# GLOSSARY

## A

**ACL** Access Control List（アクセス コントロール リスト）。権限を区別するために使用されるコンピュータ セキュリティのメカニズム。ACL は、ユーザまたはクライアントが、サーバ、ファイル システム、アプリケーションなどの特定のオブジェクトに対して持つ権限およびアクセス権を識別します。

**AES** Advanced Encryption Standard（高度暗号化規格）。SNMP 通信で使用可能な暗号化アルゴリズムの 1 つ。

**ARP** Address Resolution Protocol（アドレス解決プロトコル）。IP アドレスを MAC アドレスにマッピングする際に使用されるインターネット プロトコル。RFC 826 で定義されています。

## B

**BVI** Bridge-Group Virtual Interface（ブリッジ グループ仮想インターフェイス）。Integrated Routing and Bridging（IRB）が設定されている場合に、ブリッジ グループに関連付けられた論理レイヤ 3 専用インターフェイス。

## C

**CCM** Cisco CallManager Cisco AVVID（Architecture for Voice, Video, and Integrated Data）の一部である Cisco IP テレフォニー ソリューションのソフトウェアベースのコール処理コンポーネントを提供するシスコ製品。CallManager は、SIP、Integrated Services Digital Network（ISDN）、Media Gateway Control Protocol（MGCP）などの他の共通のプロトコルを介して開始されたコール イベントのシグナリング プロキシとして動作します。

**Cisco.com** Cisco Connection Online Web サイトに取って代わるサイト。このサイトを使用して、カスタマー サービスおよびサポートにアクセスできます。

**CSR** Certificate Signing Request（証明書署名要求）。SSL で使用するデジタル アイデンティティ証明書を要求するために、VeriSign や Thawte などの認証局に送信されるメッセージ。要求には、場所やシリアル番号などの SSL サイトを識別する情報と、選択した公開キーが含まれます。また、要求には、認証局が必要とするアイデンティティの追加の証明情報が含まれることがあります。

## D

**DES** Data Encryption Standard（データ暗号規格）。SNMP 通信で使用可能な暗号化アルゴリズムの 1 つ。

**DFP** Dynamic Feedback Protocol。負荷分散されたサーバ（ローカルとリモートの両方）が、ステータスおよびサービス提供能力の変化を動的に報告できるプロトコル。

## F

**File Transfer Protocol** — FTP *を参照してください。*

**FTP** — File Transfer Protocol（ファイル転送プロトコル）。ネットワーク ノード間でファイルを転送するために使用され、TCP/IP プロトコル スタックの一部であるアプリケーション プロトコル。FTP は、RFC 959 で定義されています。

## H

**HSRP** — Hot Standby Router Protocol（ホットスタンバイ ルータ プロトコル）。IP ネットワークにネットワーク冗長性を提供するネットワーキング プロトコル。ユーザ トラフィックが、ネットワーク エッジ デバイスまたはアクセス回線の最初のホップ障害から即時に透過的に回復するように保証します。

## I

**ICMP** — Internet Control Message Protocol（インターネット制御メッセージ プロトコル）。エラーを報告し、IP パケット処理に関連するその他の情報を提供するネットワーク層のインターネット プロトコル。RFC 792 に規定されています。

**Internet Control Message Protocol** — ICMP *を参照してください。*

## M

**MD5** — Message Digest 5（メッセージ ダイジェスト 5）またはメッセージ ダイジェスト アルゴリズム。SNMP 通信で使用可能な暗号化アルゴリズムの 1 つ。

**MIB** — Management Information Base（管理情報ベース）。SNMP や CMIP などのネットワーク管理プロトコルにより使用および管理されるネットワーク管理情報のデータベース。MIB オブジェクトの値は、SNMP コマンドまたは CMIP コマンドを使用して変更および取得できます。これらのコマンドは通常、GUI のネットワーク管理システムから実行します。MIB オブジェクトはツリー構造であり、ツリーにはパブリック（標準）ブランチとプライベート（独自）ブランチを含みます。

