ハッキングの世界

2014年8月

セクタンラボ勉強会

はじめに

- サイバー攻撃による事件が頻発しています。
- 仮想世界と現実社会がリンクしている現代社会では，「他人事」ではないはずですが・・・。

パソコン遠隔操作事件

Mt.Gox社への不正アクセスによるビットコイン盗難事件

WEBサイトへの不正アクセスによる個人情報流出事件

ネットバンキングの不正送金事件

大多数の人は，リスクを実感できていないのでは？

発表のねらい

ハッキングの実演を通じて，脅威を実感していただく

皆さんのご家庭や，業務システムの情報セキュリティ
について考える「キッカケ」となれば幸いです！

本日のお品書き

サポートが切れたOSを使うとどうなるの？

暗号化されたパスワードなら盗まれても安心？

登場人物

Aくん

仕事をバリバリこなすビジネスマン
でもパソコンは，まだXPを使っている

（注）WindowsXPは，2014年4月8日にサポートが終了しています。

ハカ太郎くん

Aくんを狙うクラッカー
その正体は誰も知らない

（注）ハッカーは高度なIT技術を有する人の総称。
技術を悪用する者はクラッカーと呼び区別する。

この物語はフィクションであり，実在の人物・団体とは一切関係ありません

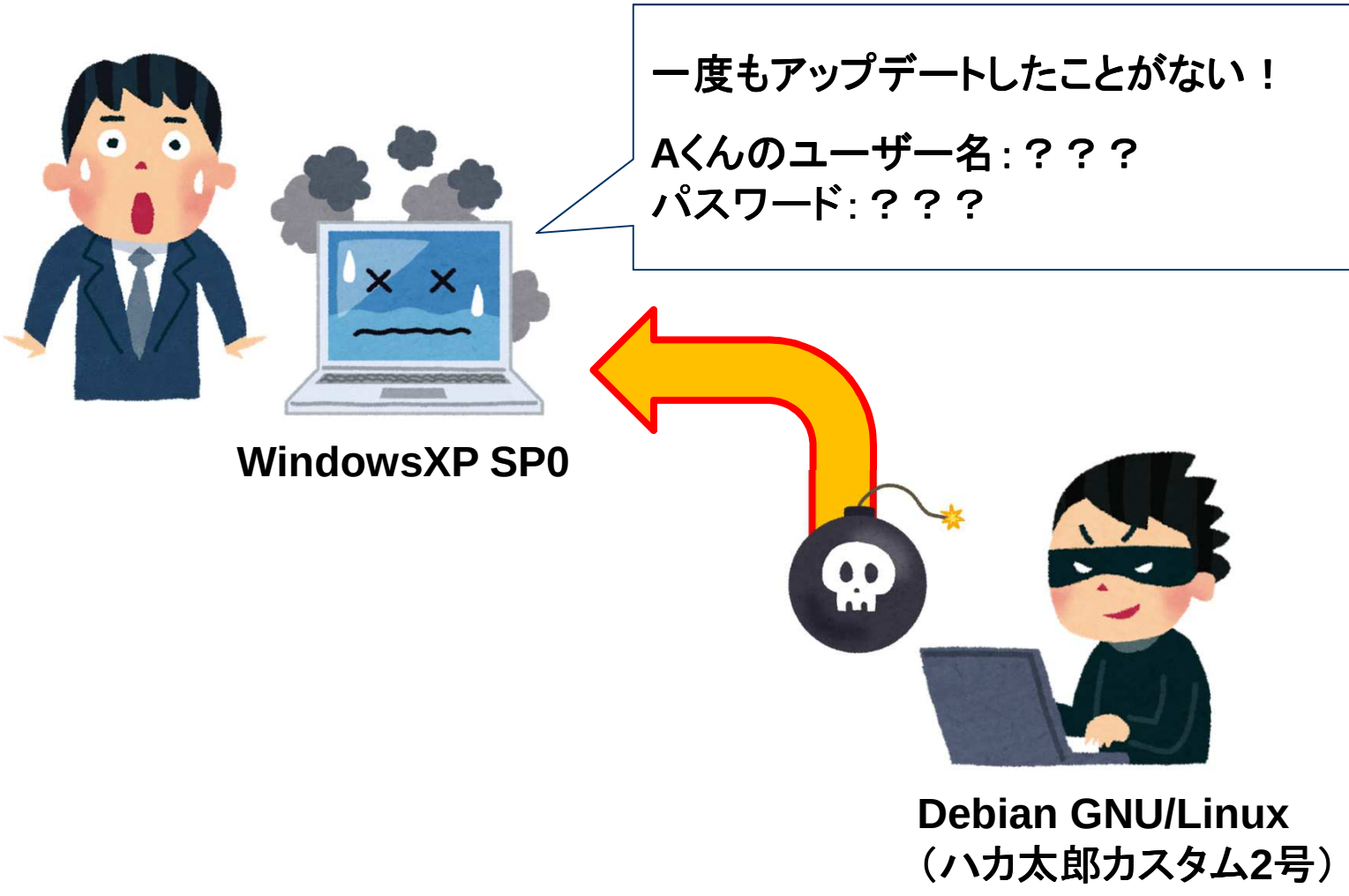
本日の1品目

サポートが切れたOSを使うとどうなるの？

百聞は一見にしかず！

まずはハク(や)ってみよう！

実演



ハッキングされた原因

- Windowsのアップデートを一度もしていなかったため，脆弱性（セキュリティ上の欠陥）が多数存在していました。
- そのため，ネットワーク経由で攻撃コードを送りつけられて，パソコンが乗っ取られてしまいました。

OS/ソフトウェアをアップデートせずに利用するのは危険！

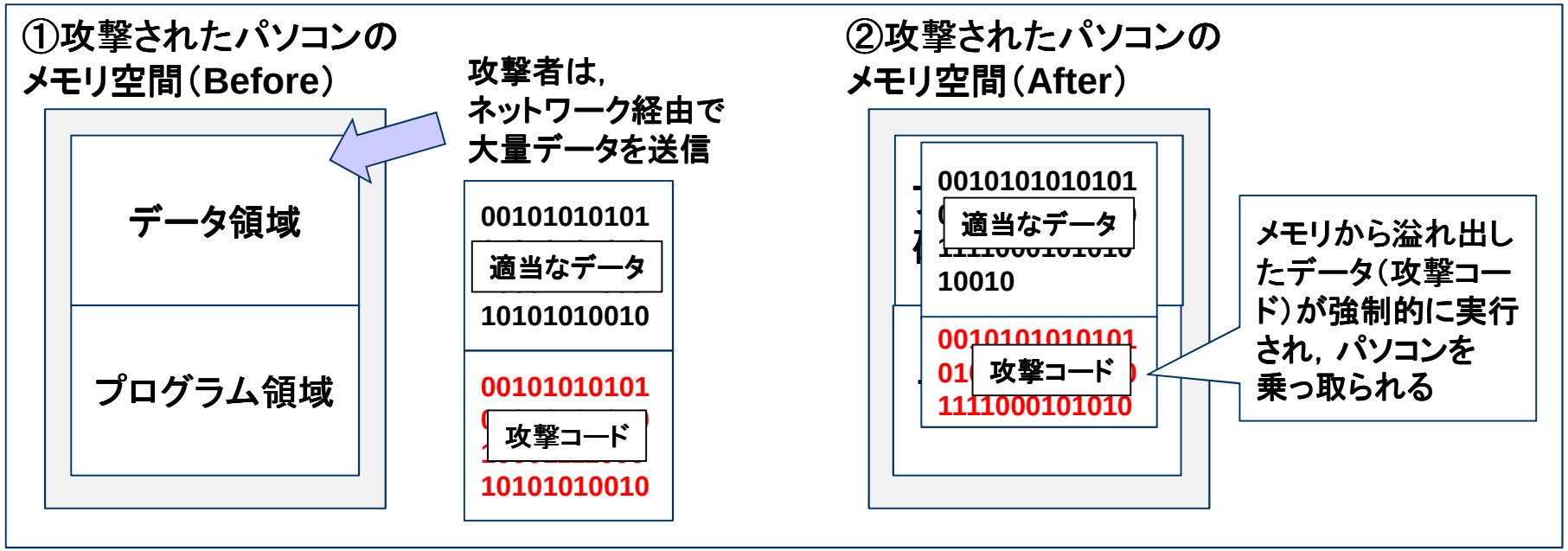
- Microsoftは毎月第2火曜日の翌日に，定例アップデートを配信しています。
- JavaやAdobe Reader/Flashなどもアップデートメッセージが表示されたら，速やかにアップデートしましょう。

