



SSL の設定情報および統計情報の表示

この章では、CSS SSL の設定情報および統計情報の表示に利用できる **show** コマンド、および **show** コマンドで表示されるフィールドについて説明します。この章の主な内容は次のとおりです。

- [証明書とキー ペアに関する情報の表示](#)
- [SSL プロキシ設定情報の表示](#)
- [CRL レコード設定の表示](#)
- [SSL URL リライト統計情報の表示](#)
- [SSL モジュール統計情報の表示](#)
- [SSL 統計情報のクリア](#)
- [SSL フローの表示](#)

証明書とキー ペアに関する情報の表示

CSS で一連の **show** コマンドを使用すれば、CSS に保存されている SSL 証明書とキー ペアに関するさまざまな情報を表示できます。次の **show** コマンドは、どのモードでも入力できます。

- **show ssl associate cert** : 証明書アソシエーション (関連付け) を表示する。
- **show ssl associate rsakey** : RSA キー ペア アソシエーションを表示する。
- **show ssl associate dsakey** : DSA キー ペア アソシエーションを表示する。
- **show ssl associate dhparam** : Diffie-Hellman パラメータ アソシエーションに関する情報を表示する。
- **show ssl associate** : CSS のファイル アソシエーションをすべて表示する。
- **show ssl files** : CSS にロードされている証明書、キー ペア、および Diffie-Hellman パラメータ ファイルをすべて表示する。

SSL 証明書の表示

CSS の証明書アソシエーションに関する要約データを表示するには、**show ssl associate cert certname** コマンドを使用します。オプションの証明書名を指定すれば、その証明書アソシエーションに対応する証明書の詳しい情報を表示できます。証明書名を指定しないと、**show ssl associate cert** の出力には、すべての証明書アソシエーションが表示されます。

すべての証明書アソシエーションに関する情報を表示するには、次のコマンドを入力します。

```
show ssl associate cert
```

表 7-1 に、**show ssl associate cert** コマンドで表示される各フィールドと、その説明を示します。

表 7-1 ssl associate cert コマンドのフィールド

フィールド	内容
Certificate Name	証明書アソシエーションの名前
File Name	証明書を含むファイルの名前
Used By List	証明書アソシエーションが、仮想サーバの VIP アドレスを含む SSL プロキシ リストで使用されているかどうか

特定の証明書アソシエーションに関する情報を表示するには、次のコマンドを入力します。

```
show ssl associate cert myrsacert1
```

表 7-2 に、**show ssl associate cert certname** コマンドで表示される各フィールドと、その説明を示します。

表 7-2 ssl associate cert certname コマンドのフィールド

フィールド	内容
Certificate	証明書を発行した認証局 (CA) の名前
Version	証明書のバージョン
Serial Number	証明書に関連付けられているシリアル番号
Signature Algorithm	公開 / 秘密キーで情報を暗号化する場合に使用されるデジタル署名アルゴリズム (RSA など)
Issuer	証明書を生成し、証明書を保証する組織。発行元は認証局 (CA) でもあります。
有効性	
Not Before	証明書の発効日
Not After	証明書の失効日
Subject	秘密キーを所有する認証済みパーティ

表 7-2 ssl associate cert certname コマンドのフィールド (続き)

フィールド	内容
公開キー情報	
Public Key Algorithm	公開キーの生成に使用されるキー交換アルゴリズムの名前 (RSA など)
RSA Public Key	キーのビット数。この値によって、Web トランザクションの保護に使用される RSA キーペアのサイズが決まります。
Modulus	証明書の作成時に使用された実際の公開キー
Exponent	キーの生成に使用する基本数の 1 つ
X509v3 Extensions	証明書に追加される X509v3 拡張の配列
X509v3 Basic Constraints	サブジェクトが CA として機能できるかどうか。証明書の署名を確認するのに使用する認証された公開キーで示します。CA として機能できる場合、証明書のパス長の制約も示されます。
Netscape Comment	証明書を表示するときに示すことができるコメント
X509v3 Subject Key Identifier	認証対象の公開キー。これにより、同じサブジェクトが使用する個々のキーを区別することができます (たとえば、キーを更新した場合など)。
X509v3 Authority Key Identifier	この証明書または CRL の署名を確認するために使用する公開キー。これにより、同じ CA が使用する個々のキーを区別することができます (たとえば、キーを更新した場合など)。
Signature Algorithm	デジタル署名に使用されるアルゴリズムの名前 (キー交換ではなく)
Hex Numbers	証明書の実際の署名。クライアントは、指定したアルゴリズムを使用してこの署名を再生成し、証明書データが変更されていないか確認できます。

