



## CHAPTER 9

# SSL サービスのモニタリング

Performance Monitor 機能を使用すると、Secure Socket Layer (SSL) モジュールの動作およびパフォーマンスの重要な点を、リアルタイムでモニタおよび解釈できます。

ここでは、SSL モジュール モニタリング機能について説明します。

- 「[SSL の概念](#)」 (P.9-1)
- 「[モジュールの集成的モニタリング](#)」 (P.9-2)
- 「[モジュールの個別モニタリング](#)」 (P.9-5)

## SSL の概念

Secure Socket Layer (SSL) は、プライバシー、認証、およびデータ整合性によってデータの安全な転送を可能にするプロトコルです。SSL では証明書、公開キー、および秘密キーを使用します。

ここでは、SSL モニタリングを理解するために必要な情報を示します。

- 「[SSL モジュールの目的](#)」 (P.9-1)
- 「[SSL モジュールのパフォーマンス](#)」 (P.9-2)

## SSL モジュールの目的

SSL サービス モジュールは、Cisco Catalyst 6500 シリーズ スイッチの統合型モジュールです。Series 6500 スイッチの任意のポートがネットワーク上の Web サーバのプロキシ SSL ポートである場合、このサーバから、リソースを大量に消費する SSL 機能をオフロードできます。1 つの SSL モジュールが複数の Web サーバのプロキシとして動作できます。

SSL モジュールは、暗号化された Web トラフィックの配送を高速化し、すべての SSL 関連タスクを実行します (Web 対応アプリケーションの配送を含みます)。そのため、Web サーバは、独自の SSL 機能を実行するよりも高速かつ大量に、暗号化されていない Web コンテンツを配送できます。

適切に設定された SSL モジュールは、次のように機能します。

- Web サイトがサポートするセキュア接続の数を増やします。
- Web サーバがより多くのコンテンツ要求を処理できるようにします。
- サーバのロード バランシングを提供します。

## SSL モジュールのパフォーマンス

Catalyst 6500 スイッチのシャーシには、最大 4 台の SSL モジュールを搭載できます。最適化された状況下では、各 SSL モジュールが以下を提供します。

- 1 秒あたり最大 2,500 の接続セットアップ。4 台のモジュールが設置されている場合、1 シャーシあたり 10,000。
- 最大 300 Mbps のバルク暗号化スループット。4 台のモジュールが設置されている場合、1 シャーシあたり 12.2 Gbps。
- 最大 60,000 の同時接続。4 台のモジュールが設置されている場合、1 シャーシあたり 240,000。

各 SSL モジュールは、独自の CPU と独自の IP アドレスを持ちます。

SSL モジュールが正しく設定されていない場合、または正しく動作していない場合、ネットワーク上の暗号化された Web サービス、および暗号化されていない Web サービスが低下することがあります。

ネットワーク上の SSL モジュールで提供されるサービス レベルが、指定されている性能を下回っていると判断される場合は、ネットワーク管理ツールで原因を切り分け、修正アクションを実行できます。

## モジュールの集成的モニタリング

ここでは、SSL モジュールを集成的にモニタする方法を説明します。

- 「SSL 使用状況およびアクティビティ統計情報の操作」(P.9-2)
- 「SSL 統計情報の操作」(P.9-3)
- 「TCP 接続統計情報の操作」(P.9-4)

## SSL 使用状況およびアクティビティ統計情報の操作

ネットワーク上のすべての有効な SSL モジュールの使用状況およびアクティビティ統計情報を表示できます。

### 手順

- 
- ステップ 1** [Monitor] > [SSL] > [Modules] を選択します。テーブルのカラムの説明については、表 9-1 を参照してください。
- ステップ 2** 1 つの SSL モジュールの詳細グラフを表示するには、[Module] カラムで、関連する IP アドレスをクリックします。
-

