

基本情報技術者試験より

Webシステムのパスワードを忘れたときの利用者認証において、合い言葉を使用する場合、合い言葉が一致した後の処理のうち、セキュリティ上最も適切なものはどれか。

- あらかじめ登録された利用者のメールアドレス宛てに、現パスワードを送信する。
- あらかじめ登録された利用者のメールアドレス宛てに、パスワード再登録用ページへアクセスするための、推測困難なURLを送信する。
- 新たにメールアドレスを入力させ、そのメールアドレス宛てに、現パスワードを送信する。
- 新たにメールアドレスを入力させ、そのメールアドレス宛てに、パスワード再登録用ページへアクセスするための、推測困難なURLを送信する。

めるかば @methuselah3 · 7月3日 #7pay
メールに気づいたのは30分後、すぐに7セブンイレブンアプリにログインしようとしたが乗っ取られているのでログインに手間取りました。その後、お困りのときはから検索すると、コールセンターの問い合わせ先が出てきました。
しかし2時間以上つながりません
241 113

めるかば @methuselah3 · 7月3日 #7pay
クレジットカードでの見えないチャージはきょうの12時過ぎから自動的に10回、計30万円行われましたが、通知はクレジットカードチャージのレシートメールのみ、そもそもアプリにログインされたことなどはわかりませんでした
348 170

めるかば @methuselah3 · 7月3日 #7pay
改めてお恥ずかしい限りですが、セブンイレブンアプリの乗っ取りにあいまして、7payの不正チャージにより30万円利用されました。
あまりに対応がひどいので、順番に対応状況を記載していきます
ハッシュタグはシンプルに #7pay
47 9,506 6,656
このスレッドを表示

めるかば @methuselah3 · 7月3日 #7pay
続報はのちほど。
21 23

めるかば @methuselah3 · 7月3日 #7pay
その後冷静にアプリからもカード情報を削除し、パスワード変更し、いったん止まりましたが、被害額は30万円です。3万×10回、セブンイレブンでは、8万〜9万づつ使われています。店名も時間もわかります。防犯カメラでわかる気がします。
3 425 293

めるかば @methuselah3 · 7月3日 #7pay
相変わらず7payコールセンターはつながりません、もう5時間ですが、ブルっという音すらしません。
問い合わせメールをしましたが、「不正利用の可能性があるので電話ください」とのこと。電話がつかないから言ってるんですけどね。
2 324 207

パスワードを忘れた場合

パスワード再設定ページを、ご登録いただいたメールアドレス宛にメールでご連絡します。

ご登録生年月日 必須 []年 []月 []日

7ID (メールアドレス) 必須 []

画像認証 必須 wxxtc [] ※別の画像を表示
※画像に表示されている英数字を半角で入力してください

ログインID・パスワードが確認出来ないお客様は他サイトのIDでご登録されている可能性があります。
他サイトのIDをご確認の上、ログインをお試下さい。
Facebook | Twitter | Google | Yahoo!JAPAN | LINE

メールを送信する

Copyright © Seven & i Holdings Co.,Ltd. All Rights Reserved.

パスワードを忘れた場合

パスワード再設定ページを、ご登録いただいたメールアドレス宛にメールでご連絡します。

ご登録生年月日 必須 []年 []月 []日

7ID (メールアドレス) 必須 []

画像認証 必須 ny3kr [] ※別の画像を表示
※画像に表示されている英数字を半角で入力してください

送付先メールアドレス []

ログインID・パスワードが確認出来ないお客様は他サイトのIDでご登録されている可能性があります。
他サイトのIDをご確認の上、ログインをお試下さい。
Facebook | Twitter | Google | Yahoo!JAPAN | LINE

メールを送信する

Copyright © Seven & i Holdings Co.,Ltd. All Rights Reserved.

事例1 : 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?

事例1 : ヤフオクID盗難事件

〈 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。

YOMIURI ONLINE (<http://www.yomiuri.co.jp/>) 2008/9/26 掲載

事例1 : 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1 : 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。

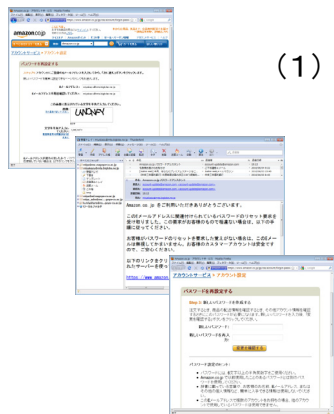
しかし, 被害に遭った会員の中には, ヤフオクでしか使っていないIDなどを用いて侵入されているケースもあり, ヤフーの主張とは食い違う点もある。

