A-4.標的型サイバー攻撃

金城学院大学
西松　高史

このセッションの目的

標的型サイバー攻撃の流れを理解する。
・攻撃者が目的とする情報を入手するまでの手順を確認
・標的型サイバー攻撃で用いるマルウェア及び各種侵入拡大ツールの動作検証

標的型サイバー攻撃を受けた時の被害や
影響範囲について、的確な想定ができる

「情報セキュリティ10大脅威2017」

出展：IPA（独立行政法人　情報処理推進機構）
https://www.ipa.go.jp/security/vuln/10threats2017.html

「情報セキュリティ10大脅威2017」

■ 「組織」向け脅威

1.標的型攻撃による情報流出
2.ランサムウェアによる被害
3.ウェブサービスからの個人情報の窃取
4.サービス妨害攻撃によるサービスの停止
5.内部不正による情報漏洩とそれに伴う業務停止
6.ウェブサイトの改ざん
7.ウェブサービスへの不正ログイン
8.IoT機器の脆弱性の顕在化（けんざいか）
9.攻撃のビジネス化
10.インターネットバンキングやクレジットカード情報の不正利用

出展：IPA（独立行政法人　情報処理推進機構）
https://www.ipa.go.jp/security/vuln/10threats2017.html

「情報セキュリティ10大脅威2017」

第1位　標的型攻撃による情報流出

企業や民間団体や官公庁等、特定の組織に対して、メールの添付ファイルやウェブサイトを利用してPCにウイルスを感染させ、そのPCを遠隔操作して、別のPCに感染を拡大し、最終的に個人情報や業務上の重要情報を窃取する標的型攻撃による被害が引き続き発生している。

出典：IPA（独立行政法人　情報処理推進機構）「情報セキュリティ10大脅威 2017」
https://www.ipa.go.jp/security/vuln/10threats2017.html

第1位　標的型攻撃による情報流出

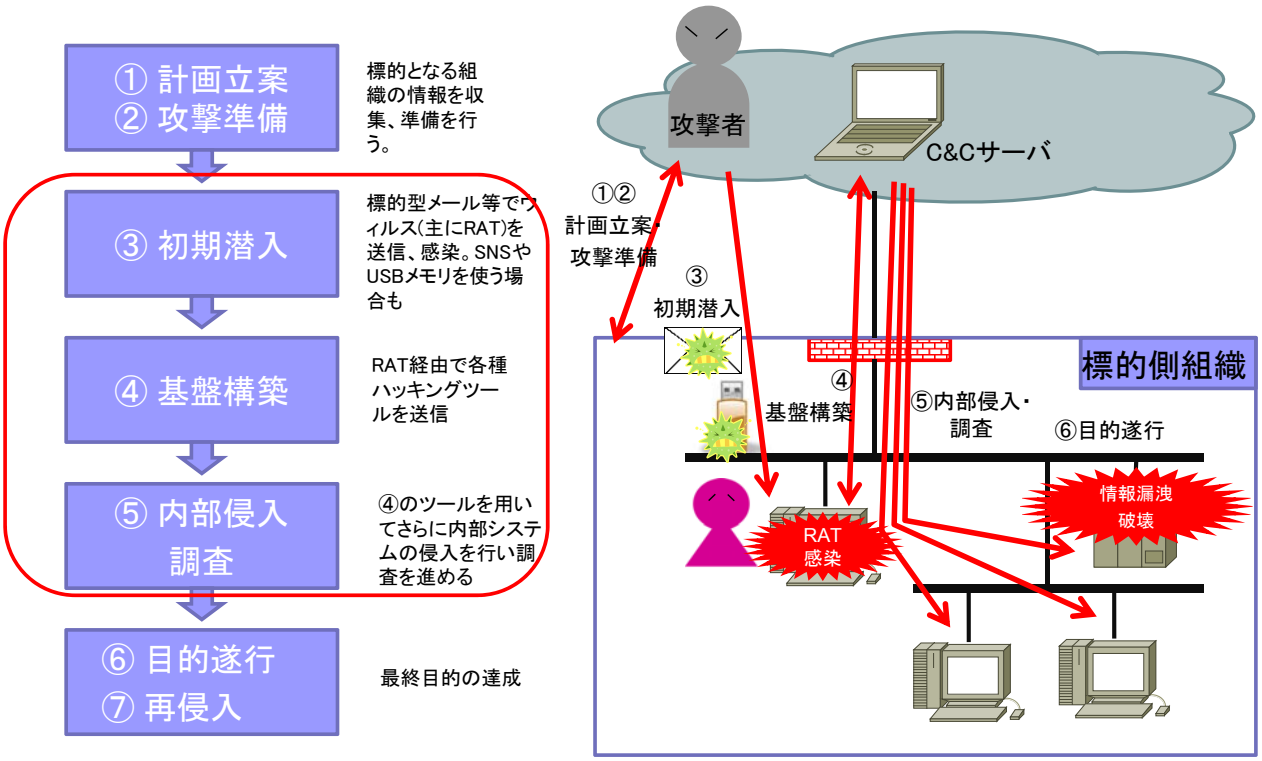
- 侵入経路
  - 電子メールから「ばらまき型」「やりとり型」
  - ウェブから「水飲み場型」
- 事例
  - 旅行会社JTBから個人情報流出（678万件）
    - 取引先になりすましメールの添付ファイルを開かせた
    - 遠隔操作で個人情報を保管しているサーバへ侵入
  - 富山大学から研究成果が流出
    - 個人情報や原子力発電所の汚染水処理に関する研究成果が流出
    - 非常勤の研究者のPCから感染

