CyberCrime Control Project

平成27年第2号

広島県警察本部
サイバー犯罪対策課
082－228－0110

～ 標 的 型 の サ イ バ ー 攻 撃 に 注 意 ～

貴方の会社が標的に！？

■　被害の現状

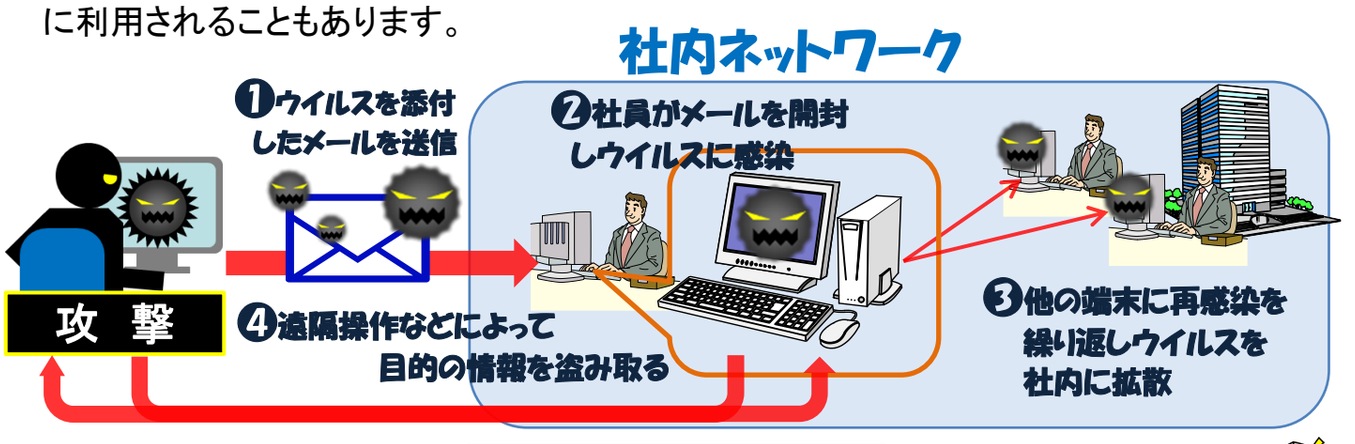
先般発生した，日本年金機構に対するサイバー攻撃に代表されるように，特定の機関・企業を対象としたサイバー攻撃は，日増しに増加しており，その手口も悪質・巧妙化しています。

一度サイバー攻撃を受け，企業の機密情報や顧客データ等の個人情報が流出すると，企業に対する信用の失墜，顧客への補償問題など，そのダメージは計り知れません。

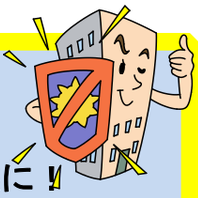
■　標的型攻撃の手口

最近は，企業の従業員等に対し，知人や取引先になりすまして，何回かメールのやり取りを行い，油断させたところでウイルスを添付したメールを送信するなど，手口が巧妙化しています。

添付ファイルを開き，端末がウイルス感染してしまうと，攻撃者と不正な通信を繰り返し，さらに別のウイルスを送りつけられたりして，新たな感染端末を増やされ，社内のネットワーク内に深く侵入されてしまい，機密情報や顧客データなどが盗み取られるといった被害に遭うのです。また，場合によっては，これらの感染端末が「踏み台」として，別のサイバー攻撃に利用されることもあります。



対　策



■　まずは…徹底した事前対策

- ○ ファイヤーウォールの設置，ウイルス対策ソフトを導入し常に最新の状態に！
- ○ ネットに接続された端末で機密情報を保管しない！
- ○ 外部への不審な通信等を監視し，ログの定期的チェックにより不審通信を遮断！
- ○ 流出した場合に備えて重要なデータは暗号化！

■　「絶対には防げない，もしウイルス感染してしまったら」との前提でルール化し，失敗時の対応を訓練！

- ○ 添付ファイルを開いてしまった場合などの対応要領をマニュアル化し，徹底を図る！
- ○ 抜き打ち的な訓練を定期的に実施し，対応を検証！