情報の倫理

2017/10/19

Kazuma Sekiguchi
class@cieds.jp

無線LANの脆弱性

- 無線LANの暗号化技術に脆弱性が見つかった
  - 無線LANはどこでも傍受できるため、アクセスポイントとクライアント間の通信を暗号化して行うのが通常
  - 暗号化しないと誰でも見ることができるほか、送受信されるデータを書き換えたり、全て盗むことが原理上可能
  - そのため、暗号化して通信し、盗聴を防ぐ
- 暗号化方式は3つ
  - WEP、WPA、WPA2
  - このうち、WEPは暗号化として意味が現在では無いので使用しない
  - WEPでは直ぐ解読できてしまうため、暗号化の意味が無い

WPA2の脆弱性

- WPA2に脆弱性があることが見つかり、現在大慌てで各社が対応中
  - 同じアクセスポイントを利用するユーザーが、この脆弱性を悪用することで、情報の抜き取り、改変ができるなどの問題が生じる可能性がある
  - アクセスポイント側のファームウェアのアップデートとクライアント側（WindowsとかMacとかiOSとかAndroid）の両方で対応が必要
  - 現時点では、Windowsのみ対応が完了している状況
  - iOSなどは近日中にアップデートが出るらしい

ウェブサービスの情報流出

- 2016年4月2.7億人分流出
- IDとパスワードがセットで流出
  - Gmail、Yahoo、Hotmailなど

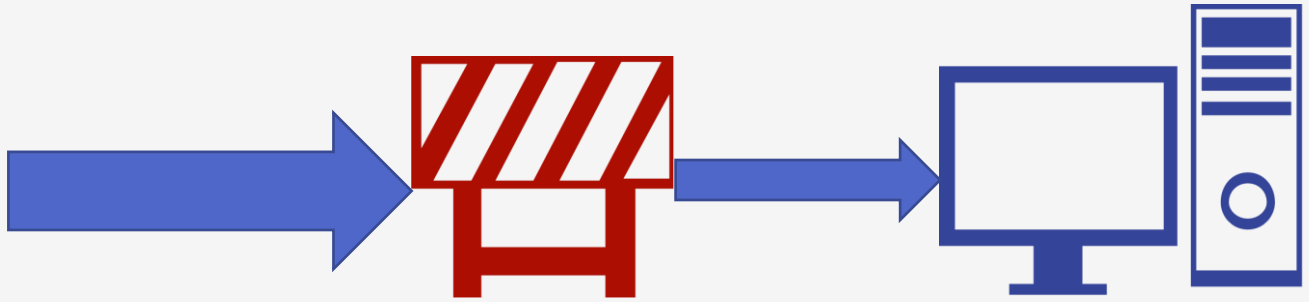
  - ロシア人クラッカーが不正アクセスして入手した模様
  - ただし、データが古いため、あまり影響は無いだろう、とも言われる

企業での情報流出

- IDなどを管理しているサーバへの攻撃
  - クラッキング
- 管理者の不注意により、データを外部に置き忘れ
  - 電車内にデータの入ったUSBメモリなどを忘れた
  - 不注意に破棄しようとし、第三者に回収された
- データを誰もがアクセスできるサーバの領域に置いておいた

サーバへの攻撃

- 実際のところ、サーバへの攻撃回数は非常に多い
  - 大企業などでは1秒間に1回程度は当たり前に行われる
  - 通常は攻撃を防ぐための多数の防御システムを構築しておく
    - ファイヤーウォールなど



```
May 20 18:08:23 serverlx01 sshd[14144]:
Failed password for invalid user oracle from
109.73.74.184 port 49209 ssh2

May 20 23:07:54 serverlx01 sshd[15635]:
Failed password for root from
119.10.114.52 port 30095 ssh2

May 20 23:07:57 serverlx01 sshd[15638]:
Failed password for root from
119.10.114.52 port 32557 ssh2

May 20 23:50:22 serverlx01 sshd[15860]:
Failed password for root from
218.104.51.42 port 64353 ssh2
```

