GLOSSARY

数字 | A | B | C | D | E | F | G | H | I | J | L | M | N | O | P | R | S | T | U | V | W | X
あ | い | お | か | き | く | こ | さ | し | す | せ | た | て | と | な | に | ね | の | は | ひ | ふ | へ | ほ | ま | め | も | ゆ | り | る | れ |

数字

3DES 「DES」を参照してください。

A

AAA Authentication, Authorization, and Accounting（認証、許可、アカウンティング）。「TACACS+」および「RADIUS」も参照してください。

ABR Area Border Router（エリア境界ルータ）。OSPF における、複数エリアへのインターフェイスを備えたルータです。

ACE Access Control Entry（アクセス コントロール エントリ）。コンフィギュレーションに入力される情報です。この情報を使用して、インターフェイス上で許可または拒否するトラフィックのタイプを指定することができます。デフォルトでは、明示的に許可されていないトラフィックは拒否されます。

ACL Access Control List（アクセス コントロール リスト）。ACE の集合。ACL を使用して、インターフェイス上で許可するトラフィックのタイプを指定することができます。デフォルトでは、明示的に許可されていないトラフィックは拒否されます。ACL は、通常、着信トラフィックの送信元であるインターフェイスに対して適用されます。「ルール」および「発信 ACL」も参照してください。

ActiveX モバイルまたはポータブル プログラムの作成に使用される、オブジェクト指向プログラミング テクノロジーとツールのセット。ActiveX プログラムは Java アプレットとほぼ同等のものです。

AES Advanced Encryption Standard（高度暗号規格）。情報を暗号化および復号化できる対称ブロック サイファです。AES アルゴリズムでは、128、192、および 256 ビットの暗号キーを使用して、データを 128 ビットのブロックで暗号化および復号化できます。「DES」も参照してください。

AH Authentication Header（認証ヘッダー）。データの整合性、認証、およびリプレイ検出を保証する IP プロトコル（タイプ 51）です。AH は、保護対象のデータ（完全 IP データグラムなど）に埋め込まれます。AH は、単体でも ESP と組み合わせても使用できます。AH は旧式の IPsec プロトコルで、ほとんどのネットワークでは ESP ほど重要ではありません。AH は認証サービスを提供しますが、暗号化サービスは提供しません。AH は、認証と暗号化の両方を提供する ESP をサポートしない IPsec ピアとの互換性を保証するために用意されています。「暗号化」および「VPN」も参照してください。RFC 2402 を参照してください。

ARP アドレス解決プロトコル。ハードウェア アドレスまたは MAC アドレスを IP アドレスにマッピングする低レベルの TCP/IP プロトコルです。ハードウェア アドレスの例として、00:00:a6:00:01:ba があります。最初の 3 つの文字グループ（00:00:a6）は製造元を示し、残りの文字（00:01:ba）はシステム カードを示します。ARP は RFC 826 で定義されています。

ASA Adaptive Security Algorithm（アダプティブ セキュリティ アルゴリズム）。ASA 1000V でインスペクションの実行に使用されます。ASA では、内部システムおよびアプリケーションそれぞれに対して明示的に設定を行わなくても、単方向（内部から外部へ）の接続が可能です。「インスペクション エンジン」も参照してください。

ASA ASA 1000V。

ASDM Adaptive Security Device Manager。単一の ASA 1000V を管理および設定するためのアプリケーションです。

auto-signon このコマンドを使用すると、クライアントレス SSL VPN ユーザはシングル サインオン方式を使用できます。NTLM 認証、基本認証、またはその両方を使用する認証のために、SSL VPN ログイン クレデンシャル（ユーザ名とパスワード）を内部サーバに渡します。

A レコード アドレス 「A」はアドレスを表します。DNS で名前からアドレスにマッピングされたレコードを指します。

B

BGP Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。BGP は、TCP/IP ネットワーク内のドメイン間ルーティングを実行します。BGP はエクステリア ゲートウェイ プロトコルです。つまり、複数の自律システムまたはドメイン間のルーティングを実行し、他の BGP システムとルーティング情報やアクセス情報を交換します。ASA 1000V は BGP をサポートしません。「EGP」も参照してください。

BLT ストリーム Bandwidth Limited Traffic ストリーム。帯域幅が制限されたストリームまたはパケット フローです。

BOOTP Bootstrap Protocol（ブートストラップ プロトコル）。ディスクレス ワークステーションがネットワークを介してブートできるプロトコルで、RFC 951 および RFC 1542 で定義されています。

BPDU Bridge Protocol Data Unit（ブリッジ プロトコル データ ユニット）。ネットワーク内のブリッジ間で情報を交換するために設定可能な間隔で送出される、スパニングツリー プロトコルの hello パケット。プロトコル データ ユニットは、パケットに相当する OSI 用語です。

C

CA Certificate Authority、Certification Authority（認証局）。証明書の発行と無効化に責任を負う第三者機関です。CA の公開キーを持つ各デバイスは、その CA によって発行された証明書を持つデバイスを認証できます。CA という用語が CA サービスを提供するソフトウェアを指す場合もあります。「証明書」、「CRL」、「公開キー」、「RA」も参照してください。

CBC Cipher Block Chaining（暗号ブロック連鎖）。アルゴリズムの暗号化強度を高める暗号技術です。CBC には、暗号化を開始するための Initialization Vector（IV; 初期ベクトル）が必要です。IV は、IPsec パケットで明示的に与えられます。

CHAP Challenge Handshake Authentication Protocol（チャレンジ ハンドシェイク認証プロトコル）。

CIFS Common Internet File System（共通インターネット ファイル システム）。プラットフォームに依存しないファイル共有システムで、ファイル、プリンタ、およびその他のマシン リソースへのネットワークを介してアクセスする機能をユーザに提供します。Microsoft 社は、Windows コンピュータのネットワーク用に CIFS を実装しています。一方、CIFS のオープン ソース実装では、Linux、UNIX、Mac OS X など他のオペレーティング システムを実行するサーバへのファイル アクセスを提供しています。

Citrix クライアント / サーバ アプリケーションの仮想化と Web アプリケーションの最適化を行うアプリケーション。

CLI コマンドライン インターフェイス。ASA 1000V に対するコンフィギュレーション コマンドやモニタリング コマンドを入力するための主要インターフェイス。

Cookie ブラウザによって保存されるオブジェクト。クッキーは、ユーザ プリファレンスなどの情報を永続的なストレージに格納したものです。

CPU Central Processing Unit（中央演算処理装置）。メイン プロセッサです。

CRC Cyclical Redundancy Check（巡回冗長検査）。エラーチェック手法。この手法では、フレームの受信側がフレームの内容に生成多項式の除算を適用して剰余を計算し、それを送信側ノードがフレームに保存した値と比較します。

CRL Certificate Revocation List（証明書失効リスト）。特定の CA が発行する、最新の無効化されたすべての証明書をリストしたデジタル署名メッセージです。CRL は、店舗が盗難に遭ったカード番号の帳簿を使用して、悪用されたクレジット カードを拒否する仕組みに似ています。証明書は、無効にされると CRL に追加されます。証明書を使用する認証を実装する場合、CRL を使用するかどうかを選択できます。CRL を使用すると、証明書が期限満了になる前に簡単に無効にできますが、一般に CRL は、CA または RA だけが管理します。CRL を使用している場合は、認証要求時に CA または RA への接続が使用できないと、認証要求が失敗します。「CA」、「証明書」、「公開キー」、「RA」も参照してください。

CRV Call Reference Value。H.225.0 によって、2 つのエンティティ間でシグナリングされるコール レッグの区別に使用されます。

CTIQBE Computer Telephony Interface Quick Buffer Encoding。Cisco CallManager と CTI の TAPI および JTAPI アプリケーションの間の IP テレフォニーで使用されるプロトコルです。CTIQBE は、TAPI/JTAPI プロトコルのインスペクション モジュールで使用され、NAT、PAT、および双方向の NAT をサポートします。このプロトコルにより、Cisco IP SoftPhone や他の Cisco TAPI/JTAPI アプリケーションは、ASA 1000V を越えて Cisco CallManager とコール セットアップおよび音声トラフィックの通信を行うことができます。

D

DES Data Encryption Standard（データ暗号規格）。DES は 1977 年に National Bureau of Standards（米国商務省標準局）から発表された秘密キー暗号化スキームで、IBM の Lucifer アルゴリズムをベースにしています。シスコは、従来の暗号化（40 ビットおよび 56 ビットのキー）、IPsec 暗号化（56 ビット キー）、および、56 ビット キーを使用して 3 倍の暗号化を実行する 3DES（トリプル DES）で DES を使用しています。3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。「AES」および「ESP」も参照してください。

