

# フィッシング対策研究101

フィッシング対策協議会 学術研究WG  
長崎県立大学 情報システム学部 情報セキュリティ学科

加藤雅彦



# Agenda

- イントロダクション
- フィッシングの現状
- スミッシングの増加
- フィッシングというビジネス
- フィッシング対策
- フィッシング対策研究
- 研究用リソース
- まとめ



# イントロダクション

---

# フィッシング対策協議会について

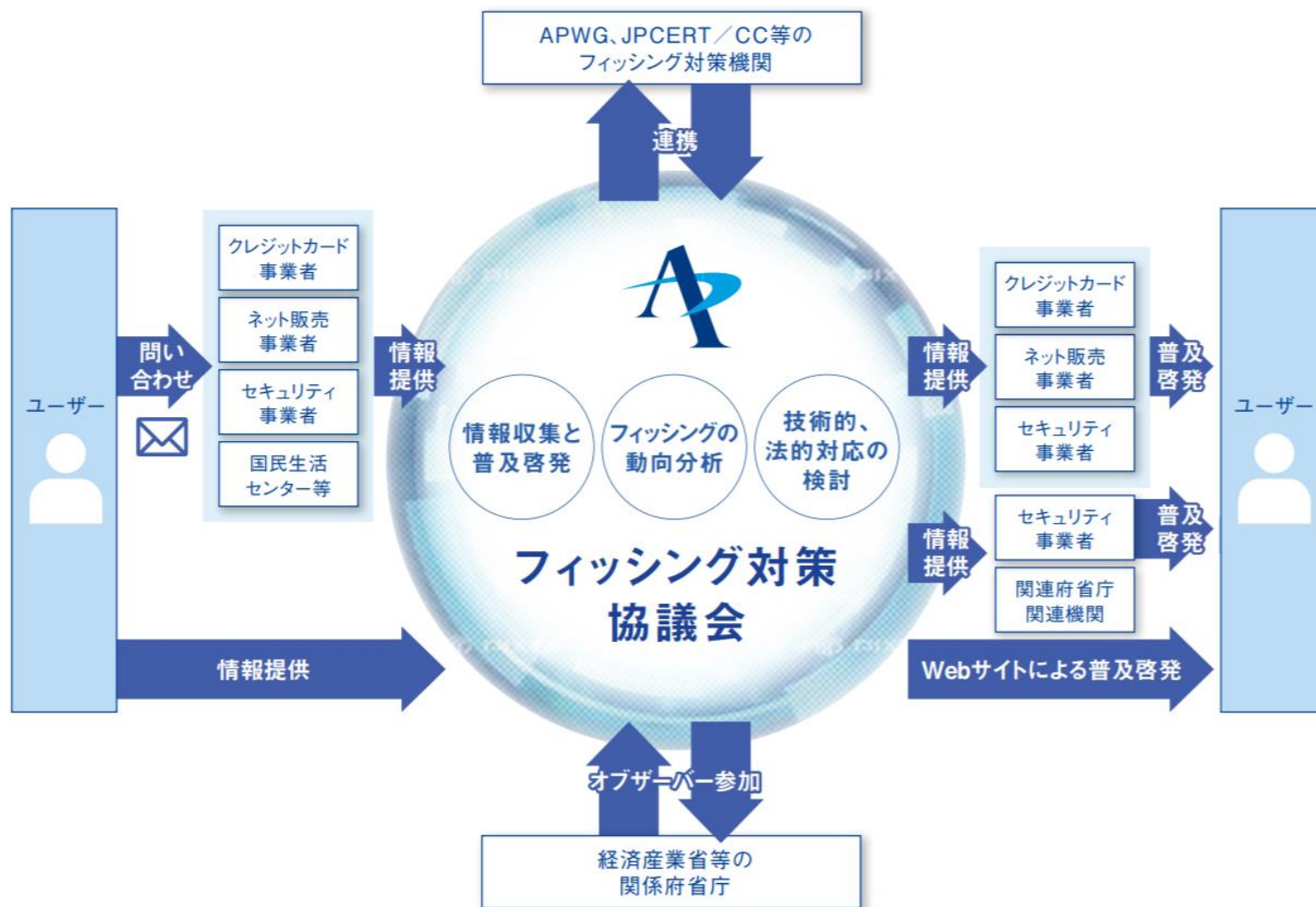


## 概要

- 設立 2005年4月
- 名称 フィッシング対策協議会 / Council of Anti-Phishing Japan
- 目的 フィッシング 詐欺に関する事例情報、技術情報の収集及び提供を中心に行うことで、日本国内におけるフィッシング詐欺被害の抑制を目的として活動
- 会員+オブザーバー 118 (2022 年 11 月時点)
  - 正会員：91, リサーチパートナー：5, 関連団体：15
  - オブザーバー：7
  - 金融機関、信販会社、オンラインサービス、セキュリティベンダーなど

# フィッシング対策協議会について

## 活動内容



### 情報発信 (事業者／ 一般向け)

- 緊急情報／お知らせ
- ガイドライン改訂 (WG活動)
- フィッシングレポート 等

### 学術研究

- フィッシングサイト早期検知
- フィッシング詐欺の全容解明

### 会員間の 情報交流

- 総会／情報交換会
- 勉強会
- ワーキンググループ活動 等

### 啓発活動

- フィッシング対策セミナー
- STOP.THINK.CONNECT.

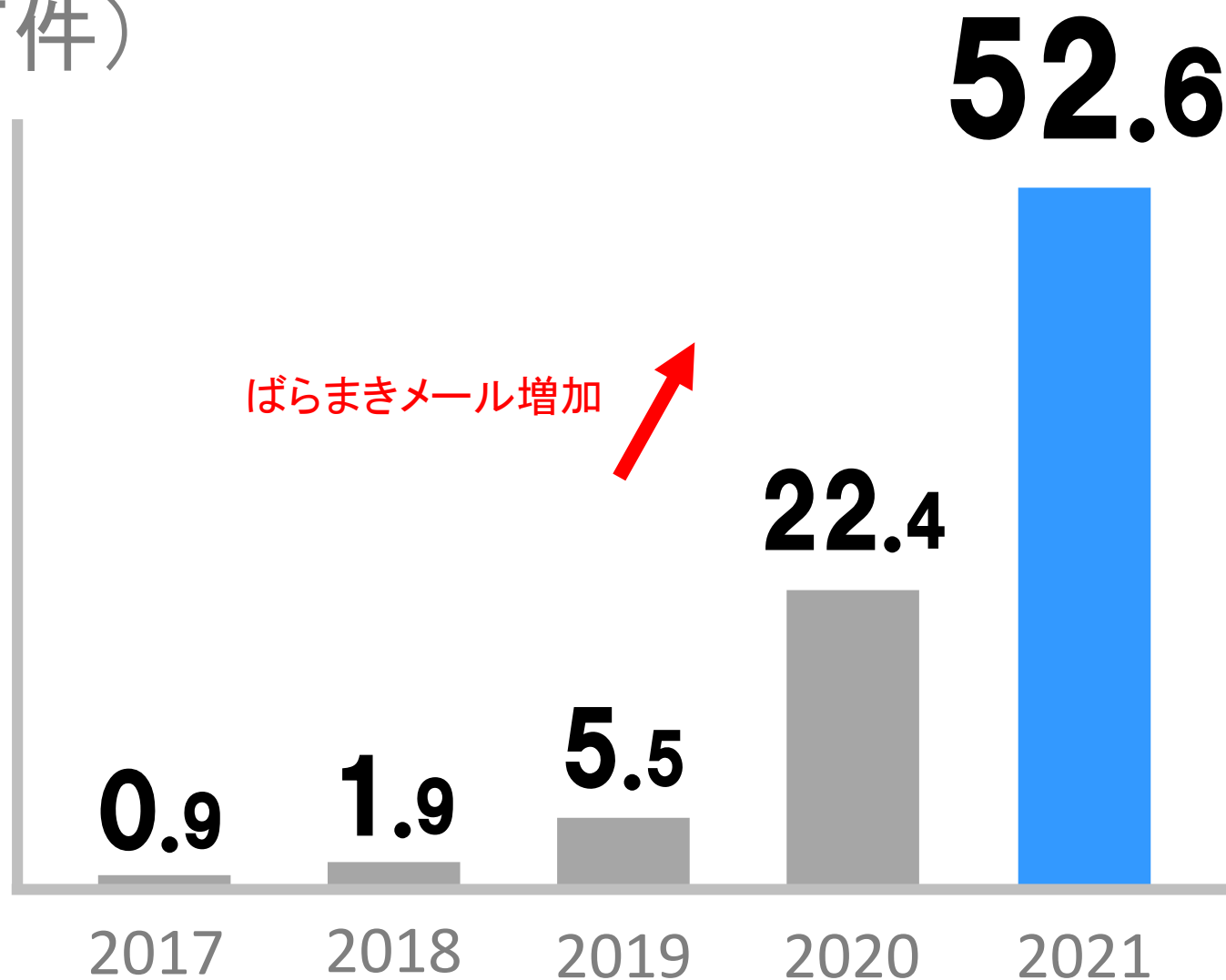


# フィッシングの現状

---

# 年別 フィッシング詐欺 報告件数

(万件)



