資料3

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4月26日（火）

内閣官房内閣サイバーセキュリティセンター

http://www.nisc.go.jp/

1. 増加する攻撃とその脅威

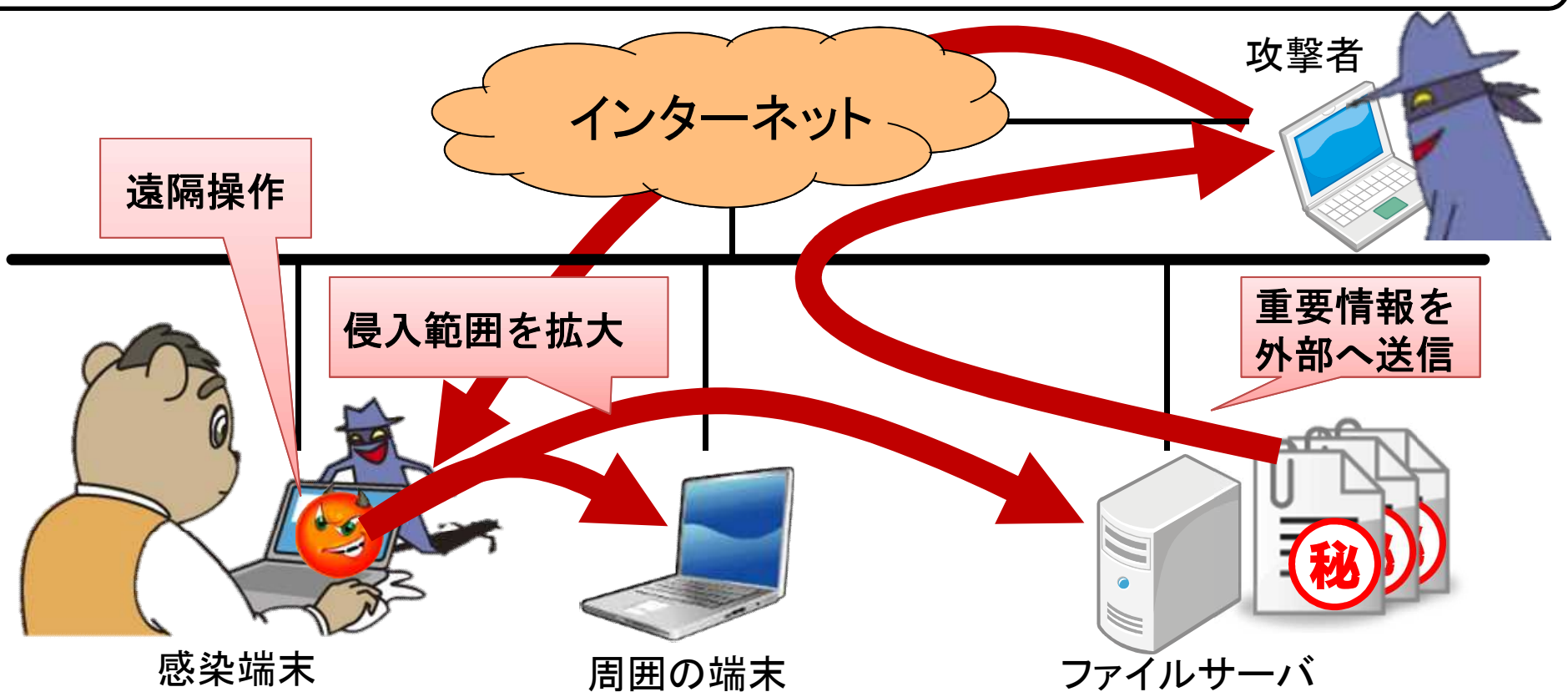
○　平成27年6月以降に公表された主な事例（政府機関・独法・特殊法人）

	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

2. 標的型攻撃の不正プログラムに感染すると

- ○ 感染すると、攻撃者から遠隔操作される状態に
- ○ 感染端末を拠点として、周囲の端末やサーバ等に対して侵入範囲を拡大
- ○ 拡大の結果、重要情報にたどり着いた場合は、外部へ送信される
- ○ 重要情報やシステムを破壊される可能性も



