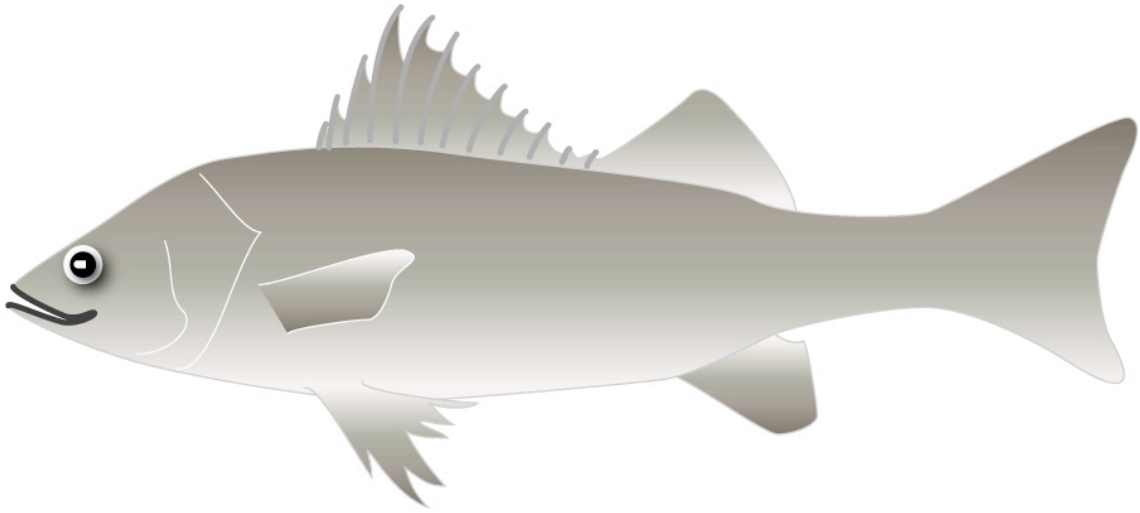

ネットワークと情報セキュリティ

安全にネットを使う基礎知識

東洋大学経営学部　　*関　勝寿*

まえがき

コンピュータシステムへの不正アクセスやフィッシング詐欺など、情報ネットワークの仕組みを悪用した事件が相次いでいる。また、各種の情報漏洩事件に見られるように、情報セキュリティ管理が適切になされていない環境下では、悪意を持たない人であっても知らないうちに他人に迷惑をかけることになりかねない。このような被害を未然に防ぐために、自宅や会社で日常的にネットワークに接続された情報機器を利用する私たちにとって、必要とされる情報技術の知識（IT リテラシー）は水準が高くなっている。しかし、情報の専門家でなければ、そのような知識を体系的に学ぶ機会は少ない。

本書では、ネットワークおよび情報セキュリティに関する知識について、情報化社会を安全に生きるために、一般の人が知っておくと役に立つ話題を中心に、若干専門的な内容にも踏み込みながら解説する。

本書は、著者が東洋大学経営学部で 2009 年度から開講している「情報処理実習 E（ネットワークと情報セキュリティ）」で使用しているテキストであり、下記のウェブサイトからダウンロード可能である。ダウンロードページには、各章の内容に関連した参考サイトをリンクしている。１章では情報倫理と情報セキュリティの大切さについて概説し、２章と３章でネットワークの仕組みについて、４章で情報セキュリティについて詳しく学習する。授業の流れに沿って章立てを編成したが、セキュリティに関する話題を中心に学習したい人は、１章と４章を最初に読み、必要に応じて２章と３章を読むと良いであろう。章末問題には、各章の内容に関連する情報処理技術者試験（主に IT パスポート試験）の過去問題を載せた。

ウェブサイト

著者のウェブサイト：http://www2.toyo.ac.jp/~seki_k/
本書のダウンロード：http://www2.toyo.ac.jp/~seki_k/security/

謝辞：表紙の絵は龍さんのフリー素材（http://www.a-ichi.com/）を使わせていただきました。

目　次

1章 情報倫理と情報セキュリティ

情報化社会の中で、情報の専門家のみならず、一般人も日常生活あるいは仕事で情報を取り扱うことが多くなっている。情報技術を活用する事で、様々な利便性を享受している一方、十分に警戒をしていないと、ネットワーク犯罪の被害を受けたり、あるいは知らないうちに自分がネットワーク犯罪の加害者となる、といった可能性がある。情報化社会を安全に生きるためには、情報倫理と情報セキュリティに関して正しい知識を持つ事が必須となっている。本章では、他人に迷惑をかけない（加害者にならない）ためのモラルである情報倫理と、ウイルスや不正アクセス、自然災害等の脅威から、重要な情報、ハードウェアやソフトウェアを守る（被害者にならない）ための情報セキュリティについて学ぶ。

学習内容とキーワード

1-1. 情報倫理：*情報発信と情報倫理、匿名性、名誉毀損、著作権、私的利用、著作物の引用、不正アクセス禁止法*

1-2. 情報セキュリティ：*コンピュータウイルス、フィッシング*

1-1. 情報倫理

【情報発信と情報倫理】

情報倫理と言っても、一般の倫理と異なる特別なものがあるわけではなく、一般の倫理をそのまま当てはめて考えれば良い。しかし、インターネットの普及により、不特定多数への情報発信が容易になったことで、情報発信にともなう情報倫理について特に意識をする必要が出て来た。インターネットが普及する前は、多くの人達に情報発信をするのは新聞、テレビ、ラジオ等のマスメディアや書籍、雑誌、映画等の出版物に限られ、情報発信には大きなコストがかかっていた。インターネットにより、ウェブサイトを開設すれば、誰でも検閲などの規制を受ける事なく、世界中の人が閲覧できるように情報発信ができることとなった。これは、言論の自由の観点からは好ましいことであるが、情報発信に伴う責任を自覚していないと、情報倫理を犯し、あるいは違法行為をする可能性もある。

そして､インターネットの普及により､ウェブサイトを構築するために HTML 言語を学ぶ、といった特殊な技術を習得することなく、ブログ、掲示板や SNS といったサイトから簡単に情報発信ができるようになった。さらに、携帯電話からもインターネットを利用できる手軽さで、子供までも情報を扱う上での被害者、加害者となっている。

情報倫理はモラルの問題であるが、法律問題とも隣り合わせとなっている。以下、情報発信に伴う情報倫理について、法律と関連づけながら考える。

【インターネットと匿名性】

「ネットでの匿名の書き込みは、誰が書いているか分からないから何を書いても大丈夫」という誤解がある。これは、２つの点で誤っている。１つ目は「匿名であれば、どんな悪い事をしても良い」という倫理そのものの問題であり、２つ目は「ネットの書き込みは匿名であり、誰が書いたかは分からない 」という思い込みである。

２章で詳しくインターネットの仕組みを学習するが、インターネットにおいて通信はサーバとクライアントとの間でなされ、その時にはお互いのネット上の住所にあたる IP アドレスの情報を交換する。掲示板に書き込みをすると、通常は書き込みをした Web サーバに書き込みをしたクライアントの IP アドレスが記録される。また、通信をしたプロバイダにも通信の記録が保存される。掲示板の管理者、掲示板を設置している Web サーバの管理者、Web サーバが設置されているインターネットサービスプロバイダ、等の記録をたどれば、どの PC から書き込みをしたのかを調査することができる。正当な理由がなければ、通常は IP アドレスの開示には応じないが、情報倫理、法律に反する書き込みがあった時には、たとえば名誉毀損の被害を受けた人から、こういった関係者に直接、あるいは警察、裁判所を通して発信者の情報開示を求めることができる。書き込みをした PC あるいは携帯電話の IP アドレスがわかれば、警察がプロバイダに問い合わせることで、発信者の身元を特定できる。

ネットの掲示板に爆破予告を書き込むと、すぐさま書き込んだ人が特定して逮捕されるのは、このような理由による。SNS の日記に友達の悪口を匿名で書いた程度で、即座に警察が動く事はめったにないとはいえ、本来ネットに匿名性はないということをよく理解して、匿名で発信する時にも、実名で発信するのと同じ程度の慎重さを持つ事が重要である。

【名誉毀損】

ネット掲示板の書き込みが名誉棄損にあたるとして逮捕されたというニュースも、いまや珍しいものではなくなっている[1]。名誉毀損とは、他人の名誉を傷つける行為であり、不法行為として損害賠償請求の民事訴訟をされることと、名誉毀損罪（刑法 230 条 1 項）として刑事罰の対象となることがある。不法行為としての名誉毀損は、人が、品性、徳行、名声、信用その他の人格的価値について社会から受ける客観的評価（社会的評価）を低下させる行為をいう 。刑法では、具体的事実を摘示することにより、ある人の社会的評価を低下させた場合、名誉毀損罪となる。

インターネット上でラーメン店チェーン運営会社を中傷する書き込みをしたとして、名誉棄損罪に問われた会社員について、最高裁判所は 2010 年 3 月 15 日に、被告側上告を棄却し、罰金 30 万円とした二審の逆転有罪判決が確定した。ネット上の個人表現での名誉棄損罪の 成立について、最高裁判所は「ほかの表現手段と比べ、より緩やかな要件を適用すべきではない」とした 。ネット情報は不特定多数が瞬時に閲覧可能で、被害が深刻な場合もあり得ることや、ネット上の反論で名誉回復が図られる保証はない点を考慮 して、メディア報道などと同じ基準で判断すべきだとした。

【著作権】

インターネット上に情報発信をする時には、著作権法違反とならないように注意する必要がある。著作権法第 2 条では、「著作とは、思想又は感情を創作的に表現したものであって、文芸、学術、美術又は音楽の範囲に属するものをいう。」とされる。著作権は著作をした時点で自動的に発生する。©マークがなくても良い。

著作権法では、「公衆によって直接受信されることを目的として無線通信又は有線電気通信の送信を行う」ことを公衆送信と言う。インターネットに接続した Web サイトは自動公衆送信に該当し、出版と同様になる。したがって、他人の著作物を掲示板に投稿する等によって Web サイトに公開すると、著作権侵害となる場合がある。

著作権法第 30 条では、著作物は、「個人的に又は家庭内その他これに準ずる限られた範囲内において使用すること」（**私的利用**）を目的とするときは、いく

---

[1] ネットで増える「名誉棄損」 ～ 相次ぐ逮捕、最高裁有罪判決も (So-net) http://www.so-net.ne.jp/security/news/newstopics_201004.html

つかの例外を除いて、使用するものが複製することができるとしている。

著作権法第 13 条では、権利の目的とならない著作物として、憲法その他の法令，国や地方公共団体などによる告示・訓令・通達、裁判所の判決 が定められている。また、著作権法第 35 条では、学校での授業に必要な資料を、必要と認められる限度において、複製する事が認められている。第 36 条では、試験問題としての複製についても定められている。

著作物の引用について、著作権法第 32 条で「公表された著作物は、引用して利用することができる。この場合において、その引用は公正な慣行に合致するものであり、かつ、報道、批評、研究その他の引用の 目的上正当な範囲内で行われるものでなければならない。」と定められている。すなわち、引用は著作権法で正当に認められた権利である。「無断引用を禁じる」等の文言を見かけることがあるが、著作権法で無断引用が認められているため、本来無断引用を禁じることはできない。しかし、引用として認められるためには必要な要件があり、要件を満たさない場合には「引用」とはならない。すなわち、引用は適切にする必要がある。

適切な引用について、著作権法 で「公正な慣行に合致し」かつ「引用の目的上正当な範囲内で行なわれる」 とあるが、判例では「全体としての著作物において、その表現形式上、引用して利用する側の著作物と引用されて利用される側の著作物とを明瞭に区別して認識することができること及び右両著作物の間に前者が主、後者が従の関係があると認められることを要する 」と解釈されている。すなわち、適切な引用には以下の要件がある。

(1) 引用の必然性がある
(2) 自分の著作が主で引用が従の関係にある
(3) 引用部分が明確に区別される
(4) 出所を明示する

タレントなどの写真をブログに掲載する場合、他人が撮ったものであれば著作権、自分が撮ったものでも肖像権の侵害になる。有名人の場合には、出演料を請求されることもある。

【不正アクセス禁止法】

不正アクセス行為の禁止等に関する法律（略称：**不正アクセス禁止法**）は、インターネット等のコンピュータネットワーク等での通信において、不正アクセス行為とその助長行為を禁止することを目的に制定された。第三条で、以下

の様に定められている。具体例については警察庁のサイト[1]で解説されている。

第三条　何人も、**不正アクセス行為をしてはならない**。
２　前項に規定する不正アクセス行為とは、次の各号の一に該当する行為をいう。
一　**アクセス制御機能**を有する特定電子計算機に **電気通信回線**を通じて当該アクセス制御機能に係る**他人の識別符号を入力して当該特定電子計算機を作動させ**、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加した**アクセス管理者**がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の**承諾を得てするものを除く**。）
二　アクセス制御機能を有する特定電子計算機に **電気通信回線**を通じて当該アクセス制御機能による特定利用の制限を免れることができる **情報（識別符号であるものを除く。）又は指令を入力**して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）
三　**電気通信回線**を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当 該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

第四条　何人も、アクセス制御機能に係る他人の識別符号を、その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして、又はこれを知っている者の求めに応じて、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る**利用権者以外の者に提供**してはならない。ただし、当該アクセス管理者がする場合又は当該アクセス管理者若しくは当該利用権者の承諾を得てする場合は、この限りでない。

【不正指令電磁的記録に関する罪】

2011 年の刑法改正で、**不正指令電磁的記録に関する罪**が新設された。以下が、その条文である。

第百六十八条の二　正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、**三年以下の懲役又は五十万円以下の罰金**に処する。
一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録
二　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録
２　正当な理由がないのに、前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。
３　前項の罪の未遂は、罰する。

[1]不正アクセス行為の禁止等に関する法律の概要（警察庁）
http://www.npa.go.jp/cyber/legislation/gaiyou/gaiyou.htm

典型的にはコンピュータウイルスが想定されているため「**ウイルス作成罪**」とも呼ばれる。すなわち、ウイルスを作成、配布した者を取り締まるための法律と理解されている。単にウイルスを作成しただけでは罪にならず、（1）正当な理由がない、（2）無断で他人のコンピューターにおいて実行させることを目的とする、の 2 点を満たさないと罪にならない。

「ウイルス作成罪」の呼称が定着しているが、実際には「不正指令電磁的記録」はコンピュータウイルスに限られない。その例として、第 4 章で解説するウェブサイトの脆弱性を突いた CSRF（クロスサイトリクエストフォージェリ）がある。不正指令電磁的記録による初の逮捕者は、CSRF によって、メールに埋め込まれたリンクをクリックさせることで、意図しない掲示板への書き込みをさせた事件（2012 年 1 月、大阪府警が逮捕）であるとされている。CSRF はウイルスとは異なるものの、「ウイルス作成罪」という呼び名が定着していたため、多くの報道では「ウイルスを作成した罪」と誤って解説されていた。

1-2. 情報セキュリティ

インターネットの発展にともない、多くの人がインターネットを使うようになり、コンピュータセキュリティが重要な課題となった。インターネットのシステムは、本来性善説の立場からセキュリティよりも利便性を重視する設計となっていたが、インターネットの普及とともに、悪意を持った人達による**コンピュータウイルス**の作成と蔓延、**フィッシング**詐欺（偽の電子メールを送信するなどして、受信者を架空の Web サイトや実在している Web サイトの偽サイトに誘導し、情報を不正に取得すること）、ネットオークション詐欺、企業のコンピュータシステムに不正に侵入して個人情報を盗み出す**個人情報漏洩**（流出）事件等の様々な犯罪が広がり、様々な情報セキュリティ対策が必要とされるようになってきた。個人情報流出事件では、企業が多額の賠償金を支払うケースもあり、企業にとって個人情報保護のための情報セキュリティ対策は企業の信頼を守ることのみならず経済的損失を防ぐためにも重要な施策となっている。

近年のネットワーク犯罪は、ますます技術的に高度化、複雑化されており、家庭、大学、企業等でインターネットを使う私たちにとって、 ネットワークのしくみとセキュリティについて正確な知識を持つ事がますます重要となっている。本書では、２章と３章でネットワークのしくみについて解説し、４章ではセキュリティ対策の具体的方法について学ぶ。

1章・章末問題

問1-1　不正アクセス禁止法に関する記述のうち、正しいものはどれか。(IT パスポート試験平成 23 年度秋期)

(1) アクセスコントロール機能を有する個人使用の PC に対してイントラネット経由で不正にアクセスしても、不正アクセス禁止法違反にはならない。
(2) 実際に被害が発生しなくても、不正アクセス行為をするだけで不正アクセス禁止法違反となる。
(3) 他人の ID とパスワードを、その利用方法を知っている第三者に教えるだけでは、不正アクセス禁止法違反にはならない。
(4) 不正アクセス禁止法違反となるのは、インターネット経由でアクセスされるものに限られる。

問1-2　不正アクセス禁止法において、不正アクセス行為に該当するものはどれか。(IT パスポート試験平成 23 年度秋期)