DHCP Dynamic Host Configuration Protocol（ダイナミック ホスト コンフィギュレーション プロトコル）。ホストに IP アドレスをダイナミックに割り当て、ホストが必要としなくなったアドレスを再利用できるようにして、ラップトップなどのモバイル コンピュータが接続先の LAN に対して適切な IP アドレスを取得できるようにするメカニズムを提供します。

Diffie-Hellman セキュアでない通信チャネル上で 2 者が共有秘密を確立できるようにする公開キー暗号化プロトコル。Diffie-Hellman は IKE 内部で使用され、セッション キーを確立します。Diffie-Hellman は、Oakley キー交換のコンポーネントです。

Diffie-Hellman グループ 1、グループ 2、グループ 5、グループ 7

Diffie-Hellman は、フェーズ 1 とフェーズ 2 の両方の SA を確立するための、大きな素数に基づく非対称暗号化を使用した公開キー暗号化の一種です。グループ 1 はグループ 2 よりも小さな素数を提供しますが、一部の IPsec ピアではこのバージョンのみがサポートされている場合があります。Diffie-Hellman グループ 5 は 1536 ビットの素数を使用し、最もセキュアであるため、AES で使用することが推奨されています。163 ビットの楕円曲線フィールド サイズを持つグループ 7 は、Movian VPN クライアントで使用するためのものですが、グループ 7（ECC）をサポートする任意のピアで動作します。「VPN」および「暗号化」も参照してください。

（注） **グループ 7** コマンド オプションは ASA バージョン 8.0(4) で非推奨になりました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。

DMZ

「インターフェイス」を参照してください。

DN

Distinguished Name（認定者名）。OSI ディレクトリ（X.500）内のグローバルな正規のエントリ名です。

DNS

Domain Name System（ドメイン ネーム システム）または Domain Name Service（ドメイン ネーム サービス）。ドメイン名を IP アドレスに変換するインターネット サービスです。

DoS

Denial of Service（サービス拒絶）。ネットワーク攻撃の一種です。ネットワーク サービスを使用できないようにすることを目的とします。

DSL

Digital Subscriber Line（デジタル加入者線）。従来の銅線ケーブル配線を介して限られた距離で高い帯域幅を提供するパブリック ネットワーク テクノロジーです。DSL のサービスは、中央オフィスとカスタマー サイトに 1 つずつ配置されたモデムのペアを介して提供されます。ほとんどの DSL テクノロジーではツイストペアの帯域幅全体を使用することはないため、音声チャネル用の部分は残されています。

DSP

Digital Signal Processor（デジタル信号プロセッサ）。DSP は音声信号をフレームに分割し、ボイス パケットに格納します。

DSS

Digital Signature Standard（デジタル署名規格）。US National Institute of Standards and Technology（国立標準技術研究所）によって設計された、公開キー暗号化に基づくデジタル署名アルゴリズムです。DSS はユーザ データグラムの暗号化は実行しません。DSS は従来の暗号化や Redcreek IPsec カードのコンポーネントですが、Cisco IOS ソフトウェアで実装されている IPsec には含まれていません。

E

echo

「ping」および「ICMP」を参照してください。「インスペクション エンジン」も参照してください。

EGP

Exterior Gateway Protocol（エクステリア ゲートウェイ プロトコル）。BGP に置き換えられました。ASA 1000V は EGP をサポートしません。「BGP」も参照してください。

EIGRP

Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）。ASA 1000V は EIGRP をサポートしません。

EMBLEM

Enterprise Management BaseLine Embedded Manageability。Cisco IOS システムのログ形式との一貫性を持たせるために設計された syslog 形式。CiscoWorks の管理アプリケーションとの互換性が高められています。

ESMTP

拡張 SMTP。SMTP の拡張バージョン。送達通知やセッション配信などの追加機能が含まれます。ESMTP は、RFC 1869「SMTP Service Extensions」で定義されています。

ESP Encapsulating Security Payload。IPsec プロトコルの 1 つです。ESP は、セキュアでないネットワーク上でセキュアなトンネルを確立するための認証および暗号化サービスを提供します。詳細については、RFC 2406 および 1827 を参照してください。

F

FQDN/IP Fully Qualified Domain Name（完全修飾ドメイン名）/IP アドレス。セキュリティ ゲートウェイとなるピアを指定する IPsec パラメータです。

FragGuard IP フラグメント保護を可能にし、すべての ICMP エラー メッセージの完全リアセンブリ、および ASA 1000V を介してルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。

FTP File Transfer Protocol（ファイル転送プロトコル）。ホスト間のファイル転送に使用される TCP/IP プロトコル スタックの一部です。

G

GMT Greenwich Mean Time（グリニッジ標準時）。1967 年に、Coordinated Universal Time（UTC; 協定世界時）に置き換えられました。

GRE Generic Routing Encapsulation（総称ルーティング カプセル化）。RFC 1701 および 1702 で定義されています。GRE は、広範なタイプのプロトコル パケットをトンネル内でカプセル化できるトンネリング プロトコルであり、リモート ポイントのルータに対して IP ネットワークを介した仮想のポイントツーポイント リンクを作成します。複数のマルチプロトコル サブネットワークを 1 つの単一プロトコル バックボーン環境で接続することにより、GRE を使用する IP トンネリングでは、単一プロトコルのバックボーン環境を越えたネットワークの拡張が可能になります。

GSM Global System for Mobile Communication。モバイル無線音声通信用に開発された、デジタル モバイル無線の規格。

H

H.225 テレビ会議などのアプリケーションで TCP シグナリングに使用されるプロトコル。「H.323」および「インスペクション エンジン」も参照してください。

H.225.0 H.225.0 セッションの確立とパケット化を規定する ITU 標準。H.225.0 では、実際には、RAS、Q.931 の使用、RTP の使用など、いくつかの異なるプロトコルが定められています。

H.245 H.245 エンドポイントの制御を規定する ITU 標準。

H.320 ISDN、フラクショナル T1、スイッチド 56 回線などの回線交換メディアを使用したテレビ会議について定めた一連の ITU-T 標準仕様。ITU-T 標準 H.320 の拡張機能により、LAN やその他のパケット交換ネットワークを使用したテレビ会議、およびインターネットを使用したテレビ会議が可能になります。

H.323 異種の通信デバイスが、標準化された通信プロトコルを使用して、相互に通信できます。H.323 は、CODEC の共通セット、コール セットアップとネゴシエーションの手順、および基本的なデータ転送方法を定義しています。

H.323 RAS Registration, Admission, and Status シグナリング プロトコル。デバイスが、登録、許可、帯域幅の変更、および VoIP ゲートウェイとゲートキーパー間のステータスと接続解除手順を実行できるようにします。

H.450.2 H.323 のコール転送補足サービス。

H.450.3 H.323 のコール宛先変更補足サービス。

HMAC SHA-1 や MD5 などの暗号化ハッシュを使用するメッセージ認証メカニズム。

HTTP ハイパーテキスト転送プロトコル。ファイルを転送するためにブラウザや Web サーバで使用されるプロトコルです。ユーザが Web ページを表示する場合、ブラウザは HTTP を使用してその Web ページで使用されるファイルを要求し、受信することができます。HTTP による伝送は暗号化されません。

HTTPS Hypertext Transfer Protocol Secure。SSL 暗号化バージョンの HTTP です。

I

IANA Internet Assigned Number Authority（インターネット割り当て番号局）。インターネットで使用されるすべてのポート番号とプロトコル番号を割り当てます。

ICMP Internet Control Message Protocol（インターネット制御メッセージ プロトコル）。ネットワーク レイヤのインターネット プロトコルであり、エラーを報告し、IP パケット処理に関するその他の情報を提供します。

IDS Intrusion Detection System（侵入検知システム）。署名によって悪意のあるネットワーク アクティビティを検出し、その署名に対してポリシーを実装する手段です。

IETF Internet Engineering Task Force（インターネット技術特別調査委員会）。インターネット用のプロトコルを定義する RFC 文書を作成する技術標準団体です。

IGMP Internet Group Management Protocol（インターネット グループ管理プロトコル）。IGMP は、IP マルチキャスト メンバーシップを隣接するマルチキャスト ルータに報告するために IPv4 システムで使用されるプロトコルです。

IKE Internet Key Exchange（インターネット キー エクスチェンジ）。IKE は共有セキュリティ ポリシーを確立し、キーを要求するサービス（IPsec など）に対してキーを認証します。IPsec トラフィックが通過する前に、各 ASA 1000V はピアの ID を確認する必要があります。確認は、両方のホストに手動で事前共有キーを入力するか、CA サービスを使用して実行します。IKE は、Oakley を部分的に使用し、また、ISAKMP フレームワーク内で SKEME と呼ばれるプロトコル スイートも部分的に使用する、ハイブリッド プロトコルです。IKE（旧称：ISAKMP/Oakley）は RFC 2409 で定義されています。

