

フィッシングメールの追跡

第12回サイバーセキュリティ勉強会2025冬 in 塩尻

株式会社ラック
サイバー・グリッド・ジャパン
次世代セキュリティ技術研究所
井上圭



井上 圭



株式会社ラック
サイバー・グリッド・ジャパン
次世代セキュリティ技術研究所
兼 サイバーセキュリティプラットフォーム開発統括部 企画

非IT企業情報システム部、MSP（Managed Service Provider）、セキュリティコンサルタントなどを経験し、2024年07月にラックに入社。脆弱性管理やセキュリティ運用について研究や講演を行い確かなテクノロジーで「信じられる社会」を目指す。

最近の発表

- CodeBlue 2022 Open Talks
- Janog 52 (CFP)
- Internet Week 2023
- NCA Annual Conference 2023 (CFP)
- OWASP Nagoya Chapter/OWASP 758 Day
- Hardening Designers Conference 2024 Session4
- Internet Week 2024 (BoF)
- NCA Annual Conference 2024 (CFP)
- OWASP Kansai 基調講演
- 総関西サイバーセキュリティLT大会
- 塩尻サイバーセキュリティ勉強会
- 他

参加団体

- 日本ネットワークセキュリティ協会 (JNSA)
 - 社会活動部会
 - 教育部会
- 日本セキュリティオペレーション事業者協議会 (ISOG-J)
 - WG1 “脆弱性トリアージガイドライン作成のための手引き”
 - WG6 “セキュリティ対応組織の教科書”
- 日本シーサート協議会 (NCA)
 - インシデント対応訓練WG
 - 脆弱性管理WG
- セキュリティトランスペアレンシーコンソーシアム (STコンソーシアム)
- 他

TLPは「TRAFFIC LIGHT PROTOCOL」の略称です。

- 機密となりうる情報の広範囲な共有と効果的な連携を促進するために作られたもの
- 機密となりうる情報の共有先を、直感的に示す仕組みを提供
- 詳細は FIRSTのページ <https://first.org/tlp/> を参照（日本語フォーマット有）

情報の共有範囲として、おおよそ以下のように定義されています。

- **TLP:RED**
 - 受信者個人の目と耳に向けた共有に限られ、その先の公開はない
- **TLP:AMBER**
 - 限定公開、Need to knowの原則に基づき組織内等にのみ共有できる
- **TLP:GREEN**
 - 限定公開、コミュニティ内に情報を共有できる
- **TLP:CLEAR**
 - 公開に制限はなく、全世界に向けて情報を共有できる

今回はここに該当し、
サイバーセキュリティの
コミュニティ内では共有可

Agenda

1. フィッシングメールについて
2. 2024/09から2025/01までの状況
3. アクセスするとどうなるのか
4. まとめ

Appendix

01 フィッシングメールについて

近年、フィッシングメールによる被害が増えています。被害を防ぐ/警戒するためには、現状を認識する必要があります。

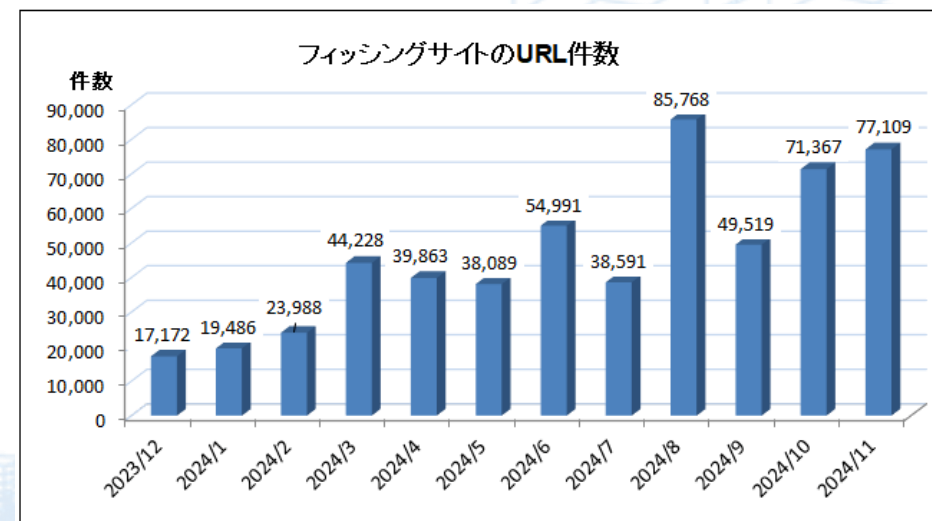
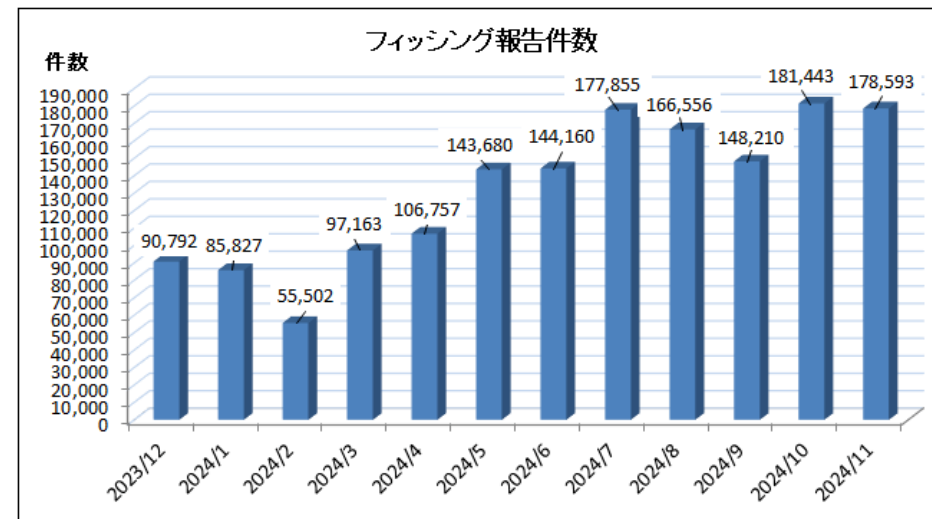
本講演では以下についてお話しすることで、被害の低減ができるようになると思います。

