A-2.
標的型攻撃などが疑われる場合の診断と初動対応の演習

東海大学
東　永祥

このセッションの目的

標的型攻撃に対する認識の再確認

（1）標的型攻撃と思われるメールを受け取った場合の初動対応を理解する
（2）サンドボックス（仮想環境）の使い方、有効性を理解する

はじめに

標的型攻撃とは

- 標的型攻撃の定義と特徴
  - 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

【定義】
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

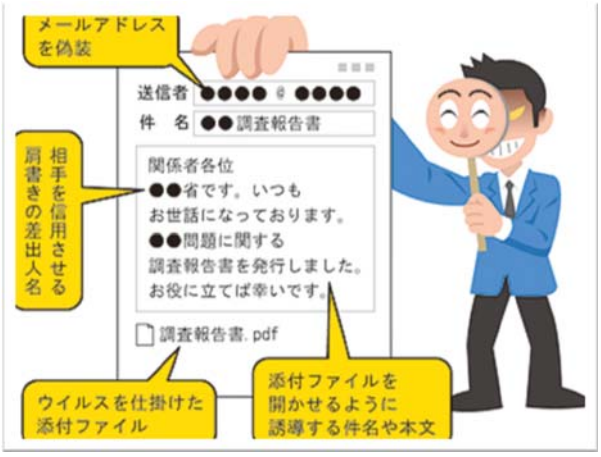
【特徴】
- 送信者名として、実在する信頼できそうな組織名や個人名を詐称
- 受信者の業務に関係の深い話題や、詐称した送信者が扱っていそうな話題
- ウイルス対策ソフトを使っていてもウイルスが検知されない場合が多い（※1）
- メールが海外のIPアドレスから発信される場合が多い（※2）
- 感染しても、パソコンが重たくなるとか変なメッセージが表示されることは余りない
- 外部の指令サーバ（C&Cサーバ）と通信（※3）
- 長期間にわたって標的となる組織に送り続けられる（内容は毎回異なる）

標的型攻撃とは（※1、2、3 補足）

- ウイルス対策ソフトで検知できない理由
  - 特定の組織や人を狙いとして送信されるため、セキュリティソフトベンダーが把握する前に対象者にメールが届いてしまうことが多いため
  - ウイルス対策ソフトで検知できればもうけもの

- 海外のIPアドレスからの送信も当たり前になってきた？！
  - クラウド化の加速により、メールシステムを外に出す大学、企業が増えてきた
  - ベンダーによっては、国外サーバを利用してサービス展開している場合もある
  - 送信日時やタイムゾーン、その他ヘッダーに書かれている情報も重要
  - ・・・でも、それにも限界がある？！

- 遠隔操作ウイルスによる被害の拡大
  - 添付ファイルや本文添付のURLにアクセスすることでRATなどの遠隔操作ウイルスに感染
  - 新たなウイルス感染、拡散、情報漏洩などの被害拡大につながる場合がある



事例から考える標的型攻撃1

（画像　IPA情報処理推進機構）
http://www.ipa.go.jp/security/keihatsu/pr2012/general/02_targeted_attack.html

