令和５年度　初級レベル

レイヤー2スイッチ基礎セミナー

オンラインセミナー
ウェビナー

一般社団法人情報通信設備協会
Information & Telecommunication Equipment Constructor's Association

V3.4

内容

①技術編 (3P)

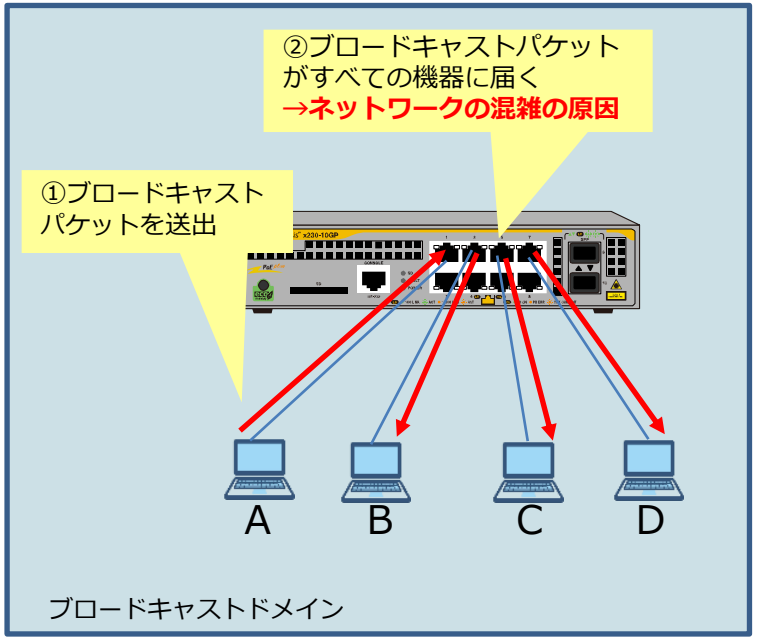
①技術編

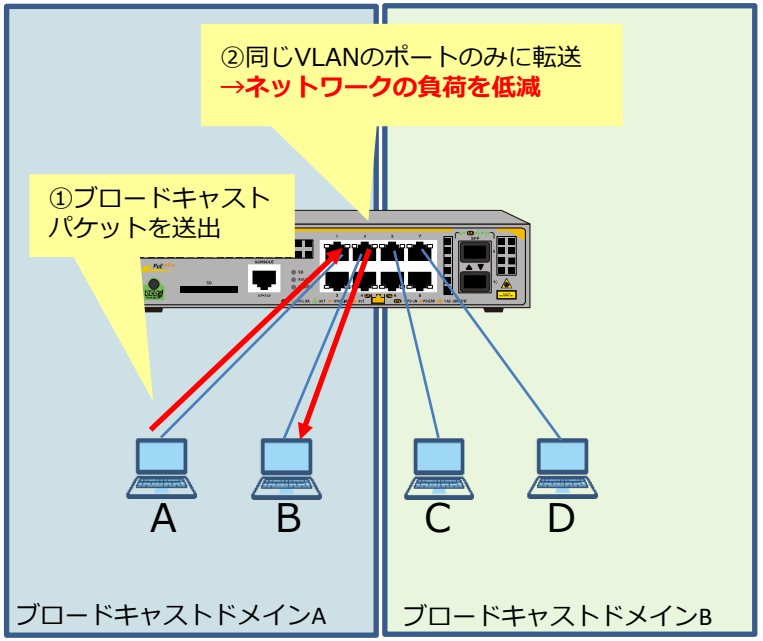
仮想化技術（VLAN）
ループ障害防止機能（ループガード）
リンクアグリゲーション（LAG）

ネットワークの分割

● ネットワークの分割

- VLAN(Virtual LAN)は、仮想的にネットワークを分割する技術です。
- ブロードキャストドメインを分割することで不要なブロードキャストデータを抑制し、機器やネットワークの負荷を低減します。