- 直近半年程度での状況で、傾向を理解する
- 実際のアクセスを基に、途中で気付ける

「フィッシング」とは

フィッシング（phishing）とは、実在する組織を騙って、ユーザネーム、パスワード、アカウントID、ATMの暗証番号、クレジットカード番号といった個人情報を搾取する事です。

-- フィッシング協議会:よくあるご質問/お問い合わせ https://www.antiphishing.jp/contact_faq.html



フィッシング対策協議会:「2024/11 フィッシング報告状況」より引用
<https://www.antiphishing.jp/report/monthly/202411.html>

フィッシング対策協議会が、2024/11分としてまとめた報告書があります。
これを少しまとめてみました。

- <https://www.antiphishing.jp/report/monthly/202411.html> (2024-12-16提供)
 - ドメインでのフィルタリング/テイクダウンは有効
 - DMARKは実在ドメインのなりすましには有効

騙られるブランド

- Amazon
- JCB
- マスターカード
- えきねっと
- PayPay
- 東京電力エナジーパートナー
- ...

フィッシングサイトのURL

- ランダムサブドメインを付与した使い捨てURL
- .comが42.5%
.cnが36.4%
.coが1.8%...
- 報告回数100回以上のドメイン名は240ドメイン、URL件数では全体の約45.3%を締め、ドメインでのフィルタやテイクダウンが効果的

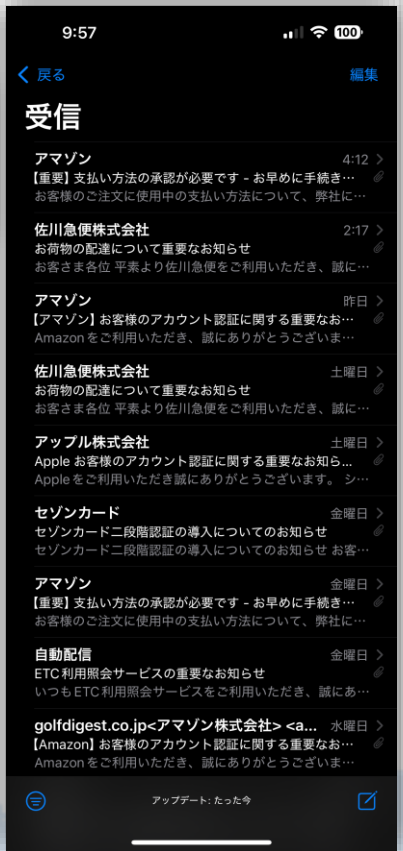
送信ドメイン認証技術：DMARK

- 実在するサービスのメールアドレス（ドメイン）を使用したなりすましを軽減できる
- ポリシーがreject/quarantineでフィルタ可能なものは38.5%
- 独自ドメイン名による”非なりすましメール”はDMARCに対応して認証成功したメールは43.2%であり、DMARKだけではフィッシングを防げない

02 2024/09から2025/01までの状況

私の持っている調査用メールアドレスに届いたフィッシングメールについて、約半年分の状況を共有します。

- ソフトバンクのドメイン (i.softbank.jp) に2024/08頃から、フィッシングとして定型的なメールが多数届き始めた
- iPhoneの「メール」アプリでしかメールを確認できず詳細が見れなかった
- 2024/12頃に、IMAPで接続ができることを知り、Thunderbirdで確認することができるようになった。



