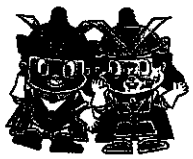
最近のサイバー攻撃情勢

平成27年9月25日(金)

大阪府警察本部 警備部 警備総務課
サイバー攻撃特別捜査隊



1

Agenda

- はじめに（サイバー攻撃とは？）
- 攻撃者とは・・守るものとは・・
- 医療機関へのサイバー攻撃の現状
- 最近のサイバー攻撃逮捕事例
- 標的型メール攻撃
- ウェブサイトに対する攻撃
- 内部犯行による情報漏洩

2

はじめに

サイバー攻撃とは？

サイバーテロ

重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させるサイバー攻撃

サイバーインテリジェンス

情報通信技術を用いて政府機関や先端技術を有する企業から機密情報を窃取するサイバー攻撃（最も安全で安価なスパイ）

コンピュータシステムやインターネットなどを利用して、標的のコンピュータに不正に侵入してデータの窃取や破壊、改ざんなどを行ったり、標的のシステムを機能不全に陥らせる攻撃

国の治安、安全保障、危機管理に多大な影響を及ぼす！

攻撃者とは・・・

国内から？　　海外から？

個人で？　　組織で？

泥棒？　　軍隊？

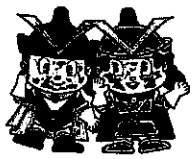
オタク？　　ストーカー？

目的は何？？？

いたずら？　　嫌がらせ？

自己顕示？　　情報窃取？

お金？　　破壊？



守るべきものとは・・

貴院には、何があるの？

何は絶対に守らなければならないの？

欲しい情報は攻撃者にしかわからない・・

サイバー攻撃から守るべきものとは

○ 人命
遠隔操作による手術、ペースメーカー

○ 保険精算システム
ずっと動かし続けている　病院運営の中枢

○ 膨大な量の個人情報
電子カルテ　氏名・住所以上に大事な
医療記録・健康保険番号

○ 職員の個人情報

医療機関へのサイバー攻撃情勢

個人医療記録はクレジットカードの個人情報よりも簡単に取得できてより価値のあるものである

Webサイト　security affairs
URL
securityaffairs.co/wordpress/35361/security/health-care-data-value.html

Health records are the new goldmine for hackers

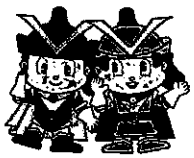
ペースメーカーをサイバーセキュリティ専科の学生がハッキング

Webサイト　security affairs

URL

securityaffairs.co/wordpress/39974/hacking/healthcare-breaching-medical-device.html

Healthcare – Breaching a medical training mannequin raises new cyber security concerns



あらゆる手段で得た個人情報をデータベース化

そのデータベースから国の業務に係る者
機密業務に係る者等を選別

更にSNS等で知り得た情報を基に行動確認

そして、その者を狙った
本物の標的型メールを送信

スパイが得る情報の9割はオープンソースから

最近の逮捕事例

１７歳ハッカー『ZeroChiaki』逮捕　日本初「身代金ウィルス」作成

- 近所の他人宅の無線LANにただ乗りし発信元の特定を困難にするソフトを使用
- 事前にレンタルサーバー会社を装い出版社員にメールを送りサーバー会社が運営するサイトに酷似したページに誘導しIDとPASSを入手
- 盗んだIDとPASSを使用し出版社のサーバーに不正アクセスしPASSを変更
- サイバー攻撃した状況をTwitter上でアピールするハッカーとして知られていた。

逮捕する際は・・

DDoS攻撃、ベトナム人逮捕
会社HPに大量アクセス　電子計算機損壊等業務妨害

- 自宅でレンタルサーバーから被害会社が使用しているサーバーに大量のアクセス信号を送信し通常の３０～３００倍以上の負荷をかけた。
- 動機は被害会社とのトラブルで「腹を立て、いたずら半分でやった」
- 同社は、サイトに接続しにくい状態になったことから数週間HPを閉鎖した

サイバー攻撃による情報漏洩は、気づかない！

ほとんどの事象で、

外部からの指摘で認知している

気づいているのは「氷山の一角」！！！
若しくは報道されていないか・・・

標的型メール攻撃

日本年金機構様を例にします

○ 本来、生体認証が必要な程、徹底して守られていた年金加入者情報が、
仕事がしにくい
との理由でファイル共有サーバが職員により勝手に作られた。(PW、暗号化なし)

○ 一太郎のぜい弱性を用いた標的型メールを受信。
流出の直接の原因となったメールは不明であるが、「医療費通知」と題したメールも3通確認。 他は、「厚生年金徴収関係研究資料」「給付研究委員会オープンセミナーのご案内」等。
攻撃者はその職種に沿ったメールを送信してくる

○ その結果、職員がメールを開いてファイル共有サーバから情報が漏洩

この事案は、情報漏えいの原因が、
たまたま標的型メールであった ことです。

対策として、

どんな機器・システムを取り入れても最後に
メールを開くのは

人

システム担当者に負担が掛かりますが、少しでも不審点が有れば連絡し易い環境を作ること

「メールを開かないで」ではなく
「開いた時にどうすべきか」が大事

万能薬は存在しない！

ウェブサイトに対する攻撃

ウェブサイトの改ざん

ウェブサイトからの情報漏洩
SQLインジェクション攻撃の多発

ウェブサイトを運営するには、
守らなければならない要素が非常に多い

管理者のパスワード
ウェブアプリケーションの脆弱性
CMSと、そのプラグインの脆弱性
データベース
・・・・

ハッキングから守るために、
それらをメンテナンスをし続けることが必要

17

サイバー攻撃対策として

攻撃の踏み台となるシステムは、
インターネット上からなくしたい
絶対安全とはいえないが、
オンライン、オフラインの切り分け

DNSを踏み台とした攻撃が、
多く観測されている
“オープンリゾルバ”の撲滅！

18

内部犯行による情報漏洩

犯罪は「割りにあわない」

「捕まれへん・ばれへん」を
「捕まるで！！！！！！」と教育してください

ベネッセの件を例にとると
男性が持ち出した個人情報　約2,300万件
受け取った報酬　４００万円
不正競争防止法違反（営業秘密の複製、開示）
5年以下の懲役若しくは500万円以下の罰金

失職・実名報道・顔判明・家族が1番の被害者・・・

貴院のとるべき対応

「情報セキュリティ」に関して、
担当する人を明確にすること

押しつけ合い、譲り合いでは話にならない

そして、意思決定機関に
担当する役員がいること

攻撃者に対抗するためには、

守る側が協力することが

不可欠です！