

# ワンタイムパスワードをすり抜ける 手口の紹介



盛岡情報ビジネス & デザイン専門学校

近藤 光 西川 聖 熊谷 颯人

# ネット不正送金の発生件数と被害金額



インターネットでの不正送金による被害が増加しています。

その一つの手口としてワンタイムパスワードをすり抜けることができるものが発生しています。

\* ワンタイムパスワードとは  
メールや SMS に送られてくる  
一回限り使えるパスワードのこと。  
仮に ID・パスワードが流出しても不正  
にログインされるのを防ぐ事ができる。

ネット不正送金発生件数と被害額

出典元

<https://www.nippon.com/ja/japan-data/h00695/>

## 手口の紹介

ある日、A 子さんがいつも利用している銀行からこんなメールが届きました。



盛序毘銀行からのお知らせ 受信トレイ x

To 自分 ▼

お客様の口座から不正と思われる送金を確認しました。

ログインの上お確かめください

<http://jyoblgln.com/home.php>

URL をクリックしたら、見慣れたログイン画面が表示され、A 子さんは、ID とパスワードを入力しました。



← → ↺ ▲ セキュリティ保護なし | jyoblglIn.com/index1.php

**ようこそ、ログインしてください。**

ID  password

[新規登録はこちらから](#)

事前に登録してあったメールアドレスにワンタイムパスワードが届き、

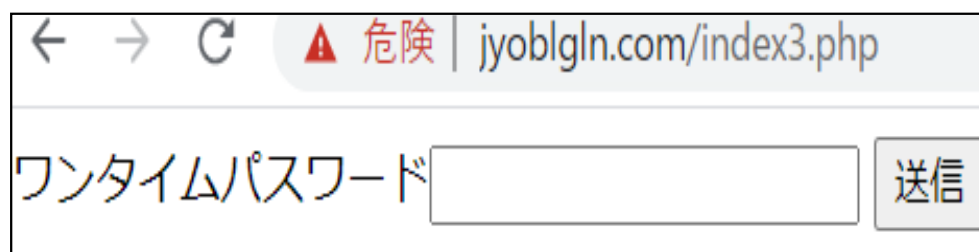


ワンタイムパスワード 受信トレイ ×

   
To 自分 ▾

🌐 英語 ▾ > 日本語 ▾ [メッセージを翻訳](#)

