ま　え　が　き

近年の情報ネットワーク分野の進展には目を見張るものがある。現在，無線通信技術，光通信技術，IP ネットワーク技術等のネットワーク技術と情報セキュリティ技術の革新により，「いつでも，どこでも，なんでも，だれでも」「安心・安全に」ネットワークにつながるユビキタスネットワーク環境が整備され，マルチメディアサービス，ソーシャルサービス，クラウドサービス等のさまざまなサービスが展開されている。さらに，人と人との情報交換にとどまらず，モノ（機械）とモノ（機械）との間で情報交換を行い，モノへの自動制御を行うサービスやモノからの情報を活用するサービスが展開され，これらのサービスを支えるためにもさまざまなネットワークやセキュリティ技術が利用されている。このように，ネットワークやセキュリティ技術の進歩は速く，扱う範囲も多岐にわたるため，全体を理解することが困難となっている。そのため，ネットワークとセキュリティの基本技術をしっかり習得してから，各種応用技術の習得へと進むのが望ましい。本書では，特にネットワークとセキュリティの基本技術を中心に詳しく説明している。また，後半部分では，ネットワークの基礎となる理論やネットワークで今後の技術として注目されている技術にも簡単に触れているので，基本技術を習得した後，必要に応じて後半部分を読み進めていただきたい。

本書は，大学において初めて情報ネットワークを学ぶ学生（特に学部 1 年生）の授業での教科書として利用されることを想定して書かれている。本書のねらいは，つぎに示すとおりである。

- 情報ネットワークの専門知識が十分でなくても，ネットワークやセキュリティの基本的な仕組みや基本技術を理解できる。
- 情報処理技術者試験（IT パスポートなど）のネットワークとセキュリ

ティ分野の学習において，出題範囲で扱う基本技術の理解をより深められる。

本書は，大学において初めて情報ネットワークを学ぶ学生を対象とした基礎的な項目と，より進んだ項目を分けており，より進んだ項目は【中級】，あるいは【上級】と記している。また，前述のように，本書は，情報処理推進機構が実施している情報処理技術者試験（IT パスポートなど）のネットワークとセキュリティ分野の出題範囲もほぼ網羅しているため，試験対策として使用することもできる。試験対策として使用する場合は，中級と上級の項目以外を中心に習得していただきたい。

全体は全 6 章で構成されており，情報ネットワークの歴史と基本技術（1 章），ネットワークのプロトコル（2 章），インターネット（3 章），情報セキュリティ（4 章），ネットワークの理論（5 章），今後の情報ネットワーク（6 章）からなっている。

1 章では，インターネット，固定通信ネットワーク，移動通信ネットワークの各種ネットワークにおける歴史と基本技術について述べている。

2 章では，ネットワークのプロトコル全般について述べている。2.1 節では，ネットワークと標準化に関する基本的な内容として，OSI 参照モデルと TCP/IP や標準化組織を概説している。2.2 節では，物理層とデータリンク層について述べている。物理層では物理層の役割，伝送媒体や伝送方式など物理層の基本技術，データリンク層ではデータリンク層の役割，フロー制御や誤り制御などデータリンク層の基本技術について述べている。また，LAN 技術として，イーサネットと無線 LAN について簡単に紹介している。2.3 節では，ネットワーク層について述べている。ネットワーク層の役割，IP アドレスの基礎，経路制御の基本的な仕組みや経路制御プロトコルについて述べている。2.4 節では，トランスポート層について述べている。トランスポート層の役割，フロー制御や再送制御などトランスポート層の基本技術について述べている。2.5 節では，アプリケーション層について述べている。アプリケーション層の代表的なプロトコルである，DNS，SMTP，POP3，HTTP，FTP について述べている。

3 章では，インターネットの構造，インターネットサービスプロバイダ (ISP)，インターネットへの接続方法などインターネットの基礎について述べている。

4 章では，情報セキュリティについて述べている。4.1 節では，セキュリティの概念，リスクマネージメント，リスク対策などセキュリティの基礎について述べている。4.2 節では，暗号化と復号，秘密鍵暗号方式や公開鍵暗号方式などの各種暗号方式，ディジタル署名等について述べている。その他，電子選挙，電子決済，電子透かし，クッキー等についても述べている。4.3 節では，認証と承認，ネットワークの脆弱性，Web アプリケーションの脆弱性，コンピュータウイルス，無線 LAN のセキュリティ，ソーシャルエンジニアリング，ファイアウォールと防御システム，VPN 等について述べている。

5 章では，ネットワークの理論について述べている。5.1 節と 5.2 節では，それぞれ情報ネットワークの設計，制御のための基礎理論である待ち行列理論とグラフ理論について述べている。

6 章では，今後の情報ネットワークについて述べている。ネットワーク分野で注目されている今後の技術として，さまざまなネットワークの技術を紹介している。

なお，各章および各節の執筆者はつぎのとおりである。

- 1 章，2.1 節，3 章，6.1 節：金
- 2.2 節，2.4 節，5.1 節，6.2〜6.4 節：花田
- 2.3 節，2.5 節，5.2 節，6.5〜6.7 節：金光
- 4.1 節：井関と吉澤
- 4.2 節：鈴木
- 4.3 節：井関

