情報処理工学 第１５回

藤田 一寿
公立小松大学保健医療学部臨床工学科

殆どの図はIPAセキュリティ10大脅威より

セキュリティ問題

まず事件は起こるものだと考える

セキュリティー１０大脅威（個人）

1.クレジットカード情報の不正利用
2.フィッシング詐欺による個人情報等の詐取
3.不正アプリによるスマートフォン利用者への被害
4.メール等を使った脅迫・詐欺の手口による金銭要求
5.ネット上の誹謗・中傷・デマ
6.偽警告によるインターネット詐欺
7.インターネットバンキングの不正利用
8.インターネットサービスへの不正ログイン
9.ランサムウェアによる被害
10.IoT機器の不適切な管理

(IPA情報セキュリティ10大脅威 2019より)

セキュリティー１０大脅威（企業）

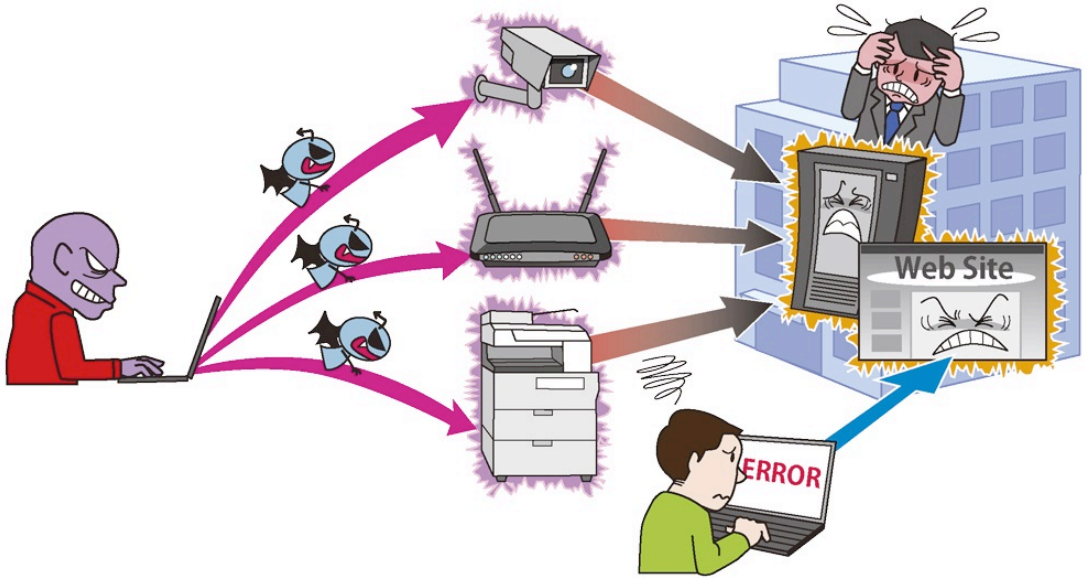
1.標的型攻撃による情報流出
2.ビジネスメール詐欺による被害
3.ランサムウェアによる被害
4.サプライチェーンの弱点を悪用した攻撃の高まり
5.内部不正による情報漏えいとそれに伴う業務停止
6.サービス妨害攻撃によるサービスの停止
7.インターネットサービスからの個人情報の窃取
8.IoT機器の脆弱性の顕在化
9.脆弱性対策情報の公開に伴う悪用増加
10.不注意による情報漏えい

(IPA情報セキュリティ10大脅威 2019より)

