CHAPTER 15

ロギング

ロギングの概要

ログ ファイルには、システムのアクティビティの例外に加えて、通常の操作が記録されます。シスコ コンテンツ セキュリティ アプライアンスのモニタリング、トラブルシューティング、およびシステム パフォーマンスの評価のためにログを使用します。

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、トラッキング 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。

ロギングとレポーティング

ロギング データは、メッセージ フローのデバッグ、基本的な日常の動作に関する情報の確認（FTP 接続の詳細、HTTP ログ ファイルなど）、アーカイブのコンプライアンスの目的に使用します。

このロギング データには、電子メール セキュリティ アプライアンスから直接アクセスすることも、任意の外部 FTP サーバに送信してアーカイブまたは読み取ることもできます。アプライアンスに FTP 接続してログにアクセスすることも、バックアップの目的でプレーン テキストのログを外部サーバにプッシュすることもできます。

レポーティング データを表示するには、アプライアンスのグラフィカル ユーザ インターフェイスの [レポート（Report）] ページを使用します。元データにはアクセスできません。また、シスコのコンテンツセキュリティ管理アプライアンス以外には送信できません。

（注） セキュリティ管理アプライアンスは、Cisco IronPort スパム隔離（ISQ）データの例外を含む、すべてのレポーティングおよびトラッキング情報を取り出します。ISQ データは、ESA から渡されます。

ログの取得

ログ ファイルは、表 15-1 に示すファイル転送プロトコルを使用して取得できます。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、CLI の logconfig コマンドを使用して設定します。

表 15-1　ログ転送プロトコル

FTP ポーリング	このタイプのファイル転送では、リモート FTP クライアントは管理者レベルまたはオペレータ レベルのユーザのユーザ名およびパスワードを使用して、アプライアンスにアクセスし、ログ ファイルを取得します。FTP ポーリング方法を使用するようにログ サブスクリプションを設定する場合は、保持するログ ファイルの最大数を指定する必要があります。最大数に達すると、最も古いファイルが削除されます。
FTP プッシュ	このタイプのファイル転送では、シスコ コンテンツ セキュリティ アプライアンスがリモート コンピュータの 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、ユーザ名、パスワード、およびリモート コンピュータ上の宛先ディレクトリが必要です。ログ ファイルは、設定されたロールオーバー スケジュールに基づいて転送されます。
SCP プッシュ	このタイプのファイル転送では、シスコ コンテンツ セキュリティ アプライアンスがリモート コンピュータの 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、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、ユーザ名、SSH キー、およびリモート コンピュータ上の宛先ディレクトリが必要です。ログ ファイルは、設定されたロールオーバー スケジュールに基づいて転送されます。
Syslog プッシュ	このタイプのファイル転送では、シスコ コンテンツ セキュリティ アプライアンスがリモート 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。Syslog サーバのホスト名を指定し、ログの送信に UDP または TCP を使用する必要があります。使用するポートは 514 です。ログのファシリティは選択できますが、ログ タイプのデフォルトはドロップダウン メニューであらかじめ選択されています。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。

ファイル名およびディレクトリ構造

AsyncOS はログ サブスクリプションで指定したログ名に基づいて、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。ディレクトリ内のログのファイル名は、ログ サブスクリプションで指定されたファイル名、ログ ファイルが開始されたタイムスタンプ、および単一文字のステータス コードで構成されています。次に、ディレクトリおよびファイル名の規則の例を示します。

```
/<Log_Name>/<Log_Filename>.@<timestamp>.<statuscode>
```

ステータス コードは、.c（「current（現在）」の意味）、または .s（「saved（保存済み）」の意味）です。保存済みのステータスのログ ファイルのみを転送する必要があります。