受信トレイ		メッセージ 937 通		🏠 クイック	
📧	🔖	📧	📧	📧	📧
件名	📧	通信相手	📧	📧	送信日時
【重要】支払い方法の...	📧	アマゾン <maru2@stockpoint.co.jp>	📧	📧	4:12
お荷物の配達について...	📧	佐川急便株式会社 <kohata@point.recruit.co.jp>	📧	📧	2:17
【アマゾン】お客様のアカ...	📧	アマゾン <darcie.eleanor@gtba.net>	📧	📧	2025/01/12 11:54
お荷物の配達について...	📧	佐川急便株式会社 <s-k@email.thegoodguys.com.au>	📧	📧	2025/01/11 19:54
Apple お客様のアカウン...	📧	アップル株式会社 <edward.finley@info-recruit-card.jp>	📧	📧	2025/01/11 2:03
セゾンカード二段階認証...	📧	セゾンカード <denka@email.thegoodguys.com.au>	📧	📧	2025/01/10 21:06
【重要】支払い方法の...	📧	アマゾン <gifu.1@eztw.net>	📧	📧	2025/01/10 20:06
ETC利用照会サービスの...	📧	自動配信 <t1pxg3nd906dyu@email.thegoodguys.com.au>	📧	📧	2025/01/10 12:18
【Amazon】お客様のア...	📧	golfdigest.co.jp <アマゾン株式会社> <amyronnie@golfdigest.co.jp>	📧	📧	2025/01/08 14:05
【重要】支払い方法の...	📧	アマゾン <with55n9@email.thegoodguys.com.au>	📧	📧	2025/01/08 7:40
ETC利用照会サービスの...	📧	自動配信 <s-business@bons.com>	📧	📧	2025/01/08 2:38
【ヤマト運輸】お荷物の...	📧	【ヤマト運輸】株式会社自動配信メール <luca.joshua@golfdigest.co.jp>	📧	📧	2025/01/07 9:16
【重要】支払い方法の...	📧	アマゾン <kawaraji3@llof.com>	📧	📧	2025/01/07 1:53
【Amazon】お客様のア...	📧	アマゾン株式会社自動配信メール <rose.riley@hotpepper.jp>	📧	📧	2025/01/06 21:41
【Amazon】お客様のア...	📧	アマゾン株式会社自動配信メール <eleanor.ryan@aqmb.com>	📧	📧	2025/01/06 10:32
ETC利用照会サービスの...	📧	自動配信 <yotominag@godg.com>	📧	📧	2025/01/06 9:20
お荷物の配達について...	📧	佐川急便株式会社 <seraph.e-hip@raxh.com>	📧	📧	2025/01/06 5:36
【ヤマト運輸】お荷物の...	📧	ヤマト運輸株式会社自動配信メール <megan.maisie@ahxj.com>	📧	📧	2025/01/06 3:25
お荷物の配達について...	📧	佐川急便株式会社 <junichi.saito@hlcc.com>	📧	📧	2025/01/05 8:26
お荷物の配達について...	📧	佐川急便株式会社 <h.suzuki8631@wxd.com>	📧	📧	2025/01/05 5:40
請求書番号：963未...	📧	東京電力エナジーパートナー株式会社 <florence.max@iipi.net>	📧	📧	2025/01/05 3:15
お荷物の配達について...	📧	佐川急便株式会社 <uchikawa@ahll.com>	📧	📧	2025/01/05 0:54
【三井住友カード】不正...	📧	三井住友銀行 <jacob.emma@research.ponta.jp>	📧	📧	2025/01/04 9:04
お荷物の配達について...	📧	佐川急便株式会社 <sinya.yoneta@hlqp.com>	📧	📧	2025/01/04 7:49
マスターカード認証通知	📧	マスターカード <amin@clax.com>	📧	📧	2025/01/04 1:54
【ヤマト運輸】お荷物の...	📧	【ヤマト運輸】 <louis.ella@stockpoint.co.jp>	📧	📧	2025/01/03 11:23
e-Tax税務署からの【未...	📧	国税庁 <kobun-of-takei@fcigp.com>	📧	📧	2025/01/03 1:22
Apple お客様のアカウン...	📧	アップル <joseph.maisie@o2.pl>	📧	📧	2025/01/02 19:09
【当選】冬のボーナスBIG...	📧	日本宝くじ振込窓口 <painstaking@impugn.com>	📧	📧	2024/12/30 20:15
【Amazon】お客様のア...	📧	アマゾン <alfie.samuel@fc2.xxx>	📧	📧	2024/12/30 19:53
ソフトバンクご利用のお...	📧	mailmagazine@byron-lambeth.com	📧	📧	2024/12/30 16:33
請求書番号：327未...	📧	東京電力エナジーパートナー <louis.thomas@zdgo.com>	📧	📧	2024/12/29 8:33
e-Tax税務署からの【未...	📧	国税庁 <watjszq@propertyagent.co.jp>	📧	📧	2024/12/21 17:47

