A-2.
典型的な標的型攻撃手法の紹介と実習

明治大学
服部　裕之

このセッションの目的

標的型攻撃の手法を実習にて確認する

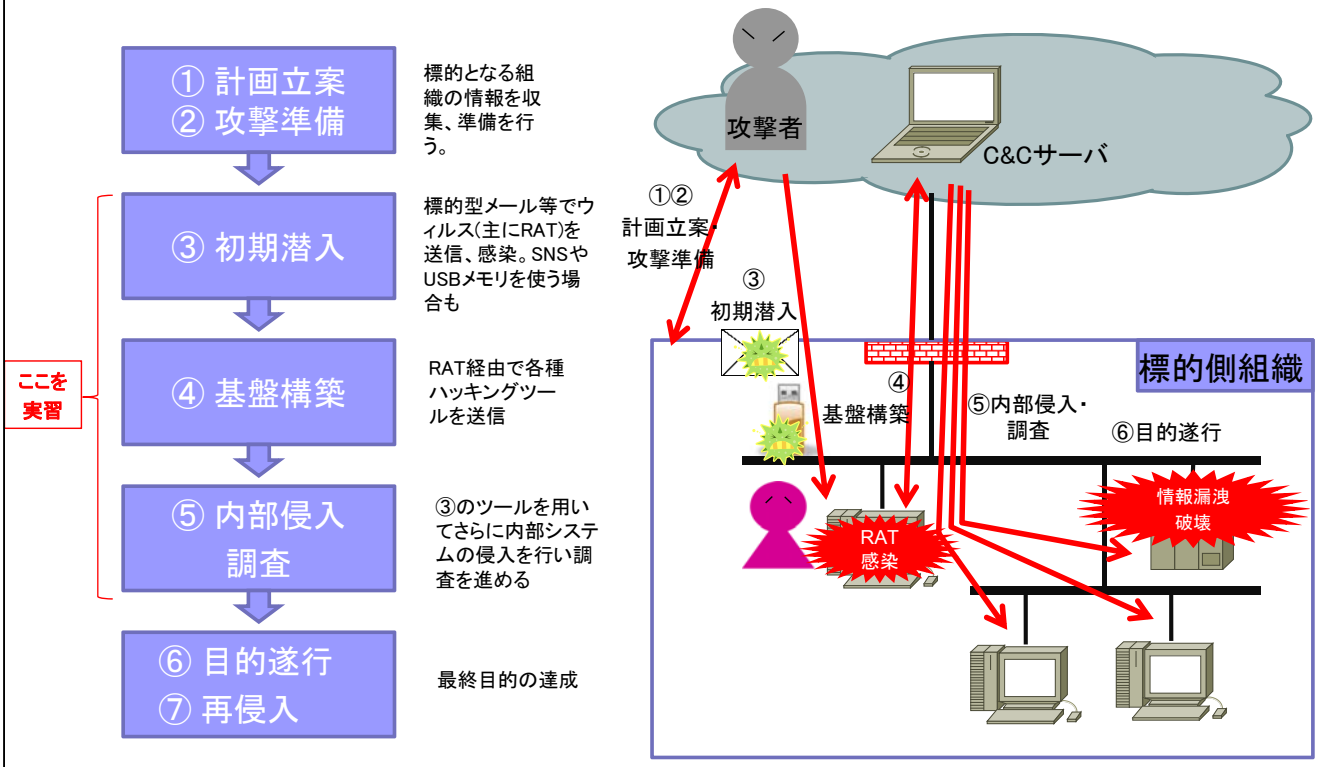
（1） 標的型攻撃における攻撃パターンを理解する
（2） RAT型ウィルスの感染によるリスクを理解する

メニュー

1. 標的型攻撃の流れ
2. マルウェア感染のメカニズム
3. RATを用いた内部システム調査
4. 内部感染の拡大
    1. Pass-the-Hash攻撃
5. 実習
6. まとめ

標的型攻撃の流れ

標的型攻撃の流れ



③ 初期潜入

- 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：　貴学学生の喫煙行為について
添付：　  証拠写真

