A-2.
遠隔操作ツール(RAT)の機能とリスク

明治大学
服部　裕之

このセッションの目的

RAT型ウィルスの動作を実習にて確認する

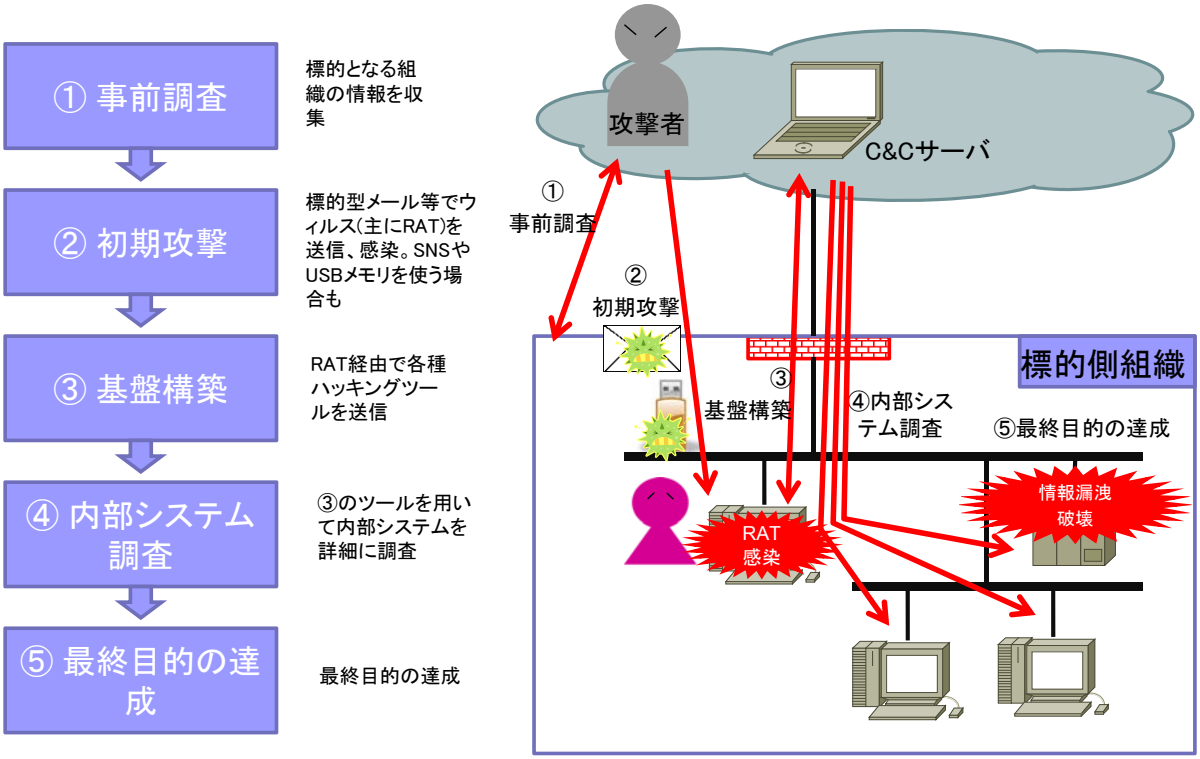
（1） 標的型攻撃における攻撃パターンを理解する
（2） RAT型ウィルスの感染によるリスクを理解する