SSL RSA 秘密キーの表示

CSS の RSA 秘密キー アソシエーションに関する情報を取得するには、**show ssl associate rsakey keyname** コマンドを使用します。オプションの RSA キーの名前を指定すれば、特定の RSA キー アソシエーションに関する情報（キーのサイズとタイプ）を表示できます。RSA キー名を指定しないと、すべての RSA キー アソシエーションのリストが表示されます。



(注) 特定のキーの内容を表示した場合だけ、キーのサイズとタイプに関する詳細が表示されます。この制約は、キーの内容を保護し、表示されないようにするために備わっています。

すべての RSA 秘密キー アソシエーションを表示するには、次のコマンドを入力します。

```
(config) # show ssl associate rsakey
```

表 7-3 に、**show ssl associate rsakey** コマンドで表示される各フィールドと、その説明を示します。

表 7-3 show ssl associate rsakey コマンドのフィールド

フィールド	内容
Key Name	RSA キー アソシエーションの名前
File Name	RSA キー ペアを含むファイルの名前
Used By List	RSA キー アソシエーションが、仮想サーバの VIP アドレスを含む SSL プロキシ リストで使用されているかどうか

特定の RSA キー ペアに関する情報を表示するには、次のコマンドを入力します。

```
(config) # show ssl associate rsakey myrsakey1  
1024-bit RSA keypair
```

SSL DSA 秘密キーの表示

CSS の DSA 秘密キー アソシエーションに関する情報を取得するには、**show ssl associate dsakey keyname** コマンドを使用します。DSA キー名を指定すれば、特定の DSA キー アソシエーションに関する情報（キーのサイズとタイプ）を表示することもできます。DSA キー名を指定しないと、すべての DSA キー アソシエーションのリストが表示されます。



(注) 特定のキーの内容を表示した場合だけ、キーのサイズとタイプに関する詳細が表示されます。この制約は、キーの内容を保護し、表示されないようにするために備わっています。

すべての DSA キー アソシエーションを表示するには、次のコマンドを入力します。

```
(config) # show ssl associate dsakey
```

表 7-4 に、**show ssl associate dsakey** コマンドで表示される各フィールドと、その説明を示します。

表 7-4 show ssl associate dsakey コマンドのフィールド

フィールド	内容
Key Name	DSA キー アソシエーションの名前
File Name	DSA キー ペアを含むファイルの名前
Used By List	DSA キー アソシエーションが、仮想サーバの VIP アドレスを含む SSL プロキシリストで使用されているかどうか

特定の DSA キー ペアに関する情報を表示するには、次のコマンドを入力します。

```
(config) # show ssl associate dsakey mydsakey1
1024-bit DSA keypair
```

SSL Diffie-Hellman パラメータの表示

Diffie-Hellman パラメータに関する情報を取得するには、**show ssl associate dhparam paramname** コマンドを使用します。パラメータ ファイル名を指定すれば、特定の Diffie-Hellman パラメータ ファイル アソシエーションに関する情報を表示することもできます。Diffie-Hellman パラメータ ファイル名を指定しないと、すべての Diffie-Hellman パラメータ ファイル アソシエーションのリストが表示されます。

すべての Diffie-Hellman アソシエーションに関する情報を表示するには、次のコマンドを入力します。

```
(config) # show ssl associate dhparam
```

表 7-5 に、**show ssl associate dhparam** コマンドで表示される各フィールドと、その説明を示します。

表 7-5 show ssl associate dhparam コマンドのフィールド

フィールド	内容
Parameter Name	Diffie-Hellman パラメータ アソシエーションの名前
File Name	Diffie-Hellman パラメータを含むファイルの名前
Used By List	Diffie-Hellman ファイル アソシエーションが、仮想サーバの VIP アドレスを含む SSL プロキシ リストで使用されているかどうか

特定の Diffie-Hellman パラメータ ファイル アソシエーションに関する情報を表示するには、次のコマンドを入力します。

```
(config) # show ssl associate dhparam mydhparam1  
512-bit DH parameters
```

SSL アソシエーションの表示

CSS に保存されている証明書とキーのすべてのアソシエーションの要約を表示するには、**show ssl associate** コマンドを使用します。

CSS の SSL アソシエーションの要約を表示するには、次のコマンドを入力します。

```
CSS11506(config)# show ssl associate
```

Certificate Name -----	File Name -----	Used by List -----
rsacert	rsacert.pem	yes
RSA Key Name -----	File Name -----	Used by List -----
rsakey	rsakey.pem	yes
DH Param Name -----	File Name -----	Used by List -----
dhparams	dhparams.pem	no
DSA Key Name -----	File Name -----	Used by List -----
dsakey	dsakey.pem	no

SSL 証明書、キー ペア、および Diffie-Hellman パラメータ ファイルの表示

CSS にロードされている証明書、キー ペア、および Diffie-Hellman パラメータ ファイルのリストを表示するには、**show ssl files** を使用します。