サービス妨害攻撃によるサービスの停止

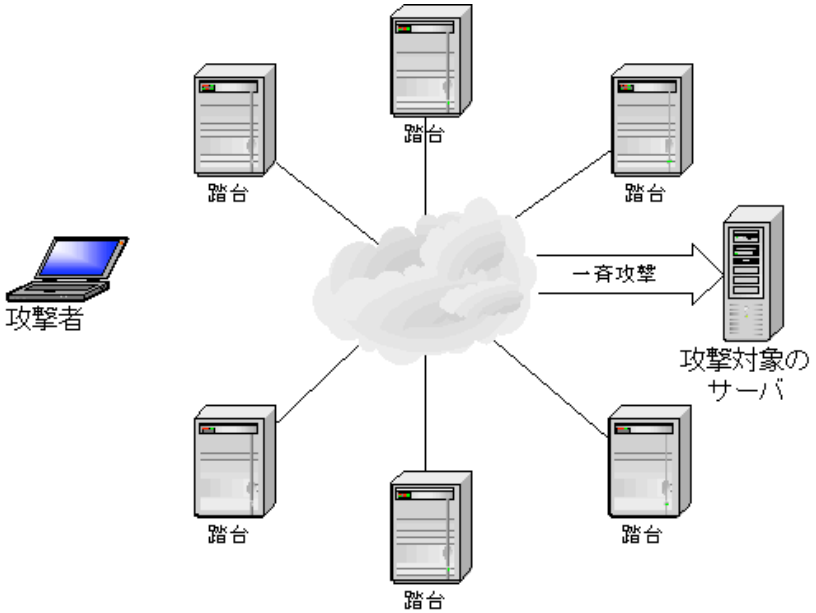
DoS(Denial of Service)攻撃

- DoS攻撃とは，サーバーなどのネットワーク機器に対するアクセスを大量に行い負荷をかけ、サービスを停止させる。
- 攻撃を効率良く行うために、大量のコンピュータを用いる事が多い（DDoS攻撃）



DDoS (Distributed DoS) 攻撃

- DDoS攻撃とは大量のマシンから1つのサービスに一斉にDoS攻撃をすること．攻撃にはボットネットと呼ばれる乗っ取られたPCで構成されるネットワークが使われる．



時刻や特定のパケットで一斉に攻撃を行う

https://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/dos.html

事例

- 2016年ヨドバシカメラの通販サイトがDDoS攻撃を受け，アクセスできない状況になった.
- 2016年Miraiというマルウェアにより DNSサービスサービスプロバイダの Dynが攻撃をうけ，その影響でTwitter，Spotify，Redditなどのサービスが利用できなくなった.
  - IoT機器に感染
  - 「admin:1234」など典型的なユーザ名とパスワードを用いているIoT機器
  - Miraiに感染したIoT機器は感染可能なIoT機器を探し，見つけたら攻撃者に報告.
  - 感染したIoT機器はボットネットを構成し，攻撃に用いられる.

DDoS攻撃に無関係な人はいない

- DDoS攻撃を効率良く行うために大量なPCを世界中から集める.
- PCにセキュリティホールがあると、第三者に攻撃の道具として自分のPCが使われる.
- トロイの木馬などのマルウェアによりPCが乗っ取られ，知らない間に加害者なることがある.
- DDoS攻撃は攻撃対象のサービスだけではなく，攻撃に参加しているPCがあれば，そのPCがある家や会社のネットワークにも負荷がかかる.

DoS攻撃・DDoS攻撃の対策

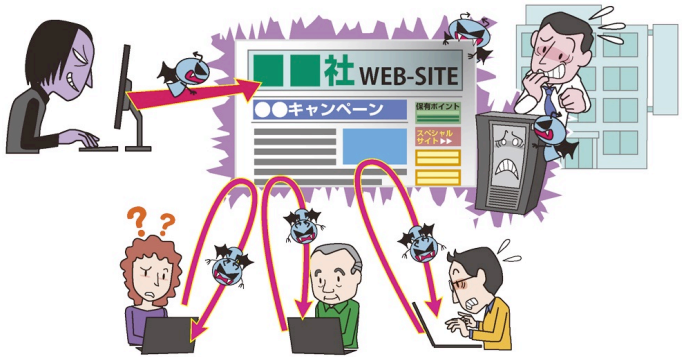
- 個人としての対策
  - ソフトウェアを最新のものにしておく.
  - セキュリティソフトを導入する.
  - 怪しげなファイルを不用意に開かない.
  - 怪しげなサイトを開かない.

