

リモートアクセス/ ネットワークセキュリティ

情報実験 第8回 (2024/06/28)

北海道大学 大学院理学院
宇宙理学専攻
鮎田 忠治

私たちの研究室の日常

- 計算サーバにアクセスし,
数値シミュレーションを実行
- 観測データの取得...など
- ウェブサーバにアクセスし,
ウェブページを編集(詳しくは次回)

研究室ではネットワークを介して別の計算機とのやりとりが行われている

ー リモートアクセス

本日のレクチャー内容

- リモートアクセス
 - リモートログイン・リモートアクセスを用いたファイル転送
 - リモートアクセスで用いられるプロトコル
 - パケット盗聴の危険性
 - 暗号化とは
- ネットワークセキュリティ
(ユーザ編, 計算機管理者編)
 - 暗号化通信
 - ポート管理
 - アクセス管理
 - セキュリティホール

本日のレクチャー内容

- リモートアクセス

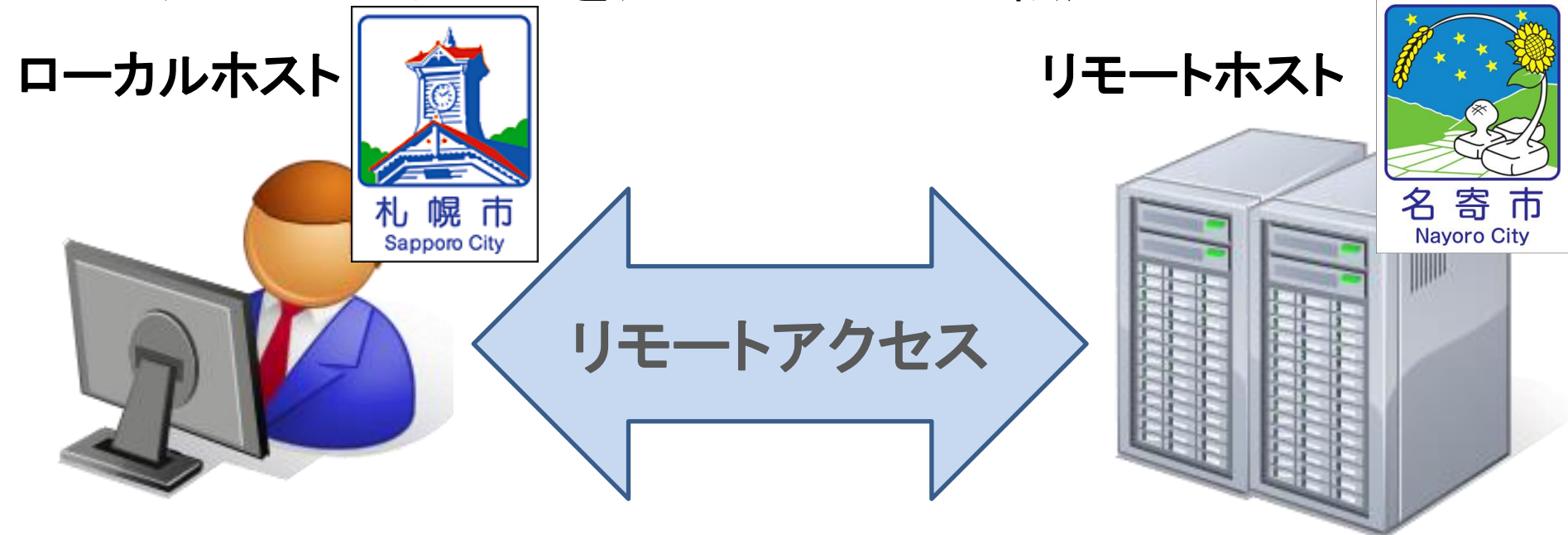
- リモートログイン・リモートアクセスを用いたファイル転送
- リモートアクセスで用いられるプロトコル
- パケット盗聴の危険性
- 暗号化とは

- ネットワークセキュリティ
(ユーザ編, 計算機管理者編)

- 暗号化通信
- ポート管理
- アクセス管理
- セキュリティホール

リモートアクセス

- 手元の計算機(**ローカルホスト**)から別の計算機(**リモートホスト**)へのネットワークを経由した接続・操作
 - リモートログイン
 - リモートアクセスを用いたファイル転送



リモートログイン

- ローカルホストからリモートホストへログインすること
 - ログイン: アカウント情報を用いて認証した後に, コマンド等を利用できる状態にすること(第 2 回)
 - 事前にリモートホストのアカウントが必要
- 主に使用するコマンド

-ssh

ユーザー認証

- リモートログインを試みるユーザーが正規のユーザーなのか確かめる必要がある
 - 事前にリモートホストのアカウントが必要
- 正規のユーザーしか持っていない情報で認証
例えば
 - パスワード方式
 - 公開鍵認証方式
- 今回利用するのはパスワード方式

リモートログインのイメージ



ssh コマンドを用いて,
リモートログインを要請



ホスト名: isono.ac.jp
アカウント名: sazae

ホスト名: fuguta.ac.jp
アカウント名: sazae

```
sazae@isono:~ $ ssh sazae@fuguta.ac.jp
```

リモートログインのイメージ



ホスト名: isono.ac.jp
アカウント名: sazae

ssh コマンドを用いて,
リモートログインを要請

ログインパスワードを要求



ホスト名: fuguta.ac.jp
アカウント名: sazae

```
sazae@isono:~ $ ssh sazae@fuguta.ac.jp  
sazae@fuguta.ac.jp's password:
```

リモートログインのイメージ



ホスト名: isono.ac.jp
アカウント名: sazae

ログインパスワードを送信

ログインパスワードを要求



ホスト名: fuguta.ac.jp
アカウント名: sazae

```
sazae@isono:~ $ ssh sazae@fuguta.ac.jp  
sazae@fuguta.ac.jp's password: (パスワードを入力)
```

リモートログインのイメージ



ホスト名: isono.ac.jp
アカウント名: sazae

ログインパスワードを送信

ログインを許可



ホスト名: fuguta.ac.jp
アカウント名: sazae

```
sazae@isono:~ $ ssh sazae@fuguta.ac.jp  
sazae@fuguta.ac.jp's password: (パスワードを入力)  
...  
sazae@fuguta:~ $ █
```

リモートアクセスを用いたファイル転送

- ローカルホストとリモートホストの間でファイルをやりとり
- 主に使用するコマンド
 - **sftp**
 - **rsync**

リモートアクセスを用いた ファイル転送のイメージ



ログインパスワードを送信



ログインパスワードを要求

ホスト名: isono.ac.jp
アカウント名: sazae

ホスト名: fuguta.ac.jp
アカウント名: sazae

```
sazae@isono:~ $ sftp sazae@fuguta.ac.jp  
sazae@fuguta.ac.jp's password: (パスワードを入力)
```

