ネットワークセキュリティと自己防衛

ユーザを認証する技術

事例：ヤフオクID盗難事件

身に覚えなく，自分が出品者に…

これを出品した本人は？　取引は？　代金は？

〈 ヤフオクID盗難，中国IPアドレスの接続150万件 〉

インターネットオークション最大手「ヤフー・オークション（ヤフオク）」の会員のIDとパスワードが盗まれ，身に覚えのない出品料を請求される被害が相次いでいる「 ID乗っ取り 」問題で，中国の特定のIPアドレスからの不正アクセスが今年5月以降だけで150万件に上っていたことが，ヤフーの調査でわかった。

ヤフーはこれまで出品料の返金には基本的に応じない姿勢だったが，不正アクセスの発信元が特定できたことで本人以外による接続と確認できたため，返金や請求放棄に向けた手続きに入った。

事例：ヤフオクID盗難事件

〈 ヤフー，出品料返金や請求放棄へ 〉

ヤフオクを巡っては，本人の知らないところでIDなどが使われ，偽ブランド品などが大量出品される被害が続発。会員は，数千円から数十万円に上る出品料などをヤフーから請求され，ヤフーとの間でトラブルになっていた。

ヤフー側はこれまで，「うちからはIDやパスワード流出はしていない」と主張。会員に出品料などを請求してきた。

その後の調査で，何者かが会員のIDなどを使い，中国の特定のIPアドレスからヤフオクへの不正アクセスを繰り返していたことが判明。関与した人物はごく少数に限られるとみられ，ヤフーでは，偽ブランド品の製造グループが商品を売りさばこうとして組織的にかかわっていた可能性があるとみている。

事例：ヤフオクID盗難事件

IDなどが流出した経緯について，ヤフーは「会員がフィッシング詐欺に遭った可能性がある」と主張。また，ヤフオクのIDやパスワードと同じものを別のサイトで使っている人もいるため，「別のサイトから流出したIDなどのリストが使われているのではないか」と推測する。

しかし，被害に遭った会員の中には，ヤフオクでしか使っていないIDなどを用いて侵入されているケースもあり，ヤフーの主張とは食い違う点もある。

身に覚えのない出品料を請求される被害について，ヤフーでは現時点で5000件を確認。被害会員に出品料を返すことを決めるとともに，システム見直しも含めた策を検討し始めた。

ヤフーは被害見込みの総額を公表していないが，中国の特定のIPアドレス以外からの不正アクセスもあり、被害総額は5000万円以上に上るとみられる。

ネットワークセキュリティ

☞ 何を守るのか?

＝ 自身，組織の有するデータ，情報，財産

☞ 何から守るのか?

＝ インターネットを標的とする犯罪者と，そのためのプログラム

- ✓ ウイルス
- ✓ スパイウェア
- ✓ オンライン詐欺
- ✓ SPAMメール
- ✓ なりすまし
- ✓ 情報漏洩・流出

どのようにして守るのか?

技術だけで防止できるもの

そうでないもの

知識・経験・勘

トピックス

ユーザを認証する技術

ユーザを認証する技術

☞ 認証とは

一定の行為または文書が正当な手続・方式でなされたこと
を公けの機関が証明すること。(広辞苑第五版)

☞ 認証の分類

(1) Authentication (2者間認証)

認証する側とされる側が事前に共有している情報を確認

＝ パスワード、暗証番号

(2) Certification (3者間認証)

