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 (2018/06/22)

北海道大学 大学院理学院

宇宙理学専攻 博士後期課程 3 年

村橋 究理基

CC BY

研究室の日常

- メールサーバからメールを取得，閲覧
- 計算サーバにアクセスし，
  数値シミュレーションを実行
- 遠方にいる研究者とテレビ会議
- 観測データの取得…など

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

- **リモートアクセス**

CC BY

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

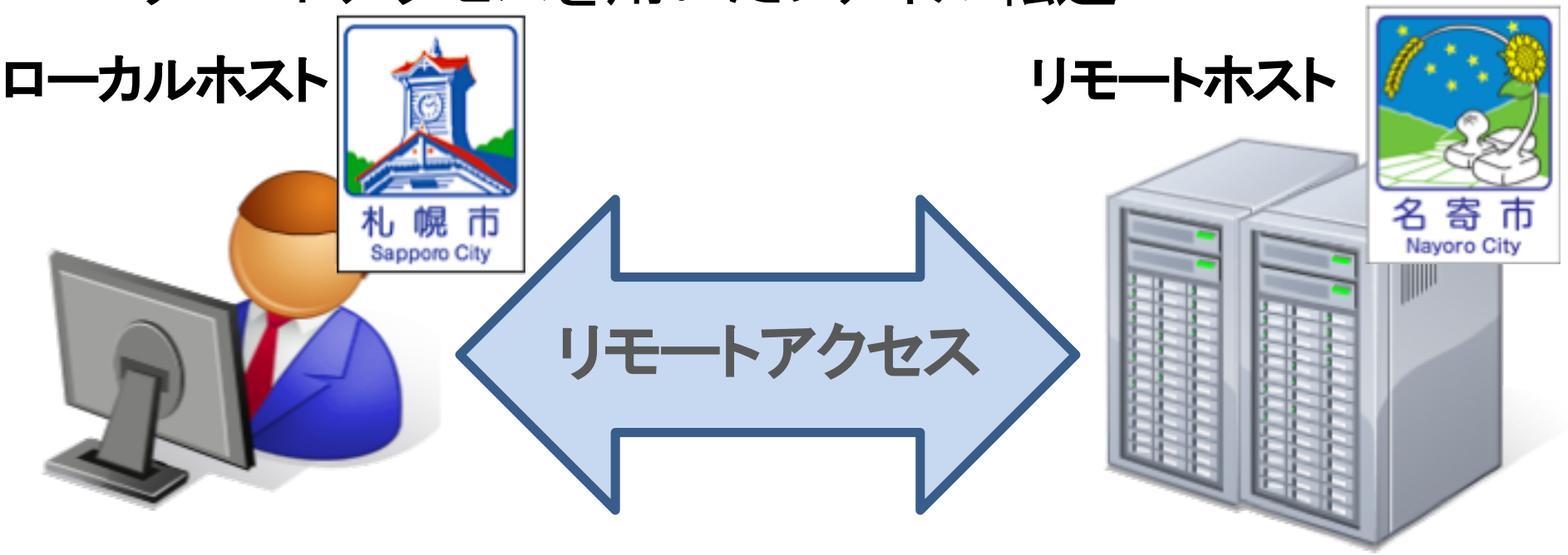
CC BY

リモートアクセス

CC BY

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



http://northern-road.jp/discover/sign/aiueo.html
http://www.city.nayoro.lg.jp/section/kikaku/prkeql000000q4bo.html

CC BY

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

CC BY

リモートログインのイメージ

ホスト名: joho18
アカウント名: hoge

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: joho24
アカウント名: hero

```
hoge@joho18:~ $ ssh  hero@joho24
hero@joho24's  password:
```

CC BY

リモートログインのイメージ

ホスト名: joho18
アカウント名: hoge

ログインパスワードを送信

ログインを許可

ホスト名: joho24
アカウント名: hero

```
hoge@joho18:~ $ ssh  hero@joho24
hero@joho24's  password: (パスワードを入力)
....
hero@joho24:~ $
```

CC BY

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
  - scp

CC BY

リモートアクセスを用いたファイル転送のイメージ

ホスト名: joho18
アカウント名: hoge

scp コマンドを用いて，
ファイル転送を要請

ログインパスワードを要求

ホスト名: joho24
アカウント名: hero

```
hoge@joho18:~ $ scp hero@joho24:/home/hero/file.txt ./
hero@joho24's  password:
```

