A-2.
痕跡調査のための事前対策

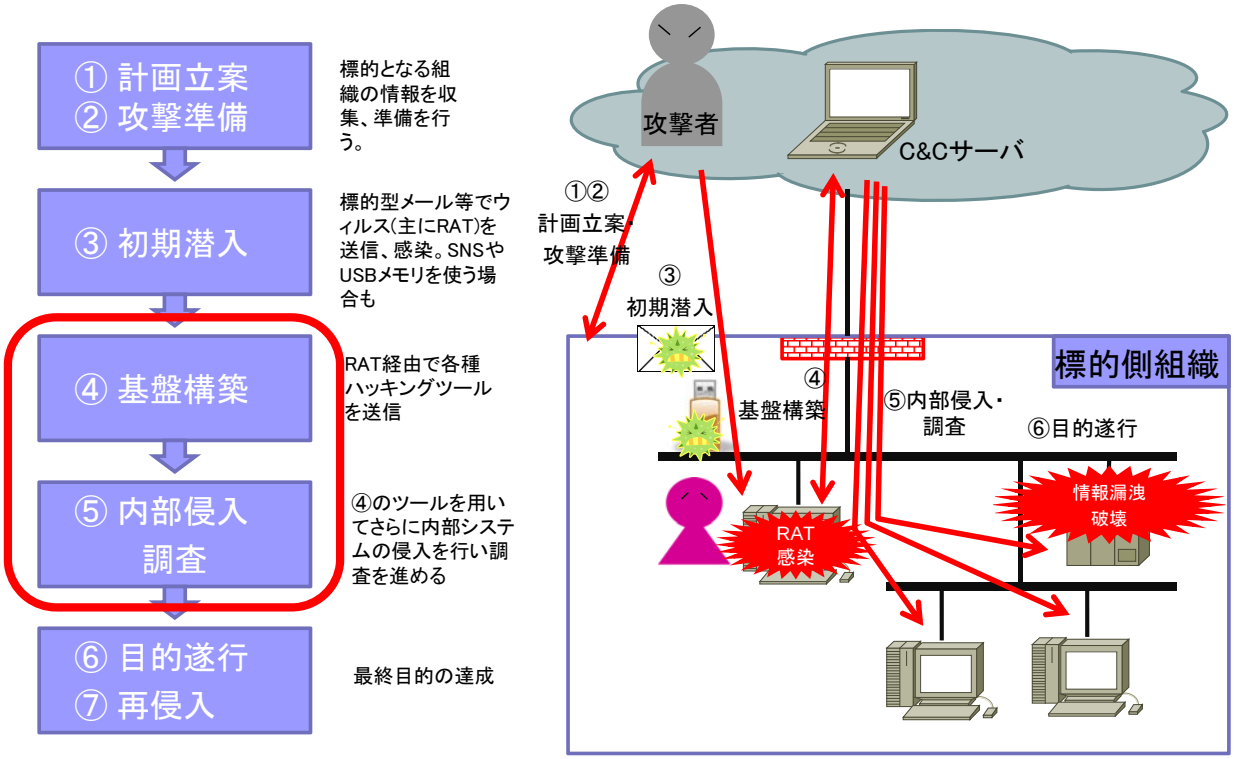
金城学院大学
西松　高史

このセッションの目標

マルウェア感染の事実や情報漏洩したファイルを調査するため、
あらかじめPCに設定すべき項目を確認する
（1） Windowsのイベントログ取得に関するデフォルト状態を
把握する
（2） 考えられる監視強化方法を検討し実施する

**サイバー攻撃を受けたときの痕跡調査が
ある程度できる環境を構築する**

標的型攻撃の流れ



インシデント対応フローチャートに沿った対応

1. インシデント発覚
2. 事実の確認・一次対応
3. インシデント対応に関する体制、手順の確認
4. インシデント情報の集約
5. 被害（情報漏えい）の調査・予想
6. 対外的窓口の設置
7. インシデント情報公開の時期と公開内容の検討
8. 再発防止計画

「痕跡調査のための事前対策」

痕跡調査のための事前対策

- きっかけはいろいろありますが…
  - 利用者から何か動きがおかしいと連絡が来た。
  - 変なファイルをクリックしたと連絡が来た。
  - 外部から連絡が来た。
- 担当者としては…とりあえず、現場で確認
  - コントロールパネル
  - イベントログの確認