## 参考

表 9-1 [SSL Modules] ページ

要素	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラートアイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な SSL エラーだけが表示されるようにフィルタ処理された画面が表示されます。「 <a href="#">インターフェイスのアイコンについて</a> 」(P.3-5) を参照してください。  イベント ブラウザ要素のリファレンス情報については、「 <a href="#">イベントブラウザ ウィンドウ</a> 」(P.3-15) を参照してください。  (注) イベントをクリアした後、1 分経過するか、ページがリフレッシュされるかのいずれか早い方まで、アラートアイコンはデバイス モニタリング ページに表示され続けます。
[Module] カラム	SSL モジュールの IP アドレスが表示されます。
[Version] カラム	SSL モジュールのソフトウェアバージョンが表示されます。
[Memory Usage %] カラム	関連する SSL モジュールが使用しているメモリのバイトの割合が表示されます。
[CPU Usage %] カラム	現在使用されている SSL モジュールの CPU 能力の割合が表示されます。これは、最近 5 秒間の平均です。
[No.Active Sessions] カラム	SSL モジュールでアクティブなセッションの数が表示されます。
[Last Updated] カラム	表示された値がポーリングまたはトラップによって提供された時間が表示されます。

## 関連トピック

- 「[Performance Monitor テーブルのオプション タスク](#)」(P.3-9)
- 「[テーブルの一般エレメント](#)」(P.3-8)

## SSL 統計情報の操作

すべての有効な SSL モジュールの SSL アクティビティ統計情報のテーブルを、表示および操作できます。

- 
- ステップ 1** [Monitor] > [SSL] > [Statistics] を選択します。テーブルのカラムの説明については、[表 9-2](#) を参照してください。
- [SSL Statistics] ページのすべての測定値は、デルタとして計算されます（あるポーリング サイクルから次のポーリング サイクルまでの差の範囲を示します）。ただし、アクティブ セッションおよびアクティブ接続の数は整数です。
- ステップ 2** 1 つの SSL モジュールの要約グラフを表示するには、[Module] カラムで、関連する IP アドレスまたは DNS 名をクリックします。
-

## 参考

表 9-2 [SSL Statistics] ページ

要素	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラートアイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な SSL エラーだけが表示されるようにフィルタ処理された画面が表示されます。「 <a href="#">インターフェイスのアイコンについて</a> 」(P.3-5) を参照してください。 イベント ブラウザ要素のリファレンス情報については、「 <a href="#">イベント ブラウザ ウィンドウ</a> 」(P.3-15) を参照してください。
[Module] カラム	モジュールの IP アドレスが表示されます。
[Connects Attempted] カラム	前回のポーリング サイクル以降に試行された SSL 接続の合計数が表示されます。
[Connects Completed] カラム	前回のポーリング サイクル以降に正常に完了した SSL 接続の合計数が表示されます。
[Connects Active] カラム	アクティブな SSL 接続の数が表示されます。
[Active Sessions] カラム	アクティブな SSL セッションの合計数が表示されます。
[Handshake Failures] カラム	前回のポーリング サイクル以降に発生したハンドシェイク失敗の数が表示されます。
[Data Failures] カラム	前回のポーリング サイクル以降に発生したデータ障害の数が表示されます。

## 関連トピック

- 「[Performance Monitor テーブルのオプション タスク](#)」(P.3-9)
- 「[テーブルの一般エレメント](#)」(P.3-8)

## TCP 接続統計情報の操作

すべての有効な SSL モジュールの TCP 接続統計情報のテーブルを、表示および操作できます。

- ステップ 1** [Monitor] > [SSL] > [TCP Connections] を選択します。テーブルのカラムの説明については、[表 9-3](#) を参照してください。
- [SSL TCP Statistics] ページのすべての測定値は、デルタとして計算されます。
- ステップ 2** 1 つの SSL モジュールの要約グラフを表示するには、[Module] カラムで、関連する IP アドレスまたは DNS 名をクリックします。

