A-3.
インシデント発生時の対応フローチャートに基づく演習

明治大学　服部　裕之
金城学院大学　西松　高史

公益社団法人　私立大学情報教育協会

このセッションの目標

標的型サイバー攻撃の「内部侵入・調査」手法を学び、
実習にて確認する

（1） 標的型サイバー攻撃における攻撃パターンを理解する
（2） 被害範囲の予測・調査を行うことができる

＝

インシデント対応フローチャートに基づき、
システム担当者としての行動がとれる！

公益社団法人　私立大学情報教育協会

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＆マルウェアの検出。
2. 既に感染しているPCは無いかどうか、確認。
3. 被害（情報漏えい）の調査・予想。
4. 報告・連絡・協議。
5. 感染拡大防止・緊急対応の検討。
6. 警察への連絡。
   セキュリティーベンダへの依頼。

メニュー

A-3-1 「内部侵入・調査」実習

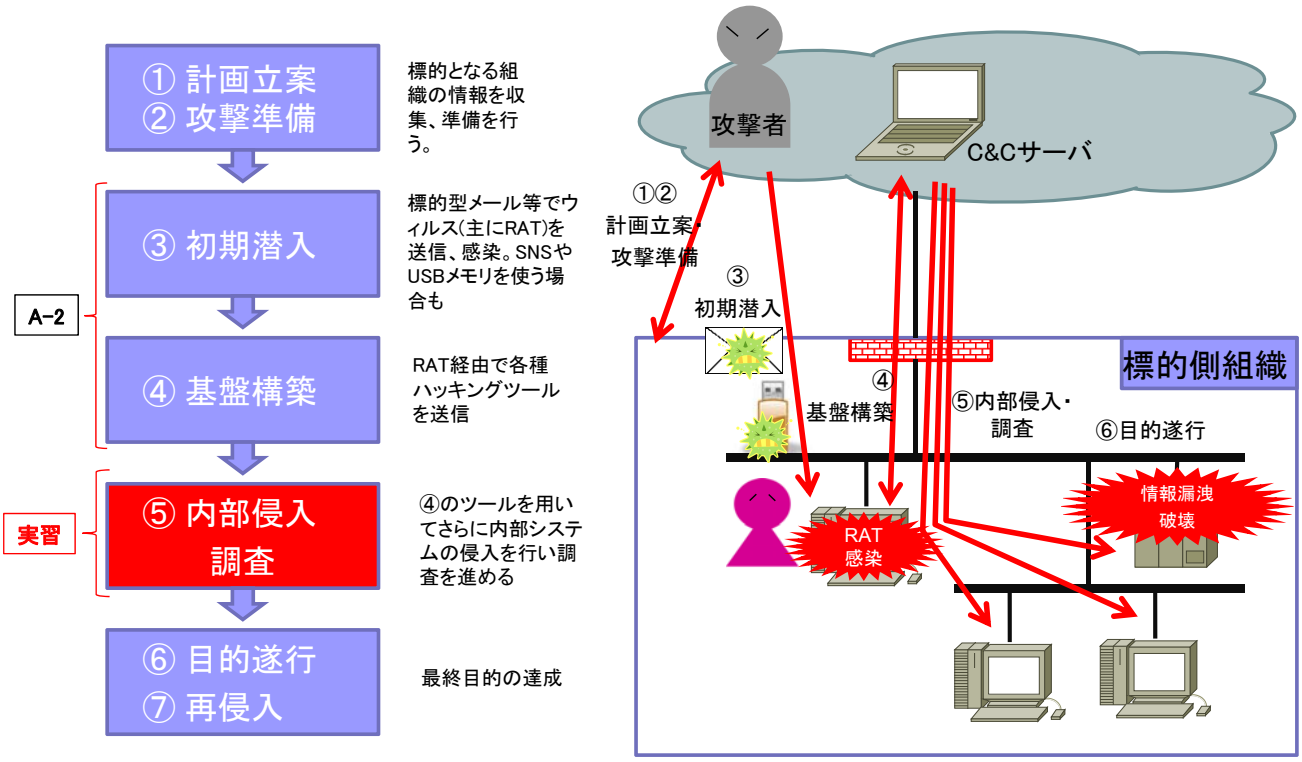
1. 標的型攻撃の流れ
2. 「内部侵入・調査」の手法
3. 実習
   1. 内部ネットワークの調査
   2. 他PCへの侵入
   3. サーバへの侵入