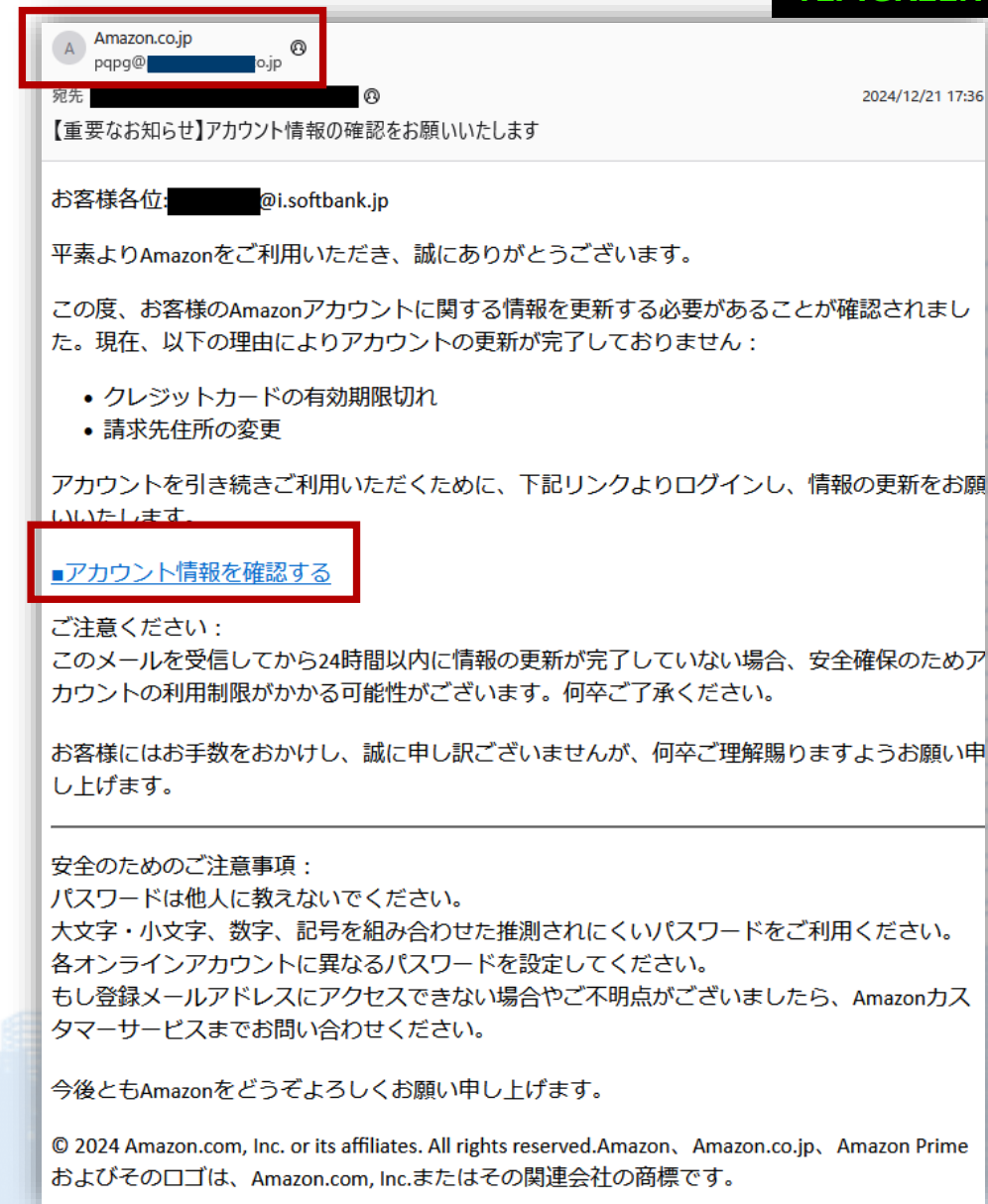
03 アクセスするとどうなるのか

今回は、調査用アドレスに届いた特定のメールについて、実際にアクセスするとどうなるかを紹介します。

- Amazonを騙るメール **騙られた被害組織です**
 - 送信元ドメインは[redacted]社を騙る
 - 表示名はAmazon.co.jpを騙る
- アカウント更新が完了しない、として入力を促す
 - カード情報などを入力させる

尚、スクリーンショットはFirefox/PCで取得していますが、i.softbank.jpへのメールであるため、通常はiPhoneの「メール」アプリでしか見れません。

- その場でメールソースなどは見れない
- 送信者のアドレスを見るのにも、ひと手間必要



メールのソースを見ると、以下のようです。

- ドメインを騙ったメールサーバが、直接送信する
- Sender, Return-Pathも当該ドメインを騙る
- DMARCはfailしている
- List-Unsubscribe等、スパムと判定されないような設定は行われている

ドメインを騙った
メールサーバ

騙られた会社は日本の会社だが、CHINANET-JSのIPアドレスでのメール送信

i.softbank.jpな
メールサーバ

DMARCでfailと判定

- From: "Amazon.co.jp"<騙られたドメイン>
- 騙られたドメインのメールサーバIPとは異なる

```
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: <pqpg@[REDACTED].co.jp>
Received: from ebmky104sc.i.softbank.jp ([172.27.13.110])
  by dimky106sc.i.softbank.jp with ESMTP
  id <20241221083552886.UHUD.28573.dimky106sc.i.softbank.jp@dimky106sb.mailsv.softbank.jp>
  for <hogehuga@i.softbank.jp>; Sat, 21 Dec 2024 17:35:52 +0900
Received: from [REDACTED].co.jp ([121.232.178.16])
  by ebmky104sc.i.softbank.jp with ESMTP
  id <20241221083552681.WFJN.15855.ebmky104sc.i.softbank.jp@ebmky104sb.mailsv.softbank.jp>
  for <[REDACTED]@i.softbank.jp>; Sat, 21 Dec 2024 17:35:52 +0900
ARC-Seal: i=1; cv=none; a=rsa-sha256; d=i.softbank.jp; s=isoftbank202401; t=1734770152;
  b=ITn6TALr40qND10QORfM/ZzWtLnBiPRaatz8WIV8D9JUBXhXvJe42mGcvxFgoxv50zskCgvvScvxgck7rSyjmZBeW/186sJv
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=i.softbank.jp; s=isoftbank202401; t=173
  bh=6GKuL0c0wNdTCJ5dMtkj2zDQ+HninFn5sJH8hAJpg=;
  h=Message-ID:From:To:Date:MIME-Version;
  b=ZWtY3AJnadGewlp+YYSaUM+vxdwQh+TVQgkkCyp4SjYsel7kB8w/xIG7WznUTnFfiMbKtiizLpm5L36kX0w5Qek3qzu
ARC-Authentication-Results: i=1; i.softbank.jp;
  dmarc=fail header.from=[REDACTED].co.jp;
  dkim=none;
  spf=permerror smtp.helo=[REDACTED].co.jp;
  spf=permerror smtp.mailfrom=[REDACTED].co.jp;
  arc=none smtp.client-ip=121.232.178.16
X-SMGAf: 32 32 02 31 -1 674052196751B994-674052196751BC7C 22 99 -1 -1
sender=pqpg@propertyagent.co.jp
Message-ID: <ad525f5b7ed06611b3ef27c92038e57d@propertyagent.co.jp>
Sender: <pqpg@[REDACTED].co.jp>
From: "Amazon.co.jp" <pqpg@[REDACTED].co.jp>
To: [REDACTED] <[REDACTED]@i.softbank.jp>
Subject: =?utf-8?B?44Q06YeN6KaB44G44GK55+I44KJ44Gb44CR44Ki44K44Km=?
  =?utf-8?B?44Oz44O15o0F5aCx44Gu56K66KqN44KS44GK6aGY44GE44GE44Gf44GX=?
  =?utf-8?B?44G+44GZ=?
Date: Sat, 21 Dec 2024 16:36:30 +0800
X-Mailer: gsbtl.62615.712
MIME-Version: 1.0
Content-Type: text/html;
  charset="utf-8"
Content-Transfer-Encoding: quoted-printable
List-Unsubscribe: <mailto:pqpg@[REDACTED].co.jp?subject=unsubscribe>

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">=0D=0A<HTML><=
HEAD>=0D=0A<META content=3D"text/html; charset=3Dutf-8" http-equiv=3DContent=
t-Type>=0D=0A<META name=3DGENERATOR content=3D"MSHTML 11.00.9600.20671"><st=
yle>=0D=0A#Kvype-XpI #aGZZzbj -0aJpkrvXY-wdv #tJyTbbPu-kRFgl-tYFCvgH #YHvTQh=
a-gFPDcBMkp-aAQQMwceQy #pHoguubB-RQQ {=0D=0Aanimation-name:none;=0D=0Aanima=
```