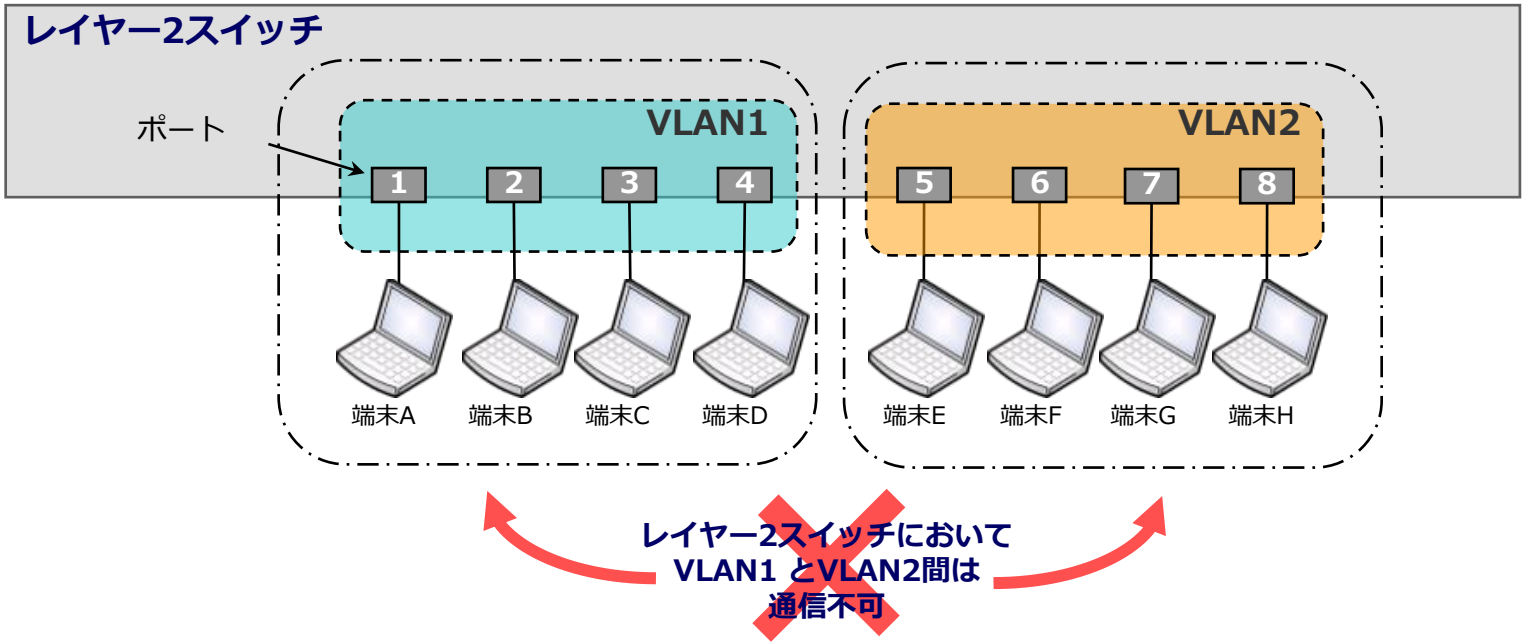
NOTE

※ブロードキャストとは、ネットワーク上に接続しているすべての端末に対して一斉にデータを送信する通信
※ブロードキャストドメインとは、ブロードキャスト通信が届くネットワークの範囲

ポートベースVLAN

ポートベースVLAN

- スイッチ内で論理的にLANを分割する機能です。
- スイッチの設定で論理的にグループ分けを行う事が可能となり、グループ構成の変更が配線の引き直しをする事なく、設定変更だけで可能になるという利点があります。
- また、ブロードキャストパケットが届く範囲を論理的に分割することも可能です。（パケットを効率的に転送）

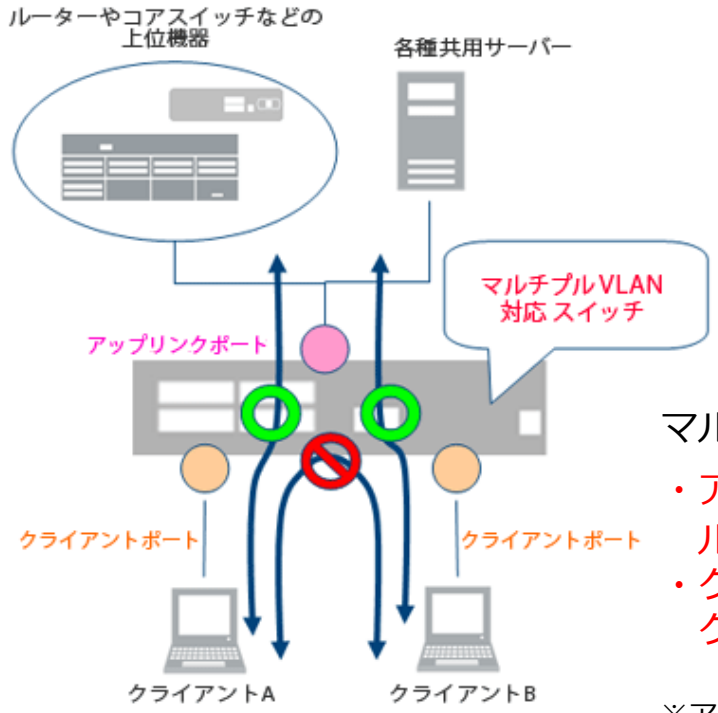


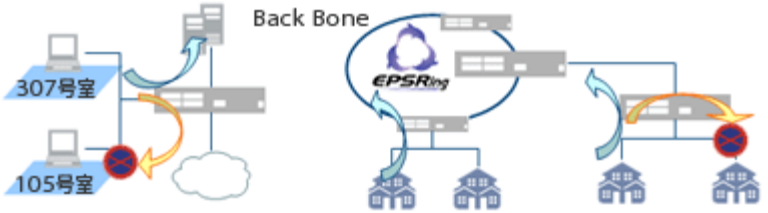
マルチプルVLAN

VLAN

■マルチプルVLAN

- パケットフィルタ等を使用せず、容易に各スペース間のセキュリティを確保し、インターネットや共用サーバーへの接続を可能にする機能です。
- 各ポートにクライアントとアップリンクを設定し、クライアント間の通信は制限、クライアントとアップリンク間の通信を許可することで、セキュリティを保ちながら、設計の柔軟性を向上させます。





マルチプルVLANでは二つの基本的なポートが存在します。

・アップリンクポート
　ルーターやスイッチ、サーバー等の共用機器が接続されるポート
・クライアントポート
　クライアント端末が接続されるポート

※アップリンクポート、クライアントポートの名称は製品により異なる場合があります。

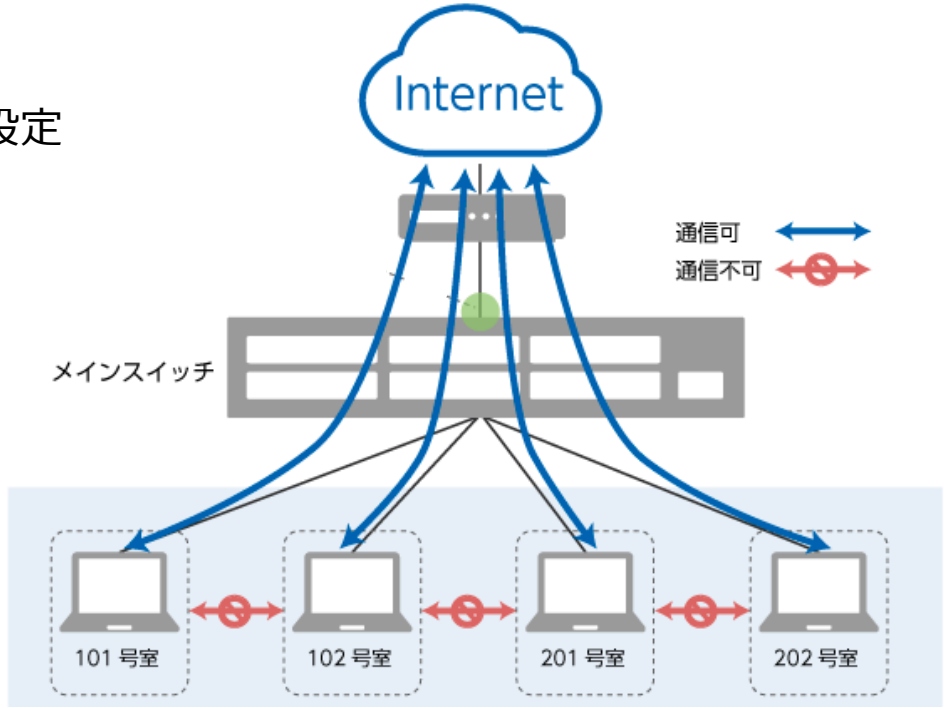
Allied Telesis

インターネットマンションの構成例 VLAN

マルチプルVLANによりポート間（居住者間）の通信を遮断することで、インターネットサービスだけを安全に提供することが可能になります。不特定多数へインターネット環境を提供する際に最適な機能です。

