

サイバー戦入門 その〇

～コンピュータとネットワークの基礎～

三村 守（防大情報工学科）

1 はじめに

サイバー戦の舞台であるサイバースペースの重要性は広く認知され、世界中の様々な組織がその活用に入力している。日常生活ではスマートフォン、IoT¹機器等のスマートデバイスが普及し、サイバースペースの影響は個人にまで急速に拡大している。今や、個人がサイバー攻撃を受け、マルウェア²に感染して知らない間に情報を盗み取られたり、脅迫を受けたりすることは珍しくない。このような状況に伴い、サイバーセキュリティあるいは情報セキュリティに関する教育も実施される機会が増えてきている。しかしながら、サイバーセキュリティに関する教育では専門用語が使用されることも多く、これらの用語に馴染みのない入門者からは内容が難しいとの声が散見されている。

情報化社会においては、これらの専門用語を検索エンジンや用語集を活用して検索することで、容易に意味を調べることができる。したがって、耳慣れない専門用語については、学習者が自らの意思で対応することが可能であり、理解を妨げる致命的な要因にはならないものと考えられる。しかしながら、難解な専門用語の意味を調べたとしても、コンピュータやネットワークの基礎的な仕組みや考え方を習得していなければ、その意味の理解は困難である。インターネットを活用して瞬時に情報を検索できる今日では、言葉で表現することが容易な形式的な知識よりも、内容の理解やスキルといった言葉で表現することが難しい暗黙知を習得する方が重要である。サイバーセキュリティに関する基礎的な内容を理解するためには、その土台となっているコンピュータやネットワークの基礎的な仕組みや考え方の理解が不可欠である。サイバースペースは、その末端や結節点を構成するコンピュータと、それらを結ぶネットワークによって構成されている。したがって、これらの素養なくして、サイバーセキュリティに関する基礎的な講義を受けたとしても、その内容を理解することは困難である。基礎的なサイバーセキュリティに関する教育の内容を難しいと感じる入門者には、コンピュータやネットワークの基礎的な仕組みや考え方を習得していない者がほとんどであると考えられる。

そこで本稿では、このような入門者を対象として、サイバーセキュリティに関する基礎的な内容を習得するために必要な、最低限のコンピュータやネットワークの仕組みや考え方を説明することを試みる。以下、第2節ではコンピュータの

¹ IoT (Internet of Things) 様々な物が共通の仕組みでインターネットに接続されて相互に情報交換する概念等の総称

² コンピュータウイルス等の不正プログラムの総称

仕組みの概要について説明する。第3節では、ソフトウェアとハードウェアの種類について説明する。第4節ではネットワークの仕組み、第5章では仮想化技術の基礎について説明し、最後にまとめと課題について述べる。

2 コンピュータの仕組み

本節では、サイバースペースの末端や結節点を構成するコンピュータの基本的な仕組みについて説明する。サイバースペースを構成するコンピュータには様々な種類があり、その代表的な機器であるスマートフォン、IoT機器等も同じような仕組みで動作している。ここで、一般的なパソコンを例としてその仕組みを説明する。コンピュータの内部では、すべての情報はビットと呼ばれる0か1の2進数のデータで処理される。物理的には、これらのデジタルデータは電子計算機であれば電圧の高低、ハードディスクであれば磁気の方角、CDやDVDであれば表面の凹凸等によって表現される。2進数で構成されたデータは膨大な長さとなるため、図1に示すように $4 \times 2 = 8$ 桁をひとくくりとして2桁の16進数で表現されることが多い。

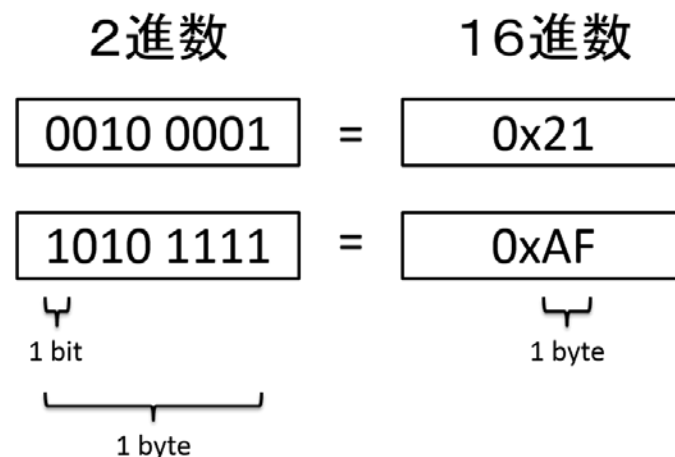


図1：2進数と16進数

16進数において、10～16の数字はA～Fのアルファベットで表現される。「0x」は、以降が16進数の表記であることを示す記号である。この2桁の16進数は、バイトと呼ばれる。つまり、1バイトは8ビットで表される。これらのデータは、コンピュータを構成するCPU³、メモリ、ハードディスク、SSD⁴等の基本的な装置によって処理される。図2にコンピュータの概要を示す。

³ CPU (Central Processing Unit)

⁴ SSD (Solid State Drive)

