ネットワーク2

http://cobayasi.com/koza/security/3_network2.pdf

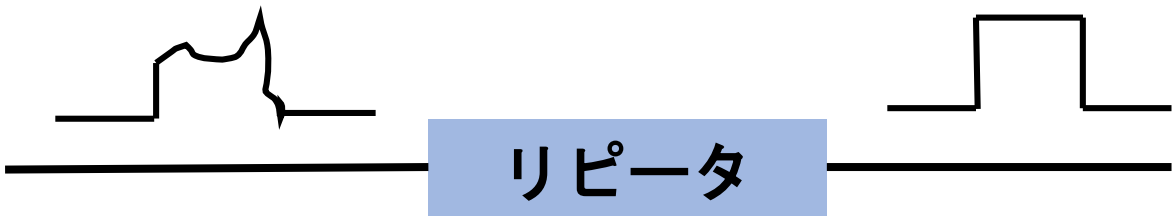
1. 通信装置①物理層
2. 通信装置②データリンク層
3. 通信装置③　ネットワーク層
4. NAT
5. アプリケーション層のプロトコル
6. 無線LAN

通信装置①物理層

テキストP265-266

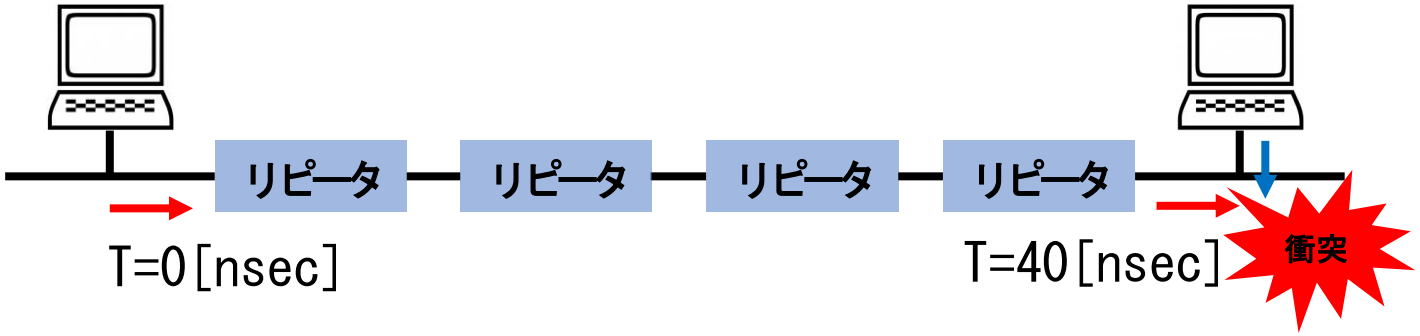
リピータ

物理層で動作するネットワーク機器で、ケーブル上の電流の増幅や整流（電気波形を整える）を行い、信号の再生や中継する



段数制限

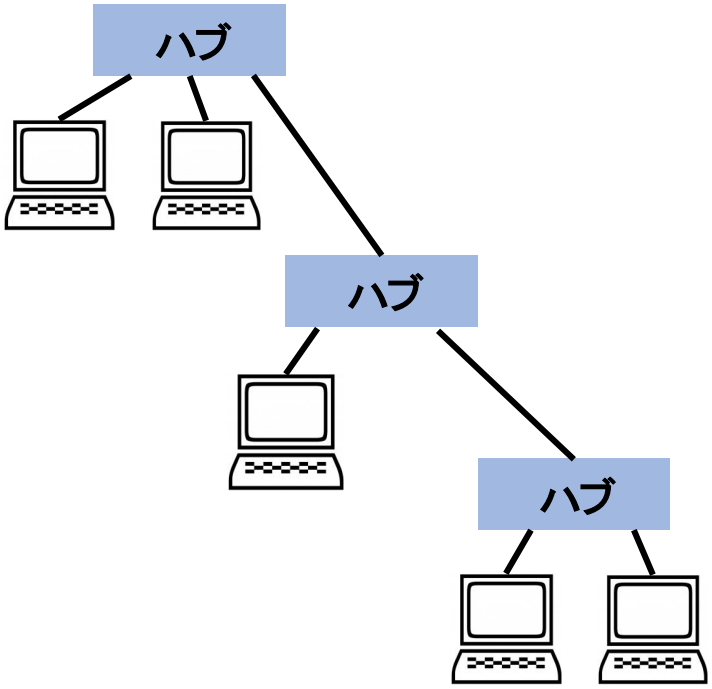
複数台のリピータを使う際には、伝送遅延が生じてコリジョン(パケット衝突)が起こらないように、使用台数を制限する



10BASE-T,10BASE-5,10BASE-2では最大4台まで、
100BASE-TXでは最大2台まで、接続できる

（リピータ・）ハブ

複数台のコンピュータを接続する（マルチポート）ことができるリピータで、ハブ同士を直列接続（カスケード接続）することで、より多くのコンピュータを接続することができる。



コラム

LANの規格

規格名	伝送速度	媒体	最大長
10BASE-5	10Mbps	同軸ケーブル	500m
10BASE-2	10Mbps	同軸ケーブル	185m
10BASE-T	10Mbps	ツイストペアケーブル	100m
100BASE-TX	100Mbps	ツイストペアケーブル	100m
1000BASE-T	1000Mbps	ツイストペアケーブル	100m

100 BASE - TX

伝送速度[Mbps]　ベースバンド転送　媒体の種類（T:ツイストペア，F:光ファイバなど）またはケーブル最大長
Xはツイストペアケーブルの伝送方式（ANSI X3T9.5分科会規定のFDDI/CDDIがベース）