攻撃の目的

- 金銭目的
  - ID、パスワードを奪い、クレジットカードの番号などを取得
  - 企業恐喝
- 顕示
  - サービスをダウンさせ、メッセージなどを掲載し、自己顕示を行う
- 興味
  - ただ単にサービスを停止する過程を楽しむ
  - 技術的欲求も含まれる

企業による情報流出への対応

- ほとんどの人はウェブサービスを利用する場合、同じIDを使い回すことが多い
  - パスワードも同じ場合、そのままのIDで他のサービスも利用できる
  - 仮に1つの会社からデータが流出した場合、パスワードが同じユーザの場合、他のサービスも乗っ取られる
  - 全てのサービスでIDとパスワードを変更して登録しておく

ウィルス、ボット、ワーム

- いわゆるウィルスは種類に応じて複数存在
  - ワーム：自己実行型。通常のアプリと同じように振る舞う
  - ボット：攻撃者が遠隔操作を行うことのできるウィルス。指示に従い、他のPCを攻撃したり、スパムメールを送出したりする
  - トロイの木馬：情報の収集を行い、攻撃者などに集めた情報を送り出す

感染経路

- インターネット、USBメモリ、CD-ROM（音楽CDから感染した例も）、メール、メールの添付ファイルなど多数に渡る
  - データを扱っている以上、いつでも感染の危険性がある
  - 通常ユーザは感染したことには気づかないことが多い
    - 知らない間に犯罪の片棒を担いでいることも多い
- 出荷されたばかりのPCからウィルス検出されたことも

- スパムメールの大半にはウィルスが添付されている
  - 開かないのが正解

ウィルス対策ソフト

- ウィルスの侵入、活動を抑制する目的のソフト
  - 通常パターンファイルと呼ばれるウィルスの特徴を集めたファイルを持ち、そこに集積されている情報とPC内のデータ、インターネットから送られてきたデータを照らし合わせて、ウィルスかどうか判別する
- 未知のウィルスには無力
  - ウィルスは1日に約6万種誕生
  - 全てに対応しきれないのが現状

ウィルス経由での情報流出

- ウィルス対策ソフトのウィルス検知率は60%程度
  - 40%程度は検知ができていないか、感染するまでに対策が間に合っていないのが現状
  - ウィルス対策ソフトを入れました＝安全と言うことではない
  - パターンファイルを更新できないようであれば、意味無い
- スマートフォン向けのウィルス対策ソフトはもっと検知率が低い
  - 実際にウィルスが動作しないと検知できないようなものが多数
  - ほとんど期待できないレベル

遠隔操作事件

- ウィルスを利用し、他者のPCを遠隔操作した上で、このPCから犯罪予告などを行ったサイバー犯罪
- 犯罪予告をされたために操作されたPCの所有者は警察などの捜査対象に
  - ログなどの記録を元に逮捕されている
- その後、ウィルスを介した遠隔操作が行われたことが判明し、逮捕された人達は誤認逮捕という結果に
  - 現在も真犯人とされた人は裁判中
- 一般人でも身に覚えが無いところでウィルスに感染し、場合によっては、犯罪に手を貸してしまう結果になることを表面化させた

スマホのウィルス

- スマホもウィルスは存在
  - 通常はアプリの形態を取り、ユーザにアプリとしてインストールさせる
    - スマホから情報を抜き取り、送信するものが多い
- スマホの場合、保存しているデータがよりパーソナルなデータ
  - 電話番号、電話帳、メール、場所など・・・
- スマホのアプリは公式のサイトからのみインストールする
  - AppStore、GooglePlay
- スマホのウィルス対策ソフトの効果は限定的
  - PCほど効率的動作ができないため、効果もそれほど高くない
  - 変なアプリをインストールしないのが一番の対策

ウィルスもさまざま

- ウィルスは情報取得型に変化しつつある
  - 以前はファイルを破壊して、PCを起動できなくするタイプが多かった
  - 現在は、PC内の情報を抜き取り、別の場所に転送して、販売や悪用することが多い
  - ファイルを暗号化し、現金を要求するようなウィルスも（身代金ウィルス、ランサムウェア）

http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=Ransomware+Raises+the+Stakes+With+CryptoLockerより
2015年5月19日取得