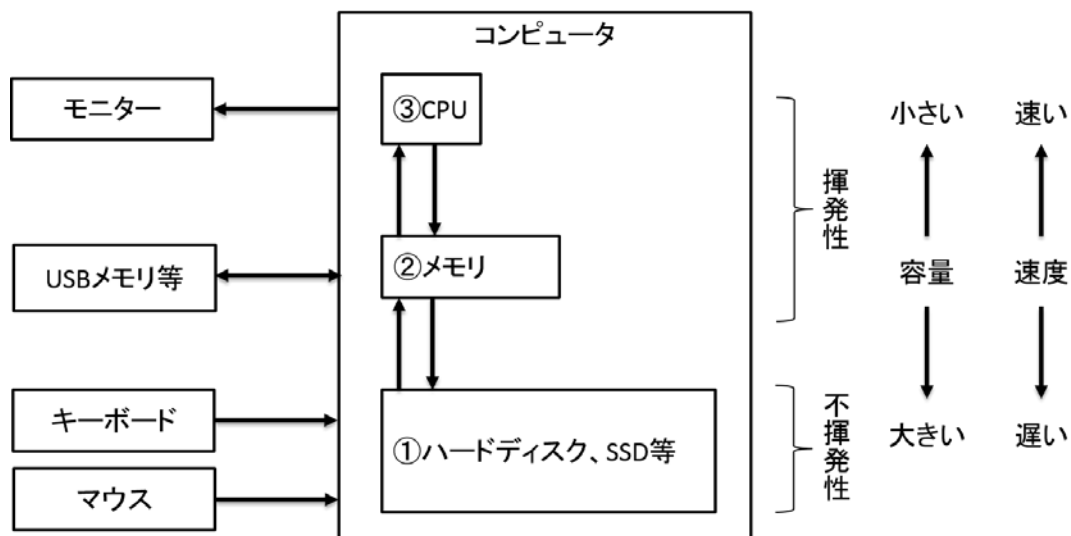


図 2：コンピュータの概要

（１）内部の仕組み

まず、コンピュータの内部について説明する。コンピュータにおいて、主なデータはハードディスク、SSD等の補助記憶装置（図2①）に保存されている。ハードディスク（HDD⁵）は、磁気を用いて大容量の情報を記録して読み書きする補助記憶装置の一種である。SSDは、後述するメモリと同等の仕組みで動作するより高速な補助記憶装置である。これらの補助記憶装置に保存されたデータは、電源が切れても保持され、この性質は不揮発性と呼ばれる。補助記憶領域に保存されたデータは、メモリ（図2②）に呼び出された後、CPU（図2③）によって処理される。メモリは、CPUで処理するデータを一時的に記憶する装置であり、主記憶装置とも呼ばれる。CPUは、コンピュータにおいて中心的に命令を実行する装置であり、中央演算装置あるいはプロセッサとも呼ばれる。メモリおよびCPUに一時的に記憶されたデータは、一般に電源が切れると失われ、この性質は揮発性と呼ばれる。なお、ハードディスク、メモリ、CPUの順に記憶できるデータの容量は小さくなり、逆に速度は速くなる。つまり、メモリは効率的にデータを処理するため、緩衝材のような役割を果たしている。

（２）外部の仕組み

次に、コンピュータの外部について説明する。コンピュータに対する指示は、マウスやキーボード等の入力装置を介して伝えられる。これらの入力装置の動作は電氣的信号に変換され、データとしてコンピュータに処理される。コンピュータに対する指示の実行結果は、モニター等の出力装置を介して確認することができる。コンピュータは、指示の実行結果を人間が分かりやすいように視覚化してモニター等に出力する。コンピュータ内部のデータは、USBメモリ、ネットワーク等を介して他のコンピュータと相互にやり取りされること

⁵ HDD (Hard Disk Drive)

もある。このような複雑なコンピュータの動作は、様々なソフトウェアによって実現されている。

3 ソフトウェアとハードウェア

本節では、コンピュータの複雑な動作を実現するソフトウェアとハードウェアの種類について説明する。

(1) ソフトウェアとハードウェアの概要

第2節では、コンピュータを構成する物理的な構成要素であるハードウェアについて説明した。ハードウェアはいわば機械であり、その機能を出荷後に修正することは難しい。そこで、出荷後に修正を要する機能はソフトウェアを用いて実現される。ソフトウェアは、ハードウェア上で動作する論理的なプログラムのことである。ハードウェアとソフトウェアの概要を図3に示す。

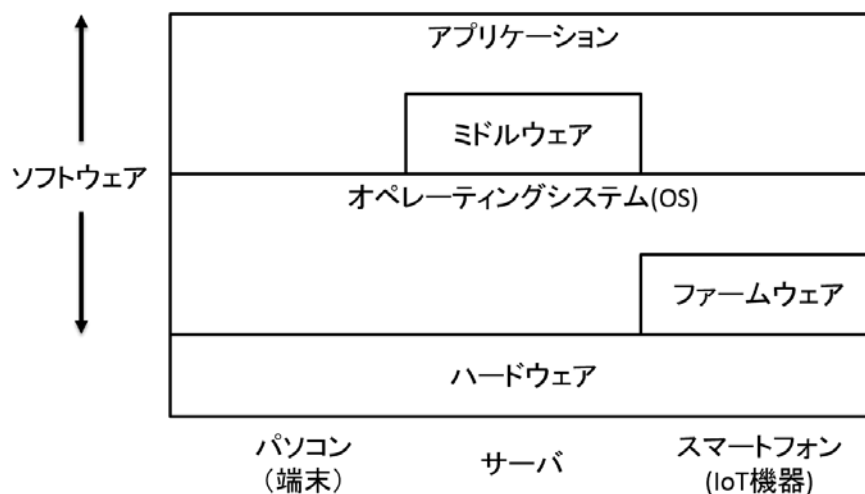


図3：ソフトウェアとハードウェアの概要

図3に示すとおり、ソフトウェアには様々な種類がある。

最も基本的なソフトウェアは、オペレーティングシステム（OS）と呼ばれるコンピュータ全体を管理するソフトウェアである。OSの種類はパソコン、サーバ⁶、スマートフォン等、機器の種類によって異なるため、基本的にOSはそのハードウェアと異なる種類のハードウェア上では動作しない。例えば、パソコンであればWindowsやMac OS、スマートフォンであればAndroidやiOS⁷がその代表例である。パソコン向けのWindowsやMac OSは、基本的にスマートフォン上では動作しない。なお、

