CHAPTER 6

SSL 情報および統計情報の表示

（注） この章の情報は、特に記載のない限り、ACE モジュールと ACE アプライアンスの両方に適用されます。

この章では、使用可能な **show** コマンドを使用して、ACE にロードされた証明書やキー ペア ファイルなどの SSL 関連情報を表示する方法について説明します。**show** コマンドは、コンテキストに関連する情報を表示します。このコンテキストに基づいて、コマンドが実行されます。この章で説明する各コマンドには、コマンド出力の説明も含まれます。

show コマンドは EXEC モード コマンドですが、**do** コマンドを使用して任意のコンフィギュレーション モードから **show** コマンドを実行できます。次に、EXEC モードまたはコンフィギュレーション モードから **show running-config** コマンドを実行する例を示します。

EXEC モードからの入力例

```
host1/Admin# show running-config
```

コンフィギュレーション モードからの入力例

```
host1/Admin(config)# do show running-config
```

この章の内容は、次のとおりです。

- CSR パラメータ セットの設定の表示
- 証明書とキー ペア ファイルのリストの表示
- 証明書情報の表示
- CRL 情報の表示

- CDP エラー統計情報の表示
- OCSP 情報の表示
- RSA キー ペア情報の表示
- 証明書チェーン グループ情報の表示
- クライアント認証グループの情報の表示
- キャッシュされた TLS および SSL セッション エントリの表示
- フロントエンドおよびバックエンドの SSL 統計情報の表示
- SSL HTTP ヘッダー挿入および切り捨てられたカウンタに関する情報
- HTTP ヘッダー挿入の統計情報の表示

CSR パラメータ セットの設定の表示

CSR パラメータ セットのサマリー レポートと詳細レポートを表示するには、EXEC モードで **show crypto csr-params** コマンドを使用します。

このコマンドの構文は次のとおりです。

show crypto csr-params {*params_set* | **all**}

引数およびキーワードは次のとおりです。

- *params_set*：引数は特定の CSR パラメータ セットです。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。ACE では、指定された CSR パラメータ セットの詳細レポートが表示されます。詳細レポートには CSR パラメータ セットの識別名の属性が含まれます。
- 現在のコンテキストのすべての CSR パラメータ セットを一覧表示するサマリー レポートを表示するには、CSR パラメータ セットを指定せずにコマンドを入力します。

たとえば、CSR パラメータ セットのサマリー レポートを表示するには、次のように入力します。

```
host1/Admin# show crypto csr-params all
```

次に、MYCSRCONFIG CSR パラメータ セットの詳細レポートを表示する例を示します。

```
host1/Admin# show crypto csr-params MTCSRCONFIG
```

表 6-1 に、**show crypto csr-params** コマンド出力に含まれるフィールドの説明を示します。

表 6-1　show crypto csr-params config_name コマンドのフィールドの説明

フィールド	説明
Country-name	証明書所有者が存在する国。
State	証明書所有者が存在する州。
Locality	証明書所有者が存在する地域。
Org-name	組織の名前（証明書所有者またはサブジェクト）。
Org-unit	組織内のユニットの名前。
Common-name	通常名（SSL サイトのドメイン名または個別のホスト名）。
Serial number	シリアル番号。
Email	E-mail Address（電子メール アドレス）。

証明書とキー ペア ファイルのリストの表示

すべての使用可能な証明書とキー ペア ファイルのリストを表示するには、EXEC モードで **show crypto files** コマンドを使用します。

たとえば、証明書とキー ペア ファイルのリストを表示するには、次のように入力します。

```
host1/Admin# show crypto files
```

表 6-2 に、**show crypto files** コマンド出力に含まれるフィールドの説明を示します。

表 6-2　show crypto files のフィールドの説明コマンド

フィールド	説明
Filename	証明書またはキー ペアを含むファイルの名前。
File Size	ファイルのサイズ
File Type	ファイルの形式（PEM、DER、または PKCS12）。

表 6-2　show crypto files のフィールドの説明コマンド（続き）

フィールド	説明
Exportable	**crypto export** コマンドを使用して ACE からファイルをエクスポートできるかどうかを示します。 • **Yes**：FTP、SFTP、または TFP サーバにファイルをエクスポートできます（第 2 章「証明書およびキーの管理」の「証明書とキー ペア ファイルのエクスポート」の項を参照）。 • **No**：保護されているためファイルをエクスポートできません。
Key/Cert	ファイルが証明書（CERT）、キー ペア（KEY）、またはその両方（BOTH）を含むかどうかを示します。

証明書情報の表示

証明書のサマリー レポートと詳細レポートを表示するには、EXEC モードで **show crypto certificate** コマンドを使用します。

このコマンドの構文は次のとおりです。

show crypto certificate {*filename* | **all**}

次のキーワードと引数があります。

- *filename*：特定の証明書ファイルの名前。最大 40 文字の英数字からなる文字列を引用符で囲まずに入力します。ACE では、指定されたファイルに対する証明書の詳細レポートが表示されます。証明書ファイルにチェーンが含まれる場合、ACE では最下位の証明書だけが表示されます（署名者は表示されません）。
- **all**：現在のコンテキストのすべての証明書ファイルを一覧表示する、証明書のサマリー レポートを表示します。

