ログ

この章は、次の項で構成されています。

概要

ログ ファイルおよびログ サブスクリプションについて

ログは、AsyncOS の電子メール動作に関する重要な情報を収集する、簡潔で効率的な方法です。これらのログには、電子メールゲートウェイでのアクティビティに関する情報が記録されます。情報は、バウンス ログや配信ログなど、表示するログによって異なります。

ほとんどのログは、プレーンテキスト（ASCII）形式で記録されますが、配信ログはリソースの効率性を保つためにバイナリ形式で記録されます。ASCII テキスト情報は、任意のテキストエディタで読むことができます。

シスコは、複数の電子メールゲートウェイからのログに対応する集中化レポーティングおよびトラッキングツールとして、M シリーズ Cisco Secure Manager Email and Web Gateway を提供しています。詳細については、シスコの担当者にお問い合わせください。

ログ サブスクリプションはログ タイプを名前、ログ レベル、およびサイズや宛先情報などのその他の制約に関連付けます。同じログ タイプで複数のサブスクリプションを使用できます。

ログ タイプ

ログタイプは、メッセージデータ、システム統計情報、バイナリまたはテキストデータなど、生成されたログにどの情報が記録されるかを示します。ログ タイプは、ログ サブスクリプショ

ンを作成するときに選択します。詳細については、ログ サブスクリプション （78 ページ）を参照してください。

AsyncOS では、次のログ タイプが生成されます。

表 *1*: ログ タイプ

ログ	説明
テキスト メール ログ	テキスト メール ログには、電子メール システムの動作に関する情報が記録されます。たとえば、メッセージの受信、メッセージの配信試行、接続のオープンとクローズ、バウンス、TLS 接続などです。
qmail 形式メール ログ	qmail 形式配信ログには、次の配信ログと同じ電子メール システムの動作に関する情報が記録されますが、qmail形式で格納されます。
配信ログ	配信ログには、電子メールゲートウェイの電子メール配信動作に関する重要な情報が記録されます。たとえば、配信試行時の各受信者の配信やバウンスに関する情報などです。ログ メッセージは「ステートレス」です。つまり、関連するすべての情報が各ログ メッセージに記録されるので、ユーザは、現在の配信試行に関する情報について前のログ メッセージを参照する必要がありません。配信ログは、リソースの効率性を保つためにバイナリ形式で記録されます。配信ログ ファイルは、提供されるユーティリティを使用して XML または CSV（カンマ区切り値）形式に変換し、後処理する必要があります。変換ツールは、次の場所にあります。 https://supportforums.cisco.com/document/33721/cisco-ironport-systems-contributed-tools
バウンス ログ	バウンス ログには、バウンスされた受信者の情報が記録されます。バウンスされた各受信者を記録する情報には、メッセージ ID、受信者 ID、エンベロープ送信元アドレス、エンベロープ宛先アドレス、受信者がバウンスされる理由、および受信者ホストからの応答コードが含まれます。また、バウンスされた各受信者メッセージの一定量を記録するように選択することもできます。この容量はバイト単位で定義され、デフォルトはゼロです。
ステータス ログ	このログ ファイルには、status detail および dnsstatus などの CLI ステータス コマンドで検出されたシステムの統計情報が記録されます。記録期間は、logconfig の setup サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。

ログ	説明
ドメイン デバッグ ログ	ドメインデバッグログには、電子メールゲートウェイと指定の受信者ホスト間のSMTP会話でのクライアントとサーバの通信が記録されます。このログ タイプは、特定の受信者ホストに関する問題のデバッグに使用できます。ログ ファイルに記録するSMTPセッションの総数を指定する必要があります。セッションが記録されるにつれ、この数は減少していきます。ログ サブスクリプションを削除または編集して、すべてのセッションが記録される前にドメインデバッグを停止できます。
インジェクションデバッグ ログ	インジェクションデバッグログには、電子メールゲートウェイと、システムに接続している指定のホスト間のSMTP会話が記録されます。インジェクション デバッグ ログは、E メール セキュリティ アプライアンスとインターネット上のホスト間の通信に関する問題をトラブルシューティングするのに役立ちます。
システム ログ	システムログには、ブート情報、仮想電子メールゲートウェイ ライセンスの期限切れアラート、DNSステータス情報、およびcommitコマンドを使用してユーザが入力したコメントが記録されます。システムログは、電子メールゲートウェイの基本的な状態のトラブルシューティングに役立ちます。
CLI 監査ログ	CLI監査ログには、システム上のすべてのCLIアクティビティが記録されます。
FTP サーバ ログ	FTP ログには、インターフェイスで有効になっている FTP サービスの情報が記録されます。接続の詳細とユーザ アクティビティが記録されます。
GUI ログ	HTTP ログを参照してください。
HTTP ログ	HTTPログには、インターフェイスでイネーブルになっているHTTPサービス、セキュアHTTPサービス、またはその両方のサービスに関する情報が記録されます。HTTPを介してグラフィカルユーザーインターフェイス（GUI）にアクセスするため、HTTP ログは基本的に、CLI監査ログのGUI版になっています。GUIでアクセスされるセッションデータ（新しいセッション、セッションの期限切れ）やページが記録されます。 これらのログには、SMTPトランザクションに関する情報（たとえば、電子メールゲートウェイから電子メールで送信されるスケジュール済みレポートに関する情報）も記録されます。

ログ	説明
NTP ログ	NTP ログには、設定されている任意のネットワーク タイム プロトコル（NTP）サーバと電子メールゲートウェイ間の会話が記録されます。詳細については「システム管理」の章の「ネットワーク タイム プロトコル（NTP）設定の編集（Time Keeping Method）」を参照してください。
LDAP デバッグ ログ	LDAP デバッグ ログは、LDAP インストールのデバッグを目的としています(「LDAP クエリー」の章を参照）。電子メールゲートウェイが LDAP サーバに送信しているクエリに関する有用な情報がここに記録されます。詳細については、次を参照してください。
アンチスパム ログ	アンチスパム ログには、最新のアンチスパム ルールのアップデート受信に関するステータスなど、システムのアンチスパム スキャン機能のステータスが記録されます。また、コンテキスト適応スキャンエンジンに関するすべてのログもここに記録されます。
アンチスパム アーカイブ	アンチスパム スキャン機能をイネーブルにすると、スキャンされ、「メッセージのアーカイブ」アクションに関連付けられたメッセージがここにアーカイブされます。この形式は、mbox 形式のログ ファイルです。アンチスパム エンジンの詳細については、「アンチスパム」の章を参照してください。
グレイメール エンジン ログ	グレイメール エンジン、ステータス、設定などの情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。
グレーメール アーカイブ	アーカイブされたメッセージ（スキャン済みの「アーカイブ メッセージ」アクションに関連付けられているメッセージ）が含まれます。この形式は、mbox 形式のログ ファイルです。
アンチウイルス ログ	アンチウイルス ログには、最新のアンチウイルス アイデンティティ ファイルのアップデート受信に関するステータスなど、システムのアンチウイルス スキャン機能のステータスが記録されます。
アンチウイルス アーカイブ	アンチウイルス エンジンをイネーブルにすると、スキャンされ、「メッセージのアーカイブ」アクションに関連付けられたメッセージがここにアーカイブされます。この形式は、mbox 形式のログ ファイルです。詳細については、「ウイルス対策」の章を参照してください。
AMP エンジン ログ	AMP エンジンのログは、システムの高度なマルウェア防御機能の状態を記録します。詳細については、ファイル レピュテーション フィルタリングとファイル分析を参照してください。

ログ	説明
AMP アーカイブ	高度なマルウェア防御エンジンがスキャン不可能またはマルウェアを含む添付ファイルがあると判断したメッセージをアーカイブするために、メール ポリシーを設定している場合、そのメッセージがここにアーカイブされます。この形式は、mbox 形式のログ ファイルです。
スキャン ログ	スキャン ログには、スキャン エンジンに関するすべての LOG および COMMON メッセージが保持されます（アラートを参照してください）。これは一般に、アプリケーションの障害、送信されたアラート、失敗したアラート、およびログ エラー メッセージになります。このログは、システム全体のアラートには適用されません。
スパム隔離ログ	スパム隔離ログには、スパム隔離プロセスに関連付けられたアクションが記録されます。
スパム隔離 GUI ログ	スパム隔離ログには、GUI を介した設定、エンド ユーザー認証、およびエンド ユーザー アクション（電子メールの解放など）を含む、スパム隔離に関連付けられたアクションが記録されます。
SMTP 会話ログ	SMTP 会話ログには、着信および発信 SMTP 会話のすべての部分が記録されます。
セーフリスト/ブロックリスト ログ	セーフリスト/ブロックリスト ログには、セーフリスト/ブロックリストの設定およびデータベースに関するデータが記録されます。
レポーティング ログ	レポーティング ログには、中央集中型レポーティング サービスのプロセスに関連付けられたアクションが記録されます。
レポーティング クエリー ログ	レポーティング クエリ ログには、電子メール ゲートウェイで実行されるレポーティング クエリに関連付けられたアクションが記録されます。
アップデータ ログ	アップデータ ログには、McAfee アンチウイルス定義のアップデートなど、システム サービスのアップデートに関するイベントが記録されます。
トラッキング ログ	トラッキング ログには、トラッキング サービスのプロセスに関連付けられたアクションが記録されます。トラッキング ログは、メール ログのサブセットになっています。
認証ログ	認証ログには、成功したユーザ ログインと失敗したログイン試行が記録されます。

ログ	説明
コンフィギュレーション履歴ログ	コンフィギュレーション履歴ログは、どのような電子メールゲートウェイの変更がいつ行われたかの情報を記録します。ユーザが変更をコミットするたびに、新しいコンフィギュレーション履歴ログが作成されます。
アップグレード ログ	アップグレードのダウンロードとインストールに関するステータス情報。
API ログ	API ログは、電子メールゲートウェイの AsyncOS API に関連するさまざまなイベントを記録します。次に例を示します。 • API が起動したか、または停止したか • API への接続に失敗したか、または閉じたか（応答提供後） • 認証が成功したか、または失敗したか • 要求に含まれるエラー • AsyncOS API とのネットワーク設定変更通信中のエラー
統合イベント ログ	統合イベント ログでは、1 行のログに各メッセージ イベントがまとめられます。このログ タイプを使用すると、分析のためにセキュリティ情報イベント管理（SIEM）ベンダーまたはアプリケーションに送信されるデータ（ログ情報）のバイト数を減らすことができます。このログは、ほとんどの SIEM ベンダーによって幅広く使用されている Common Event Format（CEF）ログ メッセージ形式です。
CSN ログ	CSN ログには、CSN データのアップロードに関する詳細が記録されます。CSN データ（電子メールゲートウェイおよび機能の使用状況の詳細）は、トレースレベルで確認できます。
Advanced Phishing Protection ログ	Advanced Phishing Protection のログには、Cisco Advanced Phishing Protection クラウドサービスに関連する情報が記録されます。ほとんどの情報は [情報（Info）] または [クリティカル（Critical）] レベルです。

ログ	説明
監査ログ	監査ログで認証、許可、アカウンティングのイベント（AAA：Authentication、Authorization、および Accounting）を記録します。 監査ログの詳細の一部を次に示します。 • ユーザ - ログオン • ユーザ - ログオンに失敗しました、パスワードが正しくありません • ユーザー - ログオンに失敗しました、ユーザー名が不明です • ユーザー - ログオンに失敗しました、アカウントの有効期限が切れています • ユーザー - ログオフ • ユーザ - ロックアウト • ユーザ - アクティブ化済み • ユーザ - パスワードの変更 • ユーザ - パスワードのリセット • ユーザ -セキュリティ設定/プロファイルの変更 • ユーザ - 作成済み • ユーザー - 削除または変更 • ユーザ設定 - ユーザが行った設定変更。 • グループ/ロール - 削除/変更済み • グループ/ロール - アクセス許可の変更 • 隔離 - 隔離内のメッセージに対して実行されるアクション。
CSA ログ	CSA ログには、Cisco Secure Awareness クラウドサービスに関連する情報が含まれています。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。
修復ログ	修復ログには、AMP レトロスペクティブ脅威判定および URL レトロスペクティブ判定に基づいた、修復ステータス、実行されたアクション、エラーなどに関連する情報が含まれています。
Email Cloud Scanner ログ	Email Cloud Scanner ログには、URL レトロスペクティブポーリングおよび URL 修復サービスに関する情報が含まれています。

ログ タイプの特徴

次の表に、各ログ タイプの特徴をまとめます。

表 *2:* ログ タイプの比較

						記載内容								
	トランザクション関連	ステートレス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個別のハードバウンス	個別のソフトバウンス	インジェクション SMTP カンバセーション	ヘッダーのロギング	配信 SMTP カンバセーション	設定情報
メール ログ	•		•			•	•	•	•	•		•		
qmail 形式配信 ログ		•			•		•	•	•			•		
配信ログ		•			•		•	•	•			•		
バウンス ログ	•		•						•	•		•		
ステータス ログ		•	•			•								
ドメイン デバッグ ログ	•		•					•	•	•			•	
インジェクション デバッグ ログ	•		•				•				•			

						記載内容								
	トランザクション関連	ステートレス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個別のハードバウンス	個別のソフトバウンス	インジェクション SMTP カンバセーション	ヘッダーのロギング	配信 SMTP カンバセーション	設定情報
システム ログ	•		•			•								
CLI監査ログ	•		•			•								
FTP サーバ ログ	•		•			•								
HTTP ログ	•		•			•								
NTP ログ	•		•			•								
LDAP ログ	•		•											
アンチスパム ログ	•		•			•								
Anti-Spam Archive				•										
グレーメール エンジン ログ	•		•			•								
グレーメール アーカイブ				•										

						記載内容								
	トランザクション関連	ステートレス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個別のハードバウンス	個別のソフトバウンス	インジェクション SMTP カンバセーション	ヘッダーのロギング	配信 SMTP カンバセーション	設定情報
アンチウイルス ログ	•		•			•								
アンチウイルス アーカイブ				•										
AMP エンジン ログ	•		•			•								
AMP アーカイブ				•										
スキャン ログ	•		•			•								•
スパム隔離	•		•			•								
スパム隔離 GUI	•		•			•								
セーフリスト/ブロックリスト ログ	•		•			•								

	記載内容													
	トランザクション関連	ステートレス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個別のハードバウンス	個別のソフトバウンス	インジェクション SMTP カンバセーション	ヘッダーのロギング	配信 SMTP カンバセーション	設定情報
レポーティング ログ	•		•		•									
レポーティング クエリ ログ	•		•		•									
アップデータ ログ			•											
トラッキング ログ	•				•	•	•	•	•	•		•		
認証ログ	•		•											
設定履歴ログ	•		•											•
API ログ	•		•											
統合イベント ログ	•		•				•	•						
CSN ログ	•		•			•								•

	記載内容													
	トランザクション関連	ステートレス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個別のハードバウンス	個別のソフトバウンス	インジェクション SMTP カンバセーション	ヘッダーのロギング	配信 SMTP カンバセーション	設定情報
Advanced Phishing Protection ログ	•		•											
監査ログ			•											

ログ取得方法

ログファイルは、次のいずれかのファイル転送プロトコルに基づいて取得できます。プロトコルは、グラフィカル ユーザ インターフェイスでサブスクリプションを作成または編集するときに設定するか、ログ サブスクリプションのプロセス中に logconfig コマンドを使用して設定します。

（注） 特定のログで「ログ プッシュ」の方法を使用している場合、そのログは CLI を使用してトラブルシューティングまたは検索目的でローカルで使用することはできません。

表 *3:* ログ転送プロトコル

手動でダウンロード	この方法では、[ログサブスクリプション（Log Subscriptions）] ページにあるログ ディレクトリへのリンクをクリックし、アクセスするログ ファイルをクリックすることによって、いつでもログ ファイルにアクセスできます。ブラウザによっては、ブラウザ ウィンドウでのファイルの表示、またはそれをテキスト ファイルとして開いたり保存することができます。この方法はHTTP（S）プロトコルを使用し、デフォルトの取得方法になっています。 （注） この方法を使用すると、この方法をCLIで指定した場合でも、レベル（マシン、グループ、またはクラスタ）には関係なく、クラスタ内のどのコンピュータのログも取得できません。
FTP プッシュ	この方法では、リモート コンピュータ上のFTPサーバに定期的にログ ファイルをプッシュします。サブスクリプションには、リモート コンピュータ上のユーザ名、パスフレーズ、および宛先ディレクトリが必要です。ログ ファイルは、ユーザが設定したロールオーバー スケジュールに基づいて転送されます。
SCP Push	この方法では、リモート コンピュータ上のSCPサーバに定期的にログ ファイルをプッシュします。この方法には、SSH1 またはSSH2 プロトコルを使用するリモート コンピュータ上の SSH SCP サーバが必要です。サブスクリプションには、リモート コンピュータ上のユーザ名、SSH キー、および宛先ディレクトリが必要です。ログ ファイルは、ユーザが設定したロールオーバー スケジュールに基づいて転送されます。

Syslog Push	この方法では、リモート syslog サーバにログ メッセージを送信します。この方法は、RFC 3164 に準拠しています。 （注） syslog プッシュを使用して転送できるのは、テキストベースのログだけです。 Syslog プッシュ方式を選択した後、以下のフィールドに次の情報を入力します。 • ホスト名（Hostname）：リモート Syslog サーバのホスト名を入力します。 • ポート（Port）：リモート Syslog サーバのポート番号を入力します。デフォルトで使用されるポート番号は 514 です。 • プロトコル（Protocol）：ログ送信に必要なプロトコル（UDP または TCP）を選択します。 • 最大メッセージサイズ（Maximum message size）：リモート Syslog サーバに送信するログメッセージの最大サイズ（バイト単位）を入力します。 （注） （TCP プロトコルの場合）最大メッセージサイズの値は 1024 ー 65535 バイトの整数である必要があります。 （注） （UDP プロトコルの場合）最大メッセージサイズの値は 1024 ー 9216 バイトの整数である必要があります。 • ファシリティ（Facility）：必要に応じて、ログに必要なファシリティを選択します。デフォルトでは、ドロップダウンリストで [認証（Auth）] ファシリティオプションが選択されています。
	• TLS：（TCP プロトコルの場合のみ適用）：TLS 接続を介して電子メールゲートウェイからリモート Syslog サーバにログメッセージを送信するには、このオプションを選択します。 • TLS オプションを選択した場合は、電子メールゲートウェイとリモート Syslog サーバ間の TLS 接続を確立するために、電子メールゲートウェイに有効なクライアント証明書を追加します。 • Syslog プッシュ方式では、電子メールゲートウェイの [SSL 設定（SSL Configuration）] ページの [その他の TLS クライアントサービス（Other TLS Client Services）] オプションで選択したものと同じ TLS バージョンを使用します。 • Syslog プッシュ方式の TLS サポートでは、DEFAULT SSL 暗号リストが使用されます。DEFAULT キーワードは OpenSSL DEFAULT 暗号ストリングで、通常は `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2` です。