CC BY

リモートアクセスを用いた ファイル転送のイメージ

ホスト名: joho18
アカウント名: hoge

ログインパスワードを送信

ファイル転送の実行

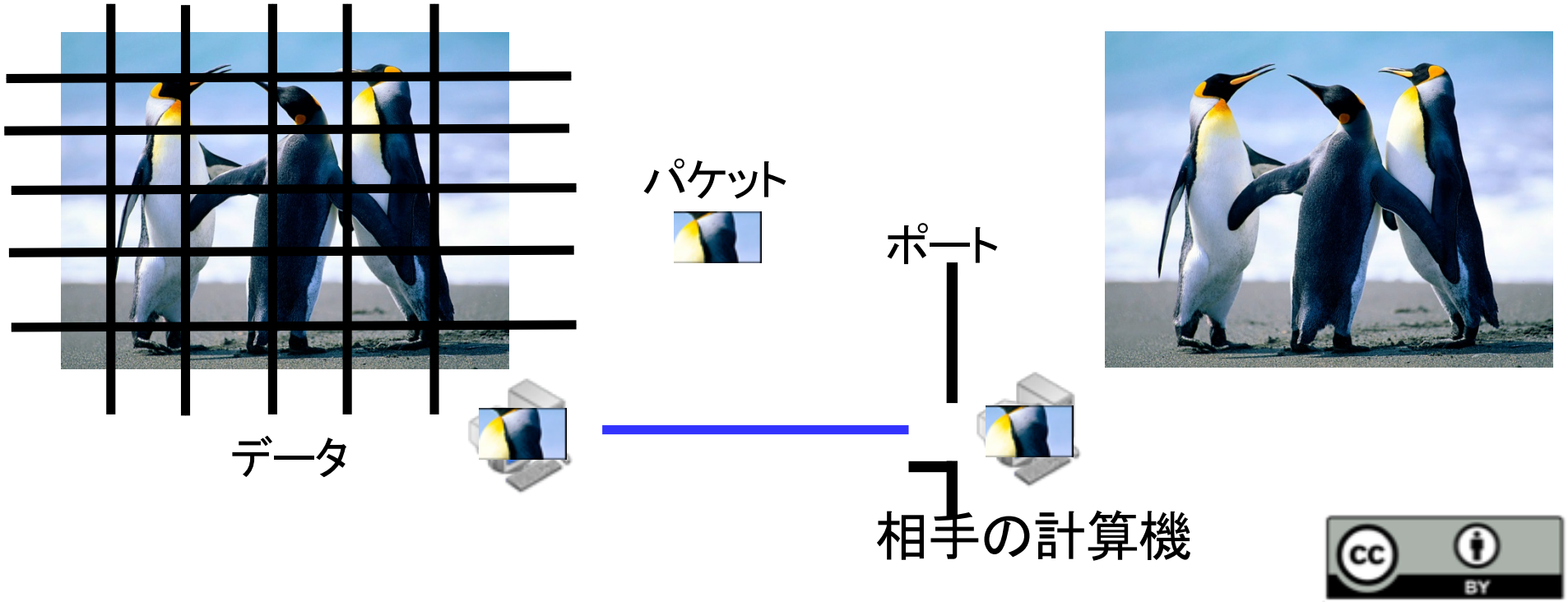
ホスト名: joho24
アカウント名: hero

```
hoge@joho18:~ $ scp hero@joho24:/home/hero/file.txt ./
hero@joho24's  password: (パスワードを入力)
file.txt                    100%    7311     7.3KB/s    00:00
hoge@joho18:~ $ ls
file.txt
```

CC BY

ファイル転送の手順 (第 4 回の復習)

