ネットワーク通信(ネットワークサービス)

1　ポートとネットワークサービス

TCP/IP プロトコルによりコンピュータ同士は、いくつものネットワークを経由しながら、遠方のコンピュータと接続することが可能となった。この機能により、様々なネットワークを利用したサービスが利用できるようになっている。

サービスを提供する側のコンピュータは一般的に、**サーバ**と呼ばれる。逆にサービスを利用する側のコンピュータは**クライアント**と呼ばれる。

1.1　ポート番号

サーバとなるコンピュータ側では、１台のコンピュータで様々なサービスを提供することから、サービスを区別する必要がある。ここで用いられるのが、**ポート番号**である。

１台毎のコンピュータに割り当てられた **IP アドレス**を、電話番号に例えるなら、**ポート番号**は**内線電話番号**に例えることができる。サーバは、サービスを要求してきたクライアントの指定するポート番号に対応した、サービスを提供するプログラムを起動する。そのサービス提供のプログラムでは、データを転送するプロトコルに沿ってサーバとクライアント間でデータ交換を行う。

表 1: ポート番号とサービスプログラム

ポート番号	プロトコル	概要
20	ftp	ファイル転送 (データ)
21	ftp	ファイル転送 (命令)
22	ssh	ファイル転送 (命令)
23	telnet	リモート接続
25	smtp	電子メール転送
53	DNS	ドメインネームサーバ
70	gopher	WWW(古い規格)
80	http	WWW
110	pop3	メールダウンロード
119	nntp	インターネットニュース
210	wais	ネットワークデータベース
512,513,514	rlogin 等	リモート接続
540	RIP	ルーティング情報

2　ドメインとルーティング

2.1　DNS(Domain Name Service)

IP アドレスによって、情報交換をする相手のコンピュータを指定することができるが、IPv4 でさえも 32 bit の数値の羅列であり、ユーザにしてみれば記憶することが難しい。

そこで電話帳の様に、名前から IP アドレス を調べる機能が必要となる。このための情報交換のプロトコルは、ドメインネームサービスと呼ばれる。

ドメインとは、所属機関毎に割り当てられた名前であり、以下のように意味を持つ。

nicole　.ei　.fukui-nct　.ac　.jp

.jp：国ドメイン

.ac：組織種別

.fukui-nct：組織ドメイン

.ei：サブドメイン

nicole：ホスト名

表 2: 国ドメインと組織種別

国	国ドメイン	組織種別	アメリカ	日本
アメリカ	なし	企業	.com	.co.jp
日本	jp	政府	.gov	.go.jp
イギリス	uk	教育機関	.edu	.ac.jp
ドイツ	de	ネットワーク組織	.net	.ne.jp
フランス	fr	公益法人	.org	.or.jp
オーストラリア	au	軍事組織	.mil	
カナダ	ca	商業目的	.biz	
トンガ王国	to	情報提供目的	.info	
ツバル共和国	tv	個人名ドメイン	.name	

2.2　RIP(Route Information Protocol)

TCP/IP では、IP アドレスのネットワーク番号部分を見て、パケットの中継先を選択する。しかしながら組織内部でのネットワーク構成なども変化するため、ルータ間でパケットを何処のルータ宛てに転送するかといった情報を一定時間ごとにやりとりしている。この宛て先情報の転送プロトコルは、RIP と呼ばれる。