リモートアクセスを用いた ファイル転送のイメージ



ファイルの転送を指示

ログインパスワードを要求



ホスト名: isono.ac.jp
アカウント名: sazae

ホスト名: fuguta.ac.jp
アカウント名: sazae

```
sazae@isono:~ $ sftp sazae@fuguta.ac.jp  
sazae@fuguta.ac.jp's password: (パスワードを入力)  
Connected to fuguta.ac.jp.  
sftp> get file.txt
```

リモートアクセスを用いた ファイル転送のイメージ



ファイルの転送を指示



ファイル転送の実行

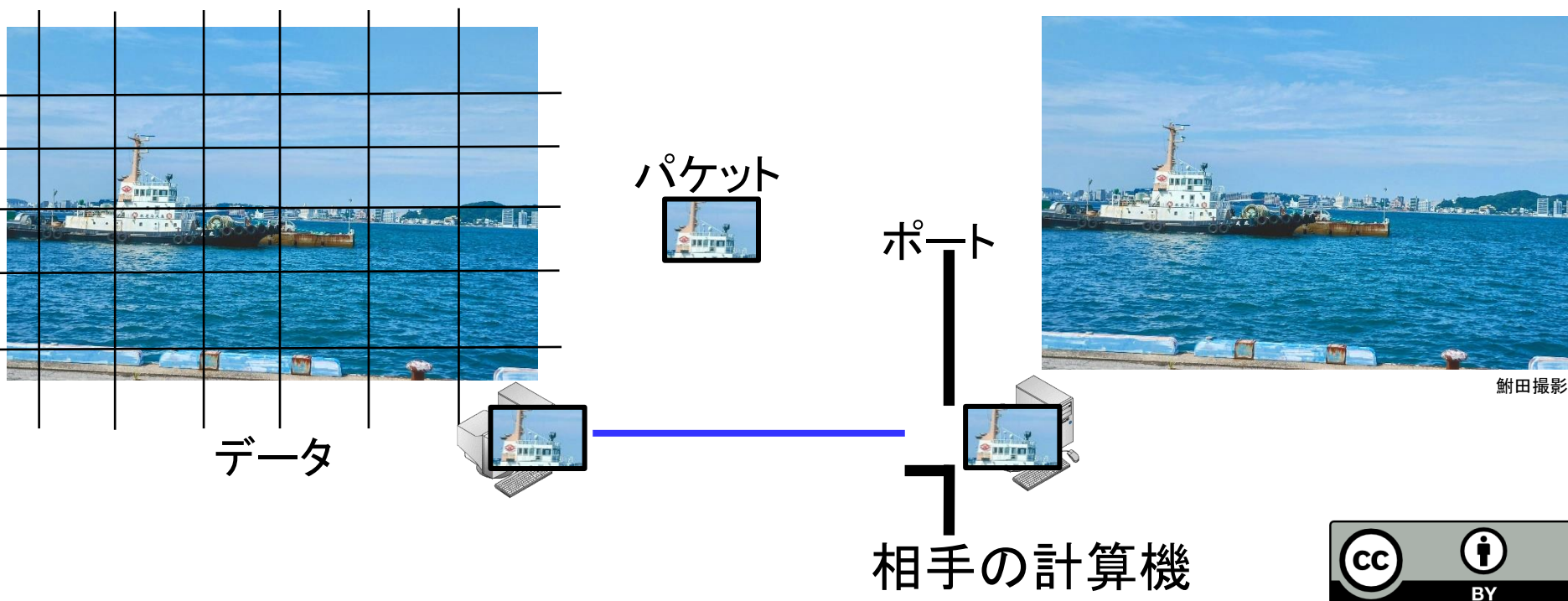
ホスト名: isono.ac.jp
アカウント名: sazae

ホスト名: fuguta.ac.jp
アカウント名: sazae

```
sazae@isono:~ $ sftp sazae@fuguta.ac.jp
sazae@fuguta.ac.jp's password: (パスワードを入力)
Connected to fuguta.ac.jp.
sftp> get file.txt
file.txt                100% 4KB   1.7MB/s   00:01
```

ファイル転送の手順 (第 4 回の復習)

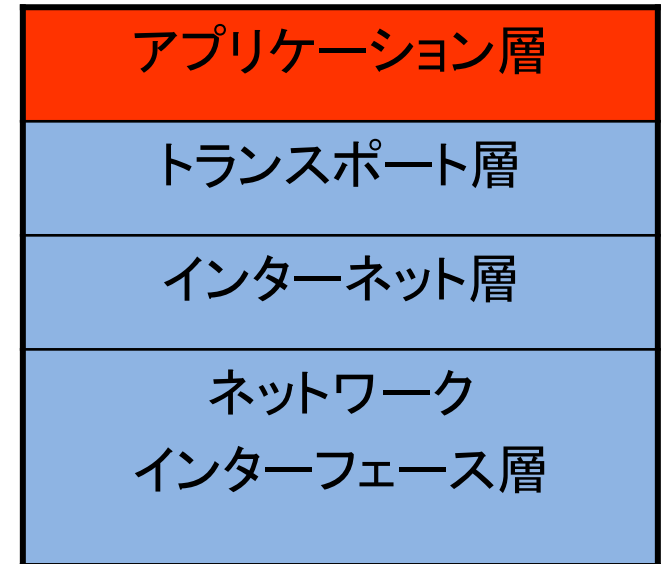
- データをパケットに分割し, 相手の計算機のポートへ転送, パケット転送完了後に結合
 - ネットワーク通信は**プロトコル**(通信規約)に従う



リモートアクセスに用いられるプロトコル

- **Telnet, FTP, SSH**

- アプリケーション層のプロトコル
- それぞれのプロトコルで用途や仕様が異なる (第 4 回)



TCP/IP の階層構造

Telnet(Teletype Network)

- 古くから利用されるリモートアクセス用プロトコル
- 使用ポート: 23番
- **通信が暗号化されない(危険・非推奨)**
 - 現在は主にポートチェック(特定のポートの開閉を確認)に使用
- このプロトコルを利用する主なコマンド
 - telnet

