CHAPTER 10

# システム ステータスのモニタリング



## セキュリティ管理アプライアンス ステータスについて

デフォルトでは、[ システム ステータス（System Status）] ページはブラウザからシスコ コンテンツセキュリティ管理アプライアンスにアクセスするときに最初に表示されるページです。（ランディング ページを変更するには、「プリファレンスの 設定」（P.14-58）を参照してください）

それ以外の場合に [ システム ステータス（System Status）] ページにアクセスするには、[ 管理アプライアンス（Management Appliance）] > [ 集約管理サービス（Centralized Services）] >[ システム ステータス（System Status）] を選択します。

サービスのモニタリングをイネーブルにして、管理対象アプライアンスを追加するまでは、[ システム情報（System Information）] セクションでのみステータス情報が提供されます。システム セットアップ ウィザードを実行し、集約管理サービスを有効にして、管理対象アプライアンスを追加すると、[ 集約管理サービス（Centralized Services）] セクションおよび [ セキュリティアプライアンスデータ転送ステータス（Security Appliance Data Transfer Status）] セクションにデータが表示されます。

ステータス情報には、次の内容が含まれます。

- **集約管理サービス：**処理キューの使用状況などの各集約管理サービスの状態、
- **システム稼働時間：**アプライアンスが動作している時間の長さ
- **CPU 使用率：**各モニタリング サービスによって使用されている CPU 容量
- **システム バージョン情報：**モデル番号、AsyncOS（オペレーティング システム）バージョン、インストール日、およびシリアル番号

### 関連項目

- 「キューの処理のモニタリング」（P.10-2）
- 「CPU 使用率のモニタリング」（P.10-2）

# セキュリティ管理アプライアンス容量のモニタリング



## キューの処理のモニタリング

電子メールと Web レポート、およびアプライアンスが最適な容量で実行されているかを判断するためのトラッキング レポートに使用される処理キューの使用率を定期的に確認できます。

処理キューには、セキュリティ管理アプライアンスによる処理を待機している集中型レポーティング ファイルおよびトラッキング ファイルが保存されます。通常、セキュリティ管理アプライアンスは、処理対象のレポーティング ファイルとトラッキング ファイルのバッチを受信します。処理キューのレポーティング ファイルまたはトラッキング ファイルの割合は、通常、ファイルが管理アプライアンスから転送され、セキュリティ管理アプライアンスで処理されると変動します。

（注）　処理キューの割合は、キューにあるファイルの数で測定されます。ファイル サイズは考慮されません。割合は、セキュリティ管理アプライアンスの処理負荷の概算のみが表示されます。

**手順**

**ステップ 1**　[ 管理アプライアンス（Management Appliance）] > [ 集約管理サービス（Centralized Services）] > [ システム ステータス（System Status）] を選択します。

**ステップ 2**　ページ上部の [ 集約管理サービス（Centralized Services）] セクションで、次に対する処理キューの割合を参照してください.

- [ 集約管理レポート（Centralized Reporting）]（[E メール セキュリティ（Email Security）] サブセクション）
- 集約メッセージトラッキング（Centralized Message Tracking）
- [ 集約管理レポート（Centralized Reporting）]（[Web セキュリティ（Web Security）] サブ セクション）

**ステップ 3**　処理キューの使用率が数時間または数日にわたって高いままである場合は、システムが容量以上に稼働しています。

この場合は、セキュリティ管理アプライアンスから管理対象アプライアンスをいくつか削除するか、追加の セキュリティ管理アプライアンスをインストールするか、その両方を行うことを検討してください。

## CPU 使用率のモニタリング

各集約管理サービスでセキュリティ管理アプライアンスが使用している CPU 容量の割合を表示するには、以下の手順に従ってください。

**ステップ 1**　[ 管理アプライアンス（Management Appliance）] > [ 集約管理サービス（Centralized Services）] > [ システム ステータス（System Status）] を選択します。

**ステップ 2**　[ システム情報（System Information）] セクションまでスクロールし、[CPU 使用率（CPU Utilization）] サブ セクションを表示します。

[CPU 使用率（CPU Utilization）] の割合は、セキュリティ管理アプライアンスの主要な集約管理サービスそれぞれに使われる CPU 処理の割合を示します。いくつかのサービスの使用率の割合は統合されている可能性があります。たとえば、電子メールと Web レポーティングは、「レポーティング サービス」の下に結合され、スパム、ポリシー、ウイルス、およびアウトブレイク隔離は「隔離サービス」の下に結合されます。セキュリティ管理アプライアンスの操作は、「セキュリティ管理アプライアンス」の汎用見出しの下にグループ化されます。