たとえば、証明書のサマリー レポートを表示するには、次のように入力します。

```
host1/Admin# show crypto certificate all
```

表 6-3 に、**show crypto certificate all** コマンド出力に含まれるフィールドの説明を示します。

表 6-3　show crypto certificate all コマンドのフィールドの説明

フィールド	説明
Certificate file	証明書ファイルの名前。
Subject	証明書を所有し、秘密キーを保持している組織の識別名。
Issuer	証明書を発行した認証局（CA）の識別名。
Not Before	開始期間。この期間の前は、証明書は有効とは見なされません。
Not After	終了期間。この期間の後は、証明書は有効とは見なされません。
CA Cert	証明書に署名した CA の証明書。

次に、MYCERT.PEM 証明書ファイルの詳細レポートを表示する例を示します。

```
host1/Admin# show crypto certificate MYCERT.PEM
```

表 6-4 に、**show crypto certificate** *filename* コマンド出力に含まれるフィールドの説明を示します。

表 6-4　show crypto certificate filename コマンドのフィールドの説明

フィールド	説明
Certificate	証明書ファイルの名前。
Data	
Version	X.509 標準のバージョン。証明書は標準のこのバージョンに準拠します。
Serial Number	証明書に関連付けられたシリアル番号。
Signature Algorithm	公開キー / 秘密キーのキー ペアによる情報の暗号化に使用するデジタル署名アルゴリズム。
Issuer	証明書を出力した CA の識別名。
Validity	
Not Before	開始期間。この期間の前は、証明書は有効とは見なされません。

表 6-4　show crypto certificate filename コマンドのフィールドの説明 （続き）

フィールド	説明
Not After	終了期間。この期間の後は、証明書は有効とは見なされません。
Subject	証明書を所有し、秘密キーを保持している組織の識別名。
Subject Public Key Info	
Public Key Algorithm	公開キーの生成に使用するキー交換アルゴリズムの名前（RSA など）。
RSA Public Key	Web トランザクションを保護するために使用される RSA キー ペアのサイズを定義するキーのビット数。
Modulus	証明書が作成された実際の公開キー。
Exponent	キーを生成するために使用するベース数の 1 つ。
X509v3 Extensions	証明書に追加される X509v3 拡張の配列。
X509v3 Basic Constraints	証明書の署名の確認に使用される認証済み公開キーを使用して、サブジェクトが CA として機能する可能性があるかどうかを示します。その場合、認証パス長の制限が指定されることもあります。
Netscape Comment	証明書が表示されたときに表示されることがあるコメント。
X509v3 Subject Key Identifier	認証される公開キー。これにより、同じサブジェクトで使用される別々のキーを区別できます（キーの更新の発生時など）。
X509v3 Authority Key Identifier	この証明書または CRL の署名の確認に使用される公開キー。これにより、同じ CA で使用される別々のキーを区別できます（キーの更新の発生時など）。
Signature Algorithm	キー交換ではなく、デジタル署名に使用されるアルゴリズムの名前。
Hex Numbers	証明書の実際の署名。証明書データが変更されていないことを確認するために、クライアントは指定されたアルゴリズムを使用してこの署名を再生成できます。

CRL 情報の表示

証明書失効リスト（CRL）またはコンテキスト内で指定された CRL の定義のリストを表示するには、EXEC モードで **show crypto crl** コマンドを使用します。このコマンドの構文は次のとおりです。

show crypto crl {*crl_name* [**detail**] | **all** | **best-effort**}

次のキーワードと引数があります。

- *crl_name*：コンテキストで設定されている特定の CRL の名前。英数字の文字列を引用符で囲まずに入力します。ACE では、指定された CRL の定義が表示されます。
- **detail**：（任意）障害カウンタを含む CRL ダウンロードの詳細な統計情報を表示します。
- **all**：コンテキストで設定されているすべての CRL のリストを表示します。
- **best-effort**：ACE 上のすべてのベストエフォート CRL の要約情報を表示します（最大 16 CRL）。

たとえば、すべての CRL のリストを表示するには、次のように入力します。

```
host1/Admin# show crypto crl all
```

特定の CRL（CRL1 など）の定義を表示するには、次のように入力します。

```
host1/Admin# show crypto crl CRL1
```

表 6-5 に、**show crypto crl** *crl_name* コマンド出力に含まれるフィールドの説明を示します。

表 6-5　show crypto crl コマンドのフィールドの説明

フィールド	説明
URL	ACE が CRL をダウンロードする URL。
Last Downloaded	ACE が CRL を最後にダウンロードしたとき。アクティブでないポリシー マップの SSL プロキシ サービスで CRL が設定されているか、SSL プロキシ サービスがポリシー マップに関連付けられていない場合、フィールドには「not downloaded yet」というメッセージが表示されます。