ログのロールオーバーおよび転送スケジュール

ログ サブスクリプションを作成するときに、ログのロールオーバー、古いファイルの転送、および新しいファイルの作成のトリガーを指定します。

次のトリガーのいずれかを選択します。

- ファイル サイズ
- 時間
  - 指定した間隔で（秒、分、時間、または日数）

値を入力するときは、画面の例に従います。

2 時間半など、複合間隔を入力するには、例 2h30m に従います。

または

- 毎日、指定した時刻に

または

- 選択した週の曜日の指定した時刻に

時刻を指定する場合は、24 時間形式を使用します。たとえば 11pm は 23:00 です。

1 日に複数のロールオーバー時間をスケジュール設定するには、時間をカンマで区切ります。たとえば、深夜と正午にログをロールオーバーするには、00:00, 12:00 と入力します。

アスタリスク（*）をワイルドカードとして使用できます。
たとえば、正確に毎時および 30 分ごとにログをロールオーバーするには、*:00, *:30 と入力します。

指定した制限に達すると（またはサイズおよび時間の両方に基づいた制限を設定している場合は最初の制限に達すると）、ログ ファイルがロールオーバーされます。FTP ポーリング転送メカニズムに基づいたログ サブスクリプションでは、ファイルが作成されると、それらのファイルが取得されるか、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、アプライアンスの FTP ディレクトリにそれらのファイルが保存されます。

（注） 次の制限に達したときにロールオーバーが実行中の場合、新しいロールオーバーはスキップされます。エラーが記録され、アラートが送信されます。

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（ログの開始時からの秒数）が含まれています。

- メール ログ
- セーフリスト/ブロックリスト ログ
- システム ログ

デフォルトでイネーブルになるログ

セキュリティ管理アプライアンスには、有効な次のログ サブスクリプションが事前設定されています。

表 15-2　事前設定されたログ サブスクリプション

ログ名	ログ タイプ	取得方法
cli_logs	CLI 監査ログ	FTP ポーリング
euq_logs	Cisco IronPort スパム隔離ログ	FTP ポーリング
euqgui_logs	Cisco IronPort スパム隔離 GUI ログ	FTP ポーリング
gui_logs	HTTP ログ	FTP ポーリング
mail_logs	Cisco IronPort テキスト メール ログ	FTP ポーリング
reportd_logs	レポーティング ログ	FTP ポーリング
reportqueryd_logs	レポーティング クエリー ログ	FTP ポーリング

表 15-2　事前設定されたログ サブスクリプション （続き）

ログ名	ログ タイプ	取得方法
slbld_logs	セーフリスト/ブロックリスト ログ	FTP ポーリング
smad_logs	SMA ログ	FTP ポーリング
system_logs	システム ログ	FTP ポーリング
trackerd_logs	トラッキング ログ	FTP ポーリング

事前定義されているすべてのログ サブスクリプションでは、ログ レベルが Information に設定されています。ログ レベルの詳細については、「ログ レベルの設定」（P.15-22）を参照してください。

適用されているライセンス キーによっては、追加のログ サブスクリプションを設定できます。ログ サブスクリプションの作成および編集については、「ログ サブスクリプション」（P.15-21）を参照してください。

ログ タイプ

ログ タイプの概要

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、およびファイル サイズや宛先情報などのその他の特性に関連付けます。コンフィギュレーション履歴ログ以外のすべてのログ 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 タイプによってログに記録されるデータが決まります。ログ サブスクリプションを作成するときにログ タイプを選択します。詳細については、「ログ サブスクリプション」（P.15-21）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 15-3　ログ タイプ

