**ワイヤレス**

WLC・・・無線LANコントローラ。複数台の無線LANアクセスポイントを管理する装置

集中管理型AP・・・アンテナの役割とデータ受信時の暗号化処理だけを行い、認証、暗号化、電波出力調整、ローミングはWLCが行う。

自律型AP・・・APのみで動作する。一台ずつ設定する必要があるため小規模なネットワークには最適。

CSMA/CA・・・WLANにおけるコリジョンを回避する通信方法。有線とは異なりコリジョン検出する機能がないためランダムな時間をおいてからデータを送信する

SOHO・・・パソコンやインターネットを活用して自宅など小規模のオフィスで仕事をする形態

BSS・・・APの有無にかかわらず無線ネットワークのグループを指し、相互に通信する無線ノードグループを指す基本サービスセットのこと

BSSID・・・BSSのグループの中で各無線ノードの識別に使用されるIDのこと。

48ビット

ESS・・・複数のBSSで構成される無線LANのネットワーク

　ESSID・・・無線LANにおけるネットワークの識別に使用されるIDのこと。

　最大32文字までの英数字

ローミング・・・無線LANクライアントが異なるAP間を渡り歩けるような機能

CAPWAP・・・WLCとAPの間で通信制御を行うためのプロトコルのひとつ

**FHRP**

HSRP・・・デフォルトゲートウェイを冗長化するためのシスコ独自のプロトコル。アクティブルータとスタンバイルータ。

VRRP・・・デフォルトゲートウェイを冗長化するためのRFC3768で標準化されたプロトコル。マスタールータとバックアップルータ。仮想IPアドレスに「物理IPアドレスとは別のIPアドレス」と「マスタールータンの物理IPアドレス」を指定することができる。

GLBP・・・デフォルトゲートウェイなどを冗長化するためのシスコ独自のプロトコル。

１つのグループ内で利用可能なデフォルトゲートウェイを複数存在させることができるためデフォルトゲートウェイの負荷分散を実現できる。

アクティブルータ・・・仮想ルータ宛てのパケットをルーティングするルータのこと。

スタンバイルータ・・・アクティブルータがダウンすると代わりにアクティブルータとなり仮想ルータ宛てのパケットをルーティングする。

**QoS**

輻輳管理・・・パケットを見てデータの通る順番や量を調節する。

輻輳回避・・・輻輳によっておこるテールドロップを防ぐためにキューに待機しているパケットを破棄すること。

テールドロップ・・・キューがいっぱいになったとき新しく到着したパケットが入りきらず破棄されてしまうこと。

帯域制御・・・特定の基準をもとに使用できるデータ転送量や通信速度を制限できること。

　シェーピング・・・トラフィック量の最大値を超過したパケットについて、バッファに蓄積し順番に処理をする手法。遅延、ジッタの要因になる。

　ポリシング・・・トラフィック量の最大値を超過したパケットはバッファへ蓄積せずに破棄する手法。損失が起こる要因ではあるが遅延、ジッタは発生しない。

**WAN**

VPN・・・仮想的なプライベートネットワーク接続のこと。WANサービスのひとつ。

インターネットVPN・・・ネットワーク上に仮想の暗号化された専用線を構築し、安全なルートを保持したうえで重要な情報をやり取りすることにより盗み見や改ざんなどの脅威から大切な情報を守ることができる。

　サイト間VPN・・・経典を接続するVPNのこと。それぞれの拠点にVPNゲートウェイを設置し、インターネット上に安全な通信経路を構築します。

　クライアントVPN・・・PCにソフトウェアを導入することでPCとAWSVPC間でVPN接続を行う

IPsec・・・インターネットVPNでよく使用されて、ネットワーク層で動作するプロトコル

GRE・・・トンネリングプロトコルのひとつである。遠く離れたLANを、あたかも隣接したLANをあたかも隣接したLANのようにトンネリングできる。

クラウド・・・インターネットなどのネットワーク経由でユーザにサービスを提供する形態のこと。

　SaaS・・・サーバ上で機能するアプリケーションまで含めたすべてをクラウド事業者が管理提供するサービスのこと

PaaS・・・アプリケーション開発環境などのミドルウェアまでを備えた形で提供されるサービスのこと

　IaaS・・・物理サーバー・ネットワーク・OSのインフラ部分のリソースだけが提供されるサービスのこと

**セキュリティ**

脆弱性・・・コンピュータのOSやソフトウェアにおいてプログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを言う。

脅威・・・リスクを発生させる要因、情報資産に損失を与える要因のことで、結果的に組織が保有する情報資産に対して害を及ぼす、または発生する可能性のあるもの

マルウェア・・・不正かつ有害に動作させる意図で作成された悪意あるソフトウェアや悪質なコードの総称。

　ウイルス・・・ほかのパソコンを攻撃したり、情報を盗む目的で悪意を持った人間によって意図的に作られた不正なプログラムのこと

　ワーム・・・独立したプログラムであり、自信を複製してほかのシステムに拡散する性質を持ったマルウェアのひとつ。

　トロイの木馬・・・正規のソフトウェアやファイルに成りすまし、ユーザに気づかされないように追う劇を仕掛けるマルウェアのひとつ。

スプフィーング・・・不正なデータを用いることにより、攻撃者や攻撃用プログラムを別の人物やプログラムに見せかけることを利用した攻撃。

　DoS攻撃・・・アクセスが集中することでサーバがパンクすることを利用し、悪意を持ってサーバに大量のデータを送り付けるサイバー攻撃のこと

　DDoS攻撃・・・ウイルスなどに感染させて不正にのっとった複数のPCを操作して行うDoS攻撃のこと。

　中間者攻撃・・・攻撃対象の通信内容を盗聴・改ざんすることを目的とした攻撃。

ソーシャルエンジニアリング・・・人間の心理的な隙や行動のミスに付け込んで個人が持つ秘密情報を入手する方法。

ブルートフォースアタック・・・（総当たり攻撃）暗号解読方法のひとつで、可能な組み合わせをすべて試す方法。

WPA・・・無線LANの通信内容を暗号化する際の暗号化のやり方

　WPAパーソナル・・・WPAの事前共有鍵PSKを使って認証するやり方。

　WPAエンタープライズ・・・WPAの認証サーバを使って認証するやり方。

サプリカント・・・ネットワーク上の利用者や端末の認証において、認証を要求する側クライアント側の機器やソフトウェアのこと。

オーセンティケータ・・・ユーザのIDを確認するため、つまりデジタル認証を実行するために使用される手段。PCからの認証情報をRADIUSサーバに中継する機器。

認証サーバ・・・ユーザ認証を行うサーバ

多要素認証・・・認証の3要素である知識情報、所持情報、生体情報のうち、2つ以上を組み合わせて認証すること

　知識要素・・・その人の頭の中にある情報のこと。

　所持要素・・・本人のみが所持しているものであり、スマホやICカードなどのこと。

　生体要素・・・その人固有の身体的特徴のこと。指紋認証や顔認証

AAA・・・情報システムが利用者を識別し利用者に応じた制御を行う際に重要な要素を表した標語

　Authentication・・・認証。ユーザID/パスワード、デジタル証明書などの有効なクレデンシャル信用情報を確認し正当なユーザであるかを決定する。

　Authorization・・・認可。認証に成功したユーザに対して提供する権限を制限する。

　Accounting・・・認証に成功したユーザに対して情報を収集する。

RADIUS・・・ネットワーク上で利用者の認証や権限の付与、利用状況の記録などを行うための通信プロトコルのひとつ。