## N

**NAT** — Network Address Translation（ネットワーク アドレス変換）。1 つの IP アドレスを使用して複数のコンピュータをインターネット（または、その他の IP ネットワーク）に接続する方式。

## P

**PAT** — Port Address Translation（ポート アドレス変換）。レイヤ 4 で一意のポート アドレスを割り当てることで、LAN 上の多数のデバイスが 1 つの IP アドレスを共有できるメカニズム。

**PEM** Privacy Enhanced Mail（プライバシー エンハンスト メール）。各種暗号化方式を使用して機密性、認証、およびメッセージの完全性を提供するインターネット E メール。インターネットで広く利用されているわけではありません。

**ping** デバイスのアクセス可能性のトラブルシューティングを実行するための共通の方式。

ping は、ICMP エコー メッセージとその応答をテストします。ping はデバイスのもっとも簡単なテストであるため、まず最初に使用されます。

ping を実行して、送信パケット、受信パケット、パケット損失のパーセンテージ、およびラウンドトリップ時間（ミリ秒単位）を表示できます。

**PKCS** Public-Key Cryptography Standard。非対称暗号法の基本アプリケーションのデータ構造およびアルゴリズムの使用方法について、RSA Laboratories によって公開されている一連の仕様。

## R

**RAS** Registration, Admission, and Status Protocol。管理機能を実行するためにエンドポイントとゲートキーパー間で使用されるプロトコル。RAS シグナリング機能は、VoIP ゲートウェイとゲートキーパー間で、登録、許可、帯域幅変更、ステータス、および解放手順を実行します。

**RBAC** Role-Based Access Control（ロールベース アクセス コントロール）。定義済みのロールに権限を割り当てることができるメカニズム。その後、ロールは実ユーザに割り当てられ、各ロールに応じて、特定の機能へのアクセスが許可または制限されます。

**RSA** Rivest, Shamir, and Adelman Signatures。認証に使用される公開キー暗号システム。

**RTSP** Real Time Streaming Protocol。IP ネットワーク経由でのマルチメディア ストリームの効率的な配信のニーズを満たす目的で設計されたクライアントサーバ マルチメディア プレゼンテーション制御プロトコル。

## S

**SCCP** Skinny Client Control Protocol。skinny クライアントと Cisco CallManager（CCM）との間で設定されるメッセージングとして、シスコが所有し定義している独自の端末制御プロトコル。skinny クライアントの例としては、Cisco 7960、Cisco 7940、802.11b ワイヤレス Cisco 7920 などの Cisco 7900 シリーズ IP Phone、および Cisco Unity ボイスメール サーバがあります。*Skinny も参照してください。*

**Simple Message Transfer Protocol** *SMTP を参照してください。*

**SIP** Session Initiation Protocol（セッション開始プロトコル）。H.323 の代替として IETF MMUSIC ワーキング グループによって開発されたプロトコル。SIP 機能は、1999 年 3 月に公開された IETF RFC 2543 に準拠しています。SIP は、IP ネットワーク経由で音声およびマルチメディア コールをセットアップするためのシグナリングを実行するプラットフォームを備えています。

**Skinny** Skinny は、Cisco CallManager との効率的な通信を可能にする簡易プロトコルです。*SCCP も参照してください。*

**SLB** Server Load Balancer（サーバ ロード バランサ）。アプリケーションのアベイラビリティ、サーバのキャパシティ、およびラウンドロビンや最小コネクションなどのロード バランシング アルゴリズムに基づいて、ロード バランシングを決定するデバイス。SLB デバイスは、ロード バランシングとサーバ / アプリケーション フィードバックを使用して、パケット フロー用の実サーバを決定し、この情報を要求元のフォワーディング エージェントに送信します。最適な宛先が決定されると、パケット フロー内の他のすべてのパケットは、フォワーディング エージェントによって実サーバにダイレクトされるため、パケット スループットが向上します。

**SMTP** Simple Mail Transfer Protocol（シンプル メール転送プロトコル）。E メール サービスを提供するインターネット プロトコル。

## T

**TCP** Transport Control Protocol。信頼性の高い全二重データ伝送を可能にする、コネクション型トランスポート層プロトコル。TCP は TCP/IP プロトコル スタックの一部です。

**traceroute** ping が失敗した理由やアプリケーションがタイムアウトした理由を理解するために役立つ診断ツール。これを使用して、デバイスまでのルート上の各ホップ（または、ゲートウェイ）とそこに到達するまでの時間を表示できます。

