

ドメイン名のテイクダウンを考える

2021年1月28日

JANOG47 Day2

長崎県立大学 岡田 雅之

自己紹介

研究情報詳細

氏名

岡田 雅之 (オカダ マサユキ)
MASAYUKI OKADA

所属

情報システム学部 情報セキュリティ学科

職名

教授



学外略歴

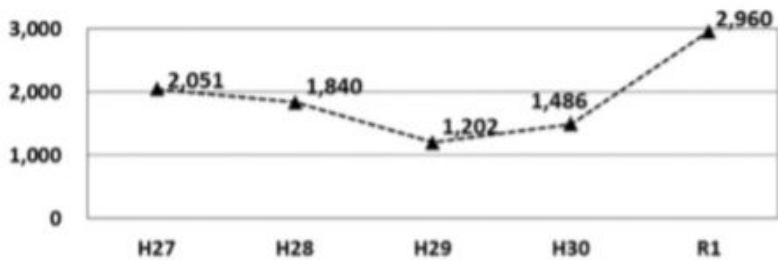
1. 東邦大学 理学部 非常勤講師 暗号と情報セキュリティ 非常勤 2018年9月 ～ (継続中)
2. 東邦大学 理学部 訪問研究員(金岡研究室) 非常勤 2016年10月 ～ (継続中)
3. 一般社団法人日本ネットワークインフォメーションセンター(JPNIC) 技術部 課長 常勤 2014年6月 ～ 2020年3月
4. 一般社団法人日本ネットワークインフォメーションセンター(JPNIC) 技術部 常勤 2004年2月 ～ 2016年5月

昨年、不正アクセスの認知件数は急増

- 2019年(令和元年)の不正アクセスの認知件数は、2,960件と前年の約2倍に増加
- 内訳を見ると、インターネットバンキングでの不正送金等が1,808件と半数以上を占める。
- 不正送金は、金銭を目的として、組織的かつ計画的に行われている。

想定を超える事態を常に意識しないといけないかもしれません。

図 1-1 過去5年の不正アクセス行為の認知件数の推移



不正アクセス行為の発生状況 出典：警察庁

表 1-3 過去5年の不正アクセス後の行為別認知件数

区分	平成27年	平成28年	平成29年	平成30年	令和元年
インターネットバンキングでの不正送金等	1,531	1,305	442	330	1,808
インターネットショッピングでの不正購入	167	172	133	149	376
メールの盗み見等の情報の不正入手	92	91	146	385	329
オンラインゲーム・コミュニティサイトの不正操作	96	124	83	199	60
インターネット・オークションの不正操作	20	34	28	29	47
知人になりすましての情報発信	83	25	110	24	30
仮想通貨交換業者等での不正送信			149	169	22
ウェブサイトの改ざん・消去	34	6	14	13	19
その他	28	83	97	188	269
計(件)	2,051	1,840	1,202	1,486	2,960

※ 平成28年以前は、「仮想通貨交換業者等での不正送信」を分類して集計していない。

脆弱性をつきフィッシングが行われる。

フィッシングメールの内容	フィッシングサイト	窃取する資格情報
VPNの設定変更の通知	Office365のログインページ	Office365
Zoomの会議に関する通知	Zoomのログインページ	社用のメールアドレス
Microsoft Teams上の会話に関する通知	Office365のログインページ	Office365
Webexの証明書に関するエラー通知	Webexのログインページ	Webex

<https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/091101/091101-01.pdf>より