## 参考

表 9-3 [SSL TCP Connections] ページ

要素	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラートアイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な SSL エラーだけが表示されるようにフィルタ処理された画面が表示されます。「 <a href="#">インターフェイスのアイコンについて</a> 」(P.3-5) を参照してください。 イベント ブラウザ要素のリファレンス情報については、「 <a href="#">イベント ブラウザ ウィンドウ</a> 」(P.3-15) を参照してください。

表 9-3 [SSL TCP Connections] ページ (続き)

要素	説明
[Module] カラム	モジュールの IP アドレスが表示されます。
[Connects Init] カラム	前回のポーリング サイクル以降に開始された TCP 接続の数が表示されます。
[Connects Established] カラム	前回のポーリング サイクル以降に確立された TCP 接続の数が表示されます。
[Connects Accepted] カラム	前回のポーリング サイクル以降に受け入れられた TCP 接続の数が表示されます。
[Connects Dropped] カラム	前回のポーリング サイクル以降にドロップされた TCP 接続の数が表示されます。
[Connects Closed] カラム	前回のポーリング サイクル以降に終了された TCP 接続の数が表示されます。
[Packet Sent] カラム	前回のポーリング サイクル以降に送信されたパケットの合計数が表示されます。
[Packet Received] カラム	前回のポーリング サイクル以降に受信されたパケットの合計数が表示されます。

#### 関連トピック

- 「Performance Monitor テーブルのオプション タスク」 (P.3-9)
- 「テーブルの一般エレメント」 (P.3-8)

## モジュールの個別モニタリング

ここでは、有効な SSL モジュールを個別にモニタする方法を説明します。

- 「モジュールの詳細グラフの表示と意味」 (P.9-5)
- 「SSL プロキシ統計情報テーブルの表示」 (P.9-6)
- 「SSL プロキシエラー テーブルの表示」 (P.9-7)

## モジュールの詳細グラフの表示と意味

1 つの検証済みの SSL モジュールの詳細グラフのページを、表示および操作できます。

#### 手順

**ステップ 1** [Monitor] > [SSL] > [Module Details] を選択します。

デフォルトでは、Performance Monitor は、IP アドレスとして最も低い番号を使用するモジュールのヘルスとパフォーマンスを説明するグラフを表示します。グラフの説明については、表 9-4 を参照してください。



**(注)** 2 つの縦 (Y) 軸を使用するグラフを解釈するときに、既知の問題が発生することがあります。最初の Y 軸は常にゼロで始まるのに対し、2 番目の Y 軸は、指定された時間範囲の最も低い値がゼロよりも大きい場合でも、その値で始まります。そのため、2 つの Y 軸を直接比較できないことがあります。

**ステップ 2** [Select Device] リストから、グラフを表示するデバイスを選択します。

## SSL モジュール グラフの種類

表 9-4 SSL モジュール グラフの意味

ラベル	説明
[CPU Usage]	<p>使用されたモジュールの CPU 能力の割合を示します。</p> <ul style="list-style-type: none"> <li>縦軸は、関連するポーリング サイクルで使用された CPU 能力の割合の平均を示します。</li> <li>横軸は、ポーリング サイクルの時刻を示します。</li> </ul>
[Memory Usage]	<p>使用されたモジュールのメモリ容量の割合を示します。</p> <ul style="list-style-type: none"> <li>縦軸は、関連するポーリング サイクルで使用されたメモリ容量の割合の平均を示します。</li> <li>横軸は、ポーリング サイクルの時刻を示します。</li> </ul>
[Error Rate]	<p>長期にわたるモジュール インターフェイス エラーのトレンドを示します。</p> <ul style="list-style-type: none"> <li>縦軸は、関連するポーリング サイクルで発生したエラーの平均数を示します。</li> <li>横軸は、ポーリング サイクルの時刻を示します。</li> </ul>
[Throughput vs. Connections]	<p>長期にわたるスループットのトレンドと接続のトレンドを比較するのに役立つ折れ線グラフが表示されます。</p> <ul style="list-style-type: none"> <li>2 種類の情報を表示するため、2 つの縦軸を使用します。 <ul style="list-style-type: none"> <li>左の（青の）縦軸は、関連するポーリング サイクルでの平均スループットをバイト単位で示します。</li> <li>右の（赤の）縦軸は、関連する時間での SSL 接続数の平均を示します。</li> </ul> </li> <li>横軸は、Performance Monitor がそれぞれの縦軸のトレンドを計算した時刻を示します。</li> </ul>