(1) 会社の重要情報にアクセスし得る者が株式発行の決定を知り、情報の公表前に当該会社の株を売買した。
(2) コンピュータウイルスを作成し、他人のコンピュータの画面表示をでたらめにする被害をもたらした。
(3) 自分自身で管理運営するホームページに、昨日の新聞に載った報道写真を新聞社に無断で掲載した。
(4) 他人の利用者 ID、パスワードを許可なく利用して、アクセス制御機能によって制御されている Web サイトにアクセスした。

問1-3　フィッシングの説明として、最も適切なものはどれか。(IT パスポート試験平成 23 年度秋期)

(1) ウイルスに感染したコンピュータを、そのウイルスの機能を利用する事によってインターネットなどのネットワークを介して外部から不正に操作する。
(2) 偽の電子メールを送信するなどして、受信者を架空の Web サイトや実在している Web サイトの偽サイトに誘導し、情報を不正に取得する。

(3) 利用者が入力したデータをそのままブラウザに表示する機能が Web ページにあるとき、その機能の脆弱性を突いて悪意のあるスクリプトを埋め込み、そのページにアクセスした利用者の情報を不正に取得する。
(4) 利用者に気づかれないように PC にプログラムを常駐させ、ファイルのデータや PC 操作の情報を不正に取得する。

問1-4　著作権法に照らして適法な行為はどれか。(基本情報技術者試験平成 23 年度特別)

(1) ある自社製品のパンフレットで使用しているスポーツ選手の写真を、撮影者に無断で、ほかの自社製品のパンフレットに使用する。
(2) 経済白書の記載内容を説明の材料として、出所を明示して Web ページに転載する。
(3) 新聞の写真をスキャナで取り込んで、提案書に記載する。
(4) ユーザ団体の研究会のように限られた対象者に対し、雑誌の記事をコピーして配布する。

問1-5　業務中に受信した電子メールの添付文書をワープロソフトで開いたら、ワープロソフトが異常終了した。受け取った電子メールがウイルスを含んでいた可能性が考えられる場合、適切な処置はどれか。(本章では解説してないが、考えてみよう) (IT パスポート試験平成 21 年度春期)

(1) PC をネットワークから切り離した後、OS の再インストールをする。
(2) PC をネットワークから切り離した後、速やかにシステム管理部門の担当者に連絡する。
(3) 現象が再発するかどうか、必要ならワープロソフトを再インストールして確かめる。
(4) 社員全員にウイルス発生の警告の電子メールを発信する。

2章 ネットワークの基本的なしくみ

日常的に利用しているインターネットであるが、その基本的なしくみはあまり理解されていない。本章では、ネットワークの基本的なしくみについて、インターネットの通信規約である TCP/IP プロトコルの内容を学習する。日常的にも様々な場面で出て来る通信の専門用語を正確に理解し、家庭や職場でネットワークの構築ができて、ネットワークのトラブルが起きた時に原因を探って解決の方法を考えるための基礎知識を身につける。そして、後の章で学習するネットワークセキュリティを理解する礎とする。

学習内容とキーワード

2-1. ネットワークとプロトコル：*ネットワーク、LAN、WAN、インターネット、プロトコル、OSI 参照モデル、プロトコルの階層化、TCP/IP プロトコル*

2-2. ネットワークの構築：*ネットワークインターフェース層、ネットワークの接続形態、星形、バス型、ネットワーク構成図、イーサネット、ネットワークインタフェースカード、MAC アドレス、リピータ、ブリッジ、ハブ、スイッチングハブ、同軸ケーブル、光ファイバー、LAN ケーブル、10BASE-T、無線 LAN、アクセスポイント、SSID、ESSID、IEEE 802.11*

2-3. IP アドレス：*IP アドレス、IPv4、IPv6、ネットワークアドレス、ホストアドレス、クラス A、クラス B、クラス C、CIDR、プレフィックス、サブネットマスク、アドレッシング、ルーティング、ルータ、ブロードバンドルータ、インターネットサービスプロバイダ、NAT、プライベートネットワーク、プライベート IP アドレス、グローバル IP アドレス*

2-4. ドメインネームシステム：*DNS、ホスト名、ドメイン名、トップレベルドメイン、セカンドレベルドメイン、DNS サーバ、名前解決、ファーミング、DNS キャッシュポイズニング、ルート DNS サーバ*

2-5. TCP とポート番号：*トランスポート層、TCP、UDP、パケット、セグメント、シーケンス番号、ポート番号、誤り検出コード、確認応答*

2-6. ネットワークの状態の調べ方：*ipconfig、ping、nslookup、tracert、netstat、arp*

2-1. ネットワークとプロトコル

【ネットワーク】

ネットワークとは、複数のコンピュータをケーブルで接続して利用する形態のこと。１台だけで利用する**スタンドアロン**と比べて、ネットワークでは次のようなことが実現できる。

⑴ 資源の共有

プログラム、データなどのソフトウェア資源と、記憶装置やプリンタなどのハードウェア資源を共有できる。

⑵ 情報の交換

データ、文字、音声などのメッセージ、画像や動画などのマルチメディア情報の交換ができる。遠隔地であっても様々な表現を用いたコミュニケーション手段として活用できる。

【ネットワークの種類】

⑴ LAN: Local Area Network – 構内情報通信網

同じ建物、敷地、学校、会社などの地域限定のネットワーク

⑵ WAN: Wide Area Network – 広域情報網

LAN どうしを接続するネットワーク

⑶ インターネット

LAN, WAN が全世界規模で相互接続されたネットワーク

要するに、世界規模の WAN

【インターネットの歴史】

インターネットは、1969 年にアメリカ国防総省の分散型コンピュータネットワーク ARPANET として誕生した。1970 年代前半に大学等の研究機関にネットワークが接続され、1991 年には商用プロバイダにも開放され、爆発的に普及して現在に至る。

インターネット上では、**TCP/IP プロトコル**に従って、世界中のコンピュータを相互に接続し、情報のやり取りを行うことができる。また、現在では、コンピュータのみならず携帯電話、テレビ、ゲーム機等の様々な機器がインターネットに接続している。

【通信プロトコル】

通信プロトコルとは、コンピュータ同士が通信を行う上で相互に決められた約束事のことで、**通信手順**、**通信規約**などとも呼ばれる。

私たちが会話に意思の疎通ができるのは、同じ単語の意味、文法規則を持っている言語を使用しているためであり、言語が異なると会話が通じないように、通信が成功するためには、プロトコルが同じでなければならない。

【OSI 参照モデル】

プロトコルの階層化によって、上位のプロトコルは自分のすぐ下のプロトコルを知っていれば、その下のプロトコルの中身を知る事なく通信をすることができる。通信プロトコルを階層化するモデルは、**OSI 参照モデル**として標準化されている。階層化されたプロトコルの一揃いのことを、プロトコルが積み重なっていることからプロトコルスタックとも、一揃いしていることからプロトコルスイートとも呼ぶ。

表 2-1：OSI 参照モデル

層（レイヤ）	説明
第 7 層 - アプリケーション層	ファイル転送や電子メールなどの具体的な通信サービスを提供
第 6 層 - プレゼンテーション層	文字コード等のデータの表現方法を変換
第 5 層 - セッション層	通信の開始から終了までを認識
第 4 層 - トランスポート層	ネットワークの端から端までの通信管理（エラー訂正、再送制御等）
第 3 層 - ネットワーク層	ネットワークにおける通信経路の選択（ルーティング）、データ中継
第 2 層 - データリンク層	直接接続されている通信機器間の通信
第 1 層 - 物理層	物理的な接続、コネクタ形状等

【TCP/IP プロトコル】

TCP/IP **プロトコル**とは、インターネットでデータ通信をするためのプロトコ

ルであり、TCP と IP を中心とした複数のプロトコルの集まりである[1](表 2-2)。TCP/IP プロトコルの一式を、インターネット・プロトコル・スイートと呼ぶことも多い。本書では、TCP/IP プロトコルを下の階層から順番に理解を進めていく。

表 2-2：OSI 参照モデルと TCP/IP モデルの比較

OSI 参照モデル	TCP/IP モデル	主なプロトコル
アプリケーション層	アプリケーション層	SMTP, POP, HTTP, FTP, Telnet, SNMP
プレゼンテーション層		
セッション層		
トランスポート層	トランスポート層	TCP, UDP
ネットワーク層	ネットワーク層	IP
データリンク層	ネットワークインターフェース層	PPP，イーサネット，ツイストペア，同軸，光ファイバ
物理層		

TCP/IP プロトコルの中心である IP と TCP の機能について、以下に簡単にまとめる。

(a) IP (Internet Protocol) の機能

(1) **アドレッシング**

ネットワークに接続されているコンピュータを見分けるために IP アドレスという番号を使う。

(2) **ルーティング**

データを宛先のコンピュータに届けるために、最適な伝送経路を選択して転送する。ルーティングの機能を担当する装置を**ルータ**と呼ぶ。

世界中の LAN や WAN がルータによって接続されたネットワークがインターネットである、とも言うことができる。情報は、ルータからルータを伝わって相手先に届く。

(b) TCP (Transmission Control Protocol) の機能

(1) データを**パケット**に分解したり、組み立てたりする。

[1] TCP/IP の基礎の基礎を理解していますか？ (ASCII)
http://ascii.jp/elem/000/000/424/424788/

(2) パケットには、分割された順番を表す**シーケンス番号**を付ける。
(3) どのアプリケーションソフトウェアのデータを使っているのかを対応する**ポート番号**により識別する。
(4) 欠損したパケットを再送して**エラーを訂正**する。

2-2. ネットワークの構築

ネットワークを構築するためには、様々なネットワーク機器とその接続方法を知る必要がある。TCP/IP モデルの最下層は**ネットワークインターフェース層**であり、これは OSI 参照モデルの**物理層**と**データリンク層**をあわせたものである。物理層では、ネットワークを構築するための様々な物理的な規格がある。また、データリンク層では物理的に接続されている機器間のデータのやりとりが規定されている。この節では、ネットワーク構築のために必要なネットワークインターフェース層の規格について学ぶ。

【ネットワークの接続形態】

ネットワークの接続形態には、下図のように**輪形（リング型）**、**メッシュ型**、**星型（車輪型、スター型）**、**フルコネクト型**、**ツリー型**、**バス型**等がある。星型ネットワークの中心部分は**ハブ**と言われる。10BASE-T などのイーサネットの論理構造はバス型である。

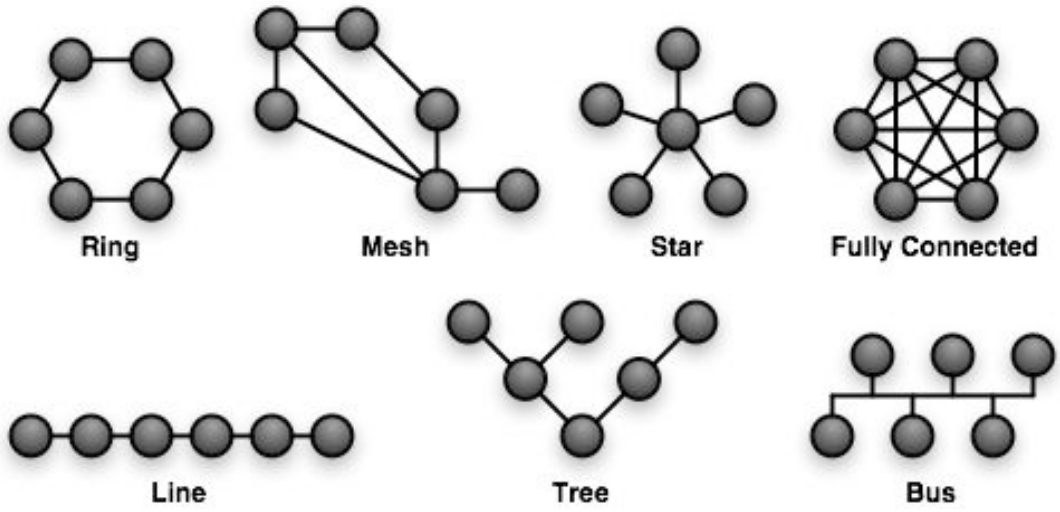

図 2-1：ネットワーク構造の種別（Wikipedia「ネットワーク構成」より）

【ネットワーク構成図】

ネットワーク機器の接続を**ネットワーク構成図**として描くと、ネットワーク構築の計画を立てる時、すでに構築されているネットワークの状況を把握してネットワークの構成を変えたりトラブルに対処したりする時に役立つ。業務用に構築されている LAN のみならず、家庭内でも PC、iPad、プリンタ、テレビ、ゲーム機、電話等、様々な機器が有線・無線ネットワークで接続されるため、ネットワークの接続状況を整理するためにネットワーク構成図を描く事は有益である。

【イーサネット】

イーサネットとは、最も普及しているネットワークの国際標準規格である。現代の LAN では、主に物理的な規格（ネットワークインターフェース層 = 物理層 + データリンク層）である「イーサネット」と、通信内容の取り決めを決めた「TCP/IP プロトコル」（ネットワーク層、トランスポート層）の組合せが一般的である。

詳しくは、Wikipedia 「イーサネット」に記述されている。ここでは、押さえておくべきポイントを列記する。

(1) 物理層、物理的構成

イーサネット上の各端末（**ネットワークインタフェース**；**ネットワークインタフェースカード**；**ネットワークアダプタ**；**ネットワークカード**；**LAN カード**）を区別するために、製造段階で割り振られる世界中でただ 1 つ固有の 48 ビットの **MAC アドレス**を持っている。MAC アドレスは、たとえば 00:00:82:af:e3:b2 のように 8 ビットごとに 16 進数で表記される。MAC アドレスは物理層に割り当てられるもので、IP プロトコル（ネットワーク層）で規定される IP アドレスとは別のものである。

(2) 機器およびケーブル

- リピータ、ブリッジ
- **ハブ**、スイッチングハブ（L2 スイッチ、レイヤー 2 スイッチングハブ）

スイッチングハブにはどんな製品があるか？

選ぶポイント：**伝送速度**とポート数

ケーブル

- 同軸ケーブル
- 光ファイバー
- **ツイステッド・ペア・ケーブル**（LAN ケーブル、イーサネット・ケーブル）
  カテゴリー5, エンハンストカテゴリー5, カテゴリー6 とは？

(3) 通信速度別・カテゴリ別イーサネット仕様

10BASE-T は 10Mbps

100BASE-TX (Fast Ethernet)は 100Mbps

1000BASE-T (Gigabit Ethernet) は 1Gbps

bps (bit per second): 伝送速度の単位。ビット毎秒。

Mbps = 10^6 bps, Gbps = 10^9 bps

1Gbps を 2 の 30 乗倍の約 10 億 7000 万 bps とする場合もあるが、大抵の場合は 10 億 bps の意味である。

計算例：100 MB（メガバイト）のファイルをダウンロードするのに、37 秒かかった。この時の伝送速度は？

→ 1 バイトは、8 ビットである。1MB は、2 の 20 乗バイトなので、100MB は 800×2^{20} ビットである。したがって、伝送速度は　$800 \times 2^{20} / 37 = 22671914$ bps = 23 Mbps

注意：イーサネットを 1000BASE-T にしても、ハブ、ネットワークアダプタといった通信経路が Gbps の伝送速度に対応していなければ、Gbps の通信速度とはならない。

【無線 LAN】

無線 LAN は電波や赤外線を用いてネットワークを構築する技術である。無線 LAN を使ってネットワークを構築することで、ネットワークケーブルの配線が不要となる。

無線 LAN では、端末同士が直接通信を行うアドホックモードと、**アクセスポイント**を中継して通信するインフラストラクチャモードがある。無線 LAN アクセスポインと各端末の無線 LAN アダプタには、SSID (ESSID)という識別名が割り当てられ、アクセスポイントは自分と同じ SSID を持つ端末同士の通信を中継する。

無線 LAN の規格である「IEEE 802.11」には、様々な規格があり[1]、それぞれ

[1] 無線 LAN (Allied Telesis)
http://www.allied-telesis.co.jp/products/list/wireless/knowl.html

周波数帯、公称伝送速度が異なる。無線通信をするためには、本来無線局免許が必要とされるが、日本の法律によって、無線免許不要で使うことの出来る周波数帯が定められている。日本の一般家電売り場で売られている無線 LAN 関係の製品は、通常、日本の法律によって免許不要と定められている周波数帯を使っているものであるが、輸入等で海外の製品を使う場合には、免許が必要とされる周波数帯を使っているものがあるので、注意が必要となる。

無線 LAN の規格で定められている公称速度は、必ずしもその速度で通信ができることが保証されているものではない。無線 LAN では、必ずデータが流れていない時間があり、平均的な通信速度は公称速度よりも遅くなる。さらに、 無線 LAN 機器間の距離が離れているか、あるいは間に障害物があって電波が弱い場合には、速度が遅くなる。