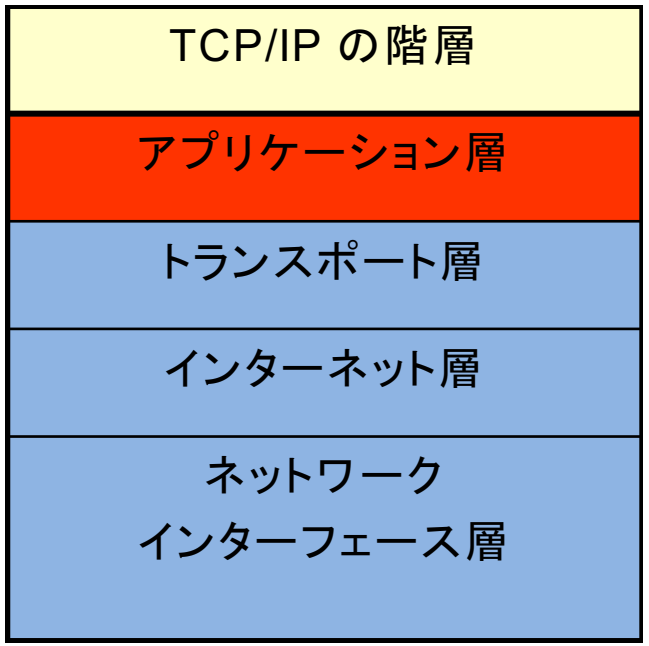
- データをパケットに分割し，相手の計算機のポートへ転送，パケット転送完了後に結合
  - ネットワーク通信は**プロトコル**(通信規約)に従う



CC BY

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)