3　電子メール

電子メールは、非常に迅速にメッセージを相手に届けることができ、そのメッセージを蓄積・加工・編集・転送できる。また、音声や画像といった情報も、複雑な文字情報に置き換えることで、転送できるようになっている。

t-saitoh　@　ei.fukui-nct.ac.jp
ユーザ名　　ドメイン名
ホスト名やサブドメイン名は、省略できる場合もある。

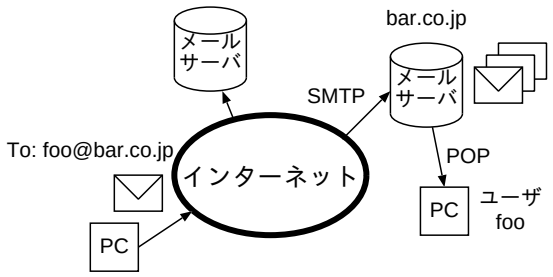

図 1: 電子メールとプロトコル

メールは、利用者のコンピュータに直接届けられるわけではなく、多くの場合はメールを蓄積する**メールサーバ**に送られる。利用者がメールを読む場合、メールサーバから自分の端末に蓄積されたメッセージを読み込み、メッセージを確認する。

このメールのやり取りにおいて、**メールを送る**時、あるいは**メールサーバ間でメールを中継**するときには、SMTP(Simple Mail Transfer Protocol) が用いられる。一方、**メールサーバからメールを読み出す**ときには、**POP** や **IMAP** と呼ばれるプロトコルが用いられる。

4　WWW(World Wide Web)

インターネットが急速に発展した原因は、情報の検索・提供システム WWW(World Wide Web) がある。これらのサービスでは、以下のようなプログラム用いられる。

WWW サーバ 情報を提供するプログラム。Apache(Unix), IIS(NT) が有名。

ブラウザ HTML などで記載された文字・画像・音声を組み合わせた情報に応じて表示するソフトウェア。Netscape Navigator,Internet Explorer が有名。

4.1　URL

インターネット上では、膨大な情報リソースが存在するため、その情報の保存されているの場所を、一意に表記するための記法が必要であり、一般的に **URL(Uniformed Resource Locator)** と呼ぶ。[1]

表 3: URL の例

http	://	www.fukui-nct.ac.jp	/	~t-saitoh/index.html
プロトコル		サーバコンピュータ名		サーバ内のファイル位置

[1]最近では、場所以外の指定にも使われるため、URI(Uniformed Resource Indicator) という用語が用いられる。

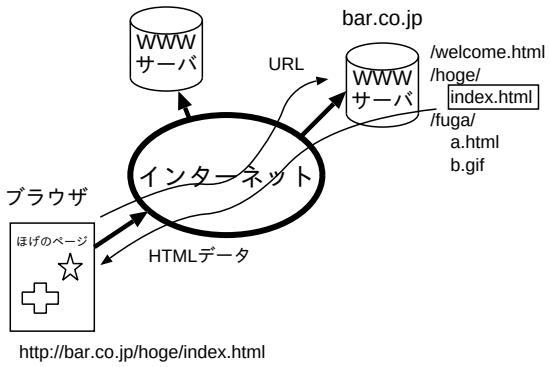

図 2: WWW とプロトコル

4.2 http(Hyper Text Transfer Protocol)

WWW において最も利用されているプロトコルであり、**HTML(Hyper Text Markup Language)** という文書のレイアウトを記述する言語によって書かれた文字データや、その中に埋めこまれる画像・音声などを転送する。

HTTP では、サーバとの HTML や画像などのデータのやりとりを行うだけ。HTML で指定されたレイアウトに従って画面に情報を表示するプログラムはブラウザ (Browser) と呼ばれる。

4.3 ftp(File Transfer Protocol)

ファイル転送プロトコル ftp (File Transfer Protocol) は、ネットワーク上に公開されているプログラムや特殊データを転送するためのプロトコルである。

WWW が普及する以前では ftp は、そのコンピュータの利用許可のあるユーザが、自分のコンピュータとのデータ交換に使われるのが多かった。しかし最近では、任意の利用者に公開するため、匿名による ftp 接続 (anonymous ftp) という方法がとられる。

4.4 nntp(Network News Transfer Protocol)

ネットワークニュースとは、任意の利用者が掲示板に情報を書き込む様に、意見や情報を交換するための物であり、様々なカテゴリ別に色々な情報が交換されている。全世界的なネットニュースでは、`alt.*`が有名。日本では、営利使用目的が禁じられているが `fj.*`では、技術的な情報なども交換されている。