	• **Syslog ディスクバッファ（TCP プロトコルのみに適用可能）**：Syslog プッシュ ログ サブスクリプションのローカルディスクバッファを設定するには、このチェックボックスをオンにします。これにより、リモート Syslog サーバーが使用できないときに、セキュアな電子メールゲートウェイがログイベントをキャッシュできるようになります。Syslog サーバーが使用可能になると、セキュアな電子メールゲートウェイは、そのログサブスクリプションのバッファ内のすべてのデータを Syslog サーバーに送信し始めます。 （注） • ログデータの損失を避けるため、この手順を開始する前に Syslog サーバーが稼働していることを確認してください。 • Syslog サーバーの予想される最大ダウンタイムに対応できる十分なスペースを確保して、ローカルディスクバッファのサイズを決定します。これにより、ログデータの損失を回避できます。 • ローカル保持用のセカンダリ ログ サブスクリプションがある場合は、セカンダリ サブスクリプションをキャンセルして、プライマリ サブスクリプション用のローカルディスクバッファ用のスペースを確保することをお勧めします。 • セキュアな電子メールゲートウェイは、Syslog サーバーへの接続が失われた後、最初の数秒間のログデータをキャッシュできない場合があります。これは、TCP 上での Syslog の特性によるものです。 • デフォルトの Syslog バッファサイズは 100 MB です。許可される最大ディスクバッファサイズは 1 GB です。サイズは、バイト（1073741824）、メガバイト（1 M）、またはギガバイト（1 G）単位で入力できます。
（統合イベント ログのみ）AWS S3 プッシュ	この方法では、Amazon Web Services（AWS）パブリック クラウドで使用可能な Amazon Simple Storage Service（S3）バケットに定期的にログファイルをプッシュします。Amazon S3 バケットにアクセスするために、サブスクリプションには S3 バケット名、アクセス キー、および秘密キーが必要です。ログ ファイルを転送するためのロールオーバー スケジュールを設定できます。 （注） この取得方法を使用するには、有効な AWS S3 バケットがあることを確認してください。詳細については、https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html にある AWS のユーザ マニュアルを参照してください。

ログ ファイル名とディレクトリ構造

AsyncOS は、ログ サブスクリプション名に基づいて各ログ サブスクリプションのディレクトリを作成します。ディレクトリ内の実際のログ ファイル名は、ユーザが指定したログ ファイル名、ログ ファイルが開始されたときのタイムスタンプ、および単一文字のステータス コードで構成されます。ログのファイル名は、次の形式で作成されます。

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

ステータス コードは、.current または .s（保存済みを示す）になります。保存済みステータスのログ ファイルだけを転送または削除するようにしてください。

ログのロールオーバーおよび転送スケジュール

ログ ファイルはログ サブスクリプションによって作成され、到達したユーザ指定の最初の条件（最大ファイルサイズまたはスケジュール設定されたロールオーバー）に基づいて、ロールオーバー（および、プッシュ ベースの取得オプションが選択されている場合は転送）されます。最大ファイルサイズとスケジュール設定されたロールオーバーの時間間隔の両方を設定するには、CLI で、または GUI の [ログサブスクリプション（Log Subscriptions）] ページで logconfig コマンドを使用します。また、GUI の [今すぐロールオーバー（Rollover Now）] ボタン、または CLI の rollovernow コマンドを使用して、選択したログ サブスクリプションをロールオーバーすることもできます。ロールオーバーのスケジュール設定の詳細については、ログ サブスクリプションのロールオーバー （84 ページ）を参照してください。

手動のダウンロードを使用して取得されたログは、指定した最大数（デフォルトは 10 ファイル）に達するか、またはシステムでログ ファイル用にさらにスペースが必要になるまで保存されます。

デフォルトで有効になるログ

電子メールゲートウェイは、多数のログサブスクリプションがデフォルトでイネーブルになった状態で事前に設定されています（適用したライセンスキーによって、その他のログが設定される場合があります）。デフォルトでは、取得方法は「手動でのダウンロード」です。

エラーだけが含まれるように 1 に設定された error_logs を除き、事前に設定されるすべてのログ サブスクリプションのログ レベルは 3 になります。詳細については、ログ レベル （79 ページ）を参照してください。新規のログ サブスクリプションの作成、または既存のログ サブスクリプションの変更については、ログ サブスクリプション （78 ページ）を参照してください。

ログ タイプ

ログ ファイル内のタイムスタンプ

次のログ ファイルには、ログ自体の開始日と終了日、AsyncOS のバージョン、および GMT オフセット（秒単位でログの始まりにのみ表示）が含まれます。

• アンチウイルス ログ
• LDAP ログ
• システム ログ
• メール ログ

テキスト メール ログの使用

これらのログには、電子メールの受信、電子メールの配信、およびバウンスの詳細が記録されます。これらのログは、特定のメッセージの配信を理解し、システム パフォーマンスを分析するうえで有益な情報源となります。

これらのログに、特別な設定は必要ありません。ただし、添付ファイル名を表示するには、適切なシステムの設定が必要です。添付ファイル名は、常に記録されるわけではありません。詳細については、メッセージ トラッキングの有効化およびメッセージ トラッキングの概要を参照してください。

次の表に、テキスト メール ログに表示される情報を示します。

表 *4:* テキスト メール ログの統計情報

統計	説明
ICID	インジェクション接続 ID。システムに対する個々の SMTP 接続を表す数値 ID であり、この接続で 1 個から数千個のメッセージが送信されます。
DCID	配信接続 ID。別のサーバに対する個々の SMTP 接続を表す数値 ID であり、この接続で 1 個から数千個のメッセージが配信されます。1 つのメッセージ送信で一部または全部の RID が一緒に配信されます。
RCID	RPC Connection ID（RPC 接続 ID）。スパム隔離に対する個々の RPC 接続を表す数値 ID です。この ID を使用して、スパム隔離との間で送受信されるメッセージを追跡します。
MID	Message ID（メッセージ ID）：この ID を使用して、ログを通過するメッセージを追跡します。
RID	Recipient ID（受信者 ID）：各メッセージ受信者に ID が割り当てられます。
新規作成（New）	新規の接続が開始されました。
開始	新規のメッセージが開始されました。

テキスト メール ログの解釈

ログ ファイルを解釈するためのガイドとして、次のサンプルを使用してください。

（注） ログ ファイルの各行には、番号が割り当てられません。ここでは、単にサンプル用として番号が割り当てられています。

表 *5:* テキスト メール ログの詳細

1	`Mon Apr 17 19:56:22 2003 Info:`
	`New SMTP ICID 5 interface Management (10.1.1.1)`
	`address 10.1.1.209 reverse dns host remotehost.com verified yes`

2	`Mon Apr 17 19:57:20 2003 Info:` `Start MID 6 ICID 5`
3	`Mon Apr 17 19:57:20 2003 Info:` `MID 6 ICID 5 From: <sender@remotehost.com>`
4	`Mon Apr 17 19:58:06 2003 Info:` `MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>`
5	`Mon Apr 17 19:59:52 2003 Info:` `MID 6 ready 100 bytes from <sender@remotehost.com>`
6	`Mon Apr 17 19:59:59 2003 Info: ICID 5 close`
7	`Mon Mar 31 20:10:58 2003 Info:` `New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25`
8	`Mon Mar 31 20:10:58 2003 Info:` `Delivery start DCID 8 MID 6 to RID [0]`
9	`Mon Mar 31 20:10:58 2003 Info:` `Message done DCID 8 MID 6 to RID [0]`
10	`Mon Mar 31 20:11:03 2003 Info: DCID 8 close`

次の表を、前述のログ ファイルを読み取るためのガイドとして、使用してください。

表 *6:* テキスト メール ログの例の詳細

行番号	説明
1	システムに対して新しい接続が開始され、インジェクション ID（ICID）「5」が割り当てられました。接続は管理 IP インターフェイスで受信され、10.1.1.209 のリモート ホストで開始されました。
2	クライアントから MAIL FROM コマンドが実行された後、メッセージにメッセージ ID（MID）「6」が割り当てられました。
3	送信者アドレスが識別され、受け入れられます。
4	受信者が識別され、受信者 ID（RID）「0」が割り当てられました。
5	MID 5 が受け入れられ、ディスクに書き込まれ、承認されます。

行番号	説明
6	受信に成功し、受信接続がクローズします。
7	次に、メッセージ配信プロセスが開始されます。192.168.42.42 から 10.5.3.25 への配信に、配信接続 ID（DCID）「8」が割り当てられました。
8	RID「0」へのメッセージ配信が開始されました。
9	RID「0」への MID 6 の配信に成功しました。
10	配信接続がクローズします。

テキスト メール ログ エントリの例

次に、さまざまな状況に基づいたいくつかのサンプル ログ エントリを示します。

メッセージのインジェクションおよび配信

1人の受信者に対するメッセージが電子メールゲートウェイにインジェクトされます。メッセージは正常に配信されます。

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com
(1.2.3.4) address 2.3.4.5 reverse dns host unknown verified no

Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None

Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970

Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>

Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID
'<37gva9$5uvbhe@mail.example.com>'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative

Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery

Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4

Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]

Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close

Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0]
[('X-SBRS', 'None')]

Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery

Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

正常なメッセージ配信

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

失敗したメッセージ配信（ハード バウンス）

2 人の受信者が指定されたメッセージが電子メールゲートウェイにインジェクトされます。配信時に、宛先ホストが 5XX エラーを返します。このエラーは、メッセージをいずれの受信者にも配信できないことを示します。電子メールゲートウェイは送信者に通知し、キューから受信者を削除します。

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address
64.81.204.225

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
error ('550', ['<george@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
error ('550', ['<jane@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

ソフト バウンスの後の正常な配信

メッセージが電子メールゲートウェイにインジェクトされます。最初の配信試行で、メッセージはソフト バウンスして、その後の配信キューに入れられます。2回めの試行でメッセージは正常に配信されます。

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]

Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
error ('466', ['Mailbox temporarily full.'])[]

Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23
2003

Mon Mar 31 20:01:28 2003 Info: DCID 5 close

Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113

Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

scanconfig コマンドのメッセージ スキャン結果

scanconfig コマンドを使用して、メッセージの構成要素を分解できない場合（添付ファイルを削除する場合）のシステムの動作を決定できます。オプションは、Deliver、Bounce、または Drop です。

次に、scanconfig を Deliver に設定したテキスト メール ログの例を示します。

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>

Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>

Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'

Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'

Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>

Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line
seen before first header


Tue Aug 3 16:36:29 2004 Info: ICID 44784 close

Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'

Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus

Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

次に、scanconfig を drop に設定したテキスト メール ログの例を示します。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line
seen before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

添付ファイルを含むメッセージ

この例では、添付ファイル名の識別を有効にするように、条件「Message Body Contains」を含むコンテンツ フィルタが設定されています。

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes

Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0

Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
```

```
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

3 つの添付ファイルの 2 番目が Unicode であることに注意してください。Unicode を表示できない端末では、このような添付ファイルは quoted-printable 形式で表示されます。

DANE のサポートによる正常なメッセージ配信

1 人の受信者に対するメッセージが電子メールゲートウェイに到達します。電子メールゲートウェイは、DNS サーバから安全な DNS MX レコード、DNS A レコード、TLSA レコードをリクエストします。DANE を [必須（Mandatory）] と選択している場合、TLSA レコードが受信者のドメインの X.509 証明書の値に対して検証されます。TLSA レコードの検証に成功した場合、メッセージが受信者に配信されます。

```
Tue Nov 13 12:13:33 2018 Debug: Trying DANE MANDATORY for example.org
Tue Nov 13 12:13:33 2018 Debug: SECURE MX record(mail.example.org) found for example.org
Tue Nov 13 12:13:33 2018 Debug: DNS query: Q('mail.example.org', 'CNAME')
Tue Nov 13 12:13:33 2018 Debug: DNS query: QN('mail.example.org', 'CNAME',
'recursive_nameserver0.parent')
Tue Nov 13 12:13:33 2018 Debug: DNS query: QIP  ('mail.example.org','CNAME','8.8.8.8',60)
Tue Nov 13 12:13:33 2018 Debug: DNS query: Q  ('mail.example.org', 'CNAME', '8.8.8.8')
Tue Nov 13 12:13:34 2018 Debug: DNSSEC Response data([], , 0, 1799)
Tue Nov 13 12:13:34 2018 Debug: Received NODATA for domain mail.example.org type CNAME
Tue Nov 13 12:13:34 2018 Debug: No CNAME record(NoError) found for domain(mail.example.org)
Tue Nov 13 12:13:34 2018 Debug: SECURE A record (4.31.198.44) found for
MX(mail.example.org) in example.org
Tue Nov 13 12:13:34 2018 Info: New SMTP DCID 92 interface 10.10.1.191 address 4.31.198.44
 port 25
Tue Nov 13 12:13:34 2018 Info: ICID 13 lost
Tue Nov 13 12:13:34 2018 Info: ICID 13 close
Tue Nov 13 12:13:34 2018 Debug: DNS query: Q('_25._tcp.mail.example.org', 'TLSA')
Tue Nov 13 12:13:34 2018 Debug: DNS query: QN('_25._tcp.mail.example.org', 'TLSA',
'recursive_nameserver0.parent')
Tue Nov 13 12:13:34 2018 Debug: DNS query: QIP
('_25._tcp.mail.example.org','TLSA','8.8.8.8',60)
Tue Nov 13 12:13:34 2018 Debug: DNS query: Q  ('_25._tcp.mail.example.org', 'TLSA',
'8.8.8.8')
Tue Nov 13 12:13:35 2018 Debug: DNSSEC Response data(['0301010c72ac70b745ac19998811b13
1d662c9ac69dbdbe7cb23e5b514b56664c5d3d6'], secure, 0, 1799)
Tue Nov 13 12:13:35 2018 Debug: DNS encache (_25._tcp.mail.example.org, TLSA,
[(2550119024205761L, 0,
'SECURE', '0301010c72ac70b745ac19998811b131d662c9ac69dbdbe7cb23e5b514b56664c5d3d6')])
Tue Nov 13 12:13:35 2018 Debug: SECURE TLSA Record found for MX(mail.example.org) in
example.org
Tue Nov 13 12:13:36 2018 Info: DCID 92 Certificate verification successful
Tue Nov 13 12:13:36 2018 Info: DCID 92 TLS success protocol TLSv1.2 cipher
Tue Nov 13 12:13:36 2018 Info: DCID 92 TLS success protocol TLSv1.2 cipher
ECDHE-RSA-AES256-GCM-SHA384 for example.org
Tue Nov 13 12:13:36 2018 Info: Delivery start DCID 92 MID 23 to RID [0]
```

証明書の検証失敗によるメッセージ配信の失敗

1 人の受信者に対するメッセージが電子メールゲートウェイに到達します。電子メールゲートウェイは、DNS サーバから安全な DNS MX レコード、DNS A レコード、TLSA レコードをリクエストします。DANE を [必須（Mandatory）] と選択している場合、TLSA レコードが受信者のドメインの X.509 証明書の値に対して検証されます。証明書の検証に失敗すると、メッセージが後ほど配信されます。安全な TLSA レコードが見つからない場合、メッセージはバウンスされます。

```
Wed Nov 14 05:52:08 2018 Debug: DNS query: QN('server1.example.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 05:52:08 2018 Debug: DNS query: QIP
('server1.example.net','CNAME','10.10.2.184',60)
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q  ('server1.example.net', 'CNAME',
'10.10.2.184')
Wed Nov 14 05:52:08 2018 Debug: DNSSEC Response data([], , 0, 284)
Wed Nov 14 05:52:08 2018 Debug: Received NODATA for domain server1.example.net type CNAME
Wed Nov 14 05:52:08 2018 Debug: No CNAME record(NoError) found for
domain(server1.example.net)
Wed Nov 14 05:52:08 2018 Debug: Secure CNAME(server1.example.net) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Debug: SECURE A record (10.10.1.198) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Info: New SMTP DCID 102 interface 10.10.1.191 address 10.10.1.198
 port 25
Wed Nov 14 05:52:08 2018 Debug: Fetching TLSA records with CNAME(server1.example.net)
for
MX(someone.cs2.example.net) in example.net
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q('_25._tcp.server1.example.net', 'TLSA')
Wed Nov 14 05:52:08 2018 Debug: SECURE TLSA Record found for MX(server1.example.net) in
 example.net
Wed Nov 14 05:52:08 2018 Debug: DCID 102 All TLSA records failed for certificate not
trusted
Wed Nov 14 05:52:08 2018 Debug: Fetching TLSA records with initial
name(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q('_25._tcp.someone.cs2.example.net', 'TLSA')
Wed Nov 14 05:52:08 2018 Debug: SECURE TLSA Record found for MX(someone.cs2.example.net)
 in example.net
Wed Nov 14 05:52:08 2018 Info: DCID 102 Certificate verification successful
Wed Nov 14 05:52:08 2018 Info: DCID 102 TLS success protocol TLSv1.2 cipher
DHE-RSA-AES128-SHA256
for example.net
Wed Nov 14 05:52:08 2018 Info: Delivery start DCID 102 MID 26 to RID [0]
Wed Nov 14 05:52:08 2018 Info: Message done DCID 102 MID 26 to RID [0]
Wed Nov 14 05:52:08 2018 Info: MID 26 RID [0] Response 'ok:  Message 31009 accepted'
Wed Nov 14 05:52:08 2018 Info: Message finished MID 26 done

Wed Nov 14 06:36:22 2018 Debug: Trying DANE MANDATORY for example.net
Wed Nov 14 06:36:22 2018 Debug: SECURE MX record(someone.cs2.example.net) found for
example.net
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q('someone.cs2.example.net', 'CNAME')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QN('someone.cs2.example.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QIP
('someone.cs2.example.net','CNAME','10.10.2.184',60)
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q  ('someone.cs2.example.net', 'CNAME',
'10.10.2.184')
Wed Nov 14 06:36:22 2018 Debug: DNSSEC Response data(['mail.example2.net.'], secure, 0,
 3525)
```

```
Wed Nov 14 06:36:22 2018 Debug: DNS encache (someone.cs2.example.net, CNAME,
[(2692348132363369L, 0,
'SECURE', 'mail.example2.net')])
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q('mail.example2.net', 'CNAME')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QN('mail.example2.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QIP
('mail.example2.net','CNAME','10.10.2.184',60)
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q  ('mail.example2.net', 'CNAME', '10.10.2.184')
Wed Nov 14 06:36:22 2018 Debug: DNSSEC Response data([], , 0, 225)
Wed Nov 14 06:36:22 2018 Debug: Received NODATA for domain mail.example2.net type CNAME
Wed Nov 14 06:36:22 2018 Debug: No CNAME record(NoError) found for
domain(mail.example2.net)
Wed Nov 14 06:36:22 2018 Debug: Secure CNAME(mail.example2.net) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 06:36:22 2018 Debug: INSECURE A record (10.10.1.197) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 06:36:22 2018 Debug: Fetching TLSA records with initial
name(someone.cs2.example.net) in example.net
Wed Nov 14 06:36:22 2018 Info: New SMTP DCID 104 interface 10.10.1.191 address 10.10.1.197
 port 25
Wed Nov 14 06:36:36 2018 Debug: DNS query: Q('_25._tcp.someone.cs2.example.net', 'TLSA')
Wed Nov 14 06:36:36 2018 Debug: SECURE TLSA Record found for MX(someone.cs2.example.net)
 in example.net
Wed Nov 14 06:36:36 2018 Debug: DCID 104 All TLSA records failed for certificate not
trusted
Wed Nov 14 06:36:36 2018 Info: MID 27 DCID 104 DANE failed for the domain example.net:
DANE Certificate verification failed
Wed Nov 14 06:36:36 2018 Info: Failed for all MX hosts in example.net
```