電子メールの信憑性確認

■怪しいメールという判断

・知らない人からのメール
・知った人からでもアドレスがいつもと違う（gmailなどのフリーメールを利用していることが多い）メール
・送信者と署名（シグネチャ）が違う
・言い回しが不自然な日本語
・日本語では使用しない漢字
・あえて正式名称を一部に含むようなURL

標的型サイバー攻撃の流れ



初期潜入

初期潜入方法

- 代表的な潜入方法
  - メールからの潜入（ばらまき型、やりとり型）
    - 不審なファイルを添付したメールを送信
    - 不審なURLリンクが本文に記載されたメールを送信
  - USBメモリからの潜入
  - Webからの潜入（水飲み場型）
- 添付ファイルを実行、またはURLリンク先にアクセスさせた後にRAT（遠隔操作ウィルス）を使って次の段階（基盤構築）に進む

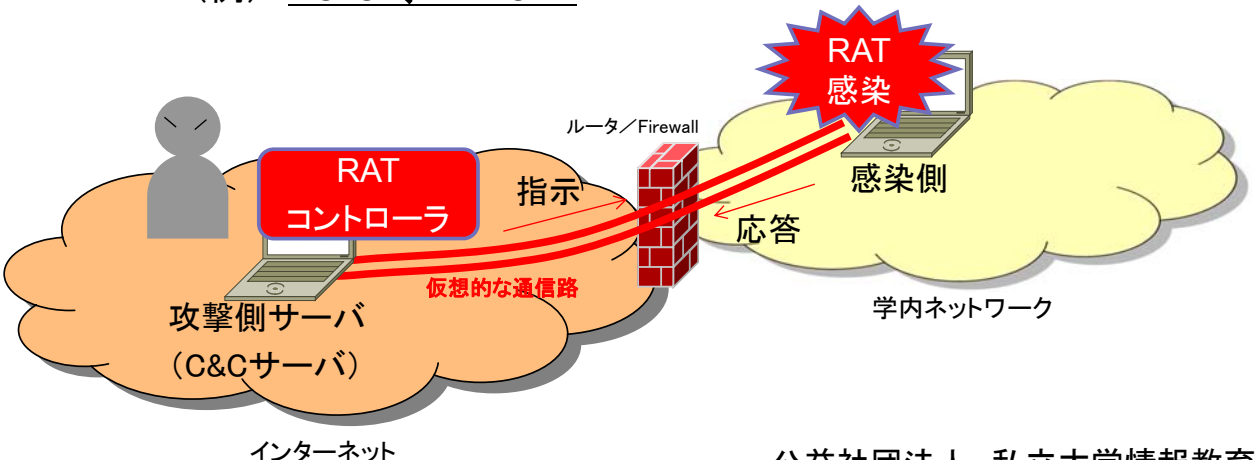
メールからの潜入

- 例：以下のメールを受信した

送信元	株式会社　ミクロソフト <micurosoft@asdfg.micurosoft.com>
宛先	SJK大学　教員A
表題	取材の依頼について
本文	はじめまして、株式会社ミクロソフトと申します。 貴学のホームページを拝見し、大変不躾ながらメールさせていただきました。 私どもが発行している会員誌にて、貴学の活動を紹介させていただきたく、 ご連絡いたしました。 当社発行の会員誌に関する詳細情報は、添付資料として 取材のお願いと合わせてお送りさせていただきました。 お忙しい中大変恐縮ではございますが、 何卒宜しくお願い申し上げます。 株式会社ミクロソフト
添付ファイル	取材のお願い.jpg