IKE Mode Configuration IKE Mode Configuration は、IETF draft-ietf-ipsec-isakmp-mode-cfg-04.txt に従って実装されます。IKE Mode Configuration は、IKE ネゴシエーションの一部として VPN クライアントに IP アドレス（およびその他のネットワーク レベル コンフィギュレーション）をダウンロードする手段をセキュリティ ゲートウェイに提供します。

IKE 拡張認証 IKE 拡張認証（Xauth）は、IETF draft-ietf-ipsec-isakmp-xauth-04.txt（拡張認証）に従って実装されます。このプロトコルは、TACACS+ または RADIUS を使用して IKE 内のユーザを認証する機能を提供します。

ILS Internet Locator Service。ILS は LDAP をベースとし、ILSv2 に準拠しています。ILS は、NetMeeting、SiteServer、および Active Directory の各製品と使用するために、Microsoft 社によって独自に開発されました。

IMAP Internet Message Access Protocol。共有可能なメール サーバに保持されている電子メールや掲示板のメッセージにアクセスする方式です。IMAP により、クライアントの電子メール アプリケーションは、実際にメッセージを転送することなく、ローカルであるかのようにリモート メッセージ ストアにアクセスすることができます。

IMSI International Mobile Subscriber Identity。GTP トンネル ID の 2 つのコンポーネントの 1 つです。もう 1 つのコンポーネントは NSAPI です。「NSAPI」も参照してください。

IP インターネット プロトコル。IP プロトコルは、相互接続されたネットワークの任意のセット間の通信に使用でき、LAN 通信にも WAN 通信にも同様に適していることから、最も広く使用されている公開プロトコルです。

IPsec IP セキュリティ。参加ピア間でのデータの機密性、整合性、および認証を提供するオープン スタンダードの枠組みです。IPsec では、これらのセキュリティ サービスが IP レイヤで実現されます。IPsec は、IKE を使用してローカル ポリシーに基づいてプロトコルとアルゴリズムのネゴシエーションを処理し、IPsec で使用される暗号キーと認証キーを生成します。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータフローを保護するために使用できます。

IPsec トランスフォーム セット トランスフォーム セットは、IPsec ポリシーに一致するトラフィックに対して使用する、IPsec プロトコル、暗号化アルゴリズム、およびハッシュ アルゴリズムを指定します。1 つのトランスフォームには、1 つのセキュリティ プロトコル（AH または ESP）とそれに対応するアルゴリズムが記述されます。ほぼすべてのトランスフォーム セットで使用される IPsec プロトコルは、認証のために DES アルゴリズムと HMAC-SHA を持つ ESP です。

IPsec フェーズ 1 IPsec をネゴシエートする最初のフェーズ。キー交換、および IPsec の ISAKMP の部分が含まれます。

IPsec フェーズ 2 IPsec をネゴシエートする 2 番目のフェーズ。フェーズ 2 では、ペイロードに使用される暗号化規則のタイプ、暗号化に使用される送信元と宛先、アクセス リストに従って処理対象とするトラフィックの定義、および IPsec ピアが決定されます。IPsec はフェーズ 2 でインターフェイスに適用されます。

IP アドレス IP プロトコル アドレス。ASA 1000V のインターフェイスの ip_address です。IP バージョン 4 のアドレスの長さは、32 ビットです。このアドレス空間は、ネットワーク番号、オプションのサブネットワーク番号、およびホスト番号の指定に使用されます。32 ビットは、4 つのオクテット（8 バイナリ ビット）にグループ化され、ピリオドまたはドットで区切られた 4 つの 10 進数値として表現されます。4 つのオクテットのそれぞれの意味は、そのネットワークでの使用方法によって決定されます。

IP プール ローカル IP アドレスの一定の範囲。名前、および開始 IP アドレスと終了 IP アドレスを持つ範囲によって指定されます。IP プールは、内部インターフェイス上のクライアントにローカル IP アドレスを割り当てるために、DHCP と VPN で使用されます。

ISAKMP Internet Security Association and Key Management Protocol。ペイロード形式、キー交換プロトコル実装の方法、およびセキュリティ アソシエーションのネゴシエーションを定義するプロトコル フレームワークです。「IKE」を参照してください。

ISP Internet Service Provider（インターネット サービス プロバイダー）。電話音声回線を使用したモデム ダイヤルインや DSL などのサービスを介してインターネットへの接続を提供する組織です。

J

JTAPI Java Telephony Application Programming Interface（Java テレフォニー アプリケーション プログラミング インターフェイス）。テレフォニー機能をサポートする Java ベースの API です。「TAPI」も参照してください。

L

L2TP Layer Two Tunneling Protocol（レイヤ 2 トンネリング プロトコル）。PPP のトンネリングを提供する、RFC 2661 で定義された IETF 標準トラック プロトコル。L2TP は PPP の拡張です。L2TP は、PPTP と古い Cisco レイヤ 2 転送（L2F）プロトコルをマージします。L2TP は、IPsec 暗号化が使用でき、PPTP より攻撃に対してセキュアであると考えられます。

LAN Local Area Network（ローカルエリア ネットワーク）。1 つのビルや敷地内など、一定の場所に配置されたネットワーク。「インターネット」、「イントラネット」、「ネットワーク」も参照してください。

LCN Logical Channel Number（論理チャネル番号）。

LDAP Lightweight Directory Access Protocol。LDAP は、管理アプリケーションやブラウザ アプリケーションが X.500 ディレクトリにアクセスできるようにします。

M

MD5 Message Digest 5。128 ビット ハッシュを作成する単方向のハッシュ アルゴリズム。MD5 と SHA-1 は両方とも MD4 のバリエーションであり、MD4 のハッシュ アルゴリズムのセキュリティを強化するように設計されています。SHA-1 は MD4 および MD5 よりもセキュアです。シスコでは、IPsec フレームワーク内の認証にハッシュを使用しています。また、SNMP v.2 のメッセージ認証にも使用します。MD5 は通信の整合性を確認し、発信元を認証して、適時性をチェックします。MD5 は SHA-1 よりもダイジェストが小さく、わずかに速いとされています。

MDI Media Dependent Interface（メディア依存インターフェイス）。

MDIX Media Dependent Interface Crossover（メディア依存インターフェイス クロスオーバー）。

MGCP Media Gateway Control Protocol（メディア ゲートウェイ コントロール プロトコル）。MGCP は、メディア ゲートウェイ コントローラやコール エージェントと呼ばれる外部コール制御要素によって VoIP コールを制御するためのプロトコルです。MGCP は IPDC プロトコルと SGCP プロトコルを統合したものです。

MS-CHAP Microsoft CHAP。

MTU Maximum Transmission Unit（最大伝送単位）。最適な応答時間で効率的にネットワーク上を転送できる 1 パケットあたりの最大バイト数です。イーサネットのデフォルト MTU は 1500 バイトですが、各ネットワークに応じてその値は異なり、シリアル接続では最小のバイト数となります。MTU は RFC 1191 で定義されています。

N

N2H2
ASA 1000V と連携動作してユーザの Web アクセスを制御する、サードパーティ製のポリシー型フィルタリング アプリケーション。N2H2 は、宛先ホスト名、宛先 IP アドレス、およびユーザ名とパスワードに基づいて HTTP 要求をフィルタリングできます。N2H2 社は 2003 年 10 月に Secure Computing 社に買収されました。

NAT
Network Address Translation（ネットワーク アドレス変換）。グローバルに固有な IP アドレスを使用する必要性を減らすメカニズムです。NAT を使用すると、グローバルに固有でないアドレスをグローバルにルーティング可能なアドレス空間に変換することによって、このようなアドレスを持つ組織をインターネットに接続できます。

NEM
Network Extension Mode（ネットワーク拡張モード）。これを使用すると、VPN ハードウェア クライアントは、VPN トンネル経由でリモート プライベート ネットワークに 1 つのルーティング可能なネットワークを提供できるようになります。

NetBIOS
Network Basic Input/Output System。Windows のホスト名登録、セッション管理、およびデータ転送をサポートする Microsoft のプロトコルです。ASA 1000V は、NBNS UDP ポート 137 および NBDS UDP ポート 138 のパケットの NAT 処理を実行することにより、NetBIOS をサポートします。

NMS
Network Management System（ネットワーク管理システム）。ネットワークの少なくとも一部分の管理に責任を負うシステム。NMS は、一般的に適度にパワーのある装備の整ったコンピュータで、エンジニアリング ワークステーションなどです。NMS はエージェントと通信して、ネットワークの統計やリソースを追跡し続けるのに役立ちます。

