資料4

NISC National center of Incident readiness and Strategy for Cybersecurity

標的型攻撃等の脅威について

平成28年8月

内閣官房内閣サイバーセキュリティセンター

(独)情報処理推進機構（IPA）

1. 増加する攻撃とその脅威

○　平成27年6月以降に公表された主な事例（政府機関・独法・特殊法人）

	省庁等	内　容
平成27年 6月1日	日本年金機構	PCが標的型メールによりウイルスに感染。個人情報が外部流出（約125万件）。
6月13日	国立医薬品食品衛生研究所 (国研)国立精神・神経医療研究センター 健康保険組合連合会	PCが1台ウイルスに感染。情報流出は確認されていない。 PCがウイルスに感染した疑い。情報流出は確認されていない。 PC2台がウイルスに感染。情報流出は確認されていない。
6月16日	(独)国際協力機構(JICA)	PC1台がウイルスに感染。さらにそのウイルスがPC10台及びサーバ8台に感染。情報流出は確認されていない。
6月17日	中間貯蔵・環境安全事業(株)	外部への不正な通信の痕跡を確認。 (8/7 情報流出は確認されなかった)
6月25日	法務省本省	端末が不正プログラムに感染した疑いがあることが判明。 情報流出は確認されていない。
7月10日	環境省本省等	PC5台がマルウェアに感染。情報流出は確認されていない。
7月17日	厚生労働省	ハローワークにおいて、端末1台がマルウェアに感染。 情報流出は確認されていない。
7月31日	内閣府	内閣府NPOホームページ上に設けられているNPOサポートデスク（委託業者管理）のメールアカウントが不正に乗っ取られた。情報流出はない。
8月7日	(独)科学技術振興機構(JST)	改ざんされたWEBサイトに業務でアクセスしたことにより、悪意あるプログラムに感染。最大で215名分の情報が流出した恐れ。
11月～ 平成28年2月	厚生労働省、金融庁、警察庁、財務省、国税庁等多数	サービス運用妨害（DoS）により、ウェブサイトが一時的に閲覧しにくい状態となった。