最後に，出版に際してお世話になったコロナ社の諸氏に感謝いたします。

2014 年 8 月

著　者

目　　次

1.　情報ネットワークの歴史と基本技術

1.1　現状のネットワーク …… 1
1.2　インターネット …… 3
　1.2.1　インターネットの歴史 …… 3
　1.2.2　パケット交換技術 …… 4
1.3　固定通信ネットワーク …… 5
　1.3.1　電 話 の 歴 史 …… 5
　1.3.2　固定通信ネットワークの構成 …… 6
　1.3.3　回 線 交 換 技 術 …… 7
1.4　移動通信ネットワーク …… 9
　1.4.1　移動通信ネットワークの歴史 …… 9
　1.4.2　移動通信ネットワークの基本構成 …… 10
　1.4.3　無 線 通 信 技 術 …… 11
　1.4.4　ネットワーク制御技術 …… 12

2.　ネットワークのプロトコル

2.1　階層モデルと標準化 …… 14
　2.1.1　プロトコル階層モデル …… 14
　2.1.2　標　　準　　化 …… 19
2.2　物理層とデータリンク層 …… 21
　2.2.1　物　　理　　層 …… 22

2.2.2　データリンク層 …… 28
2.2.3　LAN　技　術 …… 35
2.2.4　データリンク層のその他のプロトコル …… 43
2.3　ネットワーク層 …… 44
2.3.1　ネットワーク上におけるアドレスの仕組み …… 45
2.3.2　IP アドレス …… 47
2.3.3　サブネットマスク …… 49
2.3.4　ネットワークアドレスとブロードキャストアドレス …… 51
2.3.5　IP パケットの寿命 …… 52
2.3.6　その他のプロトコル（ICMP，ARP） …… 52
2.3.7　パケット到達の仕組み …… 54
2.3.8　経路制御の仕組みと種類 …… 56
2.3.9　RIP【中級】 …… 57
2.3.10　OSPF【中級】 …… 64
2.3.11　BGP【中級】 …… 69
2.3.12　IPv6 …… 71
2.4　トランスポート層 …… 72
2.4.1　トランスポート層のおもな機能 …… 72
2.4.2　トランスポート層のプロトコル …… 74
2.4.3　TCP …… 74
2.4.4　UDP …… 84
2.5　アプリケーション層 …… 84
2.5.1　アプリケーション層のプロトコル …… 85
2.5.2　名前解決（DNS） …… 85
2.5.3　電子メール（SMTP，POP3） …… 87
2.5.4　ハイパーテキストの転送（HTTP） …… 89
2.5.5　ファイル転送（FTP） …… 91

3. インターネット

3.1 ネットワークアーキテクチャ …… 92
3.2 ISP …… 93
3.2.1 ISP とは …… 93
3.2.2 ISP の提供するサービス …… 93
3.3 インターネットとの接続 …… 94
3.3.1 加入者線による接続 …… 94
3.3.2 モバイルコンピューティング …… 97
3.3.3 インターネットと LAN の接続 …… 98
3.3.4 SINET …… 99

4. 情報セキュリティ

4.1 セキュリティの基本とマネジメント …… 101
4.1.1 利便性とセキュリティ …… 101
4.1.2 リスクマネジメント …… 102
4.1.3 情報システムにおけるリスク対応 …… 103
4.1.4 セキュリティ要件と攻撃の種類 …… 104
4.2 暗号技術 …… 105
4.2.1 暗号化と復号 …… 105
4.2.2 秘密鍵暗号方式 …… 105
4.2.3 公開鍵暗号方式 …… 107
4.2.4 ハイブリッド暗号方式 …… 108
4.2.5 Diffie–Hellman 鍵交換方式【中級】 …… 108
4.2.6 離散対数問題【中級】 …… 109
4.2.7 RSA 暗号 …… 110
4.2.8 RSA 暗号によるディジタル署名 …… 111

4.2.9　一方向性ハッシュ関数【中級】 113
4.2.10　ディジタル署名アルゴリズム DSA【中級】 115
4.2.11　楕円曲線上の演算【上級】 116
4.2.12　ペアリングによる 3 者間 Diffie–Hellman 鍵交換方式【上級】 119
4.2.13　素因数分解と素数判定【中級】 120
4.2.14　電子選挙と RSA ブラインド署名【中級】 121
4.2.15　電子決済 122
4.2.16　電子透かし 122
4.2.17　クッキーとプライバシー 123
4.2.18　ソーシャルメディアとプライバシー 124
4.3　ネットワークセキュリティと対策 124
4.3.1　認証と承認 124
4.3.2　ネットワークの脆弱性 127
4.3.3　Web アプリケーションの脆弱性 132
4.3.4　バッファオーバーフロー【中級】 139
4.3.5　コンピュータウイルス 141
4.3.6　無線 LAN のセキュリティ 145
4.3.7　ソーシャルエンジニアリング 149
4.3.8　ファイアウォールと防御システム 149
4.3.9　VPN【中級】 153
4.3.10　セキュリティチェック【中級】 155

5.　ネットワークの理論

5.1　待ち行列理論 157
5.1.1　待ち行列モデル 157
5.1.2　出生死滅過程 159
5.1.3　M/M/1 161
5.1.4　M/G/1【上級】 163

5.1.5 ネットワーク性能評価への適用例【上級】 169
5.2 グラフ理論 171
5.2.1 グラフの基礎 171
5.2.2 最短経路問題 173
5.2.3 フローネットワーク【中級】 177
5.2.4 最小費用フローアルゴリズム 182

