



GLOSSARY

0 ~ 9

- 802.1X** dot1X とも呼ばれる 802.1X は、ポートベース ネットワーク アクセス コントロールの標準 IEEE です。この標準では、クライアントとオーセンティケータ（スイッチ、ワイヤレス アクセス ポイント）との間の通信に Extensible Authentication Protocol (EAP) プロトコルが使用されます。
- 802.1X-REV** 802.1X-REV は、802.1X 標準のリビジョンであり、セキュリティ暗号化およびセキュアなキー交換が含まれ、認証されるデバイスと許可されるデバイスとの間のセキュアな通信が可能になります。802.1X-REV 機能には、802.1AE MAC セキュリティ (MACSec) 暗号化および 802.1af MACSec キー共有 (MKA) プロトコルが含まれます。

A

- AAA** コンピュータ リソース アクセスの知的制御、ポリシーの実装、使用状況の監査、およびサービス 請求に必要な情報の提供を実現する管理フレームワークでの認証、許可、アカウントिंगの各 プロセスの結合です。これら 3 つのプロセスは、効果的なネットワーク管理およびセキュリティ に不可欠であると見なされています。AAA は通常、IP ベース ネットワーキングのサーバベース システムで、ユーザがアクセスするコンピュータ リソースを制御し、ネットワーク上でのユーザ アクティビティを管理および監査します。
- AAA クライアント IP アドレス** AAA クライアントの IP アドレス。これを使用して、ネットワーク デバイスと相互作用するよう に AAA クライアントを Cisco Identity Services Engine (Cisco ISE) に設定します。複数のネット ワーク デバイスを示すには、複数の IP アドレスを指定します。各 IP アドレスは、Enter キーを 押して区切ります。
- AAA サーバ** コンピュータ リソースへのユーザ アクセス要求を管理するサーバ プログラム。企業の場合は、 認証、許可、アカウントिंग (AAA) サービスを提供します。一般的に、AAA サーバは、 ネットワーク アクセス サーバおよびゲートウェイ サーバ、ユーザ情報を格納するデータベース およびディレクトリと相互作用します。現在、デバイスまたはアプリケーションと AAA サーバ との通信に使用されている標準は、RADIUS です。
- Active Directory** Active Directory は、Windows ベースの環境で使用するための、LDAP ディレクトリ サービスの Microsoft 実装です。Active Directory により、管理者は、ネットワーク全体にわたるポリシーを 割り当てたり、多数のコンピュータ システムにプログラムを同時に展開したり、重要な更新を組 織全体に適用したりできます。Active Directory では、組織に関する情報および設定が、集中型 のアクセス可能なデータベースに格納されます。
- ADR** アクセシビリティ設計要件。アクセシビリティ製品、Web サイト、およびドキュメンテーション の設計方法に関する詳細を提供します。
- AES** 高度暗号化規格。連邦情報処理標準 (FIPS) の刊行物。米国政府機関が機密 (非機密) 情報を保 護するために使用する暗号アルゴリズムを定めています。この規格では、米国政府機関 (および その他) が機密情報を保護するために使用する FIPS 承認の対称暗号化アルゴリズムとして、 Rijndael を指定しています。機密情報を保護する政府機関 (およびその他)。

- AP** アクセスポイント。無線ネットワークのハブです。無線クライアントはアクセスポイントに接続します。また、2つのクライアント間のトラフィックはアクセスポイントを通過する必要があります。
- API** アプリケーションプログラミングインターフェイス。アプリケーションプログラムを作成するプログラマーが、オペレーティングシステムまたは別のアプリケーションへの要求を作成する場合に使用する特定の手法です。
- ARP** アドレス解決プロトコル。IPアドレスを、ローカルネットワーク内で認識されている物理マシンアドレスにマッピングするプロトコルです。通常はARPキャッシュと呼ばれるテーブルを使用して、各MACアドレスと対応するIPアドレス間の相互関係を保持します。ARPは、この相互関係を構築し、両方向のアドレス変換を可能にするプロトコルルールを提供します。
- ARPANET** Advanced Research Projects Agency Network。1970年代初期に米国政府との契約の下で構築された先駆的なパケットスイッチドネットワークです。今日のインターネットの発展を導き、1990年6月に廃止されました。
-
- B**
- BIND** Berkeley Internet Name Domain。DNSの実装。DNSはドメイン名のIPアドレス解決に使用されます。
-
- C**
- CA** 認証局。セキュリティクレデンシャルとメッセージ暗号化および復号化のための公開キーを発行し、管理するネットワーク内の機関。CAは、公開キーインフラストラクチャ(PKI)の一部として、デジタル証明書の要求側が提供した情報を確認するために登録局(RA)に問い合わせます。RAが要求者の情報を確認すると、CAから証明書が発行されます。
- CAの署名** デジタル証明書の信頼性を保証するデジタルコード。CAの署名は、証明書を発行する認証局(CA)によって提供されます。
- CGI** コモンゲートウェイインターフェイス。このメカニズムは、パラメータを実行可能スクリプトに渡して応答を動的に生成するために、HTTPサーバ(Webサーバ)によって使用されます。
- CHAP** チャレンジハンドシェイク認証プロトコル。リプレイアタックを防ぐためにチャレンジごとに応答が変わる、チャレンジ/レスポンス認証メカニズムを使用するプロトコルです。
- CHAPは、リンクの確立後にサーバが要求側にチャレンジを送信する認証技術です。要求側は、一方向ハッシュ関数を使用して取得された値を格納して応答します。サーバは、この値をサーバ側で予測しているハッシュ値の計算結果と比較することによって、応答を確認します。値が一致した場合は認証が認められ、そうでない場合は、通常、接続が終了します。
- CN** 一般名(Common Name)は、LDAPディレクトリエントリでリストされている属性の1つです。
- CoA** RADIUS許可変更。セッションが認証された後で、その属性を変更するメカニズムを提供します。AAAでユーザ、またはユーザグループのポリシーに変更がある場合は、Cisco ISEなどのAAAサーバからRADIUS CoAパケットを送信して、認証を再初期化し、新しいポリシーを適用することができます。

Cookie	クライアント側の状態情報を格納し、後で取り出してサーバが使用するために、HTTP サーバとブラウザ（サーバのクライアント）間で交換されるデータ。HTTP サーバはクライアントへのデータ送信時に同時に Cookie を送信し、クライアントは HTTP 接続が終了した後もこの Cookie を保持します。サーバはこのメカニズムを使用して、HTTP ベース アプリケーションのクライアント側の永続的状态情報を保持し、以降の接続でその状態情報を取り出すことができます。
CoS	サービス クラス。類似したタイプのトラフィック（電子メール、ストリーミング ビデオ、音声、大きなドキュメントのファイル転送など）をグループ化し、各タイプを専用のサービス優先レベルを持つクラスとして処理することによって、ネットワーク内のトラフィックを管理する方法。
CRL	証明書失効リスト。取り消し済みで、もう有効ではなく、いかなるシステム ユーザも信頼すべきではない証明書（正確には、証明書のシリアル番号）のリストです。
CRUD	作成、読み取り、更新、および削除。管理対象データで実行される基本的な管理操作です。
CSS	カスケーディング スタイル シート。スタイル要素の定義が衝突した場合には定義済みの優先順位を使用して複数のソースから作成される Web ページです。
CSV	カンマ区切り形式。このファイル形式は、フィールドをカンマで区切り、レコードを改行で区切る区切りデータ形式です。
CUE	コモン ユーザ エクスペリエンス