ビジネスメール詐欺（BEC）などの対策として、メール認証技術が複数あります。

- SPF

- Sender Policy Framework
- 正規のサーバー(IPアドレス)から送信されたかを、DNSのSPFレコードをもとに検証

example.com IN TXT vspf1 ip4:203.0.113.1 -all
☞ example.comのメールは203.0.113.1から送信されたもののみを許可する

- DKIM

- Domain Keys Identified Mail
- 電子証明を付与し、送信元メールアドレスの正当性を検証

メールサーバで電子署名をし、DNS経由で検証する

- DMARC

- Domain-based Message Authentication Reporting & Conformance
- SPFとDKIMの認証結果を基に、メールを検証

SPFとDKIMを用いてメールを判定/処理する

どれも効果は高いといえるが、設定の維持やSPF/DKIMに正しく対応していないサーバのメールを拒否してしまう可能性などがあり、設定すればよいというわけでもない。

リンク先URLは以下のようにになっています

```
https://amazon.gfeqqd.com%E2%88%95lkrosb%E2%88%95voavtyenu%E2%88%95zjmbyd@lmrkthaisg. [redacted].com/caonima=wzuicwjoe.co.jp/
```

これをUnicodeとしてみると

```
https://amazon.gfeqqd.com/lkrosb/voavtyenu/zjmbyd@lmrkthaisg. [redacted].com/caonima=wzuicwjoe.co.jp/
```

のように見えて amazon¥.gfeqqd¥.comへのアクセスに見えますが、実際は

- / : 一般的に使われるスラッシュ (U+002F:SOLIDUS) で、URLの分割に使う文字
- / : 上記に似た文字 (U+2215:DIVISION SLASH) で、URL分割には使用しない文字が異なっており、“/ (所謂slash) のように見える別の文字”であるため、

```
https://amazon.gfeqqd.com%E2%88%95lkrosb%E2%88%95voavtyenu%E2%88%95zjmbyd@lmrkthaisg¥. [redacted]¥.com
```

認証情報

アクセス先

という構成になっています。@迄がユーザ名扱いの為、表示されないことが多いです。

故に、マウスオーバー等でリンク先を見分けることは困難です。

Cloudflareを利用した認証をしているように見せかける画面にリダイレクトされます。

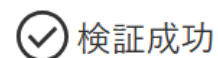
- 自動的に遷移していきます。
- 正規のCloudflareを使っている訳ではありません。

www.amazon.co.jp

あなたが人間であることを確認します。これには数秒かかる場合があります。



www.amazon.co.jp では、続行する前に接続のセキュリティを確認する必要があります。



www.amazon.co.jp からの応答を待っています...

Ray ID: 871984d0388a7372

Cloudflare によるパフォーマンスとセキュリティ

Amazon.co.jpのログイン画面らしきものに、リダイレクトされていきます。

この時点で十分怪しいドメインアクセスになっています。

https://[REDACTED].asia/ASJkejqkjc31122SEwca/?m=000&t=000&ip=2400:4051:[REDACTED]:3232&language=en-US,en;q=0.5&d=000

Shodan Maps Images Monitor Developer More

SHODAN

Singapore

Q

Login

176

[Regular View](#) |
 [Raw Data](#)

// TAGS: database ec2-product

General Information

Country	Singapore
City	Singapore
Organization	Asia Pacific Network Information Center, Pty. Ltd.
ISP	Tencent Building, Kejizhongyi Avenue
ASN	AS132203

