A-1.
テクニカル・コースの概要

中部大学
岡部　仁

標的型メール攻撃の現状（その１）

- 目的：　情報→金銭の搾取
- 経路：　メール（添付ファイル、水飲み場）、USB
  PC(事務職員、教員、実習・実習室）
  → 他PC（管理）、自サーバ（他サーバ）
  → 管理者権限の取得　→　管理サーバ
  → 情報の持ち出し（分割、暗号化）
- 迷惑メール／ウイルス対策ソフトのすり抜け
  ウイルスの難読化、暗号化ZIP等
- メールアドレス：　公開アドレス　→　必ず確認（開く）
- やり取り型：　最初からウイルスメールを送らない

標的型メール攻撃の現状（その2）

- メールの内容（文面）
  - 不自然な日本語 → Web コピペ
  - 本人名、本物メール（乗っ取りPC）→ 内部拡散
  - 件名： 本物メールの修正版で時間差少
- 添付ファイル： 偽装の工夫
  - 実行ファイル形式は危険 → Word、PDFや画像ファイル
    - 処理プログラムの脆弱性
    - 「doc」、「xls」： バイナリ形式（ウイルス仕込み容易）
    - 「docx」、「xlsx」: テキスト形式（セキュリティ強化）
  - Word、PDFや画像ファイル → 実行形式ファイル（7割）

標的型メール攻撃の現状（その3）

- 実行ファイルの偽装
  - アイコン偽装
    - 「abc.exe」 → 「abc.pdf」
    - 拡張子非表示「xyz.txt」→ 「xyz.txt.exe」
  - 実行形式の添付ファイル： メールサーバ（ソフト）で抑止
- 実行ファイル（ウイルス）をZIP形式等で圧縮
- パスワード設定の暗号化ZIPファイル（やり取り型）
  - ウイルス対策ソフト、IPSのすり抜け

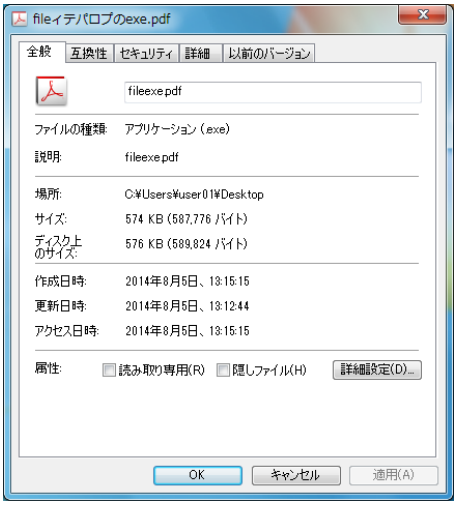
    文部科学省からの通知メール
- 対策： 実行形式ファイルの拡張子の表示

標的型メール攻撃の現状（その４）

- ファイル名の偽装
  - ユニコード制御文字RLO（Right-to-Left Override）の挿入
  - 文字を表示する流れを右から左に変更する制御文字[U+202e]

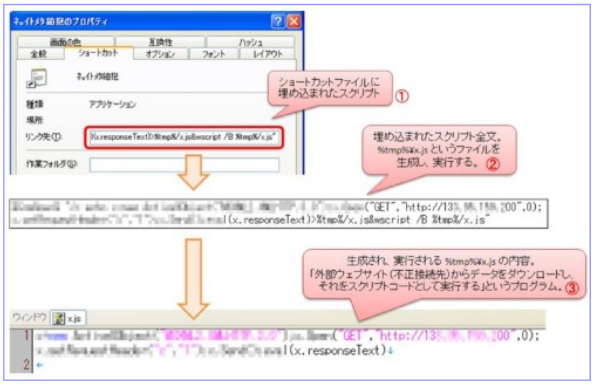
filefdp.exe
↓
(file [RLO] fdp.exe)
↓
file<u>exe.pdf</u>

