A-1.
セキュリティインシデント分析コースの概要

青山学院大学
根本　貴弘

本コースの概要

- 1．標的型サイバー攻撃による情報窃取

  情報窃取・情報流出のリスクと手口，インシデントレスポンスの基本的な流れについて確認する

- 2．標的型サイバー攻撃のインシデントレスポンス演習

  不正通信の痕跡調査，情報流出の拡大を防ぐための緊急対応手段について技術的な理解の促進を図る

標的型サイバー攻撃とは

- 情報窃取を目的とし，特定の組織を対象に継続的に行われる一連のサイバー攻撃
  - 攻撃対象
    - 政府，官公庁，企業など，重要情報を持つ組織
    - 上記に関連する他組織や個人が一時的な攻撃対象となる場合もある
    - 不正プログラムをばらまき，侵入に成功した組織

- 事前調査の後，対象組織の端末に不正プログラム(主にRAT ※1)を侵入させ，C&C通信※2による遠隔操作で情報窃取のための基盤構築，内部調査を行い目的を遂行する

※1　Remote Access Tool．ユーザがコンピュータを遠隔操作するためのツール

※2　攻撃者サーバからの命令(Command)を受信し，不正プログラムを制御(Control)する通信

  - 不正プログラムを侵入させるために様々な手口が使われる
    - メール(「連絡」を装う手口，「やりとり」を伴う手口など)
    - Web閲覧(水飲み場)
    - ソフトウェアアップデートの悪用
    - USB
    - ソーシャル・エンジニアリングを用いず直接システムの脆弱性をつく