## SSL プロキシ統計情報テーブルの表示

1 つの検証済みの SSL モジュールのプロキシ統計情報のテーブルを、表示および操作できます。

## 手順

- ステップ 1** [Monitor] > [SSL] > [Proxy Statistics] を選択します。テーブルのカラムの説明については、表 9-5 を参照してください。
- [SSL Proxy Statistics] ページのすべての測定値は、デルタとして計算されます。
- ステップ 2** [Select Device] リストから、表示するデバイスを選択します。

## 参考

表 9-5 [SSL Proxy Statistics]

要素	説明
[Proxy] カラム	プロキシ サービス名が表示されます。
[Connects Attempted] カラム	前回のポーリング サイクル以降に試行された、関連するプロキシ サービスの接続の合計数が表示されます。
[Connects Completed] カラム	前回のポーリング サイクル以降に正常に完了した、関連するプロキシ サービスの接続の合計数が表示されます。

表 9-5 [SSL Proxy Statistics] (続き)

要素	説明
[Connects in Handshake] カラム	関連するプロキシ サービスの、ハンドシェイク状態の接続数が表示されます。
[Connects in Data] カラム	関連するプロキシ サービスの、データ状態の接続数が表示されます。
[Connects in Reneg] カラム	関連するプロキシ サービスの、再ネゴシエート状態の接続数が表示されます。
[Bytes Encrypted] カラム	前回のポーリング サイクル以降の、関連するプロキシ サービスの暗号化された送信バイトの合計数が表示されます。
[Bytes Decrypted] カラム	前回のポーリング サイクル以降の、関連するプロキシ サービスの復号化された受信バイトの合計数が表示されます。

**関連トピック**

- 「Performance Monitor テーブルのオプション タスク」 (P.3-9)
- 「テーブルの一般エレメント」 (P.3-8)

## SSL プロキシ エラー テーブルの表示

1 つの検証済みの SSL モジュールのプロキシ エラーのテーブルを、表示および操作できます。

**手順**

**ステップ 1** [Monitor] > [SSL] > [Proxy Errors] を選択します。テーブルのカラムの説明については、表 9-6 を参照してください。

[SSL Proxy Errors] ページのすべての測定値は、デルタとして計算されます。

**ステップ 2** [Select Device] リストから、表示するデバイスを選択します。

**参考**

表 9-6 [SSL Proxy Errors]

要素	説明
[Proxy] カラム	プロキシ サービス名が表示されます。
[Handshake Failures] カラム	ハンドシェイク状態で発生した、関連するプロキシ サービスの SSL 失敗数が表示されます。
[Data Failures] カラム	データ状態で発生した、関連するプロキシ サービスの SSL 失敗数が表示されます。
[MAC Errors] カラム	前回のポーリング サイクル以降に発生した、関連するプロキシ サービスの Machine Authentication Code (MAC) 検証エラーの数が表示されます。
[Version Mismatch] カラム	前回のポーリング サイクル以降に発生した、関連するプロキシ サービスの SSL バージョン不一致エラーの数が表示されます。
[No Compress] カラム	圧縮アルゴリズムがサポートされていない前回のポーリング サイクル以降に発生した、関連するプロキシ サービスのエラーの数が表示されます。
[No Cipher] カラム	SSL 暗号化に互換性がない前回のポーリング サイクル以降に発生した、関連するプロキシ サービスのエラーの数が表示されます。

**関連トピック**

- 「[Performance Monitor テーブルのオプション タスク](#)」 (P.3-9)
- 「[テーブルの一般エレメント](#)」 (P.3-8)