メニュー

1. 標的型攻撃
   1. 標的型攻撃の流れ
2. RATについて
   1. RATとは
   2. RATの機能・特徴
3. 実習
4. まとめ

標的型攻撃の流れ

標的型攻撃の流れ



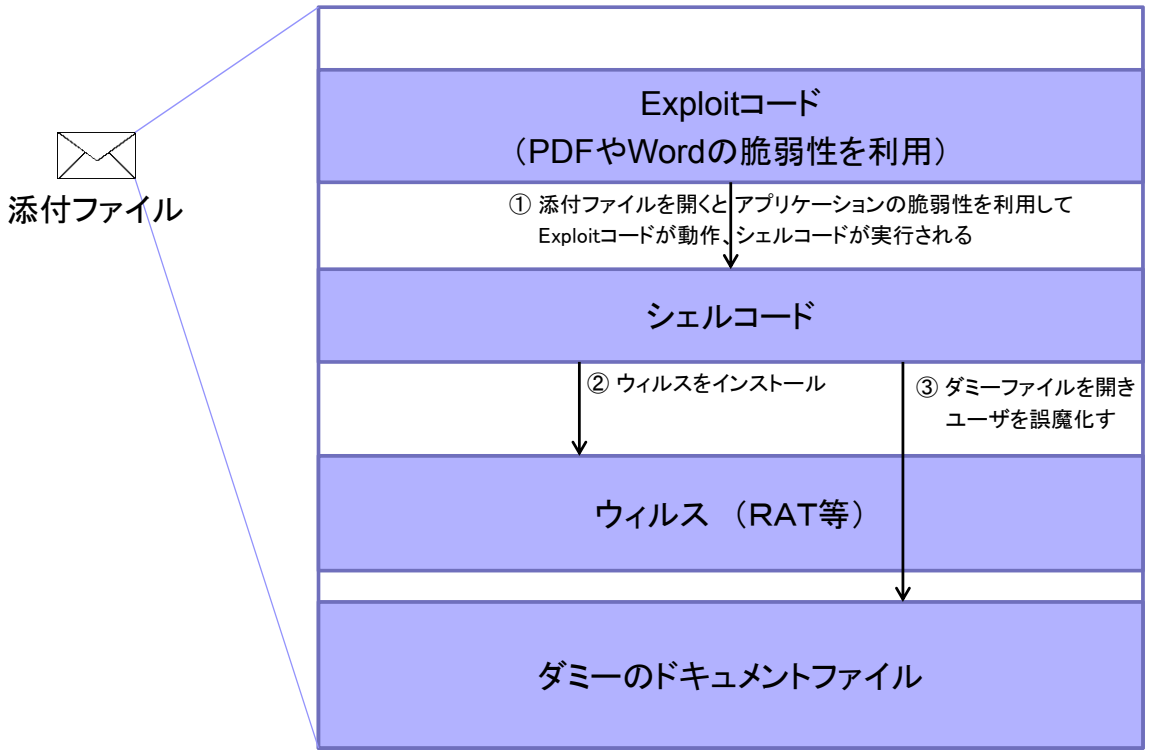
② 初期攻撃

- 標的型メール
  - □ 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
添付：　職員人事研修・開催要項

服部様。
標記研修の開催につきまして，添付のとおりお知らせしますのでご参加いただきますようお願いします。
事前課題につきましては後日改めてご案内いたします。

ウィルスを含む添付ファイル



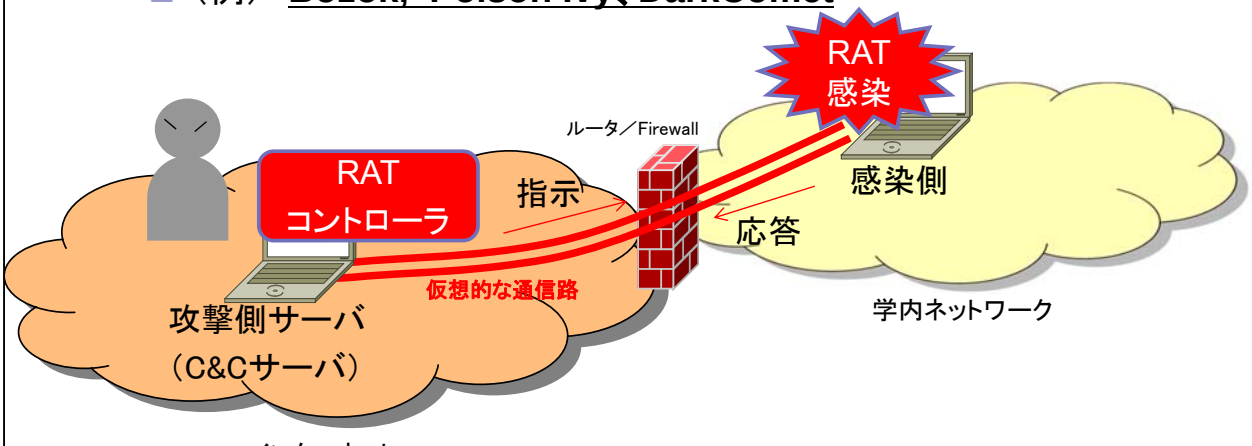
③ 基盤構築 ～ ④ 内部システム調査

- ネットワークの調査
  - 標的組織の内部ネットワークシステムを把握する
  - nmap等
- アクセス権限の入手（Pass the Hash等）
  - 各種システムのアクセス権限を入手する
  - pwdump7, Gsecdump （ハッシュ値入手）
  - Pshtoolkit, Metasploit PSEXEC module （偽装アクセス）
- 遠隔操作ツール
  - 各種システムを遠隔操作するためのツールを仕込む
  - PsTools等
- バックドア
  - RAT以外の、より発見が困難なバックドアを作成する
  - HTran