「ポート」については第 4 回参照

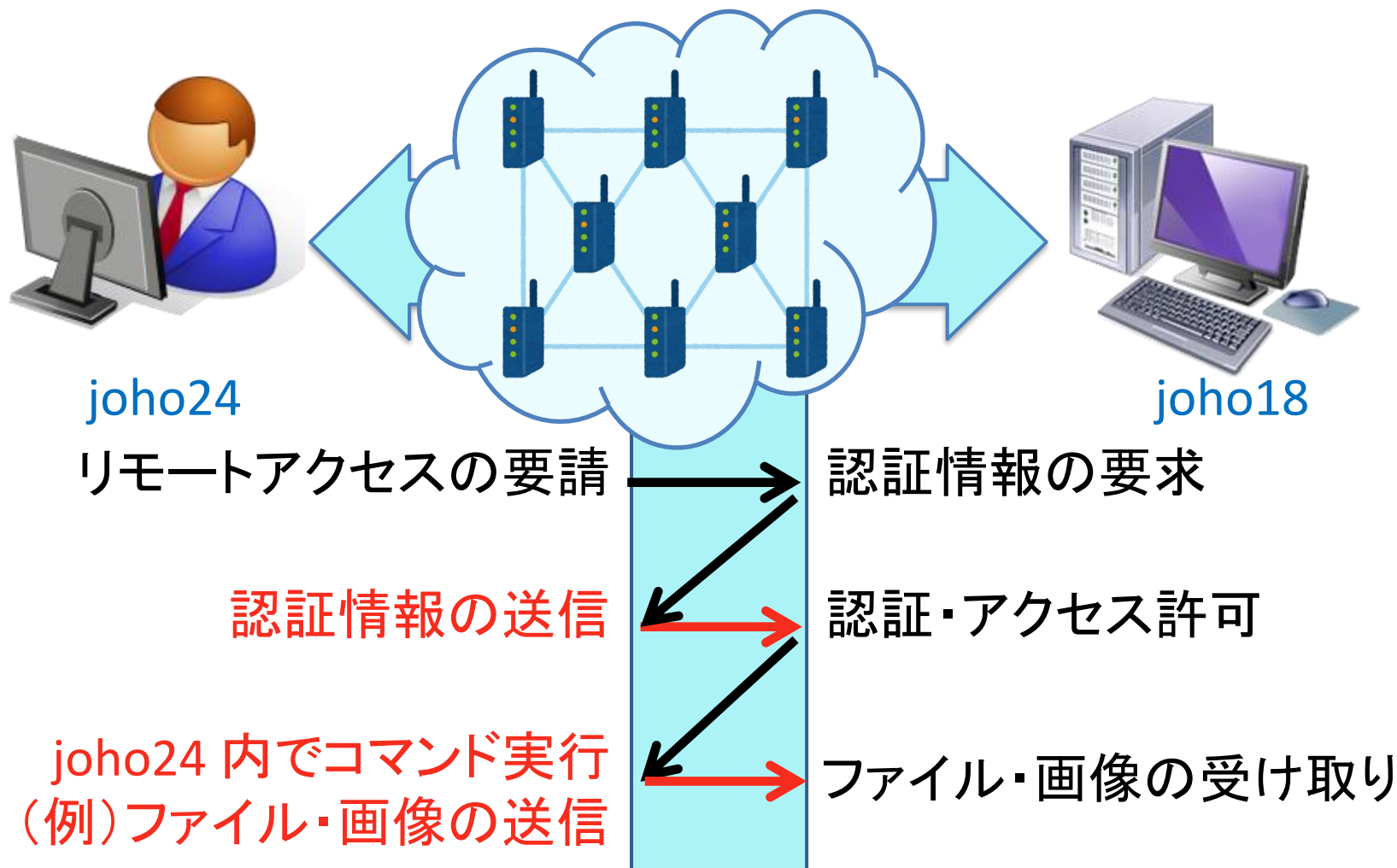
FTP(File Transfer Protocol)

- 古くから利用されるファイル転送用プロトコル
- 使用ポート: 21番
- **通信が暗号化されない(危険・非推奨)**
 - 現在は匿名利用(ユーザー名・パスワードを使用しない)の通信で利用可能
 - Debian アーカイブミラーなど
- このプロトコルを利用する主なコマンド
 - ftp

SSH (Secure Shell)

- 暗号化通信に用いられるリモートアクセス用
プロトコル
- 使用ポート : 22 番
- パケットの暗号化
 - Telnet, FTP などよりも安全に通信可能
 - 暗号化する分 telnet, ftp に比べ通信速度低下
- このプロトコルを利用する主なコマンド
 - ssh, sftp など

リモートアクセスの危険性



パケットが盗聴される危険性がある！

パケット盗聴

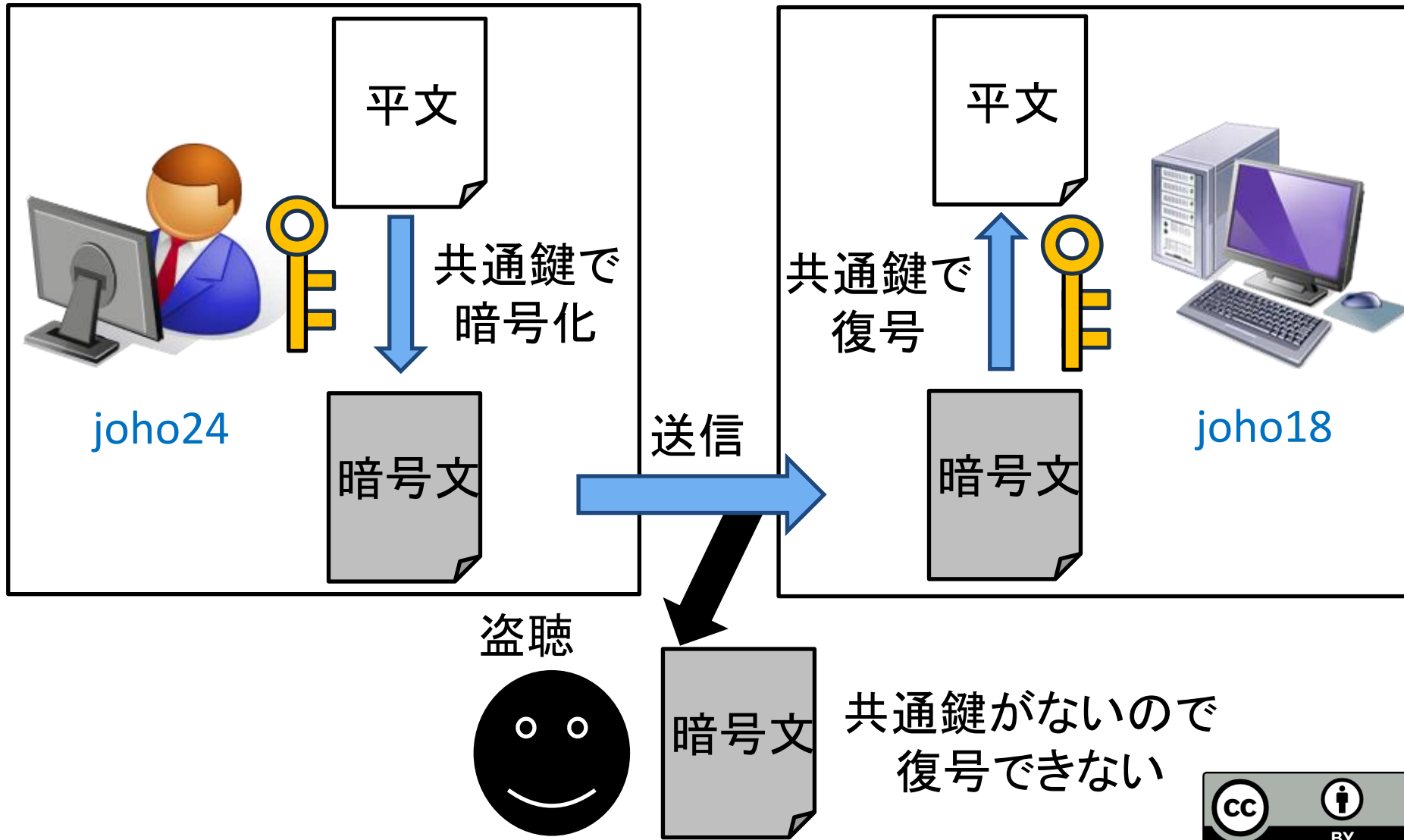
- ネットワーク上のパケット情報を盗み見ること
 - パケットはネットワーク上の様々な計算機を経由
 - いたるところで盗聴される可能性有り
- パケット盗聴への対策
 - 暗号化通信
 - SSH などの通信を暗号化するプロトコルを用いて、パケットが第三者に見られても内容が分からないようにする