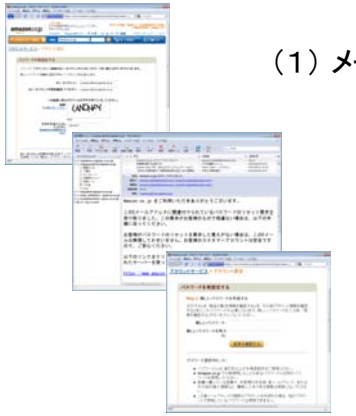
信頼できる機関が発行した証明書を基に『持ち主』の正当性を確認

＝ クレジットカード

パスワードを考える

パスワードを忘れてしまった？

Amazon.co.jp の場合



（1）メールアドレスを入力・送信

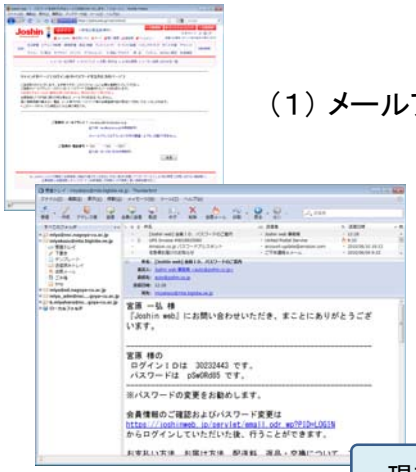
（2）メールを受信

（3）メール中のURLにアクセス

（4）Webでパスワードを再設定

パスワードを忘れてしまった？

Joshin Web の場合



（1）メールアドレス、電話番号を入力・送信

（2）メールを受信

メールにパスワードが記載！

現在は、Amazon と同様の仕組みに変更

お客様のパスワードは「〇×〇×」です。

本人以外、誰もパスワードを知り得ない……はず

↓

サーバにパスワードがそのまま保存されている！

パスワード大原則の崩壊

↓

場合によっては、大きな問題に！

パスワードファイルが盗まれると…

☞ パスワードファイル本来の形

```
miya:$1$IL.Mp57p$aDIVc/8.n1o…
nori:$1$wluVf.ci$PxJ2TjLEWMW…
gs067901:$1$BbjrLmCt$UHbfVO5…
gs067902:$1$A34uFZeE$NQhlh.w…
```

ハッシュ値

➡ 盗まれても、パスワード解読は困難

☞ あってはならないパスワードファイル

```
miya:pSw0Rd85
nori:norinori99
gs067901:Ng4mZH9gs
gs067902:209760GS
```

パスワードそのまま

➡ IDの流出！

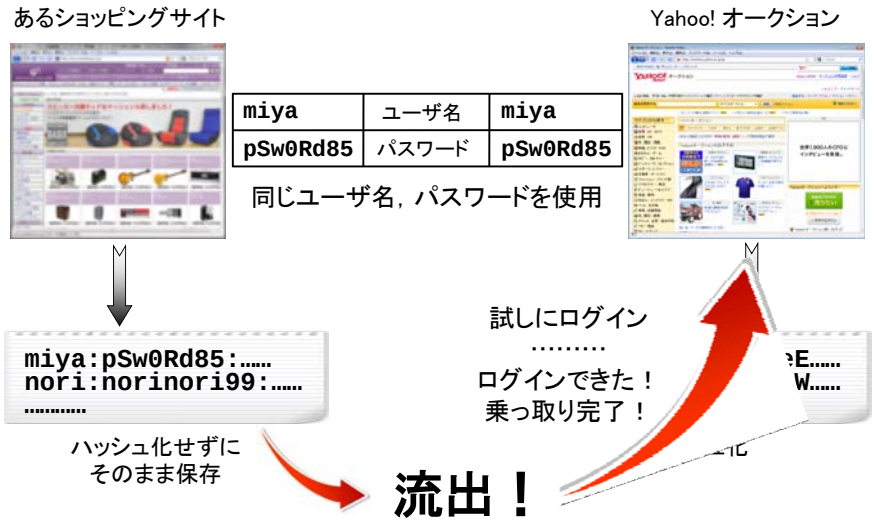
事例：ヤフオクID盗難事件

インターネットオークション最大手「ヤフー・オークション（ヤフオク）」の会員のIDとパスワードが盗まれ，身に覚えのない出品料を請求される被害が相次いでいる「ID乗っ取り」問題 …

ヤフー側はこれまで，「うちからはIDやパスワード流出はしていない」と主張。会員に出品料などを請求してきた。

IDなどが流出した経緯について，ヤフーは「会員がフィッシング詐欺に遭った可能性がある」と主張。また，ヤフオクのIDやパスワードと同じものを別のサイトで使っている人もいるため，「別のサイトから流出したIDなどのリストが使われているのではないか」と推測する。

サイトからのID流出



事例：ヤフオクID盗難事件

～ 別の記事 ～

ID乗っ取りをめぐっては，一部報道でヤフーから情報が流出した可能性があると報じていたが，ヤフーは9月6日に「情報流出の事実はない」と否定。その後，ログイン履歴を調査したところ，他社のサイトから流出したIDとパスワードを用いて，Yahoo!オークションにログインを試みる形跡が見られたという。

「入力されたIDの9割以上はYahoo!に存在せず，その中にはYahoo!では使えない『．（ドット）』や『－（ハイフン）』などの記号を含むIDも多かった。一方，Yahoo!で使われているIDが入力されたのは4%程度。不正なログインが確認されたケースでは，いずれも1～2回の入力でログインに成功していたことから，他社とYahoo!のID・パスワードが同一のユーザーが被害に遭った可能性が高い。」（ヤフー広報部）