A-3-2 「被害範囲の予想」演習

1. 「被害範囲予想報告書」の作成

A－3－1
「内部侵入・調査」

標的型攻撃の流れ

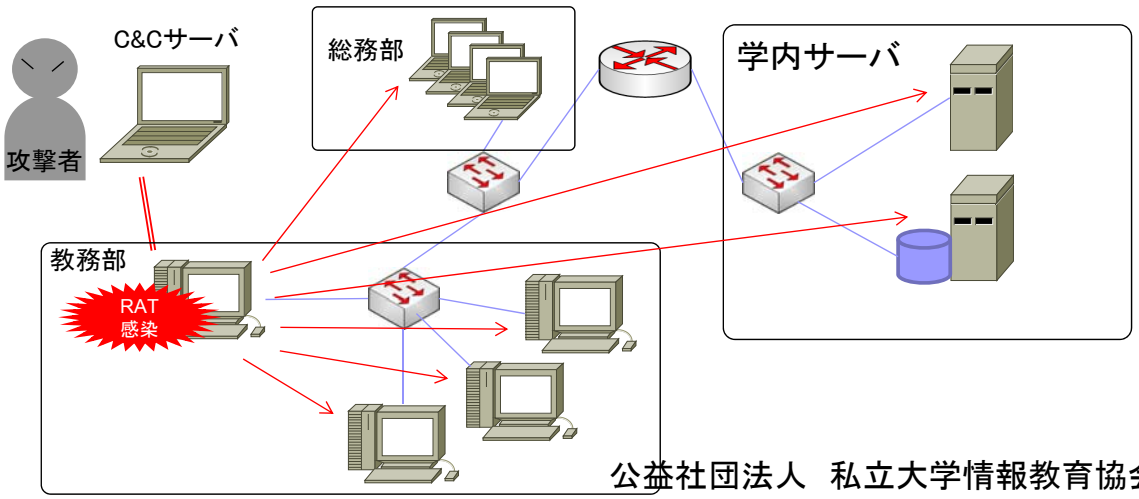


内部侵入・調査

1. 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
2. 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
3. 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