- システム管理者としての対策
  - 特定のIPアドレスやドメイン名の接続を遮断もしくは許可する.
  - 単位時間あたりのアクセス回数に制限を設ける.
  - ネットワークトラッフィクの監視システムを導入し，攻撃と思われる接続を遮断する.

ウェブサイトの改ざん

ウェブサイトの改ざん

- 企業や自治体のサイトが、他の誰かに改ざんされる
- 改ざんはどのウェブサイトでも起こりうる
- 有名かどうかは関係ない
  - マルウェア散布
    - 価格コム(2005年)
  - 政治的なメッセージの配信
    - 西宮観光協会(2015年)
    - ルスツリゾート加森観光(2015年)
    - カメラバック販売代理店銀一(2015年)
  - 他のページに誘導
    - 五島市(2015年)



何が目的で改ざんされるか

- 違法なものを販売するページに誘導するため
- 政治的なメッセージを発信するため
- 個人情報を抜き出すため（フィッシング詐欺も含む）
- 機密情報を盗むため
- マルウェアを拡散させるため

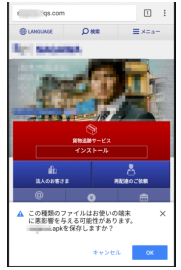
Web site改ざんの対策

- ソフトウェアのアップデート
- 2段階認証の導入 (CMSの)
- ファイアーウォールなどによるIPアドレスの制限
- 改ざん検知システムの導入
- 定期的なバックアップ

フィッシング詐欺

フィッシング詐欺

- クレジットカード会社や銀行からのお知らせを装って，クレジットカード番号や暗証番号などを聞き出す.
- 銀行やgoogleなどの偽のウェブサイトに誘導し，クレジットカード番号，暗証番号，パスワードなどを偽のウェブサイトに入力させ盗む.
  - 偽のウェブサイトは本物と瓜二つのため見分けるのは困難.
  - URLも本物と似ているもの（oが0になっているなど）を使っておりURLでも判別は難しい.
  - DNSサーバを乗っ取れば本物のURLを使った偽サイトを作ることも可能.
- 偽のショートメッセージを送り，不正サイトに誘導し，スマホの不正アプリをインストールさせそのアプリから個人情報を盗む.
(https://is702.jp/news/3352/)

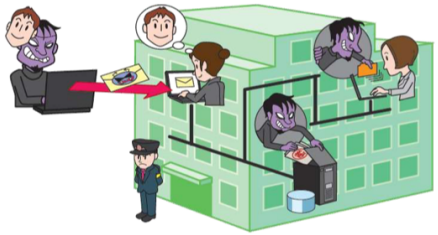


標的型攻撃

標的型攻撃

- ネットワーク経由で攻撃対象の企業や官公庁などの重要情報を不正に取得する.
- 不特定多数を狙ったものではなく，特定の企業などを狙っている.

- 標的の企業の社員にマルウェアを添付したメールを送る.
- 関係者や取引先を装い，業務関連のメールだと思わせることで標的の社員を信用させる．そして，添付されたマルウェアを開かせる.
- マルウェアを通し標的の企業のPCを遠隔操作し，機密データを盗む.



事例

- 2014年日本航空から顧客管理システムの不正アクセスが発生した.
  - メールに添付されたマルウェアに感染.
  - 2017年には日本航空は3.8億円の詐欺にもあった（メールにはマルウェアではなく偽の銀行口座がついていた）.
- 2015年石油連盟が標的型攻撃により内部情報が漏洩した.
  - 外部組織から指摘があったため発覚
- 2015年日本年金機構をターゲットにした標的型攻撃によって個人情報が125万件流出した.

標的型攻撃の対策

- ウイルス対策ソフト，セキュリティソフトの導入.
- ソフトウェアの更新する.
- 安易にメールの添付ファイルを開かない.