表 6-5　show crypto crl コマンドのフィールドの説明 （続き）

フィールド	説明
Total Number of Download Attempts	ACE が CRL をダウンロードしようとした回数。
Failed Download Attempts	ACE が CRL のダウンロードに失敗した回数。
Total Number of Download Attempts for Real CRL Data	指定された CRL を ACE がダウンロードしようとした回数（「ベスト エフォート」の試行は含まず）。
Failed Download Attempts for Real CRL Data	指定された CRL のダウンロードに ACE が失敗した回数（「ベスト エフォート」の試行は含まず）。
Successful Loads（**detail** オプション）	ACE が CRL を正常にロードした回数。
Failed Loads（**detail** オプション）	エラーが原因で ACE が CRL をロードできなかった回数。
Hours since Last Load（**detail** オプション）	ACE が最後に正常に CRL をダウンロードしてから経過した時間数。正常なダウンロードが発生しなかった場合、このフィールドには NA（適用なし）が表示されます。
No IP Addr Resolutions（**detail** オプション）	CRL のサーバ ホスト アドレスの DNS 解決に失敗した回数。
Host Timeouts（**detail** オプション）	タイム アウトした CRL へのダウンロード再試行の回数。
Next Update Invalid（**detail** オプション）	CRL の [Next Update] フィールドが無効になった回数。
Next Update Expired（**detail** オプション）	CRL の [Next Update] フィールドが期限切れになった回数。
Bad Signature（**detail** オプション）	CRL の署名検証用に設定された CA 証明書に関連して、CRL の署名の不一致が検出された回数。
CRL Found-Failed to load（**detail** オプション）	ACE の最大サイズ制限（10 MB）または CRL の形式が認識されなかったことが原因で、ACE が CRL をロードできなかった回数。ACE は DER および PEM 形式で符号化された CRL のみを認識します。

表 6-5　show crypto crl コマンドのフィールドの説明 （続き）

フィールド	説明
File Not Found（**detail** オプション）	サーバが、CRL ファイルがサーバ上に見つからなかったと応答した回数。
Memory Outage failures（**detail** オプション）	CRL データを保存するためのメモリを一時的に提供できなかったため、ACE が CRL のダウンロードに失敗した回数。
Cache Limit failures（**detail** オプション）	CRL キャッシュが使い果たされたために ACE が CRL をロードできなかった回数。
Conn Failures（**detail** オプション）	サーバとの接続を確立できなかったか、宛先システムでリッスンしてるサーバ エンティティがなかったため、ACE が CRL のダウンロードに失敗した回数。
Internal Failures（**detail** オプション）	CRL のダウンロードを妨げた ACE の内部エラー数。CRL のダウンロードを行うコンポーネント間の内部通信エラーなどがあります。
Not Eligible for download（**detail** オプション）	次の条件によって、CRL にダウンロード資格がないことが検出された回数。 • 同じ CRL のダウンロードが進行している。 • CRL がすでに正常にロードされ、まだ期限切れになっていない。
HTTP Read Failures（**detail** オプション）	サーバとの間で確立された接続でデータを読み取ることができなかったため、CRL をダウンロードするときに ACE でエラーが発生した回数。
HTTP Write failures（**detail** オプション）	サーバとの間で確立された接続から CRL ダウンロード要求を作成できなかったため、CRL をダウンロードするときに ACE でエラーが発生した回数。

たとえば、すべてのベストエフォート CRL の要約情報を表示するには、次のように入力します。

```
host1/Admin# show crypto crl best-effort
```

表 6-6 に、**show crypto crl best-effort** コマンド出力に含まれるフィールドの説明を示します。

表 6-6　show crypto crl best-effort コマンドのフィールドの説明

フィールド	説明
Best Effort CRL	現時点で存在する各ベストエフォート CRL を区別する ID。同じ CRL でも、別の時点で ID が異なる場合があります。
CRL Distribution Point	CDP の URL。ACE は URL の先頭 255 文字を表示します。
CRL Downloaded	CRL が ACE にダウンロードされているかどうかを Yes または No で示します。
CRL Issuer Name	CRL 発行元の名前。ACE は名前の先頭 255 文字を表示します。
Last Update	CRL から取得した [Last Update] フィールドの内容。ACE は、フィールドの最初の 64 文字を表示します。
Next Update	CRL から取得した [Next Update] フィールドの内容。ACE は、フィールドの最初の 64 文字を表示します。

ベストエフォート CRL が ACE サービス モジュールにない場合、ACE サービス モジュールは次のメッセージを表示します。

```
No best effort crl present in the system
```

（注）　使用中の CRL の有効期限が切れたときに ACE がクライアント証明書を拒否するかどうかを表示するには、**show parameter-map** コマンドを使用します。

CDP エラー統計情報の表示

CRL 分散ポイント（CDP）は、URL の形式で CRL の場所を示します。証明書の CDP の解析は、ベストエフォート CRL が使用中のときにのみ発生します。証明書の CDP の不一致の統計情報を表示するには、**show crypto cdp-errors** コマンドを使用します。

たとえば、CDP 統計情報を表示するには、次のように入力します。

```
host1/Admin# show crypto cdp-errors
```

表 6-7 に、**show crypto cdp-errors** コマンド出力に含まれるフィールドの説明を示します。

表 6-7　show crypto cdp-errors のフィールドの説明コマンド

フィールド	説明
Incomplete	CDP で、ホスト、ファイル名、基本情報などの CRL をダウンロードするために必要な情報が不足した回数。
Malformed	誤った属性またはベース情報を指定するなど、エラーを含む情報で CDP が不正な形式になった回数。このカウンタには、255 文字の ACE の長さ制限を超えた URL を持つ CDP も含まれます。切り捨てられた URL は誤った CRL を指すことがあります。
Unrecognized Transports	CRL に対する CDP の転送メカニズムを ACE サービスモジュールが認識またはサポートしない回数。
Missing from cert	CDP が証明書から失われた回数。
Best Effort CDP Errors Ignored	提示された証明書の CDP エラーを ACE サービス モジュールが無視し、それによって SSL 接続が許可された回数。このフィールドは、パラメータ マップ SSL コンフィギュレーション モードの **cdp-errors ignore** コマンドに関連しています。

