情報ネットワーク論 (第8回)
TCP, UDP

H15, 6, 11

ファイル保存位置

\\172.17.40.249\www\lectures\情報ネットワーク論

http://172.17.40.249**からたどることができる。**

第7回演習

・公開鍵暗号を用いた相手認証の方法について説明せよ。

・IPv6のグローバルアドレスの構造と、そのような構造となっている理由を述べよ。

暗号化技術の分類

暗号方式

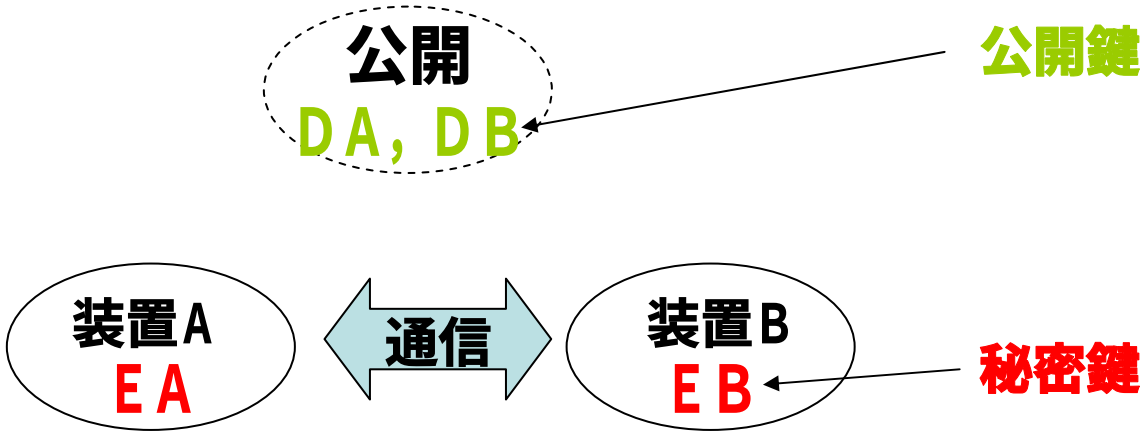
共通鍵暗号　(慣用暗号，対称暗号)

暗号化と復号に同じ暗号鍵を使う
ＤＥＳ(デス)，３ＤＥＳ(トリプルデス)，ＡＥＳなど多数
長所：演算時間が速い。
欠点：鍵の共有問題(どのようにして暗号鍵を共有するか)。

公開鍵暗号　(非対称暗号)

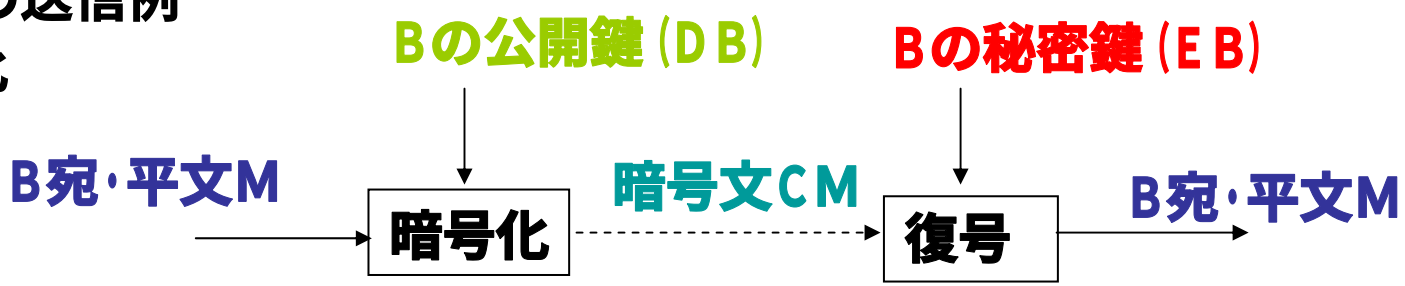
暗号化と復号に異なる暗号鍵を使う
ＲＳＡ
長所：鍵の共有問題がない。装置間の認証が可能。
欠点：演算に時間がかかる。

