インターネットセキュリティ

パケット通信方式

インターネットなどコンピュータネットワークでは、
パケット通信方式が一般に用いられる

■一般的なパケットの構造

ヘッダに含まれる項目

- パケットの種類
- 送信先・送信元アドレス
- データ量
- エラーチェック用コード
- その他、転送時に必要な情報

パケット通信方式の特徴

- 通信回線を共有できる
- ネットワークの故障に強い
- 通信効率が高い

通信システムの階層構造

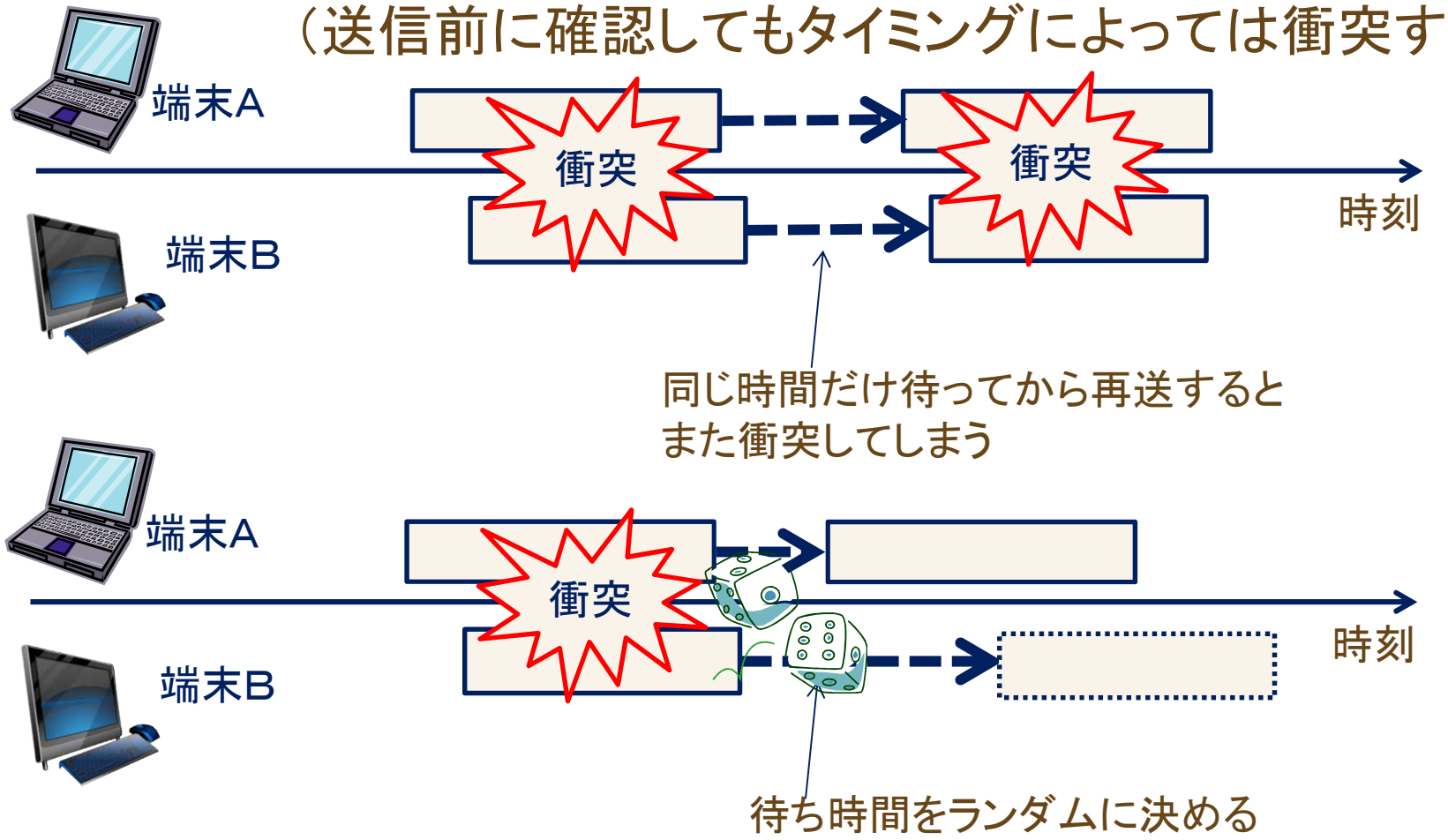
■7階層のOSI参照モデル

アプリケーション層	特定のアプリケーションに依存した処理
プレゼンテーション層	データ形式の変換・機器毎の違いの吸収
セッション層	コネクションの確立と切断、管理
トランスポート層	両端のノードでのデータ転送の管理
ネットワーク層	あて先までのデータ転送の経路管理
データリンク層	直接接続されたノード間のデータ転送
物理層	ビット列と物理信号との対応、変換

