

ネットワーク講座 #2

プロトコルとOSI参照モデル

開講者: Schneider

プロトコル (PROTOCOL)

- 相互が通信を行うために決められた約束事
 - 例えば、我々が会話するには言語を統一する必要がある(日本語同士、英語同士など). それと同じ
 - 通訳を使う場合もある → ゲートウェイ
- プロトコルを役割別に階層化することで、下位のプロトコルは上位のプロトコルを意識する必要がなく、逆に上位のプロトコルは下位のプロトコルの使い方を知るのみでよい(ブラックボックス化) → OSI(基本)参照モデル
 - 例えば、我々が電話するのに電話交換機の内部構造を知る必要はないし、言語(日本語か英語かなど)に合わせて電話交換機の構造を変える必要もない.
- 例えばイーサネットやHTTP、TCP/IPなどがプロトコル

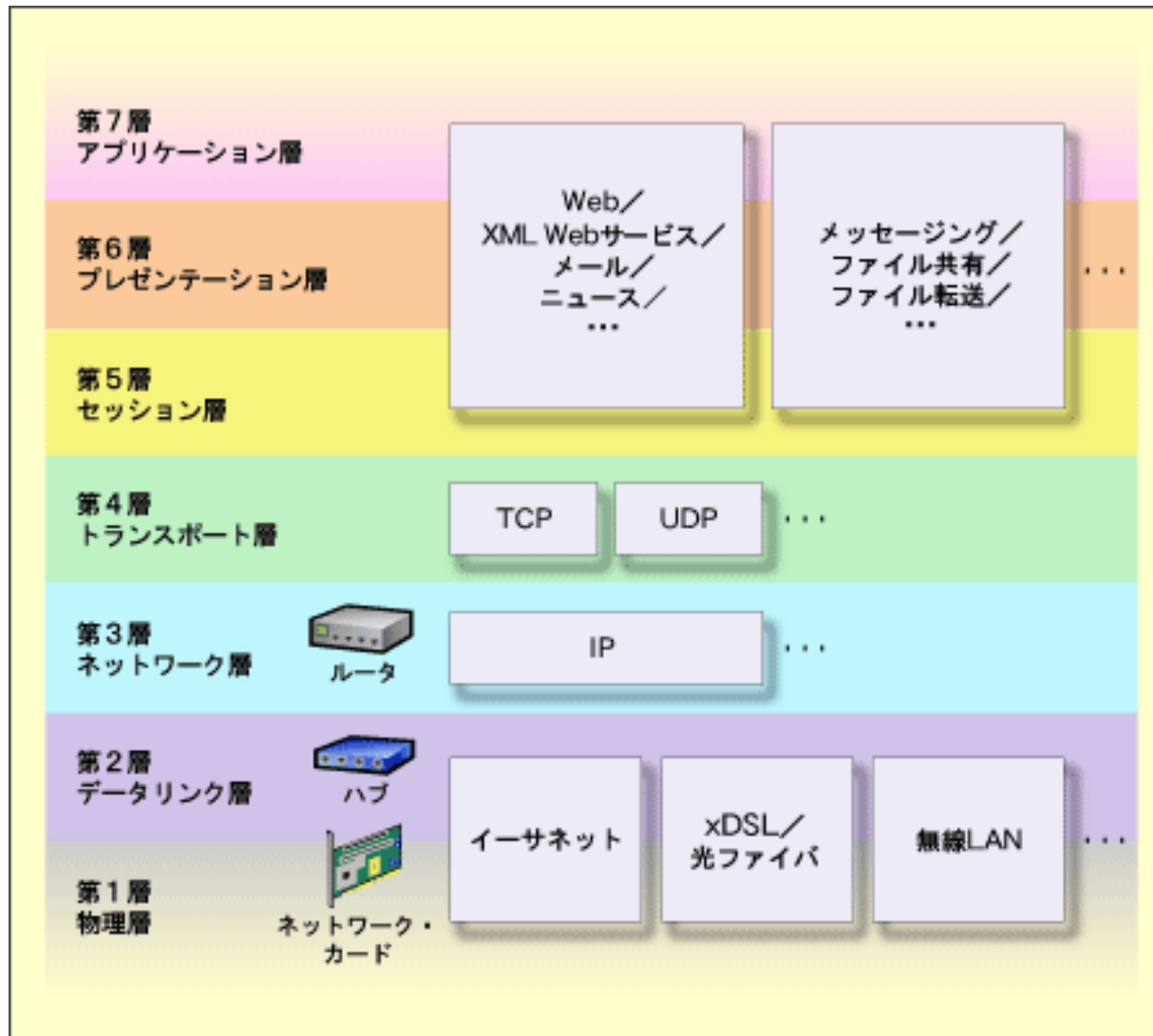


OSI参照モデル (OSI REFERENCE MODEL)

- ISO (国際標準化機構)が作成した、7つのプロトコル階層から成るネットワークの約束事
- 元々はOSI (開放型システム間相互接続)というネットワーク標準のためのモデルだが、OSIが普及せずOSI参照モデルのみが基本モデルとして残った
- これを理解することによりネットワーク障害時のトラブルシューティングにおいて問題の切り分け・解決が容易となる



OSI参照モデルの階層(レイヤ)



上から「**ア**プ**セ**ト**ネ**デ
ブ」と覚える

実際にはこの様に4層に分けられている場合が多い
(**TCP/IP参照モデル**)



第1層: 物理層

- 電氣的、物理的な機能を規定する
- 例えばケーブルの材質やコネクタの形状、データと電気信号の変換方式(例えば1なら高電圧、0なら低電圧など)を決める
- データの内容についてはこの層では規定されておらず、流れるデータ内容に合わせて変換方式を変えたりはしない
- 1000BASE-Tや**RS-232C** (いわゆるシリアルポート. 元々はモデムやコンピュータ端末の接続用に開発された)がこれに該当する



第2層: データリンク層

- 直接隣接する機器(ノード)間でのデータ通信について規定
