S1 標的型攻撃の現状と対策

企業側での対策

ネットエージェント株式会社

杉浦 隆幸

■目的

– 外部からの攻撃を防いだり、避けたりする

■ルール

– 守るのみで、攻撃しない、反撃しない
– 守りきったら勝ち
– 侵入されたら、できる限り被害が無いようにする
– 終わりは無い
– ウイルスが入ってきても被害がなければよい
– 予算と時間は限られている

THIS IS WAR!

だたし、人は死なない

100% 防ぐ方法は無い

新しいウイルスはウイルス対策ソフトが無効

ウイルス対策ソフトで検知しないこと確認してから攻撃に利用

一番弱いところから狙う

システム管理者　より　一般従業員
若　　者　　より　高年齢層
技　　術　　より　心　理

１人抜けると被害が大きくなる

- PCには重要な情報がいつの間にかいっぱい
- そこを踏み台に感染拡大、騙す手口も巧妙に

遠隔操作で社内冤罪も

- 遠隔操作機能でその人になりきって
  なんでもできる

攻撃性能は一定ではない

- 攻撃者のレベル
- 高度な攻撃方法の手の内を見せないためか

多層で段階ごとに軽減する

【1】ウィルスに入られないようにする

【2】ウィルスが入ってきても引っかからないようにする

【3】ウィルスに入られたことが分かるようにする

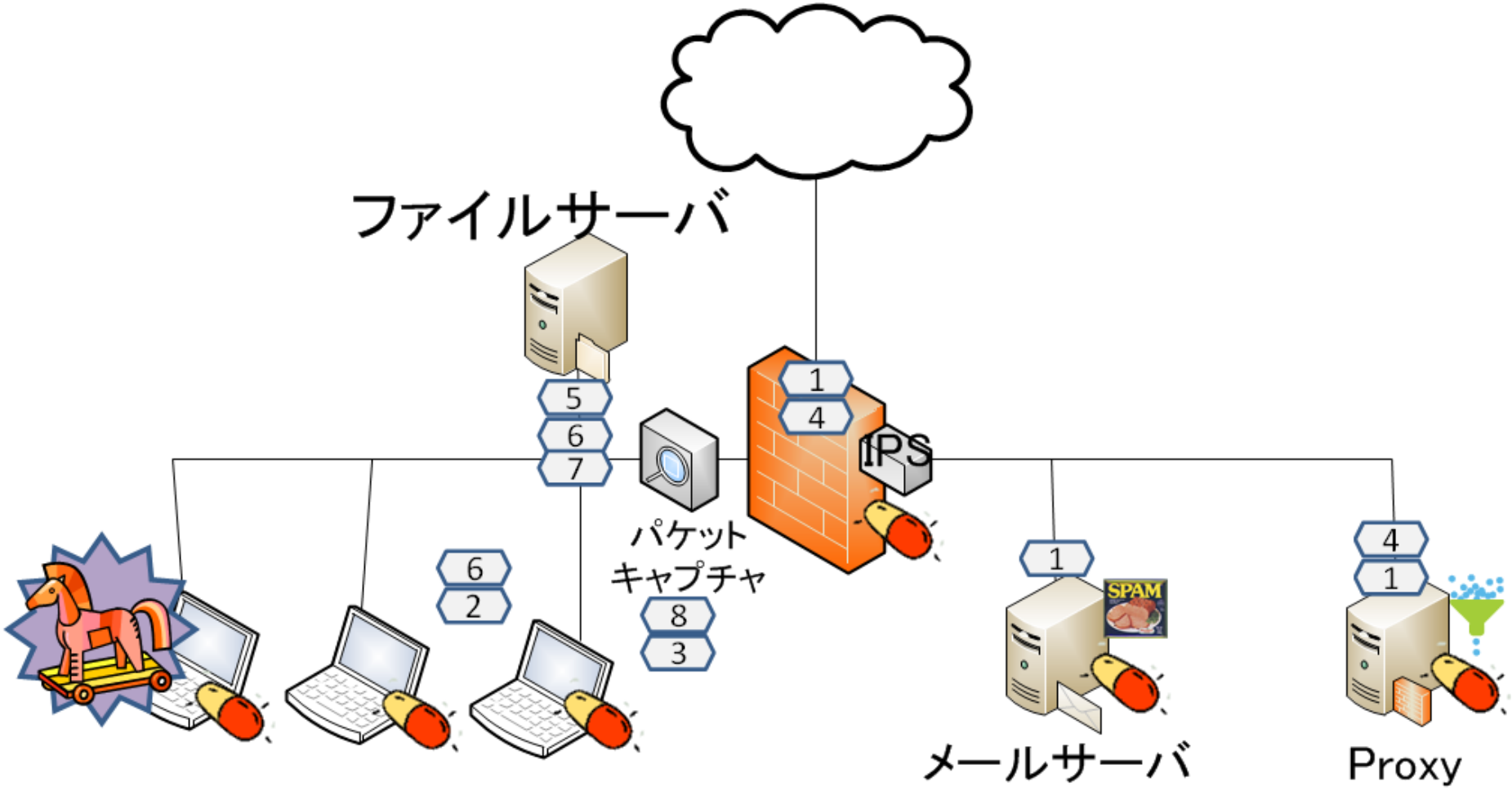
【4】ウィルス通信(≒内部情報)が出て行かないようにする

【5】ウィルスに入られた後に被害が拡散しないようにする

【6】ウィルス通信(≒内部情報)が出ていった場合にでも、
重要な情報が出ていかないようにする

【7】内部情報が出ていった場合にでも、
一度に大量に持っていかれないようにする

【8】ウィルスの長期間の侵入を許さない



１.入られないようにする

- ゲートウェイ型のウイルス対策ソフト（既知のウイルスのみ）
  - メール
    - 暗号化ZIPは対象外
  - Web
    - HTTPSは対象外
    - コンテンツフィルタ
- 新しい対策方法（未知のものにも対応）
  - メールの添付やURLを画像化製品
  - サンドボックスで実行型の対策製品