CC BY

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

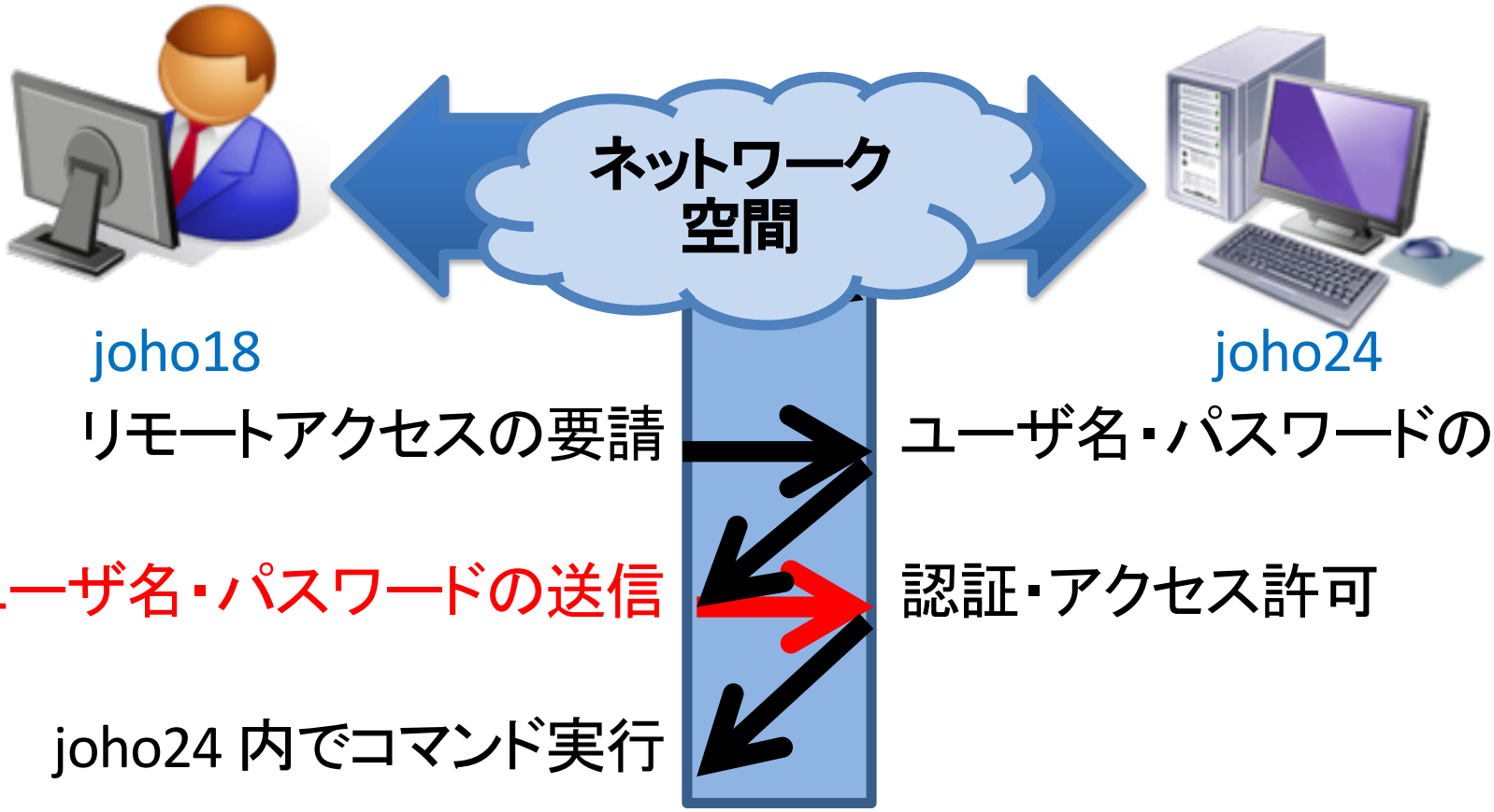
CC BY

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)**
  - 現在は匿名利用前提の通信で利用可能
    - 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

CC BY

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！

CC BY

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

CC BY

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, scp など

CC BY

ネットワークセキュリティ
-安全にネットワークを利用するために-

CC BY

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

CC BY

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
    - 日本年金機構, JTB の個人情報流出の事例
    - 実例 : http://www.chunichi.co.jp/s/article/2016060490221806.html
- 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

CC BY

社会

ツイート シェア 0

2016年6月4日 22時18分

ＡＶ閲覧しＰＣ乗っ取られる　福井、池田町議会事務局

福井県池田町は４日、「議会事務局のパソコンが乗っ取られ、議会関係のデータを抜き取られた可能性がある」と発表した。議会事務局長の５０代男性がアダルトサイトを閲覧し、遠隔操作されたという。県警もファイルの流出がないかを調べている。

町によると、事務局長は３日にアダルトサイトを複数回閲覧。画面に「あなたのパソコンはウイルスに感染しています」とのメッセージと、連絡先として「０５０」で始まる電話番号が表示された。

事務局長はこの番号に電話し、片言の日本語を話す男の声による指示通りにパソコンを操作して、遠隔操作ファイルをインストール。約１時間半にわたって電話がつながった状態で遠隔操作される状況を見ていたという。

町によると、このパソコンに入っていたのは、議員の個人情報や議案など一般に公開しているデータがほとんどだが、流出すると問題となるファイルが入っていた可能性も否定できないという。今のところ役場に６０台ほどある他のパソコンへの侵入などは確認されていない。

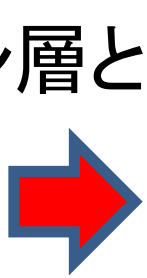
杉本博文町長と佐野和彦町議長は４日、連名の文書で謝罪した。事務局長は「不適切なサイトを閲覧したうえ、その後の対応も誤り、反省している」と話しているという。

（中日新聞）

https://web.archive.org/web/20160625093413/http://www.chunichi.co.jp/s/article/2016060490221806.html : 2016/05/25 web archive, 2017/06/20 閲覧

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中間に実装
  - 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でしばしば利用されている
    - SSL サーバ証明書が導入されたサービスを利用することが重要



CC BY

SSL 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

CC BY

HTTPS 通信の目印

CC BY

SSL サーバ証明書

- 北大の履修登録システムにおけるサーバ証明書

この証明書は以下の用途に使用する証明書であると検証されました:

SSL クライアント証明書

SSL サーバー証明書

発行対象

一般名称 (CN)	grade.academic.hokudai.ac.jp
組織 (O)	<証明書に記載されていません>
部門 (OU)	Domain Control Validated
シリアル番号	75:AD:FE:36:1D:C9:F1:E3:2A:AE:35:D6

発行者

一般名称 (CN)	GlobalSign Domain Validation CA - SHA256 - G2
組織 (O)	GlobalSign nv-sa
部門 (OU)	<証明書に記載されていません>

証明書の有効期間

発行日	2017年5月16日
有効期限	2018年7月9日

証明書のフィンガープリント

SHA-256 フィンガープリント	F6:28:29:1D:83:68:1C:C6:31:65:86:5F:64:F8:F3:8E: 45:D4:B2:43:E9:BD:78:E6:4A:12:3A:25:5C:8E:35:17
SHA1 フィンガープリント	BF:91:84:E8:9D:45:3C:CE:0B:D9:BC:3C:7F:65:22:6D:01:84:34:8D

