WLC

集中管理型ApのWLAN

複数のApを管理可能

集中管理型Ap

Apは電波の受信のみ

自律型Ap

Ap単独でWLANを提供可能

各Apで設定、制御が可能

CSMA/CA

WLANにおいてコリジョンを回避する

SOHO

小さなネットワーク

BSS

一台のApと配下の端末で構成する単純なネットワーク

BSS ID

BSSの識別名、通常はMacアドレスのまま使用

ESS

複数のApを一つのネットワークとして、一体的に運用

ESS ID

管理者がネットワークに32バイトまで任意で名称をつけて識別可能

ローミング

無線端末に再設定等を行わなくても、自動的にアクセスポイントを切り替えることができる

cap wap

WLCとAP間て通信制御を行うためのプロトコル

FHRP

ゲートウェイを冗長化するプロトコル

HSRP

シスコ独自のプロトコル

VRRP

ルータを冗長化するプロトコル

GLBP

シスコ独自のプロトコル

アクティブルーター

実際に転送処理しているルーター

スタンバイルーター

アクティブルータのバックアップをするルーター

服装管理

パケットに割り当てられた優先順位をもとに、送信をして輻輳をコントロールする

テールドロップ

キューがいっぱいになった時に、それ以降に届いたパケットを破棄する

帯域制御

特定の基準を元にして、使用できるデータ転送量、通信速度を制限

ジェーピング

事前に設定したトラフィック量が最大値に超過したパケットは、バッファに蓄積し、順番に処理する

ポリシング

事前に設定したトラフィック量が最大値に超過したパケットは破棄する

VPN

仮想的なプライベートネットワーク接続

インターネットVPN

インターネット上に暗号化された専用の通信経路を形成し、仮想的な組織内ネットワークを構築する

企業がLANにアクセスするために使用する

サイト間VPN

オフィス間など複数の拠点のネットワークを透過的に連結するために構築されるもの。

リモートアクセスVPN

オフィスとモバイル端末、オフィスと従業員の自宅など、端末から拠点に安全にアクセスできるように構築されるもの

IPsec

インターネットなどのTCP/IPネットワークで暗号通信を行うためのプロトコル

GRE

IPネットワークで使用するトンネリングプロトコルの一つ　暗号化はしない

クラウド

ネットワーク経由で、ユーザーにサービースを提供する形態

SaaS

ソフトウェアをインターネットを通じて遠隔から利用者に提供する方式。

PaaS

ソフトウェアの実行環境をインターネット上のサービスとして遠隔から利用できるようにしたもの。

IaaS

情報システムの稼動に必要なコンピュータや通信回線などの基盤（インフラ）を、インターネット上のサービスとして遠隔から利用できるようにしたもの。

脆弱性

コンピュータやソフトウェア、ネットワークなどが抱える保安上の弱点。システムへの損害や不正な操作、情報の盗み取りや改竄など、管理者や利用者にとって脅威となる行為に悪用できる可能性のある欠陥や、仕様・設計上の不備

脅威

個人や企業の情報資産に対して損失などを与える要因やリスクを発生させる要因のこと

マルウェア

コンピュータの正常な利用を妨げたり、利用者やコンピュータに害を成す不正な動作を行うソフトウェアの総称

ウイルス

コンピュータの正常な利用を妨げる有害なコンピュータプログラム（ソフトウェア）の一種で、他のプログラムの一部として自らを複製し、そのプログラムが起動されると便乗して悪質な処理を実行に移すもの。

ワーム

有害な動作を行うソフトウェアの一種で、インターネットなどを通じてコンピュータに侵入し、さらに他のコンピュータへの自身の複製を試みるもの

トロイの木馬

何らかの有用なソフトウェアなどを装って導入や実行を促し、起動すると利用者に気付かれないよう秘密裏にデータ漏洩や遠隔操作などの有害な動作を行うソフトウェア

IPスプーフィング

TCP/IPネットワークを通じた攻撃手法の一つで、IPパケットの送信元として虚偽のIPアドレスを書き入れてそのアドレスになりすます手法

DoS攻撃

通信ネットワークを通じてコンピュータや通信機器などに行われる攻撃手法の一つで、大量のデータや不正なデータを送りつけて相手方のシステムを正常に稼働できない状態に追い込むこと