D	
Deep-Drill	Cisco ISE ダッシュボード上のスパークラインをクリックすると、データの詳細なレポートが自動的に表示される機能。
DES	データ暗号規格。広く使用されている、秘密キーを使用したデータ暗号化方式です。使用できる暗号キーは 72,000,000,000,000,000（7 京 2 千兆）以上あります。特定のメッセージごとに、この莫大な数のキーの中からランダムにキーが選択されます。他の秘密キー暗号方式と同様に、送信側と受信側の両方で同じ秘密キーを知っており、また使用する必要があります。
Diffie-Hellman	Whitfield Diffie および Martin Hellman によって 1976 年に発表されたキー共有アルゴリズム。Diffie-Hellman はキーの設定であり、暗号化ではありません。ただし、作成されたキーは暗号化や高度なキー管理操作、または他の暗号法に使用される場合があります。
DIT	ディレクトリ インフォメーション ツリー (Directory Information Tree)。ネーミング コンテキストとも呼ばれます。ローカル ディレクトリ構造を構成するオブジェクトの階層。複数の DIT が LDAP サーバによってサポートされます。この情報はルート DSE によって提供されます。
DLL	ダイナミック リンク ライブラリ。コンピュータ内で実行している大きなプログラムから必要に応じてコールできる、小さなプログラムの集合。大きなプログラムとプリンタやスキャナなどの特定のデバイスとの通信を可能にする小さなプログラムは、多くの場合、DLL プログラム（通常、DLL ファイルと呼ばれる）としてパッケージ化されています。
DN	識別名。DN は、目的のエントリからディレクトリ ルートまで DIT を上向きにたどって一意にネーミング属性を示す一連の RDN で構成されます。DN は左から右に記述されます。
DNS	ドメイン ネーム システム。インターネット ドメイン名を検索して、IP アドレスに変換する方法。ドメイン名はインターネット アドレスを示す、意味のある覚えやすい「ニックネーム」です。
DSA	デジタル署名アルゴリズム。大きな数値のペアの形式でデジタル署名を作成する非対称暗号方式のアルゴリズム。署名者の ID および署名日の整合性を確認できるように、署名はルールとパラメータを使用して計算されます。

DSA (Directory System Agent)	LDAP サーバなど、DAP または LDAP 対応のディレクトリ サービスを示す X.500 の用語。
DSE (DSA Specific Entry)	ローカル ディレクトリ サーバ内のエントリ。
DSS	デジタル署名規格。非対称暗号法を含むデジタル署名アルゴリズム (DSA) について定めている米国政府規格です。
<hr/>	
E	
EAP	Extensible Authentication Protocol。PPP (ポイントツーポイント プロトコル) で使用されている認証方式を拡張する、無線ネットワークのプロトコル。多くの場合、コンピュータをインターネットに接続するときに使用されます。EAP は、トークンカード、スマートカード、証明書、ワンタイムパスワード、公開キー暗号認証など、複数の認証メカニズムをサポートできます。
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling。EAP-FAST は IEEE 802.1X と IEEE 802.11i に準拠しています。すべての EAP タイプと同様に EAP-FAST は WPA ネットワークと WPA2 ネットワークで使用できます。
EAP-MD5	Extensible Authentication Protocol-Message Digest 5。RSA Security によって開発された EAP セキュリティアルゴリズム。生成された 128 ビットの数字列またはハッシュを使用してデータ通信の信頼性を確認します。
EAP-TLS	Extensible Authentication Protocol-Translation Layer Security。クライアントとサーバの両方からの認証を要求する、EAP の高セキュリティバージョン。これらのうちの一方で適切なオーセンティケータの提示に失敗した場合、接続は終了します。クライアント コンピュータにあらかじめデジタル証明書をインストールしておくことにより、802.1X のセキュア接続を作成できます。EAP-TLS は、クライアントとサーバ間の相互認証、および整合性が保持される暗号スイートネゴシエーションやキー交換に役立つプロトコルです。クライアントとサーバの両方で X.509 証明書を使用して、相互に ID を確認します。
EditorAdmin	ネットワーク リソースの削除権限を除き、Cisco ISE ユーザ インターフェイスのすべての部分を編集する権限を持つユーザ ロール。
Ethernet	最も広く導入されている LAN テクノロジー。IEEE 802.3 規格で定められており、一般的にイーサネット LAN は同軸ケーブルまたは特別グレードのツイストペア線を使用します。デバイスはケーブルに接続され、CSMA/CD プロトコルを使用してアクセス権を競合します。
<hr/>	
F	
FTP	ファイル転送プロトコル。テキストまたはバイナリ ファイルのネットワークでの転送を定めている TCP/IP プロトコルです。
<hr/>	
H	
HelpDeskAdmin	Cisco ISE ダッシュボード、およびモニタリングとレポートでのアラームの読み取り専用権限を持つユーザ ロール。

HTML	ハイパーテキスト マークアップ言語。ワールドワイド ウェブ ブラウザ ページに表示することを目的としたファイルに、挿入されるマークアップ記号またはコードのセットです。
HTTP	ハイパーテキスト転送プロトコル。インターネット上でハイパーテキスト ドキュメントを転送するために使用されるインターネット プロトコル (IP) ファミリのプロトコルです。
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer または HTTP over SSL。HTTPS は Netscape が開発して自社のブラウザに組み込んだ Web プロトコルです。ユーザのページ要求と Web サーバから返されるページを暗号化および復号化します。URL の最初の部分 (コロンの前、アクセス スキームまたはプロトコルを指定する部分) で使用されると、この用語はセキュリティ メカニズム (通常、SSL) で拡張された HTTP を使用することを指定します。HTTPS は下位レイヤ、TCP/IP、および HTTP と TCP との間に追加された暗号化 / 認証レイヤとのやり取りに、HTTP ポート 80 ではなくポート 443 を使用します。
<hr/>	
I18n	国際化およびローカリゼーションは、ネイティブ以外の環境 (特に、他の国や文化) のソフトウェアを適合させる手段です。国際化は事実上、どのような場所でも使用できるように製品を適合させることであり、一方、ローカリゼーションは、特定のロケールで使用できるように特別な機能を追加することです。
ID	ある人が何者か、またはある物が何なのかを識別するもの。たとえば、ある物を認識するための名前などです。
IdentityAdmin	内部 ISE ID ストア内のエントリ (内部ユーザやホストなど) を追加、更新、および削除する権限を持つユーザ ロール。
ID グループ	すべてのタイプのユーザおよびホストに関連付けられる論理エンティティ。
ID ソース	Cisco ISE が認証のためにユーザ情報の取得に使用する内部ユーザ、AD、LDAP などのデータベース。
ID ソース順序	Cisco ISE が認証のためにユーザ情報を検索する一連の ID ソースが含まれたオブジェクト。Cisco ISE は、ID ソース順序で定義された順序でこれらの ID ソースを検索します。
IETF	インターネット技術特別調査委員会。TCP/IP などの標準インターネット運用プロトコルを定義している団体です。IETF は、インターネット学会のインターネット アーキテクチャ委員会 (IAB) によって管理されています。IETF のメンバーは、インターネット学会の個人および組織メンバーシップから選出されます。
IP	インターネット プロトコル。インターネット上の 1 つのコンピュータから別のコンピュータにデータを送信するための手段またはプロトコルです。インターネット上の各コンピュータ (ホストと呼ばれる) には、そのコンピュータをインターネット上の他のすべてのコンピュータと区別して一意に識別する IP アドレスが最低 1 つ割り当てられます。
IPSec	インターネット プロトコル セキュリティ。ネットワーク通信のネットワークまたはパケット処理レイヤにおけるセキュリティの開発標準です。
IP アドレス	インターネット プロトコルおよび他のプロトコルで使用するために割り当てられる、コンピュータのインターネットワーク アドレス。IPv4 アドレスは、ピリオドで区切られた 4 つの 8 ビット数値の並びで示されます。
IP スプーフィング	誤った IP アドレスを提供する方法。

- IP 転送** ホストがルータとして動作することを許可するオペレーティング システムのオプション。2 つ以上のネットワーク インターフェイス カードを持つシステムでは、システムがルータとして動作できるように IP フォワーディングを有効にしておく必要があります。
- IP フラッド** プロトコル実装で処理可能な数よりも多いエコー要求（「ping」）パケットをホストに送信する DoS 攻撃。
- ISO** 国際標準化機構。1947 年に設立された国際条約に基づかないボランティアの非政府組織。参加国の指定された標準化団体である投票メンバーと、投票権のないオブザーバ組織で構成されます。
- ISP** インターネット サービス プロバイダー。インターネット アクセスおよび関連するサービスを消費者に提供するビジネスまたは組織。以前は、ほとんどの ISP が電話会社によって運営されていました。