プロトコル（通信規約）：階層毎にプロトコルが決まっている
（ある階層のプロトコルでは他の階層のことは気にしなくてよい）

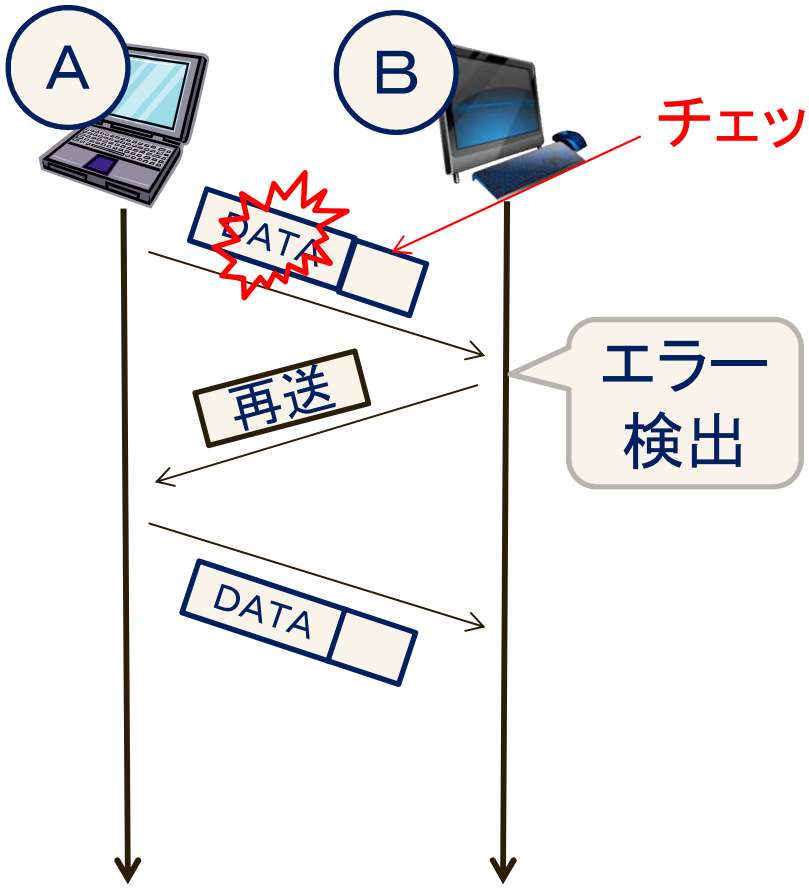
フレームの衝突と再送

複数の端末がほぼ同時にフレームを送信すると衝突してしまう
（送信前に確認してもタイミングによっては衝突する）



エラーチェックと再送

エラーチェック：衝突やノイズによるエラーを検出するしくみ



チェック
コード

偶数パリティ符号

1101011 | 1

全体で1の個数が
偶数個になるように
チェックコードを付ける

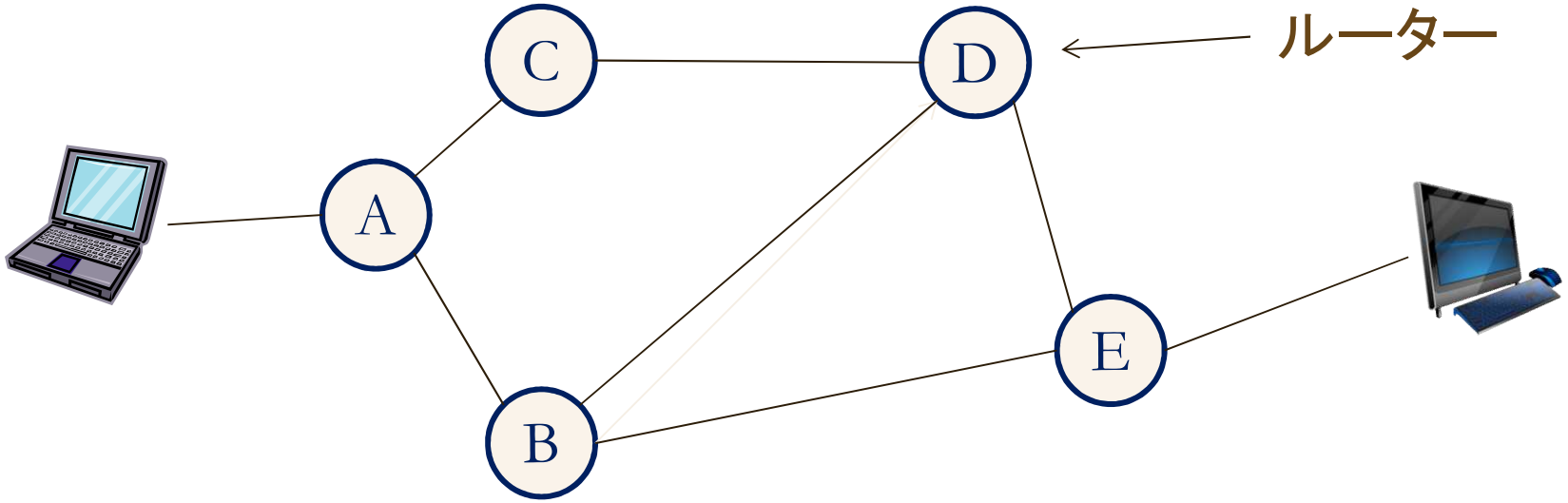
巡回符号

110101・・・・ | 10・・

$1+x+x^3+x^5+\cdots$

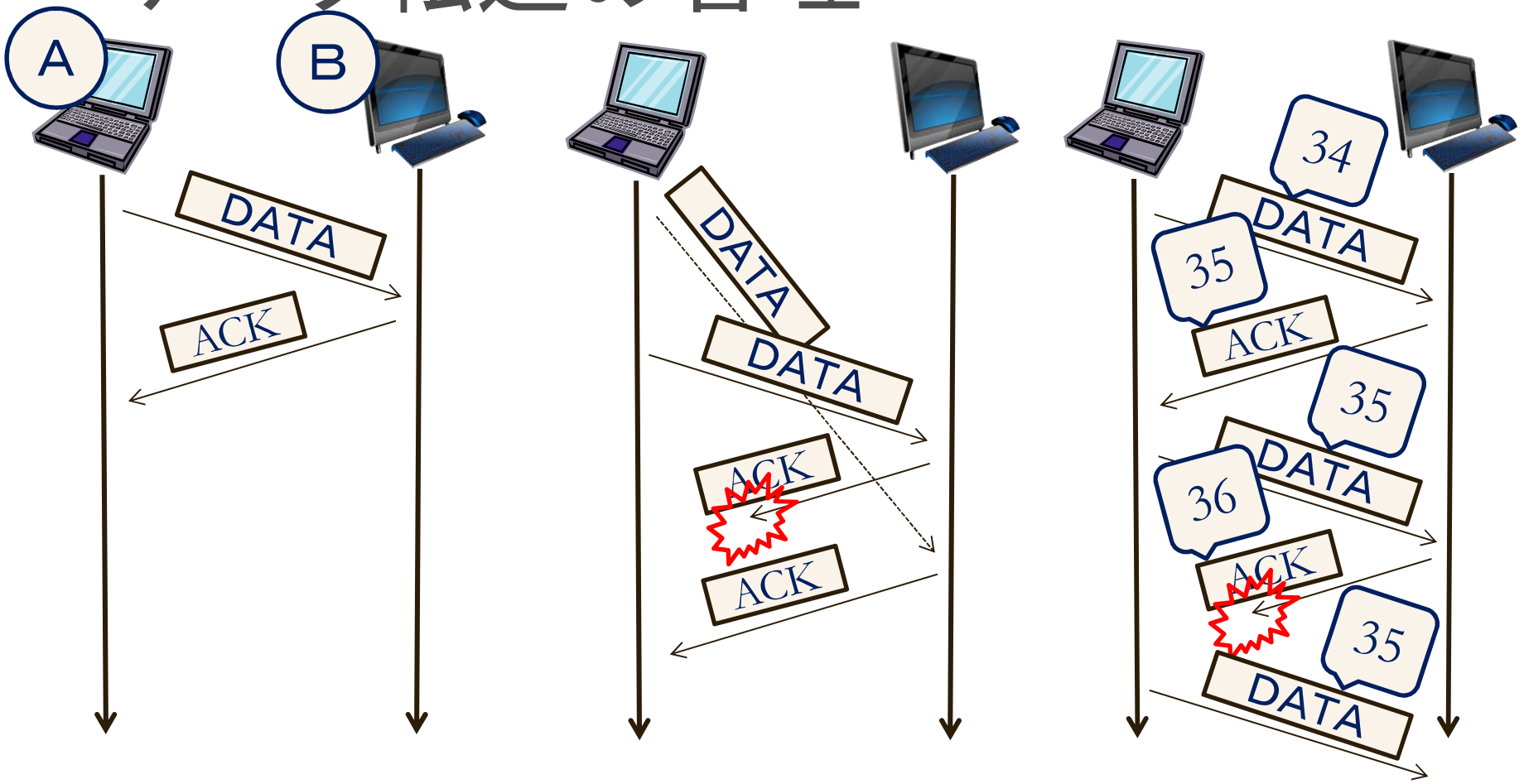
全体を多項式とみなしたとき、
この多項式がある多項式で
割り切れるようにチェックコード
を決める

ルーティング（経路探索）



- 全体を管理している人（組織）はいない
  （個々のルーターが送られてきたパケットの送り先を決める）
- 途中で状況が変化することもある（追加、故障、輻輳など）
- ミスや事故によりルーティングがおかしくなると：
  →パケットが届かない（途絶、ループなど）
  →遅延が生じる