DoS攻撃

インターネット上の多数の機器から特定のネットワークやコンピュータに一斉に接続要求を送信し、過剰な負荷をかけて機能不全に追い込む攻撃手法

中間者攻撃

通信を行う二者の間に割り込んで、両者が送受信する情報を自分が用意したものとすりかえることにより、気付かれることなく盗聴したり、通信内容に介入したりする攻撃手法

ソーシャルエンジニアリング

コンピュータシステムにアクセスするために必要な情報（パスワードなど）やその手がかりを、それを知る本人や周辺者への接触や接近を通じて盗み取る手法の総称

ブルートフォースアタック　総当たり攻撃

暗号の解読やパスワードの割り出しなどに用いられる手法の一つで、割り出したい秘密の情報について、考えられるすべてのパターンをリストアップし、片っ端から検証する方式

WPA

無線LANを暗号化するプロトコル

WAN パーソナル

暗号化する際の規格が「WPA」で「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

暗号化する際の規格が「WPA」で「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

利用者や端末などとやり取りして認証を実施するシステムや装置という意味で用いられる

認証サーバ

システムの使用やネットワークへの接続を試みた人物が登録利用者本人であるかを確認する「認証」（authentication）を行うサーバ

多要素認証

利用者の本人確認などの認証において、複数の異なる原理の認証手段を組み合わせて用いることにより精度と安全性を高める手法

知識要素

その人の頭の中にある情報のこと

【知識要素の例】

パスワード

PINコード

秘密の質問

所有要素

その人だけが持っているモノ

【所有要素の例】

スマートフォンのSMS認証やアプリ認証

トークン（ワンタイムパスワード生成端末）

ICカード

生体要素

生体要素とはその人固有の身体的特徴のこと

【生体要素の例】

指紋

虹彩

顔

声紋

静脈

位置情報

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

対象の正当性や真正性を確かめること、相手が名乗った通りの本人であると何らかの手段により確かめる本人確認（相手認証）のこと

Authorization 認可

コンピュータシステムの利用者に特定の操作権限を付与する処理や手続きを指すこと

Accounting

利用状況や履歴を記録し、課金や利用制限などに反映させる活動を表す

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一つ

キャンパスネットワーク

地理的に一つの範囲内にある複数の建物で構成された企業・組織・団体などのLAN

構内ネットワークやエンタープライズネットワークとも呼ぶ

2階層キャンパス設計モデル

2つの層で構成される小規模な環境向けのネットワーク設計

\* ﻿アクセス層：ユーザを直接収容する

\* ﻿ディストリビューション層：アクセス層のスイッチを収容

コア層がなくなっていることから、

コラプストコア（Collapsed core：つぶれたコア）設計とも呼ぶ

3階層キャンパス設計モデル

3つの層で構成される大規模な環境向けのネットワーク設計

\* ﻿アクセス層：ユーザを直接収容する

\* ﻿ディストリビューション層：アクセス層のスイッチを収容す

\* ﻿コア層：ディストリビューション層のスイッチを収容

コアスイッチは核となる拠点に配置されるのが一般的

SOHO

小規模なネットワーク構成

サービス統合型ルータ、スイッチやファイアウォールの機能も合わせて持っているルータ、自律型 APが使用される

PoE (Power over Ethernet)

LANケーブルを経由して電力を供給する仕組み

PSE(Power Sourcing Equipment ： 給電装置）

電力を供給するデバイス

（スイッチや電源装置など）

PD（ Powered Device：受電装置）

電力の供給を受けるデバイス

（IP Phoneやアクセスポイント(AP) など)