J

- Java** Sun Microsystems が開発した、オブジェクト指向プログラミング言語。Java 言語は、洗練された簡潔な設計となっており、ソース レベルとバイナリ レベルの両方でプラットフォームやオペレーティング システムを越えて移植可能です。
- JRE** Java ランタイム環境。コンピュータ システムで Java アプリケーションを実行できるようにするソフトウェア バンドルです。

K

- Kerberos** マサチューセッツ工科大学で開発されたシステム。パスワードおよび対称暗号方式（DES）を利用して、チケットベースのピア エンティティ認証サービス、およびクライアント / サーバ ネットワーク環境に配布されるアクセス コントロール サービスを実装します。

L

- LDAP クライアント** LDAP クライアントは、LDAP サーバへのアクセスを提供するソフトウェアです。大多数の標準 Web ブラウザでは、LDAP URL を使用して、限定された LDAP クライアントの機能を提供しています。LDAP ブラウザおよび Web インターフェイスはともに LDAP クライアントの非常に一般的な例です。オープン ソース クライアントのリスト。
- Lightweight Directory Access Protocol (LDAP)** LDAP は、TCP/IP 上で実行しているディレクトリ サービスを使用してデータの問い合わせおよび変更を行うネットワークング アプリケーション プロトコルです。LDAP プロトコルは、組織、個人、ネットワーク内のファイルやデバイスなどの他のリソースをパブリック インターネット上または企業イントラネット上で検索するために使用されます。

M

- MAC アドレス** 物理メディア アクセス コントロール アドレス。ネットワーク デバイスを世界中に存在する他のすべてのネットワーク デバイスと区別して一意に識別する製造業者によって割り当てられた数値です。

matchingRule (LDAP)	検索操作における属性の比較方式。matchingRule は、通常、OID と名前 (caseIgnoreMatch [OID = 2.5.13.2] など)、および操作するデータ型 (DirectoryString など) を含む ASN.1 定義です。
MD5	一方向の暗号ハッシュ関数。
MIB (管理情報ベース)	MIB は、簡易ネットワーク管理プロトコル (SNMP) を使用して管理できるネットワーク オブジェクトセットの公式な記述です。
MPPE (Microsoft Point-to-Point Encryption)	PPP (ポイントツーポイント プロトコル) およびバーチャル プライベート ネットワーク リンク上のデータを暗号化するプロトコル。
<hr/>	
N	
NAS (ネットワーク アクセス サーバ)	リモート リソースへの唯一のアクセス ポイント。NAS は、保護されたリソースへのアクセスを守るゲートウェイとして動作するように意図されています。これはたとえば、電話ネットワークからプリンタへ、またはインターネットへのゲートウェイです。
NetworkDeviceAdmin	Cisco ISE ネットワーク デバイス リポジトリを管理する権限 (デバイスの追加、更新、削除など) を持つユーザ ロール。これらの権限により、その管理者のみがネットワーク デバイスに対して読み書きアクセスができます。
<hr/>	
P	
PAP (パスワード認証プロトコル)	PAP は、リモート アクセス サーバまたはインターネット サービス プロバイダー (ISP) に対してユーザを認証するために使用される単純な認証プロトコルです。
PasswordAdmin	内部ユーザのパスワードを変更する権限を持つユーザ ロールであり、管理者アカウントを管理する管理者向けのロールです。これらの権限を持つ管理者は、他の管理者のパスワードを変更できません。
PI (プログラマチック インターフェイス)	Cisco ISE PI は、Cisco ISE と通信して Cisco ISE を設定および操作する機能を、外部アプリケーションに提供するプログラマチック インターフェイスです。PI により、Cisco ISE オブジェクトで作成、更新、削除、および読み取りの操作を実行できます。
PPP (ポイントツーポイント プロトコル)	PPP はシリアル インターフェイスを使用する 2 つのコンピュータ間の通信プロトコルであり、一般に、パーソナル コンピュータを電話回線でサーバに接続する場合に使用されます。たとえば、インターネット サーバ プロバイダーは、プロバイダーのサーバでユーザ要求に回答し、その要求をインターネットに渡して、要求に対するインターネットからの応答をユーザに転送できるように、ユーザに PPP 接続を提供します。PPP はインターネットプロトコル (IP) を使用し、その他を処理するように設計されています。場合によっては、プロトコルの TCP/IP スイートのメンバーと見なされることもあります。開放型システム間相互接続 (OSI) 参照モデルと比較すると、PPP ではレイヤ 2 (データリンク層) サービスが提供されます。基本的にこのサービスは、コンピュータの TCP/IP パケットをパッケージ化して、それらを実際にインターネット上に配置できるサーバに転送します。
PRA	定期的再評価では、ホストの準拠性を定期的に確認して Cisco ISE サーバにレポートします。

R

RADIUS サーバ	RADIUS インターフェイスをサポートするサードパーティ製サーバ。
RDN (LDAP)	相対識別名 (Relative Distinguished Name) (Relatively Distinguished Name と書かれることがよくありますが、これは正しくありません) は、X.500 の用語です。属性に与えられる、階層のそのレベルで一意的な名前です。RDN は、単一値または多値になることがあり、後者の場合、2 つ以上の属性を「+」(プラス) で結合して RDN を作成します (cn+uid など)。RDN という用語は、選択したエントリ (または検索開始場所) からディレクトリ ルート (正確にはルート DSE) まで、DIT を上向きにたどって一意に属性を示す DN の一部として使用される場合に限り意味を持ちます。
referral (LDAP)	LDAP サーバが LDAP クライアントに、LDAP クライアントが要求している情報を提供できる可能性のある、別の LDAP サーバの名前を (一般に、LDAP URL の形式で) 返す動作。
ReportAdmin	レポートの生成と表示、およびデータのモニタリングの権限を持ち、ログに読み取り専用アクセスができるユーザ ロール。
RFC (Request for Comments)	インターネット テクノロジーに適用可能な新しい研究、手法、および方法論を含む一連の文書。
rootdn (LDAP)	rootdn は slapd.conf ファイル内の紛らわしい名前を持つディレクティブです。通常のディレクトリ アクセス ルールを無視できるスーパーユーザを定義します。
RPM (RedHat Package Manager)	RPM をパッケージ管理フォーマットとして使用する Linux ディストリビューションにインストールできる、ダウンロード可能なソフトウェア パッケージ。

S

SAN (サブジェクト代替名)	証明書情報内の拡張フィールド。
Secure Sockets Layer (SSL)	Netscape 社が開発した、インターネット経由でプライベート ドキュメントを送信するプロトコル。SSL は、公開キーを使用して、SSL 接続で転送されるデータを暗号化することにより動作します。SSL は、Web ブラウジング、電子メール、インターネット ファクス、他のデータ転送などに、インターネットでの安全な通信を提供する暗号プロトコルです。SSL 3.0 と TLS 1.0 には多少違いがありますが、プロトコルは実質的には同じです。ここで使用される「TLS」という用語は、コンテキストで明確にされていない限り両方のプロトコルに適用されます。
SecurityAdmin	管理者アカウントの作成、更新、削除や、管理ロールの割り当て、およびパスワード ポリシーの変更の権限を持つユーザ ロール。
SGA デバイス	Cisco Security Group Access ソリューションをサポートするデバイス。
SLA (サービス レベル契約)	SLA は、特定のサービス レベルが合意されているサービス契約部分です。SLA は 2 者間の公式なネゴシエーションによる合意です。これは、お客様とサービス プロバイダーの間、またはサービス プロバイダー間に存在する契約です。サービス、優先度、責務、保証などに関する共通理解を書面にしたものです。可用性、サービスアビリティ、パフォーマンス、動作、または課金などのその他の属性のレベルを指定します。
SMS	Short Message Service。