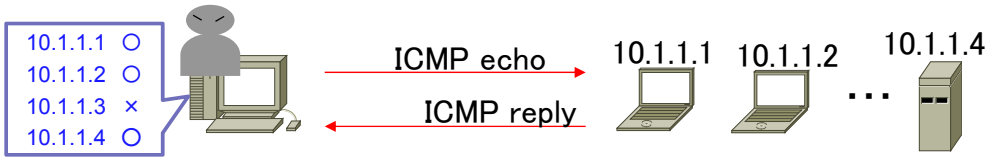
1. ネットワークの調査

- 標的組織の内部システムを把握する
  - IPアドレスの探索
  - サービスポートの探索
- 主な手法
  - ポートスキャン

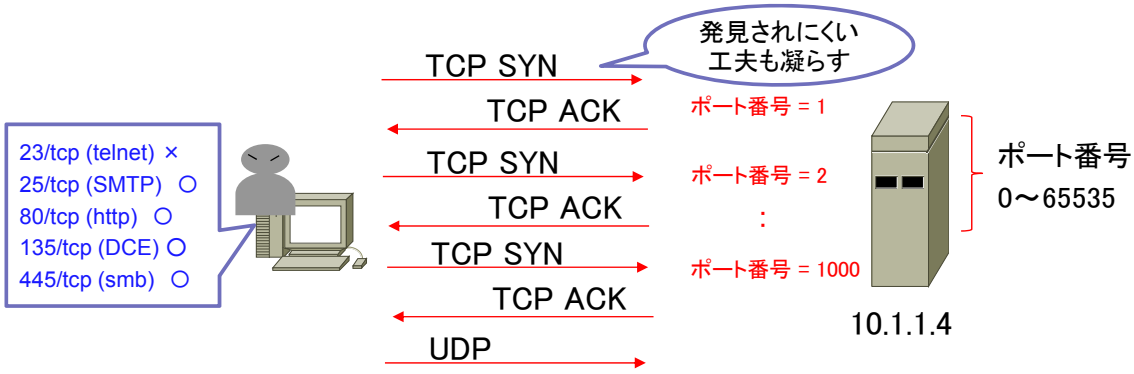


ポートスキャン

- 標的組織内のIPアドレスをしらみつぶしに調査。

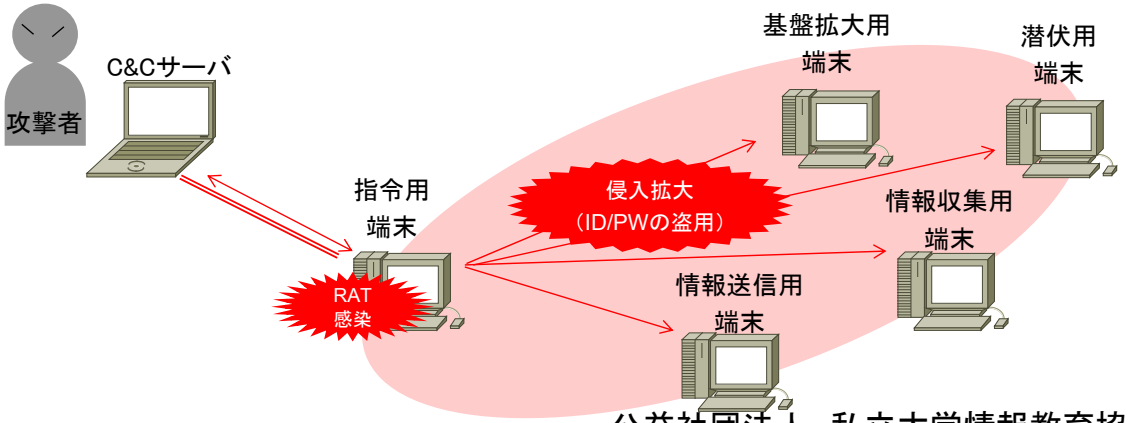


- 各端末のサービスポートをしらみつぶしに調査。



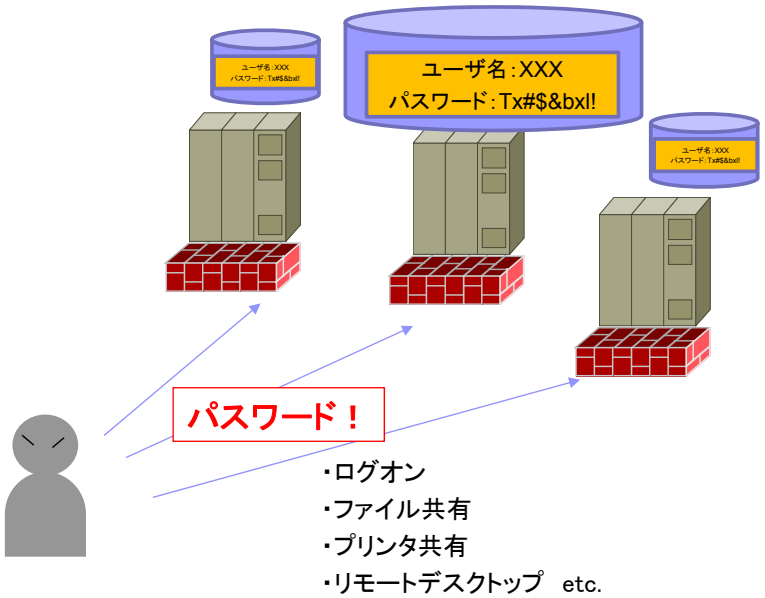
2. 端末間での侵害拡大

- 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

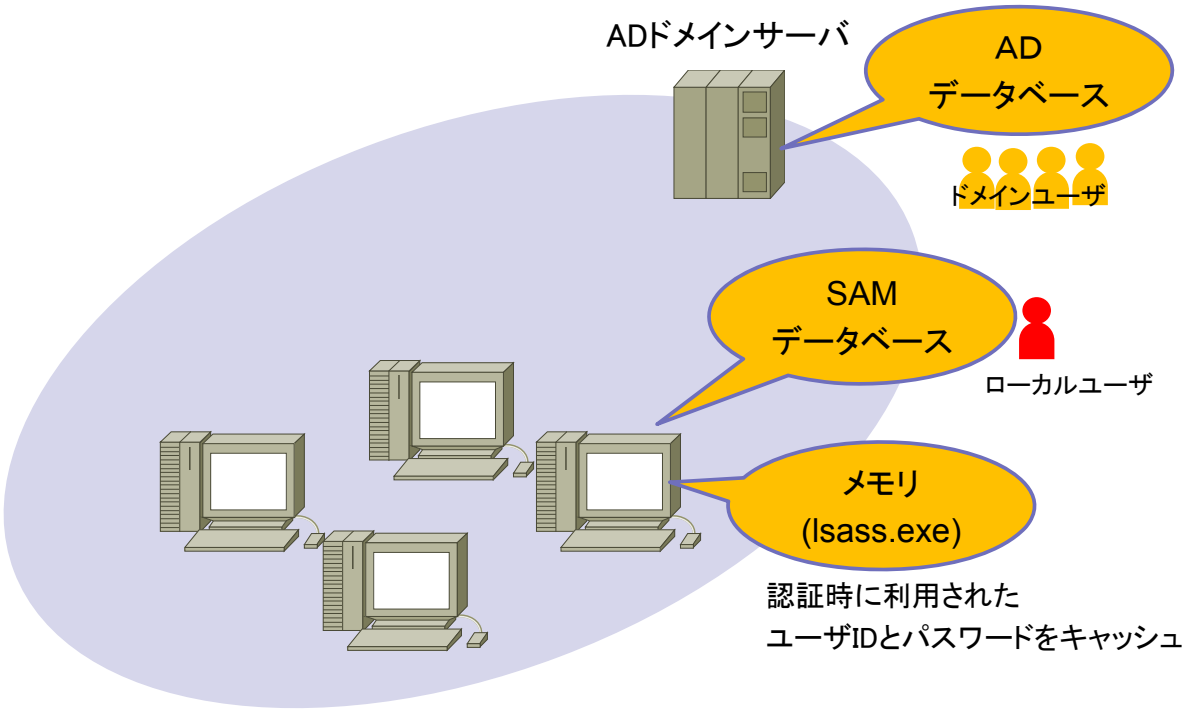


アクセス権限

- システムのセキュリティは「パスワード」で守られている。



パスワードはどこに保存されているのか?
(Windowsの場合)



パスワードはどのように保存されているのか？
(Windowsの場合)