■ 設計コンセプト
・各部屋はインターネットを利用する
・部屋間の通信は相互に遮断されているためウィルスの感染が広まる心配はありません

■ 設計のポイント
・各部屋をクライアントポートに設定
・インターネット回線をアップリンクポートに設定

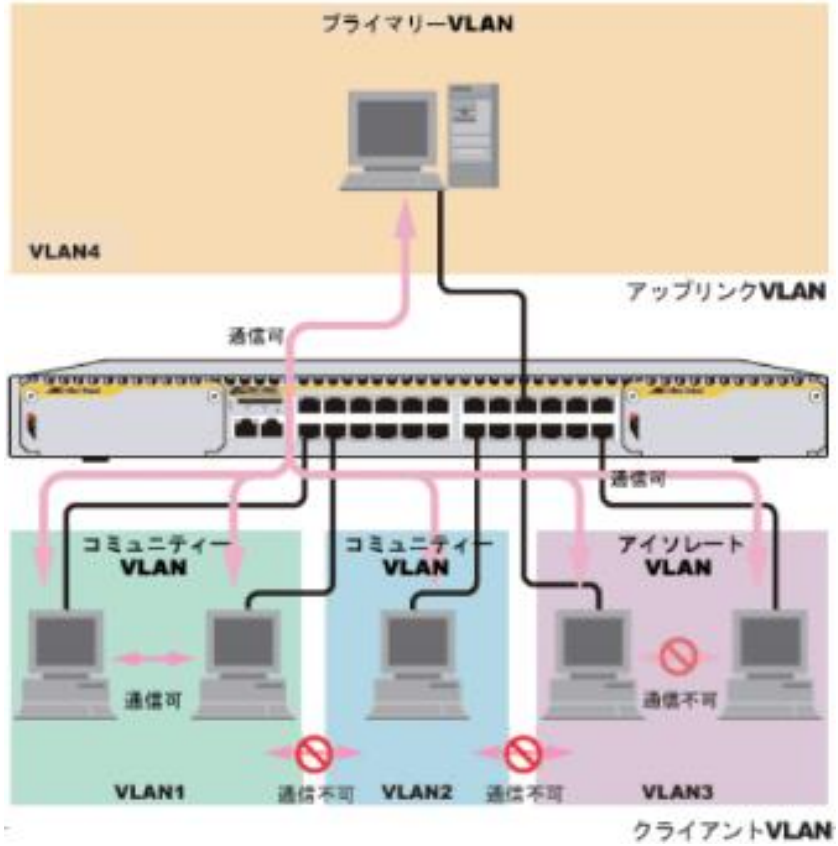


マルチプルVLANの特徴

VLAN

■ アライド製品（AlliedWare Plus 版）におけるマルチプルVLANの特徴

- AlliedWare Plusのマルチプル VLANは、プライマリーVLAN(アップリンク用VLAN)とセカンダリーVLAN（クライアント端末接続用VLAN）で構成します。また、セカンダリーVLANはアイソレートVLANとコミュニティーVLAN の二つに分かれます。
- プライマリーVLANとアイソレートVLAN間、およびプライマリーVLANとコミュニティーVLAN間の通信は可能です。



- セカンダリーVLAN間の通信は以下になります。
  - アイソレートVLAN内のクライアント端末間通信は不可
  - 同じコミュニティーVLAN内のクライアント端末間通信は可能
  - 異なるコミュニティーVLANのクライアント端末間通信は不可
  - アイソレートVLANとコミュニティーVLANのクライアント端末間通信は不可

※アップリンクポート、クライアントポートの名称は製品により異なる場合があります。

Allied Telesis

企業ネットワークの構成例

VLAN

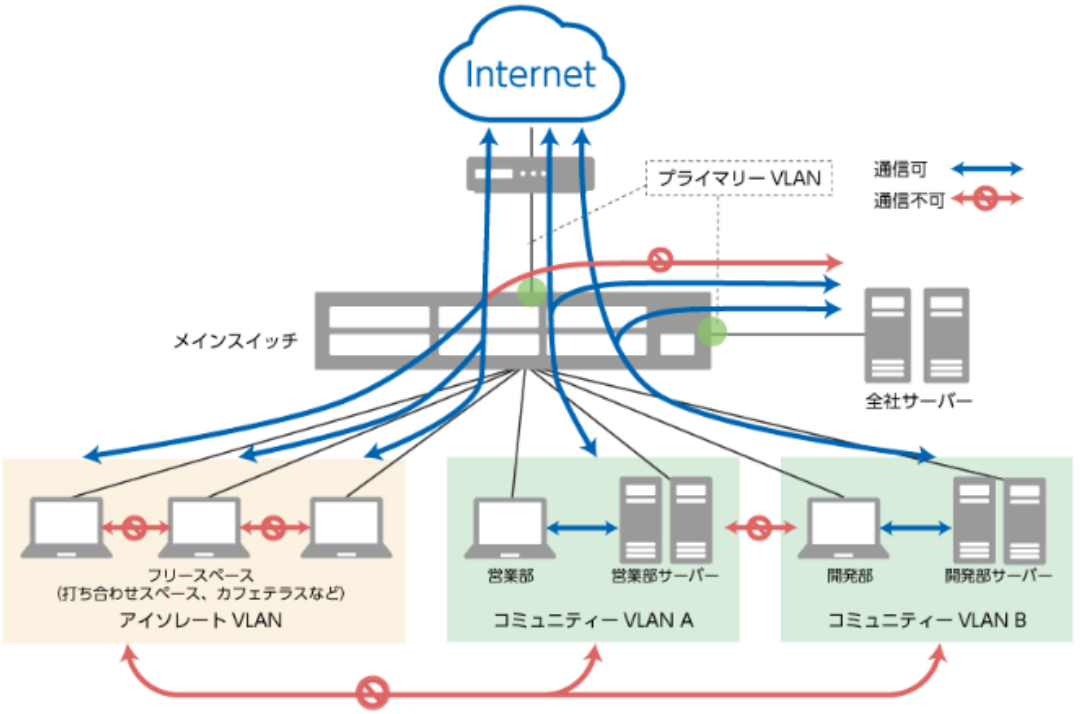
マルチプルVLANのアイソレートVLANとコミュニティーVLANを組み合わせることで、フリースペースからはインターネット接続のみを許可し、社内サーバーへは部門ネットワークからのみ接続することができるといったセキュリティを、複雑なパケットフィルタリング機能などを使わずに実現できます。

