フィッシングサイトを落とさナイト 2022秋

JPAAWG 5th General Meeting

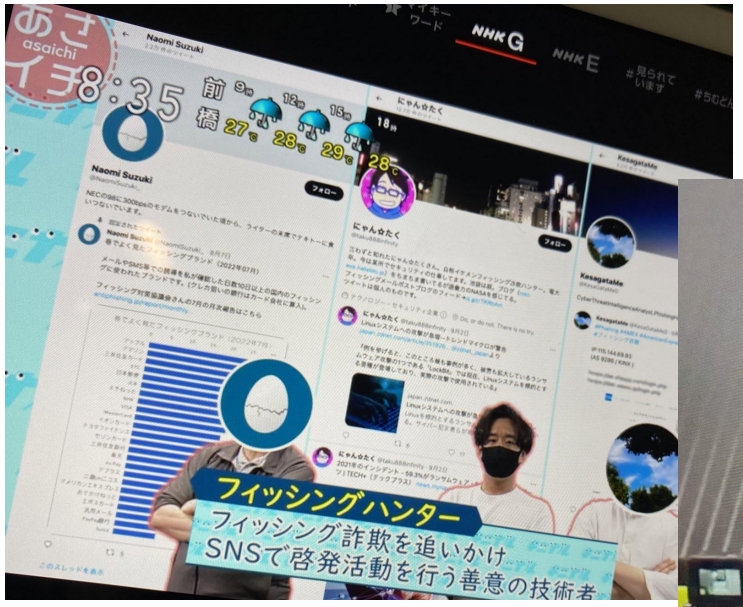
2022年11月08日　14:00 – 14:45

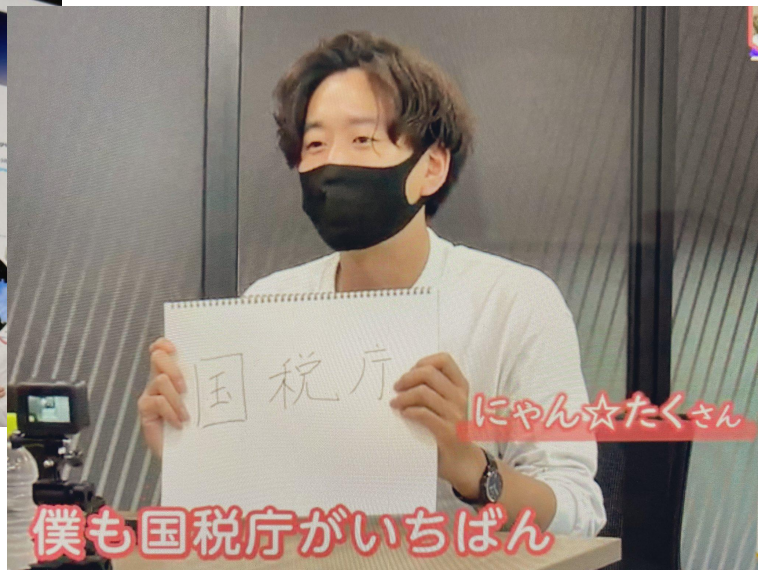

そもそも、お前ら誰だよ。

にゃん☆たく（@taku888infinity）
https://twitter.com/taku888infinity

フィッシング詐欺ハンターとして活動

＜講演（一部）＞
・サイバーセキュリティシンポジウム道後2021
（総務省共催）ナイトセッション座長
・情報セキュリティワークショップin越後湯沢2021
・ICT東京フォーラム2021
　デジタル社会における地域情報化の現状と課題
・JPAAWG 4th General Meeting（2021）
・KIISサイバーセキュリティ研究会
　セキュリティ最新情報解説サロン（2021）





引用元：2022/09/07放送のあさイチより
「あなたのキニナルことを徹底調査!フィッシング詐欺&値上げ」

nakamura (tomoaxe)