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！

CC BY

怪しそうな SSL サーバ証明書が利用されている例

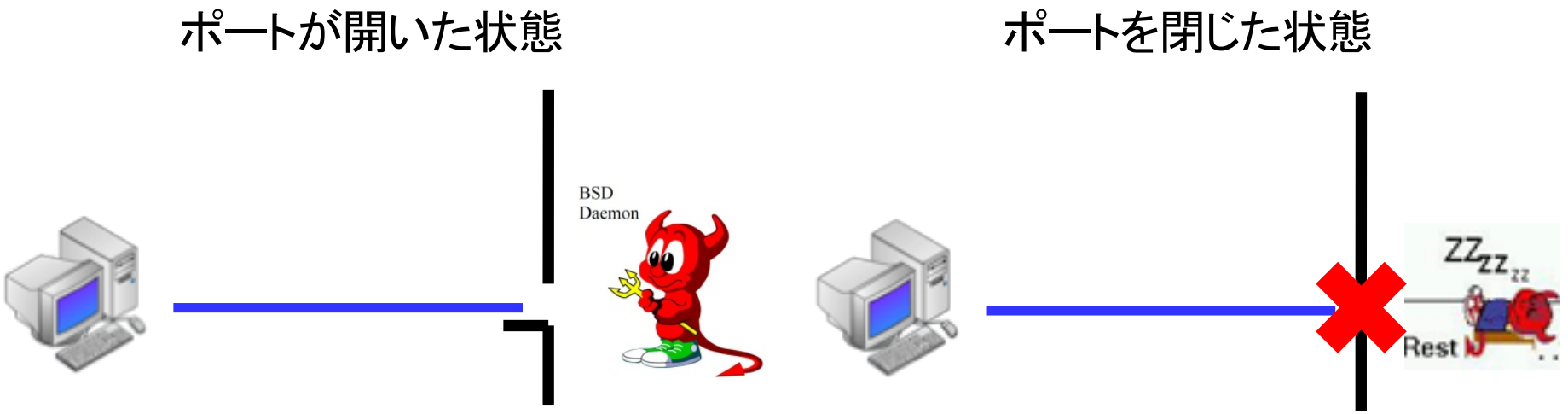
ネットワークセキュリティの原則
計算機管理者編 -ユーザを守るために-

- 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
    - **最新セキュリティ情報の取得・確認**

CC BY

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**がいる
- ポートを開閉するにはポートのデーモンを操作する
  - デーモンの起動・停止



