A-2.
標的型攻撃を受けているらしいとの連絡があった時の調査と対応

東海大学
東　永祥

このセッションの目的

標的型サイバー攻撃を受けているとメール連絡を受けた時の「信憑性調査」と、「標的型サイバー攻撃の手法」を実習を通して学ぶ

（1）メールヘッダーの見方を理解し、通報メールの信憑性を判断できる
（2）標的型サイバー攻撃の流れ・手法を理解する

標的型サイバー攻撃の流れ

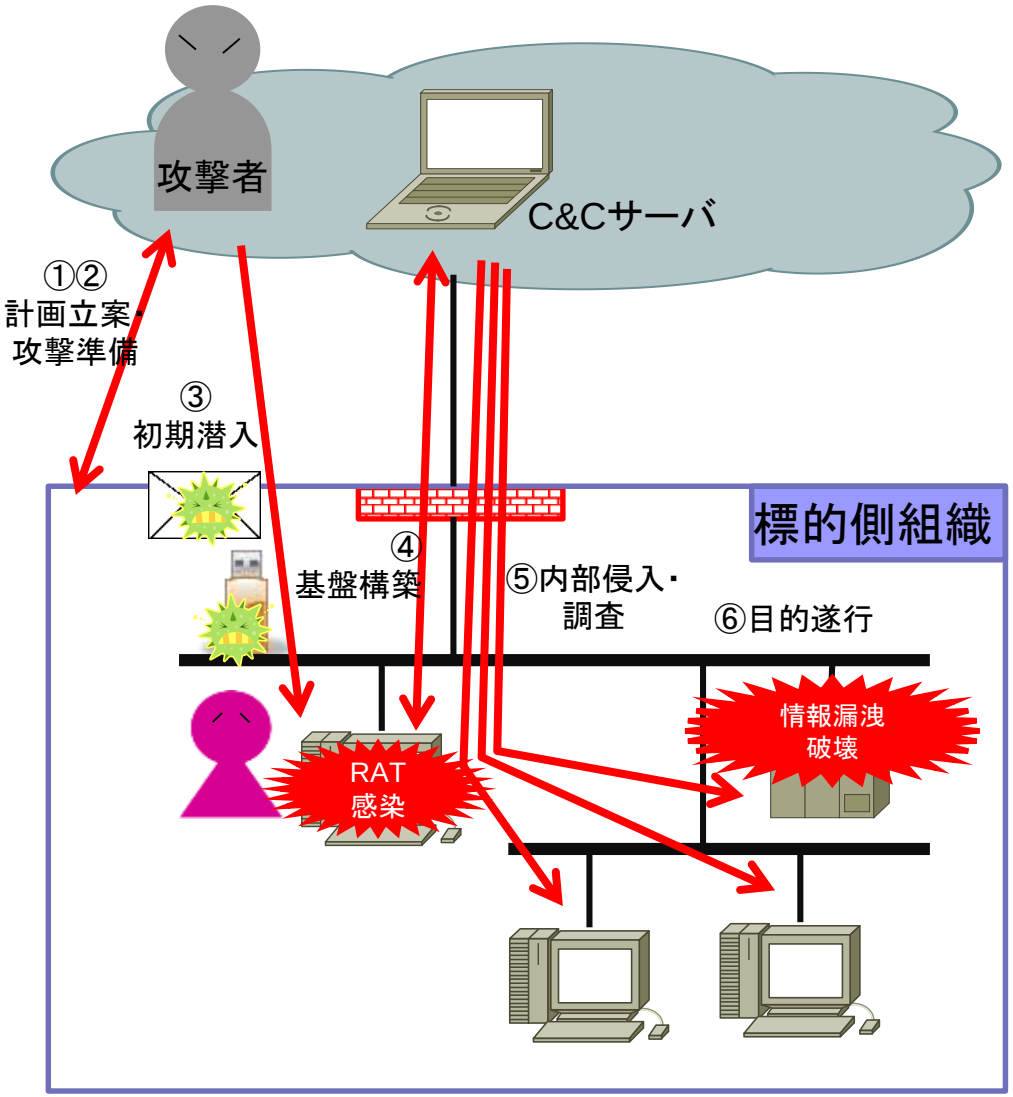
① 計画立案
② 攻撃準備
標的となる組織の情報を収集、準備を行う。

③ 初期潜入
標的型メール等でウィルス(主にRAT)を送信、感染。SNSやUSBメモリを使う場合も

④ 基盤構築
RAT経由で各種ハッキングツールを送信

⑤ 内部侵入 調査
④のツールを用いてさらに内部システムの侵入を行い調査を進める

⑥ 目的遂行
⑦ 再侵入
最終目的の達成



1. 通報メールの信憑性調査

メールの信憑性調査の必要性

- 標的型サイバー攻撃は、メール等を利用して「初期潜入」する
- 標的型サイバー攻撃を受けている可能性を知らせる外部からの通報も、メールで送られてくることが多い
  - 「通報メール自体が標的型サイバー攻撃なのでは・・・？」と思うのは当然
  - 添付ファイルのあるメールであれば尚更
- メールの本文やヘッダー情報から、通報の信憑性を調査する
- 参考
  - 標的型攻撃メールの傾向と見分け方～サイバーレスキュー隊（J-CRAT）の活動を通して（https://www.ipa.go.jp/files/000052612.pdf）
  - IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」（https://www.ipa.go.jp/files/000043331.pdf）

標的型攻撃メールの特徴

項目	特徴
内容	1．知らない人からのメールだが、開封せざるを得ない内容 （例）・大学への問い合わせを装ったメール ・大学への苦情を装ったメール
	2．これまで届いたことがない、公的機関からのお知らせ （例）・情報セキュリティに関する注意喚起 ・製品やサービスの案内
送信者	1．フリーメールアドレスからの送信
	2．送信者のメールアドレスが署名と異なる
本文	1．言い回しが不自然な日本語
	2．署名の記載内容がおかいし（該当部門が存在しない、等）
添付ファイル	1．添付ファイルがある
	2．実行形式のファイル（exe / scr / jar /cpl 等）
	3．ショートカットファイル（lnk / pif / url）
	4．拡張子と異なるファイルアイコン
	5．ファイル名が不審 （例）・二重拡張子 ・拡張子の前に大量の空白文字の挿入

疑わしいメール例（ヤマト運輸からのメール）

宅急便受取指定ご依頼受付完了のお知らせ

ヤマト運輸 <mail@kuronekoyamato.co.jp>
2016/08/17 (水) 18:19
宛先: 東 永祥

全員に返信

このメッセージはスパムとして認識されました。26 日後に削除されます。このメッセージはスパム メールでありません

このアイテムは、あと 26 日で有効期限が切れます。

Malware Alert Text.txt
550 バイト

ダウンロード　OneDrive 東海大学 に保存

ご依頼ありがとうございます。
以下の内容で受け付けました。

■お受け取りご希望日時 ： 08/18日 (木) 12時から14時まで
■伝票番号 ： 5528-7703-1710

＜お問合せ先＞
ヤマト運輸株式会社
お客様サービスセンター

メールヘッダー情報から判断する

- 疑わしいメールのヘッダー

```
Received: from vmta01.cc.u-tokai.ac.jp (150.7.250.201) by
 DB3FFO11FD026.mail.protection.outlook.com (10.47.217.57) with Mic      t SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P      ) id
 15.1.577.8 via Frontend Transport; Wed, 17 Aug 2016 09:19:39 +0000
Received: from public-gprs353102.centertel.pl (public-gprs353102.centertel.pl [37.47.10.143])
                by vmta01.cc.u-tokai.ac.jp (Postfix) with ESMTP id 6ACD040A37
                for taro@tokai-u.jp; Wed, 17 Aug 2016 18:18:07 +0900 (JST)
From: =?iso-2022-jp?B?GyRCJWQlXiVIMT9NIhsoQg==?= <mail@kuronekoyamato.co.jp>
Subject: =?iso-2022-jp?B?GyRCQnA1XkpYPHU8aDtYRGokNDBNTWo8dUlVNDBOOyROJCpDTiRpJDsbKEI=?=
To: <eisho@tokai-u.jp>
Message-ID: <f1fb-50366@GKW4FL1ZH1172.tnt.kuronekoyamato.co.jp>
Date: Wed, 17 Aug 2016 10:18:21 +0100
MIME-Version: 1.0
Return-Path: taro@tokai-u.jp
```