■ 設計コンセプト

・フリースペースからはインターネットのみを利用する。
・部門内の通信を許可する。
・部門間の通信を遮断する。
・各部門から全社サーバーとインターネットを利用する。

■ 設計のポイント

・フリースペースをアイソレートVLANのクライアントポートに設定
・営業部の端末と営業部サーバーをコミュニティーVLAN Aのクライアントポートに設定
・開発部の端末と開発部のサーバーをコミュニティーVLAN Bのクライアントポートに設定
・全社サーバーとインターネットへの接続をプライマリーVLANのアップリンクポートに設定
・インターネットへのアップリンクポートとアイソレートVLAN、コミュニティーVLAN A/Bを関連付ける
・全社サーバーへのアップリンクポートとコミュニティーVLAN A/Bを関連付ける

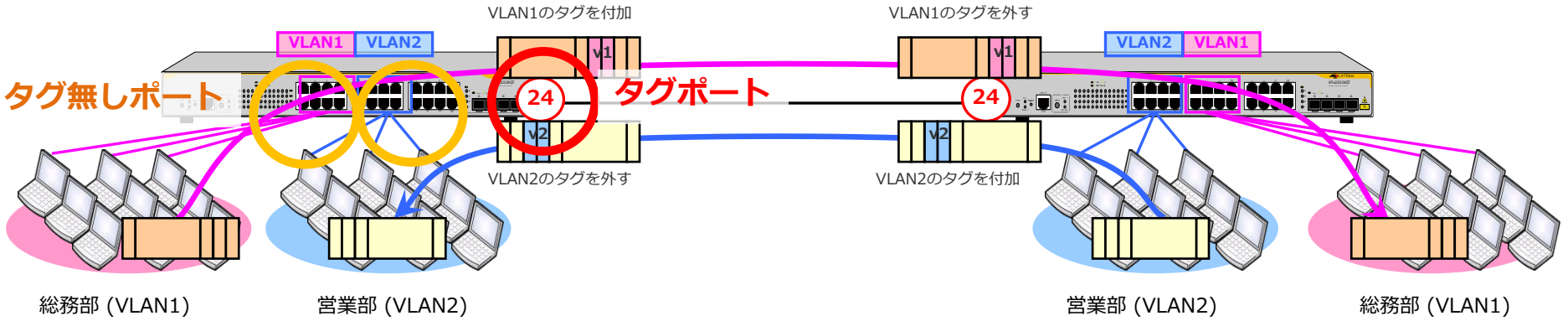


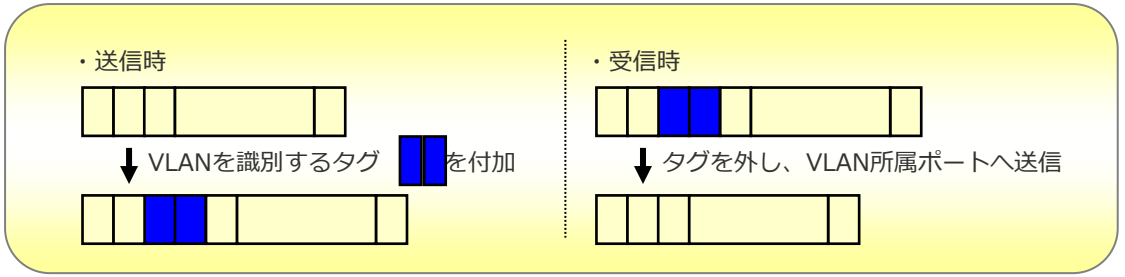
Allied Telesis

タグベースVLAN (IEEE802.1Q)

■タグベースVLAN (IEEE802.1Q)

- フレーム送出時に、VLANを識別するタグを追加することにより、1ポートで複数VLANの通信が可能です。
- タグVLANを設定しているポートは、タグポートとして複数VLANに所属可能です。
- 下図では各スイッチの24番ポートをタグポートに設定しています。

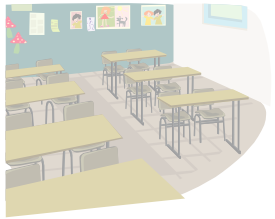




スクールネットワークの構成例

VLAN

- アクセスリストで必要なアクセスのみを許可
  - VLAN機能により生徒用と教師用のネットワークを論理的に分割し、試験問題や成績といった機密情報へのアクセスを遮断します。