**ステップ 3**　最新のデータを表示するには、ブラウザを更新します。

CPU 使用率の割合は、常に変化します。

# 管理アプライアンスからのデータ転送のステータスのモニタリング

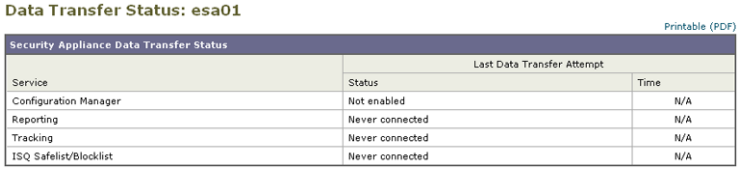
集中管理機能を実行するうえで、セキュリティ管理アプライアンスは、管理対象アプライアンスからセキュリティ管理アプライアンスにデータが正常に転送されることを前提としています。[ セキュリティ アプライアンス データ転送ステータス（Security Appliance Data Transfer Status）] セクションでは、セキュリティ管理アプライアンスに管理される各アプライアンスのステータス情報が表示されます。

デフォルトで、[ セキュリティ アプライアンス データ転送ステータス（Security Appliance Data Transfer Status）] セクションには最大 10 台のアプライアンスが表示されます。セキュリティ管理アプライアンスが 10 台を超えるアプライアンスを管理する場合、[ 表示されたアイテム（Items Displayed）] メニューを使用して表示するアプライアンスの数を選択できます。

**（注）**　[ システム ステータス（System Status）] ページの [ サービス（Services）] セクションに、データ転送ステータスの概要情報が表示されます。[ セキュリティ アプライアンス データ転送ステータス（Security Appliance Data Transfer Status）] セクションには、アプライアンス固有のデータ転送ステータスが表示されます。

[ システム ステータス（System Status）] ページの [ セキュリティ アプライアンス データ転送ステータス（Security Appliance Data Transfer Status）] セクションで、特定のアプライアンスの接続ステータスの問題を表示できます。アプライアンスの各サービスのステータスに関する詳細情報については、アプライアンス名をクリックしてアプライアンスの [ データ転送ステータス（Data Transfer Status）] ページを表示します。

**図 10-1　[データ転送ステータス（Data Transfer Status）：<アプライアンス名>] ページ**



Data Transfer Status: esa01

Printable (PDF)

| Security Appliance Data Transfer Status | | |
|---|---|---|
| | Last Data Transfer Attempt | |
| Service | Status | Time |
| Configuration Manager | Not enabled | N/A |
| Reporting | Never connected | N/A |
| Tracking | Never connected | N/A |
| ISQ Safelist/Blocklist | Never connected | N/A |

[データ転送ステータス（Data Transfer Status）：*アプライアンス名*] ページには、各モニタリング サービスで最後にデータ転送が発生した時刻が表示されます。

電子メール セキュリティ アプライアンスのデータ転送ステータスは、次のいずれかの値になります。

- [無効（Not enabled）]：モニタリング サービスが 電子メール セキュリティ アプライアンスでイネーブルになっていません。
- [接続されていません（Never connected）]：モニタリング サービスは 電子メール セキュリティ アプライアンスでイネーブルになっていますが、電子メール セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立されていません。
- [データ待機中（Waiting for data）]：電子メール セキュリティ アプライアンスが セキュリティ管理アプライアンスと接続されていて、データの受信を待機しています。
- [接続し、データ転送されました（Connected and transferred data）]：電子メール セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立され、データが正常に転送されました。
- [ファイル転送失敗（File transfer failure）]：電子メール セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立されましたが、データ転送に失敗しました。