OCSP 情報の表示

次の項で説明されている show コマンドを使用して、Online Certificate Status Protocol（OCSP）の情報を表示できます。

- OCSP サーバの統計情報の表示
- AuthorityInfoAccess 拡張エラーの統計情報の表示

OCSP サーバの統計情報の表示

OCSP サーバの統計情報を表示するには、EXEC モードで **show crypto ocspserver** コマンドを使用します。このコマンドの構文は次のとおりです。

show crypto ocspserver {*name* [**detail**] | **all** | **best-effort**}

次のキーワードと引数があります。

- *name*：設定されている OCSP サーバの ID。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
- **detail**：指定された OCSP サーバの詳細な統計情報を表示するように ACE に指示します。
- **all**：すべての設定された OCSP サーバの統計情報を表示します。
- **best-effort**：クライアント パケットからサーバ情報を取得してベストエフォート方式で取得された OCSP サーバの統計情報を表示します。

表 6-8 に、**show crypto ocspserver name detail** コマンド出力に含まれるフィールドの説明を示します。

表 6-8　show crypto ocspserver コマンドのフィールドの説明

フィールド	説明
Name	設定されている OCSP サーバの ID。
URL	OCSP サーバの URL。
Connection State	OCSP サーバへの接続の状態。取り得る値は、Connected または Not Connected です。状態が Connected の場合は、これに続く [Connected Since] フィールドが指定されます。そうでない場合は表示されません。
Connected Since	OCSP サーバとの既存の接続が確立された日時。
Total Number of Connection Attempts	OCSP サーバとの接続試行の総数。
Failed Connections	失敗した OCSP サーバとの接続試行の数。
Nonce	ナンスの状態（有効または無効）。
Req signer cert	OCSP サーバへの発信要求に署名するための、設定された署名者の証明書ファイル名。

表 6-8　show crypto ocspserver コマンドのフィールドの説明 （続き）

フィールド	説明
Req signer key	OCSP サーバへの発信要求に署名するための、設定された署名者の秘密キー ファイル名。
Resp sign.verifier	OCSP サーバの応答の署名を検証する設定された証明書。
Inactivity timeout	設定されている接続無活動タイムアウト。
Successful Connections	成功した OCSP サーバとの接続試行の数。
No IP Addr Resolutions	ホスト アドレスに対応する IP アドレスが正常に取得できなかった回数。
Host Timeouts	OCSP サーバとの接続を確立している間に、接続がタイム アウトした回数。
Conn Failures	ACE サービス モジュールが OCSP サーバとの接続を正常に確立することを妨げた接続コール エラーの数。
Internal Failures	ACE サービス モジュールが OCSP サーバとの接続を正常に確立することを妨げた内部エラーの数。
HTTP Read Failures	HTTP 読み取りコール エラーによる接続エラーの数。
HTTP Write Failures	HTTP 書き込みコール エラーによる接続エラーの数。
Inactivity timeouts	無活動が原因で OCSP サーバとの接続が終了した回数。
Requests sent	ACE サービス モジュールが OCSP サーバに送信した要求の総数。
Non-OCSP Responses	ACE で受信された非 OCSP 応答の数。
OCSP Responses	ACE で受信された OCSP 応答の数。
Malformed OCSP Responses	ACE で受信された不正な形式の OCSP 応答の数。
Nonce Mismatches	OCSP 応答がナンス文字列と一致しなかった回数。
Response verify failures	OCSP 応答が応答の署名検証に失敗した回数。
Unreliable OCSP Responses	OCSP 応答が信頼できないことが判明した回数。

表 6-8　show crypto ocspserver コマンドのフィールドの説明 （続き）

フィールド	説明
Revoked responses	証明書の失効ステータスが Revoked として示された応答の数。
Non-revoked responses	証明書の失効ステータスが非失効として示された応答の数。
Status unknown responses	サーバがクライアント（または提供された）証明書の状態を判定できなかった回数。

たとえば、OCSP_SERV1 サーバの統計情報を表示するには、次のコマンドを入力します。

```
host1/Admin# show crypto ocspserver OCSP_SERV1 detail
```

AuthorityInfoAccess 拡張エラーの統計情報の表示

AuthorityInfoAccess（AIA）拡張エラーの統計情報を表示するには、EXEC モードで **show crypto aia-errors** コマンドを使用します。このコマンドの構文は次のとおりです。

show crypto aia-errors

表 6-9 に、**show crypto aia-errors** コマンド出力に含まれるフィールドの説明を示します。

表 6-9　show crypto aia-errors コマンドのフィールドの説明

フィールド	説明
Incomplete	AIA に必要な情報が不足した回数。
Malformed	AIA の形式が誤っているか、エラーを含む情報が格納された回数。
Unrecognized Transports	URL 内の、サポートまたは認識されない転送を持つ AIA の数。
Missing from cert	AIA が証明書から失われた回数。
Invalid address	AIA に無効な IP アドレスが含まれていた回数。