公開鍵の使用方法

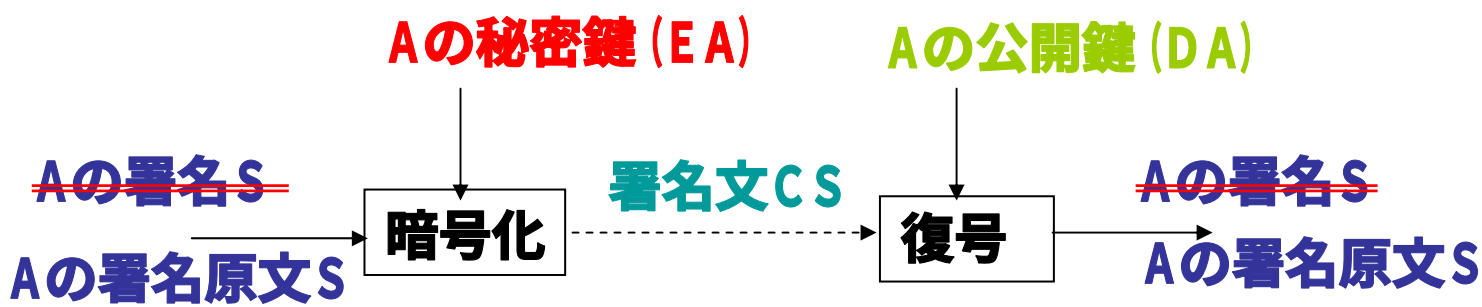


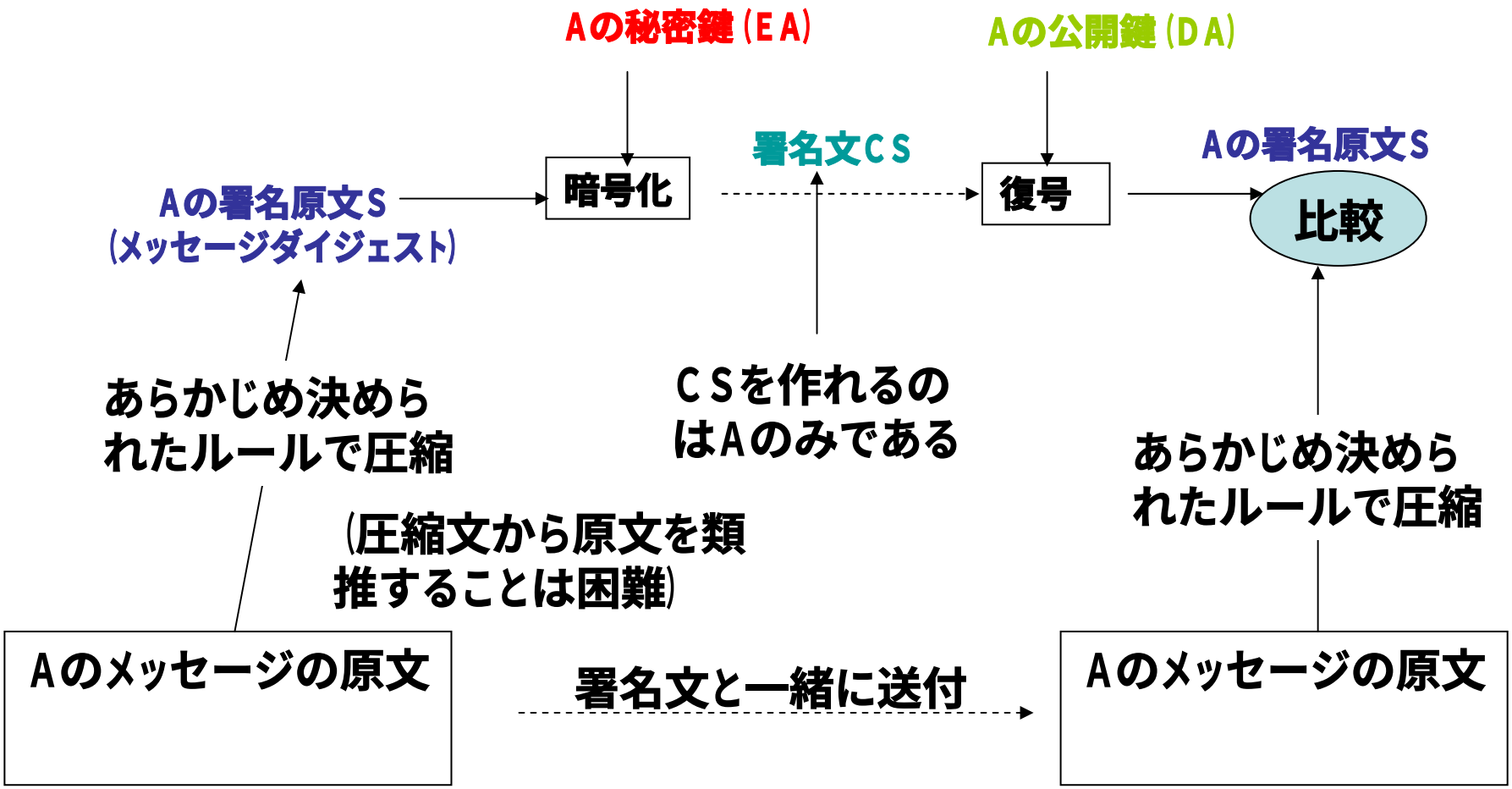
ＡからＢへの送信例

暗号化



認証





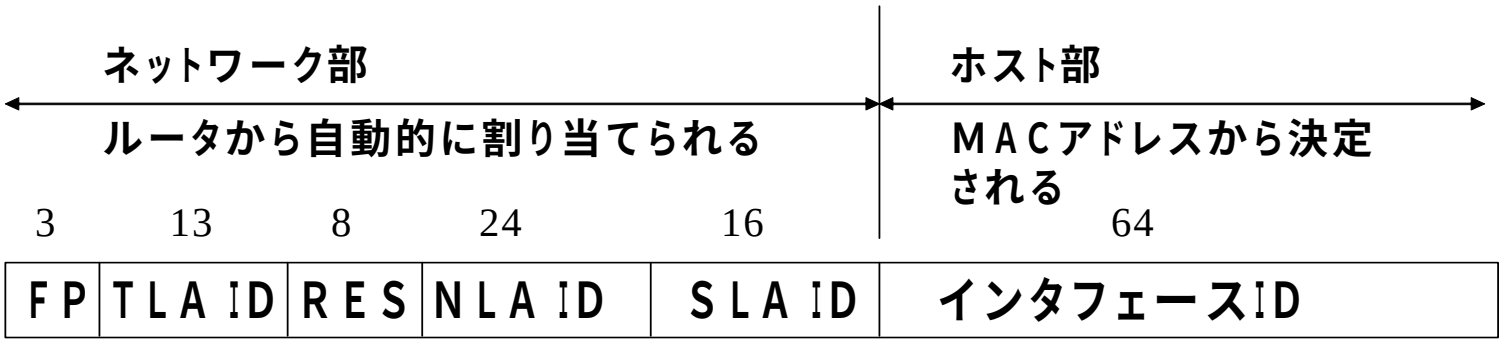
比較結果がOKであれば、以下のことが立証できる。

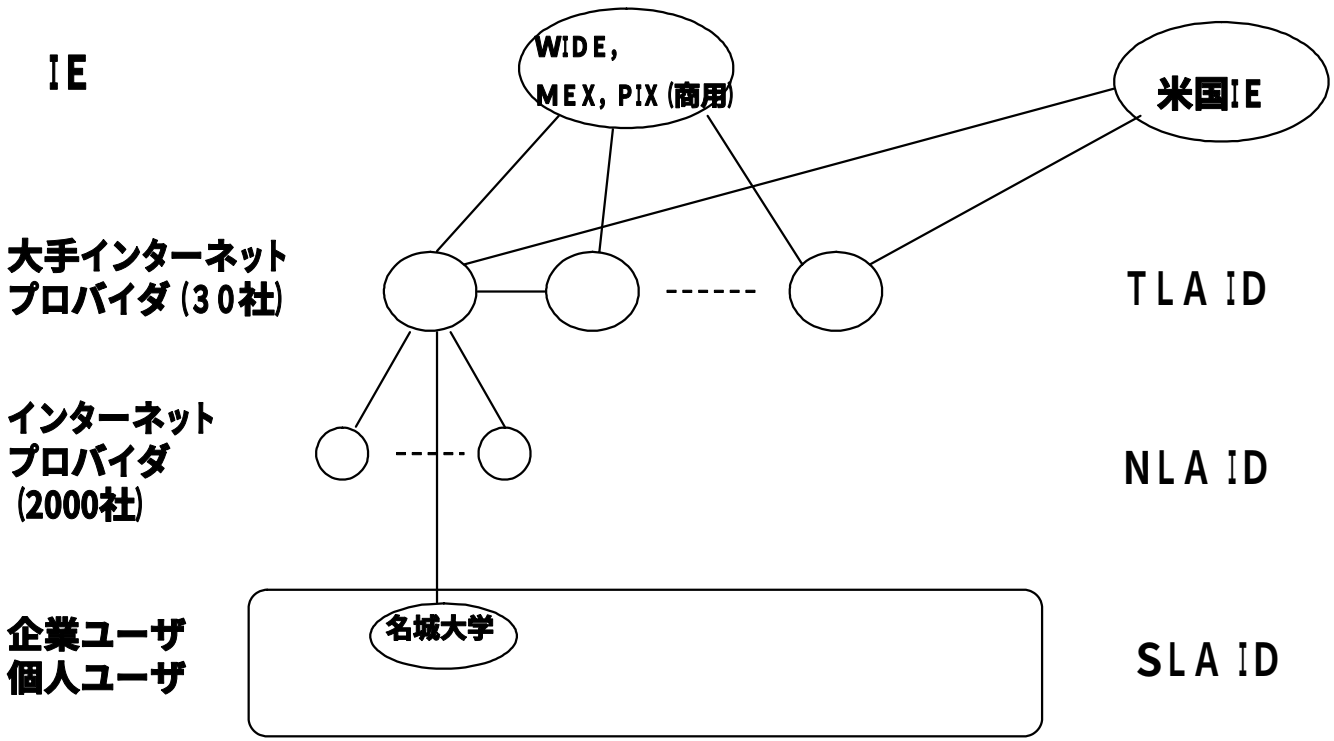
・原文は改竄されていない。

・署名文CSはAしか作れない。従って原文はAが作成したものである。

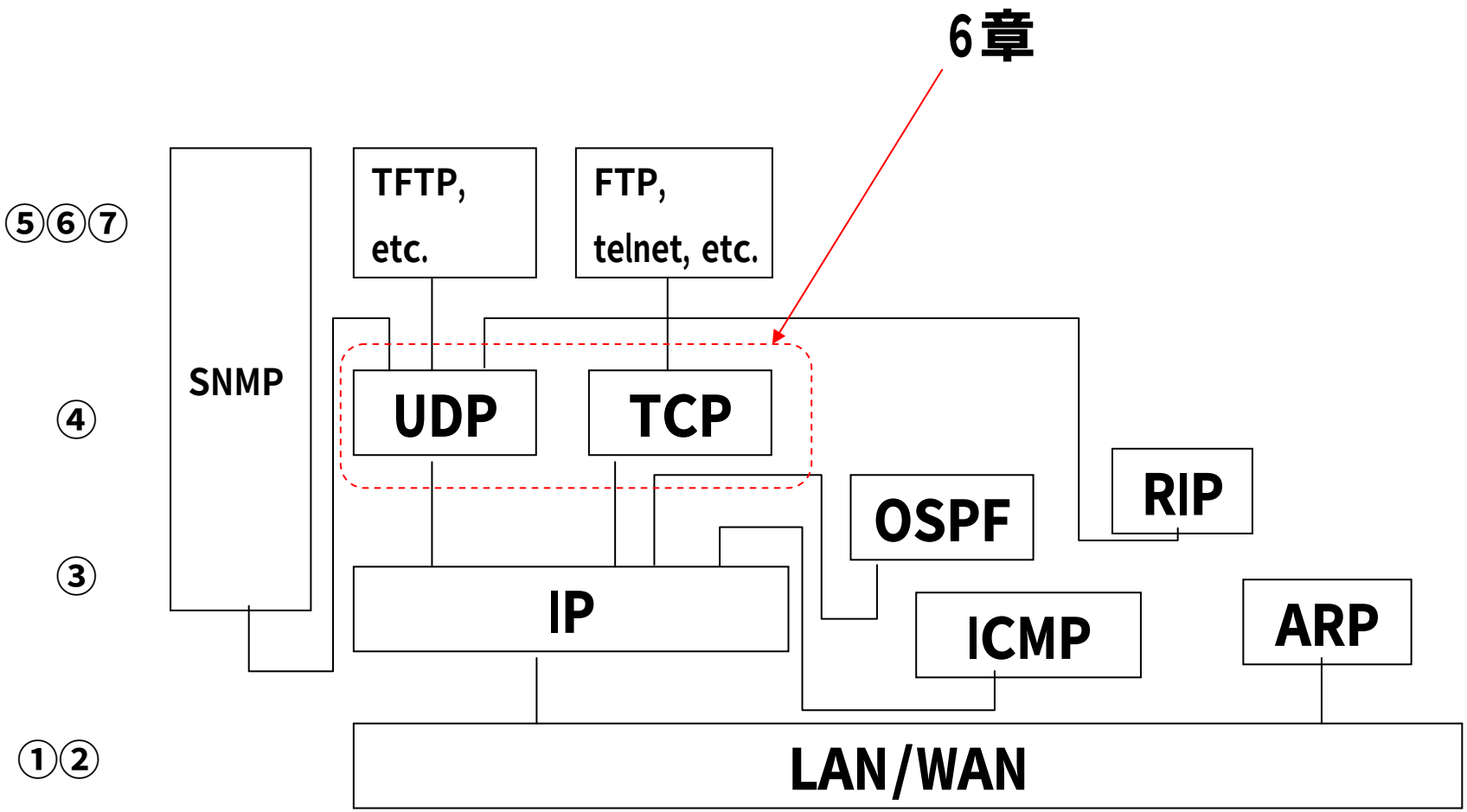
IPv6グローバルアドレスの構造

IPv6のIPアドレスはインターネットに適した階層構造になっており、経路制御表が簡単化されるように工夫されている。





本日の授業範囲


6章
⑤⑥⑦
④
③
①②
SNMP
TFTP,
etc.
FTP,
telnet, etc.
UDP
TCP
OSPF
RIP
IP
ICMP
ARP
LAN/WAN