⁶ 何らかのサービスを提供するコンピュータのこと。例えば、接続してきたコンピュータにホームページ等のコンテンツを提供するWebサーバや、郵便局のように電子メールを配送するメールサーバがある。

⁷ iPhoneに搭載されているOS

スマートフォンやI o T機器においては、OSとハードウェアの間にファームウェアという電子機器の制御プログラムが動作していることが多い。また、主にサーバにおいては、OS上にミドルウェアと呼ばれるアプリケーションに共通の機能を提供するプログラムが動作していることもある。

各OS上では、アプリケーションと呼ばれる各々の業務に応じたプログラムが動作している。例えば、ワープロ、表計算、プレゼンテーション等を実現するMS Office等のプログラムは、このアプリケーションに分類される。アプリケーションは、基本的にそのOSやハードウェア上でのみ動作するプログラムであり、他のOSやハードウェア上では動作しない。

このように、図3において上位のソフトウェアは、下位のソフトウェアやハードウェアに依存している。

(2) ファイルの種類

OSの一部およびアプリケーションは、ファイルと呼ばれるデータの論理的な集まりによって表現されている。ファイルには、実行ファイルとそれ以外のファイルがある。Windowsを例とした場合の両者の違いを図4に示す。



	実行ファイル (プログラム)	それ以外のファイル
アイコン		
具体例	メモ帳、電卓 スタートメニューから実行 するプログラム等	テキスト、ワード、エクセル、 パワーポイント、一太郎の ファイル等
拡張子	exe	docx, doc, xlsx, xls, ppt, pptx, pdf jtd等
特徴	単独で実行可能	実行には他の実行ファイル (プログラム)が必要

図4：Windowsにおける実行ファイルとそれ以外のファイルの違い

実行ファイルは単独で実行可能なプログラムのことであり、プログラムとも呼ばれる。Windowsに付属するメモ帳、電卓等のプログラムや、スタートメニューから実行されるアプリケーションの本体がその代表例である。それ以外のファイルは、単独で実行することが不可能であり、他のプログラムから呼び出されるファイルである。例えば、テキストファイルは、プログラムであるメモ帳から呼び出すことで内容を編集することができる。ワード、エクセル、パワーポイント等のファイルは、MS Office等のプログラムから呼び出される。

不正アクセス等に用いられるマルウェアに関しては、その本体は実行ファイルであることが多い。したがって、出所が不明な未知の実行ファイルについて

は、実行の可否、つまりダブルクリックするか否かを十分に検討する必要がある。スマートフォンにおいては、アプリケーションをインストールする際に、その出所や要求するアクセス権に十分注意する必要がある。

(3) 実行ファイルとソースコード

アプリケーションやマルウェアの本体は、実行ファイルであることが多い。その実行ファイルは、通常はプログラム言語を用いて作成される。プログラム言語には、大規模なアプリケーションの開発に用いられるC言語やJ a v a、動的なホームページの作成に用いられるP H P、人工知能やセキュリティの分野で用いられることが多いP y t h o n等様々な種類がある。

これらのプログラム言語では、人間が読みやすい形で逐次命令を記述し、所望の機能を実装する。所望の機能を実装するための具体的な動作手順は、アルゴリズムと呼ばれる。プログラム言語で記述された命令群はソースコードと呼ばれ、そのままでは実行することはできない。これを実行するためには、実行ファイルの形式に変換する必要がある。この変換のことをコンパイルと呼び、変換を実施するプログラムをコンパイラと呼ぶ。実行ファイルとソースコードの関係を図5に示す。