Open Ports

22

80

123

443

3306

6379


8001

// 22 / TCP

180953861 | 2024-11-28T21:19:58.22955Z

OpenSSH Ubuntu Subnuit0.10

```
SSH-2.0-Quantum & Spl Ubuntu Subnuit0.10
Key: ecdb-sh2-misc256
Key: AAAAEZYjZWblJmOTYtbnRvMTYAAAMTbnRvMTYAAABBBBqGAL5uQzWJEDHCFQjEw
RR83zL33347wTAAYeAAMNlx4Fe/dIDPvILx4oGe/GvPlKefKRGd/Lzsd=
Fingerint: 1e-0C-dB-4F-9C-aad76-81-a5-85-23-bd-dc-9F-ad-ZZ
```

 General Information	
Country	Singapore
City	Singapore
Organization	[REDACTED] er, Pty. Ltd.
ISP	[REDACTED]
ASN	[REDACTED]

また、見た目を模しているだけなので、「次に進む」以外のボタンは機能しません。

```
Amazonの
<span class="underline cursor-pointer text-[#0066c0] hover:text-[#c45500]" data-v-d13668c0="">利用規約</span>
と
<span class="underline cursor-pointer text-[#0066c0] hover:text-[#c45500]" data-v-d13668c0="">プライバシー規約</span>
に同意いただける場合はログインしてください。
```

amazon.co.jp

ログイン

Eメールまたは携帯電話番号

次に進む

Amazonの[利用規約](#)と[プライバシー規約](#)に同意いただける場合はログインしてください。

▶ お困りですか？

お仕事のための物品購入ですか？

Amazonビジネスでショッピング

初めてAmazonをご利用ですか？

次に進む

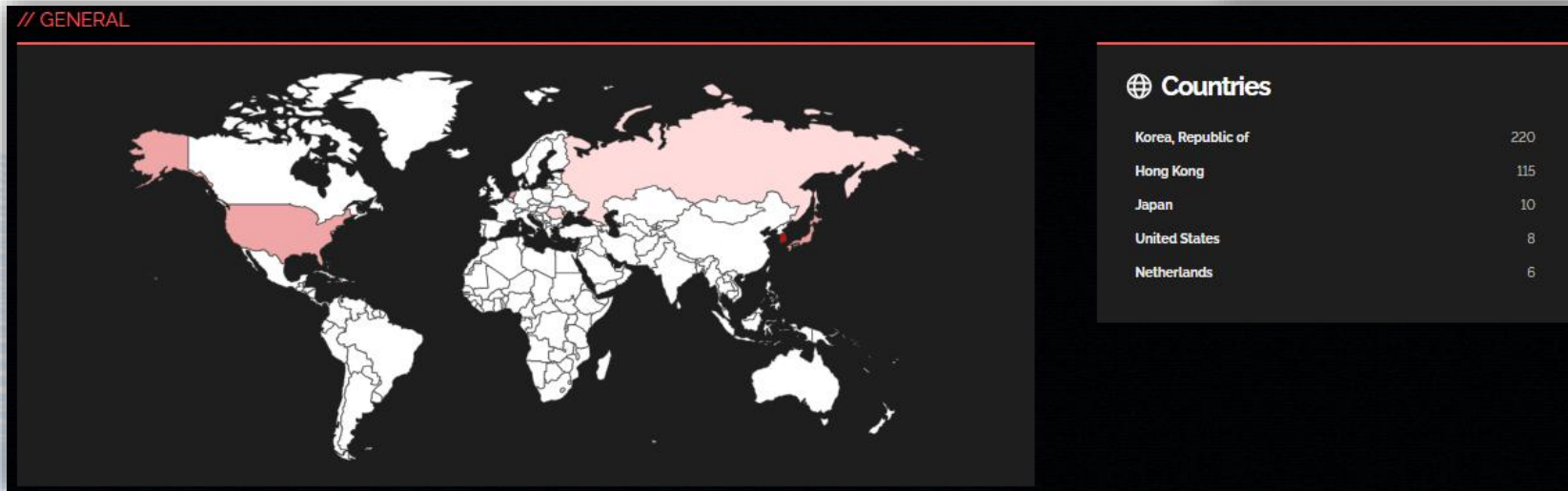
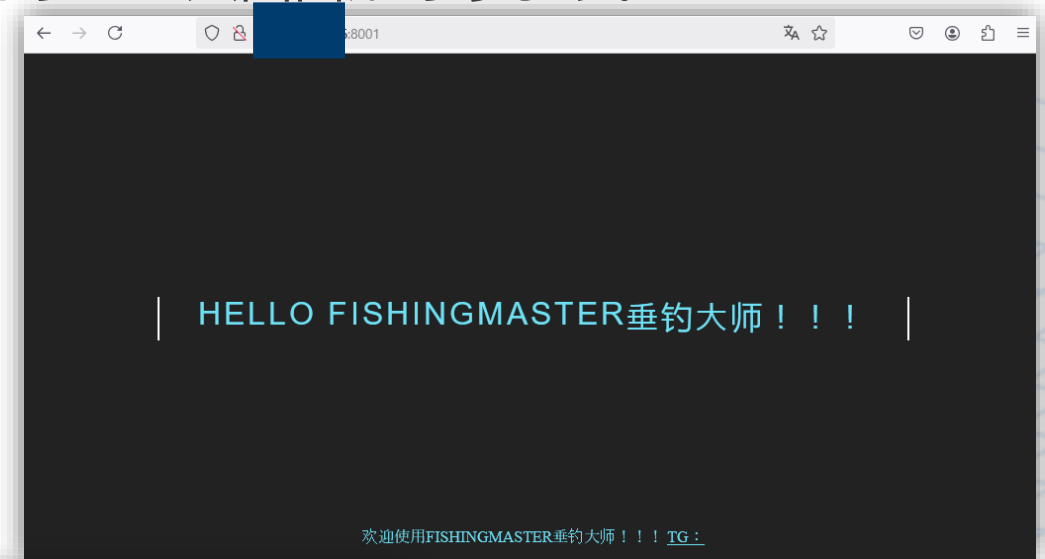
[利用規約](#) [プライバシー規約](#) [ヘルプ](#)