標的型攻撃の流れ

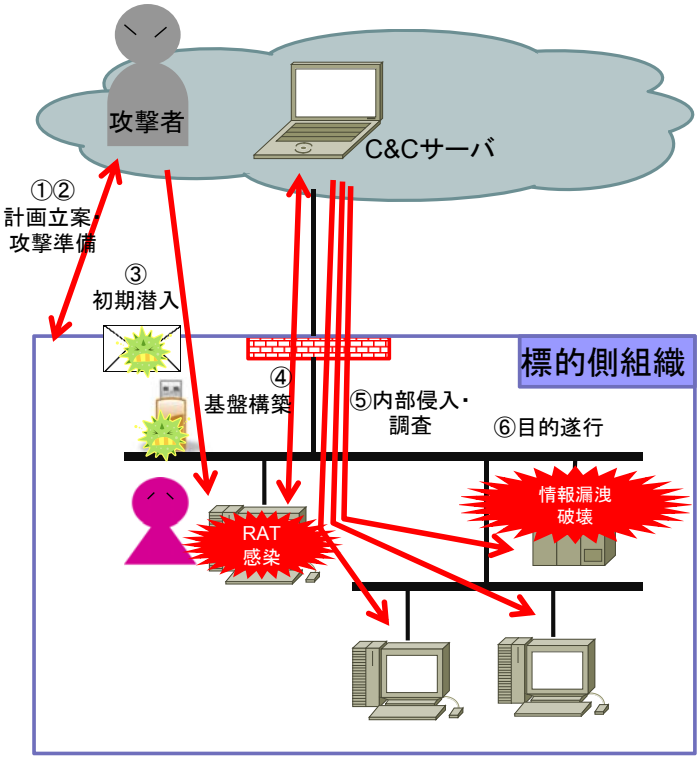
① 計画立案
② 攻撃準備
標的となる組織の情報を収集、準備を行う。

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



標的型攻撃への対策

- 入口（感染前）対策を頑張る？　出口（感染後）対策を頑張る？
- 入口対策で思いつくもの
  - ファイアウォール
  - 侵入検知システム（IDS）
  - 侵入防止システム（IPS）
  - ウイルス対策ソフト

→
- 完璧を求めるならば、それなりの費用コストが掛かる
- 攻撃手法、騙しのテクニックが多彩なため、対応しきれない

- 入口対策を強化するのも限界がある
- 現実問題、標的型攻撃の侵入を防ぎきることは難しい（と考えて行動をするべきである）
- と言うことは・・・

標的型攻撃への対策

- 出口対策の強化も図っていく必要がある
  - 「感染した・侵入された」ことを想定して、その影響・被害を小さくするための対策強化
  - 入口対策を放棄するわけではない（入口対策と＊併せて＊やるべきこと）

- 出口対策として取れることは
  - 技術的対策
    - ネットワークトラフィックを監視、学内から学外に向けて怪しい通信が行われていないか常に意識を払っておく
    - ファイアウォールやプロキシサーバーを導入し、学内から学外に向けての通信から、怪しい動き（宛先IPアドレス、通信量、など）をしている端末がないか調べる
  - 管理者としての心構え
    - 学内で標的型攻撃による被害が発生した可能性が出た際に、どれだけ冷静、且つ的確な対応が取れるかがポイント
    - 初動対応によって、被害の程度・範囲を小さくできる
    - 対応方法を多く知っていることが、対策の幅を広げる

このセッションで学ぶこと（1）

標的型攻撃への対策

- 入口でも出口でもない場所での対策

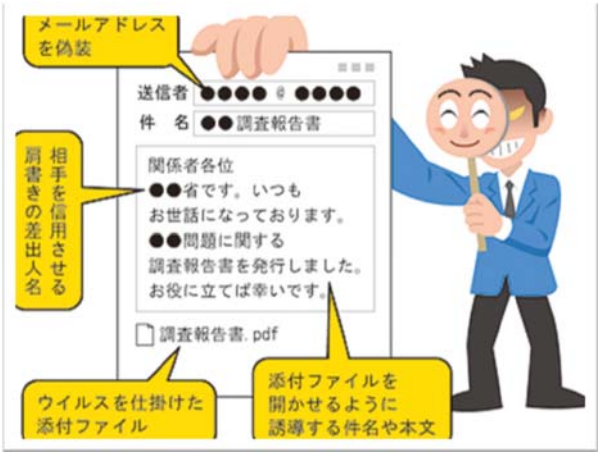
- 『利用者教育』の重要性
  - 怪しい添付ファイルは開かない
  - 怪しいメール本文にあるURLにアクセスしない

- 繰り返し、定期的な啓発活動が大切
  - 情報システム部門だけの力では限界がある？
  - 大学としての体制作りも必要

標的型攻撃対応の基本概念

標的型攻撃かどうかの判断

- 標的型攻撃なのかどうかを判断するのは難しい
  - 経験によって判断がつくようになる
  - 一般的な考え方を勉強しておくことも大切
- 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
- 本コース別添資料
  「迷惑メール対応基本フロー」
- 標的型攻撃かどうかを判断することも、初動対応の1つ