SMTP (Simple Mail Transfer Protocol)	SMTP は、インターネット プロトコル (IP) ネットワークでの電子メール伝送用のインターネット標準です。
SNMP (簡易ネットワーク管理プロトコル)	ネットワーク デバイスをモニタおよび制御して、設定、統計収集、パフォーマンス、およびセキュリティを管理する手段を提供する TCP/IP ネットワーク プロトコル。
SOAP (Simple Object Access Protocol)	非集中的な分散環境で情報を交換するための、軽量の XML ベース プロトコル。SOAP は、メッセージの内容と処理方法を示すためのフレームワークを定義するエンベロープ、アプリケーション定義のデータ型のインスタンスを表す符号化ルールのセット、リモート プロシージャ コールと応答を表現するための表記法の 3 つの部分で構成されます。
SPML (Service Provisioning Markup Language)	SPML は、サービス プロビジョニング要求の統合および相互運用のためのオープン標準プロトコルです。
SSH (セキュア シェル)	リモート マシンでコマンドを実行したり、あるマシンのファイルを別のマシンに移動したりするために、ネットワーク上の別のコンピュータにログインするプログラム。
SSL (Secure Sockets Layer)	SSL は、ネットワーク経由の通信にセキュリティを提供する暗号化プロトコルです。
SuperAdmin	システム全体における、モニタリングやトラブルシューティングなどの権限を持つユーザ ロール。SuperAdmin 権限により、管理者はすべての Cisco ISE リソースを作成、読み取り、更新、削除、および実行 (CRUDX) できます。

T

TCP/IP	伝送制御プロトコル/インターネット プロトコルは、基本的な通信言語またはインターネットのプロトコルです。TCP/IP は 2 レイヤプログラムです。上位層である伝送制御プロトコルは、メッセージまたはファイルを小さなパケットに分割してインターネットで送信し、さらに受信側の TCP レイヤでこのパケットが元のメッセージに再構成されるよう管理します。下位レイヤであるインターネット プロトコルは、パケットが正しい宛先に到着するように、各パケットのアドレス部分を処理します。
TrustSec ソリューション	Cisco TrustSec は、ポリシーベースのアクセス制御、アイデンティティ認識ネットワークング、およびデータ整合性と機密性のサービスにより、ネットワークおよびネットワーク リソースへのセキュアなアクセスを可能にする、アイデンティティベースのアクセス コントロール ソリューションです。

U

UDP	ユーザ データグラム プロトコル。インターネット プロトコル (IP) を使用するネットワークのコンピュータ間でメッセージが交換されるときに、制限されたサービスを提供する通信プロトコルです。
URL	ユニフォーム リソース ロケータ。インターネット上にあるアクセス可能なファイルの一意的なアドレスです。

V
ViewerAdmin

Cisco ISE ユーザ インターフェイスのすべての部分の読み取り専用権限、およびすべてのネットワーク リソースへの読み取り専用アクセス権限を持つユーザ ロール。

VPN

バーチャル プライベート ネットワーク。ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN では、「トンネリング」が使用され、すべての情報が IP レベルで暗号化されます。

VSA

ベンダー固有属性。リモート認証ダイヤルイン ユーザ サービス (RADIUS) の標準属性セットでは提供されない専用のプロパティまたは特性です。VSA は、リモート アクセス サーバのベンダーによって、RADIUS をベンダー サーバ用にカスタマイズするために定義されます。

W
WCS

Cisco Wireless Control System は、企業によるシスコ製無線 LAN の設計、制御、およびモニタリングを支援するように設計されているプラットフォームです。WCS は無線 LAN を計画、設定、および管理するための業界最先端のプラットフォームです。

Web サーバ

Web サーバは、クライアント / サーバ モデルおよびワールドワイド ウェブのハイパーテキスト転送プロトコル (HTTP) を使用して、Web ページを形成するファイルを Web ユーザ (要求を転送する HTTP クライアントがコンピュータにインストールされている) に提供するプログラムです。

Web サービス

Web サービスは、ネットワーク上の相互運用可能なマシン間の相互作用をサポートするように設計されているソフトウェア システムです。Web サーバ インターフェイスは、マシン処理可能な形式である WSDL で記述されます。他のシステムは、一般的に XML シリアル化を使用する HTTP と他の Web 関連標準を併用して、Web サービスと相互に作用します。

WLC (ワイヤレス LAN コントローラ)

WLC は、Cisco Unified Wireless Network (CUWN) の中心的役割を担うデバイスです。ワイヤレス クライアントの関連付けや認証といったアクセス ポイントの従来の役割は WLC によって実行されます。

WSDL (Web Services Description Language)

WSDL は、ビジネスが提供するサービスを記述し、個人および他のビジネスに、これらのサービスに電子的にアクセスする方法を提供するために使用される XML ベースの言語です。

X
X.509

公開キー インフラストラクチャの標準。X.509 は、特に、公開キー証明書の標準形式や認証パス検証アルゴリズムを定めています。

XML (Extensible Markup Language)

XML は共通の情報形式を作成して、ワールドワイド ウェブ、イントラネットなどで形式とデータの両方を共有するための柔軟な方法です。

あ
アカウントティング

ユーザ セッションをログ ファイルに記録する Cisco ISE の機能。

アクセス	必要な情報を取得する機能。データ アクセスとは、コンピュータ上の特定のデータを取得できること（通常、使用権限があること）です。
アクセス コントロール	リソースの使用権限があるユーザだけに、そのリソースの使用を許可します。
アクセス コントロール サービス	不正アクセスに対してシステム リソースを保護するセキュリティ サービス。このサービスを実装する基本メカニズムは ACL およびチケットの 2 つです。
アクセス コントロール システム (ACS)	認証、許可、アカウンティングを実行してネットワーク内のデバイスを管理する AAA サーバ。
アクセス コントロール リスト (ACL)	リソース アクセスが許可されているシステム エンティティの ID をリストすることによって、システム リソースに対するアクセス コントロールを実装するメカニズム。
アクセス ポリシー	Cisco ISE Web インターフェイスへのアクセスを、IP アドレス、TCP ポート範囲、および Secure Sockets Layer (SSL) によって制限するポリシー。
アプレット	Java プログラム。クライアントの Web ブラウザを使用してユーザ インターフェイスを提供するアプリケーション プログラムです。
暗号アルゴリズムまたは ハッシュ	暗号化アルゴリズム、暗号アルゴリズムまたはハッシュ、デジタル署名アルゴリズム (DSA)、キー共有アルゴリズムなど、暗号法の技術を利用したアルゴリズム。
暗号化	メッセージを傍受した人間にはそのメッセージが理解できないような方法で、メッセージを文字化けさせます。
暗号化	データの元の意味を隠して、知られたり使用されたりしないようにする形式（「暗号文」と呼ばれる）に、データ（「プレーンテキスト」と呼ばれる）を暗号変換すること。
暗号解析	システム設計で提供される保護の破壊または回避に必要な知識を得るために、暗号化システムの分析を処理する数理学。つまり、キーがわからない状態で暗号文をプレーンテキストに変換します。
暗号文	送信される暗号化形式のメッセージ。暗号文は暗号化されたデータです。暗号化プロセスの出力であり、適切な解読キーを使用することで判読可能な形式（プレーンテキスト）に戻せます。
アンチウイルス	既知または潜在するコンピュータ ウイルスを特定および削除するように設計されたソフトウェア プログラム。
イベント	システムまたはネットワーク内の観察可能な事象。
インライン PEP	インライン Policy Enforcement Point (IPEP) は、ネットワーク上のワイヤレス LAN コントローラ (WLC) やバーチャル プライベート ネットワーク (VPN) コンセントレータの背後にあるゲートキーパー ノードです。
エンドポイント	エンドポイントは、ネットワークのリソースとして使用できる、企業ネットワークに接続するネットワーク対応デバイスです。
エントリ (LDAP)	LDAP 対応ディレクトリに格納されているオブジェクトに与えられた名前。各エントリは、1 つの親エントリ（オブジェクト）およびゼロ個以上の子エントリ（オブジェクト）を持ちます。エントリのデータ コンテンツは 1 つまたは複数の属性で構成され、これらの属性の 1 つ（または複数）が、このオブジェクトを DIT 内で一意に識別するネーミング属性（正確には RDN）として使用されます。

