# サイバーセキュリティ PBL I

高野 祐輝

2019 年 1 月 17 日

## 1　目的と評価方法

**最優**　ファイアウォール技術とペネトレーションテストを組み合わせて，検疫ネットワークの設計と構築を行うことができる

**優**　ファイアウォール技術で DeMilitarized Zone のあるネットワーク設計と構築を行うことができる

**良**　ファイアウォール技術で適切なネットワークアクセスコントロールができる

**可**　各種サイバー攻撃手法と防御手法について論じることができる

## 2　セキュリティ哲学

### 2.1　サイバーセキュリティとは何か

### 2.2　サイバーキルチェーン

[1]

### 2.3　セキュリティポリシとユーザビリティ

[2]

## 3　TCP/IP の基礎

### 3.1　OSI 参照モデル

インターネットで利用されるプロトコルは、The Internet Engineering Task Force (IETF) という標準化団体により策定され、その標準は Request for Comments (RFC) という名のオープンな仕様として発行されている。例えば、我々が利用しているインターネットプロトコルであるインターネットプロトコル バージョン 4 は、1981 年に 791 番目の RFC として策定された [3]。

IETF 以外の通信に関する標準化団体としては International Telecommunication Union Telecommunication Standardization Sector (ITU-T) や、International Organization for Standardization (ISO) が存在する。実は、1977 年から 1982 年かけて、ITU-T や ISO がコンピュータネットワークの標準通信プロトコルとして、Open Systems Interconnection (OSI) の策定を行っていた。その当時は標準的な通信プロトコルは存

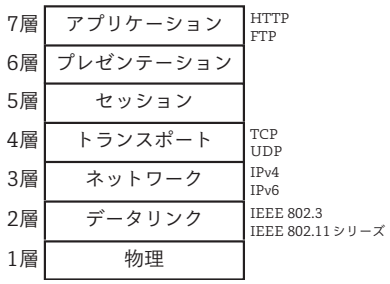


図 1　OSI 参照モデル

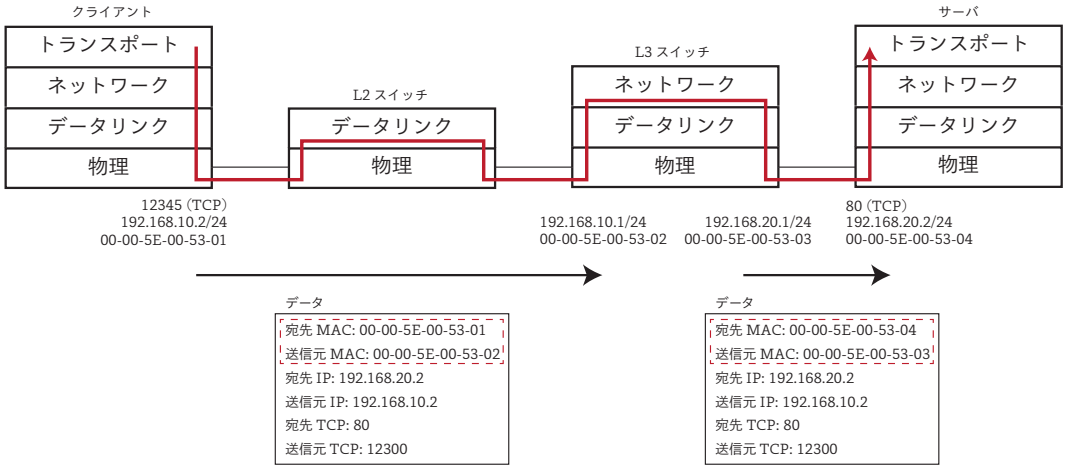


図 2　各層でのデータ転送

在せず、ベンダーごとに様々なプロトコルが利用されていたため、通信プロトコルの統一化が求められていたのである。しかしながら、最終的に OSI は主流とはならず、IETF によって策定されたインターネットプロトコルが広く利用されるようになっていった。

