

情報通信ネットワーク入門

尾崎 博一 著

コロナ社

まえがき

情報通信ネットワークやインターネットに関する教科書、解説書は数多く出版されている。タイトルを見て本書を手にした人はそれらといったい何が違うのだろうかと思うかもしれない。本書の特徴は、まず記述が平易でひとりで読み進められるということである。また、本書を読むために予備知識はほとんど必要でない。高校卒業程度の知識があればだれでも読み進めることができるはずである。しかし、基礎的な内容の解説だけに終始しているかというところでもない。他の入門的な教科書にはあまり書かれていない比較的高度なこと（しかし重要なこと）、たとえば実際に使われているデジタル変調の方式（2.4.3項、2.4.4項）、無線LANのフレームの詳細（4.10.2項）、TCPの輻輳制御の詳細（6.6.3項）、HTTPのメッセージの詳細（7.5.2項）などが本書には含まれている。

本書の執筆は2023年2月に完了したが、可能な限りこの時点の最新の技術動向を反映するようにした。情報通信の技術は日進月歩であり、ある時点で最新の技術であったものがその後廃れて使われなくなることは普通に起こる。しかし、基本的なところは変わらないのである。本書では基本を丁寧に説明しつつ最新の技術動向を紹介している。

読者には情報関連の資格取得を目指す人も多いと思う。本書の各章末の演習問題には基本情報技術者試験、応用情報技術者試験、ネットワークスペシャリスト試験等の過去問題から多くを収録した。本書で学んだ内容がどのような設問として問われるかがわかるようになっている。各章の間および演習問題の解答例は巻末に示した。また、一部解答例の補足はコロナ社の本書紹介ページ[†]にアップした。

[†] <https://www.coronasha.co.jp/np/isbn/9784339029369/>

本書の構成は次のとおりである。第1章は序論であり、最低限知っておくべき知識を整理し情報通信ネットワークの概要を説明している。第2章はデジタル通信技術の解説である。高校数学で習う三角関数の基礎がわかっているならば理解できるはずである。第3章は通信プロトコルとはいったいどのようなものであるかを説明する。第4章は私たちの最も身近にあるネットワーク（LAN）の解説である。第5章と第6章はプロトコルの中でも特に重要なTCP/IPの解説である。第5章のIPは基本的な内容が中心であるが、第6章のTCPではこの種の入門書としてはかなり詳しい内容まで紹介した。第7章はインターネットサービスとそのプロトコルの解説である。ユーザには直接見えないDHCPとDNSを最初に解説しているのは、この2つはインターネット通信を支える基本的なプロトコルだからである。第8章はブロードバンド通信と移動通信の解説である。普段何気なく使っているPCやスマートフォンの裏側でどんな技術が使われているかを理解していただきたい。第9章はセキュリティに関する解説である。心構えや人的対策などは省略して技術的な内容に特化して記述した。

本書を大学や専門学校の半期の授業で使用する場合、第1章、第3章、第8章をそれぞれ1回、その他の章をそれぞれ2回の講義とすれば、全15回で完了することができる。もっともこれに従う必要はなく担当される先生の裁量で適宜変えていただいて差し支えない。

本書では紙数の関係で割愛せざるを得なかった内容が多々あるが、読者は巻末の参考文献を参照し、さらに深い知識を身につけていただきたいと思う。

最後に本書の内容について有益なご教示をいただいた北海道情報大学の中島潤教授、廣奥暢准教授に深く感謝いたします。また、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。

2023年6月

著 者

目 次

第1章 序 論

1.1 基 礎 事 項	1
1.1.1 10進数, 2進数および16進数	1
1.1.2 基 数 変 換	2
1.1.3 単位の接頭語	4
1.1.4 単位に関する注意	4
1.2 情報通信ネットワーク	5
1.2.1 情報通信ネットワークの発展	5
1.2.2 情報通信ネットワークの役割と構成	6
1.3 通 信 の 形 態	7
1.3.1 伝送媒体による分類	7
1.3.2 通信の方向による分類	7
1.3.3 通信相手の数による分類	9
1.3.4 ネットワークのトポロジーによる分類	10
1.4 情報通信ネットワークへの要求	10
1.5 インターネット	11
1.5.1 インターネットの歴史	11
1.5.2 インターネットおよび通信一般に関する組織	12
演 習 問 題	14

第2章 デジタル通信技術

2.1	アナログとデジタル	15
2.1.1	アナログとデジタルの定義	15
2.1.2	デジタル信号の特徴	16
2.2	情報のデジタル化	18
2.2.1	標 本 化	18
2.2.2	量 子 化	19
2.2.3	符 号 化	19
2.3	ベースバンド伝送とブロードバンド伝送	20
2.3.1	ベースバンド伝送	20
2.3.2	ブロードバンド伝送	22
2.4	変 調 技 術	23
2.4.1	正 弦 波	23
2.4.2	正弦波による信号波形の合成と分解	24
2.4.3	アナログ変調とデジタル変調	26
2.4.4	OFDM	31
2.5	多 重 化 技 術	32
2.5.1	周波数分割多重	32
2.5.2	時 分 割 多 重	33
2.5.3	符号分割多重	34
2.5.4	波長分割多重	34
2.5.5	多元接続方式	34
2.6	回線交換とパケット交換	35
2.6.1	交 換 方 式	35
2.6.2	回線交換と蓄積交換	36
2.6.3	コネクション型とコネクションレス型	38
	演 習 問 題	39