※タイムラインに記載している日付は
事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

3月 4月 5月 6月

[F] メール

◆ CanadaPostを騙る

◆ Office365ボイスメールを悪用する

◆ CiscoのWebEXを装う

◇ JCBを騙る

◆ 企業の顧問弁護士を騙る

◇ ヨドバシカメラを騙る

◇ auを騙る

◇ マスク配布を騙る

◇ 特別定額給付金手続きを騙る

◇ マツモトキヨシを騙る

◇ 複数の配送業者を騙る

◇ NTTドコモを騙る

◆ 米労働省を騙る

◆ Zoomビデオ会議を装う

◆ 米FINRA職員を騙る

◆ BLMキャンペーンを装う

◇ 千葉銀行を騙る

◇ Amazonを騙る

◇ メルカリを騙る

◇ 楽天を騙る

◇ エボスカードを騙る

新型コロナウイルス関連

不正アクセスの入り口はフィッシングサイト

- 不正アクセスに利用される識別符号は、フィッシングサイトを介して被疑者に渡っているものが多い。
- フィッシングサイトは、正規のサイトと外見は同一である。
- ドメイン名からフィッシングサイトを見破ることはできるが、見破られないように利用権者を急かして焦らせる場合が多い。
- 多くの方は騙されないが、それでも少数の騙される方がいる限り、サイバー犯罪者はフィッシングサイトの構築をやめることはない。

The screenshot shows a web browser window with the address bar containing the URL `https://direct.smbc.co.jp/`, which is highlighted with a red rectangle. Below the address bar is the SMBC logo and the text "三井住友銀行" (Mitsubishi Sumitomo Bank). To the right is a button labeled "SMBC トップ" (SMBC Top). Below this is a green bar with the text "SMBCダイレクトログイン" (SMBC Direct Login).

Below the green bar is a red warning message in Japanese: "三井住友銀行 不正送金対策課の職員等を名乗り、パスワードカードを有効にする操作を促す不審な電話にご注意ください。【[くわしくはこちら](#)】" (Mitsubishi Sumitomo Bank, impersonating staff of the Anti-Fraud Unit, please be cautious of suspicious calls that urge you to activate your password card. [Click here for more details]).

The main content area is a light green box containing a login form. It has fields for "店番号" (Branch Number) and "口座番号" (Account Number), followed by a red button labeled "または" (or). Below that is a field for "契約者番号" (Contractor Number) followed by a hyphen and another field. At the bottom is a field for "第一暗証" (First PIN). Below the form is a green bar with the text "個人情報の利用目的" (Purpose of use of personal information) and a large green button labeled "ログイン" (Login) with a right arrow icon.

フィッシングサイトとは

①
実在する組織のホームページを模倣したもの。

見た目は、正規のホームページと同一で、URLも正規のURLに似せていることが多い。フリーの電子証明書を利用して、安全なサイトであるように見せかけているものもある。

②
利用者に対して、IDやパスワードの入力を要求する。

ref. 不正アクセス行為の禁止等に関する法律 第7条



三井住友銀行 不正送金対策課の職員等を名乗り、パスワードカードを有効にする操作を促す不審な電話にご注意ください。[「くわしくはこちら」](#)

フィッシングサイトの目的

フィッシングの目的は、

1. 経済的利益

2. 匿名化

3. 自己満足

フィッシングが成立する最大の原因は、利用者の誤認識。
(フィッシングサイトを**正規のサイトであると誤って判断**してしまう)

ref.

semantic attacks

どちらが本物でしょう？

トレードブローカー オンライン - Microsoft Internet Explorer

ファイル 編集 表示 お気に入り ツール ヘルプ

https://www.tradebrokeronline.com/jp

トレードブローカー オンライン

トレードブローカー オンライン

取引および投資 相場時価および調査 リタイアメント計画 銀行取引および融資

取引 マイアカウント 相場時価 注文履歴 時間外取引 IPO センター

株式 オプション 投資信託 債券 お客様向けサービス 残高

アカウント: 223-5213-6343-01 [オープン注文](#)

注文の種類:

株数:

略号:

価格の種類:

期限:

システムの応答時間やアカウントのアクセス時間は、取引量、市況、システムのパフォーマンスなどさまざまな要因によって左右されます。

(株)トレードブローカーオンラインには、成り行き注文、一括注文、および薄賣い市場で取引される証券の注文を拒否する権利があります。

[詳細はこちら。](#)

現金残高: 900,000.00 円
信用取引残高: 209,027.70 円
コール市場残高: 2,311,479.00 円
元手資金の現金取引: 900,000.00 円
元手資金の信用取引: 209,027.70 円