暗号化通信

- 共通鍵暗号方式
 - 暗号化と復号に同じ鍵を用いる
- 公開鍵暗号方式
 - 暗号化と復号に「公開鍵」と「秘密鍵」のキーペアを用いる
 - ・ 公開鍵で暗号化されたデータは、その公開鍵に対応する秘密鍵によってのみ復号できる
 - ・ 秘密鍵で暗号化されたデータは、その秘密鍵に対応する公開鍵によってのみ復号できる

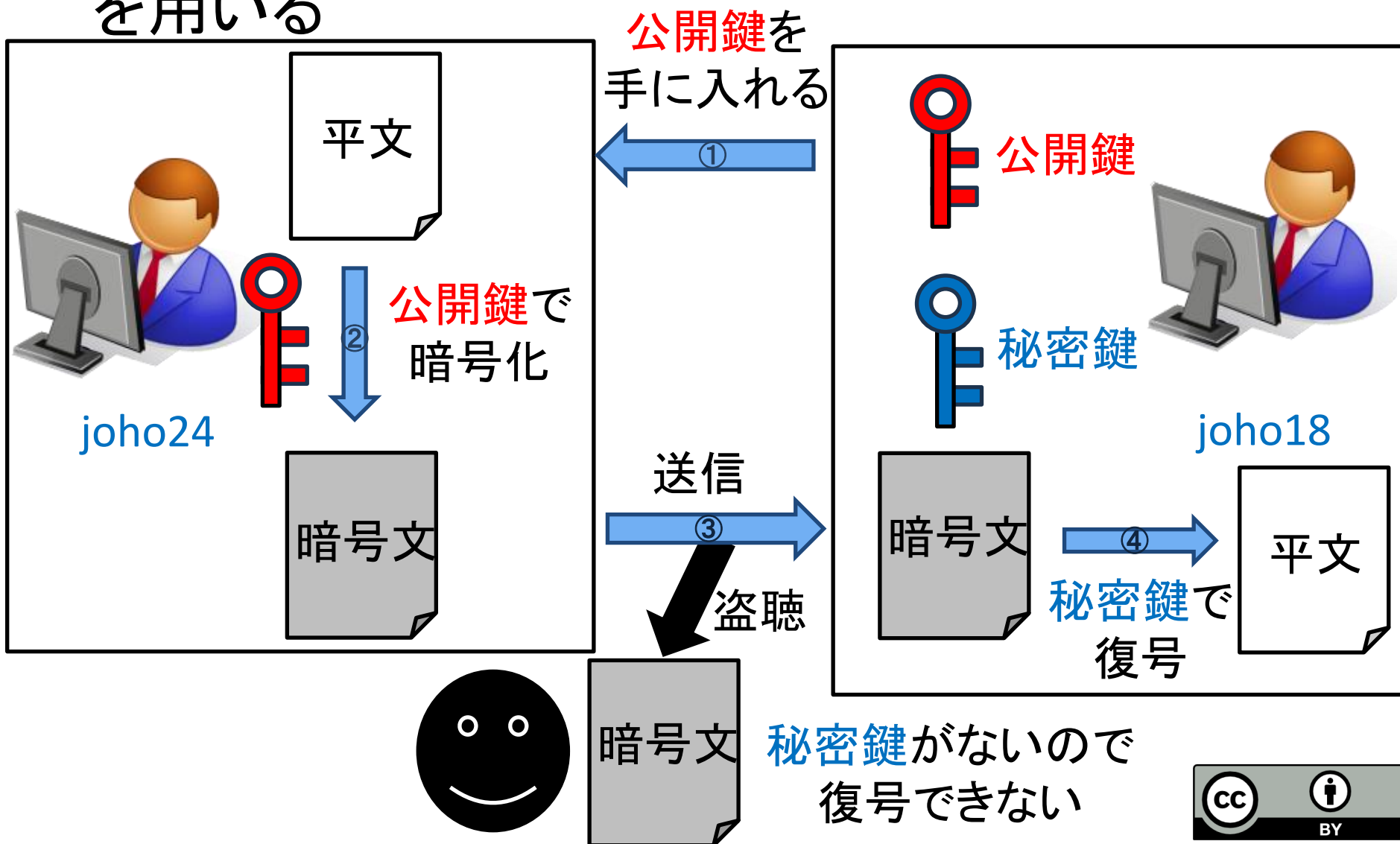
共通鍵暗号方式

- 暗号化と復号に同じ鍵を用いる



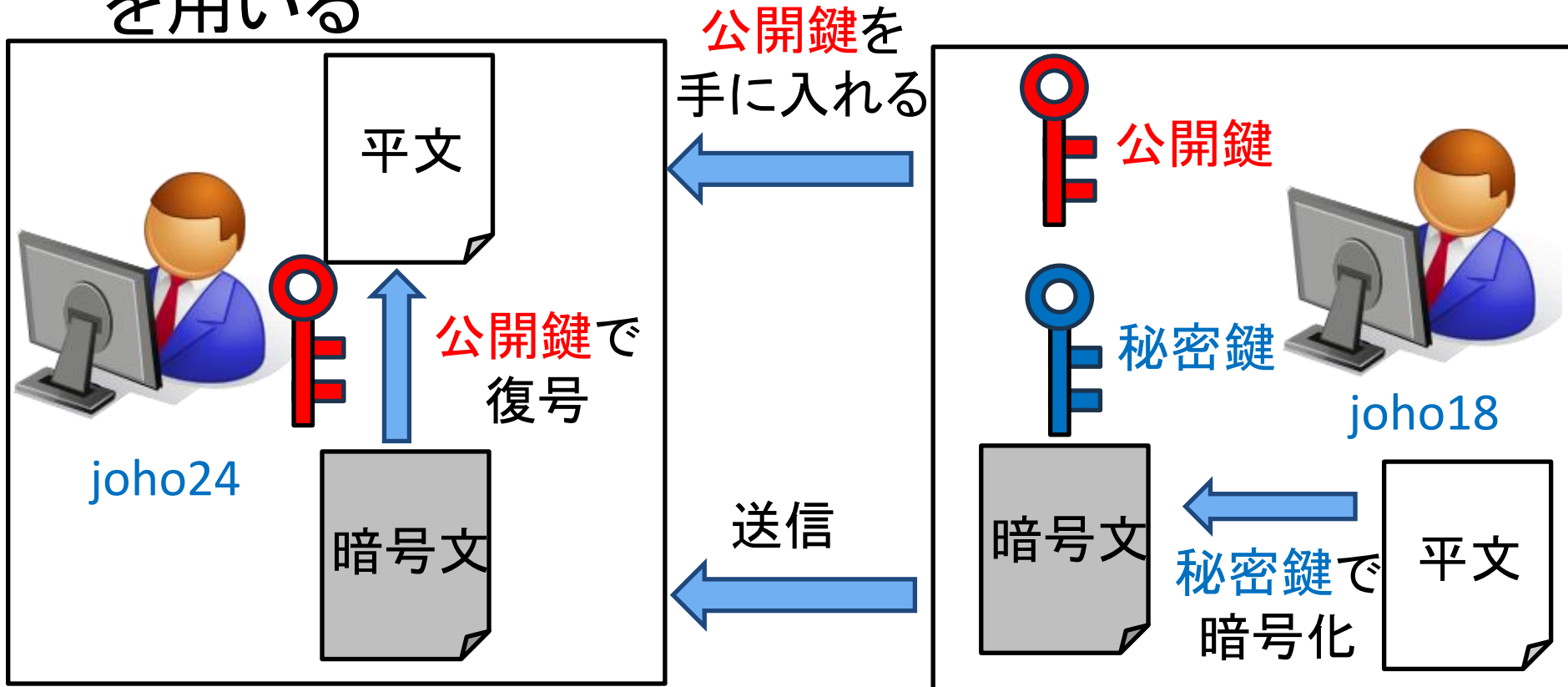
公開鍵暗号方式(復号)