6. 今後の情報ネットワーク

6.1 ユビキタスネットワーク 185
6.1.1 無線通信技術に基づいたアクセス技術 186
6.1.2 コアネットワークの技術 188
6.2 無線アドホックネットワーク 190
6.2.1 データリンク層のプロトコル 190
6.2.2 ネットワーク層のプロトコル 191
6.2.3 今後の無線アドホックネットワーク 192
6.3 無線センサネットワーク 192
6.3.1 時刻同期と位置情報 193
6.3.2 データリンク層のプロトコル 193
6.3.3 ネットワーク層のプロトコル 194
6.3.4 今後の無線センサネットワーク 194
6.4 SDN 195
6.5 P2P 197
6.6 グリッドコンピューティング 200
6.7 クラウドコンピューティング 201

引用・参考文献 203
索 引 207

1 情報ネットワークの歴史と基本技術

1.1　現状のネットワーク

図 1.1 に現状のネットワークを示す。図に示すように，現在世の中で稼働しているネットワークは 3 種類存在する。すなわち，① コンピュータ通信の**インターネット**，② 電話をベースとする**固定通信ネットワーク**，③ 携帯電話を中心とした**移動通信ネットワーク**である。これらのネットワークは物理的に別々な設備とシステムを使用して構築され相互に接続されており，それぞれ異なる事業体によって運用されている。

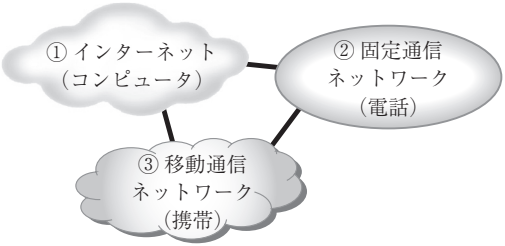

図 1.1　現状のネットワーク

〔**1**〕 **インターネット**　　インターネットの基盤は, 1969 年に軍事研究用ネットワークとして実現した **ARPANET**（advanced research projects agency network）である。複数のコンピュータを通信回線で接続しデータのやり取りを行うコンピュータネットワークとして 1990 年代なかばから世界中で急速に普及した。一方で，当初インターネットは仲間同士でコミュニケーションするネットワークとして開発された（性善説で開発された）ので，社会に広く使わ

れるようになると，セキュリティ上のさまざまな問題が起こり，セキュリティ対策が不可欠になってきている。

〔**2**〕 **固定通信ネットワーク**　1876 年にベル（A. G. Bell）が電話を発明して以来，100 年以上にわたって電話を中心とした固定通信ネットワークが構築されてきている。固定通信ネットワークとは，主として有線通信技術（通信ケーブル技術）でユーザが使用する通信機器（ネットワークの立場では端末と呼んでいる）とネットワーク機器が接続されているネットワークである。ユーザは固定した場所でネットワークを利用するので，このように呼ばれている。

2014 年現在，固定通信ネットワークは大きな曲がり角にきている。19 世紀から一貫して増え続けてきた電話数が，近年，インターネットや携帯電話の影響で減り始めており，ネットワークを根本から見直す必要に迫られた。さまざまな議論と検討を進めた結果，インターネットで使われている IP 技術に基づいて**次世代ネットワーク**（next generation network，**NGN**）と呼ぶ新しいネットワークを実現することが決まり，商用サービスも始まっている。

〔**3**〕 **移動通信ネットワーク**　自動車電話から始まった携帯電話を主とする移動通信ネットワークは，1990 年代から急速に普及し，すでに固定通信ネットワークをユーザ数で追い越している。移動通信ネットワークとは，ユーザが場所を移動しながらネットワークを利用し，ユーザの通信機器（端末）とネットワークが主として無線通信技術（電波伝送技術）で接続されているネットワークである。

1980 年代の第 1 世代から始まった移動通信ネットワークは，1990 年代の第 2 世代を経て，2000 年以降は第 3 世代として継続的に進展してきた。今後は第 4 世代，第 5 世代ならびにさらにそれ以降の世代に向けて進展することが期待されている。

本章では，この三つのネットワークの歴史と基本技術について説明する。

1.2 インターネット

1.2.1 インターネットの歴史

コンピュータネットワークのうち，一つのオフィス，建物，キャンパス等の比較的狭い地域（適当な大きさの地理的地域）に限定して設置されたネットワークを**構内情報通信網**（local area network，**LAN**）と呼ぶ。これに対して遠隔地にある LAN 同士を接続したネットワークを**広域情報通信網**（wide area network，**WAN**）と呼ぶ。

インターネット（internet）とは，Inter と Network を合成して作られた用語であり，多くの LAN あるいは WAN を相互接続した大きなネットワークを意味する。**図 1.2** に示すように，プロバイダのネットワーク，企業内ネットワーク，大学のキャンパスネットワーク，研究組織のネットワーク等，世界中で稼働している個別のコンピュータネットワークをたがいに接続してできあがった大きな世界的なネットワークである。ここで，プロバイダとは，**インターネットサービスプロバイダ**（internet service provider，**ISP**）であり，個人や企業がインターネットに接続するための仲介を行う業者あるいは組織を意味している。