- パスワードは、「ハッシュ値」に変換されて保存されている。

パスワード　**sjk2015**

↓ ハッシュ関数(MD4等)によって変換

ハッシュ値　**yc397ba5bce7afb30790c7e4b42ba**

★特徴
① パスワードの文字を1文字変えるだけで、ハッシュ値は全く別の数値になる。
② ハッシュ値から、元のパスワードを計算することはできない。

アクセス権限を入手し、内部システムへの侵入を進めるために？

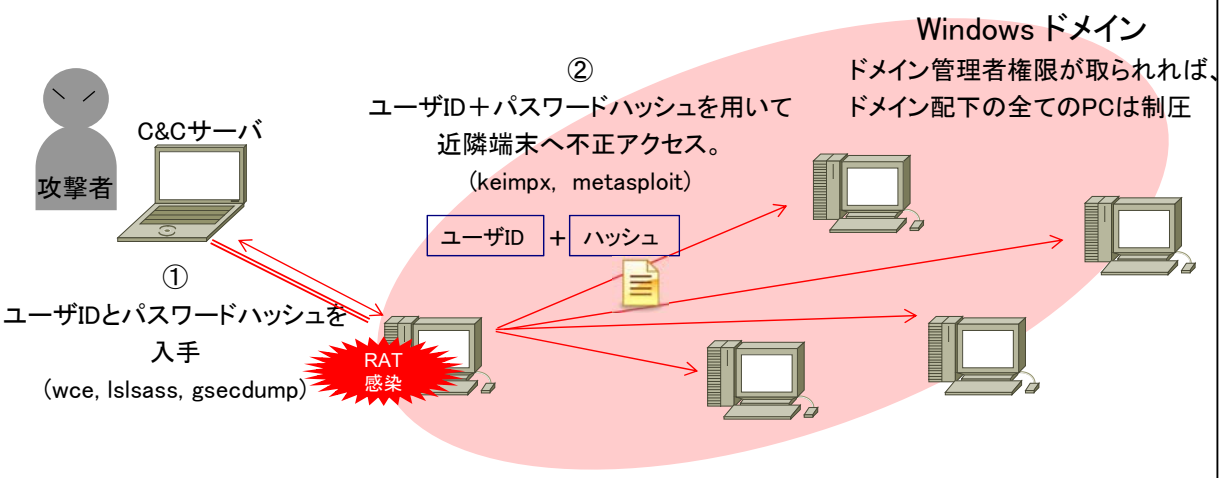
- 古いやり方：
  - パスワードハッシュとの照合でもとのパスワードを「推定」する。
    - 総当たり攻撃　（BruteForce)
    - 辞書攻撃　(レインボーテーブル）
    - 類推攻撃　(誕生日や名前などから類推)

→ いずれも、手間と時間がかかる。

- 今のやり方：
  - Pass the Hash攻撃

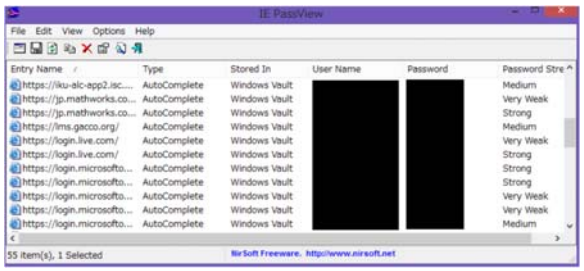
Pass the Hash 攻撃 （アクセス権限の入手）

- 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。



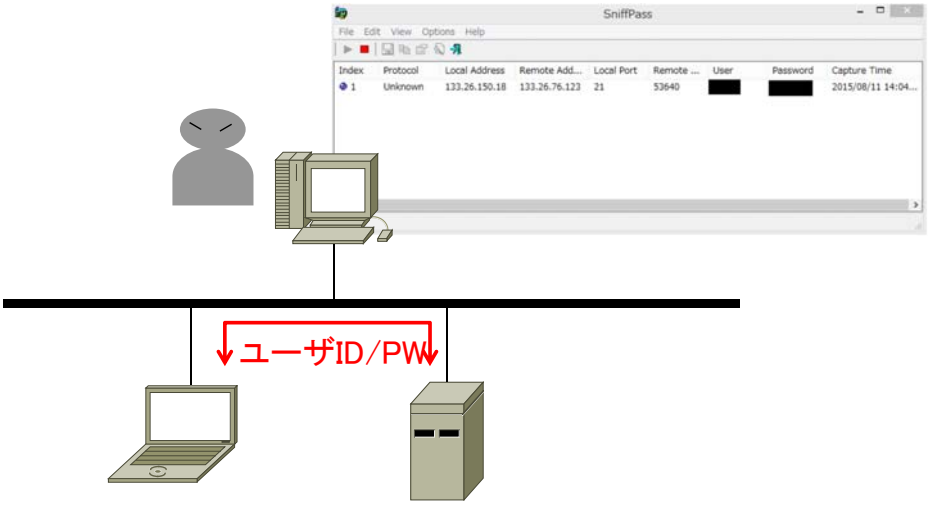
オートコンプリート機能で保存されたパスワードの盗用

- 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。
  - パスワードは、PC内部に保存されているが、取り出し可能。