- 例えば宛先・送信元の定義やアクセス制御方式など
- 物理層で発生する電気信号の誤り訂正(エラーコレクション)や再送要求を行う
- 相手に伝わったかどうかを確認する機能はこの層では存在せず、転送の信頼性は保証されていない
 - 受信通知は(通知なしに比べて)負荷が大きく、通信内容によっては通知なしの方がよい場合もある. そのためこの下位層では提供されず、より上位層であるトランスポート層で提供される (TCPとUDP)
- イーサネットや無線LAN、**PPP**が該当し、スイッチングハブがこの層の役目を担う



第3層: ネットワーク層

- 通信相手までデータを届けるための経路選択、中継を規定する
- データリンク層が隣同士(ポイントツーポイント)を担うのに対し、ネットワーク層は起点から終点まで(エンドツーエンド)を担う
- データリンク層による通信をバケツリレー式に相手まで送信する. また、データリンク層の仕様の違い(パケットサイズなど)もここで吸収する
- 全ネットワーク上で相手を一意に特定し、経路選択する必要がある、そのために(普通は)IPが用いられる
- ルータがこの役目を担う



第4層: トランスポート層

- データを確実・効率的に送るための方法を規定
- ネットワーク層によりエンドツーエンドで接続された通信の内容を高機能なものに変換する
- 例えば、ネットワーク層により送られたデータの整序(並び替え)や誤り訂正、(必要時には)再送要求を行うなど
 - データを細切れ(パケット)にして送信するが、普通ネットワーク層は細切れが元の順番通りに受信することを保証していない。そのため並び替える必要がある
- トランスポート層以上は各ホストマシン(PCなど)のオペレーティングシステム(OS)やアプリケーションソフトウェアが担当し、専用のハードウェアは一般には用意されない。TCPやUDPが該当する



第5層: セッション層

- 通信するプログラム間での通信開始から通信終了までの手順を規定
- 例えば、要求・返答の同期など
- この層により論理的(仮想的)な通信路が確立される
- この層以降は単一のプロトコル(HTTPやSMTP)で実装されることが多い
- 認証方式やアクセス権限などが該当する