ユーザー企業で働いてます

～2011年

いろいろ→無職→現在の所属

2011～2017年

Web + アプリの脆弱性診断,

セキュリティエンジニア採用, など

2017年～現在

Anti-Phishing, Anti-Abuse,

消費者啓発活動, コンプラとかガバナンスとか

KesagataMe

@KesaGataMe0

2014

通信キャリアでサイバーセキュリティ業務を開始

2018

Phishing Hunterとして始動
(所属会社がターゲットになったことがきっかけ)

2020

・金融業界でCyberThreatIntelligenceを担当
・JNSA賞を受賞

2022

・多くの業種のフィッシング詐欺サイトを追跡
・メディア等を通じて注意喚起に協力
…など、現在進行形で対策活動を推進

yakoo

@yako_hiro

CSIRT
- **Incident Manager**
- **Cybercrime Investigator**
- **Threat Intelligence Analyst**

Analysis Theme
- **2015 ZeusVM Malware**
- **2016 Gozi Malware, Rig-EK**
- **2019 Cashless Payment**
- **2020 Phishing**

『見分けようとしない！』

■本物のURLと偽物のURLを見比べてみよう

＜パターン①：そっくり＞

本物：https://www.smbc-card.com/mem/index.jsp

偽：https://www.smbc-card.com.mem-index-jsp.vip

＜パターン②：正規ドメイン.～～～＞

本物：https://www2.cr.mufg.jp/~

偽：https://www2.cr.mufg.jp.ttakasua4[.]tokyo

■「http」か「https」かの違いで判断はできない

■TLD（トップレベルドメイン）での判断は危険

例1：mercarl[.]jp/secure_center/material（メルカリのフィッシングサイト）

例2：saison[.]updated[.]jp（セゾンカードのフィッシングサイト）

・本文に記載されたURLにはアクセスしない
・アクセスする際は登録済みのお気に入り等から
　⇒お気に入りに登録させたいURLを注意喚起に記載する

※これはやっちゃダメだよ注意喚起内容※

◇「URLが正しいか確認してください」

【yaho ο .jp】←2個目のオーはオミクロン（ギリシャ文字）になっている
【rnicrosoft .com】←「m」が「 rn 」になっている
⇒目で見て判断できるのは困難（ほぼ無理）です
⇒ユーザが自分の利用している全ての会社のサービスの全てのURLを正しく判断できるとは思えません
（ちなみに自分が使っているサービスの全てのドメインを正確に列挙できますか？）

◇「当社からのメールの場合こちらのメールアドレス（ドメイン）が正しいです」

◇「メールアドレスの送信元を確認しましょう」

⇒送信元メールアドレスは簡単に偽装され送られてしまうのでメールアドレスを「正」としない

◇「このドメインから始まるURLが正しいです」

⇒サブドメインに正規サイトのドメインを定義したフィッシングサイトが多発している為
例⇒偽物：https://www2.cr.mufg.jp.ttakasua4.tokyo
本物：https://www2.cr.mufg.jp/～