キーロガー

- 厄介なのがキーロガー
  - キーボードでどのキーを押したのかを把握するソフト
  - パスワードもキーボード経由が普通なので、キーロガーが入っているとパスワードが抜き取れる
  - PCのパスワードが抜き取られると遠隔で操作が可能になる恐れ

パスワード

- ほとんどのウェブサービスではユーザ名（メールアドレス）とパスワードの組み合わせ
  - パスワードは非常に便利な仕組み
    - 特殊な機器も不要、コストも抑えることができる
    - ユーザがきちんと管理していれば一定以上のセキュリティ効果が期待できる
- 利用できるサービスが増えるに従い、ユーザが管理するパスワードも増える
  - それごとにパスワードを作成、管理するのは難しくなってきている
  - 使い回しが発生

パスワード

- 攻撃者が個人のアカウントを乗っ取る場合、アカウントは
  - ID：メールアドレス（大体は公開していることが多い）
  - パスワード：適当な英数字

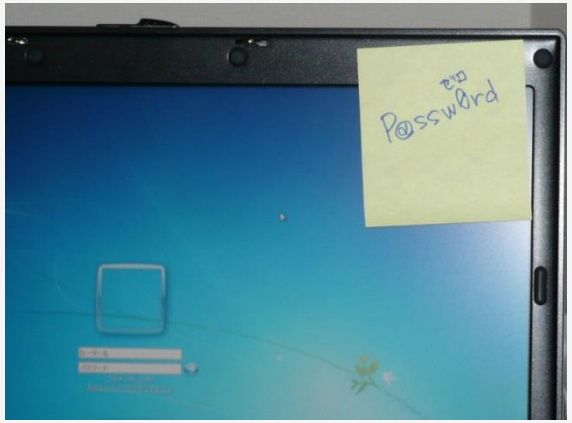
  で構築されているため、メールアドレスに正確なものを入力
  パスワードはディクショナリ攻撃

- ディクショナリ攻撃
  - パスワードには大体英単語の組み合わせで構築されていることが多いことを利用した攻撃手法
  - 辞書を用意し、それの組み合わせでパスワードを生成して、1つずつ試す
    - PCは非常に高速なため、1秒間で10個程度試すことが可能
    - いずれは当たる可能性が高い

パスワード

- 笑えないが意外に多いパスワード
  - 「12345678」
  - 「asdfghj」など
  - 「誕生日」
  - 「サービスの名前（例えば、Twitter）」

- メモに記して、画面に貼っておく
  - 会社などでたまに見かける
  - 社外の人が来たらどうする？
    - ソーシャルエンジニアリング



パスワード忘れ

- パスワードを忘れた場合、メールで送信してくれる機能が備わっているところが多い
- 「秘密の質問」に答えることでログインできるようになっているところも多い
  - 秘密の質問の場合、答えをSNSなどに記載していた場合、全く秘密では無くなり、アカウントを乗っ取られる
    - 「秘密の質問」：出身地は？とか
- 「秘密の質問」は何度も答えられる、という危険性

指紋認証

- 指紋認証など人体の一部を利用して認証をすることを「バイオメトリクス」という
  - 静脈、網膜、虹彩、音声、顔などなど
- 指紋認証が手軽かつ小型化できることから多用
  - 実際には検知率が悪いため、かなり甘い検出で一致となる
  - 寝ている人の指を使えば・・・

虹彩認証スマホ

- 虹彩＝目の瞳孔の周りにある環状のシワ。人によって形や模様が異なるため、識別が可能
  - 0.6秒スマホを見つめるだけでロック解除が可能
    - パターン入力よりも手軽
    - ロック番号入力よりも破られない
    - 起きていないと認証されない＝寝ていて認証されるのを避けられる
- 他にも顔認証なども登場
  - 新しいiPhoneに搭載されるとされるFaceIDなど
  - 100万種類の顔を見極めるとされるが、さて・・・・

