情報の倫理

2017/10/26

Kazuma Sekiguchi
class@cieds.jp

ランサムウェア

- イギリス・スペインなど全世界で大流行しているランサムウェア
- WannaCry
- 身代金ウィルス
  - PC内のファイルをすべて暗号化してしまうため、事実上すべてのファイルを利用不可

WannaCry

- Windowsに存在する脆弱性を突いてウィルス感染する
  - セキュリティパッチを当てることで、感染を防ぐことが可能（3月に公開済み）
  - ファイヤーウォールがあれば、問題が無いはずだが、外部で感染したマシンがファイヤーウォール内に持ち込まれて感染した可能性
- 世界的に感染したため、かなりの被害が発生
  - ルノー自動車工場で感染し、工場の操業不能
  - FedExのマシンが感染
  - ドイツの駅など
- イギリスの病院が感染し、急患が受け付けられない、手術不能になるなど大規模な生命に関わる危機まで発生

日本だと

- 『ランサムウェア「WannaCry／Wcry」による国内への攻撃を 16,436件確認』
  http://blog.trendmicro.co.jp/archives/14906,2017/5/16日参照
- 警察庁などが重要施設に対して確認したところいくつかの施設で感染が確認されている
  - 感染したマシンから更に感染しようとするため、万が一感染したらネットワークからすべて切断することが重要
  - 感染した場合、ファイルの復活は不可能

電子デバイスからの情報流出

- ウィルスなどの電子的手段
- 実際に操作して取得する
- のぞき見などを行う
  - 要するにさまざまな方法で情報を取得することが可能

- ロックなどをしておいてもPCなどは情報取得が可能
  - スマートフォンでもロックを解除できる方法は意外と多い
  - 暗号化しておくことで初めて情報を守ることが可能
- 情報が流出したら回収することは不可能

情報セキュリティ

- 情報セキュリティとは、企業の情報システムを取り巻くさまざまな脅威から、情報資産を機密性・完全性・可用性（三大要件）の確保を行いつつ、正常に維持すること

ISO/IEC 27002による定義

- 機密性の確保
  - 第三者によってアクセスされない
- 完全性の確保
  - 第三者によってデータが改ざんされない
- 可用性の確保
  - ハードウェアが壊れない、いつでも使える

一般的な担保

- 機密性の確保
  - パスワード、電子証明書による認証、ファイヤーウォールの設置、IPアドレスによる接続拒否設定、データセンターなど侵入されない設備へのサーバーの設置
- 完全性の確保
  - IDS（侵入検知システム）の導入、ファイル改ざん検出、バックアップシステム
- 可用性の確保
  - 電源の多重化、ハードウェアの多重化、データーセンターなどの設備が揃った場所への設置、サーバーの分散配置

データーセンター

- サーバーなどを集約して設置し、運用するための設備
  - いろんな会社がサーバーを設置して利用する共用型と1社が設備を丸々利用する占有型がある
  - 通常ビルみたいな建物内の一部スペースに設置するケースと一棟丸々データーセンターとして使用する場合がある
- 共有の場合、内部は立ち入りが厳しく制限される
  - データーセンター自体の場所が明かされないケースも
  - 他社のデータを盗むことが簡単にできてしまうため侵入が厳しく制限

Facebook社のデータセンター
http://www.itmedia.co.jp/news/articles/1306/13/news063.html
より2016年5月17日取得

さくらインターネットデーターセンター外観
http://www.atmarkit.co.jp/ait/articles/1310/29/news020.html
より2016年5月17日取得

情報セキュリティの定義上は

- 定義上は企業の情報システム
  - 実際には、企業の情報と個人の持つ情報は量の違いだけ
- 個人が狙われるケースが非常に多い
  - 個人の場合、情報の管理が杜撰
  - 新しい技術が出てくるにも関わらず、それに対する情報保護の情報提供が非常に少ない
  - 現実的にはリスクの多い技術が多いが知らずに使う