事例から考える標的型攻撃2

（画像　IPA情報処理推進機構）
http://www.ipa.go.jp/security/keihatsu/pr2012/general/02_targeted_attack.html

標的型攻撃の可能性が高い場合の対応

ここからは少し趣向を変えます

- より現実的な対応イメージを持つための背景を用意しました

背景

あなたは私立SJK大学の情報システム部門に勤めている職員です。SJK大学では、省庁や大学を狙った最近の標的型攻撃事情を受け、学内の教職員への注意喚起を積極的に行ってきました。

そんな中、注意喚起の効果からか、一人の職員から不審なメールを受け取ったとの相談を受けました。そのメールには添付ファイル（zip形式）もあります。相談してきた職員としては、どうしても中身を確認しなければならないと言われました。

さて、あなたならどうしますか？

大学職員がよく受け取るメール

- 業務連絡を装ったメール　（人事、給与）
- 取引先を装ったメール　（案件、見積り）
- 冠婚葬祭を装ったメール　（社員、親族）
- 苦情を装ったメール　（苦情窓口への攻撃）

表題：　人事研修の開催要項について

服部様。
標記研修の開催につきまして，ご参加いただきますようお願いします。
開催要項は、下記URLをご覧ください。
http://123.45.67.89/seminar.zip
事前課題につきましては後日改めてご案内いたします。

大学職員がよく受け取るメール

- 業務連絡を装ったメール　（人事、給与）
- 取引先を装ったメール　（案件、見積り）
- 冠婚葬祭を装ったメール　（社員、親族）
- 苦情を装ったメール　（苦情窓口への攻撃）

表題：　貴学学生の態度について
添付：  証拠写真.zip

私情協大学 御中。
　私は御校の近隣に在住するものです。
　最近、貴学と思われる学生が路上で座り込み、たいへん迷惑です。
　今朝撮影した写真を添付しますので、学生をよろしくご指導ください。

考えられる対応方法例

1. 外部のウイルスチェックで検査をする
2. パソコンにインストールされているウイルス対策ソフトで検査をする
3. 実際にファイルを開いてみて、その挙動をチェックする

考えられる対応方法例

1. 外部のウイルスチェックで検査をする
2. パソコンにインストールされているウイルス対策ソフトで検査をする
3. 実際にファイルを開いてみて、その挙動をチェックする

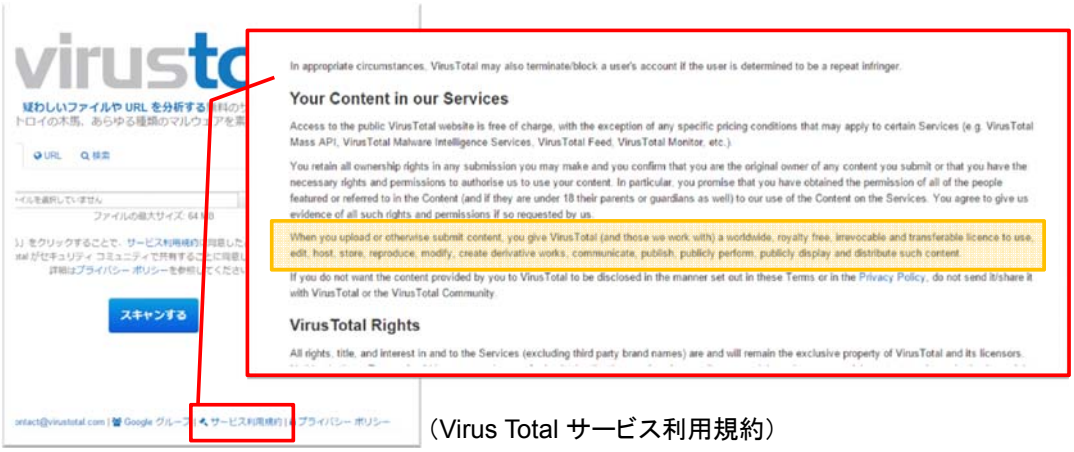
1. 外部のウイルスチェックで検査をする

- Virus Total
  - オンラインサービス（無料）
  - Virus Totalのサイト（https://www.virustotal.com/ja/）に疑わしいファイルを検査することができる
  - 複数のアンチウイルスエンジン（50種類以上）を使ってファイルをチェックする
  - Webブラウザからアクセスすればすぐに利用可能（比較的手軽に利用できる）
  - メールに添付されたファイルを調査したい場合は、メールファイル（eml形式）を検査することも可能