通信装置②データリンク層

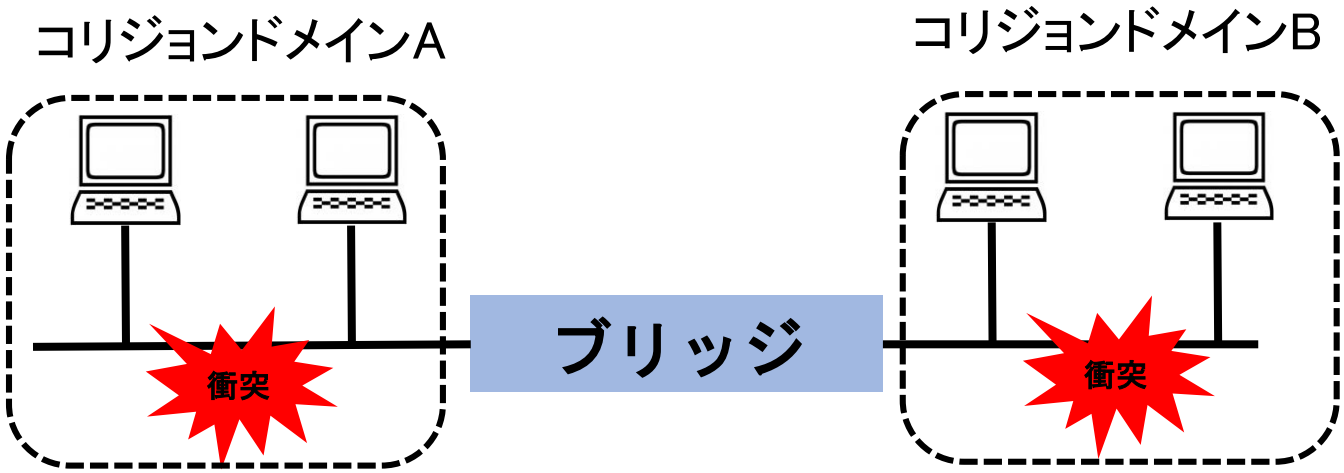
テキストP267-270

ブリッジ

データリンク層（OSI参照モデル第2層）で動作するネットワーク機器で、複数のホストを接続してLANを構成することができる。ブリッジで分割された領域を、コリジョンドメイン（またはセグメント）と呼ぶ。

コリジョン

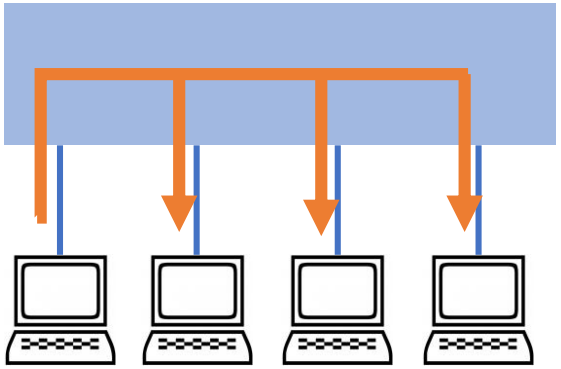
コリジョンとは、「パケットが衝突する」こと。ブリッジで、コリジョンドメインを分割することができるので、パケットの衝突範囲を分割でき、リピータの使用制約を緩和することができる。



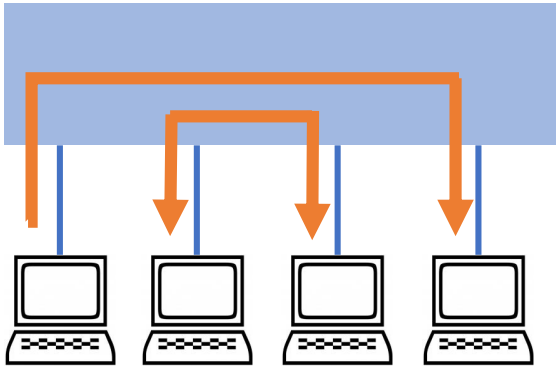
スイッチング・ハブ

　データリンク層（OSI参照モデル第2層）で動作するネットワーク機器で、多くのコンピュータを接続してLANを構成することができる。
　リピータ・ハブとは異なり、MACアドレスを学習及び認識して通信制御する。無駄な個所にパケットを流さない。

リピータ・ハブ



スイッチング・ハブ



通信装置③ネットワーク層

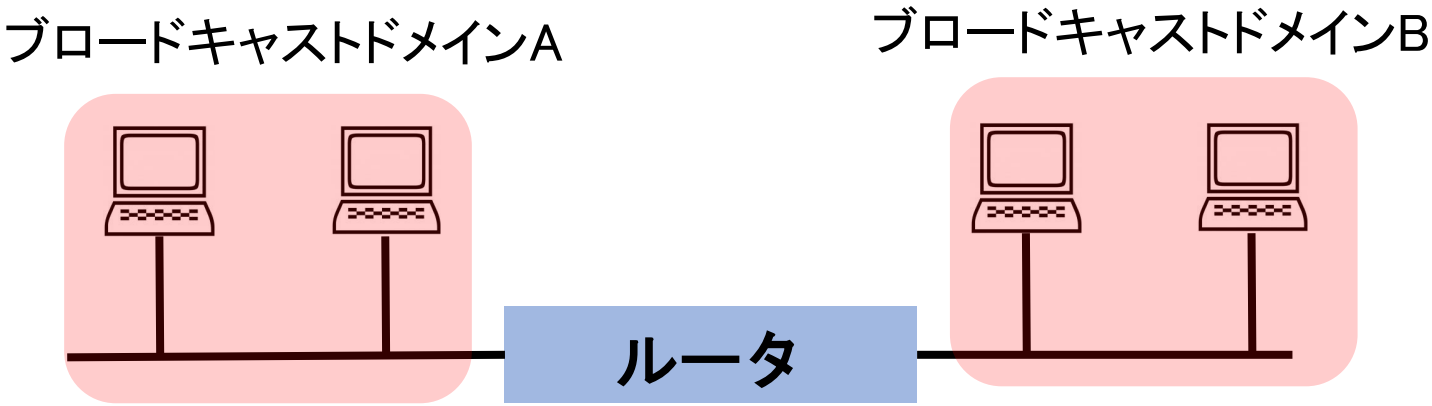
テキストP271-276

ルータ

OSI参照モデルの第3層（ネットワーク層）で働くネットワーク機器で、IPアドレスを認識してパケットを中継する。ネットワークとネットワークを接続できる唯一のネットワーク機器。