もう少しだけ詳しく！

（参考）攻撃のメカニズム

- 本日の実演では，CVE-2008-4250（MS08-067）と呼ばれる脆弱性を攻撃しました。
- これは，Windowsのファイル共有機能などに利用される「Serverサービス」に存在するスタックオーバーフローの脆弱性です。

攻撃メカニズムのイメージ図　（説明用に簡略化した概念図であり，厳密な動作原理は異なります）



よくある質問

サポートが切れていないWindowsなら安全ですか？
（サポートが切れていたから，ハッキングされたのですか？）

ウィルス対策ソフトがあれば大丈夫ですよね？

じゃあ，どうしたらいいんですか！？

本日の2品目

暗号化されたパスワードなら盗まれても安心？

不正アクセスによる情報流出の事例

- **2013年5月17日と5月23日にYahoo! Japanが発表**

Yahoo! Japan IDの管理サーバが，外部から不正アクセスを受けた

最大2,200万件のIDが流出した可能性がある。うち，148.6万件は，
「不可逆暗号化されたパスワード」なども流出した可能性が高い。

Yahoo! Japan広報のブログ

（ブログより抜粋）

Q:パスワードが漏れた可能性があると報道されているが、漏れたのはパスワードか？

A:パスワードを不可逆暗号化した文字列です。

Q:不可逆暗号化されたパスワードとは？

A:パスワードを暗号化した文字列です。この文字列を元に戻すことはできません。

「不可逆暗号」とは

- 「不可逆暗号化したパスワード」とは，元のデータ（パスワード）から，一定の計算方法により算出した，元のデータの「指紋」のような値のことです。
- この指紋を計算する関数のことを「ハッシュ関数」といい，指紋のことを「ハッシュ値」と呼びます。

特徴①同じデータからは常に同じハッシュ値が出力される

特徴②データの内容が少しでも変化すると全く異なるハッシュ値が出力される

特徴③数学的には，ハッシュ値から元のデータを計算できない

パスワード認証の仕組み

ID: Taro
Password: aaa

サンプルシステム

① 入力されたパスワードからハッシュ値を計算
47bce5c74f589f4867dbd57e9ca9f808

② IDとパスワードハッシュが一致すればログイン成功

ID/Passwordのデータベース

ユーザー名	パスワードのハッシュ値
Taro	47bce5c74f589f4867dbd57e9ca9f808 （パスワード「aaa」から算出）
Hanako	e62595ee98b585153dac87ce1ab69c3c （パスワード「aab」から算出）

百聞は一見にしかず！

まずはハク(や)ってみよう！

実演

- 「不可逆暗号」は，数学的には解読できませんが，本当に安心してよいのか確かめてみましょう。
- さきほどハッキングしたXPでも，パスワードは「不可逆暗号」された状態で保管されています。これを解読してみます。

数学的には解読できなくても，
裏ワザで攻略するのがハッキングです。

よくある質問

数学的に解読できない暗号のはずなのに何故！？

じゃあ，どうしたらいいんですか！？

まとめ

まとめ

- 情報セキュリティを確保するためには，脅威とリスクを正しく理解することが大切です。
- 本日の発表を「キッカケ」として，情報セキュリティに興味を持っていただければ幸いです。