Web セキュリティ アプライアンスのデータ転送ステータスは、次のいずれかの値になります。

- [無効（Not enabled）]：中央集中型コンフィギュレーション マネージャは、Web セキュリティ アプライアンスでイネーブルになっていません。
- [接続されていません（Never connected）]：中央集中型コンフィギュレーション マネージャは Web セキュリティ アプライアンスでイネーブルになっていますが、Web セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立されていません。
- [データ待機中（Waiting for data）]：Web セキュリティ アプライアンスが セキュリティ管理アプライアンスと接続されていて、データの受信を待機しています。
- [接続し、データ転送されました（Connected and transferred data）]：Web セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立され、データが正常に転送されました。
- [設定転送失敗（Configuration push failure）]：セキュリティ管理アプライアンスがコンフィギュレーション ファイルを Web セキュリティ アプライアンスにプッシュしようとしましたが、転送に失敗しました。
- [設定転送保留（Configuration push pending）]：セキュリティ管理アプライアンスが Web セキュリティ アプライアンスにコンフィギュレーション ファイルをプッシュする処理中です。
- [設定転送成功（Configuration push success）]：セキュリティ管理アプライアンスは Web セキュリティ アプライアンスにコンフィギュレーション ファイルを正常にプッシュしました。

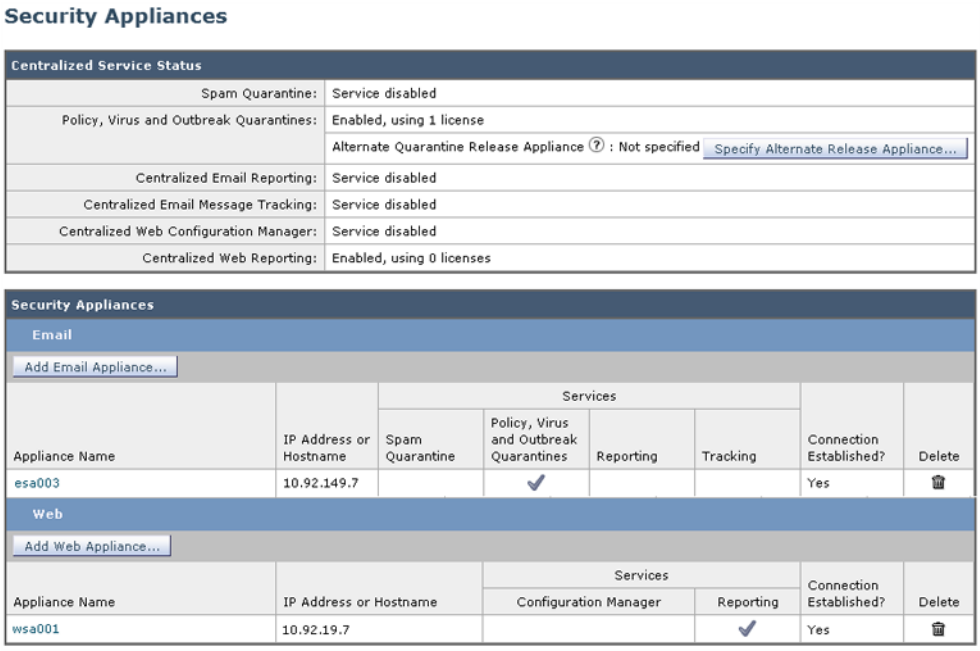
データ転送の問題は、一時的なネットワークの問題またはアプライアンスの設定の問題を反映していることがあります。ステータス [接続されていません（Never connected）] および [データ待機中（Waiting for data）] は、最初に管理対象アプライアンスをセキュリティ管理アプライアンスに追加し

たときの、通常の移行ステータスです。ステータスが最終的に [ 接続し、データ転送されました（Connected and transferred data）] に変化しなかった場合、このデータ転送ステータスは、設定の問題を示している可能性があります。

アプライアンスに [ ファイル転送失敗（File transfer failure）] ステータスが表示された場合は、そのアプライアンスをモニタして、その失敗がネットワークの問題によるものなのか、アプライアンスの設定の問題によるものなのかを判断します。データを転送できない理由がネットワークの問題ではなく、ステータスが [ 接続し、データ転送されました（Connected and transferred data）] に変化しない場合、データ転送ができるようにアプライアンスの設定を変更する必要があります。