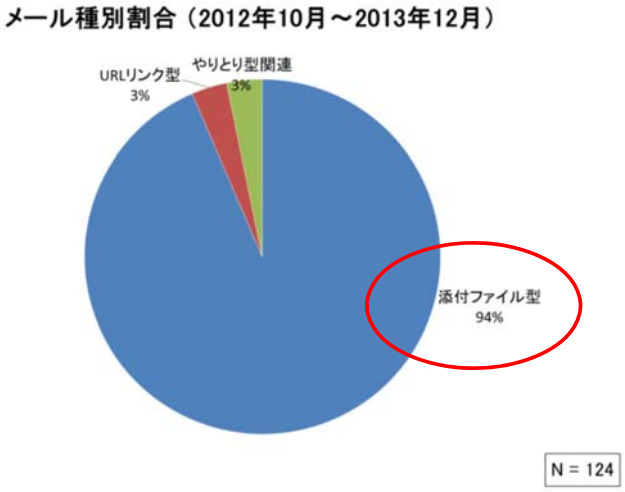
私情協大学 御中。
　私は御校の近隣に在住するものです。
　最近、貴学と思われる学生の路上喫煙がたいへん目立ちます。
　今朝撮影した写真を添付しますので、学生をよろしくご指導ください。

④ 基盤構築 ～ ⑤ 内部侵入・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攻撃等）
  - 各種システムのアクセス権限を入手する
  - lslsass, gsecdump （ハッシュ値入手）
  - keimpx, Pshtoolkit, Metasploit （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管理ツールを仕込む
  - 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

マルウェア感染のメカニズム

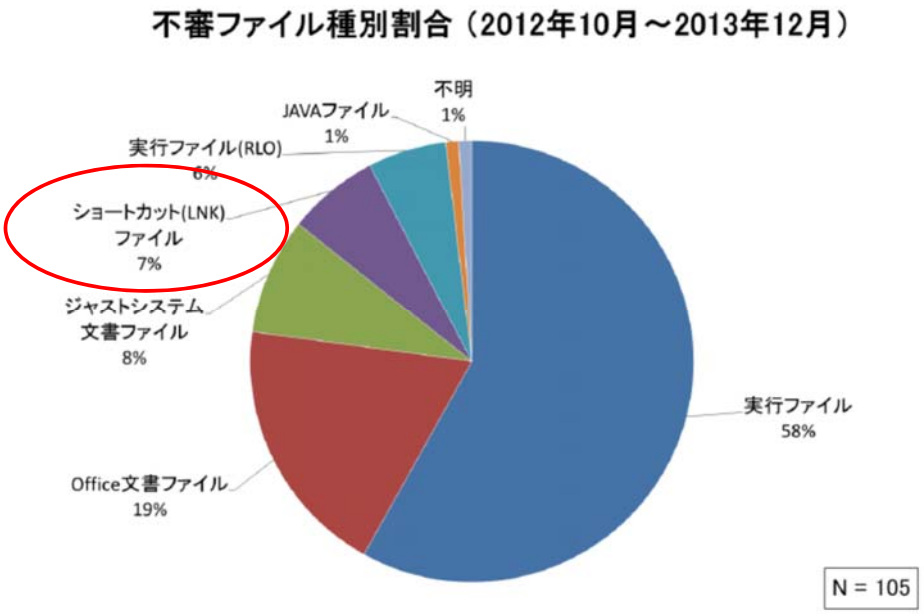
標的型メールの種別割合



出典：「標的型攻撃メールの傾向と事例分析＜2013年＞」、IPA
https://www.ipa.go.jp/files/000036584.pdf

- 添付ファイル型
  - 悪意のあるファイルが添付。受信者が開くことによってウィルスに感染。
- URLリンク型
  - メール本文中にURLリンクが記載。受信者がクリックすることでウィルスに感染。
- やりとり型
  - 最初は添付やURLを含まない通常のメールをやりとり。相手が油断したところで、悪意のあるファイルを添付またはURLを記載。