52.6

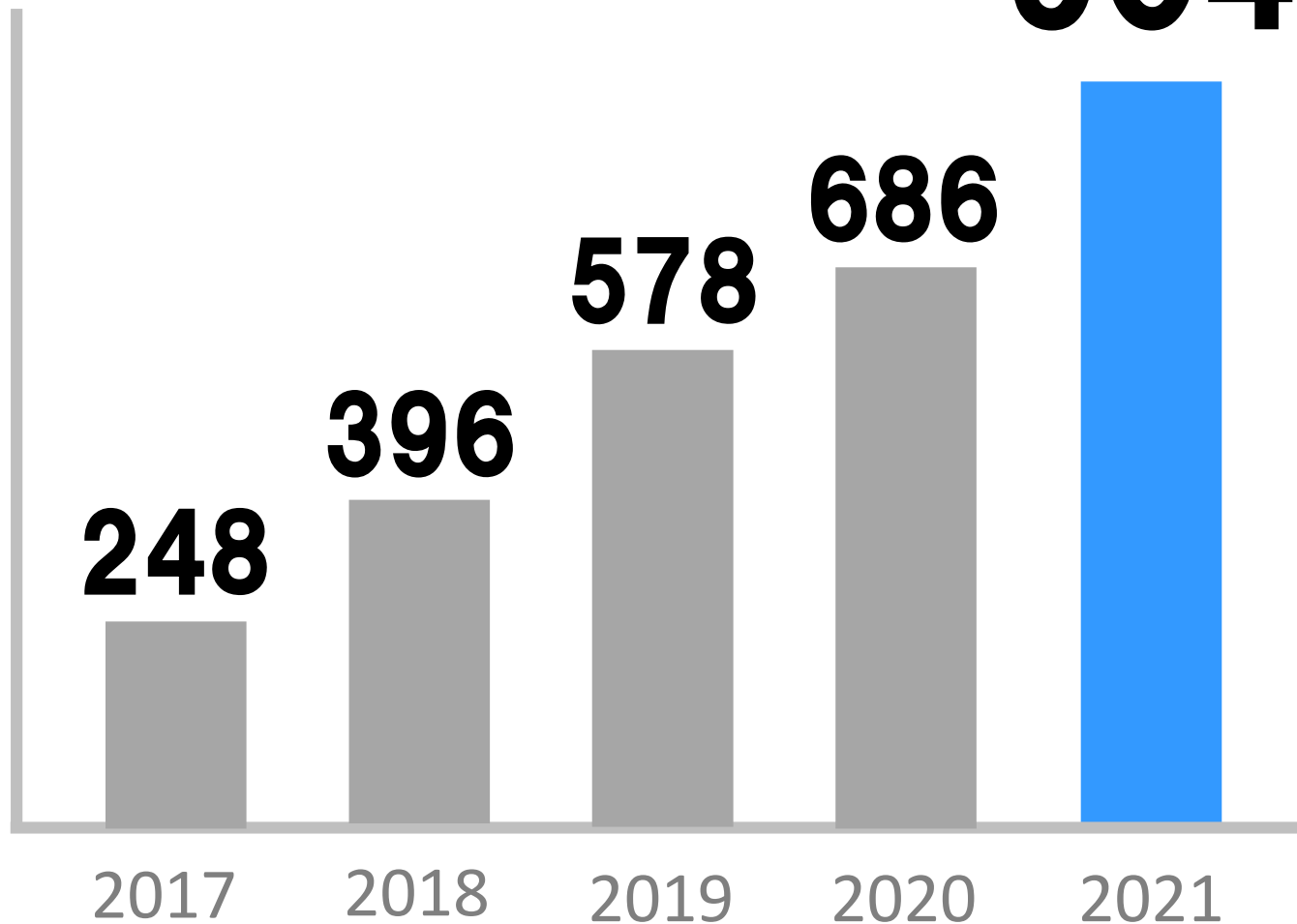
前年比

2 倍増

2021年 526,504  
2020年 224,676  
2019年 55,787  
2018年 19,960  
2017年 9,812

# 年別 フィッシング詐欺 標的ブランド件数

(件)