標的型攻撃やDoS攻撃等の、的を絞った執拗な攻撃が相次いで発覚

標的型サイバー攻撃の概要

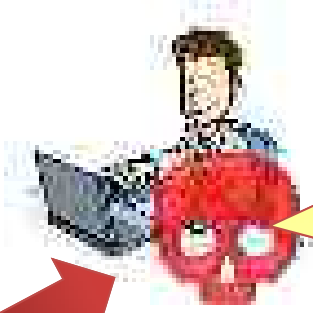
攻撃者は明確な目的を持ち、手口を変えつつ執拗に攻撃してくる

攻撃者

組織には多重の防御策が施してある

しかし攻撃者は、それを前提として攻撃してくる

企業・組織

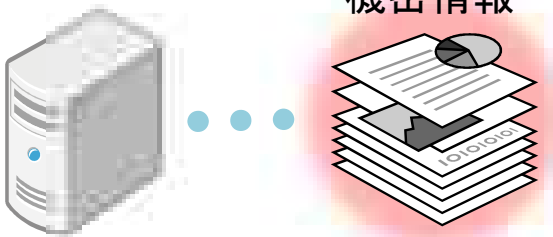


巧みに心理的効果を利用したメールを送り添付ファイルを開かせウイルス感染

組織内へ感染拡大

組織内からの攻撃は想定されていない

機密情報



標的型サイバー攻撃の仕組み

IPA

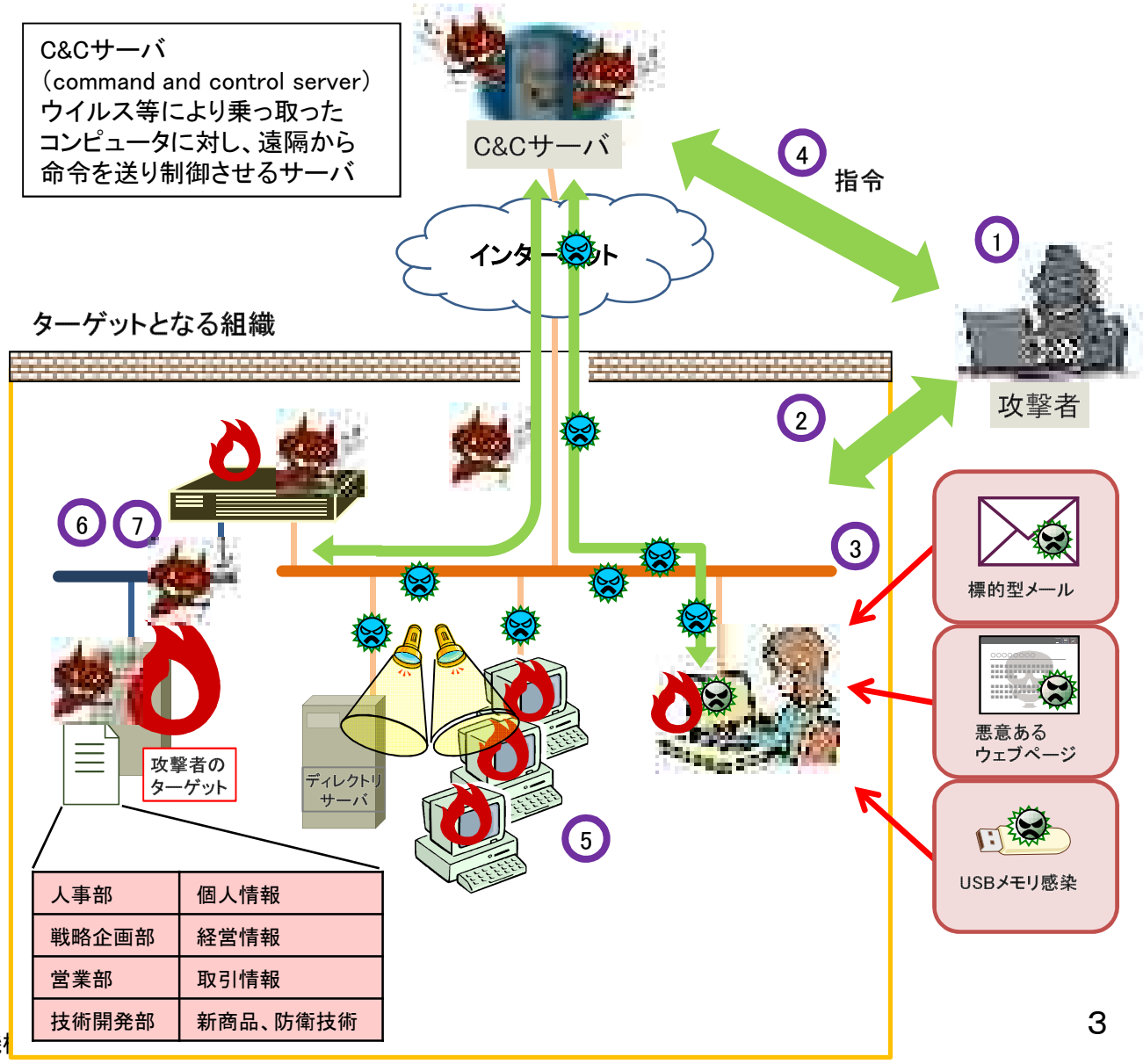
① ② [計画立案,攻撃準備]
ターゲットとなる組織を攻撃
する為の情報を収集

③ [初期潜入]
標的型メールやUSBメモリ、
ウェブサイト閲覧を通して
ウイルスに感染する。

④ [基盤構築]
侵入したPC内でバックドアを
作成し、外部のC&Cサーバと
通信を行い、新たなウイルス