- 暗号化と復号に「公開鍵」と「秘密鍵」のキーペアを用いる



公開鍵秘密鍵の応用：改ざん防止

- 暗号化と復号に「公開鍵」と「秘密鍵」のキーペアを用いる



- 秘密鍵**を用いた暗号文は joho18 にしか作れない
- joho18本人であり, 改ざんされていないことの確認

本日のレクチャー内容

- リモートアクセス
 - リモートログイン・リモートアクセスを用いたファイル転送
 - リモートアクセスで用いられるプロトコル
 - パケット盗聴の危険性
- ネットワークセキュリティ
(ユーザ編, 計算機管理者編)
 - 暗号化通信
 - ポート管理
 - アクセス管理
 - セキュリティホール

INEX のセキュリティの話

- パスワードセキュリティ(第 2 回)
 - 良いパスワードをつけてアカウントをしっかり守る
- ネットワークセキュリティ(今回)
 - ネットワーク利用に関する最低限の防衛策を知る

ネットワークセキュリティの原則

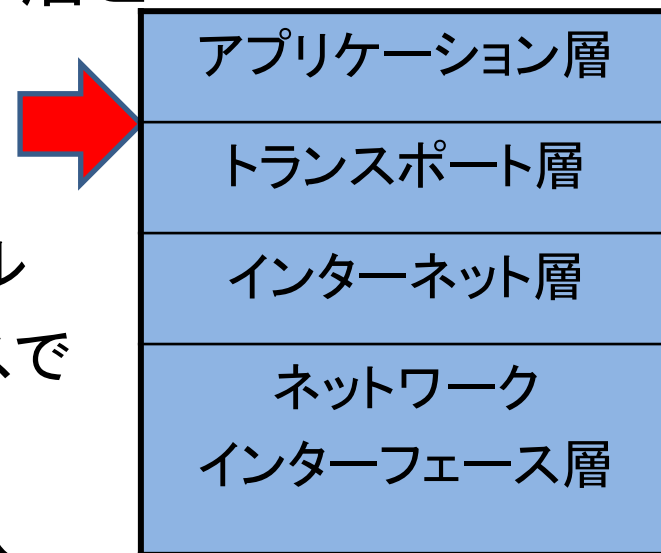
一般ユーザ編 -被害にあわないために-

- 有害データを受け取らないように予防する
 - 不要なソフトウェアのインストール等はしない
 - メールの添付ファイルや URL へ無闇にアクセスしない
- パケット盗聴の予防策を講じる
 - 暗号化通信プロトコル(SSH, **SSL/TLS**) を用いた通信の利用

SSL/TLS

(Secure Socket Layer/Transport Layer Security)

- 転送するデータを暗号化するために利用されるプロトコル
- トランスポート層とアプリケーション層との間に実装
 - HTTPS (HTTP over SSL/TLS)
 - SSL/TLS を利用した HTTP プロトコル
 - オンライン決済など多くのサービスで利用されている
 - 利用者は**SSL サーバ証明書**が導入されたサービスを利用するべき