ＴＣＰとＵＤＰ

トランスポート層プロトコル（エンドエンドのデータ転送の管理）

ＴＣＰはアプリケーションに信頼性のある通信を保証する。ＴＣＰとして複雑な制御が必要となるがアプリケーションはそれを意識しなくてよい。

ＴＣＰの中で実施する制御

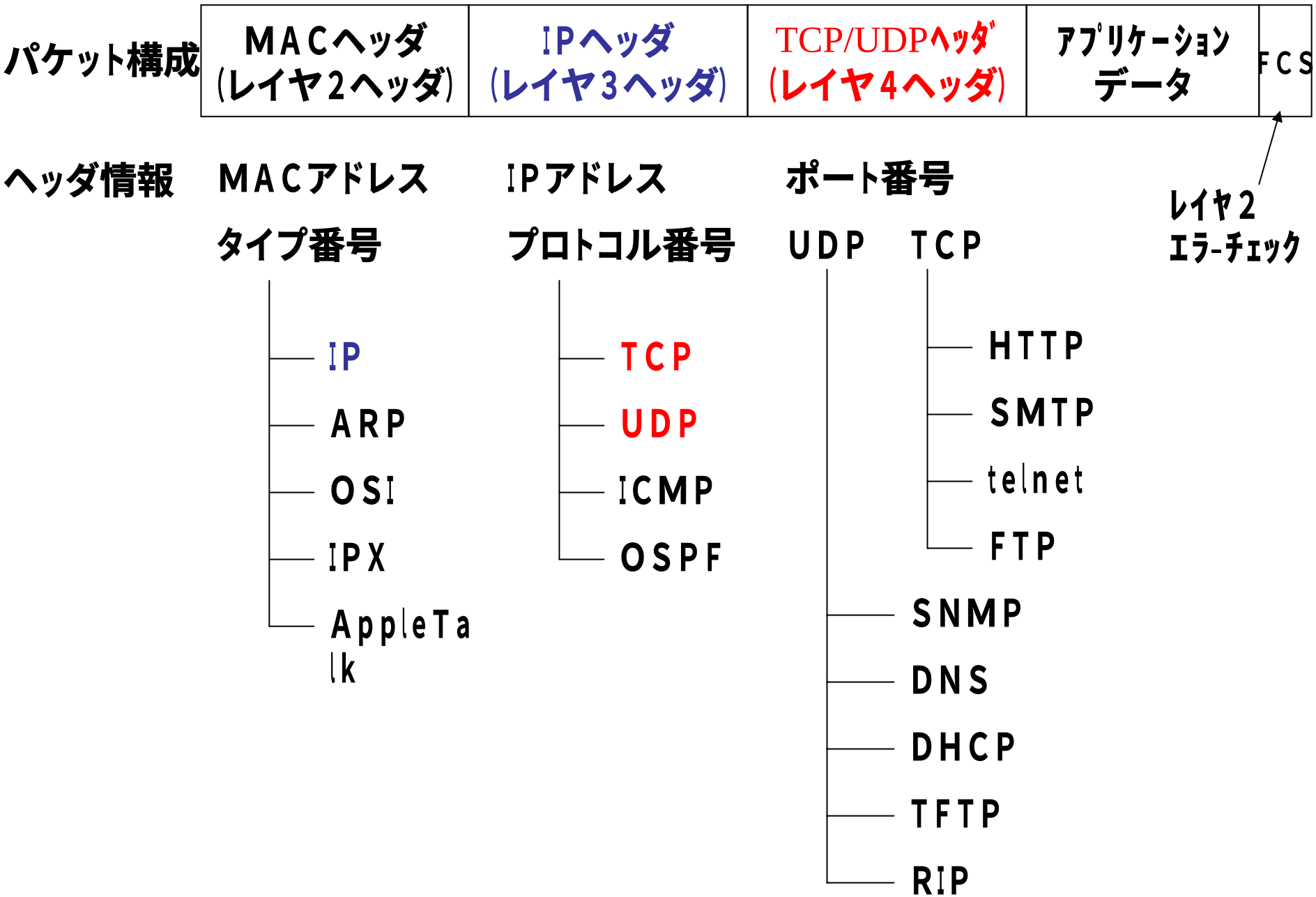
　コネクション管理、送達確認，フロー制御（流量制御），輻輳制御

ＵＤＰは複雑な制御を一切行わない。アプリケーション側が完全に制御の責任を持つ。特性に合った通信を実現できる。

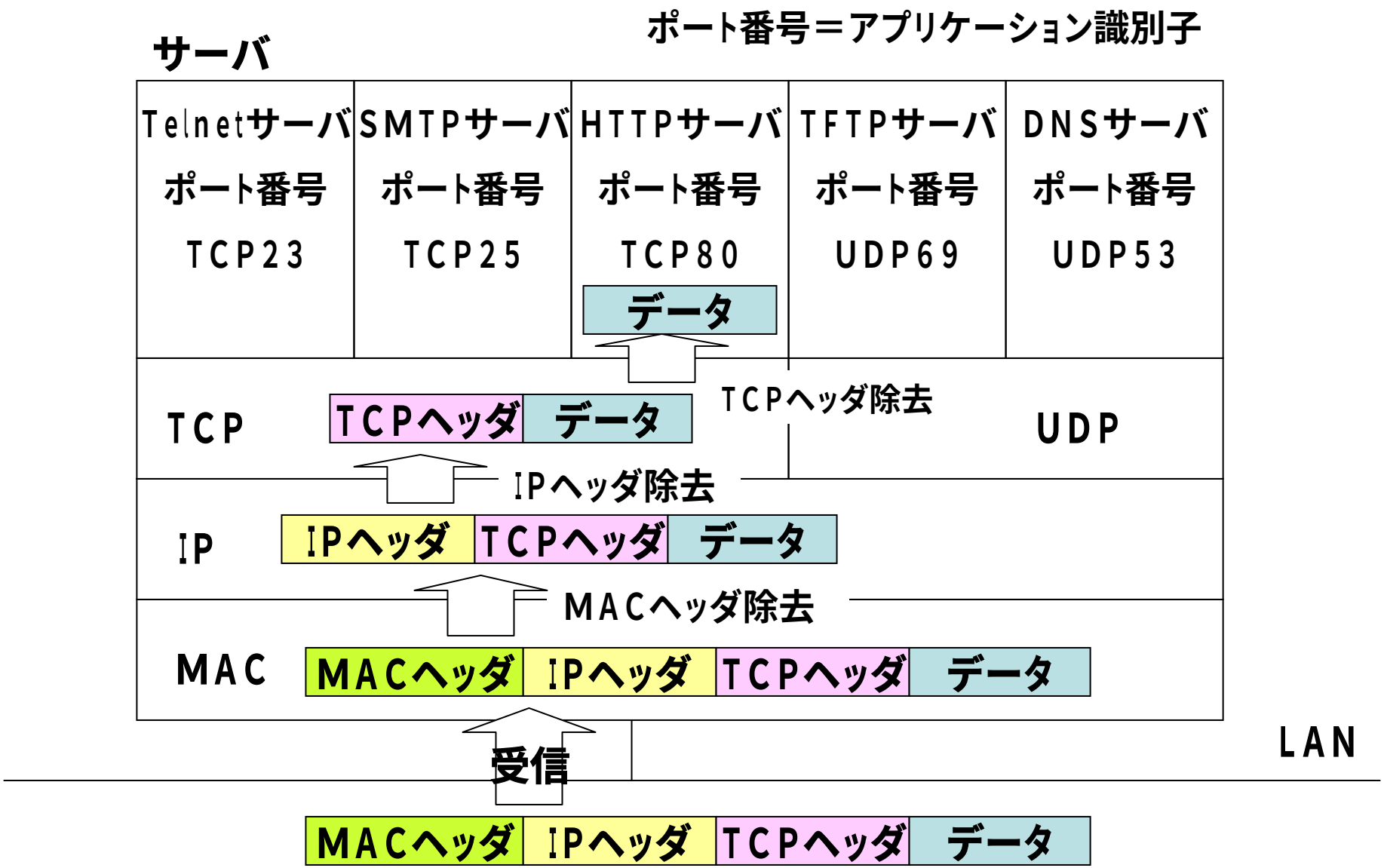
ＵＤＰに適した通信

　音声，画像などの高速リアルタイム通信，マルチキャスト（同報通信）

TCP/UDPヘッダの位置



ソフトウェアとヘッダ処理の関係（受信時）



ポート番号の決め方（たてまえ）

標準で決められている番号

サーバが提供するアプリケーションの番号（固定）

ウエルノウンポート　　0～1023

登録されたポート番号　　1024～49151

ダイナミックに割り当てられる番号

クライアントがサーバに要求をする際に割り当てる番号（動的）

ＯＳがそのクライアント内での番号の重複管理を行う

動的番号の範囲　　49152～65535

多くのシステムでは、上記の約束を無視して、1024以上の番号を動的に割り当てている。

代表的なウェルノウンポート番号（固定）

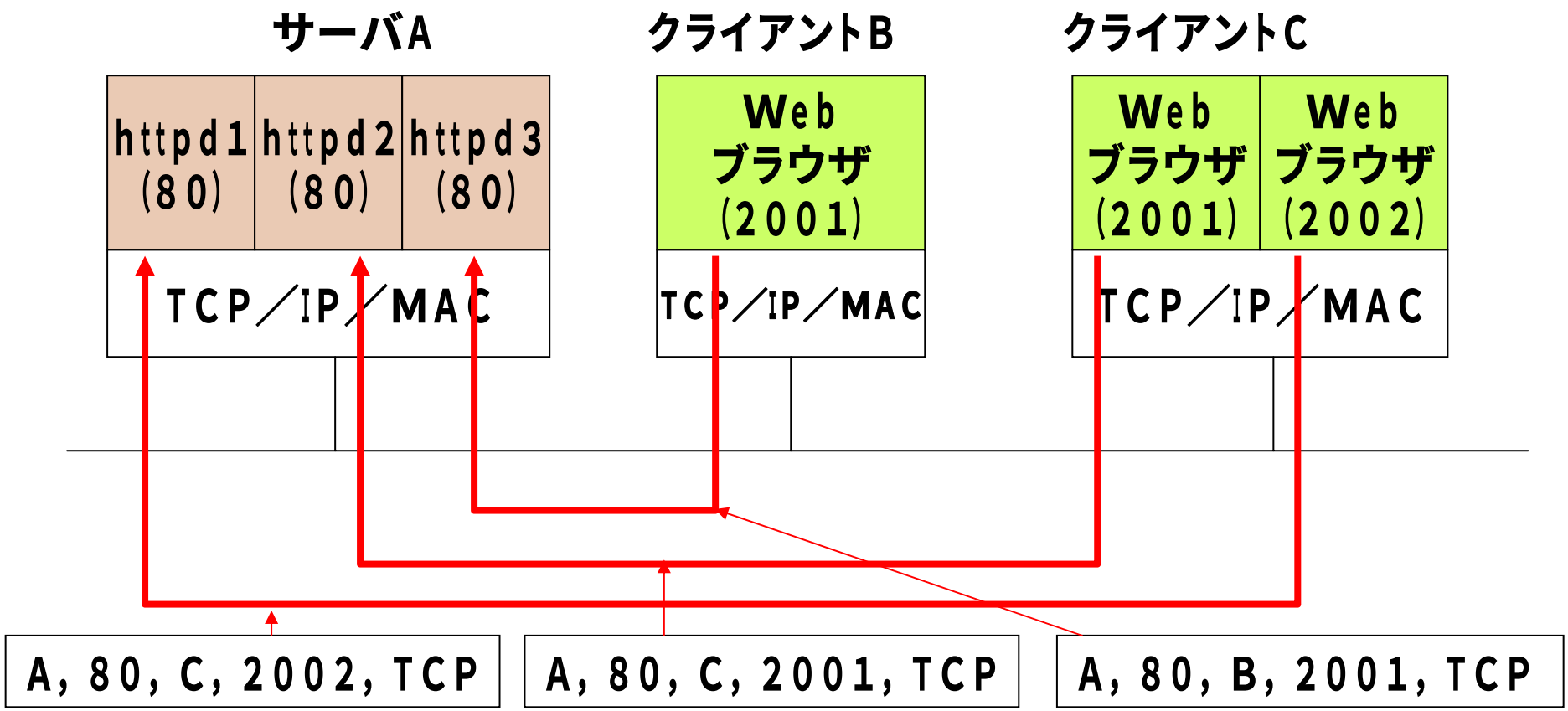
	ポート番号	内容
TCP	20	FTPデータ