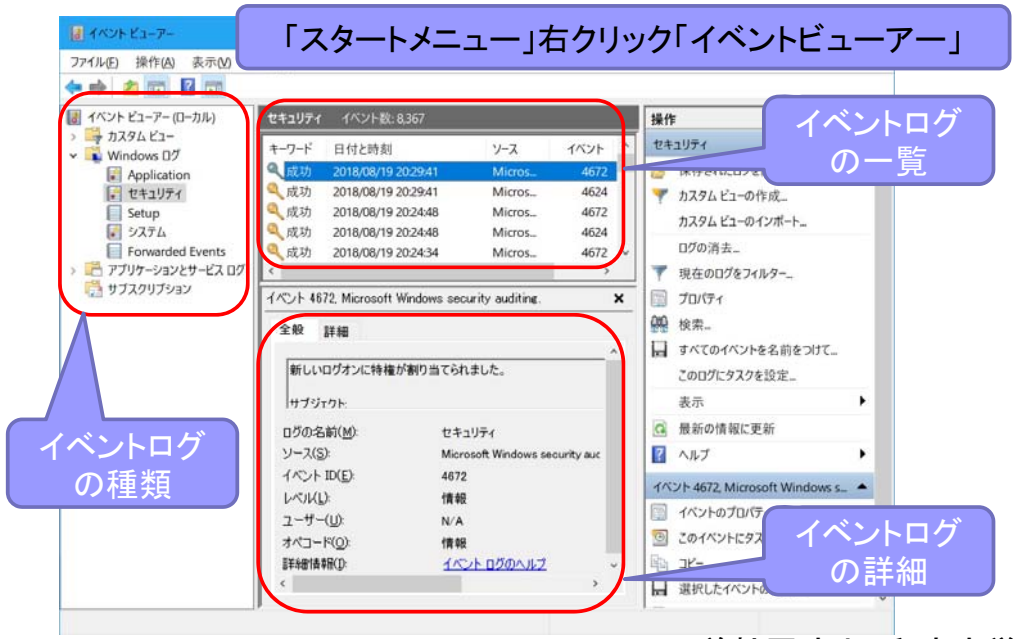
現場でアレ？とならないようにWindowsの設定でいくつかの内容を確認しておく。また、問題があれば設定強化などの対策を行う。
外部に調査依頼をするのか、しないのか、報告をどこまで行うのかなどを考えるためにもある程度の調査はできるようにしておきたい。

痕跡調査のための事前対策

- イベントログ
  - Windowsシステム内で起こった事象や動作の記録
  - イベントログの種類によって分けられる
    - アプリケーション、セキュリティ、システムなど
  - イベントログのレベル
    - 情報、警告、エラーの3段階
      - 情報：大きな問題になりにくい事象や動作の記録、参考情報
      - 警告：データの欠損を伴わない軽度のエラー
      - エラー：OS、デバイスドライバ、Windowsサービスの起動エラーなど深刻なエラー（失敗なども含まれる）

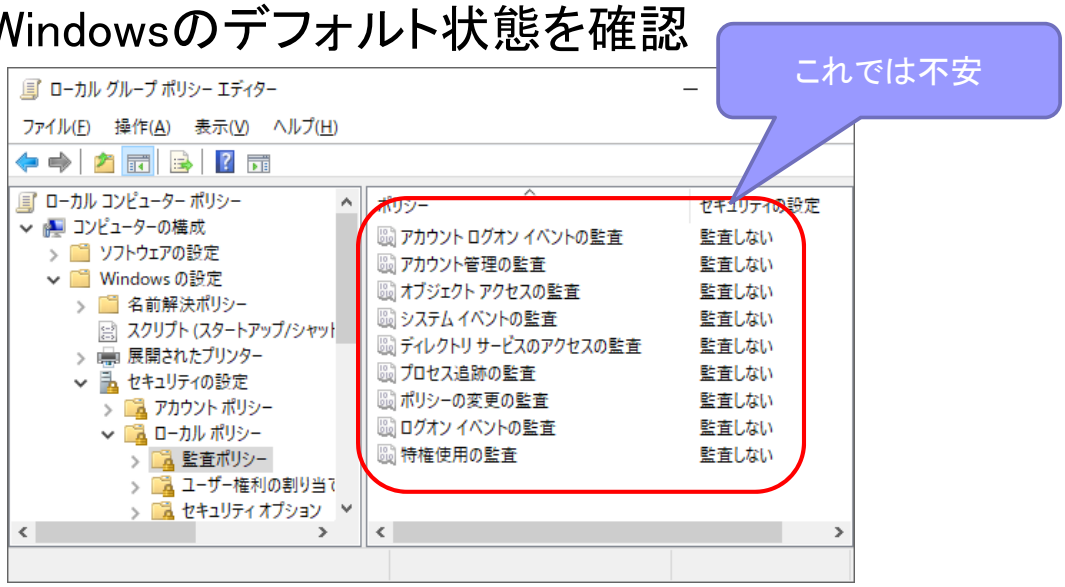
痕跡調査のための事前対策

- イベントログの確認方法
  - イベントビューアー



痕跡調査のための事前対策

- Windowsのデフォルト状態を確認



また、Windowsで標準的に搭載されている基本的なツールについては実行したイベントログが残るが、PowerShellやWindowsに搭載されていない後からインストールしたツールのほとんどはどこにも残らない