たとえば、次のように入力します。

```
(config) # show ssl files
```

表 7-6 に、**show ssl files** コマンドで表示される各フィールドと、その説明を示します。

表 7-6 show ssl files コマンドのフィールド

フィールド	内容
File Name	インポートまたは手動生成された証明書、RSA キー ペア、DSA キー ペア、または Diffie-Hellman パラメータ ファイルの名前
File Type	インポートまたは手動生成された証明書、RSA キー ペア、DSA キー ペア、または Diffie-Hellman パラメータ ファイルの形式。ファイルのタイプは、DES、PEM、PKCS#12 のいずれかの符号化形式になります。
File Size	証明書、RSA キー ペア、DSA キー ペア、または Diffie-Hellman パラメータ ファイルの合計サイズ (KB 単位)

SSL プロキシ設定情報の表示

show ssl-proxy-list コマンドを使用して、SSL プロキシ リストに関する情報を表示します。すべての SSL プロキシ リストに関する一般的な情報と、特定の SSL プロキシ リストの詳細情報のいずれかを表示できます。

特定のコマンドモードで **show ssl-proxy-list** コマンドを入力すると、その SSL プロキシ リストの設定情報が表示されます。

- **show ssl-proxy-list** :
 - このコマンドを **ssl-proxy-list** モードで実行すると、その特定の SSL プロキシ リストの詳細な設定情報が表示されます。
 - グローバル モード、コンテンツ モード、所有者モード、サービス モード、スーパーユーザ モード、およびユーザ モードでは、既存のすべての SSL プロキシ リストの一般的な設定情報が表示されます。
- **show ssl-proxy-list [ssl-server|backend-server] {number}** : SSL プロキシ リストと、リスト内の仮想 SSL サーバやバックエンド サーバに関する詳しい設定情報を表示します。設定情報を表示する SSL またはバックエンド サーバを、番号で指定することもできます。このコマンドは、**ssl-proxy-list** モードで実行できます。
- **show ssl-proxy-list list_name** : 特定の SSL プロキシ リスト、およびそのリストに関連付けられたすべての仮想 SSL サーバに関する詳しい設定情報を表示します。このコマンドは、グローバル、所有者、サービス、スーパーユーザ、ユーザの各モードで使用できます。
- **show ssl-proxy-list list_name [ssl-server|backend-server] {number}** : SSL プロキシ リストと、リスト内のすべての仮想 SSL サーバまたはバックエンドサーバに関する詳しい設定情報を表示します。設定情報を表示する SSL またはバックエンドサーバを、番号で指定することもできます。このコマンドは、グローバル、所有者、サービス、スーパーユーザ、ユーザの各モードで使用できます。

設定されているすべての SSL プロキシ リストの一般的な情報を表示するには、次のコマンドを入力します。

```
# show ssl-proxy-list
```

表 7-7 に、**show ssl-proxy-list** コマンドで表示される各フィールドと、その説明を示します。

表 7-7 show ssl-proxy-list コマンドのフィールド

フィールド	内容
Name	SSL プロキシ リストの名前
Description	SSL プロキシ リストの説明
State	SSL プロキシ リストの状態 (active または suspended)
Services Associated	SSL プロキシ リストに関連付けられているサービス数
Rules Associated	SSL プロキシ リストに関連付けられているコンテンツルールの数

たとえば、**ssl-proxy-list** モードから *ssl_list1* に関する詳細な設定情報を表示するには、次のコマンドを入力します。

```
(config-ssl-proxy-list [ssl_list1])# show ssl-proxy-list
```

グローバル設定モードから *ssl_list1* に関する詳細な設定情報を表示するには、次のコマンドを入力します。

```
(config)# show ssl-proxy-list ssl_list1
```

表 7-8 に、**show ssl-proxy-list list_name** コマンドで表示される各フィールドと、その説明を示します。

表 7-8 show ssl-proxy-list コマンドのフィールド

フィールド	内容
Description	SSL プロキシ リストの説明
Number of SSL-Servers	SSL プロキシ リストに指定されている仮想 SSL サーバの合計数
SSL-Server	仮想 SSL サーバの一意の番号
Number of Backend-Servers	SSL プロキシ リストに指定されているバックエンドサーバの合計数

表 7-8 show ssl-proxy-list コマンドのフィールド (続き)