ブロードキャストドメイン

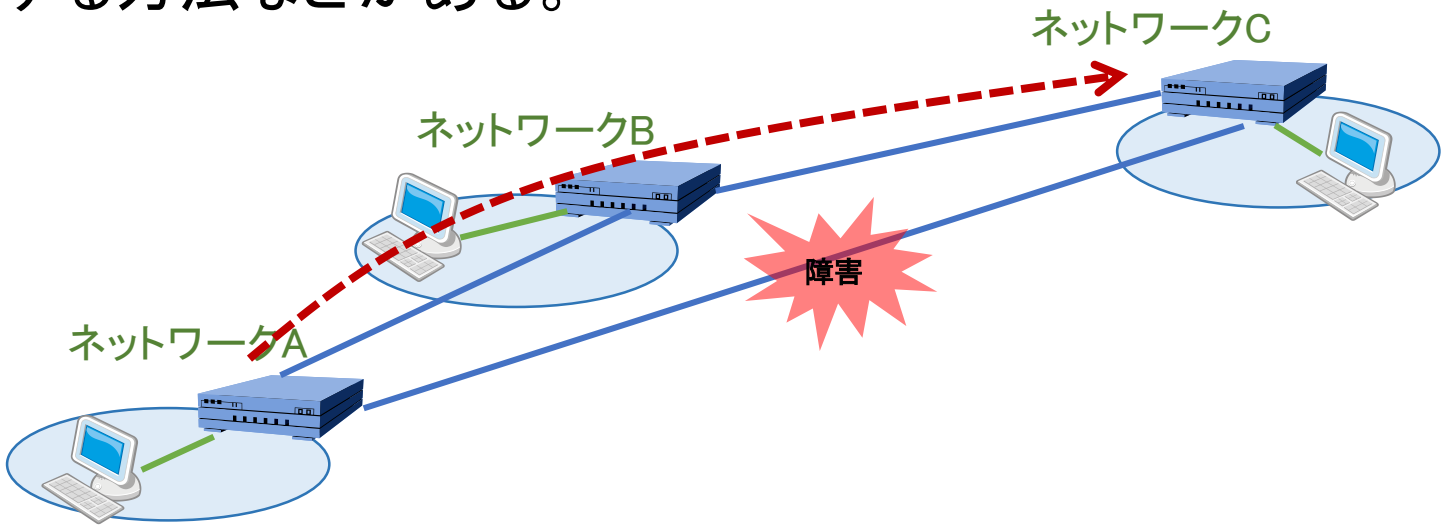
ネットワークは、ブロードキャスト・パケット（自分のネットワーク内の全ホスト宛に送信されるパケット）が届く範囲を指す



経路制御(ルーティング)

ルータの一番大事な機能であり、パケット内の宛先IPアドレスを読み取って、最適な経路を判断し、決定した経路へパケットを送信する。

最適な経路を判断する方法には、宛先ホストまでの距離や方向で判断する方法や回線の込み具合によって判断する方法などがある。



● ルーティング・テーブル

ルータが、宛先ホストまでの最適な経路を判断する情報は、表の形でルータ内に保存されている。これを、ルーティング・テーブル(経路制御表)と呼ぶ。

＜ルーティングテーブルの内容(距離と方向で判断する場合)＞

- 宛先ネットワークアドレス
- 宛先ネットワークの方向(中継するルータのIPアドレス)
- 距離(中継するルータの台数)

L3(Layer3)スイッチ

近年、ルータと同じ機能を持った通信機器として、L3スイッチが使用されている。ルータは、ルーティングなどの機能をソフトウェアで実現しているのに対して、L3スイッチは、ハードウェアで実現しているので、同じ機能がルータに比べて高速に実行できる。

L3スイッチを使ったLAN分割

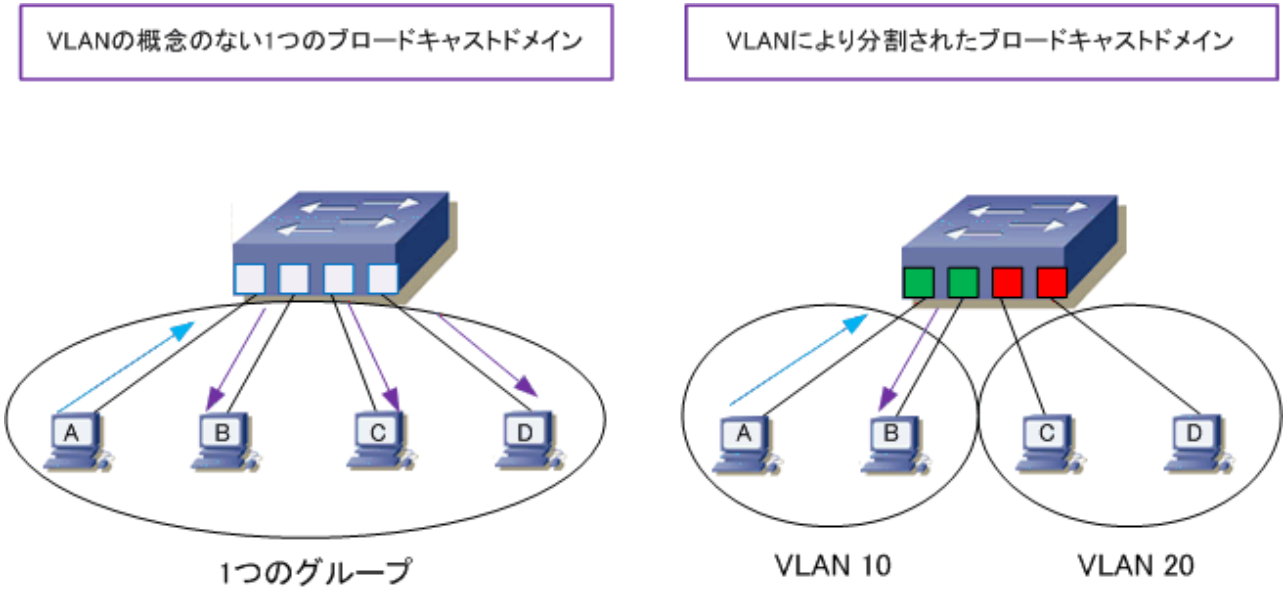
近年、会社などの組織では、組織内ネットワークのブロードキャストドメインを分割する要求が出てきた。これに、L3スイッチを利用することが増えてきた。

VLAN(Virtual LAN)

物理的な接続形態とは異なり、仮想的なLAN(セグメント)を作ることができる機能。

この機能は、VLAN機能があるスイッチング・ハブにおいて、各ポートに接続されているホストのMACアドレスとVLANの識別番号となるVLAN-IDを設定することで、実現できる。