第3章 通信プロトコル

3.1 通信プロトコルの役割	40
3.2 階層化とその実現方法	41
3.2.1 プロトコルの例と階層化	41
3.2.2 通信プロトコルの階層化	41
3.2.3 階層化の実現方法	43
3.3 OSI 基本参照モデル	44
3.3.1 物理層 (第1層)	44
3.3.2 データリンク層 (第2層)	44
3.3.3 ネットワーク層 (第3層)	45
3.3.4 トランスポート層 (第4層)	45
3.3.5 セッション層 (第5層)	46
3.3.6 プレゼンテーション層 (第6層)	46
3.3.7 アプリケーション層 (第7層)	46
3.4 インターネットのプロトコル階層	48
3.4.1 ネットワークインタフェース層	49
3.4.2 ネットワーク層	49
3.4.3 トランスポート層	49
3.4.4 アプリケーション層	49
3.5 クライアント・サーバ型とピア・ツー・ピア型	50
演習問題	51

第4章 LAN

4.1 LAN の構成	53
4.2 MAC アドレス	54
4.3 Ethernet	56
4.4 ARP	58

4.5	媒体アクセス制御と CSMA/CD	61
4.6	Ethernet に用いられるネットワーク機器	62
4.6.1	リピータ	62
4.6.2	ハブ	62
4.6.3	スイッチとブリッジ	63
4.7	スパニングツリープロトコル	64
4.8	リンクアグリゲーション	66
4.9	VLAN	67
4.10	無線 LAN	69
4.10.1	無線 LAN の規格	69
4.10.2	無線 LAN のフレーム	70
4.11	CSMA/CA	73
4.11.1	無線 LAN における媒体アクセス制御	73
4.11.2	隠れ端末問題とその回避方法	73
4.12	PAN	75
4.12.1	Bluetooth	75
4.12.2	ZigBee	75
	演習問題	76

第5章 IP とルーティング

5.1	IP アドレス	77
5.1.1	IP アドレスの必要性	78
5.1.2	IPv4 アドレスの構成	78
5.1.3	IPv4 アドレスの枯渇問題と CIDR	81
5.1.4	IPv4 アドレスの設定	82
5.1.5	IPv6 アドレスの構成	83
5.1.6	IPv6 アドレスの設定	84
5.2	IP ネットワークの構成	84
5.3	IPv4 パケット	85

5.4 IPv6 パケット	89
5.5 アドレス変換技術	91
5.5.1 プライベートアドレスと NAT	91
5.5.2 IPv4 アドレスと IPv6 アドレス	92
5.6 ルーティングプロトコル	93
5.6.1 ルーティングの方式	93
5.6.2 IGP と EGP	94
5.6.3 RIP	95
5.6.4 OSPF	96
5.6.5 BGP	98
5.7 SDN	101
5.8 MPLS	103
5.9 ICMP	103
演習問題	105

第6章 TCP と UDP

6.1 ポート番号	106
6.2 TCP の役割	108
6.3 TCP セグメント	108
6.4 コネクションの確立と解放	111
6.5 再送制御と順序制御	113
6.5.1 再送制御	113
6.5.2 順序制御	114
6.5.3 再送タイマーの調整	114
6.6 フロー制御と輻輳制御	116
6.6.1 ウィンドウ制御	116
6.6.2 フロー制御	118
6.6.3 輻輳制御	120
6.7 UDP の役割	127

6.8 UDP データグラム	127
演習問題	128

第7章 インターネットサービスとプロトコル

7.1 DHCP	130
7.2 DNS	132
7.2.1 ドメイン名とDNS	132
7.2.2 DNSの仕組み	135
7.3 電子メール	137
7.3.1 電子メールシステムとプロトコルの概要	137
7.3.2 SMTP	139
7.3.3 POP3とIMAP4	139
7.3.4 添付ファイル	140
7.4 ファイル転送	140
7.5 WWW	143
7.5.1 WWWとHTTPの概要	143
7.5.2 HTTPのメッセージ	144
7.5.3 Web情報のキャッシュ	147
7.5.4 CGI	149
7.5.5 JavaScript	150
7.5.6 cookie	151
7.6 遠隔コンピュータ制御	152
7.7 ネットワーク管理	153
演習問題	155