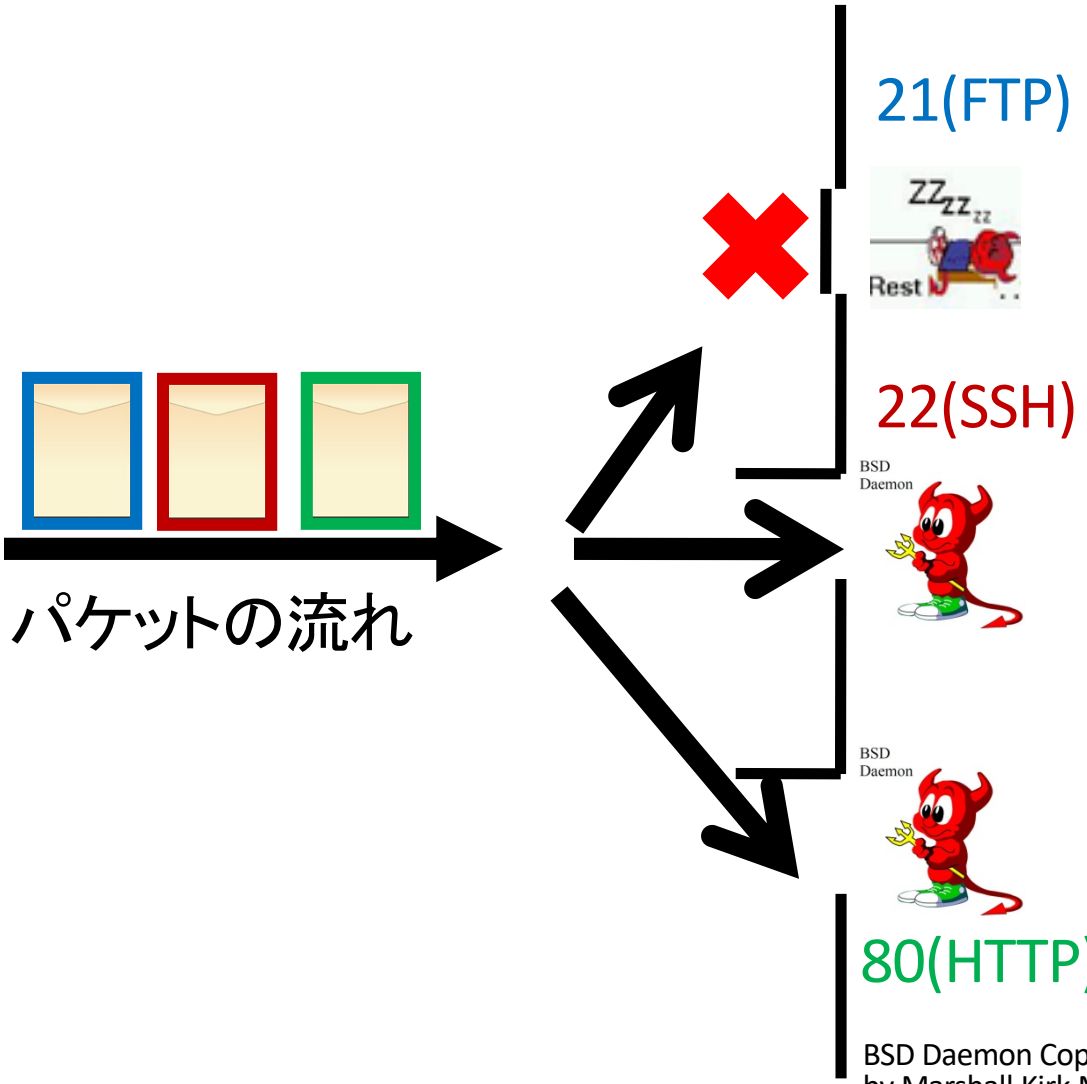
CC BY

デーモン(Daemon) (demon : 閣下じゃないよ！)

- 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
    - デーモンがいない 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

CC BY

ポートデーモン



BSD Daemon Copyright 1988
by Marshall Kirk McKusick. All Rights Reserved.

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，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

CC BY

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
  - 不要なアクセスを許可しない
    - /etc/hosts.deny

```
(例)　　ALL : ALL
(サービス名):(ドメイン名)
```

  - 一部のアクセスのみを許可する
    - /etc/hosts.allow

```
(例)　　sshd : ep.sci.hokudai.ac.jp
```

  - 記述内容は hosts.allow が優先される

CC BY

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/)

CC BY

日本経済新聞
2017年6月20日（火）

ぴあ、15万件情報流出か　ソフトの脆弱性を突く

2017/4/25 22:07

共有 保存 印刷 その他

チケット販売大手のぴあが運営を受託するチケット販売サイトからクレジットカード番号など15万件の個人情報が流出した可能性のあることが25日、判明した。企業で広く使われるサイト構築用ソフトの欠陥（脆弱性）を狙ったサイバー攻撃を受けていたという。カードが不正に使われる被害も確認され、同社は警視庁に相談している。

３月以降、企業などを狙った同様の攻撃が相次いでおり、情報処理推進機構（ＩＰＡ）などは対策を急ぐよう呼びかけている。

ぴあは３月、インターネット上の書き込みから個人情報が流出した恐れがあることを把握した。調査の結果、同社がサイトの開設と運用を委託したソフト開発会社のサーバーが不正接続されたことが原因と分かった。

不正接続は「アパッチ・ストラッツ２」というサイト構築用ソフトのセキュリティー上の欠陥を突いた。同ソフトは企業などの間で広く使われているが、３月になってＩＰＡなどがセキュリティー上の欠陥と対策を公表し、修正用のプログラムの配布も始まっていた。

http://www.nikkei.com/article/DGXLASDG25H9S_V20C17A4CR8000/ : 2017/04/25 掲載, 2017/06/20 閲覧