無効な TLSA レコードによるメッセージ配信の失敗

1 人の受信者に対するメッセージが電子メールゲートウェイに到達します。電子メールゲートウェイは、DNS サーバから安全な DNS MX レコード、DNS A レコード、TLSA レコードをリクエストします。DANE を [必須（Mandatory）] と選択している場合、TLSA レコードが受信者のドメインの X.509 証明書の値に対して検証されます。無効な TLSA レコードが見つかると、後ほどメッセージの配信が試行されるか、メッセージがバウンスされます。

```
Tue Aug 7 05:15:18 2018 Debug: Trying DANE MANDATORY for example-dane.net
Tue Aug 7 05:15:18 2018 Debug: SECURE MX record (someone.example-dane.net) found for
test-tlsabogus.net
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('someone.example-dane.net', 'CNAME')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QN ('someone.example-dane.net', 'CNAME',
'recursive_nameserver0.parent')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QIP
('someone.example-dane.net','CNAME','10.10.2.183', 60)
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('someone.example-dane.net', 'CNAME',
'10.10.2.183')
Tue Aug 7 05:15:18 2018 Debug: DNSSEC Response data ([], , 0, 300)
Tue Aug 7 05:15:18 2018 Debug: SECURE A record (10.10.1.198) found for MX
(someone.example-dane.net)
in example-dane.net
Tue Aug 7 05:15:18 2018 Info: ICID 32 close
Tue Aug 7 05:15:18 2018 Info: New SMTP DCID 61 interface 10.10.1.194 address 10.10.1.198
 port 25
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('_25._tcp.someone.example-dane.net', 'TLSA')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QN ('_25._tcp.someone.example-dane.net', 'TLSA',

'recursive_nameserver0.parent')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QIP
```

```
('_25._tcp.someone.example-dane.net','TLSA','10.10.2.183', 60)
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('_25._tcp.someone.example-dane.net', 'TLSA',
 '10.10.2.183')
Tue Aug 7 05:15:18 2018 Debug: DNSSEC Response data
(['03010160b3f16867357cdfef37bb6acd687af54f
225e3bfa945e1d37bfd37bd4eb6020'], bogus, 0, 60)
Tue Aug 7 05:15:18 2018 Debug: DNS encache (_25._tcp.someone.example-dane.net, TLSA,
[(11065394975822091L,
 0, 'BOGUS', '03010160b3f16867357cdfef37bb6acd687af54f225e3bfa945e1d37bfd37bd4eb6020')])
Tue Aug 7 05:15:18 2018 Debug: BOGUS TLSA Record is found for MX (someone.example-dane.net)

in example-dane.net
Tue Aug 7 05:15:18 2018 Debug: Trying next MX record in example-dane.net
Tue Aug 7 05:15:18 2018 Info: MID 44 DCID 61 DANE failed: TLSA record BOGUS
Tue Aug 7 05:15:18 2018 Debug: Failed for all MX hosts in example-dane.net
```

TLSA レコードが見つからない場合に状況対応型 TLS にロールバックする

1 人の受信者に対するメッセージが電子メールゲートウェイに到達します。電子メールゲートウェイは、DNS サーバから安全な DNS MX レコード、DNS A レコード、TLSA レコードをリクエストします。DANE を [状況対応型（Opportunistic）] と選択している場合、TLSA レコードが受信者のドメインの X.509 証明書の値に対して検証されます。受信者のドメインの TLSA レコードが見つからない場合、SMTP カンバセーションの暗号化に状況対応型の TLS が使用されます。

```
Wed Sep 12 06:51:32 2018 Debug: Trying DANE OPPORTUNISTIC for example-dane.com
Wed Sep 12 06:51:32 2018 Debug: SECURE MX record (mx.example-dane.com) found for
digitalhellion.com
Wed Sep 12 06:51:32 2018 Debug: DNS query: Q ('mx.example-dane.com', 'CNAME')
Wed Sep 12 06:51:32 2018 Debug: DNS query: QN ('mx.example-dane.com', 'CNAME',
'recursive_nameserver0.parent')
Wed Sep 12 06:51:32 2018 Debug: DNS query: QIP ('mx.example-dane.com',
'CNAME','8.8.8.8',60)
Wed Sep 12 06:51:32 2018 Debug: DNS query: Q ('mx.example-dane.com', 'CNAME', '8.8.8.8')
Wed Sep 12 06:51:32 2018 Debug: DNSSEC Response data ([], , 0, 1799)
Wed Sep 12 06:51:32 2018 Debug: Received NODATA for domain mx.example-dane.com type CNAME
Wed Sep 12 06:51:32 2018 Debug: No CNAME record (NoError) found for domain
(mx.example-dane.com)
Wed Sep 12 06:51:32 2018 Debug: SECURE A record (162.213.199.115) found for MX
(mx.example-dane.com)
in example-dane.com
Wed Sep 12 06:51:32 2018 Info: ICID 1 lost
Wed Sep 12 06:51:32 2018 Info: ICID 1 close
Wed Sep 12 06:51:33 2018 Info: New SMTP DCID 2 interface 10.10.1.173 address
162.213.199.115 port 25
Wed Sep 12 06:51:33 2018 Debug: DNS query: Q ('_25._tcp.mx.example-dane.com', 'TLSA')
Wed Sep 12 06:51:33 2018 Debug: DNS query: QN ('_25._tcp.mx.example-dane.com', 'TLSA',
'recursive_nameserver0.parent')
Wed Sep 12 06:51:33 2018 Debug: DNS query: QIP
('_25._tcp.mx.example-dane.com','TLSA','8.8.8.8', 60)
Wed Sep 12 06:51:33 2018 Debug: DNS query: Q ('_25._tcp.mx.example-dane.com', 'TLSA',
'8.8.8.8')
Wed Sep 12 06:51:34 2018 Debug: DNSSEC Response data ([], , 3, 1798)
Wed Sep 12 06:51:34 2018 Debug: Received NXDomain for domain _25._tcp.mx.example-dane.com'
 type TLSA
Wed Sep 12 06:51:34 2018 Debug: No TLSA record (NXDomain) found for MX
(mx.example-dane.com)
Wed Sep 12 06:51:34 2018 Debug: Falling back to conventional TLS for MX
(mx.example-dane.com)
in example-dane.com
Wed Sep 12 06:51:34 2018 Info: MID 1 DCID 2 DANE failed for the domain example-dane.com:
 No TLSA Record
```

```
Wed Sep 12 06:51:34 2018 Info: DCID 2 TLS success protocol TLSv1.2 cipher
ECDHE-RSA-AES256-GCM-SHA384
Wed Sep 12 06:51:35 2018 Info: Delivery start DCID 2 MID 1 to RID [0]
```

送信者の発信国に基づいて受信したメッセージ

この例では、ログには、受信されたメッセージが特定の送信者グループの国に基づいて表示されています。

```
Thu Apr  6 06:50:18 2017 Info: ICID 73 ACCEPT SG ALLOWED_LIST match country[us] SBRS
-10.0 country United States
```

メッセージ添付ファイル内の最大 URL 数が URL スキャン制限を超えている

この例では、ログはURL スキャンの制限を超えた、メッセージの添付ファイル内の URL の数を示しています

```
Wed Nov 8 13:35:48 2017 Info:  MID $mid not completely scanned for URL Filtering. Error:
 $error
```

メッセージ本文内の最大 URL 数が URL スキャン制限を超えている

この例では、ログはURL スキャンの制限を超えた、メッセージの本文内の URL の数を示しています。

```
Wed Nov 8 13:37:42 2017 Info: MID 976 not completely scanned for URL Filtering.
Error: The number of URLs in the message body exceeded the URL scan limit.
```

Cisco プロキシ サーバにリダイレクトされる悪意のある短縮 URL

次の例では、ある短縮 URl が、URL レピュテーション スコアが -3 であるため悪意があるものとしてマークされ、Cisco Security Proxy サーバにリダイレクトされたことがログに表示されています。

```
Tue Nov 7 10:42:41 2017 Info: MID 9 having URL: http://ow.ly/Sb6O30fJvVn has been expanded
 to http://bit.ly/2frAl1x
Tue Nov 7 10:42:42 2017 Info: MID 9 having URL: http://bit.ly/2frAl1x has been expanded
 to http://thebest01.wayisbetter.cn/?cMFN
Tue Nov 7 10:42:42 2017 Info: MID 9 URL http://thebest01.wayisbetter.cn/?cMFN has
reputation -3.854 matched Action: URL redirected to Cisco Security proxy
Tue Nov 7 10:42:42 2017 Info: MID 9 rewritten to MID 10 by
url-reputation-proxy-redirect-action filter 'aa'
```

メッセージ内の短縮 URL を展開できない

この例では、ログは、メッセージに含まれる短縮URL を実際の URL に展開できなかったことを示します。

```
Mon Oct 30 10:58:59 2017 Info: MID 36 having URL: http://ow.ly/P0Kw30fVst3 has been
expanded to http://bit.ly/2ymYWPR
Mon Oct 30 10:59:00 2017 Info: MID 36 having URL: http://bit.ly/2ymYWPR has been expanded
 to http://ow.ly/cTS730fVssH
Mon Oct 30 10:59:01 2017 Info: MID 36 having URL: http://ow.ly/cTS730fVssH has been
expanded to http://bit.ly/2xK8PD9
Mon Oct 30 10:59:01 2017 Info: MID 36 having URL: http://bit.ly/2xK8PD9 has been expanded
 to http://ow.ly/lWOi30fVssl
Mon Oct 30 10:59:02 2017 Info: MID 36 having URL: http://ow.ly/lWOi30fVssl has been
```

```
expanded to http://bit.ly/2ggHv9e
Mon Oct 30 10:59:03 2017 Info: MID 36 having URL: http://bit.ly/2ggHv9e has been expanded
 to http://ow.ly/4fSO30fVsqx
Mon Oct 30 10:59:04 2017 Info: MID 36 having URL: http://ow.ly/4fSO30fVsqx has been
expanded to http://bit.ly/2hKEFcW
Mon Oct 30 10:59:05 2017 Info: MID 36 having URL: http://bit.ly/2hKEFcW has been expanded
 to http://ow.ly/NyH830fVsq6
Mon Oct 30 10:59:06 2017 Info: MID 36 having URL: http://ow.ly/NyH830fVsq6 has been
expanded to http://bit.ly/2ysnsNi
Mon Oct 30 10:59:06 2017 Info: MID 36 having URL: http://bit.ly/2ysnsNi has been expanded
 to http://ow.ly/JhUN30fVsnL
Mon Oct 30 10:59:07 2017 Info: MID 36 having URL: http://ow.ly/JhUN30fVsnL has been
expanded to http://bit.ly/2hKQmAe
Mon Oct 30 10:59:07 2017 Info: MID 36 URL http://bit.ly/2hKQmAe is marked malicious due
 to : URL depth exceeded
Mon Oct 30 11:04:48 2017 Warning: MID 40 Failed to expand URL http://mail1.example.com/abcd
 Reason: Error while trying to retrieve expanded URL
Mon Oct 30 11:04:48 2017 Info: MID 40 not completely scanned for URL Filtering. Error:
Message has a shortened URL that could not be expanded
```

メッセージ添付ファイルでの悪意のある URL のログ エントリ

この例では、レピュテーション スコアが -9.5 で、悪意のあるメッセージの添付ファイルに含まれる URL がログに表示されています。

```
Mon Nov 6 06:50:18 2017 Info: MID 935 Attachment file_1.txt URL http://jrsjvysq.net has
 reputation -9.5 matched
Condition: URL Reputation Rule
```

抽出エラーが原因でスキャン不可とマークされたメッセージ

この例では、ログは添付ファイル抽出エラーが原因でコンテンツ スキャナによってスキャンされないメッセージを示しています。

```
Tue Oct 24 08:28:58 2017 Info: Start MID 811 ICID 10
Tue Oct 24 08:28:58 2017 Info: MID 811 ICID 10 From: <sender@example.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 ICID 10 RID 0 To: <recipient@example.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 Message-ID '<example@cisco.com>'
Tue Oct 24 08:28:58 2017 Info: MID 811 Subject 'Test mail'
Tue Oct 24 08:28:58 2017 Info: MID 811 ready 5242827 bytes from <user2@sender.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Tue Oct 24 08:28:59 2017 Info: MID 811 attachment 'gzip.tar.gz'
Tue Oct 24 08:28:59 2017 Info: MID 811 was marked as unscannable due to extraction
failures. Reason: Error in extraction process - Decoding Errors.
Tue Oct 24 08:28:59 2017 Info: ICID 10 close
Tue Oct 24 08:28:59 2017 Info: MID 811 quarantined to "Policy" (Unscannable: due to
Extraction Failure)
Tue Oct 24 08:28:59 2017 Info: Message finished MID 811 done
```

RFC 違反が原因でスキャン不可とマークされたメッセージ

この例では、ログはRFC違反が原因でコンテンツ スキャナによってスキャンされないメッセージを示しています。

```
Tue Oct 24 08:23:26 2017 Info: Start MID 807 ICID 6
Tue Oct 24 08:23:26 2017 Info: MID 807 ICID 6 From: <sender@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 ICID 6 RID 0 To: <recipient@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 Subject ‘Test Mail'
Tue Oct 24 08:23:26 2017 Info: MID 807 ready 427 bytes from <sender@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 matched all recipients for per-recipient policy
```

```
DEFAULT in the inbound table
Tue Oct 24 08:23:26 2017 Info: MID 807 was marked as unscannable due to an RFC violation.
 Reason: A Unix-From header was found in the middle of a header block.
Tue Oct 24 08:23:26 2017 Info: MID 807 queued for delivery
Tue Oct 24 08:23:26 2017 Info: ICID 6 close
```

生成またはリライトされたメッセージに対するログ エントリ

リライト/リダイレクトアクションなどの一部の機能（alt-rcpt-toフィルタ、アンチスパムRCPTリライト、bcc()アクション、アンチウイルス リダイレクションなど）によって、新しいメッセージが作成されます。ログに目を通して結果を確認し、必要に応じてMIDや、場合によってはDCIDを追加します。次のようなエントリが可能です。

```
Tue Jun  1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
```

または

```
Tue Jan 6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam

Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter
'testfilt'
```

「rewritten」エントリについては、ログ内で新しいMIDの使用を示す行の後に表示される点に注目してください。

スパム隔離エリアに送信されたメッセージ

メッセージを隔離領域に送信すると、メール ログでは、RPC 接続を識別する RPC 接続 ID（RCID）を使用して、隔離領域との間の移動が追跡されます。次のメール ログでは、スパムとしてタグが付けられたメッセージがスパム隔離に送信されています。

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make
it a reality'

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient
policy DEFAULT in the inbound table

Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect

Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local
IronPort Spam Quarantine


Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877

Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877
```

```
Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

外部脅威フィードのメール ログの例

メール ログには、受信メッセージで検出された脅威と、そのようなメッセージに対して実行されたアクションに関する情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

```
Thu Jun 7 20:48:10 2018 Info: MID 91 Threat feeds source 'S1' detected malicious URL:
'http://digimobil.mobi/' in attachment(s): malurl.txt. Action: Attachment stripped
```

SDR フィルタリングのログ エントリの例

SDR フィルタリング情報はメール ログに書き込まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

- 送信者ドメイン レピュテーションのリクエストのタイムアウト
- 送信者ドメインのレピュテーションの一般的なエラー

送信者ドメイン レピュテーションの認証の失敗

この例のログは、SDR サービスに接続する際の認証失敗のために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 08:57:18 2018 Info: New SMTP ICID 3 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 08:57:18 2018 Info: ICID 3 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 08:57:18 2018 Info: Start MID 3 ICID 3
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 From: <sender1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 RID 0 To: <recipient1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 08:57:18 2018 Info: MID 3 Subject 'Message 001'
Mon Jul 2 08:57:19 2018 Info: MID 3 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Authentication failure.
```

ソリューション

CLI で `sdradvancedconfig` コマンドを使用すると、電子メールゲートウェイを SDR サービスに接続する際に必要なパラメータを設定できます。

送信者ドメイン レピュテーションのリクエストのタイムアウト

この例のログは、SDR サービスと通信する際のリクエスト タイムアウトのために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com>
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
```

```
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Message 001'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Request timed out.
```

ソリューション

SDRリクエストがタイムアウトになると、メッセージがスキャン不可としてマークされ、設定したアクションがメッセージに適用されます。

送信者ドメイン レピュテーションの無効なホスト

この例のログは、電子メールゲートウェイで無効なSDRサービス ホストが設定されたためにSDRに基づいてフィルタ処理されなかったメッセージが表示しています。

```
Mon Jul 2 09:04:08 2018 Info: ICID 7 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:04:08 2018 Info: Start MID 7 ICID 7
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 From: <sender1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:04:08 2018 Info: MID 7 Subject 'Message 001'
Mon Jul 2 09:04:08 2018 Info: MID 7 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Invalid host configured.
```

ソリューション

CLIで`sdradvancedconfig`コマンドを使用すると、電子メールゲートウェイをSDRサービスに接続する際に必要なパラメータを設定できます。

送信者ドメインのレピュテーションの一般的なエラー

この例のログは、不明なエラーのためにSDRに基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Test mail'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Unknown error.
```

ソリューション

不明なエラーが発生すると、メッセージがスキャン不可としてマークされ、設定したアクションがメッセージに適用されます。

有効期限が切れた Cisco Advanced Phishing Protection クラウドサービス

この例では、Cisco Advanced Phishing Protectionクラウドサービスの有効期限が切れていることが、ログ に示されています。

```
Wed May 6 11:47:45 2020 Critical: The Cisco Advanced
Phishing Protection Cloud Service has expired and is disabled. Contact
your Cisco Account Manager to renew the service and enable it.
```

解決策：シスコアカウントマネージャに連絡して、サービスを更新および有効にする必要があります。

Cisco Advanced Phishing Protection クラウドサービスの有効期限に関するリマインダ

この例では、Cisco Advanced Phishing Protection クラウドサービスが特定の日付に期限切れになることが、ログによって示されています。

```
 Fri May 8 04:50:26 2020 Info: Cisco Advanced
Phishing Protection Cloud Service expires on
2020-05-10 07:00:00. You need to contact your Cisco Account
Manager to renew the service
```

解決策：シスコアカウントマネージャに連絡してサービスを更新する必要があります。

API アクセス UID と API アクセス秘密鍵がない

この例では、API アクセス UID と API アクセス秘密鍵がないため、電子メールゲートウェイで Cisco Advanced Phishing Protection クラウドサービスの有効期限をポーリングできなかったことが、ログに示されています。