ログイン制限

- ID名が同じ状態でログインに数回失敗した場合、アカウントがロックされる
  - 銀行口座の場合、暗証番号を3回間違えると窓口で解除して貰う必要がある
- 一部のウェブサービスでは実装され、30分程度試すことができないようにされている
  - 一部だけなので、全てのウェブサービスで実装されていない
  - セキュリティ対策が緩い会社も非常に多い

オンラインバンキング

- オンラインで銀行振り込みなどが可能なサービス
  - お金を直接扱うため、極めて狙われやすい
  - 通常振り込み時などには、手元にある「乱数表」を入力して正しい値を入力すると操作できるようになっている
- フィッシング詐欺のサイトなどでは、乱数表の数字を全部入力させる
  - 入力させることで、詐欺をしようとする人が乱数を手に入れることが可能
  - すべてのオンラインバンキングで乱数表の数字は全部入力させることはない

ワンタイムパスワード

- 一部の銀行で採用されている1分間だけ有効なパスワードを生成するタイプのもの
  - パスワードは1分経つと無効になるので、万が一流出しても被害が出ることはない
    - ワンタイムパスワードを抜き取るウィルスも存在するため、完全ではないとされる

対応

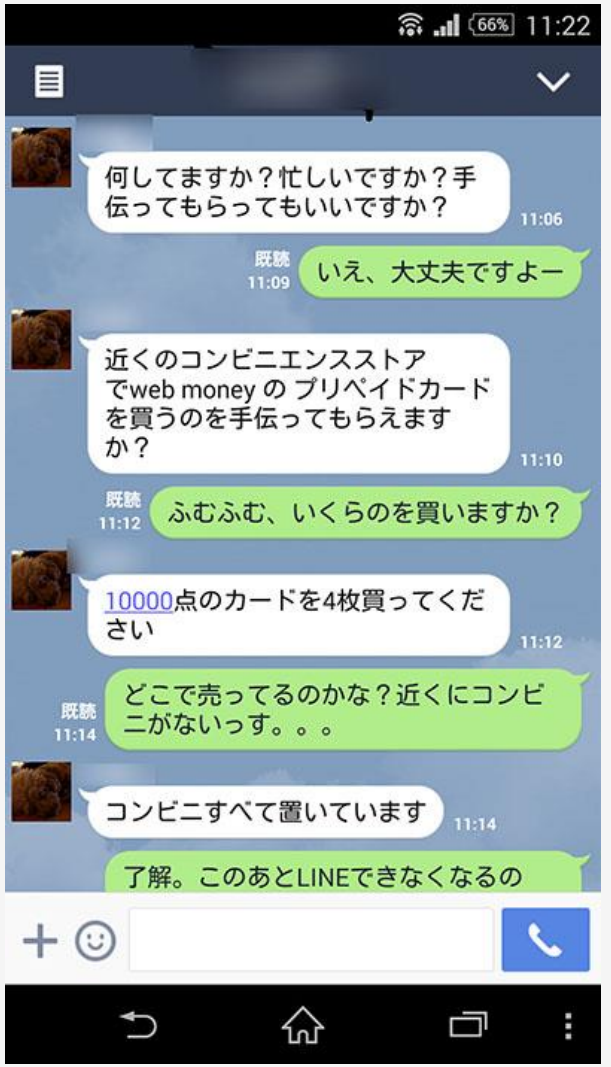
- パスワードはできる限り複雑にする
  - 記号混じりのランダムな英数字が望ましい
  - サービスによっては8文字までしか使えない、または最初の8文字だけで比較するので、最初にランダムな英数字、記号を持ってくる
  - 「秘密の質問」は通常公開しないような複雑なものを選択する

対応

- 使わなくなったサービスは退会処理などを行っておく
  - できる限り、流出の可能性を減らす
    - 退会処理をしてもデータが残っていることは多い
- 情報流出が合った場合、速やかにアカウントを確認し、不審な点が無いことを確認した上で、パスワードを変更する
  - 情報流出などの情報は常に注目しておく
  - LINE、Twitterなどは何度かパスワード流出をしている