第6層: プレゼンテーション層

- 圧縮方式や文字コードなど、データの表現形式を規定する
- これにより、データの意味が正しく伝わるようになる
- データの圧縮解凍・暗号化などが該当する



第7層: アプリケーション層

- これまでの層によるデータ通信をユーザや他のプログラムへ伝える役割を担う



その他の層

- もちろんこれらはジョークである.
- 第0層: 土建層
 - ネットワークを構成する建物を指す
- 第8層: ユーザ層
 - OSI参照モデルの何処も問題がないのに何故かトラブルシューティングが解決しない時の原因(かもしれない)
 - 要はエンドユーザ様の使い方が悪い:P
- 第9層: 財務層
 - コストに問題があることを揶揄したもの
- 第10層: 政治層
 - 政治的理由により接続できないことがあるかもしれない.
 - ~~日本の近所にあるあの国とか.~~



TCP/IP

- 現在のインターネットで使われるプロトコルの組み合わせ
- 狭義にはトランスポート層のTCPとネットワーク層のIPの二つのみを指すが、日常的には類似プロトコル(UDPなど)やTCP/IP上で使用する上位層(HTTPやSSHなど)を含めた表現である(インターネットプロトコルスイート)
- 本方式をサポートしたUNIX系OSの普及により現在の事実上の標準(デファクトスタンダード)となった
- 今日これをサポートしない汎用OSはまず存在しない(Windows, Mac OS X, BSD, Linux...)



TCP (TRANSMISSION CONTROL PROTOCOL)

- 高速性よりも確実性を重視したプロトコル
 - 高速性を重視するものはUDPであり、VoIPなどで使用される. こちらはコネクションレス型(相手に伝わったかどうかを保証されない)
- コネクション型(受信通知を必要とするもの)であり、送信失敗などを把握でき、再送信要求が可能
 - 例えば通販サイトにおいて、注文のデータ送信が確実に届かないと非常に困るだろう.
- WWWや電子メールなど多くの環境で使用される



IP (INTERNET PROTOCOL)

- LANやWANを相互接続することで特定箇所に不具合(障害)が生じててもそれを迂回して通信を確立するシステム
 - それまでは中央集約部分が死ぬと全ネットワークが死ぬ構成であり、これでは耐障害性が低い(というか、軍事用として役に立たない)ためIPが考案された
- 全世界でホスト端末を一意に特定する必要があり、それを実現するための住所として**IPアドレス**が使用される
 - 昔は各端末ごとにユニークなアドレス(**グローバルIPアドレス**)を振っていたが足らなくなったため**NAT**などの技術を使用して延命している
- アドレス長が32bitの**IPv4** (現在主流)と128bitの**IPv6** (これから移行)の二種がある



PPP (POINT TO POINT PROTOCOL)

- リンク制御プロトコル(LCP)とネットワーク制御プロトコル(NCP)を組み合わせて2点間を接続するプロトコル
 - LCPでユーザ認証をし、NCPで接続を確立する
 - NCPは上位層のプロトコルによって使い分ける必要があり、IPの場合はIPCPが用いられる
- 電話回線上で使用可能にしたPPPがダイヤルアップPPPで、90年代に使用された
- ADSLやFTTH(いわゆる光回線)による回線ではイーサネット上でPPP接続を行うPPPoEが使用される



PPPoE (PPP OVER ETHERNET)

- PPPのユーザ認証機能などをイーサネット上でも使えるようにするためにPPPをカプセル化するプロトコル
- 元々イーサネットはPPPoEを使わなくてもIPを使用して通信が行えるがイーサネットに認証機能がなく、ISP側にとって不便なのでこのような面倒な方法がとられる
 - イーサネットはコネクションレス型なのでそのままでは使用時間もわからないし、使用人数もわからない
- 一般家庭ではルータの設定画面でISPのユーザ名(メールアドレスなど)とパスワードを入力する必要があるが、これにPPPoEを使用している
- イーサネットを使用するため安価