ログ タイプ	説明
認証ログ	認証ログには、ローカルまたは外部認証されたユーザおよびセキュリティ管理アプライアンスへの GUI および CLI の両方のアクセスについて、成功したログインと失敗したログイン試行が記録されます。 外部認証がオンの場合、デバッグおよびより詳細なモードでは、すべての LDAP クエリーがこれらのログに表示されます。
バックアップ ログ	バックアップ ログはバックアップ プロセスを開始から終了まで記録します。 バックアップ スケジューリングに関する情報は、SMA ログ内にあります。
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。
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、どのようなセキュリティ管理アプライアンス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。
FTP サーバ ログ	FTP ログには、インターフェイスでイネーブルになっている 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	GUI ログには、Web インターフェイスでのページ更新の履歴、セッション データ、およびユーザがアクセスしたページが記録されます。GUI ログを使用して、ユーザ アクティビティを追跡することや、GUI でユーザに表示されたエラーを調査することができます。エラー トレースバックは、通常、このログに記録されます。 GUI ログには、SMTP トランザクションに関する情報（たとえば、アプライアンス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。
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 サービスおよびセキュア HTTP 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 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。セッション データ（新規セッション、期限切れセッションなど）、およびグラフィカル ユーザ インターフェイスでアクセスされたページが記録されます。
Haystack ログ	Haystack ログには、データ処理をトラッキングする Web トランザクションが記録されます。
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（メッセージの受信、メッセージの配信試行、接続の開始と終了、メッセージのバウンスなど）に関する情報が記録されます。 メール ログに添付ファイル名が含まれる場合に関する重要な情報については、「トラッキング サービスの概要」（P.6-1）を参照してください。
LDAP デバッグ ログ	[システム管理（System Administration）] > [LDAP] で LDAP を設定している場合は、これらのログを問題のデバッグに使用します。 たとえば、これらのログには、[テスト サーバ（Test Server）] ボタンや [テスト クエリ（Test Queries）] ボタンをクリックした結果が記録されます。 失敗した LDAP 認証の詳細については、認証ログを参照してください。
NTP ログ	NTP ログには、アプライアンスと任意の設定済みネットワーク タイム プロトコル（NTP）サーバとの通信が記録されます。NTP サーバの設定の詳細については、「システム時刻の設定」（P.14-46）を参照してください。

表 15-3　ログ タイプ（続き）

ログ タイプ	説明
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 クエリー ログには、アプライアンスで実行された、レポーティング クエリーに関連付けられたアクションが記録されます。
SMA ログ	SMA ログには、一般的なセキュリティ管理アプライアンスプロセスに関連付けられたアクションが記録されます。集約管理レポート、集約管理トラッキング、Cisco IronPort スパム隔離サービスのプロセスは含まれません。 これらのログには、バックアップ スケジューリングに関する情報が含まれます。
SNMP ログ	SNMP ログには、SNMP ネットワーク管理エンジンに関連するデバッグ メッセージが記録されます。トレースまたはデバッグ モードでは、セキュリティ管理アプライアンスへの SNMP 要求が含まれます。
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。
スパム隔離 GUI ログ	Cisco IronPort スパム隔離 GUI ログには、GUI を介した隔離設定、エンド ユーザ認証、エンド ユーザ アクション（例：電子メールの解放）など、Cisco IronPort スパム隔離 GUI に関連するアクションが記録されます。
スパム隔離ログ	Cisco IronPort スパム隔離ログには、Cisco IronPort 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。
ステータス ログ	ステータス ログには、`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。
システム ログ	システム ログには、ブート情報、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、アプライアンスの状態のトラブルシューティングに役立ちます。
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。
アップデータ ログ	時間帯のアップデートなど、サービス アップデートに関する情報。
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。

ログ タイプの比較

表 15-4 に、各ログ タイプの特徴をまとめます。

表 15-4　ログ タイプの比較

						次の情報を格納					
	トランザクション	ステートレス	テキストとして記録	バイナリとして記録	ヘッダー ロギング	定期的なステータス情報	メッセージ受信情報	配信情報	個々のハードバウンス	個々のソフトバウンス	設定情報
認証ログ	•		•								
バックアップ ログ	•		•								
CLI 監査ログ	•		•			•					
コンフィギュレーション履歴ログ	•		•								•
FTP サーバ ログ	•		•			•					
HTTP ログ	•		•			•					
Haystack ログ	•		•								
テキスト メール ログ	•		•		•	•	•	•	•	•	
LDAP デバッグ ログ	•		•								
NTP ログ	•		•			•					
レポーティング ログ	•		•			•					
レポーティング クエリー ログ	•		•			•					
SMA ログ	•		•			•					
SNMP ログ	•		•								
セーフリスト/ブロックリスト ログ	•		•			•					
スパム隔離 GUI	•		•			•					
スパム隔離	•		•			•					
ステータス ログ		•	•			•					
システム ログ	•		•			•					
トラッキング ログ	•			•	•		•	•	•	•	
アップデータ ログ	•		•								