各VLANセグメント間では、ブロードキャスト・パケットが流れないので、ブロードキャストドメインを分割することができる。



その他のLAN間接続装置

- ゲートウェイ

OSI基本参照モデルの全層（第1層～第7層）のプロトコルを解釈するネットワーク装置。

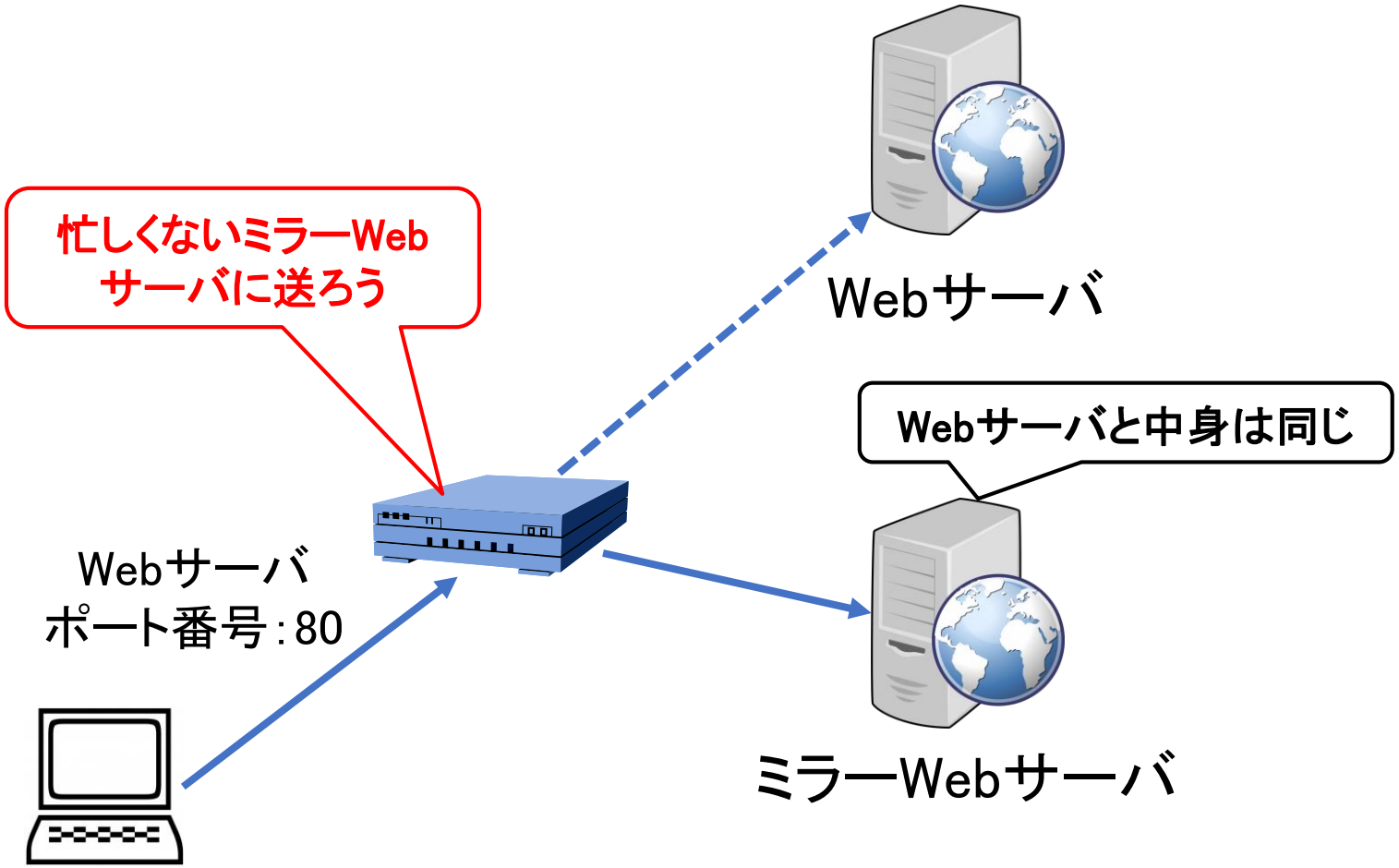
主な機能は、データ形式の変換やプロトコルの変換やアプリケーション・プロトコルのヘッダに混入した不正な情報を検出することができる。

- L4 (Layer4)スイッチ

OSI基本参照モデルの第4層のプロトコルを解釈するネットワーク装置。

第４層のプロトコルであるTCPやUDPのポート番号を、経路制御の判断情報として用い、サーバの負荷状況に応じて、パケットの転送先を変更できる。（負荷分散装置）

● 負荷分散型装置


忙しくないミラーWeb
サーバに送ろう
Webサーバ
Webサーバと中身は同じ
Webサーバ
ポート番号：80
ミラーWebサーバ

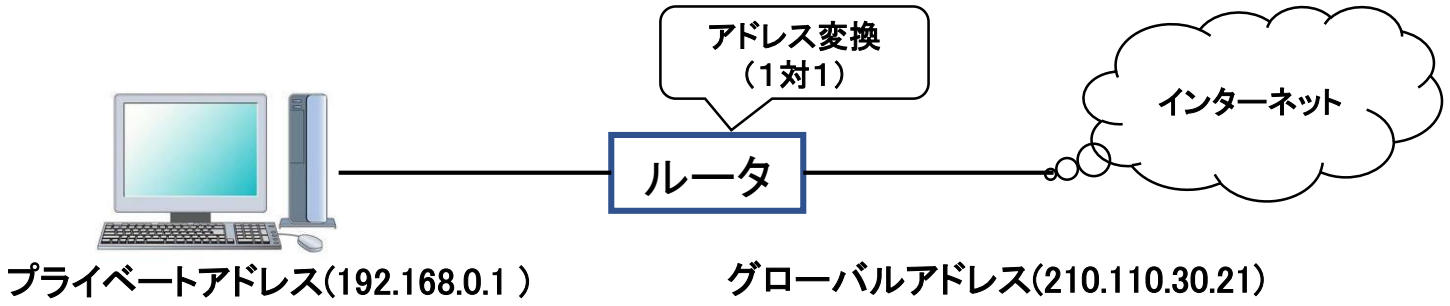
NAT(Network Address Translation)

テキストP277-280

NAT(アドレス変換)

通常、LAN内のホストに割り当てるIPアドレスは、グローバルアドレス(インターネットに直接接続するために使うIPアドレス)の使用数を節約するために、プライベートアドレス(LAN内で管理者が割り当てるIPアドレス)を使う。

