CHAPTER 6

SSL 証明書および鍵ペア情報の表示

この章では、**show** コマンドを使用して、ACE にロードされた証明書と鍵ペア ファイルなど、SSL 関連情報を表示する方法について説明します。**show** コマンドで表示されるのは、このコマンドの実行時のコンテキストに関連した情報です。この章では、各コマンドだけでなく、その出力についても説明します。

show コマンドは EXEC モードのコマンドですが、**do** コマンドを使用することにより、あらゆる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。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場合は、次の例のように入力します。

EXEC モードから：

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

コンフィギュレーション モードから：

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

この章の主な内容は、次のとおりです。

- RSA 鍵ペア情報
- 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情報の表示
- キャッシュした TLS および SSL セッション エントリの表示
- TLS および SSL 統計情報の表示

CSR パラメータ セットの設定の表示

EXEC モードで **show crypto csr-params** コマンドを使用すると、CSR パラメータ セットの要約レポートおよび詳細レポートを表示できます。

このコマンドの構文は次のとおりです。

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

引数と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。64 文字以内で、引用符のない英数字を入力します。このオプションを指定すると、ACE は、特定の CSR パラメータ セットの詳細レポートを表示します。詳細レポートには、その CSR パラメータ セットの認定者名アトリビュートが含まれます。
- 要約レポート（現在のコンテキストのすべての CSR パラメータ セットのリスト）を表示する場合は、CSR パラメータ セットを指定せずにこのコマンドを入力します。

CSR パラメータ セットの要約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
```

MYCSRCONFIG CSR パラメータ セットの詳細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 MTCSRCONFIG
```

表 6-1 に **show crypto csr-params** コマンドの出力フィールドを示します。

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	証明書オーナーの所在国
State	証明書オーナーの所在州
Locality	証明書オーナーの所在市町村
Org-name	組織名（証明書のオーナーまたはサブジェクト）
Org-unit	組織内の部署名
Common-name	通常名（SSL サイトのドメイン名または個々のホスト名）
Serial number	シリアル番号
Email	E メール アドレス

証明書および鍵ペア ファイルのリストの表示

EXEC モードで **show crypto files** コマンドを使用すると、使用可能なすべての証明書および鍵ペア ファイルのリストを表示できます。

証明書と鍵ペア 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** コマンドの出力フィールドを示します。

表 6-2　show crypto files コマンドのフィールドの説明

フィールド	説明
Filename	証明書または鍵ペアが入っているファイルの名前
Size	ファイルのサイズ
Type	ファイルのフォーマット：PEM、DER、または PKCS12
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 —** ファイルを FTP、SFTP、または TFP サーバにエクスポートできます（第 2 章「証明書および鍵の管理」の「証明書と鍵ペア ファイルのエクスポート」を参照）。 • **No —** プロテクトされているファイルはエクスポートできません。
Key/Cert	ファイルに、証明書（CERT）、鍵ペア（KEY）、両方（BOTH）のどれが含まれているかを示します。

証明書情報の表示

EXEC モードで **show crypto certificate** コマンドを使用すると、証明書の要約レポートおよび詳細レポートを表示できます。

このコマンドの構文は次のとおりです。

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

キーワードと引数は次のとおりです。

- *filename* — 特定の証明書ファイルの名前。40 文字以内で、引用符のない英数字を入力します。このオプションを指定すると、ACE は、指定されたファイルの証明書の詳細レポートを表示します。証明書ファイルにチェーンが含まれている場合、ACE は最下位の証明書だけを表示します（署名者は表示されません）。
- **all** — 証明書の要約レポートが表示されます。このレポートには現在のコンテキストのすべての証明書ファイルのリストが表示されます。

証明書の要約レポートを表示する場合は、次のように入力します。

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

表 6-3 に **show crypto certificate all** コマンドの出力フィールドを示します。

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	証明書のオーナーで、秘密鍵を所持している組織の認定者名
Issuer	証明書を発行した認証局（CA）の認定者名
Not Before	開始日時（この日時になるまで証明書は無効）
Not After	終了日時（この日時を過ぎると、証明書は無効）
CA Cert	証明書に署名した CA の証明書