（Virus Total サイトトップ画面）

1. 外部のウイルスチェックで検査をする

- Virus Total利用時の注意点
  - あくまでも『感染しているか』の検査のみで、『駆除』はしてくれない
  - 検査のためにサイトにアップロードしたファイルは、ウイルス／マルウェア研究のためなどに使われる場合がある
    - アップロードファイルを利用する旨は、Virus Totalの「サービス利用規約」に書かれている
    - 機密性の高いメールを本文ごと検査に上げた場合、学外の人にその内容が知られてしまう可能性がある（情報流出？！）



（Virus Total サービス利用規約）

1. 外部のウイルスチェックで検査をする

- Virus Total利用時の注意点
  - パスワード付の添付ファイルまでは検査するのは難しい

- 利用におけるいくつかの注意点はあるが、内容に問題のないファイルを検査する分には有効的な手段の1つ

考えられる対応方法例

1. 外部のウイルスチェックで検査をする
2. パソコンにインストールされているウイルス対策ソフトで検査をする
3. 実際にファイルを開いてみて、その挙動をチェックする

これらの対応を、サンドボックスを使って行うことで、
より安全な調査が可能となる

このセッションで学ぶこと（2）

サンドボックス

- 定義
  - 特定のプログラムを、他に影響を与えないよう保護／隔離された領域で実行することで、当該プログラムの挙動確認やその他システムが不正にアクセスされないようにすることができる環境
- 環境構築
  - アプライアンス製品
    - FortiSandbox（FORTINET社）
    - FireEye（FireEye社）
    - Threat Emulation（Check Point社）
    - WildFire（Palo Alto Networks社）

→
- 導入にそれなりの費用が掛かる
- 最近は各社クラウド版製品も出している

  - 学内ネットワークから切り離されているパソコン
    - 学内利用者提供用、事務処理用などの予備パソコンを利用
    - OSやウイルス対策ソフトのアップデート時のみ学内ネットワークに接続し、調査時には切り離して利用する