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。

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

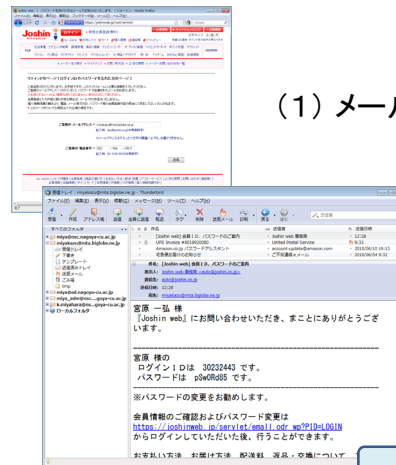
(2) メールを受信

(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$NQh1h.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:Nq4mZH9gs
gs067902:209760GS
```

パスワードそのまま

➡ IDの流出！

事例1: ヤフオーク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?

事例1: ヤフオークID盗難事件

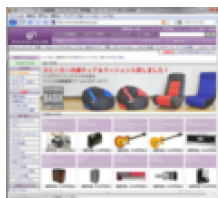
インターネットオークション最大手「ヤフー・オークション(ヤフオーク)」の会員のIDとパスワードが盗まれ, 身に覚えのない出品料を請求される被害が相次いでいる「ID乗っ取り」問題...

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, ヤフオークの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

あるショッピングサイト



miya	ユーザ名	miya
pSw0Rd85	パスワード	pSw0Rd85

同じユーザ名, パスワードを使用

Yahoo! オークション



miya:pSw0Rd85:.....
nori:norinori99:.....
.....

ハッシュ化せずに
そのまま保存

流出!

試しにログイン
.....
ログインできた!
乗っ取り完了!

事例1: ヤフオーク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1: 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、クレジットカード名義、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

miya:pSw0Rd85:.....
nori:norinori99:.....
.....

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?

他のサイトでパスワードを使い回しましたね？

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
- (7) 使い回しをしない

「使い回しをしない」

という原則を破ったユーザの自業自得

ネットから現実の行動プライバシーへ

PASMO マイページ (すでにサービス終了)

ICカード利用履歴

月日	種別	利用場所	ポイント	残額
0514	入場	桜山	****OP	****OP
	出場	池下	*1840	
0515	入場	池下	****OP	****OP
	出場	桜山	*1410	
0515	入場	桜山	****OP	****OP
	出場	池下	*1180	
0517	入場	池下	****OP	****OP
	出場	桜山	*850	
0517	入場	桜山	****OP	****OP
	出場	池下	*720	
0520	入場	池下	****OP	****OP
	出場	池下	*490	
0520	バス等	名市バス	****OP	****OP
			*290	
0520	入場	桜山	****OP	****OP
	出場	池下	*80	
0521	現金		****OP	****OP
			*2080	
0521	入場	池下	****OP	****OP
	出場	桜山	*1820	

SF(電子マネー)利用履歴

月日	種別	利用場所	残額
06/03	入	JC名古屋	
	出	JC金山	¥2200
05/16	現金		¥2360
05/10	入	JC金山	
	出	JC名古屋	¥360
03/12	入	JC名古屋	
	出	JC金山	¥520
03/10	入	地和光市	
	出	地 東京	¥680
03/09	入	東武池袋	
	出	和光市	¥950
03/09	入	船橋	
	出	池袋	¥1190

ネットに公開する人多数

- カード番号
 - 氏名(カタカナ)
 - 生年月日
 - 電話番号
- が分かれば登録できてしまう

第三者が知り得る情報のみでユーザー登録



重大なセキュリティ上の欠陥



マイページ 会員登録

カードの登録

PASMOに登録されている情報を入力してください。なお、カード購入日およびカード交換、再発行、氏名・生年月日・電話番号変更当日は、カードの確認できませんので、翌日以降にご登録ください。

カード番号 (半角英数)

氏名(カタカナ) 姓: 名: (半角カタカナ)

生年月日 1987 年 月 日

電話番号 (半角英数)

お問い合わせ日時 2007/04/02 11:33:04

表示している情報は、お問い合わせにより、確定が遅延する場合があります。

定期券情報 鉄道定期券:
三崎口 ↔ 市 湘南
經由: 京急堀内 R上大岡
定期券 通学 継続 6ヶ月 2007/4/8~2007/10/7
バス定期券:

SF残額履歴

月日	種別	利用駅	種別	利用駅	残額
0327	入	秋葉原	出	品川	*1180
0327	入	品川	出	秋葉原	*1340
0327					*1500

正しい手続き

タッチ!

仮パスワード発行

PASMO マイページ
仮パスワード
Hu7p#zA3

2015年4月1日
渋谷駅#0287

ICカード番号 + 仮パスワード で登録

ポイントカード



Tサイト登録によってネットで履歴を確認

あらゆる消費行動にポイントを付与 = 行動履歴範囲の拡大

T会員情報 Tカード(持っている)

Tカード番号: 0000422701735964
半角数字、16文字または9文字
[Tカード番号の確認方法](#)

下記の情報を登録します

- メール: scicafe_nagoya@yahoo.co
- 性別: 男性
- 生年月日: 19710417

利用規約の同意

Tポイントの付与を受けるには、カルチュア・コンビニエンスサービス利用規約及び、期間固定Tポイントサービス利用規約に入力いただいた情報は、CCCが取得します。ファミマTカード・T会員規約(CCC)及びポイントサービス利用規約(CCC)

同意する

登録

Tポイント履歴

反映日	利用日	ご利用内容詳細	内容	ポイント数
15/04/15	15/04/14	T S U T A Y A 池下店	貯める	5
15/04/15	15/04/14	ドラッグユタカ 池下店	貯める	1
15/04/14	15/04/13	ENEOS	貯める	9
15/04/16	15/04/13	ファミリーマート 塩付通	貯める	2

任意の Yahoo! Japan ID
 +
 ターゲットの {
 ・ Tカード番号
 ・ 生年月日

が分かれば、本人でなくとも登録可能 →
 ・ 本名
 ・ 住所
 ・ 電話場合 } ばれてしまう! →

ポイント履歴を閲覧
 = 生活行動履歴の漏洩