NSAPI
Network Service Access Point Identifier。GTP トンネル ID の 2 つのコンポーネントの 1 つです。もう 1 つのコンポーネントは IMSI です。「IMSI」も参照してください。

NSSA
Not-So-Stubby Area。RFC 1587 で定義されている OSPF 機能です。NSSA は Cisco IOS ソフトウェア リリース 11.2 で初めて導入されました。既存のスタブ エリア機能をシスコ独自でない方法で拡張した機能であり、限定的な方法でスタブ エリアに外部ルートを注入することができます。

NTLM
NT LAN Manager。Microsoft Windows のチャレンジ / レスポンス認証方式です。

NTP
Network Time Protocol（ネットワーク タイム プロトコル）。

O

Oakley
認証済みキー関連情報の取得方法を定義するキー交換プロトコル。Oakley の基本メカニズムは Diffie-Hellman キー交換アルゴリズムです。Oakley は、RFC 2412 で定義されています。

OSPF
Open Shortest Path First。OSPF は、IP ネットワーク用のルーティング プロトコルです。OSPF は、ネットワーク帯域幅を効率的に使用し、かつトポロジ変更後のコンバージェンスが高速であるため、大規模なネットワークに広く展開されているルーティング プロトコルです。ASA 1000V は OSPF をサポートしません。

OU
Organizational Unit（組織ユニット）。X.500 ディレクトリの属性です。

P

PAC PPTP Access Concentrator（PPTP アクセス コンセントレータ）。PPP 操作と PPTP プロトコル処理の機能を持つ 1 つ以上の PSTN 回線または ISDN 回線に接続されたデバイスです。PAC は、1 つ以上の PNS にトラフィックを渡すために TCP/IP を設定する必要があります。PAC は IP 以外のプロトコルもトンネリングできます。

PAT 「ダイナミック PAT」、「インターフェイス PAT」、「スタティック PAT」を参照してください。

PDP Packet Data Protocol（パケット データ プロトコル）。

Perfmon ASA 1000V の機能。接続数 / 秒や xlate 数 / 秒など、広範な機能統計情報を収集し、報告します。

PFS Perfect Forward Secrecy（完全転送秘密）。PFS は、IPsec のフェーズ 1 とフェーズ 2 の SA で異なるセキュリティ キーを使用することにより、セキュリティを強化します。PFS を使用しない場合は、両方のフェーズで同じセキュリティ キーを使用して SA が確立されます。PFS は、所定の IPsec SA キーが他のシークレット（他のキーなど）から派生していないことを保証します。つまり、PFS では、攻撃者があるキーを突破しても、そこから他のキーを導出することはできないことが保証されます。PFS がイネーブルになっていない場合、IKE SA 秘密キーが解読されれば、IPsec 保護データがすべてコピーされ、IKE SA シークレットの知識を使用して、この IKE SA によって設定された IPsec SA を脆弱化することができると推測されます。PFS を使用すると、攻撃者が IKE を突破しても、直接 IPsec にアクセスすることはできません。その場合、攻撃者は各 IPsec SA を個別に突破する必要があります。

ping ホストが別のホストにアクセス可能かどうかを判別するために送信する ICMP 要求。

PIX Private Internet eXchange。Cisco PIX 500 シリーズの ASA 1000V には、小規模 / ホーム オフィス向けのコンパクトなプラグアンドプレイ デスクトップ モデルから、きわめて要求の厳しい企業やサービス プロバイダーの環境に適したキャリアクラスのギガビット モデルまで、広い範囲の製品があります。Cisco PIX ASA 1000V は、変化の速いネットワーク環境に対応した強固なマルチレイヤ防御機能を構築するための、堅牢な企業クラスの統合ネットワーク セキュリティ サービスを提供します。PIX は、Cisco ASA 5500 シリーズに置き換えられました。

PKCS12 秘密キーや証明書などのデータをはじめとする PKI 関連データの転送規格。この規格をサポートするデバイスを使用すると、管理者は単一セットの個人 ID 情報を維持することができます。

PNS PPTP Network Server（PPTP ネットワーク サーバ）。PNS は、汎用コンピューティング / サーバ プラットフォームで動作するように設計されています。PNS は PPTP のサーバ側の処理を担当します。PPTP は、TCP/IP に完全に依存し、インターフェイス ハードウェアに依存しないため、PNS では LAN デバイスや WAN デバイスなどの IP インターフェイス ハードウェアを任意に組み合わせて使用することができます。

POP Post Office Protocol。クライアント電子メール アプリケーションが、メール サーバからメールを取得するために使用するプロトコル。

PPP Point-to-Point Protocol（ポイントツーポイント プロトコル）。アナログ電話回線とモデムを使用したダイヤルアップの ISP アクセス用に開発されました。

PPTP ポイントツーポイント トンネリング プロトコル。PPTP は、Microsoft 社によって、Windows ネットワークへのセキュアなリモート アクセスを可能にするために導入されました。ただし、攻撃に対して脆弱であるため、一般に PPTP が使用されるのは、より強力なセキュリティ方式が使用できない場合や、それが必要でない場合だけです。PPTP ポートは、pptp、1723/tcp、および 1723/udp です。PPTP の詳細については、RFC 2637 を参照してください。「PAC」、「PPTP GRE」、「PPTP GRE トンネル」、「PNS」、「PPTP セッション」、および「PPTP TCP」も参照してください。

PPTP GRE PPP トラフィックをカプセル化するためのバージョン 1 の GRE。

PPTP GRE トンネル PNS と PAC のペアで定義されるトンネル。このトンネル プロトコルは、GRE の修正バージョンによって定義されています。このトンネルでは、PAC と PNS の間で PPP データグラムが伝送されます。多数のセッションが 1 つのトンネルに多重化されます。TCP 上で動作する制御接続により、セッションおよびトンネル自体の確立、解放、および維持が制御されます。

PPTP TCP PPTP のコール制御情報と管理情報の受け渡しに使用される標準の TCP セッション。制御セッションは、PPTP トンネルでトンネリングされているセッションに論理的に関連付けられていますが、これとは別に存在しています。

PPTP セッション PPTP はコネクション型です。PAC に接続された各ユーザの状態は、PNS と PAC で維持されます。ダイヤル ユーザと PNS の間でエンドツーエンドの PPP 接続が試行されると、セッションが作成されます。セッションに関連するデータグラムは、PAC と PNS の間でトンネル経由で送信されます。

R

RA Registration Authority（登録局）。CA の認可されたプロキシ。RA は証明書登録を実行し、CRL を発行することができます。「CA」、「証明書」、「公開キー」も参照してください。

RADIUS Remote Authentication Dial-In User Service（リモート認証ダイヤルイン ユーザ サービス）。RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント / サーバ システムです。RADIUS プロトコルの規格は、RFC 2058 と RFC 2059 で定義されています。「AAA」および「TACACS+」も参照してください。

RFC Request for Comments（コメント要求）。RFC 文書は、インターネットを使用した通信用のプロトコルや規格を定義します。RFC は IETF によって作成および発行されます。

RIP Routing Information Protocol（ルーティング情報プロトコル）。UNIX BSD システムに付属の Interior Gateway Protocol（IGP）です。インターネットで最も広く使用される IGP です。RIP はルーティング メトリックとしてホップ カウントを使用します。

RLLA Reserved Link Local Address（予約済みリンク ローカル アドレス）。マルチキャスト アドレスは 224.0.0.0 ～ 239.255.255.255 の範囲ですが、ユーザが使用できるのは 224.0.1.0 ～ 239.255.255.255 だけです。マルチキャスト アドレス範囲の最初の 224.0.0.0 ～ 224.0.0.255 の部分は予約済みであり、RLLA と呼ばれます。これらのアドレスは使用できません。

RPC Remote Procedure Call（リモート プロシージャ コール）。RPC は、クライアントで作成または指定されるプロシージャ コールで、サーバで実行され、結果はネットワーク経由でクライアントに返されます。

RSA 可変長キーを使用した公開キー暗号化アルゴリズム（名前は発明者である Rivest、Shamir、Adelman の名前に由来する）。RSA の主な欠点は、DES などの一般的な秘密キー アルゴリズムと比較すると、大幅に計算が遅いことです。シスコの IKE の実装では、秘密キーの取得には Diffie-Hellman 交換が使用されています。この交換は、RSA（または事前共有キー）を使用して認証できます。Diffie-Hellman 交換では、DES キーは（暗号化された形式であっても）ネットワークを越えませんが、RSA の暗号化および署名の手法では越えます。RSA はパブリック ドメインではないため、RSA Data Security からライセンスを取得する必要があります。