4.5 サーチエンジン

インターネット内に存在するデータは巨大であり、その中から目的のデータを探すのは極めて大変である。このために保存されているキーワードと URL のデータベースから、該当するサイトを検索するシステムは、サーチエンジンと呼ばれる。

Directory 型 Yahoo に代表される方式で、ページ作者が URL と宣伝文章をカテゴリ別に登録する方式。カテゴリの中から、必要最低限の情報を探すのに便利。

Robot 型 google に代表される方式で、サーチロボットがリンクをたどりながら文章中のキーワードと URL を対応づけたデータベースを自動的に作成する。全インターネットの情報は巨大であり、巨大なデータベースシステムを構築しないと困難。

5 リモート接続

ネットワーク接続した先のコンピュータの、資源を用いる場合 **telnet,rlogin,ssh** 等のリモート接続プロトコルが用いられる。(ssh は次章で説明)

5.1 telnet

オペレーティングシステムの UNIX で使われる、最もシンプルなリモート接続方法であり、相手側コンピュータの利用権限があれば、キーボード入力により様々な命令を伝えることができる。[2]

管理者の利用権限を持てば、接続先のコンピュータを自由に操れるため、クラッキングの最終段階では telnet が用いられる。このため最近では telnet プロトコルは、外部組織から利用できないように設定するのが普通である。

5.2 rlogin

接続先のコンピュータに命令を実行させたり、ファイルをコピーしたりといった操作を行うためのプロトコル。

接続相手の確認方法が単純であるため、セキュリティ的に問題があり、これも外部組織からは利用できないように設定するのが普通。

6 公開鍵暗号

6.1 パケット盗聴 (スニッファ)

Ether ネットでは、基本的にバス型結線であるため、同じ信号線を共有する 10BASE/2,5 や単純な HUB では、パケットの盗聴が可能である。

またインターネットを介した通信で、サーバ等がクラッキングされると、盗聴用プログラムを仕掛けられ、通信データを盗み読みされる可能性がある。最近の事例では、無線 LAN を利用した通信でも、電波を他の機器で受信しパケットを盗聴される可能性もある。[3]

このため不特定多数の利用が想定される場所では、以下に述べるような暗号化は必須である。

[2]MS-Windows や X Window の様に、グラフィック画面とマウスによるコンピュータ操作は、一般的に GUI(Graphical User Interface) と呼ばれる。しかしマウス操作だけでは、命令を複雑に組み合わせることが難しい。これに比べ、キーボード入力による命令は、簡易的なプログラム命令を使い、複雑な処理も可能となる。この様にキーボードによるテキストベースの操作は、CUI(Character User Interface) と呼ばれる。

[3]無線 LAN では WEP と呼ばれる暗号化や指定機器以外がアクセスできない利用制限が必須

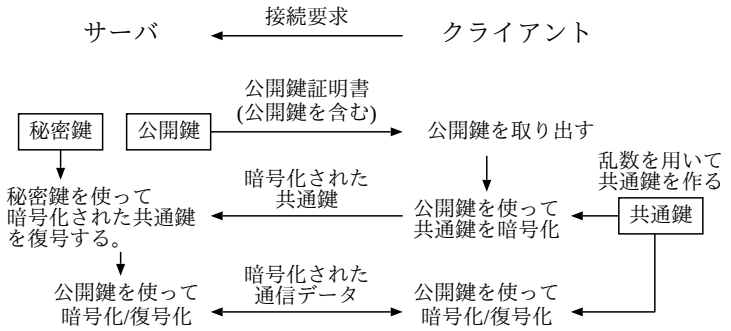

図 3: 公開鍵暗号を用いた通信

6.2 パケット盗聴対策

このような不正アクセスを防ぐためには一般的に、以下の手法が用いられる。

ワンタイムパスワード パスワードが盗聴によって盗まれると、なりすましにより被害が拡大する可能性がある。そこでパスワードを盗み見られても、同じパスワードを使わなければ良いという考え方。利用者は、専用のソフトによって作られた複数の使い捨てパスワードを記録して持ち、接続する度毎に次々と違うパスワードを用いる。しかし通信するデータなどは、暗号化しないためその他のデータ等は盗み見られる危険性がある。