第8章 ブロードバンド通信と移動通信

8.1 ブロードバンド通信	157
8.2 ブロードバンドアクセス方式	158

8.2.1 FTTH	158
8.2.2 CATV	161
8.2.3 公衆無線 LAN, WiMAX その他	162
8.3 リアルタイム通信	163
8.3.1 リアルタイム性	163
8.3.2 リアルタイム通信に用いられるプロトコル	164
8.3.3 RTP	165
8.3.4 RTCP	166
8.3.5 VoIP	167
8.3.6 SIP	168
8.4 移動通信の歴史と世代	169
8.5 4G ネットワークの構成と仕組み	170
8.6 5G ネットワークの特徴	172
演習問題	173

第9章 ネットワークセキュリティ

9.1 情報セキュリティの要素	175
9.2 セキュリティに対する脅威と備え	176
9.2.1 DoS 攻撃	176
9.2.2 さまざまな攻撃手法	178
9.2.3 マルウェア	179
9.2.4 ファイアウォール	180
9.2.5 侵入検知/防止システム	181
9.3 暗号技術	182
9.4 共通鍵暗号方式と公開鍵暗号方式	184
9.4.1 2つの暗号方式	184
9.4.2 AES	185
9.4.3 RSA	186
9.5 電子署名と SHA	188

9.6 認 証 技 術	190
9.7 認 証 局 と PKI	192
9.8 プロトコルとセキュリティ	194
9.8.1 WPA	194
9.8.2 IPsec	194
9.8.3 TLS	196
演 習 問 題	197
参 考 文 献	199
問と演習問題の解答例	201
索 引	207

トを受け入れられるようになる。これを「ウィンドウが開く」と表現する。ウィンドウが開くと受信側はそれを送信側に ACK で伝える決まりになっている。送信側はこれを受けてセグメントの送信を再開する。

6.6.3 輻輳制御

LAN, 特に有線 LAN の内部ではネットワークの混雑が発生することは稀であるから, 前節で述べたフロー制御さえあればセグメントを順調に転送することができる。しかし, インターネットを介して離れた端末にセグメントを転送する場合は, フロー制御だけでは不十分である。インターネットには多くの TCP コネクションが同時に存在し, 同一の経路 (伝送路) 上にも多くのパケットが流れている。各端末がフロー制御だけに基づいて, パケットを次々に送り出すとネットワーク上で混雑や渋滞が発生することがある。間にあるルータの受信バッファがいっぱいになると, その後到着するパケットは破棄されてしまう。その場合, TCP は再送を行うから, 混雑はますますひどくなる。ネットワーク上で発生するパケットの混雑のことを輻輳 (congestion) と呼ぶ。

TCP には輻輳を回避するための仕組みがあり, その動作を輻輳制御 (congestion control) と呼ぶ。輻輳制御では輻輳がなるべく発生しないようにセグメントの送信数が調整される。フロー制御が相手端末の受信バッファの空き状況に応じて送信量を調整するのに対して, 輻輳制御はネットワークの混雑状況に応じて送信量を調整するのである。

〔1〕輻輳の検出 さて, 輻輳制御を行うためにはネットワークの混雑状況を知る必要があるが, TCP は直接的にそれを知ることができない。それは輻輳が TCP の下にあるネットワーク層で発生する現象だからである。したがって, TCP は何らかの方法で混雑状況を推定するより仕方がない。そこで TCP は2つの現象に着目する。ひとつは送信時に起動するタイマーのタイムアウト発生である。相手から一定時間内に ACK が返ってこない場合は, 途中で混雑が発生しており, パケットが破棄されたと判断するのである。もうひとつは,

同じACKの重複受信（**重複ACK**）である。TCPには順序違いのセグメントを受信した際には、正しいセグメントを要求するACKをただちに返さなければならないという規則があることはすでに述べた（6.5.2項参照）。相手が順序違いのパケットを受信するということは、ネットワーク内で発生している混雑のためにパケットが途中で破棄されたと判断するのである。TCPは重複ACKを3回受信すると回復動作に入る。重複ACKを3回受信するということは、最初に受け取った（正常な）ACKを含めると全部で4回同じACKを受信することになる。

〔2〕 **スロースタートと輻輳回避** 輻輳の検出は以上のように行うが、送信量の調整は前節で述べた送信ウィンドウ（スライディングウィンドウ）の中にさらに**輻輳ウィンドウ**（congestion window）という小さなウィンドウを作って行う。輻輳ウィンドウは連続して送信できるセグメント数にさらに枠をはめる働きをする。

コネクション確立直後の輻輳ウィンドウの初期値は基本的に1セグメントである。したがって、最初の送信は1セグメントだけ行い、これにACKが返るとウィンドウをスライドさせて輻輳ウィンドウを1セグメント分増やす。つまり、2セグメント連続して送信できるようになる。2セグメント送信して2つACKが返ると今度はウィンドウサイズを4セグメントに増やす。つまり、ACKがひとつ返るごとに輻輳ウィンドウを1セグメント分増加させるのである。この動作を続けると輻輳ウィンドウは $1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 16 \rightarrow \dots$ のように指数関数的に増加し、一度に連続して送信するセグメントが増えていく。この動作を**スロースタート**（slow start）という。送信セグメント数が急速に増えるためスローとは奇妙な名前にも思われるが、「最初は1セグメントからゆっくり始める」という意味でスロースタートと呼んでいる。以上のように輻輳ウィンドウは最初、急速に成長するが、あらかじめ決められた大きさに到達するとスロースタートをやめて次の動作に移る。この閾値のことを**スロースタート閾値**（slow start threshold：**ssthresh**）という。