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

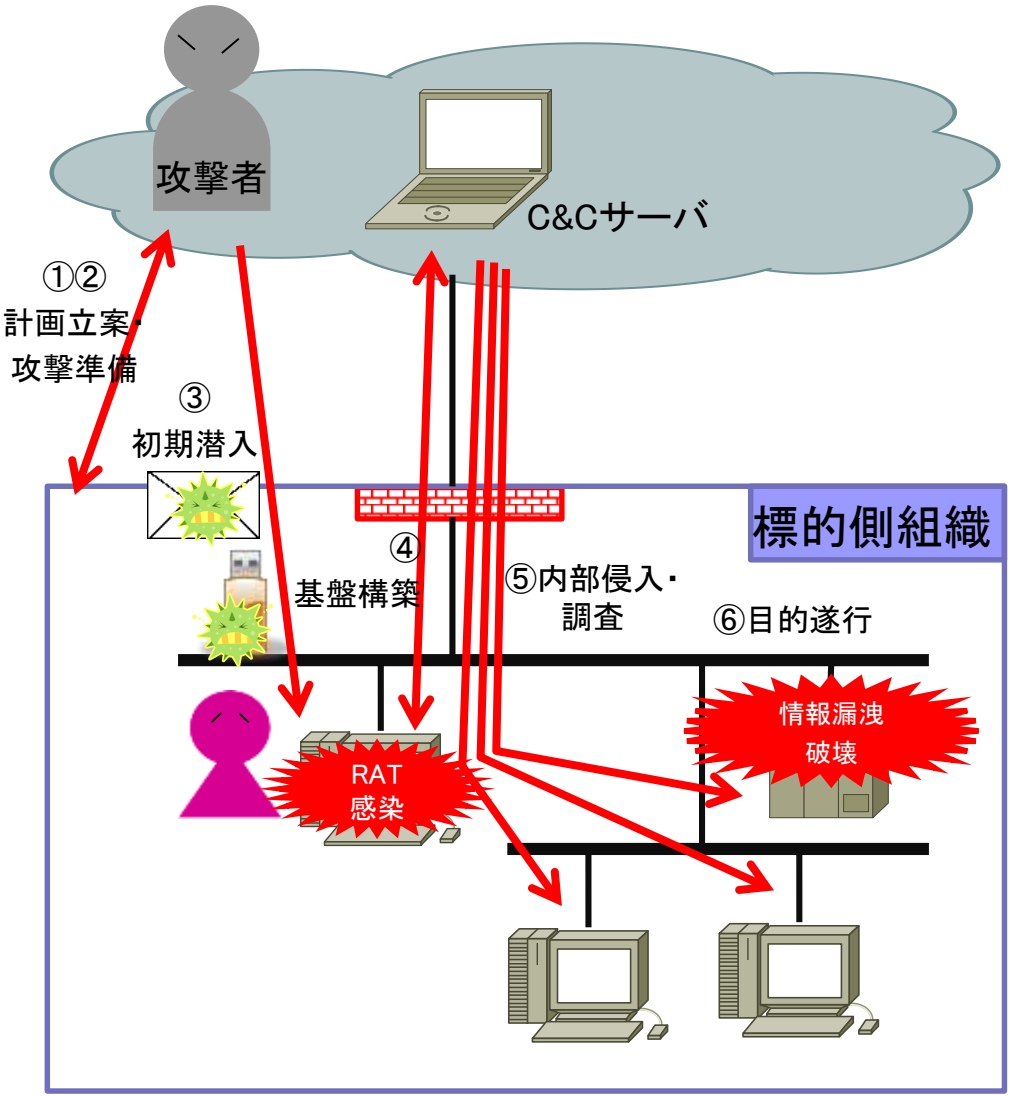
RAT経由で各種ハッキングツールを送信

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



標的型攻撃メールとは

- 情報窃取を目的として特定の組織に送られるウイルスメール [1]
  - 送信者名として，実在する信頼できそうな組織名や個人名を詐称
  - 受信者の業務に関係の深い話題や，詐称した送信者が扱っていそうな話題
  - ウイルス対策ソフトを使っていてもウイルスが検知されない場合が多い
  - メールが海外のIPアドレスから発信される場合が多い
  - 感染しても，パソコンが重たくなるとか変なメッセージが表示されることは余りない
  - 外部の指令サーバ（C&Cサーバ）と通信
  - 長期間にわたって標的となる組織に送り続けられる（内容は毎回異なる）

[引用1] IPA（独立行政法人 情報処理推進機構）：標的型攻撃／新しいタイプの攻撃の実態と対策（2011年11月）
https://www.ipa.go.jp/files/000024542.pdf

[参考] 平成27年の傾向
- 標的型メール攻撃件数：3,828件（過去最多）
  - ばらまき型：3,508件　（平成26年は1,474件，平成25年は259件）
  - **ばらまき型以外：320件（平成26年は249件，　平成25年は233件）**
- 添付ファイルのファイル形式
  - Word文書：53%　（平成26年は2%）
  - 圧縮ファイル：40%　（平成26年は97%）

標的型攻撃メール

[参考] 警視庁：平成27年におけるサイバー空間をめぐる脅威の情勢について（2016年3月）
https://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf

標的型攻撃メール例(「連絡」を装う手口)

- 業務連絡を装うメール．複数の組織を標的としたようなメールもある
  - 内部組織や外部組織，複合機からの連絡メールを偽装したもの

[参考] 青山学院大学情報メディアセンター:
【注意喚起】添付ファイルの付いた不審なメールについて(2015年10月)http://www.aim.aoyama.ac.jp/c/4662/
【注意喚起】人事課を装った添付ファイル付きの不審なメールについて(2016年1月)http://www.aim.aoyama.ac.jp/info/aim/5052/
【注意喚起】文部科学省を装った添付ファイル付きの不審なメールについて(2016年5月)http://www.aim.aoyama.ac.jp/info/aim/5607/

[送信元アドレス] RNP0026738E40D2@aoyama.ac.jp
[件名] Message from “RNP0026738E40D2”
[内容]
このメールは『RNP0026738E40D2』(MP C5503 JPN)から送信されたものです。

読み取り日時: 2015.10.08 7:20:34 (+0900)
問い合わせ先: xxxx@aoyama.ac.jp

西東京複合機より送信

添付されていたファイルは，
「Word文書」形式

- 「ばらまき型メール」の日本語化・巧妙化に伴い，標的型攻撃と同等のリスクの懸念
  - クロネコヤマト，日本郵便の配達通知メールを偽装したもの

[参考] ヤマト運輸:ヤマト運輸の名前を装った添付ファイル付きの不審メールにご注意くださいhttp://www.kuronekoyamato.co.jp/info/info_160629.html
[参考] 日本郵便:日本郵便を装った不審メールにご注意ください.
http://www.post.japanpost.jp/notification/notice/2016/0607_01.html

標的型攻撃メール例(「やりとり」を伴う手口)

- はじめから攻撃(不正プログラムの送付)を行わず，偵察を通じ標的組織からの返信を待ち，返信のあった連絡先に対して攻撃を行う
- 事前調査で盗みとった業務メールの文面が利用される場合もある

表 2014年10月の「やり取り型」攻撃の事例(メールの流れ) [2]

No.	種別	内容
1	偵察	某所の研究員を名乗る者から，当該組織がウェブサイトで公開している記事への質問について，問い合わせ窓口の確認の無害なメールが届いた．宛先のメールアドレスは，当該組織のウェブサイトから知ったと書かれていた．
2	返信	質問を受け付ける旨，返信した．
3	攻撃	「質問内容を送付する」という内容で，**パスワード付きzipファイル**が添付されたメールが届いた．更に，**パスワードは別途送付する**旨が書かれていた(このzipファイルの中には，Word文書ファイルのアイコンに偽装した実行ファイル形式のウイルスが入っていた)．
4	偵察	約1分半後，zipファイルのパスワードを通知するメールが送られた．メールの文面には，「このメールは自動で配信されています．」などと書かれており，**メール暗号化システムが自動的にパスワードを作成・送付しているかのように見えるものに偽装**されていた．
5	返信	添付ファイルの内容が確認できなかったこと，そして，**メール本文に用件を記載して再送いただくよう**返信した．
6	偵察	約40分後，記事の内容に関する質問が**メール本文に書かれて**再送されてき

