はじめに

このマニュアルでは、Cisco 4700 シリーズ Application Control Engine（ACE）Appliance 上で Secure Sockets Layer（SSL）機能を設定する手順について説明します。具体的には、証明書と鍵、SSL 終了、SSL 開始、およびエンドツーエンド SSL を設定する方法について説明します。

ACE は、次のインターフェイスで設定できます。

- CLI（コマンドライン インターフェイス）：ACE の設定、管理、および監視のコマンドを入力するラインベースのユーザ インターフェイス
- Device Manager の GUI（グラフィカル ユーザ インターフェイス）：ACE の設定、管理、および監視を実行する Web ブラウザベースの GUI

ここで説明する内容は、次のとおりです。

対象読者

このマニュアルは、ACE の設定を担当する、研修を受けた認定サービス技術者を対象としています。

- システム管理者
- システム オペレータ

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	説明
第 1 章「概要」	SSL 暗号法および ACE の SSL 機能の概要について説明します。
第 2 章「証明書および鍵の管理」	証明書 / 鍵ペア ファイルのインポートおよびエクスポート方法を含む、ACE での SSL 証明書 / 鍵ペア ファイルの管理方法について説明します。
第 3 章「SSL 終了の設定」	ACE を SSL プロキシ サーバとして設定し、ACE とクライアントの間で SSL 終了を実行する方法について説明します。
第 4 章「SSL 開始の設定」	ACE を SSL プロキシ クライアントとして設定し、ACE と Web サーバの間で SSL 開始を実行する方法について説明します。
第 5 章「エンドツーエンド SSL の設定」	ACE を SSL プロキシ クライアントおよび SSL プロキシ サーバとして設定して SSL 終了と SSL 開始の両方を実行し、クライアントと Web サーバ間のエンドツーエンド SSL 接続を提供する方法について説明します。
第 6 章「SSL 証明書および鍵ペア情報の表示」	ACE のSSL 設定に関連するデータと統計情報を表示する方法について説明します。

関連資料

ACE には、このマニュアルに加え、次のマニュアルが付属しています。

マニュアル タイトル	説明
『*Release Note for the Cisco 4700 Series Application Control Engine Appliance*』	ACE の動作に関する考慮事項、警告、および CLI コマンドについて説明しています。
『*Cisco Application Control Engine Appliance Hardware Installation Guide*』	ACE アプライアンスの設置情報が記載されています。
『*Regulatory Compliance and Safety Information for the Cisco Application Control Engine Appliance*』	ACE アプライアンスの適合認定および安全に関する情報が記載されています。
『*Cisco 4700 Series Application Control Engine Appliance Quick Start Guide*』	ACE アプライアンスの Device Manager および CLI を使用して、初期設定および VIP ロードバランシング設定を実行する手順が説明されています。
『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』	ACE で次の管理タスクを実行する方法について説明しています。 • ACE の設定 • リモート アクセスの確立 • ソフトウェア ライセンスの管理 • クラス マップとポリシー マップの設定 • ACE ソフトウェアの管理 • SNMP の設定 • 冗長性の設定 • XML インターフェイスの設定 • ACE ソフトウェアのアップグレード

マニュアル タイトル	説明
『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』	単一のコンテキストまたは複数のコンテキストで ACE を稼働する方法について説明しています。
『*Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*』	ACE で次のルーティングおよびブリッジングのタスクを実行する方法について説明しています。 • イーサネット ポートの設定 • VLAN インターフェイスの設定 • ルーティングの設定 • ブリッジングの設定 • Dynamic Host Configuration Protocol（DHCP）の設定
『*Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*』	ACE で、次のサーバ ロード バランシング機能を設定する方法について説明しています。 • 実サーバおよびサーバ ファーム • サーバ　ファーム内の実サーバ間でトラフィックをロード バランシングするためのクラス マップとポリシー マップ • サーバ ヘルス モニタリング（プローブ） • スティッキ性 • ファイアウォール負荷分散 • TCL スクリプト
『*Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*』	ACE のアプリケーション アクセラレーションおよび最適化の機能を設定する方法について説明しています。このマニュアルには、それらの機能の概要と説明も記載されています。