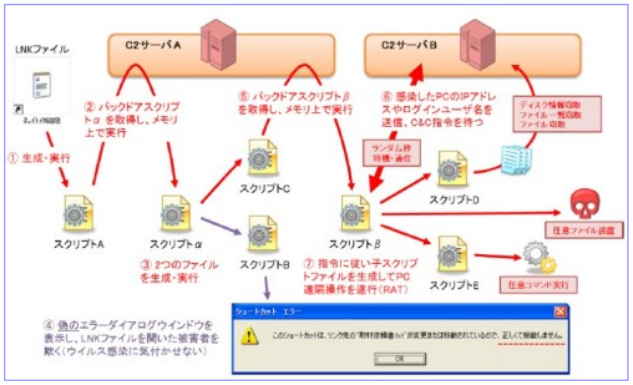
・名前の変更
・Unicode制御文字の挿入
・RLO



標的型メール攻撃の現状（その５）

- ショートカットウイルス(ウイルス実態のないものも)
  ショートカットのリンク先にスクリプトを仕込む
  「lnk」拡張子は表示されない
- ドライブ・バイ・ダウンロード

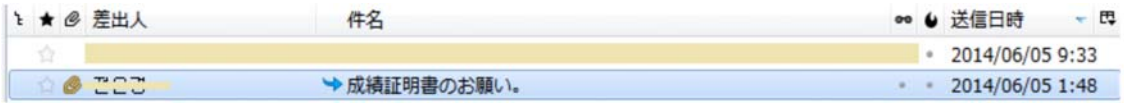




（IPAレポートより引用）

依頼・相談・苦情メール

- 以下のようなメールが届きました。あなたはどうしますか？



- メール／添付ファイル
  - ・開かない教育（注意）

重点の移動

  - ・開封後の気付き(監視)と通報（情報共有）

標的型メール攻撃と影響

その攻撃組織の**特別な目的意図性**、攻撃活動の継続性並びに窃取される情報が**国益や知財問題に影響**する。（IPA）

大学を狙う要素

・グローバルIPの運用
・インターネット接続帯域が大きく、24時間稼働しているサーバ、PCが多い
・セキュリティ意識が必ずしも高くない。端末が一元管理されていない。

組織が大学の場合

◆ 情報漏えい
- ● 学生（個人）情報
- ● 大学組織情報
- ● 国家（自治体）プロジェクト情報
- ● 科研費、共同研究プロジェクト情報

◆ 財政に影響する金銭搾取（不正ネットバンキング送金）：　法人救済は条件有

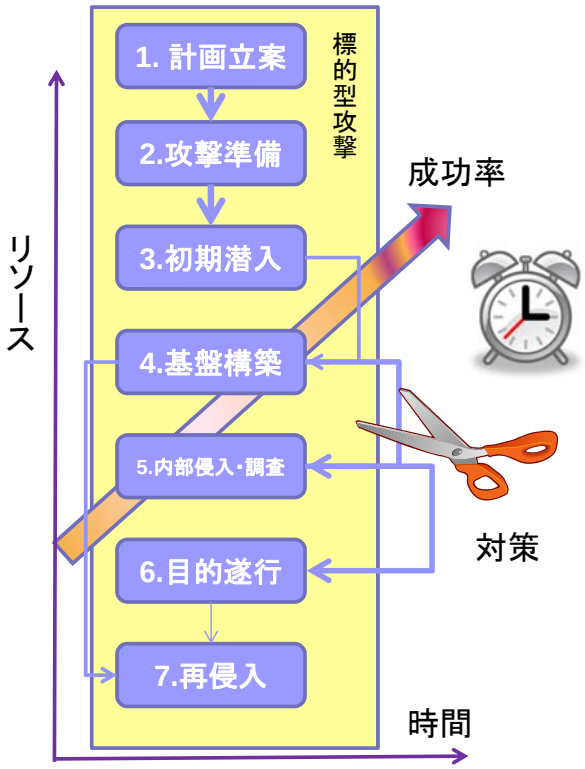
◆ その他

→
- ● 損害賠償、謝罪等経費
- ● 事後対応経費

→
- ● 学生募集／就職採用の低下
- ● 補助金の削減
- ● 外部資金の低下

大学経営・組織存続問題（終焉？）

標的型攻撃と対応



- 各攻撃段階が結ばれ、リソースと時間を加えた攻撃
- 対策： 各段階をつなぐ線を断ち切る
  時間を掛けさせる。
- 侵入ありきの前提
- 早期発見： アラーム

柔道では（ソフトバンク・テクノロジー：辻氏）
「技あり」は2本で負け、「有効」ではまだ戦える。押え込みも30秒経過しないと1本にはならない。
早期発見と正しい対応で、一本を取られない対策(経済的対応）