データ転送の管理

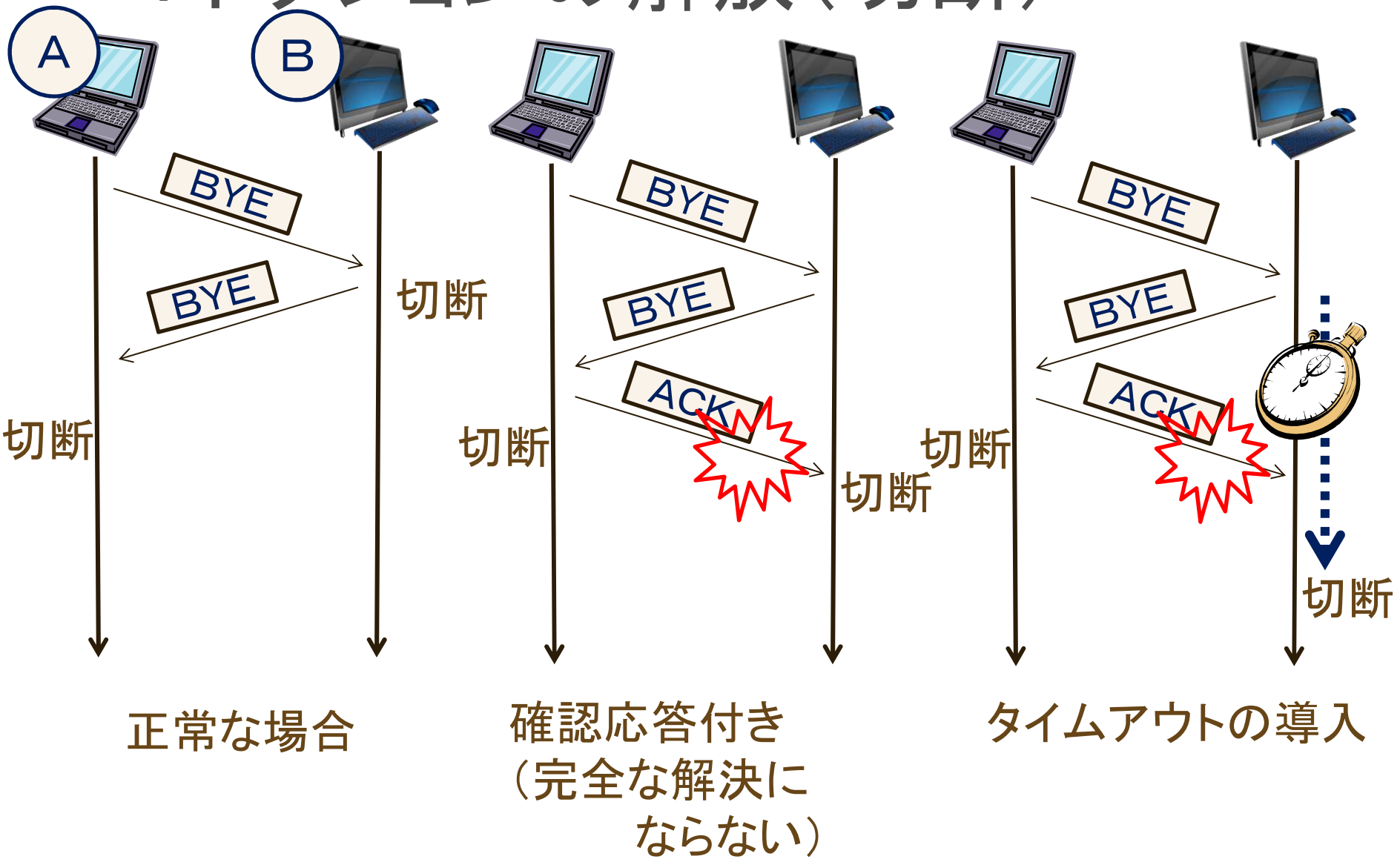


正常な場合

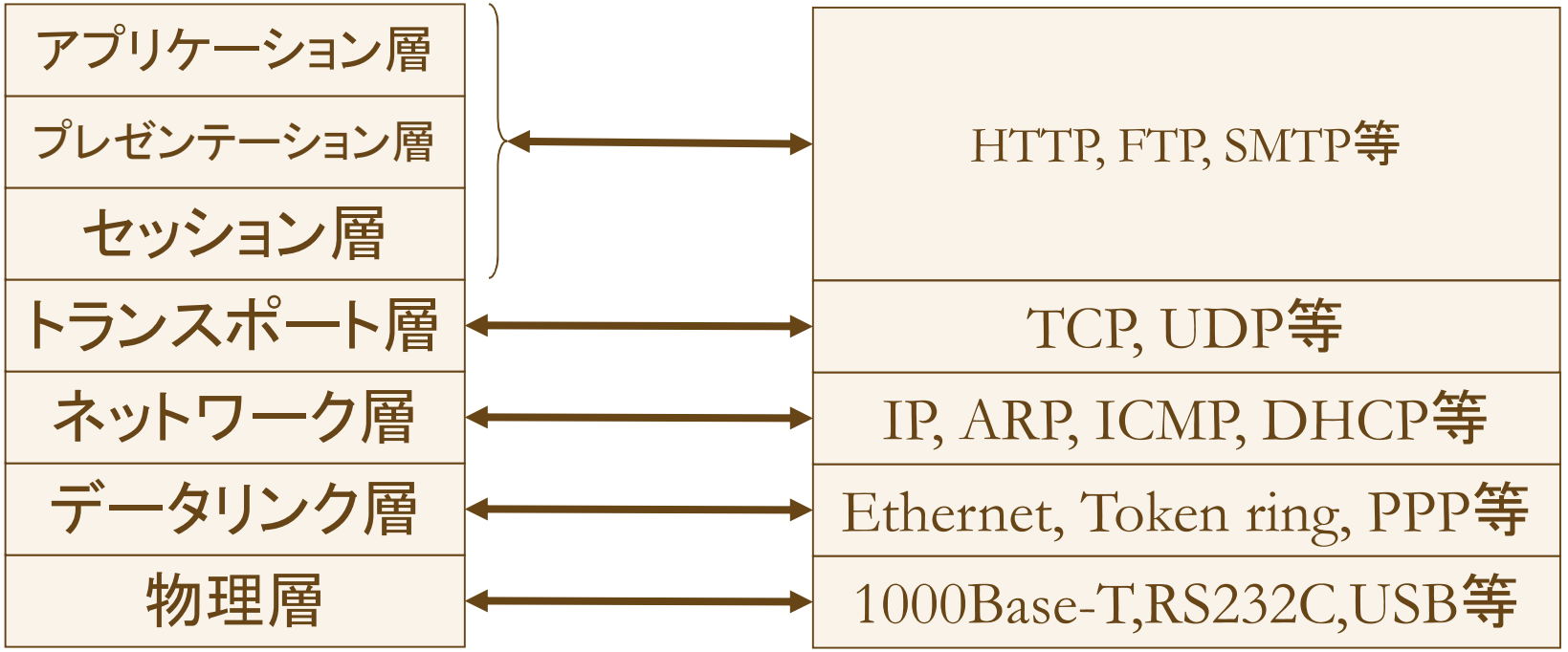
遅延や消失がある場合
（二重に受信してしまう）

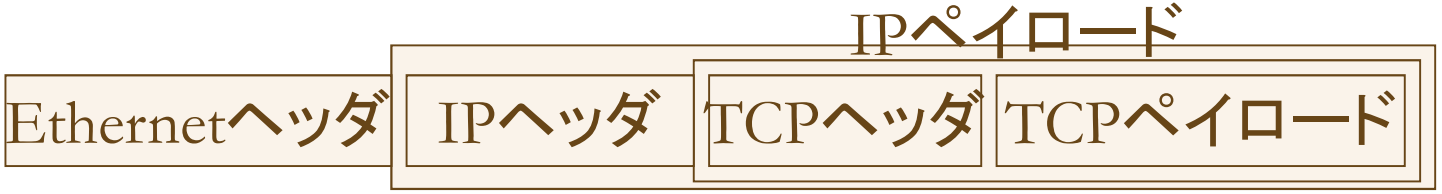
シーケンス番号
の導入

コネクションの解放（切断）



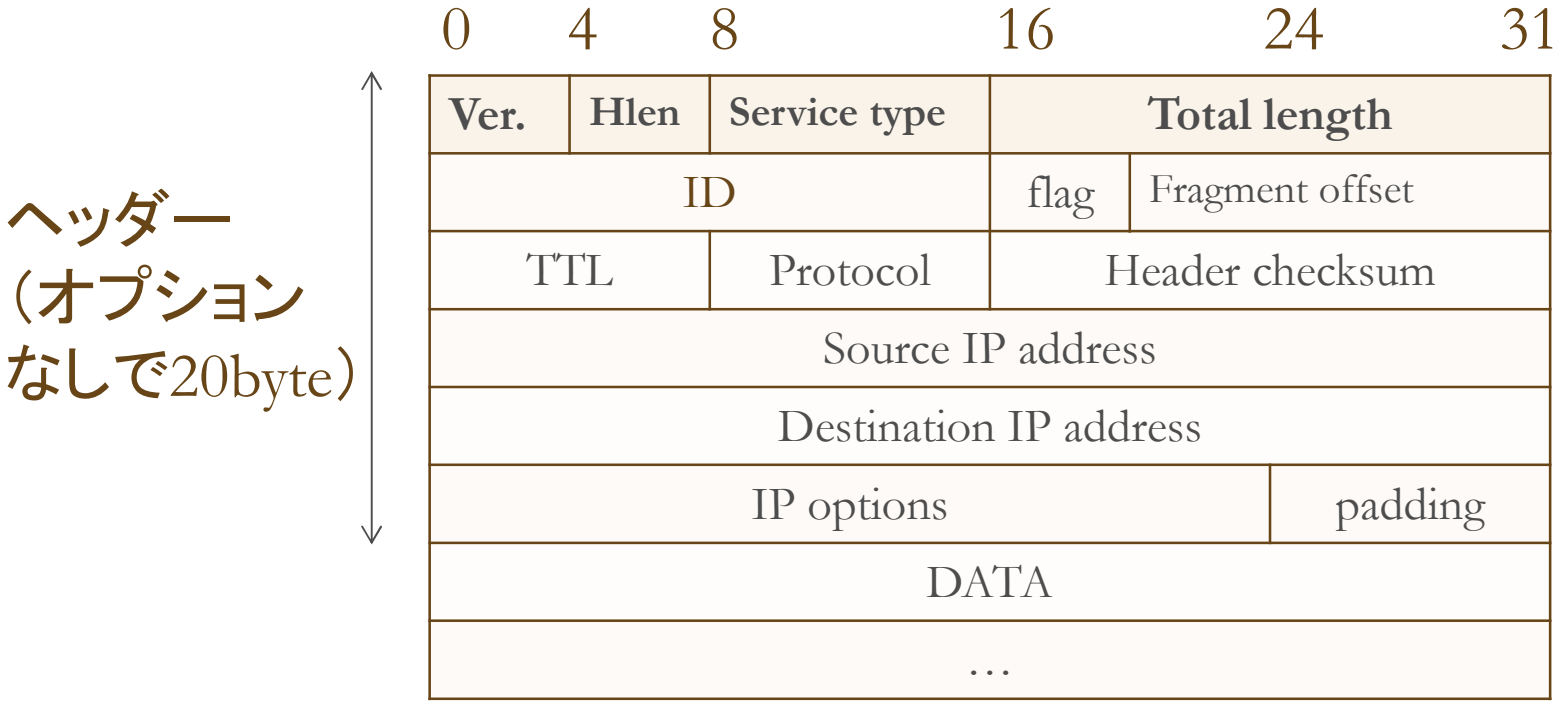
OSI参照モデルとTCP/IPの関係





IPプロトコル

- 現在はversion4。Vesion6(IPv6)への移行が進められている
- ネットワークに接続する全てのホスト(コンピュータ)に一意に32bitのIPアドレスを割り振る(IPv6では128bit)



IP（version4）アドレス

- 32bitの2進数
  （例：11000000101010000000000000000001）
- （人間には）見にくいので、8bitずつに区切り、それぞれを10進数に変換する

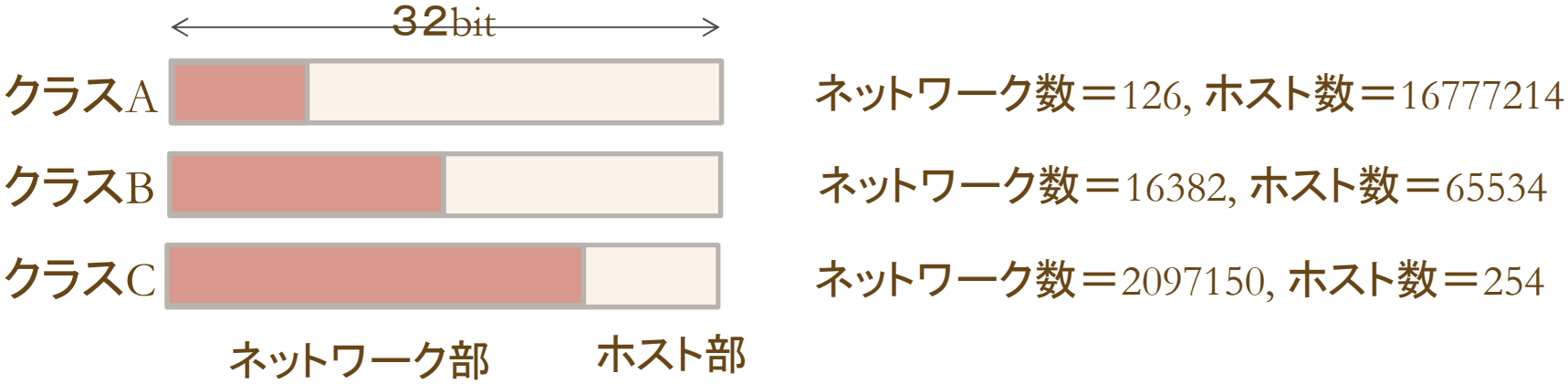
  11000000 10101000 00000000 00000001

  ↓

  192 . 168 . 0 . 1（ピリオドで区切る）

IPアドレスの構造

- ルーティングを容易にするためIPアドレスを前半（ネットワーク部）と後半（ホスト部）に分けて使用する
- ネットワーク部を何ビットにするかによってクラスA（8bit）、クラスB（16bit）、クラスC（24bit）がある
- サブネットマスクを利用することでネットワーク部のビット数をネットワーククラスに関わらず柔軟に指定できる
- 同じネットワークに属するホスト同士は直接通信できる



特別なIPアドレス

- ブロードキャストアドレス：同一のネットワークに接続している全てのホストが対象
  （255.255.255.255 ; 全てのビットが1のアドレス）
  異なるネットワークには転送されない
- ループバックアドレス：自分自身を表すアドレス(127.0.0.1)
- プライベートアドレス：外部と直接接続しない環境で用いるアドレス(10.*.*.*、172.16.*.*～172.31.*.*、192.168.*.*）。
  誰でも自由に使用できる。外部と接続できるアドレスはグローバルアドレスと呼ぶ。
  プライベートアドレスを使用しているホストが外部に接続する際は、アドレスをグローバルアドレスに変換したり(NAT)、他のサーバに中継してもらう（proxy）

トランスポート層のプロトコル

- TCP：通信をするホスト間であらかじめセッションを確立し、信頼性のある通信チャンネルを提供するプロトコル
- UDP：TCPと異なりセッションの確立をしない。信頼性は劣るがその分プロトコルが軽量で速度面や効率面で有利なこともある

<table>
<tr><td colspan="2">Source port</td><td colspan="2">Destination port</td></tr>
<tr><td colspan="4">Sequence number</td></tr>
<tr><td colspan="4">Acknowledgement number</td></tr>
<tr><td>Hlen</td><td>Res.</td><td>code</td><td>window</td></tr>
<tr><td colspan="2">Check sum</td><td colspan="2">Urgent pointer</td></tr>
<tr><td colspan="3">options</td><td>padding</td></tr>
<tr><td colspan="4">DATA</td></tr>
<tr><td colspan="4">…</td></tr>
</table>

TCPパケットの構造

<table>
<tr><td>Source port</td><td>Destination port</td></tr>
<tr><td>Message length</td><td>Check sum</td></tr>
<tr><td colspan="2">DATA</td></tr>
<tr><td colspan="2">…</td></tr>
</table>