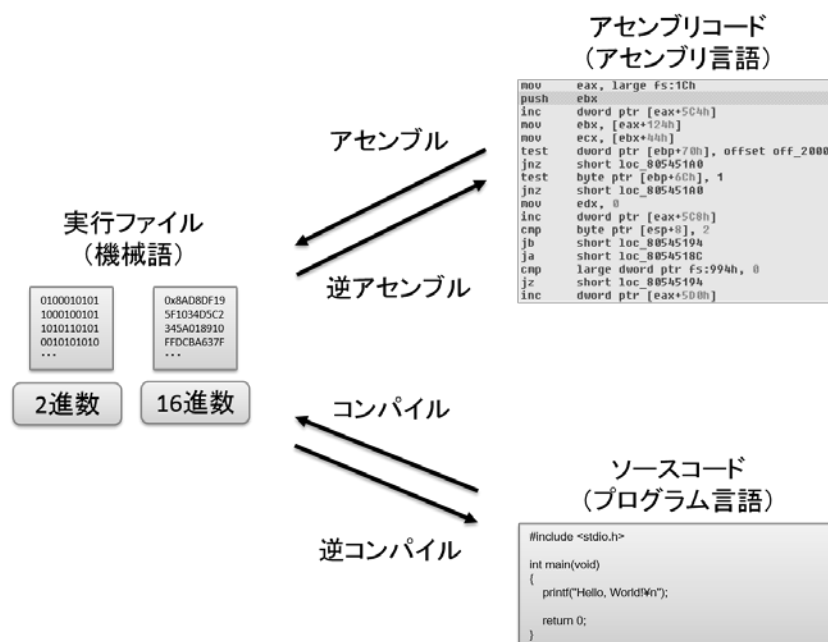


図5：実行ファイルとソースコードの関係

実行ファイルは、CPUに対応した機械語で記述されており、その中身は2進数あるいは16進数で表現される。例えば、最も一般的なIntel社製のCPUであれば、x86と呼ばれる機械語が用いられている。機械語は人間から見ると単なる数字の羅列であり、その意味を覚えることは難しい。この機械語には、mov（ムーブ）、push（プッシュ）、inc（インクリメント）等の1対1に対応した人間にも覚えやすい表記の命令が存在する。その機

機械語と1対1に対応した命令は、アセンブリ言語と呼ばれる。実行ファイルは、このアセンブリ言語を用いて作成することもできる。ただし、アセンブリ言語はプログラム言語に比べ、より詳細で膨大な命令を記述する手間がかかるため、一般にアプリケーションの開発に用いられることは少ない。アセンブリ言語を用いて記述された命令群はアセンブリコードと呼ばれ、実行ファイルに変換することができる。この変換のことをアセンブルと呼び、変換を実施するプログラムをアセンブラと呼ぶ。

アプリケーションやマルウェアについては、実行ファイルのみが利用者に配布され、ソースコードはその開発者が保有している場合がほとんどである。したがって、マルウェアのようにその機能の詳細を分析する必要がある場合には、実行ファイルをアナリストが読みやすいようにアセンブリコードやソースコードに変換する必要がある。この変換は逆アセンブルあるいは逆コンパイルと呼ばれ、専用の特別なプログラムを用いて実施される。

4 ネットワークの仕組み

本節では、サイバースペースの末端や結節点を結ぶネットワークの基本的な仕組みについて説明する。

(1) ネットワークの階層

アナログ電話のような伝統的な通信方式とコンピュータを結ぶネットワークの違いの一つとして、階層という考え方が挙げられる。図6にネットワークの階層を示す。

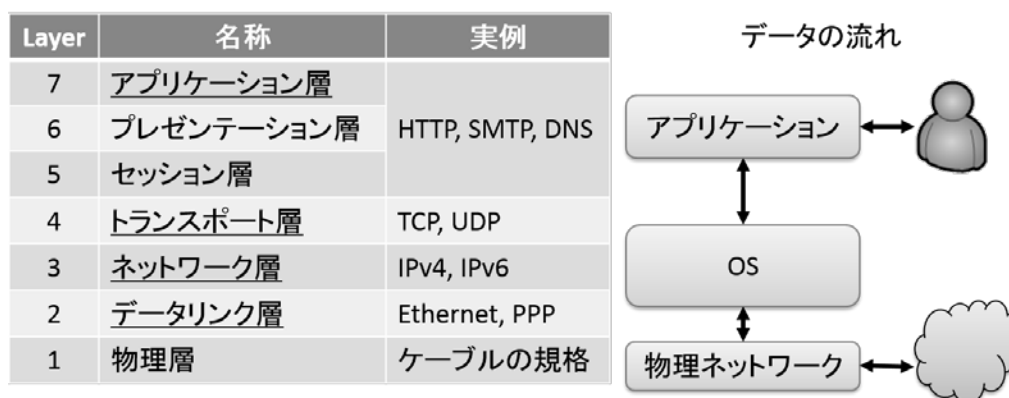


図6：ネットワークの階層

この階層はOSI⁸参照モデルと呼ばれており、実際の通信規約はこの階層で定められた役割に従って実装されている。Webブラウザ⁹等のアプリケーションは利用者からの命令を受け、そのデータはOSを経由してネットワークに流れる。反対にネットワークから受信したデータはOSを経由し、アプリケーション

⁸ OSI (Open Systems Interconnection)

⁹ IE (Internet Explorer)、Chrome、Safari 等のホームページを閲覧するためのソフトウェア

ョンによって視覚化されて利用者に認識される。

第1層の物理層は、ケーブルのコネクタのピンの数、形状、電位信号等の物理的な企画を定めたものである。

第2層はデータリンク層と呼ばれ、直接的に接続されている機器の物理的な宛先、伝送方式等について定めている。最も一般的なパソコンに用いられている方式は、イーサネットと呼ばれている。伝統的な電話回線を利用する場合には、PPP¹⁰と呼ばれる方式が用いられることもある。

第3層はネットワーク層と呼ばれ、ネットワーク全体における論理的な宛先、通信経路等を定めている。具体的には、IPバージョン4やこれを拡張したバージョン6が用いられている。現在のインターネットでは、IPバージョン4が用いられている。

第4層はトランスポート層と呼ばれ、通信するコンピュータ同士のポート番号等の管理を実施する。ポート番号とは、Web、メール等のサービスの種類を区別するために用いられる番号であり、0～65535の数字で示される。ポート番号を使用する主な通信規約は、TCP¹¹およびUDP¹²である。TCPは1対1で接続を確立し、データの送達の確認、欠損データの再送、エラー訂正等の機能を持つ信頼性の高い通信規約であり、多くのアプリケーションに用いられている。これに対しUDPには接続という概念がなく、データの送達を確認しない。UDPは、動画のストリーミング等のように、信頼性よりも即時性が求められる場合に用いられる。