をダウンロードする

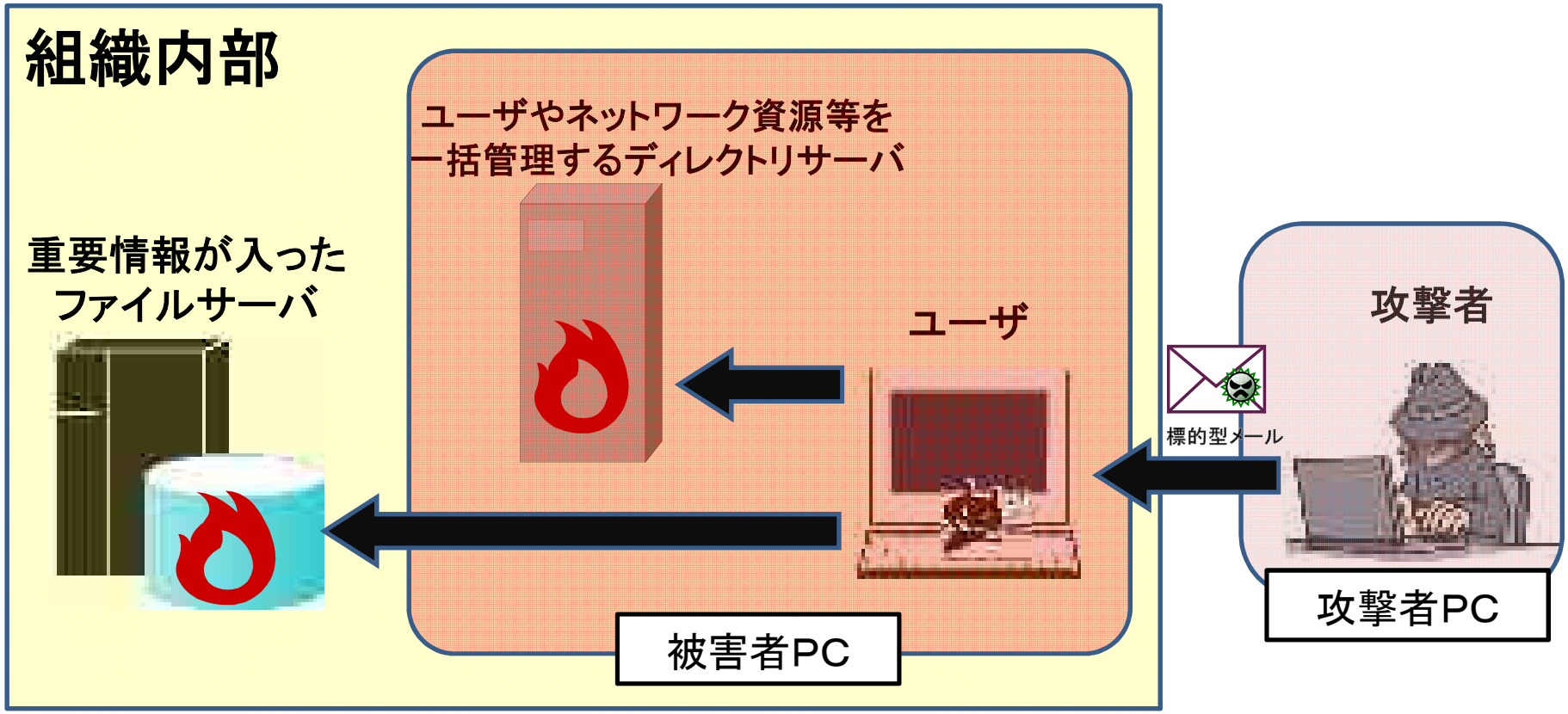
⑤ [内部侵入・調査]
情報の存在箇所特定や情報の
取得を行う。
攻撃者は取得情報を基に新た
な攻撃を仕掛ける

⑥ ⑦ [目的遂行,再侵入]
攻撃専用のウイルスをダウンロード
して、攻撃を遂行する



デモンストレーション構成

- 標的型攻撃などにより組織内のユーザにウイルスを感染させる
- 更なる攻撃により情報を収集する
- 重要な情報を窃取する



デモでは、攻撃者PC と被害者PC を用意し、ファイルサーバへのアカントを入手

2. 標的型攻撃に関するまとめ

① インターネットに接続した政府システムは、標的型攻撃を受ける

② 不審メールは年々巧妙化し、見抜くことは困難

③ 侵入を前提とし、その拡大や活動を阻止・検知する「多重防御」を備えたシステム対策が重要

④ 実際にインシデントが発生した場合に備え、迅速に適切な対処が行えるように準備

⑤ ルールに基づき、サイバー攻撃に係る情報は、可能な限り速やかに各府省庁窓口→NISCへ連絡