TLD “.pl” はポーランド
IPアドレスはポーランド
※ ポーランド：中央ヨーロッパ

+0100は中央ヨーロッパ時間

- Date情報
  - 日本からの送信であれば “+0900” が普通
- Received情報
  - 送信元メールアドレス（From情報）は偽装可能だが、Receivedは偽装不可能

標的型攻撃と思われるメール例1（日本郵政からのメール）

差出人: 日本郵便 - 日本郵政 <anatoliyvind0ib@rambler.ru>
送信日時: 2016年3月15日 9:20
宛先: kumiko@tw.city.aizuwakamatsu.fu; 東海 花子
件名:

拝啓
配達員が注文番号903550077691の商品を配達するため電話で連絡を差し上げたのですが、つながりませんでした。従ってご注文の品はターミナルに返送されました。ご注文登録時に入力していただいた電話番号に誤りがあったことが分かりました。このメールに添付されている委託運送状を印刷して、最寄りの日本郵政取り扱い郵便局までお問い合わせください。
敬具
日本郵政ジャパンの宛先：
〒108-0845
東京都港区芝浦4-13-23
MS芝浦ビル13F
日本郵政
3/15/2016 01:19:52

日本郵政からのメールなのに、差出人のメールアドレスのドメインがロシア

宛先に自分以外のメールアドレスが含まれている

日本郵政ホームページ
http://www.japanpost.jp/information/2016/20160216115665.html

標的型攻撃と思われるメール例2（楽天からのメール）

安全と思われるメール例（JPCERTからのメール）

メールヘッダー情報から判断する

- 安全なメールヘッダー

```
Received: from vmta01.cc.u-tokai.ac.jp (vmta01.cc.u-tokai.ac.jp [172.16.1.11])
 by vmta03.cc.u-tokai.ac.jp (Postfix) with ESMTPS id E10EA40975
 for <contact@ml.tokai-u.jp>; Thu, 24 Dec 2015 17:26:09 +0900 (JST)
Received: from mx.jpcert.or.jp (mx.jpcert.or.jp [210.148.223.5])
 by vmta01.cc.u-tokai.ac.jp (Postfix) with ESMTP id 0BF1940E6A
 for <contact@ml.tokai-u.jp>; Thu, 24 Dec 2015 17:26:08 +0900 (JST)
X-PGP-Universal: processed;
 by pgpgw.jpcert.or.jp on Thu, 24 Dec 2015 17:26:06 +0900
References:
<SG2PR06MB0856205AB47FCF15FA898378E2E70@SG2PR06MB0856.apcprd06.prod.outlook.com>
To: "contact@ml.tokai-u.jp" <contact@ml.tokai-u.jp>
From: JPCERT/CC WW Group <ww-info@jpcert.or.jp>
X-Enigmail-Draft-Status: N1110
Date: Thu, 24 Dec 2015 17:25:59 +0900
```

TLD “.jp” は日本
IPアドレスも日本

+0900は日本時間

２．標的型サイバー攻撃の流れと手法

２－１．初期潜入

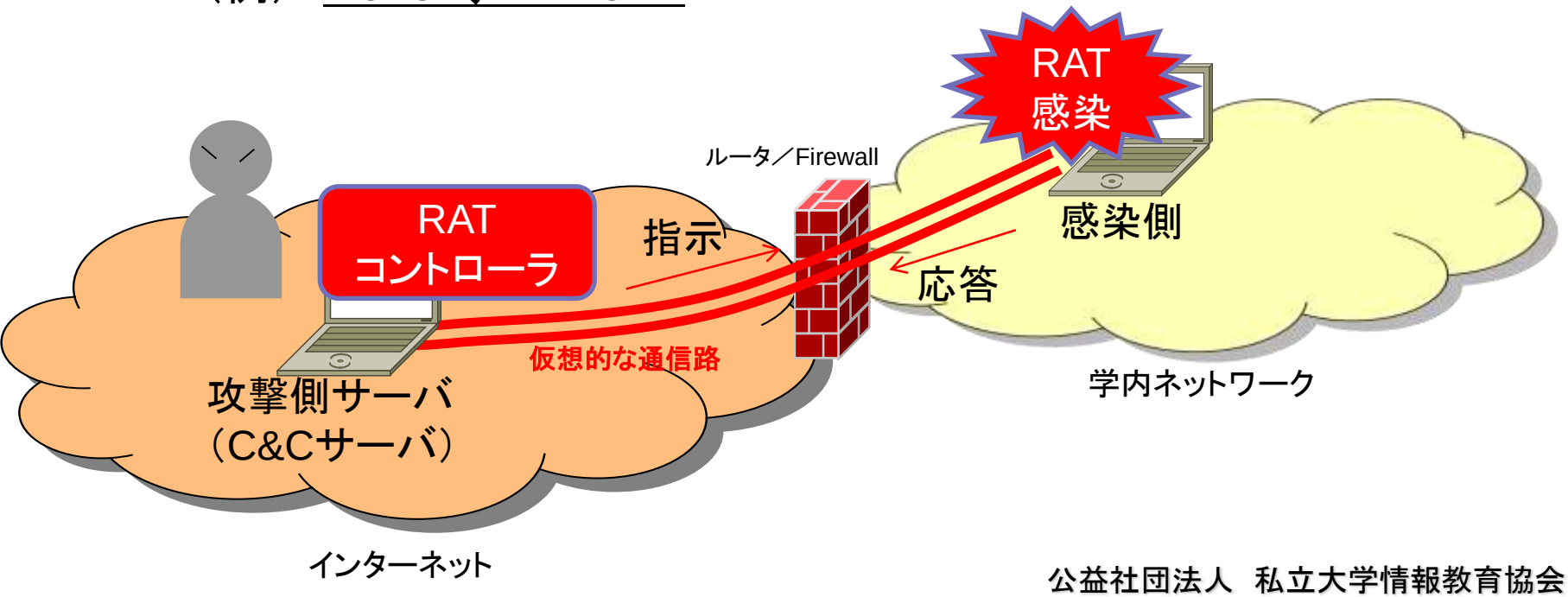
初期潜入方法

- 代表的な潜入方法
  - メールからの潜入
    - 不審なファイルを添付したメールを送信
    - 不審なURLリンクが本文に記載されたメールを送信
  - USBメモリからの潜入