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、コンフィギュレーション ファイルで構成され、ユーザの名前、ユーザが変更を行った設定の場所の説明、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があります。ユーザが変更をコミットするたびに、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

次のコンフィギュレーション履歴ログの例は、システムにログインできるローカル 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 "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>
```

CLI 監査ログの使用

表 15-5 に、CLI 監査ログに記録される統計情報を示します。

表 15-5　CLI 監査ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
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
========  ==========  =========  ===========  ====\n
admin     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 15-6 に、FTP サーバ ログに記録される統計情報を示します。

表 15-6　FTP サーバ ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
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、ログファイルのステータス情報、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 15-7 に、HTTP ログに記録される統計情報を示します。

表 15-7　HTTP ログに記録される統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
ID	セッション ID。
req	接続元マシンの IP アドレス。
user	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、管理者ユーザによるグラフィカル ユーザ インターフェイスの使用（システム セットアップ 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=190
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
```

Cisco IronPort スパム隔離ログの使用

表 15-8 に、Cisco IronPort スパム隔離ログに記録される統計情報を示します。

表 15-8　Cisco IronPort スパム隔離ログの統計情報

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、実行されたアクション（メッセージの隔離、隔離領域からの解放など）で構成されます。

Cisco IronPort スパム隔離ログの例

次のログの例は、隔離から admin@example.com に 2 個のメッセージ（MID 8298624 と MID 8298625）が解放された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
```

Cisco IronPort スパム隔離 GUI ログの使用

表 15-9 に、Cisco IronPort スパム隔離 GUI ログに記録される統計情報を示します。

表 15-9　Cisco IronPort スパム隔離 GUI 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。

Cisco IronPort 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。

表 15-10　Cisco IronPort スパム隔離 GUI ログの例

```
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
```

Cisco IronPort 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。ステータス情報も、1 分ごとにメール ログに書き込まれます。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、「トラッキング サービスの概要」（P.6-1）を参照してください。

表 15-11 に、テキスト メール ログに表示される情報を示します。

表 15-11　テキスト メール ログの統計情報

統計	説明
ICID	Injection Connection ID（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 です。システムへの 1 つの SMTP 接続で、単一のメッセージまたは多数のメッセージを送信できます。
DCID	Delivery Connection ID（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）。Cisco IronPort 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、Cisco IronPort 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	メッセージ ID。この ID を使用して、メッセージのフローをログで追跡します。
RID	受信者 ID。各メッセージ受信者には、ID が割り当てられます。
New	新規の接続が開始されました。
Start	新規のメッセージが開始されました。

例

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 15-12　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`

前述のログ ファイルを読み取るためのガイドとして、表 15-13 を使用してください。

表 15-13　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。この接続は管理 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、確認応答されました。
6	受信が成功し、受信接続が終了しました。
7	メッセージ配信プロセスが開始されました。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	配信接続が終了しました。

テキスト メール ログ エントリの例

次の例で、さまざまなケースに基づくログ エントリを示します。

メッセージ受信

1 人の受信者に対するメッセージがアプライアンス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の例

```
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アプライアンスにインジェクトされます。配信時に、宛先ホストが *5XX* エラーを返しました。これは、メッセージをどちらの受信者にも配信できなかったことを示します。アプライアンスは、送信者に通知して、キューからそれらの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
```

最終的に正常に配信されるソフト バウンスの例

メッセージがアプライアンス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
```

メッセージ スキャン結果（scanconfig）

次のプロンプトで、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）の動作を scanconfig コマンドを使用して決定した場合、

```
If a message could not be deconstructed into its component parts in order to remove
specified attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[3]>
```

メール ログに以下が表示されます。

scanconfig で、メッセージを分解できない場合に配信するように設定した場合。

```
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
```

scanconfig で、メッセージを分解できない場合にドロップするように設定した場合。

```
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
```