904

標的ブランドの

多様性

# 2022/9の状況（1）

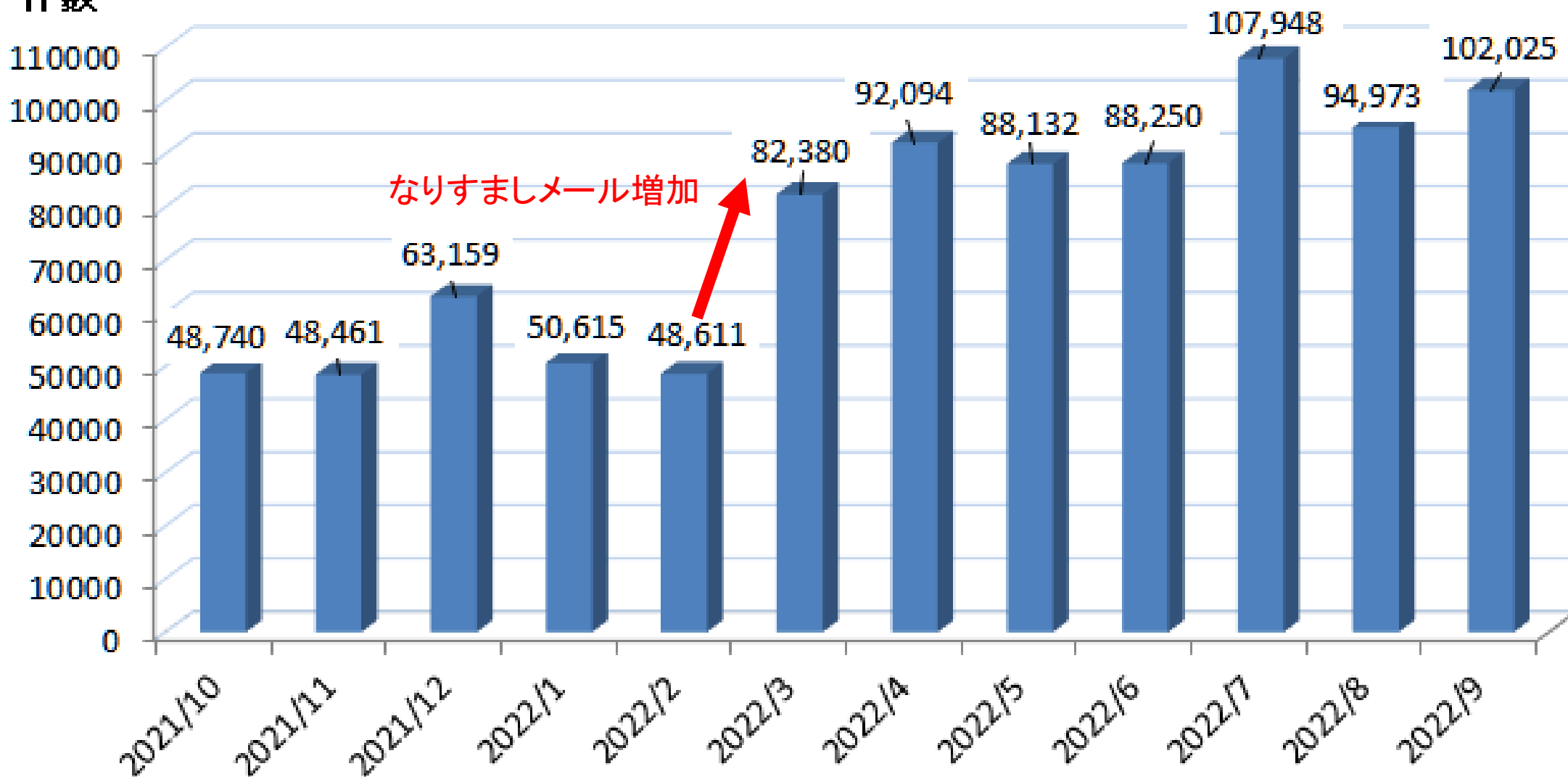
フィッシング対策協議会より引用

<https://www.antiphishing.jp/report/monthly/>



## フィッシング報告件数

件数



なりすましメール増加

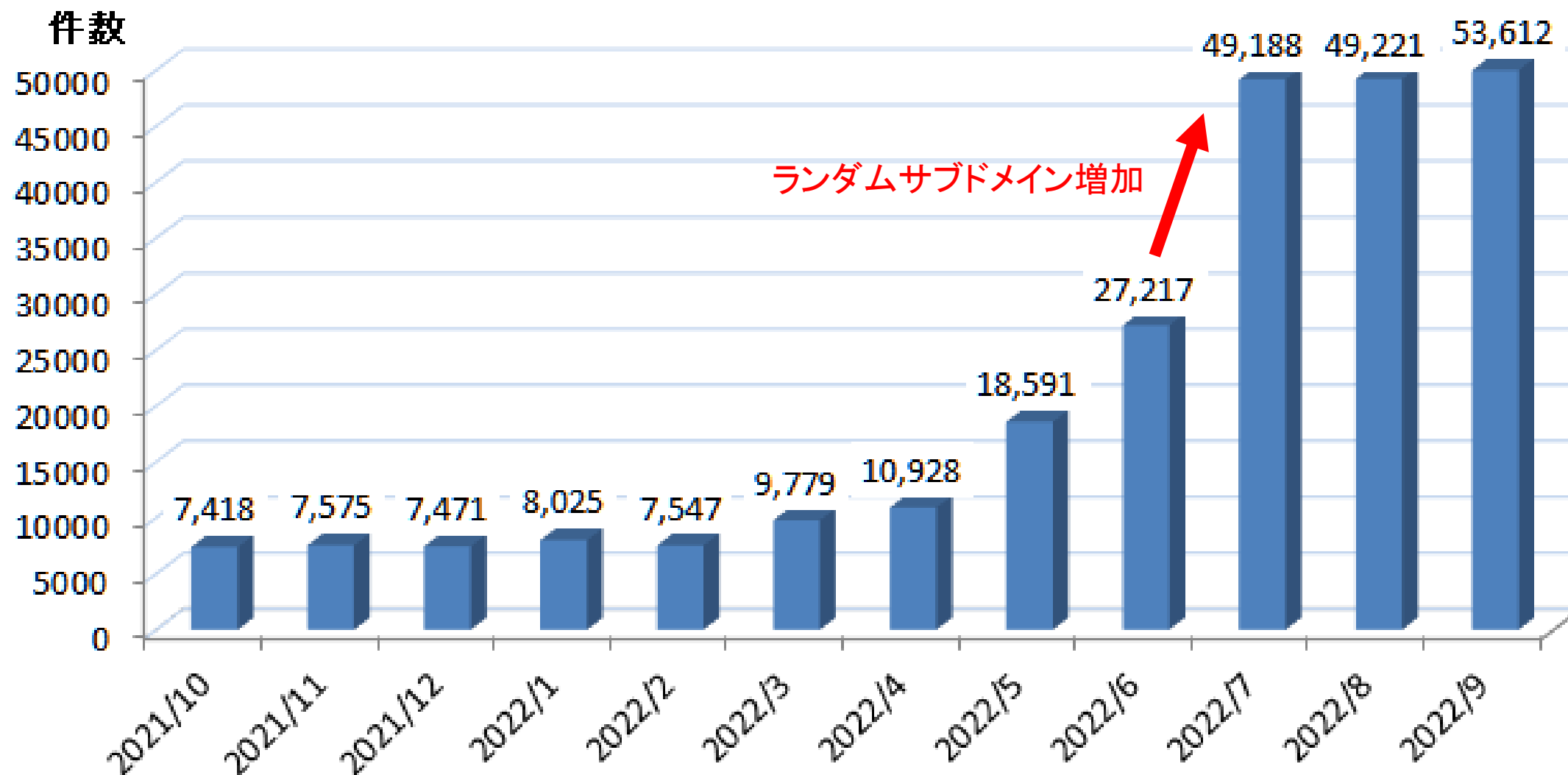
# 2022/9の状況（2）

フィッシング対策協議会より引用

<https://www.antiphishing.jp/report/monthly/>



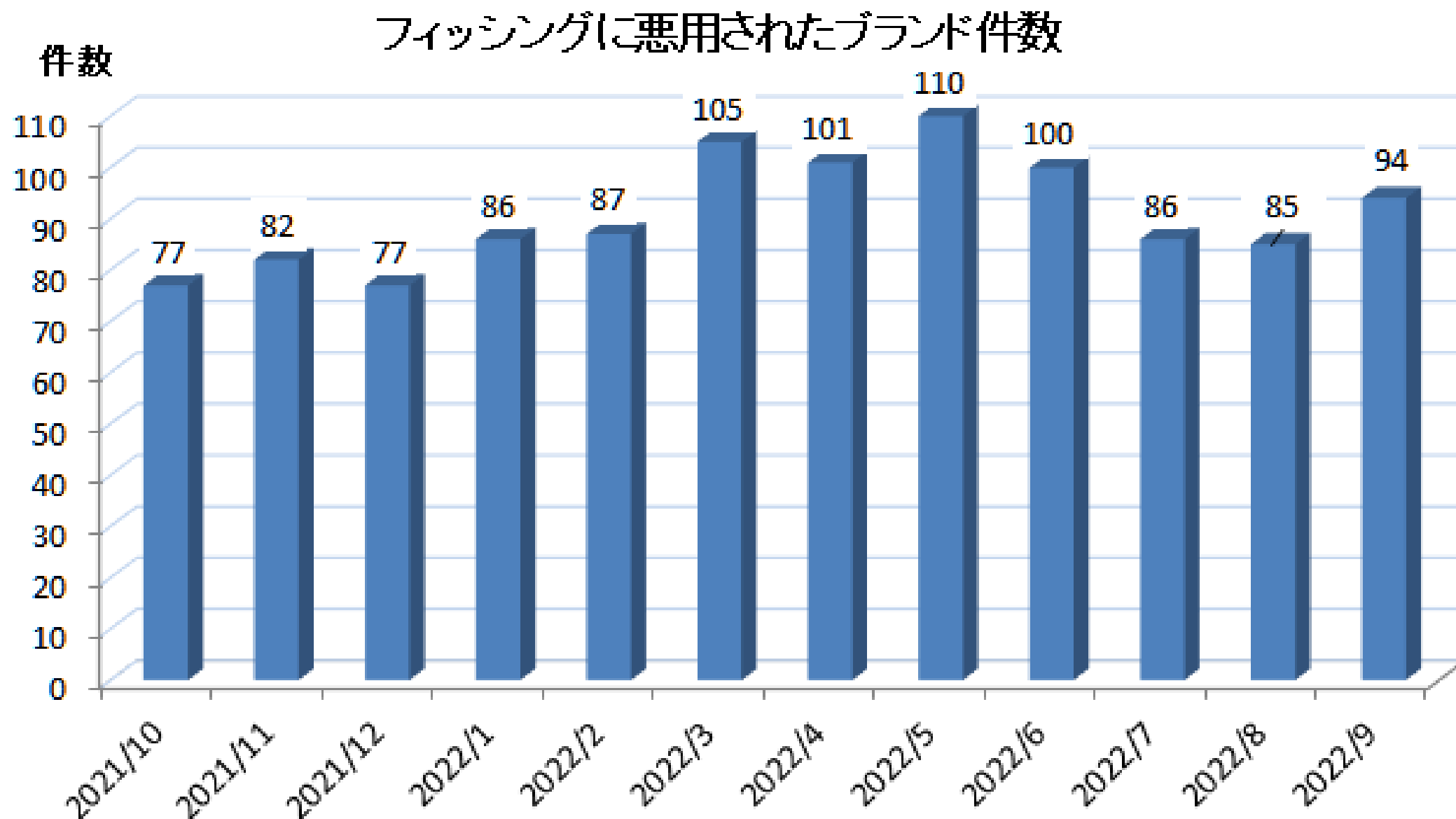
## フィッシングサイトのURL件数



# 2022/9の状況（3）

フィッシング対策協議会より引用

<https://www.antiphishing.jp/report/monthly/>



# 標的の多様化 – 巧妙な手段による収益化

- クレジットカード情報の詐取を目的としたケースが多い
- 詐取したIDで振り込み先変更、保険契約者貸付制度悪用で金銭不正授受などの事例も（生保）

| 業種         | 標的ブランド                                            |
|------------|---------------------------------------------------|
| 邦銀系        | メガバンク、ネットバンク、地銀・都市銀                               |
| クレジットカード系  | 銀行系、国際ブランド、地方ブランド、ペイメントサービス                       |
| FinTech系   | 仮想資産サービス・プロバイダー（VASP:VirtualAssetServiceProvider） |
| モバイル系      | 大手通信キャリア、メッセージャー                                  |
| ネットショッピング系 | 家電量販店、ネットショッププラットフォーム、フリーマーケット                    |
| 運送系        | 国内運送                                              |
| 生命保険系      | 生命保険                                              |
| その他 アカウント系 | コンビニ、ISP、メールサービス、公的サービス、インフラ、クラウドサービス             |

# 詐欺と正規の見分けは困難（１）



## ■ メール / SMS

- 送信者・送信元メールアドレスは簡単に偽装できる
- SMSは情報量が少ないため正規かどうかの判断が困難

## ■ webページ

この文字はUTF-8でCE BF(“o”は6F) “m(エム)”ではなく“rn(アールエヌ)”

- URLを目で見て判断できない (yahoo.jp / rnicrosoft .com)
- サブドメインに正規ドメインを入れる手口

# 詐欺と正規の見分けは困難（2）

普通のなりすまし送信

メールソフトの表示では見分けがつかない

差出人: "Amazon.co.jp" <account-update@amazon.co.jp>  
日時: 2021年7月8日 9:44:47 JST  
件名: 【アマゾン】注文状況が変更されました

お客様の注文とアマゾン アカウントを変更させていただいております。請求先住所が変更されたなど、理由で発生する可能性があります。アカウントにログインして画面の指示に従うことで、アカウントの停止状態を解除していただけます。

他組織のドメインを使ってなりすまし送信

自分関係ない、と思っ  
ていても巻き込まれる

From: 楽天市場 <admini@rakuten.co.jp>  
日付: 2021/07/07 5:28  
件名: Amazon.co.jp アカウントの支払い方法を確認できず、注文を出荷できません。



Amazon お客様 [REDACTED]

Amazon に登録いただいたお客様に、Amazon アカウントの情報更新をお届けします。  
残念ながら、Amazon のアカウントを更新できませんでした。

受信者のメールアドレス  
や  
他人のメールアドレス  
を使って送信

自分関係ない、と思っ  
ていても巻き込まれる

差出人: [REDACTED]@k6.dion.ne.jp <[REDACTED]@[REDACTED].com>  
日時: 2021年7月8日 7:56:55 JST  
宛先: [REDACTED] <[REDACTED]@k6.dion.ne.jp>  
件名: Rakuten.co.jp(ご登録のアカウント(名前、パスワード、その他個人情報)の確認  
CID:856734

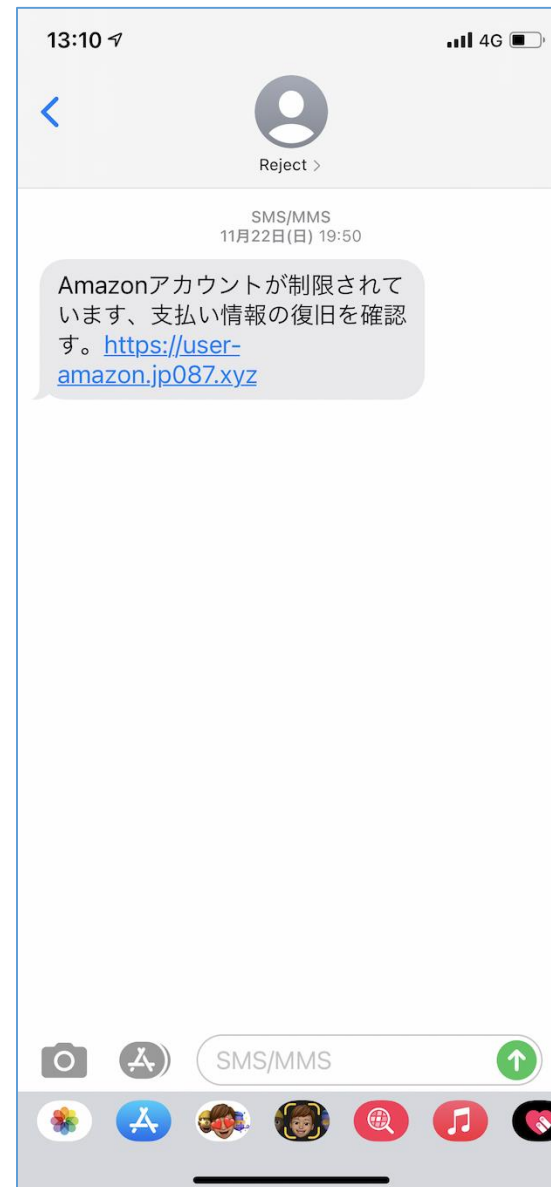
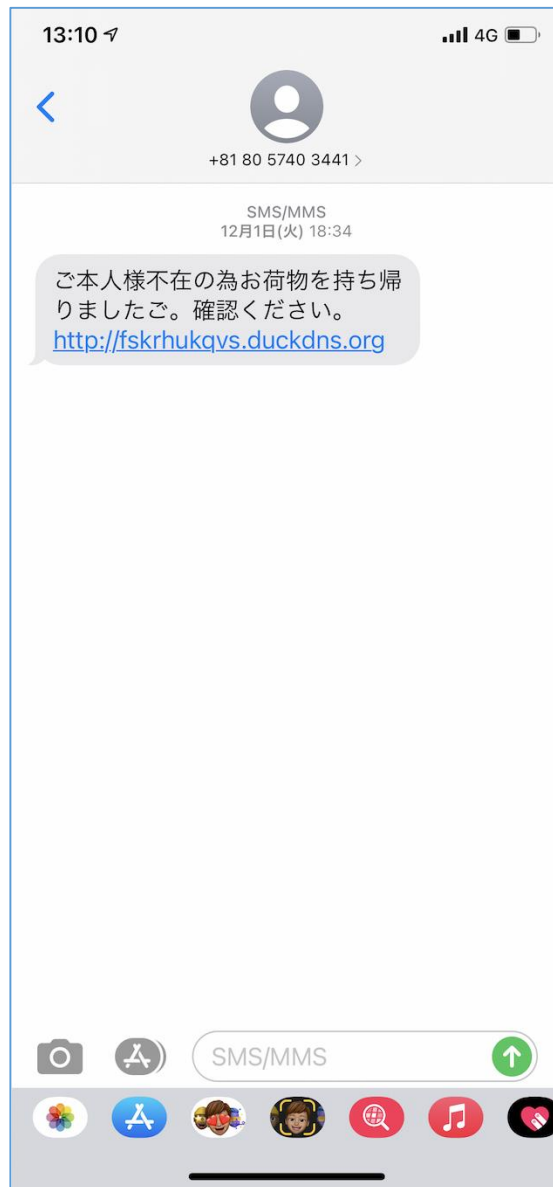
**Rakuten Card**

本メールはお客様によるお楽天アカウントのご更新が必要な場合にお知らせする

[REDACTED]@k6.dion.ne.jp様

お客様の注文と楽天アカウントを停止させていただいております。請求先住所が変更されたなど、理由で発生する可能性があります。アカウントにログインして画面の指示に従うことで、アカウント

# 詐欺と正規の見分けは困難（3）



# 詐欺と正規の見分けは困難（４）



**Paidyアプリなら予算の設定や  
コンビニでの  
バーコード支払いが可能に**



 App Store  
からダウンロード

 Google Play  
で手に入れよう

**MyPaidyにログイン**

Paidyで使用したメールアドレスと携帯電話番号を入力してください。ログインに必要な認証コードをお送りします。

※ Paidyのご利用が初めての方は、以下の同意条項をご確認いただき、同意の上でご入力ください。

メールアドレス  
hello@paidy.com

個人情報取扱に関する同意条項に同意して

次へ

携帯電話番号の変更はこちら

© Paidy Inc.