その他のプロトコル

- **HTTP** (Hyper Text Transfer Protocol)
 - WWWに使用される
- **FTP** (File Transfer Protocol)
 - ファイル転送に使用される
- **Telnet** (Telecommunication Network)
 - 遠隔でシェルにログインする
- **SSH** (Secure Shell)
 - 暗号化で安全に遠隔ログインする
- **SMTP** (Simple Mail Transfer Protocol)
 - メール送信に使用
- **POP** (Post Office Protocol)
 - メール受信に使用



TELNET (TELECOMMUNICATION NETWORK)

- IPネットワークにおいて遠隔地にあるサーバを端末(ターミナル)から操作するためのプロトコル
- 元々は信頼されたネットワーク内でのみ使用することを前提としたプロトコルのため暗号化されず、パスワードなども平文のまま通信してしまう
 - したがって、**パケットキャプチャ**などをされるとパスワードを覗き見されてしまう
 - ちなみに自分宛以外のパケットも受け取る設定を**プロミスキャスモード(無差別モード)**という. ネットワークの管理・監視に使用されるが、上のように盗聴にも使用される
- そのため現在は暗号化付きの**SSH**に置き換わりつつある



SSH (SECURE SHELL)

- ハイブリッド暗号方式(後述)を用いて高速かつ安全に通信を行いターミナルを操作するプロトコル
- パスワード認証、公開鍵暗号方式(後述)、ワンタイムパスワード(チャレンジレスポンス)など多くの認証・暗号化方式に対応しており環境に合わせて使い分けることができる
 - ただし、パスワード認証をブルートフォースアタック(総当たり攻撃)により突破されサーバのクラッキングが行われたという事例も多いため、公開鍵暗号方式が推奨される
 - まあJoe Pass(ユーザ名=パスなこと)だったりとかアレなサーバも多いが.
- SSH1とSSH2の2つがあるが1は脆弱性があるため2が推奨される