添付ファイルのあるメッセージ

この例では、添付ファイル名の識別をイネーブルにするように、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。

生成またはリライトされたメッセージ

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'
```

（注） 「Rewritten」エントリは、新しい MID の使用を示すログの行の後に表示されます。

Cisco IronPort スパム隔離へのメッセージの送信

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、メッセージにスパムのタグが付けられ、Cisco IronPort 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 Cisco
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
```

NTP ログの使用

表 15-14 に、NTP ログに記録される統計情報を示します。

表 15-14　NTP ログに記録される統計情報

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、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、アプライアンスから 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
```

レポーティング ログの使用

表 15-15 に、レポーティング ログに記録される統計情報を示します。

表 15-15　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アプライアンスを示しています。

```
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

表 15-16 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 15-16　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 クエリー ログの例は、アプライアンスによって、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 クエリー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_CONTEN
T_FILTER', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECI
PIENTS_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_ascendin
g=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_SUMM
ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range 2007-08-29 to
2007-10-01 with key constra
ints 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.
```

セーフリスト/ブロックリスト ログの使用

表 15-17 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 15-17　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、アプライアンスによって 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表示されます。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXXX-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.
```

SMA ログの使用

表 15-18 に、SMA ログに記録される統計情報を示します。

表 15-18　SMA 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。

次の SMA ログの例は、電子メール セキュリティ アプライアンスからトラッキング ファイルをダウンロードする中央集中型トラッキング サービスと、電子メール セキュリティ アプライアンスからレポーティング ファイルをダウンロードする中央集中型レポーティング サービスを示しています。

```
Wed Oct  3 13:26:39 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.17 - /export/tracki
ng/tracking.@20071003T202244Z_20071003T202544Z.s
Wed Oct  3 13:28:11 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.15 - /export/tracki
ng/tracking.@20071003T202443Z_20071003T202743Z.s
Wed Oct  3 13:28:46 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.17 - /export/tracki
ng/tracking.@20071003T202544Z_20071003T202844Z.s
Wed Oct  3 13:31:27 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.15 - /export/tracki
ng/tracking.@20071003T202743Z_20071003T203043Z.s
Wed Oct  3 13:31:28 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from
172.29.0.15 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.000F1F6ECA7C-2RWDB51.v1.tgz
Wed Oct  3 13:31:53 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.17 - /export/tracki
ng/tracking.@20071003T202844Z_20071003T203144Z.s
Wed Oct  3 13:32:31 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from
172.29.0.17 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.0019B9B316E4-JZ41PC1.v1.tgz
Wed Oct  3 13:34:40 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.15 - /export/tracki
```

```
ng/tracking.@20071003T203043Z_20071003T203343Z.s
```

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 を含む 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

表 15-19 に、ステータス ログ ラベル、およびそれと一致するシステム統計情報を示します。

表 15-19　ステータス ログの統計情報

統計	説明
CPULd	CPU 使用率。
DskIO	ディスク I/O 使用率。
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）。
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。

表 15-19　ステータス ログの統計情報 （続き）

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	作業キューにある現在のメッセージ数。
QuarMsgs	システム隔離にある個々のメッセージ数（複数の隔離領域に存在するメッセージは一度だけカウントされます）。
QuarQKUsd	システム隔離メッセージによって使用されたキロバイト数。
LogUsd	使用されたログ パーティションの割合。
CASELd	CASE スキャンで使用された 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領域の大きさ。
EuQ	Cisco IronPort スパム隔離内のメッセージ数。
EuqRls	Cisco IronPort スパム隔離解放キュー内のメッセージ数。

ステータス ログの例

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp 6318
DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15 FltrHrdBnc 0
ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0
CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis 504791 CchEct
```

```
15395 CchExp 55085 CPUTTm 228 CPUETm 181380 MaxIO 350 RAMUsd 21528056 MMLen 0 DstInMem 4
ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd 0 CASELd 3 TotalLd 3 LogAvail
17G EuQ 0 EuqRls 0
```

システム ログの使用

表 15-20 に、システム ログに記録される統計情報を示します。

表 15-20　システム ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
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: 6.0.0-206 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.
```