MYCCERT.PEM 証明書ファイルの詳細レポートを表示する場合は、次のように入力します。

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

表 6-4 に **show crypto certificate** *filename* コマンドの出力フィールドを示します。

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（データ部）	
Version	X.509 標準のバージョン。証明書はこのバージョンの標準に準拠しています。
Serial Number	証明書のシリアル番号
Signature Algorithm	公開鍵 / 秘密鍵の鍵ペアで情報暗号化に使用されるデジタル署名アルゴリズム
Issuer	証明書を発行した CA の認定者名
Validity（有効期間）	
Not Before	開始日時（この日時になるまで証明書は無効）
Not After	終了日時（この日時を過ぎると、証明書は無効）
Subject	証明書のオーナーで、秘密鍵を所持している組織の認定者名
Subject Public Key Info（サブジェクトの公開鍵情報）	
Public Key Algorithm	公開鍵の生成に使用された鍵交換アルゴリズムの名前（RSA など）
RSA Public Key	鍵のビット数（セキュアな Web トランザクションに使用される RSA 鍵ペアのサイズ）
Modulus	その証明書の確立に使用された実際の公開鍵
Exponent	鍵の生成に使用された基本数の 1 つ
X509v3 Extensions（X509v3 拡張）	証明書に追加された一連の X509v3 拡張情報
X509v3 Basic Constraints	サブジェクトが、証明書の署名の検証に使用される証明済み公開鍵で、CA として機能するかどうかを示します。その場合、証明パスの長さも制限できます。
Netscape Comment	証明書閲覧時に表示されるコメント

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
X509v3 Subject Key Identifier	証明される公開鍵。同じサブジェクトが使用する複数の鍵を区別できるようにします（たとえば、鍵のアップデートが発生した場合など）。
X509v3 Authority Key Identifier	この証明書または CRL の署名を検証するために使用される公開鍵。同じ CA が使用する複数の鍵を区別できるようにします（たとえば、鍵のアップデートが発生した場合など）。
Signature Algorithm	鍵交換ではなく、デジタル署名に使用されたアルゴリズムの名前
Hex Numbers	証明書の実際の署名。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し、証明書データが変更されていないことを確認できます。

CRL 情報の表示

ACE に対する証明書失効リスト（CRL）またはコンテキスト内の特定の CRL の定義を表示するには、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* | **all**}

キーワードと引数は次のとおりです。

- *crl_name* — コンテキストで設定された特定の CRL 名。引用符のない英数字を入力します。ACE は、指定された CRL の定義を表示します。
- **all** — コンテキストで設定されたすべての CRL のリストを表示します。

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
```

CRL1 など、特定の CRL 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* コマンドの出力フィールドを示します。

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 は、この URL から CRL をダウンロードします。
Last Downloaded	最後に ACE が CRL をダウンロードした日時を表します。アクティブではないポリシー マップまたはサービスが関連付けられていないポリシー マップの SSL プロキシ サービスに CRL が設定されている場合、フィールドに「not downloaded yet」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 (for This Name of CRL)	名前付き URL について、成功したダウンロード試行の総数です。 **（注）** 複数の論理設定 CRL 名が同じ CRL データを指す場合があります。
Failed Download Attempts (for This Name of CRL)	名前付き URL について、失敗したダウンロード試行の数です。 **（注）** 複数の論理設定 CRL 名が同じ CRL データを指す場合があります。
Total Number of Download Attempts for Real CRL Data	SSL プロキシ サービスでのクライアント認証に対して ACE にダウンロードされた実 CRL について、成功したダウンロード試行の総数です。
Failed Download Attempts for Real CRL Data	SSL プロキシ サービスでのクライアント認証に対して ACE にダウンロードされた実 CRL について、失敗したダウンロード試行の数です。

（注） 使用中の CRL が失効している場合に ACE がクライアント証明書を拒否するかを確認するには、**show parameter-map** コマンドを使用します。

RSA 鍵ペア情報

EXEC モードで **show crypto key** コマンドを使用すると、鍵ペア ファイルの要約レポートおよび詳細レポートを表示できます。

このコマンドの構文は次のとおりです。

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

キーワードと引数は次のとおりです。

- *filename* — 特定の鍵ペア ファイルの名前。40 文字以内で、引用符のない英数字を入力します。ACE は、指定されたファイルの鍵ペアの詳細レポートを表示します。
- **all** — 使用可能なすべての鍵ペア ファイルのリストが含まれた鍵ペアの要約レポートを表示します。

鍵ペアの要約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 6-6 に **show crypto key** コマンドの出力フィールドを示します。

表 6-6　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 鍵ペアが含まれた鍵ペア ファイルの名前
Bit Size	ファイルのサイズ
Type	鍵交換アルゴリズムのタイプ（RSA など）

MYKEYS.PEM 鍵ペア ファイルに含まれている公開鍵と秘密鍵の詳細レポートを表示する場合は、次のように入力します。

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

表 6-7 に **show crypto key** *filename* コマンドの出力フィールドを示します。

表 6-7　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 鍵ペアのサイズ（ビット）
Modulus	公開鍵の 16 進値。このフィールドの値は、セキュリティ上、表示されません。

証明書チェーン グループ情報の表示

EXEC モードで **show crypto chaingroup** コマンドを使用すると、チェーン グループ ファイルの要約レポートおよび詳細レポートを表示できます。

このコマンドの構文は次のとおりです。

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

キーワードと引数は次のとおりです。

- *filename* — 特定のチェーン グループ ファイルの名前。64 文字以内で、引用符のない英数字を入力します。ACE は、指定されたファイルのチェーン グループの詳細レポートを表示します。詳細レポートには、そのチェーン グループに設定されている証明書のリストが含まれています。
- **all** — 使用可能な各チェーン グループ ファイルのリストが含まれたチェーン グループの要約レポートを表示します。要約レポートにも、各チェーン グループに設定されている証明書のリストが含まれています。

チェーン グループの要約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
```