- 添付ファイルを実行、またはURLリンク先にアクセスさせた後にRAT（遠隔操作ウィルス）を使って次の段階（基盤構築）に進む

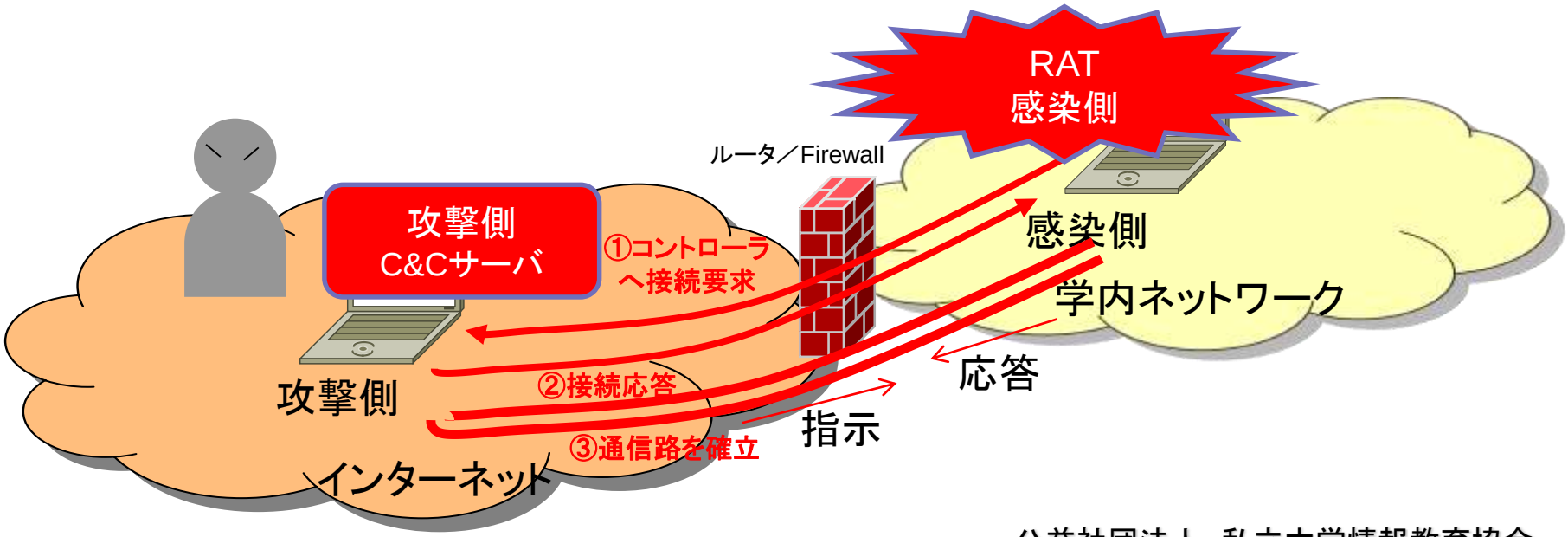
RATとは

- RAT = Remote Admin Tool (?)
  Remote Access Trojan(?)
- 「バックドア通信」を行うウイルスの総称
  - インターネット上の攻撃側サーバ(C&Cサーバ)からの指示により、ウイルスの拡散や情報収集の足がかりに
  - （例） **Bozok、H-Worm**



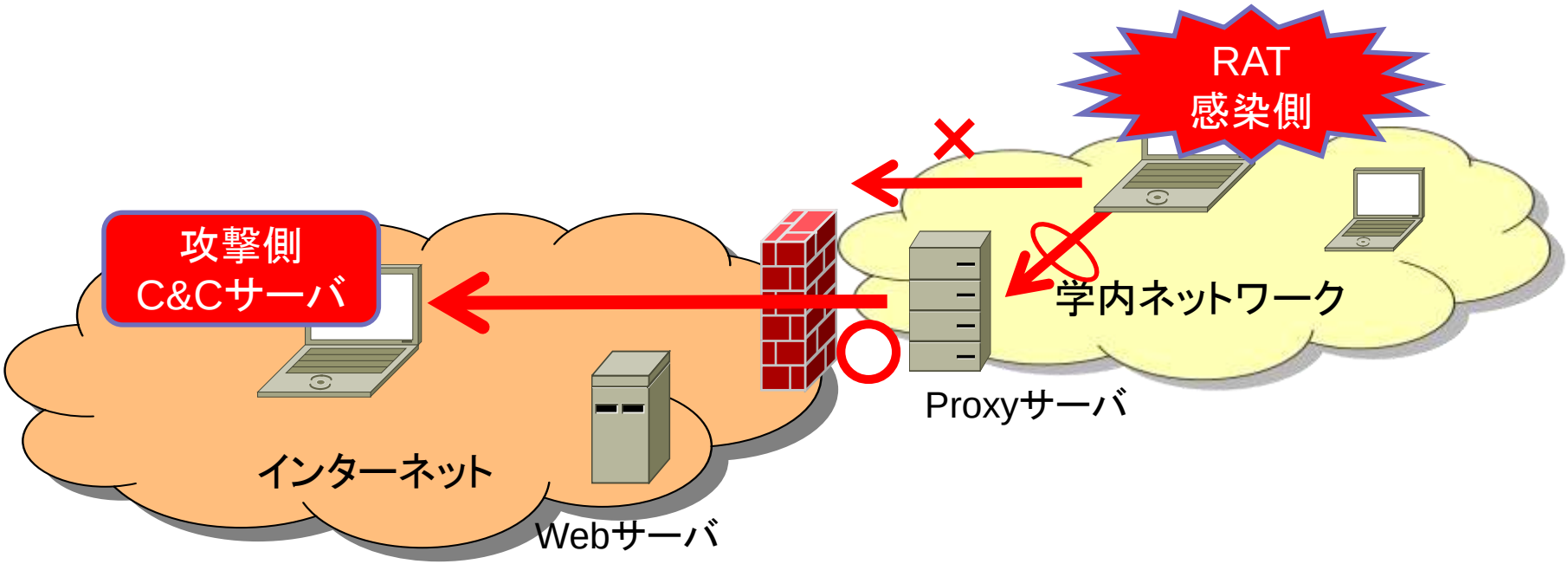
RATの特徴 （1）

- 攻撃側への着呼型
  - もともと内部ネット→外部ネットへ通信可能なサービスを模して、感染PC～攻撃PC間の通信路を確立
  - 通常の通信と、RAT通信の見分けが困難
    - ポート番号： 80/tcp(http) とか 443/tcp(https)とか