生徒用VLANから教師用VLANへの
ルーティングができないように制御

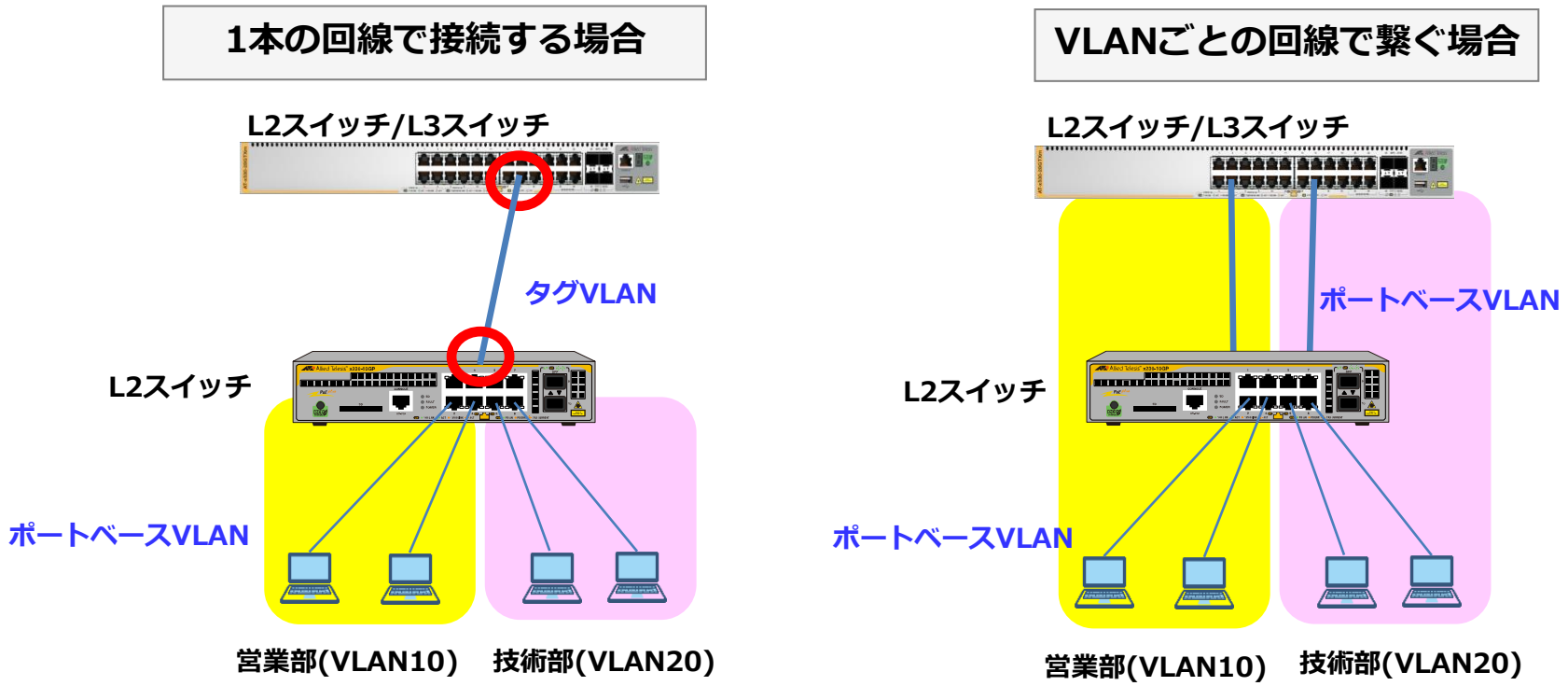
生徒はSSID“student”を使用することで
「学習系ネットワーク」へ所属

教師はSSID“teacher”を使用することで
「校務系ネットワーク」へ所属

Allied Telesis

ポートベースVLAN設定時のスイッチ間接続

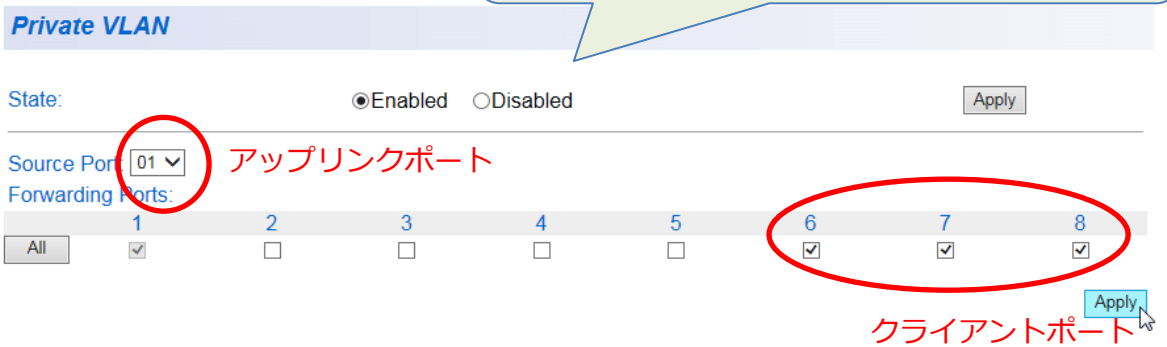
- ポートベースVLANを設定したスイッチを他スイッチと接続する場合、接続する回線数により設定するVLANが異なります。
  - 1本のケーブルで接続する場合は、そのケーブルに複数VLANのトラフィックが流れるため、スイッチ間はタグベースVLANを設定して接続します。
  - 設定されたVLANごとに別々のケーブルで接続する場合は、スイッチ間は端末と同じポートベースVLANを設定して接続します。



レイヤー２スマートスイッチ GS950シリーズのVLAN設定例

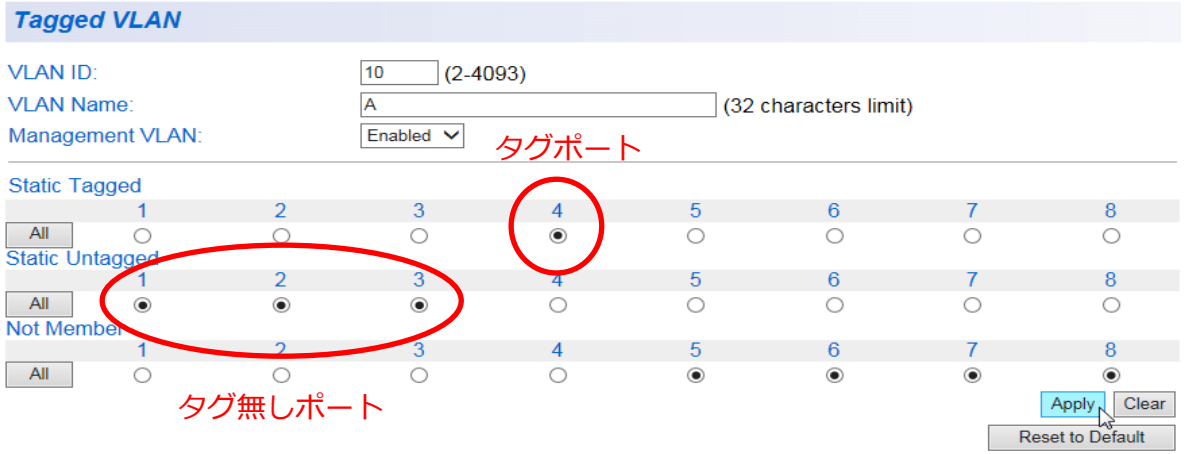
マルチプルVLAN

Web GUIの設定画面なので
操作が簡単！



アップリンクポートとクライアントポートの組み合わせ（マッピング）を複数設定することにより、マルチプルVLANの動作を実現します。

タグベースVLAN(IEEE802.1Q)