共通鍵暗号 パスワードも含めた全てのデータ通信を、盗み見られる危険性をなくすために、暗号化が用いられる。簡単な方式では、一つの共通鍵を用いて暗号化を行う。

DES 鍵長 56 bit。処理は簡単な半面、鍵が間違って公開されると簡単に解読できる可能性がある。

公開鍵暗号 暗号化の安全のために、公開鍵と秘密鍵の 2 つを用いた通信方法。

RSA 大きな数の素因数分解の複雑さを元にした暗号。現在、安全性の高い通信で広く利用されている暗号。

楕円曲線暗号 楕円曲線上の離散対数問題が難しいことを元にした暗号

6.3 ssh(Secure Shell Protocol)

telnet,rlogin などのリモート接続では、単純なパスワードによる確認しか行われないため、外部組織との接続には極めて危険である。

そこで、公開鍵暗号を用いてデータすべてを暗号化して telnet,rlogin 等と同じようなリモート接続を実現するプロトコル ssh(Secure Shell Protocol) が利用される。

6.4 SSL(Secure Socket Layer)

http,telnet といった様々な通信プロトコルを、公開鍵暗号により暗号化するための共通の方式として、SSL が広く普及している。Web の http プロトコルを SSL により暗号化した通信 (https) 等は、安全性の高い電子商取り引きなどで利用されている。

しかし暗号化通信技術は、マフィアやテロリストが利用するとデータ通信の悪用の歯止めが効かないため、これらの技術はアメリカからの輸出規制法の対象となっている場合も多い。

7　ネットワークとクラッキング

ネットワーク接続により、コンピュータを不正使用するクラッキング被害が増加している。以下に主なクラッキング手法などを述べる。

7.1　ウィルス

アプリケーションプログラムに、複製能力のある悪意のあるプログラムをまぎれ込ませたものは、**ウィルス**と呼ばれる。

一般的に、ワードプロセッサや表計算などのデータでも、簡易的なプログラム機能の**マクロ**を利用した**マクロウィルス**が含まれている場合が増えている。さらに、これらのウィルスプログラムでは、電子メールに添付し増殖するタイプのものは被害が大きい。

この様な被害を防ぐためには、以下のような点に注意する必要がある。

- ネットワークからダウンロードしたプログラム、データには注意する。
- 電子メールに添付されているファイルを不用意に開かない。
- セキュリティ的に不備の指摘されているプログラムを利用しない。
- **ワクチン**などと呼ばれる対ウィルスソフトを利用する。

7.2　ポートスキャン

サーバ側でネットワークサービスとしてインストールされているプログラムで、バッファオーバーラン[4] 等に代表される**プログラムの不備**があった場合、情報が盗まれたり、不当にコンピュータを使うといった被害が発生するかもしれない。

クラッカーが、この様な不備のあるプログラムを発見するには、プログラムを用いてすべての IP アドレスと不備が報告されているプログラムのポート番号について、絨毯爆撃するように白み潰しにチェックすれば良い。

すべてのポートをチェックするような手段を用いた、クラッキングは**ポートスキャン**と呼ばれる。この様な被害を防ぐためには、

- 使用していないネットワークサービスは、起動されないように設定する。
- 不備のあるネットワークサービスのプログラムは、修繕されたプログラムに置き換える。
- 外部ネットワークからの接続を選択的に拒否するようなソフトウェアを導入する。(パーソナル FireWall)