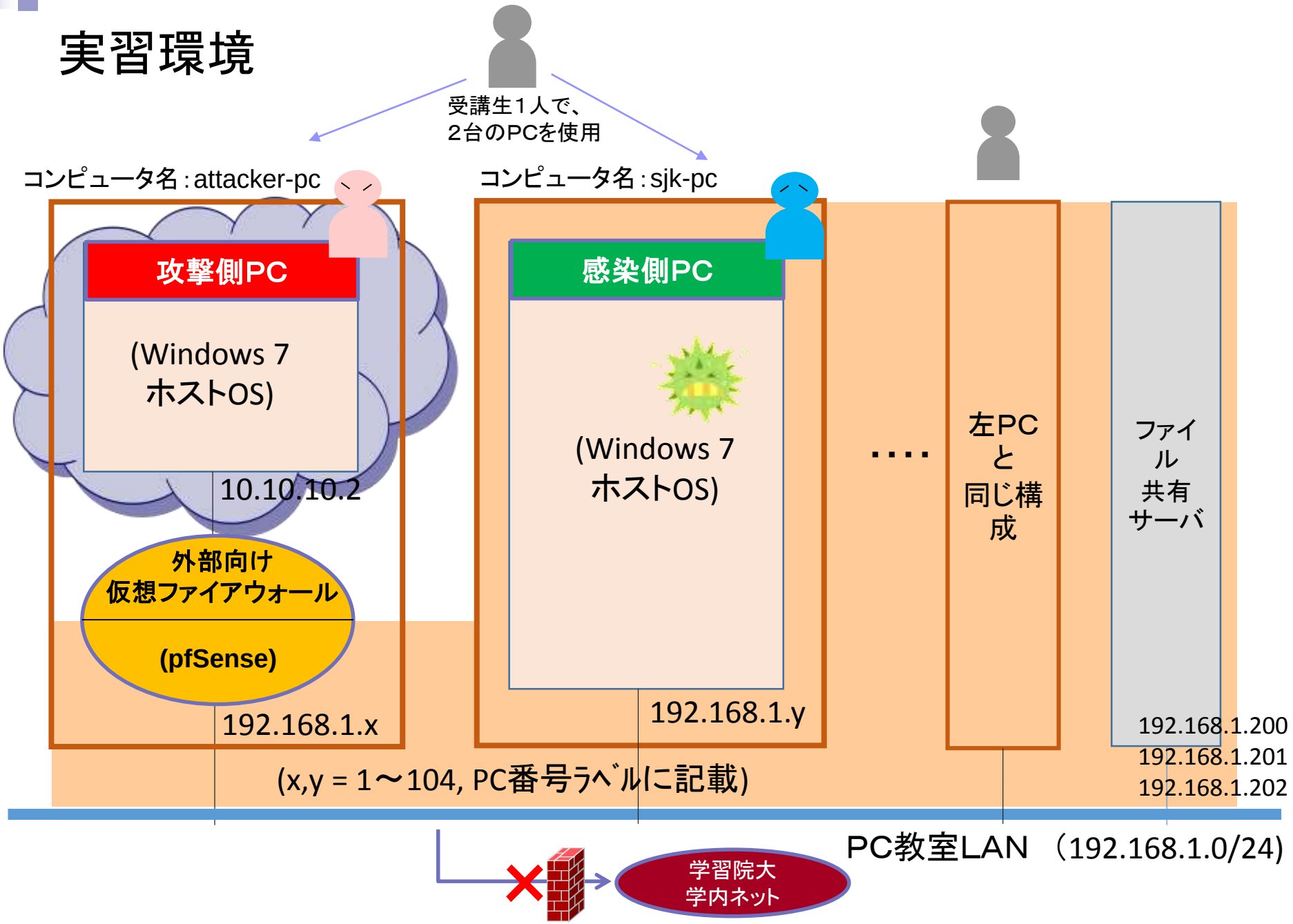
RATの特徴 （2）

- 出口対策が困難
  - Proxyサーバに対応しているRATもある
    - 感染PCからインターネットへブラウザでアクセス可能ならば、攻撃側PCから感染PCのコントロールが可能



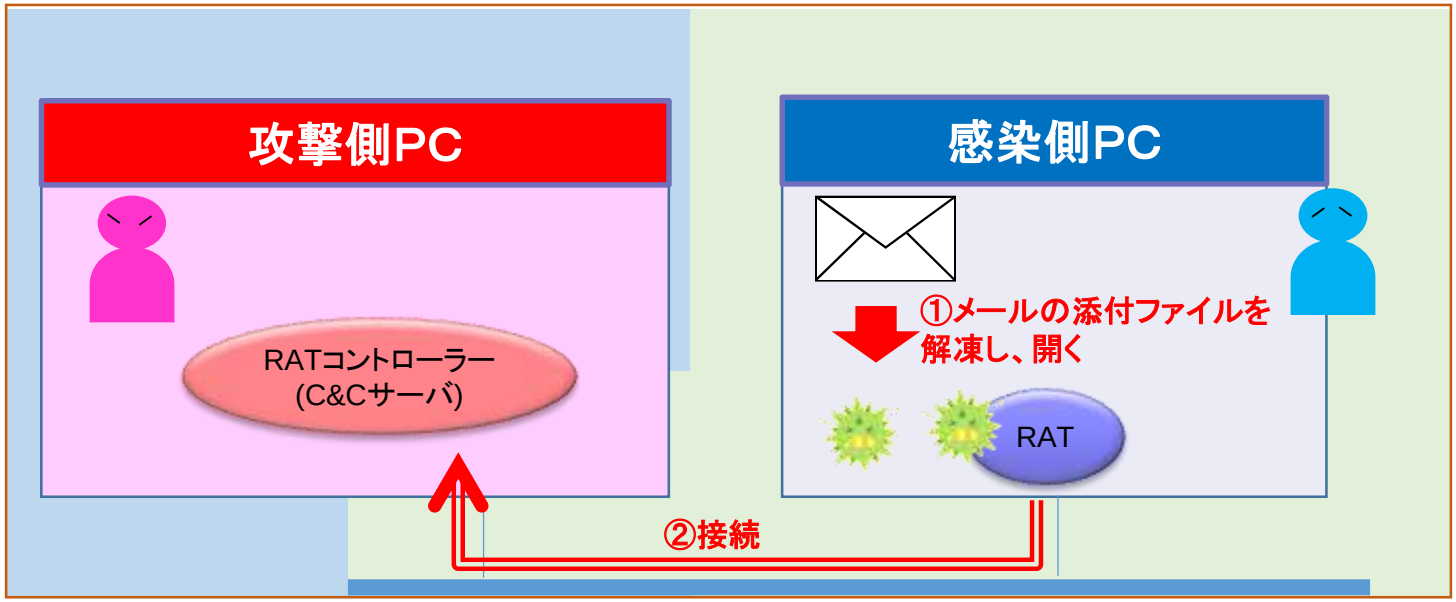
実習1
RATを使った初期潜入を体験

実習環境


受講生1人で、
2台のPCを使用
コンピュータ名：attacker-pc
コンピュータ名：sjk-pc
攻撃側PC
(Windows 7
ホストOS)
感染側PC
(Windows 7
ホストOS)
10.10.10.2
外部向け
仮想ファイアウォール
(pfSense)
192.168.1.x
192.168.1.y
・・・・
左PC
と
同じ構
成
ファイ
ル
共有
サーバ
192.168.1.200
192.168.1.201
192.168.1.202
(x,y = 1～104, PC番号ﾗﾍﾞﾙに記載)
PC教室LAN （192.168.1.0/24)
学習院大
学内ネット

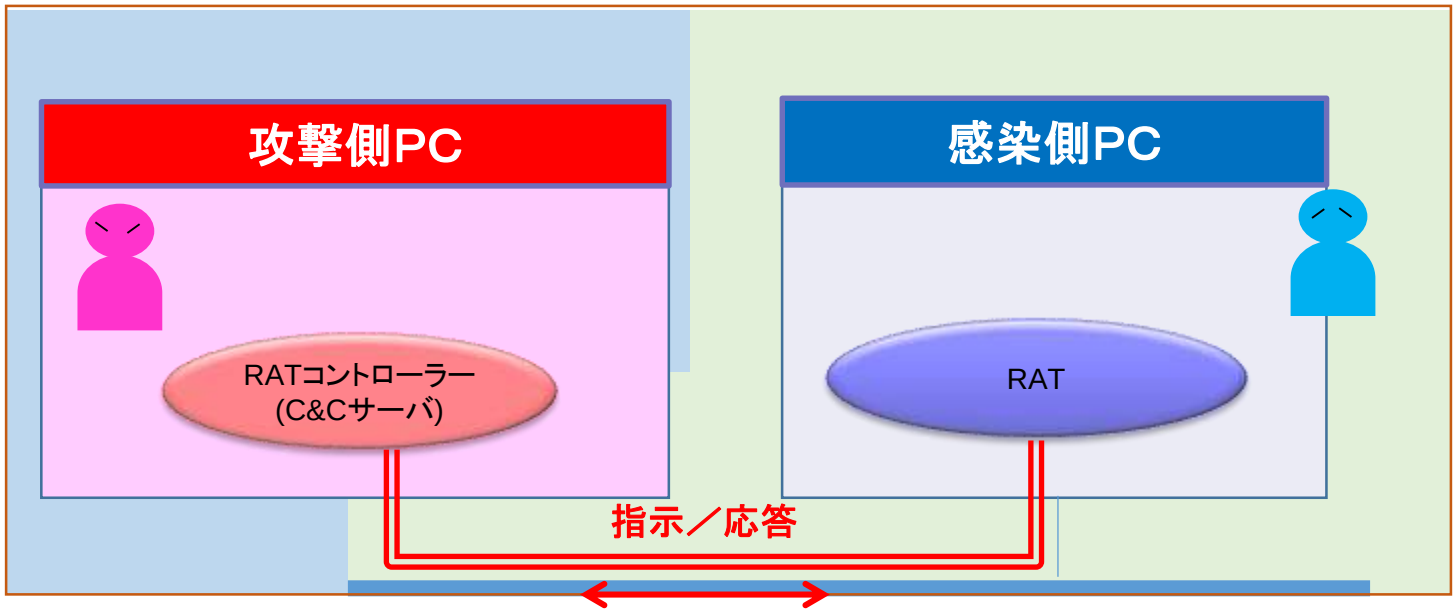
マルウェア感染

- 感染側PCで、添付ファイルを開く
- その結果、PCはマルウェアに感染
- 感染側PCから、攻撃側PCのC&Cサーバに接続



攻撃側PCからの操作

- 感染側PCから攻撃側PCのC&Cサーバに接続されると、遠隔での操作が可能となる



２－２. 基盤構築

基盤構築

- 初期潜入に成功すると、攻撃者は次に潜入先の内部情報を窃取するための「基盤構築」を行う

- 基盤構築の段階では、内部情報を窃取するためのツールを送り込み、インストールされる

- 現在の標的型サイバー攻撃は「潜伏型」と「速攻型」の2種類に大別できる
  - 「潜伏型」：重要情報窃取を果たすまで活動する
    - 潜入してから実際に攻撃を開始、終了までの期間が長いもの（平均5か月）
    - 潜入後、攻撃（情報窃取）のための基盤を拡大する
    - 攻撃終了の際には痕跡も消していく
  - 「速攻型」：重要情報窃取に向けた、最低限の情報を入手する
    - 潜入してから攻撃が終了するまでの期間が数時間～1日程度
    - 潜入後の基盤拡大、痕跡消去は行わない