2-3. IP アドレス

インターネットのプロトコルである IP では、ネットワークに接続されているコンピュータを見分ける**アドレッシング**のために、**IP アドレス**を使う。

IP には、バージョンがある。現在広く使われているのは **IP バージョン４** (IPv4)であり、次世代の IP として **IP バージョン６** (IPv6)がある。

【IPv4】

IPv4 では、IP アドレスは 8 ビット×4 = 32 ビットで表現される。

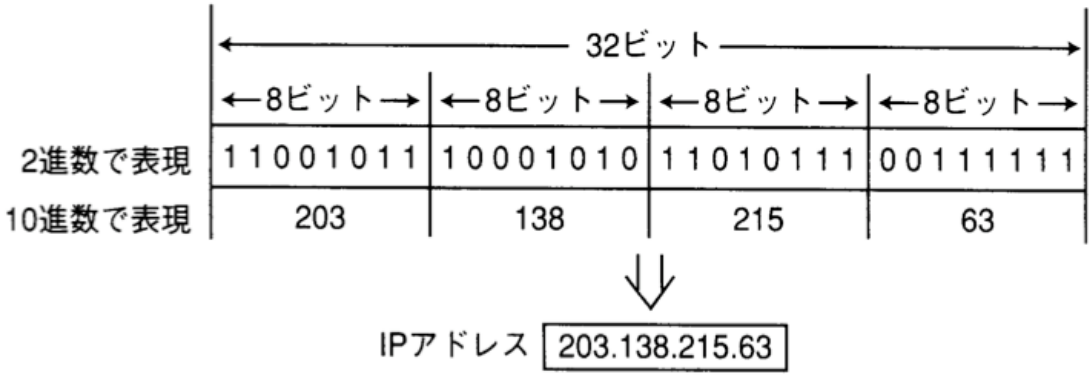

図 2-2：IP アドレス 203.138.215.63 の意味

したがって、IPv4 では最大 2^{32}=42 億 9496 万 7296 個の IP アドレスが使え

る。

【IPv6】

現在、IPv6 への移行が検討されているのは、IPv4 では IP アドレスでは足りなくなって来ているためである（特に、急速にインターネット利用が伸びている新興国で)。IPv6 では、IP アドレスは 16 ビット×8=128 ビットで表現される。

例: f0f0:100:20:3:1000:100:20:3

したがって､IPv6 では最大 2^{128} = 340 澗 2823 溝 6692 穣 0938 秭 4634 垓 6337 京 4607 兆 4317 億 6821 万 1456 個の IP アドレスが使える。例えば、NTT のフレッツ・光ネクストでは、IPv6 が採用されている。

本書では、以後特に断らなければ IPv4 を取り扱うものとする。

【ネットワークアドレスとホストアドレス】

IPv4 では、IP アドレスは 32 ビットの数値を 8 ビットごとに区切って表記されている。この IP アドレスは、**ネットワークアドレス**と**ホストアドレス**に分けられる。たとえば、133.79.247.13 という 32 ビットの IP アドレスが、最初の 24 ビット（133.79.247 まで）がネットワークアドレスで、最後の 8 ビット(13)がホストアドレスである、といったように分ける。ネットワークアドレスが同じ IP アドレスは、１つのネットワークとして扱われ[1]、データリンク層で通信がされる。ネットワークアドレスが異なる IP アドレスは、異なるネットワークであり、データリンク層の上のネットワーク層(IP)の通信が必要とされる。

以下の図では､最初の 24 ビットがネットワークアドレスであり､192.168.1.xx であらわされる IP アドレスはすべて同一のネットワークに所属するが、192.168.1.1 と 192.168.2.1 は異なるネットワークである。

ネットワークアドレスの長さは一定ではなく、**クラス A からクラス E** までの５種類に分けられる（表 2-3)。

通常使われるのはクラス A からクラス C までであり、ネットワークアドレスの長さが 8 ビット単位、つまり 1 バイト単位で区切られているため、IP アドレスの数字表記に対応している。それぞれのクラスごとに、割当可能な IP アドレスの数、つまりホストアドレスの数が異なる。クラス A が約 1,677 万台(2^{24}-2

[1] ネットワークアドレスとホストアドレス
http://www.itbook.info/study/p54.html

台)、クラス B が 65,534 台(2^{16}-2 台)、クラス C が 254 台(2^{8}-2 台)のホストを接続できる。東洋大学では、ネットワークアドレス 133.79.0.0 のクラス B のアドレスを取得しているため、65,534 台のパソコンをインターネットに接続できる。

表 2-3：アドレスクラス

クラス	アドレス範囲	ネットワークアドレス長	ホストアドレス長	先頭ビット
クラス A	0.0.0.0-127.255.255.255	8 ビット	24 ビット	0
クラス B	128.0.0.0-191.255.255.255	16 ビット	16 ビット	10
クラス C	192.0.0.0-223.255.255.255	24 ビット	8 ビット	110
クラス D	224.0.0.0-239.255.255.255	—	—	1110
クラス E	240.0.0.0-255.255.255.255	—	—	1111

【CIDR】

アドレスクラスでは、ネットワークアドレスとホストアドレスの境界が 8 ビット単位で制御される。もっと細かいビットでネットワークアドレス長を制御するために、CIDR（サイダー; Classless Inter-Domain Routing）が用いられる。CIDR 記法は、133.79.0.0/16 のように、IP アドレスの後にスラッシュと数字を書く。スラッシュの後に書かれる数字は、**ネットワークアドレス長（プレフィックス長）**である。

例えば、CIDR で 133.79.0.0/16 と書かれた場合、133.79.0.0 を 2 進数表記して、10000101.01001111.00000000.00000000 とした時の、先頭の 16 ビット 10000101.01001111 までが**プレフィックス**となり、残りの 16 ビットがホストアドレスとなる。開始アドレスは 10000101.01001111.00000000.00000000、すなわち 133.79.0.0 で、終了アドレスは 10000101.01001111.11111111.11111111、すなわち 133.79.255.255 となる。CIDR で 133.79.0.0/20 と書いた場合、先頭の 20 ビット 10000101.01001111.0000 までがプレフィックスとなり、残りの 12 ビットがホストアドレスとなる。開始アドレスは 133.79.0.0 で、終了アドレスは 10000101.01001111.00001111.11111111、すなわち 133.79.15.256 となる。

【サブネットマスク】

サブネットマスクとは、IP アドレスのネットワーク部とホスト部を区別する

ための数値である。ネットワーク部を 1、ホスト部を 0 とした数値を、IP アドレスと同じ記法で表す。先頭 16 ビットをネットワークアドレス部とするとき（CIDR 表記では、IP アドレスの後に/16）のサブネットマスクは、２進数表記で 11111111.11111111.00000000.00000000、10 進数表記で 255.255.0.0 となる。先頭 20 ビットをネットワークアドレス部とする時のサブネットマスクは、２進数表記で　11111111.11111111.11110000.00000000、10 進数表記で 255.255.240.0 となる。

【アドレッシングとルーティング】

IP の機能には、アドレッシングとルーティングがある。**アドレッシング**とは IP アドレスによってコンピュータにインターネット上の住所を割り当てる機能であり、**ルーティング**とは、IP アドレスを元に、宛先のコンピュータへ向けて、最適な伝送経路を選択してパケット（データ）を転送する機能である。

【ルータ】

ルーティングの機能を担当する装置を**ルータ**と呼ぶ。ルータはネットワーク間を相互接続する通信機器であり、OSI 基本参照モデルの第 1 層（物理層）から第３層（ネットワーク層 / IP プロトコル）までの接続を担当する。スイッチングハブが第 2 層（データリンク層）までの接続を担当するのに対して、ルータでは第３層までの接続を担当する。したがって、同一のネットワーク（ネットワークアドレスが同じ IP アドレス）の通信は、スイッチングハブを経由して接続できるが、異なるネットワーク間の通信には、ルータを経由する必要がある。

【ブロードバンドルータ】

家庭からインターネットに接続する際には、ISDN、ADSL、FTTH、ケーブルテレビ(CATV)といったサービスを利用する。各社様々なサービスが提供されており、サービスに応じて、必要な機器を購入またはレンタルする。

ブロードバンドルーターを使うと、家庭から ADSL、FTTH、(CATV) を使ってインターネットに接続することができる。ブロードバンドルータの基本的な機能はルータとスイッチングハブであり、インターネットサービスプロバイダのアカウントを設定することで、インターネットに接続する機能を持つ。ブロードバンドのインターネット回線に接続できるルータという意味で、ブロード

バンドルータという名前がつけられているのであろう。

ブロードバンドルータは、DHCP や NAT 機能を有しているものが多い。また､LAN 側に有線のポートのみをもっているものを有線ブロードバンドルータ、有線のみならず無線で接続可能なものを無線ブロードバンドルータと呼ぶ。

【NAT とプライベートネットワーク】

NAT (Network Address Translation; ネットワークアドレス変換)とは、インターネット上の IP アドレスやポート番号を別のものに変換する技術である。主にプライベート IP アドレスを使用するホストからインターネットにアクセスするために利用される。

限りある IP アドレスを有効に使うために、インターネットに割り当てられる IP アドレス（**グローバル IP アドレス**）と、LAN 内だけに割り当てられる IP アドレス（**プライベート IP アドレス**）を別途用意して、NAT によって、グローバル IP アドレスとプライベート IP アドレスを変換することがある。

プライベートアドレスを使う利点は以下の 2 つである。

(1) IP アドレスの節約（1 つのグローバル IP アドレスでたくさんの PC を接続可能）

(2) 外部攻撃からの防御（インターネットからプライベートアドレス空間へ通信を開始することができない）

プライベート IP アドレスは、表 2-4 のアドレス空間が予約されている。

表 2-4：プライベートアドレス空間

クラス	範囲	サブネットマスク
クラス A	10.0.0.0-10.255.255.255	255.0.0.0
クラス B × 16	172.16.0.0-172.31.255.255	255.240.0.0
クラス C × 256	192.168.0.0-192.168.255.255	255.255.0.0

2-4. ドメインネームシステム

インターネットに接続されているコンピュータは、固有の IP アドレスを持っている。通信をする時には、通信相手のコンピュータを IP アドレスで指定し、識別する。IP アドレスは、4 つの数字の組み合わせであるため、人間にとって覚える事は難しい。そこで、DNS (Domain Name System) が開発された。DNS

は、コンピュータの IP アドレスを人間にとって覚えやすいホスト名あるいはドメイン名という名前で扱う機構である。たとえば、東洋大学の Web サーバは、IP アドレス 133.79.224.9 とともに、ホスト名 www.toyo.ac.jp を持っている。インターネットでは、ホスト名とドメイン名がしばしば同じ意味で使われるが、両者には微妙な違いがある。本書では、厳密に区別はしない。

ドメイン名は、ピリオド(.)で複数のラベルを区切って構成する[1]。ラベルには、英字(A～Z)、数字(0～9)、ハイフン(-)が使用でき、英字の大文字と小文字は区別しない（ただし、国際化ドメイン名の１つとして日本語ドメイン名も存在する)。ドメイン名の一番右側のラベルを「**トップレベルドメイン**(TLD)」、そこから左へ「**セカンドレベルドメイン**(SLD)」「サードレベルドメイン」…と呼ぶ。たとえば、www.toyo.ac.jp であれば、一番右の jp がトップレベルドメイン、そこから左へ順番に ac がセカンドレベルドメイン toyo がサードレベルドメインとなる。右側から順番に、www.toyo.ac.jp であれば「日本の」「大学等の教育機関であるところの」「東洋大学の」「www サーバ」と読むことができる。

TLD は、ICANN (The Internet Corporation for Assigned Names and Numbers; アイキャン）の下部組織の IANA (Internet Assigned Numbers Authority) が管理している。IANA は、IP アドレス・ドメイン名・ポート番号（後述）を管理している。TLD には、表 2-5 のような区分けがある[2]。

表 2-5：TLD の区分け

区分け	例
ジェネリックトップレベルドメイン (gTLD)	.com .info .net .org
制限付きジェネリックトップレベルドメイン	.biz .name .pro
国別コードトップレベルドメイン (ccTLD)	.jp .cn .kr .us .uk .aq
スポンサードトップレベルドメイン (sTLD)	.aero .coop .asia .tel .gov .edu
インフラ用トップレベルドメイン	.arpa

日本の ccTLD である .jp の元の JP ドメインは、日本レジストリサービスが管理する。JP ドメインは、自由に SLD を登録できる汎用ドメインと SLD でドメイン登録者の属性を表す属性型ドメイン(ccSLD)がある（表 2-6)。属性型ドメインの一種である地域型ドメインには、一般地域型ドメイン名と、地方公共団

[1] ドメイン名のしくみ (JPNIC) http://www.nic.ad.jp/ja/dom/system.html
[2] Root Zone Database (IANA) http://www.iana.org/domains/root/db/

体ドメイン名の２種類がある。個人で地域型ドメインを取得するフィッシングの危険性があるため、地域型ドメイン名は廃止して、地方公共団体はすべて lg.jp ドメインに移行するべきとの指摘がある[1]。

表 2-6 属性型 JP ドメインの例

ドメイン	属性（おおまかな定義）
ac.jp	日本の大学等の教育機関
ad.jp	JPNIC 会員
co.jp	日本で登記された会社
ed.jp	日本の高校までの教育機関
go.jp	日本の政府機関
gr.jp	日本の任意団体
lg.jp	日本の地方公共団体
ne.jp	日本のネットワークサービス
or.jp	日本の法人

【DNS サーバ】

DNS サーバまたはネームサーバーとは、ドメイン名と IP アドレスを対応づけるためのハードウェア（サーバ）あるいはソフトウェアである。たとえば、東洋大学のサイトを見ようと http://www.toyo.ac.jp にアクセスすると、

(1) www.toyo.ac.jp というドメイン名に対する IP アドレスを、DNS サーバに問い合わせる
(2) DNS サーバから、www.toyo.ac.jp というドメイン名に対する IP アドレスが 133.79.224.9 であるという返答が返ってくる（名前解決）。
(3) IP アドレス 133.79.224.9 に、http プロトコルで Web ページを要求する

といったような流れで、通信が開始される。DNS サーバが動いていなければ、http://www.toyo.ac.jp にアクセスしようとしたときに、その IP アドレスを知ることができないため、エラーとなる。DNS サーバは重要であるため、通常はプライマリ DNS サーバとセカンダリ DNS サーバの２つを設定する。

DNS サーバの信頼性は非常に重要である。もし、銀行の振込をしようとして、銀行のサイトに接続しようとしたときに、犯罪者が作成した偽の銀行サイトに

[1] 地域型ドメイン名は廃止してはどうか (高木浩光@自宅の日記)
http://takagi-hiromitsu.jp/diary/20090607.html

接続してしまったら、被害を受ける。このように、DNS を攻撃して偽のサイトへ誘導するフィッシング攻撃を**ファーミング**(pharming)という。ファーミングには、DNS サーバを攻撃する方法、キャッシュサーバの情報を書き換える **DNS キャッシュポイズニング**、PC の hosts ファイルを書き換える方法等がある。

名前解決を依頼された DNS サーバは、

(1) ルート DNS サーバ　（世界に 13 個存在する）
(2) jp を管理している DNS サーバ
(3) ac.jp を管理している DNS サーバ
(4) toyo.ac.jp を管理している DNS サーバ

といったように、DNS サーバのツリーをルート DNS サーバから下にたどって、名前解決をする。同じ問い合わせを何度も繰り返さないで済むように、一定期間結果を保持するキャッシュの仕組みを持っている。

2-5. TCP とポート番号

TCP/IP では、**トランスポート層**のプロトコルとして主に TCP と UDP が用いられる。通常は TCP が用いられ、速度が重視してその分信頼性が低い通信に UDP が用いられる。TCP は、データを**パケット（セグメント）**に分解して、**シーケンス番号**を付け（仮想回線）、通信先の指定した**ポート番号**のサービス（アプリケーション層のプロトコル）へと配信し、受信した側は**誤り検出コード**で通信エラーを検出し、正しいパケットが届いたときは受信ホストに　**確認応答**(ACK; ACKnowledgement)を返し、受信側で確認応答が一定時間内に返って来ない時にはデータを再送する自動再送要求する。受信側は、受信したセグメントをシーケンス番号順に並べ替え、組み立てる。

ポート番号とは、通信先のサービスを特定するための番号である。 TCP と UDP それぞれに 0 から 65535 までのポート番号が指定できる。IP アドレスを建物の住所にたとえるなら、ポート番号は部屋番号に相当する。

TCP や UDP の特定のポート番号とそのポート番号を用いるサービスの組み合わせは、ポート番号 0～1023 番は Well known port numbers、1024～49151 番は Registered port numbers として、IANA が管理している[1]。クライアント

[1] Service Name and Transport Protocol Port Number Registry (IANA)
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

が自由に決めるポート番号は 49152～65535 番である。以下に、代表的なポート番号とサービス名を挙げる。

(1) TCP/20：FTP (データ)
(2) TCP/21：FTP (制御)
(3) TCP/22：SSH
(4) TCP/23：Telnet
(5) TCP/80：HTTP
(6) TCP/110：POP3
(7) TCP/443：HTTPS