複数のVLANを複数の筐体にまたがって作成したい場合や、802.1Q対応サーバーを複数VLANから共用したい場合などに利用します。

ループ障害の脅威

- ネットワークループは身近に潜む大きな問題です。
- 人為的なミスよる誤接続が、システム全体に波及する大きな障害に発展することもあります。

未端でループ発生

↓

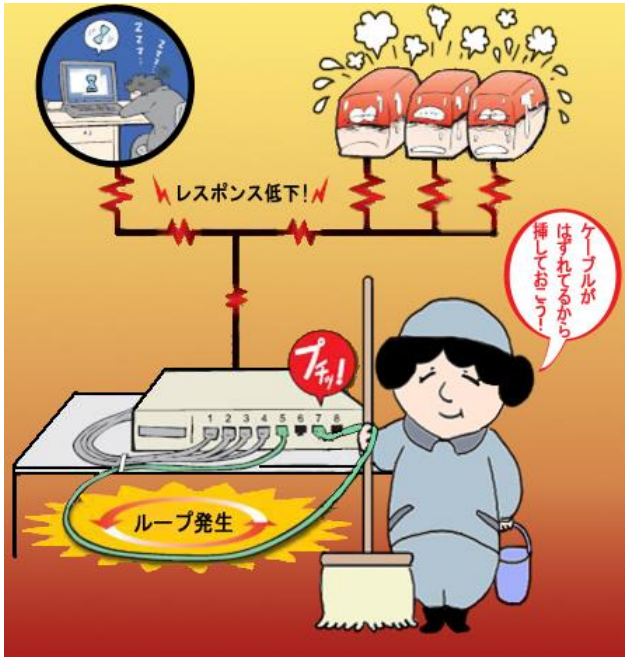
上位ネットワークに対する負荷発生

↓

サーバの応答が著しく低下

↓

サーバへの接続不可
通信継続不可

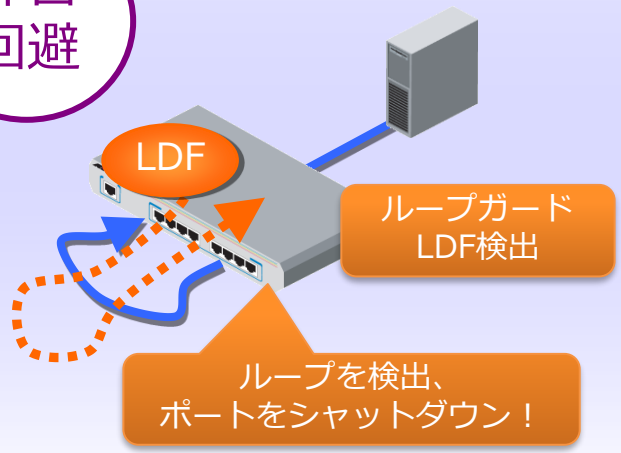


◆ループによるシステム障害の事例◆
2011年1月、東京消防庁で約4時間半にわたり119番通報が繋がりにくくなる障害が発生。
後日、LANケーブルの誤接続が原因だったと発表された。LANケーブルは予備のもので、一方の端子だけが機器に接続されていたが、職員が誤ってもう一方の端子を機器の空きポートに接続したとみられる。

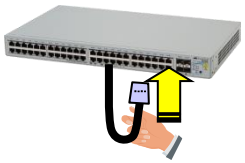
ループガードの必要性

- ループガード機能
  - 末端のスイッチにてループガード機能 (LDF検出) を使用することで、当該スイッチの配下における、ケーブルの誤接続によるネットワークグループでのネットワーク全面停止を未然に防止します。