実習２
内部情報窃取ツールのインストール

ネットワーク調査ツール

- nmap
  - ポートスキャンをするためのツール
  - コマンド（nmap）と様々なオプションを組み合わせることで、内部ネットワークに接続されているコンピューターの情報を調査することが可能
  - OSを推定することも可能
  - オプション例
    - -A：OSとサーバーアプリケーションのバージョンを調査
    - -O：OSのバージョンを調査
    - -P0：pingスキャンを行わない
    - -F：限定したポートのみ調べる

- 攻撃側PCから感染側PCにnmapを（サイレント）インストールする
  - 気づかれずに感染側PC内部ネットワークの情報調査基盤を構築する

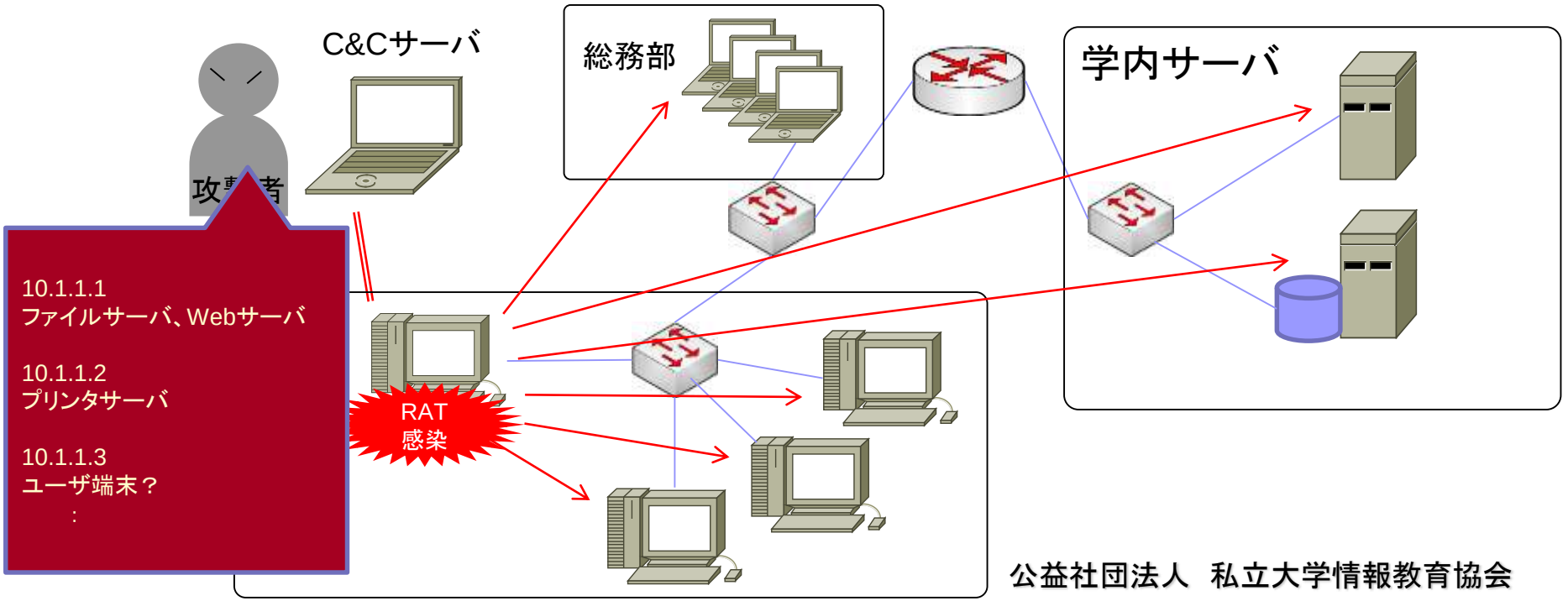
２－３．内部侵入・調査

内部侵入・調査

1. ネットワークの調査
   - 標的組織の内部ネットワークシステムを把握
   - nmap等
2. 端末間での侵害拡大
   - 他端末のアクセス権限を入手、他端末へ侵害
   - pwdump7, Gsecdump （ハッシュ値入手）
   - Pshtoolkit, Metasploit PSEXEC module（偽装アクセス）
3. サーバへの侵入
   - ユーザ端末からサーバへのリモート操作
   - PsTools