# 管理対象アプライアンスの設定ステータスの表示

セキュリティ管理アプライアンスで、[ 管理アプライアンス（Management Appliance）] > [ 集約管理サービス（Centralized Services）] > [ セキュリティ アプライアンス（Security Appliances）] を選択します。




[ 集約サービスのステータス（Centralized Service Status）] セクションに、有効化されているサービスと、サービスごとに使用中のライセンス数が表示されます。[ セキュリティ アプライアンス（Security Appliances）] セクションには、追加したアプライアンスがリスト表示されます。チェック マークは、イネーブルになっているサービスを示し、[ 接続が確立されていますか？（Connection Established?）] カラムは、ファイル転送アクセスが正しく設定されているかどうかを示します。

### 関連項目

- 「リリースされたメッセージを処理する代替アプライアンスの指定」（P.8-8）
- 「管理対象アプライアンスの追加について」（P.2-12）

## Web セキュリティ アプライアンスの追加ステータス情報

Web セキュリティ アプライアンスに関する追加ステータス情報については、「Web セキュリティ アプライアンスのステータスの表示」（P.9-21）を参照してください。

# レポーティング データ アベイラビリティ ステータスのモニタリング

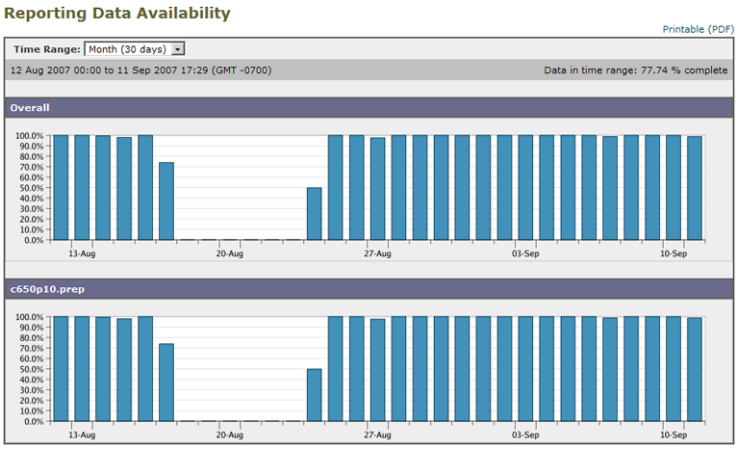
セキュリティ管理アプライアンスによって、指定された期間のレポーティング データのアベイラビリティをモニタできるようになります。アプライアンスに応じたセクションを参照してください。

- 「電子メール セキュリティ レポート データの可用性のモニタリング」（P.10-6）
- 「Web セキュリティ レポート データの可用性のモニタリング」（P.10-7）

## 電子メール セキュリティ レポート データの可用性のモニタリング

セキュリティ管理アプライアンスで電子メール セキュリティ アプライアンスからのレポーティング データをモニタするには、[ メール（Email）] > [ レポート（Reporting）] > [ 有効なレポート データ（Reporting Data Availability）] ページを表示します。

**図 10-2　[ 有効なレポート データ（Reporting Data Availability）] ページ**




[ 有効なレポート データ（Reporting Data Availability）] ページから、指定された期間に セキュリティ管理アプライアンスが 電子メール セキュリティ アプライアンスから受信したレポーティング データの割合を表示できます。棒グラフは、時間範囲内に受信したデータの完全性を示します。

レポーティング データ アベイラビリティは、前の日、週、年についてモニタできます。セキュリティ管理アプライアンスが 電子メール セキュリティ アプライアンスから受信したレポーティング データが 100% 未満の場合は、データが不完全なことがすぐにわかります。データ アベイラビリティ情報を使用して、レポーティング データの検証およびシステムの問題のトラブルシューティングができます。

（注）　ハードウェア障害または他の理由で、電子メール セキュリティ アプライアンスの交換が必要になった場合、置き換えられた電子メール セキュリティ アプライアンスからのデータは失われませんが、そのデータはセキュリティ管理アプライアンスで正常に表示されません。