[4] データ入力で、想定データサイズより大きいデータを与えることで、不当にプログラムを実行させる手法。

7.2.1 ファイアウォール (FireWall)

ネットワークやコンピュータに関する知識に乏しい人が、サーバを運用している場合、不備のあるネットワークサービスのプログラムを利用して、クラッキング被害に合う事例が多い。この様な事態を防ぐには、ファイアウォール (FireWall:防火壁) と呼ばれる機器を使うのが有効である。

ネットワーク通信のパケットには、IP アドレスやポート番号情報が付加されている。ファイアウォールでは、危険なネットワーク通信を防ぐために、以下のような通信制限を加える。

1. 許可されたポート番号以外のネットワークを拒否
2. アタックを繰り返す危険なコンピュータの IP アドレスの通信を拒否

7.2.2 トロイの木馬

不備のあるサーバプログラムを使わないとか、ファイアウォールを利用するといったセキュリティ対策では、万全な対処とはならない。

例えばメールや Web の通信により、トロイの木馬と呼ばれるプログラムを相手に送り付け、そのプログラムがファイアウォールの内部のネットワークから情報を盗み出したりする場合がある。

このため、ファイアウォールだけでなくパソコンでメールの内容や Web 通信の内容をチェックするといったセキュリティ対策ソフトの導入も重要である。

7.3 DoS アタック

セキュリティ対策がある程度行われていれば、ポートスキャン等の方法によるアタックでも、最終的に情報を盗んだり不当にコンピュータを操作する等を防ぐことは難しい。

しかしプログラムの不備によっては、サーバプログラムが異常終了したり誤った動作をする場合がある。この場合、情報が盗まれるといった被害でなく、適切なサービスを提供できなくなるという問題が発生する。これを **DoS(Denial of Service) アタック**と呼ぶ。

最近は、ポートスキャンなどによって不当操作できる大量のコンピュータを使って**サーバに同時に大量のデータを送りつけ**、サーバの処理能力を溢れさせたり、ネットワークの通信容量を溢れさせたりすることで、サービスを提供できなくする被害が問題となっている。この様な手法は、**分散 DoS アタック**と呼ばれるが、サーバにすれば通常のサービス依頼と区別ができないため、アクセス制限による対策ができないため、対応が難しい。

7.4 スパイウェア

パソコンの中の重要な情報の入っているファイルや、パソコン利用者のキー操作を記録した情報を送信させて、情報を盗むことを目的とした、ソフトウェア。愉快犯目的のウィルスと違い、悪意のある発病がないので、長期間気づかず被害が拡大する場合もある。

7.5 フィッシング

金融機関や公的な企業からの正規のメールに似せた、偽物のメール等を使い、偽物の Web サイトに誘導し、パスワード入力などをさせて、情報を悪用する手口。

7.6 ボット (bot)

本来は、ソフトウェアで自動化処理を行うロボットのようなプログラムの総称。しかし最近では、ウィルスの中にボットを埋め込み、遠隔操作でボットを埋め込まれたパソコンを悪用する手口が広がっている。

分散 DoS アタックに使われたり、最近では**迷惑メール (SPAM)** の多くが、このボットを利用して送信されている。

7.7 総当り攻撃 (ブルートフォースアタック)

パスワードが設定されていても、簡単なパスワードであれば、考えられる全てのパスワードを入力すればいつかは解読されてしまう。このような手法はブルートフォースアタックと呼ばれる。

パスワードに使われそうな単語を作って、おきその単語の組み合わせを用いる辞書攻撃などは、特に危険である。また、最近では 1 人の利用者が複数のサイトを利用することが多い。そして、複数のサイトで同一パスワードを利用していると、1 つのサイトがクラックされパスワード情報が盗まれた場合、他のサイトも被害にあうことが増えている。

このため、使い捨ての**ワンタイムパスワード**を併用する、**2 段階認証**を利用するサイトが増えている。