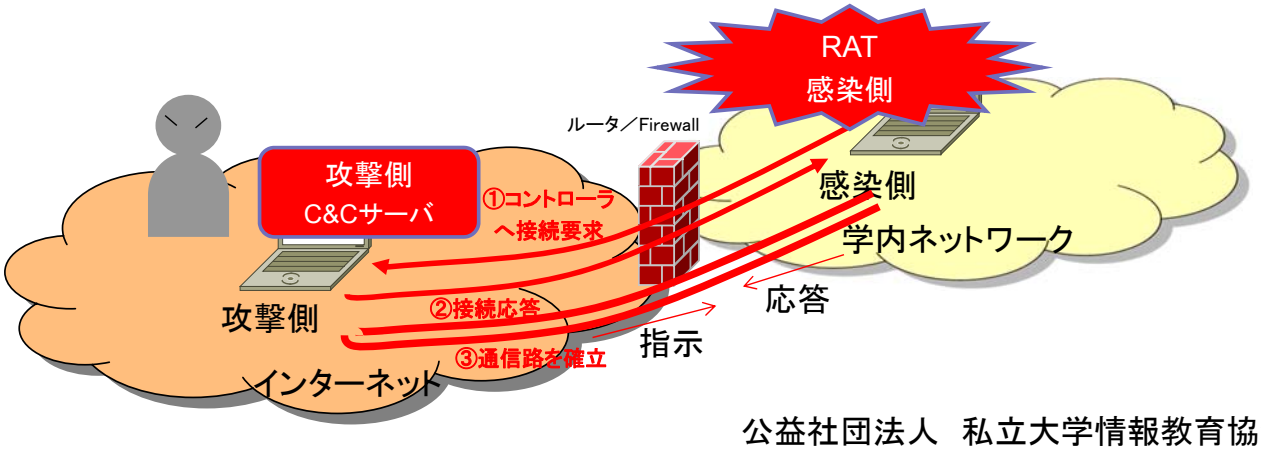
RATとは

- 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**



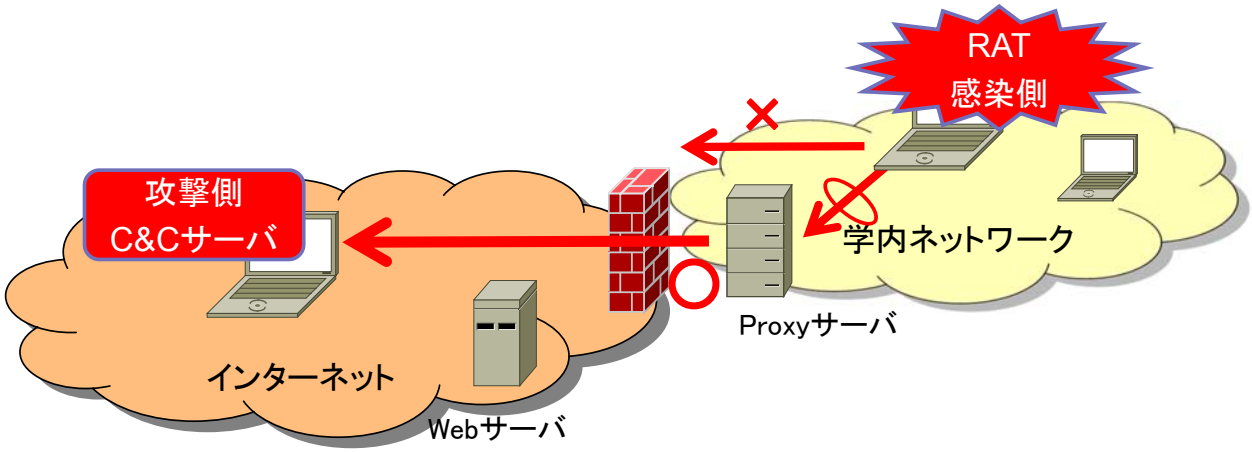
RATの特徴 （1）

- 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）

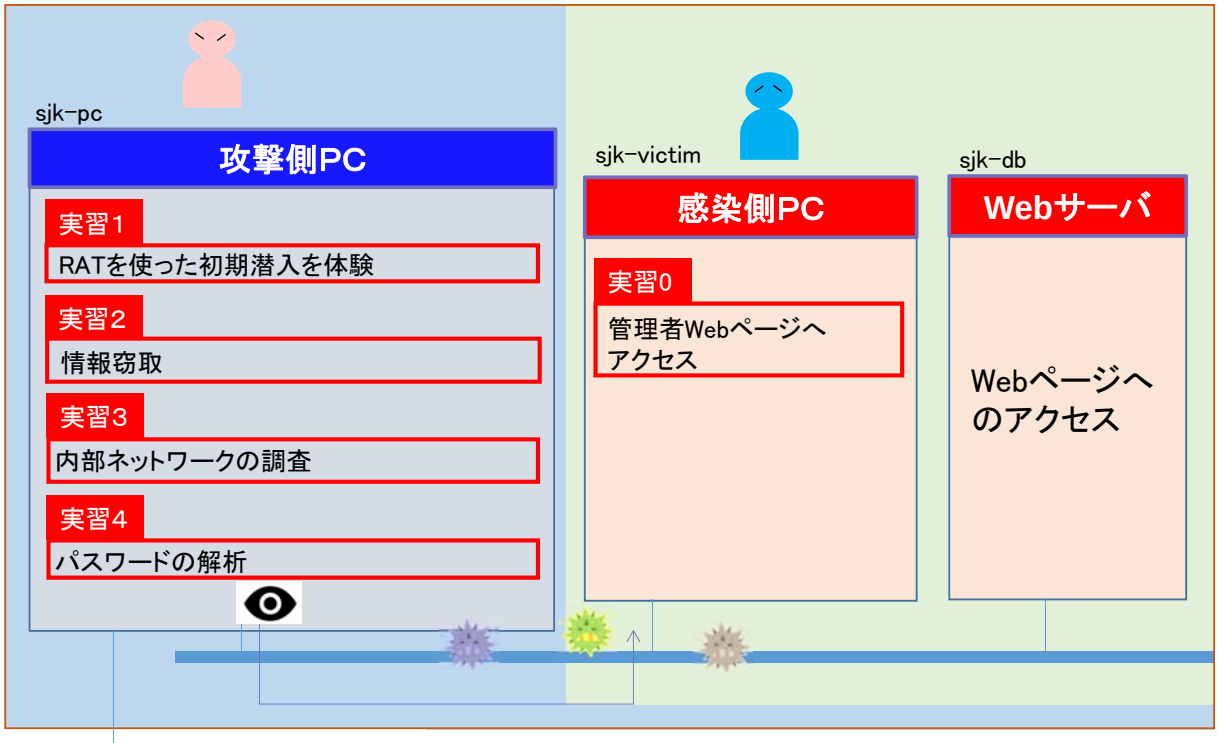
- 出口対策が困難
  - Proxyサーバに対応しているRATもある
    - 感染PCからインターネットへブラウザでアクセス可能ならば、攻撃側PCから感染PCのコントロールが可能



実習

- 管理者Webページへのアクセス
  - オートコンプリートを使ってパスワードを記憶
- RATを使った初期潜入を体験
  - RATの感染
  - RATの操作
    - RATで何ができるのか、どんな機能があるのか確認
- 情報窃取
  - デスクトップ上にあるファイルを窃取
- 内部ネットワークの調査
  - 同じネットワークに接続しているPCを探す
- パスワードの解析
  - オートコンプリートを使った場合のパスワードを解析する