たとえば、OCSP の AIA エラーを表示するには、次のコマンドを入力します。

```
host1/Admin# show crypto aia-errors
```

RSA キー ペア情報の表示

キー ペア ファイルのサマリー レポートと詳細レポートを表示するには、EXEC モードで **show crypto key** コマンドを使用します。

このコマンドの構文は次のとおりです。

show crypto key {*filename* | **all**}

次のキーワードと引数があります。

- *filename* : 特定のキー ペア ファイルの名前。最大 40 文字の英数字からなる文字列を引用符で囲まずに入力します。ACE では、指定されたファイルに対するキー ペアの詳細レポートが表示されます。
- **all** : 利用可能なすべてのキー ペア ファイルを一覧表示する、キー ペア サマリー レポートを表示します。

たとえば、キー ペアのサマリー レポートを表示するには、次のように入力します。

```
host1/Admin# show crypto all
```

表 6-10 に、**show crypto key** コマンド出力に含まれるフィールドの説明を示します。

表 6-10　show crypto key コマンドのフィールドの説明

フィールド	説明
Filename	RSA キー ペアを含むキー ペア ファイルの名前。
Bit Size	ファイルのサイズ
Type	RSA などのキー交換アルゴリズムのタイプ。

次に、MYKEYS.PEM キー ペア ファイルに含まれている公開キーと秘密キーの詳細レポートを表示する例を示します。

```
host1/Admin# show crypto key MYKEYS.PEM
1024-bit RSA keypair
```

表 6-11 に、**show crypto key** *filename* コマンド出力に含まれるフィールドの説明を示します。

表 6-11　show crypto key filename コマンドのフィールドの説明

フィールド	説明
Key Size	RSA キー ペアのサイズ（ビット単位）。
Modulus	公開キーの 16 進数値。秘密キーのモジュラスはセキュリティのために表示されません。

証明書チェーン グループ情報の表示

チェーン グループ ファイルのサマリー レポートと詳細レポートを表示するには、EXEC モードで、**show crypto chaingroup** コマンドを使用します。

このコマンドの構文は次のとおりです。

show crypto chaingroup {*filename* | **all**}

次のキーワードと引数があります。

- *filename*：特定のチェーン グループ ファイルの名前。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。ACE では、指定されたファイルに対するチェーン グループの詳細レポートが表示されます。詳細レポートには、チェーン グループに設定されている証明書のリストが含まれます。
- **all**：使用可能な各チェーン グループ ファイルを一覧表示するチェーン グループのサマリー レポートを表示します。サマリー レポートには、各チェーン グループ用に設定された証明書も一覧表示されます。

たとえば、チェーン グループのサマリー レポートを表示するには、次のように入力します。

```
host1/Admin# show crypto chaingroup all
```

次に、MYCERTGROUP チェーン グループのために設定されている証明書の詳細レポートを表示する例を示します。

```
host1/Admin# show crypto chaingroup MYCERTGROUP
```

表 6-12 に、**show crypto chaingroup** コマンド出力に含まれるフィールドの説明を示します。

表 6-12　show crypto chaingroup コマンドのフィールドの説明

フィールド	説明
Certificate	証明書のファイル名。
Subject	証明書を所有し、秘密キーを保持している組織の識別名。
Issuer	証明書を出力した CA の識別名。

クライアント認証グループの情報の表示

各認証グループの証明書のリストまたは、指定したクライアント認証グループの証明書のリストを、各証明書のサブジェクトと発行元情報を含めて表示するには、EXEC モードで、**show crypto authgroup** コマンドを使用します。

このコマンドの構文は次のとおりです。

show crypto authgroup {*group_name* | **all**}

次のキーワードと引数があります。

- *group_name*：特定の認証グループ ファイルの名前。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。
- **all**：各認証グループの証明書のリストを表示します。

たとえば、各認証グループの証明書のリストを表示するには、次のように入力します。

```
host1/Admin# show crypto authgroup all
```

各証明書のサブジェクトと発行元情報を含む AUTH-CERT1 グループの各証明書を表示するには、次のように入力します。

```
host1/Admin# show crypto authgroup AUTH-CERT1
```

表 6-13 に、**show crypto authgroup** *group_name* コマンド出力に含まれるフィールドの説明を示します。

表 6-13　show crypto authgroup group_name コマンドのフィールドの説明

フィールド	説明
Certificate	証明書のファイル名。
Subject	証明書を所有し、秘密キーを保持している組織の識別名。
Issuer	証明書を出力した CA の識別名。

キャッシュされた TLS および SSL セッション エントリの表示

現在のコンテキストに含まれる、キャッシュされた TLS と SSL クライアントおよびサーバ セッション エントリの数を表示するには、EXEC モードで **show crypto session** コマンドを使用します。

このコマンドの構文は次のとおりです。

show crypto session

例を示します。

```
host1/Admin# show crypto session
```

SSL パラメータ マップ設定の表示

SSL パラメータ マップの設定を表示するには、EXEC モードで **show parameter-map** コマンドを使用します。このコマンドの構文は次のとおりです。

show parameter-map *name*

name 引数は、既存の SSL パラメータ マップの名前を指定します。SSL パラメータ名として、最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。