企業間ネットワークの弱さ

- 1つの情報を企業間で共有または相互に送受信するシステムは多い
  - 銀行振り込み、Suicaなどの電子マネー、Tポイントなど
- 企業によっても管理体制が異なる
  - 脆弱なところを突かれたら、一斉にデータが流出する
- バングラデシュ中銀事件
  - 銀行間の国際決済システム「SWIFT」の脆弱性を突いて現金8000万ドルを取得
  - バングラデシュ中銀にマルウェアが仕込まれていた
    - 正当な発注として処理された模様

銀行間の国際決済システム「SWIFT」

- 世界で最もセキュアなネットワークであり、“支払いシステムのロールスロイス”とも言うべき存在
- バングラデシュ中銀のセキュリティ体制に問題
- SWIFTの管理、指導が甘かったという指摘
  - SWIFT自体の管理はベルギーにある協同組合形式の国際銀行間通信協会が運営・管理

- 日本の銀行間の決済・振り込みなどは全銀手順
  - 一般社団法人全国銀行資金決済ネットワークが運営

電子カルテ

- 病院などで医師が記入する電子カルテ
  - 基本的に閉じたネットワークで運用されているため外部流出の危険は少ない
  - 緊急時に他の病院でもカルテを閲覧できることで、病人を救う可能性を上げることが可能
    - カルテにより、持病、投薬記録、検査結果などを確認可能
- 他の病院で閲覧可能＝ネットワークで接続する
  - ネットワークで接続すると攻撃される可能性が飛躍的に高まる
  - 機微情報を扱うため、不正な手段で情報が入手されたら被害が甚大
  - 全ての病院で厳重な管理を行えるとは限らない

クラウドカルテ

- 地域ごとの病院連携として既にカルテの共有が始まっている
  - 北海道旭川市、宮城県気仙沼市・石巻市、長野県長野市・松本市、静岡県中部、岡山市・倉敷市、島根県、大分県別府市、長崎県など
- 医療の重複受診、投薬管理などによる医療費軽減
- 災害時の医療支援として有効

個人情報

- 個人情報の流出は常に付きまとう
- 個人情報
  - 氏名、年齢、性別、学籍番号、電話番号、メールアドレス、履歴
    姉妹の有無、出身地などなど
  - 本人を特定できる情報は全て個人情報
  - 複合で特定できるものも個人情報
- 機微情報
  - 病歴、金融資産、宗教などの差別を冗長する可能性のある情報

個人情報の保護

- 個人情報を収集するときは、利用目的を明らかにし、同意を得る必要がある
  - 個人情報保護法
- 収集した個人情報は、外部に漏洩することがないように適切に保護する義務

- 特に機微情報に触れる可能性のある職業では守秘義務がある
  - 個人情報保護法ではない
  - 医師、弁護士など

でもやっぱり流出する

- ベネッセ個人情報流出
  - 2014年　2070万件の流出
  - 結果として、ベネッセの営業ツールがDMから変更する事態に
  - 内部の勤務者がDBからデータを引き抜いて名簿業者に転売
  - 名簿を購入したJustsystemなども倫理を問われる事態に
- 日本年金機構情報流出
  - 2015年　101万件
  - 個人情報の他、年金額などの情報も流出
  - 詐欺などへの悪用懸念
  - 端末のマルウェア感染による流出

でもやっぱり流出する

- 早稲田大学個人情報流出
  - 2015年　3300人分の流出
  - 事務用パソコンが不正なプログラムに感染
  - 保存されていた個人情報が流出したほか、学内用のウェブサイトの改ざん
- Yahoo!ID流出
  - 2013年　2200万件のIDが流出
  - 個人情報自体には該当しないが、他との複合で個人を特定できる可能性がある
  - YahooAuctionなどで利用できるため、危険