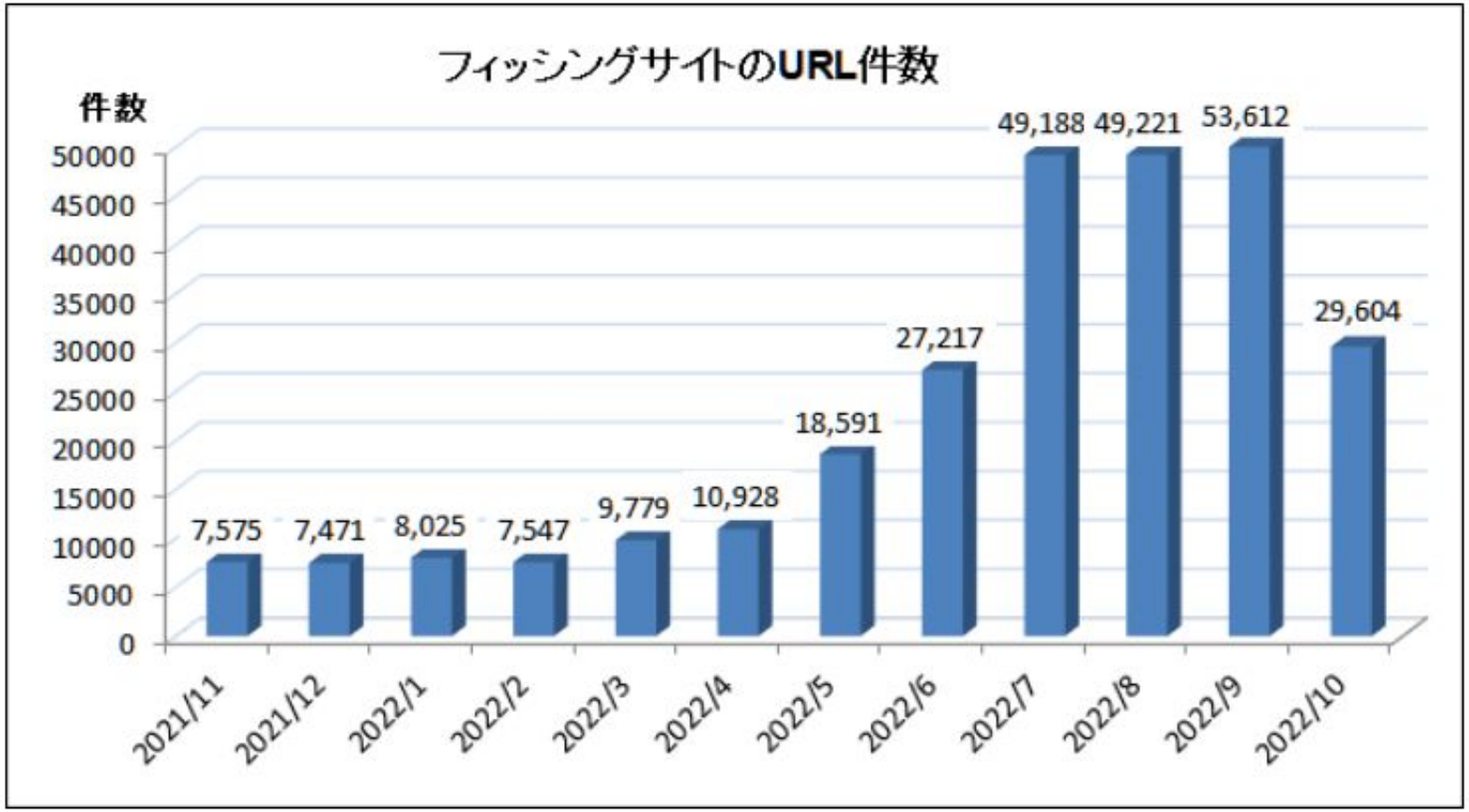
◇フィッシングサイトのURLを無害化せず注意喚起する（特にメールで周知する場合）

⇒無害化（デファング/defang）しない場合ユーザーが間違ってアクセスしてしまう危険性がある
無害化実例：hxxps://www2[.]cr[.]mufg[.]jp[.]ttakasua4[.]tokyo