第5～7層はアプリケーション層としてひとくくりにされることが多く、ここでWeb、メール等の様々な通信サービスを規定する。具体的には、Webサービスを提供するHTTP¹³、電子メールを提供するSMTP¹⁴、ドメイン名をIPアドレスに変換する名前解決を行うDNS¹⁵等が挙げられる。これらのサービスは、表1に示すように、下位の層では決まった通信規約や宛先ポート番号を用いる。

¹⁰ PPP (Point-to-Point Protocol)

¹¹ TCP (Transmission Control Protocol)

¹² UDP (User Datagram Protocol)

¹³ HTTP (Hyper Text Transfer Protocol)

¹⁴ SMTP (Simple Mail Transfer Protocol)

¹⁵ DNS (Domain Name Service)

表 1：主なサービスの通信規約とポート番号

通信規約	トランスポート層	宛先ポート番号	用途
F T P	T C P	2 0 ～ 2 1	ファイルの転送
S M T P	T C P	2 5	メールの送信
D N S	U D P ／ T C P	5 3	名前解決
H T T P	T C P	8 0	W e b
P O P 3	T C P	1 1 0	メールの受信
I M A P	T C P	1 4 3	メールの受信

(2) パケットの構造

ネットワークを流れるデータは、パケットと呼ばれる単位に小分けにされて宛先に届けられる。ネットワークを流れるパケットの構造を図 7 に示す。

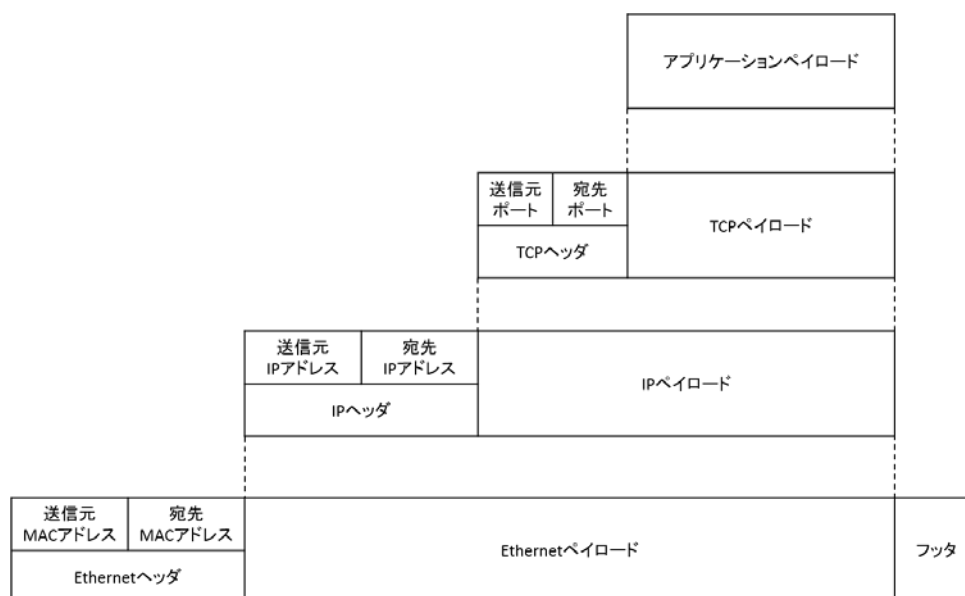


図 7：パケットの構造

パケットは、ヘッダ、フッタおよびペイロードから構成されている。ヘッダおよびフッタには、そのデータをどのように扱うべきかを示した情報が記述されている。ペイロードは、そのパケットの中身である。ヘッダはパケットの先頭から各階層に対応して付与されており、ペイロードには上位の階層のヘッダも含まれている。ネットワーク機器やパソコンでは、各階層のヘッダに記載された情報からそのパケットの物理的な宛先を示すMACアドレス¹⁶、論理的な宛先を示すIPアドレス、ポート番号等を判断して処理する。