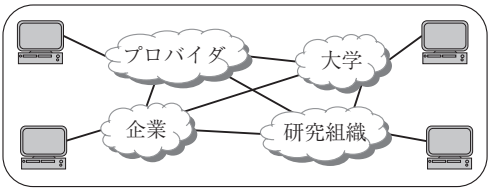

図 1.2 インターネットとはなにか

図 1.3 にインターネットの歴史を示す。インターネットが世界に広く普及したのは，1990 年代からである。図 1.3 に示しているように，最初はアメリカの研究機関を中心に展開していたネットワークであったが，1990 年代に入り，商用でのインターネット利用が盛んになった。特に，**WWW**（world wide web）が誕生し使われるようになって，広く世界に普及するようになった。さらに，

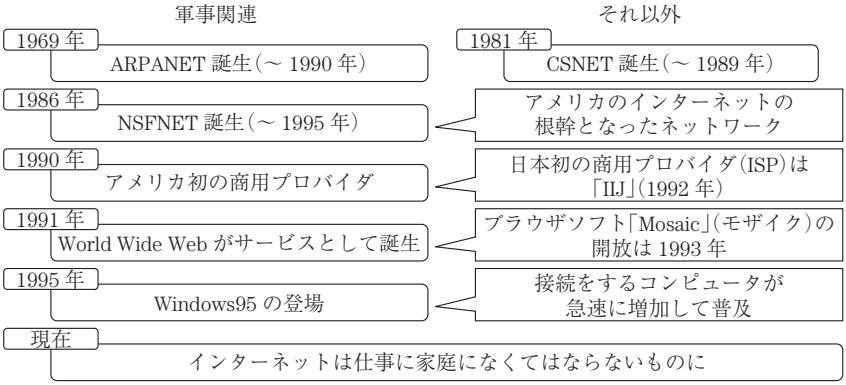

図 1.3　インターネットの歴史

1995 年以降には，家庭でも PC が普及し，個人利用も盛んになり，現在では，コミュニケーション手段の一つとして重要な存在となっている。

1.2.2　パケット交換技術

インターネットでは，コンピュータ同士がやり取りするデータを**パケット**として扱っている。パケットとは，**図 1.4** に示すように，コンピュータが扱う 1 と 0 のデータ（bit 列）を一定の長さで区切り，データの順番や宛先のアドレスなどを入れたヘッダを付けたものである。パケットは「小包」という意味で，あるまとまった本や果物を宅急便の箱に入れて，宛先ラベルを貼って送るのと同じ考え方である。

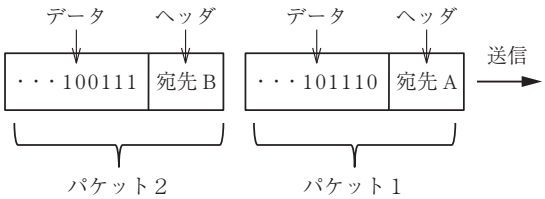

図 1.4　パケットとは

ネットワークにはそれぞれのコンピュータからのパケットがばらばらになって流れてくるが，パケットを処理するネットワークの機器（ルータなど）が，パケットヘッダの宛先を見て相手のコンピュータに届くように制御している。送

信先のコンピュータに届いたパケットは，もとの 1 と 0 の bit 列に組み立てられる。このような通信制御技術を**パケット交換**技術と呼んでいる。

パケット交換技術では，同じ物理的な通信回線を用いて複数のコンピュータからのパケットを同時に扱うこと（多重化）ができるので，通信回線を効率的に使用することが可能となる。また，ある物理的な通信回線が障害などで使えない場合も，ほかの回線を使って送信先に届けることができる。しかし，ネットワークに流れるパケットが増えてくると，ネットワーク機器の処理性能には限界があるので，パケットが届く時間が遅くなる（遅延が大きくなる），あるいはパケットが届かない（パケットが消失する）場合が発生し，ネットワークサービスとして品質が悪化する問題が発生する。

1.3　固定通信ネットワーク

1.3.1　電 話 の 歴 史

電話は 1876 年に米国のベル（A. G. Bell）によって発明され，その利便性からすぐに社会へ普及した。1878 年には世界最初の電話局が米国のコネチカット州ニューヘブン市で開局し，固定通信ネットワークの構築が行われた。日本には 1887（明治 20）年にイギリスより電話機が輸入されるとともに，固定通信ネットワークの構築が行われ始めた。しかし，第二次世界大戦前は，電話はまだ一般庶民にとって身近なものではなく，電話が本格的に社会に普及するのは戦後の 1970 年代である。

戦後の電話網の進展はつぎのとおりである。

〔1〕　電話増設の時代：1945〜1978 年　1945 年から 1978 年ごろまでは，電話番号を回せば日本中のどこでもすぐつながる電話，申し込めばすぐに家に設置される電話を目指して，電話網が増設された時代である。戦争で残った電話は 47 万台程度であったが，NTT の前身である日本電信電話公社が発足する 1952 年には，戦前の水準である 150 万台まで回復した。1955 年には，電話網の進展を目的としてクロスバ交換機が国産化され，1960 年には，加入者数が急

増し 360 万台となった。さらに，1965 年には 730 万台，1975 年には 3 030 万台，1980 年には 3 850 万台と進展した。その結果，1978 年ごろには，全国電話網の自動即時化（電話番号を回せばすぐにつながる）と，電話申し込みの積滞が解消した（申し込めばすぐに設置される）。