RSH リモート シェル。ユーザがリモート システムにログインせずにそのシステムでコマンドを実行できるようにするプロトコル。たとえば、RSH を使用すると、各通信サーバに接続することなく複数のアクセス サーバのステータスを確認し、コマンドを実行して、通信サーバとの接続を切断することができます。

RTP Real-Time Transport Protocol（リアルタイム転送プロトコル）。一般に、IP ネットワークで使用されます。RTP は、音声、ビデオ、シミュレーション データなどのリアルタイム データをマルチキャストまたはユニキャストのネットワーク サービスとして、アプリケーションがリアルタイムにデータを転送できるように、エンドツーエンドのネットワーク転送機能を提供するように設計されています。RTP は、ペイロード タイプの識別、シーケンス番号付け、タイムスタンプ処理、配信のモニタリングなどのサービスをリアルタイム アプリケーションに提供します。

RTSP Real Time Streaming Protocol。音声やビデオなど、リアルタイム データの制御配信を可能にします。RTSP は、RTP や HTTP などの主要プロトコルと連携動作するように設計されています。

S

SA Security Association（セキュリティ アソシエーション）。データ フローに適用されるセキュリティ ポリシーとキー関連情報のインスタンスです。SA は、IPsec の 2 つのフェーズにおいて、IPsec ピアによってペアで確立されます。SA は、セキュアなトンネルの作成に使用される暗号化アルゴリズムとその他のセキュリティ パラメータを指定します。フェーズ 1 の SA（IKE SA）は、フェーズ 2 の SA をネゴシエートするためのセキュアなトンネルを確立します。フェーズ 2 の SA（IPsec SA）は、ユーザ データの送信に使用されるセキュアなトンネルを確立します。IKE と IPsec の両方で SA を使用しますが、これらは互いに独立しています。IPsec SA は単方向であり、各セキュリティ プロトコル内で固有です。保護されたデータ パイプでは 1 組の SA が必要であり、プロトコルごとに 1 方向あたり 1 つずつ必要です。たとえば、ピア間で ESP をサポートしているパイプの場合は、各方向に 1 つの ESP SA が必要です。SA は、宛先（IPsec エンドポイント）アドレス、セキュリティ プロトコル（AH または ESP）、および Security Parameter Index（SPI; セキュリティ パラメータ インデックス）によって固有に識別されます。IKE は IPsec に代わって SA のネゴシエーションと確立を行います。ユーザは手動で IPsec SA を確立することもできます。IKE SA は、IKE のみによって使用され、IPsec SA の場合とは異なり双方向です。

SCCP Skinny Client Control Protocol。Cisco CallManager と Cisco VoIP 電話の間で使用されるシスコの専用プロトコルです。

SDP Session Definition Protocol。マルチメディア サービスを定義するための IETF プロトコルです。SDP メッセージは、SGCP メッセージや MGCP メッセージの一部である場合があります。

SGCP Simple Gateway Control Protocol（簡易ゲートウェイ コントロール プロトコル）。外部コール制御要素（コール エージェントと呼ばれる）によって VoIP ゲートウェイを制御します。

SHA-1 Secure Hash Algorithm 1。SHA-1 [NIS94c] は、1994 年に公開された SHA の修正版です。SHA は MD4 をモデルとした、それにきわめて近い設計であり、160 ビットのダイジェストを生成します。SHA は 160 ビットのダイジェストを生成するので、128 ビットのハッシュ（MD5 など）よりも Brute-Force アタックへの抵抗力が強化されますが、速度は遅くなります。SHA 1 は、National Institute of Standards and Technology（国立標準技術研究所）と National Security Agency（国家安全保障局）によって共同開発されました。このアルゴリズムは、他のハッシュ アルゴリズムと同様に、ハッシュ値（メッセージ ダイジェストとも呼ばれる）を生成するために使用されます。メッセージ ダイジェストは、下位レイヤのプロトコルでメッセージの内容が伝送中に変更されないように保証するために使用される CRC と同様の動作をします。SHA-1 は、一般に MD5 より安全であるとされています。

SIP Session Initiation Protocol（セッション開始プロトコル）。特に 2 者間の音声会議などのコール処理セッションまたは「コール」が使用可能になります。SIP は SDP と連携して、コール シグナリングを行います。SDP はメディア ストリーム用のポートを指定します。SIP の使用により、ASA 1000V は任意の SIP VoIP ゲートウェイと VoIP プロキシ サーバをサポートすることができます。

SKEME 認証済みキー関連情報の導出方法を定義するキー交換プロトコル。キー リフレッシュが迅速です。

SMTP Simple Mail Transfer Protocol（シンプル メール転送プロトコル）。SMTP は、電子メール サービスをサポートするインターネット プロトコルです。

SNMP 簡易ネットワーク管理プロトコル。管理情報ベースと呼ばれるデータ構造を使用してネットワーク デバイスを管理する標準方式。

SQL*Net Structured Query Language（SQL; 構造化照会言語）プロトコル。クライアントとサーバのプロセス間通信に使用される Oracle のプロトコル。

SSH Secure Shell（セキュア シェル）。強力な認証と暗号化機能を提供する、TCP/IP などの信頼性の高いトランスポート レイヤで実行されるアプリケーション。

SSL Secure Socket Layer。アプリケーション レイヤと TCP/IP の間に常駐してデータ トラフィックの透過的な暗号化を提供するプロトコル。

T

TACACS+ Terminal Access Controller Access Control System Plus（ターミナル アクセス コントローラ アクセス コントロール システム プラス）。コマンド認可も含めて AAA サービスをサポートするクライアント / サーバ プロトコルです。「AAA」および「RADIUS」も参照してください。

TAPI Telephony Application Programming Interface（テレフォニー アプリケーション プログラミング インターフェイス）。テレフォニー機能をサポートする Microsoft Windows のプログラミング インターフェイスです。

TCP 伝送制御プロトコル。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 代行受信 TCP 代行受信機能では、オプションの初期接続制限値に到達すると、初期接続カウントがしきい値未満になるまで、影響を受けるサーバに向けられたすべての SYN が代行受信されます。各 SYN に対して、ASA 1000V は、サーバの代わりに空の SYN/ACK セグメントで応答します。ASA 1000V は、該当するステート情報を保持し、パケットをドロップして、クライアントの ACK を待ちます。ACK が受信されると、クライアントの SYN セグメントのコピーがサーバに送信され、ASA 1000V とサーバの間で TCP 3 ウェイ ハンドシェイクが実行されます。この 3 ウェイ ハンドシェイクが完了した場合は、通常どおり接続を再開できます。接続フェーズのいずれかの部分でクライアントが応答しない場合、ASA 1000V は指数バックオフを使用して必要なセグメントを再送信します。

TDP Tag Distribution Protocol（タグ配布プロトコル）。TDP は、タグ スイッチング ネットワーク内の複数のネットワーク レイヤ プロトコルのタグ バインディング情報を配布、要求、および解放するために、タグ スイッチング デバイスによって使用されます。TDP はルーティング プロトコルを置き換えません。代わりに、TDP はルーティング プロトコルから取得した情報を使用してタグ バインディングを作成します。TDP は、TDP セッションをオープン、モニタ、クローズしたり、これらのセッション中に発生したエラーを示したりする目的でも使用されます。TDP は、順次配信が保証されたコネクション型のトランスポート レイヤ プロトコル（TCP など）で動作します。TDP を使用しても、タグ バインディング情報（他のプロトコルに関するピギーバッキング情報など）を配布するその他のメカニズムの使用は妨げられません。

Telnet インターネットなどの TCP/IP ネットワーク用のターミナル エミュレーション プロトコル。Telnet はリモートから Web サーバを制御するための一般的な方法ですが、セキュリティ上の脆弱性により、SSH が使用されるようになってきています。

TFTP Trivial File Transfer Protocol。TFTP は、ファイル転送用のシンプルなプロトコルです。このプロトコルは UDP 上で実行され、RFC 1350 で詳細に説明されています。

TID Tunnel Identifier（トンネル識別子）。

TLS Transport Layer Security。SSL に代わる将来の IETF プロトコルです。

TSP TAPI Service Provider（TAPI サービス プロバイダー）。「TAPI」も参照してください。

U

UDP ユーザ データグラム プロトコル。IP プロトコル スタックにおけるコネクションレス型トランスポート レイヤ プロトコルです。UDP は、確認応答や送達保証を行わずにデータグラムを交換するシンプルなプロトコルであるため、エラー処理や再送信は他のプロトコルによって行う必要があります。UDP は RFC 768 に定義されています。

Unicast RPF Unicast Reverse Path Forwarding（ユニキャスト逆経路転送）。ユニキャスト RPF は、パケットがルーティング テーブルに従った正しい発信元インターフェイスと一致する送信元 IP アドレスを持つように保証することによって、スプーフィングに対するガードを行います。