UDPパケットの構造

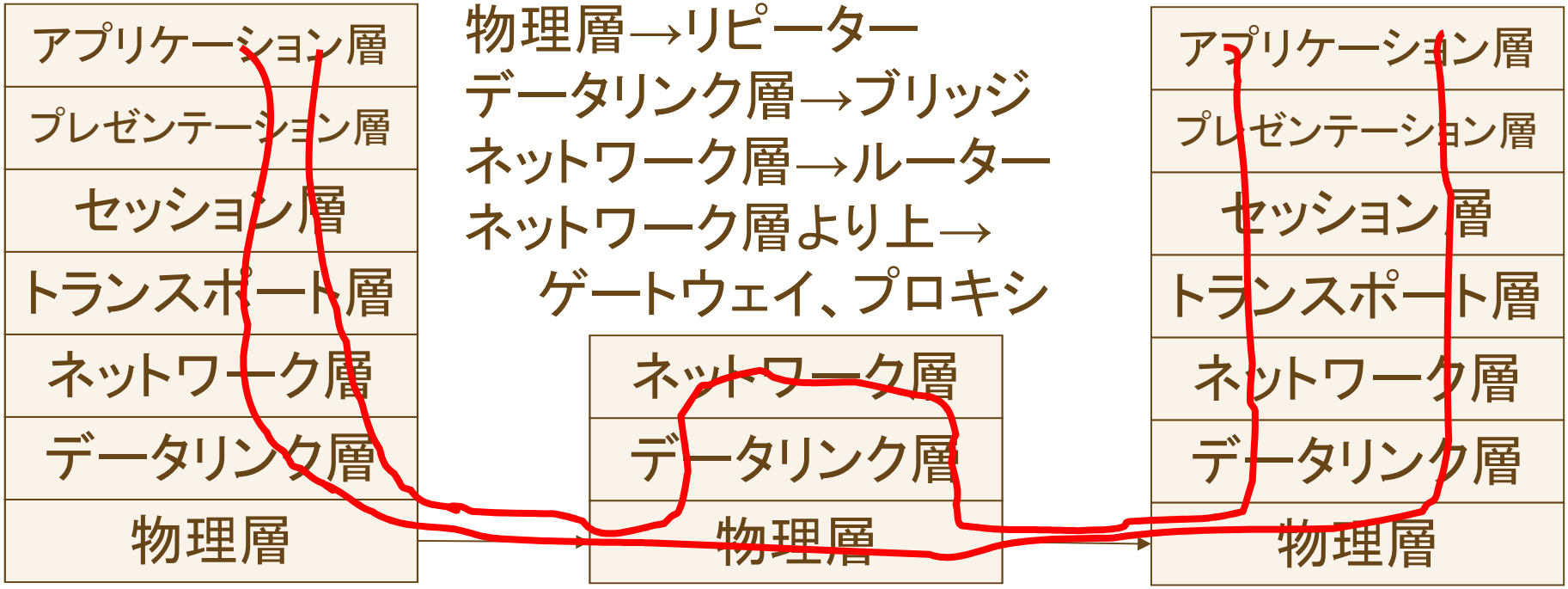
その他のプロトコル

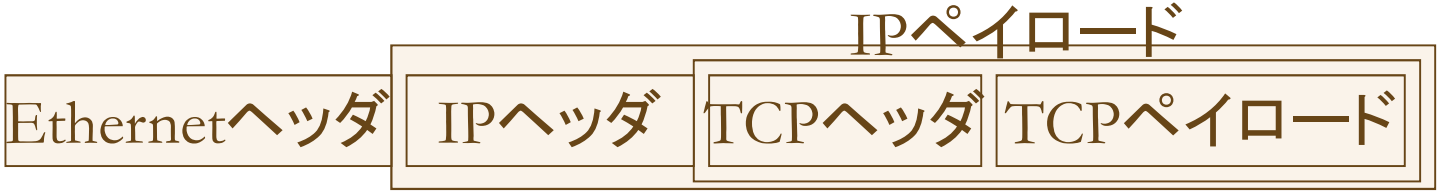
- ICMP: IPパケットを転送する際に生じた問題を報告したり、ネットワークの状態を制御あるいは診断するために用いる
- ARP：IPアドレスからその相手のMACアドレス（データリンク層のアドレス）を求めるために用いる
- DHCP：ネットワークに接続されたホストに対して動的にIPアドレス等の情報を割り当てるためのプロトコル
- DNS：ドメイン名（www.example.co.jp等）から、対応するIPアドレス等の関連情報を検索するためのプロトコル

ネットワークにおける中継

どの階層で中継をするのかによって、
特性が異なる

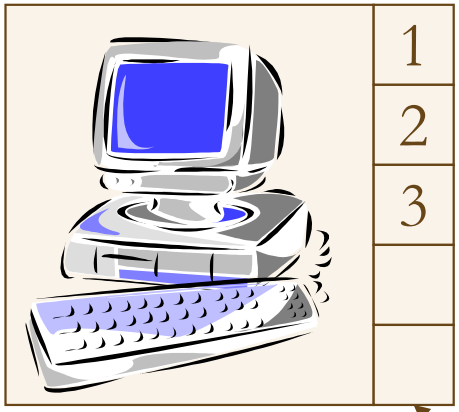
中継を行う階層が:
物理層→リピーター
データリンク層→ブリッジ
ネットワーク層→ルーター
ネットワーク層より上→
ゲートウェイ、プロキシ





ネットワークのセキュリティ

- インターネットプロトコル
  - IPプロトコル
  - TCPとUDP
  - ポート番号



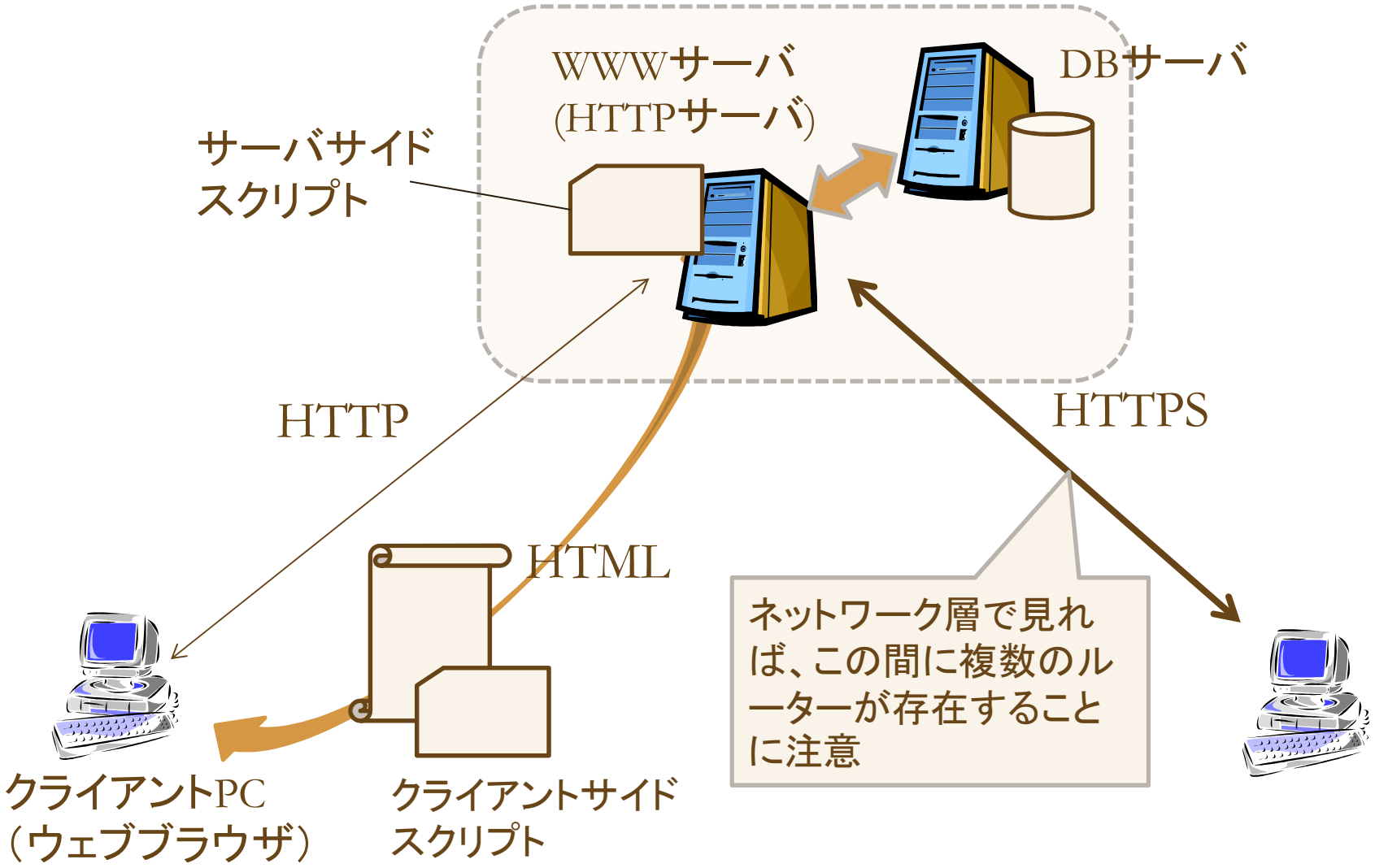
	アプリケーション層	S/MIME
	プレゼンテーション層	SSH
	セッション層	
TCP,UDP	トランスポート層	SSL/TLS
IP	ネットワーク層	IPSEC
Ethernet	データリンク層	
	物理層	

サービス毎にポート番号が決められている

主なサービスとセキュリティ（1）

- HTTP(80): WWWに用いられるプロトコル
  - 暗号化されていない
  - スクリプト（サーバサイド、クライアントサイド）の脆弱性に注意が必要
- HTTPS(443): 同上
  - TLSにより認証、暗号化される（最近、デフォルトでHTTPS接続が増えている）
- Telnet(23) : リモートホストを遠隔操作する
  - パスワードも暗号化されずに送信されるため危険。SSH等を用いる。
- FTP(20,21) : ファイル転送を行う
  - パスワードを含め暗号化されない。SFTP等を用いる

WWWのしくみ


WWWサーバ
(HTTPサーバ)
DBサーバ
サーバサイド
スクリプト
HTTP
HTTPS
HTML
ネットワーク層で見れば、この間に複数のルーターが存在することに注意
クライアントPC
（ウェブブラウザ）
クライアントサイド
スクリプト