オーセンティケータ (AT)	常に信頼ネットワークの一部となるデバイス。
オブジェクト セレクタ	特定の機能のために選択できる項目が含まれたポップアップ ダイアログボックス。オブジェクトセレクタは、多くの場合、選択したオプションに関する入力を提供するために別のダイアログにリンクされています。
<hr/>	
か	
外部 ID ソース	(ポリシーでの定義に従って) 内部ユーザおよび外部ユーザのクレデンシャルと認証確認を実行するために Cisco ISE がアクセスする外部データベース。
外部ユーザ	外部 ID ソースで定義されたユーザ。
拡張 ACL	Cisco ルータにおける標準 ACL のさらに強力な形式。IP アドレス (発信元または宛先)、ポート (発信元または宛先)、プロトコル、およびセッションが確立されているかどうかに基づいて、フィルタリング決定を行うことができます。
カットスルー	パケットが宛先に転送される前にパケットのヘッダーだけが読み取られるスイッチング方式。
カプセル化	あるデータ構造をしばらくの間隠しておくために、別の構造体の中に格納しておくこと。
監査	情報や資産を、ポリシーに準拠し、脆弱性から保護されているものとして保証するための情報の収集および資産の分析。
完全修飾ドメイン名	ホスト名の後ろに完全ドメイン名を付けたサーバ名。
管理操作	ネットワーク内の Cisco ISE サーバを効果的に展開および管理するために実行する必要がある操作のセット。
管理ペルソナ	Cisco ISE 上で実行される管理サービス。これにより、Cisco ISE を管理および維持できます。
キー	暗号法では、キーは、暗号化されたテキストを生成するために、アルゴリズムを使用して暗号化されていないテキストの文字列またはブロックに適用されたり、または暗号化されたテキストを復号化したりする変数の値です。キーの長さは、特定のメッセージに含まれるテキストの復号化がどの程度難しくなるかを考慮するうえで、1 つの要因となります。
偽装通信	正常なシステム操作を使用して、2 つのパーティ間で密かに情報をやり取りする方法。たとえば、ファイル サーバ上の使用可能なハード ドライブ容量を変更することで情報をやり取りできます。
基本認証	要求ごとにユーザ名とパスワードを送信することで機能する、最も簡単な Web ベースの認証スキーム。
機密性	情報を表示する権限があるユーザだけに情報が明示されることを保証する必要性。
キャッシュ	特別な高速ストレージ メカニズム。メイン メモリの予約済みセクションまたは独立した高速ストレージ デバイスを使用できます。パーソナル コンピュータでは、通常、メモリ キャッシングとディスク キャッシングの 2 つのタイプのキャッシングが使用されます。
許可	だれかまたは何かが行うことに対する承認、許可、または権限付与。
許可サーバ (AS)	認証サービスと許可サービスを提供する、Cisco ISE などの AAA サーバ。

許可されるプロトコル アクセス サービス	許可されるプロトコル アクセス サービスは、Cisco ISE がネットワーク リソースへのアクセスを要求するデバイスとの通信に使用する一連のプロトコルが含まれている設定可能なオブジェクトです。
許可プロファイル	RADIUS ベースのネットワーク アクセス サービスに使用される基本的な「権限コンテナ」。許可プロファイルは、ネットワーク アクセス要求に付与されるすべての権限を定義する場所です。応答で返される VLAN、ACL、URL リダイレクト、セッションタイムアウト、再許可タイマー、またはその他の RADIUS 属性を許可プロファイルに定義します。
クイック ビュー	ユーザ インターフェイスの場所に関する情報を提供するポップアップ ダイアログ。
クライアント	サーバと呼ばれる別のシステム エンティティによって提供されるサービスを要求して使用するシステム エンティティ。場合によっては、サーバ自身が別のサーバのクライアントになることもあります。
クライアント/サーバ	1つのプログラム（クライアント）が別のプログラム（サーバ）のサービスを要求し、サーバがその要求を実行するという、2つのコンピュータ プログラム間の関係を示します。クライアント/サーバの概念は、単一のコンピュータ内のプログラムでも使用できますが、ネットワークにおいてより重要な概念です。ネットワークでは、クライアント/サーバ モデルにより、さまざまな場所に効率的に配布されているプログラムを簡単に相互接続できます。
グローバル システム オプション	EAP-TTLS、PEAP、および EAP-FAST のランタイム特性の設定および EAP-FAST PAC の生成。
ゲートウェイ	別のネットワークへの入り口として機能するネットワーク ポイント。
ゲスト ユーザ	ゲスト ユーザは、ネットワークに一時的にアクセスするためにゲスト ユーザ アカウントを必要とするユーザです。
検索 (LDAP)	ベース ディレクトリ名 (DN)、範囲、および検索フィルタを定義することによって実行される動作。
公開キー	暗号法における公開キーとは、公開キーから派生される秘密キーと組み合わせた場合に、メッセージおよびデジタル署名の効果的な暗号化に使用できる暗号キーとして、指定機関から提供される値のことです。 公開キーと秘密キーを組み合わせることを、非対称暗号方式と呼びます。公開キーを使用するためのシステムを、公開キー インフラストラクチャ (PKI) と呼びます。
公開キー インフラストラクチャ (PKI)	PKI を使用すると、インターネットなどの基本的に安全ではないパブリック ネットワークのユーザでも、信頼できる機関を通じて取得および共有される公開暗号キーと秘密暗号キー ペアを使用することにより、データや金銭を安全かつ内密に交換できます。公開キー インフラストラクチャは、個人または組織を識別できるデジタル証明書と、証明書を格納したり、必要に応じて無効にしたりできるディレクトリ サービスを提供します。PKI のコンポーネントは一般に理解されていますが、さまざまなベンダー アプローチおよびサービスが出現しつつあります。その一方で、PKI のインターネット標準は変わらず有効です。
固定オーバーレイ	特定の機能への複数オプションの指定を簡素化する、固定化されたポップアップ ダイアログ。固定オーバーレイは通常、特定のユーザ インターフェイス機能に関連する要素にリンクされています。

コミュニティ ストリング	簡易ネットワーク管理プロトコル (SNMP) 要求に有効なソースを識別し、アクセス可能な情報の範囲を制限するために使用される文字列。Ravlin 装置はパスワードなどのコミュニティ ストリングを使用して、限定された管理ステーションのセットだけにその MIB へのアクセスを許可します。
コンピュータ ネットワーク	ホスト コンピュータと、これらのホスト コンピュータでデータ交換できるサブネットワークまたはインターネットワークの集合。
<hr/>	
さ	
サーバ	クライアントと呼ばれる他のシステム エンティティからの要求に応じて、サービスを提供するシステム エンティティ。
サービス拒絶	システム リソースに対する許可済みアクセスの妨害、またはシステムの動作や機能の遅延。
サービス選択ポリシー	どのアクセス ポリシーが着信要求に適用されるかを決定するルールのセット。
サービス プロビジョニング	サービス プロビジョニングは、特定のアクティビティを実行するために必要な IT システムの構成要素または提供物を「事前準備」することを示します。これには、ユーザ アカウントやシステム、ネットワーク、アプリケーションのアクセス権限などのデジタル サービスのプロビジョニングと、携帯電話やクレジット カードなどの非デジタル、つまり「物理的な」リソースのプロビジョニングがあります。
サイファ	暗号化および復号化のための暗号アルゴリズム。判読可能なメッセージ (プレーンテキストまたはクリアテキストと呼ばれる) を、判読不能、スクランブル、または非表示のメッセージ (暗号文と呼ばれる) に変換するための方式。
サフィックス (LDAP)	ルート、ベースとも呼ばれる、DIT 内の一番上のエントリを示す多数の用語の 1 つ。このエントリは、通常、OpenLDAP の slapd.conf ファイルの suffix パラメータで定義されるため、一般的にこの用語が使用されます。ルート DSE は一種のスーパー ルートです。サフィックスのネーミング。
サブタイプ (LDAP)	LDAPv3 では、多数のサブタイプを定義します。現時点で規定されているのは binary (RFC 2251) および lang (RFC 2596) の 2 つです。サブタイプは、属性の参照時に使用され、たとえば cn;lang-en-us=smith は US 英語を使用して検索を実行することを指定します。UTF-8 (cn に使用) ではすべての言語タイプを使用できるため、サブタイプは符号化には影響しません。言語サブタイプは大文字と小文字が区別されます。
差分バックアップ	ユーザが Monitoring & Report Viewer データベースの小規模なバックアップを定期的に作成できるようにするスケジュール ジョブ。
サポートバンドル	サポート バンドルには、Cisco ISE ログ メッセージが含まれおり、TAC の診断情報の準備に使用できます。
時間プロファイル	ゲスト アカウントに異なるアクセス時間レベルを割り当てます。
式ビルダー	メニューおよび他のポップアップ ダイアログから選択できるようにすることで、式の作成を簡素化するポップアップ ダイアログ。
指数バックオフ アルゴリズム	ネットワーク デバイスが飽和状態のリンクのデータ送信をタイムアウトし続けられないように、実行中に TCP タイムアウト値を調整するために使用されます。
システム管理	管理者グループによって実行されるロールベースの管理機能。

