A-5.
サイバー攻撃に対する調査と対応

明治大学
服部　裕之

公益社団法人　私立大学情報教育協会

このセッションの目標

サイバー攻撃を受けた時の
「痕跡調査」と「一時対応」を学び、実習にて確認する

① PCの調査・対応が行えるようになる
② サイバー攻撃に備えて事前に何を行えばよいのかがわかる

ランサムウェア＋標的型サイバー攻撃

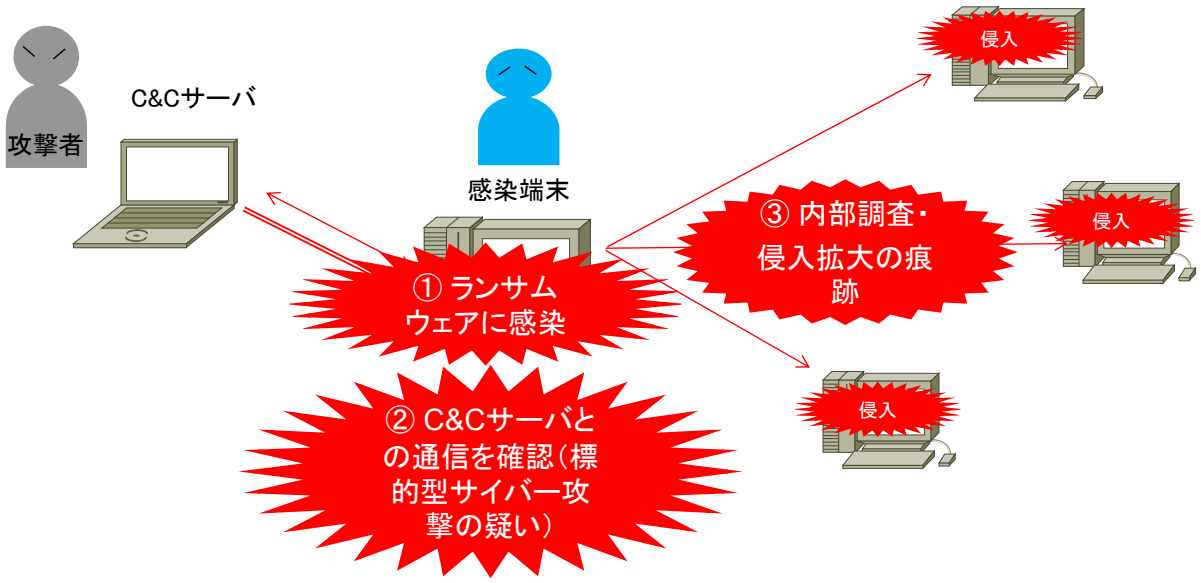
- ランサムウェアに感染しただけではなく、実は標的型サイバー攻撃を受けていた。

- ストーリー
  - PCがランサムウェアに感染した。
  - 感染経路がわからない。
  - 被害者（PC利用者）に聞いても「何もしていないのに、突然、ファイルが暗号化された」

実は、既にマルウェアに感染していた！

標的型サイバー攻撃を受けていたことに気づかなかった

ストーリー概要



実習

- 遠隔操作ツール（RAT）を用いたランサムウェアの感染

実習1 □ インシデント発生！
- 被害者（感染PC利用者）は、情報センターへ相談に

- 情報センター技術スタッフによる対応

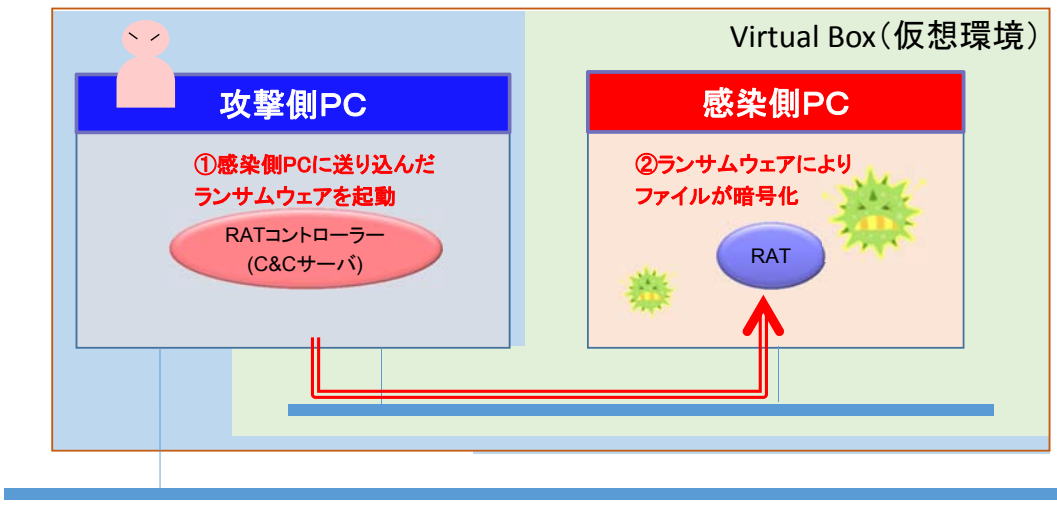
実習2 □ PCの状況把握
- ランサムウェアの種類を調査
- 他に怪しい振る舞いはないか？
  - □ プロセス調査
  - □ 通信状況の把握

実習3 □ 情報漏えいの痕跡調査
- イベントログの調査

実習4 □ PCの証拠保全
- 外部業者に調査委託するための作業

実習1　遠隔操作によるランサムウェアの起動と感染

- 攻撃側PCから、感染側PCのランサムウェアを起動
- その結果、感染側PCで突然ファイルが暗号化、脅迫文が表示される



ランサムウェア感染のメカニズム

「不審な添付」フォルダ

（通常属性ファイル）

ショートカットのリンク先：

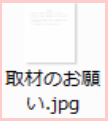
C:¥Windows¥system32¥cmd.exe /c start server.exe & start 取材のお願い.jpg & exit