フィールド	内容
backend-server	バックエンド サーバの一意の番号
VIP Address	仮想 SSL サーバまたはバックエンド サーバの VIP アドレス (1 つの SSL プロキシ リストに対応)
VIP Port	仮想 SSL サーバまたはバックエンド サーバの仮想 TCP ポート (1 つの SSL プロキシ リストに対応)
Server Address	バックエンド SSL サーバの回線 IP アドレス
Server Port	SSL 接続を開始するために使用するバックエンド SSL サーバ ポート
Type	SSL のタイプ
RSA Certificate	RSA 証明書の名前
RSA Keypair	RSA キーの名前
DSA Certificate	DSA 証明書の名前
DSA Keypair	DSA キー ペアの名前
DH Param	Diffie-Hellman パラメータ アソシエーションの名前
Client Authentication	仮想 SSL サーバ上でのクライアント認証の状態 (enabled または disabled)
Client Authentication Failure	CSS によるクライアント認証失敗への応答方法 (ignore、redirect、reject)。デフォルトは reject です。
Authentication Redirect URL	クライアント認証失敗への応答方法を redirect に設定した場合に、CSS がクライアント接続をリダイレクトする URL
CA Certificate	クライアント認証のために CSS にインポートされた CA 証明書の名前
CRL	CRL レコードの名前
Session Cache Timeout	SSL セッション ID が失効するまでの時間の長さ (この時間が経過すると、CSS は完全な SSL ハンドシェイクを要求して、新しい SSL 接続を確立する)
SSL Version	指定した SSL (バージョン 3.0)、TLS (バージョン 1.0)、または使用中の SSL および TLS プロトコル

表 7-8 show ssl-proxy-list コマンドのフィールド (続き)

フィールド	内容
Re-handshake Timeout	SSL 再ハンドシェイク メッセージを開始するまでの CSS の待機時間
Re-handshake Data	CSS とクライアント間で交換されるデータの最大量(この量に達すると、CSS は SSL ハンドシェイク メッセージを送信し、SSL セッションを再確立する)
Virtual TCP Inactivity Timeout	ほとんど、あるいはまったく活動が存在しない、クライアントとの TCP 接続を終了するまでの CSS の待機時間
Virtual TCP Syn Timeout	データの転送前に TCP 3 ウエイ ハンドシェイクが正常に完了しなかった、クライアントとの TCP 接続を終了するまでの CSS の待機時間
Server TCP Inactivity Timeout	ほとんど、あるいはまったく活動が存在しない、サーバとの TCP 接続を終了するまでの CSS の待機時間
Server TCP Syn Timeout	データの転送前に TCP 3 ウエイ ハンドシェイクが正常に完了しなかった、サーバとの TCP 接続を終了するまでの CSS の待機時間
Cipher Suite(s)	SSL コンテンツ ルールに割り当てられた暗号スイートの名前 (サポートされているすべての暗号スイートと、個々の SSL サーバでの値については、表 4-1 参照)
Weight	暗号スイートに割り当てられている優先順位
Port	バックエンドの HTTP 接続を送信するときに使用するバックエンドのコンテンツ ルールの TCP ポート
Server	バックエンドの HTTP 接続を送信するときに使用するバックエンドのコンテンツ ルールの VIP アドレス
URL Rewrite Rule(s)	
Number	SSL サーバの URL リライト ルールの数
Rule	リダイレクトする URL のドメイン名
VIP Port	URL リライト ルールが一致したときに、HTTPS の場所を含むように HTTP Header Location フィールドを書き換えるために使用するポート

表 7-8 show ssl-proxy-list コマンドのフィールド (続き)

フィールド	内容
Clear Port	URL リライト ルールのマッチングを行うために使用するポート
Server	暗号スイートで使用されるバックエンドのコンテンツルールに割り当てられた IP アドレス
HTTP Header Insert Prefix	クライアント証明書、サーバ証明書、およびセッションフィールドのそれぞれの前に挿入される、設定済みのプレフィックス テキスト文字列
HTTP Header Insert	HTTP 要求ヘッダーに挿入されるフィールド情報のタイプ。Client Cert (クライアント証明書)、Server Cert (サーバ証明書)、または Session Data (SSL 接続情報)。ヘッダーに挿入されるフィールドの情報については、 第 4 章「SSL 終了の設定」 を参照。
HTTP Header Insert Static	HTTP 要求ヘッダーに挿入される設定済みのスタティック テキスト文字列
Default Field	クライアント証明書、サーバ証明書またはセッションフィールドの HTTP ヘッダー挿入を実行する場合のデフォルト文字列
HTTP Client-Cert Field	Default Field カラムに表示されるクライアント証明書フィールドに設定された文字列
HTTP Server-Cert Field	Default Field カラムに表示されるサーバ証明書フィールドに設定された文字列
HTTP Session Field	Default Field カラムに表示されるセッション フィールドに設定された文字列

CRL レコード設定の表示

すべての Certificate Revocation List (CRL; 証明書失効リスト) の設定を表示するには、**show ssl crl-record** コマンドを使用します。特定の CRL レコードの設定を表示するには、**show ssl crl-record name** コマンドを使用します。