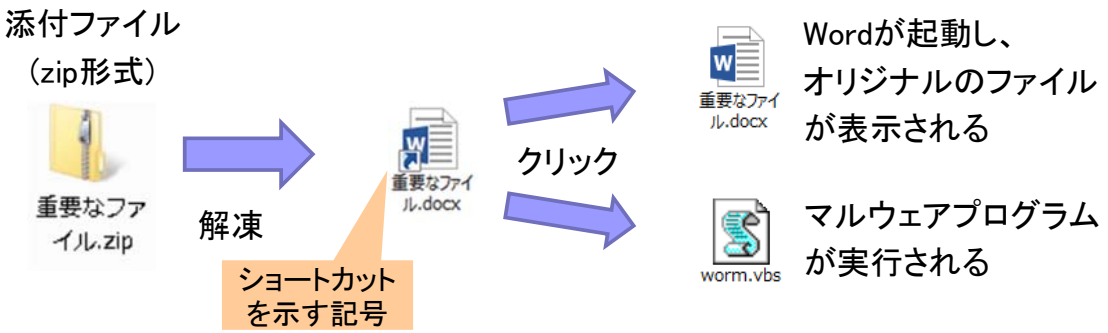
添付ファイル型　～何が添付されている？～



出典：「標的型攻撃メールの傾向と事例分析＜2013年＞」、IPA
https://www.ipa.go.jp/files/000036584.pdf

ショートカットを悪用した手口

- 添付ファイル(ZIP)を解凍すると、ショートカット(.lnk)ファイルが表示される。
- ショートカット(.lnk)ファイルを開くと、マルウェアに感染する。



マルウェア感染のメカニズム (例：H-worm)

（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 worm.vbs&start 重要なファイル.docx&exit

【意味】

（1）worm.vbsを起動し、

（2）重要なファイル.docx　を開く

（Hidden + System属性ファイル）

オリジナルファイル　（word）

マルウェアプログラム（vbs）

【動作】

（1）Windowsのレジストリを書き換え、メモリに常駐。

（2）既存USBメモリに対して、以下の操作を行う。

（2-1）オリジナルのファイルを、同名のショートカットに書き換える。

（2-2）マルウェアプログラム本体をUSBメモリにコピー。

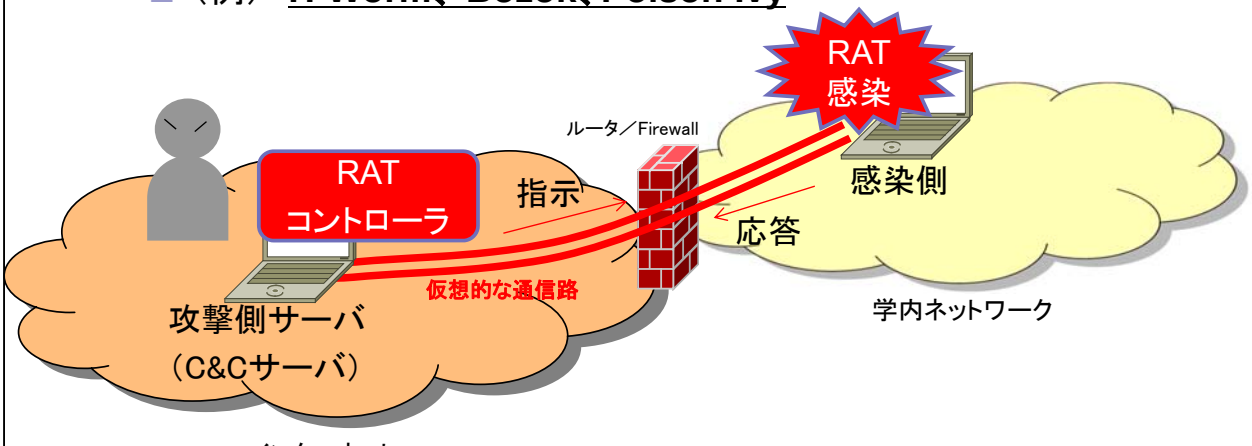
（2-3）オリジナルのファイルとマルウェアプログラム本体を「保護されたオペレーティングシステムファイル属性」に変更。