〔2〕 ディジタル化の時代：1968〜1997 年　このように，電話網の規模の充実化が進展するとともに，技術革新に伴う質的な充実として，電話網のディジタル化が進展した。ディジタル化は，半導体技術やディジタル回路技術の発展とともに，伝送路の高品質化と経済化を目指して，まず，伝送装置のディジタル化から始まった。さらに，交換機のディジタル化へと進み，コンピュータのソフトウェア技術を取り込んだプログラム制御の電子・ディジタル交換機が実用化された。こうしたディジタル技術で実現される電話網を総合ディジタル通信網 **ISDN**（integrated services digital network）と呼び，日本電信電話公社とその後民営化された NTT によって，約 30 年間にわたってその実現が進められた。

1.3.2　固定通信ネットワークの構成

図 1.5 に日本の固定通信ネットワークの構成例を示す。図 1.5 に示すように，固定通信ネットワークは，多数の**交換機**と，交換機と交換機をつなぐ**伝送路**からなっている。さらに，交換機は電話機（通信端末）が直接接続している**加入者線交換機**（local switch，**LS**）と**中継交換機**（toll switch，**TS**）がある。LS は同じ地域における電話同士（例えば，同じ千葉市内の電話）を接続する交換

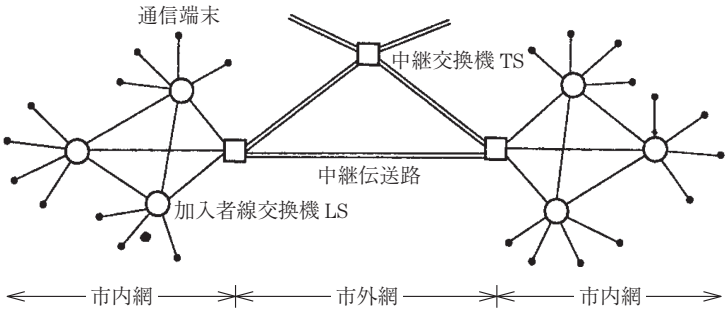

図 1.5　固定通信ネットワークの構成例

機であり，LS が扱う範囲を市内網と呼ぶ。TS は遠く離れた電話同士（例えば，千葉市の電話と神戸市の電話）を接続するのに必要な交換機であり，TS が扱う範囲を市外網と呼ぶ。伝送路も交換機の種類に応じて分類され，中継交換機同士をつなぐ伝送路として中継伝送路がある。

図 1.6 に，**加入者線**の構造例を示している。電話を使用するために電話会社に加入しているユーザを加入者と呼んでいるが，図 1.6 は加入者が一戸建ての自宅に住んでいる例である。家の中にある電話機（通信端末）の音声信号は，まず，近くの電柱にある接続端子箱に伝送される。その後，電柱間のケーブル（架空ケーブル）で伝送され，マンホールに入る。マンホールの中では地下ケーブルで伝送され電話局の加入者線交換機に接続される。また，中継伝送路は交換機同士を接続する中継ケーブルであるが，場合によっては，無線を使う場合もある。

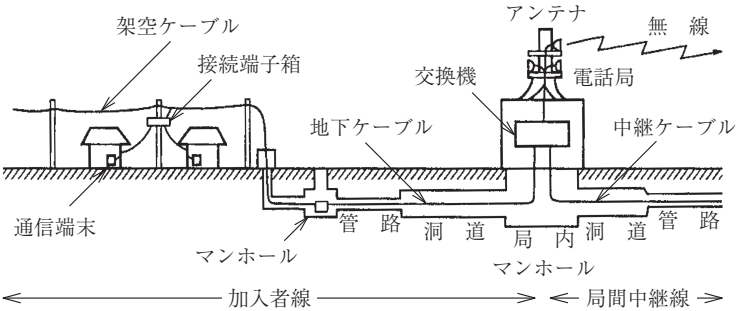

図 1.6　加入者線の構造例

1.3.3　回線交換技術

前述した固定通信ネットワークによって，どのように電話サービスが実現されているかを説明する。**図 1.7** に交換機を中心とした固定通信ネットワークを示す。前述したように，自宅の電話機，あるいは公衆電話機は加入者線によって地域の加入者線交換機に接続しており，加入者線交換機はさらにその上位の中継交換機に接続されている。このように多数の交換機を相互接続した固定通信ネットワークによって，日本中の電話機が電話番号を入力するだけで，電話

索　　引

【あ】

アクセスコントロールリスト 150
アドホックモード 40
誤り回復 31
誤り検出 31
誤り制御 30
誤り訂正 33
アンカプセル化 18
暗号化 105
暗号化技術 153
暗号文 105

【い】

イーサネット 36
位相偏移変調 26
位相変調 26
位置情報管理用データベース 12
一方向性ハッシュ関数 113
移動通信ネットワーク 1, 9
インターネット 1, 3
インターネットサービスプロバイダ 3
イントラネット 151
インフラストラクチャーモード 40

【う】

ウイルス定義ファイル 144
ウィンドウサイズ 78

【え】

エラーコード 139
エリア 65, 68

【お】

重み付きグラフ 173

【か】

回線交換 9
開放型システム間相互接続 15
仮想組織 200
仮想リンク 198
カット 178
加入者線 7
加入者線交換機 6
カプセル化 17
ガーベッジコレクションタイマー 59
可用性 104
監　査 102
完全性 104
管理的セキュリティ対策 103