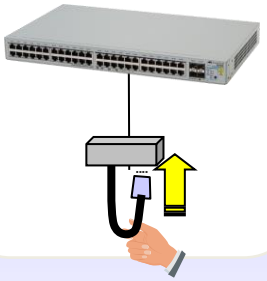
障害回避



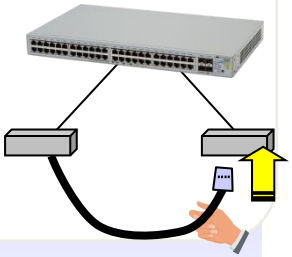
① スイッチ内でケーブル誤接続



② 配下スイッチ内でケーブル誤接続



③ 配下のスイッチ間でケーブル誤接続



上記全てのパターンでループ事故を防止可能！

フロアスイッチやエッジスイッチ等、
さまざまな機器でループ防止（LDF検出）機能をサポート

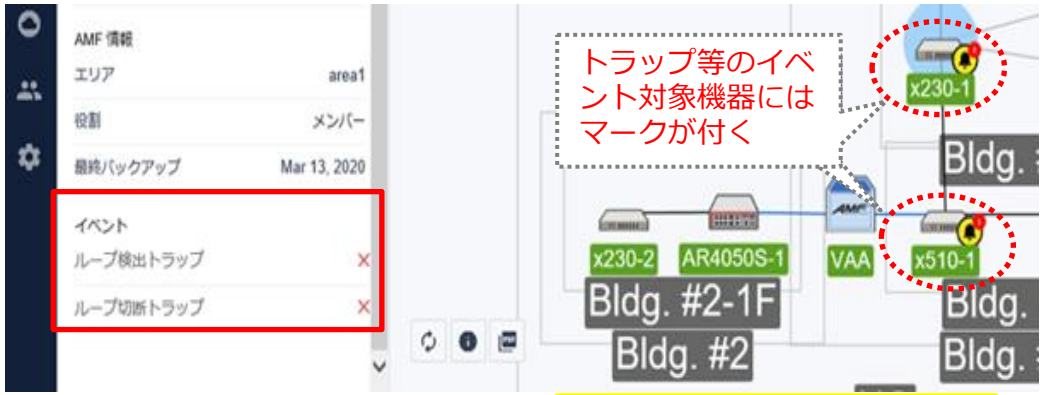
▼このマークが目印▼

ループ防止（LDF検出）機能を
搭載していることを表すマーク

ループガード(LDF)と管理マネージャとの連携

管理マネージャとの連携により、早期障害検出と障害箇所特定を容易に実現します！

- ループ発生箇所の早期発見
  - 管理マネージャとの連携により、障害の検知および、障害箇所の早期特定が可能です。



対象の機器を選択するとイベント内容を確認可能

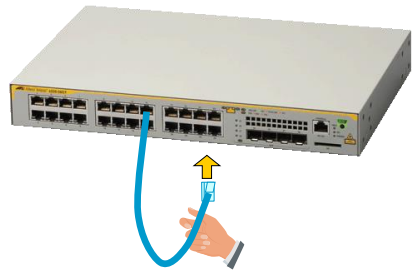
Force MDI

ポートの極性を固定することにより、誤接続によるネットワークループを未然に防止します!

- Force MDI機能
  - 主にエッジスイッチに搭載されているループ防止機能
  - ポートの極性(MDI/MDI-X)を固定設定することで、誤接続によるリンクアップを回避

- 防止可能なループ

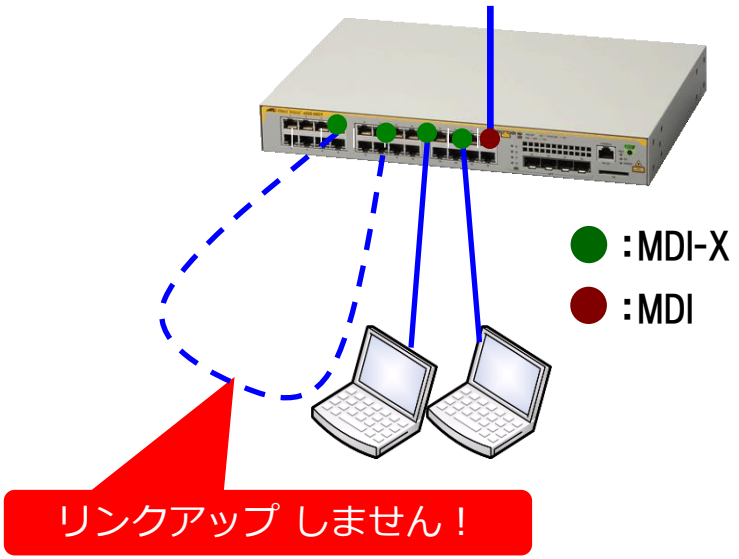
同一スイッチ内でのケーブル誤接続



ループガード機能：Force MDIの動作説明

【Force MDI】

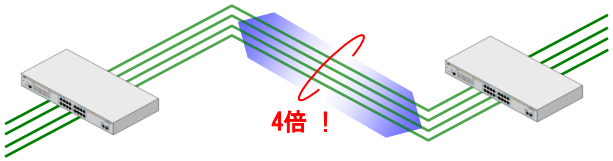
アップリンクポートはMDI固定、PC接続ポートはMDI-X固定。通常はストレートケーブルを使うため、ループは発生しない

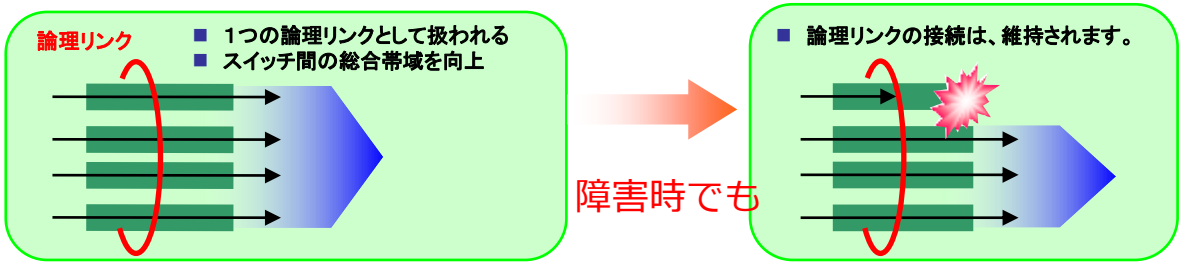


リンクアグリゲーション

LAG

- リンクアグリゲーション とは<IEEE 802.1AX-2008 （IEEE 802.3ad同等)>
  - 複数のポートをグループ化する機能
    - 冗長性　:グループ内のあるポートがDownしても他のポート経由で通信を継続
    - 負荷分散:グループ内の全てのポートを使用
  - 束ねられたポートのグループを、リンクアグリゲーショングループ(LAG)、チャンネルグループ、トランクグループと呼びます。