【意味】

(1) server.exeを起動し、

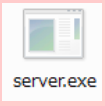
(2) 取材のお願い.jpg を開く

（Hidden + System属性ファイル）



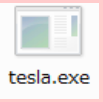
取材のお願い.jpg

・取材依頼の文書本体



Server.exe（RATプログラム（Bozok））

・C&Cサーバと接続し指示を待つ



tesla.exe（ランサムウェア（TeslaCrypt））

・ランサムウェアTeslaCrypt

・「取材のお願い」ショートカットからは起動しない

この後、被害側組織で行うことは？（順不同）

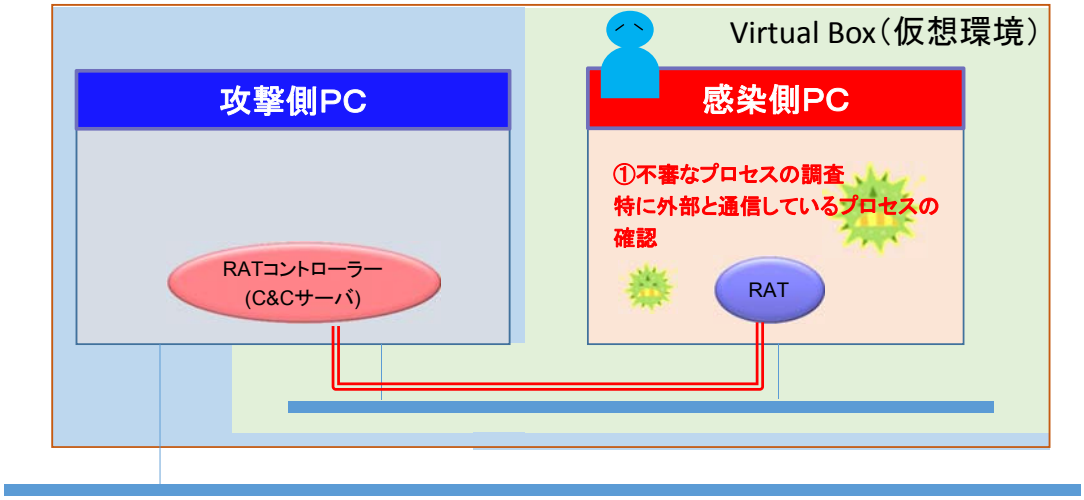
- PCの調査
  - 実習2 □ 状況把握
    - ランサムウェアに感染しただけなのか？ 他には？
  - 実習3 □ 痕跡調査
    - 情報漏えいや内部侵入の形跡はないか？
  - 実習4 □ 証拠保全
    - 業者への本格的な調査依頼
  - □ ウィルス駆除
  - 実習3 □ ファイルの復旧
    - 復号ツールやバックアップの利用
- 被害拡大の防止
  - □ 通信制限の強化やネットワークの遮断
    - ＜補足資料＞参照
- ネットワークの調査
  - □ 痕跡調査
    - ＜補足資料＞参照

どの順序で対応するのがベストか？

（実習の順番どおりの対応が良いとは限らない）

実習2　PCの状況把握

- 不審なプロセス、不審なネットワーク通信の現状調査



状況把握に便利なツール

- プロセス関連

実習で使用 ⇒

  - Process Hacker
    - http://processhacker.sourceforge.net/
  - Process Explorer
    - https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer

⇒ どちらも不審なプロセスを、外部のウィルススキャンサイト(Virustotal等)で簡単にチェックすることができる。

- 自動起動、レジストリの調査
  - Autoruns
    - https://technet.microsoft.com/ja-jp/sysinternals/bb963902.aspx