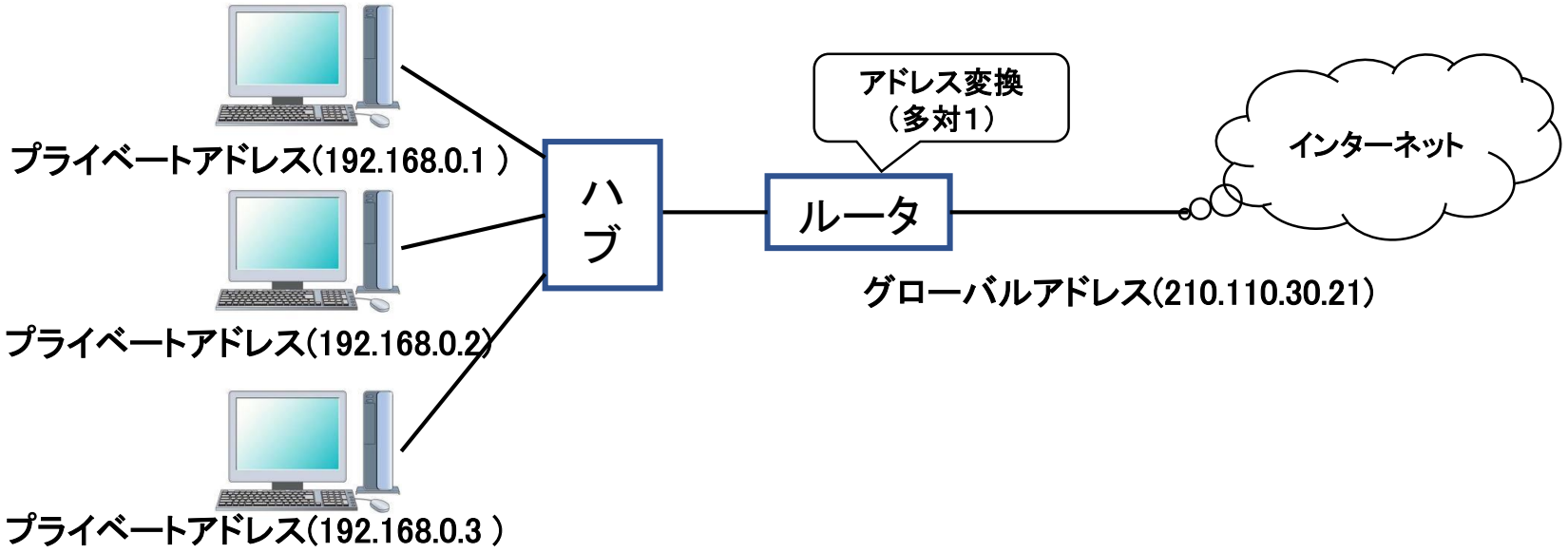
プライベートアドレスを割り当てられたLAN内のホストを、インターネットに接続するために、プライベートアドレスとグローバルアドレスを変換するための機能をNATと呼ぶ。



IPマスカレード
または　NAPT(Network Address Port Translation)

※ルータの製造会社によって、呼び方が違う

複数のプライベートアドレスが割り当てられたLAN内のホストを、インターネットに接続するために、プライベートアドレスとグローバルアドレスを変換するための機能をIPマスカレード（またはNAPT:ナプト）と呼ぶ。



アプリケーション層のプロトコル

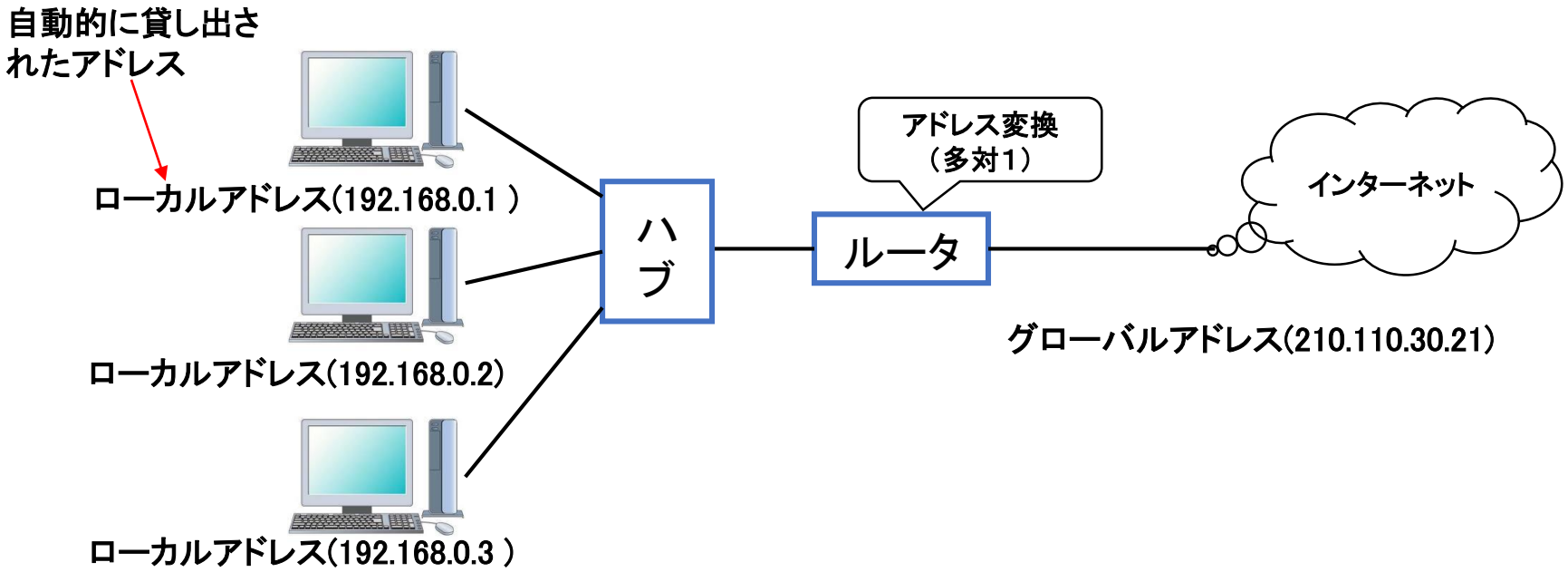
テキストP281-290

アプリケーション層の役割

プロトコル名	用途		ポート番号
DHCP	クライアントへの自動IPアドレスの割当		546,547(UDP)
DNS	ドメイン名とIPアドレスの変換		53(UDP)
SMTP	メール	送信	25(TCP)
POP3		受信	110(TCP)
IMAP4		受信	993(TCP)
TELNET	他の端末への遠隔操作		23(TCP)
HTTP	HTMLデータの送受信		80(TCP)
FTP	ファイルの送受信		20,21(TCP)
HTTPS	SSL機能を使ったHTTP通信		443(TCP)