アカウント乗っ取り

- LINEのアカウントを乗っ取って知り合いの振りをして、プリペイドカードの番号を奪う
- パスワードを使い回していたためにアカウントを乗っ取られた例が多い
- PCからの接続を拒否しておく、PINコードを設定しておくなどの対応が有効
  - パスワードの使い回しをしない



http://trendy.nikkeibp.co.jp/article/column/20140716/1059149/?SS=expand-digital&FD=-781260321より
2015年5月19日取得

実例

- GoogleWallet（Googleの決済システム）にクレジットカード番号登録済みの状態
  - Googleのアカウントと GoogleWalletのアカウントは同一
  - 第三者がGoogleのアカウントに何らかの方法でログイン成功
  - GooglePlayで高額なソフトを大量購入
    - 全てクレジットカード登録済みのため、そのまま決済が実行
    - クレジットカード停止処置

600小判 (あやかし陰陽録 【無料カードバトルRPG】 by Zynga)	￥600	2014年3月26日	キャンセルしました	Androidアプリ
1000小判 (あやかし陰陽録 【無料カードバトルRPG】 by Zynga)	￥1,000	2014年3月26日	キャンセルしました	Androidアプリ
1000小判 (あやかし陰陽録 【無料カードバトルRPG】 by Zynga)	￥1,000	2014年3月26日	処理済み	Androidアプリ
1000小判 (あやかし陰陽録 【無料カードバトルRPG】 by Zynga)	￥1,000	2014年3月26日	処理済み	Androidアプリ
1000小判 (あやかし陰陽録 【無料カードバトルRPG】 by Zynga)	￥1,000	2014年3月26日	処理済み	Androidアプリ
1000小判 (あやかし陰陽録 【無料カードバトルRPG】 by Zynga)	￥1,000	2014年3月26日	処理済み	Androidアプリ
600小判 (あやかし陰陽録 【無料カードバトルRPG】 by Zynga)	￥600	2014年3月26日	処理済み	Androidアプリ
600小判 (あやかし陰陽録 【無料カードバトルRPG】 by Zynga)	￥600	2014年3月26日	処理済み	Androidアプリ
600小判 (あやかし陰陽録 【無料カードバトルRPG】 by Zynga)	￥600	2014年3月26日	処理済み	Androidアプリ
600小判 (あやかし陰陽録 【無料カードバトルRPG】 by Zynga)	￥600	2014年3月26日	処理済み	Androidアプリ

Simeji,BaiduIME

- BaiduIMEおよびSimejiが利用者に無断で入力内容をBaidu社に送信していると判明し問題
- 入力内容の他、個別の端末ID、利用デバイス名（機種名）などの付帯情報も送信
  - パスワードなどは送信されていないと説明
- ソフトのバグということで修正され、現在はクラウド変換を利用していない限り送信されていない