→
- サンドボックス用に常に確保することが難しい

サンドボックス

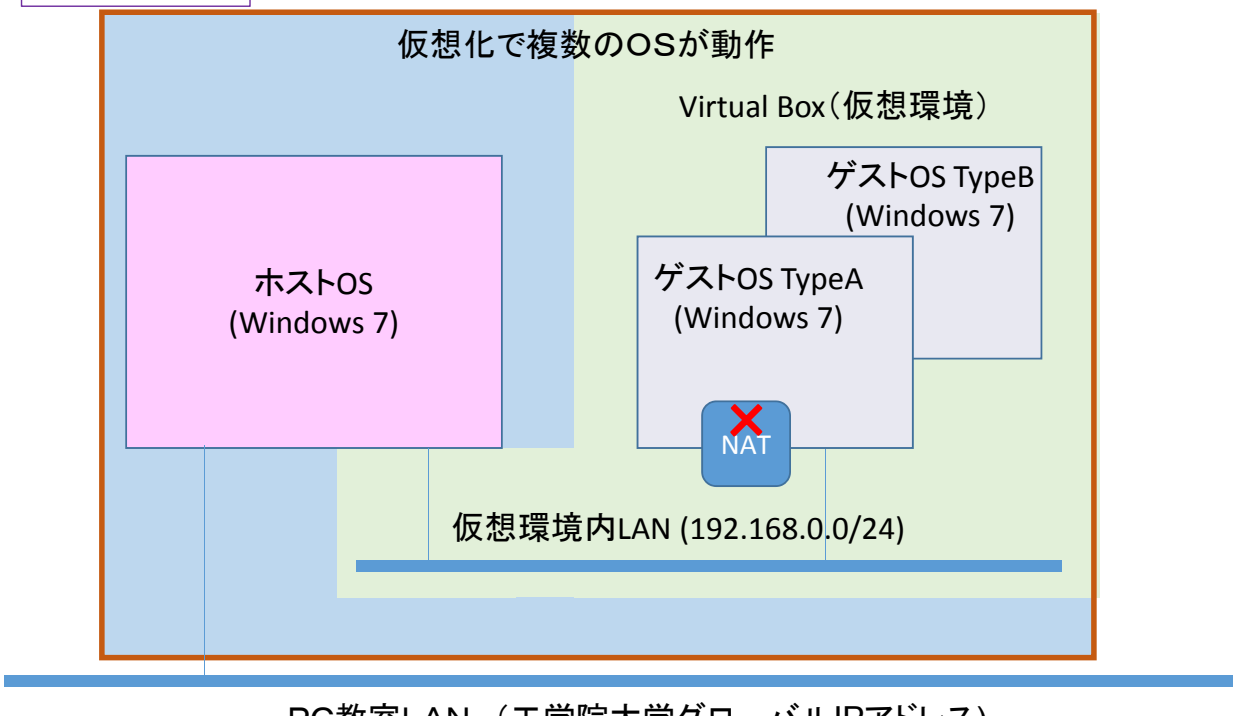
- 環境構築
  - 仮想環境
    - Virtual Box（https://www.virtualbox.org）
    - VMware Player（https://www.vmware.com/products/player）

このセッションの実習環境

- 仮想環境によるサンドボックス構築のメリット
  - 無料ソフトウェアで環境構築が可能
  - 検証環境の維持が容易
    - スナップショットを使って検証前の起動イメージのバックアップを作成することで、検証によってウイルス／マルウェア感染した環境からの復旧が容易
    - 物理パソコンで同じことをやった場合は、環境復元までに時間がかかる
- Windowライセンスの確認は必要
  - 仮想環境で利用してよいライセンス契約になっているかの事前確認は必要

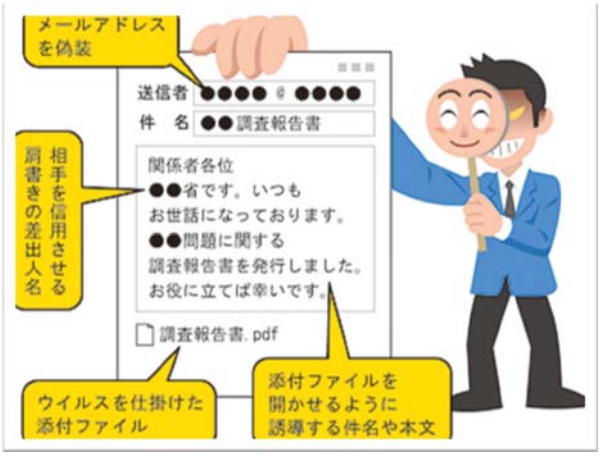
実際に仮想環境上のパソコンを操作しましょう

実習環境構成



実際に仮想環境上のパソコンを操作しましょう

- サンドボックスとして、2つの仮想環境（TypeA／TypeB）が用意されています
  - TypeA：ウイルス対策ソフトがインストールされている環境
  - TypeB：ウイルス対策ソフトがインストールされていない環境
- 仮想環境のゲストOSは、ホストOSとのみ通信できます
  - NAT機能はOFFにしているので、ホストOSから先への通信はできません
- 調査依頼されたファイルは既に入手していて、仮想環境上に保存されていることとします



事例から考える標的型攻撃3

（画像　IPA情報処理推進機構）
http://www.ipa.go.jp/security/keihatsu/pr2012/general/02_targeted_attack.html