実際多い

2017/10/23 入試情報サイトで個人情報が閲覧可能に - 京都精華大
2017/10/23 図書館のウェブサーバから個人情報流出の可能性 - 島根大
2017/10/23 交付前のマイナンバーカードが所在不明、保管中に紛失 - 横浜市
2017/10/20 紙袋に入れた受託イベント参加者の個人情報を紛失 - FVC
2017/10/20 訪問サービス中に車上あらし、個人情報が盗難 - 長岡の高齢者介護施設
2017/10/20 キャンペーン応募用紙が箱ごと所在不明 - 静岡のスーパー
2017/10/19 メール誤送信で助成金交付団体のメアド流出 - 環境再生保全機構
2017/10/18 市有地売却先に用地取得関連の情報含む書類を置き忘れ - 大阪市
2017/10/17 県立高校で解答用紙が盗難、教諭が買い物途中に - 埼玉県
2017/10/17 誤送信で講座受講者のメールアドレス流出 - 首都大学東京
2017/10/16 採用内定者の個人情報含む資料が所在不明 - 国立病院機構
2017/10/16 委託先で顧客情報含む領収書を紛失 - 京葉ガス
2017/10/16 メール誤送信でボランティア協力者のメアド流出 - ハンガー・フリー・ワールド
2017/10/13 店舗で金庫持ち去り、現金と顧客情報が被害に - ステーキのどん
2017/10/12 振込詐欺被害者の個人情報を誤ってネット公開 - 大阪府
2017/10/12 5年前に終了したプリントゴッコ通販サイトに不正アクセス - 顧客情報が流出
2017/10/11 診療予約サービスに不正アクセス - 患者情報約60万件が流出か

http://www.security-next.com/category/cat191/cat25より10月25日取得

マイナンバー

- 共通番号制度の導入
  - 基礎年金番号、健康保険番号、パスポートの番号などがバラバラに管理されている（先進国では異例）
  - 個人を特定する番号を共通化して、効率的な行政サービスを目指す
  - 2015年に国民への番号割り当てを行う（紙のカードで通知）
  - 2016年から利用開始
- 希望者はICカードへ切り替え可能
  - 行政機関などで利用可能となる
- 将来的にさまざまな機関が紐付けられる可能性
  - 保険証なども統合されるかも？

住民基本台帳

- これも共通番号制度の1つ
- 国民一人一人に番号が付与されている点は変わらない
  - 住基は地方自治体が利用する面が多かった
  - マイナンバーは個人が番号を保持し、提示することで利用できる
- カードは地方自治体発行のため、バラバラ

- プライバシーの問題、セキュリティ上の問題が取りざたされる
  - いくつかの地方自治体が接続しない、という決定をする
- マイナンバーの発行に伴い機能停止

個人情報の保護

- 個人情報を企業に提供する場合は、利用目的を確認する
  - 実際のところ、企業が流出させてしまった場合、手の打ちようがない
  - 無駄な情報は安易に提供しないのが自衛策

- ネットで個人情報に該当するような事柄は書かない

個人情報をネットから

- 過去にストーカーだったという方がインターネットに載っている何気ない情報から簡単に身元を割り出すことができる、と注意を喚起するツイート
- 以前は「ストーキング以外に愛情表現がわからなかった」「住所や職場、電話番号に家族構成など全部調べるのが得意」
- とある人物の個人情報をネットに掲載されている写真などを手がかりに調べてみたところわずか1日で以下が判明
- **本人と子供の本名、住所、電話番号、子供が取り組んでいるスポーツ、子供が通っている中学校と小学校**

個人情報をネットから

- 何気なくネットにアップしている写真やふとした情報からあらゆる個人情報を探られる可能性がある
- 特定に至ったきっかけは相手がネットにアップしていた子供の運動会の写真
- 子どもが通っている学校が判明したことから通学路がわかってしまうため、悪意を持ったストーカーであれば家族への危険性が増すことになると指摘。
- ネットで得た個人情報を元にゴミ捨て場を特定すればもっと沢山の個人情報を入手できる