(注) CRL が正常にダウンロードされたかどうかを確認するには、**show ssl statistics ssl** コマンドの出力と、CSS のシステムログ メッセージの内容を調べます。**show ssl statistics** コマンドの詳細については、「[SSL モジュール統計情報の表示](#)」を参照してください。

たとえば、すべての CRL レコードの設定を表示するには、次のように入力します。

```
(config) # show ssl crl-record
```

表 7-9 に、**show ssl crl-record** コマンドで表示される各フィールドと、その説明を示します。

表 7-9 show ssl crl-record コマンドのフィールド

フィールド	内容
CRL Record	設定済みの CRL レコード名
Signer Cert	CSS にインポートされた CA 証明書の名前。この証明書は、CRL が CA から発行されたことを証明します。
Update Delay	CSS 上の CRL を更新するまでの CSS の待機時間
CRL URL	CSS が最新の CRL をダウンロードする URL

SSL URL リライト統計情報の表示

1 つ以上の SSL モジュールの URL リライト ルールの統計情報を表示するには、**show ssl statistics** コマンドを使用します。このコマンドでは、SSL モジュールで受信し評価されたフロー数と、検出され書き換えられた HTTP 300 シリーズリダイレクトの数に関する統計が表示されます。

このコマンドのシンタックスは次のとおりです。

```
show ssl urlrewrite {slot number}
```

slot number オプションを指定すると、CSS 11503 または CSS 11506 シャーシ内の特定の SSL モジュールの URL リライトに関する情報が表示されます（複数のモジュールが装着されていることが前提になります）。有効なスロット番号は、2 および 3（CSS 11503）または 2～6（CSS 11506）です。スロット番号を指定しないで **show ssl urlrewrite** コマンドを実行すると、シャーシ内のすべての SSL モジュールの URL リライト統計情報が表示されます。

たとえば、すべての SSL モジュールの URL リライト統計情報を表示するには、次のコマンドを入力します。

```
# show ssl urlrewrite
```

たとえば、CSS 11506 のスロット 5 にある SSL モジュールの URL リライト統計情報を表示するには、次のコマンドを入力します。

```
# show ssl urlrewrite slot 5
```


表 7-10 に、`show ssl urlrewrite` コマンドで表示される各フィールドと、その説明を示します。

表 7-10 `show ssl urlrewrite` コマンドのフィールド

フィールド	内容
Virtual	仮想 SSL サーバの VIP アドレス
Port	仮想 SSL サーバの 仮想 TCP ポート
Searches	バックエンド サーバから受信したフローのうち、SSL モジュールで HTTP 300 シリーズ リダイレクトの有無が評価されたフローの総数
Redirects Found	SSL モジュールで HTTP 300 シリーズ リダイレクトが存在するかを調べ、それが検出されたフローの総数
Redirects Rewritten	SSL モジュールで調べたフローのうち、設定した URL リライト ルールの 1 つと一致した HTTP 300 シリーズ リダイレクトがあったものの総数。この数は、この VIP アドレスで書き換えられたリダイレクトの総数を表します。

SSL モジュール統計情報の表示

show ssl statistics コマンドを使用して、1 つ以上の SSL モジュールの暗号化コンポーネントおよびクライアント認証の統計情報を表示します。このコマンドをオプションなしで実行すると、CSS シャーシ内のすべての SSL モジュールに関する統計情報が表示されます。

このコマンドのシンタックスは次のとおりです。

```
show ssl statistics {component} {slot number}
```

このコマンドのオプションと変数は次のとおりです。

- *component* : 統計情報を表示する、SSL モジュール内の特定のコンポーネント。次のコンポーネントがあります。
 - **backend-session-cache** : CSS がクライアントとして動作するバックエンド SSL または SSL 開始についてのカウンタ統計情報を表示する。
 - **crypto** : 暗号化チップのカウンタ統計情報を表示する。
 - **session-cache** : CSS が SSL サーバとして動作する SSL 終了についてのカウンタ情報を表示する。
 - **ssl** : SSL サーバカウンタのカウンタ統計情報を表示する。
 - **ssl-proxy-server** : SSL モジュールに SSL 終了を提供する SSL プロキシリスト コンポーネントのカウンタ統計情報を表示する。
- *slot number* : CSS シャーシ内の特定の SSL モジュールのコンポーネントに関する統計情報を表示する（複数のモジュールが装着されていることが前提）。**show ssl statistics** コマンドの直後に、必ず *slot number* を指定します。有効なスロット番号は、2 および 3（CSS 11503）または 2～6（CSS 11506）です。スロット番号を指定しないで **show ssl statistics** コマンドを実行すると、装着されているすべての SSL モジュールの統計情報が表示されます。

