



## INDEX

### C

#### CDP

クライアント証明書のエラー [3-20](#)

#### Certificate Authority

認証局 [1-4](#)

close-protocol 動作、定義 [3-21, 4-17](#)

#### CRL 分散ポイント (CDP)

エラー統計情報の表示 [6-10](#)

#### CSR パラメータ セット

概要 [2-8](#)

国 [2-10](#)

作成 [2-9](#)

州または地域 [2-11](#)

詳細レポートとサマリー レポート [6-2](#)

シリアル番号 [2-11](#)

組織名 [2-12](#)

組織ユニット [2-13](#)

地域 [2-12](#)

通常名 [2-10](#)

電子メール アドレス [2-13](#)

### H

#### HTTP ヘッダー挿入

SSL クライアント証明書 [3-63](#)

SSL サーバ証明書 [3-58](#)

SSL セッション [3-52](#)

設定例 [3-70](#)

#### HTTP ヘッダーの挿入

SSL クライアント証明書 [3-63](#)

SSL サーバ証明書 [3-58](#)

SSL セッション [3-52](#)

設定例 [3-70](#)

### O

#### OCSP

サーバ、SSL プロキシ サービスへの適用 [3-42](#)

サーバ、設定 [3-41](#)

失効チェックのプライオリティ [3-43](#)

注意事項および制約事項 [3-40](#)

ナンス [3-42](#)

Online Certificate Status Protocol。「OCSP」を参照

---

**P**PKI [1-2](#)

---

**R**

RSA キー ペア

概要 [1-3](#)生成 [2-7](#)説明 [2-3](#)

---

**S**

SSL

ACE 機能の概要 [1-10](#)PKI の概要 [1-2](#)RSA キー ペア [1-3](#)URL 書き換え、設定 [3-48, 3-49](#)

エンドツーエンド

概要 [5-2](#)エンドツーエンドの設定例 [5-6](#)

開始

概要 [4-2](#)設定 [4-5](#)開始の設定例 [4-38](#)概要 [1-1](#)キーと証明書の生成 [2-6](#)機能 [1-7](#)基本的な ACE の設定 [1-10](#)グローバル サイト証明書、準備 [2-15](#)公開キー インフラストラクチャ  
(PKI) [1-2](#)サンプル キーと証明書の使用 [2-6](#)

終了

概要 [1-11, 3-2](#)設定 [3-5](#)終了の設定例 [3-78](#)証明書 [1-3, 2-16](#)

証明書署名要求

グローバル サイト [2-15](#)生成 [2-14](#)設定の前提条件 [1-12](#)

設定フロー図

SSL 開始 [4-4](#)SSL 終了 [3-4](#)エンドツーエンド SSL [5-4](#)統計情報のクリア [6-27](#)統計情報の表示 [6-20](#)

パラメータ マップ

SSL/TLS バージョンの定義 [3-23](#)暗号スイートの追加 [3-11](#)期限切れまたは無効なクライアント証  
明書の無視またはリダイレク  
ト [3-15](#)期限切れまたは無効なサーバ証明書の  
無視 [4-15](#)作成 [3-8](#)ハンドシェイク [1-5](#)

プロキシ サービス

SSL パラメータ マップの関連付け **3-28**

プロキシ サービス (クライアント)

SSL 開始の作成 **4-21**

SSL パラメータ マップの関連付け **4-22**

サーバ認証の有効化 **4-23**

プロキシ サービス (サーバ)

SSL 終了の作成 **3-27**

キー ペアの指定 **3-29**

クライアント認証の有効化 **3-31**

証明書チェーン グループの指定 **3-30**

証明書の指定 **3-30**

SSL および TLS 統計情報 **6-27**

SSL 開始のプロキシ サービス (クライアント) **4-21**

SSL 終了のプロキシ サービス (サーバ) **3-27**

SSL 証明書のアップグレード **2-22**

SSL パラメータ マップ

再ハンドシェイク パラメータの定義 **3-22, 4-18**

## T

TLS

統計情報のクリア **6-27**

統計情報の表示 **6-20**

## U

URL

書き換え、設定 **3-48, 3-49**

## あ

アクション リスト

ポリシー マップとの関連付け **3-69**

暗号スイート

サポート **3-14**

指定 **3-12, 4-12**

## え

エンドツーエンド SSL **5-2**

## き

キー (SSL)

インポートまたはエクスポート **2-16**

概要 **1-2**

キー交換 **1-3**

冗長構成での同期 **2-3**

キー ペア、指定 **3-29**

キー ペア ファイル

サマリー レポートと詳細レポートの表示 **6-15**

証明書ファイルとキー ペア ファイルの表示 **6-3**

機密性 [1-3](#)