# Web セキュリティ レポート データの可用性のモニタリング

セキュリティ管理アプライアンスで Web セキュリティ アプライアンスからのレポーティング データをモニタするには、[Web] > [ レポート（Reporting）] > [ 使用可能なデータ（Data Availability）] ページを表示します。

[ 使用可能なデータ（Data Availability）] ページからデータの更新およびソートができ、リソース使用率および Web トラフィックの問題箇所をリアルタイムに表示できます。


Web Reporting Data Availability

Printable (PDF)

Web Reporting Data Range

Displaying 1 - 2 of 2 appliances.

| Web Security Appliance | Web Reporting | | Web Tracking and Reporting Detail | | Status |
|---|---|---|---|---|---|
| | From | To | From | To | |
| vmw098-wsa08.sma | 26 Aug 2010 09:00 | 27 Aug 2010 02:22 | 26 Aug 2010 11:00 | 27 Aug 2010 02:22 | Ok |
| vmw095-wsa11.sma | N/A | N/A | N/A | N/A | Never Connected |
| Overall: | 26 Aug 2010 09:00 (GMT +03:00) | 27 Aug 2010 02:22 (GMT +03:00) | 26 Aug 2010 11:00 (GMT +03:00) | 27 Aug 2010 02:22 (GMT +03:00) | |

Displaying 1 - 2 of 2 appliances.

（注）　[ 有効な Web レポート データ（Web Reporting Data Availability）] ウィンドウでは、Web Reporting と Email Reporting の**両方が**ディセーブルの場合にのみ、Web Reporting がディセーブルであると表示されます。

このページから、すべてのデータ リソース使用率および Web トラフィックの問題箇所を表示できます。リスト表示されている Web セキュリティ アプライアンス リンクのいずれかをクリックすると、そのアプライアンスのレポーティング データ アベイラビリティを表示できます。

レポーティング データ アベイラビリティは、前の日、週、年についてモニタできます。セキュリティ管理アプライアンスが Web セキュリティ アプライアンスから受信したレポーティング データが 100% 未満の場合は、データが不完全なことがすぐにわかります。データ アベイラビリティ情報を使用して、レポーティング データの検証およびシステムの問題のトラブルシューティングができます。

URL カテゴリに関するスケジュール設定されたレポート内でデータ アベイラビリティが使用されている場合に、いずれかのアプライアンスでデータに欠落があると、ページの下部に「この時間範囲の一部のデータは使用不可でした。(Some data in this time range was unavailable.)」というメッセージが表示されます。欠落がない場合は何も表示されません。

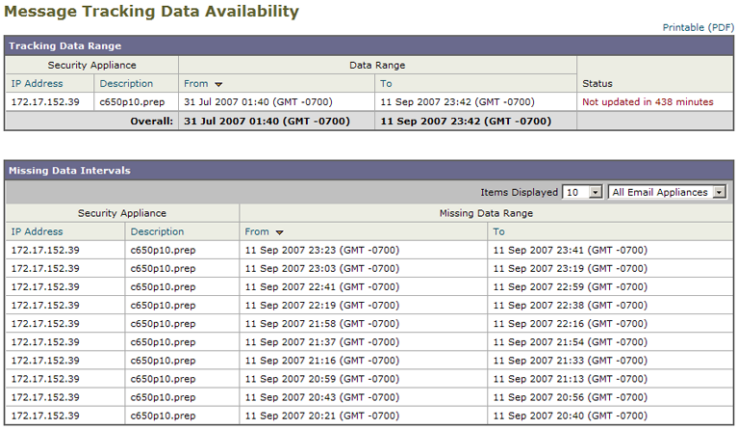
Web セキュリティ アプライアンスの [ 使用可能なデータ（Data Availability）] ページの詳細については、「[ 使用可能なデータ（Data Availability）] ページ」を参照してください。

# 電子メール トラッキング データ ステータスのモニタリング

電子メール トラッキング データのステータスをモニタするには、[ メール（Email）] > [ メッセージ トラッキング（Message Tracking）] > [ 有効なメッセージ トラッキング データ（Message Tracking Data Availability）] ページを表示します。

（注）　電子メール セキュリティ アプライアンスは、アプライアンスから取得したレポーティング データとトラッキング データのコピーを作成し、データ ファイルのコピーをデフォルト ディレクトリとは別の追加フォルダに保存します。次に、これらのフォルダのいずれかからデータを取り出すように、セキュリティ管理アプライアンスを設定できます。