```
 Wed May 6 17:52:52 2020 Critical: Failed to poll
for the Cisco Advanced Phishing Protection Cloud Service
expiry date. You need to add the API Access UID and API Access
secret key.
```

解決策：API アクセス UID と API アクセス秘密鍵を追加する必要があります。

無効な API アカウント UID または API アクセス秘密鍵

この例では、無効な API アクセス UID や API アクセス秘密鍵が原因で、電子メールゲートウェイが Cisco Advanced Phishing Protection クラウドサービスの有効期限をポーリングできなかったことが、ログで示されています。

```
Wed May 6 17:52:52 2020 Critical: Failed to poll
for the Cisco Advanced Phishing Protection Cloud Service
expiry date because the API Access Key is invalid. You need
to re-configure the API Access UID and secret key
```

解決策：API アクセス UID と秘密鍵を再設定する必要があります。

配信ログの使用

配信ログには、AsyncOS の電子メール配信動作に関する重要な情報が記録されます。ログメッセージは「ステートレス」です。つまり、関連するすべての情報が各ログメッセージに記録されるので、ユーザは、現在の配信試行に関する情報について前のログメッセージを参照する必要がありません。

配信ログには、受信者ごとの電子メール配信動作に関連するすべての情報が記録されます。すべての情報は、論理的にレイアウトされ、シスコが提供するユーティリティを使用して変換し

た後は、人による読み取りが可能になります。変換ツールは、次の場所にあります。
https://supportforums.cisco.com/document/33721/cisco-ironport-systems-contributed-tools

配信ログは、リソースの効率性を保つためにバイナリ形式で記録されて転送されます。次の表に、配信ログに記録される情報を示します。

表 7：配信ログの統計情報

統計	説明
配信ステータス（Delivery status）	success（メッセージは正常に配信されました）またはbounce（メッセージはハード バウンスされました）
Del_time	配信時間
Inj_time	インジェクション時間。del_time - inj_time = time 受信者メッセージがキューに留まっていた時間
Bytes	メッセージ サイズ
Mid	メッセージ ID
Ip	受信者ホストIP。受信者メッセージを受信またはバウンスしたホストのIP アドレス
From	Envelope From（Envelope Sender または MAIL FROM としても知られます）
Source_ip	送信元ホスト IP。着信メッセージのホストの IP アドレス
コード	受信者ホストからの SMTP 応答コード
返信（Reply）	受信者ホストからの SMTP 応答メッセージ
Rcpt Rid	受信者 ID。受信者 ID は <0> から始まります。複数の受信者が指定されたメッセージには、複数の受信者 ID が付きます。
受信者（To）	エンベロープ受信者
Attempts	配信試行回数

配信ステータスが bounce であった場合は、次の追加情報が配信ログに表示されます。

表 8：配信ログのバウンス情報

統計	説明
理由	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
コード	受信者ホストからの SMTP 応答コード
エラー（Error）	受信者ホストからの SMTP 応答メッセージ

ログヘッダーを設定している場合（メッセージ ヘッダーのロギング （82 ページ）を参照）、ヘッダー情報は配信情報の後に表示されます。

表 *9:* 配信ログのヘッダー情報

統計	説明
顧客データ（Customer_data）	ログに記録されるヘッダーの始まりを示す XML タグ
ヘッダー名（Header Name）	ヘッダーの名前
値	ログに記録されるヘッダーの内容

配信ログ エントリの例

ここでは、さまざまな配信ログ エントリの例を示します。

正常なメッセージ配信

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

配信ステータス バウンス

```
<bounce del_time="Sun Jan 05 08:28:33.073 2003" inj_time="Mon Jan 05 08:28:32.929 2003"

bytes="4074" mid="94157762" ip="0.0.0.0" from="campaign1@yourdomain.com"

source_ip="192.168.102.1 "reason="5.1.0 - Unknown address error" code="550"

error="["Requested action not taken: mailbox unavailable"]">


<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

</bounce>
```

ログヘッダー付きの配信ログ エントリ

```
<success del_time="Tue Jan 28 15:56:13.123 2003" inj_time="Tue Jan 28 15:55:17.696 2003"
bytes="139" mid="202" ip="10.1.1.13" from="campaign1@yourdomain.com"
source_ip="192.168.102.1" code="250" reply="sent">


<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

<customer_data>
```

```
<header name="xname" value="sh"/>

</customer_data>

</success>
```

バウンス ログの使用

バウンス ログには、バウンスされた各受信者に関するすべての情報が記録されます。次の表に、バウンス ログに記録される情報を示します。

表 *10* : バウンス ログの統計情報

統計	説明
タイムスタンプ	バウンス イベントの時刻
ログ レベル（Log level）	このバウンス ログの詳細レベル
バウンス タイプ（Bounce type）	Bounced または Delayed（ハードバウンスまたはソフトバウンスなど）
MID/RID	メッセージ ID および受信者 ID
From	エンベロープ送信者
受信者（To）	エンベロープ受信者
理由	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
応答	受信者ホストからの SMTP 応答コードおよびメッセージ

また、ログに記録するメッセージサイズを指定しているか、**ログヘッダー**を設定している（メッセージ ヘッダーのロギング （82 ページ）を参照）場合、メッセージおよびヘッダー情報はバウンス情報の後に表示されます。

表 *11* : バウンス ログのヘッダー情報

ヘッダー	ヘッダー名およびヘッダーのコンテンツ。
メッセージ（Message）	ログに記録されるメッセージのコンテンツ。

バウンス ログ エントリの例

ソフトバウンスされた受信者（バウンス タイプ = Delayed）

```
Thu Dec 26 18:37:00 2003 Info: Delayed: 44451135:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>
```

```
Reason: "4.1.0 - Unknown address error" Response: "('451',
['<user@sampledomain.com> Automated block triggered by suspicious
activity from your IP address (10.1.1.1). Have your system administrator
send e-mail to postmaster@sampledomain.com if you believe this block is
in error'])"
```

ハードバウンスされた受信者（バウンス タイプ = Bounced）

```
Thu Dec 26 18:36:59 2003 Info: Bounced: 45346670:0 From:<campaign1@yourdomain.com>
To:<user2@sampledomain.com>


Reason: "5.1.0 - Unknown address error" Response: "('550', ['There is no such active
account.'])"
```

メッセージ本文およびログヘッダー付きのバウンス ログ

```
Wed Jan 29 00:06:30 2003 Info: Bounced: 203:0 From:<campaign1@yourdomain.com>
To:<user@sampledomain.com>


Reason:"5.1.2 - Bad destination host" Response: "('000', [])" Headers: ['xname:
userID2333']' Message: Message-Id:



<1u5jak$6b@yourdomain.com>\015\012xname: userID2333\015\012subject:
Greetings.\015\012\015\012Hi Tom:'
```

（注） テキスト文字列 \015\012 は、改行を表します（CRLF など）。

ステータス ログの使用

ステータス ログには、status、status detail、および dnsstatus などの CLI ステータス コマンドで検出されたシステム統計情報が記録されます。記録期間は、logconfig の setup サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。

ステータス ログの読み取り

次の表に、ステータス ログ ラベルと、一致するシステム統計情報を示します。

表 *12*：ステータス ログの統計情報

統計	説明
CPULd	CPU 使用率
DskIO	Disk I/O 使用率

統計	説明
RAMUtil	RAM 使用率
QKUsd	使用されているキュー（キロバイト単位）
QKFre	空いているキュー（キロバイト単位）
CrtMID	メッセージ ID（MID）
CrtICID	インジェクション接続 ID（ICID）
CRTDCID	配信接続 ID（DCID）
InjBytes	インジェクトされたメッセージの合計サイズ（バイト単位）
InjMsg	インジェクトされたメッセージ
InjRcp	インジェクトされた受信者
GenBncRcp	生成されたバウンス受信者
RejRcp	拒否された受信者
DrpMsg	ドロップされたメッセージ
SftBncEvnt	ソフト バウンスされたイベント
CmpRcp	完了した受信者
HrdBncRcp	ハード バウンスされた受信者
DnsHrdBnc	DNS ハード バウンス
5XXHrdBnc	5XX ハード バウンス
FltrHrdBnc	フィルタ ハード バウンス
ExpHrdBnc	期限切れハード バウンス
OtrHrdBnc	その他のハード バウンス
DlvRcp	配信された受信者
DelRcp	削除された受信者
GlbUnsbHt	グローバル配信停止リストとの一致数
ActvRcp	アクティブ受信者
UnatmptRcp	未試行受信者
AtmptRcp	試行受信者

統計	説明
CrtCncIn	現在の着信接続
CrtCncOut	現在の発信接続
DnsReq	DNS 要求
NetReq	ネットワーク要求
CchHit	キャッシュ ヒット
CchMis	キャッシュ ミス
CchEct	キャッシュ例外
CchExp	キャッシュ期限切れ
CPUTTm	アプリケーションが使用した合計 CPU 時間
CPUETm	アプリケーションが開始されてからの経過時間
MaxIO	メール プロセスに対する 1 秒あたりの最大ディスク I/O 動作
RamUsd	割り当て済みのメモリ（バイト単位）
SwIn	スワップインされたメモリ。
SwOut	スワップアウトされたメモリ。
SwPgIn	ページインされたメモリ。
SwPgOut	ページアウトされたメモリ。
MMLen	システム内の合計メッセージ数
DstInMem	メモリ内の宛先オブジェクト数
ResCon	リソース保持の tarpit 値（大量のシステム負荷により、着信メールの受け入れがこの秒数だけ遅延します）
WorkQ	ワーク キューにある現在のメッセージ数
QuarMsgs	ポリシー、ウイルス、および Outbreak 隔離にある個々のメッセージ数（複数の隔離エリアに存在するメッセージは一度だけカウントされます）
QuarQKUsd	ポリシー、ウイルス、および Outbreak 隔離メッセージによって使用されるキロバイト
LogUsd	使用されるログ パーティションの割合

統計	説明
SophLd	Sophos アンチウイルススキャンで使用される CPU の割合
McafLd	McAfee アンチウイルス スキャンで使用される CPU の割合
CASELd	CASE スキャンで使用される CPU の割合
TotalLd	CPU の合計消費量
LogAvail	ログ ファイルに使用できるディスク スペース
EuQ	スパム隔離内の推定メッセージ数
EuqRls	スパム隔離解放キュー内の推定メッセージ数
RptLD	レポートの処理中の CPU 負荷
QtnLd	隔離処理中の CPU 負荷
EncrQ	暗号化のキュー内のメッセージ

ステータス ログの例

```
Fri Feb 28 12:11:48 2020 Info: Status: CPULd 45 DskIO 22 RAMUtil 22 QKUsd 6676975
QKFre 1711633 CrtMID 6130195 CrtICID 722770 CrtDCID 54 InjMsg 4572789 InjRcp
4575323 GenBncRcp 255536 RejRcp 20388 DrpMsg 469642 SftBncEvnt 0 CmpRcp 3650806 HrdBncRcp
 255536
DnsHrdBnc 23 5XXHrdBnc 28 FltrHrdBnc 255485 ExpHrdBnc 0
OtrHrdBnc 0 DlvRcp 3394965 DelRcp 305 GlbUnsbHt 0 ActvRcp 65 UnatmptRcp 65 AtmptRcp 0
CrtCncIn 9
CrtCncOut 0 DnsReq 7756744 NetReq 7769130 CchHit 8373490 CchMis
1989637 CchEct 1625236 CchExp 1569329 CPUTTm 37 CPUETm 62 MaxIO 465600 RAMUsd 1473355956
 MMLen 54782
DstInMem 11 ResCon 0 WorkQ 54710 QuarMsgs 375
QuarQKUsd 145096 LogUsd 26 SophLd 15 BMLd 0 CASELd 0 TotalLd 100 LogAvail 116G EuQ 64
EuqRls 0 CmrkLd 0
McafLd 9 SwIn 122 SwOut 5295 SwPgIn 368 SwPg Out 63639
SwapUsage 4% RptLd 0 QtnLd 19 EncrQ 0 InjBytes 516664777890
```

ドメイン デバッグ ログの使用

ドメインデバッグログには、電子メールゲートウェイと指定の受信者ホスト間のSMTP会話でのクライアントとサーバの通信が記録されます。このログタイプは主に、特定の受信者ホストに関する問題のデバッグに使用されます。

表 *13*: ドメイン デバッグ ログの統計情報

統計	説明
タイムスタンプ	バウンス イベントの時刻

統計	説明
ログ レベル（Log level）	このバウンス ログの詳細レベル
From	エンベロープ送信者
受信者（To）	エンベロープ受信者
理由	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
応答	受信者ホストからの SMTP 応答コードおよびメッセージ

ドメイン デバッグ ログの例

```
Sat Dec 21 02:37:22 2003 Info: 102503993 Sent: 'MAIL FROM:<daily@dailyf-y-i.net>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'RCPT TO:<LLLSMILE@aol.com>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'DATA'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '354 START MAIL INPUT, END WITH "." ON A
LINE BY ITSELF'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '250 OK'
```

インジェクション デバッグ ログの使用

インジェクション デバッグ ログには、電子メールゲートウェイと、システムに接続している指定のホスト間の SMTP 会話が記録されます。インジェクション デバッグ ログは、インターネットから接続を開始するクライアントと電子メールゲートウェイ間の通信に関する問題をトラブルシューティングするのに役立ちます。このログでは、2 つのシステム間で伝送されたすべてのバイトが記録され、接続ホストに「送信」または接続ホストから「受信」に分類されます。

記録するホストの会話を指定するには、IP アドレス、IP 範囲、ホスト名、または部分ホスト名を指定する必要があります。IP 範囲内で接続している IP アドレスがすべて記録されます。部分ドメイン内のホストがすべて記録されます。システムは、接続している IP アドレスに対してリバース DNS ルックアップを実行して、ホスト名に変換します。DNS に対応する PTR レコードがない IP アドレスは、ホスト名に一致しません。

記録するセッション数も指定する必要があります。

インジェクション デバッグ ログ内の各行には、次の表に示す情報が含まれます。

表 *14*：インジェクション デバッグ ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
ICID	インジェクション接続 ID は、別のログ サブスクリプションで同じ接続に関連付けることができる固有識別子です。
Sent/Received	「Sent to」と記された行は、接続ホストに送信された実際のバイトです。「Rcvd from」と記された行は、接続ホストから受信した実際のバイトです。
[IPアドレス（IP Address）]	接続ホストの IP アドレス。

インジェクション デバッグ ログの例

```
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '220 postman.example.com
ESMTP\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'HELO
mail.remotehost.com\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250
postman.example.com\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'MAIL
FROM:<sender@remotehost.com>\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 sender
<sender@remotehost.com> ok\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'RCPT
TO:<recipient@example.com>\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 recipient
<recipient@example.com> ok\015\012'
Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'DATA\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '354 go ahead\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'To:
recipient@example.com\015\012Date: Apr 02 2003 10:09:44\015\012Subject: Test
Subject\015\012From: Sender <sender@remotehost.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'This is the content of the
message'
Wed Apr 2 14:30:04 Info: 6216 Sent to '172.16.0.22': '250 ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'QUIT\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '221
postman.example.com\015\012'
```

システム ログの使用

表 *15 :* システム ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	ログに記録されたイベント。

システム ログの例

次のシステム ログの例は、commit を実行したユーザの名前と入力されたコメントを含む、いくつかの commit エントリを示しています。

```
Wed Sep 8 18:02:45 2004 Info: Version: 4.0.0-206 SN: XXXXXXXXXXXX-XXX

Wed Sep 8 18:02:45 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:02:45 2004 Info: System is coming up

Wed Sep 8 18:02:49 2004 Info: bootstrapping DNS cache

Wed Sep 8 18:02:49 2004 Info: DNS cache bootstrapped

Wed Sep 8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Password

Wed Sep 8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW

Thu Sep 9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds

Thu Sep 9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI
log for examples

Thu Sep 9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.
```

CLI 監査ログの使用

表 *16 : CLI* 監査ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
PID	コマンドが入力された特定の CLI セッションのプロセス ID。
メッセージ	メッセージは、入力された CLI コマンド、CLI 出力（メニュー、リストなど）、および表示されるプロンプトで構成されます。

CLI 監査ログの例

次の CLI 監査ログの例は、who および textconfig CLI コマンドが入力された PID 16434 の情報を示しています。

```
Thu Sep 9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '


Thu Sep 9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername Login Time Idle Time Remote Host What\n======== ========== =========
=========== ====\nadmin Wed 11AM 3m 45s 10.1.3.14 tail\nadmin 02:32PM
0s 10.1.3.14 cli\nmail3.example.com> '


Thu Sep 9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n-
NEW - Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[]>
'
```

FTP サーバ ログの使用

表 *17 : FTP* サーバ ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
ID	接続 ID。FTP 接続ごとの別個の ID
メッセージ	ログ エントリのメッセージ セクションは、ログファイル ステータス情報、またはFTP 接続情報（ログイン、アップロード、ダウンロード、ログアウトなど）になります。

FTP サーバ ログの例

次の FTP サーバ ログの例には、接続（ID:1）が記録されています。着信接続の IP アドレスのほか、アクティビティ（ファイルのアップロードとダウンロード）およびログアウトが示されています。

```
Wed Sep 8 18:03:06 2004 Info: Begin Logfile

Wed Sep 8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21

Wed Sep 8 18:03:06 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:03:06 2004 Info: System is coming up

Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds

Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86

Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS

Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes
```

```
Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes

Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

HTTP ログの使用

表 *18 : HTTP* ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
ID	セッション ID
申請	接続マシンの IP アドレス
ユーザ	接続ユーザのユーザ名
メッセージ	実行されたアクションに関する情報。GET コマンド、POST コマンド、またはシステム ステータスなどが含まれる場合があります。

HTTP ログの例

次の HTTP ログの例は、管理者ユーザと GUI の対話（システム設定ウィザードの実行など）を示しています。

```
Wed Sep 8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port
443

Wed Sep 8 18:17:23 2004 Info: http service listening on 192.168.0.1:80

Wed Sep 8 18:17:23 2004 Info: https service listening on 192.168.0.1:443

Wed Sep 8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds

Wed Sep 8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST
/system_administration/system_setup_wizard HTTP/1.1 303

Wed Sep 8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/system_administration/ssw_done HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/incoming_mail_overview HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190
HTTP/1.1 200

Wed Sep 8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=19
0 HTTP/1.1 200

Wed Sep 8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/quarantines HTTP/1.1 200
```

NTP ログの使用

表 *19 : NTP* ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、サーバへの簡易ネットワークタイムプロトコル（SNTP）クエリーまたは adjust: メッセージで構成されます。

NTP ログの例

次の NTP ログの例は、電子メールゲートウェイから NTP ホストへの 2 度のポーリングを示しています。

```
Thu Sep 9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652

Thu Sep 9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096

Thu Sep 9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152

Thu Sep 9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

スキャン ログの使用

スキャンログには、電子メールゲートウェイのスキャンエンジンのすべての LOG および COMMON メッセージが含まれています。使用可能な COMMON および LOG アラート メッセージのリストについては、「システム管理」の章の「アラート」を参照してください。

表 *20 :* スキャン ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、いずれかのスキャン エンジンのアプリケーションの障害、送信されたアラート、失敗したアラート、またはログエラーメッセージで構成されています。

スキャン ログの例

次のログの例は、Sophos アンチウイルスに関する警告アラートを送信している電子メールゲートウェイの履歴を示しています。

```
Wed Feb 23 22:05:48 2011 Info: Internal SMTP system attempting to send a message to
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...' (attempt #0).