個人情報をリアルから取得

- 引っ越し業者が業務上知り得た情報を利用して、引っ越しをした女性に対してLINEで連絡
  - 会社に連絡し「会社に言ったところ連絡先を消してくれましたが電話口での謝罪のみ」という処分
- 引っ越し業者は企業Webサイトにて個人情報保護方針を掲載
  - 目的外使用をしない、と明示

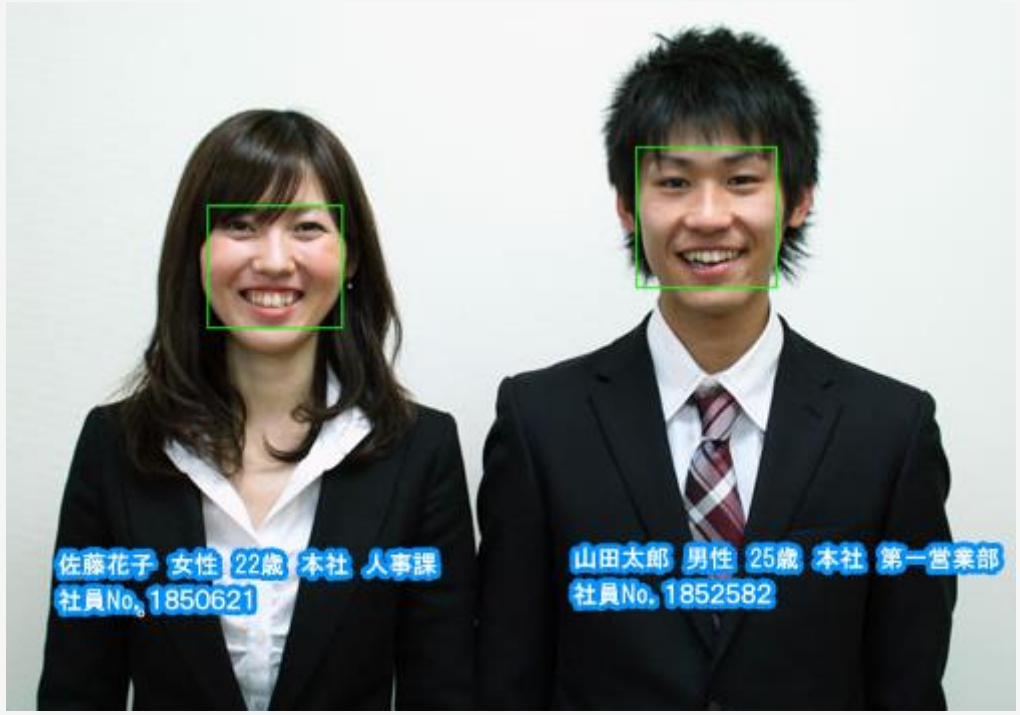
- 実際のところ対応策は無い
  - プライバシーマーク取得企業であれば、JIPDECに連絡すると取り消し処分になる

監視カメラ

- 防犯用・設備監視用などに多数の監視カメラが利用
- 最近のものはネットワーク上から閲覧が可能なものが多い
  - 流出していたり、第三者が閲覧できる状況にあるものも
- 2016年ロシアのサイトが第三者によってアクセスできる監視カメラを公開
  - 日本など120カ国以上のデータ
  - 日本では6000台以上の監視カメラを確認可能
  - 精神病院隔離病棟、有名コーヒーチェーン店、コンビニ、マッサージ店、理髪店など業種を問わず広く公開状態になっている

監視カメラから特定

- 監視カメラのデータから人物の顔を検出することは可能
  - 多数の監視カメラを組み合わせることで、本人の行動を追跡可能
  - 属性などを取得、格納しているシステムと組み合わせれば、名前なども瞬時に把握可能
  - Facebookでのタグ付けも同じ仕組み
- 肖像権・プライバシーの侵害という争いも
- イギリスでは犯罪捜査に活用



http://www.systemtokyo.jp/category6/entry46.htmlより2016年5月17日取得