- 異常な（不審な）通信を見つけ，通信を遮断する
- データは暗号化しておく

ソーシャルエンジニアリング（ソーシャルハッキング）

- 人間の心理的な隙や行動のミスにつけ込み，機密情報の入手やネットワークへの侵入を行うこと.

- なりすまし
  - 電話やメールで知り合い，取引先，官公庁などになりすまし，重要な情報を盗み出すなどする.

- ショルダハッキング
  - パスワードやクレジットカードなど重要な情報を覗き見る.

- トラッシング
  - 攻撃する上で必要となる様々な情報をゴミ箱から拾う.

情報漏えい

故意ではない情報漏洩

- 忘れ物
  - ノートパソコン，USBフラッシュメモリ，書類.
- ファイル交換ソフト
  - ウイルスに感染することで機密ファイルが共有され全世界にばら撒かれる.
- メールの送信先の間違い
- インターネットサービスの設定ミス
  - パスワードを掛けるべきところをかけていなかった.
- 公開してはいけないファイルを公開する.
  - 2015年FRBが誤って内部資料を公開
    (https://www.nikkei.com/article/DGXLASGM25H21_V20C15A7NNE000/)
  - 2018年Amazonが誤ってメールアドレスを公開
  - 2018年経産省が入札情報を誤って公開

故意ではない情報漏洩

- パスワードが簡単すぎ不正アクセスされ情報漏洩
- ハードディスクの捨てる際，OSのゴミ箱フォルダに機密ファイルを移し削除する.
  - OS上では消えたように見えても，データはハードディスク上に残ったまま.データ復旧ソフトを用いると，消したデータをもとに戻せることがある.
  - 確実に削除するには，ディスクを破壊するかディスクを何度か乱数などで上書きする必要がある.

  - 事例
    - 2019年HDDの処理を委託されたブロードリンクの社員が，そのHDD持ち出しをオークションサイトで転売した．そのHDDは神奈川県のPCから取り出されたもので，落札者がデータ復旧ソフトを用いると神奈川県の公文書がそのHDDから見つかった.

意図的な情報漏洩

- 従業員が故意に内部情報を外部に漏洩させる
  - 処遇の不満などによるストレスの発散
  - 借金返済のため情報を売る

- 事例
  - 2014年ベネッセの顧客情報が漏洩していることが発覚.
    - システム開発・運用を行っていた子会社のシンフォームに再委託先企業の社員が顧客情報を持ち出し，250万で売却.