	21	FTP制御
	23	telnet
	25	メール転送（SMTP）
	80	WWW（HTTP）
	110	メール受信（POP）
	443	暗号化WWW（HTTPS）
UDP	53	DNS
	67	DHCPサーバ
	68	DHCPクライアント
	161	ネットワーク管理（SNMP）
	520	ルーティング制御（RIP）

通信の識別

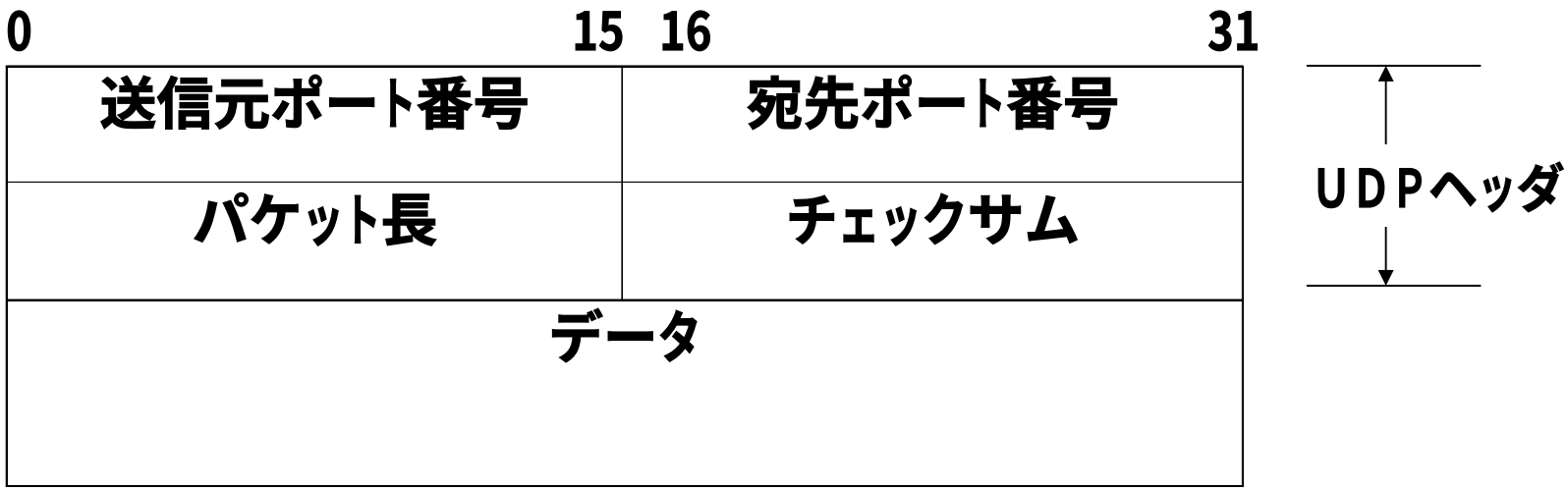
以下の5つの数字の組合せで通信を識別する。

①宛先IPアドレス，②送信元IPアドレス，

③宛先ポート番号，④送信元ポート番号，⑤プロトコル番号



ＵＤＰヘッダフォーマット



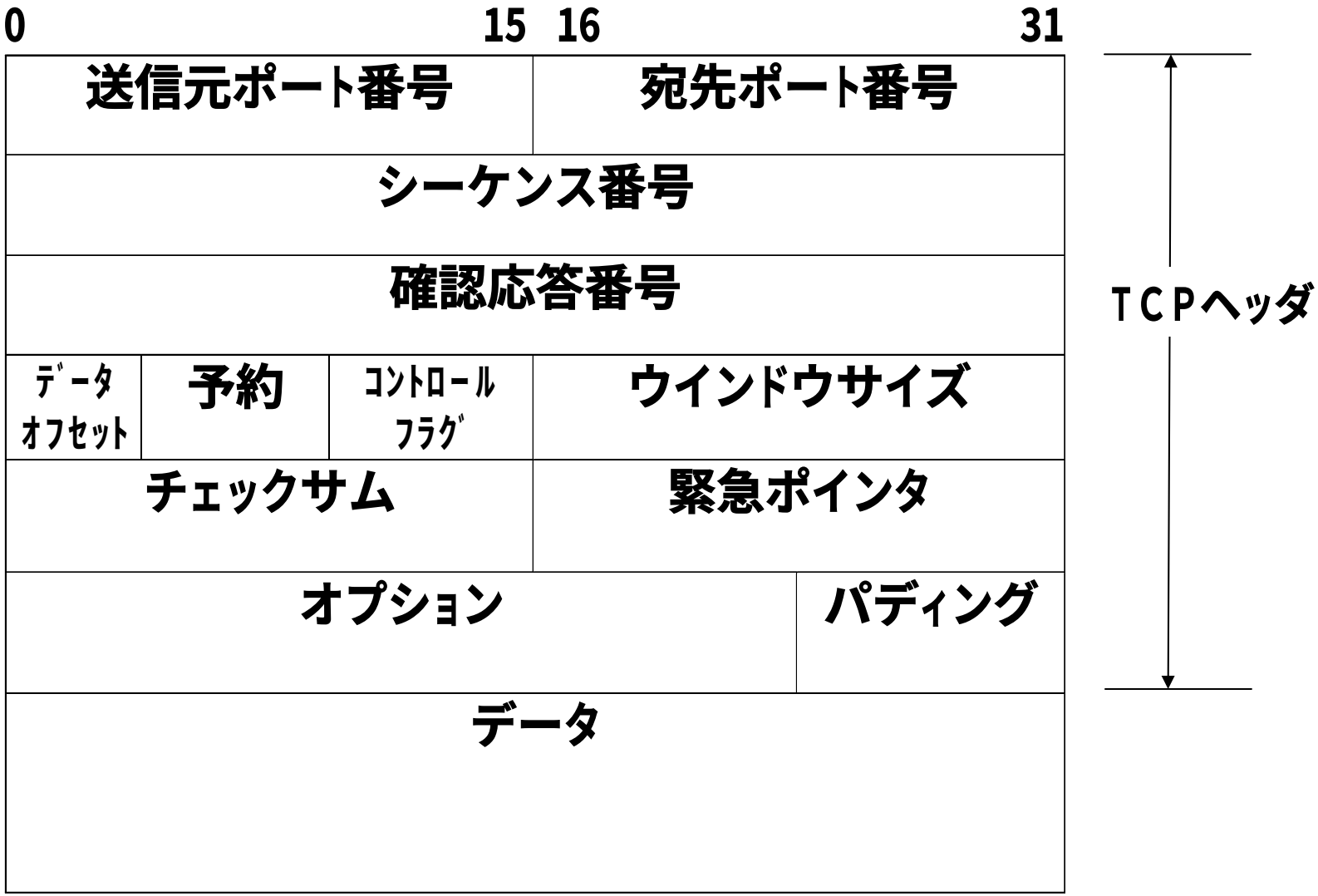
送信元ポート番号；送信元のポート番号を示す。オプション。

宛先ポート番号；宛先のポート番号を示す。

パケット長；ＵＤＰヘッダとデータの長さの和。バイト単位。

チェックサム；ＵＤＰヘッダとデータの信頼性を提供するためのフィールド。
オプション。

ＴＣＰヘッダフォーマット



送信元ポート番号;送信元のポート番号を示す。

宛先ポート番号;宛先のポート番号を示す。

シーケンス番号;送信したデータの位置を示す。送信するたびに送信データのバイト長が加算される。初期値はコネクション確立時に決定される。

確認応答番号;次に受信すべきデータのシーケンス番号を示す。

データオフセット;ＴＣＰのヘッダ長を示す。4バイト長。オプションがない場合は5が入る。

予約;将来の拡張用。0にする。

コントロールフラグ;