【き】

技術的障害対策 104
技術的セキュリティ対策 103
技術的犯罪対策 104
基本方針 101
機密性 104
逆引き 87
強制的ブラウズ 136

【く】

クッキー 123
クライアントサーバモデル 197
クラウドコンピューティング 201
グリッドコンピューティング 200
クロスサイトスクリプティング 133, 134
クロスサイトリクエストフォージェリ 134
グローバル IP アドレス 98

【け】

計算グリッド 200
経路制御 54
経路表 54
ゲートウェイ 19

【こ】

コアネットワーク 10
広域情報通信網 3
公開鍵暗号方式 107
交換機 6
公衆無線 LAN 97
構内情報通信網 3
国際電気通信連合 19
国際標準化機構 15
国立情報学研究所 99
呼処理 8
誤操作対策 104
固定通信ネットワーク 1, 5

コネクション解放 77
コネクション確立 75
コネクション管理 75
コネクション指向型通信 73
コネクションレス型通信 73
コンピュータウイルス 141

【さ】

最小カット 179
再送制御 80
最大フロー 179
最大フローアルゴリズム 179
最大フロー最小カット定理 178
サニタイジング 134, 137
サブネット 49
サブネット化 49
サブネットマスク 49
サプリカント 148

【し】

辞書アタック 126
辞書攻撃 147
次世代送電網 194
次世代ネットワーク 2
事前共有キー 147
実施手順 102
時分割多重化方式 27
周波数 11
周波数分割多重化方式 27
周波数偏移変調 26
周波数変調 26
従量制 95
出次数 173
出生死滅過程 159
承　認 124
情報セキュリティの三大要件 104
情報セキュリティポリシー 101
情報セキュリティマネジメントシステム 103
自律システム 57, 92
シングルエリア OSPF 68
侵入検知システム 152
侵入防御システム 152
振幅偏移変調 26
振幅変調 26

【す】

スイッチングハブ 18
スター型 34
スタックスネット 144
スタンダード 101
ストアードプロシージャ 137
スニッファ 153
スニッフィング 153
スパイウェア 142
スーパーピア 199
スピア型ウイルス 142
スプリッタ 95
スプリットホライズン 63
スマートグリッド 194
スライディングウィンドウ方式 30, 78
スロースタート 82

【せ】

静的ルーチング 56
正引き 87
セキュリティスキャナ 156
セキュリティ要件 104
セグメント 16
セッションハイジャック 136
セッションリプレイ 136
セルラー方式 12
ゼロデイアタック 143
全二重伝送 28

【そ】

総当り攻撃 147
ソーシャルエンジニアリング 149
ソーシャルメディア 124

【た】

ダイアルアップ接続 94
ダイクストラの最短経路決定アルゴリズム 67
ダイクストラ法 173
対策基準 101
楕円曲線上の離散対数問題 116
多重化方式 27

【ち】

チャレンジ&レスポンス認証 125
中継交換機 6
頂　点 171
直角位相振幅変調 26

【つ】

ツイストペアケーブル 22
通信プロトコル 14

【て】

定額制 96
定義ファイル 142
ディジタル署名 111
ディジタル署名アルゴリズム 115
データグリッド 201
デバッグオプション 135
電子決済 122
電子透かし 122
電子選挙 121
電磁波 23
伝送路 6
電　波 23

【と】

統一資源位置指定子 91
透過性 201
統合脅威管理 153
同軸ケーブル 23
動的ルーチング 56

ドメイン名 86
トランジット 92
トリガードアップデート 64
トロイの木馬 141
トンネリング技術 153, 154

【に】

入次数 173
認　証 124
認証・許可・アカウンティングモデル 126

【ね】

ネットワークアドレス 51
ネットワークのアクセス技術 186

【の】

ノード 171
ノードの次数 172

【は】

バイオメトリクス認証 127
バイポーラ方式 26
ハウジングサービス 94
パケット 4
パケット課金制 97
パケットキャプチャー 153
パケットキャプチャリング 153
パケット交換 5
バス型 34
パスワードクラッキング 125
パスワード認証 124
バックオフ時間 42
バックドア 135
バックボーンエリア 68
バッファオーバーフロー 139
バッファオーバーラン 139
ハニーポッド 153
パラメータ改ざん 135
ハンドオーバー 13
半二重伝送 28

【ひ】

ピアツーピアネットワーク 197
ピアリング 93
光ファイバケーブル 23
ビジネスグリッド 201
非武装地帯 151
秘密鍵暗号方式 105
標準エリア 68
標的型ウイルス 142
平　文 105

【ふ】

ファイアウォール 149
ファジング 156
ファーミング 143
フィッシング 143, 149
復　号 105
復号化 105
輻　輳 82
輻輳回避フェーズ 83
輻輳制御 82
双子の悪魔 148
物理アドレス 16
物理的セキュリティ対策 103
負閉路除去法 183
プライベート IP アドレス 98
ブリッジ 18
ブルートフォースアタック 126, 147
フルルート 92
フレーム 16
フレーム化 29
フロー 177
プロシージャ 102
フロー制御 29, 78
ブロードキャストアドレス 51
ブロードバンド接続 96
ブロードバンド伝送 26
フローネットワーク 177
分散型 DoS 攻撃 130