[引用2] IPA(独立行政法人 情報処理推進機構):組織外部向け窓口部門の方へ:「やり取り型」攻撃に対する注意喚起 ～ 国内5組織で再び攻撃を確認 ～
https://www.ipa.go.jp/security/topics/alert20141121.html

総合演習の概観（24日実施）

「標的型攻撃による情報窃取に対するインシデントレスポンス」

- 目標：
  情報流出インシデントに対し，その事実の確認および対応についてSJK大学インシデント対応フローに沿い，
  - システム技術担当者（情報部門技術者）…　セキュリティインシデント分析コース受講
  - セキュリティ施策管理者（情報部門管理者）…　セキュリティ政策・運営コース受講者
  - CISO　…　運営委員

  の三者の協働作業を机上演習体験し問題点等について，組織的な解決策を討議し，インシデント対応フローで対応可能不可能な状況を確認する．また，大学特有の問題点について洗い出しを行う

- 想定シナリオ：
  私立SJK大学（学生数4000人・教職員数400人）の学生個人情報の流出対応
  外部から電子メールで上記の通知があり，これに対しSJKインシデント対応フローに沿い，対応をする（机上演習）

- 演習手順概要：
  - 4フェーズ（①検知／②調査および対応（封じ込め）／③回復・復旧／④事後対応）に分け，演習（対応）を行う
  - フェーズ毎にCISOに報告する（報告に対するCISOの対応判断はすべて「Yes」とする）
  - 報告（議論の要約、問題点等）は，時系列にまとめる

本コースの位置付け

インシデント対応フローチャートに沿った対応

1. 外部からの指摘
2. 事実の確認・一次対応
    1. ネットワークレベルでの調査・対応
    2. PCレベルでの調査・対応

本コースの対象

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

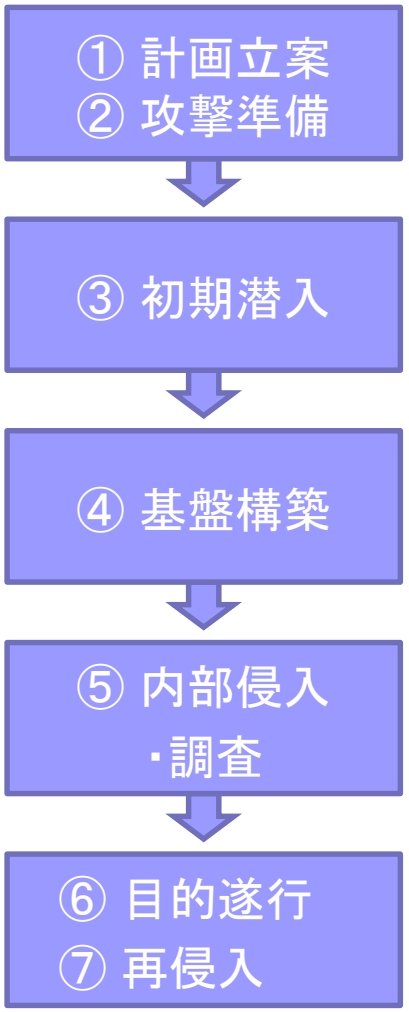
本コースのプログラム

A-1　セキュリティインシデント分析コースの概要

A-2　標的型サイバー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

A-3　標的型サイバー攻撃の調査と対応(ネットワーク編)

A-4　標的型サイバー攻撃の調査と対応(PC編)



A-2の概要

- 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
  - Ratを使った初期潜入
  - 内部情報窃取ツールのインストール
  - 内部ネットワークの調査

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

A-3の概要

- 標的型サイバー攻撃を受けた時の「ネットワーク機器の痕跡調査」と「一時対応」手法を学び実習にて確認する
  - ファイアウォールでの痕跡調査
  - IPS/IDSでの痕跡調査

1. 標的型サイバー攻撃を受けた時にネットワークレベルでの調査・対応が行えるようになる

A-4の概要

- 標的型サイバー攻撃を受けた時の「PCの痕跡調査」と対応を学び，実習にて確認する
  - 攻撃者がよく使うWindowsコマンド
  - PCのログの確認（痕跡調査）

1. ログ取得の準備をし，確認することができる
2. 被害範囲の予測・調査を行うことができる
3. PCの調査・対応が行えるようになる