次に例を示します。

```
host1/Admin# show parameter-map SSL_PARAMMAP
```

表 6-14 に、サーバに SSL セッション情報を提供する HTTP ヘッダーに関連する、**show parameter-map** コマンド出力に含まれるフィールドの説明を示します。このコマンドで表示されるその他のフィールドについては、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

表 6-14　show parameter-map のフィールドの説明コマンド

フィールド	説明
Parameter-map	SSL パラメータ マップの名前
Type	SSL
Description	以前に入力されていた SSL パラメータ マップのテキスト説明
version	SSL または TLS のバージョン
close-protocol	**close-protocol** コマンドの状態（なし）
expired-crl	**expired-crl** コマンドの状態（許可または拒否）
cdp-errors	**cdp-errors** コマンドの状態（許可または拒否）
authentication-failure any	**authentication-failure any** コマンドの状態（無視）
session-cache timeout	**session-cache timeout** コマンドの状態（有効または無効）

表 6-14　show parameter-map のフィールドの説明コマンド （続き）

フィールド	説明
queue-delay timeout	**queue-delay timeout** コマンドの状態（有効または無効）
rehandshake	**rehandshake enabled** コマンドの状態（有効または無効）
purpose-check	**purpose-check** コマンドの状態（有効または無効）

フロントエンドおよびバックエンドの SSL 統計情報の表示

現在のコンテキストのフロントエンドおよびバックエンドの SSL 統計情報を表示するには、EXEC モードで **show stats crypto** コマンドを使用します。このコマンドは、アラート、認証、暗号化、ヘッダーの挿入、リダイレクト、および終了の統計情報を表示します。これらの統計情報をクリアするには、「SSL および TLS の統計情報のクリア」を参照してください。

バックエンド SSL 統計情報を表示するには、このコマンドの構文は次のようになります。

show stats crypto client [alert | authentication | cipher | termination]

フロントエンド SSL 統計情報を表示するには、このコマンドの構文は次のようになります。

show stats crypto server [alert | authentication | cipher | insert | redirect | termination]

キーワードは次のとおりです。

- **client**：バックエンド SSL 統計情報を表示します。オプションを指定しない場合、すべての統計情報が表示されます。
- **server**：フロントエンド SSL 統計情報を表示します。オプションを指定しない場合、すべての統計情報が表示されます。
- **alert**：（任意）送受信されたアラート メッセージの統計情報を表示します。

- **authentication**：（任意）認証統計情報を表示します。
- **cipher**：（任意）暗号化統計情報を表示します。
- **insert**：（任意）**server** キーワードを指定すると、このオプションはヘッダー挿入の統計情報を表示します。
- **redirect**：（任意）**server** キーワードを指定すると、このオプションは SSL リダイレクトの統計情報を表示します。
- **termination**：（任意）SSL 終了の統計情報を表示します。

たとえば、バックエンドの統計情報を表示するには、次のように入力します。

```
host1/Admin# show stats crypto client
```

フロントエンド統計情報を表示するには、次のように入力します。

```
host1/Admin# show stats crypto server
```

表 6-15 に、**show stats crypto** コマンド出力に含まれるフィールドの説明を示します。HTTP ヘッダー挿入のカウンタがどのように機能するかの説明については、「SSL HTTP ヘッダー挿入および切り捨てられたカウンタに関する情報」の項を参照してください。

表 6-15　show stats crypto のフィールドの説明コマンド

フィールド	説明
クリプト クライアントまたはサーバの終了の統計情報：	
SSLv3/TLSv1 negotiated protocol	接続をネゴシエートするときにプロトコルが使用される回数。
SSLv3 full handshakes	エラーなく完了した SSLv3 ハンドシェイクの数。
SSLv3 resumed handshakes	セッション ID を使用しているときに再開された SSLv3 ハンドシェイクの数。
SSLv3 handshakes	セッション ID を使用しているときの SSLv3 ハンドシェイクの数。
TLSv1 full handshakes	エラーなく完了した TLSv1 ハンドシェイクの数。
TLSv1 resumed handshakes	セッション ID を使用しているときに再開された TLSv1 ハンドシェイクの数。

表 6-15　show stats crypto のフィールドの説明コマンド （続き）

フィールド	説明
TLSv1 handshakes	セッション ID を使用しているときの TLSv1 ハンドシェイクの数。
SSLv3 handshake failures	セッション ID を使用しているときの SSLv3 ハンドシェイク失敗の数。
SSLv3 failures during data phase	セッション ID を使用しているときの SSLv3 データ交換失敗の数。
TLSv1 handshake failures	セッション ID を使用しているときの TLSv1 ハンドシェイク失敗の数。
TLSv1 failures during data phase	セッション ID を使用しているときの TLSv1 データ交換失敗の数。
Handshake Timeouts	ハンドシェイクがタイム アウトになった回数。
total transactions	すべての SSL トランザクションの総数。
SSLv3 active connections	SSLv3 アクティブ接続の数。
SSLv3 connections in handshake phase	ハンドシェイク フェーズでの SSLv3 接続の数。
SSLv3 conns in renegotiation phase	再ネゴシエーション（再ハンドシェイク）フェーズでの SSLv3 接続の数。
SSLv3 connections in data phase	セッションのデータ交換フェーズでの SSLv3 接続の数。
TLSv1 active connections	TLSv1 アクティブ接続の数。
TLSv1 connections in handshake phase	ハンドシェイク フェーズでの TLSv1 接続の数。
TLSv1 conns in renegotiation phase	再ネゴシエーション（再ハンドシェイク）フェーズでの TLSv1 接続の数。
TLSv1 connections in data phase	セッションのデータ交換フェーズでの TLSv1 接続の数。
クリプト クライアントまたはサーバのアラート統計情報：	
SSL alert... rcvd/sent	通常の SSL アラート メッセージが受信または送信された回数。