RATについて

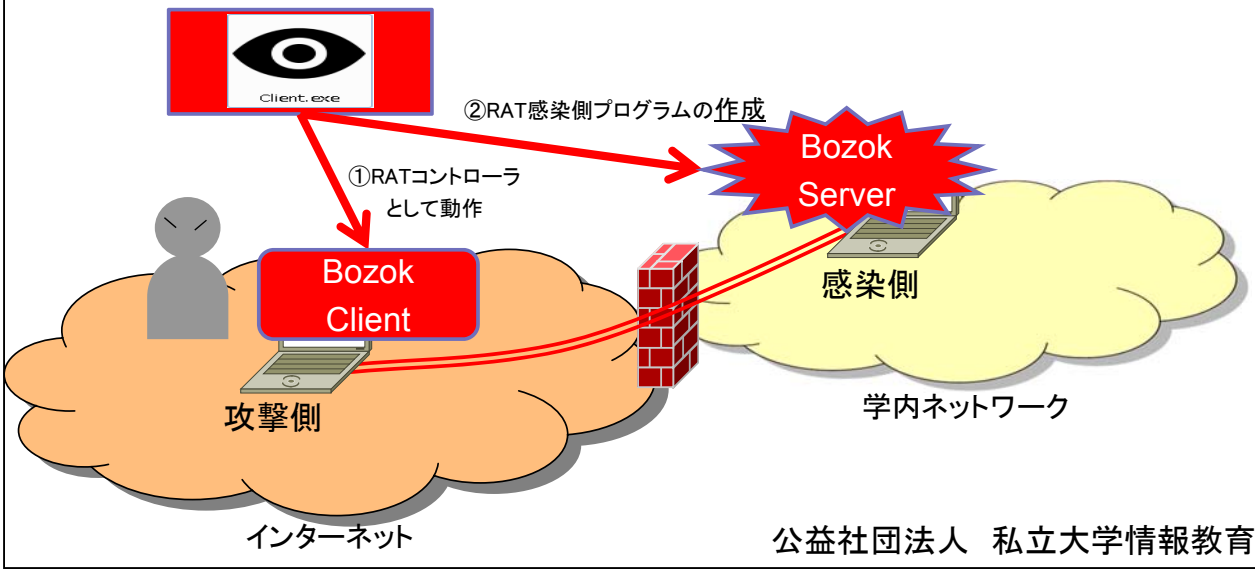
RATとは

- RAT = Remote Admin Tool (?)
  Remote Access Trojan(?)
- 「バックドア通信」を行うウィルスの総称
  - 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、ウィルスの拡散や情報収集の足がかりに。
  - （例） **Bozok, Poison Ivy、DarkComet**