今年ってフィッシング詐欺系の話題何かあった？

2022年のトレンド（1月～3月）

・フィッシングサイトが増加した原因の始祖が・・・
⇒1つのIPに複数のドメインが紐づくようになった



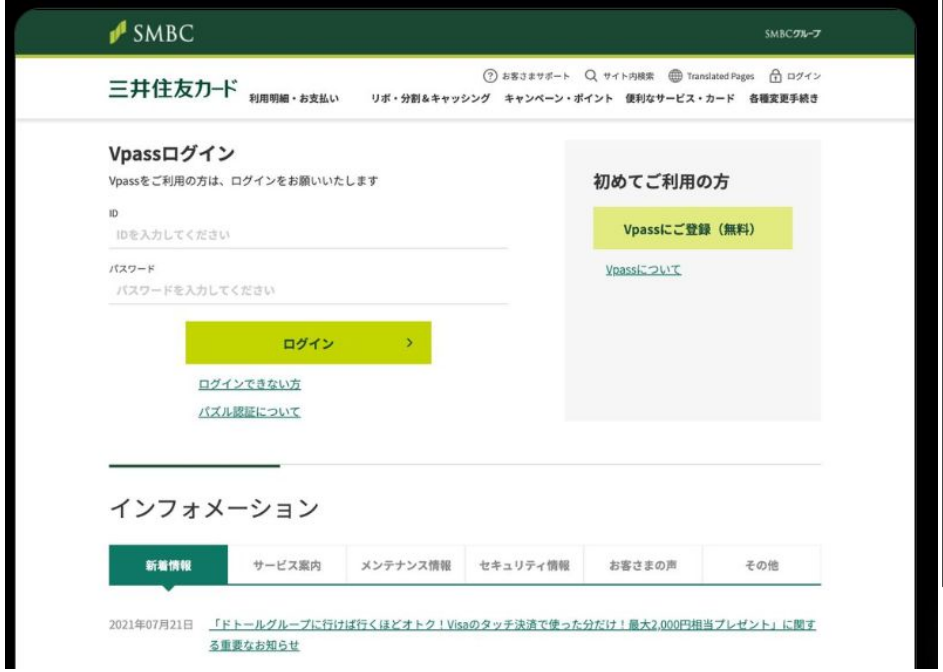
https://www.antiphishing.jp/report/monthly/202210.html

2022年のトレンド（4月～6月）

- ウクライナ人道支援のフィッシングサイト誕生
- エロエロマーメイド
- kesagatameドメイン爆誕⁉…そしてフィッシングサイト内に…

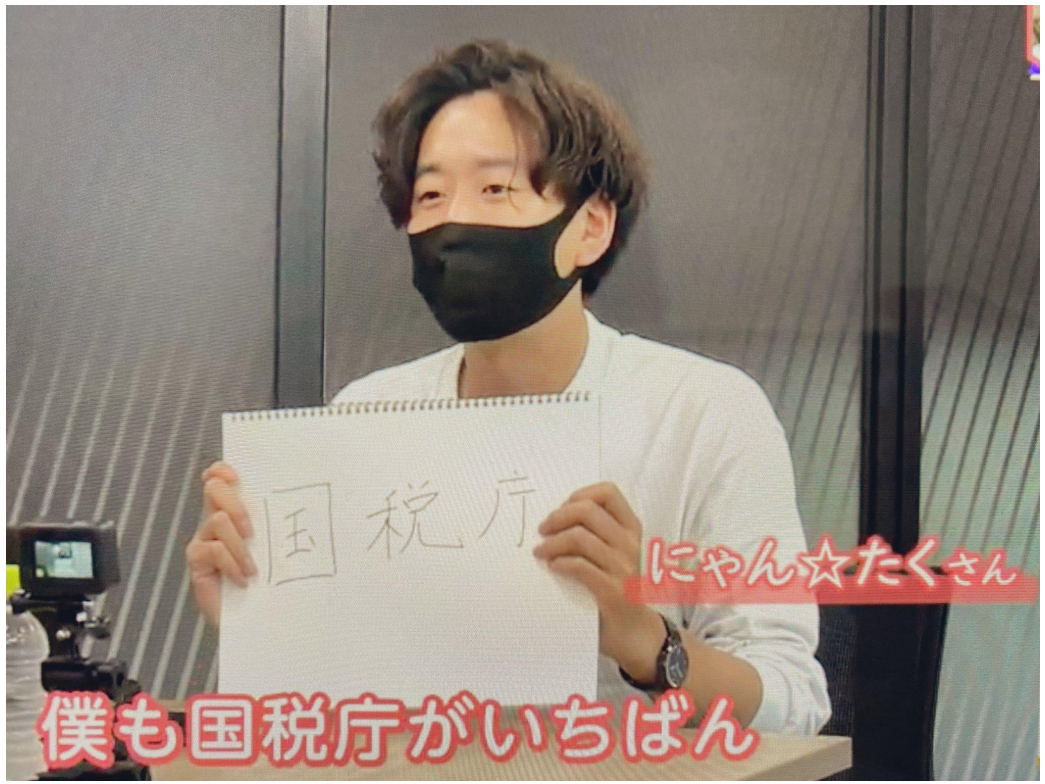
IP:185.149.21.209
(AS 8100 / ASN-QUADRANET-GLOBAL)