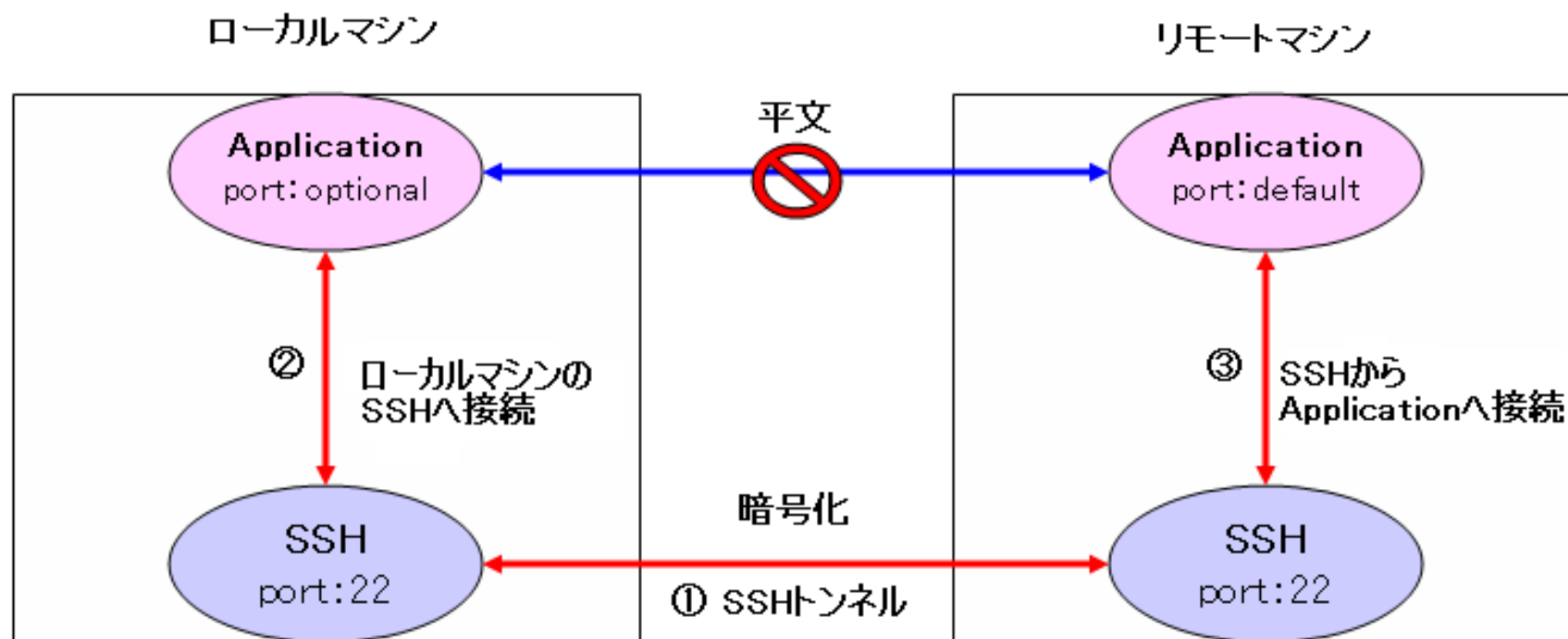


SSH (SECURE SHELL)

- 直接通信するのではなくSSHの通信路へ迂回して通信する機能(ポートフォワーディング)をもつ
 - 外から(認証外からは)SSHによる通信にしか見えないため、安全に通信を行うことができる
 - 直接リモートデスクトップなどを待機しているとルータの外からブルートフォースアタックなどにより用意に突破されてしまう。これを利用することで安全に待機することができる
 - 当然、SSHの暗号化がパスワード認証だと大差ないが。



SSH (SECURE SHELL)



チャレンジレスポンス認証

- サーバは**チャレンジ**というランダムな文字列を渡す
- クライアントはパスワードとチャレンジを特定のアルゴリズムにしたがって合成して**レスポンス**を作る
 - レスポンスは**一方向関数**(**ハッシュ関数**など)によって作られ、レスポンスから元のパスワードを復元することができない
 - **x**(引数)から**y**(結果)を求めるのは簡単だが**y**から**x**を求めるのが困難な関数を一方向関数という. 一方向関数のうち、与えられた原文から固定長の擬似乱数(**ハッシュ値**)を返すのがハッシュ関数で、**要約関数**、**メッセージダイジェスト関数**ともいう. データが改竄されるとハッシュ値が変わるのでデータの信頼性を確保する. ハッシュ値から元の原文を復元するのは不可能で、同じハッシュ値を作るのも困難. **MD5**や**SHA**などがある(**MD5**は脆弱性が発見されているので注意).
- サーバはそのレスポンスが正しいかどうかを確認する

脆弱性 (VULNERABILITY)

- ヴァルネラビリティともいう
- 情報システムにおいて、悪意ある第三者が脅威となる行為(情報の改竄やシステムの乗っ取りなど)へ利用できる問題点のこと
- 欠陥やバグ、想定外の使用法、設計ミスなどが原因
 - これらはセキュリティホールと呼ばれる
- 類似語のセキュリティホールと違い、ソーシャルエンジニアリングといったコンピュータシステム外のものも含む
 - 話術や経歴詐称でパスワードを(それとなく)聞き出したり、パスワード入力を後ろから覗き見したり(ショルダーハッキング)、パスワード変更のお知らせメールを不正に送りパスワードを(偽サイトで)入力させ入手するなどがソーシャルエンジニアリング



パケット (PACKET)

- TCP/IPにおいて、データを送受信するために細切れにしたもの
- 先頭部(ヘッダ)に送信元情報や送信先情報、プロトコル情報などが記されており、これにしたがってスイッチングハブやルータはデータを配送する
- 小分割することで再送時にも最小限で済み、**トラフィック**(混雑)を軽減できる
- 携帯電話における情報単位としても有名で、1パケットは128byteである
 - したがって、現在の移動通信に使用するパケット数は膨大な数となる