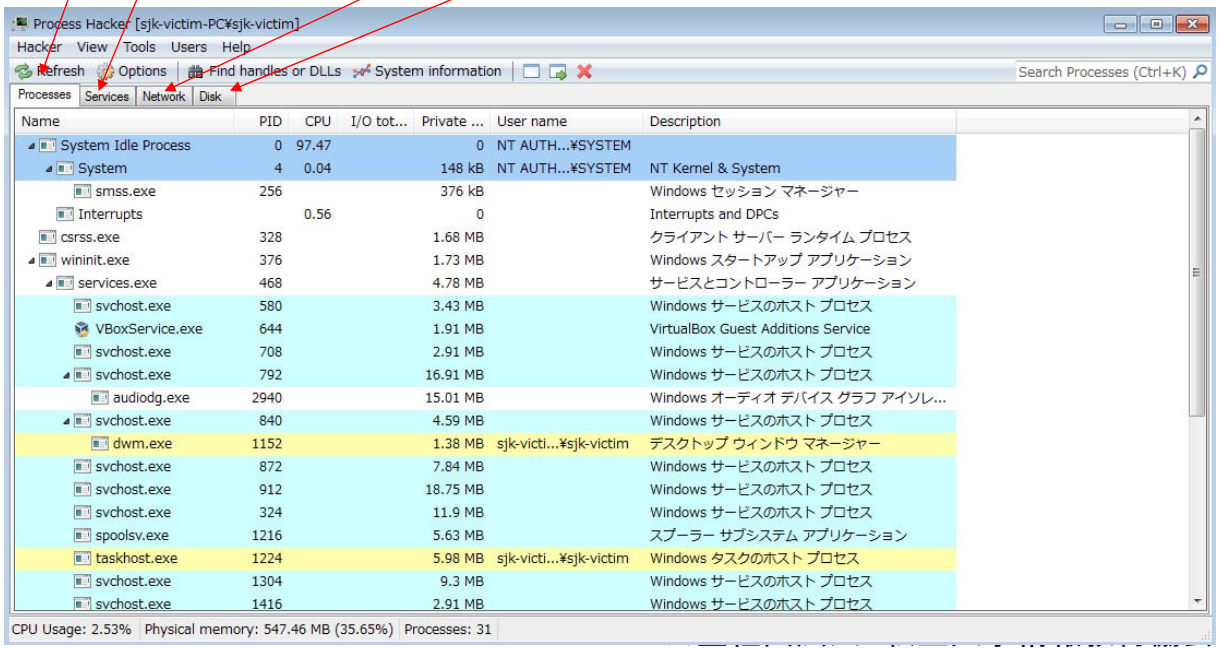
Process Hacker

プロセスの起動状況

サービスの動作状況

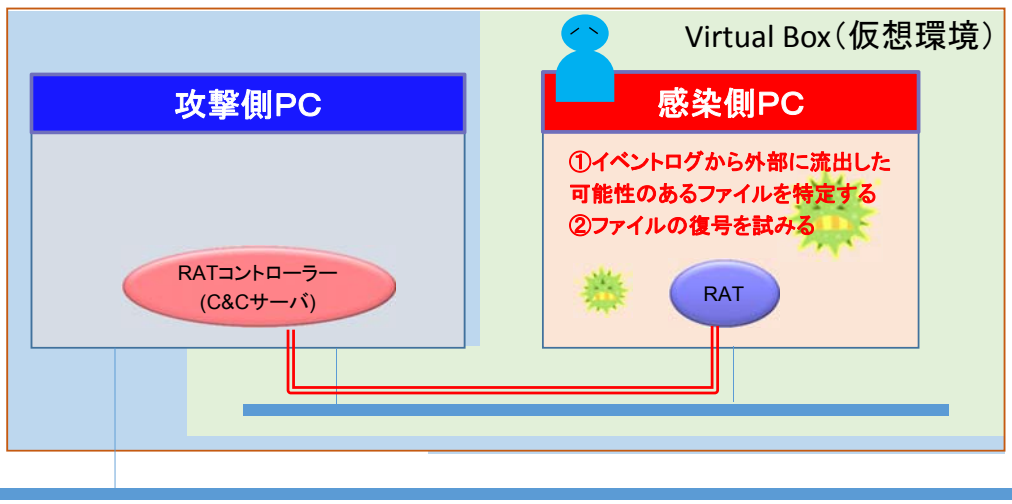
ネットワーク通信の状況

ディスクアクセスの状況



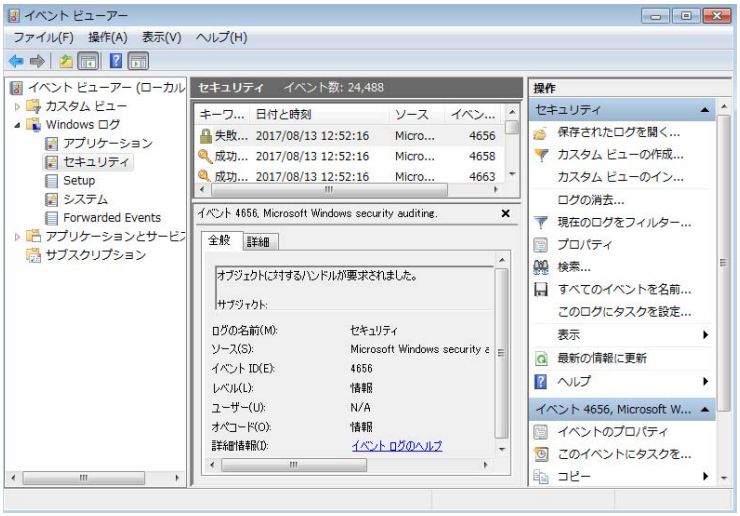
実習3　情報漏えいの痕跡調査

- イベントログより、外部に流出した可能性のあるファイルを特定する



「イベントログ」とは

- システムやアプリケーションの動作状況や利用者の操作などを記録したもの。
- 閲覧方法
  - 「コントロールパネル」→「管理ツール」→「イベントビューアー」



イベントログでわかること

- 利用者の操作
  - ログオン／ログオフ
  - プログラムの起動
  - ファイルのアクセス
- システムの動作
  - サービスプロセス
  - スケジュールされたタスク
  - ハードウェアに関すること
  - ネットワークの動作

マイクロソフト 「イベントログ」
https://technet.microsoft.com/ja-jp/library/cc722404(v=ws.11).aspx

「プログラムの起動」ログ

- 「Windows」→「Sysmon」→「Operational」ログ
- 攻撃ツールを実行した痕跡はないか？
  - ネットワークの調査
    - nmap, net share 等
  - アクセス権限の入手
    - lslsass, gsecdump, wce, mimikatz, pwdumpx （ハッシュ値入手）
    - keimpx, pshtoolkit, metasploit （偽装アクセス）
    - iepv （キーロガー、キャッシュ調査）
  - 遠隔操作、ファイルアクセス
    - PsExec, net use 等
  - バックドア
    - HTran

JPCERT/CC
「インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書」
https://www.jpcert.or.jp/research/ir_research.html

「ファイルのアクセス」ログ

- 「Windows」→「Security」ログ
- 流出した可能性のあるファイルは無いか？

【監査対象の指定】

「誰」が「どのファイル」に「何をした」

- 「誰」
  - ・全員(Everyone)
  - ・グループ
  - ・個人
- 「何をした」
  - ・読み取り、書き込み、追加、削除
  - ・アクセス権の変更、所有者の変更
  - ・etc.

事前準備

Windows標準設定では、さほど詳細なログは取れない

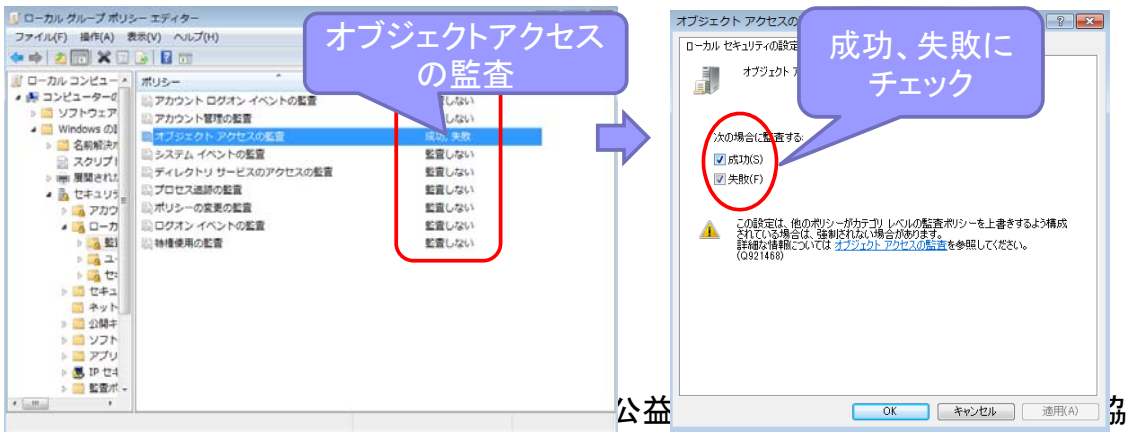
↓

事前の設定が必要

1. 監査ポリシーの有効化
   - 取得するログの指定
2. 監査対象の指定（ファイルのアクセス）
   - ログ取得の対象となるユーザ、操作内容を指定
3. Sysmonのインストール
   - より詳細なイベントログを取るための追加ツール
   - プロセスの起動、ネットワーク通信などを記録する