スロースタートの次のフェーズ（動作）は**輻輳回避**（congestion avoidance）と呼ばれる。輻輳回避では輻輳ウィンドウを少しずつ大きくしていく。輻輳ウィンドウ内のすべてのセグメントは連続的に一挙に送信される。この時に ACK 待ちのタイマーはひとつだけ起動する（セグメントごとではない）。そして RTT 後にこれらに対する ACK がやはり連続的に戻ってくる。これらの ACK によりウィンドウ全体が大きくスライドし、次のセグメント群を送信できるようになる。輻輳回避のフェーズでは、送信した輻輳ウィンドウ内のセグメントに対するすべての ACK に対して輻輳ウィンドウを約 1 セグメント増やす。たとえば、輻輳ウィンドウ内の 10 セグメントを送信し、10 個の ACK が戻ってくると輻輳ウィンドウを 11 セグメントに拡大するのである。ただし、すべての ACK が戻ってきた時点で 1 セグメント増やすのではなく、そういう割合になるようにひとつひとつの ACK に対してバイト単位で少しずつ増やしていくという方法を取る。輻輳回避では、輻輳ウィンドウの増加はスロースタートに比べてはるかに緩やかなものとなる。

輻輳回避フェーズにおける輻輳ウィンドウサイズの増加には限界がある。それは相手端末から通知されるウィンドウサイズである。相手端末から通知されるウィンドウサイズを特に**広告ウィンドウサイズ**（advertised window size）と呼ぶ。広告ウィンドウサイズを超えてセグメントを送信しないことは前項のフロー制御で述べた。図 6.8 はスロースタートと輻輳回避における輻輳ウィンド

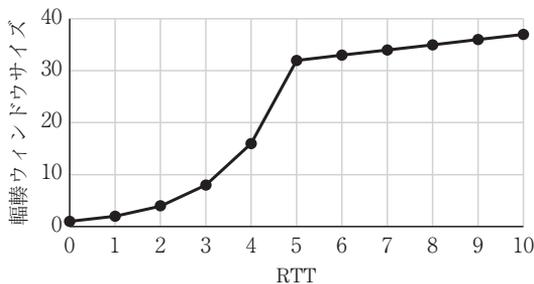


図 6.8 スロースタートと輻輳回避における輻輳ウィンドウサイズ

ウサイズの変化を示している。この例では ssthresh を 32 MSS としている。スロースタートで始まり、 $5 \times \text{RTT}$ の時点で輻輳回避に切り替わっている。