キュー遅延時間、設定 [3-24](#)

再ハンドシェイク [4-18](#)

サンプル キー [3-29](#)

## く

クイック スタート

SSL 開始 [4-6](#)

SSL 終了 [3-6](#)

エンドツーエンド SSL [5-5](#)

クライアント証明書

CDP エラー [3-20](#)

認証失敗 [3-14](#)

有効化 [3-31](#)

クライアント証明書の CDP エラーの無視 [3-20](#)

クライアント認証

CRL の使用 [3-33](#)

クラス マップ

SSL 開始用のレイヤ 3 およびレイヤ 4 [4-33](#)

SSL 開始用のレイヤ 7 [4-29](#)

SSL 終了用のレイヤ 3 およびレイヤ 4 [3-73](#)

説明、入力 [3-11, 4-12](#)

クリア [6-27](#)

セッション キャッシュ情報 [3-25](#)

## し

識別名

概要 [2-8](#)

設定 [2-9](#)

終了通知メッセージ、送信 [3-21, 4-17](#)

冗長性

証明書とキーの同期 [2-3](#)

証明書

目的確認の無効化 [3-22, 4-18](#)

証明書 (SSL)

アップグレード [2-22](#)

インポートまたはエクスポート [2-16](#)

概要 [1-2](#)

期限切れまたは無効なクライアント証明書の無視またはリダイレクト [3-15](#)

期限切れまたは無効なサーバ証明書の無視 [4-15](#)

グローバル サイト証明書 [2-15](#)

グローバル サイトの準備 [2-15](#)

公開キーの検証 [2-23](#)

サブジェクト [1-4, 2-2](#)

冗長構成での同期 [2-3](#)

証明書署名要求、生成 [2-14](#)

チェーン [1-4, 2-25](#)

認証グループの作成 [2-27](#)

発行元 [1-4, 2-2](#)

## さ

サーバ認証、認証グループの使用 [4-23](#)

ルート権限 [1-4](#)

証明書失効リスト (CRL)

拒否 [3-25, 4-21](#)

クライアント認証での使用 [3-33](#)

サーバ認証での使用 [4-24](#)

失効チェックのプライオリティ [3-43](#)

署名の検証 [3-38](#)

ダウンロード [3-35, 4-27](#)

リストの表示 [6-7](#)

証明書、指定 [3-30](#)

証明書チェーン グループ

作成 [2-25](#)

サマリー レポートと詳細レポートの表示 [6-16](#)

証明書の目的確認、確認の無効化 [3-22, 4-18](#)

証明書ファイル

サマリー レポートと詳細レポートの表示 [6-4](#)

証明書ファイルとキー ペア ファイルの表示 [6-3](#)

---

## せ

セッション ID 再利用キャッシュ タイムアウト、設定 [3-25, 4-20](#)

設定例

SSL エンドツーエンド [5-6](#)

SSL 開始 [4-38](#)

SSL 終了 [3-78](#)

---

## ち

チェーン グループ [2-25](#)

---

## と

統計情報

SSL および TLS のクリア [6-27](#)

SSL および TLS の表示 [6-20](#)

ドメイン

参照、有効化 [3-45](#)

名前、デフォルトの設定 [3-46](#)

名前の検索リスト、設定 [3-46](#)

ネーム サーバ、設定 [3-47](#)

ドメイン ネーム システム (DNS) クライアント、設定 [3-44](#)

---

## な

ナンス [3-42](#)

---

## に

認証 [1-3](#)

クライアント認証の失敗 [3-14](#)

グループ、証明書の設定 [2-27](#)

---

## は

バージョン、SSL または TLS の定義 [3-23](#),  
[4-19](#)

---

## ほ

### ポリシー マップ

#### レイヤ 3 およびレイヤ 4

SSL プロキシ サービスの関連付  
け [3-76](#)

クラス マップの関連付け [3-75](#), [4-35](#)

作成 [3-74](#), [4-34](#)

すべての VLAN にグローバルに適  
用 [3-76](#), [4-37](#)

特定の VLAN への適用 [3-77](#), [4-37](#)

レイヤ 7 ポリシー マップの関連付  
け [4-36](#)

#### レイヤ 7

SLB ポリシー アクションの指  
定 [4-32](#)

クラス マップの関連付け [4-31](#)

作成 [4-30](#)

---

## め

メッセージ整合性 [1-5](#)

メッセージ認証コード (MAC) [1-2](#), [1-5](#)