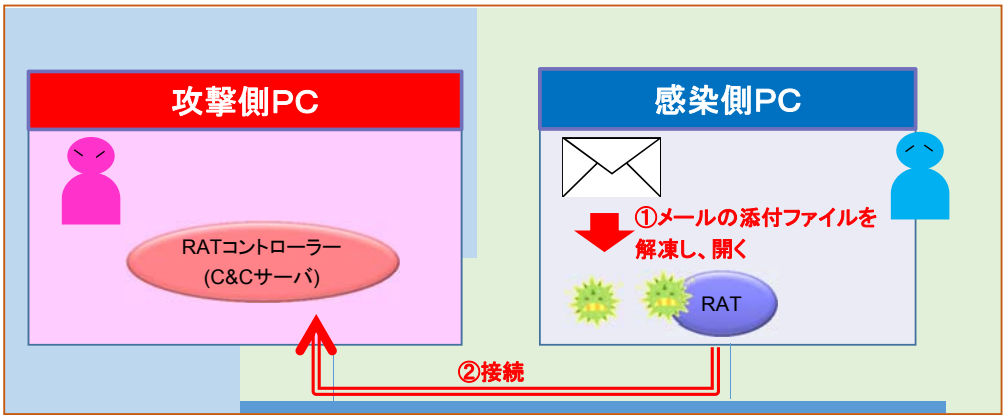
実習概要



実習1
RATを使った初期潜入を体験

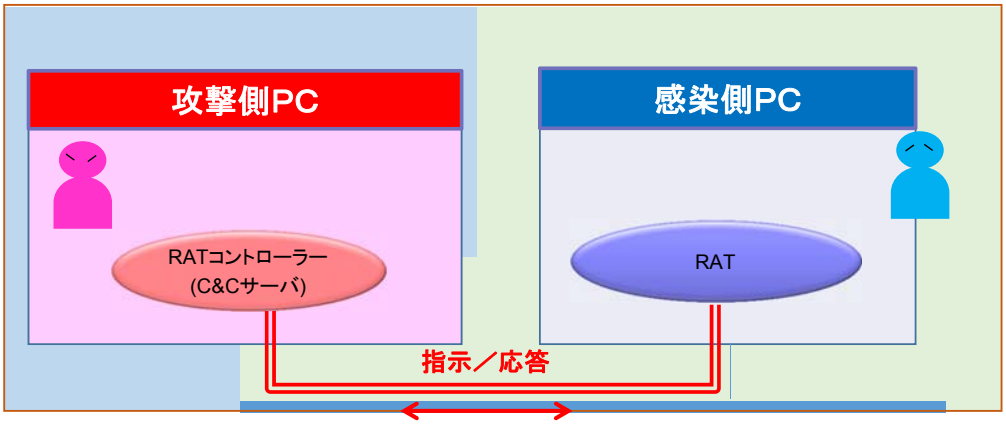
マルウェア感染

- 感染側PCで、添付ファイル（取材のお願い.jpg）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



基盤構築

基盤構築

- 初期潜入に成功すると、攻撃者は次に潜入先の内部情報を窃取するための「基盤構築」を行う
- 基盤構築の段階では、内部情報を窃取するためのツールを送り込み、インストールされる
- 現在の標的型サイバー攻撃は「潜伏型」と「速攻型」の2種類に大別できる
  - 「潜伏型」: 重要情報窃取を果たすまで活動する
    - 潜入してから実際に攻撃を開始、終了までの期間が長いもの（平均5か月）
    - 潜入後、攻撃（情報窃取）のための基盤を拡大する
    - 攻撃終了の際には痕跡も消していく
  - 「速攻型」: 重要情報窃取に向けた、最低限の情報を入手する
    - 潜入してから攻撃が終了するまでの期間が数時間～1日程度
    - 潜入後の基盤拡大、痕跡消去は行わない

基盤構築

- 今回は以下のツールを前もって準備し感染側PCにインストールを行った。
  - 圧縮ツール(7-zip)
  - ネットワーク調査ツール(nmap)
  - パスワード解析ツール(IE PassView)

実習2
情報窃取

情報窃取

- 感染側PCのデスクトップ上に保存してあるフォルダを攻撃側PCへコピーする
  - 対象フォルダの確認
  - ファイル圧縮作業
  - 圧縮されたファイルを攻撃側PCへコピー

内部侵入・調査

内部侵入・調査

- 内部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
  - nmap等
- 端末間での侵害拡大
  - 他端末のアクセス権限を入手、他端末へ侵害
  - パスワードの窃取（IE PassViewなど）
  - pwdump7, Gsecdump （ハッシュ値入手）
  - Pshtoolkit, Metasploit PSEXEC module（偽装アクセス）
- サーバへの侵入
  - ユーザ端末からサーバへのリモート操作
  - PsToolsなど