図 6.9 はスロースタートと輻輳回避における送受信の様子を時系列的に表したものである。この図では簡単のために ssthresh を 8 MSS としている。

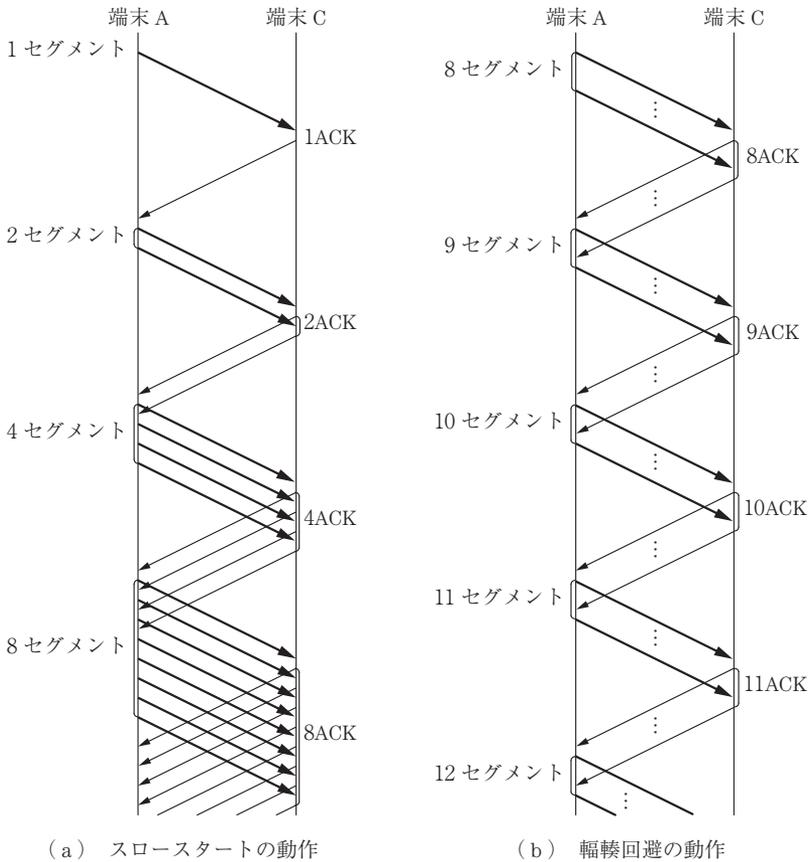


図 6.9 スロースタートと輻輳回避

〔3〕 **輻輳検出時の処理** さて、輻輳ウィンドウが増加を続ける中で送信タイマーのタイムアウトが発生したとしよう。この場合、TCP はネットワークに輻輳が発生していると判断し、輻輳ウィンドウのサイズを 1 セグメントに減らし、スロースタートから再開する。つまり、送信量を一挙に減らして輻輳

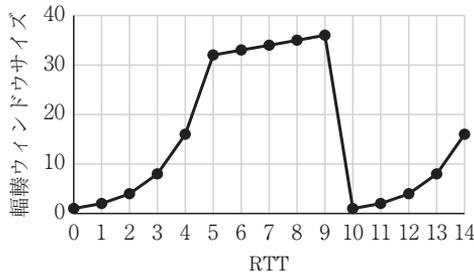


図 6.10 タイムアウト発生時の輻輳ウィンドウの変化

ウィンドウの増加を最初からやり直す。図 6.10 は、輻輳回避中にタイムアウトが発生した時の輻輳ウィンドウの変化を示している。9×RTT の時点でタイムアウトが発生し、輻輳ウィンドウサイズを 1 セグメントに減らし、スロースタートから再開している。

次に重複 ACK を 3 回受信した場合を考える。その場合は、まず、途中で破棄されたと思われる 1 セグメントだけをすぐに再送する。これをジェイコブソンの高速再送 (Jacobson's fast retransmit) と呼ぶ。そして、スロースタート閾値 (ssthresh) をその時点のフライトサイズの半分まで減少させる。また、輻輳ウィンドウのサイズはこの新しい ssthresh に MSS を 3 個分付け加えた値にセットする。重複 ACK を受信している間、ウィンドウはスライドしないので、新しいセグメントは基本的に送信できないが、それでは転送効率が悪いので重複 ACK を受信するたびに暫定的に 1 セグメントずつ輻輳ウィンドウを増加させる。この一時的な輻輳ウィンドウサイズの増加をインフレーション (inflation) と呼ぶ⁵⁾。インフレーションで拡大した輻輳ウィンドウ内に新たに送信できるセグメントがあれば送信する。

輻輳発生を検出して輻輳ウィンドウサイズを減少させる動作はわかりやすいが、なぜインフレーションのような動作を行うのだろうか。それは次の理由による。重複 ACK を受信するということは、相手端末は何かしかのセグメントを受信していることを意味している。したがって、たまたま 1 パケットだけ破棄された、あるいはそれほどひどい輻輳は発生していないと判断して、できる

だけセグメントの送信を続けるのである。上に述べたフライトサイズ $\times 1/2 + 3$ MSS の 3 MSS は重複 ACK 3 回分の受信に対応したものである。インフレーションがしばらく続くにしても、やがて正常な ACK が返るから、その時点で輻輳ウィンドウのサイズを先ほど更新した `ssthresh` に再度設定し直す。つまり、インフレーションで暫定的に増やした分を一挙に帳消しにするのである。

正常な ACK が返ると輻輳ウィンドウは大きくスライドし、新しいセグメント群を送信できるようになる。そして輻輳回避の動作を再開する。以上述べたように、重複 ACK を 3 回受信した場合はスロースタートからやり直しをするのではなく、`ssthresh` と輻輳ウィンドウを減少させて輻輳回避の動作を継続するのである。重複 ACK 3 回の受信から高速再送とインフレーションによるセグメントの送信を経て、正常 ACK の受信で輻輳回避に戻るまでの過程を**高速回復** (fast recovery) と呼ぶ。

図 6.11 は、輻輳回避中に重複 ACK を 3 回受信した時の輻輳ウィンドウの変化を示している。この図では簡単のために高速回復による過渡的な状態 (輻輳ウィンドウのインフレーション) は省略している。9 \times RTT の時点で重複 ACK 受信による輻輳ウィンドウの減少が起きているが、スロースタートに戻るのではなく輻輳回避動作を再開している。また、図 6.12 には高速再送と高速回復の動作例を示す。この例ではセグメントを 4 個送信し、その先頭のセグメントが破棄された場合の動作を示している。図 6.12 (a) は輻輳ウィンドウ内のセグメントとスライドの様子を示し、同図 (b) はセグメント送受信の様子を表