イントラネットとエクストラネット

- インターネット技術(Webサーバや電子メール、ファイルサーバなど)を企業内の情報システムに取り入れ業務支援に活用するネットワークシステムを**イントラネット**という
- イントラネット同士(例えば支部間など)で接続したものを**エクストラネット**という



VPN (VIRTUAL PRIVATE NETWORK)

- 本来、通信内容を傍受されたりしないためには専用線が必要だが、国際化した現在では現実的にそれが不可能であることも多い
 - 例えば、アメリカの本社と日本の支社を専用線でつなぐのはまず無理だし、国内でも北海道と沖縄を中小企業が専用線でつなぐのはコスト的に無理だろう。
- そのため、通常の一般回線を暗号化により私用回線(プライベートネットワーク)として使用する技術が必要となり、それを実現するのがVPN
- 暗号化にはIPSecやSSLなどが使用される
- 徳島大学でも申請すればVPN接続により学外からでも一部サービスを利用できる



PPTP (POINT TO POINT TUNNELING PROTOCOL)

- PPPにトンネリング機能を付加したもので、Microsoftにより考案された。データリンク層に対応する
 - パケットを別のプロトコルのパケットで包みこみ(カプセル化)、外部から遮断するのをトンネリングという。包み込む際に暗号化する
- PPTP自体は暗号化しない(トンネリングのみ)のためMS-CHAPによる認証とRC4による暗号化を組み合わせる
- アルゴリズムが単純なため高速で、かつ多くのプラットフォームで使用可能だが、現行の認証方式であるMS-CHAPv2に特定条件下で脆弱性が存在し、悪意ある第三者により中間者攻撃(MITM)を受ける可能性がある



中間者攻撃 (MAN-IN-THE-MIDDLE ATTACK)

- 送信者(暗号理論ではアリスという)と受信者(ボブという)の間に立ってメッセージを盗み見たり、内容を変更したりすること(ちなみにこの中間者をマロリーという)
 - アリス、ボブといった名称は多くがブルース・シュナイアーの暗号技術大全という本に由来する
 - アリス、ボブそれぞれではきちんと(それぞれボブとアリスと)認証を行なっているように見える
- そのため、お互いの公開鍵(南京錠みたいなもの)が本物であるかを保証する必要がある → 認証局(CA)
 - 南京錠でいうところの南京錠側が公開鍵で、それを開ける鍵が秘密鍵に相当する. このような方式を公開鍵暗号方式という. 公開鍵は暗号化(鍵を閉める)に使用し、秘密鍵は復号化(鍵を開ける)に使用する. このように暗号化と復号化で別の手順を用いる方法を非対称暗号方式という.



公開鍵暗号方式

- 各メンバーごとに公開鍵と秘密鍵のペア2本が必要となる
 - 公開鍵は共通であるというのはよくある間違いである.
- まずボブは(アリス用の)公開鍵を世界に公開する
- アリスはその公開鍵を用いて暗号化し、ボブへ送る
- ボブはその公開鍵に対応した秘密鍵を用いて復号化する
- 盗聴者(イヴ)や改竄者(マロリー)はボブ宛の通信を傍受しても、秘密鍵を持たないので復号化できない
 - イヴやマロリーは公開鍵なら入手できるが、公開鍵から秘密鍵を作れないため意味がない(南京錠だけあっても意味がない)



共通鍵暗号方式

- 秘密の合言葉みたいなもの
- 暗号化と復号化に同じ(あるいは片方からもう一方を容易に把握可能な)鍵を用いる. このような方式を**対称暗号方式**という
- どうやってボブがアリスにその合言葉を安全に伝えるかが問題となる
- メンバ数が N のとき、鍵数が $_NC_2$ 個も必要になり、 N が大きくなると管理が大変となる
 - 公開鍵暗号方式は $2N$ 個. $N > 5$ で共通鍵の方が多くなる
- **DES**や**AES**などが使用例
 - ちなみに**AES**暗号化・復号化を高速化する**CPU**機能があり、**AES-NI**という. **Intel Core iシリーズ**の一部や**AMD Aシリーズ**の一部などに搭載されている