hxxps://jp-smuc.eroero-marmaid.com



2022年のトレンド（7月～9月）

- 国税庁のフィッシング、スミッシングが増加



基本多言語面		数学用英字		数学用英字・太字斜体		数学用英字・太字	
a	U+0061	a	U+1D5BA	***a***	U+1D656	**a**	U+1D41A
b	U+0062	b	U+1D5BB	***b***	U+1D657	**b**	U+1D41B
c	U+0063	c	U+1D5BC	***c***	U+1D658	**c**	U+1D41C
d	U+0064	d	U+1D5BD	***d***	U+1D659	**d**	U+1D41D
e	U+0065	e	U+1D5BE	***e***	U+1D65A	**e**	U+1D41E
f	U+0066	f	U+1D5BF	***f***	U+1D65B	**f**	U+1D41F
g	U+0067	g	U+1D5C0	***g***	U+1D65C	**g**	U+1D420
h	U+0068	h	U+1D5C1	***h***	U+1D65D	**h**	U+1D421
i	U+0069	i	U+1D5C2	***i***	U+1D65E	**i**	U+1D422
j	U+006A	j	U+1D5C3	***j***	U+1D65F	**j**	U+1D423
k	U+006B	k	U+1D5C4	***k***	U+1D660	**k**	U+1D424
l	U+006C	l	U+1D5C5	***l***	U+1D661	**l**	U+1D425
m	U+006D	m	U+1D5C6	***m***	U+1D662	**m**	U+1D426
n	U+006E	n	U+1D5C7	***n***	U+1D663	**n**	U+1D427
o	U+006F	o	U+1D5C8	***o***	U+1D664	**o**	U+1D428
p	U+0070	p	U+1D5C9	***p***	U+1D665	**p**	U+1D429
q	U+0071	q	U+1D5CA	***q***	U+1D666	**q**	U+1D42A
r	U+0072	r	U+1D5CB	***r***	U+1D667	**r**	U+1D42B
s	U+0073	s	U+1D5CC	***s***	U+1D668	**s**	U+1D42C
t	U+0074	t	U+1D5CD	***t***	U+1D669	**t**	U+1D42D
u	U+0075	u	U+1D5CE	***u***	U+1D66A	**u**	U+1D42E
v	U+0076	v	U+1D5CF	***v***	U+1D66B	**v**	U+1D42F
w	U+0077	w	U+1D5D0	***w***	U+1D66C	**w**	U+1D430
x	U+0078	x	U+1D5D1	***x***	U+1D66D	**x**	U+1D431
y	U+0079	y	U+1D5D2	***y***	U+1D66E	**y**	U+1D432
z	U+007A	z	U+1D5D3	***z***	U+1D66F	**z**	U+1D433