マニュアル タイトル	説明
『*Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*』	次の ACE セキュリティ機能の設定方法について説明しています。 • セキュリティ Access Control List（ACL; アクセス コントロール リスト） • TACACS+（Terminal Access Controller Access Control System Plus）、Remote Authentication Dial-In User Service（RADIUS）、または Lightweight Directory Access Protocol（LDAP）サーバを使用したユーザ認証とアカウンティング • アプリケーション プロトコルと HTTP ディープ パケット インスペクション • TCP/IP 正規化および終了パラメータ • Network Address Translation（NAT; ネットワーク アドレス変換）
『*Cisco 4700 Series Application Control Engine Appliance System Message Guide*』	ACE でシステム メッセージのロギングを設定する方法について説明しています。また、ACE によって生成されるシステム ログ（syslog）メッセージの一覧とそれぞれの説明も記載されています。
『*Cisco 4700 Series Application Control Engine Appliance Command Reference*』	すべての CLI コマンドをモード別にアルファベット順で一覧し、それぞれについて、構文、オプション、および関連コマンドを含めた説明が記載されています。
『*Cisco 4700 Series Application Control Engine Appliance Device Manager GUI Configuration Guide*』	ACE 上のフラッシュ メモリに常駐し、ブラウザベースのインターフェイスでアプライアンスを設定および管理できる Device Manager GUI の使用方法が説明されています。
『*Cisco CSS-to-ACE Conversion Tool User Guide*』	CSS と ACE 間の変換ツールを使用して、Cisco Content Services Switches（CSS）の実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを ACE に移行する方法について説明しています。

記号と表記法

このマニュアルでは、次の表記法を使用しています。

表記	説明
太字	コマンド、コマンド オプション、およびキーワードは**太字**で示しています。本文中のコマンドも太字で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。また、新しい用語の初出箇所、書籍のタイトル、強調するテキストもイタリック体で示しています。
{ }	必須の引数とキーワードを囲みます。
[ ]	省略可能な引数とキーワードを囲みます。
{ x | y | z }	必ずどれか 1 つを選択しなければならないキーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の **`screen`** フォント	コマンドラインでユーザが入力しなければならない情報は、**太字**の **`screen`** フォントで示しています。
*イタリック体*の *`screen`* フォント	ユーザが値を指定する引数は、*イタリック体*の *`screen`* フォントで示しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、かぎカッコ（<>）で囲んで示しています。

（注）は、次のように表しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意は、次のように表しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

構文の形式および ACE CLI のナビゲート方法の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Command Reference*』を参照してください。

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

http://www.cisco.com/en/US/support/index.html

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
  - Product Alert の受信登録
  - Field Notice の受信登録
  - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（http://www.cisco.com/techsupport）の、利用頻度の高いドキュメントを日本語で提供しています。

Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

Service Request ツールの使用

Service Request ツールには、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

日本語版の Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/jp/go/tac/sr/

シスコの世界各国の連絡先一覧は、次の URL で参照できます。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

その他の情報の入手方法

シスコの製品、サービス、テクノロジー、ネットワーキング ソリューションに関する情報について、さまざまな資料をオンラインで入手できます。

- シスコの E メール ニュースレターなどの配信申し込みについては、Cisco Subscription Center にアクセスしてください。

  http://www.cisco.com/offer/subscribe

- 日本語の月刊 Email ニュースレター「Cisco Customer Bridge」については、下記にアクセスください。

  http://www.cisco.com/web/JP/news/cisco_news_letter/ccb/

- シスコ製品に関する変更やアップデートの情報を受信するには、Product Alert Tool にアクセスし、プロファイルを作成して情報の配信を希望する製品を選択してください。Product Alert Tool には、次の URL からアクセスできます。

  http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

- 『*Cisco Product Quick Reference Guide*』はリファレンス ツールで、パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。『*Cisco Product Quick Reference Guide*』を発注するには、次の URL にアクセスしてください。

http://www.cisco.com/go/guide

- ネットワークの運用面の信頼性を向上させることのできる最新の専門的サービス、高度なサービス、リモート サービスに関する情報については、Cisco Services Web サイトを参照してください。Cisco Services Web サイトには、次の URL からアクセスできます。

  http://www.cisco.com/go/services

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、ロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/

- DVD に収録されたシスコの技術マニュアル（Cisco Product Documentation DVD）は、Product Documentation Store で発注できます。Product Documentation Store には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/docstore

- 日本語マニュアルの DVD は、マニュアルセンターから発注できます。マニュアルセンターには下記よりアクセスください。

  http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/manual_center/index.shtml

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を発行しています。Cisco Press には、次の URL からアクセスできます。

  http://www.ciscopress.com

- 日本語のシスコプレスの情報は以下にアクセスください。

  http://www.seshop.com/se/ciscopress/default.asp

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスできます。

  http://www.cisco.com/ipj

- 『*What's New in Cisco Product Documentation*』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを見つけることができます。

  http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

- シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

  http://www.cisco.com/public/countries_languages.shtml

オープン ソース ライセンスに関する通知

次に、このソフトウェア ライセンスに関連する通知を示します。

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.See below for the actual license texts.Actually both licenses are BSD–style Open Source licenses.In case of any license issues related to OpenSSL please contact openssl–core@openssl.org.

OpenSSL License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.(http://www.openssl.org/)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission.For written permission, please contact openssl–core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

© 1995–1998 Eric Young (eay@cryptsoft.com).All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non–commercial use as long as the following conditions are adhered to.The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code.The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography–related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:"This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].