ＵＲＧ;緊急に処理すべきデータが含まれていることを示す。

ＡＣＫ;1のとき確認応答番号フィールドが有効であることを示す。

ＰＳＨ;1の場合受信データをすぐに上位アプリケーションに渡す。

ＲＳＴ;コネクションを強制的に切断するための指示。

ＳＹＮ;コネクションの確立要求であることを示す。

ＦＩＮ;コネクションの切断要求であることを示す。

ウィンドウサイズ；確認応答番号で示した位置から、受信可能なデータサイズを通知する。

チェックサム；ＴＣＰヘッダとデータの信頼性を提供するためのフィールド。必須。

チェックサムの演算方法

・ＴＣＰ擬似ヘッダを作成する。

・全長が１６ビットの倍数となるように0を追加する。

・ＴＣＰヘッダのチェックサムフィールドを1とする。

・１６ビット単位で１の補数の和を求める。

・求まった和の１の補数をチェックサムフィールドに入れる。

排他的論理和

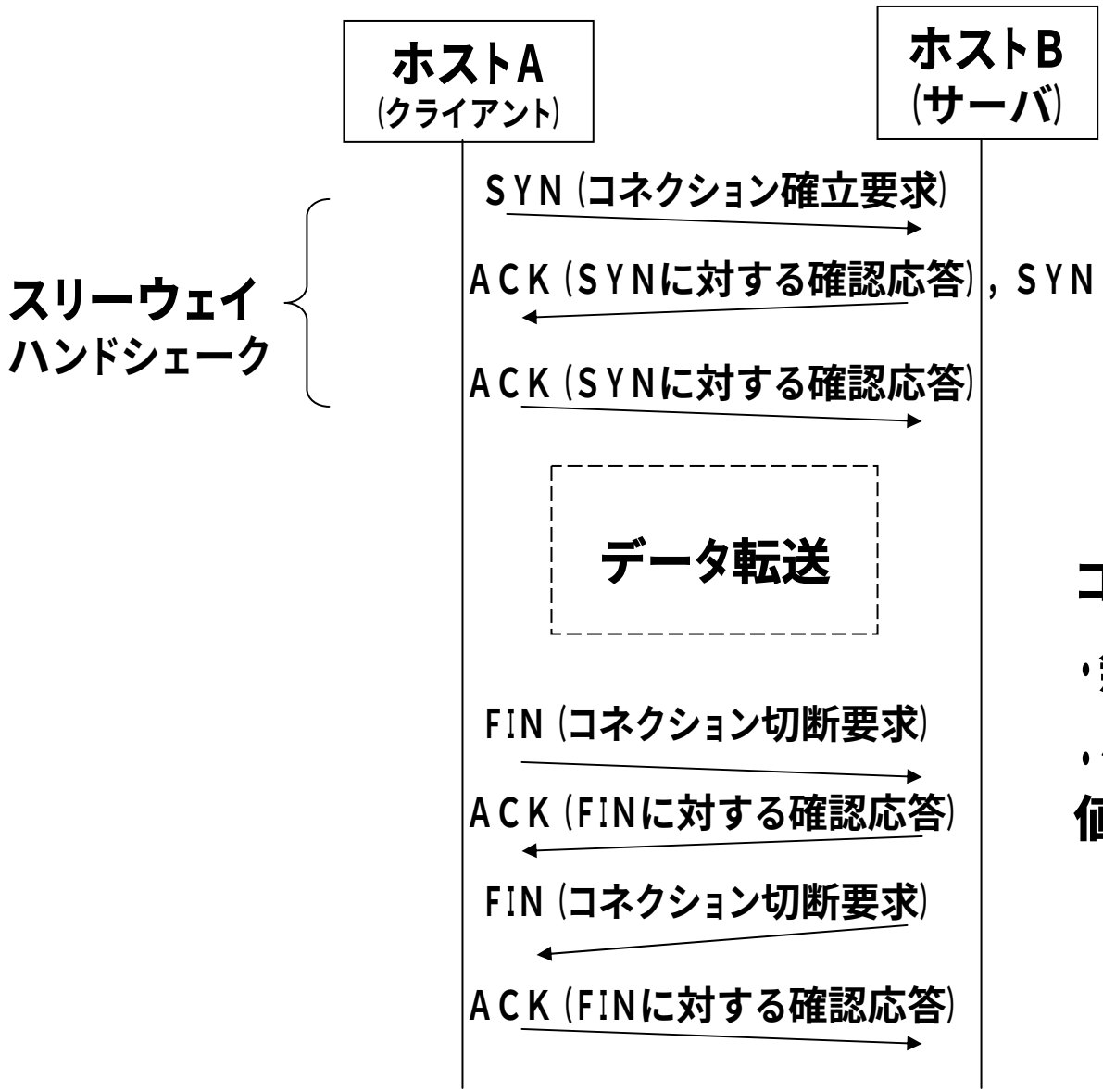
A	B	C
0	0	0
0	1	1
1	0	1
1	1	0

ＴＣＰ擬似ヘッダ

ＴＣＰの機能

- コネクション管理（相手の状態確認と通信の準備）
- 送達確認
  - シーケンス番号（パケットの順序制御）
  - 確認応答（パケットが相手に届いたことの確認）
- ウィンドウ制御
  - スライディングウィンドウ方式（連続送信に係わる再送制御）
  - フロー制御（受信バッファサイズによる制御）
  - ふくそう制御（ネットワークの混雑度による制御）
- その他
  - 遅延確認応答（応答を故意に遅らせる処理）
  - ピギーバック（データの送信パケットで確認応答を兼ねる方法）