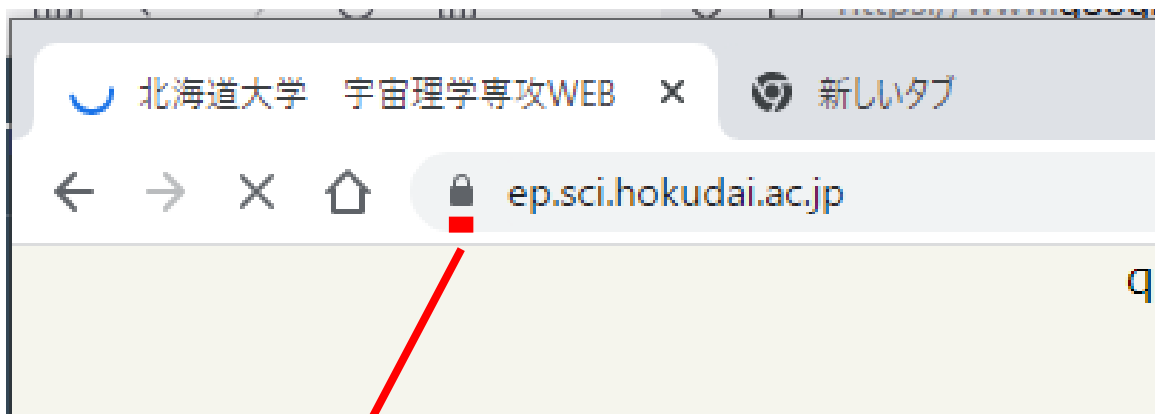
TCP/IP の階層構造

SSL/TLS サーバ証明書

SSL/TLS を利用した通信であることを示す
電子証明書

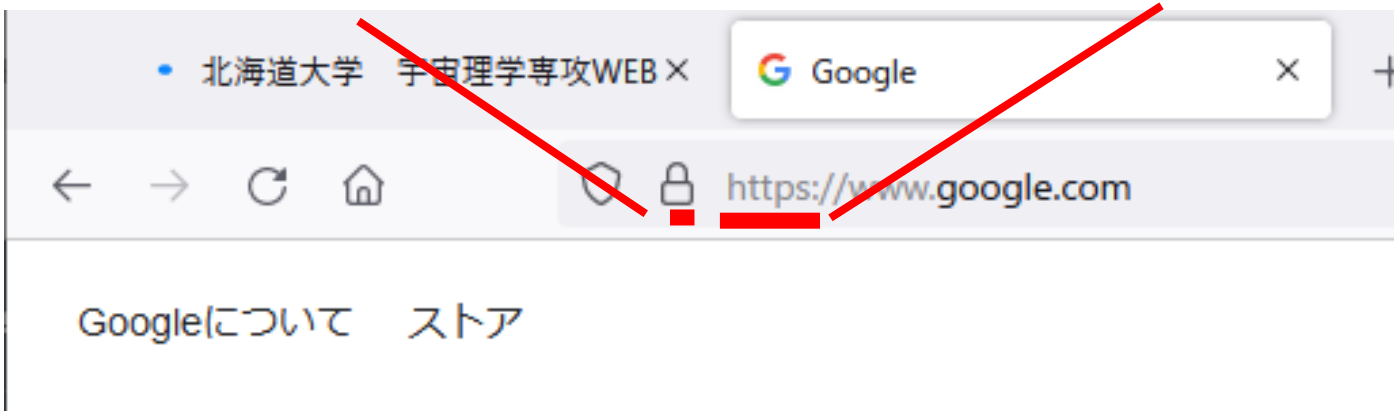
- (信頼できる) 認証局が発行
 - 認証局：電子証明書を発行する機関
 - 国立情報学研究所 など
- 「暗号化証明」と「実在証明」を担う
 - 暗号化証明：適切な暗号化 (SSL/TLS) の利用を証明
 - 実在証明：ページ等を管理する組織等が実在し信頼に足ることを証明
- 通信の「なりすまし」「盗聴」「改ざん」を防ぐ

HTTPS 通信の目印



鍵マーク

https の文字



SSL サーバ証明書 (北大履修登録システム)

grade.academic.hokudai.ac.jp

NII Open Domain CA - G7
RSA

Security Communication
RootCA2

主体者名

国 JP
州/県 Hokkaido
場所 Sapporo
組織 Hokkaido University
組織単位 Gakumubu
共通名 grade.academic.hokudai.ac.jp

発行者名

国 JP
組織 SECOM Trust Systems CO.,LTD.
共通名 NII Open Domain CA - G7 RSA

有効期間

開始日 Thu, 21 Jul 2022 01:33:49 GMT
終了日 Mon, 21 Aug 2023 01:33:49 GMT

主体者代替名

DNS 名 grade.academic.hokudai.ac.jp

公開鍵情報

アルゴリズム RSA
鍵サイズ 2048
冪剰余 65537
母数 94:34:AF:B0:A3:60:DF:F9:D6:D7:6C:AC:63:86:89:EC:46:3A:81:BD:5C:84:5D:6D:1B:C...

grade.academic.hokudai.ac...

NII Open Domain CA - G7
RSA

Security Communication
RootCA2

主体者名

国 JP
組織 SECOM Trust Systems CO.,LTD.
共通名 NII Open Domain CA - G7 RSA

発行者名

国 JP
組織 SECOM Trust Systems CO.,LTD.
組織単位 Security Communication RootCA2

有効期間

開始日 Tue, 15 Dec 2020 08:46:22 GMT
終了日 Tue, 29 May 2029 05:00:39 GMT

公開鍵情報

アルゴリズム RSA
鍵サイズ 2048
冪剰余 65537
母数 E1:DA:27:70:D0:CD:DB:EF:92:CC:C8:90:A5:34:01:E0:AF:CB:C6:65:E7:74:37:CD:46:1...

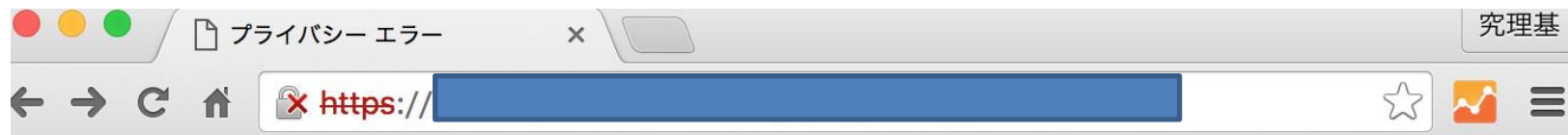
その他の情報

シリアル番号 22:B9:B1:85:87:A6:99:43:B5:EC:36:8F:4C:AF:68:F7
署名アルゴリズム SHA-256 with RSA Encryption
バージョン 3
ダウンロード PEM (証明書) PEM (チェーン)

怪しい SSL サーバ証明書

- 信頼できる認証局が発行したわけではない証明書
 - ページ等を管理する組織等が, 自身を認証局として発行した証明書を用いることがある
 - 信頼に足るページ (管理者, 組織等) であるか, 考えて利用しなければならない!
 - 期限が切れてる = 更新がされていない

怪しそうな SSL サーバ証明書が利用されている例



信頼のおける機関だろうか？

この接続ではプライバシーが保護されません

攻撃者が、**www.ep.sci.hokudai.ac.jp** 上のあなたの情報（パスワード、メッセージ、クレジットカード情報など）を不正に取得しようとしている可能性があります。

NET::ERR_CERT_COMMON_NAME_INVALID

☐ セキュリティに関する事象についての詳細を Google に自動送信します。 [プライバシー ポリシー](#)

詳細設定

セキュリティで保護されたページに戻る



ネットワークセキュリティの原則

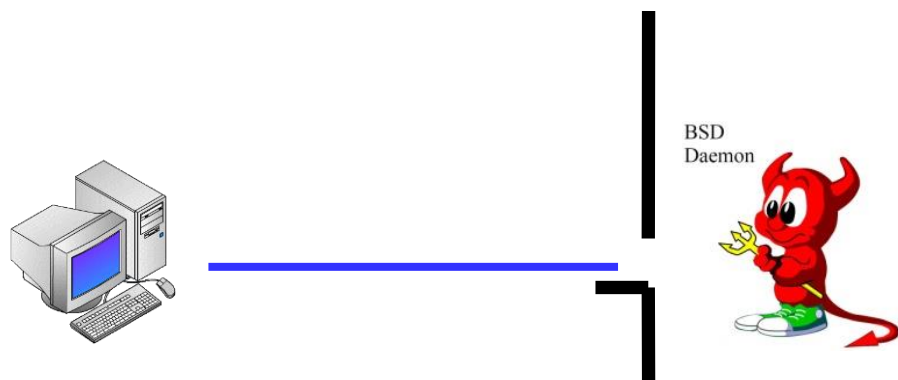
計算機管理者編 -ユーザを守るために-

- 計算機への不正アクセスを未然に防ぐ
 - ネットワーク空間との接点を最小限にする
 - **ポートの管理**
 - 不要なポートを閉める
 - **アクセス制限**
 - 必要外のホストによるアクセスを制限する
 - セキュリティホール (OS やソフトウェアの欠点)をなくす
 - **最新版のソフトウェアを利用する**
 - **最新のセキュリティ情報の取得・確認**