相場時価

日経平均株価 10,257.56 +18.91 +0.18%
ジャスダック 48.79 -0.11 -0.22%
TOPIX 900.95 -3.16 -0.35%

市場データは、少なくとも 20 分は遅れています。
[市場情報の詳細](#)

[お問い合わせ](#) | [サイトマップ](#) | [プライバシーおよびセキュリティ](#) | [トレードブローカー オンラインについて](#) | [沿革](#) | [提携方針](#)

© 2005 TradeBroker Online, Inc. All rights reserved.
株式会社トレードブローカーオンライン 金融商品取引業者 関東財務局長(金商)第123456号

インターネット

トレードブローカー オンライン - Microsoft Internet Explorer

ファイル 編集 表示 お気に入り ツール ヘルプ

http://www.tradebrokeronline.com/jp

トレードブローカー オンライン

トレードブローカー オンライン

取引および投資 相場時価および調査 リタイアメント計画 銀行取引および融資

取引 マイアカウント 相場時価 注文履歴 時間外取引 IPO センター

株式 オプション 投資信託 債券 お客様向けサービス 残高

アカウント: 223-5213-6343-01 [オープン注文](#)

注文の種類:

株数:

略号:

価格の種類:

期限:

システムの応答時間やアカウントのアクセス時間は、取引量、市況、システムのパフォーマンスなどさまざまな要因によって左右されます。

(株)トレードブローカーオンラインには、成り行き注文、一括注文、および薄賣い市場で取引される証券の注文を拒否する権利があります。

[詳細はこちら。](#)

現金残高: 900,000.00 円
信用取引残高: 209,027.70 円
コール市場残高: 2,311,479.00 円
元手資金の現金取引: 900,000.00 円
元手資金の信用取引: 209,027.70 円

相場時価

日経平均株価 10,257.56 +18.91 +0.18%
ジャスダック 48.79 -0.11 -0.22%
TOPIX 900.95 -3.16 -0.35%

市場データは、少なくとも 20 分は遅れています。
[市場情報の詳細](#)

[お問い合わせ](#) | [サイトマップ](#) | [プライバシーおよびセキュリティ](#) | [トレードブローカー オンラインについて](#) | [沿革](#) | [提携方針](#)

© 2005 TradeBroker Online, Inc. All rights reserved.
株式会社トレードブローカーオンライン 金融商品取引業者 関東財務局長(金商)第123456号

インターネット

どちらが本物？

direct.jp-bank.japanpost.jp/ikf.cn.com/tp1web/U016101SCK.htm

Google Map RAKUTEN Web Mail Hulu Movies PhotoGet MovieGet Twitter Facebook

ゆうちょダイレクト | ログイン (お客さま番号入力)

ゆうちょダイレクト

新規登録のご案内

ログイン (お客さま番号入力)



ご注意ください!

トークンに表示されるワンタイムパスワードは以下のお取り引きの確認画面でのみ使用します。

ゆうちょ銀行あて振替

他金融機関あて振込

WEB連動振替決済サービス

税金・各種料金の払込み

トークンの利用登録

トークンの時刻の同期

これらのお取り引きの確認画面以外でワンタイムパスワードの入力を求められた場合は、コンピュータウイルスによる不正な画面表示が行われている可能性がありますので、絶対に入力しないでください。

お客さま番号を入力し、「次へ」をクリックしてください。
お客さま番号を忘れた場合には？
[照会・再発行・初期化の手続き](#)

(半角数字)

お客さま番号 - -

お客さま番号は、[4桁](#)・[4桁](#)・[5桁](#)と区切って半角で入力してください。



お客さまの財産を守るためPhishWallをご利用ください ([詳細はこちら](#))



ゆうちょダイレクトを狙った犯罪にご注意ください ([詳細はこちら](#))

[新規登録のご案内はこちら](#)

ホームへ

ご利用上の注意

- ブラウザの「戻る」「進む」ボタンは使用しないでください。
ゆうちょダイレクトの画面上のボタンで操作してください。

お知らせ

- ゆうちょダイレクトを狙った犯罪にご注意ください ([詳細はこちら](#))