HTTPセッションの例

GET http://www.example.ac.jp/~hoge/index.html HTTP/1.1
Host:www.example.ac.jp

HTTP/1.1 200 OK
Date: Mon, 04 Jul 2005 05:10:05 GMT
Server: Apache
Last-Modified: Tue, 28 Jun 2005 02:00:23 GMT
ETag: "b70607-1223-42c0af37“
Accept-Ranges: bytes
Content-Length: 4643
Connection: close
Content-Type: text/html

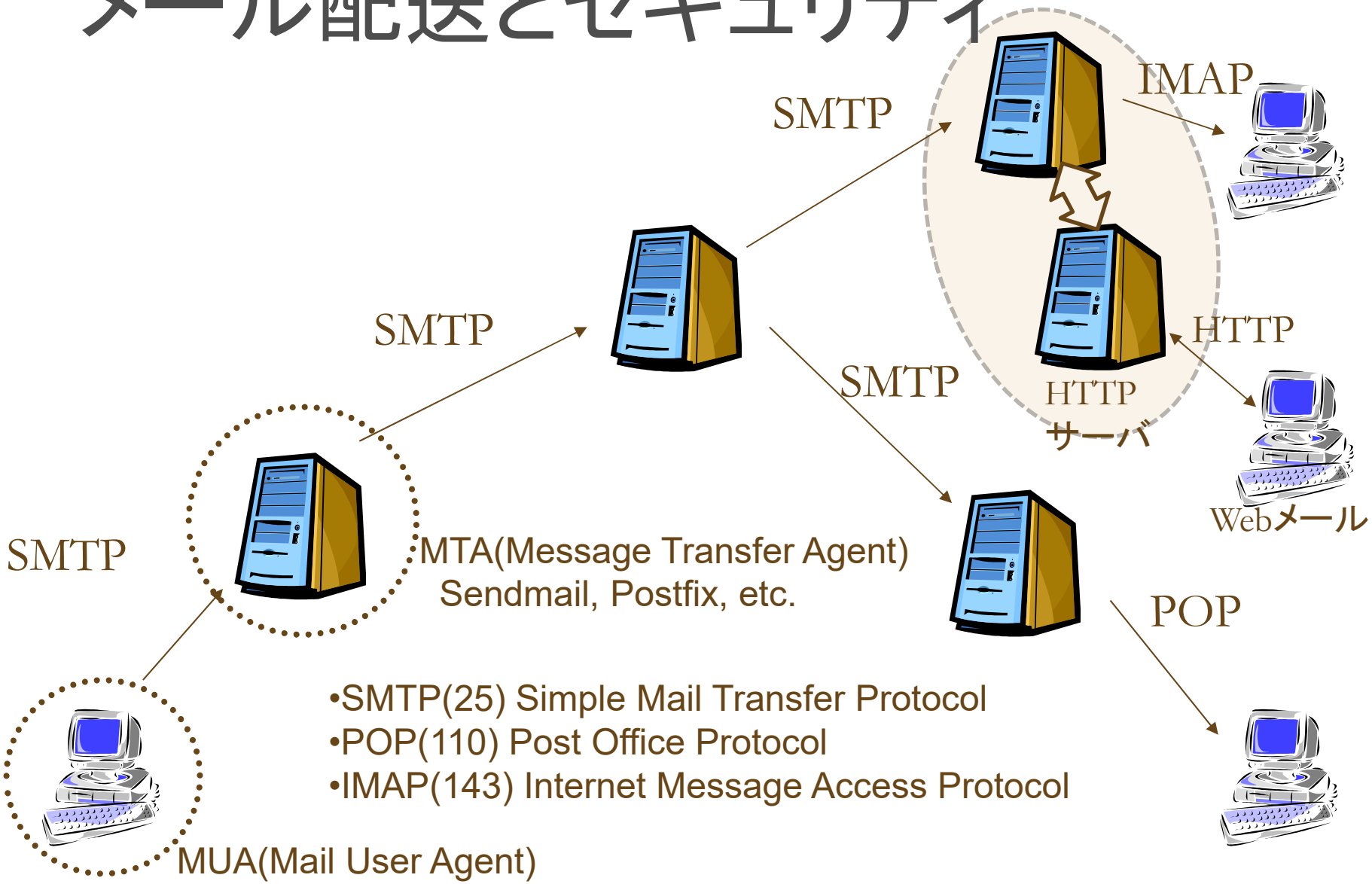
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="ja">
<head> <title>Example Page</title>
<meta name="Author" content="Hiroyuki INABA">
<meta http-equiv="Content-type" content="text/html;charset=ISO-2022-JP">
</head>
<body bgcolor="white" text="black">
<h1>Example Page</h1>
途中省略
</body>
</html>

HTTPセッションは、ページ毎に完結する（以前の閲覧ページには関係しない）

主なサービスとセキュリティ（2）

- SMTP(25):メールの配送に用いられる
  - 暗号化されない（smtps(465 or 587)を利用する）
  - ユーザ認証なし（→不正中継、SMTP-AUTHの利用）
- POP(110):受信メールサーバからメールを取り出す
  - （パスワードを含め）暗号化されない（POP over TLS(995)を利用する）
- IMAP(143) : 受信メールサーバ上のメールにアクセス
  - 暗号化されない(IMAP over TLS(993)を利用する

メール配送とセキュリティ

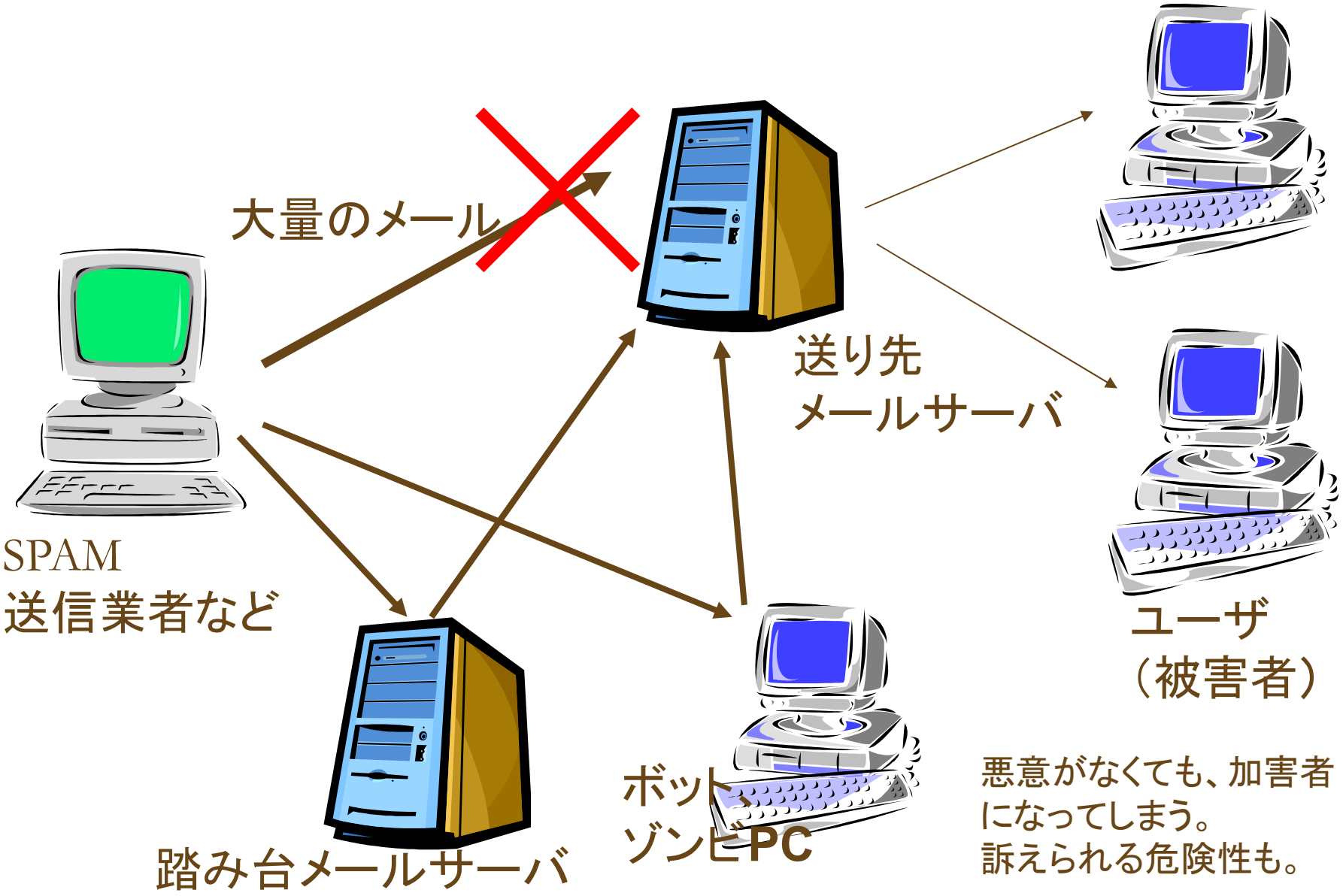


SMTPセッションの例

- 220 hoge.kit.ac.jp ESMTP Sendmail 8.12.10/8.12.10; Thu, 30 Jun 2009 18:30:42 +0900
- HELO foo.example.ac.jp
- 250 hoge.kit.ac.jp Hello [133.16.***.***], pleased to meet you
- MAIL FROM:nobody@foo.example.ac.jp　←本物かどうかの確認はない
- 250 2.1.0 nobody@foo.example.ac.jp... Sender ok
- RCPT TO:inaba@hoge.kit.ac.jp
- 250 2.1.5 inaba@hoge.kit.ac.jp... Recipient ok
- DATA
- 354 Enter mail, end with "." on a line by itself
- To: inaba@hoge.kit.ac.jp
  Date: Thu, 30 Jun 2009 18:30:42 +0900

  This is a test mail.
  .
- 250 2.0.0 j5U9UgOO026220 Message accepted for delivery
- QUIT
- 221 2.0.0 hoge.kit.ac.jp closing connection

メールの不正中継


大量のメール
送り先
メールサーバ
SPAM
送信業者など
ユーザ
（被害者）
踏み台メールサーバ
ボット
ゾンビPC
悪意がなくても、加害者
になってしまう。
訴えられる危険性も。