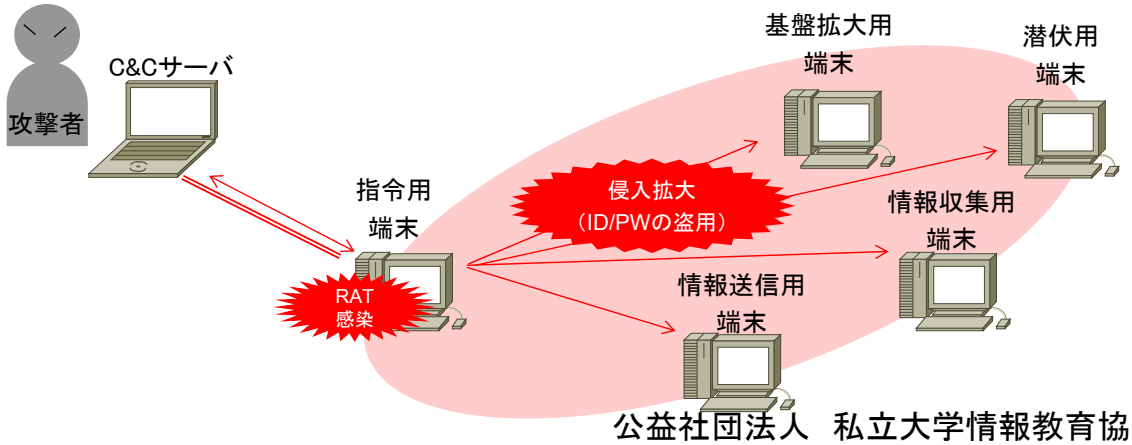
ネットワーク調査ツール

- nmap
  - 指定したホストやネットワークに対してポートスキャンをするためのツール
  - コマンド（nmap）と様々なオプションを組み合わせることで、内部ネットワークに接続されているコンピューターの情報を調査することが可能
  - OSを推定することも可能
  - オプション例
    - -A：OSとサーバーアプリケーションのバージョンを調査
    - -O：OSのバージョンを調査
    - -P0：pingスキャンを行わない
    - -F：限定したポートのみ調べる

実習3
内部ネットワークの調査

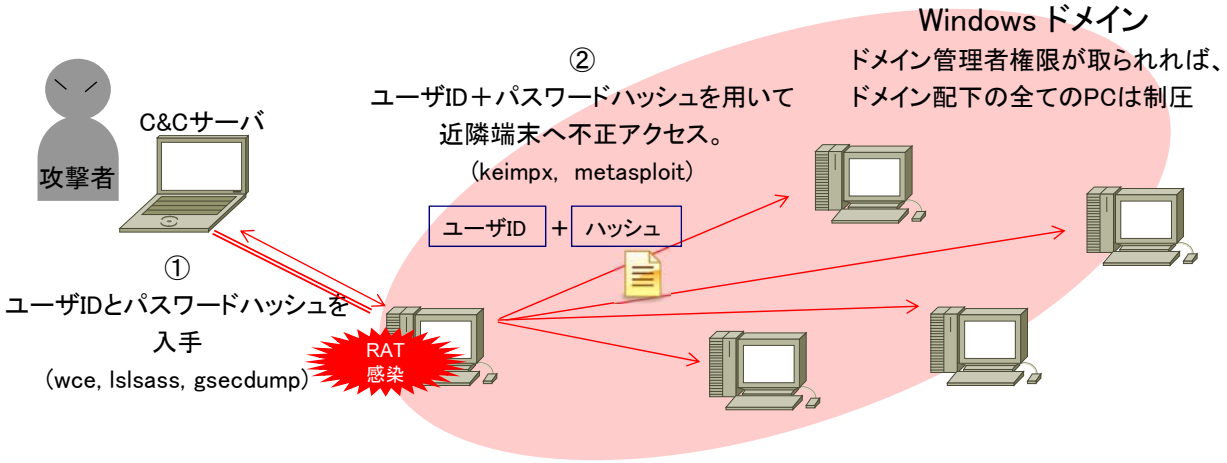
端末間での侵害拡大

- 他端末へ攻撃、外部からコントロールできる端末を複数台、確保する。
- 主な手法
  - Pass the Hash攻撃
  - オートコンプリート機能による保存パスワードの盗用
  - ネットワークモニタリング