痕跡調査のための事前対策

- Windowsの設定で対応
  - イベントログ保存のための設定
    - 時刻の同期
      - 時間がずれていると時系列がわからなくなる
      - ADサーバとの時刻同期（ADサーバの時刻も確認）
      - 仮想システムの場合、同期していない場合があるので注意
    - ログ格納エリアの容量とログローテーションの設定

あとで解説

      - 12ヶ月程度必要
      - ディスク容量の確認
      - 別サーバでイベントログの保存（集中管理）
        - WinRMなどを利用

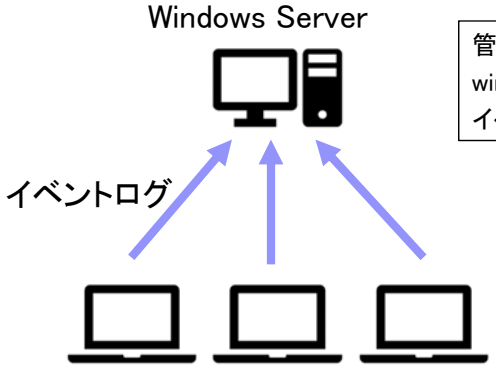
痕跡調査のための事前対策

- 別サーバでイベントログ保存
  - Windowsでもイベントログの集中管理ができます。
  - 有償の資産管理システムなどで各端末のイベントログを集中管理する機能もありますが、Windows OSにもWinRMを利用した設定が可能です。

被害端末のイベントログは消されてしまうことがあるため、別サーバで管理することも有効

痕跡調査のための事前対策

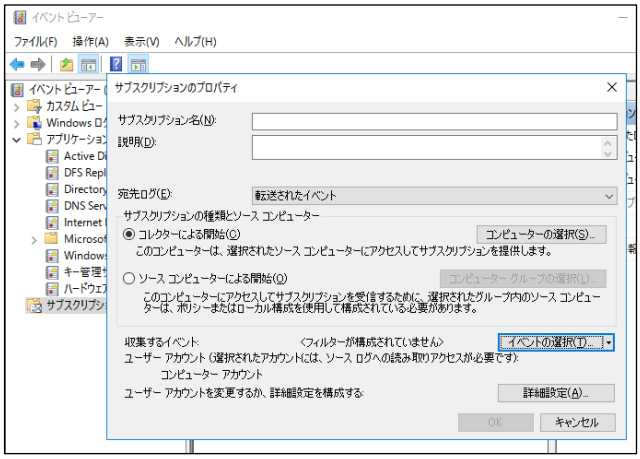
- 別サーバでログ保存



Windows 10など

管理者権限のコマンドプロンプトで
winrm quickconfig

管理者権限で
winrm quickconfig
イベントビューアの「サブスクリプション」を設定



痕跡調査のための事前対策

- ログの保存期間
  - 総務省は曖昧な書き方
    - 国民のための情報セキュリティサイト
    - http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/22.html
    - 保存期間に関しての明記はない。
  - 一般社団法人JPCERTコーディネーションセンター
    - 高度サイバー攻撃への対処におけるログの活用と分析方法　1.0版（2015年11月17日）
    - https://www.jpcert.or.jp/research/APT-loganalysis_Report_20151117.pdf
    - P.12 コラム「ログ保存期間に関する考え」
    - 1年以上にすることが望ましい。

比較的、納得できる

では、何年が良いのか？ → 結局、全部必要かも

痕

■ I

コラム

ログ保存期間に関する考え方

ログ保存期間は、次のように決めることが望ましい。

① ログを採取すべきシステムそれぞれのログの量を見積もる。
② 攻撃を受けていた場合には、どの程度まで過去に遡って調査する必要があるのかと、ログの長期保存に伴うコストとのトレードオフを考慮して保存期間を決定する。

JPCERT/CC では、インシデント対応支援や高度サイバー攻撃の調査等の結果から、ひとつの参考値として 1 年分のログを保存することを推奨している。しかしながら、長期間にわたる高度サイバー攻撃や、採取したログを統計的に調査して初めて検知できるマルウエアもあるため、ログを調査すべき期間は長引く傾向にある。次は、ログ保存期間について参考となる情報である。