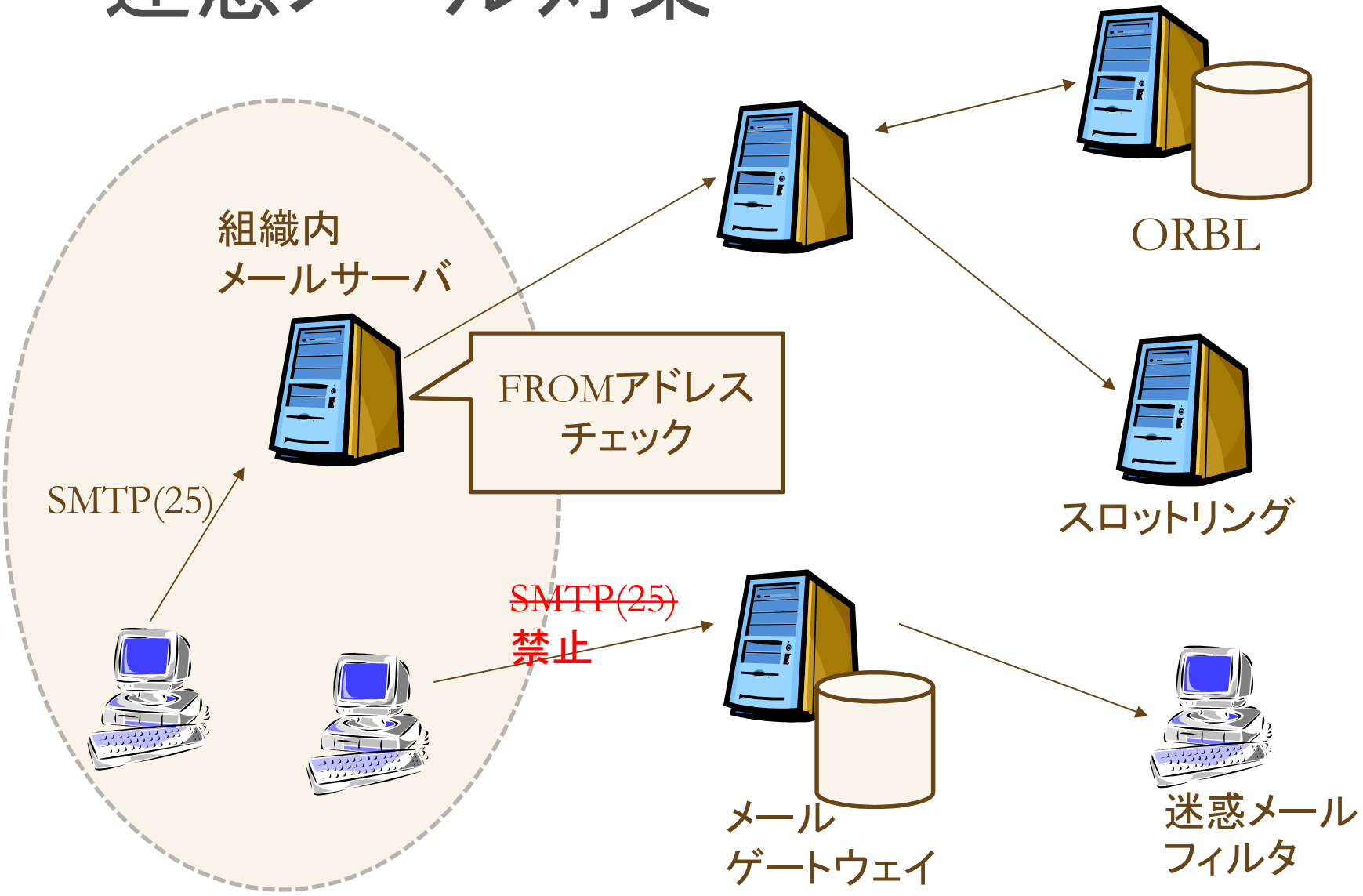
POPセッションの例

- +OK Qpopper (version 4.0.5) at hoge.kit.ac.jp starting. <18282.1120293721@hoge.kit.ac.jp>
- USER inaba
- +OK Password required for inaba.
- PASS hogepass ←パスワードが平文で流れる
- +OK inaba has 3 visible messages (0 hidden) in 5152 octets.
- STAT
- +OK 3 5152
- LIST
- +OK 3 visible messages (5152 octets)
  1 1602
  2 1926
  3 1624
  .
- RETR 1
- +OK 1614 octets
  (1番目のメールの内容が送られる)
  .
- DELE 1
- +OK Message 1 has been deleted.
- QUIT
- +OK Pop server at hoge.kit.ac.jp signing off.

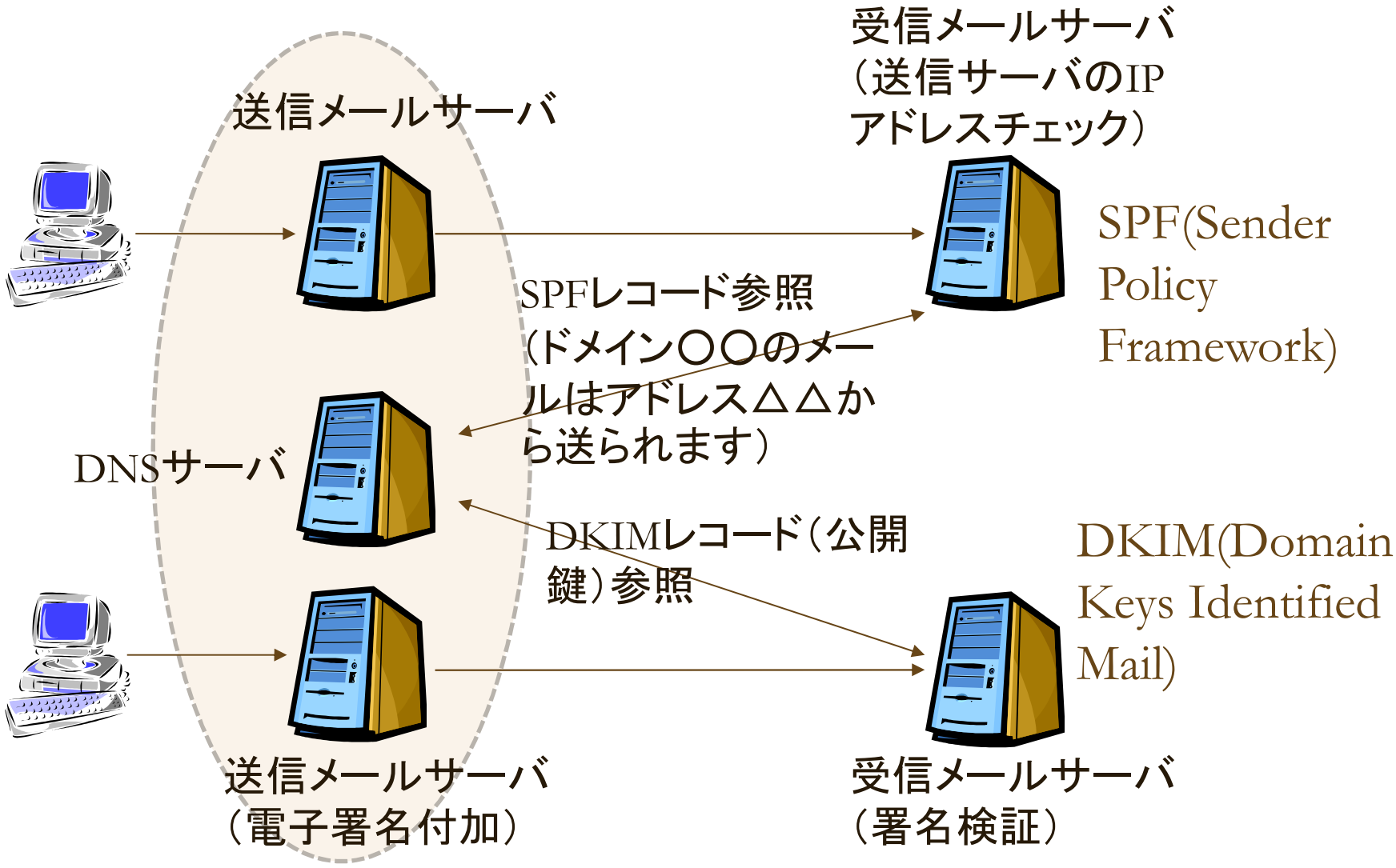
迷惑メール(SPAM)対策

- メールサーバにおける技術的対策
  - OP25B(Outbound Port 25 Blocking)
    外部とのport25向け通信を禁止する
  - 送信ドメイン認証
    正しい送信サーバから送信していることを確認。
    SPFとDKIMがある。
  - ORBL(Open Relay Black List)
    踏み台に利用されているサーバのブラックリスト
  - スロットリング
    SMTPの返答をわざと遅らせる
  - フィルタリング
    迷惑メールをフィルタ。GW型とクライアント型がある。
    誤検知(False Positive, False Negative)は避けられない

迷惑メール対策


組織内
メールサーバ
FROMアドレス
チェック
SMTP(25)
ORBL
スロットリング
~~SMTP(25)~~
禁止
メール
ゲートウェイ
迷惑メール
フィルタ