WAN(Wide Area Network）

広い範囲にわたるネットワーク

通信事業者（キャリア）のWANサービスを利用して中継する

LAN (Local Area Network)

建物内や敷地内などの限定された範囲のネットワーク

WANのトポロジ

①ポイントツーポイント

拠点間を1対1で接続する構成

②ハブ・アンド・スポーク型（スター型)

ハブを中心としてその他スポークを放射状に接続する構成

③パーシャル（部分）メッシュ型

重要な拠点などの一部をメッシュにする構成

対障害性はフルメッシュ型に劣る

コストと対障害性のバランスの取れた構成

④フルメッシュ型

拠点同士が全て直接通信できる構成

どこかの拠点で障害が発生しても、他の通信に影響しない

信頼性は高いが、コストも高い

専用線

1対1で拠点間をつなぐサービス

﻿通信速度が保証され信頼性も高い

セキュリティが高くない

コストが高くなる。

﻿1対1の接続になるため、拠点が増えると接続する回線を増やす必要があり、拡張性に欠ける

HDLC(High-level Data Link Control ）

専用線などのポイントツーポイント接続で使用するデ-タリンク層プロトコル

HDLCは各ベンダが独自に実装しているので、対向ルータが別ベンダである場合、HDLCでは通信不可

■ PPP

ポイントツーポイント接続で使用するプロトコル

HDLCと違って複数のネットワーク層のプロトコルを転送でき、さまざまな回線で使用できます。異なるベンダの機器同士でも通信が可能

VPN

仮想的なプライベートネットワーク接続

WANサービスの一つ

VPNは拠点間で安全な通信を可能にし、コストを抑えることが可能

拡張性を持つ

VPNを利用することで、

それぞれの拠点のプライベートなネットワークが直接繋がっているように見せかけることができる

今までは専用線やフレームリレーが利用されてきましたが、より手軽でコストが低い、かつセキュリティが確保されているVPNの利用が増えている

インターネットVPN

インターネットを利用するVPNのこと

解読されないように暗号化が必要になる

サイト間VPN

拠点間のLAN接続するためのVPN接続のこと

拠点にVPN対応のルータを設置をして各拠点のルータ間でトンネルが作成され、暗号化や復号を各ルータで行う

各端末にVPN接続用のソフトウェアをインストールする必要がないのが特徴

リモートアクセスVPN

モバイル端末やテレワークの際に自宅から社内のネットワークに接続されるためのVPN接続

こ拠点にVPNを受ける機器、PCにはVPN接続用のソフトウェアのインストールも必要

ソフトウェアにより端末からトンネルが作成されて、暗号化を行うのが特徴

IP-VPN

通信事業者が用意した閉域網を利用するVPN

閉域網とは、限られた利用者のみが使えるネットワーク

インターネットとは隔離されているネットワークの為、インターネットVPNより安全

インターネットVPNよりコストがかかる

通信事業者側はMPLSという技術を使って宛先を識別

MPLS (Multi Protocol Label Switching)

パケットにラベルと呼ばれる情報を付与して、転送の処理はそのラベルに基づいて通信を行う

このラベルのみ使って転送先の検索を行うので、読み込む情報も少なく、転送処理の高速化が可能

VPNの技術

トンネリング

通信したい端末の間に、ネットワーク上で仮想的に専用線を作成すること

トンネリングでは、相手と通信するためのパケットを別のプロトコルのデータ部に隠蔽（カプセル化）を行う

■暗号化

インターネットなどにデータを送信する際に元のパケットにある重要な情報を隠蔽すること

暗号化を行い、宛先の拠点のルータで復号を行います。

トンネリングで使用するプロトコル

\_PPTP (Point-to-Point Tunneling Protocol)

PPPを拡張したプロトコル

トンネリングのカプセル化に関係

PPTPには暗号化の機能がないので、暗号化プロトコルMPPE(Microsoft Point to PointEncryption)を組み合わせて使用

■L2TP (Layer2 Tunneling Protocol)