【へ】

閉　路 173
ベストエフォート型 46
ベースバンド伝送 25
ペネトレーションテスト 156
ベルマンフォード法 175
辺 171

【ほ】

ポイズンリバース 64
ホスティングサービス 94
ボット 142
ボットネット 130
ポート番号 16, 75

【ま】

マクロウイルス 141
待ち行列モデル 157
マルウェア 143
マルチエリア OSPF 68
マンチェスタ方式 26

【み】

蜜つぼ 153

【む】

無害化 134, 137
無向グラフ 172
無線アクセスネットワーク 10
無線アドホックネットワーク 190
無線センサネットワーク 192
無線伝送媒体 23
無線 LAN 40
無線 PAN 186

【め】

メッセージ認証符号 114
メディアアクセス制御方式 34

【も】
モデム 94
モバイルコンピューティング 97

【ゆ】
有向グラフ 172
有向循環グラフ 173
有向非循環グラフ 173
有線伝送媒体 22
ユビキタスネットワーク 185

【よ】
容　量 177

【り】
離散対数問題 109
リスク対応 102
リピータ 18
流　量 177
リレーアタック 127
リング型 34

【る】
ルータ 19
ルーチング 54
ルーチングテーブル 54
ルートキット 143
ルート再配送 69
ルートポイズニング 63

【れ】
レイヤ 2 VPN 154
レイヤ 3 VPN 154

【ろ】
ロ　グ 155
ログサーバ 155

【わ】
ワイヤレスユビキタス
　ネットワーク 190
ワーム 142
ワンタイムパスワード認証 125

【A】
AAA モデル 126
ACL 150
ADSL 95
ADSL モデム 95
AES 147
ALG 19
AM 26
AMI 方式 26
Anonymous FTP 91
ANSI 21
ARP 52
ARP スプーフィング攻撃 129
ARPANET 1
ARQ 31
AS 57, 92
ASK 26

【B】
BGP 57, 69
Bluetooth 187

【C】
Chaptcha 127
C.I.A 104
CSMA/CA 34, 41
CSMA/CD 34, 38
CSRF 134
CVE 156

【D】
DAG 173
DDoS 攻撃 130
Deauth Attack 147
DH 109
Diffie–Hellman 鍵交換方式 109, 119
DMZ 151
DNS 86
DNS キャッシュポイズニング 131, 144
DNSSEC 132
DoS 攻撃 130
DSA 115
DSU 95

【E】
EAP 147
EGP 57
End-to-End 45
ESS–ID ステルス 146
EXE Crypter 143

【F】
Face Routing 194
FDM 27
FM 26
FMC 188
Ford–Fulkerson 法 179
FSK 26
FTP 91
FTTH 96

【G】
Go-back-N ARQ 32
Greedy Routing 194

【H】
HDLC 44

HLR 12
HTTP 89
HTTP 応答 89
HTTP 要求 89

【I】

IaaS 202
ICMP 52
IDS 152
IEEE 21
IEEE802 21
IEEE802.1x 147
IEEE802.11i 146
IETF 19
IGP 56
IP 45
IP アドレス 16, 47
IP スプーフィング攻撃 128
IP パケット 16, 52
IP マスカレード 99
IPS 152
IPsec 155
IPsec–VPN 155
IPv4 71
IPv6 71
ISDN 6, 95
ISMS 103
ISO 15
ISP 3, 93
ITU 19
ITU–T 20
IX 93

【J】

JPCERT/CC 144
JPNIC 98
JVN 156

【L】

LAN 3, 35
LEACH 193
LLC 副層 16
LMAC 193
LS 6
LSA 65
LSDB 65
LSU パケット 65
L2 スイッチ 18
L3 スイッチ 19

【M】

MAC アドレス 16, 36, 146
MAC 副層 16
MAC（メッセージ認証符号） 114
MACA 191
MACAW 191
M/G/1 163
M/G/1/∞/∞/FCFS 163
M/G/1/∞/∞/Priority 167
M/M/1 161
M2M 194

【N】

NAPT 151
NAT 99, 151
NGN 2
NII 99
No-Execute（NX）Memory Protection 140
NRZ 方式 25

【O】

OFDM 186
ONF 195
OPEN メッセージ 70
OpenFlow 196
OpenVAS 156
OSI 参照モデル 15
OSI プロトコル 15
OSPF 57, 64

【P】

PDCA サイクル 103
PM 26
POP before SMTP 89
POP3 88
PPP 44
PPPoE 155
PPTP 155
PSK 26
PSK キー 147
P2P network 197

【Q】

QAM 26

【R】

RADIUS 126
RADIUS サーバ 148
RBS 193
RFC 19
RFID タグ 187
RIP 57
RSA 暗号 110
RSA ブラインド署名 121

【S】

SaaS 202
salt 125
SDN 195
Selective-Repeat ARQ 33
SINET 99
S–MAC 193
SMTP 87
SMTP 認証 89
SMTP Auth 89
SPF ツリー 65
SQL インジェクション 137
SSL–VPN 155
Stop-and-Wait ARQ 31
SYN クッキー 131
SYN フラッド攻撃 130