システム管理者	Cisco ISE GUI で定義された、さまざまなアクセス権限を持つ管理者。これらの管理者は、ネットワーク内の Cisco ISE 展開を管理します。
システム設定	システム パフォーマンスを設定するために管理者グループによって実行される、ロールベースの管理機能。
システムヘルス ダッシュボード	関連付けられた Cisco ISE インスタンスのヘルス ステータスに関する情報を提供する Monitoring & Report Viewer Dashboard。
修復	保護されたネットワークへのアクセスを認証されるためにホストが行う操作。
出力	出力は、データ パケットが信頼ネットワークを出るポイントであり、ここでセキュリティ グループ タグ (SGT) がパケットから削除され、出力ポリシーが適用されます。
出力フィルタリング	アウトバウンド トラフィックのフィルタリング。
衝突	複数のシステムが同時に同じ回線で送信した場合に発生します。
証明書	公開キーなどのユーザまたはデバイス属性のデジタル表現であり、信頼できる秘密キーで署名されています。
証明書認証プロファイル	証明書認証プロファイルは、ユーザの身元を保証するための証明書ベースの認証で使用される ID ソースです。
証明書ベースの認証	HTTP トラフィックを認証および暗号化するために、Secure Sockets Layer (SSL) および証明書を使用すること。
侵入検知	コンピュータおよびネットワーク用のセキュリティ管理システム。IDS はコンピュータまたはネットワーク内のさまざまな領域から情報を収集および分析して、侵入（組織外からの攻撃）と誤用（組織内からの攻撃）の両方を対象に、可能性のあるセキュリティ侵害を識別します。
信頼性	元の情報の正当性および適合性。
スキーマ (LDAP)	(名目上) 関連付けられることがある属性およびオブジェクト クラスのパッケージ。すべての ASN.1 関連情報を読み取りおよび解析できるように、アプリケーションで使用（参照）するオブジェクト クラスおよび属性をまとめたスキーマが LDAP サーバに対して特定されます。OpenLDAP では、これは <code>slapd.conf</code> ファイルで行われます。
スパークライン	縦線で長期にわたるトレンドを示す、Cisco ISE ダッシュボード上のウィジェットのタイプ。スパークラインの高さは、指定された期間（60 分や直前の 24 時間など）でのインスタンスの最大数のパーセンテージに基づきます。スパークラインをクリックすると、機能に関する詳細なデータを示す Deep-Drill レポートが生成されます。
スポンサー グループ	同じ権限セットを割り当てられたスポンサー ユーザのグループ。
スポンサー ユーザ	スポンサー ユーザは、ゲスト ユーザ アカウントを作成するユーザです。多くの場合、ネットワーク アクセスを提供する組織の従業員です。特定の職務上の役割を持つ個人、または Microsoft Active Directory (AD) などの企業のディレクトリに対して認証を行う従業員である場合もあります。
整合性	情報が偶然または故意に変更されておらず、また正確かつ完全であることを保証する必要性。
セキュリティ グループ アクセス (SGA)	セキュリティ グループ アクセス (SGA) は、信頼ネットワークのクラウドを確立して、セキュアなネットワークを構築するソリューションです。Cisco SGA ソリューションは、以前は Cisco TrustSec (CTS) ソリューションと呼ばれていました。

セキュリティ ポリシー	システムまたは組織がどのようにセキュリティ サービスを提供して機密に関わる重要なシステム リソースを保護するかを、指定または規定するルールおよび慣例のセット。
セッション	セッションは、ネットワーク トラフィックが渡される 2 つのホスト間の仮想接続です。
セッション (LDAP)	LDAP クライアントが bind コマンドを送信すると、クライアントとサーバ間でセッションが発生します。セッションは匿名または認証済みのいずれかになります。
セッション キー	対称暗号化のコンテキストで、一時的または比較的短い期間使用されるキー。通常、セッション キーは単一の接続またはトランザクション セットの期間など、2 つのコンピュータ間の定義済みの通信期間に使用されるか、または比較的大容量のデータを保護し、そのために頻繁にキーを入力する必要があるアプリケーションで使用されます。
セッション条件	カスタム条件、および日時条件。
設定管理	既知のベースライン条件を再確立して管理するプロセス。
全二重	一度に両方向にデータを伝送する二重通信チャネルのタイプ。同時に 2 つの方向にデータを送信することを意味しています。送信者と受信者の両方で同時に送信できる通信方式です。
属性 (LDAP)	エントリ内のデータは属性値のペアに含まれています。各属性には名前（場合によっては、略称）があり、 objectClass に属しています。属性の特性については、ASN.1 定義で詳しく説明されています。1 つまたは複数の objectClasses をスキーマに含めることができます。属性の ASN.1 定義に応じて、1 つのエントリ内に同じ名前を持つ属性の属性値のペアを複数指定できます。1 つ（または複数）の属性、ネーミング属性、または RDN により、エントリは常に一意に識別されます。

た	
対応策	脅威が検出された後、エクスプロイトが実行されないようにする対処的方法。侵入防御システム (IPS) では、一般的に、侵入者がこれ以上コンピュータ ネットワークにアクセスしないようにする対応策が展開されています。その他の対応策としては、パッチ、アクセス コントロール リスト、およびマルウェア フィルタがあります。
ダイジェスト認証	Web クライアントがパスワードの MD5 ハッシュを計算して、パスワードを持っていることを証明できるようにします。
ダッシュレット	ダッシュレットは、テキスト、フォーム要素、テーブル、グラフ、タブ、およびネストされたコンテンツ モジュールなどのさまざまなウィジェットを表示する UI コンテナです。
チェックサム	関数によって計算され、データ オブジェクトのコンテンツによって決まる値。データ内の変更を検出するために、オブジェクトに格納されるか、またはオブジェクトと一緒に送信されます。
チャレンジ/レスポンス	ユーザにいくつかの個人情報の入力（レスポンス）を要求（チャレンジ）する一般的な認証技術。スマート カードを利用する大部分のセキュリティ システムは、チャレンジ/レスポンスに基づいています。スマート カードに入力するコード（チャレンジ）がユーザに与えられます。次に、スマート カードによって、ユーザがログインするために提示できる新しいコード（レスポンス）が示されます。
中断	システムのサービスおよび機能の正常な動作に割り込んだり、動作を妨害したりする状況またはイベント。
積み上げ棒	長期にわたるパラメータの分布を表す水平の色セグメントで構成される、Cisco ISE ダッシュボード上のウィジェットのタイプ。
ディクショナリ	RADIUS プロトコル、内部ユーザ、および内部ホストの属性を設定するストア。