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、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。

トラッキング 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、転送されます。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 URL にあります。

```
http://tinyurl.com/3c518r
```

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」（P.15-22）
- 「GUI でのログ サブスクリプションの作成」（P.15-23）

- 「ロギングに対するグローバル設定」（P.15-24）
- 「ログ サブスクリプションのロールオーバー」（P.15-26）
- 「ホスト キーの設定」（P.15-28）

ログ サブスクリプションの設定

ログ サブスクリプションによって、シスコ コンテンツ セキュリティ アプライアンスに、またはリモートに保存される個々のログ ファイルが作成されます。ログ サブスクリプションは、プッシュ（別のコンピュータに配信）またはプル（アプライアンスから取得）されます。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 15-21　ログ ファイルの属性

属性	説明
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、「ログ タイプの概要」（P.15-4）を参照してください。
Name	後で参照するための、ログ サブスクリプションのわかりやすい名前。
Log Filename	ディスクに書き込むときのファイルの物理名。システムに複数のコンテンツ セキュリティ アプライアンスがある場合、ログ ファイルを生成したアプライアンスを識別できる一意のログ ファイル名を使用します。
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、ロールオーバーされます。
Rollover by Time	時間に基づいてログ ファイルをロールオーバーするタイミング。「ログのロールオーバーおよび転送スケジュール」（P.15-2）のオプションを参照してください。
Log Level	各ログ サブスクリプションの詳細レベル。
Retrieval Method	ログ ファイルをアプライアンスから転送するときに使用する方式。

[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ログ設定（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 タイプを入力するプロンプトが表示されます（「ログ タイプの概要」（P.15-4）を参照）。ほとんどのログ タイプで、ログ サブスクリプションの *ログ レベル* の入力も要求されます。

（注） コンフィギュレーション履歴ログのみ：コンフィギュレーション履歴ログからコンフィギュレーションをロードする可能性がある場合は、コンフィギュレーションにマスクされたパスワードが含まれているとロードできないことに注意してください。[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ログ設定（Log Subscriptions）] ページで、パスワードをログに含めるかどうかを尋ねるプロンプトが表示されたら、[はい（Yes）] を選択します。CLI の `logconfig` コマンドを使用する場合は、プロンプトで `y` を入力します。

ログ レベルの設定

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。詳細なログ レベルを設定すると、省略されたログ レベルを設定した場合と比べて、大きなログ ファイルが作成され、システム パフォーマンスに大きな影響を与えます。詳細なログ レベル設定には、省略されたログ レベル設定に含まれるすべてのメッセージと、追加のメッセージが含まれます。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 タイプごとに異なるログ レベルを指定できます。

表 15-22　ログ レベル

ログ レベル	説明
Critical	エラーだけがログに記録されます。最も省略されたログ レベル設定です。このログ レベルでは、パフォーマンスおよび重要なアプライアンスのアクティビティをモニタすることはできません。ただし、詳細ログ レベルのように、ログ ファイルがすぐに最大サイズに達することはありません。このログ レベルは、syslog レベル Alert と同等です。
Warning	すべてのシステム エラーと警告が記録されます。このログ レベルでは、パフォーマンスおよび重要なアプライアンスのアクティビティをモニタすることはできません。Critical ログ レベルよりは早く、ログ ファイルが最大サイズに達します。このログ レベルは、syslog レベル Warning と同等です。
Information	システムの動作が逐次記録されます。たとえば、接続のオープンや配信試行が記録されます。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。
Debug	Information ログ レベルよりも詳細な情報が記録されます。エラーをトラブルシューティングするときは、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 Debug と同等です。
Trace	使用可能なすべての情報が記録されます。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 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　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ログ設定（Log Subscriptions）] ページで、[ログ設定を追加（Add Log Subscription）] をクリックします。

ステップ 2　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 3　該当する場合は、最大ファイル サイズを指定します。

ステップ 4　該当する場合は、ログをロールオーバーする日、時刻、または時間間隔を指定します。詳細については、「ログのロールオーバーおよび転送スケジュール」（P.15-2）を参照してください。