まとめ

- 標的型攻撃かどうかを一目で見分けることは難しい
  - ウイルス対策ソフトで必ず検知されるとは限らない
  - 仮想環境を検知して動きを止めるマルウェアも存在する
- 複合的な結果から判断した方がよい
  - 複数のウイルス対策ソフトを利用する
  - プロセスモニターのようなツールを並行稼働させておく
  - （余裕があったら）物理パソコンで検証してみる
  - 標的型攻撃に関する情報収集などを日ごろから意識しておくことで、他で起きた事例を参考に判断することもできる
- 初動対応としての範囲の見極めが必要
  - あくまでも初動対応なので、細かい調査より以後の対応の判断材料を得ることを優先
  - 大まかな状況が分かった時点で上司などへ報告、その後の対応指示を仰ぐなど組織としての対応に移行する

【参考】添付ファイルがzip形式ではなかった場合

- プレビュー機能が備わっているメールソフトを利用している場合は、プレビューを活用することも有効
- Office365 や Gmail などのプレビューを利用することで、ダウンロードせずに添付ファイルの中身を確認することが可能
- プレビュー機能は万全ではないので、あくまでも手段の1つとして活用する
  - 対応していない形式のファイルはプレビューできない
  - Windows OS と親和性の高い Internet Explorer でのプレビュー利用はできるだけ避けた方がよい

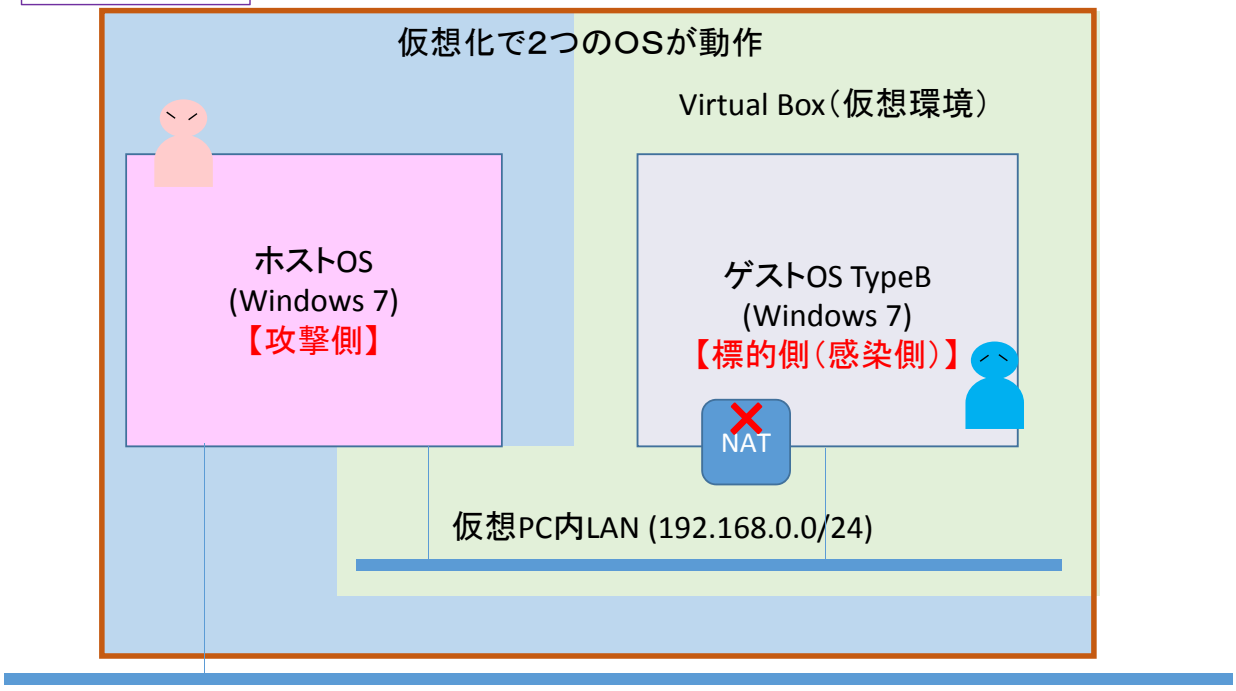
【参考】拡張子表示の設定も有効

- Windows のデフォルトでは、ファイル拡張子が非表示になっている
- これを利用し、Word形式などに見せかけたファイルを添付してくる場合がある（例：報告書.docx）
- しかし、実際は実行形式のファイルというパターンもある（例：報告書.docx.exe）
- 添付ファイルをダウンロードしてしまった場合でも、拡張子を表示する設定にしていれば、実行形式のファイルであることに気付くことができる、かもしれない