たとえば、CSS シャーシのスロット 5 にある SSL モジュールの SSL 統計情報をすべて表示するには、次のコマンドを入力します。

```
# show ssl statistics slot 5
```

表 7-11 に、**show ssl statistics** コマンドで表示される各フィールドと、その説明を示します。

表 7-11 show ssl statistics コマンドのフィールド

フィールド	内容
Component	<p>統計情報を表示する SSL モジュールの特定のコンポーネントを示します。SSL 統計情報機能は、次のとおりです。</p> <ul style="list-style-type: none"> • ssl-proxy-server : SSL モジュールに SSL 終了を提供する SSL プロキシ リスト コンポーネントのカウント統計情報を表示する。 • crypto : SSL モジュールの暗号化チップのカウント統計情報を表示する。 • ssl : SSL サーバ カウンタのカウント統計情報を表示する。
Slot	<p>統計情報を表示する SSL モジュールのスロット番号を示します。有効なスロット番号は、2 (CSS 11501)、2 および 3 (CSS 11503)、または 2 ~ 6 (CSS 11506) です。</p>

SSL プロキシ リスト統計情報

Handshake started for incoming SSL connections	クライアントから SSL モジュールへの着信 SSL 接続で、ハンドシェイク プロセスが開始された回数
Handshake completed for incoming SSL connections	クライアントから SSL モジュールへの着信 SSL 接続で、ハンドシェイク プロセスが完了した回数
Handshake started for outgoing SSL connections	SSL モジュールからクライアントへの発信 SSL 接続で、ハンドシェイク プロセスが開始された回数
Handshake completed for outgoing SSL connections	SSL モジュールからクライアントへの発信 SSL 接続で、ハンドシェイク プロセスが完了した回数
HTTP header insert of session data	バックエンド サーバに送信する HTTP 要求のヘッダーに、CSS が SSL 接続データ情報を挿入した回数
HTTP header insert of client certificate data	バックエンド サーバに送信する HTTP 要求のヘッダーに、CSS がクライアント証明書情報を挿入した回数
HTTP header insert of server certificate data	バックエンド サーバに送信する HTTP 要求のヘッダーに、CSS がサーバ証明書情報を挿入した回数

表 7-11 show ssl statistics コマンドのフィールド (続き)

フィールド	内容
HTTP header insert of user defined prefix	バックエンド サーバに送信する HTTP 要求のヘッダーに、CSS がプレフィックス フィールドを挿入した回数
HTTP header insert of static phrase	バックエンド サーバに送信する HTTP 要求のヘッダーに、CSS が設定済みのスタティック テキストを挿入した回数
Active SSL flows high water mark	CSS 上のアクティブな SSL フローの最大数
暗号化統計情報	
RSA Private	要求された RSA 秘密キーの計算数
RSA Public	要求された RSA 公開キーの計算数
DH Shared	要求された Diffie-Hellman 共有秘密キーの計算数
DH Public	要求された Diffie-Hellman 公開キーの計算数
DSA Sign	要求された DSA 署名数
DSA Verify	要求された DSA 検証数
SSL MAC	要求された SSL MAC の計算数
TLS HMAC	要求された TLS HMAC の計算数
3DES	要求された 3 DES の計算数
ARC4	要求された ARC4 の計算数
HASH	要求されたピュア ハッシュの計算数
RSA Private Failed	失敗した RSA 秘密キーの計算数
RSA Public Failed	失敗した RSA 公開キーの計算数
DH Shared Failed	失敗した Diffie-Hellman 共有秘密キーの計算数
DH Public Failed	失敗した Diffie-Hellman 公開キーの計算数
DSA Sign Failed	失敗した DSA 署名の数
DSA Verify Failed	失敗した DSA 検証の数
SSL MAC Failed	失敗した SSL MAC の計算数
TLS HMAC Failed	失敗した TLS HMAC の計算数
3DES Failed	失敗した 3 DES の計算数

表 7-11 show ssl statistics コマンドのフィールド (続き)

フィールド	内容
ARC4 Failed	失敗した ARC4 の計算数
HASH Failed	失敗したピュア ハッシュの計算数
Hardware Device Not Found	暗号化ハードウェアが呼び出され、利用可能なハードウェア アクセラレーション デバイスが見つからなかった回数
Hardware Device Timed Out	暗号化ハードウェアが指定した時間内にアクセラレーション要求を完了できなかった回数。この機能は、現時点では実装されていません。このカウンタは常に 0 です。
Invalid Crypto Parameter	CSS から無効なパラメータでハードウェア アクセラレーション機能が要求された回数。無効なパラメータには、処理できない無効なビット長、長さが 4 バイトの倍数以外のバッファ、偶数の 4 バイト境界で始まらないバッファ、フラグメントが過度に多いか、または過度に少ない (入力なしなど) バッファへの操作要求、無効な (意味のない) 機能の要求などがあります。
Hardware Device Failed	ハードウェア アクセラレーション デバイスで障害が発生した回数。このカウンタは、DMA エラーだけをカウントします。
Hardware Device Busy	ハードウェア アクセラレーション デバイスがビジーで、アクセラレーション要求を受け入れられなかった回数
Out Of Resources	利用できるハードウェア バッファがなく、暗号化ハードウェアでアクセラレーション要求を受け入れられなかった回数
Cancelled -- Device Reset	CSS のリブートのために cancelled ステータスが返された回数
SSL 統計情報	
RSA Private Decrypt calls	RSA 秘密復号化呼び出しの数
RSA Public Decrypt calls	RSA 公開暗号化呼び出しの数