ステップ 5　該当する場合は、ログ レベルを指定します。

ステップ 6　（コンフィギュレーション履歴ログのみ）パスワードをログに含めるかどうかを選択します。

（注）　マスクされたパスワードが含まれているコンフィギュレーションはロードできません。コンフィギュレーション履歴ログからコンフィギュレーションをロードする可能性がある場合は、[はい（Yes）] を選択してパスワードをログに含めます。

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　[ログ設定（Log Subscriptions）] ページの [ログ名（Log Name）] カラムにあるログ名をクリックします。

ステップ 2　ログ サブスクリプションを更新します。

ステップ 3　変更を送信し、保存します。

ロギングに対するグローバル設定

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 メトリックを定期的に記録します。[ログ設定（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。

- システムが測定を記録するまで待機する時間（秒単位）
- 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

すべてシスコ コンテンツ セキュリティ アプライアンスのログには、次の 3 項目を任意で記録できます。

- [メッセージ ID（Message-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 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
  ```

- [リモート応答（Remote Response）] : 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 会話配信時の 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 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、シスコ コンテンツ セキュリティ アプライアンスはデフォルトで、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 ホストが別のシスコ コンテンツ セキュリティ アプライアンスである場合は、エントリ「Message MID accepted」がログに記録されます。

- [オリジナルの件名（Original Subject Header）]：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。[ログ設定のグローバル設定（Log Subscriptions Global Settings）] ページ（または、CLI の logconfig -> logheaders サブコマンド）で、記録するヘッダーを指定します。アプライアンスは、指定されたメッセージ ヘッダーをテキスト メール ログおよびトラッキング 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。

（注） 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。

（注） 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 15-23　ログ ヘッダー

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')]
```

GUI を使用したロギングのグローバル設定

手順

ステップ 1　[ログ設定（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）] ボタンをクリックします。

ステップ 2　システム メトリクスの頻度、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指定します。

これらの設定の詳細については、「ロギングに対するグローバル設定」（P.15-24）を参照してください。

ステップ 3　ログに加えるその他のヘッダーを入力します。各エントリはカンマで区切ります。

ステップ 4　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

AsyncOS がログ ファイルをロールオーバーすると、次のことが行われます。

- ロールオーバーのタイムスタンプで新規のログ ファイルが作成され、文字「c」の拡張子によって現在のファイルとして指示されます。
- 現在のログ ファイルが、保存済みを示す文字「s」の拡張子付きに名前変更されます。
- 新たに保存されたログ ファイルがリモート ホストに転送されます（プッシュ ベースの場合）。
- 同じサブスクリプションから以前に失敗したログ ファイルが転送されます（プッシュ ベースの場合）。
- 保持するファイルの合計数を超えた場合は、ログ サブスクリプション内の最も古いファイルが削除されます（ポーリング ベースの場合）。

ログ サブスクリプション内のログのロールオーバー

「ログのロールオーバーおよび転送スケジュール」（P.15-2）を参照してください。

GUI を使用したログの即時ロールオーバー

手順

ステップ 1　[ログ設定（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　[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することもできます。