フィッシングサイトを落とさナイト 2022秋

・フィッシングの利益構造はどうなっているのでしょうか

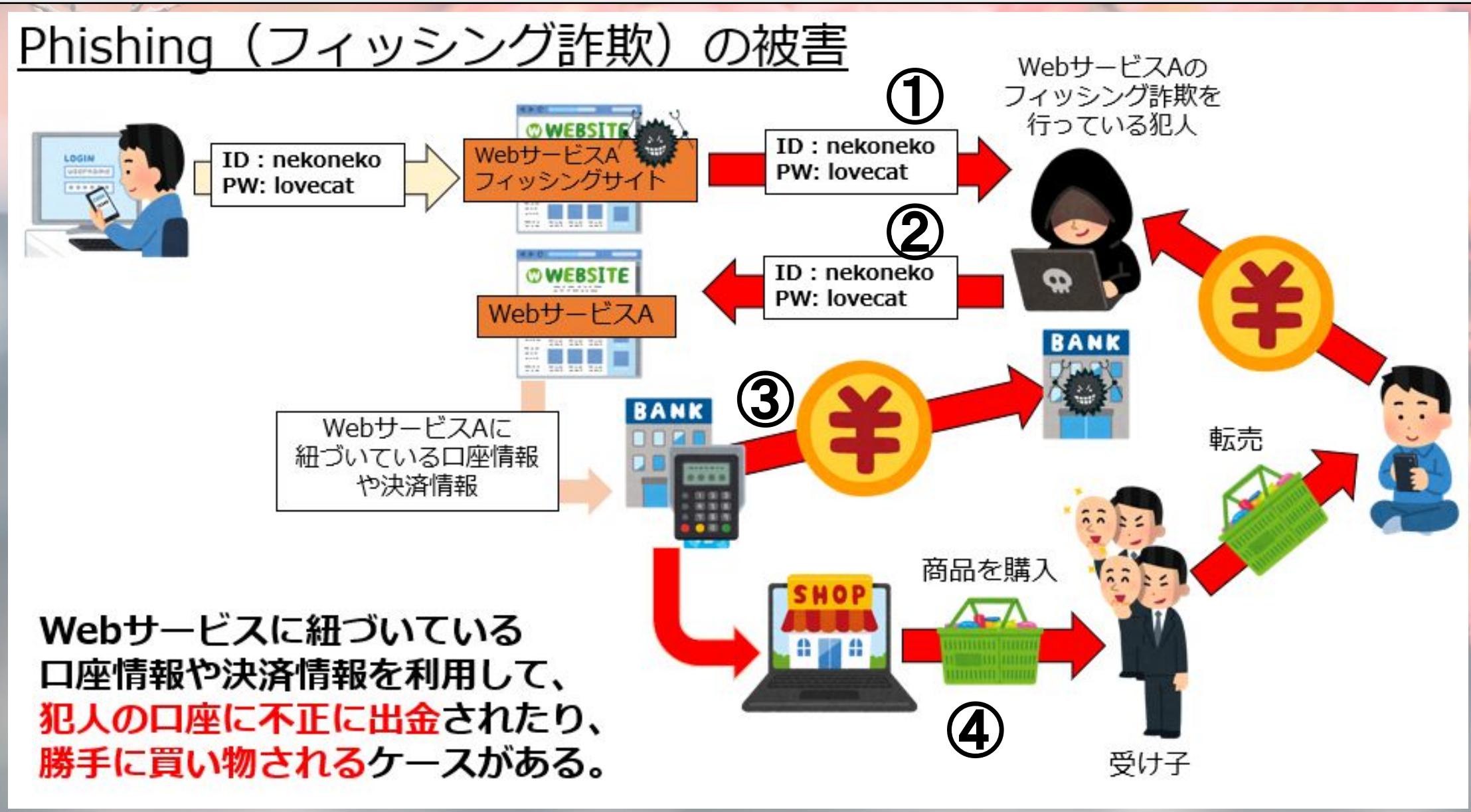
・落ちにくいホスティングやレジストラを攻略する上で
心がけている事はありますでしょうか？
・フィッシングサイトのホスティング先事業者への通報は
どのくらい効果があるのか

・この技術さえ広まればフィッシングも減るのに、、といったものは
あると思いますか？（例えばFIDO2とか）

・「不審な」「怪しい」の表現に変わる、相応しいフィッシングサイトの
名称をどのようにしたら良いか。
・フィッシングサイトとのいたちごっこは長いこと続いていると
思いますが、将来収束すると考えますか?

フィッシングサイトを落とさナイト 2022秋

・フィッシングの利益構造はどうなっているのでしょうか



フィッシングサイトを落とさナイト 2022秋

- 落ちにくいホスティングやレジストラを攻略する上で心がけている事はありますでしょうか？
- フィッシングサイトのホスティング先事業者への通報はどのくらい効果があるのか

【.ci（コートジボワール）】ドメインの撃ち落とし（2022年6月）

Address lookup

lookup failed **presse.ci**

Could not find an IP address for this domain name.