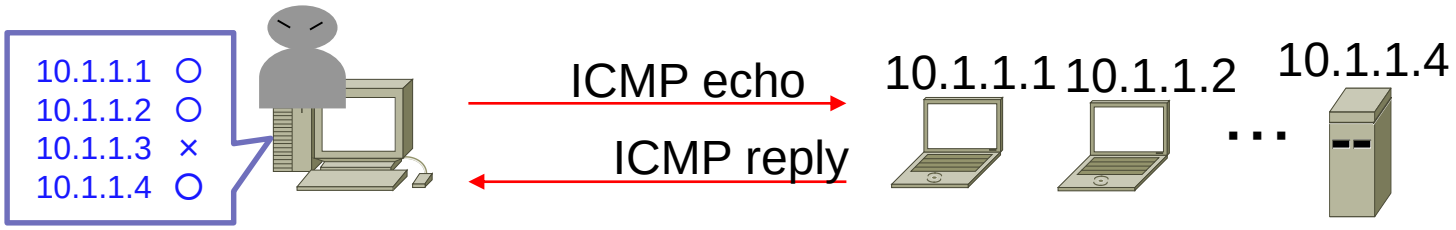
1. ネットワークの調査

- 標的組織の内部システムを把握する
  - IPアドレスの探索
  - サービスポートの探索
- 主な手法
  - ポートスキャン

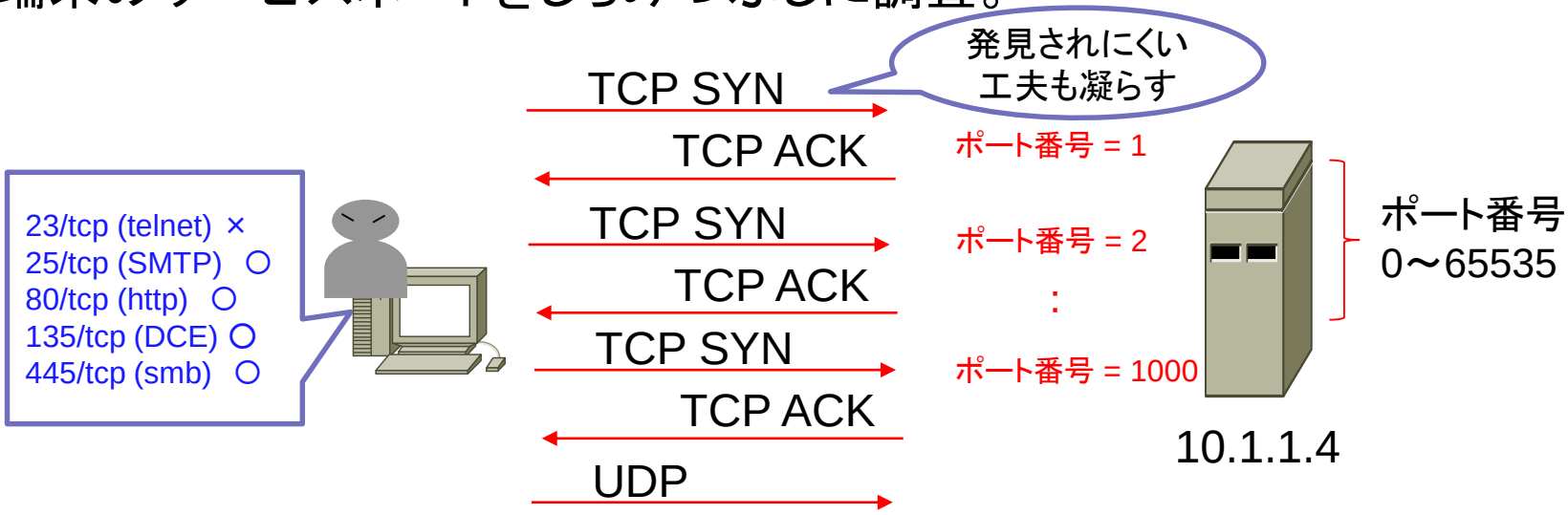


ポートスキャン

- 標的組織内のIPアドレスをしらみつぶしに調査。



- 各端末のサービスポートをしらみつぶしに調査。



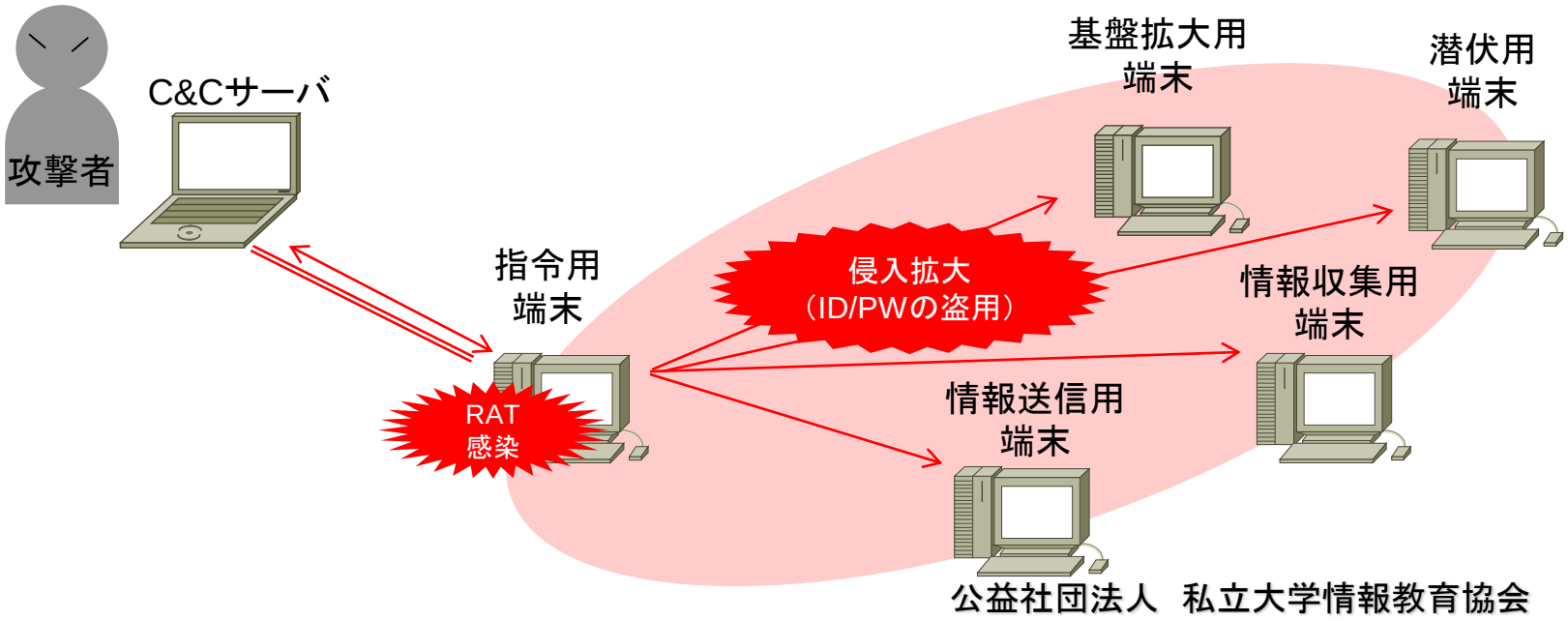
実習３
内部ネットワークを調べる

内部ネットワークの調査

- nmapを利用
  - nmapコマンドを使って、感染側PCの内部ネットワーク（192.168.1.0/24）の調査（ポートスキャン）を実施する
  - 内部ネットワークにある稼働中の他のPC、及び各PCで使われているサービスポートの情報を窃取する

2. 端末間での侵害拡大

- 他端末へ攻撃、外部からコントロールできる端末を複数台、確保する
- 主な手法
  - Pass the Hash攻撃
  - オートコンプリート機能による保存パスワードの盗用
  - ネットワークモニタリング