Wed Feb 23 22:05:48 2011 Info: Internal SMTP system successfully sent a message to
```

```
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...'.


Wed Feb 23 22:05:48 2011 Info: A Anti-Virus/Warning alert was sent to alerts@example.com
with subject "Warning <Anti-Virus> mail3.example.com: sophos antivirus - The Anti-Virus
database on this system is...".
```

アンチスパム ログの使用

表 *21 :* アンチスパム ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、アンチスパムアップデートの確認と結果（エンジンまたはアンチスパムルールのアップデートが必要であったかどうかなど）で構成されます。

アンチスパム ログの例

次のアンチスパム ログの例は、アンチスパム エンジンによる、スパム定義のアップデートおよび CASE アップデートの確認を示しています。

```
Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19103) : case-daemon: server
successfully spawned child process, pid 19111

Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19111) : startup: Region profile:
Using profile global

Fri Apr 13 18:59:59 2007 Info: case antispam - engine (19111) : fuzzy: Fuzzy plugin v7
successfully loaded, ready to roll

Fri Apr 13 19:00:01 2007 Info: case antispam - engine (19110) : uribllocal: running URI
blocklist local

Fri Apr 13 19:00:04 2007 Info: case antispam - engine (19111) : config: Finished loading
configuration
```

グレイメール ログの使用

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージには、グレイメールエンジン、ステータス、設定などの情報が含まれます。

グレイメール ログの例

```
Tue Mar 24 08:56:45 2015 Info: graymail [BASE] Logging at DEBUG level

Tue Mar 24 08:56:45 2015 Info: graymail [HANDLER] Initializing request handler

Tue Mar 24 08:56:50 2015 Info: graymail [ENGINE] Loaded graymail scanner library

Tue Mar 24 08:56:50 2015 Info: graymail [ENGINE] Created graymail scanner instance

Tue Mar 24 08:56:50 2015 Info: graymail [HANDLER] Debug mode disabled on graymail process


Tue Mar 24 08:56:50 2015 Info: graymail [HANDLER] Starting thread WorkerThread_0
```

アンチウイルス ログの使用

表 *22:* アンチウイルス ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、アンチウイルス アップデートの確認と結果（エンジンまたはウイルス定義のアップデートが必要であったかどうかなど）で構成されます。

アンチウイルス ログの例

次のアンチウイルス ログの例は、Sophosアンチウイルスエンジンによる、ウイルス定義（IDE）とエンジン自体のアップデートの確認を示しています。

```
Thu Sep 9 14:18:04 2004 Info: Checking for Sophos Update

Thu Sep 9 14:18:04 2004 Info: Current SAV engine ver=3.84. No engine update needed

Thu Sep 9 14:18:04 2004 Info: Current IDE serial=2004090902. No update needed.
```

このログを一時的にDEBUG レベルに設定すると、アンチウイルスエンジンが所定のメッセージについて特定の判定を返した理由を診断するのに役立ちます。DEBUG ロギング情報は冗長です。使用の際は注意してください。

AMP エンジン ログの使用

AMP エンジン ログには、次の詳細が含まれます。

- ファイル レピュテーション サーバに送信されたファイル レピュテーション クエリーと、ファイル レピュテーション サーバから受信された応答。
- ファイル分析（ファイル分析サーバにファイルがアップロードされている場合）。ファイル分析の状態は、ファイル分析サーバから応答が受信されるまで定期的に記録されます。

AMP エンジン ログ エントリの例

次に特定のシナリオに基づく AMP エンジン ログ エントリの例を示します。

ファイル レピュテーションとファイル分析サーバの初期化

```
Wed Oct 5 15:17:31 2016 Info: File reputation service initialized successfully
Wed Oct 5 15:17:31 2016 Info: The following file type(s) can be sent for File Analysis:
 Microsoft Windows / DOS Executable, Microsoft Office 97-2004 (OLE), Microsoft Office
2007+ (Open XML), Other potentially malicious file types, Adobe Portable Document Format
 (PDF). To allow analysis of new file type(s), go to Security Services > File Reputation
 and Analysis.
Wed Oct 5 15:17:31 2016 Info: File Analysis service initialized successfully
```

ファイル レピュテーション サーバが未構成

```
Tue Oct 4 23:15:24 2016 Warning: MID 12 reputation query failed for attachment
'Zombies.pdf' with error "Cloud query failed"
```

ファイル レピュテーション クエリーの初期化

```
Fri Oct 7 09:44:04 2016 Info: File reputation query initiating. File Name = 'mod-6.exe',
 MID = 5, File Size = 1673216 bytes,
File Type = application/x-dosexec
```

統計	説明
ファイル名（File Name）	SHA-256 ハッシュ ID がファイル レピュテーション サーバに送信されるファイルの名前。 ファイル名が使用できない場合、ファイル名が不明であると表現します。
MID	電子メールパイプラインを通過するメッセージの追跡に使用されるメッセージ ID。

統計	説明
ファイル サイズ（File size）	SHA-256 ハッシュ識別子がファイル レピュテーション サーバに送信されるファイルのサイズ。
ファイル タイプ（File Type）	SHA-256 ハッシュ識別子がファイル レピュテーション サーバに送信されるファイルのタイプ。 次のファイル タイプがサポートされています。 • Microsoft Windows / DOS Executable • Microsoft Office 97-2004（OLE） • Microsoft Office 2007+（Open XML） • その他の悪意がある可能性のあるファイル タイプ • Adobe Portable Document Format（PDF）

ファイル レピュテーション サーバからファイル レピュテーション クエリーに対して受信した応答

```
Fri Oct 7 09:44:06 2016 Info: Response received for file reputation query from Cloud.
File
Name = 'mod-6.exe', MID = 5, Disposition = MALICIOUS, Malware = W32.061DEF69B5-100.SBX.TG,
Reputation Score = 73, sha256 =
061def69b5c100e9979610fa5675bd19258b19a7ff538b5c2d230b467c312f19, upload_action = 2
```

統計	説明
ファイル名（File Name）	SHA-256 ハッシュ ID がファイル レピュテーション サーバに送信されるファイルの名前。 ファイル名が使用できない場合、ファイル名が不明であると表現します。
MID	電子メール パイプラインを通過するメッセージの追跡に使用されるメッセージ ID。
傾向（Disposition）	ファイル レピュテーション傾向値は次のとおりです。 • MALICIOUS • CLEAN • FILE UNKNOWN：レピュテーション スコアがゼロの場合。 • VERDICT UNKNOWN：傾向が FILE UNKNOWN でありスコアが非ゼロの場合。 • LOW RISK：ファイル分析の後でファイルに動的なコンテンツが見つからない場合、判定は「LOW RISK」です。ファイル分析用にファイルは送信されず、メッセージは電子メール パイプラインを通過します。
マルウェア（Malware）	マルウェア脅威の名前。

統計	説明
レピュテーション スコア（Reputation score）	ファイル レピュテーション サーバによってファイルに割り当てられるレピュテーション スコア。 ファイル傾向が **VERDICT UNKNOWN** の場合、電子メールゲートウェイはファイルレピュテーション判定を、レピュテーションスコアとしきい値に基づいて調整します。
アップロード アクション（Upload Action）	特定のファイルに実行される、ファイル レピュテーション サーバによって推奨されるアップロード アクションの値： • 0：アップロード用に送信する必要はありません。 • 1：アップロード用にファイルを送信します。 （注） 電子メールゲートウェイはアップロードアクションの値が「1」の場合にファイルをアップロードします。 • 2：アップロード用にファイルを送信しません。 • 3：アップロード用にメタデータのみを送信します。

分析のためのファイル アップロードとファイル分析プロセス

```
Wed Sep 28 11:31:58 2016 Info: File uploaded for analysis. SHA256:
e7ae35a8227b380ca761c0317e814e4aaa3d04f362c6b913300117241800f0ea

Wed Sep 28 11:36:58 2016 Info: File Analysis is running for SHA:
e7ae35a8227b380ca761c0317e814e4aaa3d04f362c6b913300117241800f0ea

Fri Oct 7 07:39:13 2016 Info: File Analysis complete. SHA256:
16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc, Submit Timestamp:
1475825466, Update Timestamp: 1475825953, Disposition: 3 Score: 100, run_id: 194926004
Details: Analysis is completed for the File
SHA256[16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc]
Spyname:[W32.16454AFF50-100.SBX.TG]
```

統計	説明
SHA256	対応するファイルの SHA-256 ハッシュ ID。
送信タイムスタンプ（Submit Timestamp）	電子メールゲートウェイによってファイルがファイル分析サーバにアップロードされた日付と時刻。
更新タイムスタンプ（Update Timestamp）	ファイルに対するファイル分析が完了した日付と時刻
傾向（Disposition）	ファイル レピュテーションの判定結果で、次の値があります。 • 1 - マルウェアの検出なし • 2 - 正常 • 3 - マルウェア

統計	説明
スコア（Score）	ファイル分析サーバによってファイルに割り当てられる分析スコア。
実行 ID（Run ID）	ファイル分析サーバが特定のファイル分析についてファイルに割り当てる数値（ID）。
詳細（Details）	ファイル分析中にエラーが報告された場合は追加情報。そうでない場合は、ファイルに対する最終的な分析が完了していることを示します。
スパイ名（Spy Name）	ファイル分析中にファイル内にマルウェアが見つかった場合は、脅威の名前。

ファイルが分析用にアップロードされない

```
Wed Sep 14 12:27:52 2016 Info: File not uploaded for analysis. MID = 0 File
SHA256[a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82] file
mime[text/plain] Reason: No active/dynamic contents exists
```

統計	説明
MID	電子メール パイプラインを通過するメッセージの追跡に使用されるメッセージ ID。
ファイル MIME（File MIME）	ファイルの MIME タイプ。
理由	以下に示すのは、upload_action が '1' に設定されている場合でも、ファイルがファイル分析サーバにアップロードされない理由の値の 1 つです。 • 別のノードでファイルがすでにアップロードされている：ファイルはすでに別の電子メールゲートウェイを介してファイル分析サーバにアップロードされています。 • ファイル分析が進行中：ファイルは進行中のアップロードのためにすでに選択されています。 • ファイルはファイル分析サーバにすでにアップロード済み • サポート対象のファイル タイプではない • ファイル サイズが範囲外：アップロード ファイルのサイズがファイル分析サーバによって設定されているしきい値を超えています。 • アップロード キューが満杯であった • ファイル分析サーバのエラー • アクティブなコンテンツまたは動的コンテンツが存在していない • 一般または不明エラー

ファイル アップロード制限が原因でファイル分析がスキップされたファイル アップロード

```
Tue Jun 20 13:22:56 2017 Info: File analysis upload skipped. SHA256:
b5c7e26491983baa713c9a2910ee868efd891661c6a0553b28f17b8fdc8cc3ef,Timestamp[1454782976]
details[File SHA256[b5c7e26491983baa713c9a2910ee868efd891661c6a0553b28f17b8fdc8cc3ef]
file
mime[application/pdf], upload priority[Low] not uploaded, re-tries[3], backoff[986]
discarding ...]
Tue Jun 20 13:22:56 2017 Critical: The attachment could not be uploaded to the
File Analysis server because the appliance exceeded the upload limit
```

統計	説明
SHA256	対応するファイルの SHA-256 ハッシュ ID。
Timestamp	ファイル分析サーバへのファイルのアップロードが失敗した日付と時刻。
詳細（Details）	ファイル分析サーバのエラーの詳細。
ファイル MIME（File MIME）	ファイルの MIME タイプ。
アップロード優先順位（Upload priority）	[アップロード優先順位（Upload priority）] の値は以下のとおりです。 • [高（High）] - PDF ファイル タイプを除くすべての選択されたファイル タイプの場合。 • [低（Low）] - PDF ファイル タイプのみの場合。
再試行回数（Re-tries）	当該のファイルに対して実行されたアップロード試行の回数。 （注） 1 ファイルに対し、最大 3 回までアップロードを試行できます。
バックオフ（x）（Backoff (x)）	電子メールゲートウェイがファイル分析サーバにファイルをアップロードしようとする前に待機する必要がある秒数（x）。これは、電子メールゲートウェイが 1 日あたりのアップロード制限に達したときに発生します。
重要（理由）（Critical (Reason)）	電子メールゲートウェイがアップロード制限を超えたため、ファイル分析サーバに添付ファイルをアップロードできませんでした。

ファイル分析サーバのエラーが原因でファイル分析がスキップされたファイル アップロード

```
Sat Feb 6 13:22:56 2016 Info:SHA256:
69e17e213732da0d0cbc48ae7030a4a18e0c1289f510e8b139945787f67692a5,Timestamp[1454959409]
details[Server Response HTTP code:[502]]
```

統計	説明
SHA256	対応するファイルの SHA-256 ハッシュ ID。

統計	説明
Timestamp	ファイル分析サーバへのファイルのアップロードが試行された日付と時刻。
詳細（Details）	ファイル分析サーバのエラーに関する情報。

受信したファイル レトロスペクティブ判定

```
Fri Oct 7 07:39:13 2016 Info: Retrospective verdict received. SHA256:
16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc, Timestamp: 1475832815.7,
Verdict: MALICIOUS, Reputation Score: 0, Spyname: W32.16454AFF50-100.SBX.
```

統計	説明
SHA256	対応するファイルの SHA-256 ハッシュ ID。
Timestamp	ファイル分析サーバからファイルのレトロスペクティブな判定を受信した日時。
判定	ファイルのレトロスペクティブな判定の値は「悪意のある」または「正常」です。
Reputation Score	ファイル レピュテーション サーバによってファイルに割り当てられるレピュテーション スコア。
Spyname	ファイル分析中にファイル内にマルウェアが見つかった場合は、脅威の名前。

スパム隔離ログの使用

表 *23 :* スパム ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、実行されたアクション（メッセージの隔離、隔離エリアからの解放など）で構成されます。

スパム隔離ログの例

次のログの例は、隔離から admin@example.com にメッセージ（MID 8298624）が解放されていることを示しています。

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work
queue)
```

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work
queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

スパム隔離 GUI ログの使用

表 *24 :* スパム *GUI* ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、ユーザ認証などの実行されたアクションで構成されます。

スパム隔離 GUI ログの例

次のログの例は、成功した認証、ログイン、およびログアウトを示しています。

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82

Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83

Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin

Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO session:10.251.23.228

Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228

Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

LDAP デバッグ ログの使用

表 *25 : LDAP* デバッグ ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	LDAP デバッグ メッセージ。

LDAP デバッグ ログの例

（注） ログ ファイルの各行には、番号が割り当てられません。ここでは、単にサンプル用として番号が割り当てられています。

1	Thu Sep 9 12:24:56 2004 Begin Logfile
2	Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa
3	Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa
4	Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa
5	Thu Sep 9 12:28:08 2004 LDAP: Clearing LDAP cache
6	Thu Sep 9 13:00:09 2004 LDAP: Query '(&(ObjectClass={g})(mailLocalAddress={a}))' to server sun (sun.qa:389)
7	Thu Sep 9 13:00:09 2004 LDAP: After substitute, query is '(&(ObjectClass=inetLocalMailRecipient) (mailLocalAddress=rroute.d00002b.loc@ldap.route.local.add00002.qa))'
8	Thu Sep 9 13:00:09 2004 LDAP: connecting to server
9	Thu Sep 9 13:00:09 2004 LDAP: connected
10	Thu Sep 9 13:00:09 2004 LDAP: Query (&(ObjectClass=inetLocalMailRecipient) (mailLocalAddress=rroute.d00002b.loc@ldap.route.local.add00002.qa)) returned 1 results
11	Thu Sep 9 13:00:09 2004 LDAP: returning: [<LDAP:>]

前述のログ ファイルを読み取るためのガイドとして、使用してください。

表 *26 : LDAP* デバッグ ログの例の詳細

行番号	説明
1	ログ ファイルが開始されます。

行番号	説明
2 3 4	リスナーは、明確に「sun.masquerade」というLDAPクエリーによって、マスカレードにLDAPを使用するように設定されています。 アドレスemployee@routing.qaがLDAPサーバで検索され、一致が検出されます。その結果のマスカレードアドレスはemployee@mail.qaであり、マスカレードの設定によってこのアドレスがメッセージヘッダー、エンベロープ送信者、またはその両方に書き込まれます。
5	ユーザは手動でldapflushを実行しています。
6	クエリーは、sun.qa、ポート389に送信されます。クエリーテンプレートは(&(ObjectClass={g})(mailLocalAddress={a}))です。 {g}は、発信側フィルタ（rcpt-to-groupまたはmail-from-groupルール）で指定されたグループ名に置換されます。 {a}は、当該のアドレスに置換されます。
7	ここで代入（前述のとおり）が実行されます。LDAPサーバに送信される前のクエリーはこのようになります。
8	サーバへの接続がまだ確立されていないので、接続します。
9	サーバに送信されるデータです。
10	結果は、確実に空になります。つまり、1つのレコードが返されますが、クエリーはフィールドを要求していないので、データは報告されません。これらは、データベースに一致があるかどうかをクエリーでチェックするときに、グループ クエリーとアクセプト クエリーの両方に使用されます。

セーフリスト/ブロックリスト ログの使用

次の表に、セーフリスト/ブロックリスト ログに記録される統計情報を示します。

表 *27*：セーフリスト/ブロックリスト ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

セーフリスト/ブロックリスト ログの例

次のセーフリスト/ブロックリストログの例は、電子メールゲートウェイによって 2 時間ごとにデータベースのスナップショットが作成されていることを示しています。送信者がデータベースに追加された時刻も示されます。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC:
10800 seconds Fri Sep 28 14:22:33 2007 Info: System is coming up.


Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.

.......................

Mon Oct 1 14:16:09 2007 Info: SLBL: The database snapshot has been created.

Mon Oct 1 14:37:39 2007 Info: SLBL: The database snapshot has been created.

Mon Oct 1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.

Mon Oct 1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.