【T】

TA 95
TACACS 126
TCP 74
TCP/IP 15

TDM 28
Tier1 92
Tier2 92
TKIP 146
T–MAC 193
TR 20
TRAMA 193
TS 6, 20
TTL 52

【U】

UDP 74, 84
UPDATE メッセージ 70
URL 91
UTM 153
UWB 187

【V】

VANET 192
VO 200
VPN 153

【W】

WAN 3
WEP 43, 146
Wireshark 153
WPA 43, 146
WPA–PSK 147
WPA–802.1x 147
WPA2 43, 147
WPA2–PSK 147
WPA2–802.1x 147
WWW 3

【X】

XSS 133, 134

【Z】

ZigBee 187

【数字】

2 進数 46
3 ウェイハンドシェイク 75, 130
3GPP 20

—— 著 者 略 歴 ——

井関　文一（いせき　ふみかず）

1984 年　東京理科大学理工学部物理学科卒業
1986 年　東京都立大学大学院理学研究科修士修了（物理学専攻）
1988 年　東京都立大学大学院理学研究科博士課程退学（物理学専攻）
1988 年　富士通株式会社勤務
1989 年　東京情報大学電算センタ助手
1999 年　博士（工学）（東京農工大学）
2002 年　東京情報大学助教授
2008 年　東京情報大学教授
現在に至る

金　　武完（きむ　むわん）

1974 年　大阪大学工学部電子工学科卒業
1980 年　大阪大学大学院後期課程修了（電子工学専攻）
工学博士
1980 年　株式会社富士通研究所（研究室長），富士通株式会社（開発部長）勤務
1998 年　日本モトローラ（シニアマネージャ），日本ルーセント（ディレクタ），ソフトバンクモバイル（企画部長）勤務
2005 年　東京情報大学教授
現在に至る

花田　真樹（はなだ　まさき）

1996 年　早稲田大学理工学部資源工学科卒業
1999 年　北陸先端科学技術大学院大学修士課程修了（情報科学専攻）
1999 ～ 2000 年　INS エンジニアリング（現ドコモ・システムズ）株式会社勤務
2003 年　早稲田大学大学院国際情報通信研究科修士課程修了（国際情報通信学専攻）
2003 年　早稲田大学国際情報通信研究センター助手
2006 年　早稲田大学大学院博士課程満期退学（国際情報通信学専攻）
2007 年　博士（国際情報通信学）（早稲田大学）
2007 年　NTT アドバンステクノロジ株式会社勤務
2008 年　東京理科大学助教
2011 年　東京情報大学助教
2014 年　東京情報大学准教授
現在に至る

金光　永煥（かねみつ　ひでひろ）

2002 年　早稲田大学理工学部数理科学科卒業
2002 ～04 年　株式会社アルファシステムズ勤務
2006 年　早稲田大学大学院国際情報通信研究科修士課程修了（国際情報通信学専攻）
2006 ～09 年　早稲田大学メディアネットワークセンター助手
2012 年　早稲田大学大学院国際情報通信研究科博士後期課程修了
博士（国際情報通信学）
2012 年　早稲田大学メディアネットワークセンター（現 早稲田大学グローバルエデュケーションセンター）助教
現在に至る

鈴木　英男（すずき　ひでお）

1986 年　名城大学理工学部電気工学科卒業
1988 年　名古屋工業大学大学院工学研究科博士前期課程修了（電気情報工学専攻）
1992 年　東北大学大学院工学研究科博士課程後期修了（電気及通信工学専攻）
博士（工学）
1993 年　東北大学助手
1993 ～95 年　米国 Stanford 大学客員研究員兼任
1996 年　米国 JVC Laboratory of America 研究員
1999 年　東京情報大学講師，法政大学非常勤講師
2004 年　東京情報大学助教授
2007 年　東京情報大学准教授，千葉大学非常勤講師
現在に至る

吉澤　康介（よしざわ　こうすけ）

1981 年　東京大学工学部精密機械工学科卒業
1981 ～84 年　郵政省電波監理局勤務
1986 年　東京大学工学部境界領域研究施設研究生
1989 年　東京大学大学院工学系研究科修士課程修了（情報工学専攻）
工学修士
1994 年　東京大学大学院工学系研究科博士課程単位取得満期退学（情報工学専攻）
1994 年　駿台電子情報専門学校講師
1996 年　関東学園大学，関東短期大学非常勤講師
1997 年　関東学園大学助教授
2003 年　東京情報大学助教授
2007 年　東京情報大学准教授
現在に至る

情報ネットワーク概論
— ネットワークとセキュリティの技術とその理論 —
Information Network
— Network and Security Technology with Theory —
© Masaki Hanada 2014

2014 年 10 月 3 日 初版第 1 刷発行 ★

検印省略

著 者 井関文一
金光永煥
金武完
鈴木英男
花田真樹
吉澤康介
発行者 株式会社 コロナ社
代表者 牛来真也
印刷所 三美印刷株式会社

112–0011 東京都文京区千石 4–46–10
発行所 株式会社 コロナ社
CORONA PUBLISHING CO., LTD.
Tokyo Japan
振替 00140–8–14844・電話(03)3941–3131(代)
ホームページ http://www.coronasha.co.jp

ISBN 978–4–339–02484–5 (中原) (製本：愛千製本所)
Printed in Japan

本書のコピー，スキャン，デジタル化等の無断複製・転載は著作権法上での例外を除き禁じられております。購入者以外の第三者による本書の電子データ化及び電子書籍化は，いかなる場合も認めておりません。
落丁・乱丁本はお取替えいたします