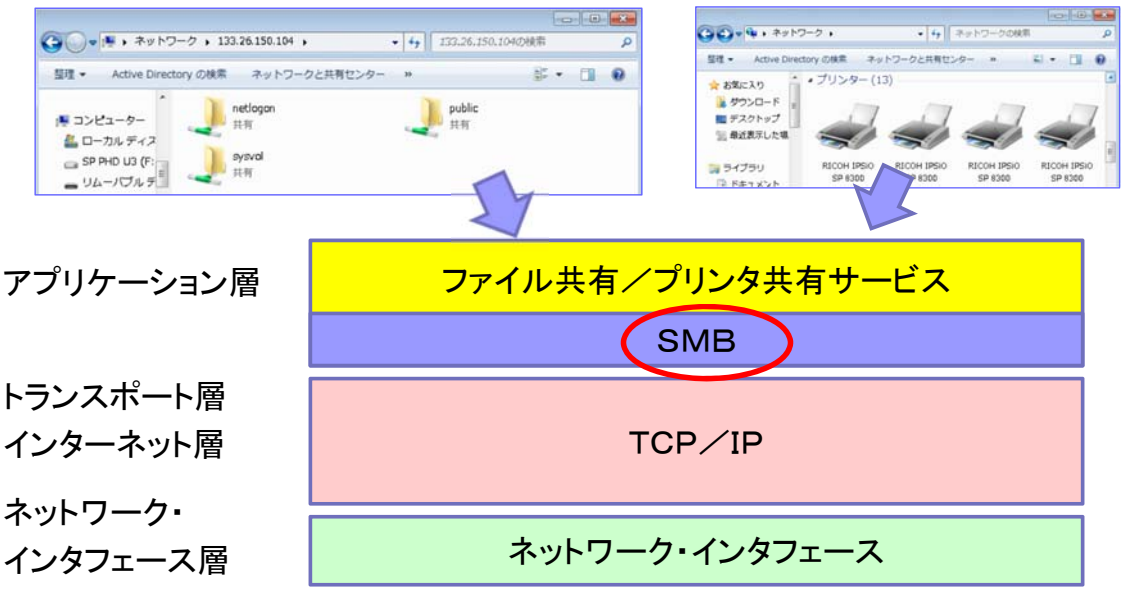
Pass the Hash 攻撃 （アクセス権限の入手）

- Windowsの認証を回避し、ユーザ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。



Pass the Hashのしくみ

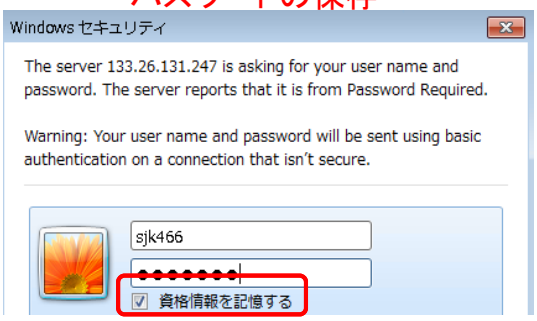
- ファイル共有やプリンタ共有の機能を悪用している。
- SMB通信プロトコルを使用。



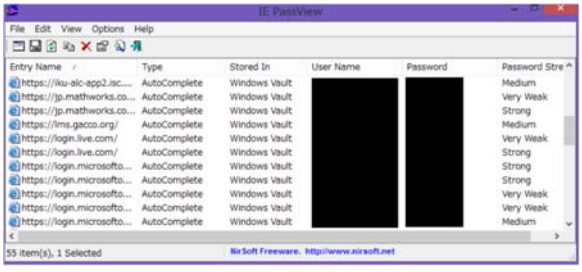
オートコンプリート機能で保存されたパスワードの盗用

- オートコンプリート
  - キーボードからの入力を補助する機能。
  - 一度ブラウザから入力した「ユーザID＋パスワード」を、次回のアクセスからは自動入力に。
  - PC内部に保存されているパスワードは、（ツールで）読み取り可能。