2-6. ネットワークの状態の調べ方

この節では、ネットワークの状態をコマンドプロンプト（Windows で動作する端末ウィンドウ）で調べる方法を紹介する。

コマンドプロンプトは、「アクセサリ」「コマンドプロンプト」から起動する。コマンドプロンプトを起動したら、「ipconfig」と入力すると、IP アドレス、サブネットマスク、デフォルトゲートウェイ（ルーター）等の情報が表示される。

次に「ipconfig /all」と入力すると、さらに詳しい情報が表示される。これは、ipconfig という命令に /all というオプションを指定して実行をしたことになる。このように、命令には通常いくつかのオプションを指定して実行することができる。コマンドの使い方は /? というオプションを指定する。つまり、「ipconfig /?」と実行することで、ipconfig の使い方を知ることができる。

以下のコマンドを実行してみよう。また、コマンドの使い方を /? オプションを使って調べてみよう。

(1) ping www.toyo.ac.jp （www.toyo.ac.jp へネットワークが通じているかどうかを調べる)
(2) nslookup www.toyo.ac.jp (www.toyo.ac.jp の IP アドレスを調べる)
(3) nslookup 133.79.224.9 (133.79.224.9 のホスト名を調べる)
(4) tracert www.toyo.ac.jp (www.toyo.ac.jp への経路を調べる。外部のネットワークは、途中の経路が隠される場合が多い。)
(5) netstat –an (ネットワーク接続状態を確認する)
(6) arp –a (MAC アドレスと IP アドレスの対応を表示する)

２章・章末問題

問 2-1　ネットワークのデータ伝送速度を表す単位はどれか。(IT パスポート試験平成 23 年度秋期)

(1) bps　(2) fps　(3) ppm　(4) rpm

問 2-2　ネットワークインタフェースカードの役割として、適切なものはどれか。(IT パスポート試験平成 23 年度秋期)

(1) PC やアナログ電話など、そのままでは ISDN に接続できない通信機器を ISDN に接続するための信号変換を行う。
(2) PC やプリンタなどを LAN に接続し、通信を行う。
(3) 屋内の電力線を使って LAN を構築するときに、電力と通信用信号の重ね合わせや分離を行う。
(4) ホスト名を IP アドレスに変換する。

問 2-3　室内で複数のコンピュータを接続する LAN を構築したい。必要なものはどれか。(IT パスポート試験平成 23 年度秋期)

(1) インターネット　(2) スプリッタ　(3) ハブ　(4) モデム

問 2-4　最大 32 文字までの英数字が設定でき、複数のアクセスポイントを設置したネットワークに対しても使用できる、無線 LAN のネットワークを識別するものはどれか。(IT パスポート試験平成 23 年度特別)

(1) ESSID　(2) IP アドレス　(3) MAC アドレス　(4) RFID

問 2-5　TCP/IP 階層モデルにおいて、TCP が属する層はどれか。(基本情報技術者試験平成 23 年度秋期)

(1) アプリケーション層　(2) インターネット層
(3) トランスポート層　　(4) リンク層

問 2-6　TCP/IP ネットワークにおいて、ネットワークの疎通確認に使われるものはどれか。（基本情報技術者試験平成 23 年度秋期）

(1) BOOTP　(2) DHCP　(3) MIB　(4) ping

問 2-7　OSI 基本参照モデルにおけるネットワーク層の説明として、適切なものはどれか。（基本情報技術者試験平成 22 年度秋期）

(1) エンドシステム間のデータ伝送を実現するために、ルーティングや中継などを行う。
(2) 各層のうち、最も利用者に近い部分であり、ファイル転送や電子メールなどの機能が実現されている。
(3) 物理的な通信媒体の特性の差を吸収し、上位の層に透過的な伝送路を提供する。
(4) 隣接ノード間の伝送制御手順（誤り検出、再送制御など）を提供する。

問 2-8　TCP 及び UDP のプロトコル処理において、通信相手のアプリケーションを識別するために使用されるものはどれか。（基本情報技術者試験平成 23 年度特別）

(1) MAC アドレス　(2) シーケンス番号　(3) プロトコル番号　(4) ポート番号

3章 ネットワークサービス

全章でネットワークの基本的なしくみについて、TCP/IP プロトコルに基づいて学んだ。本章では、TCP/IP プロトコルの階層の中で最上位に位置するアプリケーション層に属する、様々なネットワークサービスのプロトコルについて学ぶ。アプリケーション層には、Web、メール、ファイル転送、ファイル共有、プリンタ共有、内蔵時計合わせ、チャット等、様々な通信サービスに対応するプロトコルがある。その中でも、特に重要性が高い Web とメールのしくみを中心に、関係するセキュリティの話題を交えながら解説する。

学習内容とキーワード

3-1. Web のしくみ:*HTTP*、*URL*、*HTTPS*、*Web サーバ*、*Web ブラウザ*、*HTML*、*クッキー*、*Web サイトの脆弱性*、*クロスサイトスクリプティング*、*SQL インジェクション*、*クロスサイトリクエストフォージェリ* 、*セッションハイジャック*

3-2. メールのしくみ：*SMTP*、*POP before SMTP*、*SMTP-AUTH*、*S/MIME*、*POP*、*POP3*、*APOP*、*POP over SSL*、*メールの書式*、*メールアドレス*、*文字コード*、*MIME*、*HTML メール*、*ヘッダ情報*、*ヘッダフィールド*、*迷惑メール*、*スパム*、*特定電子メール法*

3-3. 様々なアプリケーション層のプロトコル：*DHCP*、*FTP*、*NTP*、*ファイル共有*、*NetBEUI*、*NetBIOS*、*SMB*、*CIFS*、*TLS*、*SSL*

3-1. Web のしくみ

【HTTP のしくみ】

HTTP（HyperText Transfer Protocol; ハイパーテキスト転送プロトコル)とは、Web ブラウザと Web サーバの間で HTML (HyperText Markup Language) などのコンテンツ送受信に用いられる通信プロトコルである。

HTTP を理解するために、Windows PC で以下を実行してみよう（Mac ではターミナルを使う)。

(1) スタート→プログラム→アクセサリ→コマンドプロンプトを起動する。

(2) 「telnet www2.toyo.ac.jp 80」と入力してリターンキーを押す。
(3) 画面には何も表示されないが、「GET /~seki_k/security/hello.html」と入力してリターンキーを押す。
(4) 画面には何が表示されるか？

上記手順では、以下のような HTTP の動作となっている。まず、 telnet www2.toyo.ac.jp 80 で、www2.toyo.ac.jp というホスト名のコンピュータ（サーバ）に対して、HTTP のデフォルトのポートである 80 番ポートで HTTP プロトコルの通信を開始する。次に、サーバに対して HTTP の GET メソッドによるリクエストを発行する。GET メソッドとは、指定した URL のリソースを取り出す HTTP の最も基本的な動作である。サーバは、クライアントから GET メソッドを受け取り、指定された URL のリソースをクライアントに返す。サーバからクライアントに返された URL のリソースが、画面に表示された中身である。

HTTP のデフォルトのポート番号は 80 である。SSL で暗号化され、セキュリティを確保した HTTP は HTTPS と呼ばれ、443 番ポートが使われる。たとえば、Web ブラウザで http://www.toyo.ac.jp にアクセスすると、www.toyo.ac.jp というホスト（Web サーバー）に対して、http プロトコルを用いて、80 番ポートで通信をする。URL の最初 http:// は、http プロトコルを用いていることを意味するが、厳密にはこの http はプロトコルではなく、スキームである。

HTTP で、デフォルトの 80 番以外のポートを使用する場合には、ポートを明示する必要がある。URL の最後に「:ポート番号」として明示する。たとえば、www.toyo.ac.jp の 8080 番ポートであれば、http://www.toyo.ac.jp:8080 となる。Web サーバで 80 番以外のポートが使われ理由として、以下のようなことがある。Web サーバで広く使われている UNIX 系の OS では、1024 番よりも小さいポート番号を開く（そのポートを使うサーバープログラムを動かす）ために、システム管理者の権限（ルート権限）が必要となる。たとえば 8080 番のポートを使えば、システム管理者の権限ではなくて一般ユーザーの権限で動かすことができるため、HTTP サーバープログラムにセキュリティホールがあるときに、一般ユーザー権限が乗っ取られても。システム管理者権限が乗っ取られることを防ぐことができる。そのため、セキュリティのことを考えて、あえて 80 番ではなくて 8080 番ポートを使う場合がある。

【Web サーバ】

Web サーバは、HTTP に則って、クライアントの Web ブラウザに対して、HTML などのリソースを提供するプログラム（ソフトウェア）及びそのプログラムが動作するコンピュータ（ハードウェア）のことである。

【Web ブラウザ】

Web ブラウザは、HTTP に則って、Web サーバに対して、HTML などのリソースを要求して、Web サーバから送られてきた情報を解釈して表示するためのソフトウェアである。Microsoft Windows では Internet Explorer が標準添付され、Mac OS X では Safari が標準添付される。標準添付のブラウザ以外にも、様々な Web ブラウザがある。たとえば、Mozilla Firefox、Google Chrome、Opera 等である。画像を表示せずにテキストだけを表示する Web ブラウザ、スマートフォンや携帯電話端末の様に表示画面の小さい Web ブラウザ、視覚障害者用にテキストを読み上げる Web ブラウザ等、様々なものがある。一般に、Web ブラウザの古いバージョンには不具合が多いため、セキュリティのためには新しいバージョンにする方が良い。

【HTML】

HTML（HyperText Markup Language）とは、Web 上のドキュメントを記述するための言語である。HTML でマークアップされたドキュメントは、他のドキュメントへのハイパーリンクを設定できるハイパーテキストである。Web ブラウザで Web サイトを表示し、「ソースを表示」機能を使う事で、そのサイトの HTML を表示することができる。

【クッキーとセキュリティ】

クッキー（Cookie）とは、HTTP における Web サーバと Web ブラウザ間で状態を管理するプロトコル、あるいはそのプロトコルに基づいて Web ブラウザに保存された情報である。

クッキーは、ショッピングサイトにおけるカートやログイン状態の管理のように、ユーザを識別したり、セッション管理を実現したりする目的で使用される。あるサイトにログインして、次にアクセスした時にパスワードを入力しないでログインをした状態が保存されている時は、ログインしているという情報が Web ブラウザのクッキーに保存されている。掲示板への書き込みで、以前に

入力した名前やメールアドレスがフォームに残っているのも、クッキーを利用している。クッキーにはユーザ名、パスワードを初めとして様々な個人情報が保存されることがあるため、他人が使用する PC を利用する時には、使用後にクッキーを消去すると良い。特に、公共の場所に設置されている PC を使用する場合には、サービスにログインした場合にはログアウトをする、個人情報を入力しない、使用後にブラウザの履歴やキャッシュ、クッキーを消去する、といった対策を取ると良い。また、次の項目で述べるように、クッキーにセッション情報が保存されている場合に、セッション情報 を盗まれる攻撃を受ける一因となることがある。

【Web サイトの脆弱性】

Web サービスにアプリケーションの脆弱性があると、様々な被害が発生する[1]。以下に代表的な例を挙げる。

クロスサイトスクリプティング(Cross Site Scripting; CSS, XSS)は、Web サイトの訪問者の入力をそのまま画面に表示する掲示板等のプログラムに、悪意のあるスクリプトを混入させる攻撃方法、およびその攻撃を許すアプリケーションの脆弱性である。この脆弱性を突いた攻撃をされた Web サイトを訪問すると、攻撃者が埋め込んだ悪意のあるスクリプトを自分の Web ブラウザで実行することとなるため、クッキーの情報が盗み取られたり、ウイルスをダウンロードさせられたり、悪意のあるサイトへの踏み台にさせられる、という被害を受けることとなる。この脆弱性は、HTML タグやスタイルシート(CSS; Cascading Style Sheet)の入力を許容するサイトにおいて、HTML やスタイルシートを出力する時に、スクリプトが埋め込まれないようにタグを変換するエスケープ処理が適切に施されていない時に起きる。

SQL インジェクションは、Web アプリケーションが、ユーザが入力した入力値を元にデータベースを操作する SQL 文を使っている場合に、アプリケーションが想定しない SQL 文を入力値として送り込む事で、データベースを不正に操作する攻撃方法、およびその攻撃を許すアプリケーションの脆弱性である。この脆弱性により、データベース情報を参照されることによる情報漏洩、データベースを書き換えることによる Web サイトの書き換えといった被害が生じ、攻撃者に寄って書き換えられた Web サイトを訪問する事で、ウイルスをダウンロ

[1] Web アプリケーションの脆弱性（NEC）
http://www.nec.co.jp/soft/siteshell/merit/merit01.html

ードさせられたり、悪意のあるサイトへの踏み台にさせられたりする、という被害を受けることになる。この脆弱性は、入力値を SQL 文に使うアプリケーションにおいて、SQL 文を生成する時に、不正な処理が実行されないように入力値を変換するエスケープ処理が適切に施されていない時に起きる。

クロスサイトリクエストフォージェリ(Cross Site Request Forgeries; CSRF, XSRF)は、次のような手順で Web サイトを攻撃する手法であり[1]、クッキーに保存された情報を利用することで、掲示板に意図しない書き込みをさせられる、あるいはオンラインショップで買い物をさせられる、といった被害が起こる。

(1) 攻撃者が、攻撃用の Web ページを作成する。あるいは、HTML メールに攻撃用の画像ファイルを読み込ませる。
(2) 第三者が、攻撃用の Web ページにアクセスする。
(3) 第三者は、攻撃者が用意した任意の HTTP リクエストを送信させられる。
(4) 送信させられた HTTP リクエストによって、攻撃者の意図した操作が行われる。この時に、Web ブラウザが保存しているクッキーを利用する。たとえば、ブラウザがオンラインショッピングサイトのログイン情報をクッキーに保存している場合に、攻撃用の Web ページでショッピングサイトに向けて買い物をするという HTTP リクエストを送信させられる事で、意図せずに買い物をさせられることとなる。

CSRF による被害を防ぐためには、Web サイトへのログイン情報をクッキーに保存する機能を利用する、こまめにログアウトする、攻撃者が用意した攻撃用の Web サイトにアクセスしない、HTML メールを利用しない、メーラーのイメージブロック機能を使う、といった対策が考えられる。

セッションハイジャックは、ネットワーク通信におけるセッションを、通信当事者以外が乗っ取る攻撃である。HTTP におけるセッションハイジャックは、クッキーでセッション管理がなされている場合に、クッキーに保存されているセッション ID を第三者が盗み取り、そのセッション ID を名乗る事で第三者がそのユーザになりすます。セッションハイジャックの手法として、例えばここまでに挙げたクロスサイトスクリプティング、SQL インジェクション、クロスサイトリクエストフォージェリが使われる。

以上、代表的な Web アプリケーションの脆弱性について簡単に述べた。他の脆弱性の例、脆弱性の対策等については、参考サイトを参照のこと。このよう

[1]まだまだ残っている CSRF 攻撃（技術評論社）
http://gihyo.jp/dev/serial/01/php-security/0023

な脆弱性のある Web サービスを利用すると、様々な被害を受けることとなる。脆弱性のある Web サービスを利用しない事がその対策の１つとなるが、Web サービスに脆弱性があるかどうかを一般利用者が判断する事は難しい。また、自分でプロバイダと契約して Web サイトを開設する場合に、Web サービスの脆弱性に対して細心の注意が必要となる。

3-2. メールのしくみ

【メール送信とセキュリティ】

SMTP（Simple Mail Transfer Protocol）は、電子メールを転送するプロトコルである。通常 TCP/25 番ポートを利用する。SMTP は当初ユーザー認証機構を備えていなかったが、POP before SMTP と呼ばれる SMTP プロトコル外の機構による利用ユーザー制限方法が考案され 、さらに、SMTP-AUTH（SMTP Authentication）という認証機構が標準化された。これらの認証機構は、不特定の者による迷惑メールの送信を防ぐことができるが、メール本文が暗号化されるわけではないので、メールが SMTP サーバ間を転送される間で、受信者以外の第三者が通信の中身を傍受する事により、メールの中身 を盗み見られ、あるいは改ざんされる可能性がある。したがって、メールは機密情報を送信するには必ずしも適していない技術である。４章で学習する公開鍵暗号方式を使った S/MIME あるいは PGP によって、メール本文を暗号化し、電子署名（デジタル署名）を付与することができる。

【メール受信とセキュリティ】

POP（Post Office Protocol）は、ユーザーがメールサーバから自分のメールを取り出す時に使用する、メール受信用プロトコル。現在は、改良された POP3（POP Version 3）が使用されている。通常、POP3 では TCP/110 番ポートが使われる。電子メールを読み取る時には、ユーザー名、パスワード、メール本文がインターネット上を平文で流れる。したがって、通信途中で、受信者以外の第三者が通信の中身を傍受することにより、ユーザー名、パスワード、メールの中身を盗み見られる（盗聴）可能性があり、また通信の中身を変えることで改ざんの可能性もある。このように POP はセキュリティの低いプロトコルである。