（3）RATの動作を開始。C&Cサーバと接続し指示を待つ。

RATを用いた
内部システム調査

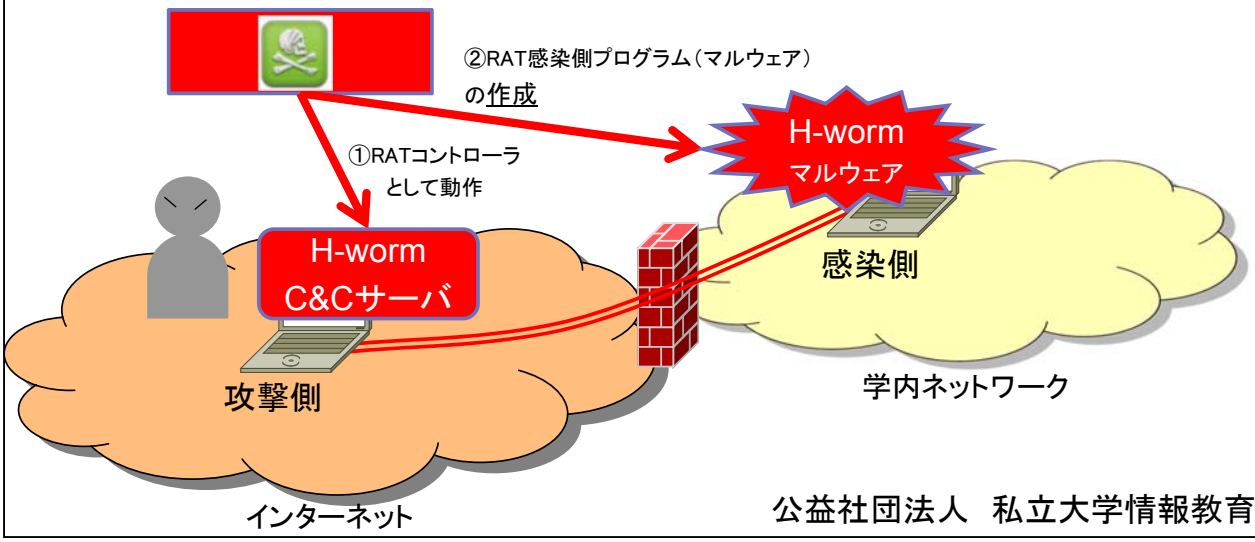
RATとは

- 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） **H-Worm、Bozok、Poison Ivy**



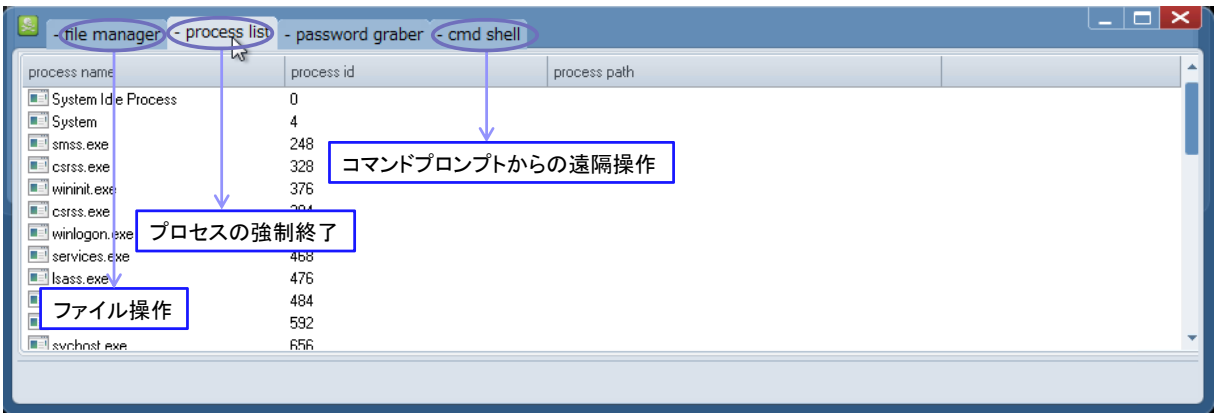
H-worm

- RATの一種。
  - コントローラ機能　(C&Cサーバ)
  - マルウェア作成ツール　(H-worm)
- http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/now-you-see-me-h-worm-by-houdini.html