© 1996-2024, Amazon.com, Inc. またはその関連会社

尚、空いている8001ポートを見ると、煽りもしくはサービス画面があります。

- 垂钓大师：**釣りマスター**
- 欢迎使用：**いらっしゃいませ**

フィッシングキットなのか調査者への煽りなのか、よく分かりませんが、同じようなサイトが複数見つかります。



メールアドレスを入ると、パスワード画面に遷移します。
これも同様に、「ログイン」以外のリンクは動作しません。



The screenshot shows the Amazon.co.jp login page. At the top is the Amazon logo. Below it is the title 'ログイン' (Login). The email field is pre-filled with a redacted address '@example.com' and has a '変更' (Change) link. The password field is empty, with a 'パスワードを忘れた場合' (Forgot password) link. A yellow 'ログイン' (Login) button is below the password field. At the bottom of the form is a checked checkbox for 'ログインしたままにする' (Keep me signed in) and a '詳細' (Details) link. Below the form are links for '利用規約' (Terms of Use), 'プライバシー規約' (Privacy Policy), and 'ヘルプ' (Help). The footer contains the copyright notice '© 1996-2024, Amazon.com, Inc. またはその関連会社'.

amazon.co.jp

ログイン

■@example.com [変更](#)

パスワード [パスワードを忘れた場合](#)

[ログイン](#)

☒ ログインしたままにする [詳細](#) ▼

[利用規約](#) [プライバシー規約](#) [ヘルプ](#)