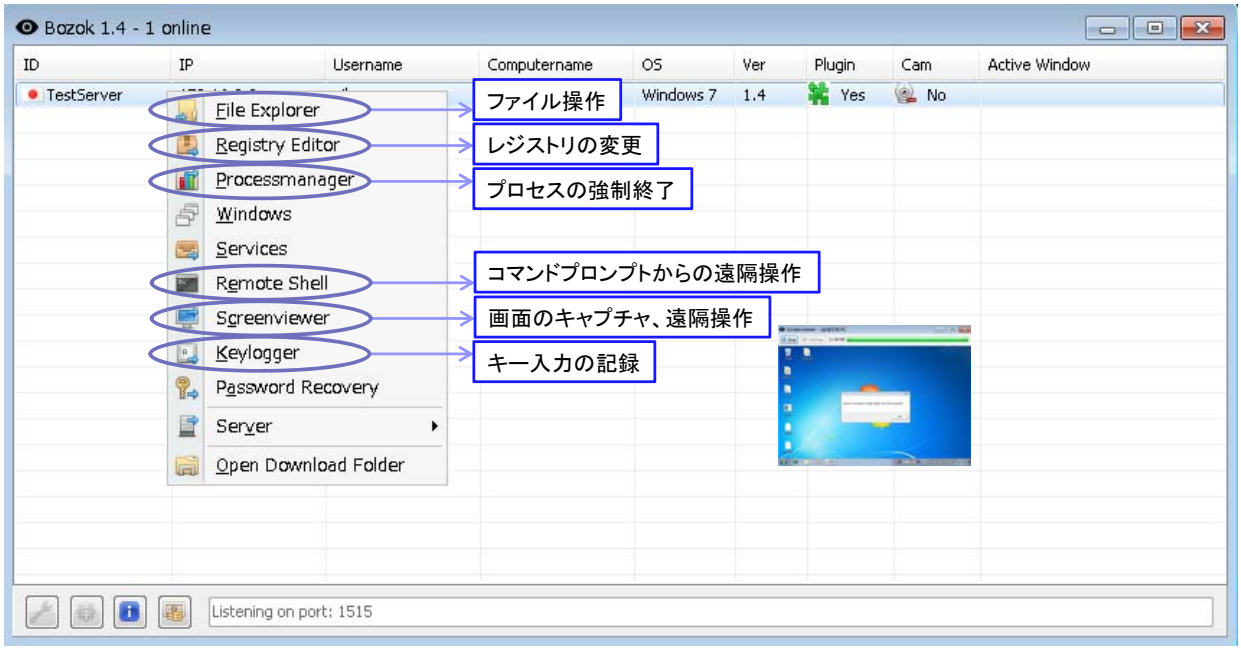
Bozok

- RATの一種。
  - コントローラ機能　(Bozok Client)
  - 感染側プログラム作成ツール　(感染側プログラム＝Bozok Server)
- http://ss-rat.blogspot.jp/