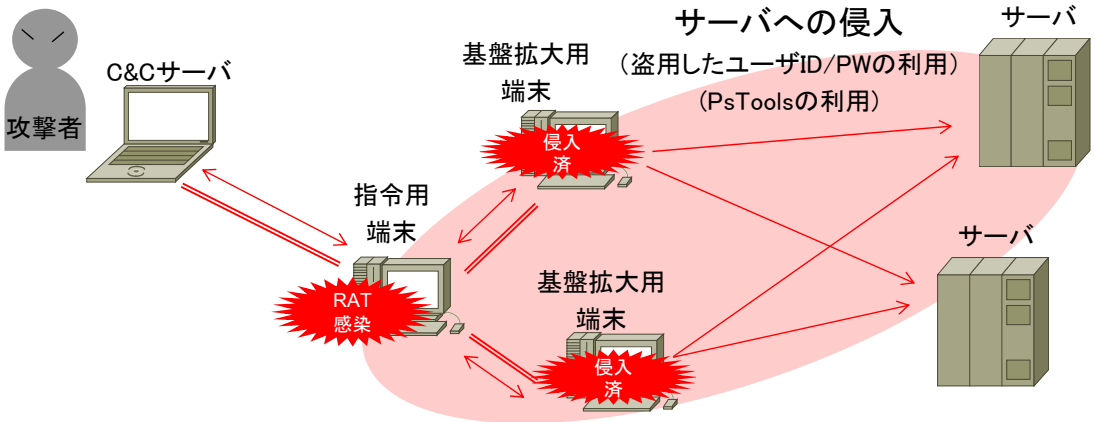
ネットワークモニタリング

- 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。



3. 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

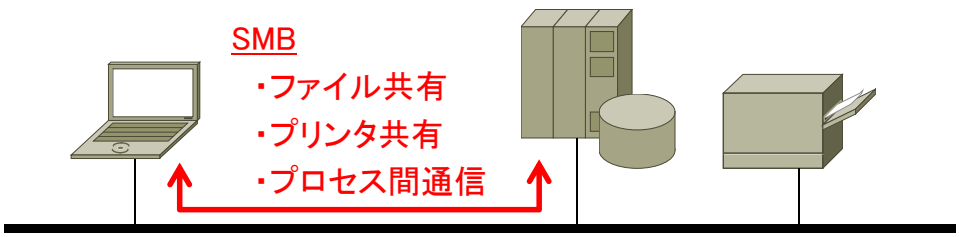


PsTools

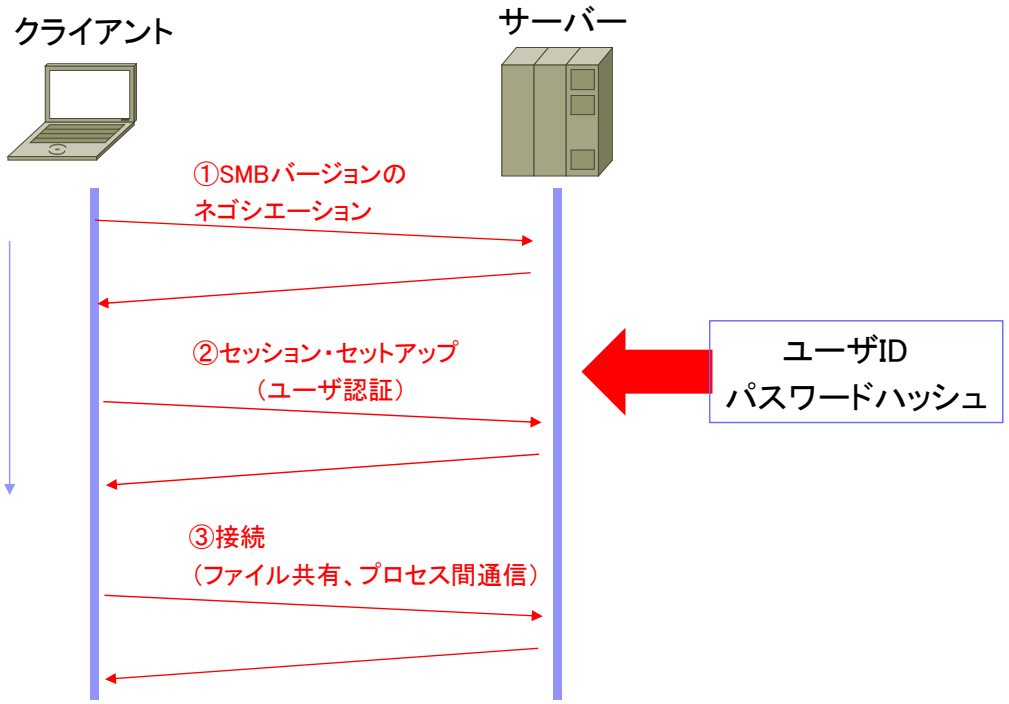
- Windows管理ユーティリティ
- Microsoftがフリーで配布
  - https://technet.microsoft.com/ja-jp/sysinternals/bb897553
- コマンド例
  - PsExec・・・リモートでプロセスの実行を行う
  - PsKill・・・リモートでプロセスの強制終了を行う
  - PsShutdown・・・リモートでシステムのシャットダウンを行う
- サーバ側で、ファイル共有サービスが動いていれば動作。
  - SMBのプロセス間通信機能を使用
  - 感染端末と同じドメインであれば、パスワードも不要。