ユーザー名とパスワードの認証を暗号化した APOP という方法が提案された

が、メール本文は暗号化されず、また暗号化もあまり強度なものではない。ネットワーク経路を暗号化する方法として、次節で解説する SSL プロトコルの上で POP プロトコルを使用する POP over SSL（ポート番号は 995 番）といった方法がある。

他にも、メールサーバ上の電子メールにアクセスし操作するため の IMAP (Internet Message Access Protocol) というプロトコルがある。

【メールの書式】

メールの書式については、RFC5322 という技術文書で定められている。**メールアドレスは**「ローカル部@ドメイン」の形式で、ドメインはメールサーバを特定するホスト名である。ローカル部に使用できる文字は、アルファベットの大文字と小文字、数字、「! # $ % & ' * + - / = ? ^ _ ` { | } ~」といった記号、「.」（先頭と末尾以外で使用可能、２個以上連続してはならない）である。さらに、いくつかの細かいルールがある。

メールで使用する**文字コード**については、最初は US-ASCII のみであったが、MIME (Multipurpose Internet Mail Extensions) により、様々な文字コードが使えるように拡張された。現在の日本語メールでは、MIME の枠組みで定義された ISO-2022-JP が広く使われ「JIS コード」と呼ばれる。最近では、メールの文字コードとして Unicode（UTF-7 または UTF-8）が利用されることも増えて来ている。

元来は、メールはプレーンテキスト形式のみであったが、MIME の普及に伴って、メール本文を HTML によって記述した HTML 形式のメールも使われるようになった。一方、**HTML メール**には、メール本文中に悪意あるスクリプトが埋め込まれる、画像を読み込ませる 事で不正な処理を実行させたりメルを読み込んだ情報を収集したりする、といったようなセキュリティの問題もあり、この点に関しては「4-4. セキュリティ対策」で取り上げる。

メールはヘッダ情報と本文によって構成される。代表的な **ヘッダフィールド**を以下に記す。

(1) From: 送信者のメールアドレス。このフィールドは送信者が自由に設定することが可能であるため、悪意のある者がなりすましをすることが可能である。
(2) To: 受取人（宛先）のメールアドレス。複数のメールアドレスを並べることもできる。
(3) Cc: 本来の送信先以外に、コピーを送信する相手のメールアドレス。

(4) Bcc: 本来の送信先以外に、コピーを送信する相手のメールアドレスで、メール受信者にはそのメールアドレスが見えない。
(5) Reply-To: 送信者が返信先として希望するメールアドレス。
(6) Subject: 話題を表す短い文。
(7) Date: 送信した日時。
(8) Return-Path: SMTP 通信で送信元として伝えられるメールアドレス。
(9) Received: このメールが届くまでに経由したメール転送エージェントの IP アドレスと経由した日時

To, Cc, Bcc に指定したメールアドレスには、すべてメールが配信されるが、それぞれ意味が異なるので、適切なメッセージフィールドを使うと良い。

【迷惑メール】

インターネットの普及とともに、受信者の意向を無視して、無差別大量送信されるメール（**迷惑メール、スパム**）が急増した。宣伝を送信する側から見ると、郵便による宣伝と比べると、安価に大量のメールを送信できるというメリットがあるためである。内容としては、出会い系サイト、アダルトサイト、ネズミ講、マルチ商法、架空請求、オンラインカジノ、薬品販売、等が多い。

メールアドレスは、ウェブページや掲示板に掲載されているメールアドレスを自動的に収集したもの、個人情報の漏洩等がある。このように収集された大量のメールアドレスは、悪質業者間で売買されているため、一度アドレスが収集されると、色々なところから迷惑メールが届くことになる。迷惑メールに対して返信をすると、迷惑メールを送信する者にとって「このメールアドレスは受信者が内容を読んでいるものである」という情報が伝わるため「生きたメールアドレス」として、迷惑メール送信者にとって特に都合の良いメールアドレスのリストに入って広まるため、迷惑メールには直接返信するべきではない。削除するか、メールソフトに迷惑メールであると認識させてフィルタリング機能を向上させるか、メールヘッダの Received フィールドを読む事で送信元のプロバイダを調べて、プロバイダに通報する、といった対策が考えられる。

迷惑メールを規制するために、**特定電子メールの送信の適正化等に関する法律**（略称：**特定電子メール法**、迷惑メール防止法）が制定され、営利団体や個人事業者が自己又は他人の営業につき広告又は宣伝を行うための手段として送信するメールを「特定電子メール」として、特定電子メールの送信に一定の制限を設けた。違反した場合には、行政措置による罰則がある。しかし、４章で

学習するように、ウイルスに感染した多数の PC をボットネットとして操り、ボットネットから迷惑メールを送信する、といった手段によって、迷惑メールの真の送信者を突き止めるのが困難となっている。なお、2008 年に迷惑メール防止法が改定され、従来のオプトアウト方式からオプトイン方式へと変わったが、迷惑メールには返信しない、という原則を考えれば、「メールを送らないでほしい」と返信をすることが必要とされるオプトアウト方式は、そもそもナンセンスであった。

3-3. 様々なアプリケーション層のプロトコル

【DHCP】

DHCP (Dynamic Host Configuration Protocol) とは、コンピュータがネットワーク接続する際に必要な情報を自動的に割り当てるプロトコルのことをいう。DHCP を使うことによって、以下のような情報を自動設定することができる。

(1) ホスト名
(2) IP アドレス・サブネットマスク
(3) デフォルトルーター（ゲートウェイ）
(4) DNS サーバ・DNS ドメイン名
(5) NIS サーバ・NIS ドメイン名
(6) プリンタサーバ
(7) NTP サーバ

現在、多くのインターネットサービスプロバイダでは DHCP サーバを提供しているため、インターネットに接続する PC では「IP アドレスを自動的に取得する」設定にすることで、プロバイダの DHCP サーバから自動的にこれらの情報を取得してインターネットに接続する事が可能となる。また、ブロードバンドルータを利用してインターネットに接続する場合も、ルータの DHCP 機能を使う事で同様に自動設定ができる。

【FTP】

FTP (File Transfer Protocol)は、ネットワークでファイルの転送を行うための通信プロトコルである。認証機能がない簡易な TFTP (Trivial File Transfer Protocol) もある。

【NTP】

NTP (Network Time Protocol) は、ネットワークに接続される機器において、時計を正しい時刻へ同期するための通信プロトコルである。

【Windows のファイル共有】

Windows の**ファイル共有**（共有フォルダ）、**プリンタ共有**の仕組みは複雑である。なぜ複雑なのかというと、歴史的な経緯が複雑だからである。以前は、NetBEUI（NBF:NetBIOS Frames protocol）が用いられていたが、今日は TCP/IP (NBT: NetBIOS over TCP/IP)へほとんど置き換えられている。その上に、SMB (Server Message Block) や CIFS (Common Internet File System) といったプロトコルがある。つまり、上から［SMB / CIFS］→ NetBIOS → TCP/IP という構造である。

NBT では、TCP と UDP の 137,138,139,445 番ポートが使われる。したがって、無防備にファイル共有をしている PC をインターネットに接続すると、インターネットに不要なポートが開放され、セキュリティのリスクが生じる。この問題については、後の授業で再び取り上げる予定である。

【TLS / SSL】

TLS はセキュリティを要求する通信のためのプロトコルであり。TLS の元となったプロトコルが SSL であり、SSL という名称が広く普及しているため、SSL とも呼ばれる。アプリケーション層の任意のプロトコルと組み合わせることが可能で、暗号化、認証、改ざん検出のセキュリティ機能を提供する。HTTP を組み合わせると HTTPS、POP と組み合わせると POP over SSL となる。

【その他】

IRC (Internet Relay Chat): チャット
NNTP (Network News Transfer Protocol): ネットニュース
Telnet: 汎用的な双方向 8 ビット通信
SSH: 暗号や認証などの技術を利用して、安全に通信
SNMP (Simple Network Management Protocol): ネットワーク機器の監視
XMPP (Extensible Messaging and Presence Protocol): インスタントメッセンジャー

３章・章末問題

問 3-1　迷惑メールを受信したときに避けるべき行動はどれか。(IT パスポート試験平成 23 年度秋期)

(1) 電子メールの経路情報などから送信元プロバイダが判明したときに、迷惑メールが送られてくることを、そのプロバイダに通報する。
(2) 発信者に対して苦情を申し立てるために、迷惑メールに返信する。
(3) 迷惑メールは開かずに削除する。
(4) メールソフトの迷惑メールフィルタを設定し、以後、同一発信者からの電子メールを迷惑メールフォルダに振り分ける。

問 3-2　電子メールの安全性や信頼性に関する記述のうち、適切なものはどれか。(IT パスポート試験平成 23 年度秋期)

(1) 暗号化しなくても、受信者以外の者が、通信途中で電子メールの本文や添付ファイルの内容を見ることはできない。
(2) 受診した電子メールの差出人欄の電子メールアドレスが知人のものであっても、本人からの電子メールであるとは限らない。
(3) 受診した電子メールは、必ず受信者に到達する。
(4) 電子メールの本文や添付ファイルの内容を通信途中で改ざんする事はできない。

問 3-3　プロトコルに関する記述のうち、適切なものはどれか。(IT パスポート試験平成 23 年度秋期)

(1) HTML は、Web データを送受信するためのプロトコルである。
(2) HTTP は、ネットワーク監視のためのプロトコルである。
(3) POP は、離れた場所にあるコンピュータを遠隔操作するためのプロトコルである。
(4) SMTP は、電子メールを送信するためのプロトコルである。

問 3-4　電子メールの送信例のうち、受信者への配慮の観点から、最も適切なものはどれか。（IT パスポート試験平成 22 年度秋期）

(1) 会員から抽出した 100 名のアドレスを一度にあて先（To）に入れて、会員満足度調査のアンケートを電子メールで送った。
(2) 自社製品を紹介する大容量の資料を、圧縮せずに電子メールに添付して得意先に送った。
(3) 製品の質問メールへの回答で、その内容を知ってもらいたい複数の顧客のアドレスを Cc に入れて返信した。
(4) 特別企画のホームページの URL を特定の限られた顧客に知らせるために、アドレスを Bcc に入れて送信した。

問 3-5　クッキー(cookie)に関する記述 a～c のうち、適切なものだけをすべて挙げたものはどれか。（IT パスポート試験平成 22 年度秋期）

a　Web サイトを前回閲覧した際に入力した ID やパスワードなどは、別の PC を利用して閲覧する場合でもクッキーで引き継がれるので再入力が要らない。
b　インターネットカフェなどで一時的に PC を借用して Web サイトを閲覧したときは、閲覧が終わったらクッキーを消去すべきである。
c　クッキーに個人情報が保存されている場合、クロスサイトスクリプティングなどで、その個人情報が盗まれることがある。

(1) a, b　(2) a, b, c　(3) a, c　(4) b, c

問 3-6　DHCP の説明として、適切なものはどれか。（基本情報技術者試験平成 23 年度特別）

(1) IP アドレスの設定を自動化するためのプロトコルである。
(2) ディレクトリサービスにアクセスするためのプロトコルである。
(3) 電子メールを転送するためのプロトコルである。
(4) プライベート IP アドレスをグローバル IP アドレスに変換するためのプロトコルである。

4章 情報セキュリティ対策

インターネットの普及とともに、セキュリティの不備を突いた様々な攻撃が増加した。本章では、ネットワークの様々な攻撃方法、サイバー犯罪の実例について理解した上で、そのような攻撃による被害を防ぐためのセキュリティ対策を学習する。セキュリティを軽視する事により、個人的に被害を受けるのみならず、個人情報漏洩等で所属する組織へ損害を与えることもあり、情報セキュリティはますます重要となっている。本章で具体的なセキュリティ対策について学ぶとともに、その技術的背景についての理解を深めてほしい。

学習内容とキーワード

4-1. ネットワークとセキュリティ：*コンピュータセキュリティ、盗聴、なりすまし、改ざん、セキュリティと利便性*

4-2. コンピュータシステムに対する攻撃方法: *ソーシャル・エンジニアリング、ポートスキャン、DoS 攻撃、辞書攻撃、コンピュータウイルス、ワーム、トロイの木馬、スパイウェア、スマートフォンウイルス、ルートキット、ボットネット*

4-3. サイバー犯罪の増加：*ネットワーク利用犯罪、不正アクセス禁止法違反、コンピュータ・電磁的記録対象詐欺*

4-4. セキュリティ対策：*ネットワーク感染、セキュリティホール、脆弱性、ゼロデイアタック、JPCERT/CC、アンチウイルスソフトウェア、ファイアーウォール、プロキシサーバ、DMZ、メール添付感染、ファイル共有ソフト、外部記憶媒体感染、パスワードの管理、ソーシャルエンジニアリング対策*

4-5. 暗号化技術：*暗号化、平文、暗号文、鍵、復号、解読、共通鍵暗号、公開鍵暗号、公開鍵、秘密鍵、RSA 暗号、素因数分解、公開鍵の認証、認証局、SSL、暗号化、認証、改ざん検出、盗聴、なりすまし、 公開鍵証明書、サーバ証明書、電子署名、デジタル署名、 改ざん、ハッシュ関数、ハッシュ値、無線 LAN のセキュリティ、WEP、WPA、WPA2*

4-6. セキュリティポリシー：*情報セキュリティポリシー、機密性、完全性、可用性、個人情報漏洩、情報セキュリティ基本方針、情報セキュリティ対策基準、情報漏洩対策、個人情報保護法、個人情報保護方針*

4-1. ネットワークとセキュリティ

コンピュータセキュリティとは、**災害**、**誤用**および**不正な利用**からコンピュータを守ることである。不正な利用とは、第三者による秘密情報へのアクセスや、許可されていない操作の実行などが含まれ、以下のようなものである。

(1) **盗聴**：インターネットの通信は、暗号化されていないため、中継点にいる人間は誰でも盗聴できる。

(2) **なりすまし**：他人のふりをして不正行為をすること。

(3) **改ざん**：データを破壊したり、書き換えたりされること。

一般に、**セキュリティと利便性**はトレードオフの関係にあるものとされる。たとえば､ID とパスワードによる認証を導入する事でセキュリティが高まるが、利用する度に ID とパスワードを入力することは大変なので､利便性が損なわれる｡利便性を上げるためにパスワードをなくすると､セキュリティが失われる。従来のコンピュータシステムは利便性を優先させ、またインターネットの設計思想が性善説に基づいている。インターネットの普及とともにセキュリティの欠点を突いた犯罪が増加し、セキュリテ ィを向上させるための技術的改良が重ねられて来た。

利便性を優先させたシステムでは、セキュリティが犠牲となっていることがある。また、ソフトウェアの欠陥により、本来操作できないはずの操作ができてしまったり、見えるべきでない情報が見えてしまったりするような不具合を「セキュリティホール」と言う。

セキュリティについて無知なままインターネットを利用し、犯罪者に不正利用されることで、様々な被害を受けることになる。セキュリティについて熟知していても、その危険性がゼロになるわけではないが、一通りの知識を持っていることで、被害を予防できることもある。

泥棒から家を守るためには､泥棒がどのような経路で家に侵入してくるか（玄関なのか､窓なのか)､といった手口をよく知った上で､対策を練る必要がある。同様に、セキュリティについて考えるためには、犯罪者がどのようにして自分の PC を不正利用しようとしているかを知ることが有効である。

Web サーバ、メールサーバ、DNS サーバ等のサーバを運営するサーバ管理者は、サーバに対する不正なアクセスを防ぐために、常に最新のセキュリティ情報を元に対策をする必要がある。企業のネットワーク等のネットワ ーク管理者は、外部から企業ネットワークへの侵入を防ぐために、対策を講じなければな

らない。現代社会では、こういったコンピュータネットワークの専門家のみならず、一般の人たちも、セキュリティの知識を必要とする。なぜならば、家庭のコンピュータをインターネットに接続することで、様々なセキュリティリスクが生じるためである。また、会社等の組織に所属して、そこでウイルス感染等の被害にあうと、業務に支障が出るばかりでなく、会社の機密情報を漏洩し、会社に損害（金銭的損害及び会社の信用損失）を与えることにもなる。

4-2. コンピュータシステムに対する攻撃方法

セキュリティとは、コンピュータシステムに対する攻撃に対して防御をすることである。したがって、セキュリティについて知るためには、コンピュータに対してどのような攻撃が存在するか、その危険性を知ることが第一歩である。以下に、いくつかの攻撃方法を紹介する。

【ソーシャル・エンジニアリング】

ソーシャル・エンジニアリングとは、人間の心理的な隙をついて、話術や盗み見などの社会的手段によってパスワード、個人情報等の情報を入手する、次のような手法である。

(1) **ショルダーサーフィン**：銀行の ATM で暗証番号を入力しているところを肩越しに覗いて盗み見る。パスワードが書かれたメモを盗み見て暗記する。
(2) **なりすまし**：会社の上司やシステム管理者を装って電話してパスワードを聞き出す。銀行や警察を装って電話して暗証番号を聞き出す。宅急便を名乗って電話して住所を聞き出す。
(3) **トラッキング**：ゴミとして破棄されたものから情報を取得する。