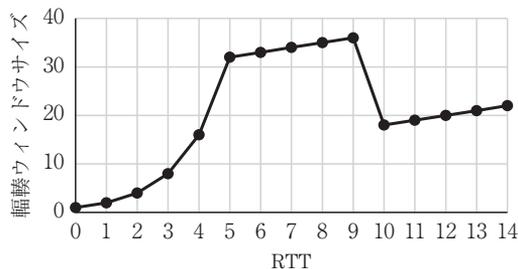
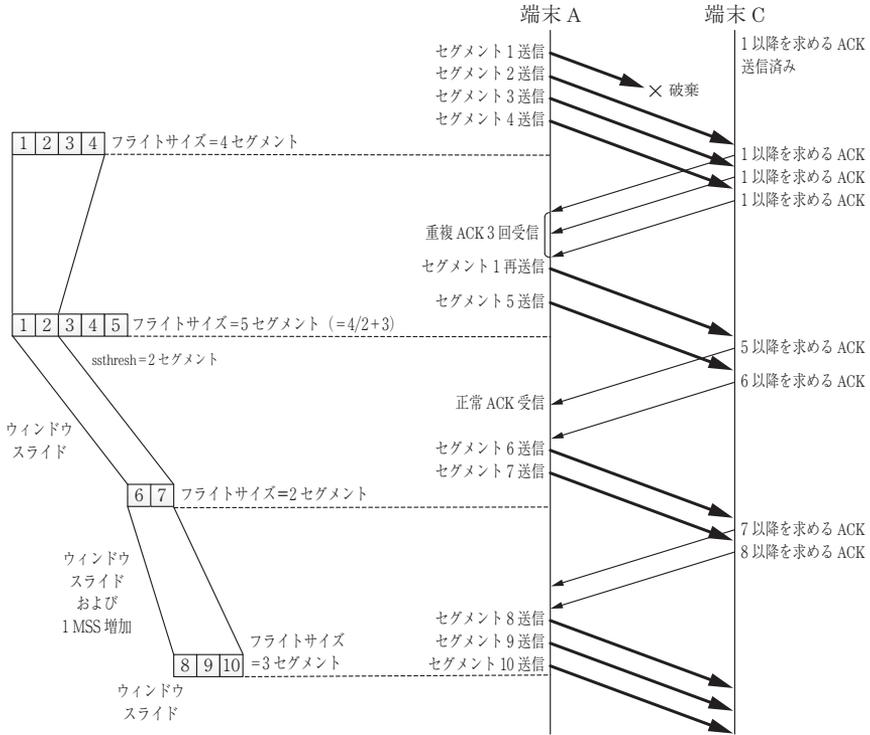


図 6.11 重複 ACK を 3 回受信した時の輻輳ウィンドウの変化



(a) 輻輳ウィンドウの中身とスライドの様子 (b) セグメント送受信の様子

図 6.12 高速再送および高速回復の動作例

している。

以上述べた輻輳制御は最も標準的な方法であり通称 **Reno** と呼ばれる。Reno を基本として送信ウィンドウ内の複数のセグメント欠落に対して回復動作を速めた改良版は **New Reno** と呼ばれる。ただし、New Reno が Reno と表記されている場合がある。標準的な方法以外にもいろいろな輻輳制御の方法が提案され、実際に使われている。特に伝送速度が高速で RTT が長い場合、スロースタートによる輻輳制御では伝送効率が悪いので、3 次関数の曲線を利用して急速に送信量を増加させる **cubic** という方法が現在では広く用いられている。

索引

【あ】	鍵配送問題	185	公開鍵	185	
アクセスネットワーク	6	角周波数	23	公開鍵暗号方式	185
アクセスポイント	54	隠れ端末問題	74	公開鍵基盤	193
アドレス解決	60	片方向通信	7	交換	35
アドレス学習機能	63	カプセル化	43	公衆無線 LAN	162
アドレステーブル	63	可用性	175	高速回復	125
アナログ信号	15	完全性	175	高調波	25
アナログ変調	26	カーンのアルゴリズム	115	呼制御	167
アプリケーション層	46, 49	【き】		コーデック	20
暗号技術	182	基数変換	1	コネクション	38
暗号文	182	基本波	25	コネクション型	38
【い】		機密性	175	コネクションレス型	38
位相	23	キャッシュ	147	コロン付き 16 進表記	83
位相偏移変調	26	キャッシュサーバ	147	【さ】	
位相変調	26	キャリア	23	再送制御	113
インタフェース ID	83	キャリア伝送	23	再送タイマー	113
インフレーション	124	共通鍵	185	雑音	16
【う】		共通鍵暗号方式	184	サブキャリア	31
ウイルス	179	距離ベクトル型	95	サブネットプレフィックス	83
ウィンドウサイズ	110, 118	【く】		サブネットマスク	82
ウィンドウ制御	116	クライアント・サーバ型	50	【し】	
ウェルノウンポート番号	106	クラウドコンピューティ ング	172	ジェイコブソンの高速再送	124
【え】		クラスフルアドレス	79	辞書攻撃	178
エージアウト	60	グローバルアドレス	91	システムコール	107
エッジコンピューティング	172	【け】		ジッタ	167
エフェメラルポート番号	107	ケーブルモデム	161	時分割多重	33
【か】		ケルクホフスの原理	184	周期	23
回線交換	36	減衰	16	周波数	24
鍵	183	【こ】		周波数成分	25
		コアネットワーク	6	周波数帯域	26
				周波数分割多重	32