【お客さまに実施していただきたいセキュリティ対策】

- トークンのご利用 ([詳細はこちら](#))
- 不正送金対策ソフト「Phish Wallプレミアム」のご利用 (無料)
- OSやインストールしているソフト等は常に最新の状態で使用
- メーカーのサポート期限が経過したOSやソフト等は使用しない
- ウイルス対策ソフトの導入および最新の状態への更新
- 取扱確認メールなどの送付先に携帯電話・スマートフォンのメールアドレスを登録 ([詳細はこちら](#))
- ※フリーメールなどブラウザ上でパスワード等を入力し、メールの開覧が可能なメールアドレスのご登録はお控えください。

JAPAN POST BANK Co., Ltd. direct.jp-bank.japanpost.jp/tp1web

Google Map RAKUTEN Web Mail Hulu Movies PhotoGet MovieGet Twitter Facebook

ゆうちょダイレクト | ログイン (お客さま番号入力)

ゆうちょダイレクト

新規登録のご案内

ログイン (お客さま番号入力)



ご注意ください!

トークンに表示されるワンタイムパスワードは以下のお取り引きの確認画面でのみ使用します。

ゆうちょ銀行あて振替

他金融機関あて振込

WEB連動振替決済サービス

税金・各種料金の払込み

トークンの利用登録

トークンの時刻の同期

これらのお取り引きの確認画面以外でワンタイムパスワードの入力を求められた場合は、コンピュータウイルスによる不正な画面表示が行われている可能性がありますので、絶対に入力しないでください。

お客さま番号を入力し、「次へ」をクリックしてください。
お客さま番号を忘れた場合には？
[照会・再発行・初期化の手続き](#)

(半角数字)

お客さま番号 - -

お客さま番号は、[4桁](#)・[4桁](#)・[5桁](#)と区切って半角で入力してください。



お客さまの財産を守るためPhishWallをご利用ください ([詳細はこちら](#))



ゆうちょダイレクトを狙った犯罪にご注意ください ([詳細はこちら](#))

[新規登録のご案内はこちら](#)

ホームへ

ご利用上の注意

- ブラウザの「戻る」「進む」ボタンは使用しないでください。
ゆうちょダイレクトの画面上のボタンで操作してください。

お知らせ

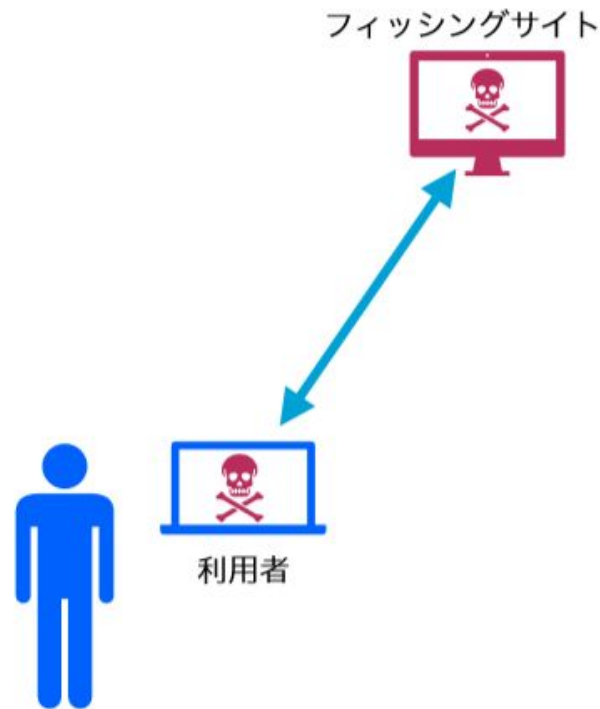
- ゆうちょダイレクトを狙った犯罪にご注意ください ([詳細はこちら](#))