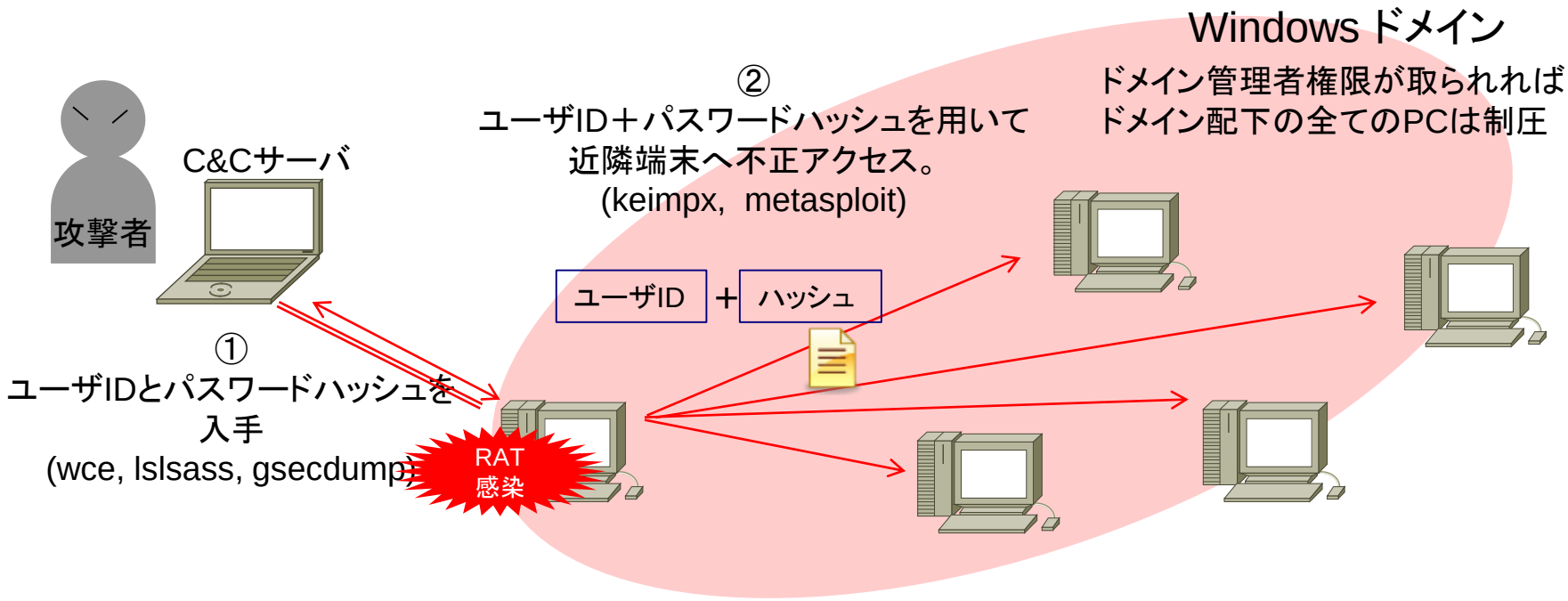


Pass the Hash 攻撃 （アクセス権限の入手）

- Windowsの認証を回避し、ユーザIDとパスワードのハッシュ値のみを使い不正アクセスする手法

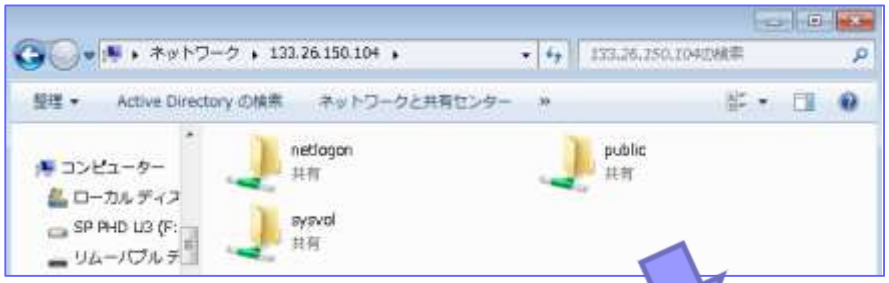
  ⇒ **生のパスワードが分からなくても、アクセスできる。**

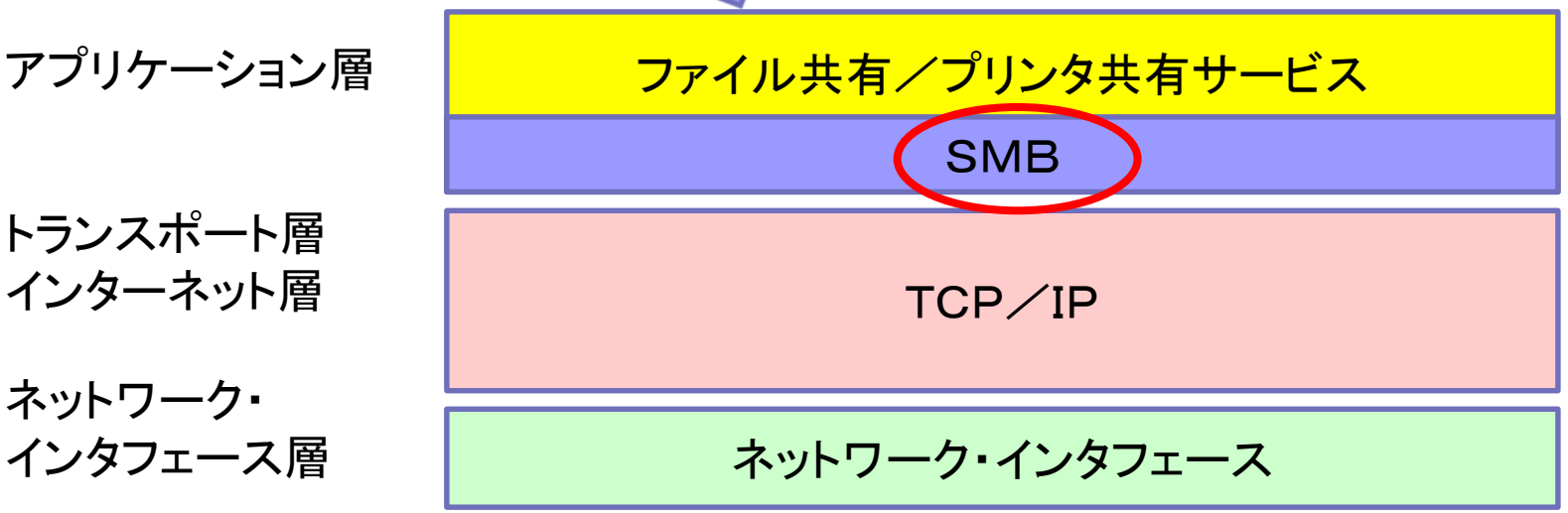
- ドメイン管理の場合、1台のPCがやられると、全てのPCが被害にあう恐れがある。



Pass the Hashのしくみ

- ファイル共有やプリンタ共有の機能を悪用している
- SMB通信プロトコルを使用

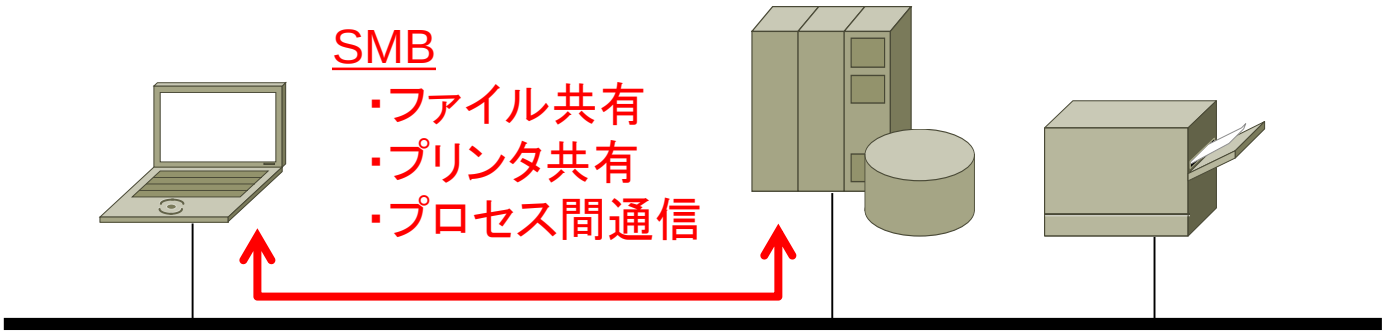




SMB　- Server Message Block

- IBMが設計しMicrosoftが改良した通信プロトコル
  - SMB1.0＝CIFS(Common Internet File System)
- 使用目的
  - ファイル共有やプリンタ共有
  - プロセス間通信
- 使用ポート
  - 135/tcp、445/tcp、1025～65535/tcp

ADサーバからユーザ端末へのポリシー配布にも使用



パスワードはどのように保存されているのか？ (Windowsの場合)

- パスワードは、「ハッシュ値」に変換されて保存されている。

パスワード　**sjk2016**

↓ ハッシュ関数(MD4等)によって変換

ハッシュ値　**a2404b2df08becb206acdadb67d28dd6**

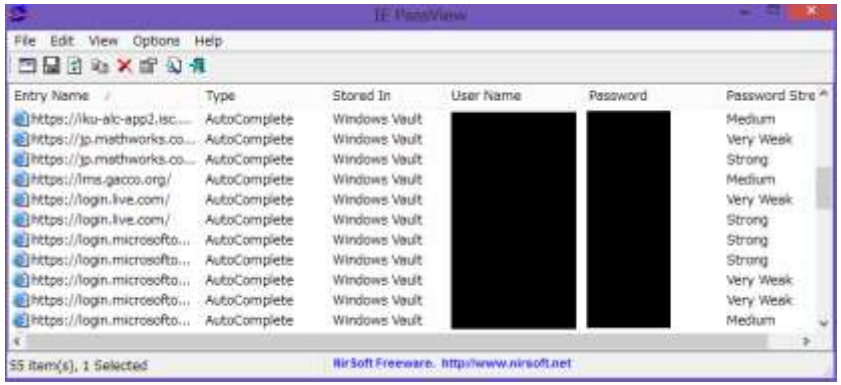
★特徴
① パスワードの文字を1文字変えるだけで、ハッシュ値は全く**別の数値**になる。
② ハッシュ値から、**元のパスワードを計算することはできない。**

オートコンプリート機能で保存されたパスワードの盗用

- オートコンプリート
  - キーボードからの入力を補助する機能
  - 一度ブラウザから入力した「ユーザID＋パスワード」を、次回のアクセスからは自動入力に
  - PC内部に保存されているパスワードは、（ツールで）読み取り可能