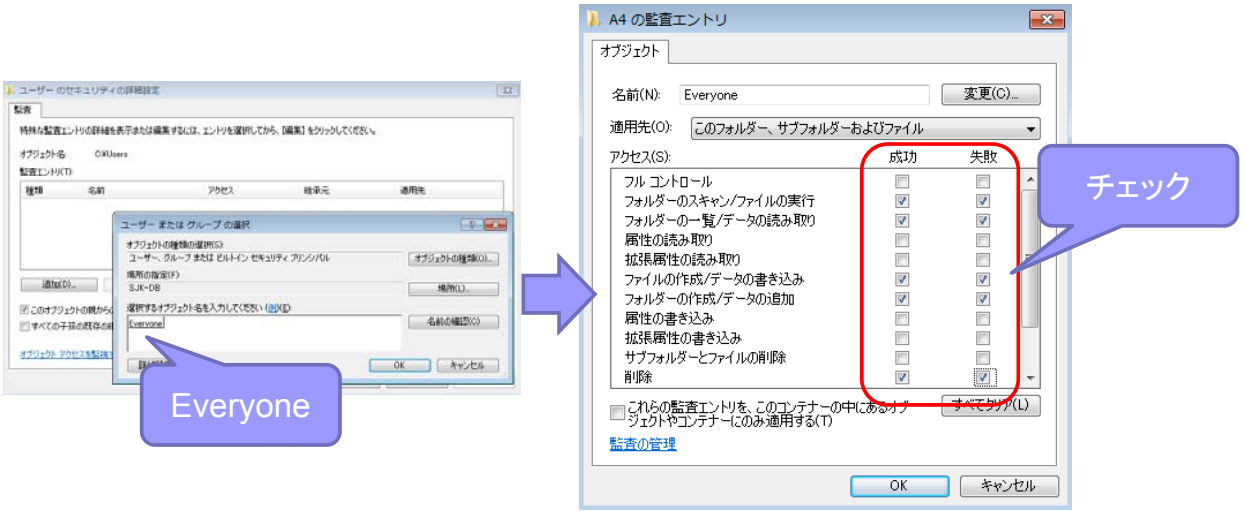
準備1.　監査ポリシーの有効化

- どのような行為をイベントログに残すのか？
- それは成功した時か？失敗したときか？
  - ローカルグループポリシーエディター(gpedit.msc)で設定
    - 「ローカルコンピューターポリシー」→「コンピューターの構成」→「Windowsの設定」→「セキュリティの設定」→「ローカルポリシー」→「監査ポリシー」→「オブジェクトアクセスの監査　（ファイルアクセスの監査）」



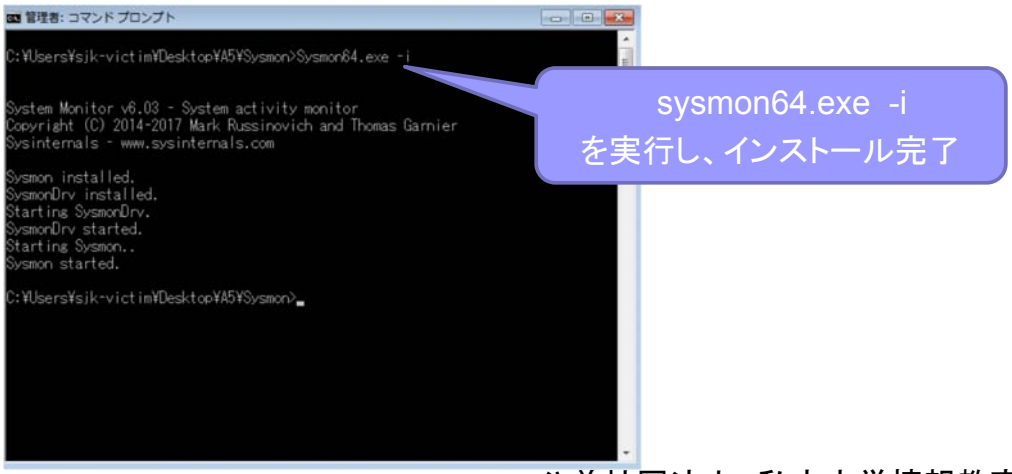
準備2.　監査対象の指定

- 誰が、どんな操作をしたときにイベントログに残すのか？
- フォルダの「プロパティ」で設定
  - 「プロパティ」→「セキュリティ」→「詳細設定」→「監査」→「追加」
  - 対象ユーザーを選択（全員ならばEveryone）



準備3.　sysmonのインストール

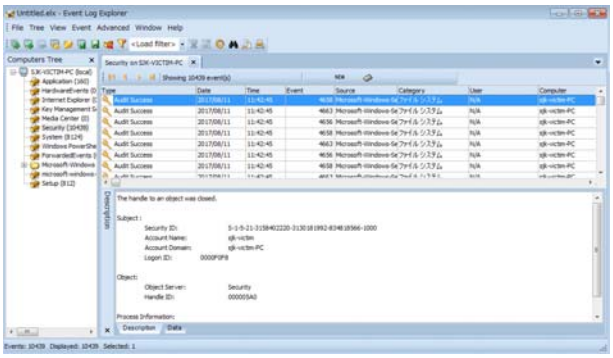
- ユーザ毎の行為の詳細（プロセスの起動、ネットワーク通信など）を記録
- イベントログの［アプリケーションとサービス ログ］-［Microsoft］-［Windows］-［Sysmon］-［Operational］に記録される。
- https://docs.microsoft.com/ja-jp/sysinternals/downloads/sysmon より入手。