データリンク層で動作するプロトコル。

カプセル化に関係

PPTPと同様に暗号化の機能がないので、暗号化プロトコル、IPsecと組み合わせて使用

■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

IPsecはトンネリングと暗号化の両方の機能を備えている

\* ﻿完全性：VPNを通過したデータが変更されない

\* ﻿機密性：VPNを通過したデータが盗聴されない

\* ﻿データ発信元の認証：送信されてきたデータが送信元からのデータと保証する

・アンチリプレイ：不正に再送されたパケットは破棄する

--IPsecの構成プロトコルー-

IPsecは二つのセキュリティプロトコルから成り立っています。

"AH (Authentication Header)

認証機能とデータが改善されていないことを保証するプロトコル

■ESP (Encapsulated Security Payload)

AHの機能に加えて、暗号化を行うプロトコル

--IPsec動作モードー

暗号化を行う際の動作モード

■トランスポートモード

元のIPヘッダを使用して、デー夕部のみ暗号化

■トンネルモード

IPヘッダとデータ部両方を暗号化し、新しいIPヘッダを付与

設定でトンネリングする拠点間のルータで

合わせておかなければいけない項目が多い！

--その他のVPN--

•SSL-VPN

SSL(Secure Socket Layer）という暗号化プロトコルを使用したVPN

リモートアクセスVPNで利用

■広域イーサネット

拠点間を接続するために利用されるサービス

通信事業者の広域イーサネット網を使用し、網内はデータリンク層のプロトコルであるイーサネットで通信を行います。

※IP-VPNではネットワーク層のプロトコルしか使わないので、IPしか使用できないが、広域イーサネットではデータリンク層のプロトコルで転送を行うので、IP以外のネットワーク層のプロトコルによる拠点間通信が可能となるのが特徴

広域イーサネット網は共有ネットワークなので、通信が混在しないようにVLANタグで識別

EoMPL

クラウド

コンピュータリソースをインターネットなどを介して、サービスの形で必要に応じて利用する形態が特徴

クラウドサービスの事業者が大規模のデータ

センターに多数のサーバを用意しており、そこにリソースを導入し、サービスの利用者はインターネットを介して利用

オンプレミス

自社の敷地内にサーバなどのリソースを所有して利用・管理すること

従来のサーバー

1台の物理的なマシンに一つのOSをインストールして動かすのが主流

仮想サーバー

1台の物理的サーバ上でハイパーバイザを使用し、仮想マシンを動かす

■ハイパーバイザ

コンピュータを仮想化するためのソフトウェア

仮想マシンを複数構築したり、それぞれの仮想マシンで別々のOで動かしたりすることが可能

最大のメリットは、サーバのリソースを分割して有効利用できる点

また、仮想マシンの追加が設定で簡単に行うことができ、物理的にサーバを増やす必要がないので、設置スペースを削減できるという点も大きなメリット

仮想スイッチという仮想的なレイヤ2スイッチを物理サーバ内に形成

仮想マシンは仮想NICという仮想的なポートを持ち、そのポートを介して仮想スイッチと接続

クラウドのサービスの形態

■プライベートクラウド

企業専用のクラウドとして利用する形態

パブリッククラウドよりも導入コストや管理コストが上がりますが、専用で使えるのでセキュリティの向上や企業に合わせた環境の構築が可能

■パブリッククラウド

利用者を限定せずに複数のユーザーや企業に向けてクラウド環境を提供する形態

利用者が必要な時に必要な分だけ自由にサーバやネットワークリソースを利用可能

パブリッククラウドには 提供されるサービスの範囲によって分類される

SaaS (Sofeware as a Service)

サーバ上で機能するアプリケーションまで含めた全てをクラウド事業者が管理提供するサービス

・PaaS (Platfarm as a Service)

アプロケーション開発環境などのミドルウェアまで備えた形で提供されるサービス

• laaS (Infrastracture as a Service)

物理サーバ・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