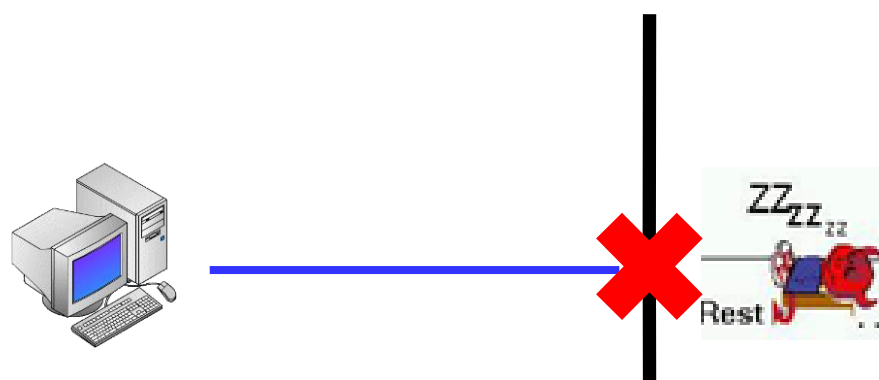
ポートの管理

- 各ポートにはパケットを取り扱う**デーモン**というプログラムがある.
- ポートを開閉するにはデーモンを操作する
 - デーモンの起動・停止

ポートが開いた状態



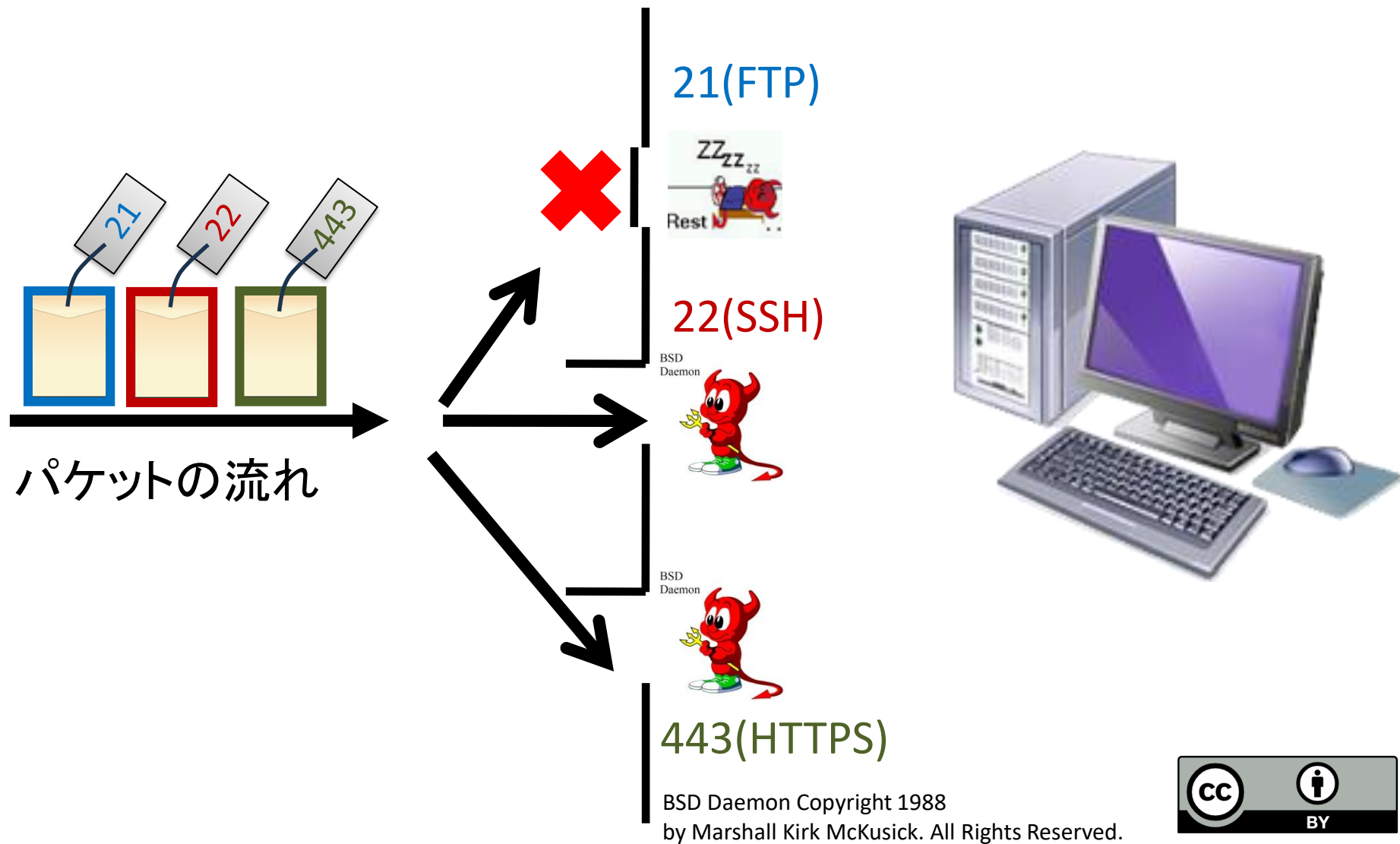
ポートを閉じた状態



デーモン(Daemon) (demon : 闇下じゃないよ！)

- Unix のバックグラウンドで動くプログラム
 - Windows では Windows サービスに相当
- ポートデーモン
 - 各ポートで待機し, パケットの受け取りを担当するデーモン
 - デーモンがない or 停止している場合
パケットは受け取れない
 - ポートの利用を前提としたソフトウェアとともにデーモンがインストールされる

ポートデーモン



デーモンの停止方法

- systemctl コマンド を使ってデーモンを停止
 - systemctl コマンド: デーモン管理用コマンド
 - ssh のデーモンを停止する:

```
(例) # systemctl stop sshd.service
```

 - ただし, この場合には計算機やソフトウェアを再起動するとデーモンは復帰
- デーモンを含む不要なソフトウェアをアンインストール
 - ※不要なものはそもそもインストールしない

アクセス制限

- TCP Wrapper
 - アクセス可能なホストやドメインを設定するソフトウェア
 - アクセスを許可しない
 - /etc/hosts.deny
- 一部のアクセスのみを許可する
 - /etc/hosts.allow
- 記述内容は hosts.allow が優先される

(例) ALL : ALL
(サービス名):(ドメイン名)

(例) sshd : ep.sci.hokudai.ac.jp

最新セキュリティ情報の取得・確認

- セキュリティ対策済みの最新版ソフトウェアをインストール
 - 自動アップデート機能の利用
 - 手動アップデートの実施
- セキュリティアナウンスの注視
 - JPCERT (<https://www.jpcert.or.jp/>)

JPCERT (Japan Computer Emergency Response Team)