表 7-11 show ssl statistics コマンドのフィールド (続き)

フィールド	内容
DH Compute key calls	Diffie-Hellman 計算キー呼び出しの数
DH Generate key calls	Diffie-Hellman 生成キー呼び出しの数
DSA Verify calls	DSA 検証呼び出しの数
DSA Sign calls	DSA 署名呼び出しの数
MD5 raw hash calls	MD5 のピュア ハッシュ呼び出しの数
SHA1 raw hash calls	SHA1 ピュア ハッシュ呼び出しの数
3-DES calls	3-DES 呼び出しの数
RC4 calls	RC4 呼び出しの数
SSL MAC (MD5) calls	MD5 アルゴリズムを使用した SSL メッセージ認証コード (MAC) の計算数
SSL MAC (SHA1) calls	SHA アルゴリズムを使用した SSL MAC の計算数
TLS MAC (MD5) calls	MD5 アルゴリズムを使用した TLS MAC の計算数
TLS MAC (SHA1) calls	SHA アルゴリズムを使用した TLS MAC の計算数
Level 1 Alerts Received	レベル 1 アラートの受信数
Level 2 Alerts Received	レベル 2 アラートの受信数
Level 1 Alerts Sent	レベル 1 アラートの送信数
Level 2 Alerts Sent	レベル 2 アラートの送信数
SSL received bytes from TCP	SSL が TCP から受信したバイト数
SSL transmitted bytes to TCP	SSL が TCP へ送信したバイト数
SSL received Application Data bytes	SSL モジュールで受信したアプリケーションデータのバイト数
SSL transmitted Application Data bytes	SSL モジュールから送信したアプリケーションデータのバイト数
SSL received non-application data bytes	SSL モジュールで受信したアプリケーション以外のデータ (ハンドシェイク、アラート、および変更暗号) のバイト数

表 7-11 show ssl statistics コマンドのフィールド (続き)

フィールド	内容
SSL transmitted non-application data bytes	SSL モジュールから送信したアプリケーション以外のデータ (ハンドシェイク、アラート、および変更暗号) バイトの数
RSA Private Decrypt failures	失敗した RSA 秘密復号化呼び出しの数
MAC failures for packets received	着信 SSL メッセージの MAC を検証できなかった回数
Rehandshake TimerAlloc failed	SSL モジュールが再ハンドシェイク タイマーを割り当てできなかった回数
Successful client authentications	CSS がクライアント証明書を認証した回数
Client authentication failures	CSS がクライアント証明書を認証できなかった回数
Unknown issuer certificates	CSS がクライアント証明書の発行元を識別できなかった回数
Signature unable to decrypt	CSS がクライアント証明書のシグニチャを復号化できなかった回数
Invalid issuer keys	CSS がクライアント証明書の無効なキーを検出した回数
Not yet valid certificate	CA によって検証されていない証明書を CSS が受信した回数
Expired certificates	期限切れのタイム スタンプ付きの証明書を CSS が受信した回数
Revoked certificate	発行元によって取り消されたクライアント証明書を CSS が受信した回数
CRLs not obtained from host	CSS がホストから CRL を取得しようとしたときにタイムアウトが発生した回数
CRLs obtained but failed to load	CSS が正常に CRL を取得したが、ロードに失敗した回数

表 7-11 show ssl statistics コマンドのフィールド (続き)