Mon Oct 1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

レポーティング ログの使用

次の表は、レポート ログに記録された統計情報を示しています。

表 *28 :* レポーティング ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

レポーティング ログの例

次のレポーティングログの例は、情報ログレベルに設定された電子メールゲートウェイを示しています。

```
Wed Oct 3 13:39:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:39:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40
```

```
Wed Oct 3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692

Wed Oct 3 13:40:53 2007 Info: Period hour using 36800 (KB)

Wed Oct 3 13:40:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:40:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:40:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds

Wed Oct 3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41

Wed Oct 3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692

Wed Oct 3 13:41:53 2007 Info: Period hour using 36800 (KB)

Wed Oct 3 13:41:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:41:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:41:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
```

レポーティング クエリー ログの使用

次の表に、レポーティング クエリー ログに記録される統計情報を示します。

表 *29:* レポーティング クエリー ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

レポーティング クエリー ログの例

次のレポーティングクエリログの例は、電子メールゲートウェイによって、2007 年 8 月 29 日から 10 月 10 日までの期間で毎日の発信メールトラフィッククエリが実行されていることを示しています。

```
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804479.

Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804480.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610228.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTENT_FILTER',
```

```
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_PROCESSED'] for rollup period "day" with
 interval range 2007-08-29 to 2007-10-01
with key constraints

None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from
0 to 2 sort_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610229.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval
 range 2007-08-29 to
2007-10-01 with key constraints None sorting on
['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning
results from 0 to 2 sort_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

アップデータ ログの使用

表 *30*：アップデータ ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、システム サービス アップデート情報のほか、AsyncOS によるアップデートの確認と、スケジュールされている次回アップデートの日時で構成されます。

アップデータ ログの例

次のログの例は、電子メールゲートウェイが新規の McAfee アンチウイルス定義でアップデートされていることを示しています。

```
Fri Sep 19 11:07:51 2008 Info: Starting scheduled update

Fri Sep 19 11:07:52 2008 Info: Acquired server manifest, starting update 11

Fri Sep 19 11:07:52 2008 Info: Server manifest specified an update for mcafee

Fri Sep 19 11:07:52 2008 Info: mcafee was signalled to start a new update

Fri Sep 19 11:07:52 2008 Info: mcafee processing files from the server manifest

Fri Sep 19 11:07:52 2008 Info: mcafee started downloading files

Fri Sep 19 11:07:52 2008 Info: mcafee downloading remote file
"http://stage-updates.ironport.com/mcafee/dat/5388"

Fri Sep 19 11:07:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:12:52
2008

Fri Sep 19 11:08:12 2008 Info: mcafee started decrypting files
```

```
Fri Sep 19 11:08:12 2008 Info: mcafee decrypting file
"mcafee/dat/5388" with method "des3_cbc"

Fri Sep 19 11:08:17 2008 Info: mcafee started decompressing files

Fri Sep 19 11:08:17 2008 Info: mcafee started applying files

Fri Sep 19 11:08:17 2008 Info: mcafee applying file "mcafee/dat/5388"

Fri Sep 19 11:08:18 2008 Info: mcafee verifying applied files

Fri Sep 19 11:08:18 2008 Info: mcafee updating the client manifest

Fri Sep 19 11:08:18 2008 Info: mcafee update completed

Fri Sep 19 11:08:18 2008 Info: mcafee waiting for new updates

Fri Sep 19 11:12:52 2008 Info: Starting scheduled update

Fri Sep 19 11:12:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:17:52
2008

Fri Sep 19 11:17:52 2008 Info: Starting scheduled update

Fri Sep 19 11:17:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:22:52
2008
```

アップデータ ログの例

この例では、ログは、無効にされている自動更新、Sophos Anti-virus 定義に適用されているバックアップを表示します。

```
Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “postx”

Fri Mar 10 15:05:55 2017 Debug: postx updates disabled

Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “postx”

Fri Mar 10 15:05:55 2017 Trace: command session starting

Fri Mar 10 15:05:55 2017 Info: Automatic updates disabled for engine Sophos engine

Fri Mar 10 15:05:55 2017 Info: Sophos: Backup update applied successfully

Fri Mar 10 15:05:55 2017 Info: Internal SMTP system attempting to send a message to
abshastr@ironport.com
with subject ‘Automatic updates are now disabled for sophos’ attempt #0).

Fri Mar 10 15:05:55 2017 Debug: amp feature key disabled

Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “amp”

Fri Mar 10 15:05:55 2017 Debug: amp feature key disabled
```

トラッキング ログについて

トラッキング ログには、AsyncOS の電子メール動作に関する情報が記録されます。ログ メッセージは、メール ログに記録されたメッセージのサブセットです。

トラッキングログは、メッセージ トラッキング データベースを作成するため、電子メール ゲートウェイのメッセージ トラッキング コンポーネントで使用されます。ログ ファイルはデータベースの作成プロセスで消費されるので、トラッキング ログは一過性のものになります。トラッキング ログの情報は、人による読み取りや解析を目的とした設計になっていません。

Cisco Secure Manager Email and Web Gateway を使用することで、複数の電子メール ゲートウェイからのトラッキング情報の表示もできます。

認証ログの使用

認証ログには、成功したユーザ ログインと失敗したログイン試行が記録されます。

表 *31* : 認証ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、電子メール ゲートウェイにログインしようとしたユーザのユーザ名、ユーザ権限ロールの詳細（「admin」、「operator」など）、およびそのユーザが正常に認証されたかどうかという情報で構成されます。

認証ログの例

次のログの例は、「admin」、「joe」、および「dan」というユーザによるログイン試行を示しています。

```
Wed Sep 17 15:16:25 2008 Info: Begin Logfile

Wed Sep 17 15:16:25 2008 Info: Version: 6.5.0-262 SN: XXXXXXX-XXXXX

Wed Sep 17 15:16:25 2008 Info: Time offset from UTC: 0 seconds

Wed Sep 17 15:18:21 2008 Info: User admin was authenticated successfully.

Wed Sep 17 16:26:17 2008 Info: User joe failed authentication.

Wed Sep 17 16:28:28 2008 Info: User joe was authenticated successfully.

Wed Sep 17 20:59:30 2008 Info: User admin was authenticated successfully.

Wed Sep 17 21:37:09 2008 Info: User dan failed authentication.
```

コンフィギュレーション履歴ログの使用

コンフィギュレーション履歴ログは、ユーザの名前、ユーザが変更を行った設定の場所の説明、および変更を保存するときにユーザが入力したコメントがリストされた追加のセクションを持つコンフィギュレーション ファイルで構成されます。ユーザが変更を保存するたびに、変更後のコンフィギュレーション ファイルを含む新しいログが作成されます。

コンフィギュレーション履歴ログの例

次の設定履歴ログの例は、システムへのログインを許可されているローカルユーザを定義するテーブルにユーザ（admin）がゲスト ユーザを追加したことを示しています。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<!--

XML generated by configuration change.

Change comment: added guest user

User: admin

Configuration are described as:

This table defines which local users are allowed to log into the system.

Product: Cisco IronPort M160 Messaging Gateway(tm) Appliance

Model Number: M160

Version: 6.7.0-231

Serial Number: 000000000ABC-D000000

Number of CPUs: 1

Memory (GB): 4

Current Time: Thu Mar 26 05:34:36 2009

Feature "Cisco IronPort Centralized Configuration Manager": Quantity = 10, Time
Remaining = "25 days"

Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"

Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"

Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"

Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"

-->

<config>
```

外部脅威フィードのエンジン ログの使用

ETF ログには、ETF エンジン、ステータス、設定などに関する情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

外部脅威フィードのエンジン ログの例

```
Thu Jun 7 04:54:15 2018 Info: THREAT_FEEDS: Job failed with exception: Invalid URL or
Port Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: A delta poll is scheduled for the source:
```

```
 S1
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: A delta poll has started for the source: S1,
 domain: s1.co, collection: sss
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: Observables are being fetched from the source:
 S1 between 2018-06-07 04:34:13+00:00 and 2018-06-07 05:04:13.185909+00:00
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: 21 observables were fetched from the source:
 S1
Thu Jun 7 05:19:14 2018 Info: THREAT_FEEDS: A delta poll is scheduled for the source:
S1
Thu Jun 7 05:19:14 2018 Info: THREAT_FEEDS: A delta poll has started for the source: S1,
 domain: s1.co, collection: sss
```

ETF ソース設定の失敗 - 無効なコレクション名

この例では、無効なコレクション名が原因で、電子メールゲートウェイが外部脅威フィードソースから脅威フィードを取得できなかったことがログに示されています。

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com, cause of failure: Invalid Collection name
```

ソリューション

Web インターフェイスの [メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] ページに移動するか、CLI で `threatfeedsconfig > sourceconfig` サブコマンドを使用して、設定した外部脅威フィードソースの正確なコレクション名を入力します。

ETF ソース設定の失敗 - HTTP エラー

この例では、HTTP エラーが原因で、電子メールゲートウェイが外部脅威フィードソースから脅威フィードを取得できなかったことがログに示されています。

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com , cause of failure: HTTP Error
```

ソリューション

Web インターフェイスの [メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] ページに移動するか、CLI で `threatfeedsconfig > sourceconfig` サブコマンドを使用して、設定した外部脅威フィード ソースの正確なポーリング パスまたはユーザ認証クレデンシャルを入力します。

ETF ソース設定の失敗 - 無効な URL

この例では、無効な URL が原因で、電子メールゲートウェイが外部脅威フィードソースから脅威フィードを取得できなかったことがログに示されています。

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com , cause of failure: HTTP Error
```

ソリューション

Web インターフェイスの [メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] ページに移動するか、CLI で `threatfeedsconfig > sourceconfig`

サブコマンドを使用して、設定した外部脅威フィード ソースの正確なホスト名またはポート番号を入力します。

統合イベント ログの使用

ログ タイプを統合イベント ログとしてログ サブスクリプションを設定する場合、ログ出力の 1 行に特定のメッセージ属性を含めるには、[ログフィールド（Log Fields）] オプションを使用します。

ログタイプが統合イベントログのログサブスクリプションを設定すると、次のログフィールドがデフォルトで選択されます。

- ICID
- DCID
- シリアル番号
- MID

（注） [選択されたログフィールド（Selected Log Fields）] リストからはデフォルトのログフィールドを削除できません。

統合イベント ログの例

この例のログには、ログ タイプが統合イベント ログのログ サブスクリプションを設定するときに選択された使用可能なすべてのフィールドが表示されます。

```
Thu Jun 30 08:04:50 2022: CEF:0|Cisco|C100V Email Security Virtual Appliance|14.0.0-657
|ESA_CONSOLIDATED_LOG_EVENT|Consolidated Log
Event|5|deviceExternalId=42127C7DDEE76852677B-F80CE8074CD3
ESACustomLogs={'label2': ['value20'], 'label1': ['value1', 'value2']}
ESALogHeaders={'reply-to': ['test@esa.com ', 'newsletter@esa.com'], 'from':
['any@esa.com']}
ESAMID=1053 ESAICID=134 ESAAMPVerdict=UNKNOWN ESAASVerdict=NEGATIVE ESAAVVerdict=NEGATIVE

ESACFVerdict=MATCH end=Thu Mar 18 08:04:46 2021 ESADLPVerdict=NOT_EVALUATED
dvc=10.10.193.13 ESAAttachmentDetails={'test.txt': {'AMP': {'Verdict': 'FILE UNKNOWN',
'fileHash': '7f843d263304fb0516d6210e9de4fa7f01f2f623074aab6e3ee7051f7b785cfa'},
'BodyScanner':
{'fsize': 10059}}} ESAFriendlyFrom=test@esa.com ESAGMVerdict=NEGATIVE start=Thu Mar 18
08:04:29 2021
deviceInboundInterface=Incomingmail deviceDirection=0 ESAMailFlowPolicy=ACCEPT
suser=test@esa.com
cs1Label=MailPolicy cs1=DEFAULT ESAMFVerdict=NOT_EVALUATED act=QUARANTINED
ESAFinalActionDetails=To POLICY
cs4Label=ExternalMsgID cs4='<20210318070601.40490.18684@mail1.example.com>'
ESAMsgSize=11873 ESAOFVerdict=POSITIVE
duser=9076@testing.com ESAHeloIP=10.11.1.2 cfp1Label=SBRSScore cfp1=None ESASDRDomainAge=27
 years 2 months 15 days
cs3Label=SDRThreatCategory cs3=N/A cs6Label=SDRRepScore cs6=Weak ESASPFVerdict={'mailfrom':
 {'result': 'None',
'sender': 'test@esa.com'}, 'helo': {'result': 'None', 'sender': 'postmaster'}, 'pra':
{'result': 'None', 'sender':
'test@esa.com'}}shost=unknown ESASenderGroup=UNKNOWNLIST src=10.11.1.2 msg='Testing'
```

ログ フィールド	CEF フィールド名	CEF フィールド値
プレフィックス フィールド		
	CEF形式のバージョン（CEF format version）	例：0
	アプライアンスベンダー（Appliance vendor）	例：Cisco
	アプライアンス製品（Appliance product）	例：C100V Email Security Virtual Appliance
	アプライアンスのバージョン（Appliance version）	例：13.0.0-234
	イベントクラスID（Event Class ID）	例：ESA_CONSOLIDATED_LOG_EVENT
	イベント名（Event Name）	例：Consolidated Log Event
	重大度	例：5
GUI フィールド		
シリアル番号（Serial Number）	deviceExternalId	例：42156AC79142E979C5CD-02DE66639E9C
ICIDタイムスタンプ（ICID Timestamp）	start	例：Mon Jul 29 11:22:22 2019
ICID	ESAICID	例：199
リスナー名（Listener Name）	deviceInboundInterface（着信メールの場合） deviceOutboundInterface（送信メールの場合）	例：Inbound 例：Outbound
送信者IP（Sender IP）	src	例：10.10.2.75
送信者ドメイン（Sender Domain）	shost	例：demo.cisco.com
メールの方向（Mail Direction）	deviceDirection	例：0 0：着信 1：発信

ログ フィールド	CEF フィールド名	CEF フィールド値
メールの言語（Mail Language）	cs5	例： cs5Label=ESAMsgLanguage cs5=English
SBRS スコア（SBRS Score）	cfp1	例：cfp1Label=SBRSScore, cfp1=1.1
Data IP	dvc	例：10.10.2.75
メール送信者の地理的位置（Mail Sender Geo Location）	cs2	例：cs2Label=GeoLocation cs2=India
大きすぎる送信者からのメッセージ（Message Too Big from Sender）	ESAMsgTooBigFromSender	例：true 可能な値： true/false
レート制限IP（Rate Limited IP）	ESARateLimitedIP	例：10.10.2.75
メールポリシー名（Mail Policy Name）	cs1	例：cs1Label=MailPolicy cs1=default
メール フローポリシー名（Mail Flow Policy Name）	ESAMailFlowPolicy	例：ACCEPT
送信者グループ名（Sender Group Name）	ESASenderGroup	例：UNKNOWNLIST
DHA IP	ESADHASource	例：10.10.2.75
受信者（Recipients）	duser	例：demo@test.com
リモートIP/Heloドメイン IP（Remote IP/Helo Domain IP）	ESAHeloIP	例：10.10.2.75
リモートホスト/Heloドメイン（Remote Host/ Helo Domain）	ESAHeloDomain	例：test.com
TLS発信接続ステータス（TLS Outgoing Connection Status）	ESATLSOutConnStatus	例：Success 可能な値： Success/Failure
TLS発信プロトコル（TLS Outgoing Protocol）	ESATLSOutProtocol	例：TLSv1.2

ログ フィールド	CEF フィールド名	CEF フィールド値
TLS発信暗号（TLS Outgoing Cipher）	ESATLSOutCipher	例：ECDHE-RSA-AES128-GCM-SHA256
TLS着信接続ステータス（TLS Incoming Connection Status）	ESATLSInConnStatus	例：Success 可能な値： Success/Failure
TLS着信プロトコル（TLS Incoming Protocol）	ESATLSInProtocol	例：TLSv1.2
TLS着信暗号（TLS Incoming Cipher）	ESATLSInCipher	例：ECDHE-RSA-AES128-GCM-SHA256
DMARC判定（DMARC Verdict）	ESADMARCVerdict	例：Success 可能な値： PermFailure/TempFailure/ Reject/Success
DKIM判定（DKIM Verdict）	ESADKIMVerdict	例：Pass 可能な値： Pass/Neutral/TempError/ PermError/HardFail/None
SPF判定（SPF Verdict）	ESASPFVerdict	例：ESASPFVerdict={'mailfrom': {'sender': 'test@cisco.com', 'result': 'SoftFail'}, 'helo': {'sender': 'postmaster', 'result': 'None'}} 可能な値： Pass/Neutral/SoftFail/Fail/ TempError/PermError
危険性のない送信元（Friendly From）	ESAFriendlyFrom	例：demo@test.com
送信者（Mail From）	suser	例：demo@test.com
Reply-To	ESAReplyTo	例：demo@test.com
Subject	msg	例：This is a sample subject
MID	ESAMID	例：101

ログ フィールド	CEF フィールド名	CEF フィールド値
メッセージID（Message ID）	cs4	例：cs1Label=ExternalMsgID cs1=20190729112221.42958.40626 @vm21esa0075.cs21
メッセージ サイズ	ESAMsgSize	例：ESAMsgSize=32199
SDRレピュテーションスコア（SDR Reputation Score）	cs6	例：cs6Label= SDRRepScore cs6=Tainted
SDR統合ドメイン使用年数（SDR Consolidated Domain Age）	ESASDRDomainAge	例：1 year 21 days
SDR統合脅威カテゴリ（SDR Consolidated Threat Category）	cs3	例：cs3Label= SDRThreatCategory cs3=mal
メッセージフィルタ判定（Message Filters Verdict）	メッセージフィルタ判定（Message Filters Verdict）	例：MATCH 可能な値： NOT EVALUATED/MATCH/NO MATCH
AS判定（AS Verdict）	ESAASVerdict	例：POSITIVE 可能な値： Not EVALUATED/NEGATIVE/SUSPECT/ BULK_MAIL/SOCIAL_MAIL/MARKE TING_MAIL/POSITIVE
AV判定（AV Verdict）	ESAAVVerdict	例：POSITIVE 可能な値： NOT EVALUATED/NEGATIVE/REPAIRED /ENCRYPTED/UNSCANNABLE/POSI TIVE

ログ フィールド	CEF フィールド名	CEF フィールド値
AMP判定（AMP Verdict）	ESAAMPVerdict	例：UNKNOWN 可能な値： NOT EVALUATED/CLEAN/FA_PENDING/ UNKNOWN/SKIPPED/ UNSCANNABLE /LOW_RISK/MALICIOUS
グレイメール判定（Graymail Verdict）	ESAGMVerdict	例：POSITIVE 可能な値： NOT EVALUATED/POSITIVE/NEGATIVE
コンテンツフィルタ判定（Content Filters Verdict）	ESACFVerdict	例：MATCH 可能な値： NOT EVALUATED/MATCH/NO MATCH
アウトブレイクフィルタ判定（Outbreak Filters Verdict）	ESAOFVerdict	例：NEGATIVE 可能な値： NOT EVALUATED/POSITIVE/NEGATIVE
DLP判定（DLP Verdict）	ESADLPVerdict	例：VIOLATION 可能な値： NOT EVALUATED/NO TRIGGER/VIOLATION/NO VIOLATION
URLの詳細（URL Details）	ESAURLDetails	例： {url1:{expanded_url:<>, category:<>, wbrs_score:<>, in_attachment:<>, Attachment_with_url:<>,},url2:{…}} （注） 255 文字を超えるURL は切り捨てられます。

ログ フィールド	CEF フィールド名	CEF フィールド値
ファイルの詳細（File Details）	ESAAttachmentDetails	例： {name1:{source: {<>hash:<>, verdicts:<>}}} （注） 255 文字を超えるファイル名は切り捨てられます。
メールボックス自動修復の詳細（Mailbox Auto-Remediation Details）	ESAMARAction	例： {action:<>;succesful_rcpts=<>;failed_recipients=<>;filename=<>}
DCID	ESADCID	例：199
DCIDタイムスタンプ（DCID Timestamp）	end	例：Mon Jul 29 09:55:07 2019
DANEステータス（DANE Status）	ESADaneStatus	例：Success 可能な値： success/failure
DANEホスト（DANE Host）	ESADaneHost	例：testdomain.com
メッセージの最終アクション（Message Final Action）	act	例：act=DELIVERED 可能な値： DROPPED/BOUNCED/DELIVERED：メッセージが検疫されていない場合。 QUARANTINED：メッセージが検疫されている場合。 DQ：メッセージが遅延検疫に送信される場合。これは例外であり、検疫タイプではありません。

ログ フィールド	CEF フィールド名	CEF フィールド値
メッセージの最終アクションの詳細（Message Final Action Details）	ESAFinalActionDetails	例： act=DROPPED ESAFinalActionDetails= By AMP act=QUARANTINED ESAFinalActionDetails=To SPAM
カスタムログエントリ	ESACustomLogs	例： ESACustomLogs={'label2': ['value20']、'label1': ['value1'、'value2']}
カスタムログヘッダー	ESALogHeader	例： ESALogHeaders= {'reply-to': ['test@esa.com ', 'newsletter@esa.com'], 'from': ['any@esa.com']

（注） 選択されたログフィールドに値がない場合（たとえば、DKIMが電子メールゲートウェイで有効になっていないときの「DKIMVerdict」）、そのログフィールドはログメッセージに含まれません。

CSN ログの使用

CSN ログには、CSN データのアップロードに関する詳細が記録されます。CSN データ（電子メールゲートウェイおよび機能の使用状況の詳細）は、トレースレベルで確認できます。

CSN データログエントリの例：

- この例では、電子メールゲートウェイのスマートライセンスが Cisco Smart Software Manager（CSSM）に登録されていないため、CSN データがシスコに送信されなかったことが、ログに示されています。