注意喚起

最終更新: 2024-06-12

2024	2023	2022	2021	2020	その他の年 ▾
------	------	------	------	------	---------

深刻且つ影響範囲の広い脆弱性などに関する情報を告知するための文書です。

情報システムや制御システムに関わる端末やネットワークの構築・運用管理業務、組織内CSIRT業務、セキュリティ関連業務などに関与する担当者、技術者、研究者等を対象としています。

※2018年1月分から注意喚起のページ表示デザインが変わりました。

<注意>

以下の各文書で紹介しているソフトウェア、バージョン、URL等は、各文書の発行時点のものであり、変更されている可能性があります。

2024		
公開日	注意喚起内容	テキスト (PGP署名付き)
2024-06-12	2024年6月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	2.66KB
2024-05-15	2024年5月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	3.51KB
2024-05-15	Adobe AcrobatおよびReaderの脆弱性 (APSB24-29) に関する注意喚起 (公開)	4.06KB

JPCERT (Japan Computer Emergency Response Team)

2024年6月マイクロソフトセキュリティ更新プログラムに関する注意喚起

最終更新: 2024-06-12

✕ ポスト

✉ メール

JPCERT-AT-2024-0012

JPCERT/CC

2024-06-12

I. 概要

マイクロソフトから同社製品の脆弱性を修正する2024年6月のセキュリティ更新プログラムが公開されました。これらの脆弱性を悪用された場合、リモートからの攻撃によって任意のコードが実行されるなどの可能性があります。マイクロソフトが提供する情報を参照し、早急に更新プログラムを適用してください。

マイクロソフト株式会社

2024年6月のセキュリティ更新プログラム

<https://msrc.microsoft.com/update-guide/releaseNote/2024-Jun>

マイクロソフト株式会社

2024年6月のセキュリティ更新プログラム (月例)

<https://msrc.microsoft.com/blog/2024/06/202406-security-update/>

Debian GNU/Linux における セキュリティホール対応

- パッケージはこまめに更新される
- ソフトウェアアップデート用コマンド
 - apt update
 - 最新版のパッケージ情報を取得(セキュリティ対策も含む)
 - apt upgrade
 - 最新版のダウンロード・インストール

まとめ1: リモートアクセス

- リモートアクセス
 - ローカルホストからリモートホストへのネットワークを経由した接続・操作
 - ネットワークを経由したファイル転送
 - 公開鍵暗号方式を用いた通信
- リモートアクセス用プロトコル
 - Telnet, FTP, SSH など
 - 通信内容が暗号化されるプロトコルであるSSH の使用を心がける

まとめ2: ネットワークセキュリティ

ネットワークを安全に利用するために気をつけること！

ユーザ

- 暗号化通信を利用する
 - ネットワーク上における盗聴を防ぐ
- 有害なデータの受け取りの防止
 - 添付ファイル, URL などに無闇にアクセスしない

管理者

- 不要なソフトウェアやポートデーモンの削除・停止
- アクセス制限の設定
- セキュリティの向上: セキュリティホールへの対応
 - 最新のセキュリティ情報の取得
 - ソフトウェアのアップデートを実行



本日の実習

- 最新のソフトウェアアップデートを実行
- リモートログイン・ファイル転送
 - 他の情報実験機にログイン・ファイル転送
- ネットワークセキュリティ入門
 - 他の情報実験機からのアクセスを制限

参考文献

- ネットワークセキュリティ, INEX 2022
(2022/07/01)
 - <http://www.ep.sci.hokudai.ac.jp/~inex/y2022/0701/>
- JPCERT CC
 - <https://www.jpcert.or.jp/>
- ファイアウォール&ネットワークセキュリティ実線
テクニック-すべてのPC UNIX ユーザとサイト管理
者に贈る最強セキュリティガイド, 技術評論社,
2001 年 10 月
- 名寄市の新しいカントリーサインが決定しました,
北海道名寄市
 - <http://www.city.nayoro.lg.jp/section/kikaku/prkeql00000q4bo.html>

参考文献

- カントリーサイン(50音順一覧), 北の道ナビ
 - <http://northern-road.jp/discover/sign/aiueo.html>
- SSL/TLS とは・SSL サーバ証明書とは,
GlobaSign GMO INTERNET GROUP
 - <https://jp.globalsign.com/service/ssl/about>
- 認証局【CA】Certificate Authority / CA局, IT
用語辞典 e-Words
 - <http://e-words.jp/w/%E8%AA%8D%E8%A8%BC%E5%B1%80.html>
- メール配送の仕組み, INEX 2014
(2014/07/04)
 - <http://www.ep.sci.hokudai.ac.jp/~inex/y2014/0704/>

参考文献

- ネットワークセキュリティ, INEX 2020
(2020/05/29)
 - <http://www.ep.sci.hokudai.ac.jp/~inex/y2020/0529/>
- R.L. Rivest, A. Shamir, and L. Adleman. (1978)
A Method for Obtaining Digital Signatures and
Public-Key Cryptosystems. *Association for
Computing Machinery*, 21, (2) 120–126.
<https://doi.org/10.1145/359340.359342>

付録: RSA暗号

- RSA暗号はR.L. **R**ivest, A. **S**hamir, and L. **A**dlemanの3人によって考案された暗号様式
 - 世界初の公開鍵暗号であり現代でも広く使われている
 - RSA は3人の著者の頭文字から
- 基本原理はフェルマーの小定理と2元の中国剰余定理(Chinese remainder theorem)を利用したもの
 - フェルマーの小定理: $a^p \equiv a \pmod{p}$... p は素数
 - 中国剰余定理(2元): n, m が互いに素の時以下を満たす整数 N が0以上 nm 未満に1つだけ存在する

$$N \equiv a \pmod{n}$$

$$N \equiv b \pmod{m}$$

付録: RSA暗号

- RSAの暗号化/複合化の概要

<準備>

桁が大きな素数の組 P, Q を決め, $P-1$ と $Q-1$ の最小公倍数を L とします. 次に L と互いに素な L 未満の E を決め, $ED = 1 \pmod{L}$ となるような正の整数 D を求めます. 後の計算過程より E の値が小さいほど暗号化の処理時間は短くなります.

<暗号化> (E と N が公開鍵)

送信したい平文を M , $N(=PQ)$ とすると M の暗号化は

$$C = M^E \pmod{N} \quad \cdots C \text{ は暗号文}$$

<復号化> (D と N が秘密鍵)

暗号化した M の復号化は

$$M' = C^D \pmod{N} \quad \cdots M' \text{ は復号文}(=M)$$

付録: RSA暗号

- 逆方向の計算の難しさ

- ＜べき乗関数の逆計算の難しさ＞

E と N から平文 M を推測しようとする、 E のべき乗関数のmodの逆計算をすることになり、この計算は大変難しい。

- ＜大きな素数2つの合成数 N を素因数分解する難しさ＞

また復号に必要な秘密鍵 D は、 L が分かれば単純なmodの逆計算をすることで求めることが可能。しかし L を求めるには N を素因数分解する必要がある。

P 素因数分解の演算処理は基本的に総当たりで約数を見つけていく方法しかなく、現在 P , Q には約300桁の素数が使われている。これを素因数分解するのは難しい。