MYCERTGROUP チェーン グループに設定されている証明書の詳細レポートを表示する場合は、次の例のように入力します。

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

表 6-8 に **show crypto chaingroup** コマンドの出力フィールドを示します。

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

フィールド	説明
Certificate	証明書ファイルの名前
Subject	証明書のオーナーで、秘密鍵を所持している組織の認定者名
Issuer	証明書を発行した CA の認定者名

クライアント認証グループ情報の表示

各認証グループの証明書のリスト、または特定のクライアント認証グループの証明書（証明書ごとに Subject および Issuer 情報を含む）を表示するには、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**}

キーワードと引数は次のとおりです。

- *group_name* — 特定の認証グループ ファイル名。64 文字以内で、引用符のない英数字を入力します。
- **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
```

証明書ごとに Subject および Issuer 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 6-9 に **show crypto authgroup** *group_name* コマンドの出力フィールドを示します。

表 6-9　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	証明書ファイルの名前
Subject	証明書のオーナーで、秘密鍵を所持している組織の認定者名
Issuer	証明書を発行した CA の認定者名

キャッシュした 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でキャッシュした TLS/SSL クライアント およびサーバ セッション エントリを表示するには、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

たとえば、次のように入力します。

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

TLS および SSL 統計情報の表示

現在のコンテキストの TLS/SSL クライアントまたはサーバ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。

このコマンドの構文は次のとおりです。

show stats crypto {**client** | **server**}

キーワードは次のとおりです。

- **client —** TLS および SSL クライアントの統計情報を表示します。
- **server —** TLS および SSL サーバの統計情報を表示します。

たとえば、クライアント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
```

サーバ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 server
```

表 6-10 に **show stats crypto** コマンドの出力フィールドを示します。

表 6-10　show stats crypto コマンドのフィールドの説明

フィールド	説明
SSL alert... rcvd/sent	標準的な SSL アラート メッセージの送受信回数
SSLv2/v3 client hello received	受信した ClientHello メッセージの数
SSLv3/TLSv1 negotiated protocol	バージョンが接続で使用された回数
SSLv3 full handshakes	エラーなしで終了したハンドシェイクの数
SSLv3 resumed handshakes	セッション ID を使用して再開されたハンドシェイクの数
Cipher sslv3...	接続で暗号スイートが使用された回数
TLSv1 full handshakes	エラーなしで終了したハンドシェイクの数
TLSv1 resumed handshakes	セッション ID を使用して再開されたハンドシェイクの数
Cipher tlsv1...	接続で暗号スイートが使用された回数
Total SSL client authentications	認証されたクライアント接続の数。サーバの統計情報を表示している場合にのみ、フィールドは増分します。
Failed SSL client authentications	認証の失敗したクライアント接続の数。サーバの統計情報を表示している場合にのみ、フィールドは増分します。
SSL client authentication cache hits	認証されたクライアントが再接続して、キャッシュ エントリが検出された回数。サーバ統計情報を表示している場合にのみ、フィールドは増分します。
SSL static CRL lookups	静的に定義された CRL に対して実行されたルックアップの数
SSL best effort CRL lookups	ベストエフォートを使用して実行されたルックアップの数
SSL CRL lookup cache hits	キャッシュ結果が使用された CRL ルックアップの数

表 6-10　show stats crypto コマンドのフィールドの説明（続き）

フィールド	説明
SSL revoked certificates	失効した証明書にあたった回数
SSL CRL download failed	失敗した CRL ダウンロードの数
Total SSL server authentications	ACE が実行しようとしたサーバ証明書認証の数。クライアントの統計情報を表示している場合にのみ、フィールドは増分します。
Failed SSL server authentications	失敗したサーバ証明書認証の数。クライアントの統計情報を表示している場合にのみ、フィールドは増分します。
Handshake FlushRX/TX operations	SSL ハンドシェイクが終了した回数
Xscale messages rcvd/sent for ME	SSL ハンドシェイク中に SSL プロセッサ間でやり取りされたメッセージの数
Xscale rcvd abort msg before hdshk	SSL ハンドシェイクが打ち切られた回数
Finish msg split across ssl recs	クライアントによって SSL Finished メッセージが複数の SSL レコードに分割された回数