人間の心理的な隙をついた詐欺という意味で、パスワードの変更を促すメールを送信し、偽のサイトへ誘導してパスワードを入力させる **フィッシング**や、振り込め詐欺も、同類である。

【ポートスキャン】

２章、３章で学んだように、インターネットの通信は、クライアントが、サーバの IP アドレス宛に、ポート番号を指定して、データ（パケット）を送り、サーバがクライアントに対してパケットを返す、といった仕組みになっている。サーバでは、Web サーバであれば HTTP のポートである TCP/80 番ポート等、

必要なポートを開いて、クライアントからの通信を待っている。通常、使わないポートは閉じられているため、閉じられているポートに対してパケットを送っても、何も返事がない。

攻撃者が、どのポートが開いているかを調べるために、あらゆるポートに対して接続を試みることを**ポートスキャン**と言う。攻撃者は、ポートスキャンによって開いているポートを見つけてから、そのポートに脆弱性があるかどうかを調べ、脆弱性があればそこから侵入をする。

システム管理者が、セキュリティをチェックするためにポートスキャンを実行する事もある。不用意にポートスキャンを実行すると、不正アクセスと見なされる可能性があるので注意が必要である。

このように、不要なポートを開けていることは、そのポートから攻撃をされ得るため、セキュリティリスクとなる。

【DoS 攻撃】

DoS 攻撃（Denial of Service attack）とは、サーバ等に大量の通信データ（パケット）を送りつける攻撃を行い、サービスの提供を不可能な状態にすることである。**サービス停止攻撃**、**サービス拒否攻撃**とも言われる。攻撃を受けたサーバは、大量のパケットを処理しなければならないため、ネットワーク機器の処理能力の限界を超えると、システムが不安定になる、停止する、誤動作する、破壊される、といった被害を受ける。後述のボットネットを使って、多数の踏み台となるコンピュータからいっせいに Dos 攻撃をする **DDoS 攻撃**（協調分散型 Dos 攻撃、Distributed Denial of Service attack）によって、甚大な被害が生じることがある。

【辞書攻撃】

辞書に載っている単語を利用して、パスワードやメールアドレス等の特定文字列を推測する方法を **辞書攻撃**と言う。 フィッシングによって取得された 34,000 個のパスワードを調査したところ、それらの 3.8% は辞書に載っている一単語であり、他の 12% は一単語の末尾に数字を一個加えたものだった[1]（フィッシングにかからない用心深い人を入れた母集団では、もっと割合が低くなるかもしれない）。トップ５は password1、abc123、myspace1、password、

[1] Net users picking safer passwords (ZDNet)
http://www.zdnet.com/news/report-net-users-picking-safer-passwords/150640

blink182 (バンド名)だったと言う。ターゲットの個人情報（自分、恋人、友人、家族の名前、ユーザー名、電話番号、誕生日、出身地等）を加えることもある。英単語の辞書ではなく、全ての文字の組み合わせを試す方法を、**総当たり攻撃**（**ブルートフォースアタック**）と言う。英語の小文字 26 種類 6 文字の総当たり攻撃は、26^6=3 億程度の組み合わせを試し、英語の小文字＋大文字＋数字 62 種類 8 文字の総当たり攻撃は 62^8=218 兆程度の組み合わせを試すことになる。使用する文字の種類と文字数を大きくするほど、総当たり攻撃に対して破られにくくなる。

スパムを送信するために携帯電話のメールアドレスに対して辞書攻撃及び総当たり攻撃がなされている。

【コンピュータウイルス】

コンピュータに被害をもたらす不正なプログラムを**コンピュータウイルス**と言う。コンピュータウイルスを、以下のように区別することもあり、すべてをまとめてウイルスと呼ぶ事もある。

(1) **ウイルス**とは、「自分自身の複写、又は自分自身を変更した複写を他のプログラムに組み込むことによって繁殖し、感染したプログラムを起動すると実行されるプログラム。」(JIS X0008)である。それ自体は独立したプログラムではなくプログラムの断片であり、宿主となるファイルに感染する。

(2) **ワーム**とは、独立したプログラムであり、自身を複製して他のシステムに拡散する性質を持った悪意のあるソフトウェア（**マルウェア**）である。宿主を必要としない。

(3) **トロイの木馬**とは、一見有用なアプリケーションであるが、不正な動作をさせる機能を含んだものである。自己増殖機能がない。

(4) トロイの木馬の中でも、不正な動作の種類によっては**スパイウェア**として区別されることがある。主に、ユーザーに関する情報を、ユーザーの了解を得ずに（インストール時の利用条件に書かれている場合もある）自動的にソフトウェアの作成元へ送信して収集するものをスパイウェアと言う。

PC に感染するウイルスだけではなく、携帯電話や**スマートフォン**に感染するウイルスもある[1]。

---

[1] スマホウイルスはどのくらい怖いのか？（ITmedia, 2011/11/11）
http://www.itmedia.co.jp/news/articles/1111/11/news006.html

【ルートキット】

コンピュータシステムへの侵入をした後で、侵入者が後にコンピュータシステムへ侵入を繰り返すことを可能とするために**ルートキット**をインストールすることがある。ルートキットをインストールされたコンピュータは、攻撃者が自由に操れるようになるため、DoS 攻撃等さらなる攻撃の踏み台にされる。また、**キーロガー**の機能によって、キーボードの入力を傍受されることで、クレジットカード番号やパスワード等の入力が盗み取られる可能性がある。多くの場合、ルートキットはトロイの木馬でもある。

【ボットネット】

ルートキットの技術を使い、**ボット**という外部の人物によってコントロールされるようになったコンピュータによって構成される**ボットネット**と言われるネットワークが広まっている。総務省、経済産業省が連携して、ボットの駆除・対策を目的とした**サイバークリーンセンター**（CCC; Cyber Clean Center）[1]を運営している。CCC のサイトでは、ボットの感染経路として以下の５つを挙げている。

(1) **ネットワーク感染型**：プログラムのセキュリティホールを悪用して感染。
(2) **メール添付感染型**：メールの添付ファイルをクリックして感染。
(3) **Web 閲覧感染型**：ホームページに埋め込まれたウイルスをダウンロードして感染。
(4) **Web 誘導感染型**：迷惑メールの URL 等をクリックしアクセスしたホームページからウイルスをダウンロードして感染。
(5) **外部記憶媒体感染型**：USB メモリ、デジタルカメラ、ミュージックプレーヤーなどの外部記憶媒体を介在して感染。

ボットには、感染している事に気付きにくい、自動で機能追加をする、種類が多い、犯罪を目的とする、という特徴がある。犯罪者は、ボットネットを使って迷惑メールの送信、DoS 攻撃などの攻撃、ネットワーク感染、ネットワークスキャン、自分自身のバージョンアップ、指令サーバの変更、クレジットカード番号やパスワードのスパイ活動をする。

---

[1] https://www.ccc.go.jp/

4-3. サイバー犯罪の増加

警察庁サイバー犯罪対策ウェブサイト[1]の統計によれば、**サイバー犯罪**の検挙件数は、2001 年には 1339 件であったが、2010 年には 6933 件と、9 年間で 5 倍に増加している。内訳は、**ネットワーク利用犯罪が最も多く**、続いて**不正アクセス禁止法違反**、**コンピュータ・電磁的記録対象犯罪**となっている。最も多いネットワーク利用犯罪の中では、詐欺罪が最も多く 3 割を占めている（2010 年)。

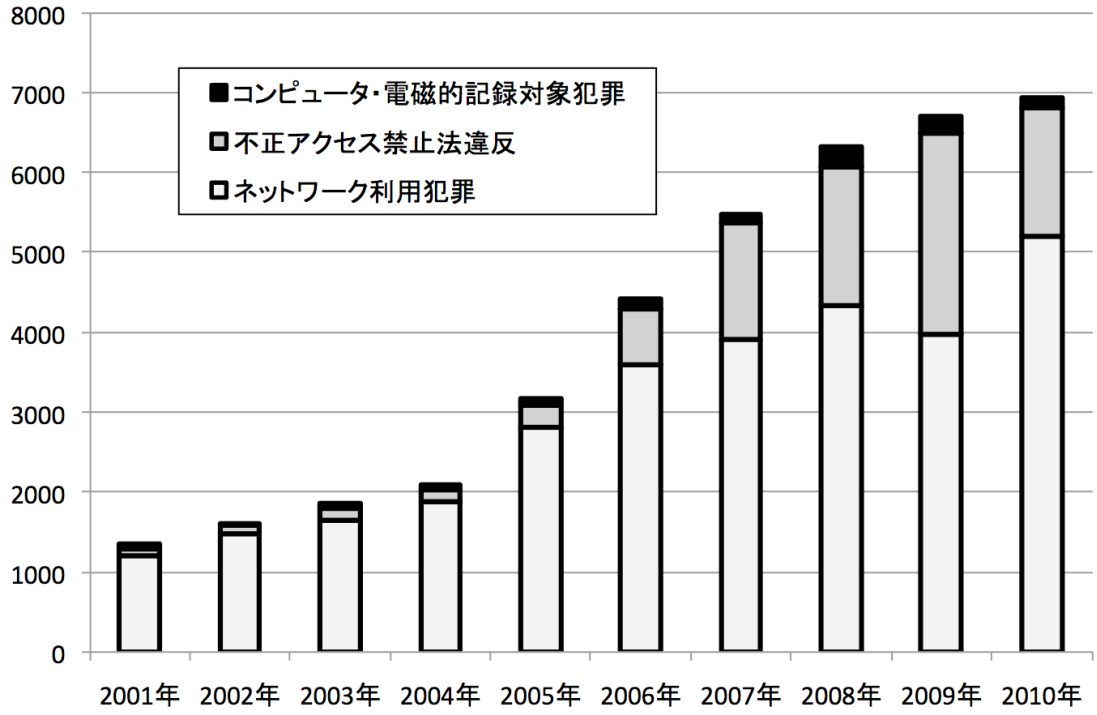

図 4-1 : サイバー犯罪検挙数の推移（警察庁ホームページのデータから作成）

以下に、警察庁のサイトに報告されているサイバー犯罪検挙事例を挙げる。

【ネットワーク利用犯罪】

詐欺 : (1) 東日本大震災の被災者を装い、インターネットの電子掲示板に「義援金のご協力をお願いします」等の虚偽の内容を掲載し、義援金の名目で現金をだまし取ろうとした。 (2) インターネット・オークション会社を装って、サー

[1] http://www.npa.go.jp/cyber/

バに不具合が生じた事実がないにもかかわらず、サーバの修理費用を要求する架空の支払い請求の電子メールを送信して、この電子メールを閲覧した者に修理費用を支払わなければならないと誤信させ、電子マネーをだまし取った。(3)インターネット・オークションサイトに不正アクセス行為を行い、商品を売ると虚偽の出品情報を掲示し、多数の落札者に被疑者らが管理する口座に代金を振り込ませ、だまし取った。不正アクセス禁止法違反でも検挙。

器物破損：音楽ファイル等を装ったコンピュータウイルスを、ファイル共有ソフトの利用者に公開し、これをダウンロードし実行した者のパーソナルコンピュータにウイルスを感染させ、内蔵のハードディスクに保存されているファイルを感染させた。

特定電子メール送信適正化法違反：出会い系サイトの広告宣伝を行うため、大手インターネットサイト等であるかのように偽った数百の虚偽のメールアドレスを使用して、中国やフィリピン等の海外経由で電子メールを不特定多数に送信した。

著作権法違反：他人の著作物である単行本コミックを、ファイル共有ソフトを利用して公衆送信し不特定多数の者に閲覧させ、著作権を侵害した。

商標法違反：ファイル共有ソフト等インターネット上から入手した海賊版ソフトウェアが使用できるよう人気ゲーム機を改造し、インターネット・オークションで「ハック済みゲーム機」として販売した。

わいせつ図面公然陳列：海外のレンタルサーバを利用して携帯電話の掲示板サイトを開設し、利用者にわいせつな画像を掲載 させていた。掲示板を開設した者と、わいせつな画像を投稿した者達が検挙された。

脅迫：被疑者が勤務先の学校を買い異なった事を逆恨みし、勤務先で撮影した動画を動画サイトに投稿すると共に、「生徒の名簿を使って、住所、名前に顔写真を付けてアップロードする」と個人情報をインターネット上に流出させるかのような内容を同サイトに掲載し、脅迫した。

麻薬特例法違反：薬物の譲渡および使用の仲間を募集するインターネット掲示板を開設し、同掲示板を使用して薬物の譲渡が行われることを認識しながら、書き込みを削除することなく放置した。

携帯電話不正利用防止法違反：インターネット上の掲示板に、「飛ばしチップ売ります」などと書き込み、携帯電話会社の承諾を得ず、携帯電話機及び携帯電話用 IC チップ（SIM カード）を販売した。

【不正アクセス禁止法違反】

不正アクセス禁止法違反、電子計算機使用詐欺 : (1) 被疑者の元勤務先である保育園名義のインターネットバンキング口座に不正にアクセスし、現金を自己が管理する架空名義の口座に振り替えた。詐欺罪でも検挙。 (2) インターネット上のサイト上で知り合った者に株式投資を勧めて口座を開設させ、言葉巧みに口座の ID・パスワードを聞き出して不正にアクセスし、別口座に現金５００万円を移した。

【コンピュータ・電磁的記録対象詐欺】

電子計算機使用詐欺：不正に入手した他人名義のクレジットカード情報を利用して、インターネット上のチケット販売サイトでチケットを購入した。

4-4. セキュリティ対策

この節では、これまでに学んだコンピュータのネットワークシステムに対する攻撃、そういった攻撃を元としてのサイバー犯罪による被害を防ぐためのセキュリティ対策について学ぶ。

【ソフトウェアのセキュリティホール対策】

Windows 等の基本ソフトや、その他のプログラムの**セキュリティホール**（**脆弱性**）や設定の不備を悪用し感染する**ネットワーク感染**を防ぐためには、セキュリティホールをなくすことが必要となる。ソフトウェアにセキュリティホールが発見されると、製品の開発元から**修正プログラム**が公開される。Windows であれば、Microsoft Update（Windows Update）を通して修正プログラムが配布されている。常に、最新のバージョンにアップデートする必要がある。ところが、実際には最新のバージョンへの更新がなされていないコンピュータが多いため、すでに発見され、セキュリティホールの修正プログラムが発表されているセキュリティホールを利用して、感染を広めるウイルス、ボットが多い。

Windows XP 以降では、Microsoft Update を、自動的に実行するように設定できるので、それを利用するべきである。また、Microsoft では、毎月第２水曜日（アメリカ時間では火曜日だが、日本では水曜日）に、セキュリティホールに関する更新をまとめてするように計画されている。最低でも、毎月第２水曜日には、その更新をしなければならない。

マイクロソフトでは、マイクロソフトセキュリティーセンター[1]でセキュリティ更新プログラムの情報を公開している。最新の更新では、Windows の重要な更新はいくつあり、それぞれ、どのようなセキュリティホールが修正されたか、調べてみよう。

なお、Windows 以外の OS を使っている場合にも、常に最新のバージョンにアップデートする必要がある。たとえば、Mac OS X では、ソフトウェア・アップデートを定期的に実行するように設定をするべきである。

また、Microsoft 以外のソフトウェアのセキュリテ　ィ更新は、Microsoft Update から更新することができない。したがって、使用するソフトウェアのセキュリティ情報を得て、可能な限り自動的にアップデートする等の設定をして、最新のソフトにアップデートするように心がけるべきである。

セキュリティホールを狙った攻撃が、セキュリティホールの修正プログラムや修正バージョンが提供される前に起こることを**ゼロデイアタック**（ゼロデイ攻撃）と呼ぶ。そのようなリスクもあるため、常にセキュリティ更新を実施していたとしても、その他のセキュリティ対策を採ってリスクを減らす必要性がある。

JPCERT/CC[2]では、深刻かつ影響範囲の広い脆弱性などに関する情報を注意喚起している。ここで、ソフトウェアの脆弱性情報が得られることがある。

訪問した Web サイトに脆弱性がある場合にも、ウイルスをダウンロードさせられる、といった被害を受けることがある。Web サイトの脆弱性については、「3-1 Web サービス」の中で取り上げた。

【アンチウイルスソフトウェア】

アンチウイルスソフトウェアとは、コンピュータウイルスを検出・除去するためのソフトウェアである。単に「アンチウイルス」、または「ウイルス対策ソフトウェア」などとも言う。様々なソフトウェアが販売、またはフリーで配布されている。

コンピュータウィルスの特徴などを記録したデータファイル（**パターンファイル**）とコンピュータ内部でやりとりされるデータを照合する。ウィルスは、頻繁に新種があらわれるため（自動的に新種が次々と生まれるようなウィルス