ディクショナリ攻撃	ディクショナリ内のフレーズまたはワードのすべてを試して、パスワードまたはキーを解読しようとする攻撃。可能なすべての組み合わせを試す総当たり攻撃に対して、ディクショナリ攻撃では定義済みのワードリストが使用されます。
データグラム	Request for Comment 1594 には、「発信元と宛先のコンピュータと転送ネットワーク間の以前の交換に依存することなく、発信元から宛先のコンピュータに十分な情報を送信する、完全独立した自己充足型のデータ エンティティである」と記述されています。この用語は、一般に「パケット」という用語に置き換えられています。データグラムまたはパケットはメッセージの単位であり、IP によって処理され、インターネットで転送されます。たとえば電話での音声会話のように、2つの通信点の間に固定期間の接続がないため、データグラムまたはパケットは以前の交換に依存することなく完全独立している必要があります。(このようなプロトコルをコネクションレス型と呼びます)。
デーモン	多くの場合、システム ブート時に開始され、システム上でユーザ介入なしで実行し続けるプログラム。デーモンプログラムは、必要に応じて要求を他のプログラム (またはプロセス) に転送します。デーモンは、他の多くのオペレーティング システムによりサポートされていますが、UNIX 用語とは別の名前と呼ばれている場合もあります。たとえば、Windows では、デーモンがシステム エージェントおよびサービスと呼ばれます。
デジタル証明書	Web 上でビジネスまたは他のトランザクションを実行するときに、ユーザのクレデンシャルを証明する電子的な「クレジットカード」。これは、認証局によって発行されます。デジタル証明書には、ユーザ名、シリアル番号、有効期限、証明書保持者の公開キーのコピー (メッセージおよびデジタル署名の暗号化に使用される)、および認証発行局のデジタル署名が格納され、これにより受信者はその証明書が本物であることを確認できます。
デジタル署名	メッセージの送信者を一意に識別し、送信されてからメッセージが変更されていないことを証明するメッセージのハッシュ。
デジタル封筒	暗号化されたセッション キーを使用する暗号化メッセージ。
デバイス管理	ネットワーク デバイス上で実行される管理操作を制御および監査する機能。ネットワーク デバイス管理者ロールには、ネットワーク デバイス上で管理操作を実行するための完全なアクセス権があります。
等式 (LDAP)	ワイルドカードを含まない検索フィルタで使用すると、等式により属性の比較ルールが定義されます。このとき、コンテンツと長さの両方が正確に一致している必要があります。ワイルドカードが使用された場合、これはサブ文字列と呼ばれ、SUBSTR ルールが使用されます。
匿名 (LDAP)	LDAP セッションは、セッションの開始 (バインドの送信) 時にユーザ識別名または秘密が指定されなかった場合、匿名となります。
ドメイン	名前で識別される認識の範囲、または一部のプログラム エンティティや多数のネットワーク ポイントまたはアドレスに関する事実の集合。インターネットでは、ドメインはネットワーク アドレスのセットで構成されます。インターネットのドメイン ネーム システム (DNS) では、ドメインは、サブドメインまたはホストを示すネーム サーバ レコードと関連付けられた名前です。Windows NT および Windows 2000 では、ドメインはユーザ グループ用のネットワーク リソース (アプリケーション、プリンタなど) のセットです。ユーザがネットワーク内のさまざまなサーバに格納されているリソースにアクセスするために必要なことは、ドメインにログインすることだけです。
ドメイン名	インターネット上の組織または他のエンティティの位置を示します。たとえば、ドメイン名「www.abc.org」は、「abc.org」のインターネット アドレスをインターネット ポイント 199.0.0.2 に位置付け、さらに「www」という名前特定のホスト サーバを示します。ドメイン名の「org」の部分は、組織またはエンティティの目的を示し (この例では「組織」、トップレベル ドメイン名と呼ばれます。ドメイン名の「sans」の部分は組織またはエンティティを定義し、トップレベル名という呼び方に合わせて、セカンドレベル ドメイン名と呼ばれます。

な

内部 ID ソース	内部ユーザおよびエンドポイントの認証に使用される、内部ユーザの属性およびクレデンシャル情報を格納するデータベース。
内部ユーザ	内部 ID ソースで定義されたユーザ。
名前空間 (LDAP)	特定のディレクトリ インフォメーション ツリー (DIT) にある (または DIT 内に含まれているか、DIT によってバインドされている) すべての DN を示す用語。DIT ルートが <code>dc=example,dc=com</code> の場合、 <code>cn=people,dc=example,dc=com</code> は名前空間にあると言えますが、 <code>ou=people,dc=example,dc=com</code> は名前空間にあるとは言えません。これは <code>dc=example,dc=com</code> 名前空間にあることとなります。
入力	入力は、データ パケットが宛先へのパス上で最初にセキュリティ グループ アクセス (SGA) 対応デバイスに遭遇するポイントであり、ここでパケットにセキュリティ グループ タグ (SGT) が付けられます。
認証	主張されている ID の正確さを確認するプロセス。
認証済み (LDAP)	セッションの開始 (バインドの送信) 時にユーザ識別名および秘密が指定された場合、セッションは認証済みとなります。
ネーミング コンテキスト (LDAP)	ルートの識別名 (DN) から始まり、これを含む一意の名前空間。namingContext またはディレクトリ インフォメーション ツリー (DIT) とも呼ばれます。
ネーミング属性 (LDAP)	ディレクトリ インフォメーション ツリー (DIT) 内のエントリごとの一意の識別子。相対識別名 (RDN) とも呼ばれます。
ネットワーク デバイス グループ	ネットワーク デバイス グループ (NDG) は、場所およびタイプ別のネットワーク デバイスの論理グループです。
ネットワーク リソース	ネットワーク デバイス グループ (NDG)、ネットワーク デバイス、AAA クライアント、外部ポリシー サーバなど、Cisco ISE ネットワークにアクセスするデバイス リポジトリ内のすべてのネットワーク デバイスを定義する場所です。

は

ハイブリッド暗号化	2 つ以上の暗号化アルゴリズムを組み合わせた暗号法の適用。特に対称と非対称の暗号化の組み合わせです。
ハイブリッド攻撃	数字および記号をディクショナリ ワードに追加することによって、ディクショナリ 攻撃方式を強化します。
バインド (LDAP)	LDAP サーバに接続するときに実行される順序の最初の操作をバインドと呼びます。バインド操作により、認証に使用されるエントリの識別名および使用されるパスワードが送信されます。匿名バインドの場合、両方とも値は NULL です。
ハッシュ関数	大きなテキストの一方方向の「チェックサム」を生成するために使用されます。このチェックサムは逆向きには使用できません。このハッシュ関数の結果を使用すると、大きなファイルが変更されたかどうかを、そのファイルを相互に比較せずに確認できます。よく使用されるハッシュ関数は MD5 および SHA1 です。

ハブ	1つのポートで受信したデータを他のすべてのポートに繰り返すことで機能するネットワーク デバイス。これにより、1つのホストで送信されたデータが、ハブ上の他のすべてのホストに再送信されます。有線、無線に関係なく、スター型ネットワークの中心デバイスになります。無線アクセス ポイントは無線ネットワークのハブとして動作します。
非カプセル化	特定のレイヤのヘッダーを取り去って、パケットの残りをプロトコル スタック上の次の上位層に渡すプロセス。
非対称キー交換	非対称キーまたは公開キーの暗号法は、キー ペア の概念に基づいています。それぞれのペアの半分 (片方のキー) だけで情報を復号化できるように、残りの半分 (もう片方のキー) で情報を暗号化できます。キー ペア の片方である秘密キーを知っているのは指定されたオーナーだけであり、もう片方の公開キーは広く公開されますが、オーナーと関連付けられています。
ファイアウォール	TCP/IP フラグメンテーション攻撃。この攻撃は、さまざまなメディア間でより効率的に転送できるように IP でパケットがフラグメントに分解されるため、発生します。TCP パケット (およびそのヘッダー) は IP パケットで伝送されます。この攻撃では、2 つめのフラグメントに不正なオフセットが格納されます。パケットを再構築したときに、ポート番号が上書きされます。
フィルタ	どのパケットを使用して、どのパケットを使用しないかを指定するために使用されます。スニファで使用すると、どのパケットを表示するかを決定できます。また、ファイアウォールでは、どのパケットをブロックするかを決定できます。
フィルタリング ルータ	セキュリティ ポリシーに応じて、データ パケットの通過を選択的に妨げるインターネットワーク ルータ。フィルタリング ルータは、ファイアウォールまたはファイアウォールの一部として使用できます。ルータは、通常、ネットワークからパケットを受信して、2 つめのネットワーク上のいずれの場所に転送するかを決定します。フィルタリング ルータは同じことを行いますが、最初に何らかのセキュリティ ポリシーに従って、そもそもパケットを転送する必要があるかどうかを判断します。ポリシーは、ルータにロードされているルール (パケット フィルタ) によって実装されます。
復号化	暗号化されたメッセージを元のプレーンテキストに変換するプロセス。
ブラウザ	ワールドワイド ウェブ上のサーバから情報を取得して表示できるクライアント コンピュータ プログラム。
フラグメンテーション	データ ファイルを、ストレージ メディアの 1 つの場所に連続した単一のビット順序で格納するのではなく、複数の「塊」、つまりフラグメントで格納するプロセス。
ブリッジ	LAN を、同じプロトコルを使用する別の LAN に接続する製品 (イーサネットやトークン リングなど)。
フレーム	アドレス指定および必要なプロトコル制御情報を備えたユニットとして、ネットワーク ポイント間で送信されるデータ。フレームは、通常、シリアル ビット単位で送信され、データを「囲む」ヘッダー フィールドおよびトレーラ フィールドが含まれます。(一部の制御フレームにはデータは含まれません)。
ブロードキャスト	同じメッセージを複数の受信者に同時に送信すること。1 つのホストからネットワーク上のすべてのホストへの送信です。
ブロードキャスト アドレス	UDP または ICMP プロトコルを使用して、特定のネットワーク上のすべてのホストにデータグラムをブロードキャストするために使用されるアドレス。
プロキシ	HTTP プロキシは、HTTP クライアントとサーバ間における通信の仲介として動作するサーバです。
ブロック暗号	一度に 1 つのデータ ブロックを暗号化します。