URL Uniform Resource Locator（ユニフォーム リソース ロケータ）。ハイパーテキスト文書やその他のサービスにブラウザを使用してアクセスするための標準アドレッシング方式です。たとえば、http://www.cisco.com などです。

UTC Coordinated Universal Time（協定世界時）。経度ゼロのタイムゾーンです。このタイムゾーンは、以前はグリニッジ標準時（GMT）およびズールー時と呼ばれていました。UTC は 1967 年に GMT の代わりに協定世界時となりました。UTC は、天文時ではなく、原子時間に基づいています。

UUIE User-User Information Element（ユーザ対ユーザ情報要素）。メッセージ内の関連ユーザを識別する H.225 パケットの要素です。

V

VLAN Virtual LAN（仮想 LAN）。複数の異なる LAN セグメント上に配置されていながら、同一の物理ネットワーク ケーブルに接続されているかのように通信できるように（管理ソフトウェアを使用して）設定された、1 つまたは複数の LAN 上にあるデバイスのグループ。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。

VoIP Voice over IP。VoIP は、電話による通話やファクスなどの通常の音声トラフィックを、IP ベースのネットワーク上で伝送します。DSP が音声信号をフレームにセグメント化し、2 つからなるグループにカップリングしてボイス パケットに格納します。これらのボイス パケットは、ITU-T 仕様 H.323 に準拠する IP を使用して伝送されます。

VPN Virtual Private Network（バーチャル プライベート ネットワーク）。パブリック ネットワークを使用した 2 つのピア間のネットワーク接続を、厳密なユーザ認証とすべてのデータ トラフィックの暗号化によってプライベート化したものです。VPN は、PC などのクライアント間、または ASA 1000V など ヘッドエンドの間で確立することができます。

VSA Vendor-Specific Attribute（ベンダー固有属性）。RADIUS の RFC ではなく、ベンダーによって定義された RADIUS パケットの属性です。RADIUS プロトコルは、IANA によって割り当てられたベンダー番号を VSA の識別に利用します。これにより、異なるベンダーで同じ番号の VSA の使用が可能になります。ベンダー番号と VSA 番号の組み合わせにより、VSA が固有になります。たとえば、ベンダー番号 9 に関連付けられた VSA セットでは、cisco-av-pair VSA は属性 1 になります。ベンダーごとに最大 256 の VSA を定義できます。1 つの RADIUS パケットに、任意の VSA 属性 26（Vendor-specific）が格納されます。VSA はサブ属性と呼ばれる場合もあります。

W

WAN Wide-Area Network（ワイドエリア ネットワーク）。広範な地理的領域に分散するユーザにサービスを提供し、多くの場合、共通の通信事業者が提供する送信デバイスを使用するデータ通信ネットワークです。

WCCP Web Cache Communication Protocol（Web キャッシュ通信プロトコル）。選択したタイプのトラフィックを Web キャッシュ エンジンのグループに透過的にリダイレクトして、リソースの使用状況を最適化し、応答時間を短縮します。

WEP Wired Equivalent Privacy。無線 LAN 用のセキュリティ プロトコルであり、IEEE 802.11b 規格で定義されています。

WINS Windows Internet Naming Service。特定のネットワーク デバイスに関連付けられた IP アドレスを確認する Windows システムであり、「名前解決」とも呼ばれます。WINS は、現在使用可能なネットワーク デバイスの NetBIOS 名と各デバイスに割り当てられた IP アドレスが自動的にアップデートされる分散データベースを使用します。WINS は、ルーティング型ネットワーク環境で NetBIOS 名から IP アドレスへのダイナミック マッピングを登録し、クエリーを実行するための分散データベースを提供します。WINS は、複雑なネットワークにおける名前解決で発生する問題を解決できるように設計されているため、このようなルーティング型ネットワークでの NetBIOS の名前解決には最適な選択肢です。

X

X.509 デジタル証明書の定義に広く使用されている規格。X.509 は実際には ITU 勧告であり、公式には規格としての使用が定義または承認されていない状態です。

xauth 「IKE 拡張認証」を参照してください。

xlate xlate は変換エントリとも呼ばれ、1 つの IP アドレスから別の IP アドレス、または 1 つの IP アドレスとポートのペアから別のペアへのマッピングを表します。

あ

アクセス モード ASA 1000V の CLI では複数のコマンド モードが使用されます。各モードで使用可能なコマンドが異なります。「ユーザ EXEC モード」、「特権 EXEC モード」、「グローバル コンフィギュレーション モード」、「コマンド固有のコンフィギュレーション モード」も参照してください。

圧縮 符号化しない表現よりも少ないビット数やその他の情報処理単位を使用して情報を符号化するプロセス。圧縮によって転送パケットのサイズを小さくし、通信のパフォーマンスを高めることができます。

アドレス解決プロトコル 「ARP」を参照してください。

アドレス変換 ネットワーク アドレスまたはポート（あるいはその両方）から別のネットワーク アドレスまたはポートへの変換。「IP アドレス」、「インターフェイス PAT」、「NAT」、「PAT」、「スタティック PAT」、「xlate」も参照してください。

暗号化 ネットワーク上のセキュアな通信のために使用される、暗号化、認証、整合性、キーなどのサービス。「VPN」および「IPsec」も参照してください。

暗号化 データに特定のアルゴリズムまたは暗号を適用して、情報の表示を許可されていないユーザがそのデータを理解できない状態にすること。「復号化」も参照してください。

暗黙のルール デフォルト ルールに基づいて、またはユーザ定義ルールの結果として、ASA 1000V によって自動的に作成されるアクセス ルール。

い

インスペクション エンジン ASA 1000V は、トラフィック内に埋め込まれたアドレッシング情報の位置を確認するために、一定のアプリケーションレベルのプロトコルを検査します。インスペクションにより、このような埋め込みアドレスを NAT で変換したり、変換の影響を受けるチェックサムやその他のフィールドをアップデートすることができます。多くのプロトコルでは、セカンダリの TCP または UDP ポートを開いているため、各アプリケーション インスペクション エンジンはセッションをモニタして、セカンダリ チャネルのポート番号も確認します。予約済みポートでの初期セッションは、ダイナミックに割り当てられるポート番号のネゴシエーションに使用されます。アプリケーション インスペクション エンジンは、この初期セッションをモニタし、ダイナミックに割り当てられたポートを特定し、所定のセッションの間、それらのポート上でのデータ交換を許可します。ASA 1000V で検査が可能なプロトコルには、CTIQBE、FTP、H.323、HTTP、MGCP、SMTP、SNMP などがあります。

インターネット IP を使用したグローバル ネットワーク。LAN ではありません。「イントラネット」も参照してください。

インターフェイス 特定のネットワークと ASA 1000V の間の物理的な接続。

インターフェイス IP アドレス ASA 1000V ネットワーク インターフェイスの IP アドレス。各インターフェイスの IP アドレスは、固有である必要があります。複数のインターフェイスに対して、同じ IP アドレスや、同じ IP ネットワーク上に存在する IP アドレスを指定することはできません。

インターフェイス PAT PAT の IP アドレスが外部インターフェイスの IP アドレスでもあるという状態で使用される PAT。「ダイナミック PAT」および「スタティック PAT」を参照してください。

インターフェイス名 ASA 1000V のネットワーク インターフェイスに割り当てられた、読んで理解できる形式の名前。内部インターフェイスと外部インターフェイスのデフォルト名は、それぞれ「inside」と「outside」です。「内部」および「外部」も参照してください。

イントラネット イントラネットワーク。IP を使用した LAN です。「ネットワーク」および「インターネット」も参照してください。

お

オブジェクト グルーピング ネットワーク オブジェクト（プロトコル、サービス、ホスト、ネットワークなど）のグループにアクセス制御文を適用できるようにすることにより、アクセス制御を簡略化します。

か

外部 ASA 1000V の外部（インターネット）にある他の非信頼ネットワークに接続する最初のインターフェイス。通常はポート 0 です。「インターフェイス」、「インターフェイス名」、「発信」も参照してください。

カットスルー プロキシ

ASA 1000V で、ユーザ認証後のトラフィック フローの高速化を可能にします。カットスルー プロキシは、最初にアプリケーション レイヤでユーザの身分証明を要求します。ユーザの認証が終わると、セキュリティ アプライアンスはセッション フローをシフトし、すべてのトラフィック フローがセッション ステート情報を維持したまま送信元と宛先の間で直接かつ迅速にやり取りされるようにします。

き

キー

暗号化、復号化、または認証に使用されるデータ オブジェクト。

キャッシュ

以前に実行されたタスクから再利用可能な情報を蓄積した一時的なリポジトリ。これにより、タスクの実行に必要な時間が短縮されます。キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮したりする必要性を減らすことができます。

