「令和７年度 IT 人材育成研修会」参加報告

第１技術班　松田　翼

次期高専統一ネットワークシステムにおける知識・技能の習得を目的とした研修を受講したため報告する.

1.　実施の概要

実施日：令和７年１２月４日、５日
実施場所：東八重州シティービル、東京都中央区八丁堀 3-14-2
内容：高専統一ネットワーク機器のネットワークスイッチ、アクセスポイント、ファイアウォールの設定方法や、ネットワークの設定に必要な知識である VLAN や ACL の解説を受講した。

2.　報告

ネットワークの基礎的な考え方として、VLAN（Virtual Area Network）、SVI（Switch Virtual Interface）、ACL（Access Control List）の解説が行われた。その上で、スイッチやファイアウォールの実機に対してコンフィグを投入するハンズオン演習を受講した。

ハンズオン演習の概要としては、SVI を設定した VLAN をポート別に定義し、それぞれの VLAN 間ルーティングを有効にした上で、ポートから ping 送信を行い通信の可否を確認することで、ACL を想定通りに適用させる演習を行った。なお、ポートには本校内での実際の運用と同様に 802.1X 認証を適用させた。

ハンズオン演習では図１のとおり、２番ポートには VLAN xx、３番ポートには VLAN yy を untagged 設定した。Cisco 製スイッチがデファクトスタンダードとなっているため、Tagged（タグ付き）ポートがスイッチ同士やサーバーと接続するトランク接続ポート、Untagged（タグなし）ポートがパソコンやプリンター等と接続するアクセス接続ポートと考えるとよい。よって２番ポートは VLAN xx の機器を通すアクセスポート、３番ポートは VLAN yy の機器を通すアクセスポートとなる。４番ポートには Default VLAN を untagged し、802.1x 認証及び MAC アドレス認証を有効化した。よって、４番ポートは 802.1x 認証をクリアしたパソコンなどが接続できるアクセスポートとなる。本校内の壁コンセントのポート設定は、本演習の４番ポートと同様の設定のアクセスポートとなる。

１番ポートは上位スイッチと接続するトランクポートである。そのため VLAN xx、VLAN yy をそれぞれ tagged 設定することで、複数の VLAN タグで識別して通すことができるようにしている。

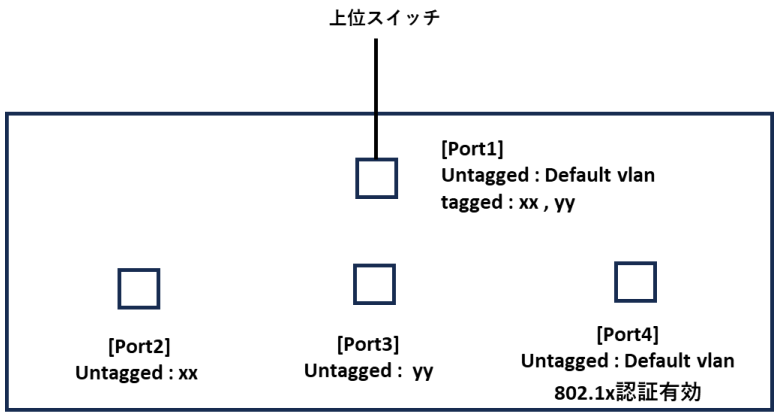

図１　ハンズオン演習でのポート設定

ファイアウォールの実機演習では、オブジェクトの作成を行った。ファイアウォールでは、IP アドレスやサブネットの設定はオブジェクトを作成することで行う。さらに、バーチャル IP のオブジェクト作成も行った。バーチャル IP は主に宛先ネットワークアドレス変換（DNAT）を行うために使用される。外部ネットワークからの通信を特定の内部サーバーなどに転送する際に、外部向けの公開 IP アドレスと内部の実際のプライベート IP アドレスを紐付ける役割を果たす。なお、IP プールのオブジェクト作成も行った。IP プールは、送信元ネットワークアドレス変換（SNAT）を行うために使用される、一つまたは複数の IP アドレスの集合である。内部から外部へ通信するファイアーウォールポリシーに IP プールを使用する。

これらのオブジェクトを使用してファイアーウォールポリシーを作成し、ping 送信を行うことでポリシーが想定どおりに適用されているか確認を行った。