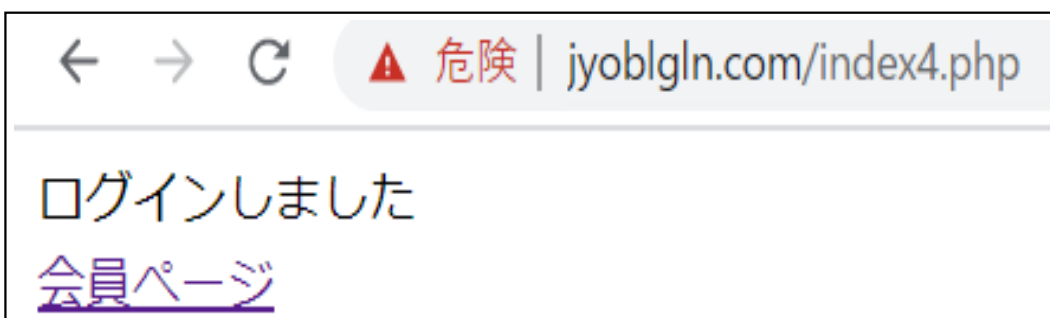
538300



← → ↺ ▲ 危険 | jyoblglIn.com/index3.php

ワンタイムパスワード

先ほどのワンタイムパスワードを入力して、ログイン成功しました。

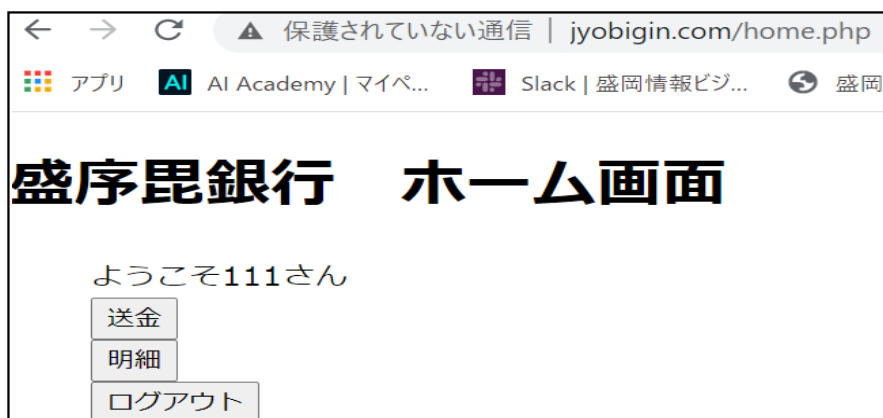


← → ↺ ▲ 危険 | jyoblglIn.com/index4.php

ログインしました

[会員ページ](#)

# しかし、その裏で



不正ログインされ勝手に  
送金されていたのです!!

Q. なぜ A 子さんは、不正ログインされてしまったか？

A. 先ほど入力していたサイトは、偽サイトだったからです。

A 子さんが入力した URL( **偽サイト** )

<http://jyoblglgn.com>

正規の URL

<https://jyobigin.com>

左の通り、正規サイトと偽サイトの  
URL は異なっている!!

偽サイトにID・パスワード・ワンタイムパスワードを入力しますと、攻撃者側のデータベースに格納されます。

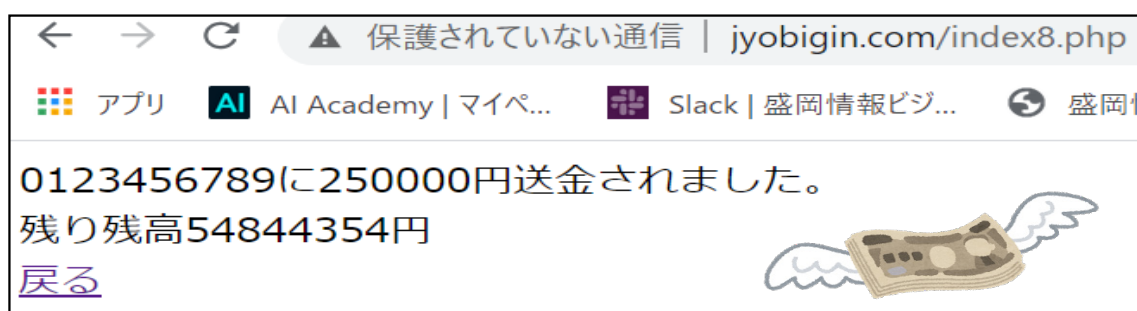
numid	id	password
2	111	k9551027k
3	111	k9551027k

numid	id	one
1	111	221130
2	111	538300

攻撃者は格納された情報を元に正規サイトに入力しログインします。

Q, 正規サイトに不正ログインされてしまうと、どのようなことが起きるのか？

A. アカウントの乗っ取りなどがあります。  
今回の場合は、下の画像の通り勝手にログインされ攻撃者の口座に送金されてしまいます。



\* 不正ログインされた際は、その会社に速やかに連絡してください

# 不正ログインをされないための対策



メールや SMS( ショートメッセージ ) でログインを促されても、メール内に記載されている URL をクリックしない。

心配の方は、普段利用しているWEBブラウザー(Google等)からアクセスしてください



自分が開こうとしている URL アドレスを確認する。

企業名やサービス名のつづりが間違っているときや余分な文字が入っているときは、偽サイトの可能性が高いので**注意**！！

例

本物

偽物

apple.com → app1e.com

amazon.com → amozon.com



SSL 通信で暗号化しているか確認

URL の最初が「**https**」から始まるものやアドレスバーに鍵マークが付いているか確認する！！

\* 最近では、偽物でも SSL 通信を用いているので過信はしない



セキュリティ対策ソフトをインストールしておく

フィッシング詐欺に対応するセキュリティソフトをインストールして、常に最新の状態にしておくことで被害に遭う危険性を低くすることができます。