**Transport Control Protocol** TCP *を参照してください。*

## U

**URI** Uniform Resource Identifier（ユニフォーム リソース識別子）。インターネット オブジェクトの名前をカプセル化し、それにネーム スペースの識別名をラベル付けした形式化された識別情報のタイプ。登録済みネーム スペース内の名前と登録済みプロトコルまたはネーム スペースを参照するアドレスから成るユニバーサル セットのメンバーを生成します。[RFC 1630]

## V

**VLAN** Virtual LAN（仮想 LAN）。（管理ソフトウェアを使用して）設定された 1 つ以上の LAN 上のデバイス グループ。実際には多数の異なる LAN セグメントに配置されている場合でも、同じケーブルに接続されているかのように通信できます。VLAN は物理接続ではなく論理接続に基づいているため、柔軟性がとても高い機能です。

**VLAN トランキング プロトコル** VTP を参照してください。

**VTP** VLAN Trunking Protocol（VLAN トランキング プロトコル）。VTP ドメイン内の VLAN の追加、削除、および名前の変更を管理することで、VLAN 設定の一貫性を維持するレイヤ 2 メッセージング プロトコル。VTP を使用すると、VLAN 名の重複、無効な VLAN タイプの指定、セキュリティ違反などのさまざまな問題によって生じる不正な設定および設定の矛盾が最小限に抑えられます。

**VTP ドメイン** VLAN 管理ドメインとも呼ばれ、同じ VTP ドメイン名を共有し、トランクで相互接続された 1 つ以上のネットワーク デバイスから構成されるドメイン。

## W

**Web サーバ**　他の人がアクセスできる Web ページを含むマシン。

## あ

**アクティブ化**　コンテンツ要求または接続をロード バランシングするために、エンティティをリソース プールに入れ、キープアライブ機能を起動します。一時停止 も*参照してください。*

**アドミニストレーティブ ディスタンス**　2 つのプロトコルが同じ宛先に関するルート情報を提供している場合に、ルータがどのルーティング プロトコルを使用するか決定するために、最初に使用する基準。アドミニストレーティブ ディスタンスは、ルーティング情報のソースの信頼性を示す評価基準です。アドミニストレーティブ ディスタンスはローカルでだけ有意義で、ルーティング アップデートによってアドバタイズされることはありません。

アドミニストレーティブ ディスタンスの値が小さいほど、プロトコルの信頼性は高くなります。値の範囲は、接続されたインターフェイスの場合の 0 およびスタティック ルートの場合の 1 から、未知のプロトコルの場合の 255 までです。

## い

**一時停止**　将来のロードバランシング コンテンツ要求または接続に備えて、リソース プールからエンティティを削除します。サービスまたはデバイスを一時停止しても既存のコンテンツ フローには影響しませんが、追加の接続が一時停止したエンティティまたはコンテンツにアクセスするのを防ぐことができます。アクティブ化 も*参照してください。*

**イベント**　各仮想コンテキスト、管理システム、ハードウェア コンポーネントを含むシステムの各部分のアクティビティを通知する ACE アプライアンス Device Manager からのメッセージ。

**イベント タイプ**　アラーム、ログ、監査、攻撃ログ。

**インターフェイス**　1. ネットワーク接続。

2. 2 つのシステムまたはデバイス間の接続。

3. テレフォニーにおいて、共通の物理相互接続特性、信号特性、および交換される信号の意味によって定義される共有境界。

## お

**オブジェクト**　ACE アプライアンス Device Manager を使用して管理できる物理エンティティ、サービス、またはリソース。

**オブジェクト グループ**　サーバ、クライアント、サービス、ネットワークなどの類似のオブジェクトの論理グループ。オブジェクト グループを作成することで、各オブジェクトを個々に指定することなく、多数のオブジェクトに共通の属性を適用できます。

## か

**仮想コンテキスト** ユーザが ACE アプライアンスを複数の仮想デバイスに分割できる概念。各仮想コンテキストには、ポリシー、インターフェイス、リソース、および管理者の専用のセットが含まれるため、管理者はより効率的にシステム リソースとサービスを管理できます。