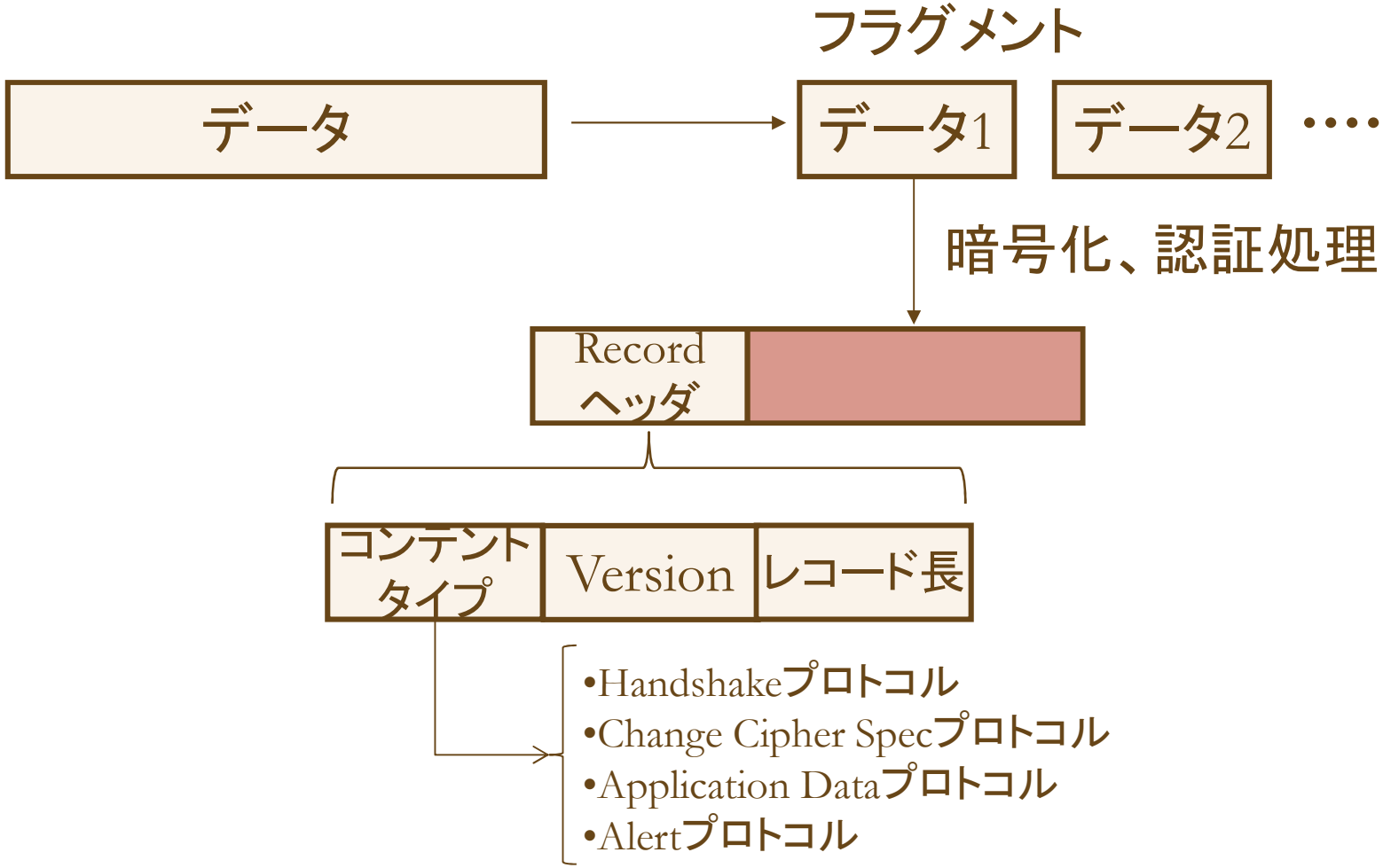
送信ドメイン認証


送信メールサーバ
受信メールサーバ
（送信サーバのIP
アドレスチェック）
SPF(Sender
Policy
Framework)
SPFレコード参照
（ドメイン○○のメー
ルはアドレス△△か
ら送られます）
DNSサーバ
DKIMレコード（公開
鍵）参照
DKIM(Domain
Keys Identified
Mail)
送信メールサーバ
（電子署名付加）
受信メールサーバ
（署名検証）

SSL/TLS(Secure Socket Layer/ Transport Layer Security)

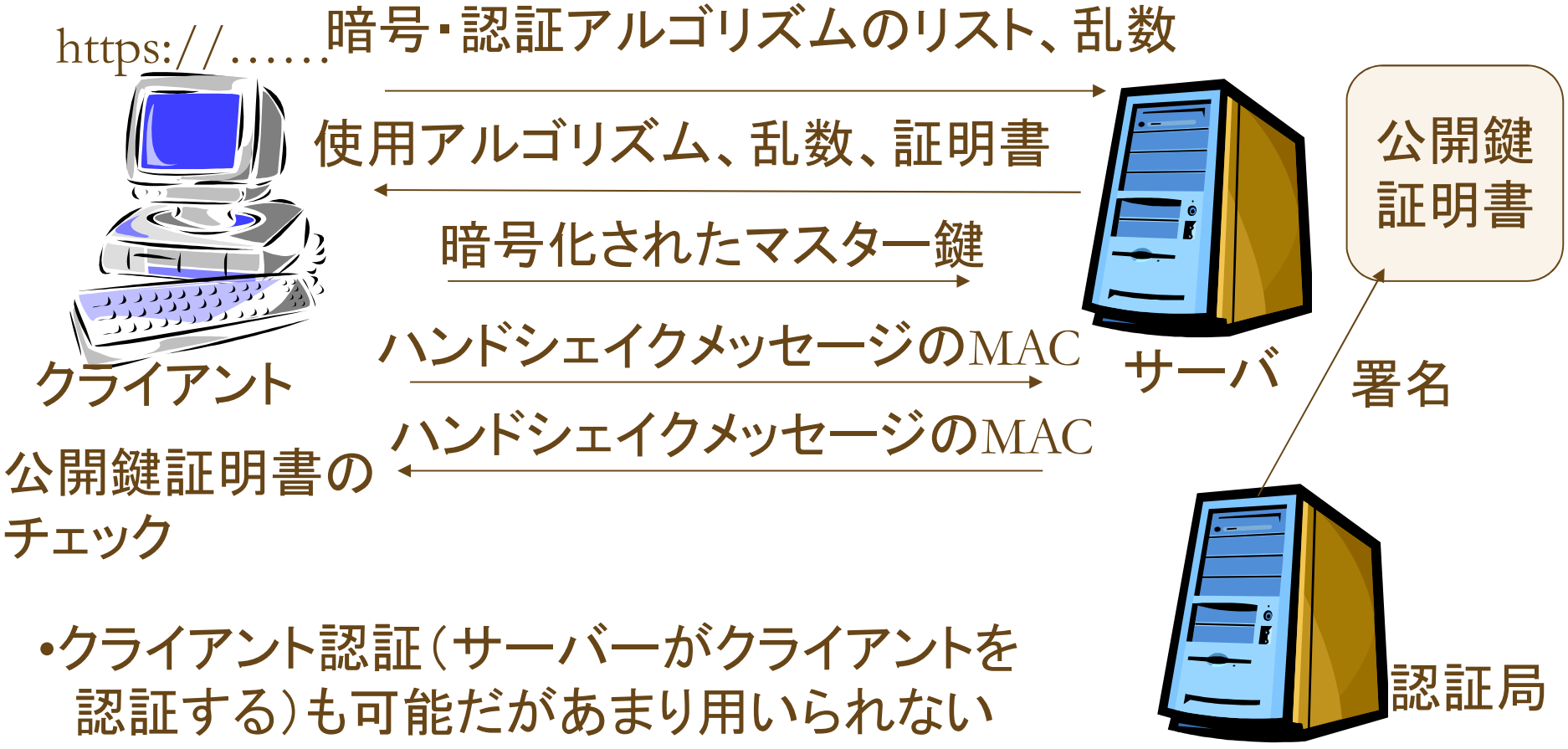
- SSL/TLS : トランスポート層のセキュリティ機能を提供する規格。当初は、Web(HTTP)の暗号化に用いるため開発された。
- 歴史
  - SSL2(1994): Netscape社がリリース。重大な欠陥あり
  - SSL3.0(1995): Netscape社がSSL2の設計からやり直してリリース。2014年に重大な欠陥(Poodle攻撃)が見つかった。
  - TLS1.0(1999): SSL3を元に作られた(RFC2246)。SSL3との互換性はない
  - TLS1.1(2006): セキュリティに関する細かい修正
  - TLS1.2(2008):暗号スイートの整理、認証付き暗号の導入
  - TLS1.3(2018) : 暗号アルゴリズムの整理、高速化、前方秘匿性の確保