周波数偏移変調	26	全二重通信	8	電子メール	137
周波数変調	26	専用線	35	伝送時間	17
受信バッファ	117			伝送速度	4
順序制御	114	【そ】		伝送媒体	7
情報源符号化	20	総当たり攻撃	178	伝送符号化	20
情報セキュリティの3要素		送信ウィンドウ	116	伝送路	7
	175	送信バッファ	116	電波（電磁波）	169
情報セキュリティの7要素		双方向通信	7	伝搬時間	17
	175	ソケット	107	【と】	
処理時間	17	ソフトリアルタイム性	163	ドット付き10進表記	79
真正性	175	【た】		トップレベルドメイン	133
侵入検知システム	181	帯域	26	ドメイン名	133
振幅	23	ダイクストラのアルゴリズム	97	ドライブバイダウンロード	178
振幅偏移変調	26	ダイナミックルーティング	93	トラップ	154
振幅変調	26		93	トラフィックエンジニアリング	103
信頼性	10, 175	タイプ	57	トランクポート	68
【す】		タイムスタンプオプション	111	トランスポート層	45, 49
スイッチ	63	【ち】		トレーラ	42
スイッチングハブ	63	遅延	17	トロイの木馬	179
スクランブル	22	蓄積交換	36	【な】	
スター型	10	チャレンジレスポンス方式	192	名前解決	133
スタティックルーティング		重複ACK	114, 121	【に】	
	93	【つ】		認証技術	190
スパニングツリー		通信プロトコル	40	認証局	192
プロトコル	65	通信路符号化	20	【ね】	
スプリッタ	159	【て】		ネットワークアドレス	80
スライディングウィンドウ		デジタル証明書	192	ネットワークインタフェース層	49
	116	デジタル署名	189	ネットワークスライシング	173
スロースタート	121	デジタル信号	15	ネットワーク層	45, 49
スロースタート閾値	121	デジタル変調	26	ネットワーク部	79
【せ】		テザリング	163	【の】	
制御プレーン	102	データプレーン	102	ノンス	192
正弦波	23	データリンク層	44		
脆弱	176	デフォルトゲートウェイ	54		
性能	10	電子証明書	192		
責任追及性	175	電子署名	189		
セキュリティ	10				
セキュリティホール	178				
セッション	38				
セッション層	46				
ゼロデイ攻撃	178				