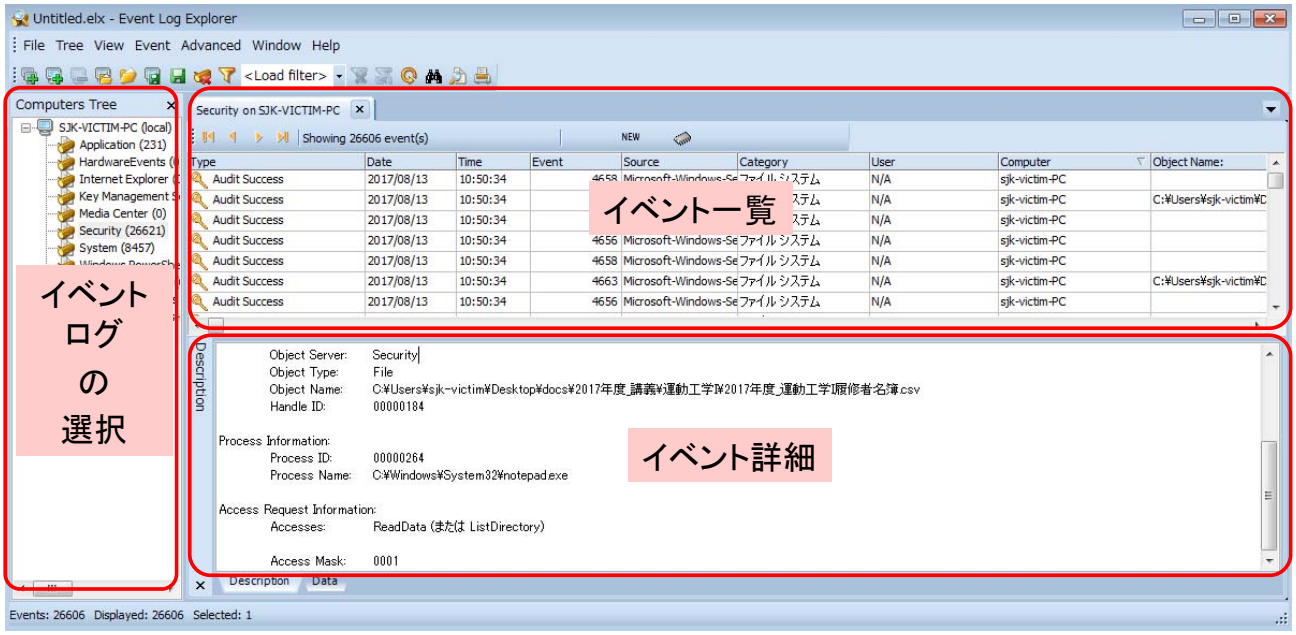
状況把握に便利なツール

- イベントログの調査
  - イベントビューアー （OS付属）
    - 「コントロールパネル」→「管理ツール」→「イベントビューアー」
  - Event Log Explorer
    - https://eventlogxp.com/jap/
    - 個人版ならば無料で使用可能