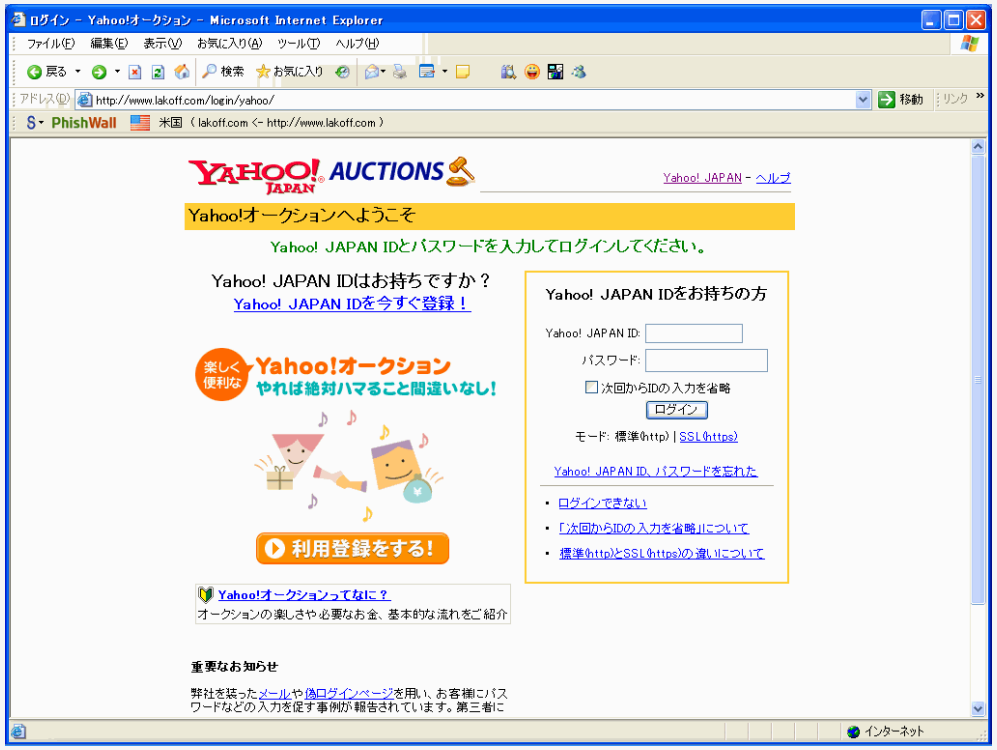
フィッシング詐欺のサイト

- 見た目は本物と同じ
- URLが違っている
  - 但しぱっと見は分からない程度にしか違いが無い
- オンラインバンキングなどではサーバー証明書などを確認
  - メールなどのリンクからオンラインバンキングにアクセスしない

https://www.antiphishing.jp/news/alert/mufg20131118.htmlより
2015年5月19日取得

フィッシング詐欺

- 旧来はオンラインバンキングなどで盛ん
- 本来のサイトと全く同じデザインで構成され、ユーザが利用しようとIDとパスワードを入力したらその情報を盗み取るサイト
- デザインだけでは判別が付かない
  - 見た目にだまされないことが必要



http://www.securebrain.co.jp/about/news/2005/11/phishing-case.htmlより引用

フィッシング詐欺見極め

- URLを偽ることは不可能
  - ID、パスワードを入力するようなサイトではURLを確認する

  - URLが異なっていた場合は、利用しない
    - サービス名とURLには関連がある
- ブラウザでは常にURLを表示するようにしておくべき

メールによるフィッシング詐欺誘導

- URLを含んだメールを送信し、URLをクリックするように誘導
- URLとして表示されているところと違うサイト（フィッシングサイト）へと移動させる

http://spotlight-media.jp/article/24326512706024506 8より引用

個人のPCへの攻撃

- 全てのソフトウェアには何らかの不具合、バグが存在する
  - セキュリティ上に問題がある場合、セキュリティホールと呼ぶ
  - Windowsやブラウザに問題がある場合、その不具合を利用し、攻撃者が攻撃するすることが可能
- インターネットへの接続が常時接続が当たり前になったため、攻撃しやすい
  - WindowsやMacなどのOSにセキュリティホールが残ったままだと攻撃者がそこから侵入することが可能

個人のPCへの攻撃

- セキュリティホールを塞ぐパッチが登場した場合、即時適用することが必要
  - 適用しない場合、攻撃手法が周知されているため、攻撃されやすい
  - 古いOSなどの場合、セキュリティパッチが提供されないため、サポート切れのOSは利用しないこと
    - Windowsの場合7以前はサポート外
    - Macの場合は、OS X10.10以前はサポート外
      （公式には言われていない）

セキュリティパッチを当てていないPC

- パッチを当てていないPCをネットに接続していた場合、5時間でウィルスに感染
  （http://pc.nikkeibp.co.jp/article/NPC/20070412/268177/）

- WindowsXP,Vistaはサポート切れ
  - 以降はセキュリティパッチが提供されないため、利用しないこと