く

クライアント / サーバ コンピューティング

トランザクションをクライアント（フロントエンド）とサーバ（バックエンド）の 2 つの部分で分担する分散コンピューティング（処理）ネットワーク システム。分散コンピューティングとも呼ばれます。「RPC」も参照してください。

クライアント アップデート

ユーザがアップデート適用対象となるクライアントのリビジョンをアップデートできるようにします。アップデートのダウンロード元となる URL または IP アドレスを提供し、Windows クライアントの場合はオプションで VPN クライアント バージョンのアップデートが必要であることをユーザに通知します。

クリプト マップ

ASA 1000V で VPN の設定に使用される、固有の名前とシーケンス番号を持つデータ構造。クリプト マップは、セキュリティ処理が必要なデータ フローを選択し、そのようなフロー、およびそのトラフィックを送信する必要のある暗号化ピアに対するポリシーを定義します。クリプト マップは、インターフェイスに対して適用されます。クリプト マップには、IKE と IPsec を使用する VPN 用のセキュリティ ポリシーを指定するために必要な、ACL、暗号規格、ピアなどのパラメータが含まれます。「VPN」も参照してください。

グローバル コンフィギュレーション モード

グローバル コンフィギュレーション モードでは、ASA 1000V コンフィギュレーションを変更できます。このモードでは、ユーザ EXEC、特権 EXEC、およびグローバルの各コンフィギュレーション コマンドをすべて使用できます。「ユーザ EXEC モード」、「特権 EXEC モード」、「コマンド固有のコンフィギュレーション モード」も参照してください。

こ

公開キー

公開キーは、Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）に関連するデバイスによって生成されるキー ペアの 1 つです。公開キーで暗号化されたデータは、それに関連付けられた秘密キーを使用した場合にのみ復号化できます。デジタル署名が秘密キーを使用して作成されている場合、受信者は送信者の公開キーを使用して、メッセージがその送信者によって署名されていることを確認することができます。このようなキー ペアの特性により、インターネットなどのセキュアでないメディアで、スケーラブルかつセキュアな認証方式が可能になります。

コマンド固有のコンフィギュレーション モード
いくつかのコマンドは、グローバル コンフィギュレーション モードから、コマンド固有のコンフィギュレーション モードに移行します。このモードでは、ユーザ EXEC、特権 EXEC、グローバルの各コンフィギュレーション コマンド、およびコマンド固有のコンフィギュレーション コマンドをすべて使用できます。「グローバル コンフィギュレーション モード」、「特権 EXEC モード」、「ユーザ EXEC モード」も参照してください。

コンフィギュレーション、コンフィギュレーション ファイル
ASDM や CLI で管理される設定、プリファレンス、およびプロパティと同等の内容を表す ASA 1000V 上のファイル。

さ

サイトツーサイト VPN
サイトツーサイト VPN は、リモート ネットワークを 1 つの VPN として接続する 2 つの IPsec ピア間に確立されます。このタイプの VPN では、どちらの IPsec ピアもトラフィックの宛先や送信元ではありません。各 IPsec ピアは、その IPsec ピアに接続されている LAN 上のホストに暗号化と認証のサービスを提供します。各 LAN 上のホストは、一対の IPsec ピア間に確立されたセキュアなトンネル経由でデータを送受信します。

サブネット マスク
「マスク」を参照してください。

し

事前共有キー
事前共有キーは、限定された一定数の IPsec ピアを持つネットワークに適した IKE 認証方式を可能にします。この方式では、IPsec ピアの各ペアにキーを設定する必要があるため、スケーラビリティに限界があります。新しい IPsec ピアをネットワークに追加するときには、そのピアと通信するすべての IPsec ピアに対して事前共有キーを設定する必要があります。証明書と CA を使用すると、よりスケーラブルな IKE 認証方式を実現できます。

実行コンフィギュレーション
ASA 1000V の RAM で現在実行中のコンフィギュレーション。ASA 1000V の動作特性を決定しているコンフィギュレーションです。

証明書
ユーザまたはデバイスの ID と、その証明書を発行した CA の公開キーを格納した署名付き暗号オブジェクト。証明書には有効期限があり、攻撃を受けたことがわかった場合は CRL に配置することもできます。また、証明書は IKE ネゴシエーションの否認防止を行います。つまり、特定のピアとの IKE ネゴシエーションが完了したことを第三者に証明できます。

シリアル伝送
データ キャラクタのビットを 1 つのチャネルで順次伝送するデータ伝送方式。

す

スタティック PAT
スタティック Port Address Translation（ポート アドレス変換）。スタティック PAT は、ローカル ポートからグローバル ポートへのマッピングも行うスタティック アドレスです。「ダイナミック PAT」および「NAT」も参照してください。

スタンバイ装置
「セカンダリ装置」を参照してください。

ステートフル インスペクション
ネットワーク プロトコルは、ステート情報と呼ばれる特定のデータを、2 つのホスト間のネットワーク接続の各エンドポイントで保持しています。ステート情報は、パケットの送達保証、データのシーケンス指定、フロー制御、トランザクション ID やセッション ID などのプロトコルの機能を実装するために必要な情報です。プロトコルのステート情報の一部は、各プロトコルの使用中にパケットに格納されて送信されます。たとえば、Web サーバに接続されたブラウザは HTTP を使用し、TCP/IP プロトコルをサポートします。各プロトコル レイヤは、そのレイヤで送受信するパケット内にステート情報を保持します。ASA 1000V とその他の一部のファイアウォールは、各パケット内のステート情報を検査し、パケットに格納されたすべてのプロトコルについてその情報が最新で有効であることを確認します。この機能はステートフル インスペクションと呼ばれ、コンピュータ セキュリティの特定のタイプの脅威に対して強力な防壁を作成することを目的としています。

スプーフィング
フィルタやアクセス リストなどのネットワーク セキュリティ メカニズムを乱すことを目的としたタイプの攻撃。スプーフィング攻撃では、実際とは異なるアドレスから送信されているかのようなパケットが送信されます。

スプリット トンネリング
リモート VPN クライアントがプライベート ネットワークへの暗号化アクセスとインターネットへの非暗号化アクセスの消去を同時に実行できるようにします。スプリット トンネリングをイネーブルにしていない場合、VPN クライアントと ASA 1000V の間のすべてのトラフィックが IPsec トンネル経由で送信されます。VPN クライアントから発信されるすべてのトラフィックがトンネル経由で外部インターフェイスに送信され、リモート サイトからインターネットへのクライアント アクセスは拒否されます。

せ

セカンダリ装置
2 台の ASA 1000V がフェールオーバー モードで動作している場合のバックアップ。

セキュリティ サービス
「暗号化」を参照してください。

セキュリティ プロファイル インターフェイス
ポリシーを適用する ASA 1000V だけで使用されるインターフェイスです。

た

ターボ ACL
ACL をコンパイルして複数のルックアップ テーブルのセットにすることにより、ルックアップを高速化します。元の ACL エントリ数とは無関係に、少数かつ一定数のルックアップからなる複数のテーブルに対して、パケット ヘッダーを使用してアクセスします。

ダイナミック NAT
「NAT」および「アドレス変換」を参照してください。

ダイナミック PAT
Dynamic Port Address Translation（ダイナミック ポート アドレス変換）。ダイナミック PAT を使用すると、複数の発信セッションが 1 つの IP アドレスから発信されているように見えます。PAT がイネーブルになっていると、ASA 1000V は、各発信変換スロット（xlate）用に PAT IP アドレスから固有のポート番号を選択します。この機能は、ISP が発信接続に十分な数の固有の IP アドレスを割り当てられない場合に役立ちます。グローバル プール アドレスは、常に PAT アドレスが使用されるよりも前に使用されます。「NAT」、「スタティック PAT」、「xlate」も参照してください。

て

データ機密性
攻撃者から読み取られないようにデータを操作するすべての方式を表します。一般に、このような操作は、データの暗号化、および通信の関係者のみが入手できるキーによって実現されます。

データ整合性
秘密キーまたは公開キーのアルゴリズムに基づく暗号化を使用して、保護されたデータの一部を受信するユーザが、そのデータが搬送中に変更されていないことを確認できるメカニズム。

データ発信者認証
保護されたデータがその送信者のみから発信されていることを受信者が確認できるセキュリティ サービス。このサービスには、データ整合性サービスと、秘密キーが送信者と受信者の間だけで共有されるキー配布メカニズムが必要です。

デジタル証明書
「証明書」を参照してください。

転送モード
各パケットのデータ部分（ペイロード）のみを暗号化し、ヘッダーはそのままの状態にする IPsec 暗号化モード。転送モードはトンネル モードより安全性が低くなります。