延長実習　遠隔操作ウイルスの操作体験

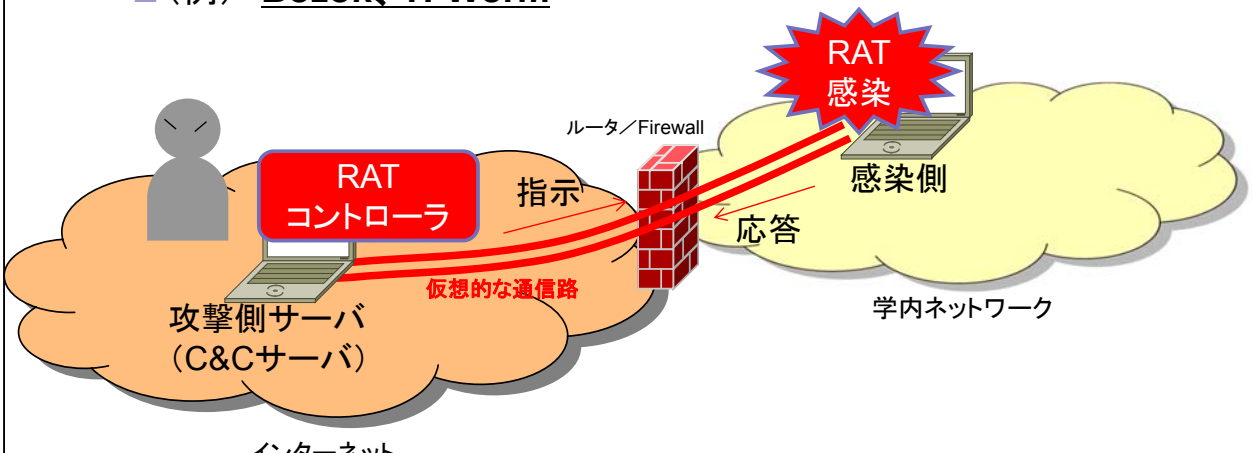
実は今回の実習環境はこうなっています

実習環境構成



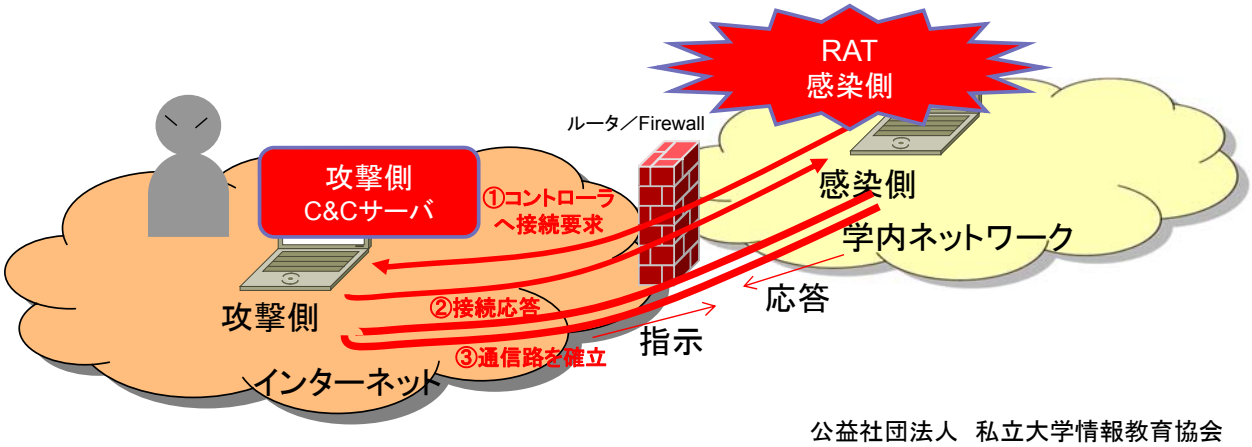
RATとは

- 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**



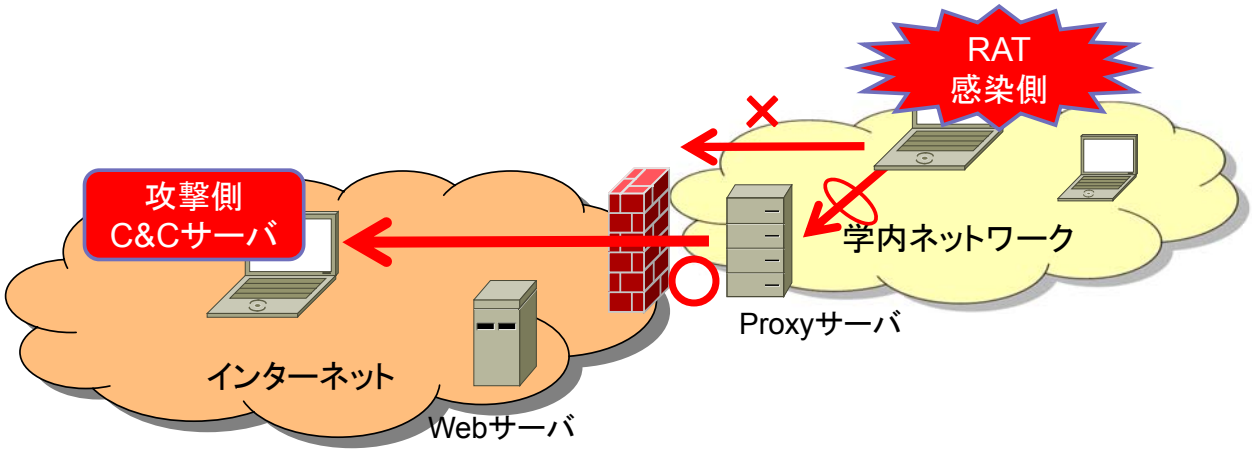