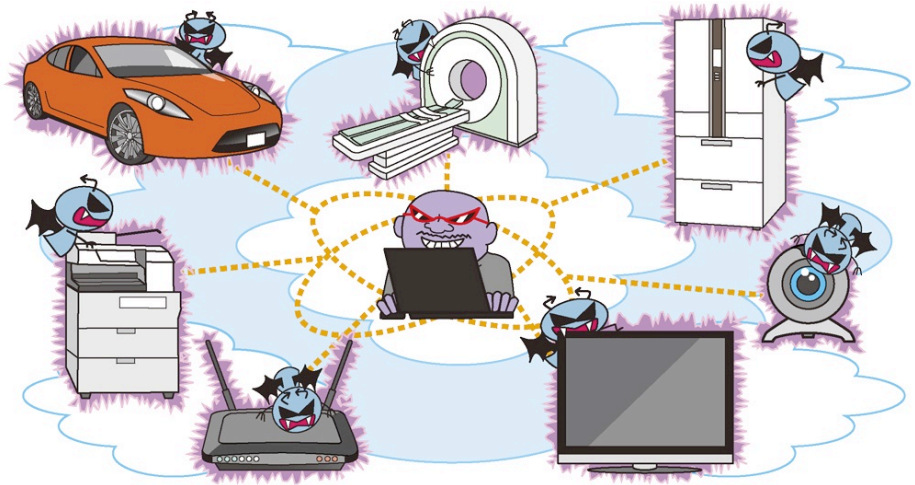
IoT機器のセキュリティー

IoT機器

- IoT (Internet of Things)とはモノのインターネットとも呼ばれ，あらゆるモノがインターネットにつながる社会やその様子を表す．
- 現在でも，パソコンやスマートフォンだけではなく，テレビ，スマートスピーカー，車，監視カメラ，電子レンジなどもインターネットに繋がっている場合がある．
- IoT機器とは，インターネットに繋がるあらゆるモノのことで，特にパソコンやスマートフォンのような以前からインターネットにつながっていたIT機器以外を指すことが多い．
- IoT機器は，見た目がパソコンやスマートフォン (IT機器)に見えないため，一般ユーザだけではなくメーカーもセキュリティに対する意識が低くなる．
- IoT機器はIT機器と同等の機能を有するため（LinuxなどのOSが入っている），IT機器と同等のセキュリティ対策をする必要がある．

IoTのセキュリティ問題

- IoT機器にマルウェアを感染させ，マルウェアをばらまく.
- IoT機器マルウェアを感染させ，DDoS攻撃を行う.
- IoT機器から機密情報を窃取する.
- IoT機器を遠隔制御する.



なぜ問題が起こるのか

- IoT機器に対するセキュリティに対する意識の低さ
- 例
  - 管理者権限のIDとパスワードがadmin：1234など典型的なものに設定されている.
  - しかも，その設定をユーザが変更できないように作られている機器がある.

監視カメラの事例

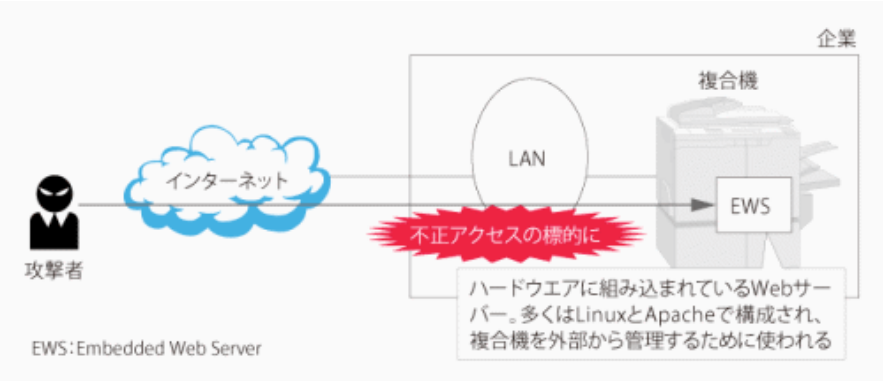
- 監視カメラはインターネットから動画の視聴，カメラの向きの制御などが行えるものがある．

- 監視カメラの画像の流出
  - 監視カメラの中には，画像がインターネットに公開される設定になっているものがある．世界中の監視カメラ画像を見られるサイトも存在する．
- 監視カメラの乗っ取り
  - 2018年上尾市の河川監視カメラに不正アクセスがあり，「I'm hacked. bye2」と監視カメラの画像に表示された．さらに，パスワードが変更され，制御不可能になった (https://www.sankei.com/region/news/180428/rgn1804280045-n1.htm, https://scan.netsecurity.ne.jp/article/2018/05/01/40886.html)

プリンタと複合機の事例

- プリンタや複合機はインターネットから印刷，スキャンされた資料の閲覧，設定の変更などが行えるものがある.

- 2013年複数の大学等で，複合機で読み取った情報がインターネット上で閲覧できる状態となっていたことが判明した.