**Paidyアプリなら予算の設定や  
コンビニでの  
バーコード支払いが可能に**



 App Store  
からダウンロード

 Google Play  
で手に入れよう

**MyPaidyにログイン**

Paidyで使用したメールアドレスと携帯電話番号を入力してください。ログインに必要な認証コードをお送りします。

※ Paidyのご利用が初めての方は、以下の同意条項をご確認いただき、同意の上でご入力ください。

携帯電話番号  
09000000000

個人情報取扱に関する同意条項に同意して

次へ

携帯電話番号の変更はこちら

© Paidy Inc.

**LINE Pay**

**本人確認システム**

LINE Payでは、不正利用を未然に防ぐため、所定の手続きでの「本人確認」を行っています。

携帯電話番号

確認のクエリ

お問い合わせ| プライバシーポリシー| 利用規約| グローバル

LINE Pay をかたるフィッシング (2022/01/11)

**LINE Pay**

**アカウントで不正な取引がありました。払い戻しを申請できません**

LINE Payでは、第三者による不正行為によって発生した損害を補償する制度を導入しています。

**補償の申請方法**

LINE Payのお問い合わせフォームに、お支払い情報を入力し、「払い戻しを申し込む」を選択して、払い戻しリクエストを送信してください。

システムは、24時間以内に疑わしいトランザクションを確認します。

承認後、補償額は48時間以内に自動的に銀行カードに送金されます。

払い戻しの確認

お問い合わせ| プライバシーポリシー| 利用規約| グローバル

**LINE Pay**

送金・支払い・出金など全てのLINE Payサービスが補償の対象となり、損害額はLINE Payがカバーします。

カード所有者

クレジットカード番号   

MM YYYY CVV 

郵便番号

払い戻しを申し込む

お問い合わせ| プライバシーポリシー| 利用規約| グローバル

# 技術だけでは解決が困難なことも



- ブランドホルダー管理外のところで発生する被害
  - 見えないものや理解できないものを保護することはできない
  - 外部で発生する被害を常時監視することはできない
- セクターを越えた被害状況の把握
  - Aセクターを狙った攻撃が、明日はBセクターで発生するかも？
  - 他社の状況について把握することは困難



# スミッシングの増加

---

## SMSを使ったフィッシング詐欺 Smishing = SMS + phishing



本日商品を発送致しました。  
詳細は配送状況をご確認ください。  
[http://ntdocomc\[redacted\].ddns.net](http://ntdocomc[redacted].ddns.net)

出典: フィッシング対策協議会

# SMSの特徴

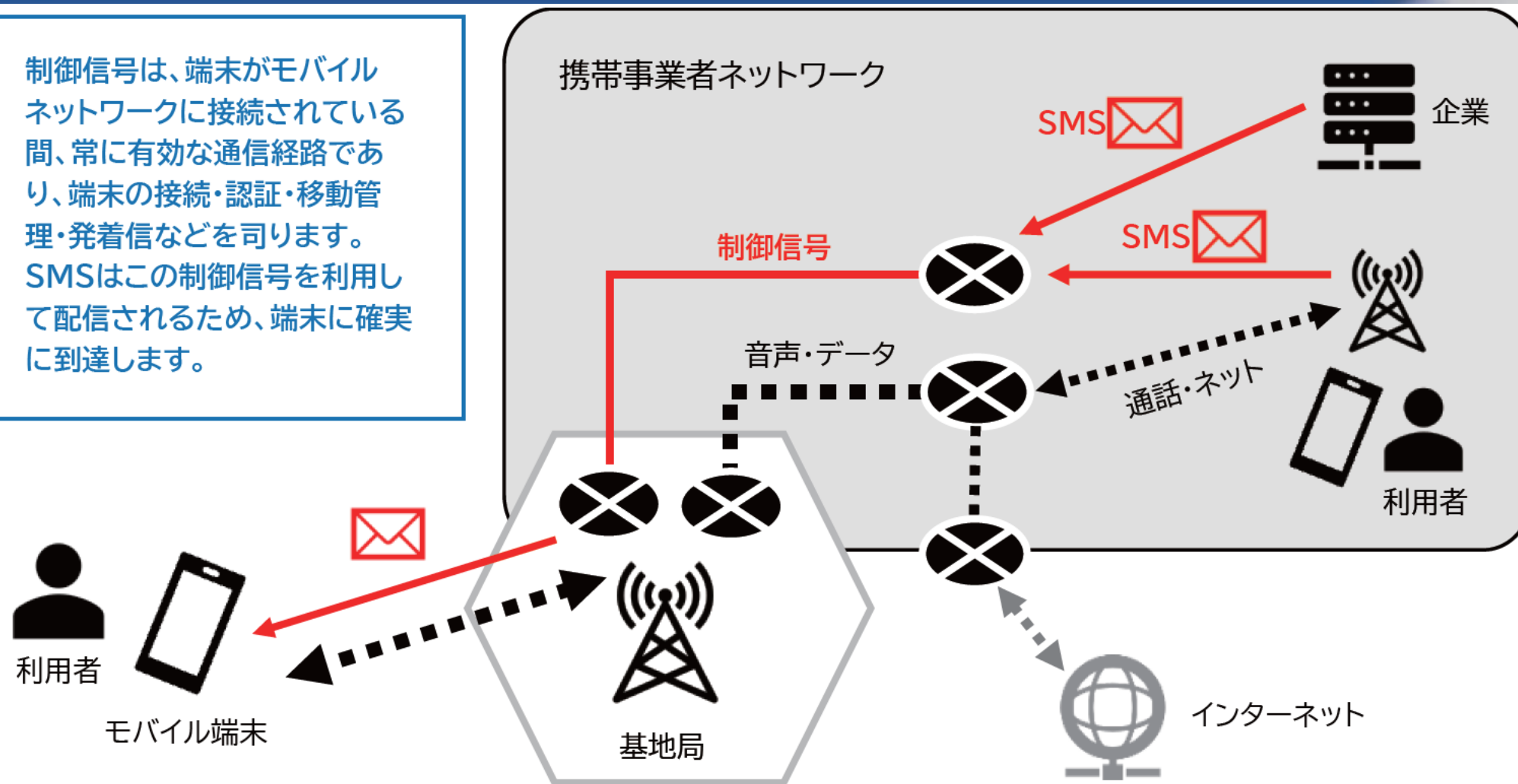


SMSは電話番号と紐づいており確実に届き、開封率が高いと言われる

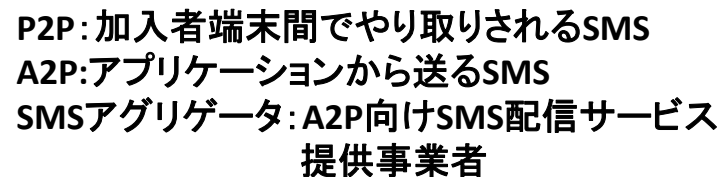
|           | 電子メール                    | SMS                                                    |
|-----------|--------------------------|--------------------------------------------------------|
| 端末への配信方式  | プル方式                     | プッシュ方式（強制受信）                                           |
| 発信者ID     | メールアドレス                  | 自由に設定できる（余地が大きい）                                       |
| 受信者       | メールアドレス                  | 電話番号                                                   |
| 迷惑メールフィルタ | 受信者の許諾を得ることで送信元や内容で判定OK  | 通信の秘密の取り扱いについて公式には未整理                                  |
| 送信料金      | 無料                       | 有料                                                     |
| メッセージ長・形式 | 長さは自由<br>形式はテキスト or HTML | 1通あたり半角英数字160文字<br>（連結すれば半角英数字1530文字）<br>形式はプレーンテキストのみ |

# SMSの仕組み

制御信号は、端末がモバイルネットワークに接続されている間、常に有効な通信経路であり、端末の接続・認証・移動管理・発着信などを司ります。SMSはこの制御信号を利用して配信されるため、端末に確実に到達します。



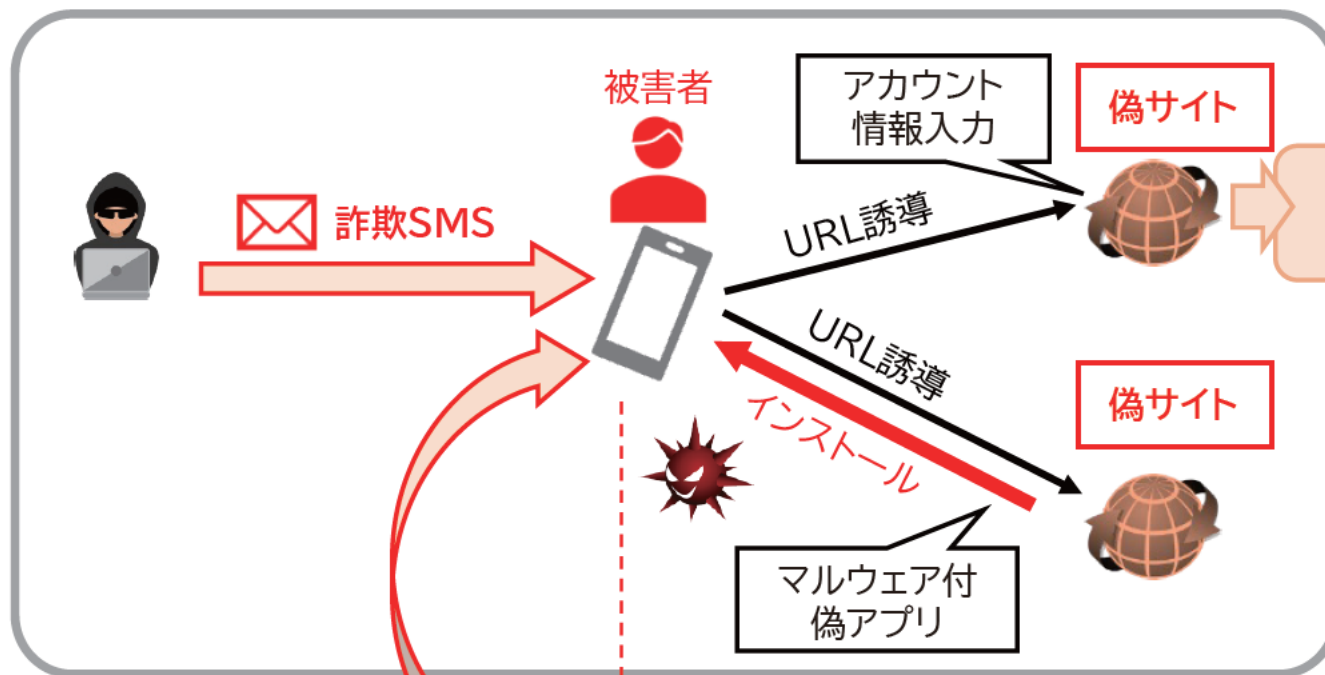
レポート「スミッシングの実態と対策」, マクニカ,  
[https://www.macnica.co.jp/business/security/mnc/phishing\\_report\\_202207.pdf](https://www.macnica.co.jp/business/security/mnc/phishing_report_202207.pdf)