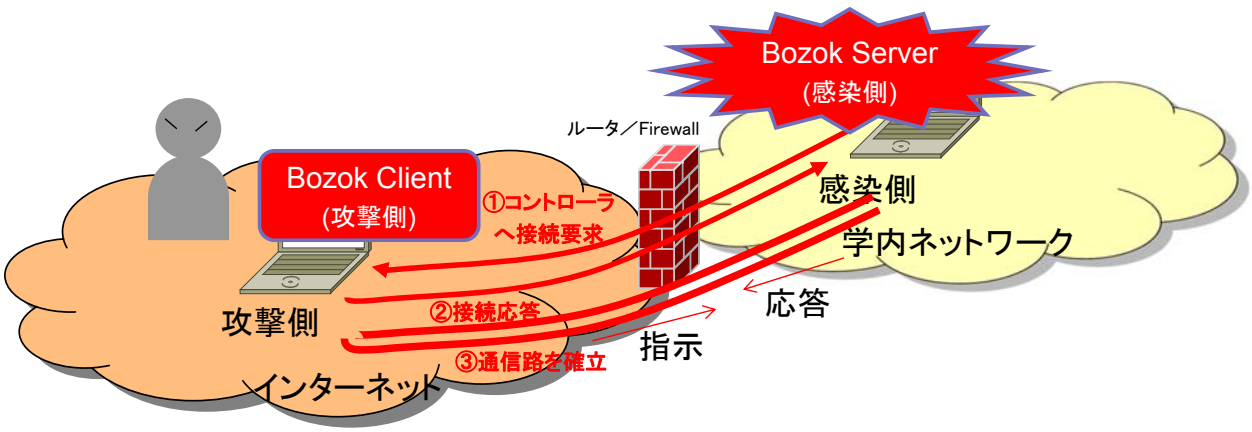
RATの機能

- Bozok による感染側PCの遠隔操作（例）



Bozok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。

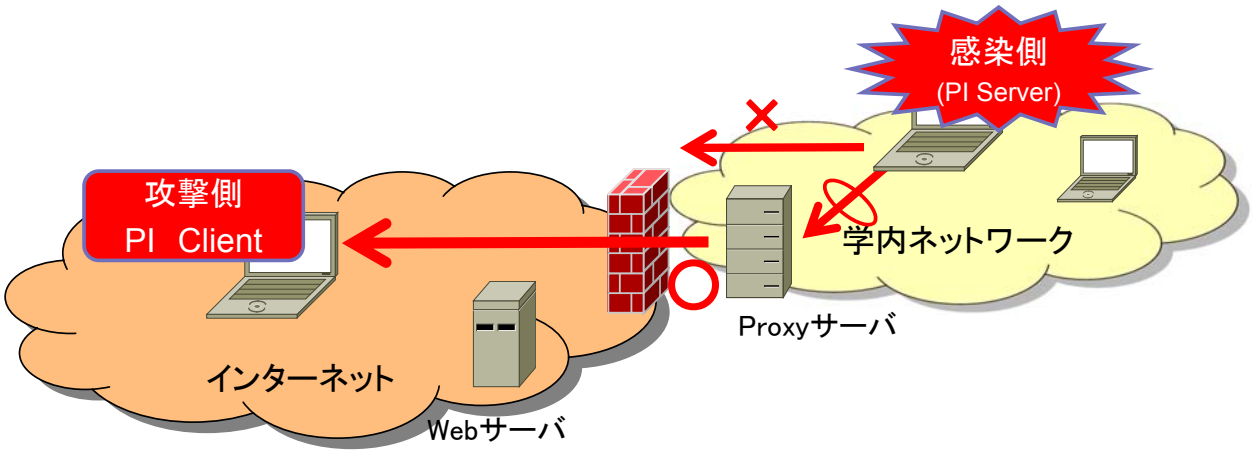


Bozokの特徴 （2）

- 出口対策が困難
  - 通常の通信と、RAT通信の見分けが困難。
    - Bozokはポート番号：1515を使う。
    - ポート番号の変更は可能。（80とか443とか）

他のRATの特徴 （例：Poison Ivy）

- Proxyサーバに対応している
  - 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、攻撃側から感染PCのコントロールが可能。

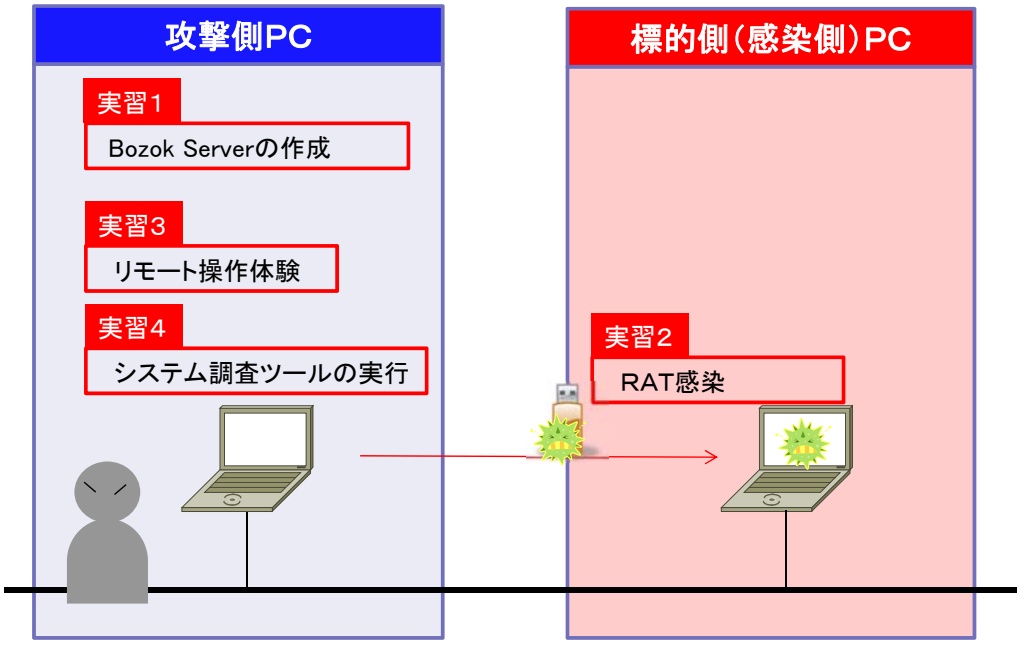


実習

実習環境

- ひとり1台のPCを使用します。
- 実習は隣どうし2名のペアで行います。
- 片方のPCが「攻撃側」、もう片方のPCが「感染側」となります。

実習概要



まとめ

- 標的型攻撃における攻撃パターン
  - 事前調査→初期攻撃→基盤構築
    →内部システム調査→最終目標の達成

- RAT型ウィルスの感染によるリスク
  - インターネットとの境界ファイアウォールによる防御は無力に。
  - 発見が困難。
  - 内部システムが丸裸にされる危険性。