【は】

媒体アクセス制御 61

バイト 1

パケット交換 36

パケットフィルタリング 180

バス型 10

バス属性 100

パスベクトル型 99

パスワード 190

波長分割多重 34

ハッシュ関数 189

ハードリアルタイム性 163

ハブ 62

パルス符号変調 20

反射攻撃 190

搬送波 23

半二重通信 8

【ひ】

ピア・ツー・ピア型 51

ひずみ 16

ビット 1

否認防止 175

非武装地帯 180

秘密鍵 185

標本化 18

標本化周波数 18

標本化定理 18

平文 182

【ふ】

ファイアウォール 180

フィッシング 178

フォーマット 40

フォワーディング 93

輻輳 120

輻輳ウィンドウ 121

輻輳回避 122

輻輳制御 120

符号化 19

符号分割多重 34

物理層 44

フライトサイズ 117

プライベートアドレス 91

フラグメント 87

フラッディング 63

プリアンプル 57

フーリエ級数 24

フーリエ変換 26

ブリッジ 64

プレゼンテーション層 46

プレフィックス 82

フレーム 53

プロシージャ 40

フロー制御 118

プロセス 42

ブロードキャスト 9

ブロードキャストアドレス 90

ブロードキャストストーム 64

ブロードバンド通信 157

ブロードバンド伝送 23

分散クラウド 172

【へ】

ベストエフォート 45

ベースバンド伝送 20

ヘッダ 42

変調 23

【ほ】

ホスト部 79

ポート番号 106

ポーリング 154

【ま】

待ち時間 17

マルウェア 179

マルチキャスト 9

【む】

無線 LAN 69

無線通信 7

【め】

メディアコンバータ 158

【ゆ】

有線通信 7

ユニキャスト 9

【ら】

ラウンドトリップタイム 115

ラベル 103

【り】

リアルタイム性 163

離散フーリエ変換 32

リピータ 62

量子化 19

量子化雑音 19

リンクアグリゲーション 66

リング型 10

リンクステート型 97

リンクローカルアドレス 92

【る】

ルーティング 77

ルーティングテーブル 93

ルーティングプロトコル 93

ルートドメイン 133

【れ】

レゾルバ 135

【わ】

ワーム 179

	[A]	DNS キャッシュ	136	IDS	181
		DNS キャッシュポイズ		IEEE	13
A/D 変換	18	ニング	178	IEEE802.11	69
ADSL	157	DoS	176	IEEE802.3 規格	57
AES	185	DQPSK	29	IETF	13
AM	26	DSCP	86	IFG	58
AP	54			IGP	94
APNIC	12	[E]		IMAP4	138
ARP	58	EGP	94	IMS	171
ARPANET	11	eNodeB	171	IoT	81
ARP テーブル	60	EPC	170	IP	77
AS	94	ESP	195	IPS	181
ASK	26	Ethernet	53	IPsec	194
	[B]			IPv4	77
		[F]		IPv6	77
Base64	140	FCS	57	IP アドレス	77
BGP	98	FDM	32	IP アドレス枯渇問題	81
Bluetooth	75	FDMA	35	IP マスカレード	92
bps	4	FFT	32	IP マルチメディアサブシス	
BPSK	28	FM	26	テム	171
	[C]	FMC	38	ISM 帯	69
		FQDN	134	ISP	13
CA	192	FSK	26	ITU-T	14
CATV	161	FTP	140		[J]
CDM	34	FTPS	141		
CDMA	35	FTTB	158	JavaScript	151
CGI	149	FTTH	157	JPNIC	13
CIDR	82				[L]
CMTS	161	[G]			
cookie	151	GE-PON	160	LAN	53
CSMA/CA	73			LSB	3
CSMA/CD	61	[H]		LSR	103
CTS	74	HFC	161	LTE	169
cubic	126	HMAC	189		[M]
	[D]	HSS	172		
		HTML	143	MAC アドレス	54
D/A 変換	18	HTTP	143	MIB	154
DBPSK	29	Hz	24	MIME	139
DDoS	177			MME	172
DHCP	130	[I]		MPLS	103
DIX 規格	57	ICANN	12	MSB	3
DMZ	180	ICMP	103	MSS	111
DNS	133	ICT	6	MSS オプション	111

MTU	86				
		[R]			
[N]					
		RAN	170	TDMA	35
NAPT	92	Reno	126	TELNET	152
NAT	92	RFC	13	TLD	133
NDP	84	RIP	95	TLS	196
NFV	172	RIR	12	TTL	88
NGN	37	RSA	186	[U]	
NIR	13	RSTP	66	UDP	127
NR	172	RTCP	164	UDP データグラム	127
NSFNET	11	RTP	164	URI	145
N 対 N 通信	9	RTS	74	[V]	
		RTT	115	VLAN	67
[O]				VLSM	96
		[S]		VoIP	167
OFDM	31	SA	195	VoLTE	171
OLT	159	SACK オプション	111	VPN	195
ONU	159	SDH	14	[W]	
OpenFlow	103	SDN	102, 172	WDM	34
OSI 基本参照モデル	44	SFD	58	WEP	194
OSPF	96	SFTP	141	Wi-Fi	70
OUI	55	S-GW	171	Wi-Fi スポット	162
		SHA	189	WiMAX	162
[P]		SIP	168	WPA	194
P2P	51	SMTP	138	WWW	143
PAN	75	SNMP	153	[Z]	
PCM	20	SNMP エージェント	154	ZigBee	75
PDU	42	SNMP マネージャ	154	[数字]	
P-GW	171	SPI	195	1 次変調	32
PKI	193	SQL インジェクション	178	1 対 1 通信	9
PM	26	SSH	152	1 対 N 通信	9
PON	159	STB	161	2 次変調	32
POP3	138	STP	65	3 ウェイハンドシェイク	111
PSK	26			4G	169
		[T]		5G	169
[Q]		TCP	108		
QAM	29	TCP コネクション	108		
QPSK	29	TCP セグメント	108		
QUIC	147	TDM	33		

— 著者略歴 —

1983年 京都大学工学部電気工学科卒業
1985年 京都大学大学院工学研究科修士課程修了（電子工学専攻）
1985年 日本電気株式会社（NEC）勤務（～2011年）
2007年 会津大学大学院非常勤講師（～2014年）
2009年 博士（コンピュータ理工学）（会津大学）
2011年 北海道情報大学教授
現在に至る

情報通信ネットワーク入門

Introduction to Information and Communication Networks

© Hirokazu Ozaki 2023

2023年8月24日 初版第1刷発行



検印省略

著者	尾崎博一
発行者	株式会社 コロナ社
代表者	牛来真也
印刷所	新日本印刷株式会社
製本所	有限会社 愛千製本所

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 <https://www.coronasha.co.jp>

ISBN 978-4-339-02936-9 C3055 Printed in Japan

(齋藤)



JCOPY <出版者著作権管理機構委託出版物>

本書の無断複製は著作権法上での例外を除き禁じられています。複製される場合は、そのつど事前に、出版者著作権管理機構(電話 03-5244-5088, FAX 03-5244-5089, e-mail: info@jcopy.or.jp)の許諾を得てください。

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います。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いません。落丁・乱丁はお取替えいたします。