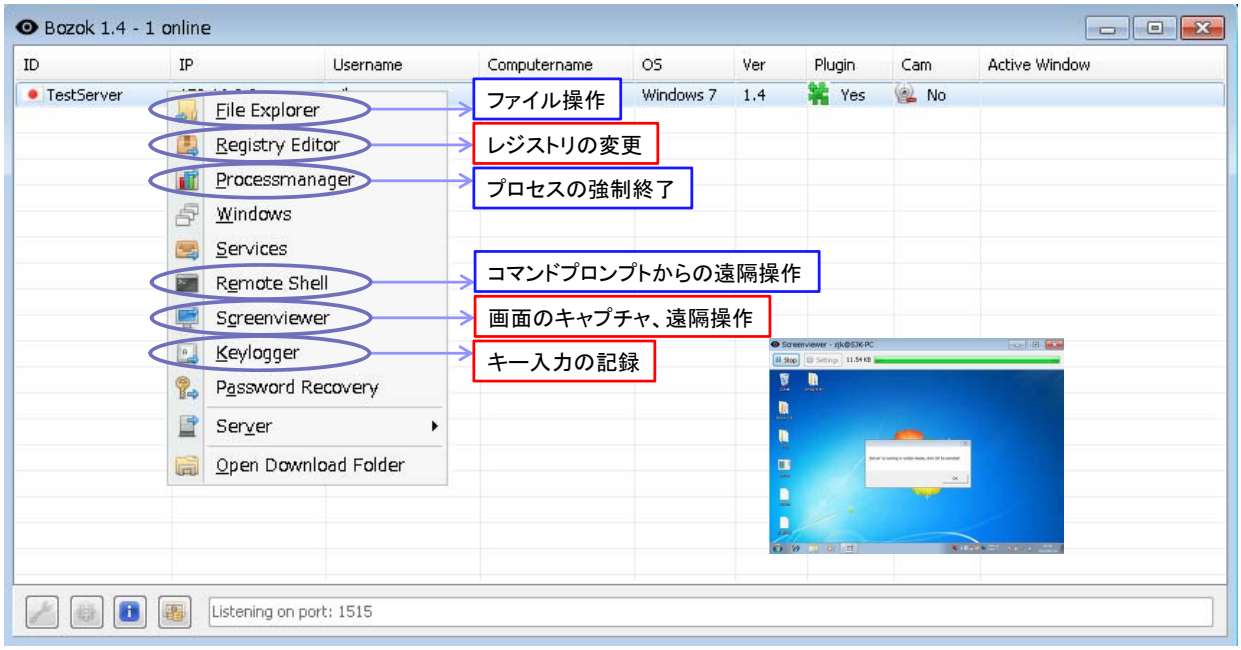
RATの機能 (1/2)

- H-worm に感染したPCの遠隔操作（例）



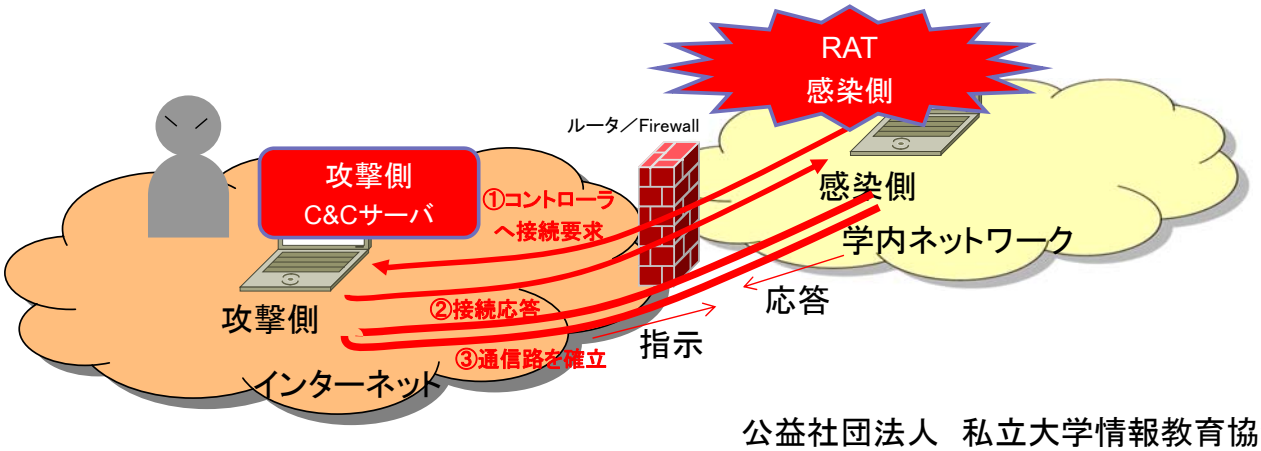
RATの機能 (2/2)