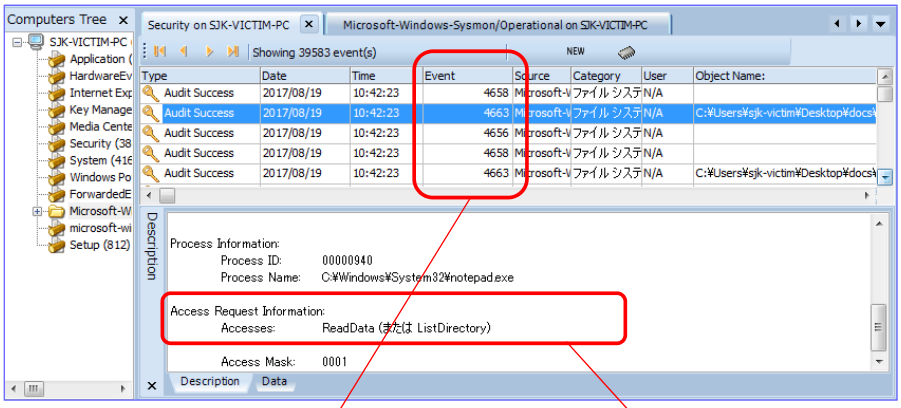
実習で使用



Event Log Explorer



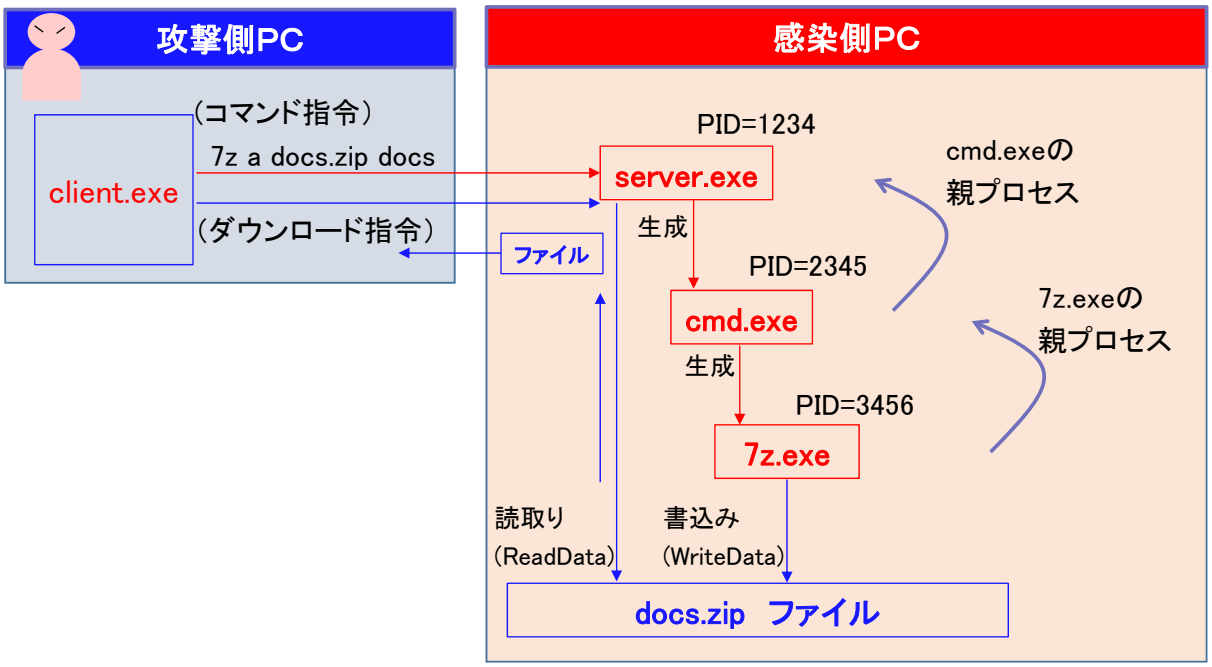
イベントIDと操作内容について



イベントID	意味
4656	ファイルオープン
4663	ファイルアクセス
4690	ファイルコピー
4660	ファイル削除
4658	ファイルクローズ

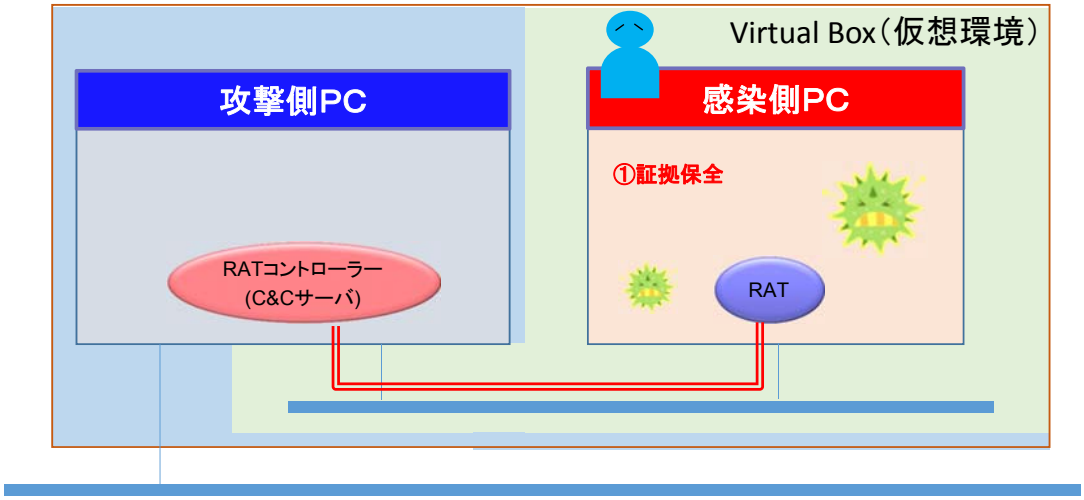
操作内容(Accesses)	説明
DELETE	オブジェクトの削除
ReadData(または ListDirectory)	フォルダ、ファイルの読取り
WriteData(または AddFile)	フォルダへのファイル操作、ファイルへの書込み
AppendData(または AddSubDirectory または CreatePipeInstance)	データの追加、フォルダの作成
実行/スキャン	フォルダのスキャン、ファイルの実行
DeleteChild	フォルダとフォルダ内のファイル削除

プロセスの相関



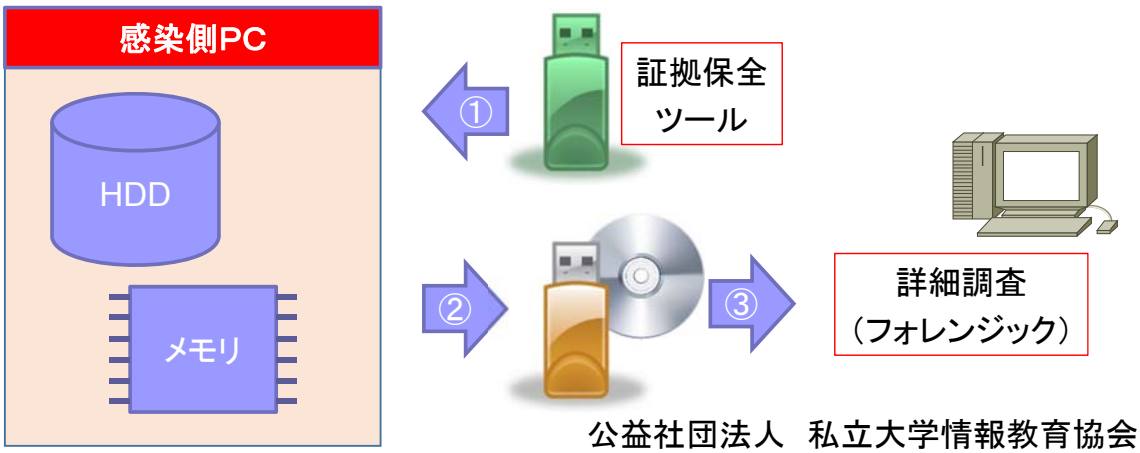
実習4　PCの証拠保全

- 外部業者に調査委託するための作業



証拠保全とは

- PCの詳細調査（フォレンジック）に必要な情報を取り出し、安全な場所に保管すること
  - メモリ
    - ネットワーク情報、プロセス情報、ユーザー入力情報等
  - 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

- ToolBox ATTK
  - トレンドマイクロ社の調査ログ収集用ツールキット

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6版」 2017年5月9日
https://digitalforensic.jp/home/act/products/df-guideline-6th/

まとめ

- イベントログの設定
  - ファイルアクセス
  - 起動プロセス

    ⇒痕跡調査のために、あらかじめ採取する設定にする。
    （ログの保存期間、ディスク容量に留意）

- インシデント対応手順の確認
  - 証拠保全を実施するタイミング
  - 復旧を優先か？
  - 調査（原因、被害範囲の特定）を優先か？

    ⇒事前にケース毎の検討を

補足資料

【補足資料】

1. 被害拡大の防止
   - □ ネットワークの遮断、通信制限の強化

2. ネットワークの調査
   - □ ネットワークレベルでの痕跡調査

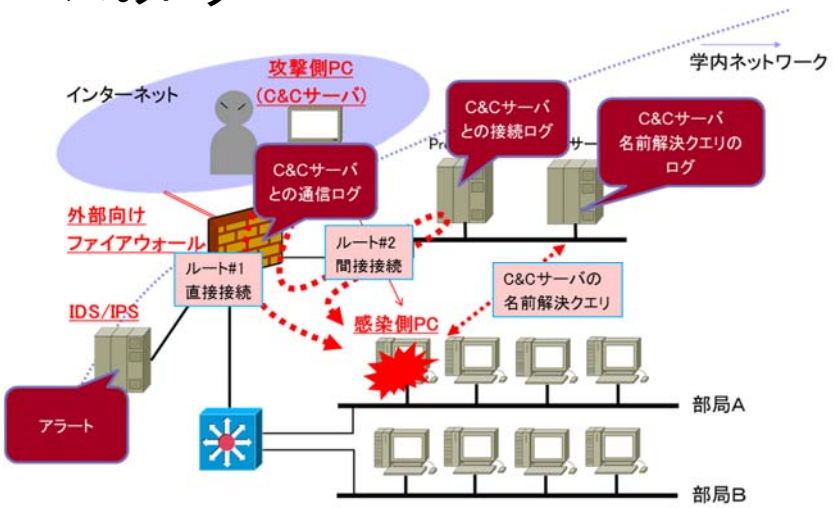
3. 事後対策
   - □「内部侵入・調査」の兆候をいち早く検知する仕組み
   - □「内部侵入・調査」の拡大がやりにくいネットワークの構築