(3) パケット配送の仕組み

次に、直接的に接続されている機器の物理的な伝送方式について説明する。

¹⁶ MAC(Media Access Control) アドレス

図 8 に直接的に接続されたコンピュータの例を示す。

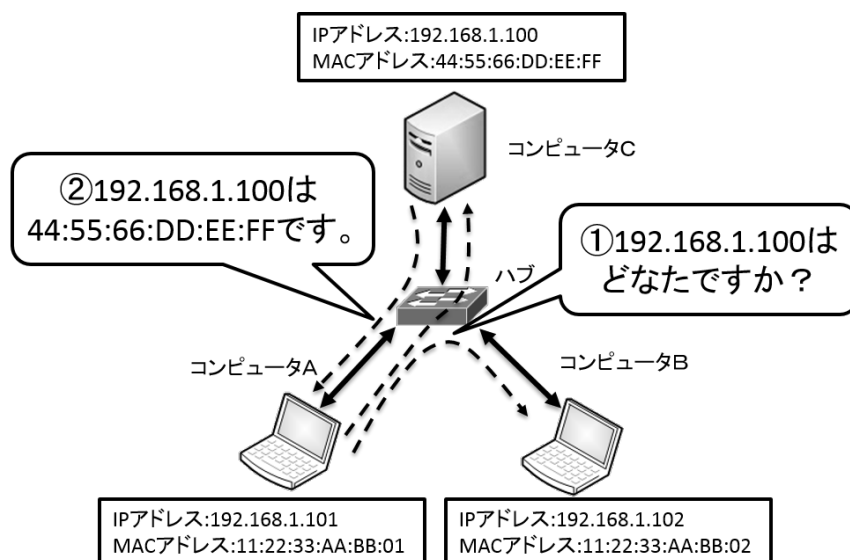


図 8：直接的に接続されたコンピュータ

この例では、3 台のコンピュータが、中央のハブ¹⁷と呼ばれる機器を経由して直接的に接続されている。ネットワークにおいて、最終的にパケットを宛先のコンピュータに配送するためには、論理的な宛先を示す IP アドレスではなく、物理的な宛先を示す MAC アドレスが必要となる。したがって、IP アドレスから 1 対 1 に対応する MAC アドレスを求める必要がある。MAC アドレスとは、ネットワーク上で各コンピュータを一意に識別するためにネットワークアダプタに割り当てられた物理アドレスであり、ハードウェアアドレスとも呼ばれる。MAC アドレスは、6 バイトの 16 進数で表記され、先頭半分の 3 バイトは製造業者を示している。

ここで、コンピュータ A からコンピュータ C にパケットを送信する場合について説明する。なお、コンピュータ A はコンピュータ C の IP アドレスを知っているものとする。コンピュータ C の IP アドレスに対応する MAC アドレスを入手するために、コンピュータ C の IP アドレス（192.168.1.100）を付与したパケットをハブに接続するすべてのコンピュータに送信（ブロードキャスト）する（図 8 ①）。ここで、192.168.1.100 の IP アドレスを持つコンピュータ C は、自身の MAC アドレスを送信元に返信する（図 8 ②）。この時、コンピュータ B は 192.168.1.100 の IP アドレスを持たないため、このブロードキャストを無視する。このブロードキャストにより、コンピュータ A はコンピュータ C の MAC アドレスを知ることができる。これらの動作は通信規約に定められており、各コンピュータはこの通信規約に基づいて動作している。以後、コンピュータ C の IP アドレスと M

¹⁷ L2 スイッチが用いられる場合もある。

ACアドレスのペアはしばらくの間保持され、パケットの配送に用いられる。なおこの時に、ブロードキャストを受信したコンピュータCは、コンピュータAのIPアドレスとMACアドレスのペアを記録する。これにより、コンピュータCはコンピュータAにパケットを配送することができる。

(4) ルーティング

次に、ネットワーク全体における論理的なパケットの配送について説明する。図9に直接的に接続されていない複数のネットワークの例を示す。

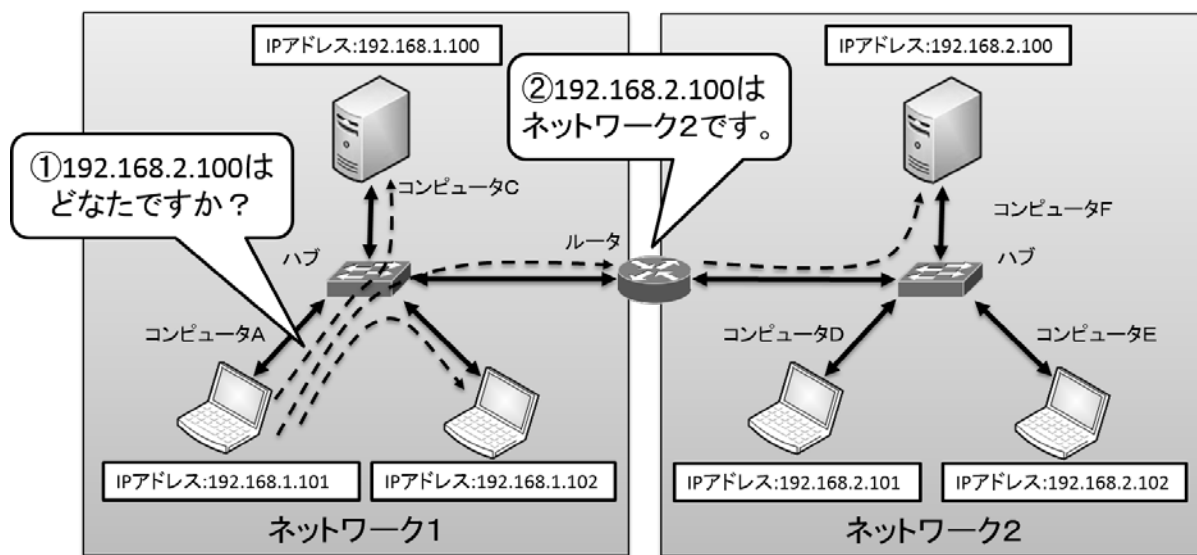


図9：複数のネットワーク

ここで、ネットワーク1に属するコンピュータAから、ネットワーク2に属するコンピュータFにパケットを送信する場合について説明する。なお、コンピュータAはコンピュータFのIPアドレスを知っているものとする。まず、コンピュータFのIPアドレスに対応するMACアドレスを入手するために、ハブに接続するすべてのコンピュータにブロードキャストする(図9①)。今回の場合には、コンピュータFはこのハブに直接接続していないため、その応答は得られない。このような場合には、あらかじめ指定したルータ¹⁸がこれを処理する。ここで、このルータにコンピュータFのIPアドレスに対応するMACアドレスが登録されている場合には、そのパケットはコンピュータFに転送される(図9②)。ルータがそのIPアドレスに対応するMACアドレスを知らない場合には、そのパケットはあらかじめ設定されたそのIPアドレスに対応する別のルータに転送される。以後、そのIPアドレスに対応する宛先が見つかるまでこの手順が繰り返される。この手順はルーティングと呼ばれており、巨大なインターネットを支える重要な仕組みとなっている。