```
Tue Apr 7 12:52:47 2020 Warning: Device is not
registered with CSSM. Skipping upload of CSN data
```

解決策：Cisco Smart Software Manager（CSSM）に電子メールゲートウェイのスマートライセンスを登録します。

- この例では、Cisco Security Services Exchange（SSE）の接続エラーが原因で、CSN データがシスコに送信されなかったことが、ログに示されています。

```
Thu Apr 9 13:32:46 2020 Warning: The appliance
failed to upload CSN data. reason for failure:
SSE error: HTTP Error 503: Service Unavailable
```

解決策：電子メールゲートウェイで CSN を無効にしてから、もう一度有効にします。

Advanced Phishing Protection ログの使用

Advanced Phishing Protection のログには、Cisco Advanced Phishing Protection クラウドサービスに関連する情報が記録されます。ほとんどの情報は [情報（Info）] または [クリティカル（Critical）] レベルです。

Advanced Phishing Protection のデータログのエント例：

- この例では、サービスが期限切れになったため、電子メールゲートウェイが Cisco Advanced Phishing Protection クラウドサービスにメッセージヘッダーを転送できなかったことが、ログに示されています。

  ```
  Wed May 6 18:21:40 2020 Info: eaas : You cannot
  forward the MID [877] Message Headers to Cisco Advanced
  Phishing Protection Cloud Service as the service has
  expired
  ```

- この例では、Cisco Advanced Phishing Protection クラウドサービスが期限切れになり、電子メールゲートウェイで無効になっていることが、ログに示されています。

  ```
  Wed May 6 18:21:40 2020 Info: eaas : Cisco
  Advanced Phishing Protection Cloud Service has expired
  and is disabled. Contact your Cisco Account manager to
  renew the service and then enable it.
  ```

  解決策：シスコアカウントマネージャに連絡して、サービスを更新してから有効にします。

- この例では、Cisco Advanced Phishing Protection クラウドサービスが特定の日付に期限切れになることが、ログで示されています。

  ```
  Fri May 8 04:50:26 2020 Info: eaas : Cisco
  Advanced Phishing Protection Cloud Service expires on
  2020-05-10 07:00:00. You need to contact your Cisco Account
  manager to renew the service.
  ```

  解決策：シスコアカウントマネージャに連絡して、サービスを更新します。

監査ログの使用

監査ログで認証、許可、アカウンティングのイベント（AAA：Authentication、Authorization、および Accounting）を記録します。ほとんどの情報は、デバッグレベルまたはトレースレベルです。

監査ログエントリの例：

- この例では、ユーザ（admin など）が次の場合にログが表示されます。
  - 電子メールゲートウェイの Web インターフェイスにログインする必要があります。

- 電子メールゲートウェイの Web インターフェイスからログアウトしました。

```
Tue Aug 25 12:33:17 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Destination IP:
192.168.2.2,
Event: Successful login
Tue Aug 25 12:33:17 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: Session established
 successfully
Tue Aug 25 12:33:58 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: User logged out
Tue Aug 25 12:33:58 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: Session terminated
```

- この例では、ユーザー（admin）が `logconfig` CLI コマンドを入力したことがログに示されています。

```
Thu Oct  8 13:33:38 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
 User: admin,
Source IP: 192.168.1.1, Event: User input was 'logconfig'
Thu Oct  8 13:33:46 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
 User: admin,
Source IP: 192.168.1.1, Event: User input was 'Enter'
```

- この例では、ユーザー（admin）が電子メールゲートウェイのレガシー Web インターフェイスで GUI ページを表示したことがログに示されています。

```
Thu Oct  8 13:35:07 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /network/dns, Event: User visited the web page.
Thu Oct  8 13:35:13 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /system_administration/sslconfig, Event: User
visited the web page.
Thu Oct  8 13:35:24 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /monitor/mail_reports/threatfeeds_report, Event:
User visited the web page.
```

- この例では、新しいユーザ（admin）が Web インターフェイスを使用して電子メールゲートウェイに追加されても、変更はコミットされていないことがログに示されています。

```
Thu Oct  8 13:36:30 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /system_administration/access/users, Event: Added
 user "admin" and changes
will reflect after commit.
Thu Oct  8 13:37:22 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /system_administration/access/users, Event: Deleted
 user "admin" and changes
will reflect after commit.
```

- この例では、電子メールゲートウェイの Web インターフェイスでコミットされなかったすべての変更がユーザ（admin）によって破棄されたことがログに示されています。

```
Thu Oct  8 13:39:44 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /commit, Event: User discarded all uncommitted
changes.
```

- この例では、ユーザ（adminなど）がCLIを介してコミットされなかったすべての変更を破棄したことがログに示されています。

```
Thu Oct  8 13:41:38 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
 User: admin,
Source IP: 192.168.1.1, Event: User discarded all uncommitted changes.
```

- この例では、ユーザ（adminなど）がWeb UIセッションタイムアウトの設定を変更したことがログに示されています。

（注） 電子メールゲートウェイで行われた設定変更の詳細を表示するには、設定履歴ログを表示するか、監査ログのデバッグモードを有効にします。

```
Thu Oct  8 13:45:46 2020 Info: Appliance: mail1.example.com, User: admin,
Event: The following configuration changes were commited with comment - 'N/A'
Thu Oct  8 13:45:46 2020 Info: * [standalone] Number of seconds before the Web UI
session times out.
```

- この例では、認証に失敗したため、AsyncOS APIがログサブスクリプションを取得できなかったことがログに示されています。

```
Thu Oct  8 13:52:28 2020 Debug: 08/Oct/2020 13:52:28 +0000 Error - Code: 401,
Details: Unauthorized (No permission -- see authorization schemes)
Thu Oct  8 13:52:28 2020 Info: Appliance: mail1.example.com, Interaction Mode: API,

User: admin, Role: Role Not Available, Source IP: 192.168.1.1, Destination IP:
192.168.2.2,
Location: GET /esa/api/v2.0/config/logs/subscriptions/ HTTP/1.0, Event: User is not
 valid.
```

- この例では、認証に成功したため、AsyncOS APIがログサブスクリプションを取得できたことがログに示されています。

```
Thu Oct  8 13:52:37 2020 Info: Appliance: mail1.example.com, Interaction Mode: API,

User: admin, Role: Administrator, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,

Location: GET /esa/api/v2.0/config/logs/subscriptions/ HTTP/1.0, Event: API Access
Success.
```

- この例では、ログに次の内容が表示されています。
  - CLIを使用して電子メールゲートウェイに新しいユーザ（admin）が追加されましたが、変更はコミットされませんでした。
  - 既存のユーザアカウントの詳細は、CLIを使用して電子メールゲートウェイで更新されましたが、変更はコミットされませんでした。

```
Thu Oct  8 13:42:48 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,

User: admin, Source IP: 192.168.1.1, Event: Added user "hops" and changes will reflect
 after commit
Thu Oct  8 13:43:26 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
 User: admin,
```

```
Source IP: 192.168.1.1, Event: Updated user "hops" and changes will reflect after
commit
```

- この例では、ユーザー（admin）が電子メールゲートウェイの新しい Web インターフェイスでメッセージトラッキング検索を実行したことがログに示されています。

```
Mon Oct 12 04:04:47 2020 Info: Appliance: mail1.example.com, Interaction Mode: API,
 User: admin,
Role: Administrator, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,
Location: GET
/esa/api/v2.0/message-tracking/messages?startDate=2020-10-12T00:00:00.000Z
&endDate=2020-10-12T04:13:00.000Z&ciscoHost=All_Hosts&searchOption=messages&offset=0&limit=100
 HTTP/1.0,
Event: API Access Success.
```

（注） 電子メールゲートウェイの新しいWebインターフェイスで実行するアクション（トラッキング、レポート、隔離の検索など）は、これらのアクションに使用される対応する API に基づき、ログとして記録されます。

CSA ログの使用

Cisco Secure Awareness クラウドサービスの情報はメールログに記録されます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

Cisco Secure Awareness ログエントリの例：

- この例では、無効なトークンが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Tue Oct 13 10:12:59 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
of an invalid token.
```

解決策：Cisco Secure Awareness クラウドサービスから有効な認証トークンを取得してください。

- この例では、接続エラーが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
of a connection error.
```

解決策：電子メールゲートウェイを Cisco Secure Awareness クラウドサービスに接続するために使用するファイアウォール設定を確認します。

- この例では、内部サーバエラーが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
of an internal server error.
```

解決策：詳細については、シスコ テクニカル サポートにお問い合わせください。

- この例では、SSL 証明書の検証の失敗が原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 11:02:46 2020 Warning: CSA:
 The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
the SSL certificate verification failed.
```

解決策：必要なプロキシサーバの CA 証明書を電子メールゲートウェイのカスタム認証局リストに追加します。

- この例では、プロキシ認証の失敗が原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 11:09:48 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed
because the proxy authentication failed.
```

解決策：電子メールゲートウェイでプロキシサーバが正しい認証ログイン情報を使用して設定されているかどうかを確認します。

- この例では、Cisco Secure Awareness クラウドサービスでレポート API が有効になっていなかったことが原因で、Cisco Secure Awareness クラウドサービスへの要求が失敗したことがログに示されています。

```
Mon Aug 17 15:35:42 2020 Warning: CSA:
The download of the Repeat Clickers list failed.
A request to the CSA cloud service failed because
the Report API was not enabled on the CSA cloud service
```

解決策：Cisco Secure Awareness クラウドサービスの [環境（Environment）] > [設定（Settings）] > [レポートAPI（Report API）] タブで [レポートAPIを有効にする（Enable Report API）] チェックボックスをオンにします。

- この例では、Cisco Secure Awareness 機能が特定の日付で期限切れになることがログに示されています。

```
2020-10-15 08:00:11,968 INFO csa The Cisco Security
Awareness feature expires on 2029-12-28T23:59:59Z. You need to
contact your Cisco Account Manager to renew the license.
```

解決策：シスコアカウントマネージャに連絡して、ライセンスを更新します。

- この例では、Cisco Secure Awareness 機能のライセンスの有効期限が切れており、電子メールゲートウェイでこの機能が無効になっていることがログに示されています。

```
2020-10-27 13:33:21,714 CRITICAL csa The Cisco Security
Awareness feature license has expired, and the feature is
disabled on your email gateway. Contact your Cisco Account Manager
to renew the license.
```

解決策：シスコアカウントマネージャに連絡して、ライセンスを更新します。

- この例では、ダウンロードされたリピートクリッカーリストが空であることがログに示されています。

```
Tue Oct 13 10:10:18 2020 Info: CSA: The downloaded
Repeat Clickers list is empty.
```

解決策：Cisco Secure Awareness クラウドサービスでシミュレートされたフィッシングメッセージを作成し、組織内の受信者に送信します。

- この例では、ダウンロード試行の最大数に達したため、Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Fri Oct 16 05:22:08 2020 Warning: CSA: The download
of the Repeat Clickers list from the Cisco Security Awareness
cloud service failed because you have reached the maximum
number of attempts.
```

解決策：Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードする試行回数を増やすには、シスコサポートに連絡してください。

修復ログの使用

修復ログには、AMP レトロスペクティブ脅威判定および URL レトロスペクティブ判定に基づいた、修復ステータス、実行されたアクション、エラーなどに関連する情報が含まれています。

修復ログエントリの例：

- この例では、メッセージがメールボックスで見つからなかったため、メールゲートウェイが URL レトロスペクティブ判定に基づいてメールボックスからのメッセージを修復できなかったことがログに示されています。

```
MID: 35 No messages in recipient's secondcloud@mar-esa.com
mailbox matched the criteria for which remediation was initiated due to
URL retrospection.
```

解決策：

-
  - メッセージが配信され、ユーザーのメールボックスに存在するかどうかを確認します。
  - 電子メールゲートウェイと Exchange Online サービスの接続をテストします。アカウント プロファイルの作成 を参照してください。
  - 「電子メールゲートウェイと Exchange Online サービスおよび Exchange オンプレミス サービス間の接続の問題が検出されました。（Connectivity Issues Between Appliance and Exchange online and Exchange on-premise Services Detected.）」というアラートを受信しているかどうかを確認します。アラート を参照してください。

Email Cloud Scanner ログの使用

Email Cloud Scanner ログには、URL レトロスペクティブポーリングおよび URL 修復サービスに関する情報が含まれています。ほとんどの情報は[情報（Info）]または[デバッグ（Debug）]レベルです。

Email Cloud Scanner のログエントリの例

- この例では、ログは、無効なトークンが原因でクラウドクエリが失敗したことを示しています。

```
Fri Feb 11 10:51:51 2022 Warning: ECS: Cloud query failed.
'Invalid token.'
```

解決策：詳細については、シスコ テクニカル サポートにお問い合わせください。

- この例では、登録が完了しなかったためにクラウドクエリが失敗したことがログに示されています。

```
Fri Feb 11 12:11:11 2022 Warning: ECS: Cloud query failed.
'Registration not complete.'
```

解決策：詳細については、シスコ テクニカル サポートにお問い合わせください。

- この例では、ログは、不正なリクエストが原因でクラウドクエリが失敗したことを示しています。

```
Fri Feb 11 10:56:05 2022 Warning: ECS: Cloud query failed.
'Received bad request with error: {\n  "message": "Bad Request"\n}'
```

解決策：詳細については、シスコ テクニカル サポートにお問い合わせください。

ログ サブスクリプション

ログ サブスクリプションの設定

電子メールゲートウェイでは、既存のログサブスクリプションを削除しないようにすることを推奨します。

[システム管理（System Administration）]の[ログサブスクリプション（Log Subscriptions）]ページ（または CLI の **logconfig** コマンド）を使用して、ログ サブスクリプションを設定します。ログ サブスクリプションによって、エラーを含む AsyncOS アクティビティの情報を保存するログ ファイルが作成されます。ログ サブスクリプションは、取得されるか、または別のコンピュータに配信（プッシュ）されるかのどちらかです。一般に、ログ サブスクリプションには次の属性があります。

表 *32 :* ログ ファイルの属性

属性	説明
ログタイプ（Log type）	記録される情報のタイプと、ログサブスクリプションの形式を定義します。詳細については、表「ログ タイプ」を参照してください。
ログ名（Log Name）	今後の参照に使用するログ サブスクリプションのニックネーム。
ログ フィールド（Log Fields）	特定のメッセージの統合イベント ログ行に含める必要があるログ フィールドを選択します。 （注） [シリアル番号（Serial Number）]および[MID]ログ フィールドはデフォルトで選択されており、これらの選択を解除することはできません。 （注） このフィールドは、ログ タイプが統合イベント ログのログ サブスクリプションを設定する場合にのみ適用されます。
ファイル名（File Name）	ディスクに書き込むときのファイルの物理名に使用されます。複数の電子メールゲートウェイを使用している場合、ログファイルを生成したシステムを識別するため、ログファイル名を固有にする必要があります。
ファイルサイズ別ロールオーバー（Rollover by File Size）	ファイルの最大サイズ。このサイズに到達すると、ローリング オーバーされます。
時刻によりロールオーバー（Rollover by Time）	ファイルのロールオーバーの時間間隔を設定します。
レート制限（Rate Limit）	指定した時間範囲（秒単位）内での、ログファイルのログ記録されるイベントの最大数を設定します。 デフォルトの時間範囲の値は 10 秒です。
ログ レベル（Log level）	ログ サブスクリプションごとに詳細のレベルを設定します。
取得方法（Retrieval method）	ログサブスクリプションが電子メールゲートウェイから取得される方法を定義します。

ログ レベル

ログ レベルによって、ログに送信される情報量が決定します。ログには、5つの詳細レベルのいずれかを設定できます。詳細レベルを高くするほど大きいログ ファイルが作成され、システムのパフォーマンスが低下します。詳細レベルの高い設定には、詳細レベルの低い設定に保持

されるすべてのメッセージと、その他のメッセージも含まれます。詳細レベルを上げるほど、システムのパフォーマンスは低下します。

（注） ログ レベルは、すべてのメール ログ タイプに対して選択できます。

表 *33*：ログ レベル

ログ レベル	説明
クリティカル	詳細レベルの最も低い設定。エラーだけがログに記録されます。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできませんが、ログ ファイルがすぐには最大サイズに達しなくなります。このログ レベルは、syslog レベルの「Alert」と同等です。
警告	システムによって作成されたすべてのエラーと警告。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできません。このログ レベルは、syslog レベル「Warning」と同等です。
情報	情報設定では、システムの秒単位の動作がキャプチャされます。たとえば、接続のオープンや配信試行などです。Information レベルは、ログに推奨される設定です。このログ レベルは、syslog レベル「Info」と同等です。
デバッグ（Debug）	エラーの原因を調べるときは、Debug ログ レベルを使用します。この設定は一時的に使用し、後でデフォルト レベルに戻します。このログ レベルは、syslog レベルの [デバッグ（Debug）] と同等です。
トレース（Trace）	Trace ログ レベルは、開発者にのみ推奨されます。このレベルを使用すると、システムのパフォーマンスが大きく低下するので、推奨されません。このログ レベルは、syslog レベルの [デバッグ（Debug）] と同等です。

GUI でのログ サブスクリプションの作成

手順

ステップ 1 [システム管理（System Administration）]> [ログサブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 [ログサブスクリプションを追加（Add Log Subscription）] をクリックします。

ステップ 3 ログ タイプを選択し、ログ名（ログ ディレクトリ用）とログ ファイル自体の名前を入力します。

ステップ 4 （統合イベント ログのみ）特定のメッセージのログ行に含める必要があるログ フィールドを選択します。

ステップ 5 AsyncOS がログ ファイルをロールオーバーする前の最大ファイル サイズ、およびロールオーバー間の時間間隔を指定します。ファイルのロールオーバーの詳細については、ログサブスクリプションのロールオーバー （84 ページ）を参照してください。

ステップ 6 ログ レベルを選択します。使用可能なオプションは、[クリティカル（Critical）]、[警告（Warning）]、[情報（Information）]、[デバッグ（Debug）]、または [トレース（Trace）] です。

ステップ 7 ログの取得方法を設定します。

ステップ 8 変更を送信し、保存します。

ログ サブスクリプションの編集

手順

ステップ 1 [システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 [ログ設定（Log Settings）] カラムでログの名前をクリックします。

ステップ 3 ログ サブスクリプションを変更します。

ステップ 4 変更を送信し、保存します。

ロギングのグローバル設定

システムは、テキスト メール ログおよびステータス ログ内にシステムの測定を定期的に記録します。[システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] ページの [グローバル設定（Global Settings）] セクションにある [設定を編集（Edit Settings）] ボタン（または、CLI の `logconfig -> setup` コマンド）を使用して、次の情報を設定します。

- システムの測定頻度。これは、システムが測定を記録するまで待機する時間（秒単位）です。
- メッセージ ID ヘッダーを記録するかどうか。
- リモート応答ステータス コードを記録するかどうか。
- 元のメッセージのサブジェクト ヘッダーを記録するかどうか。
- メッセージごとにログに記録するヘッダーのリスト。

すべてのログには、次の 3 つのデータを任意で記録できます。

1. メッセージ ID

   このオプションを設定すると、可能な場合はすべてのメッセージのメッセージ ID ヘッダーがログに記録されます。このメッセージ ID は、受信したメッセージから取得される場合と、AsyncOS 自体で生成される場合があります。次に例を示します。