RATの特徴 （1）

- 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



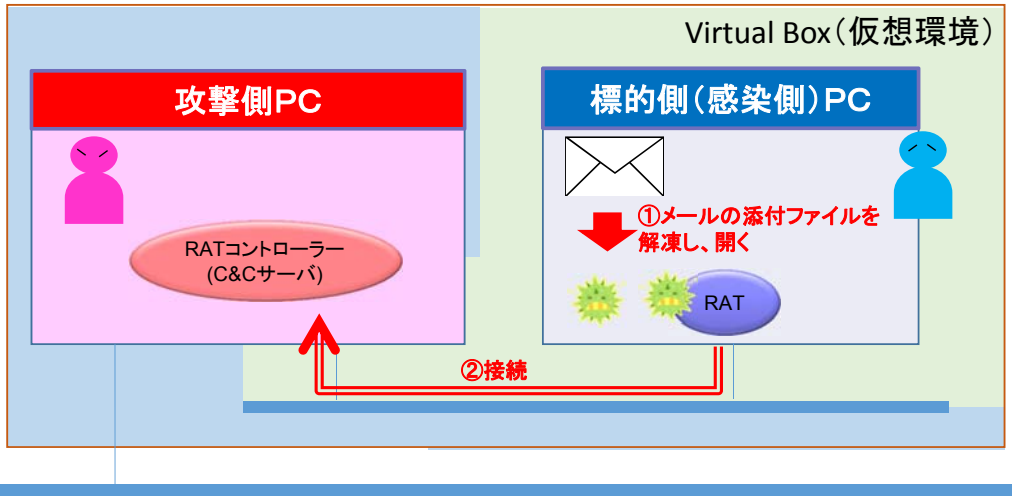
RATの特徴 （2）

- 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



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