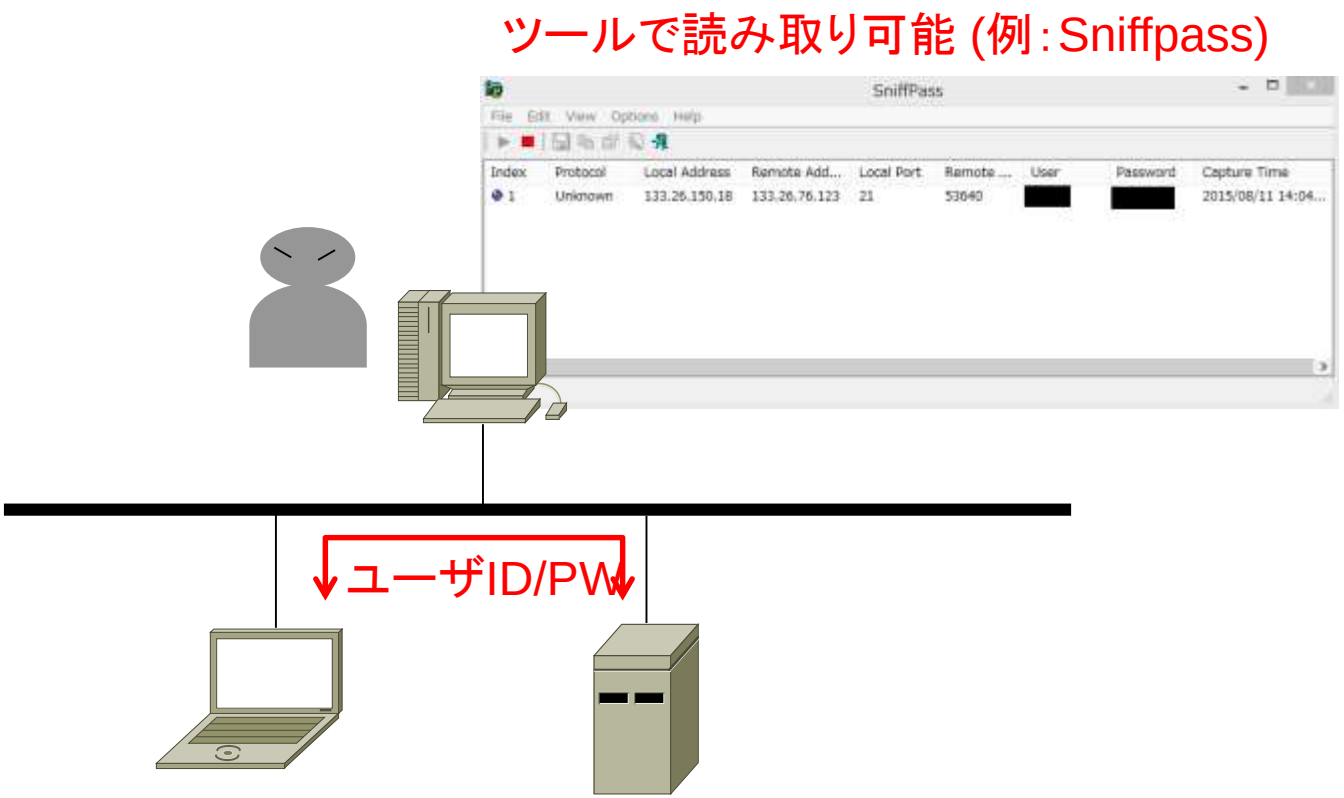
パスワードの保存

ツールで読み取り可能 (例：IE PassView)



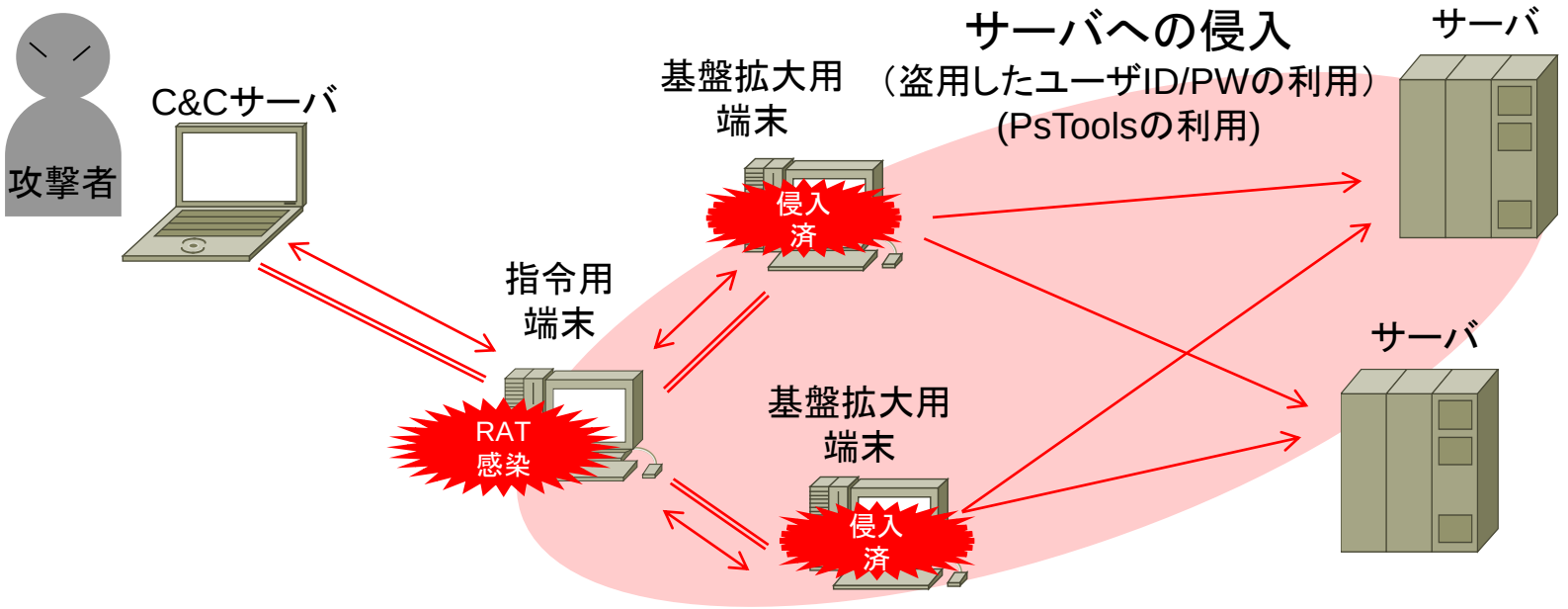
ネットワークモニタリング

- ネットワーク上を流れる情報をモニタリング
- 暗号化されていない「ユーザID/パスワード」を入手可能



3. サーバへの侵入

- 感染端末を足掛かりとして、サーバへの侵入を試みサーバ上の重要情報にアクセスする
- 主な手法
  - PsTools



PsTools

- Windows管理ユーティリティ
- Microsoftがフリーで配布
  - https://technet.microsoft.com/ja-jp/sysinternals/bb897553
- コマンド例
  - PsExec・・・リモートでプロセスの実行を行う
  - PsKill・・・リモートでプロセスの強制終了を行う
  - PsShutdown・・・リモートでシステムのシャットダウンを行う
- サーバ側で、ファイル共有サービスが動いていれば動作
  - SMBのプロセス間通信機能を使用
  - 感染端末と同じドメインであれば、パスワードも不要

まとめ

- メールの信憑性調査
  - 通報メール自体が標的型サイバー攻撃の場合がある
  - メール本文、ヘッダー情報から信頼できるものかを判断する
  - 添付ファイルがある場合は更に慎重に調査する

- 標的型サイバー攻撃の手法
  - 初期潜入
    - メールの添付ファイルやURLリンクを使ってRATを送信、感染させる
  - 基盤構築
    - RAT経由で内部情報を窃取するためのツールを送り込む
  - 内部侵入・調査
    - 内部ネットワークシステムの調査・把握
    - 他端末のアクセス権を入手して侵害拡大
    - サーバーに侵入