補足1.　被害拡大の防止

- ■ 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

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

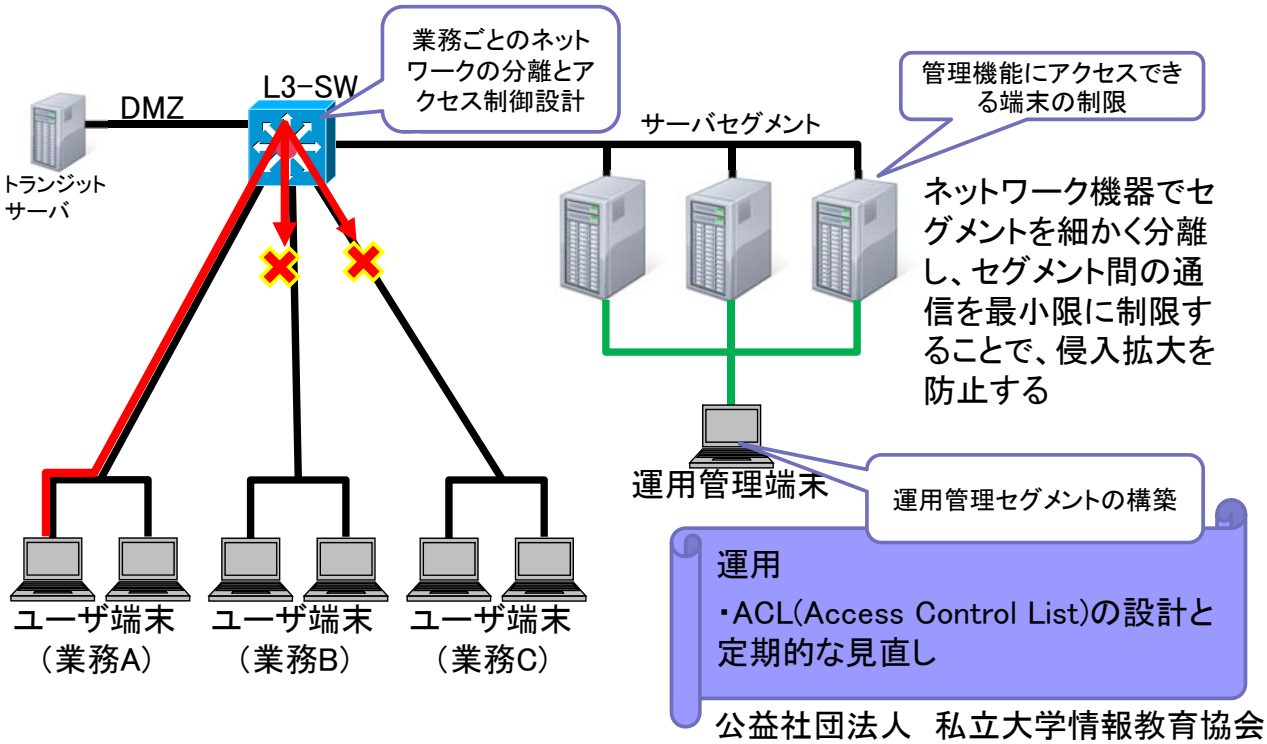


補足3. 事後対策

- ネットワークレベルの対策
  - ① ネットワークの分離設計とアクセス制御
    - 業務ごとにサブネットを分割
    - ユーザ端末とシステム管理用端末の分離
- 端末レベルの対策
  - ② ユーザ端末間のファイル共有禁止
  - ③ オートコンプリートの禁止
  - ④ キッティング時に設定した共通アカウントの削除
- ドメインレベルの対策
  - ⑤ 管理者権限アカウントのキャッシュ禁止
- 監視の強化
  - ⑥ トラップアカウントによる認証ログの監視と分析