コネクションの確立と切断（P１９４）

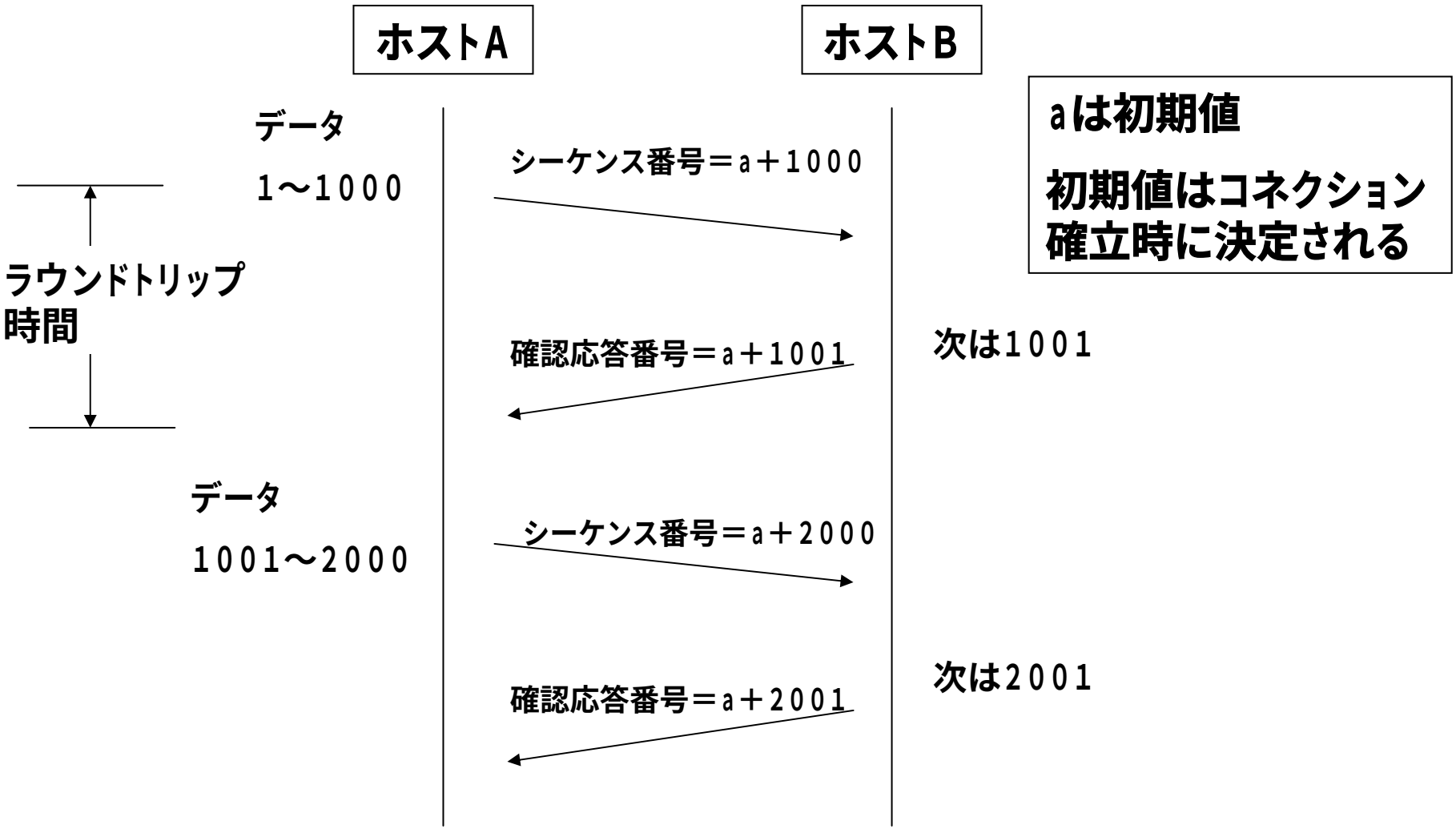


コネクション確立の意味

・無駄な転送を行わない。

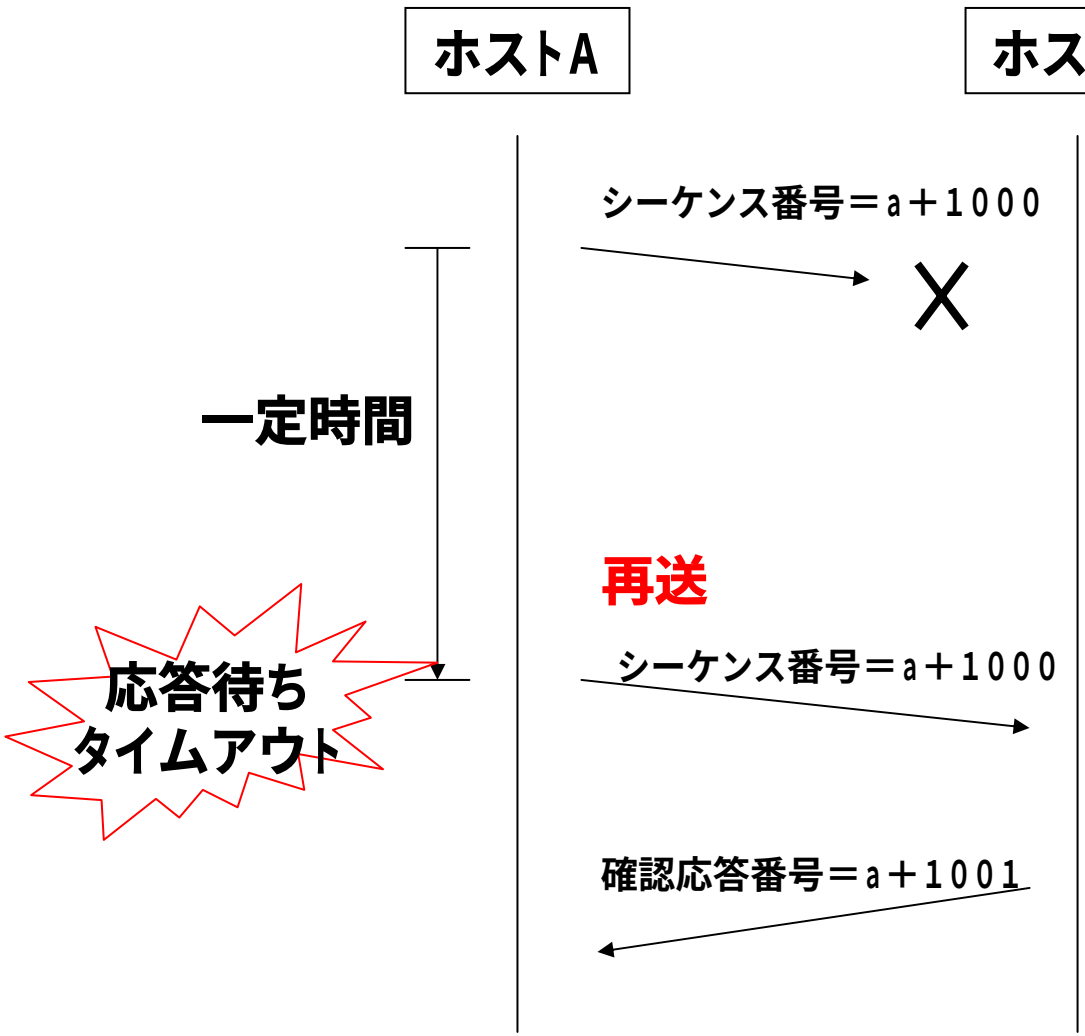
・シーケンス番号の初期値を決定する。

正常時のデータ送信（P１９０）



ラウンドトリップ時間が大きいとスループットが悪くなる。

送信パケットが喪失した場合（P１９１）



データ喪失の原因

・ネットワークの輻輳

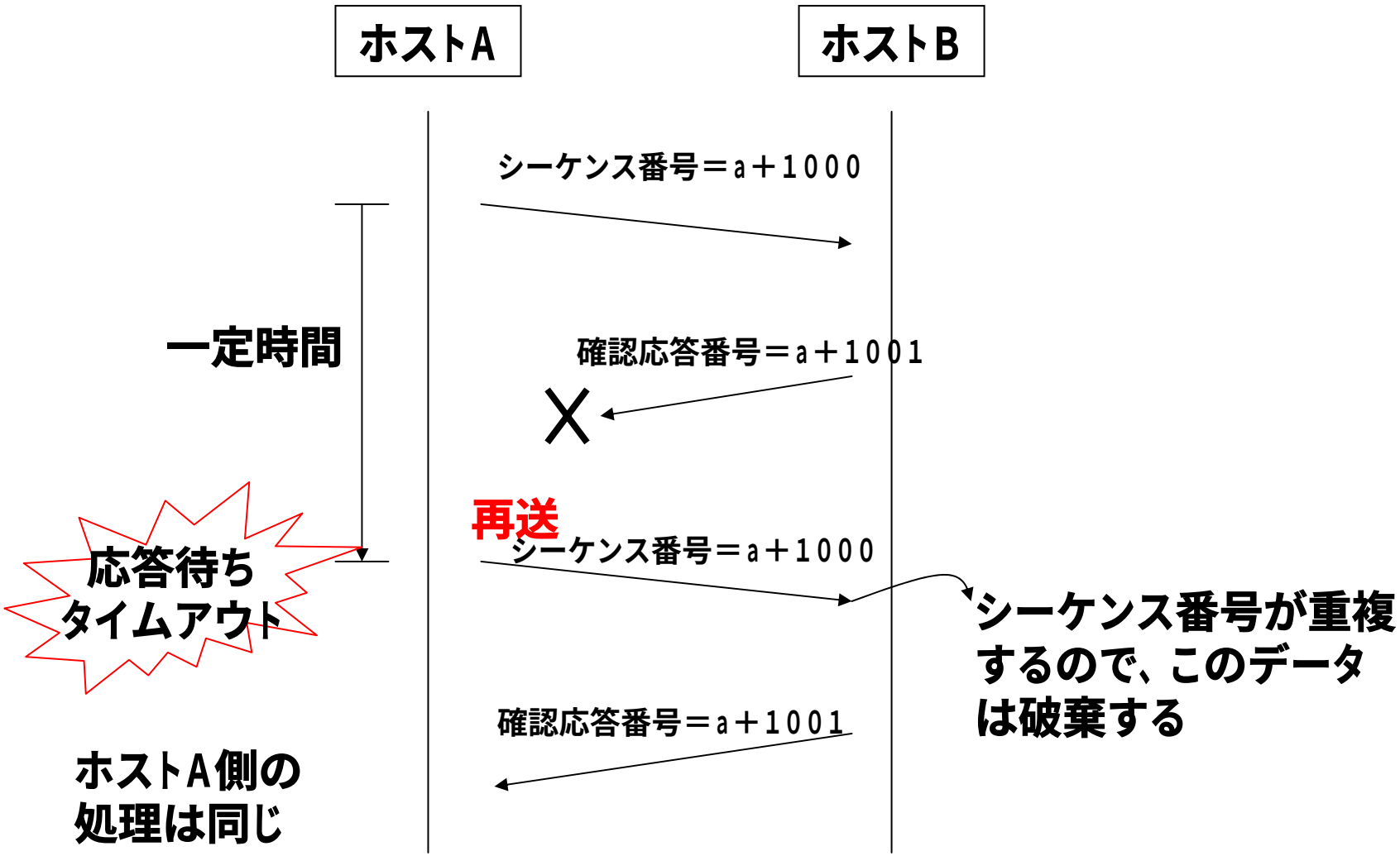
・ノイズによるパケット破壊

ＴＣＰでは肯定確認応答（ＡＣＫ）とタイムアウトの組合せで再送制御を行う。

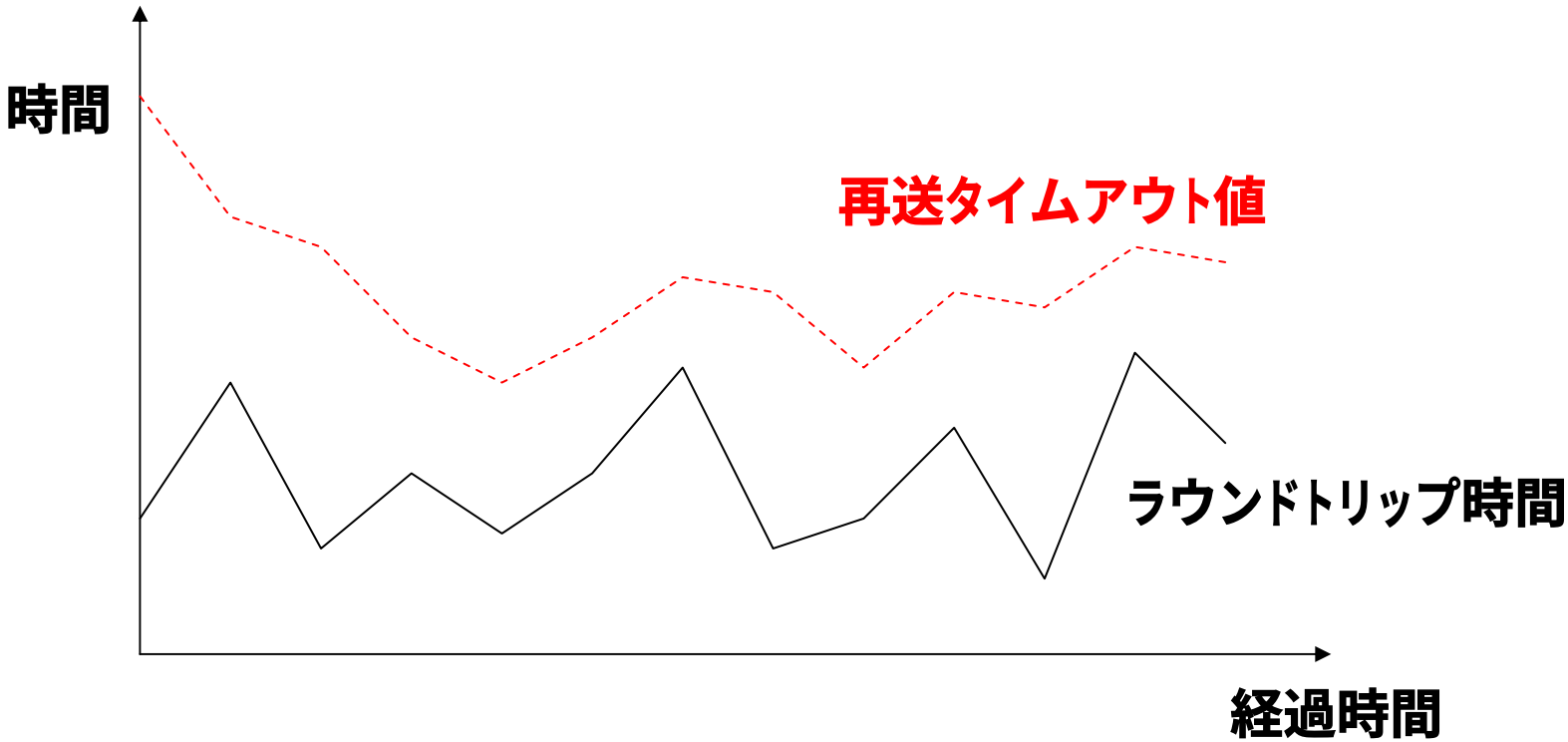
否定確認応答（ＮＡＫ(*)）は使わない。

(*)Negative Acknowledgement

確認応答が喪失した場合（P１９２）



ラウンドトリップ時間の計測と再送タイムアウト値の時間推移（P193）