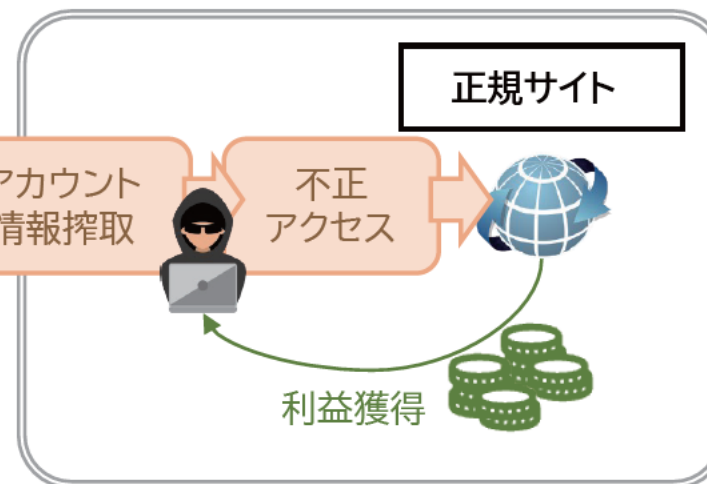
 **フィッシング対策協議会**  
Council of Anti-Phishing Japan

# スミッシング被害の流れ

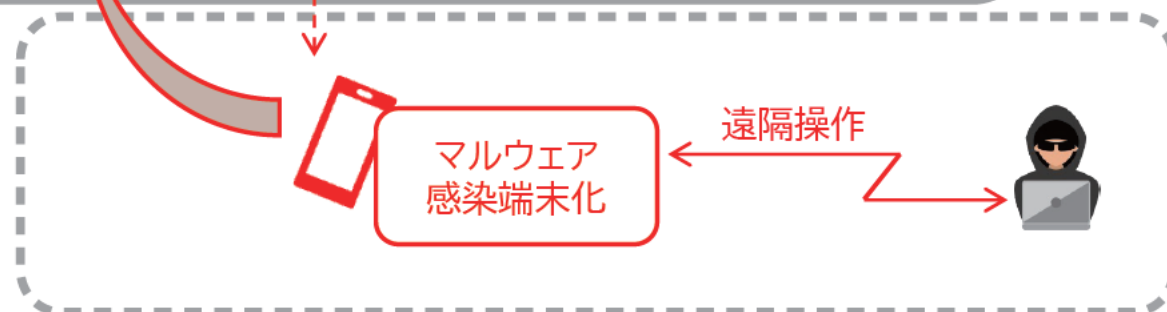
## SMS配信～偽サイト誘導



## 目的実行

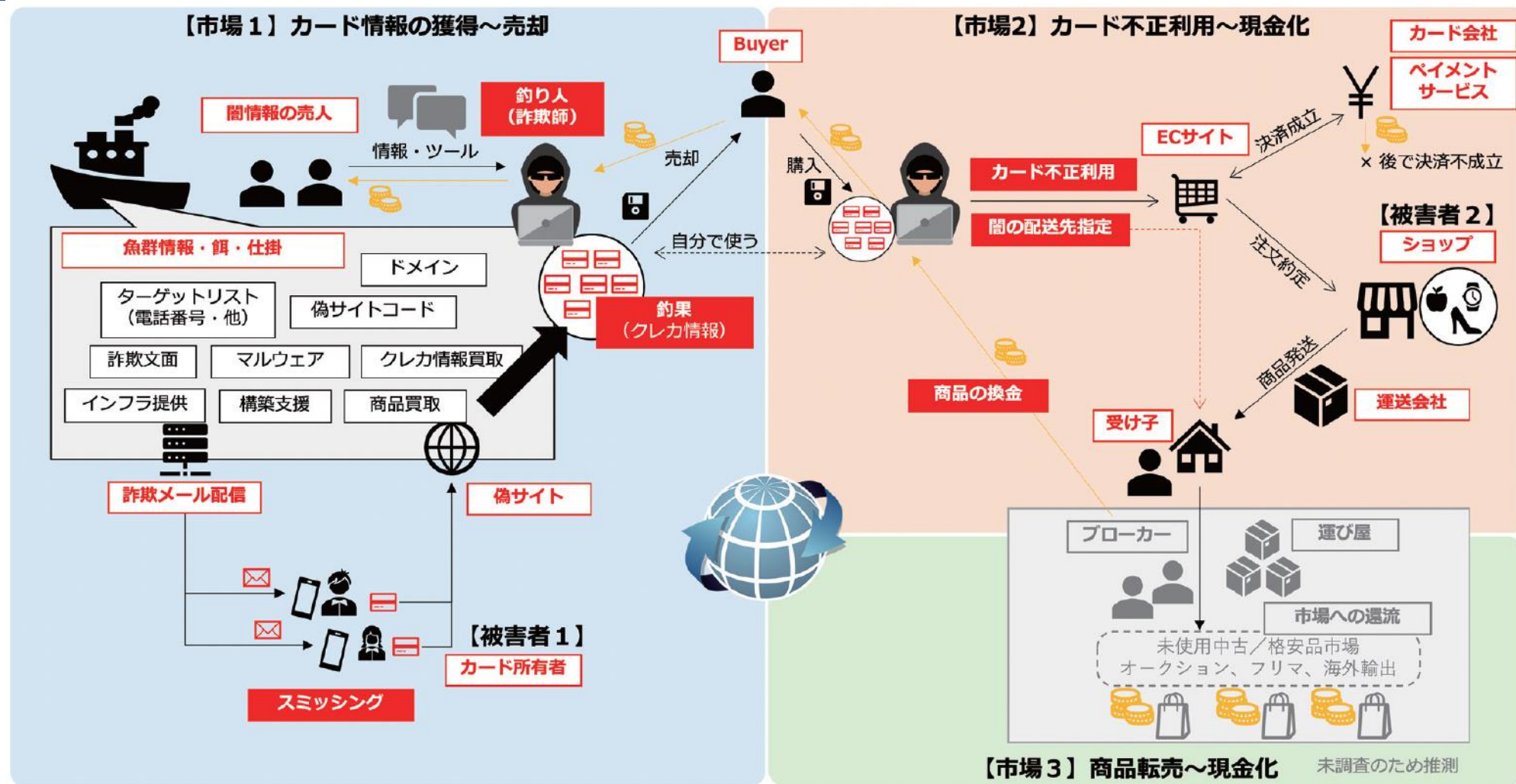


## 踏み台確保



レポート「スミッシングの実態と対策」, マクニカ,  
[https://www.macnica.co.jp/business/security/mnc/phishing\\_report\\_202207.pdf](https://www.macnica.co.jp/business/security/mnc/phishing_report_202207.pdf)

# スミッシング犯罪のエコシステム

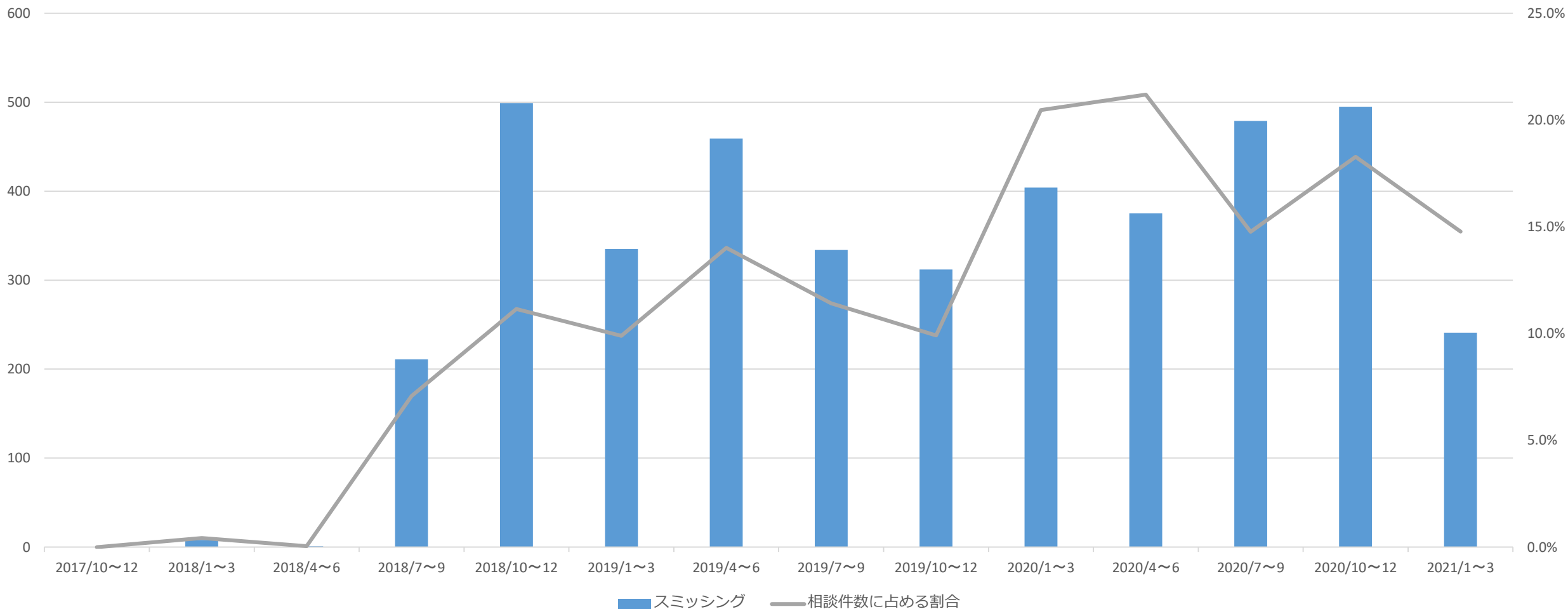


レポート「スミッシングの実態と対策」, マクニカ,  
[https://www.macnica.co.jp/business/security/mnc/phishing\\_report\\_202207.pdf](https://www.macnica.co.jp/business/security/mnc/phishing_report_202207.pdf)