DHCP（Dynamic Host Configuration Protocol）

IPアドレスを自動的に貸し出す



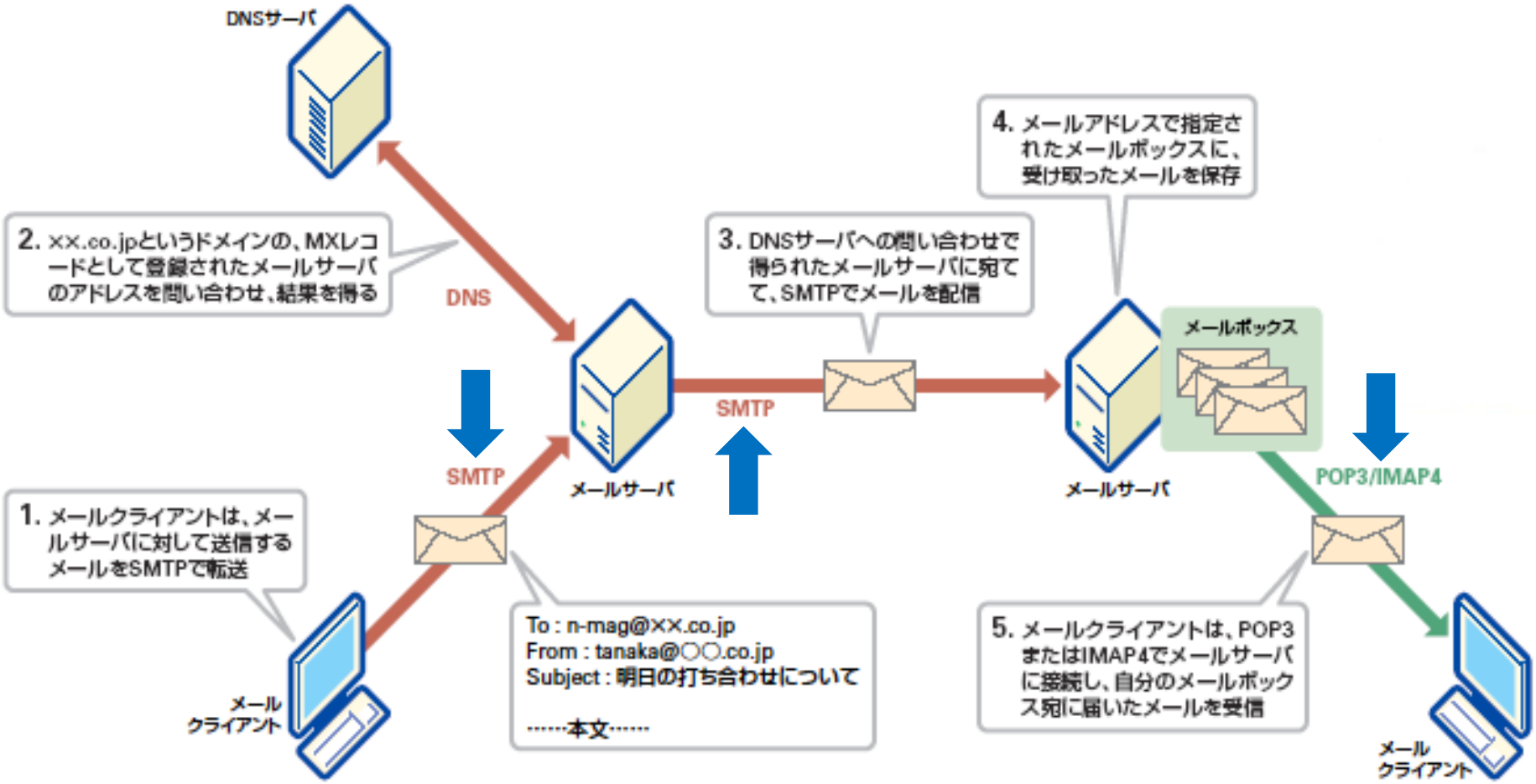
DNS（Domain Name System）

IPアドレス:　192.168.1.2

一対一で対応している

ドメイン名:　www.tokai.ac.jp

メールプロトコル


DNSサーバ
2. ××.co.jpというドメインの、MXレコードとして登録されたメールサーバのアドレスを問い合わせ、結果を得る
DNS
3. DNSサーバへの問い合わせで得られたメールサーバに宛てて、SMTPでメールを配信
4. メールアドレスで指定されたメールボックスに、受け取ったメールを保存
メールボックス
SMTP
SMTP
メールサーバ
メールサーバ
POP3/IMAP4
1. メールクライアントは、メールサーバに対して送信するメールをSMTPで転送
To : n-mag@××.co.jp
From : tanaka@○○.co.jp
Subject : 明日の打ち合わせについて
……本文……
5. メールクライアントは、POP3またはIMAP4でメールサーバに接続し、自分のメールボックス宛に届いたメールを受信
メールクライアント
メールクライアント

その他のメールプロトコル

- MIME（Multipurpose Internet Mail Extensions）

  電子メールで、各国語や画像、音声、動画などを扱うための規格。MIMEに電子メールの暗号化と電子署名の機能を追加した規格に、S/MIME（Secure MIME）がある。

セキュアなSMTP

電子メールの送信時に、本人認証機能をつけたプロトコル

- POP Before SMTP

  電子メールを受信するときに、POP3を使ってIDとパスワードで本人認証する。メール受信したIPアドレスのホストに、一定時間だけSMTP接続（メール送信する）を許可する。