---

[1] セーフティとセキュリティ センター (Microsoft)
http://www.microsoft.com/ja-jp/security/default.aspx
[2] http://www.jpcert.or.jp/

も存在する)、パターンファイルやウィルス検索エンジンは、頻繁に更新されている。したがって、アンチウイルスソフトをインストールしたら、常に最新のウイルスに対応するようにアップデートをするように設定をする必要がある。

なお、不正なアンチウイルスソフトウェアをダウンロードさせようとする攻撃も存在する[1]。

【不要なポートを閉じる】

4-2 節の「ポートスキャン」の項で説明したように、開いているポートがあるとセキュリティのリスクとなる。コンピュータをサーバとして運用していなくても、Windows では、デフォルトで開いているいくつかのポートがある。Windows XP Professional では、

123/udp (ntp)
135/tcp, 135/udp (rpc)
137/udp (netbios 名前解決)
138/udp (netbios ブラウジング)
139/tcp, 139/udp, 445/tcp, 445/udp (ファイル／プリンタ共有)
500/udp (IPsec の鍵交換)

といったポートが開いているとされている。

基本的には、使わないポートは閉じるべきである。たとえば、NetBIOS サービスを停止すには TCP/IP のプロパティの「全般」タブに表示される「詳細設定」ボタンを押し、「WINS」タブで、「NetBIOS over TCP/IP を無効にする」を選べばよい。これで 137,138,139 番ポートが閉じられる。しかし、135 番ポートのように、簡単に止められないポートも存在する。

【ファイアーウォール】

ファイアーウォール（防火壁）とは、ある特定のコンピュータネットワークとその外部との通信を制御し、内部のコンピュータネットワークの安全を維持することを目的としたソフトウェア、あるいはそのソフトウェアを搭載したハードウェアである（中国国内のインターネットユーザーを「有害情報」から守るために中国政府が設置した大規模なインターネットのフィルタリングをグレ

[1]不正アンチウィルス・ソフトウェアに導くサモア地震のニュース（F-Secure）
http://blog.f-secure.jp/archives/50283874.html

ートファイアーウォール；The Great Firewall of China; GFW と言う[1]。Windows XP SP2 以降では、簡易的なファイアーウォールが搭載されており、デフォルトで有効になっている。

ファイアーウォールには「**パケットフィルタ型**」「**サーキットレベルゲートウェイ型**」「**アプリケーションゲートウェイ型**」があり、それぞれ OSI 参照モデルにおけるネットワーク層（レイヤ３）、トランスポート層（レイヤ４）、アプリケーション層（レイヤ７）で通信の許可／不許可を判断し、制御する（Wikipedia「ファイアーウォール」参照）。この中で、最後のアプリケーション型ゲートウェイとは、パケットではなく、HTTP や FTP といったアプリケーションプロトコルのレベルで外部との通信を代替し、制御するものであり、 **プロキシサーバ**とも呼ばれる。プロキシサーバを使うことで、アクセス URL チェック、ウイルスチェック、情報漏洩検出といった通信の中身のチェックが可能となる。

ブロードバンドルータの NAT 機能を適切に設定することで、パケットフィルタ型のファイアーウォールとして使うことができる。ただし、ルータのパスワードを適切に設定し、外部よりルータの設定画面に接続できないように設定し、ファームウェアを最新のものに更新し、ポートフォワーディングや IP フォワーディングの利用には注意を払う必要がある。

【DMZ】

内部ネットワークと外部ネットワークをファイアーウォールによって隔離して、内部ネットワークを外部ネットワークからの攻撃から守る方法について紹介した。Web サーバーやメールサーバなどのサーバーを運用する場合には、外部からの接続に対して、ポートを解放する必要がある。もしそのようなサーバーを内部ネットワークに置いている場合、それらのサーバーが外部の 攻撃者から攻撃されて侵入された場合には、サーバーを通して内部ネットワークを攻撃される可能性がある。

そこで、組織の内部ネットワークと危険の多い外部ネットワークの間に設置されている隔離されたネットワーク領域（サブネットワーク）を設置する方法があり、このネットワーク領域を**非武装地帯**（DMZ, demilitarized zone）と呼ぶ。

---

[1]中国のグレートファイアウォールを乗り越える「西廂計劃」　ほか（Internet Watch）
http://internet.watch.impress.co.jp/docs/column/security/20100709_379029.html

【メール添付型感染】

メールを通してのウイルス感染を防ぐためには、以下の対策が考えられる。

(1) **HTML 形式の電子メールはプレビューしない。プレビューする場合には、画像ファイルを読み込まない。**HTML 形式の電子メールが危険な理由は２つある。(1) HTML メールには、JavaScript のようなスクリプトを組み込むことができるため、不正なスクリプトを埋め込んだメールを表示しただけで、セキュリティホールを悪用した攻撃を受けてしまうことがある。(2) HTML メールには画像を埋め込むことができる。迷惑メールには、送信者ごとに URL が異なる小さな画像ファイル（ ウェブビーコン）が埋め込まれていて、その URL が呼び出されることによって「誰が迷惑メールを読んだか」という情報を得るようになっている。「メールを読んだ」ことが知られると、そのメールアドレスが「生きている」メールアドレスであることが分かり、迷惑メールが送られてくる件数が増える。また、攻撃用の画像ファイルを読み込ませることで、クロスサイトリクエストフォージェリの攻撃を受ける可能性がある。

(2) **添付ファイル付きの電子メールには十分気をつける。**まず、見知らぬ人からのメールについては、添付ファイルを安易に開いてはいけない。知人からのメールであっても、その添付ファイルが本当に知人から送られて来たものなのか、メールの内容を見て怪しいときには確認をする必要がある。メールの **From に記載されるメールアドレスは、偽装することが可能**であり、第三者が From を知人のメールアドレスに変えてウイルスメールを送る可能性がある。**公的機関を装ったウイルスメール**もあるため、注意が必要である。また、ウイルスの中には、アドレス帳に登録されているメールアドレス宛に勝手にメールを送るものもあるため、そのメールが、確かに送信者本人が書いたものであるかどうか、もし不審な点があれば疑う必要がある。受信した**添付ファイルの拡張子を表示**して怪しいファイルを見分けるための設定をしておくと良い。ファイルの種類をアイコン画像で見分ける習慣がついていると、実行ファイルのアイコンを Word のアイコン画像とする、といったようにアイコンの画像は偽装できるため、ファイルの種類を拡張子で確認する習慣をつける。Windows では、拡張子が表示されない設定となっているため、拡張子を表示するようにする。

なお、メールを送る際には、受信者に「怪しい」と思われないようなメール

を書くことが、マナーである。そのためには、以下のような心配りが必要となる（関連：3-2 章）。

(1) 件名（Subject）に簡潔に具体的な用件を書く。

良い件名：「情報処理実習 E の課題について」

→ 具体性のある件名は、迷惑メールでは自動生成しにくい。

悪い件名：「こんにちは」「よろしくお願いします」

→ 中身を読まないで捨てられてしまう可能性あり。

(2) 信頼できるメールアドレスから送信する。携帯メールのアドレスでは、学生であることが分からない。

→ 過去の講義、DNS について

(3) 発信者の情報を書く。署名を使うと良い。

(4) HTML メールを使わない。

(5) 不要な添付ファイルを送らない。本文に書けば良い内容は本文に書く。

(6) 添付ファイルを送る必要がある場合には、添付ファイルの内容について本文で説明する。

【ファイル共有ソフト】

ファイル共有ソフトとは、インターネットを通じてファイルを不特定多数で共有することを目的としたソフトウェアである。 **ファイル交換ソフト**とも呼ばれる。ファイル共有ソフトの中でも、P2P アプリケーションは、インターネットに対してポートを開いてサーバー的な動作をする場合が多く、またアプリケーション同士が常時接続している場合が多いため、アプリケーションにセキュリティホールがある場合には、ウイルスが P2P に感染拡大する脆弱性を持っている。また、P2P ネットワーク上に存在するファイルの中で、特に匿名性の高いシステムが使われている場合には、ウイルスを感染拡大しようとする人にとって都合が良いため、ウイルスに感染しているファイルが多い。P2P ネットワーク上でダウンロードされているファイルの半分以上は、 ウイルスであるとされている。

Winny や Share などをインストールしたパソコンから、**暴露ウイルス**により個人情報や機密情報が漏洩する事件が発生している。Winny の P2P ネットワーク上に流出した個人情報や機密情報は、P2P ネットワーク上から情報を削除することが困難である、という特徴がある。

【外部記憶の自動実行】

USB メモリ、デジタルカメラ、ミュージックプレーヤーなどの外部記憶媒体を介在してウイルスに感染することがある[1]。他のパソコンで使っていた USB メモリ等の外部記憶に保存されているファイルに、 ウイルスが混入されている場合には、それを実行することでウイルスに感染する。学会発表等で、USB メモリ内にスライド用の PowerPoint ファイルを実行することで､そのパソコンがウイルスに感染し､さらに他のユーザーの USB メモリ内のファイルがウイルスに感染する、といった被害も出ているため、スライドを実行する前に ウイルスチェックをする、ウイルス対策ソフトのマクロ ウイルス対策機能を使う、マクロ実行不可能な pptx ファイルを使う、といったような対策が必要となる。

Windows 2000 以降には、パソコンに USB メモリが接続されると、その USB メモリの中に置かれた autorun.inf というファイルで指定されているプログラムを自動的に実行する機能がある。USB メモリ感染型ウイルスは、この機能を悪用して感染活動を行うため、上記のように明示的にファイ ルを実行しなくても、感染する。対策としては、以下が考えられる。

1. 出所不明の USB メモリを使用しない。
2. 信頼できないコンピュータでは USB メモリを使用しない。
3. USB メモリの自動実行をさせないように OS の設定をする[2]。
4. セキュリティ機能がついた USB メモリを使用する。

【パスワードの管理】

辞書攻撃や総当たり攻撃による被害を防ぐためには、容易に推測されるパスワード（単語や自分の個人情報を組み合わせたもの、qwerty 等）を使わない、小文字、大文字、数字、あるいは記号をまぜてなるべく長い文字数のパスワードとする、定期的にパスワードを変更する、アカウント作成時に付与されたパスワードを変更する、複数のサービスで同じパスワードを使わない、パスワードのメモを残さない、といった対策が必要となる[3]。しかし、そのような覚えにくいパスワードをサービスごとにたくさん作成して、それを頻繁に変更して、

---

[1] USB メモリで拡がるウイルス「オートラン」は、なぜ怖い（ASCII）
http://ascii.jp/elem/000/000/544/544216/

[2] Windows の自動実行機能を無効にする方法（Microsoft）
http://support.microsoft.com/kb/967715/ja

[3] パスワードの管理と注意（IPA）
http://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/pass.html

どこにもメモせず、忘れない、ということはよほどの記憶力がなければ難しく、どこかで妥協をしてしまいセキュリティが低下しかねない。パスワードを管理するソフト（例えば ID Manager[1]）を導入することも 1 つの方法である。

【ソーシャルエンジニアリング対策】

ショルダーサーフィン、なりすまし、トラッキング等のソーシャルエンジニアリング対策として、企業では

1. スクリーンセーバロック
2. クリーンディスク
3. 機密情報書類のシュレッダー破棄の徹底
4. コールバックを利用した ID 払い出し確認
5. 管理者との面識を作る

等の対策が採られている。

フィッシング詐欺のようにサイバー犯罪にもソーシャル的な要素が入っている。安易に騙されないように、警戒心を持つ事が重要である。

4-5. 暗号化技術

【暗号化】

インターネット上での通信は、パケットが相手先に届くまでに数々のルータを経由するために、途中の経路で悪意のある第三者が通信の中身を盗み見ることが可能である。そこで、機密情報をやりとりする際には、通信の中身を傍受されても通信内容が分からない様に、通信内容を**暗号化**する必要が出る。暗号化の手順は、以下の通りとなる。

1. 暗号化したい文（**平文**：ひらぶん）を用意する。
2. 暗号方式を決定し、暗号文を作成（**暗号化**）する。
   暗号方式がきまった上で、暗号文を作成する際に利用する値を**鍵**という。
3. 暗号文を相手に送る。
   暗号文が周囲に盗聴されたとしても、平文は知られずに済む。
4. 正当な受信者が暗号文を**復号**する。
   正当な受信者以外が暗号文から平文を得ようとする不正な作業は**解読**という。

通信の暗号化は、インターネットの技術が生まれるよりも前にも、おこなわ

[1] http://www.woodensoldier.info/soft/idm.htm

れていた。古典的な暗号には、**換字式暗号**（たとえば各文字を A→B→C と一定数シフトする**シーザー暗号**）や**転置式暗号**があり、これらの暗号には「鍵」の概念がない。また、これらの古典的暗号は、比較的解読が容易である。そのため、現代では機密情報の通信に古典的暗号が使われることはないが、機密の保持を目的とせず、冗談の落ち、パズルの解法、ネタばれ情報、不快表現 等を隠すために ROT13 [1]（13 シフトのシーザー暗号、暗号化と復号が同じ）が用いられることがある。

現代暗号は、鍵を用い、アルゴリズムが公開されているものが多い。鍵の取り扱いによって、共通鍵暗号と公開鍵暗号の 2 種類に分けることができる。

【共通鍵と公開鍵】

暗号化と復号に同一の鍵を用いる暗号方式を**共通鍵暗号**と言う。1976 年に公開鍵暗号が登場する前は、暗号と言えば共通鍵暗号であった。一方、 **公開鍵暗号**は、暗号化と復号に別個の鍵を使い、暗号化の為の鍵を公開できるよう にした暗号方式である。

共通鍵暗号の長所は、扱いが簡単で処理速度が速いということであり、短所は、通信の相手先ごとに固有の鍵を作成しなければならないことと、あらかじめ安全な方法で相手に鍵を渡さなければならないことである。共通鍵暗号方式には、DES、AES 等がある。

公開鍵暗号は、**公開鍵**と**秘密鍵**の対になる 2 つの鍵を使って、暗号化と復号を行う暗号方式である。暗号化には公開鍵を用いて、復号には非公開の秘密鍵を用いる。長所は、暗号化に必要な公開鍵のやりとりが容易になることであり、短所は、複雑な計算をするために暗号化と復号に要する処理時間がかかることである。

このように、公開鍵暗号と共通鍵暗号には、それぞれ長所と短所があるため、通常は両方を組み合わせた形で暗号化が実装されている。すなわち、 その場限りの共通鍵を使って暗号化し、その共通鍵の配送のみを公開鍵暗号で行 う。こうすることで、鍵のやりとりが安全になり、また暗号化と復号 に要する処理時間が短くなる。

公開鍵暗号を初めて実現した **RSA 暗号**が、よく用いられている。RSA 暗号は、桁数が大きい合成数の**素因数分解**問題が困難であることを安全性の根拠とした

[1] http://rot13.com/

公開鍵暗号である[1]。

公開鍵暗号方式による暗号化、復号の手順は以下の通りである。

1. 受信者は自分の公開鍵 P を全世界に公開する。
2. 送信者は、公開鍵 P を使ってメッセージを暗号化してから送信する。
3. 受信者は、公開鍵 P と対になる秘密鍵 S を使って受信内容を復号する。
4. 暗号化された文を傍受した者は、公開鍵 P は知っているが、秘密鍵 S は分からない。P から S を割り出すことは、計算時間的に極めて難しい。そのため、暗号文を解読することはおよそできない。

【公開鍵暗号の安全性】

公開鍵暗号は、正当な受信者が正当な方法で作成された暗号文を復号できる「**正当性**」と、正当な受信者以外が暗号文のすべてまたは一部を解読できないという「**秘匿性**」を持つことが要求される。

RSA 暗号では、大きな素数 p,q が与えられたときにその積 n=pq を計算するのは簡単であるが、n を素因数分解するのには時間がかかる、ということが利用されている。理論的には n を素因数分解することが可能であるが、現実的に時間がかかりすぎてしまうため、解読が困難となるような、桁数の大きい n を選ぶのである。

公開鍵暗号は、秘密鍵が漏洩すれば解読されてしまう。また、秘密鍵を失ったら、復号ができなくなる。したがって、秘密鍵の取り扱いには注意が必要である。

【公開鍵の認証】

公開鍵暗号の安全性を確保するには、どの公開鍵がどのユーザのものであるのかという対応をきちんとつけておく必要がある。もし、公開鍵とユーザとの対応が間違っていると、間違ったユーザの公開鍵を使って暗号文を送信してしまう。そこで、一般に信頼できる第三者機関が**認証局**を公開鍵とユーザーの情報を対応づけする方法が取られている。