プロトコル	電気通信接続のエンドポイントで通信時に使用する特別なルールセット。プロトコルは、電気通信接続のさまざまなレベルに存在します。たとえば、ハードウェア デバイス レベルのデータ交換プロトコルや、アプリケーション プログラム レベルのデータ交換プロトコルがあります。開放型システム間相互接続 (OSI) として知られている標準モデルでは、電気通信交換の各レイヤに、交換の両端で認識および順守する必要があるプロトコルが 1 つまたは複数あります。多くの場合、プロトコルは業界標準または国際標準で記述されています。
プロファイリング	エンドポイントなどの ID を一連の条件に基づいて分類するために照合できます。
分解	バイナリ プログラムを取得して、そこからソース コードを抽出するプロセス。
ヘッダー	プロトコル スタックでパケットを処理するために必要なパケット内の追加情報。
傍受	ファシリティまたはネットワークへのアクセスを可能にする情報がもれるおそれのあるプライベートな会話を聞くこと。
ポート設定	さまざまな IP アドレスまたはポート設定で 2 つ以上の LDAP インスタンスを作成することにより、異なる LDAP サーバまたは同じ LDAP サーバ上の異なるデータベースを使用して認証するように Cisco ISE を設定できます。
ポスチャ	保護されたネットワーク リソースにアクセスするホストの準拠性を確認します。
ホスト	インターネット上の他のコンピュータに対して完全双方向アクセスが可能なコンピュータ。または、Web サーバで 1 つ以上の Web サイトにページを提供しているコンピュータです。
ホストベース ID	ホストベースの侵入検知システムは、オペレーティング システムの監査レコードから得られる情報を使用して、侵入検知ソフトウェアがインストールされているホストで発生するすべての動作を監視します。これらの動作は、あらかじめ定義されているセキュリティ ポリシーと比較されます。侵入検知システムによって必ず使用される処理能力の増加のために、この監査証跡の分析は潜在的に大きなオーバーヘッド要件をシステムに課します。監査証跡のサイズおよびシステムの処理能力によっては、監査データを確認することによってリアルタイム分析機能が失われる可能性があります。
ポリシー サービス ペルソナ	ポリシー サービスは、要求を評価および処理する Cisco ISE 上で実行される実行時サービスです。
ポリシー条件	ポリシーに基づくルール ベースの共通条件。アクセス要求を評価して決定を返すために使用されるルールのセットです。
ポリシー要素	ポリシー条件 (たとえば、時刻や日付、またはユーザ選択属性に基づくカスタム条件) および権限 (許可プロファイルなど) を定義するグローバルな共有オブジェクト。ポリシー要素は、ポリシー ルールの作成時に参照されます。
本人拒否	認証システムが、有効なユーザの認識に失敗する場合。

ま

メトリック メーター	ネットワーク アクティビティを示す、一目で確認できるデータ ビューを提供するウィジェットのタイプ。スパークラインおよび積み上げ棒により、指定された期間 (60 分や 24 時間など) で発生したインスタンスの数が示されます。
モニタリングとレポート	ネットワークおよびそのデバイスの状態と健全性をモニタリングし、さまざまなタイプのレポートを生成できる、Cisco ISE の機能。

や

- ユーザ属性設定** 内部ユーザの ID 属性設定からなる管理タスク。
- ユーザ ロール** ユーザ ロールは、ユーザが Cisco ISE ネットワーク上で実行できるタスクを決定する権限セットです。関連する権限があるため、ユーザ ロールにより ISE ユーザ インターフェイスに表示される内容が決まります。

ら

- リモート認証ダイヤルイン ユーザ サービス (RADIUS)** RADIUS は、リモート アクセス サーバが中央サーバと通信してダイヤルイン ユーザを認証し、要求されたシステムまたはサービスへのアクセスを許可できるようにする、クライアント / サーバ プロトコルおよびソフトウェアです。RADIUS を使用すると、企業は、すべてのリモート サーバが共有できる中央データベースでユーザ プロファイルを管理できます。また、管理された単一のネットワーク ポイントで適用可能なポリシーを設定できるため、より優れたセキュリティが得られます。中央サービスがあるため、より簡単に課金状況を追跡したり、ネットワーク統計情報を保持したりすることもできます。
- ルート (LDAP)** ルート エントリ (別名、ベース、サフィックス) は DIT の一番上のエントリを示す多数の用語の 1 つです。ルート DSE は一種のスーパー ルートです。
- ルート DSE (LDAP)** 概念的に LDAP 階層の一番上のエントリ。スーパー ルートとして見なされ、通常、非表示です (たとえば、通常の操作ではアクセスできません)。ルート、ベース、またはサフィックスと混同されることがあります。DSE は DSA Specific Entry の略で、DSA は Directory System Agent (DAP または LDAP アクセスを提供するディレクトリ対応サービス) の略です。ルート DSE に関する情報は、OpenLDAP で OpenLDAPProoDSE クラスオブジェクトを問い合わせることにより取得できます。この情報により、サポート対象のプロトコルバージョン、サポート対象のサービス、およびサポート対象のネーミング コンテキストまたは DIT に関する情報が得られます。
- 例外アクション** 条件のセットが一致しない場合にトリガーされる単一の設定可能アクション。
- レイヤ 2 トンネリング プロトコル (L2TP)** インターネット上でバーチャル プライベート ネットワークを操作できるようにするために、インターネット サービス プロバイダーによって使用されるポイントツーポイント トンネリング プロトコルの拡張。
- レイヤ 2 フォワーディング プロトコル (L2F)** IP を介した PPP のトンネリングを使用して、ダイヤルアップ サーバで開始され、ダイヤルアップ ユーザに対して透過的なダイヤルアップ リンクの仮想拡張をネットワーク上に作成するインターネット プロトコル (シスコが開発)。
- ローカル操作 (セカンダリ サーバ専用)** セカンダリ サーバを登録または登録解除したり、[分散システムに参加 (Join a Distributed System)] ページからセカンダリ サーバおよびローカル モード要求を複製したりするために実行する操作。
- ロール (Role)** それぞれに関連付けられた権限セットを持つ一般的な管理タスクのセット。管理者は複数の定義済みロールを持つことができ、また 1 つのロールは複数の管理者に適用できます。
- ログ設定** ログイング カテゴリとメンテナンス パラメータを使用して、アカウントिंग メッセージ、AAA 監査および診断メッセージ、システム診断メッセージ、管理監査メッセージについて生成されるログを設定および格納できるようにするシステム。
- 露出** 機密データを直接不正なエンティティに公開する危険な処理。

わ

割り込み

何かが発生したことを OS に通知する信号。