【お客さまに実施していただきたいセキュリティ対策】

- トークンのご利用 ([詳細はこちら](#))
- 不正送金対策ソフト「Phish Wallプレミアム」のご利用 (無料)
- OSやインストールしているソフト等は常に最新の状態で使用
- メーカーのサポート期限が経過したOSやソフト等は使用しない
- ウイルス対策ソフトの導入および最新の状態への更新
- 取扱確認メールなどの送付先に携帯電話・スマートフォンのメールアドレスを登録 ([詳細はこちら](#))
- ※フリーメールなどブラウザ上でパスワード等を入力し、メールの開覧が可能なメールアドレスのご登録はお控えください。

考えられるフィッシング対策の候補

- ・ ユーザーの知識や環境に左右されないフィッシング対策として、フィッシングサイトを閉鎖する、フィッシングサイトをネットワーク上で遮断する、の2通りが考えられる。
- ・ 海外に設置されているフィッシングサイトを閉鎖させるのは現実的には困難である。
- ・ また、フィッシングサイトは次から次に新しく作成されるため、即効性のある対策が求められる。
- ・ ネットワーク上におけるフィッシングサイトの遮断の方が実現可能性は高い と考えるひともいるが様々な課題があり悪手。



思いつく対策といたちごっこの例

- 悪いサイトのドメイン名をWHOISで引いてTake Down
 - GDPRの影響などでWHOISの情報はどんどん隠蔽
 - フィッシングサイトの寿命は2時間程度と短命
- ドメイン名のレジストラで対応してもらえれば？
 - 悪い人御用達のレジストラが存在しそう
 - 完全匿名でドメイン名を運用可能か？
 - 本人確認 なし！
 - 課金 匿名決済OK!
 - 連絡先 到達しなくてもスルー
 - 結果としてコンタクト不能
- フィッシングのサイトはID/PASSがでたらめでもログインできるので試す？
 - フィッシングメールに偽サイトの ID/PASSがつけられるようになりました

脱法？レジストラの例

- お金さえ支払えば、個人情報
の収集、本人確認はほぼスルー
- でも決済から足跡がつくのでは？



WhoisGuard Privacy Protection is now free – forever!

WhoisGuard by Namecheap is a service that offers **privacy protection for your domain, keeping your sensitive data safe**. Because your data is as important to us as it is to you.

When you **register a domain**, ICANN requires registrars to provide them with your contact information (such as name, email, address, and phone number). This is then added to the Whois database. This database lists the owners of every domain name online, and it can be searched by anyone on the Internet.

WhoisGuard hides this information from spammers, marketing firms, and online fraudsters. Instead, the Whois database will display generic WhoisGuard contact information. It's the best global domain privacy option you'll find anywhere — guaranteed. **Because at Namecheap, we care about your privacy protection.**