# スミッシングによる被害件数



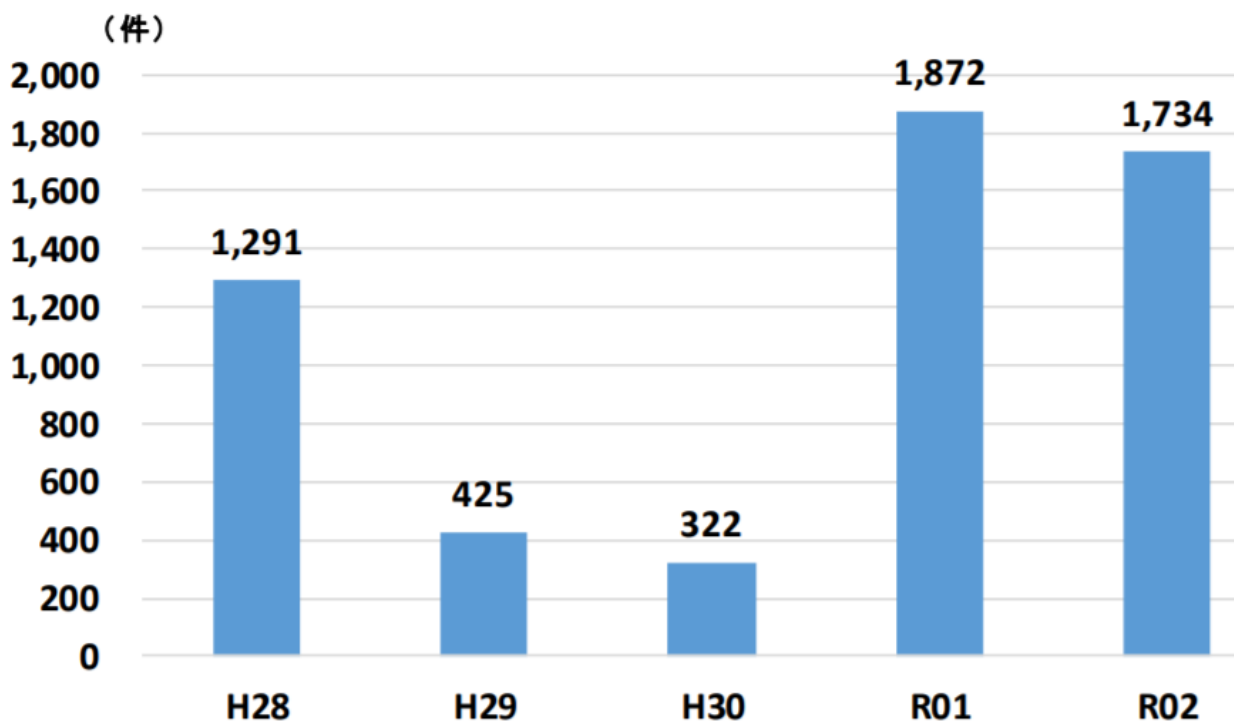
「宅配便業者をかたる偽SMS」相談件数の推移(3か月ごと)



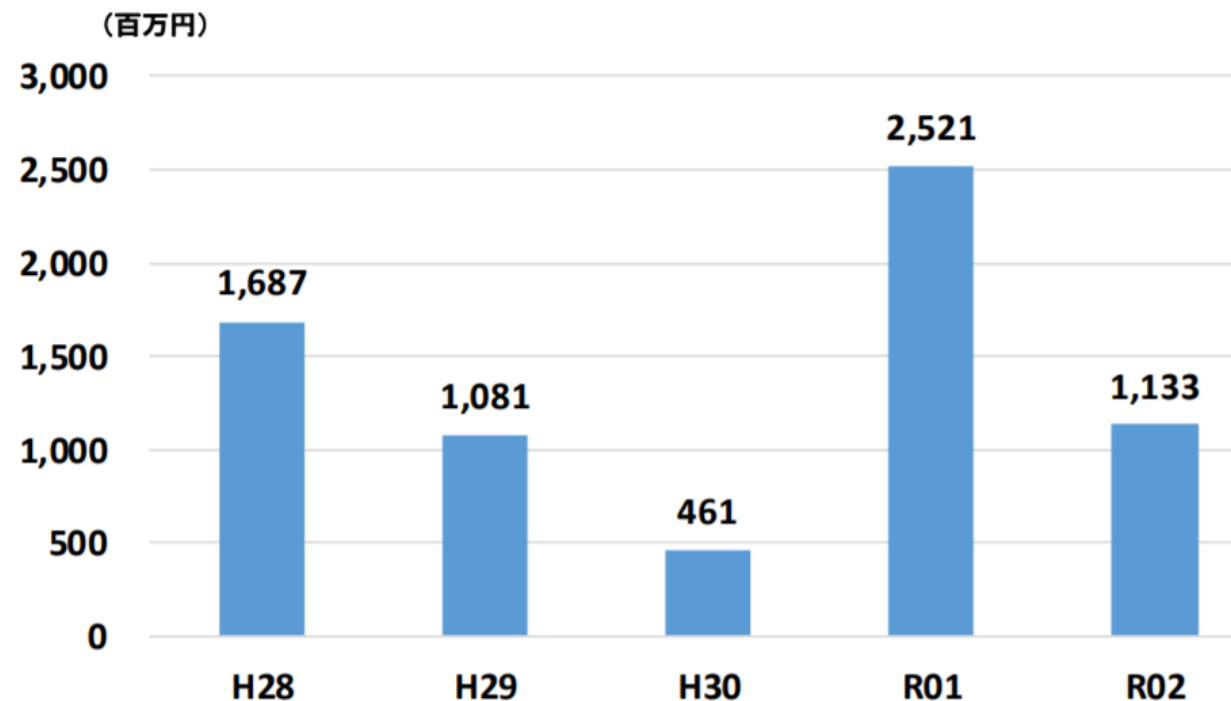
出典) <https://www.ipa.go.jp/security/txt/2021/q1outline.html>、<https://www.ipa.go.jp/security/txt/2019/q4outline.html>、<https://www.ipa.go.jp/security/txt/2018/q4outline.html>

# ネットバンク不正送金の発生数

【図表12：インターネットバンキングに係る不正送金事犯の発生件数の推移】



【図表13：インターネットバンキングに係る不正送金事犯の被害額の推移】



出典: [https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02\\_cyber\\_jousei.pdf](https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_cyber_jousei.pdf)



# フィッシングという「ビジネス」

---

# フィッシング「ビジネス」の分析

- 協議会・学術研究WGでは「フィッシング詐欺のビジネスプロセス分類」を分析し、結果を公開

## :: 協議会からのお知らせ

### 「フィッシング詐欺のビジネスプロセス分類」を公開 (2021/03/16)

2021年03月16日

協議会は、長崎県立大学との [共同研究プロジェクト](#) の活動成果の1つとして、学術論文「フィッシング詐欺のビジネスプロセス分類」を公開しました。

この内容は、3月15日(月)に第186回マルチメディア通信と分散処理・第92回コンピュータセキュリティ合同研究発表会にて発表いたしました。

フィッシング詐欺には、ウェブサイトを模倣したもの、偽のアプリを利用したもの、電子メールやテキストメッセージ、音声メッセージを利用したものなど、様々な種類があります。このため、これら様々なタイプのフィッシング詐欺に対抗可能な本質的な方法は未だ確立されていないのが現状です。したがって、効率的な対策方法を特定するために、フィッシング詐欺の全体像を把握することが不可欠です。本研究では、フィッシング詐欺をビジネスであると定義し、その営利活動におけるプロセス进行分类することを試みました。その手法として、2つの事例分析を実施しました。結果として、提案手法が実際のフィッシング詐欺を特定するためのプロセスとして適用可能であることを確認することができました。提案手法を用いることで、フィッシング詐欺におけるプロセスを体系的に理解し、フィッシング詐欺の脅威を予測することが容易になりました。

[フィッシング詐欺のビジネスプロセス分類 \(論文\)](#) (PDF : 817KB) 

[フィッシング詐欺のビジネスプロセス分類 \(CSEC発表資料\)](#) (PDF : 1.10MB) 

# フィッシング詐欺の全体的なプロセス

犯罪者は効率的に利益を得るために様々な手法を組み合わせる

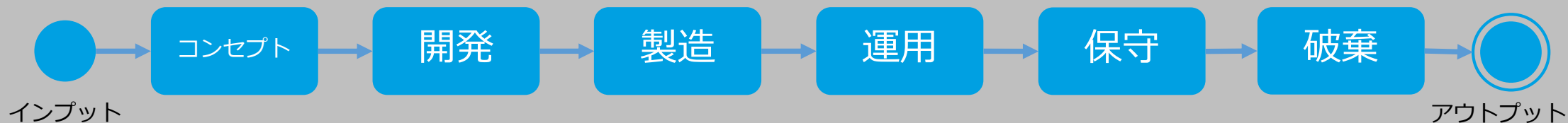


# 研究目的：全体像把握 & 対策の検討

犯罪者は効率的に利益を得るために様々な手法を組み合わせる



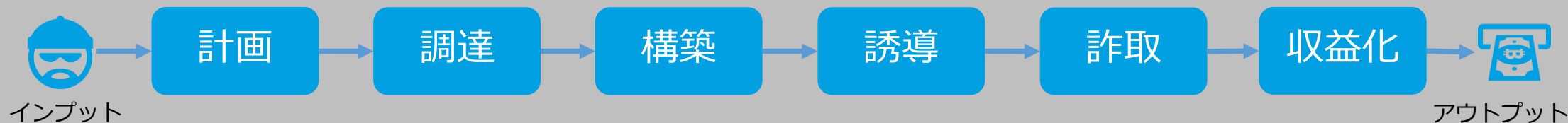
インプットをプロセスアクティビティにて処理し, アウトプットに変換する活動, ISO 15288:2015



図：一般的なシステムライフサイクルフェーズ



フィッシング詐欺をビジネスとして捉える. 6つの活動を定義



図：フィッシング詐欺ビジネスプロセス

## フィッシング詐欺ビジネスプロセスの提案. 共通ルールで分析

# 研究方法：ケーススタディ



フィッシング詐欺ビジネスプロセスを2つの事例に対し照合

- **事例1: 16Shop フィッシングキット**

同一の「[Phishing as a Service \(PHaaS\)](#)」**提供者**による変遷に注目

- **事例2: LINEを騙るフィッシング詐欺**

同一の「[標的](#)」を狙う**詐欺者**の変遷に注目

|       | 16Shop事例分析        | LINE事例分析           |
|-------|-------------------|--------------------|
| 観測期間  | 2018年7月 – 2018年8月 | 2016年10月 – 2020年5月 |
| 調査対象数 | 115 URLs（無作為に抽出）  | 1,025 URLs         |
| TLD   | 22 件              | 14件                |
| AS番号  | 39 件              | 51件                |

