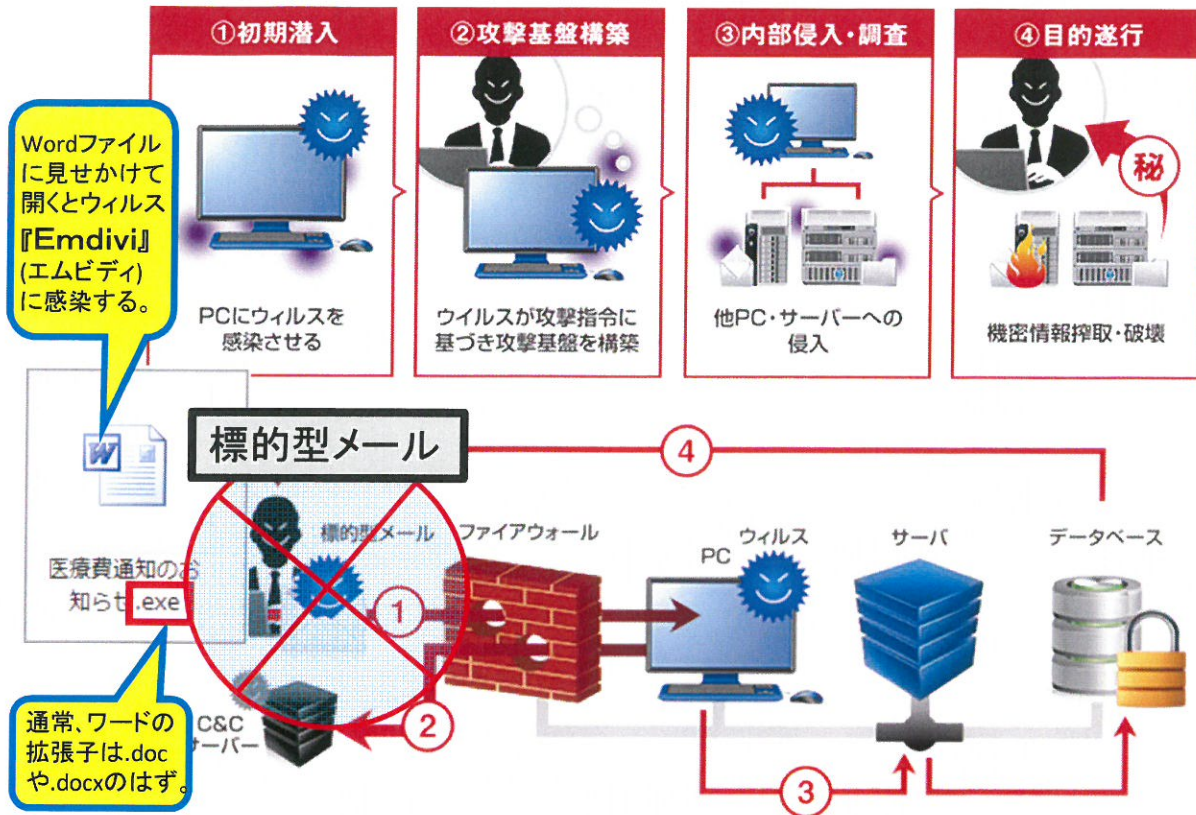


①年金機構から個人情報125万件を流出させた「標的型(メール)攻撃」の典型的な流れ

資料1



(出典) 東芝HP「標的型攻撃の典型的な流れ」https://www.toshiba.co.jp/cl/sol/security/attack/index_j.html
 (出典) トレンドマイクロ社HP「医療費通知に偽装した不審メールが法人利用者に遠隔操作ツールを拡散」
http://blog.trendmicro.co.jp/archives/10251?cm_re=articles_-_blog_-_10251&_ga=1.11417396.1630584872.1413850187

②実践的サイバー防御演習(略称:サイダー) (CYDER: Cyber Defense Exercise with Recurrence)

演習のイメージ

大規模仮想LAN環境 (NICT「StarBED」により実現)

石川県能美市

研究開発用の新世代超高速通信網 NICT「JGN-X」

サイバー攻撃への対処方法を体得

仮想ネットワークに対して疑似攻撃を実施 (実際のマルウェアを使用)

疑似攻撃者

都内(品川)

演習の特徴

- サイバー攻撃が発生した場合の被害を最小化するための一連の対処方法(攻撃を受けた端末の特定・隔離、ログの解析による侵入経路や被害範囲の特定、同種攻撃の防御策、上司への報告等)を体得
- 150台の高性能サーバーのクラウド環境による数千規模の仮想ネットワーク(国の行政機関や大企業を想定)上で演習を実施
- 我が国固有のサイバー攻撃事例を徹底分析し、最新の演習シナリオ(平成27年度は、年金機構への標的型攻撃を参考にしたシナリオ)を用意

注目①

平成27年度の実績

- 官公庁、重要インフラ事業者など約80組織、約200人が演習に参加
- 平成28年度は地方自治体等に対象を拡大し、500組織、1500人を目標に実施予定

注目②

平成28年度から、技術的知見を有するNICTを実施主体とすることにより、演習の質の向上や継続的・安定的な運用を実現するための法案を本国会に提出
(注:現在は総務省が民間企業に委託して実施)

(出典) 総務省「サイバーセキュリティに関する総務省の取組」(平成28年3月31日) <https://www.kantei.go.jp/jp/singi/keizaisaisei/jkkaigou/dai40/siryou10.pdf>
 (出典) NECHP「総務省主催の「実践的サイバー防御演習(CYDER)」を実施」http://jpn.nec.com/press/201510/20151026_02.html
 (出典) 日立HP「総務省主催の「実践的サイバー防御演習(CYDER)」を実施」<http://www.hitachi.co.jp/New/cnews/month/2015/10/1026b.html>