SMB　- Server Message Block

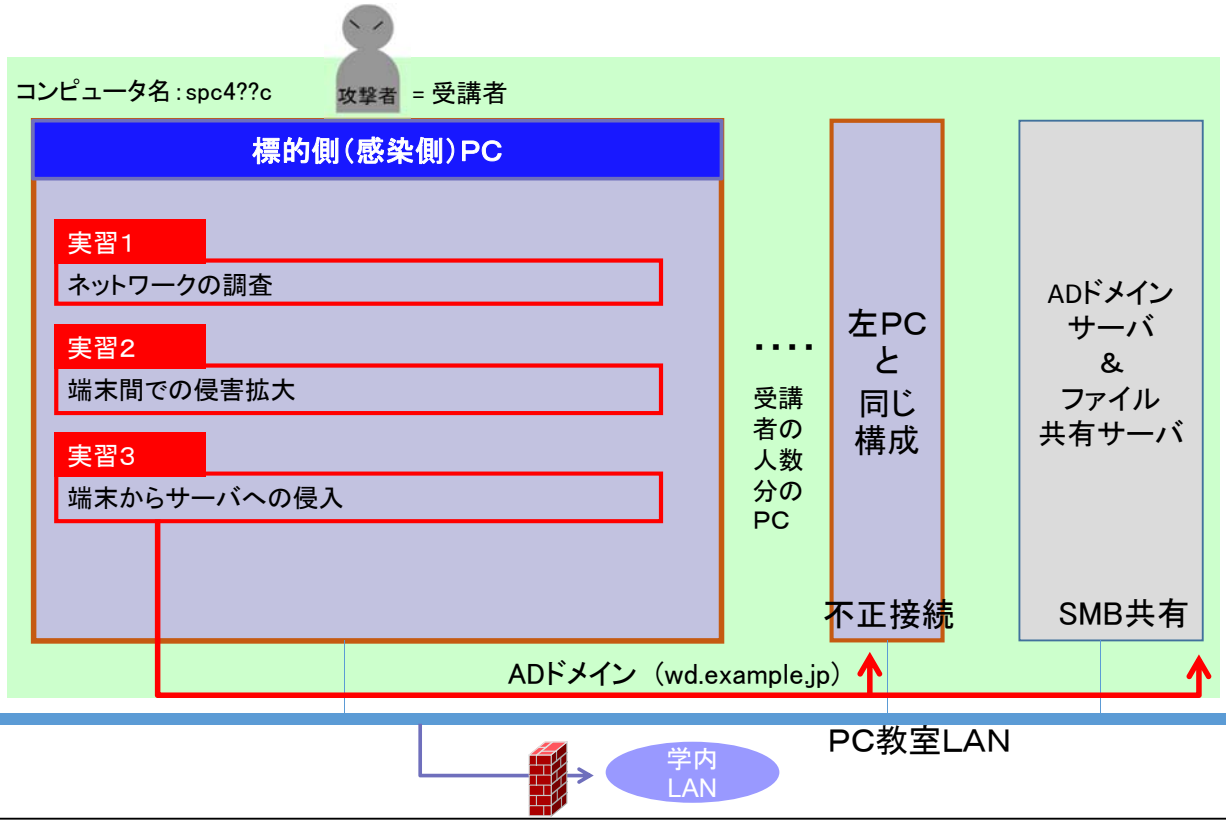
- IBMが設計しMicrosoftが改良した通信プロトコル
  - SMB1.0＝CIFS(Common Internet File System)
- 使用目的
  - ファイル共有やプリンタ共有
  - プロセス間通信
- 使用ポート
  - 135/tcp、445/tcp、1025～65535/tcp



SMB通信の概要



実習.「内部侵入・調査」概要



Ａ－３－２
「被害範囲の予想」演習

被害範囲の予想

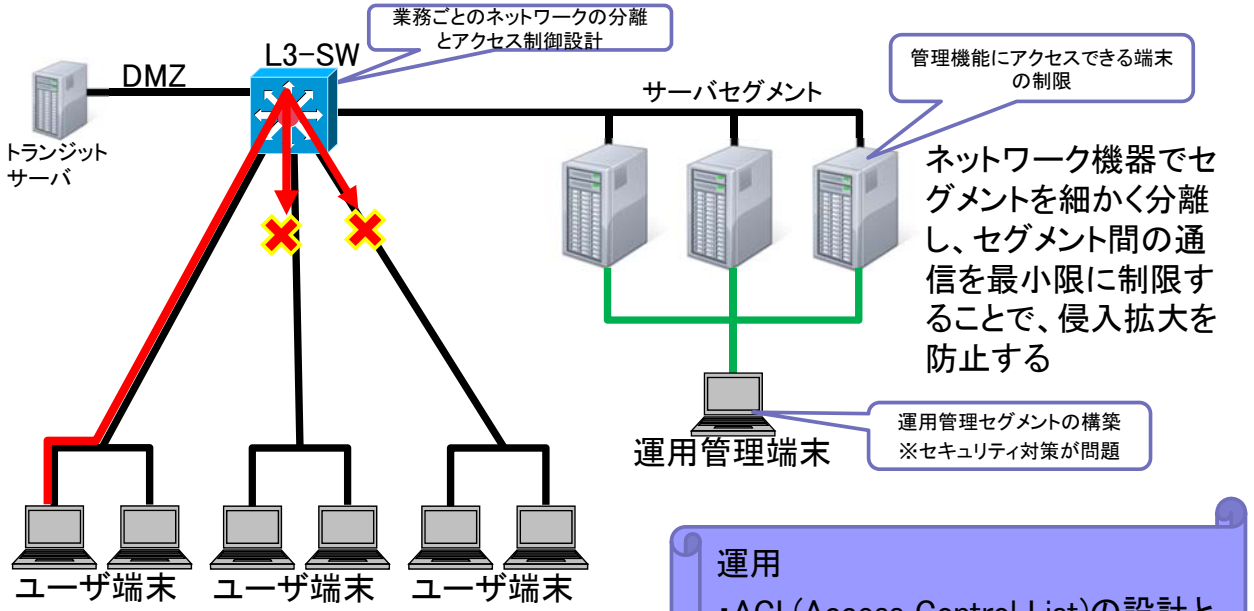
- 演習１
  SJK大学のシステム構成を元に、それぞれのサブシステムが被害にあう（あっている）可能性を予測する。
  - 後にセキュリティ業者へ調査依頼を行う際の優先順位を検討する際の資料にしたい（費用と時間の面で）。
  - サブシステムごとに被害の可能性を3段階（高、中、低）くらいに区分する。
  - ⇒「被害範囲予想報告書」の当該項目に記入
- 演習２
  流出した可能性がある情報は何かを予測する。
  - 被害にあった可能性があるサブシステムに、もともと保存されていたファイル情報を元に予測。
  - ⇒「被害範囲予想報告書」の当該項目に記入