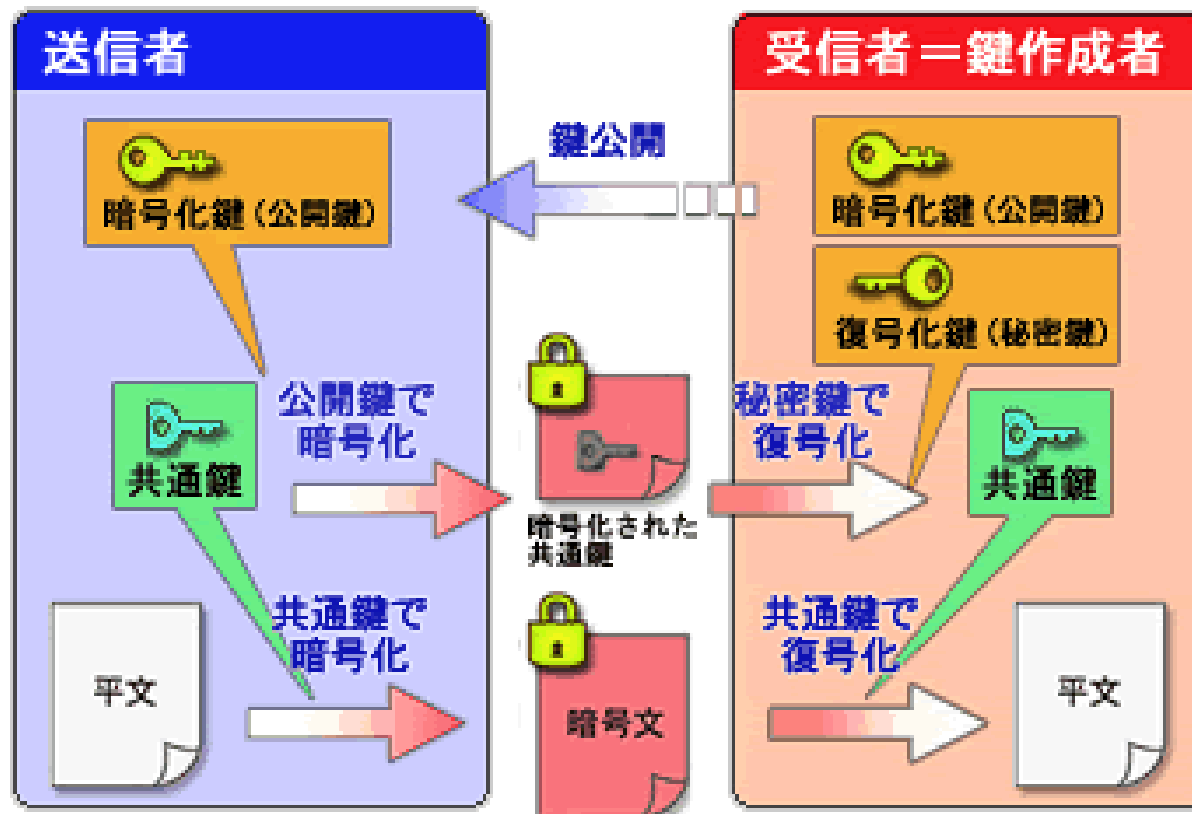
ハイブリッド暗号方式

- 公開鍵暗号方式は安全性が高いが処理が遅いというデメリットがある
- 対する共通鍵暗号方式は高速だがどうやって鍵を安全に渡すかという問題がある
- そのため、共通鍵を公開鍵で暗号化するという方式が存在し、これをハイブリッド暗号方式という