Domain Whois record

Queried **whois.nic.ci** with "**presse.ci**"...

```
Domain Name: presse.ci
Registry Domain ID: 114934-CoCCA
Registry WHOIS Server: whois.nic.ci
Updated Date: 2022-06-13T15:19:25.406Z
Creation Date: 2020-04-15T22:32:58.96Z
Registry Expiry Date: 2023-04-15T22:32:58.180Z
Registrar Registration Expiration Date: 2023-04-15T22:32:58.180Z
Registrar: AFRIREGISTER
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverHold https://icann.org/epp#serverHold
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry RegistrantID:
RegistrantName: Redact
```

Address lookup

lookup failed **asso.ci**

Could not

Domain Whois reco

Queried **whois.nic.ci** with

```
Domain Name: asso.ci
Registry Domain ID: 11
Registry WHOIS Server:
Updated Date: 2022-06-
Creation Date: 2020-03-10T23:29:14.455Z
Registry Expiry Date: 2023-03-10T23:29:14.5
Registrar Registration Expiration Date: 202
Registrar: AFRIREGISTER
Domain Status: serverHold https://icann.org/epp#serverHold
Registry RegistrantID: X4pJh-XbuAo
```

ポイントは…相手への愛？

付録 D–プロバイダーへのテイクダウン要請文例

To whom it may concern,

[簡潔な企業プロファイル].

The website is located at the following address:

＜当該フィッシングサイトのURI＞

For your information, the fraudulent website appears to be a forgery of this legitimate website:

<正規サイトのURL>

Please take all necessary measures to suspend services of this fraudulent site.

We highly appreciate your cooperation on this matter.

Thank you very much. Sincerely,
--
[担当者、送信者の名前]
[担当者、送信者の所属部署]
[企業名]
[国際電話番号]
[担当者、送信者のメールアドレス]

https://www.antiphishing.jp/report/antiphishing_guideline_2022.pdf

フィッシングサイトを落とさナイト 2022秋

- この技術さえ広まればフィッシングも減るのに、、といったものはあると思いますか？（例えばFIDO2とか

Cloudflare、Twilioと同じフィッシング攻撃を受けるも完全回避　ハードキーが鍵

2022年08月10日 17時04分 公開　[ITmedia]

印刷　見る　Share　B!　71　1

GraphQL徹底入門｜RESTと比較、API・フロントの実装から学ぶ
デジタルサイネージで商品の売り上げが3倍以上に!?

米CDN（Content Delivery Network）大手のCloudflareは8月10日（現地時間）、米Twilioが7日に発表したものと同じ高度なソーシャルエンジニアリング攻撃を受けたが、日頃の備えが奏功し、すべて阻止したと発表した。

Twilioが攻撃されたのとほぼ同時期に、Cloudflareの多数の従業員に対する攻撃があった。3人の従業員がこれにだまされたが、自社製品「Cloudflare One」ですべてのアプリへのアクセスに物理的なセキュリティキー（ハードキー）による認証を義務付けていたため、攻撃を阻止できたとしている。

攻撃が始まったのは7月20日。セキュリティチームに対し、少なくとも76人の従業員が、個人用および仕事用のスマートフォンで不審なテキストメッセージを受け取ったと報告した。攻撃者がどのようにして従業員の電話番号リストを入手したかはまだ特定できていない。

https://www.itmedia.co.jp/news/articles/2208/10/news164.html

プレスリリース　2022.09.06

シェアする 0　ツイート　B! 3　Pocket

フィッシングメール対策として、Yahoo! JAPANから配信するメールにアイコンが表示される規格「BIMI」を導入

～ Gmailなど「BIMI」にシステム対応しているメールソフトでアイコンが表示され、Yahoo! JAPANから配信された正規のメールがひと目でわかる ～

ヤフー株式会社（以下、Yahoo! JAPAN）は本日、フィッシングメール対策を目的に、Yahoo! JAPANから配信するメールにアイコンが表示される規格「BIMI（Brand Indicators for Message Identification）」（以下、「BIMI」）を導入しました。
これにより、Gmail（※1）など「BIMI」にシステム対応しているメールソフト（※2）に、Yahoo! JAPANのアイコンが表示されるため、ユーザーはYahoo! JAPANから配信された正規のメールがひと目でわかるようになります。