表 6-15　show stats crypto のフィールドの説明コマンド （続き）

フィールド	説明
クリプト クライアントまたはサーバの認証統計情報：	
Total SSL client authentications	認証済みクライアント接続の数。このフィールドは、サーバの統計情報を表示する場合にだけ増加します。
Failed SSL client authentications	認証に失敗したクライアント接続の数。このフィールドは、サーバの統計情報を表示する場合にだけ増加します。
SSL authentication cache hits	認証されたクライアントが再接続され、キャッシュ エントリが見つかった回数。このフィールドは、サーバの統計情報を表示する場合にだけ増加します。
SSL static CRL lookups	スタティックに定義された CRL に対する参照の数。
SSL best effort CRL lookups	ベスト エフォートを使用した参照の数。
SSL CRL lookup cache hits	キャッシュの結果が使用された CRL 参照の数。
SSL static OCSP lookups	スタティックに設定された OCSP サーバに対する参照の数。
SSL best effort OCSP lookups	ベストエフォート OCSP サーバを使用している参照の数。
SSL OCSP lookup cache hits	キャッシュの結果が使用された参照の数。
SSL revoked certificates	証明書失効の発生数。
Total SSL server authentications	ACE が実行しようとしたサーバ証明書の認証の数。このフィールドは、クライアントの統計情報を表示する場合にだけ増加します。
Failed SSL server authentications	失敗したサーバ証明書の認証の数。このフィールドは、クライアントの統計情報を表示する場合にだけ増加します。
クリプト クライアントまたはサーバの暗号化統計情報：	
Cipher sslv3/tlsv1...	接続で暗号スイートが使用された回数。

表 6-15　show stats crypto のフィールドの説明
コマンド （続き）

フィールド	説明
クリプト クライアントまたはサーバのリダイレクトの統計情報：	
Redirects due to cert not yet valid	証明書がまだ無効なために行われたリダイレクトの数。
Redirects due to cert expired	証明書が期限切れになったために行われたリダイレクトの数。
Redirects due to unknown issuer cert	ACE が発行元の証明書を取得できないために行われたリダイレクトの数。
Redirects due to cert revoked	証明書が取り消されたために行われたリダイレクトの数。
Redirects due to no client cert	クライアントがクライアント証明書を送信しなかったために行われたリダイレクトの数。
Redirects due to no CRL available	CRL が使用できなかったために行われたリダイレクトの数。
Redirects due to expired CRL	CRL が期限切れになったために行われたリダイレクトの数。
Redirects due to bad cert signature	証明書に不正な署名があるために行われたリダイレクトの数。
Redirects due to other cert error	他のリダイレクト フィールドには適用されない証明書エラーによって行われたリダイレクトの数。
クリプト クライアントまたはサーバのヘッダー挿入統計情報：	
Session headers extracted	ACE が正常に HTTP ヘッダー情報のビルドに追加した SSL ネゴシエート済みのセッション パラメータの情報が含まれる、HTTP ヘッダーの数[1]。
Session headers failed	ACE が HTTP ヘッダー情報のビルドに追加できなかった SSL ネゴシエート済みのセッション パラメータの情報が含まれる、HTTP ヘッダーの数[1]。
Server cert headers extracted	ACE が正常に HTTP ヘッダー情報のビルドに追加した SSL サーバ証明書の情報が含まれる、HTTP ヘッダーの数[1]。
Server cert headers failed	ACE が HTTP ヘッダー情報のビルドに追加できなかった SSL サーバ証明書の情報が含まれる、HTTP ヘッダーの数[1]。

表 6-15　show stats crypto のフィールドの説明コマンド （続き）

フィールド	説明
Client cert headers extracted	ACE が正常に HTTP ヘッダー情報のビルドに追加した SSL クライアント証明書の情報が含まれる、HTTP ヘッダーの数[1]。
Client cert headers failed	ACE が HTTP ヘッダー情報のビルドに追加できなかった SSL クライアント証明書の情報が含まれる、HTTP ヘッダーの数[1]。
Headers truncated	組み合わされたヘッダー情報が 512 バイトを超えたため ACE によって切り詰められた、SSL ネゴシエート済みのセッション パラメータ、サーバ証明書、またはクライアント証明書の情報が含まれる HTTP ヘッダーの数。[1]
Headers insert buffer limit hit	バッファが 512 バイトの制限に達し、ヘッダー挿入を実行するために利用できない回数。このフィールドは、バッファ領域の不足が原因でヘッダーのどの部分も挿入されない場合に増加します。