と

登録局
「RA」を参照してください。

特権 EXEC モード
ASA CLI での最上位の権限レベル。すべてのユーザ EXEC モード コマンドは、特権 EXEC モードで動作します。**enable** コマンドを入力した後、特権 EXEC モードのプロンプトが次のように表示されます。

```
hostname> enable
hostname#
```

「コマンド固有のコンフィギュレーション モード」、「グローバル コンフィギュレーション モード」、「ユーザ EXEC モード」も参照してください。

トラフィック ポリシング
トラフィック ポリシング機能は、各トラフィックが設定されている最大レート（ビット / 秒）を超えないことを保証します。したがって、1 つのトラフィック フローでリソース全体が占有されないことを保証します。

トランスフォーム セット
「IPsec トランスフォーム セット」を参照してください。

トンネル
あるプロトコルを別のプロトコル内にカプセル化してデータを転送する方式。トンネリングは、非互換性、実装の簡略化、セキュリティなどの理由で使用されます。たとえば、トンネルにより、リモート VPN クライアントはプライベート ネットワークに暗号化アクセスを実行できます。

トンネル モード
各パケットのヘッダーとデータ部分（ペイロード）の両方を暗号化する IPsec 暗号化モード。トンネル モードは転送モードより安全性が高くなります。

な

内部
ASA 1000V によって保護された内部の信頼できるネットワークに接続する最初のインターフェイス。通常はポート 1 です。「インターフェイス」および「インターフェイス名」も参照してください。

に

認証

ユーザの ID とデータの整合性を検証する暗号プロトコルおよびサービス。IPsec フレームワークの機能の 1 つです。認証により、データストリームの整合性が確保され、搬送中に改ざんされないことが保証されます。また、認証により、データストリームの発信元が確認されます。「AAA」、「暗号化」、「VPN」も参照してください。

ね

ネットマスク

「マスク」を参照してください。

ネットワーク

ASA 1000V のコンフィギュレーションから見ると、ネットワークは 1 つのホストではなく、特定の IP アドレス空間の一部を共有するコンピューティング デバイスのグループです。ネットワークは複数のノードとホストで構成されます。「ホスト」、「インターネット」、「イントラネット」、「IP」、「LAN」、および「ノード」も参照してください。

の

ノード

通常はホストとは呼ばれない、ルータやプリンタなどのデバイス。「ホスト」および「ネットワーク」も参照してください。

は

ハッシュ、ハッシュ アルゴリズム

ハッシュ アルゴリズムは、任意の長さのメッセージに対して動作する単方向の機能であり、暗号化サービスがデータの整合性を保証するために使用する固定長のメッセージ ダイジェストを作成します。MD5 は、SHA-1 よりもダイジェストが小さく、わずかに速いとされています。シスコでは、SHA-1 フレームワークの実装において MD5 と IPsec の両方のハッシュを使用しています。「暗号化」、「HMAC」、「VPN」も参照してください。

発信

発信元インターフェイスよりもセキュリティ レベルの低いインターフェイスを宛先とするトラフィック。

発信 ACL

発信トラフィックに適用される ACL。

ひ

非対称暗号化

公開キー システムとも呼ばれます。非対称暗号化では、他の任意のユーザの公開キーに誰でもアクセスすることができます。公開キーにアクセスしたユーザは、その公開キーを使用してキー所有者に暗号化メッセージを送信することができます。「暗号化」および「公開キー」も参照してください。

秘密キー

秘密キーは、送信者と受信者の間だけで共有されるキーです。「キー」および「公開キー」を参照してください。

ふ

フィックスアップ 「インスペクション エンジン」を参照してください。

プール 「IP プール」を参照してください。

フェーズ 1 「IPsec フェーズ 1」を参照してください。

フェーズ 2 「IPsec フェーズ 2」を参照してください。

不揮発性ストレージ、メモリ RAM とは異なり、電源が入っていなくても内容を保持しているストレージまたはメモリ。不揮発性ストレージ デバイス内のデータは、パワーオフ / パワーオン（電源再投入）を実行しても失われません。

復号化 暗号化されたデータに特定のアルゴリズムまたは暗号を適用して、情報の表示を許可されたユーザがそのデータを理解できる状態にすること。「暗号化」も参照してください。

プライマリ、プライマリ ユニット 2 台の ASA 1000V（プライマリとセカンダリ）がフェールオーバー モードで動作している場合に、通常動作している方の装置。

フラッシュ、フラッシュ メモリ ASA 1000V の電源がダウンしている場合にコンフィギュレーション ファイルを保存するために使用される不揮発性ストレージ デバイス。

プロキシ ARP ASA 1000V が、グローバル プール内の IP アドレスに対する ARP 要求に応答できるようにします。「ARP」も参照してください。

プロトコル、プロトコルのリテラル ネットワーク ノード間の通信用のパケット交換について定義した規格。プロトコルはレイヤ構造で連携動作します。ASA 1000V のコンフィギュレーションでは、プロトコルはセキュリティ ポリシーの定義の一部として、リテラル値またはポート番号で指定されます。ASA 1000V で指定可能なプロトコルのリテラル値は、ahp、eigrp、esp、gre、icmp、igmp、igrp、ip、ipinip、ipsec、nos、ospf、pcp、snp、tcp、および udp です。

へ

ヘッドエンド パブリック ネットワーク経由の VPN クライアント接続に対して、プライベート ネットワークへのエントリ ポイントとして機能するファイアウォール、コンセントレータ、またはその他のホスト。「ISP」および「VPN」も参照してください。

変換 「xlate」を参照してください。

ほ

ポート TCP および UDP プロトコルのパケット ヘッダー内で、パケットの送信元または宛先である上位レベルのサービスを識別するフィールド。

ホスト TCP/IP ネットワーク上で IP アドレスを持つ任意のデバイスの名前。「ネットワーク」および「ノード」も参照してください。

ホスト / ネットワーク アドレス変換（xlate）や ACE など、ASA 1000V のコンフィギュレーションにおいて、1 つのホストまたはネットワーク サブネットを識別するために他の情報とともに使用される IP アドレスとネットマスク。

ポリシー NAT

アクセス リストに送信元と宛先のアドレス（またはポート）を指定することにより、アドレス変換の対象となるローカル トラフィックを識別します。

ま

マスク

インターネット アドレスが、ネットワーク、サブネット、およびホストの部分にどのように分割されているかを示す 32 ビットのマスク。マスク内では、ネットワークとサブネットの部分に使用されるビット位置にビットが指定され、ホストの部分にはゼロが指定されます。マスクには少なくとも標準ネットワークの部分が必要であり、サブネット フィールドはネットワークの部分と連続している必要があります。

め

メッセージ ダイジェスト

メッセージ ダイジェストは、メッセージの整合性を保証するために使用される MD5 や SHA-1 などのハッシュ アルゴリズムによって作成されます。

も

モード

「アクセス モード」を参照してください。

モード コンフィギュレーション

「IKE Mode Configuration」を参照してください。

モジュラ ポリシー フレームワーク

Cisco IOS ソフトウェアのモジュラ QoS CLI と同様の方法で ASA 1000V の機能を設定するための手段です。

ゆ

ユーザ EXEC モード

ASA CLI での最下位の権限レベル。ユーザ EXEC モードのプロンプトは、初めて ASA 1000V にアクセスしたときに次のように表示されます。

```
hostname>
```

「コマンド固有のコンフィギュレーション モード」、「グローバル コンフィギュレーション モード」、「特権 EXEC モード」も参照してください。

り

リプレイ検出

受信者がリプレイ攻撃を無効にするために、古いパケットまたは重複したパケットを拒否できるセキュリティ サービス。リプレイ攻撃は、攻撃者が古いパケットまたは重複したパケットを受信者に送信し、受信者がその偽のパケットを正当なものと認識するというしくみの攻撃です。リプレイ検出は、シーケンス番号と認証を組み合わせて使用することで実行され、IPsec の標準機能となっています。

リフレッシュ

ASA 1000V から実行コンフィギュレーションを取得して、画面をアップデートします。アイコンとボタンで同じ機能が実行されます。

る

ルート、ルーティング
ネットワークを通過するパス。

ルール
特定の状況に対するセキュリティ ポリシーを定義するために、ASA 1000V のコンフィギュレーションに追加される条件文。「ACE」、「ACL」、「NAT」も参照してください。

れ

レイヤ
ネットワーキング モデルは、異なるプロトコルと関連付けられた複数のレイヤを実装しています。最も一般的なネットワーキング モデルは OSI モデルです。これは 7 つのレイヤで構成されます。これらのレイヤの順番は、物理、データリンク、ネットワーク、トランスポート、セッション、プレゼンテーション、およびアプリケーションです。