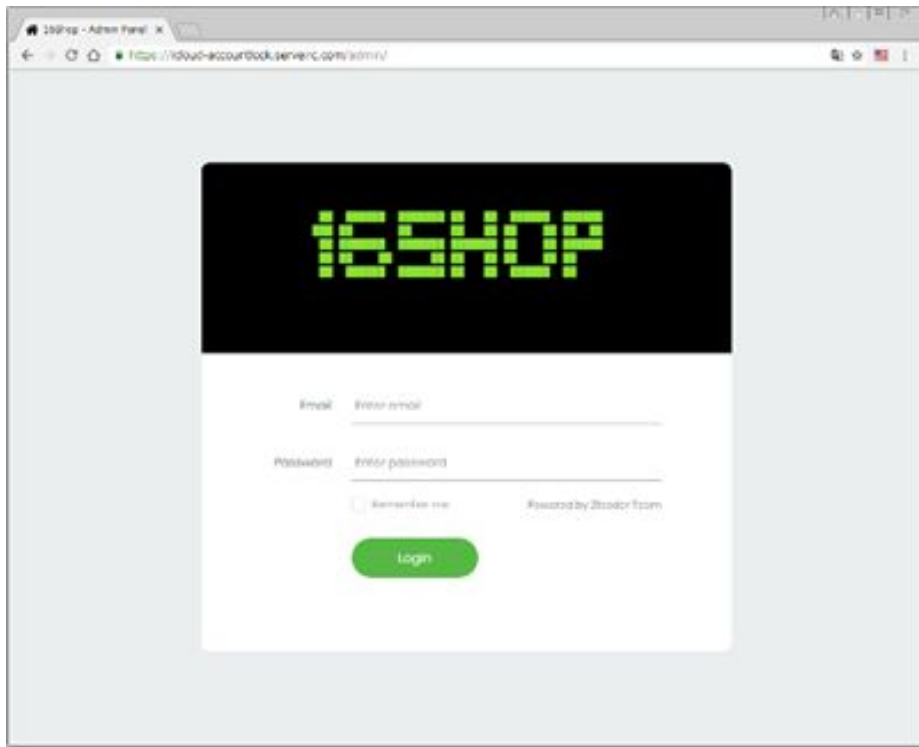
決済情報からの追跡は？

- プリペイド事前決済カードなどの利用も可能
- ほぼ本人確認は不可能
- （プリペイド決済について問題があると述べているわけではありません）



と対策を考えてもなかなかいたちごっこな状態

Phishing as a Service ?



DASHボード

16SHOP

 Statistic

 Antibot Setting

 List Visitor

 Bot Detected

 Reset Statistic

 Logout

Statistic

0

CLICKS

0

LOGIN

0

EMAIL LOGIN

0

BANK LOGIN

0

CREDIT CARD

0

VBV

0

UPLOAD PHOTO

0

BOT DETECTED

Credit Card (0)

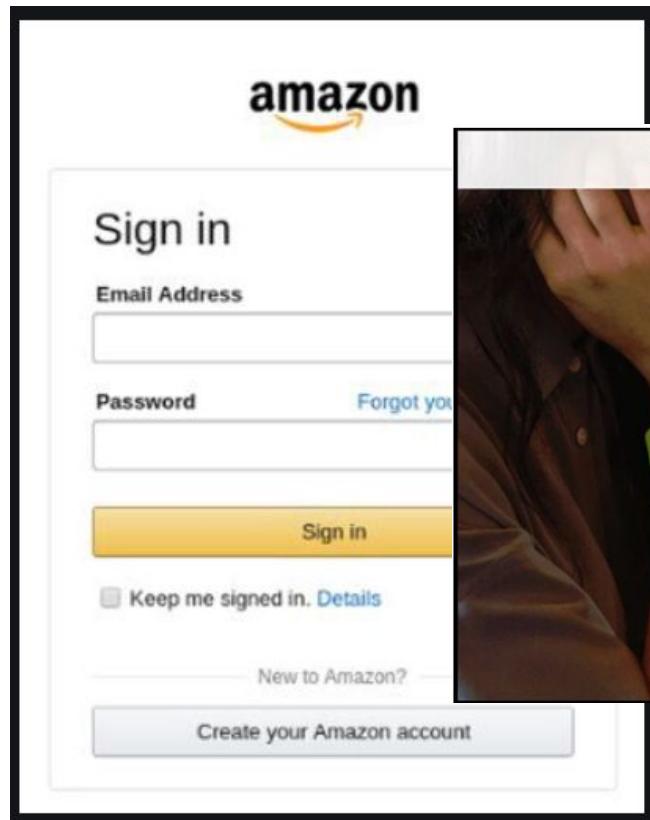
Country

BIN

Device

Not found

これはどちらも16SHOPが生成したサイト



The image shows a screenshot of the Amazon sign-in page. At the top, the Amazon logo is displayed. Below it, the text "Sign in" is prominently shown. Underneath, there are input fields for "Email Address" and "Password". A yellow "Sign in" button is positioned below the password field. To the right of the password field, there is a link that says "Forgot your password?". Below the sign-in button, there is a checkbox labeled "Keep me signed in." followed by a link "Details". At the bottom, there is a link "New to Amazon?" and a button labeled "Create your Amazon account".



というわけで、

- フィッシングサイトなどの悪性サイトの対策は最終的にはテイクダウンしない
- しかしながら、お願いベースの停止依頼はなかなか有効でない
- このような現状でテイクダウンはどうやって行われているのか？

佐々木さんよろしくおねがいします。