フィールド	内容
CRLs with invalid signatures	CSS が、CSS 上の署名者証明書で CRL の署名者を検証できなかった回数
CRL out of memory error	SSL モジュールがメモリ不足で CRL を保存できなかった回数。CRL をメモリに保持できないと、着信するすべてのクライアント認証は失敗します。
セッション キャッシュの統計情報	
Handshakes Accepted from Client	SSL モジュールがクライアントから受け付けたハンドシェイクの数
Handshakes Renegotiated	SSL モジュールが再ネゴシエートしたハンドシェイクの数
Handshakes Completed	SSL モジュールがクライアントとの間で正常に完了したハンドシェイクの数
Session ID Misses	ピアからオファーされ、キャッシュ内を調べたが、見つからなかったセッション ID の数
Session ID Timeouts	タイムアウトに達して失効したキャッシュ内のセッションの数
Session Cache Full	キャッシュが上限に達した回数
Session ID Hits	ピアによってオファーされ、SSL モジュールがキャッシュ内で見つけたセッション ID の数
Total Number of Items Cached	キャッシュ内のセッションの合計数
バックエンドセッション キャッシュの統計情報	
Handshakes Sourced to Server	SSL モジュールがサーバにオファーしたハンドシェイクの数
Handshakes Renegotiated	SSL モジュールが再ネゴシエートしたハンドシェイクの数
Handshakes Completed	SSL モジュールがサーバとの間で正常に完了したハンドシェイクの数
Session ID Misses	サーバに送信する既存の有効なセッション ID が存在しなかった回数

表 7-11 show ssl statistics コマンドのフィールド (続き)

フィールド	内容
Session ID Timeouts	タイムアウトに達して失効したキャッシュ内のセッションの数
Session Cache Full	キャッシュが上限に達した回数
Session ID Hits	サーバにオファーする有効なセッション ID が存在した回数
Total Number of Items Cached	キャッシュ内のセッションの合計数

SSL 統計情報のクリア

clear ssl statistics コマンドを使用して、CSS シャーシにあるすべての SSL モジュールに関する SSL 統計情報の内容をクリアします。**show ssl statistics** コマンドの出力で、リセットされた統計情報は 0 になります。

特定のモジュールの SSL 統計情報をクリアするには、**clear ssl statistics** コマンドの直後に **slot number** を指定します。有効なスロット番号は、2 および 3 (CSS 11503) または 2 ~ 6 (CSS 11506) です。

SSL 統計情報カウンタをクリアするには、次のコマンドを入力します。

```
# clear ssl statistics
```

SSL フローの表示

show ssl flows コマンドを使用して、各 VIP アドレス、ポート、および SSL モジュールのアクティブなフローに関する情報を表示します。出力には、TCP プロキシフロー、アクティブな SSL フロー (TCP プロキシフローのサブセット)、およびプロトコルのハンドシェイク フェーズで発生する SSL フロー (アクティブな SSL フローのサブセット) が表示されます。

このコマンドのシンタックスは次のとおりです。

```
show ssl flows {slot number}
```

slot number オプションを指定すると、CSS シャーシ内の特定の SSL モジュールのアクティブなフローに関する情報が表示されます (複数のモジュールが装着されていることが前提)。有効なスロット番号は、2 および 3 (CSS 11503) または 2 ~ 6 (CSS 11506) です。スロット番号を指定しないで **show ssl flows** コマンドを実行すると、装着されているすべての SSL モジュールの統計情報が表示されます。

CSS のすべての SSL の SSL フローを表示するには、次のコマンドを入力します。

```
# show ssl flows
```

CSS シャーシ内の特定の SSL モジュール、たとえばスロット 5 に取り付けられたモジュールの SSL フローを表示するには、次のコマンドを入力します。

```
# show ssl flows slot 5
```

表 7-12 に、`show ssl flow` コマンドで表示される各フィールドと、その説明を示します。

表 7-12 `show ssl flows` コマンドのフィールド

フィールド	内容
SSL Acceleration Flows for Slot	フローを表示する SSL モジュールのスロット番号。有効なスロット番号は、2 (CSS 11501)、2 および 3 (CSS 11503)、または 2 ~ 6 (CSS 11506) です。
Virtual	SSL サーバの仮想アドレス
Port	SSL サーバの仮想 TCP ポート
TCP Proxy Flows	SSL 仮想 IP アドレスで代行されている TCP 接続の数。これらの接続は次のいずれかの状態にあります。 <ul style="list-style-type: none"> • TCP ハンドシェイクまたはティアダウンフェーズ (SSL トラフィックを搬送していない状態) • 確立済み TCP フェーズ (SSL トラフィックを搬送している状態)
Active SSL Flows	アクティブな SSL 接続を搬送している TCP プロキシフローの現在の数。これらのフローは、SSL Client Hello メッセージが CSS で受信された確立済みの TCP 接続です。SSL フローは、SSL アラートメッセージの送信または受信によってティアダウンプロセスが開始されるまで、このアクティブな状態のまま変わりません。Active SSL Flows の数は、TCP Proxy Flows カラムのサブセットです。
SSL Flows in Handshake	SSL プロトコルのハンドシェイク フェーズにあり、まだデータを送信していないアクティブな SSL フローの現在の数。SSL Client Hello メッセージは CSS で受信されたが、最終的な完了メッセージはまだ送信されていない状態です。SSK Flows in Handshake の数は、Active SSL Flows カラムのサブセットです。