デモをご覧ください

３．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

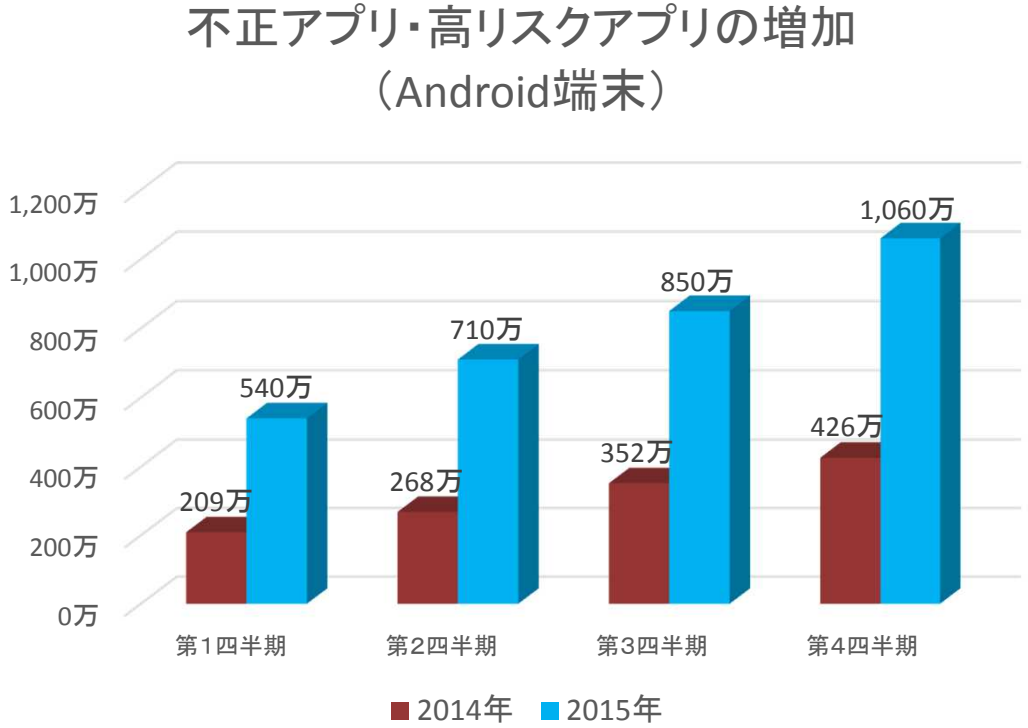
③侵入を前提とし、その拡大や活動を阻止・検知する「多重防御」を備えたシステム対策が重要

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

4. スマートフォン等の不正アプリの増加とその脅威

○ 不正アプリは、増加傾向
○ 不正アプリにより、スマートフォンの電話帳にあるメールアドレスを抜き取るなどの、情報窃取の被害に至る事例も



2014年データと比較すると、Android向け不正プログラムの累積数は2015年末までの期間で倍増。

（出典）トレンドマイクロ（株）「Trend Labs 2015年 年間セキュリティラウンドアップ」

■不正アプリによる被害の事例

2013.7.24(水）読売新聞
「3700万件情報抜き取る」

2013.7.24(水）朝日新聞
「不正アプリで3700万件流出」

ウイルス対策ソフトウェアや節電アプリ等を装った不正アプリをインターネット上で公開していた。
この不正アプリにはウイルス検知機能や節電機能等はなく、スマートフォンの電話帳のメールアドレスを抜き取って外部へ送信するものだった。

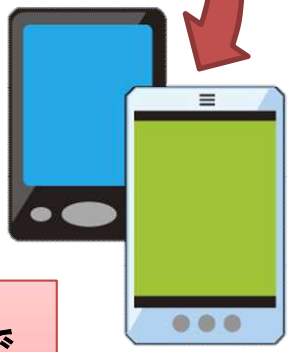
5. ご留意いただきたい事項（不正アプリの脅威）

○ 「不正アプリ」を導入してしまうと、スマートフォンを乗っ取られ、盗聴される・盗撮される・追跡されるなどの様々な被害に

公式マーケットに酷似したアプリ提供サイト

問題のないアプリであるかのような説明

インストールしてしまうと・・・



盗聴・盗撮・追跡などの被害に！

デモをご覧ください