(5) 一般的なネットワークの構成

¹⁸ デフォルトゲートウェイあるいはデフォルトルータと呼ばれる。

最後に、企業、組織等の一般的なネットワークの構成について説明する。図10に一般的なネットワークの構成を示す。

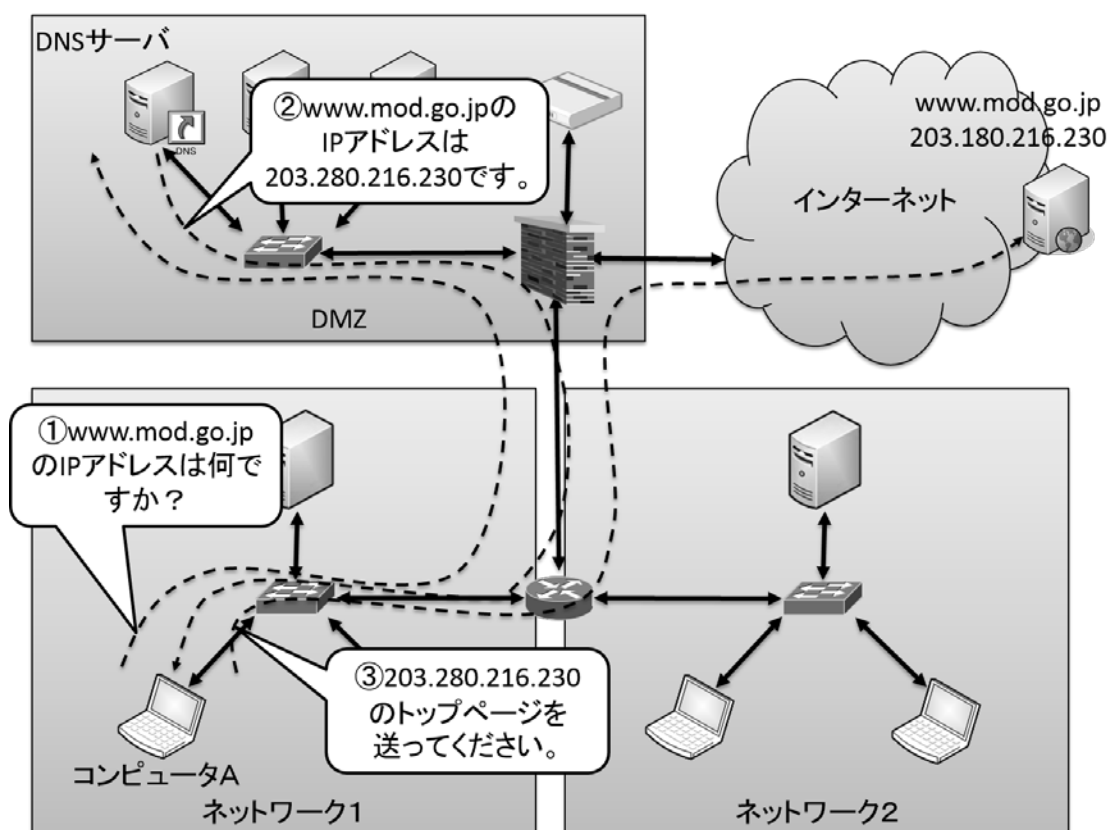


図10：一般的なネットワークの構成

このネットワークでは、利用者はネットワーク1および2に属するコンピュータを利用しており、DMZ¹⁹を介してインターネットにアクセスする。DMZとは、もともとは軍事用語の非武装地帯を示す用語であり、安全な内部のネットワークと、安全ではないインターネットの間に設けられる緩衝領域のことである。DMZには、DNSサーバ、メールサーバ、Webサーバ等の各種サービスを提供するコンピュータが設置されていることが多い。このように、何らかのサービスを提供するために常時稼動しているコンピュータをサーバと呼ぶ。これに対し、そのサービスを利用するために、サーバに接続するコンピュータをクライアントと呼ぶ。

ここで、ネットワーク1に属するコンピュータAが、インターネット上のあるホームページを閲覧する場合について説明する。まず、閲覧したいホームページのIPアドレスを、DNSサーバに問い合わせる(図10①)。これに対し、DNSサーバは対応するIPアドレスを応答する(図10②)。次に、コンピュータAは得られたIPアドレスに接続し、トップページのコンテンツを

¹⁹ DMZ (DeMilitarized Zone)

送付するように要求する（図10③）。このような手順により、コンピュータAには指定したホームページのコンテンツが表示される。この時、コンピュータAはクライアントであり、DNSサーバやコンテンツを提供するコンピュータはサーバである。

5 仮想化技術の基礎

コンピュータの仮想化にはリソースの有効活用、コスト削減、可用性の向上等のメリットがあり、クラウドに代表されるように様々な場面で用いられている。コンピュータの仮想化技術の主な分類を主に図11に示す。