ラウンドトリップ時間を毎回測定する。

ラウンドトリップ時間と揺らぎの時間を考慮してタイムアウト時間を決定する。

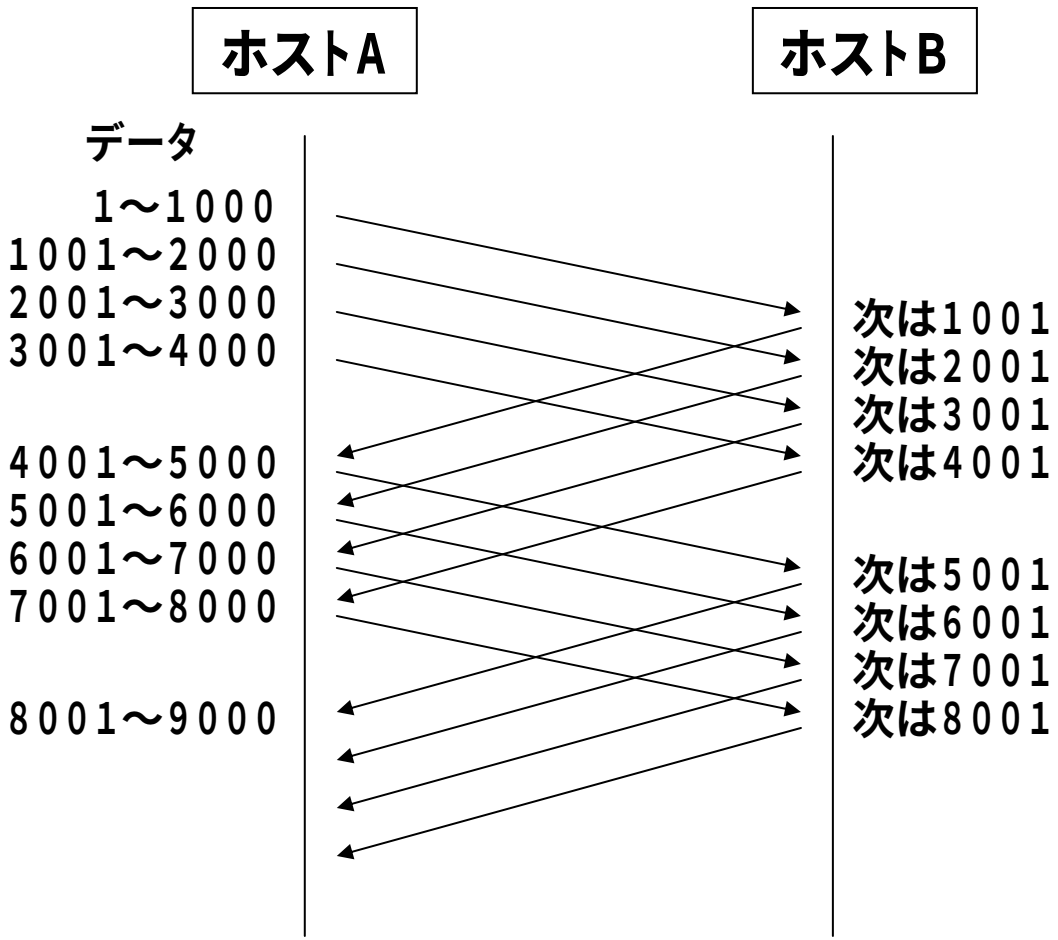
タイムアウト値は0.5秒の整数倍。初期値は6秒。

リトライアウトするとコネクションを強制的に切断する。

ウィンドウ制御による効率向上（Ｐ１９６）

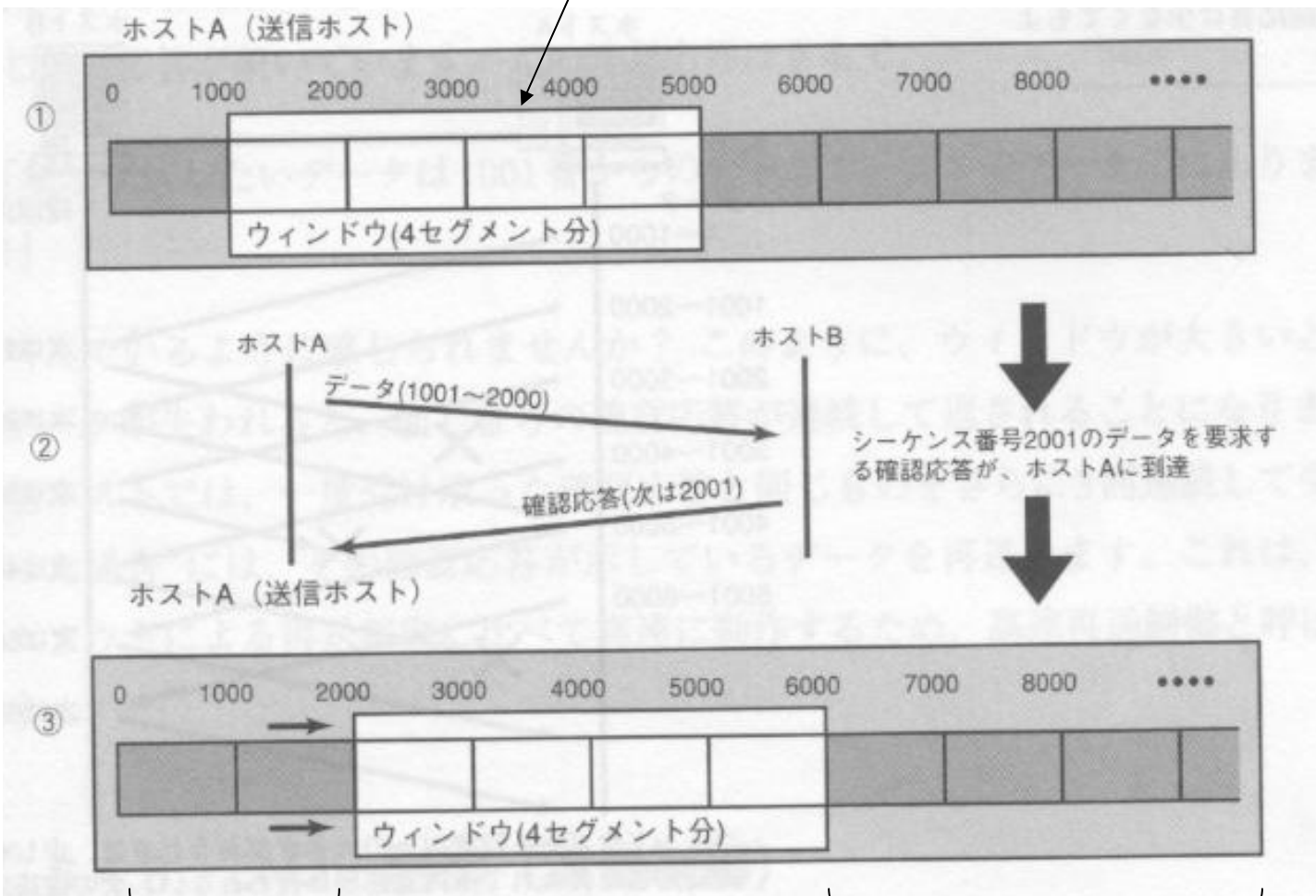
確認応答を待たずに送信できるデータの大きさをウィンドウサイズと呼ぶ。

ウィンドウサイズが４０００（バイト）のとき、確認応答の値に比べて４０００だけ大きなデータまで送信してよい。



スライディングウィンドウ方式（P197）

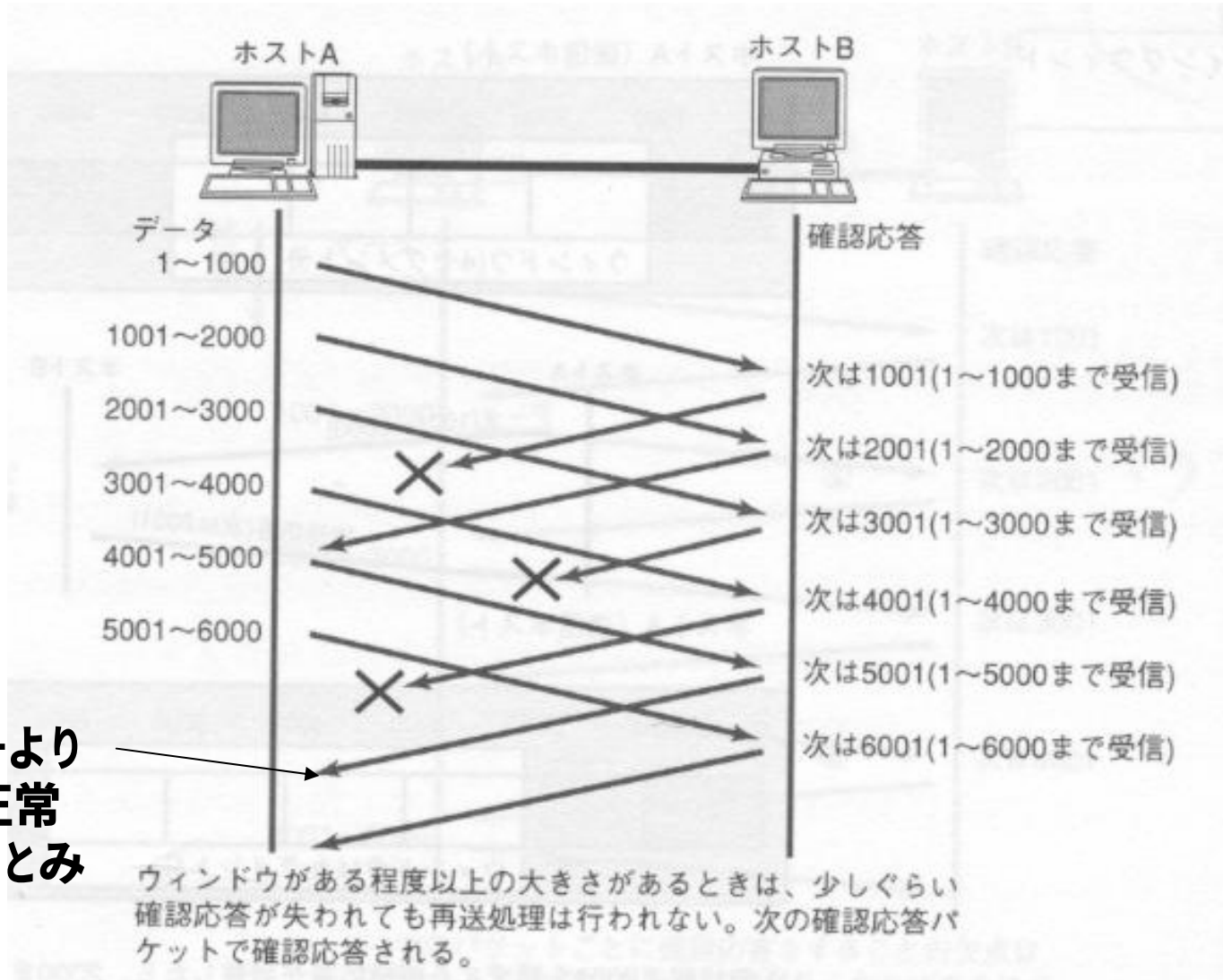
確認応答がなくても送信してよい範囲。
ただし、再送に備えてデータを残しておく必要がある。



送達確認部分（データ削除可）

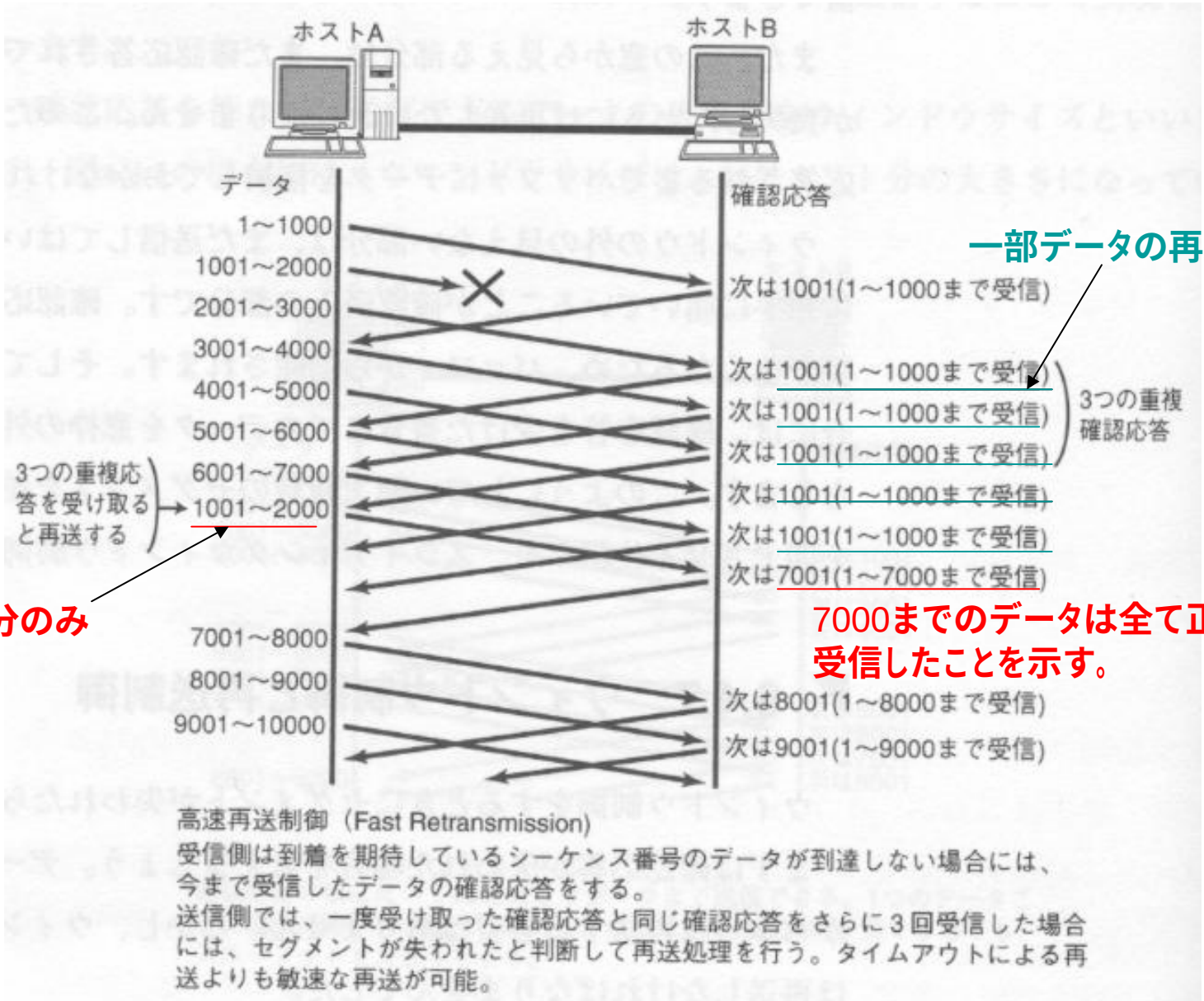
まだ送信してはいけない部分

確認応答は少なくてもよい(P198)



シーケンス番号より前のデータは正常に受信したものとみなす。

高速再送制御（P198）



高速再送制御（Fast Retransmission）
受信側は到着を期待しているシーケンス番号のデータが到達しない場合には、今まで受信したデータの確認応答をする。
送信側では、一度受け取った確認応答と同じ確認応答をさらに3回受信した場合には、セグメントが失われたと判断して再送処理を行う。タイムアウトによる再送よりも敏速な再送が可能。

実習の実施

日時：6月18日（水）および6月25日

場所：情報科学科実験室（2棟303）

1限の学生は1限と2限に別れて受講

　3年学籍番号J01～J35・・・・1限

　3年学籍番号J36以降および4年・・・・2限

3限の学生はそのまま3限に受講

内容：LANモニタ（Ethereal）によるパケットの観測

演習

① ＴＣＰとＵＤＰはどのように使い分けたらよいか。また、それぞれどのようなプロトコルに適用されているか。

② ＴＣＰの転送効率を向上させるために実現されているウィンドウ制御機能の例をあげ、その概要を説明せよ。