「内部侵入・調査」の予防策

- ネットワークレベルの対策
  - ① ネットワークの分離設計とアクセス制御
    - 業務ごとにサブネットを分割
    - ユーザ端末とシステム管理用端末の分離
- 端末レベルの対策
  - ② ユーザ端末間のファイル共有禁止
  - ③ オートコンプリートの禁止
  - ④ キッティング時に設定した共通アカウントの削除
- ドメインレベルの対策
  - ⑤ 管理者権限アカウントのキャッシュ禁止
- 監視の強化
  - ⑥ トラップアカウントによる認証ログの監視と分析

①ネットワークの分離設計とアクセス制御

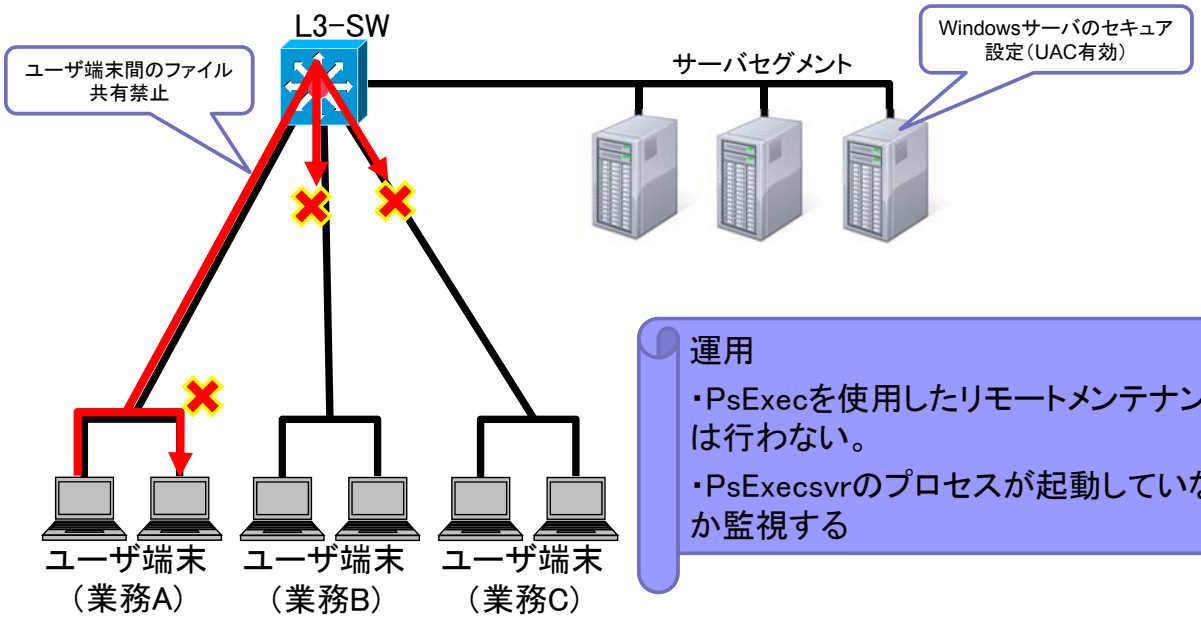
- 攻撃者の侵入範囲の限定およびサーバへの侵入拡大防止が目的



運用
・ACL(Access Control List)の設計と定期的な見直し

②ユーザ端末間のファイル共有禁止

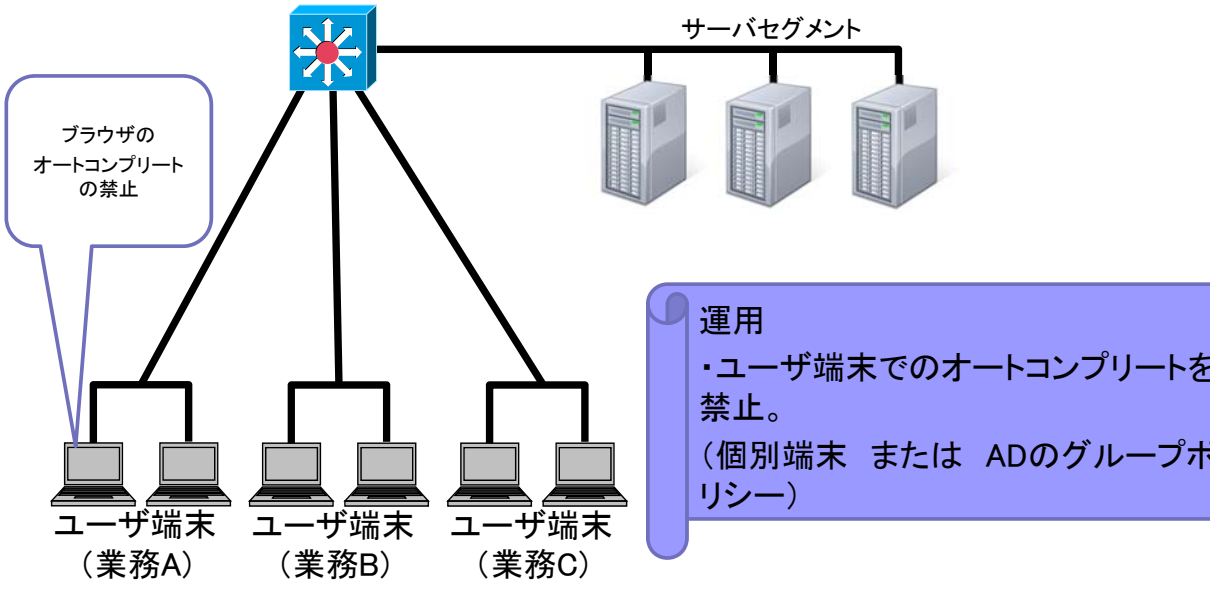
- ユーザ端末から必要な通信先(File Serverなど)に限定したファイル共有を許可することにより、侵入拡大を防止することが目的