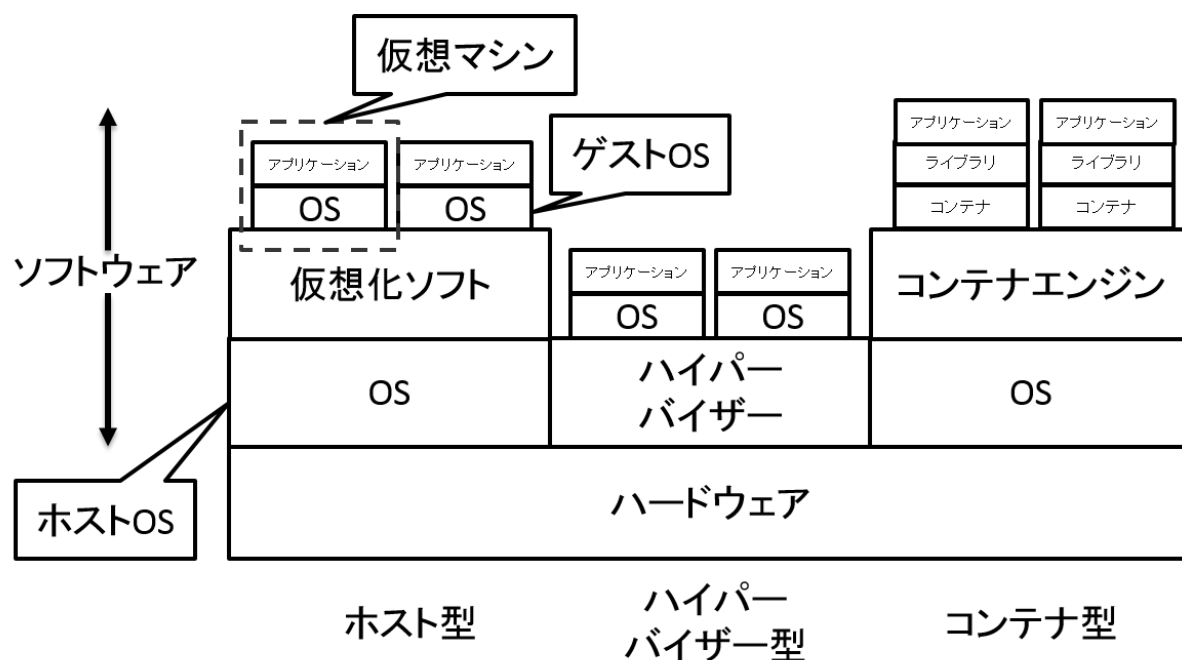


図11：仮想化ソフトの種類

VMware Player、Virtual Box等のホスト型では、OSの上に仮想化ソフト（アプリケーション）をインストールし、その仮想化ソフトで仮想マシンを作成し、そのイメージをファイルとして管理することが可能である。この時、仮想化ソフトが動作するOSをホストOSと呼び、仮想マシン上にインストールされるOSをゲストOSと呼ぶ。この方式では、コンピュータが仮想マシンとして完全に仮想化されるため、完全仮想化とも呼ばれる。完全仮想化では、仮想マシンをファイルとして手軽に管理することができ、ゲストOSがそのまま動作する等のメリットがある。しかしながら、パフォーマンスは他の方式と比べるとやや劣る傾向がある。

Hyper-V、KVM等のハイパーバイザー型は、初めから仮想マシンの動作を前提とした方式であり、ホストOSの代わりにハイパーバイザーと呼ばれるソフトウェアがインストールされる。ハイパーバイザー型では、ハードウェアの

CPUの仮想化機能を利用するため、準仮想化とも呼ばれる。準仮想化ではハードウェアに直接アクセスすることが可能であるため、パフォーマンスはホスト型と比べるとやや優れています。しかしながら、ハードウェアに直接アクセスするために、専用のドライバやOSの対応が必要となる場合がある。

Docker等のコンテナ型では、コンテナと呼ばれる分離されたアプリケーションの実行環境を作成し、独立して動作させることができる。コンテナ型ではOSを起動せず、ホストOSに対応するライブラリを読み込んでアプリケーションを起動する。そのため、起動が早く処理が軽量という特徴がある。しかしながら、コンテナはホストOSと中核部分を共有するため、同一とする必要がある。

6 おわりに

本稿では、サイバーセキュリティの入門者を対象として、基礎的な内容を習得するために必要な、最低限のコンピュータやネットワークの基礎的な仕組みや考え方を説明することを試みた。第2章ではコンピュータの仕組みの概要について説明し、第3章ではソフトウェアとハードウェアの種類について説明した。最後の第4章では、ネットワークの仕組みについて説明した。

本稿で説明した内容は、サイバーセキュリティの基礎的な内容を理解するための必須の素養である。したがって、本稿の内容を理解することができなければ、サイバーセキュリティに関する基礎的な教育を受けたとしても、その内容をきちんと理解することは困難である。本稿で説明した内容が、サイバーセキュリティに関する基礎的な内容を理解するために役立てば幸いである。

本稿で示した内容はあくまでも最低限の素養であり、著者が独自に選定した内容である。したがって、コンピュータやネットワークに関する基礎的な内容を体系的に網羅できているわけではない。さらに本稿では、正確性よりも分かりやすさを優先して説明したため、厳密には不正確な内容も含まれている。サイバーセキュリティの基礎的な内容をしっかりと習得するためには、コンピュータやネットワークに関する基礎的な内容を体系的に学ぶ必要がある。また、次々と生まれている新たな専門用語については、学習者が自発的に検索エンジンや用語集を活用して継続的に学ぶ必要がある。