- Bozok に感染したPCの遠隔操作（例）



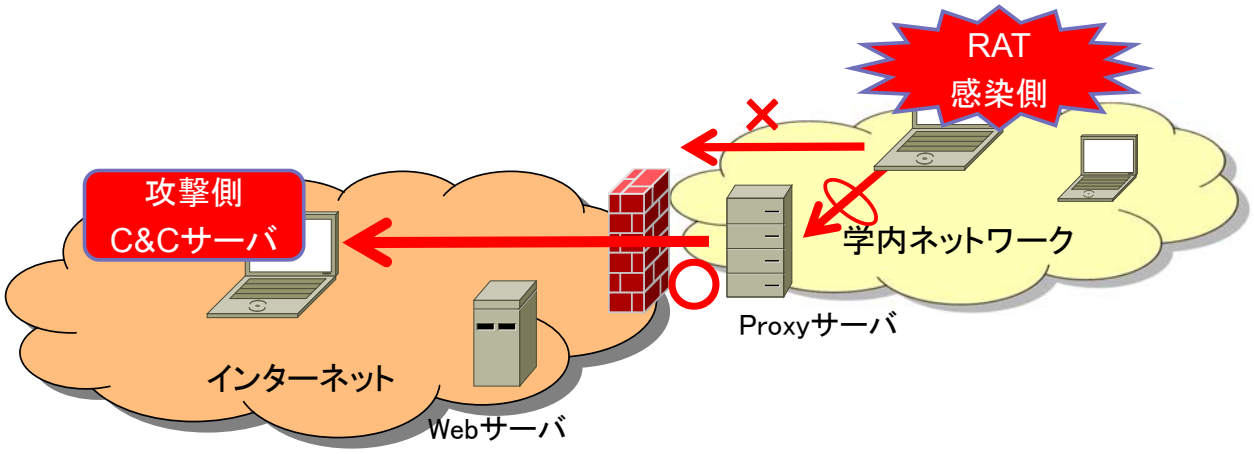
RATの特徴　（1）

- 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）

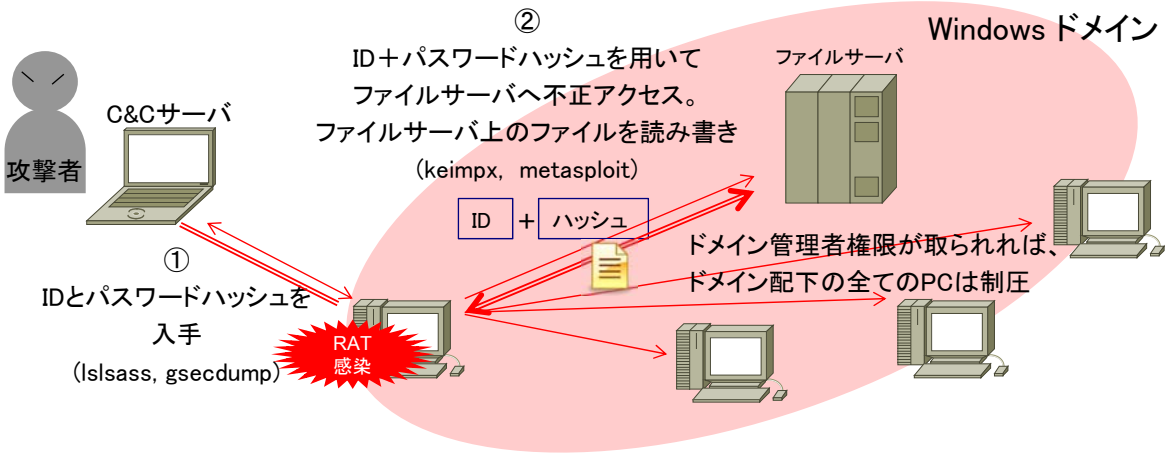
- 出口対策が困難
  - Proxyサーバに対応しているRATもある。
    - 感染PCからインターネットへブラウザでアクセス可能ならば、攻撃側PCから感染PCのコントロールが可能。



内部侵入の拡大

Pass the Hash 攻撃 （アクセス権限の入手）

- Windowsの認証を回避し、IDとパスワードのハッシュ値のみを使い不正アクセスする手法
  - ⇒ 生のパスワードが分からなくても、アクセスできる。
- ドメイン管理の場合、1台のPCがやられると、全てのPCが被害にあう恐れがある。



実習

まとめ

- 標的型攻撃における攻撃パターン
  - 事前調査→初期潜入→基盤構築
    →内部侵入・調査→目的遂行

- 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。
  - 内部システムが丸裸にされる危険性。
  - 検知が困難。
    - 感染したことに気づかない。侵入されていることに気づかない。