    - 暗号化ファイルは対象外になりやすい

2. 入ってきても引っかからないようにする

- ウイルス対策ソフト(エンドポイント)
  - 既知のウイルスのみ対応
  - 検出力より、防御力重視で
- 演習メール
  - 予防接種型(一般従業員の経験値稼ぎ)
    - 日本のセキュリティスペシャリストにより高度な詐欺メール(演習用)の手法が確立
    - 多くの人が開いてしまうメールが送られる。
      - これをどう防げば？
      - 効果が短期的のため、定期的に実践する必要がある
    - あまりにも高度なものは専門家でも開いてみるまで安全かどうかわからない。

2. 入ってきても引っかからないようにする

- 一般的な対策
  - アップデート
    - OS
    - Office
    - ブラウザほか周辺
    - Adobe Flash, Reader
    - Java
    - 他、常に自身で最新を保てないソフトウェア
  - ウイルス対策ソフト

2．入ってきても引っかからないようにする

- 添付ファイル
  - 安易に添付ファイルを開かない
  - できる限り添付ファイルをスルーする
  - 開きたくなる添付ファイルは標的型攻撃と思う（要電話確認）

→出所の不明なファイルをダウンロードしたり、ファイルを開いたりしない

- 本文
  - 安易にURLリンクをクリックしない。

3. 入られたことが分かるようにする

- IDS（まともに運用できれば）
  - 多くの通信はIDSで検知可能
- パケット解析
  - パケット解析が出来れば見つけることも可能になる
  - 後から調べるためにはフルに近いパケットキャプチャが必須
    - HTTPSなどで暗号化されたらわからない部分が多くなる

4. 出て行かないようにする

- プロキシサーバがある環境であれば、認証プロキシが有効
  - 共通パスワードでも効果が高い
- プロキシサーバのポートが 80 8080 3128 8000などでなければ、なお良い
- IPSが有効に働く場合もある
- プロキシサーバ必須の環境でなければ、有効な対策は難しい