**図 10-3　[有効なメッセージ トラッキング データ（Message Tracking Data Availability）] ページ**



Message Tracking Data Availability

Printable (PDF)

Tracking Data Range

| Security Appliance | | Data Range | | |
|---|---|---|---|---|
| IP Address | Description | From | To | Status |
| 172.17.152.39 | c650p10.prep | 31 Jul 2007 01:40 (GMT -0700) | 11 Sep 2007 23:42 (GMT -0700) | Not updated in 438 minutes |
| | Overall: | 31 Jul 2007 01:40 (GMT -0700) | 11 Sep 2007 23:42 (GMT -0700) | |

Missing Data Intervals

Items Displayed 10 | All Email Appliances

| Security Appliance | | Missing Data Range | |
|---|---|---|---|
| IP Address | Description | From | To |
| 172.17.152.39 | c650p10.prep | 11 Sep 2007 23:23 (GMT -0700) | 11 Sep 2007 23:41 (GMT -0700) |
| 172.17.152.39 | c650p10.prep | 11 Sep 2007 23:03 (GMT -0700) | 11 Sep 2007 23:19 (GMT -0700) |
| 172.17.152.39 | c650p10.prep | 11 Sep 2007 22:41 (GMT -0700) | 11 Sep 2007 22:59 (GMT -0700) |
| 172.17.152.39 | c650p10.prep | 11 Sep 2007 22:19 (GMT -0700) | 11 Sep 2007 22:38 (GMT -0700) |
| 172.17.152.39 | c650p10.prep | 11 Sep 2007 21:58 (GMT -0700) | 11 Sep 2007 22:16 (GMT -0700) |
| 172.17.152.39 | c650p10.prep | 11 Sep 2007 21:37 (GMT -0700) | 11 Sep 2007 21:54 (GMT -0700) |
| 172.17.152.39 | c650p10.prep | 11 Sep 2007 21:16 (GMT -0700) | 11 Sep 2007 21:33 (GMT -0700) |
| 172.17.152.39 | c650p10.prep | 11 Sep 2007 20:59 (GMT -0700) | 11 Sep 2007 21:13 (GMT -0700) |
| 172.17.152.39 | c650p10.prep | 11 Sep 2007 20:43 (GMT -0700) | 11 Sep 2007 20:56 (GMT -0700) |
| 172.17.152.39 | c650p10.prep | 11 Sep 2007 20:21 (GMT -0700) | 11 Sep 2007 20:40 (GMT -0700) |

[有効なメッセージ トラッキング データ（Message Tracking Data Availability）] ページによって、セキュリティ管理アプライアンスに対するデータ欠落インターバルを表示できるようになります。データ欠落インターバルは、セキュリティ管理アプライアンスが組織の電子メール セキュリティ アプライアンスからメッセージ トラッキング データを受信しなかった期間です。

特定の管理対象アプライアンス、またはシステムにあるすべての電子メール セキュリティ アプライアンスのデータ アベイラビリティをモニタできます。メッセージ トラッキング データのデータ欠落インターバルが検出された場合は、データが不完全なことがすぐにわかります。データ アベイラビリティ情報を使用して、メッセージ トラッキング データの検証およびシステムの問題のトラブルシューティングができます。

# 管理対象アプライアンスのキャパシティのモニタリング

セキュリティ管理アプライアンスからの管理対象アプライアンスの容量をモニタできます。すべての電子メールまたは Web セキュリティ アプライアンスの総合的な容量および個別のアプライアンスの容量を確認できます。

| 表示する容量 | 参照先 |
|---|---|
| 管理対象の Web セキュリティ アプライアンス | 「[システム容量（System Capacity）] ページ」（P.5-61） |
| 管理対象の電子メール セキュリティ アプライアンス | 「[システム容量（System Capacity）] ページ」（P.4-44） |

# アクティブな TCP/IP サービスの識別

セキュリティ管理アプライアンスで使用されるアクティブな TCP/IP サービスを識別するには、コマンドライン インターフェイスで `tcpservices` コマンドを使用します。