OSI 自体は残らなかったが、OSI 策定の際に考案された OSI 参照モデルと呼ばれるネットワークの抽象化手法は、今日でも広く受け入れられている。図 1 は、OSI 参照モデルによるネットワークの抽象化モデルを表している。OSI 参照モデルでは、ネットワークの機能を階層構造にもとづいて抽象化しており、この抽象化をレイヤリングなどと呼ぶ。OSI 参照モデルでは、下から順に 1 層に物理層、2 層にデータリンク層、3 層にネットワーク層、4 層にトランスポート層、5 層にセッション層、6 層にプレゼンテーション層、7 層にアプリケーション層が位置する。ちなみに、各層のことをレイヤ 1、レイヤ 2 といったり、更に略して L1、L2 などということもある。

図 2 は各層でデータ転送が行われている様子を示している。[*1] データリンク、ネットワーク、トランスポート層にはそれぞれアドレスがあり、各層は、そのアドレスに基づいて転送を行う。データリンク層のアドレスは 42 ビットで表され、文字で表現すると 00-00-5E-00-53-02 といった表記になる。図 2 中で宛先 MAC と示される値は、データリンク層の宛先 MAC アドレスを示している。なお、MAC は Media Access Control の略である。データリンク層は、ローカルなネットワークでの通信を行うために用いられる。そのため、MAC

[*1] この図の意味することは現時点では理解できないかもしれないが、この図の意味することろを説明するのが本節の目標であるため、現段階で理解できなくても問題ない。

アドレスはそのローカルな環境では一意に識別できる必要がある。データリンク層の詳細については 3.2 節で解説する。

ネットワーク層のアドレスは、192.168.10.2/24 で表される 32 ビットの IP アドレスとなり、/24 はネットワークのサブネット長を示している。図 2 では、192.168.10.0/24 と 192.168.20.0/24 というサブネットが示されている。ネットワーク層、すなわち IP は、全世界で通信を行うために用いられるプロトコルであり、基本的には IP アドレスは世界で一意に識別できるように割り当てるのが設計理念となっている（現実的にはそうはなっていないが)。なお、前述のアドレスは IPv4 アドレスであるが、IPv6 の場合は 128 ビットのアドレス空間を持つ。ネットワーク層の詳細については 3.3 節で解説する。

トランスポート層のアドレスは 16 ビットで示され、一般的にポート番号と呼ばれ、TCP や UDP はポート番号をもとにアプリケーションプロセスの識別を行う。よく利用されるポート番号は、インターネット上で利用される識別情報の管理割当を行っている Internet Assigned Number Authority (IANA) が定義しており [4]、一般的にこのようなポート番号を Well Known ポート番号と呼ぶ。例えば、TCP の 80 番ポートは HTTP で利用され、普段我々が Web を閲覧する際は、Web ブラウザが Web サーバの TCP80 番ポートへ接続する。

図 2 では、クライントからサーバの TCP80 番ポートへむけて通信を行っている様子を示している。一般的に、インターネット上の通信ではデータ中に含まれる各層のアドレスをもとに、L2 または L3 スイッチが転送を行う。L2 スイッチのことをスイッチングハブといったり、L3 スイッチのことをルータということもあるが、本書では L2 スイッチ、L3 スイッチと呼ぶことにする。この図が示すように、L2 スイッチ、L3 スイッチによってデータが転送されても、データ中の IP アドレスとポート番号は変わらないが、MAC アドレスは L3 スイッチでの転送時に更新される。これは、MAC アドレスはローカルなネットワーク内でのみ通用するアドレスであり、L3 スイッチはローカルなネットワーク同士をつなぎ合わせる役割を持っているためである。以降の節では、データリンク、ネットワーク、トランスポートの動きについて詳しく説明する。

**重要ポイント**

- インターネット関連のプロトコルは、IETF が発行する RFC によって標準化されている
- コンピュータネットワークはレイヤで考えることができる

参考文献

[1] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, Vol. 1, p. 80, 2011.

[2] B. Fraser. Site security handbook, September 1997. RFC2196.

[3] J. Postel. Internet protocol, September 1981. RFC0791.

[4] Internet Assigned Number Authority (IANA). Service Name and Transport Protocol Port Number Registry. https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.