標的型攻撃の7つの段階

	段階等	内　容	コース	対策箇所等
1.	計画立案段階	Webサイト、SNS等情報取集		踏み台
2.	攻撃準備段階	マルウェアの作成、テスト、C&Cサーバ		練習台
3.	初期潜入段階	標的型（なりすまし）メール送信 ・マルウェア添付ファイル、USB ・ドライブバイダウンロード(DBD)	A-2(攻撃手法) A-3(痕跡解析)	入口対策 対策訓練
4.	基盤構築段階	遠隔操作（RAT)の構築	A-2 A-3	出口対策
5.	内部侵入・調査段階	パスワード搾取、ADサーバ、他ネット侵入	A-2 A-3	内部・出口対策
6.	目的遂行段階	目的情報の取得、暗号・細分化で外部送信	A-3	内部・出口対策
7.	再侵入	バックドア		入口・出口対策
	予防（軽減）対策 調査・事後対応		A-4 A-5	内部・出口対策

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 裕之氏

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. 内部侵入の拡大手法
   - Pass-the-Hash攻撃
   - 他PCへのアクセス
5. 実習
6. まとめ

A-3　標的型攻撃のインシデント分析・実習

デロイトトーマツ リスクサービス株式会社　岩井 博樹氏

実際の現場で行っている状況を踏まえた事例紹介と調査方法の実習

- マルウェアのバリエーション
  - なぜ、ウイルス対策ソフト等に検知されない
- 感染（内部侵入）拡大のパターン
- 感染したPCの痕跡調査方法
- その他

A-4　標的型攻撃に強いネットワークの設計

金城学院大学　西松 高史氏

- ネットワークの設計で被害を少なくすることができる“かも”しれない対策の確認
  - 『「標的型メール攻撃」対策に向けたシステム設計ガイド　～攻撃者が“内部探索しづらい（歩きづらい）システム設計策を施す～』を元にした要素技術の紹介
    - 内部活動を困難にし、ミスを誘い、内部侵入拡大の早期発見
  - 監視強化策と防御遮断策
    - 攻撃・対策マトリックスシート作成演習

脅威シナリオ	遮断設計対策（防止）	発見策（検知）

A-5　標的型攻撃に強いネットワークソリューション

シスコシステムズ合同会社 葛生 晋一氏

- 持続型標的攻撃(APT：Advanced Persistent Threat)
  - B　攻撃発生前（Before)
    - 既に潜んでいる可能性が高く、認識できていない。侵入即攻撃でない
    - Webﾏﾙｳｪｱの99%がJavaベース：　次世代FW通過
  - D　攻撃中(During)
    - 潜伏期間、攻撃に関わる通信の検出：　巧妙化（検出？）
  - A　攻撃発生後(After)
    - ネットワーク上で実際に目に見える挙動：　挙動の検出
- レトロスペクティブ　「A」　→　「D」に時間をさかのぼる
  - マルウェアの変化の来歴をさかのぼる
  - 侵入経路、影響範囲の割り出し　⇒　効果的な封じ込め
- 実習またはデモンストレーション

S-1　総合演習：インシデントレスポンス演習

- 目標
  - 標的型攻撃の確認
  - 正確な情報収集の促進
  - 対応戦略結滞のための要因収集

- 演習方法
  - サイバー防火訓練：　インシデントを想定したグループ（技術者と管理者等）による机上演習
    - フェーズ１　検知から被害の最小化：　封じ込め
    - フェーズ２　再発防止計画：　攻撃に強いネットワーク設計
    - フェーズ３　まとめ：　情報セキュリティ事故最終報告書の作成

まとめ

- 情報セキュリティ事故（インシデント）の**予防対策に完全（100%）はない**
- 事故発生時に「被害を**最小限に抑える**」、「速やかに復旧させる」対応

攻撃手法等の習得により早期の状況確認と事前対応策を習得

- 情報セキュリティ事故対応（インシデントレスポンス演習）

インシデント発生時の適切な対応と
再発（経済的な）防止対策を習得

7月16日発足
サイバーレスキュー隊（J－CRAT）：IPA

http://www.ipa.go.jp/about/press/20140716_1.html