TLS　Recordプロトコル



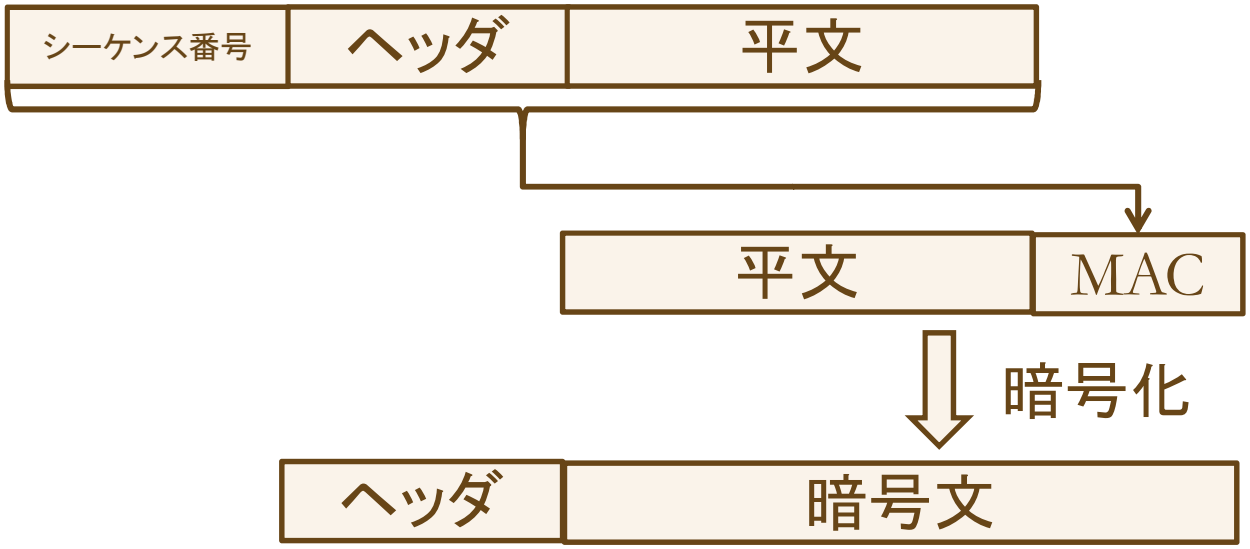
TLS　ハンドシェイクプロトコル

•サーバー認証（クライアントがサーバーを認証する場合）

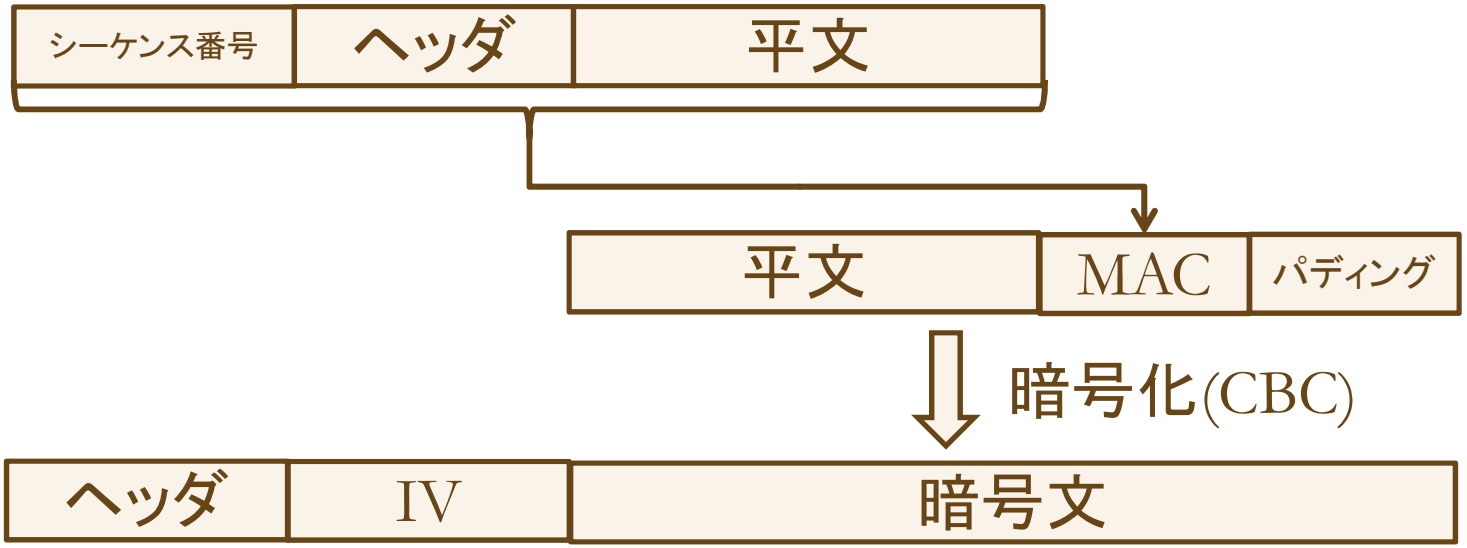


•クライアント認証（サーバーがクライアントを認証する）も可能だがあまり用いられない

TLS 暗号化処理（ストリーム暗号）

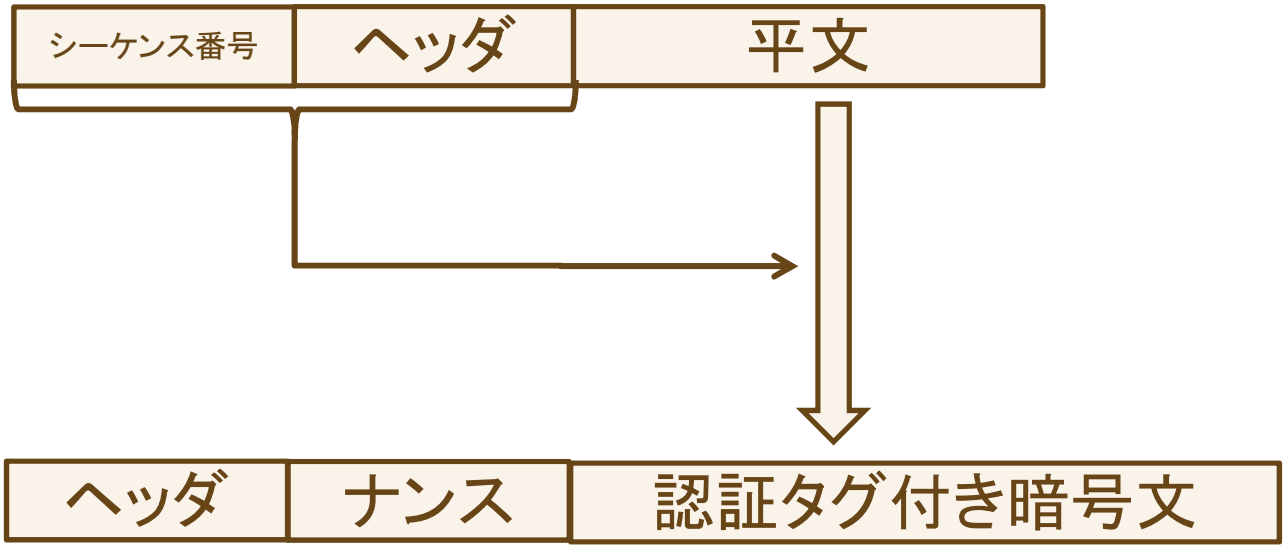


TLS 暗号化処理(ブロック暗号)



- TLS1.0ではひとつ前のブロックの暗号文をIVとして利用するためIVは送られなかったが、BEAST攻撃に脆弱であるため利用は推奨されない

TLS 暗号化処理（AEAD（認証付き暗号））



- AEAD方式として、GCM(Galois Counter Mode)、CCM(Counter with CBC-MAC)が用いられる

TLS 暗号スイート

TLSで利用できる、認証方式、暗号方式、暗号化モードなどのパラメータをまとめたもの

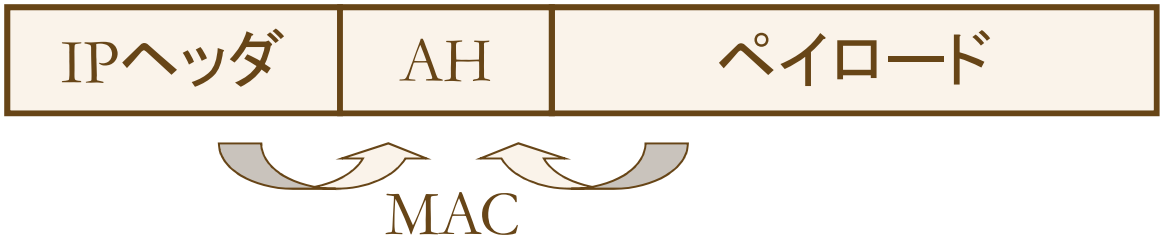
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_WITH_AES_128_CCM 等

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
鍵交換 認証 暗号化 鍵長 暗号モード MAC/PRF
(楕円曲線DH)

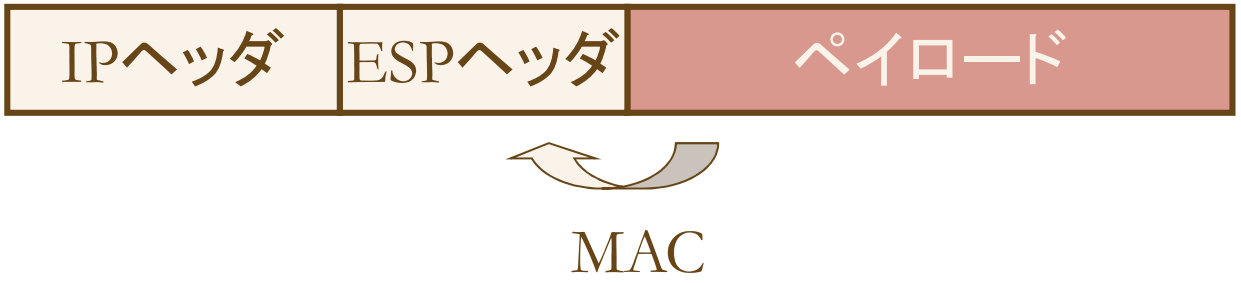
IPSEC

■IPSECのパケット構造（AHとESPの2種類がある）

AH(認証ヘッダ)：IPパケットの改ざんを防止する
（メッセージ認証、再送攻撃対策）

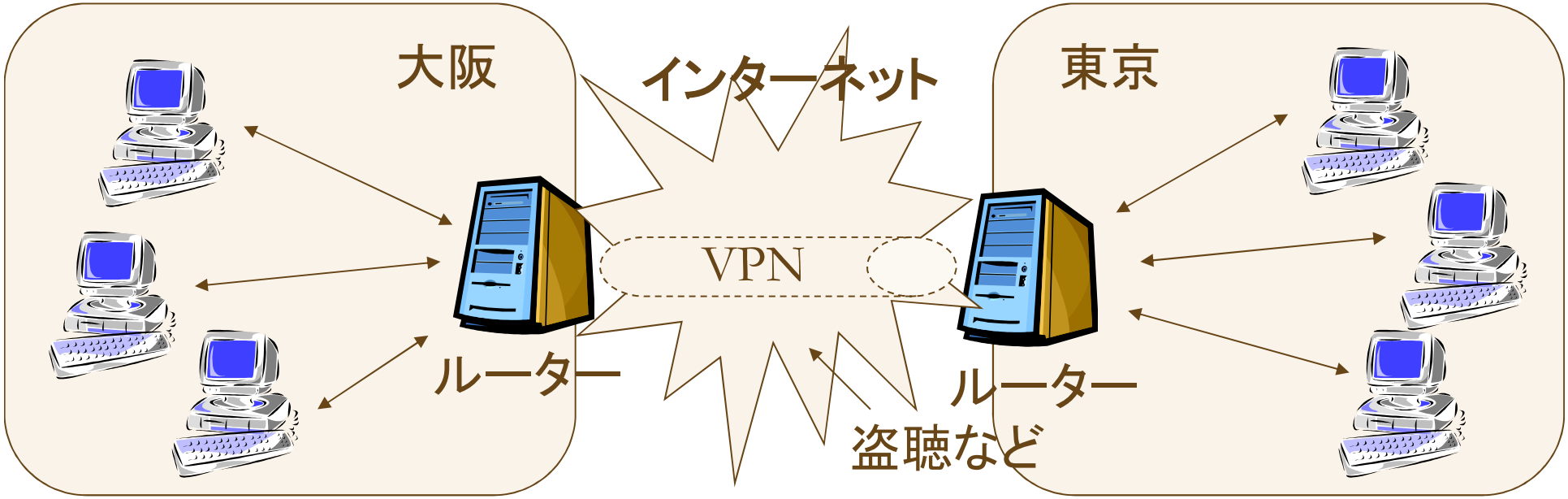


ESP：IPペイロードの暗号化と認証
（IPヘッダは保護されない）



IPSEC（2）

■トンネルモード（VPNを実現する際に用いられる）



SSL-VPNについて

アプリケーション層
プレゼンテーション層
セッション層
トランスポート層
ネットワーク層
データリンク層
物理層

SSL

IPsec

- SSL-VPNの特徴
  - OSやルーターの設定変更が不要
  - NAT環境、Proxy経由のWeb通信のみの環境でも使える
  - VPNソフト（クライアント）のインストールが不要な場合も

- SSL-VPNの注意点
  - 認証方式に注意
  - クライアントPCのセキュリティ
  - 公衆PCからの接続