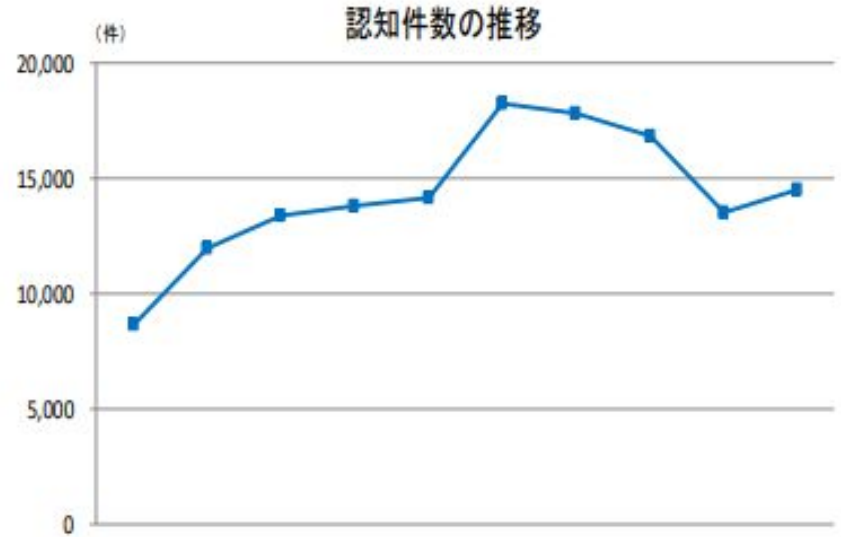
「BIMI」は、送信ドメインの認証技術である「DMARC（Domain-based Message Authentication, Reporting and Conformance）」（以下、「DMARC」）（※3）と「認証マーク証明書（VMC）」（以下、「VMC」）（※4）によって成り立つ仕組みです。

https://about.yahoo.co.jp/pr/release/2022/09/06a/

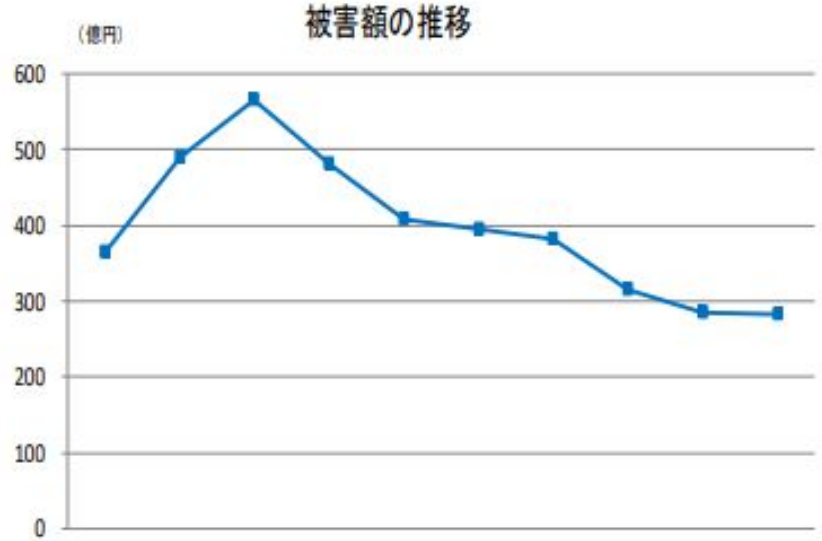
フィッシングサイトを落とさナイト 2022秋

・フィッシングサイトとのいたちごっこは長いこと続いていると思いますが、将来収束すると考えますか?

フィッシング詐欺 ≒ 特殊詐欺（オレオレ詐欺）



区分＼年次	H24	H25	H26	H27	H28	H29	H30	R1	R2	R3
認知件数	8,693	11,998	13,392	13,824	14,154	18,212	17,844	16,851	13,550	14,498



区分＼年次	H24	H25	H26	H27	H28	H29	H30	R1	R2	R3
被害額	364.4	489.5	565.5	482.0	407.7	394.7	382.9	315.8	285.2	282.0

https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/tokushusagi_toukei2021.pdf

フィッシング詐欺ハンターに必要な心得や経験などありますか？

にゃん☆たく
@taku888infinity

nakamura
@tomoaxe

KesagataMe
@KesaGataMe0

yakoo
@yako_hiro

本日はご清聴ありがとうございました！
またどこかでお会いしましょう！！！