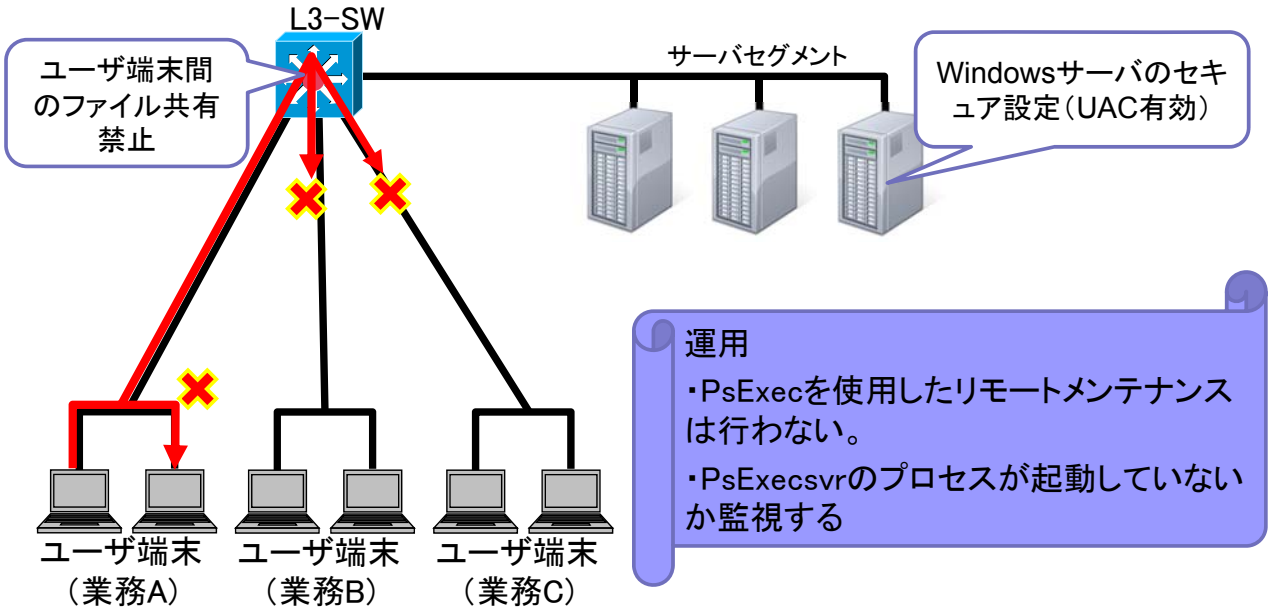
①ネットワークの分離設計とアクセス制御

- 攻撃者の侵入範囲の限定およびサーバへの侵入拡大防止が目的



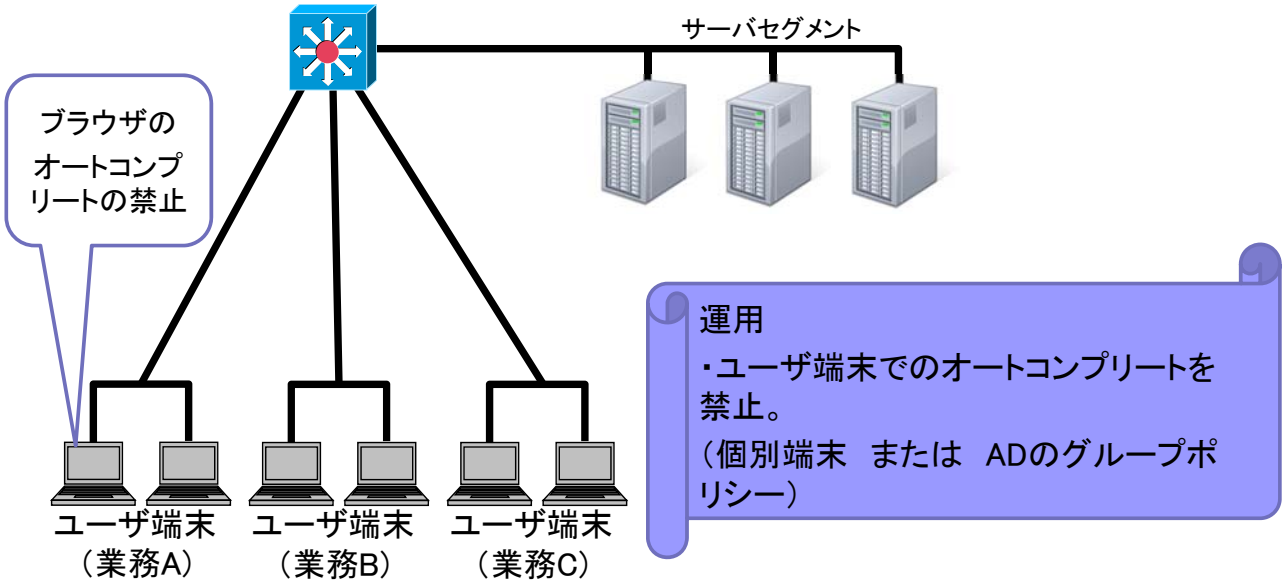
②ユーザ端末間のファイル共有禁止

- ユーザ端末から必要な通信先(File Serverなど)に限定したファイル共有を許可することにより、侵入拡大を防止することが目的



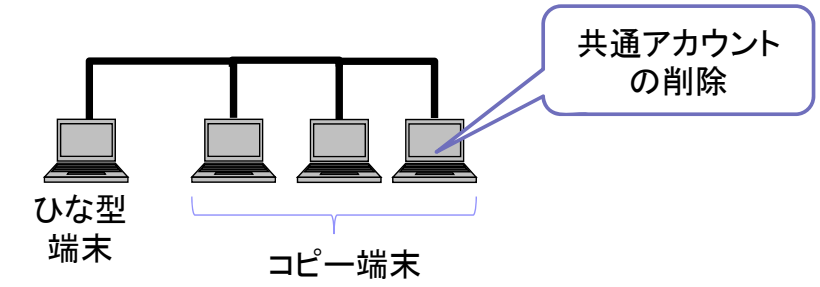
③オートコンプリートの禁止

- 認証情報（ID/PW）が端末上に保存されることを抑制。攻撃者に窃取され内部サービスへの侵入拡大を防ぐことが目的



④キッティング時に設定した共通アカウントの削除

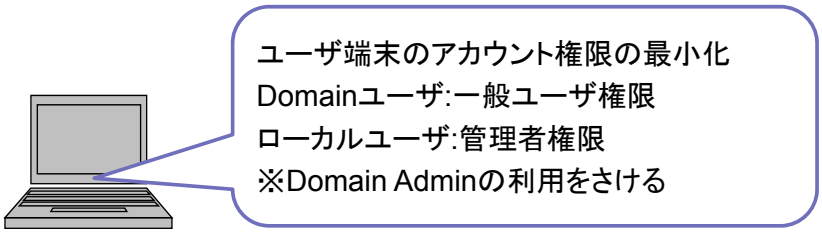
- ひな型を複数のPCに展開する際、同じアカウントがコピーされてしまう。これを削除することにより、Pass the Hash攻撃による他端末への侵入拡大を防ぐことが目的



運用
・共通アカウントを削除

⑤管理者権限アカウントのキャッシュ禁止

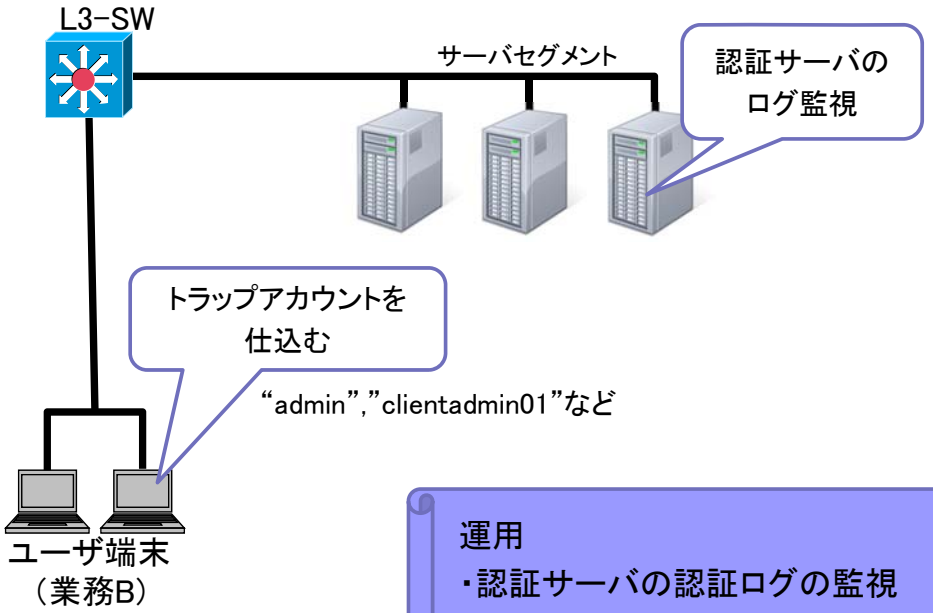
- リモートからのパッチ配布などの管理者権限が必要な運用を維持しつつ、各サーバに影響を与えないアカウント運用を実現することが目的



運用
・ユーザ端末でのDomain Adminでログインを禁止。
・ユーザ端末でDomain Adminグループのユーザがログインしていないか定期的に確認。

⑥トラップアカウントによる認証ログの監視と分析

- ユーザ端末上で通常業務で使用しないトラップアカウントを仕込み、重点的に監視を行うことで、不正なアクセスと正常なアクセスを見分けることが目的



運用
・認証サーバの認証ログの監視