**仮想サーバ** 仮想サーバは、実サーバのグループを表し、実サーバ ファームに関連付けられます。

## く

**クラス マップ** ネットワーク トラフィックのタイプを分類するメカニズム。ACE アプライアンス Device Manager は、クラス マップを使用して、ACE アプライアンスによって送受信されたネットワーク トラフィックを分類します。トラフィックのタイプには、ACE アプライアンスを経由できるレイヤ 3/ レイヤ 4 トラフィック、ACE アプライアンスによって受信できるネットワーク管理トラフィック、およびレイヤ 7 HTTP ロードバランシング トラフィックが含まれます。

## こ

**コンテキスト** 仮想コンテキストを参照してください。

## さ

**サーバ ファーム** 同じコンテンツを内包するサーバの集合。

**サーバ ロード バランサ** SLB *を参照してください。*

**サービス** コンテンツの一部が物理的に常駐する場所。このリリースでは、コンテンツ ルール、所有者、仮想サーバ、実サーバなどを総称してサービスと呼ぶこともあります。

## し

**しきい値** ネットワークが実行すると予測される範囲。しきい値を超えるか、予測された下限を下回った場合は、問題が潜在する領域を調べます。特定のデバイスのしきい値を作成できます。

**実サーバ** 実サーバは、サーバ ファームに割り当てられた物理デバイスです。

**障害** システム コンポーネントがパフォーマンスしきい値を超えたか、正常に機能していない場合に発生する異常な状態。

**冗長性** インターネットワーキングでは、障害の発生時に、冗長のデバイス、サービス、または接続が障害の生じたデバイス、サービス、または接続の機能を実行でうるようにするための、デバイス、サービス、または接続の二重化。

**証明書署名要求** CSR *を参照してください。*

**証明書チェーン** 証明書チェーンは、SSL で使用される証明書の階層型リストで、サブジェクトの証明書、ルート CA 証明書、および中間 CA 証明書を含みます。

## す

**スティッキ** 同じクライアントが複数の接続で同じサーバを取得するように保証する機能。アプリケーションが同じサーバとの一貫した定常的な接続を必要とする場合に使用されます。接続に関する状態テーブルを保持しているシステムに接続している場合は、スティッキ機能を使用して、再度同じ実サーバに戻り、システムのステートフルネスを維持できます。

## ち

**チェックポイント** 修正する前の、既知で不変の ACE の実行コンフィギュレーションのスナップショット。実行コンフィギュレーションを変更するときに問題が発生した場合は、コンフィギュレーションを以前の不変のコンフィギュレーション チェックポイントにロールバックできます。

## と

**特殊な設定ファイル（special configuration file）** 設定ファイルやキープアライブ スクリプトの一部など、ACE アプライアンス上の管理対象ファイル リソース。

## に

**認定者名** SSL で使用され、サイトを認証するために必要な情報と認証局を提供する属性のセット。

## ほ

**ポート** 1. インターネットワーキング デバイス（ルータなど）のインターフェイス。物理エンティティ。

2. IP 用語では、下位レイヤから情報を受信する上位層プロセス。ポートは番号が付けられ、番号付きのポートはそれぞれ特定のプロセスに関連付けられます。たとえば、SMTP はポート 25 に関連付けられます。ポート番号は、well-known アドレスとも呼ばれます。

3. 本来の設計対象とは異なるハードウェア プラットフォーム、または異なるソフトウェア環境で稼働できるように、ソフトウェアまたはマイクロコードを書き換えること。

## ゆ

**ユーザ ロール** 機能へのアクセス権をユーザ アカウントに付与するメカニズム。

## り

**リソース クラス**　デバイス（ACE アプライアンスなど）が使用できる定義済みのリソースと割り当てのセット。リソース クラスを使用することで、単一のデバイスによって使用可能なリソースがすべて使用されてしまうのを防ぐことができます。

## れ

**例外**　関連する障害のグループ。

## ろ

**ロード バランシング**　各種アルゴリズムに基づいて、ネットワーク要求をサーバ クラスタ内の使用可能な複数のサーバに拡散する処理。

**ロール**　ユーザ ロール *を参照してください。*