日経新聞

テスラモデルSの遠隔操作

- テスラ車の通信機能に存在した脆弱な仕様をついて車載情報端末用の車内ネットワークに侵入
- 車載情報端末のWebブラウザーに存在した脆弱性を攻撃して、任意のコードを実行可能に
- 車載情報端末のLinuxカーネルに存在した脆弱性を攻撃して、ルート権限を取得
- 情報端末用の車内ネットワークと、制御系ネットワーク（CAN）とをつなぐ「コントローラー」を攻撃して、コントローラーのファームウエアを書き換え
- コントローラーから電子制御ユニット（ECU）に偽のコマンドを送り自動車を遠隔操作

http://business.nikkeibp.co.jp/atcl/report/15/061700004/072800212/

IoT機器のセキュリティ対策

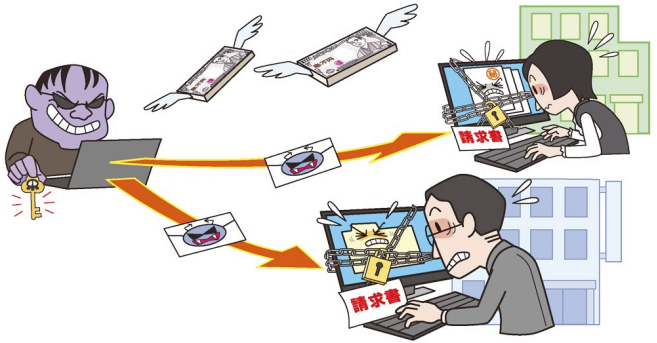
- IoT機器は一見すると機能が限定され安全に見えるが，中身はパソコンと同じであると考えて，パソコンやネットワーク機器と同様のセキュリティ対策を行う.

- ソフトウェアを最新のものにする.
- 初期設定を使わず，よりセキュリティの高い設定にする.
  - ID，パスワードだけではなく，ネットワークの設定も.

ランサムウェア

ランサムウェアとは

- マルウェアの一種
- コンピュータの利用者のシステムへの利用を制限する.
- 制限を解除するために身代金 (ransom)を支払うよう要求する.
- ウェブサイトの閲覧，メールの添付ファイル，ネットワークの接続により感染する.
- ランサムウェアによる利用制限の例
  - コンピュータを操作不能にする.
  - ファイルの暗号化によりファイルを読み取り不可能にする.



事例

- 2017年本田技研工業がランサムウェアに感染し，工場が1日操業停止となった.
- 2016年サンフランシスコ市営鉄道のシステムがランサムウェアに感染し，コンピュータシステムが停止した．システムが停止している間，運賃を無料にし対応した.
- 2016年Android向けのランサムウェアがスマートテレ部をロックする事例が確認される.

(トレンドマイクロ)

ランサムウェア対策

- ソフトウェアを最新の状態にする
- ウイルス対策ソフトの導入する
- 不審なメールや不審なウェブサイトを開かない
- データのバックアップを定期的に取っておく
  - ランサムウェアによりデータが読み取れなくなった場合に有効である.

全般的な対策

- すべてのソフトを常に最新の状態にしておく.
- ウイルス対策ソフトの導入する.
  - しかし，全てのウイルスを検知できるわけではない.
- 簡単なパスワードにしない.
- セキュリティの高い設定にする.
- 機密情報を持ち出さない.
- メールに添付されているファイルを安易に開かない.
- ITセキュリティに関わる事案が起こった後のことを考えておく.

国家試験への対策

- セキュリティに関する問題が近年出題されている
- 年によって出題される問題が異なるため，予測することは難し.
- セキュリティ10大ニュースはチェックしておくと良い.

- 前半の計算は国家試験を受験する３年後に内容が変わることは無いが，後半のコンピュータの知識に関しては変わる可能性があることに注意すること.

期末試験

- 国家試験，ME2種の過去問から出題
- 知識問題は選択式，計算問題は記述式
- 持ち込みなし
- 評価は期末試験８割，提出レポート２割

- 不合格となった学生がいた場合は，追試の連絡を掲示板（物理的 and/or 電子的）にて行う.
- 追試は，期末試験終了後なるべく早く行う.

- 定期試験ができると国家試験もできるようになるので頑張ろう.