パスワードの保存



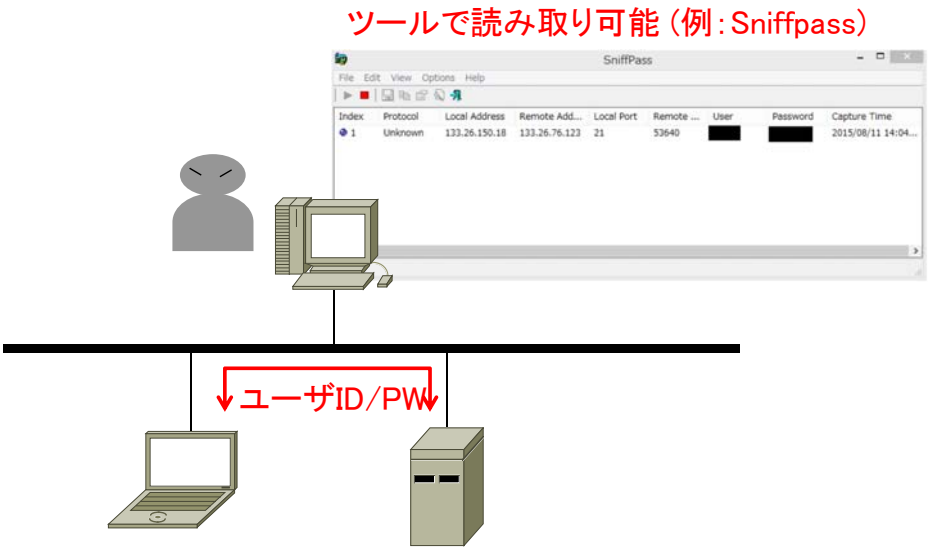
ツールで読み取り可能（例：IE PassView）



実習4
パスワードの解析

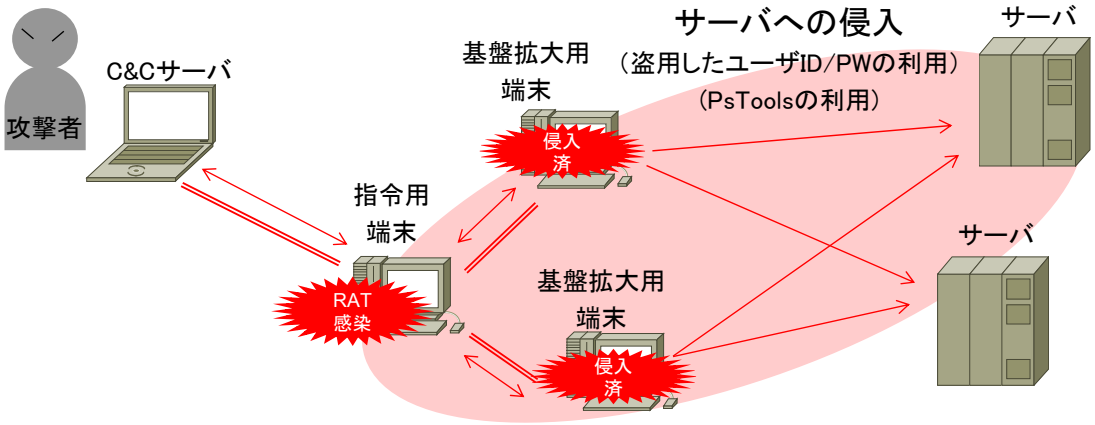
ネットワークモニタリング

- ネットワーク上を流れる情報をモニタリング。
- 暗号化されていない「ユーザID/パスワード」を入手可能。



サーバへの侵入

- 感染端末を足掛かりとして、サーバへの侵入を試みサーバ上の重要情報にアクセスする。
- 主な手法
  - PsTools



PsTools(PsExec)

- Windows管理ユーティリティ
- Microsoftがフリーで配布
  - https://technet.microsoft.com/ja-jp/sysinternals/bb897553
- コマンド
  - PsExec・・・リモートでプロセスの実行を行う
  - PsKill・・・リモートでプロセスの強制終了を行う
  - PsShutdown・・・リモートでシステムのシャットダウンを行う
- サーバ側で、ファイル共有サービスが動いていれば動作。
  - SMBのプロセス間通信機能を使用
  - 感染端末と同じドメインであれば、パスワードも不要。

まとめ

- メールの信憑性調査（すべてのメールに対して）
  - 通報メール自体が標的型サイバー攻撃の場合がある
  - メール本文、ヘッダー情報から信頼できるものかを判断する
  - 添付ファイルがある場合は更に慎重に調査する
- 標的型サイバー攻撃の手法
  - 初期潜入
    - メールの添付ファイルやURLリンクを使ってRATを送信、感染させる
  - 基盤構築
    - RAT経由で内部情報を窃取するためのツールを送り込む
  - 内部侵入・調査
    - 内部ネットワークシステムの調査・把握
    - 他端末のアクセス権を入手して侵害拡大
    - サーバーに侵入