※件数はすべて重複を除く、ユニーク件数

# フィッシングビジネスプロセスの理解

## プロセスの体系的な理解により、各段階の主要因子を特定

| フィッシング詐欺<br>ビジネスプロセス | 16Shop事例分析により<br>判明した因子                | LINE事例分析により<br>判明した因子                     |
|----------------------|----------------------------------------|-------------------------------------------|
| 計画                   | 動機, 機会, 標的, <b>詐欺の開始時期</b> , 詐取を狙うeKYC | 動機, 機会, 標的, <b>誘導試行回数の期待値</b> , 詐取を狙うeKYC |
| 調達                   | 調達先の傾向, <b>調達サービスを支えるコミュニティ</b>        | 調達先の傾向                                    |
| 構築                   | <b>技術習熟度</b> , 帰属情報                    | <b>構築期間</b> , <b>設置のタイミング</b>             |
| 誘導                   | 疑念払拭の手法, 作業品質                          | 疑念払拭の手法, 作業品質                             |
| 詐取                   | 被害認知に至るまでの引き延ばし工作                      | 被害認知に至るまでの引き延ばし工作                         |
| 収益化                  | 換金対象, <b>二次被害</b>                      | 換金対象                                      |

## 主要因子の観測により進行段階の特定、脅威予測/対策を支援する

※補足 **水色**の表記はどちらか一方の事例のみで判明した因子



# フィッシング対策

---

# 事業者による対策・利用者による対策



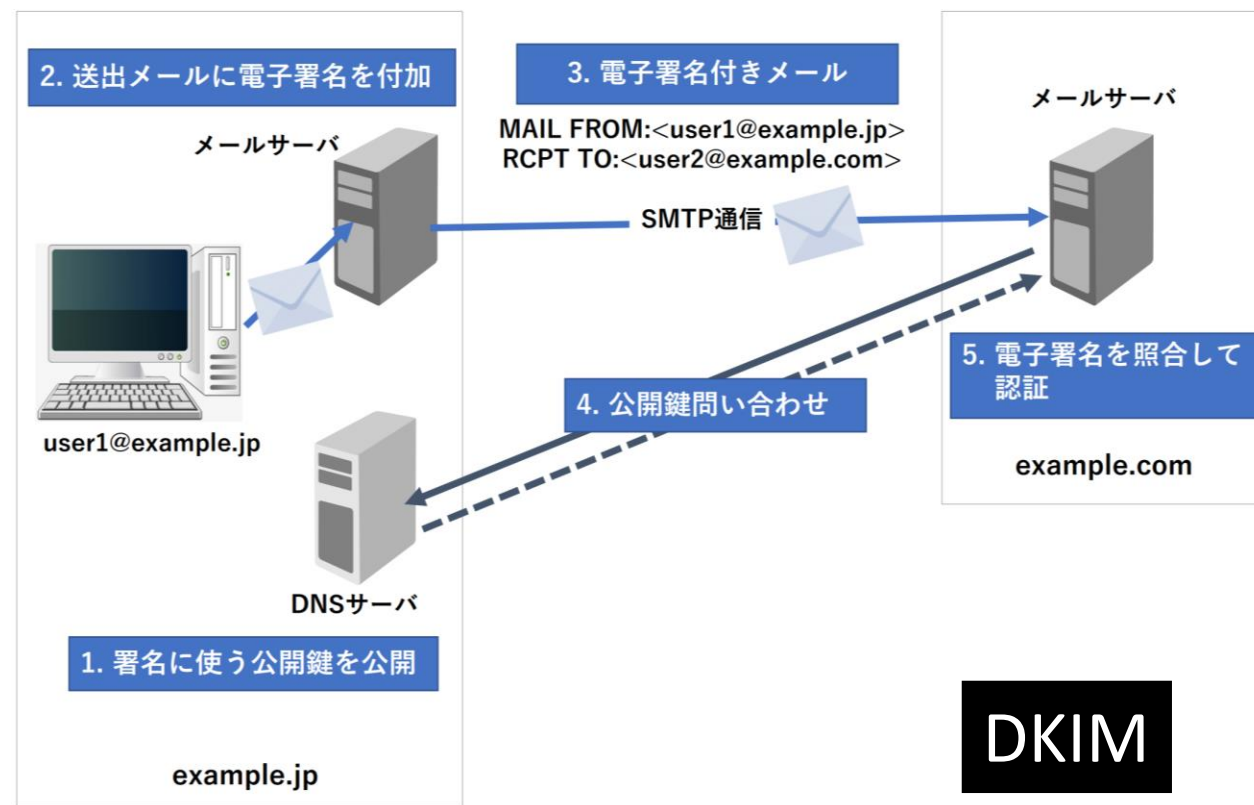
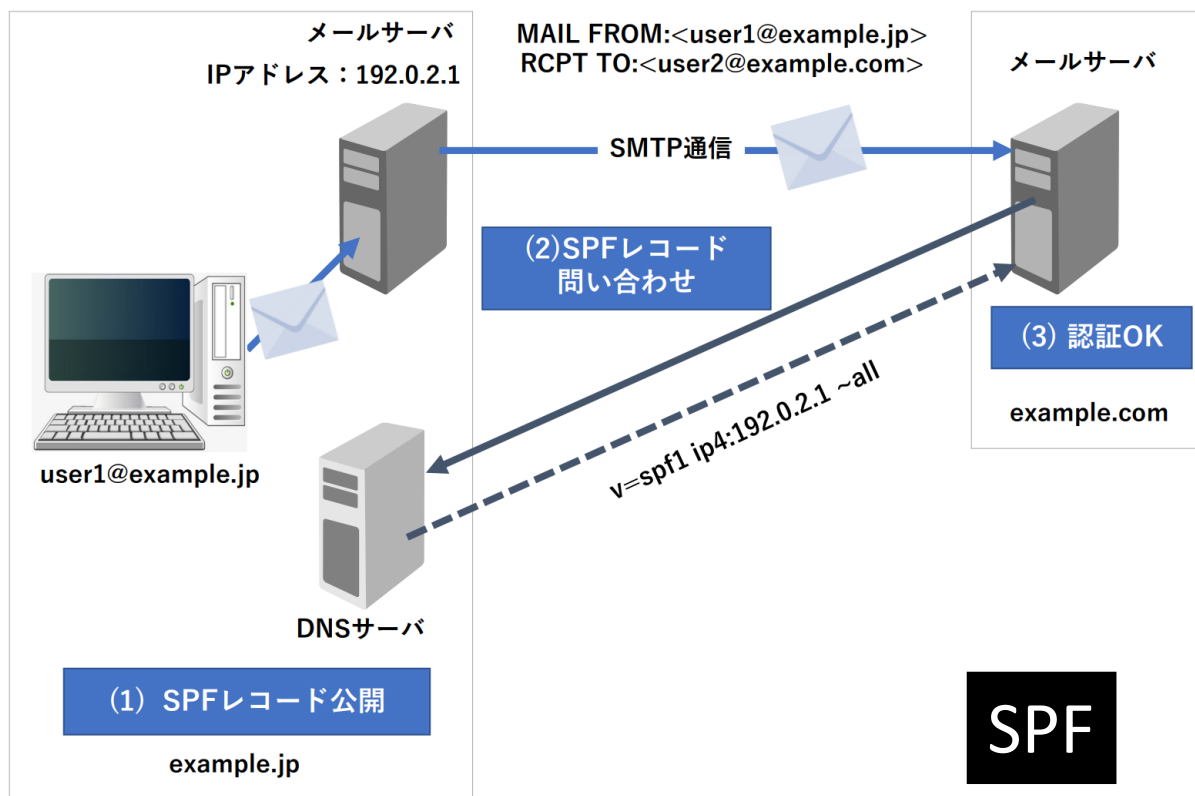
|                                           |
|-------------------------------------------|
| 4. WEBサイト運営者におけるフィッシング詐欺対策.....           |
| 4.1. WEBサイト運営者におけるフィッシング詐欺の被害とは.....      |
| 4.2. 利用者を守るためのフィッシング詐欺対策とは.....           |
| 4.3. フィッシング詐欺被害の発生を抑制するための対策.....         |
| 4.3.1. 利用者が正規メールとフィッシングメールを判別可能とする対策..... |
| 4.3.2. 利用者が正規サイトを判別可能とする対策.....           |
| 4.3.3. フィッシング詐欺被害を拡大させないための対策.....        |
| 4.3.4. ドメイン名に関する配慮事項.....                 |
| 4.3.5. フィッシング詐欺対策のための組織体制.....            |
| 4.3.6. 利用者への啓発活動.....                     |
| 4.4. フィッシング詐欺被害の発生を迅速に検知するための対策.....      |
| 4.5. フィッシング詐欺被害が発生してしまった際の対策.....         |
| 4.5.1. フィッシング詐欺被害状況の把握.....               |
| 4.5.2. フィッシングサイトテイクダウン活動.....             |
| 4.5.3. フィッシングメール注意勧告.....                 |
| 4.5.4. 関係機関への連絡、報道発表.....                 |
| 4.5.5. 生じたフィッシング詐欺被害への対応.....             |
| 4.5.6. 事後対応.....                          |

|                                      |
|--------------------------------------|
| 5. 利用者におけるフィッシング詐欺対策.....            |
| 5.1. フィッシング詐欺への備え.....               |
| 5.1.1. パソコンやモバイル端末は、安全に保つ.....       |
| 5.1.2. 不審なメールに注意する.....              |
| 5.1.3. 電子メールにあるリンクはクリックしないようにする..... |
| 5.1.4. アカウント情報の管理.....               |
| 5.2. フィッシング詐欺に遭ってしまった時.....          |
| 5.2.1. 詐取された情報の識別.....               |
| 5.2.2. 関連機関への連絡.....                 |