ハイブリッド暗号方式

- イメージ的には、最初に南京錠本体を送り、合言葉が記された紙を南京錠本体で暗号化して送り返してもらい、その後の通信ではその合言葉で暗号化・復号化する感じ



ハイブリッド暗号方式

- まずボブはアリス用の秘密鍵を公開する
 - アリスはその秘密鍵を用いて共通鍵を暗号化し、ボブに伝える
 - ボブはその共通鍵を用いて暗号化しアリスへ送る
 - アリスは共通鍵を用いて復号化する
 - イヴやマロリーは共通鍵を知ることができないので復号化できない
-
- 低速な公開鍵暗号方式は一度だけで後は高速な共通鍵暗号方式を用いるため、普通の公開鍵暗号方式より高速で普通の共通鍵暗号方式より安全である



L2TP (LAYER 2 TUNNELING PROTOCOL)

- MicrosoftのPPTPとCiscoの**L2F**を統合したもので、PPTP同様L2(データリンク層)で機能する
- PPTP同様にトンネリングのみのため、暗号化の**IPSec**と認証方式(MS-CHAPv2など)を併用する
 - このIPSecとの組み合わせを**L2TP/IPSec**と呼び、これを単にL2TPと呼ぶことも多い(普通はL2TPのみでは使えない)
 - こちらのMS-CHAPv2は前述の脆弱性とは無関係だそう(カプセル化が違うため)だが、一応避ける人も少なくない
 - IPSecのみでもVPNは実現できる(**トランスポートモード**)が、汎用性が低い
 - PPTPに比べて対応機種が少なく、また機器への負荷も大きいため速度で劣り、これまであまり使われなかった



SSL (SECURE SOCKET LAYER)

- 歴史的理由により**TLS**とも呼ばれる(厳密には別物)
- 公開鍵と**証明書**(お互いが本物であることを証明)を組み合わせる**公開鍵証明書**により認証する
- 成りすましを防ぐために信頼された第三者である認証局(CA)により**電子署名(デジタル署名)**され、中間者攻撃などを防ぐ
- 主にWebサイトの認証に使用される(**HTTPS**)



SSL-VPN

- SSLを用いたVPNで、Webブラウザベースで使用する
- 徳島大学でもこれを用いている
 - アクセスすると証明書が信頼できないと出るのでアレだが.
- クライアントのネットワーク構成によって設定の変更など(いわゆる**NAT越え**)が不必要
 - 原理的にはHTTPS通信ができればよい
- 反面、他のVPNに比べて構築が面倒
- これを実現するソフトウェアとしては**OpenVPN**や**Citrix NetScaler Gateway**などが有名



VPN OVER SSH

- SSHのポートフォワーディング機能を用いて擬似的にVPNを構築する技術
- 直接的にはファイアウォールで確立できない通信路を、SSHによるトンネリング・暗号化を経由して擬似的に確立する
- 多くの場合SSHアプリケーションが必要となり、OS標準では使用できない



VoIP (VOICE OVER IP)

- TCP/IPを用いて音声通信を行う技術
- 割と前(90年代後半)からあった技術だが、一般家庭への常時接続インターネット回線の普及、移動通信システム(3.5G通信や3.9G通信)の高速化・安定化及び多機能携帯電話(スマートフォン)の普及により一般化している
- LINE、Skype、Viber、Google Talk (現Google+ ハングアウト)などが有名
 - その性質上、チャットサービスと複合していることがほとんど
- 電話回線がなくてもインターネット回線があれば使用でき、将来的には現在の電話システムを置き換えるものとなるかもしれない → VoLTE
- 災害時の緊急電話として注目されている



VoLTE (VOICE OVER LTE)

- 次世代通信技術(4G)である**LTE-Advanced**への橋渡しとなる3.9G通信技術**LTE**を利用したVoIP
 - 日本国内のLTEとしてはNTTドコモの**docomo LTE Xi** (旧Xi)やKDDIの**au 4G LTE**、ソフトバンクモバイルの**SoftBank 4G / 4G LTE**、イー・アクセスの**EMOBILE LTE**がある
 - 拡張規格の**LTE-Advanced**は2015年度中に提供開始予定(NTTドコモの場合)
- パケット通信により1回線でも複数の電話を行うことができる
 - VoLTEは今年中に提供予定(NTTドコモの場合)