```
Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
```

2. リモート応答

   このオプションを設定すると、可能な場合はすべてのメッセージのリモート応答ステータス コードがログに記録されます。次に例を示します。

```
Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
```

   リモート応答文字列は、SMTP カンバセーション配信時の DATA コマンドへの応答後に受信される、人が読み取ることのできるテキストです。この例では、接続ホストが data コマンドを実行した後のリモート応答が、「queued as 9C8B425DA7」となります。

```
[...]

250 ok hostname

250 Ok: queued as 9C8B425DA7
```

   文字列の先頭にある空白や句読点（および、250 応答の場合は OK 文字）は除去されます。文字列の末尾については、空白だけが除去されます。たとえば、電子メールゲートウェイはデフォルトで、DATA コマンドに対して「250 Ok: Message MID accepted」という文字列で応答します。したがって、リモートホストが別の 電子メールゲートウェイである場合は、文字列「Message MID accepted」がログに記録されます。

3. オリジナルの件名

   このオプションをイネーブルにすると、各メッセージの元のサブジェクト ヘッダーがログに記録されます。

```
Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2

Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>

Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>

Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'

Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

メッセージ ヘッダーのロギング

場合によっては、メッセージがシステムを通過するときに、メッセージのヘッダーの存在と内容を記録する必要があります。[ログサブスクリプションのグローバル設定（Log Subscriptions Global Settings）] ページ（または、CLI の logconfig -> logheaders サブコマンド）に、記録するヘッダーを指定します。電子メールゲートウェイは、指定されたメッセージヘッダーをテキストメールログ、配信ログ、およびバウンスログに記録します。ヘッダーが存在する場合、システムはヘッダーの名前と値を記録します。ヘッダーが存在しない場合は、ログに何も記録されません。

（注） システムは、ロギングに指定したヘッダーに関係なく、メッセージの記録処理中に随時、メッセージに存在するすべてのヘッダーを評価します。

SMTP プロトコルについての RFC は、http://www.faqs.org/rfcs/rfc2821.html にあります。この RFC には、ユーザ定義のヘッダーが規定されています。

logheaders コマンドを使用してヘッダーをログに記録するように設定している場合、ヘッダー情報は配信情報の後に表示されます。

表 *34 :* ヘッダーのログ（*Log Headers*）

ヘッダー名	ヘッダーの名前
値	ログに記録されるヘッダーの内容

たとえば、ログに記録するヘッダーとして「date, x-subject」を指定すると、メールログに次の行が表示されます。

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0]
[('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

統合イベントログのメッセージヘッダーのロギング

統合イベントログにメッセージヘッダーの存在と内容を記録する必要があるシナリオでは、[ログサブスクリプションのグローバル設定（Log Subscriptions Global Setting）] ページに記録するカスタムログヘッダーを指定できます（または CLI の `logconfig > ceflogheaders` サブコマンドを使用）。電子メールゲートウェイは、指定されたカスタムログヘッダーを統合イベントログに記録します。ヘッダーが存在する場合、システムはヘッダーの名前と値を記録します。ヘッダーが存在しない場合は、ログに何も記録されません。

（注） 統合イベントログに追加できるカスタムログヘッダーは 25 個だけです。

[選択したログフィールド（Selected Log Fields）] にある [カスタムログヘッダー（Custom Log Headers）] を使用して [統合イベントログ（Consolidated Event Logs）] ログサブスクリプションを設定すると、CEF ログエントリが [統合イベントログ（Consolidated Event Logs）] に表示されます。

（注） 電子メールゲートウェイでは、Syslog プッシュ方式で統合イベントログを使用する場合、CEF ログ行に 65535 文字の制限があります。外部の SIEM ソリューションには、CEF ログファイルに許可される文字数に制限が定義されている場合もあります。メールゲートウェイと SIEM ソリューションで許可されている文字数に基づいて、ログに記録されるヘッダーと統合イベントログ サブスクリプション フィールドを適切に設定してください。

表 *35 :* ヘッダーのログ（*Log Headers*）

ヘッダー名	ヘッダーの名前
値	ログに記録されるヘッダーの内容

たとえば、ログに記録するヘッダーとして「date, x-subject」を指定すると、[統合イベントログ（Consolidated Event Logs）] に次の行が表示されます。

```
Thu Jun 30 08:04:50 2022: CEF:0|Cisco|C100V Email Security Virtual Appliance|14.0.0-657
|ESA_CONSOLIDATED_LOG_EVENT|Consolidated Log
Event|5|deviceExternalId=42127C7DDEE76852677B-F80CE8074CD3
ESALogHeaders={'reply-to': ['test@esa.com ', 'newsletter@esa.com'], 'from':
['any@esa.com']}
```

GUI を使用したロギングのグローバル設定の構成

手順

ステップ 1 [システム管理（System Administration）]>[ログサブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 [グローバル設定（Global Settings）] セクションまでスクロールします。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 システム測定頻度、メール ログにメッセージ ID ヘッダーを加えるかどうか、リモート応答を加えるかどうか、および各メッセージの元のサブジェクトヘッダーを加えるかどうかを含めた情報を指定します。

ステップ 5 ログに加えるその他のヘッダーを入力します。

ステップ 6 変更を送信し、保存します。

ログ サブスクリプションのロールオーバー

電子メールゲートウェイ上のログファイルが大きくなりすぎないようにするために、ログファイルがユーザ指定の最大ファイルサイズまたは時間間隔に達すると、AsyncOS は「ロールオーバー」を実行してログファイルをアーカイブし、着信するログデータ用の新しいファイルを作

成します。ログサブスクリプション用に定義された取得方法に基づいて、古いログファイルは取得のために電子メールゲートウェイ上に保管されるか、または外部のコンピュータに配信されます。電子メールゲートウェイからログファイルを取得する方法の詳細については、ログ取得方法 （12 ページ）を参照してください。

AsyncOS は、ログ ファイルをロールオーバーするときに次のアクションを実行します。

- ロールオーバーのタイムスタンプと、saved（保存済み）を示す文字「**s**」拡張子を使用して、現在のログ ファイルの名前を変更します。
- 新しいログ ファイルを作成し、「**current**」の拡張子を使用して、そのファイルを最新として指定します。
- 新しく保存されたログ ファイルをリモート ホストに転送します（プッシュ ベースの取得方法を使用している場合）。
- 同じサブスクリプションから、以前に失敗したログ ファイルをすべて転送します（プッシュ ベースの取得方法を使用している場合）。
- 保存すべきファイルの総数を超えた場合は、ログ サブスクリプション内の最も古いファイルを削除します（ポーリング ベースの取得方法を使用している場合）。

  ログ サブスクリプションのロールオーバーの設定は、GUI の [システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] ページ、または CLI の logconfig コマンドを使用して、サブスクリプションを作成または編集するときに定義します。ログ ファイルのロールオーバーをトリガーするために使用できる 2 つの設定は次のとおりです。

- 最大ファイル サイズ。
- 時間間隔。

ファイル サイズによるロールオーバー

AsyncOS は、ログ ファイルで使用されるディスク領域が多くなりすぎないようにするために、最大ファイル サイズに達したログ ファイルをロールオーバーします。ロールオーバーのための最大ファイル サイズを定義する場合は、メガバイトを示す m とキロバイトを示す k のサフィックスを使用します。たとえば、ログ ファイルが 10 MB に達したら AsyncOS によってロールオーバーされるようにする場合は、「10m」と入力します。

時刻によりロールオーバー

ロールオーバーを定期的に実行されるようにスケジュールする場合は、次のいずれかの時間間隔を選択できます。

- **[なし（None）]**。AsyncOS は、ログ ファイルが最大ファイル サイズに達した場合にのみロールオーバーを実行します。
- **[カスタム時間間隔（Custom Time Interval）]**。AsyncOS は、以前のロールオーバーから指定された時間が経過した後にロールオーバーを実行します。スケジュール設定されたロールオーバーのためのカスタムの時間間隔を作成するには、d、h、および m をサフィックスとして使用して、ロールオーバー間の日数、時間数、および分数を入力します。

- **[日次ロールオーバー（Daily Rollover）]。**AsyncOS は、毎日指定された時刻にロールオーバーを実行します。日単位のロールオーバーを選択した場合は、24 時間形式（HH:MM）を使用して、AsyncOS がロールオーバーを実行する時刻を入力します。

  GUI では、[日次ロールオーバー（Daily Rollover）] オプションのみが提供されます。CLI の logconfig コマンドを使用して日単位のロールオーバーを設定する場合は、[週次ロールオーバー（Weekly Rollover）] オプションを選択し、アスタリスク（*）を使用して AsyncOS がすべての曜日にロールオーバーを実行することを指定します。

- **[週次ロールオーバー（Weekly Rollover）]。**AsyncOS は、1 つ以上の曜日の指定された時刻にロールオーバーを実行します。たとえば、毎週水曜日と金曜日の午前 0：00 にログファイルをロールオーバーするように AsyncOS を設定できます。週単位のロールオーバーを設定するには、ロールオーバーを実行する曜日と 24 時間形式（HH:MM）の時刻を選択します。

  CLI を使用している場合は、ダッシュ（-）を使用して日の範囲を指定するか、アスタリスク（*）を使用してすべての曜日を指定するか、またはカンマ（,）を使用して複数の日と時刻を区切ることができます。

  次の表に、CLI を使用して、水曜日と金曜日の午前 0:00（00:00）にログ サブスクリプションのファイルをロールオーバーする方法を示します。

表 *36 : CLI* での週単位のログ ロールオーバーの設定

`Do you want to configure time-based log files rollover? [N]> y`
`Configure log rollover settings:`
`1. Custom time interval.`
`2. Weekly rollover.`
`[1]> 2`
`1. Monday`
`2. Tuesday`
`3. Wednesday`
`4. Thursday`
`5. Friday`
`6. Saturday`

```
7. Sunday

Choose the day of week to roll over the log files.  Separate multiple days with comma,

or use "*" to specify every day of a week.
Also you can use dash to specify a range like "1-5":

[]> 3, 5

Enter the time of day to rollover log files in 24-hour format (HH:MM).
You can specify hour as "*" to match every hour, the same for minutes.
Separate multiple times of day with comma:

[]> 00:00
```

オンデマンドでのログ サブスクリプションのロールオーバー

GUI を使用してログ サブスクリプションをただちにロールオーバーするには、次の手順を実行します。

手順

ステップ 1 [システム管理（System Administration）]>[ログサブスクリプション（Log Subscriptions）]ページで、ロール オーバーするログの右側のチェックボックスをオンにします。

ステップ 2 任意で、[すべて（All）]チェックボックスをオンにして、すべてのログをロールオーバー対象として選択できます。

ステップ 3 ロールオーバー対象として1つまたは複数のログを選択すると、[今すぐロールオーバー（Rollover Now）]ボタンがイネーブルになります。[今すぐロールオーバー（Rollover Now）]ボタンをクリックして、選択したログをロール オーバーします。

GUI での最近のログ エントリの表示

はじめる前に

GUI を介してログを表示するには、管理インターフェイスで HTTP または HTTPS サービスをイネーブルにしておく必要があります。

手順

ステップ 1 [システム管理（System Administration）]>[ログサブスクリプション（Log Subscriptions）]を選択します。

ステップ 2 テーブルの [ログファイル（Log Files）] カラムでログ サブスクリプションを選択します。
ステップ 3 サインインします。
ステップ 4 ログ ファイルのいずれかを選択して、ブラウザに表示するか、またはディスクに保存します。

CLI での最近のログ エントリの表示（tail コマンド）

AsyncOS は、電子メールゲートウェイに設定されたログの最新エントリを表示する tail コマンドをサポートしています。tail コマンドを実行して現在設定されているログの番号を選択すると、そのログが表示されます。Ctrl+ C を押して、tail コマンドを終了します。

例

次の例では、tail コマンドを使用してシステム ログを表示します。（このログは commit コマンドによるユーザのコメントを特に追跡します）。tail コマンドは、tail mail_logs のように、表示するログの名前をパラメータとして指定することもできます。

```
mail3.example.com> tail

Currently configured logs:

1. "antispam" Type: "Anti-Spam Logs" Retrieval: Manual Download

2. "antivirus" Type: "Anti-Virus Logs" Retrieval: Manual Download

3. "asarchive" Type: "Anti-Spam Archive" Retrieval: Manual Download

4. "authentication" Type: "Authentication Logs" Retrieval: Manual Download

5. "avarchive" Type: "Anti-Virus Archive" Retrieval: Manual Download

6. "bounces" Type: "Bounce Logs" Retrieval: Manual Download

7. "cli_logs" Type: "CLI Audit Logs" Retrieval: Manual Download

8. "encryption" Type: "Encryption Logs" Retrieval: Manual Download

9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download

10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: Manual Download

11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: Manual Download

12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: Manual Download

13. "gui_logs" Type: "HTTP Logs" Retrieval: Manual Download

14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download

15. "reportd_logs" Type: "Reporting Logs" Retrieval: Manual Download

16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: Manual Download

17. "scanning" Type: "Scanning Logs" Retrieval: Manual Download

18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: Manual Download
```

```
19. "sntpd_logs" Type: "NTP logs" Retrieval: Manual Download

20. "status" Type: "Status Logs" Retrieval: Manual Download

21. "system_logs" Type: "System Logs" Retrieval: Manual Download

22. "trackerd_logs" Type: "Tracking Logs" Retrieval: Manual Download

23. "updater_logs" Type: "Updater Logs" Retrieval: Manual Download


Enter the number of the log you wish to tail.

[]> 19

Press Ctrl-C to stop.

Mon Feb 21 12:25:10 2011 Info: PID 274: User system commit changes: Automated Update for
Quarantine Delivery Host

Mon Feb 21 23:18:10 2011 Info: PID 19626: User admin commit changes:

Mon Feb 21 23:18:10 2011 Info: PID 274: User system commit changes: Updated filter logs
config

Mon Feb 21 23:46:06 2011 Info: PID 25696: User admin commit changes: Receiving
suspended.

^Cmail3.example.com>
```

ホスト キーの設定

`logconfig -> hostkeyconfig` サブコマンドを使用して、電子メールゲートウェイから他のサーバにログをプッシュするときに、SSH で使用するホストキーを管理します。SSH サーバには、秘密キーと公開キーの 2 つのホスト キーが必要です。秘密ホスト キーは SSH サーバにあり、リモート マシンから読み取ることはできません。公開ホスト キーは、SSH サーバと対話する必要のある任意のクライアント マシンに配信されます。

（注） ユーザ キーを管理するには、セキュア シェル（SSH）キーの管理を参照してください。

`hostkeyconfig` サブコマンドによって、次の機能が実行されます。

表 *37*：ホスト キーの管理：サブコマンドのリスト

コマンド	説明
新規作成（New）	新しいキーを追加します。
編集（Edit）	既存のキーを変更します。

コマンド	説明
削除（Delete）	既存のキーを削除します。
スキャン（Scan）	ホスト キーを自動的にダウンロードします。
印刷（Print）	キーを表示します。
ホスト（Host）	システム ホスト キーを表示します。これは、リモート システムの「known_hosts」ファイルに配置される値です。
フィンガープリント（Fingerprint）	システム ホスト キーのフィンガープリントを表示します。
ユーザ（User）	リモート マシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモート システムの「authorized_keys」ファイルに配置される値です。

次の例では、AsyncOS によってホスト キーがスキャンされ、ホスト用に追加されます。

```
mail3.example.com> logconfig

Currently configured logs:

[ list of logs ]

Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- SETUP - General settings.

- LOGHEADERS - Configure headers to log.

- HOSTKEYCONFIG - Configure SSH host keys.

[]> hostkeyconfig

Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]

Choose the operation you want to perform:

- NEW - Add a new key.

- EDIT - Modify a key.
```

```
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> scan
Please enter the host or IP address to lookup.
[]> mail3.example.com
Choose the ssh protocol type:
1. SSH1:rsa
2. SSH2:rsa
3. SSH2:dsa
4. All
[4]>
SSH2:dsa
mail3.example.com ssh-dss
[ key displayed ]
SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed ]
SSH1:rsa
mail3.example.com 1024 35
[ key displayed ]

Add the preceding host key(s) for mail3.example.com? [Y]>
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]
2. mail3.example.com ssh-rsa [ key displayed ]
3. mail3.example.com 1024 35 [ key displayed ]
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
```

```
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>
Currently configured logs:
[ list of configured logs ]
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>
```

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。