運用
・PsExecを使用したリモートメンテナンスは行わない。
・PsExecsvrのプロセスが起動していないか監視する

③オートコンプリートの禁止

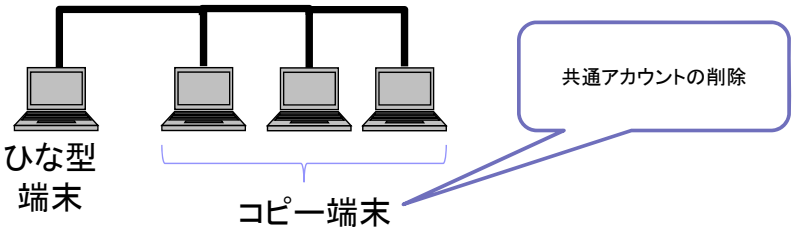
- 認証情報（ID/PW）が端末上に保存されることを抑制。攻撃者に窃取され内部サービスへの侵入拡大を防ぐことを目的



運用
・ユーザ端末でのオートコンプリートを禁止。
（個別端末　または　ADのグループポリシー）

④キッティング時に設定した共通アカウントの削除

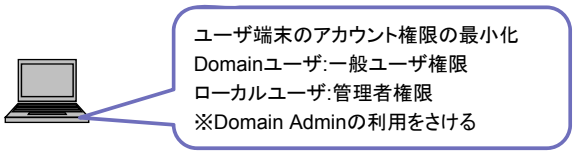
- ひな型を複数のPCに展開する際、同じアカウントがコピーされてしまう。これを削除することにより、Pass the Hash攻撃による他端末への侵入拡大を防ぐことを目的



運用
・共通アカウントを削除

⑤管理者権限アカウントのキャッシュ禁止

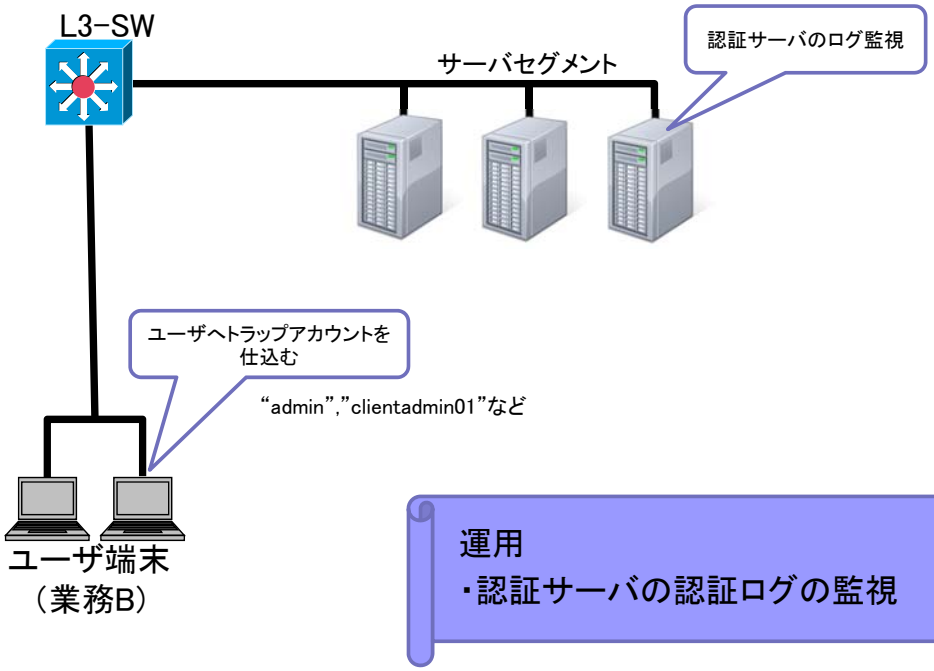
- リモートからのパッチ配布などの管理者権限が必要な運用を維持しつつ、各サーバに影響を与えないアカウント運用を実現することを目的



運用
・ユーザ端末でのDomain Adminでログインを禁止。
・ユーザ端末でDomain Adminグループのユーザがログインしていないか定期的に確認。

⑥トラップアカウントによる認証ログの監視と分析

- ユーザ端末上で通常業務で使用しないトラップアカウントを仕込み、重点的に監視を行うことで、不正なアクセスと正常なアクセスを見分けることが目的



運用
・認証サーバの認証ログの監視

報告書の作成

- 被害範囲予想報告書
  - 調査すべきサーバ・端末の範囲
  - 標的型攻撃今回の標的になり得る情報資産の一覧
  - 調査費用試算

まとめ

- 余分なものは見せない
  - 機能別ネットワークの設計
  - 運用管理ルール（アカウント管理など）
- いかに速く気づくか
  - ログの確認の徹底
  - 罠を仕掛けておく
- 対策製品の導入
  - 対費用効果

参考資料

- IPA　独立行政法人情報処理推進機構
  - 『高度標的型攻撃』対策に向けたシステム設計ガイド
    ～入口突破されても攻略されない内部対策を施す～
    https://www.ipa.go.jp/files/000046236.pdf