【SSL による認証】

３章で解説した TLS (SSL)は、様々なアプリケーション層のプロトコルと組み合わせることが可能で、特に Web と組み合わせて、ウェブ認証としてよく用

[1] RSA 暗号体験入門（CyberSyndrome) http://www.cybersyndrome.net/rsa/

いられる。SSL は**暗号化、認証、改竄検出**の機能を提供する。すなわち、**盗聴、なりすまし、改竄を防ぐ**。

（1）**暗号化**：**盗聴を防ぐ**ために、共通鍵暗号方式に基づく暗号が提供される。クライアントとサーバーの双方で生成した乱数から共通鍵が生成される。鍵の盗聴を防ぐために、サーバーの公開鍵で鍵を暗号化するか、あるいは公開鍵暗号方式で鍵を交換する（Diffie-Hellman 鍵共有アルゴリズム）。

（2）**認証**：**なりすましを防ぐ**ために、サーバの公開鍵の正当性を保証する**公開鍵証明書**に基づく認証（**サーバ証明書**）が提供される。サーバ証明書は、サーバの公開鍵を認証局の秘密鍵で暗号化した**電子署名**（**デジタル署名**）であり、受信者は電子署名を認証局の公開鍵で検証し、サーバの公開鍵の正当性を確認する。サーバー証明書にはホスト名が書き込まれており、クライアントは自分が接続しようとしているサーバーのホスト名と一致するかどうか確認することができる。証明書には**有効期限**が設定されている。認証局そのものの信頼性は、信頼できる認証局から認証を受けることによって確認される。したがって、通常ウェブブラウザをインストールする際に、実績ある大手の認証 機関の**ルート証明書**が**信頼できる認証局**として登録される。なお、信頼できる認証局からの認証を受けず、自分で自分を認証している証明書は、「私は信頼できます、保証します」と言っている詐欺と同じで、信頼できない。このような証明書を、オレオレ詐欺にもじって「オレオレ証明書」などと揶揄されることがある。

（3）**改ざん検出**：送信するデータと、（1）で生成された共通鍵から、**ハッシュ関数**によって**ハッシュ値**（**メッセージダイジェスト**、**ダイジェスト**）を生成し、データに付加する。データが第三者によって改竄された場合、第三者は共通鍵を知らないためにハッシュ値を付加することができないため、改 ざんが検出される。

このように、SSL は安全に通信をするために作られたプロトコルであるが、「SSL だから安全である」とは言えない。日頃、どのようなことに気をつけるべきであろうか。特に、パスワードや個人情報を入力する Web サイトを安全に利用する、すなわちフィッシング詐欺の被害を防止する方法について、「安全な Web サイト利用の鉄則[1]」（産業技術総合研究所）で解説されている。

【無線 LAN のセキュリティ】

無線 LAN は、電波によって通信が行われるため、第三者によって通信内容を

[1] https://www.rcis.aist.go.jp/special/websafety2007/

傍受され、盗聴、なりすまし、改竄される危険性がある。したがって、暗号化通信によってセキュリティを確保する必要性がある。 解読技術が進んでいるため、やや古い暗号方式である WEP は簡単に解読されてしまう[1]。WEP は暗号化としては意味をなしておらず、WPA または WPA2 を使うべきである。

4-6. 情報セキュリティポリシー

【情報セキュリティポリシー】

情報セキュリティポリシーとは、企業などの組織における情報資産（デジタルデータのみならず紙媒体も含む）の情報セキュリティ対策について総合的・体系的かつ具体的にとりまとめたものである。単にセキュリティポリシーと呼ばれることも多い。検索エンジンで「セキュリティポリシー」と検索してみよう。様々な企業、自治体等のセキュリティポリシーを読むことができる。

情報セキュリティとは、JIS Q 27002 によって、情報の機密性、完全性、可用性を維持することと定義されている。それぞれ、以下のような意味である。

機密性：アクセスを認められた者だけがアクセスできること。

完全性：情報が破壊、改竄又は消去されないこと。

可用性：情報へのアクセスを認められた者が、必要な時に情報にアクセスできること。

情報セキュリティ対策を十分にしないと、企業では顧客の情報が漏れてしまうなどの情報漏洩・情報流出、情報システムの停止やデータの破壊等の損害を受けることになる。2004 年に起きた Yahoo！BB 顧客情報漏洩事件は、不正アクセスによる約 450 万人分の**個人情報漏洩**で、ソフトバンク BB の公表した被害総額は 100 億円を超える。

情報セキュリティポリシーは**情報セキュリティ基本方針**と**情報セキュリティ対策基準**で構成される。「基本方針」で根本的な考え方を定め、必要に応じて Web サイトで公表する。「対策基準」で、基本方針を実現するために、具体的に遵守するべき内容を記述する。たとえば、人的セキュリティ、技術的セキュリティ、物理的・環境的セキュリティなどに分けて、それぞれ対策基準を策定する。情報セキュリティポリシーに含まれない実施手順で、対策基準に定められ

---

[1] 一瞬にして無線 LAN の WEP を解読する方法がついに登場、まもなく解読プログラムを公開予定（Gigazine）
http://gigazine.net/news/20081013_wep_morii/

た内容を、業務上で実施するための手順を具体的に表す。

システム上のセキュリティ対策が適切にされていても、組織に所属する人のセキュリティ意識が低ければ、適切な運用ができないため、このようなセキュリティポリシーを組織として定め、文書化し、構成員が実行できるように組織として取り組む。

セキュリティ管理の国際的なガイドラインとしては、BSI（英国規格協会）が作成した BS7799 という企業・団体向けの情報システムセキュリティ管理のガイドラインが有名である。BS7799 は以下の 2 部から構成され、

第 1 部：情報セキュリティマネジメントのための実践規範

第 2 部：情報セキュリティマネジメントシステムのための仕様

具体的には以下の 10 個のセキュリティ管理分野が規定されている。

(1) セキュリティ基本方針
(2) 組織のセキュリティ
(3) 資産の分類および管理
(4) 人的セキュリティ
(5) 物理的および環境的セキュリティ
(6) 通信および運用管理
(7) アクセス制御
(8) システムの開発および保守
(9) 事業継続管理
(10) 適合性

日本では、BS7799 の第 2 部を基にした ISMS 適合性評価制度が実施され、企業の情報セキュリティマネジメントシステム(ISMS)が、BS7799 の第 1 部を元とした ISO/IEC 17799 に準拠していることが認定される。

IPA（情報処理推進機構）では、中小企業向け情報セキュリティ対策のための自社診断シートとパンフレットを作成している[1]。自社診断シートの具体的な情報セキュリティ対策のチェック項目を見て、それぞれの項目がどのような理由でチェック項目としてあげられているか、考えてみよう。

【情報漏洩対策】

情報セキュリティ対策の目的の 1 つに、**情報漏洩対策**がある。情報セキュリ

[1] 中小企業向け情報セキュリティ対策（IPA）
http://www.ipa.go.jp/security/manager/know/sme-guide/

ティの観点からは、機密情報が漏洩する事は情報の機密性が失われることとなる。2004年にYahoo! BB登録者の個人情報約460万人分が漏洩した事件[1]では、ソフトバンクはYahoo!BB加入者全員に、お詫びとして500円の金券を送った。ソフトバンク BB が発表した被害総額は 100 億円を超える。その後、様々な個人情報漏洩事件が発生し、報道されている。このような情報漏洩事件が発覚すると、損害賠償で金銭的な被害を受け、企業の信用を失う。

個人情報を含む機密情報が漏洩する要因には、以下のようなものがある。

(1) ノートパソコンやUSBメモリ等の記憶媒体の持ち運びと紛失、盗難[2]
(2) コンピュータウイルスの感染[3]
(3) 悪意ある者による不正アクセス
(4) 業務委託先を含む内部関係者の意図的な漏洩

【プライバシーと個人情報】

2003 年に**個人情報の保護に関する法律**（略称：**個人情報保護法**）が成立し、2005 年に全面施行された。この法律により、5000 件を超える個人情報を所持して事業に用いている事業者は個人情報取扱事業者とされ、個人情報取扱事業者が法律に定められている適切な対処を行わないと、刑事罰が科される場合がある。

個人情報、プライバシーに対する関心の高まりから、多くの企業のウェブサイトではプライバシーポリシーあるいは**個人情報保護方針**が定め、収集した個人情報をどのように取り扱うかを明記している。ウェブサイトによっては、この中に「第三者に情報提供する場合がある」と明記されている場合 もあり、個人情報をインターネットに送信する際には、プライバシーポリ シーを読んで納得することが求められる。

【何が個人情報なのか】

個人情報保護法第２条では、個人情報とは「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を

---

[1] 主な個人情報流出事件（本川裕）
http://www2.ttcn.ne.jp/honkawa/2795b.html
[2]どうする？USBメモリによる情報漏えいやウイルス感染（ASCII）
http://ascii.jp/elem/000/000/455/455750/
[3] 警視庁の情報１万件が流出…巡査長ＰＣウィニー感染で（読売新聞）
http://www.yomiuri.co.jp/net/security/ryusyutsu/20070613nt0d.htm

識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。」と定義されている。氏名、生年月日、電話番号、住所は個人情報である。メールアドレスについては議論があるが、個人情報であると解釈される場合が多い。携帯電話の契約者固有 ID は、携帯電話会社によっても解釈が分かれている[1]。

[1] ウィルコムから回答「契約者固有 ID は弊社にとって個人情報」（高木浩光）
http://takagi-hiromitsu.jp/diary/20100403.html

４章・章末問題

問 4-1　外部のストレージサービスの利用を検討している。可用性の観点でサービスを評価する項目として、適切なものはどれか。(IT パスポート試験平成23 年度秋期)

(1) 緊急のメンテナンスに伴うサービスの計画外の停止期間
(2) サービス利用の際のユーザインタフェースの分かりやすさ
(3) 保管データや利用者に対するアクセス権の設定の自由度
(4) 利用するストレージの単位容量当たりの費用

問 4-2　受診した電子メールに PKI（公開鍵基盤）を利用したディジタル署名が付与されている場合に判断できる事だけを全て挙げたものはどれか。(IT パスポート試験平成 23 年度秋期)

a 電子メールの添付ファイルはウイルスに感染していない。
b 電子メールの内容は通信途中において、他の誰にも盗み見られていない。
c 電子メールの発信者は、なりすましされていない。
d 電子メールは通信途中で改ざんされていない。

(1) a, b　(2) a, c　(3) b, d　(4) c, d

問 4-3　電子メールを介したウイルスの被害に遭わないために注意するべきこととして、適切なものだけをすべて挙げたものはどれか。(IT パスポート試験平成 23 年度特別)

a 信用できる人からの電子メールであっても、添付ファイルのウイルスチェックを行う。
b 添付ファイルの種類が音声や画像などの非実行ファイルであっても、ウイルスチェックを行う。
c 不審な電子メールは、メールソフトのプレビュー機能で内容の安全性を確認してから閲覧する。

(1) a, b　(2) a, b, c　(3) a, c　(4) b, c

問 4-4　A 社の Web サーバは、認証局で生成した Web サーバ用のディジタル証明書を使って SSL/TLS 通信を行っている。PC が A 社の Web サーバに SSL/TLS を用いてアクセスしたときに PC が行う処理のうち、サーバのディジタル証明書を入手した後に、認証局の公開鍵を利用して行うものはどれか。（情報セキュリティスペシャリスト試験平成 23 年度秋期）

(1) 暗号化通信に利用する共通鍵を生成し、認証局の公開鍵を使って暗号化する。
(2) 暗号化通信に利用する共通鍵を認証局の公開鍵を使って復号する。
(3) ディジタル証明書の正当性を認証局の公開鍵を使って検証する。
(4) 利用者が入力して送付する秘匿データを認証局の公開鍵を使って暗号化する。

問 4-5　SSL に関する記述のうち、適切なものはどれか。（IT パスポート試験平成 23 年度秋期）

(1) Web サイトを運営している事業者がプライバシーマークを取得していることを保証する。
(2) サーバのなりすましを防ぐために、公的認証期間が通信を中継する。
(3) 通信の暗号化を行うことによって、通信経路上での通信内容の漏洩を防ぐ。
(4) 通信の途中でデータが改ざんされたとき、元のデータに復元する。

問 4-6　ブルートフォース攻撃に該当するものはどれか。（応用情報技術者試験平成 23 年度秋期）

(1) 可能性のある文字のあらゆる組み合わせのパスワードでログインを試みる。
(2) コンピュータへのキー入力を全て記録して外部に送信する。
(3) 盗聴者が正当な利用者のログインシーケンスをそのまま記録してサーバに送信する。
(4) 認証が終了してセッションを開始してる、ブラウザと Web サーバの間の通信で、Cookie などのセッション情報を盗む。

問 4-7　情報セキュリティに関して発生したインシデントのうち、可用性が損なわれる直接の原因となったものはどれか。（IT パスポート試験平成 23 年度特別）

(1) PC がウイルスに感染し、知らないうちに PC 内の情報が流出した。
(2) 空調の故障で温度が上がり、サーバが停止した。
(3) サーバに不正侵入されて個人情報が盗まれた。
(4) ファイルの中の取引データの金額を誤って更新した。

問 4-8　職場でのパスワードの取扱いに関する記述 a～d のうち、適切なものだけを全て挙げたものはどれか。(IT パスポート試験平成 23 年度秋期)

a 業務で使用するパスワードをプライベートで Web サービスに利用する。
b 個人用パスワードはシステム管理者にも教えない。
c パスワードは定期的に変更するだけでなく、第三者に知られた可能性がある場合にも変更する。
d 付与された初期パスワードは、最初にログインしたときに変更する。

(1) a, b, c　(2) a, c　(3) b, c, d　(4) c, d

問 4-9　情報セキュリティ基本方針の説明として、適切なものはどれか。(IT パスポート試験平成 23 年度秋期)

(1) 一度決められた情報セキュリティ基本方針は、ビジネス環境や技術が変化しても変更すべきでない。
(2) 情報セキュリティに関する組織の取り組み姿勢を示したものであり、組織のトップによって承認され、公表される。
(3) セキュリティビジネスを拡大するための重点的な取組みについて、株主や一般に広く公開されるものである。
(4) 組織のセキュリティの考え方に基づいて、具体的なセキュリティ施策について述べたものである。

問 4-10　プライバシーマークを取得している事業者が、個人情報に関する理念や取組みを内外に宣言する文書はどれか。(IT パスポート試験平成 23 年度特別)

(1) 個人情報保護ガイドライン　(2) 個人情報保護規定
(3) 個人情報保護方針　(4) 個人情報保護マニュアル

問 4-11　オンラインショッピングサイトに接続したとき、ブラウザに SSL 鍵マークが表示された。さらに、サーバ証明書が、目的のオンラインショッピングサイトの運営者のものであることを確認した。このとき、次の a～c のうち、判断できるもの（○）と判断できないもの（×）の適切な組合せはどれか。（IT パスポート試験平成 22 年度秋期）

a　アクセスしているショッピングサイト運営者の財務状況は安定している。
b　アクセスしているショッピングサイトは偽のサイトではない。
c　利用者が入力した個人情報、注文情報を途中経路で盗み見られることはない。

	a	b	c
(1)	○	○	○
(2)	×	○	○
(3)	×	○	×
(4)	×	×	○

問 4-12　攻撃者が、システムの利用者になりすましてシステム管理者に電話をかけ、パスワードを忘れたと言ってパスワードを初期化してもらい、システムに侵入した。このような行為を何というか。（IT パスポート試験平成 22 年度春期）

(1) Dos 攻撃　　(2) 総当たり攻撃
(3) ソーシャルエンジニアリング　　(4) バックドア

問 4-13　非常に大きな数の素因数分解が困難なことを利用した公開鍵暗号方式はどれか。（基本情報技術者試験平成 23 年度特別）

(1) AES　(2) DSA　(3) IDEA　(4) RSA

問 4-14　企業のネットワークにおける DMZ の設置目的として、最も適切なものはどれか。（IT パスポート試験平成 23 年度特別）

(1) Web サーバやメールサーバなど、社外に公開したいサーバを、社内のネットワークから隔離する。
(2) グローバル IP アドレスをプライベート IP アドレスに変換する。
(3) 通信経路上にあるウイルスを除去する。
(4) 通信経路を暗号化して、仮想的に専用回線で接続されている状態を作り出す。

関　勝寿（せきかつとし）
東洋大学経営学部　准教授
東京大学大学院農学生命科学研究科博士課程修了。博士（農学）。
応用情報技術者。環境科学、土壌科学を専門とし、IT を活用した研究・教育をしている。東洋大学経営学部では、これまで「情報処理実習 A」（オフィスソフトの使い方）、「情報処理実習 E」（情報セキュリティ）、「情報処理実習 F」（Web ページの作成）、「数理・情報実習講義 A」（情報処理とプログラミングの基礎）「数理・情報実習講義 B」（Java で学ぶアルゴリズムとデータ構造の基礎）といった多彩な情報科目を担当してきた。
ホームページ：http://www2.toyo.ac.jp/~seki_k/
Twitter: @seki

ネットワークと情報セキュリティ　―安全にネットを使う基礎知識―
Network and information security – Literacy for using network safely –

2012 年 5 月 10 日　初版発行

発行所　東洋大学経営学部

http://www2.toyo.ac.jp/~seki_k/security/