ステップ 3　[今すぐロールオーバー（Rollover Now）] ボタンをクリックします。

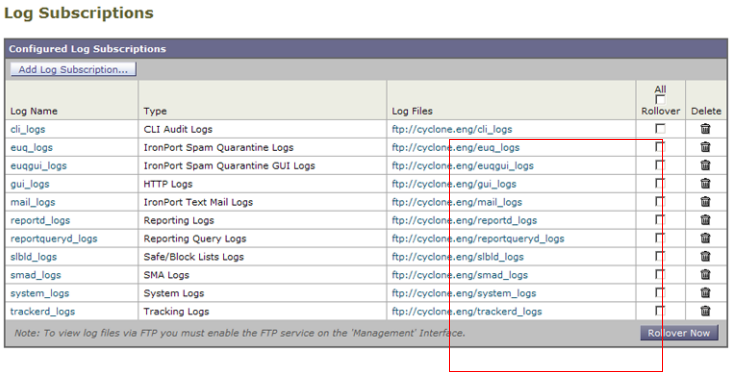
CLI を介したログの即時ロールオーバー

rollovernow コマンドを使用して、一度にすべてのログ ファイルをロールオーバーするか、リストから特定のログ ファイルを選択します。

グラフィカル ユーザ インターフェイスでの最近のログ エントリの表示

GUI を介してログ ファイルを表示するには、[ログ設定（Log Subscriptions）] ページのテーブルの [ログ ファイル（Log Files）] カラムにあるログ サブスクリプションをクリックします。ログ サブスクリプションへのリンクをクリックすると、パスワードを入力するプロンプトが表示されます。次に、そのサブスクリプションのログ ファイルのリストが表示されます。いずれかのログ ファイルをクリックして、ブラウザに表示したり、ディスクに保存したりすることができます。グラフィカル ユーザ インターフェイスを介してログを表示するには、管理インターフェイスで FTP サービスをイネーブルにしておく必要があります。

図 15-1　　グラフィカル ユーザ インターフェイスでのログ ファイルの表示



最新のログ エントリの表示（tail コマンド）

AsyncOS では、アプライアンス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、現在設定されているログのうち、表示するログの番号を選択します。Ctrl を押した状態で C を押して、tail コマンドを終了します。

（注）　コンフィギュレーション履歴ログは、tail コマンドを使用して表示することができません。FTP または SCP を使用する必要があります。

例

次に、tail コマンドを使用してシステム ログを表示する例を示します tail コマンドは、次の例のように、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。

```
tail system_logs

Welcome to the Cisco IronPort M600 Messaging Gateway(tm) Appliance
example.srv> tail

Currently configured logs:
```

```
1. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
2. "euq_logs" Type: "Cisco IronPort Spam Quarantine Logs" Retrieval: FTP Poll
3. "euqgui_logs" Type: "Cisco IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
4. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
5. "mail_logs" Type: "Cisco IronPort Text Mail Logs" Retrieval: FTP Poll
6. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
7. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
8. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
9. "smad_logs" Type: "SMA Logs" Retrieval: FTP Poll
10. "system_logs" Type: "System Logs" Retrieval: FTP Poll
11. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
Enter the number of the log you wish to tail.
[]> 10

Press Ctrl-C to stop.
Thu Sep 27 00:18:56 2007 Info: Begin Logfile
Thu Sep 27 00:18:56 2007 Info: Version: 6.0.0-422 SN: 001143583D73-FT9GP61
Thu Sep 27 00:18:56 2007 Info: Time offset from UTC: 0 seconds
Thu Sep 27 00:18:47 2007 Info: System is coming up.
Thu Sep 27 00:23:05 2007 Warning: DNS query network error '[Errno 64] Host is down' to
'172.16.0.3' looking up 'downloads.cisco.com'
Fri Sep 28 22:20:08 2007 Info: PID 688: User admin commit changes:
Fri Sep 28 23:06:15 2007 Info: PID 688: User admin commit changes:
^Cexample.srv>
.
```

ホスト キーの設定

logconfig -> hostkeyconfig サブ コマンドを使用して、シスコ コンテンツ セキュリティ アプライアンス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、お使いの電子メール セキュリティ アプライアンスのユーザ ガイドまたはオンライン ヘルプの「Managing Secure Shell (SSH) Keys」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 15-24　ホスト キーの管理：サブコマンドのリスト

コマンド	説明
New	新しいキーを追加します。
Edit	既存のキーを変更します。
Delete	既存のキーを削除します。
Scan	ホスト キーを自動的にダウンロードします。
Print	キーを表示します。
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。
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。
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、コマンドによってホスト キーがスキャンされ、ホストに追加されます。

```
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. SSH2:rsa
2. SSH2:dsa
3. All
[3]>

SSH2:dsa
mail3.example.com ssh-dss
[ key displayed ]

SSH2:rsa
mail3.example.com ssh-rsa
[ 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.
[]>

mail3.example.com> commit
```