5. 入られた後に被害が拡散しないようにする

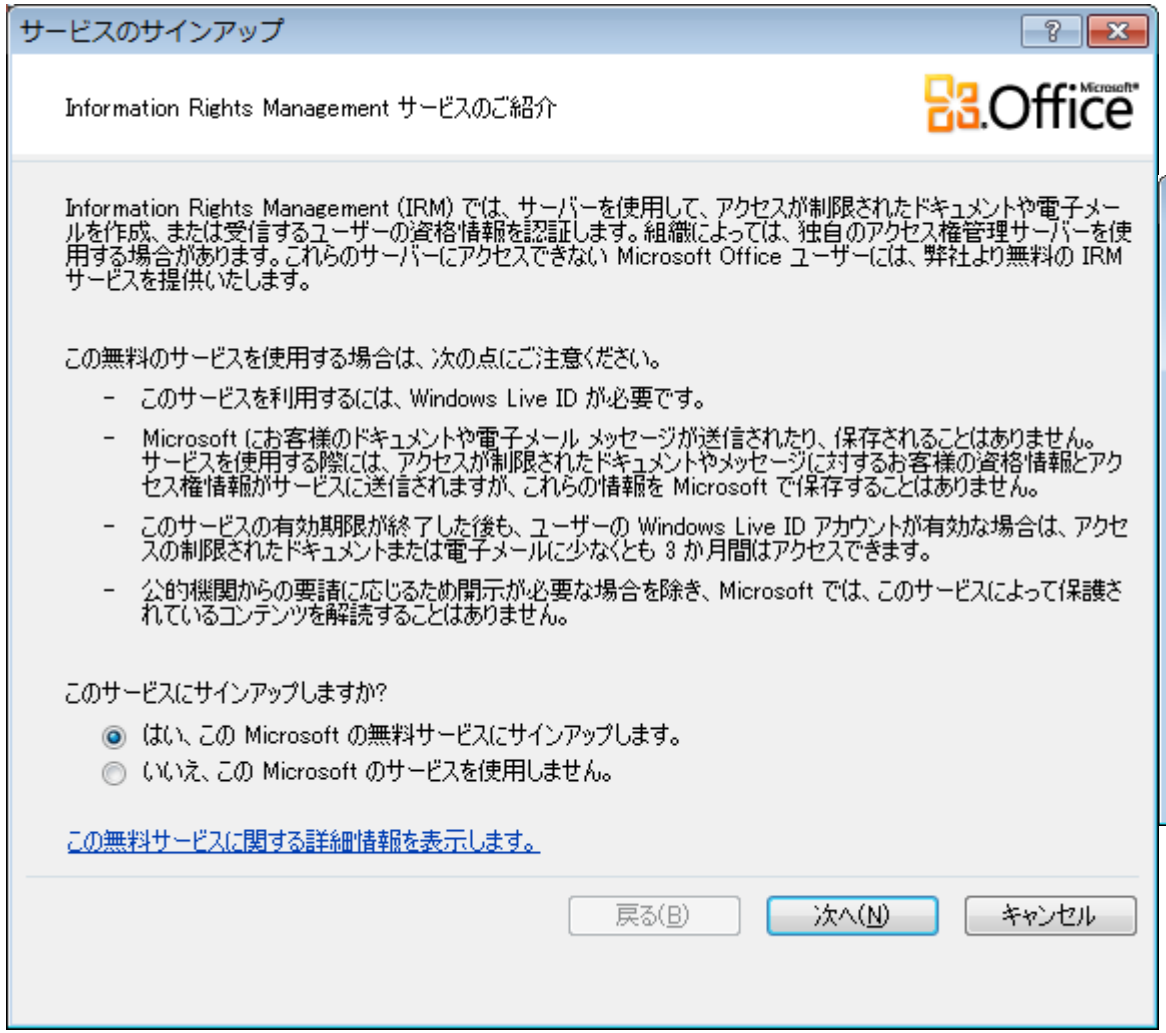
- 脆弱性を突くことが多い
  - リモートデスクトップや安易なパスワードによる
- できる限りローカル管理者権限を与えない
- アップデート管理
  - LAN内のアップデート管理がしっかりしていればそこを拠点に被害が拡大しにくい。

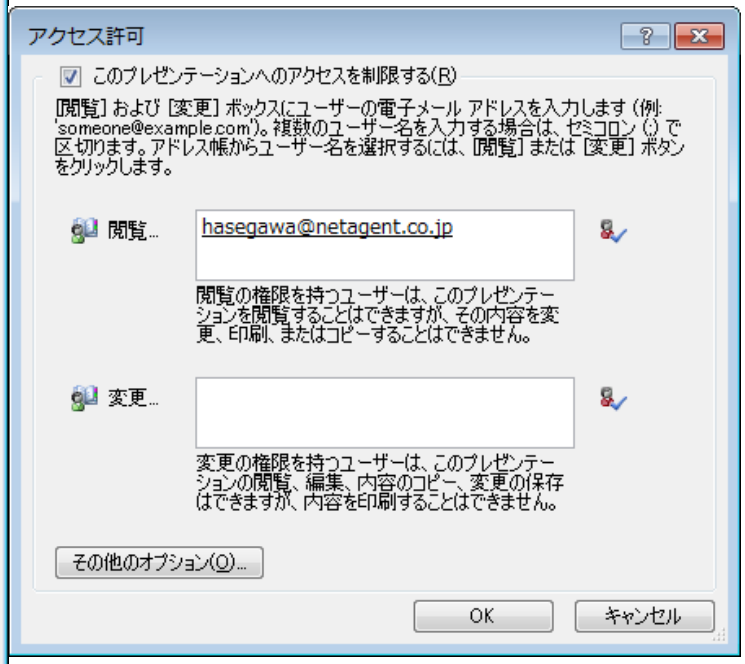
- 古いOS古いソフトのアップデート
  - WindosXP,Office2003 マシンの寿命は来期まで、来期中にアップデートが必要

6. 出ていった場合にでも、重要な情報が出ていかないようにする

- DRM
  - Right Management Serviceを使えば、企業から個人まで閲覧・変更できる権限を各個人に与えることができる。
  - 小規模、個人向けは Infomation Right Management (RIM) サービス（要Windows Live ID）で利用できる。
  - 企業向けは Active Directory Rights Management サービス (AD RMS)(ADのバックアップは必須：ADがなくなるとファイルが読めなくなる）
  - 顧客情報や、機密情報など他人に見られて困るファイルは必ずアクセス制限をする。
- 重要な情報の管理
  - パスワードとアクセス制限

DRM例





7.出ていった場合にでも、一度に大量に持っていかれないようにする。

- デスクトップ、ドキュメントフォルダにファイルを置かない
- ファイルサーバのアクセス制限をきつくする
- Tempフォルダをクリーニングする
- メールをWebベースにする

8.長期間の侵入を許さない

- 定期的にやられていないかを徹底的に調べる
  - パケットキャプチャからのパケット解析が有効

リスクゼロのネットワーク社会を目指して

ネットエージェント株式会社
03-5625-1243
E-mail:info@netagent.co.jp
URL :http://www.netagent.co.jp/