- Mandiant 社の「APT1」のレポートによれば、標的型攻撃は平均で 1 年程度、最長では 4 年 10 ヶ月継続している。(*3)
- 内閣サイバーセキュリティセンター (NISC) は、平成 24 年にログ保存期間として 1 年以上を推奨している。 (*4)
- PCIDSS (Payment Card Industry Data Security Standard) では、即時にアクセスできるオンラインに保存で 3 か月間、オフライン保存で 1 年間を監査証跡の履歴保持に関する要件 (10.7) としている。 (*5)
- 独立行政法人情報処理推進機構 (IPA) は、標的型攻撃メールが 9 組織に対して 31 ヶ月間に渡り送られる攻撃を確認したと平成 27 年に報告している。 (*1)

ログ保存期間は 1 年以上にすることが望ましい。しかしながら、ログを長期間保存すると次の様な問題が生じる。

- 記憶媒体 (テープや光ディスクなど) が大量に必要となる

痕跡調査のための事前対策

- マルウェアの最新動向
  - ファイルレスマルウェア
    - マルウェアに埋め込まれた命令を実行する際、PowerShellなどの信頼性が高いプログラムを利用するため、その命令は正当なものとして扱われる。
    - ストレージには何も書き込まれないため、今後、対応する可能性はあるが、現状ではシグネチャベースのアンチウイルスソフトウェアなどの標準的なセキュリティ製品は弱体化するか、または完全に役に立たない。

あやしいPowerShellのスクリプトを某ウイルスチェッカーの入ったPCに置いていて、何も反応がなかったので、Windows10のみ入ったマシンで同じことをしたらWindows Defenderが反応してびっくりしたことがあります。

痕跡調査のための事前対策

- Windowsのイベントログ監視強化（1）
  - 監査ポリシー変更（有効化）
    - Windowsに標準で搭載されている詳細なイベントログを取得するための設定
  - PowerShellのイベントログ採取
    - PowerShellの詳細なイベントログを取得するための設定
  - 時刻の同期確認
    - ADに参加している場合は気にすることがないと思われるが、サーバとの連携が切れている場合やADサーバ自体の時間がずれていることがあるので確認する。

痕跡調査のための事前対策

- Windowsのイベントログ監視強化（2）
  - Sysmonのインストール
    - マイクロソフトが提供するツールで、システムのスタートアップからシャットダウンまでの間、プロセスの作成、ネットワーク接続、ファイルの作成日変更のアクティビティを監視して、イベントログに記録する。内容はイベントビューアーで確認することができる。
  - イベントログ容量の最大サイズの変更
    - 12ヶ月程度、イベントログが保存できるような設定を行う。PCの利用方法によって、イベントログの量が変わるので、確認が必要である。

痕跡調査のための事前対策

- イベントログ、実行履歴、レジストリエントリ
  - 専用のフォレンジックソフトウェアやフォレンジックに関する知識がなくても可能
  - イベントビューアーを利用
- 攻撃手法の研究
  - 攻撃者によって使われることが多い代表的なツールを実行した痕跡を探す

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（第2版）」：2017-11-09
https://www.jpcert.or.jp/research/ir_research.html

痕跡調査のための事前対策

- ツール分析結果
  - 攻撃者がよく使うツールについて痕跡調査結果を解説している。

JPCERT/CC
「ツール分析結果シート」
https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/

ダウンロードしたものを「A2」フォルダーに置きました。
時間があるときに見てください。
「ToolAnalysisResultSheet_jp-master¥index.html」

実習

実習

1. Windowsの設定強化

- 監査ポリシー変更
  - ローカル　グループポリシー　エディター
- PowerShellのイベントログ採取の設定
  - ローカル　グループポリシー　エディター
- 時刻の同期確認
- Sysmonのインストール
  - マイクロソフト社のサイトからダウンロード
- イベントログ容量の最大サイズの変更
  - イベントビューアー

実習

2. イベントログの確認

- イベントビューアーで確認
  - 監査ポリシー
  - PowerShell
  - Sysmon

まとめ

- 事前準備
  - 監査ポリシーの有効化とsysmonのインストール
    - PowerShellのイベントログも必要
  - イベントログの容量と時間同期の確認
- 連絡があれば、とりあえずイベントビューアーで確認
  - 攻撃者がよく使うコマンドの実行履歴
- 無理をせず、プロにフォレンジックを依頼
- 対策製品の導入
  - 対費用効果

参考資料

- JPCERTコーディネーションセンター（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
- マクニカネットワークス
  標的型攻撃の実態と対策アプローチ　第1版
  - http://www.macnica.net/security/report_01.html