INTERNET Watch 2008/9/26 掲載
（http://internet.watch.impress.co.jp/cda/news/2008/09/26/20967.html ）

事例：ヤフオクID盗難事件

～ 関連するかもしれない記事 ～

〈 通販サイト「ナチュラム」で約65万件の個人情報流出の可能性 〉

ミネルヴァ・ホールディングスは6日，連結子会社のナチュラム・イーコマースが運営するショッピングサイト「アウトドア＆フィッシング ナチュラム」において，外部からの不正アクセスにより個人情報が流出した可能性があるとして，事態を公表した。流出した可能性のあるデータは65万 3424件で，そのうちクレジットカード番号（下4桁を除く）が含まれるものが8万6169件あったとしている。

個人情報項目は，必須項目がユーザーIDとパスワード，氏名，メールアドレスの4項目。任意項目が住所や携帯電話番号，電話番号，FAX番号，生年月日，クレジトカード名義，クレジットカード有効期限，クレジットカード番号（下4桁は保持していない），家族構成管理コード，性別管理コードの10項目となっている。

INTERNET Watch 2008/8/6 掲載
（http://internet.watch.impress.co.jp/cda/news/2008/08/06/20498.html ）

問題は？

ユーザ名　:miya
パスワード :pSw0Rd85

ハッシュ化せずにそのまま保存

問題 ①: サイトの責任

ユーザ名　:miya
パスワード :pSw0Rd85

同じパスワードを使っている

問題 ②: 誰の責任?

他人（他のサイト）にパスワードを教えましたね?

結論として

望ましいパスワード管理

(1) 短すぎるものは避け，ある程度の長さとする

(2) アルファベット（大文字・小文字），数字，記号を混ぜる

(3) 類推されやすいもの（個人情報など）は避ける

(4) 定期的に変更する

(5) メモには残さない

(6) 他人に教えてはいけない

原則を破ったユーザの自業自得

望ましいパスワード管理

(1) 短すぎるものは避け，ある程度の長さとする

(2) アルファベット（大文字・小文字），数字，記号を混ぜる

(3) 類推されやすいもの（個人情報など）は避ける

(4) 定期的に変更する

(5) メモには残さない

(6) 他人に教えてはいけない

(7) 使い回しをしない

新しい認証手段

(1) ICカード

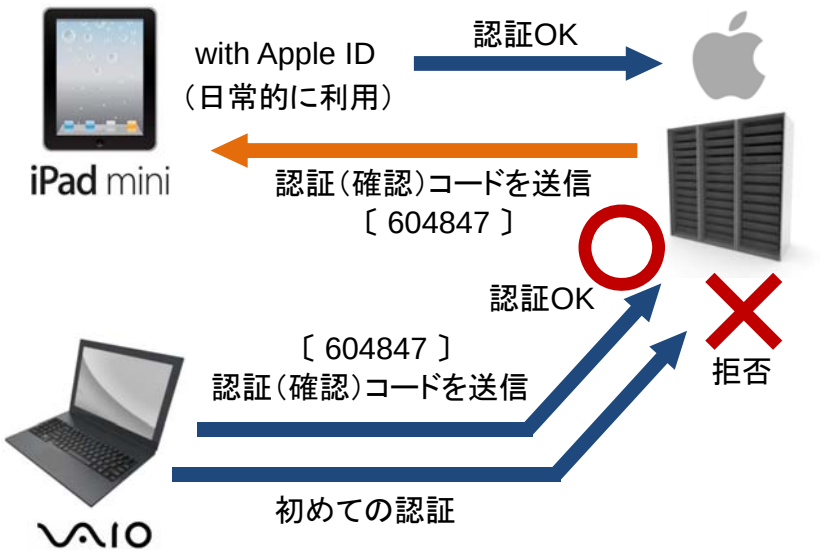
(2) 乱数表

(3) ワンタイムパスワード （トークン、カード、メール送信）

(4) バイオメトリクス
（指紋、虹彩、静脈、声紋、署名 など ）

(5) 2段階認証

2段階認証



まとめ
ユーザを認証する技術

パスワード ＝ ユーザを守る要

（1）パスワードは本人以外、誰も知り得ない

！ この常識が崩れてきている

（2）パスワードの使い回しをしない

（3）さまざまな攻撃手段を知る

（4）攻撃に強いパスワードの考案

（5）新たな認証手段の利用