日本経済新聞
2017年6月20日（火）

ぴあ、15万件情報流出か　ソフトの脆弱性を突く

2017/4/25 22:07

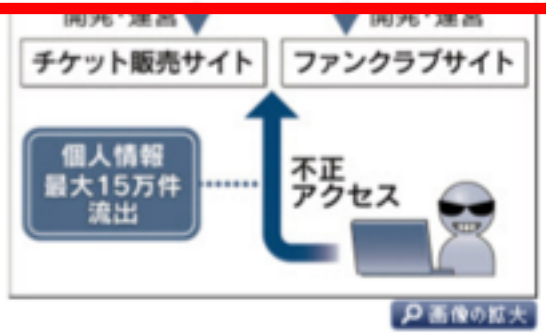
チケット販売
ど15万件の個人
ト構築用ソフト
使われる被害も

3月以降、企
でおり、情報処
急ぐよう呼びか

ぴあは3月、
人情報が流出し
の結果、同社が
ト開発会社のサーバーが不正接続されたことが原因
と分かった。

不正接続は「アパッチ・ストラッツ2」というサイト構築用ソフトのセキュリティー上の欠陥を突いた。同ソフトは企業などの間で広く使われているが、3月になってIPAなどがセキュリティー上の欠陥と対策を公表し、修正用のプログラムの配布も始まっていた。

不正接続は「アパッチ・ストラッツ2」というサイト構築用ソフトのセキュリティー上の欠陥を突いた。同ソフトは企業などの間で広く使われているが、3月になってIPAなどがセキュリティー上の欠陥と対策を公表し、修正用のプログラムの配布も始まっていた。



http://www.nikkei.com/article/DGXLASDG25H9S_V20C17A4CR8000/ : 2017/04/25 掲載, 2017/06/20 閲覧

JPCERT (Japan Computer Emergency Response Team)

サイバーインシデントがなくなるその日まで

お問い合わせ　採用情報　サイトマップ　English

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

検索

最新情報を取得 (RSS | メーリングリスト)　HTTPS　モバイル

インシデントとは | 緊急情報を確認する | JPCERT/CCに依頼する | 公開資料を見る | 情報を受け取る | コラム&ブログ | JPCERT/CCについて

HOME > 緊急情報を確認する > 注意喚起

印刷用レイアウト　印刷

緊急情報を確認する
- 注意喚起
- インターネット定点観測
- JVN
- 脆弱性対策情報

おすすめ情報
- 平成 30 年度「制御システムセキュリティカンファレンス2019 運営業務」に関する入札のご案内
- 分析センターだより「攻撃グループBlackTechが使うマルウエアPLEADダウンローダ(2018-05-28)」
- 分析センターだより「プラグインをダウンロードして実行するマルウエアTSCookie(2018-03-01)」
- ランサムウエア対策特設サイト

注意喚起

最終更新: 2018-06-13

2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010 | 2009 | 2008 | 2007 | 2006 | 2005 | 2004年以前

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。

2018

公開日	注意喚起内容	テキスト (PGP署名付き)
2018-06-13	2018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)	6.02KB
2018-06-08	Adobe Flash Player の脆弱性 (APSB18-19) に関する注意喚起 (公開)	5.48KB
2018-05-15	メールクライアントにおける OpenPGP および S/MIME のメッセージの取り扱いに関する注意喚起 (公	3.71KB

JPCERT 注意喚起 (https://www.jpcert.or.jp/at/2018.html) 2018/06/21 閲覧

Debian GNU/Linux における セキュリティホール対応

- 堅牢なパッケージ管理システムでソフトウェアの安全性を審査している
- 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

CC BY

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
- 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

CC BY

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

CC BY

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

CC BY

参考文献

- ネットワークセキュリティ, INEX 2017 (2017/06/21)
  - http://www.ep.sci.hokudai.ac.jp/~inex/y2015/0617/lecture/pub/
- 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/prkeql000000q4bo.html

CC BY

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
- AV閲覧しPC乗っ取られる 福井、池田町議会事務局, 中日新聞, 2016/06/04
  - http://www.chunichi.co.jp/s/article/2016060490221806.html
- ぴあ、15万件情報流出か　ソフトの脆弱性を突く, 日本経済新聞, 2017/04/25
  - http://www.nikkei.com/article/DGXLASDG25H9S_V20C17A4CR8000/
- SSL/TLS とは・SSL サーバ証明書とは, GlobaSign GMO INTERNET GROUP
  - https://jp.globalsign.com/service/ssl/knowledge/
- 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

CC BY