© 1996-2024, Amazon.com, Inc. またはその関連会社

カード情報画面を更新する画面らしきものに遷移します。

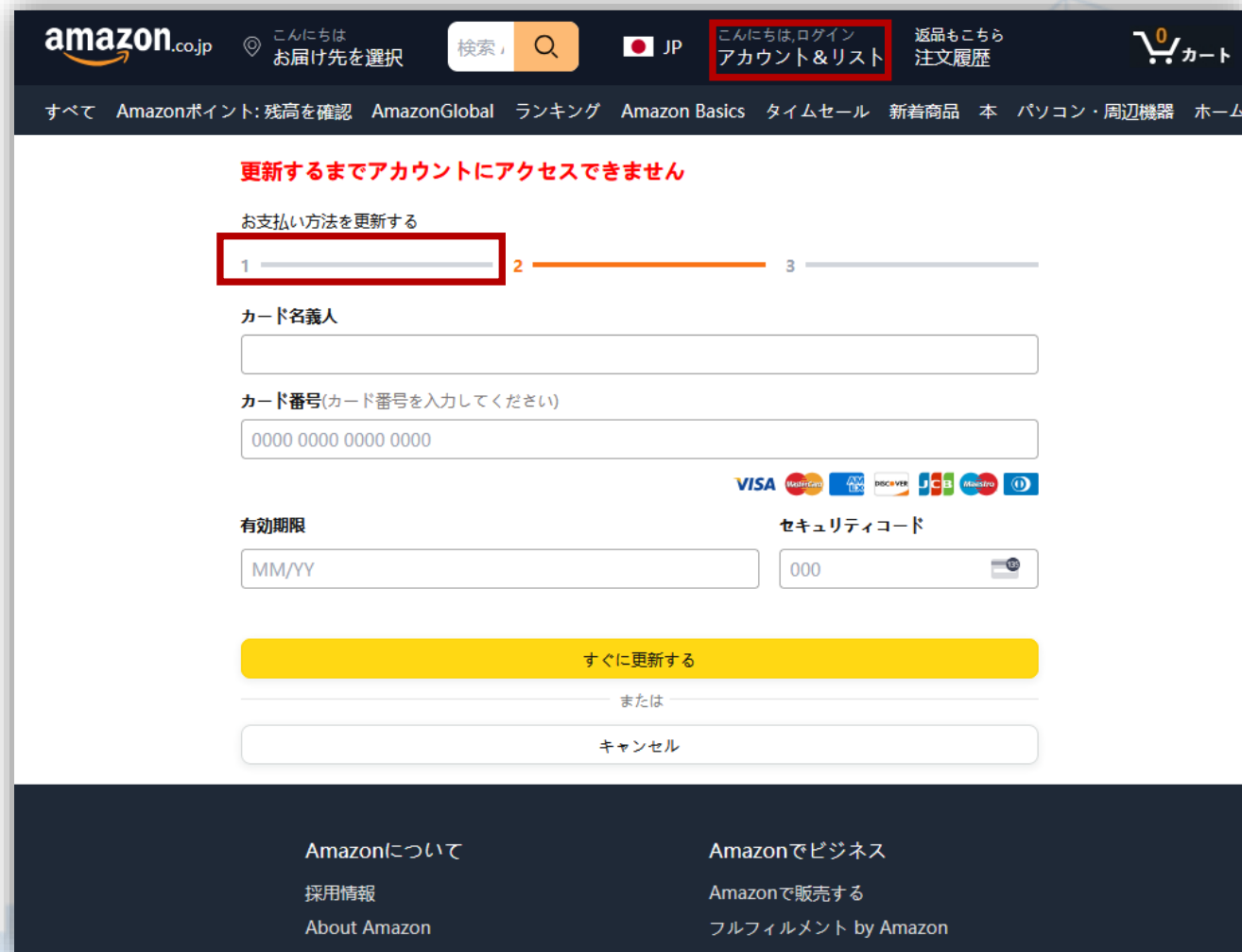
色々おかしい部分があります。

- ログインしたのに
「こんにちは、ログイン」表示
- 設定の「1」が飛ばされて、「2」からの設定になっている
- 日本の漢字ではないものが混じる

返品はこちら
注文履歴

新着商品

すべてのカテゴリ ▾ 検索 Amazon



amazon.co.jp こんにちは お届け先を選択 検索 JP こんにちは、ログイン アカウント&リスト 返品はこちら 注文履歴 カート

すべて Amazonポイント: 残高を確認 AmazonGlobal ランキング Amazon Basics タイムセール 新着商品 本 パソコン・周辺機器 ホーム

更新するまでアカウントにアクセスできません

お支払い方法を更新する

1 2 3

カード名義人

カード番号(カード番号を入力してください)

0000 0000 0000 0000

VISA MasterCard AMEX JCB Diners Club

有効期限

MM/YY

セキュリティコード

000

すぐに更新する

または

キャンセル

Amazonについて
採用情報
About Amazon

Amazonでビジネス
Amazonで販売する
フルフィルメント by Amazon

カード情報を更新するとどうなるのか

今回は、正規のテスト用カード番号を入れましたが、
「カード番号が無効です。修正して再提出してください。」
で拒否されました。

他の同様なフィッシングでは、1分ほど認証しているふりをして、

- 何事もなかったのように終わる
 - 延々と認証したふりを繰り返す
- という動作をするものもあります。

また、入力値検証をしている物もあり
おそらくカードのCheck Digitを確認している
物もあるようです。

amazon.co.jp

こんにちは
お届け先を選択

検索

JP

こんにちは、ログイン
アカウント&リスト

返品はこちら
注文履歴

カート

すべて Amazonポイント: 残高を確認 AmazonGlobal ランキング Amazon Basics タイムセール 新着商品 本 パソコン・周辺機器 ホーム&

更新するまでアカウントにアクセスできません

お支払い方法を更新する

1 2 3

カード名義人

Xi J

カード番号(カード番号を入力してください)

211

カード番号が無効です。修正して再提出してください。

有効期限

25/02

セキュリティコード

244

すぐに更新する

または

キャンセル

2025-01-11時点で来たフィッシングメールを見ると、全体がBase64エンコードされており、ソースをパッと見ただけでは分からないようになっていました。

- HTMLがBase64 Encodeされているだけで、中身は依然と同じ傾向
- ツールでBase64 DecodeをするとURL部分がUnicode解釈されてしまっており、
/ (SOLIDUS:U+002F)
/ (DIVISION SLASH:U+2215)
が全く分からない表示となる場合が多い
(上下に並べると分かりやすいが)

結果的に「リンクにマウスを置いてURLを確認する作業」は有効ではなくなりました。



04 まとめ

他社を騙るフィッシングメールは無くすことはできませんが、軽減できると思われます。
詐欺URLとしての通報は有効ですし、DMARKも実在企業にとっては有効と考えられます。

- URLが通報されることで、ブラウザで当該サイトへのアクセスがブロックされるようになります。フィッシングやコンピュータ技術に詳しくない人に対しても有効な対策となり得ます。

対策としてやれることは以下の通りです。

- 利用者
 - パスワードマネージャーを使う
 - SMSのリンクからアプリのインストールは行わないようにする
- サービス提供者
 - DMARCポリシーに従ったメールの配信を行い、迷惑メール対策の強化する
 - 搾取された認証情報の不正利用対策として、パスキーなどID/パスワード以外の認証方法追加など、認証強化を検討する



Appendix

参考URL

- 警視庁
 - フィッシング対策
 - ✓ <https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html>
- フィッシング対策協議会
 - <https://www.antiphishing.jp/>
 - 2024/11 フィッシング報告現状
 - ✓ <https://www.antiphishing.jp/report/monthly/202411.html>
- 総務省
 - 国民のためのサイバーセキュリティサイト：フィッシング詐欺とは？
 - https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/risk/04/
- チェッカー
 - SPF
 - ✓ <https://dmarcian.com/spf-survey/>
 - DKIM
 - ✓ <https://dmarcian.com/dkim-inspector/>
 - DMARK
 - ✓ <https://dmarcian.com/dmarc-inspector/>
 - dig, nslookup, etc..
- Unicode
 - /:Unicode U+002F:SOLIDUS
 - ✓ <https://0g0.org/search/002F/>
 - /:Unicode U+2215:DIVISION SLASH
 - ✓ <https://0g0.org/unicode/2215/>

Thank you!

Any Question?

※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。

※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。

※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。

※ LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。その他記載されている会社名、製品名は一般に各社の商標または登録商標です。





※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。

※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。

※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。

※ LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。その他記載されている会社名、製品名は一般に各社の商標または登録商標です。