メールだけに適用されます。IronPort AsyncOS は、メッセージを受け入れて受信者のホストにリレーするために、リスナーを使用してメッセージが満たす必要のある基準を指定します。リスナーを「電子メールのインジェクタ」として、または指定する IP アドレスごとに実行される「SMTP デーモン」として考えることもできます。

IronPort AsyncOS は、デフォルトでインターネットから電子メールを受信する特性を持つ*パブリック*リスナーと、内部（グループウェア、POP/IMAP などのメッセージ生成）システムからだけの電子メールの受け入れを目的とした*プライベート*リスナーを区別します。

れ

レート制限

レート制限では、リモート ホストから受け入れるセッション単位の最大メッセージ数、メッセージ単位の最大受信者数、最大メッセージ サイズ、時間単位の最大受信者数、および最大同時接続数を制限します。

ろ

ログ サブスクリプション

IronPort アプライアンスのパフォーマンスをモニタするログ ファイルの作成。ログ ファイルは、ローカル ディスクに保存され、リモート システムに転送および保管することもできます。ログ サブスクリプションの典型的な属性には、名前、モニタ対象コンポーネント（電子メール操作、サーバ）、形式、転送方法などがあります。