1. 詳細については、「SSL HTTP ヘッダー挿入および切り捨てられたカウンタに関する情報」の項を参照してください。

SSL HTTP ヘッダー挿入および切り捨てられたカウンタに関する情報

SSL HTTP ヘッダー挿入のために ACE を設定するとき、ACE はクライアントとの SSL ハンドシェイク時に HTTP ヘッダー情報のビルドを作成します。この情報は、アクション リストで指定する SSL ネゴシエート済みのセッション パラメータ、クライアント認証パラメータ、またはサーバ証明書パラメータに基づきます。セッションの最初の HTTP 要求を受信すると、ACE は HTTP ヘッダー挿入処理を実行し、HTTP ヘッダーのビルドを挿入します。

HTTP ヘッダーのビルドを作成している間、ACE は次のカウンタを使用して、挿入される情報の成功率を追跡します。

- 「抽出された（ヘッダー タイプ）ヘッダー」のカウンタ：ACE は、HTTP ヘッダー挿入処理のために構築された情報に正常に追加できるヘッダーの数だけ、対応するヘッダー タイプ カウンタ（セッション、サーバ証明書、またはクライアント証明書）を増加させます。
- 「失敗した（ヘッダー タイプ）ヘッダー」のカウンタ：ACE は、HTTP ヘッダー挿入処理のために構築された情報に正常に追加できないヘッダーの数だけ、対応するヘッダー タイプ カウンタ（セッション、サーバ証明書、またはクライアント証明書）を増加させます。ACE は、内部エラー（メモリを割り当てられない場合など）または証明書フィールドを解析するときのエラー（証明書のデータ フィールドに無効な日付が指定されている場合など）のいずれかが発生したため、ヘッダーを挿入することができません。
- 切り詰められたヘッダー：組み合わされたヘッダー情報が 512 バイトを超えたためヘッダーを切り詰めるたびに、ACE はこのカウンタを増加させます。

ACE では、セッションごとに 1 つのヘッダー情報のビルドのみを作成します。これは、セッション中に ACE が受信するすべての HTTP 要求に情報を挿入するように ACE を設定する場合にも、同じビルドが挿入されることを意味します。すべてのセッション HTTP 要求に同じビルドが使用されるため、カウンタはビルド プロセスの間だけ増加し、ACE が HTTP ヘッダー挿入処理を実行するたびには増加しません。HTTP ヘッダー挿入処理の成功率を追跡するカウンタについては、「HTTP ヘッダー挿入の統計情報の表示」の項を参照してください。

（注）　HTTP 要求に情報を挿入するときでなく、SSL ハンドシェイクの間に ACE がヘッダー情報を取得する場合があります。この状況は、ACE がヘッダー情報を取得した後、最初の GET を受け取る前に SSL ハンドシェイクが失敗した場合に発生することがあります。このような場合、SSL カウンタは増加しますが、HTTP カウンタは増加しません。

HTTP ヘッダー挿入の統計情報の表示

EXEC モードで **show stats http** コマンドを使用すると、SSL セッション情報が含まれる HTTP ヘッダーに関連する情報を含む HTTP 統計情報を表示できます。このコマンドの構文は次のとおりです。

show stats http

表 6-16 に、サーバに SSL セッション情報を提供する HTTP ヘッダーに関連する、**show stats http** コマンド出力に含まれるフィールドの説明を示します。このコマンドで表示されるその他のフィールドについては、『*Server Load-Balancing Guide, Cisco ACE Application Control Engine*』を参照してください。

表 6-16　show stats http コマンドのフィールドの説明

フィールド	説明
SSL headers inserted	対応するアクション リストに定義された SSL セッション、クライアント証明書、およびサーバ証明書の情報を含むすべての HTTP ヘッダーを HTTP 要求に挿入して、ACE が正常に HTTP ヘッダー挿入処理を実行した回数。
SSL header insert errors	対応するアクション リストに定義された SSL セッション情報を含む HTTP ヘッダーを挿入できなかったため、ACE が HTTP ヘッダー挿入処理を完全に失敗した回数。
SSL spoof headers deleted	ACE がクライアント接続を介して受信した HTTP 要求から HTTP ヘッダーを削除した回数。HTTP ヘッダーのスプーフィングを防ぐため、ACE が挿入する必要があるヘッダーのいずれかに一致する SSL セッション情報を含む HTTP ヘッダーを受信した場合はすべて削除されます。

SSL および TLS の統計情報のクリア

EXEC モードで **clear stats crypto** コマンドを使用することで、現在のコンテキストの **show stats crypto** コマンドによって表示される SSL および TLS の統計情報をクリアできます。このコマンドの構文は次のとおりです。

clear stats crypto [**client** | **server** [**alert** | **authentication** | **cipher** | **termination**]]

オプションは次のとおりです。

- **client**：（任意）現在のコンテキストの TLS と SSL のクライアント統計情報をすべてクリアします。

- **server**：（任意）現在のコンテキストの TLS と SSL のサーバ統計情報をすべてクリアします。
- **alert**：（任意）バックエンド SSL アラートの統計情報をクリアします。
- **authentication**：（任意）バックエンド SSL 認証の統計情報をクリアします。
- **cipher**：（任意）バックエンド SSL 暗号化統計情報をクリアします。
- **termination**：（任意）バックエンド SSL 終了の統計情報をクリアします。

client または **server** のオプションを入力しない場合、ACE はクライアントとサーバの両方の統計情報をクリアします。

たとえば、すべての TLS および SSL の統計情報をクリアするには、次のように入力します。

```
host1/Admin# show stats crypto
```