- **SMTP Authentication**
  SMTPに本人認証を追加したプロトコル

HTTP

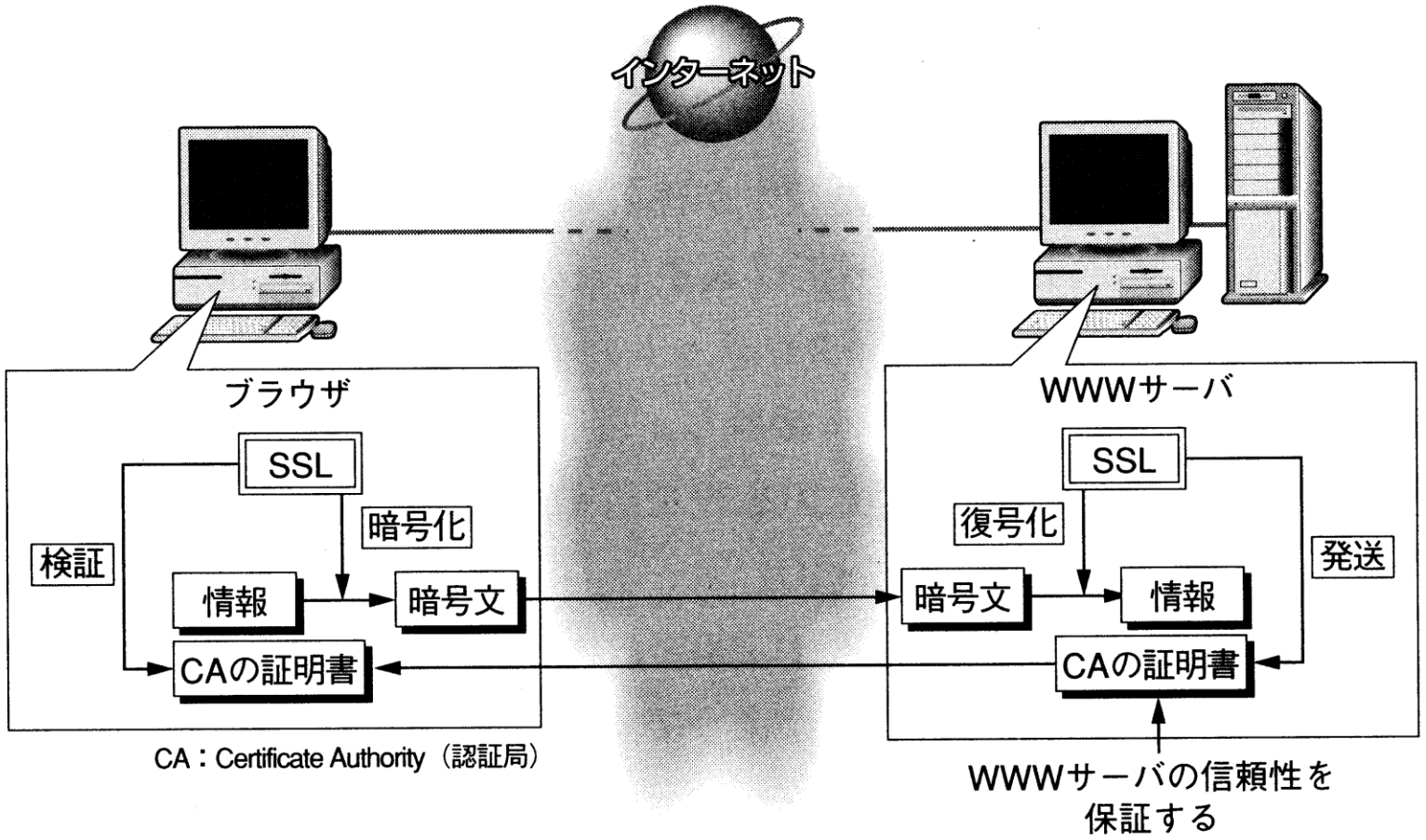
WebサーバとWebクライアントの間でデータを送受信するために用いられるプロトコル。
Webページを構成するHTMLファイルや、ページに関連付けられたスタイルシート、スクリプト、画像、音声、動画などのファイルを、データ形式などのメタ情報を含めてやり取りすることができる。

HTTPS

HTTPに送受信データの暗号化、ディジタル署名、認証の機能を追加したプロトコル。SSL(Secure Sockets Layer)を使うことにより、WebサーバとWebクライアントの間でやり取りするデータを暗号化することができる。

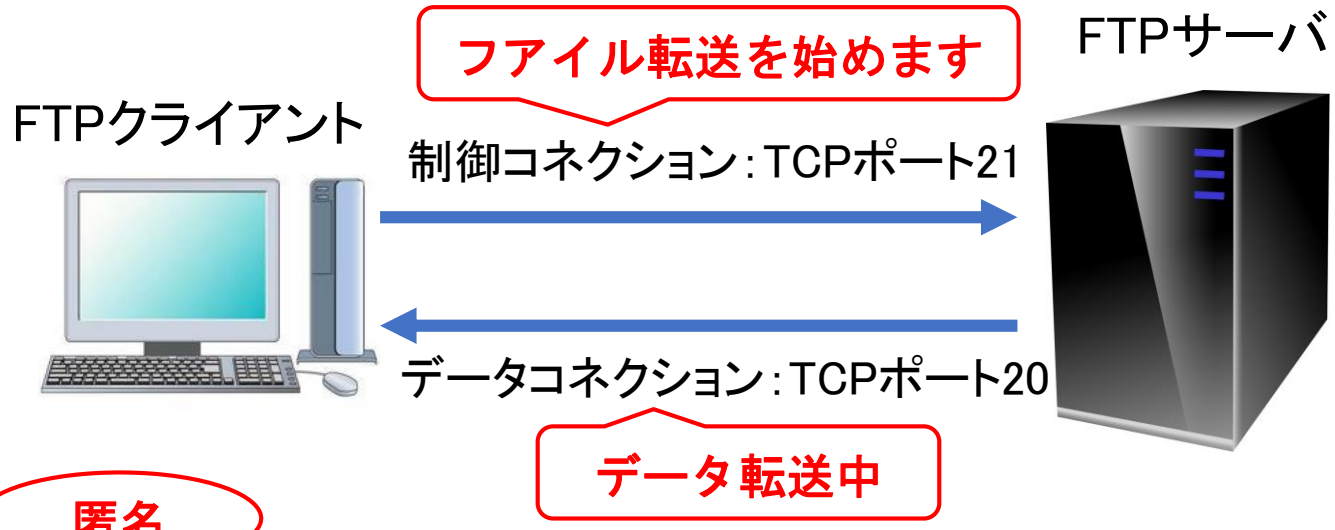
● SSL（Secure Sockets Layer）

SSLにより
・WWWサーバはCAの証明書をブラウザに送り、ブラウザはそれを検証してWWWサーバの信頼性を確認する
・ブラウザからWWWサーバへは情報を暗号化して送る（WWWサーバからブラウザへも同様）



FTP(File Transfer Protocol)