NOTE

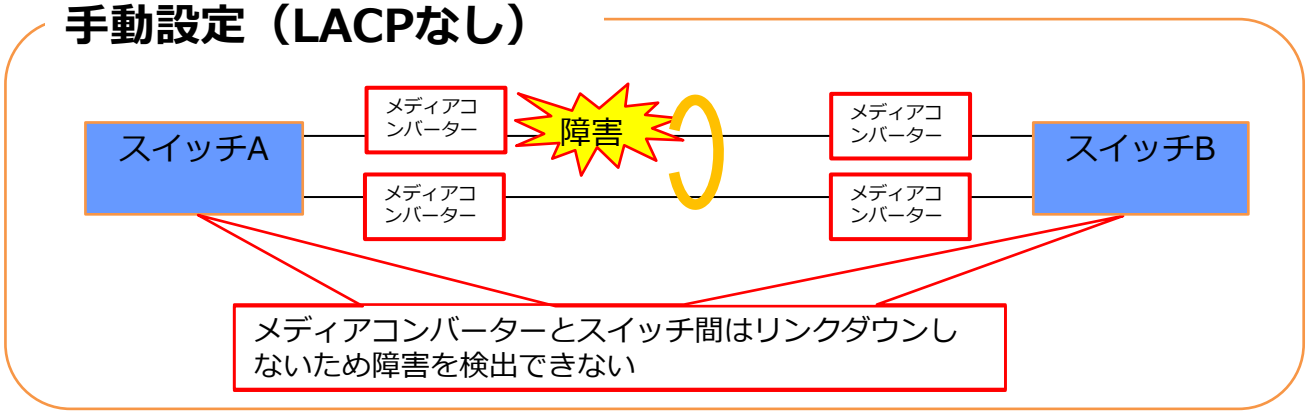
リンクアグリゲーション設定時の注意事項

・対向に接続するスイッチにおきましても、同様のリンクアグリゲーション設定が必要となります。
・トランクグループに所属するポートは、全て同じVLANに所属する必要があります。
・トランクグループに所属するポートは、全て同じタイプのメディアである必要があります。
　例: 同一トランクグループにおいて、1000BASE-SXポート、1000BASE-LXポートの混在はサポート対象外
・トランクグループ設定可能数、トランクグループ所属可能ポート数は機種により異なります。
　例：AT-x230-10GPの場合
　　グループ数:最大10グループ(手動設定・自動設定の総数)、ポート数: 8ポート/グループ

マニュアル・コンフィグレーション（手動設定）

LAG

- グループ化するポートを手動で設定する方法です。
- 機器間でネゴシエーションを行わないため、経路上にメディアコンバーター等の中継装置が介していると、障害を検知できないことがあります。
  - メディアコンバーターには、スマートミッシングリンク機能＊等の障害通知機能が必要です
- 手動設定のリンクアグリゲーションには以下の条件があります。
  - トランクグループの所属ポートは、全て同一VLAN所属、かつ、同一タグ設定(タグポートをグループ化する場合)にしておく必要があります。
  - トランクグループの所属ポートは、全て同一の通信速度・デュプレックスモードに予め設定する必要があります。
  - トランクグループ設定可能数、およびトランクグループ所属可能ポート数は機種ごとに異なります。



＊スマートミッシングリンク機能は、メタルケーブル側と光ファイバー側ポートの間で、リンク状態を中継する機能です。経路内で発生した障害を接続する機器に自動的に通知します。

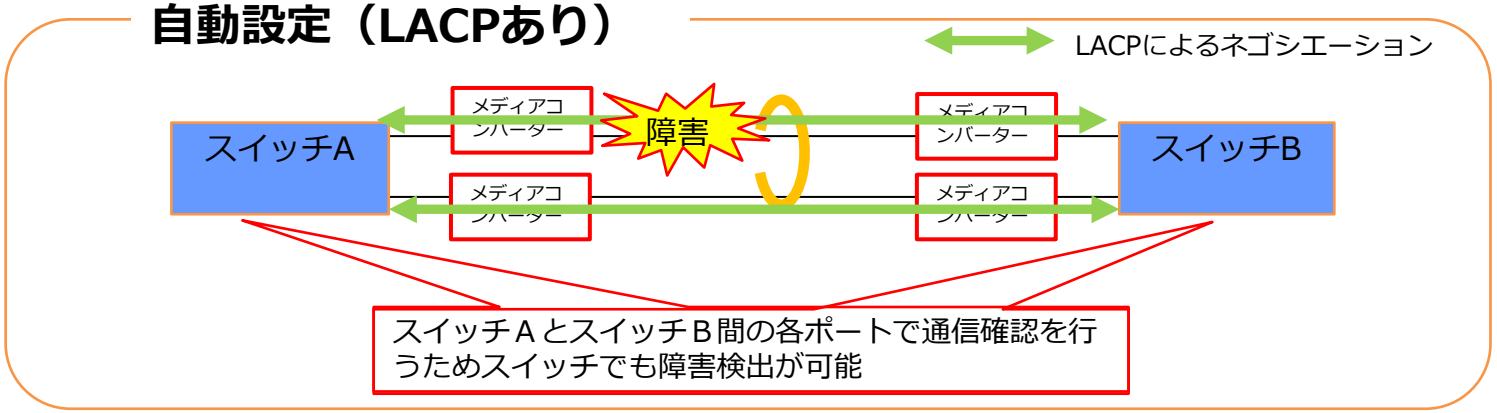
Allied Telesis

ダイナミック・コンフィグレーション（自動設定）

LAG

- LACP（Link Aggregation Control Protocol）という制御プロトコルを利用し、グループ化するポートを機器同士で自動でネゴシエーションする方法です。
- 自動設定のリンクアグリゲーションには以下の条件があります。
  - LACPでは、次の条件を全て満たすポート群が同一のトランクグループを構成する候補となります。

    同一対向機器（各ポートが同じ相手に接続されていること）、同一所属VLAN、同一タグ設定、
    同一通信速度、FullDuplexモード、同一ポート鍵（LACPポート鍵の元となるデフォルト値は1）
  - 上記の条件を満たすポートが9ポート以上ある場合は、以下の基準にしたがってメンバーポートが8ポート選択されます。（回線数はコマンド設定可能、選択外のポートはStanby）
    - ✓ ポートプライオリティーが最も小さいポート
    - ✓ ポートプライオリティーが等しい場合は、ポート番号の小さいポート
  - EPSR（リングプロトコル）との併用はできません。
  - トランクグループ設定可能数、およびトランクグループ所属可能ポート数は機種ごとに異なります。



負荷分散アルゴリズム

- リンクアグリゲーション使用時の負荷分散アルゴリズムは、送信元及び宛先のレイヤー2、レイヤー3、レイヤー4のヘッダ情報を使用して送出ポートを決定します。
  - ✓ レイヤー2ヘッダ情報（送信元及び宛先MACアドレス、VLAN ID、Ethernetタイプ）
  - ✓ レイヤー3ヘッダ情報（始点及び終点IPアドレス）
  - ✓ レイヤー4ヘッダ情報（始点及び終点TCP/UDPポート）

  ※ レイヤー2スイッチは「レイヤー2ヘッダ情報」を使用します。

- 受信フレームにIPヘッダが無い時は、レイヤー2ヘッダ情報を参照し、負荷分散を行います。また、IPヘッダがある時は、レイヤー3、レイヤー4ヘッダ情報を参照し、負荷分散を行います。このアルゴリズムはマニュアル、ダイナミックとも同様です。