クライアントとFTPサーバの間で、ファイルをやり取りするためのプロトコル。パスワード認証と2回のTCPコネクションで接続・転送する。



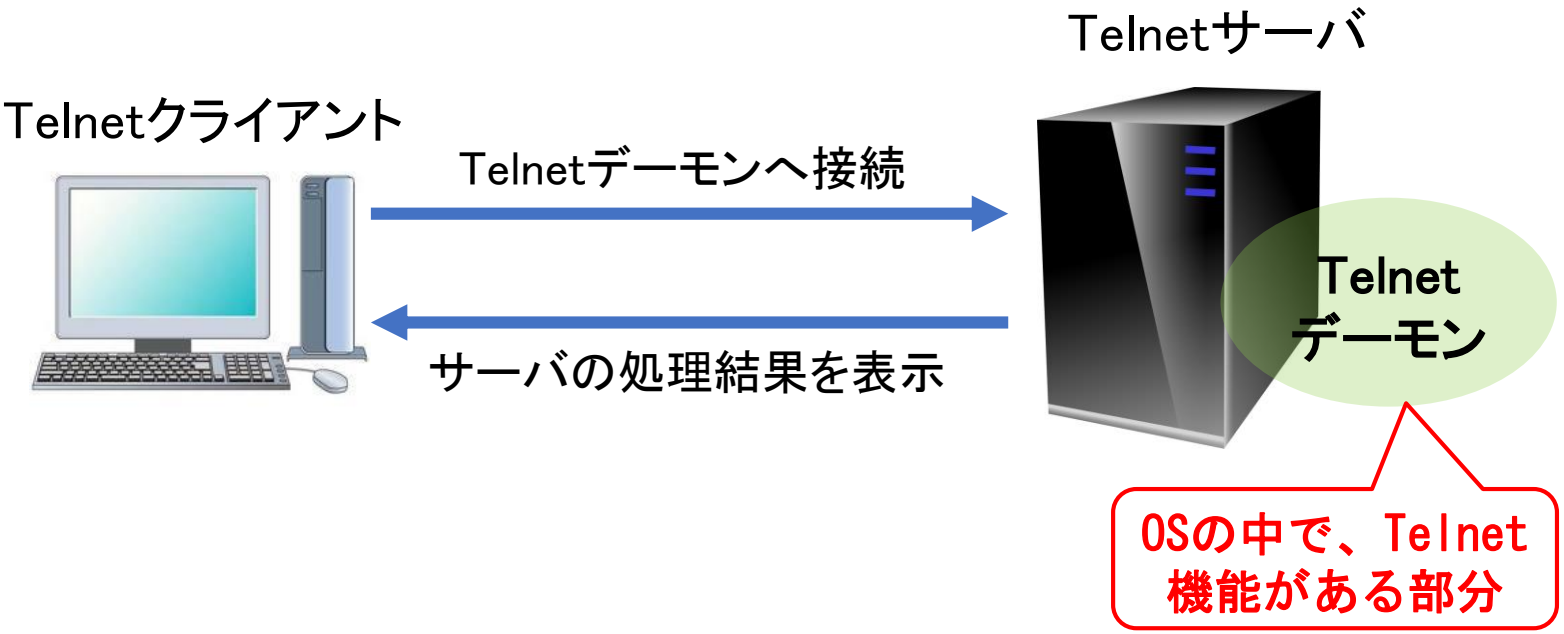
- Anonymous FTP(アノニマス FTP)

ファイルの送受信を行うFTPを、誰でも匿名で自由に利用できるようにする。不特定多数へのソフトウェアやデータの公開・配布などのために利用される。

TELNET

ネットワークを通じて別のコンピュータにアクセスし、遠隔操作するためのプロトコル。

このプロトコルで、クライアント上に仮想端末を構成して、サーバに接続する。仮想端末から、TELNETの操作コマンドを入力するが、実行するのはサーバ。仮想端末は、コマンド入力・表示やサーバの実行結果を表示する機能のみ。



無線LAN

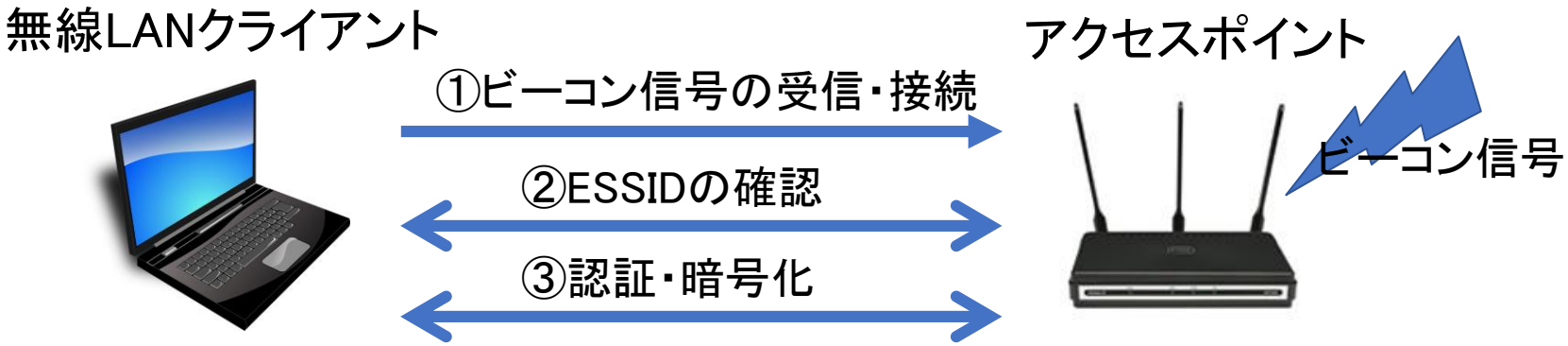
テキストP291-294

無線LAN

従来、同軸ケーブルやツイストペアケーブルなどの有線を使って構築していたLANを、電波などの無線を使って構築する

	IEEE802.11b	IEEE802.11a	IEEE802.11g	IEEE802.11n	IEEE802.11ac
通信速度	11Mbps	54Mbps	54Mbps	600Mbps	1.3Gbps
周波数	2.4GHz	5GHz	2.4GHz	2.4GHz/5GHz	5GHz
特徴	早くから普及	周波数により場所等に制限	11bと上位互換	11a,11b,11gと上位互換	2.4GHz帯の運用機器も配慮
長所	機器が安い		11b機器との混在可能	通信速度が速い。11a,11b,11g機器との混在可能	通信速度が速い。これまでの規格と混在可能
短所	通信速度が遅い	11bとの互換なし	家電製品と干渉	家電製品と干渉	

無線LANのアクセス手順



① ビーコン信号の受信・接続

アクセスポイントが常に送信しているビーコン信号を、無線LANクライアントが受信して、アクセスポイントの存在を認識する

② ESS-IDの確認

アクセスポイントに設定されているESS-ID(アクセスポイントの名前)を、無線LANクライアントが受信し、クライアントに設定済みのESS-IDと比較する。一致すると、ネットワークへのアクセスが許可される。

③ 認証と暗号化

アクセスポイントがクライアントを認証し、送信するパケットを暗号化する。これ以降、クライアントとアクセスポイント間でやり取りする全パケットは、暗号化される。

WEP(Wired Equivalent Privacy)暗号

無線LANでよく使用している暗号化方式の1つであるが、構成上の欠陥があり、以下の弱点が指摘されている

① MACヘッダが暗号化できず、ペイロード(パケット内の本来送りたい情報部分)のみ暗号化する
② アクセスポイントごとにWEPキー(秘密鍵)が設定され、ユーザごとには、キーを変えることができない
③ 暗号化方法に構造上の弱点がある

セキュリティの向上

- WPA/WPA2(Wi-Fi Protected Access)
  WEPに代わる暗号方式として、無線LANに使用している。また、WPA2は、WPAにAES（米国総務省標準の暗号）を採用し、キーを一定時間ごとに更新する。

- IEEE802.1x認証の導入
  ユーザごとに異なるキーを配布し、認証することができる。認証の方法は、RADIUS認証(認証サーバを使った認証方法)を採用している。このため、アクセスポイントのための情報と認証のための情報を分離することができ、安全な通信ができる。