フィッシング対策協議会,  
フィッシング対策ガイドライン  
2022年度版目次より抜粋

# 送信ドメイン認証

メールが正規の送信元から送られてきたか、検証できる技術  
現在、SPF、DKIM、DMARCの3種類がある



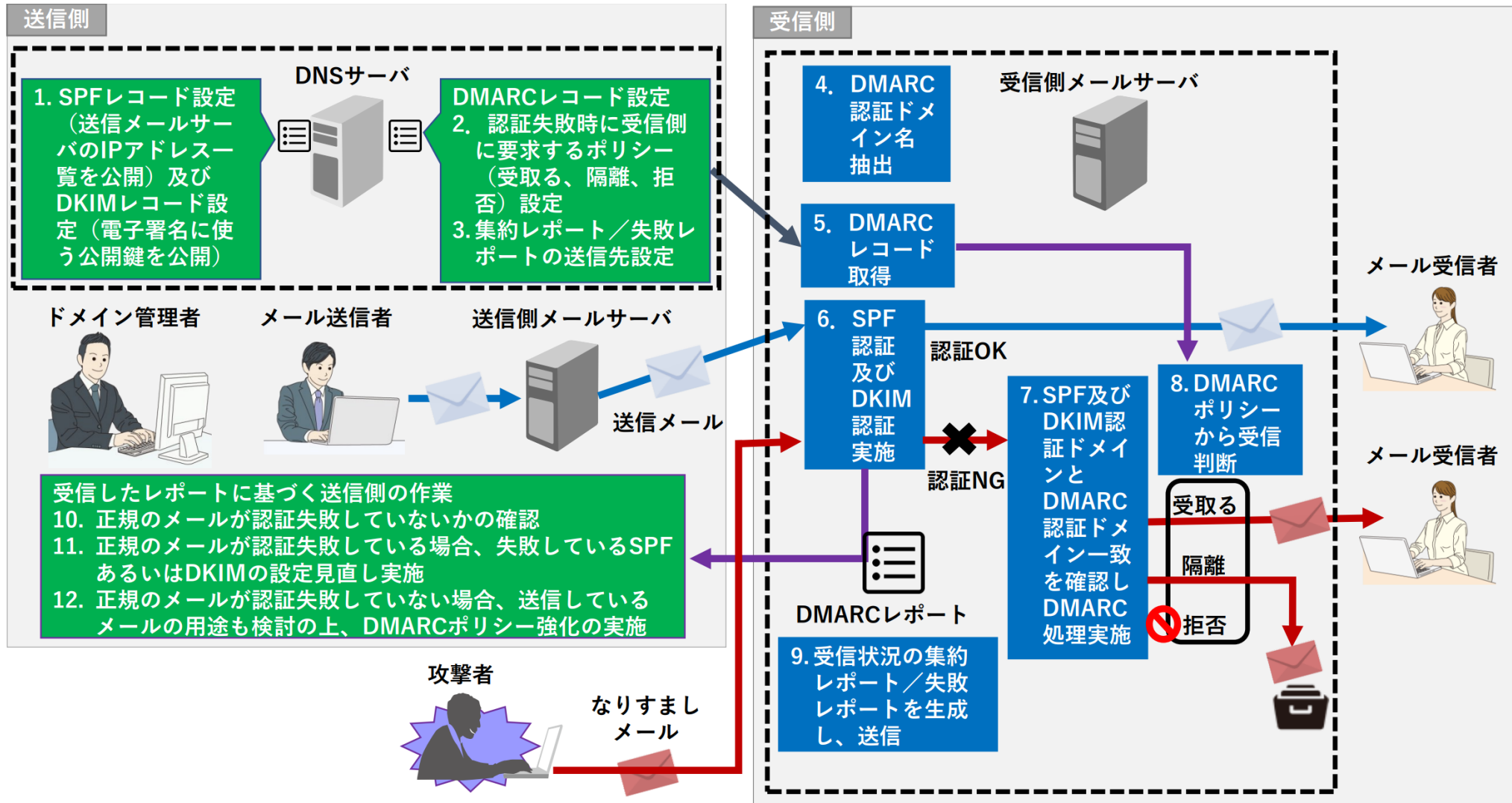
図は [https://www.dekyo.or.jp/soudan/data/anti\\_spam/meiwakumanual3/manual\\_3rd\\_edition.pdf](https://www.dekyo.or.jp/soudan/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf) より引用

# SPFとDKIM



|      |                                                                          |
|------|--------------------------------------------------------------------------|
| SPF  | Sender Policy Framework                                                  |
| 検証方法 | 正規のサーバー(IPアドレス)から送信されたかを検証                                               |
| 検証対象 | メールソフトで表示されないほうのメールアドレス(エンベロップ From)                                     |
| 導入   | 送信側の設定はSPFレコードをDNSへ登録するだけで容易                                             |
| 利点   | 受信時に検証を行っている事業者が多い(しかし多くは fail しても素通し)                                   |
| 欠点   | 単体ではエンベロップ From に独自ドメインを使用して、SPFの検証をpass (回避) するなりすまし送信は検出できない           |
| DKIM | DomainKeys Identified Mail                                               |
| 検証方法 | 電子署名でメールを検証。S/MIMEはメール本文のみが署名対象だが、DKIMはメール配信時につけられるヘッダー情報やメール本文も署名対象にできる |
| 検証対象 | 署名対象の情報(差出人、日付時刻、受信者などのヘッダー情報およびメール本文)                                   |
| 導入   | S/MIMEと同様に、送信側は各メールへDKIM署名するためのシステムが必要                                   |
| 利点   | メールを転送されても検証可能                                                           |
| 欠点   | 署名に使うドメインを指定できるため、単体では検証を回避可能                                            |

# DMARC





## SPFとDKIMの欠点を補い、有用な機能を実現

|       |                                                                                                                                                                                                                                                   |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DMARC | Domain-based Message Authentication, Reporting, and Conformance                                                                                                                                                                                   |
| 検証方法  | SPFとDKIM の検証結果を使って検証。SPF+DMARC など、片方だけでも可                                                                                                                                                                                                         |
| 検証対象  | メールソフトで表示されるほうのメールアドレスで検証                                                                                                                                                                                                                         |
| 導入    | すでにSPFまたはDKIMが設定されていれば、送信側の設定はDMARC レコードをDNS へ登録するだけで容易                                                                                                                                                                                           |
| 利点    | <p>SPFのみでは正規メールとして誤判定されるなりすまし送信を検出できる</p> <p>ドメイン管理者側が、検証失敗したメールの扱いを指定できる<br/>(迷惑メールフォルダーへ配信、拒否等のポリシーを宣言)</p> <p>迷惑メールフィルターも送信ドメイン認証結果を利用するため、組み合わせることで、より効果が高くなる</p> <p>受信側から送られる DMARC レポートで、検証結果や効果を確認できる。正規メールの検証成功数、なりすまし送信の検知、配信規模の把握など</p> |
| 欠点    | 大手のメールサービスは対応しているが、日本国内の事業者や ISP は対応が遅れている                                                                                                                                                                                                        |



# フィッシング対策研究

---

IEEE Xplore Search Results

ieeexplore.ieee.org/search/searchresult.jsp?action=search&newsearch=true&matchBoolean=true&queryText=("%5CDocument%20Title%3Aphishing")

IEEE.org | IEEE Xplore | IEEE SA | IEEE Spectrum | More Sites

SUBSCRIBE

Cart

Create Account

Personal Sign In

IEEE Xplore®

Browse

My Settings

Help

Institutional Sign In

IEEE

All

ADVANCED SEARCH

Search within results

Per Page: 25

Export

Set Search Alerts

Search History

Showing 1-25 of 773 for ("Document Title":phishing) ×

☐ Conferences (689)

☐ Journals (52)

☐ Magazines (25)

☐ Early Access Articles (6)

☐ Books (1)

Show

☒ All Results

☐ Open Access Only

Year

Single Year

Range

2004

2022

From

To

☐ Select All on Page

Sort By: Relevance

☐ Spear-Phishing campaigns: Link Vulnerability leads to phishing attacks, Spear-Phishing electronic/UAV communication-scam targeted

Muhammad Sawood Baig; Faisal Ahmed; Ali Mobin Memon

2021 4th International Conference on Computing & Information Sciences (ICCIS)

Year: 2021 | Conference Paper | Publisher: IEEE

Abstract

HTML

☐ Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email

Need Full-Text

access to IEEE Xplore for your organization?

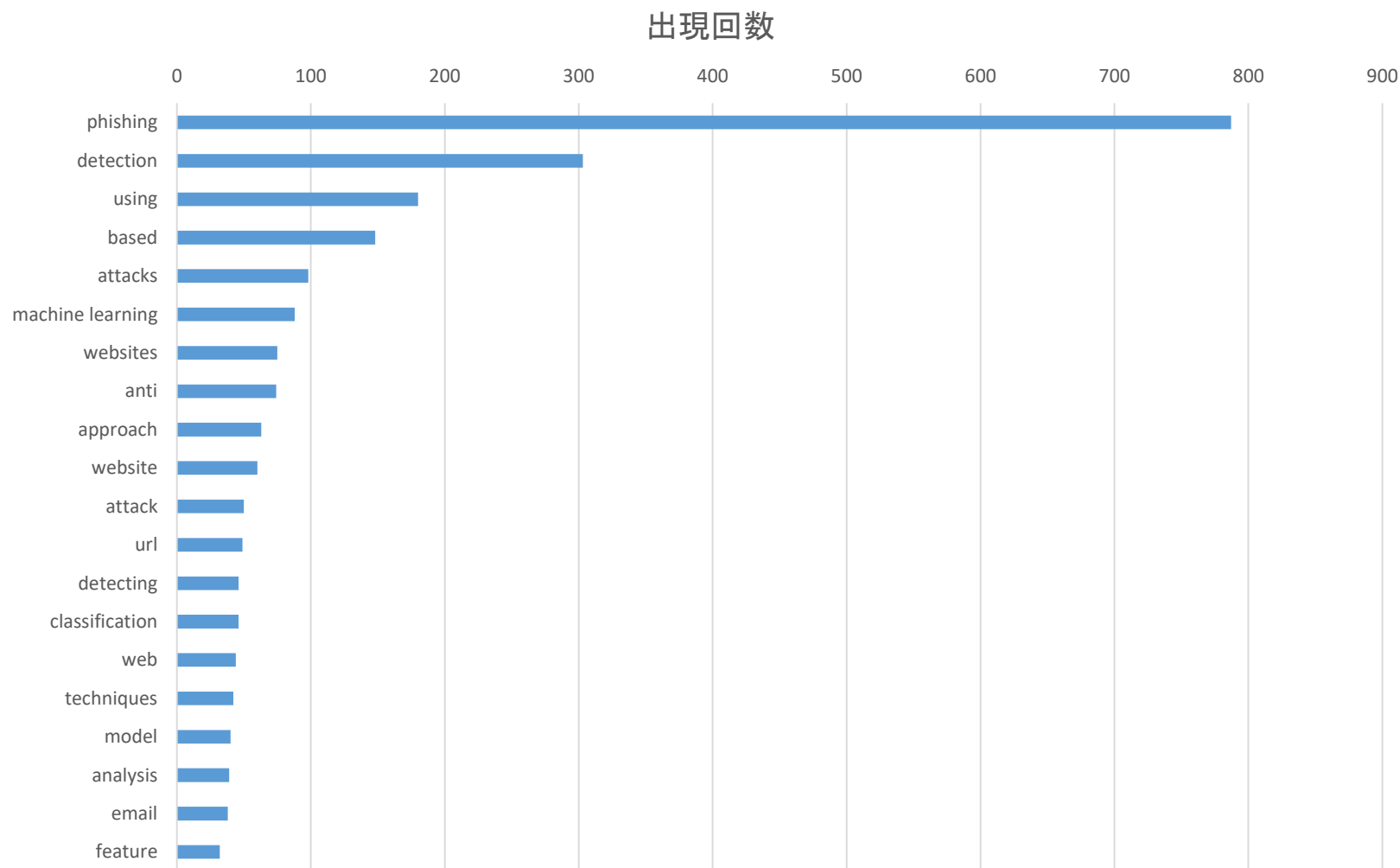
CONTACT IEEE TO SUBSCRIBE >

IEEE

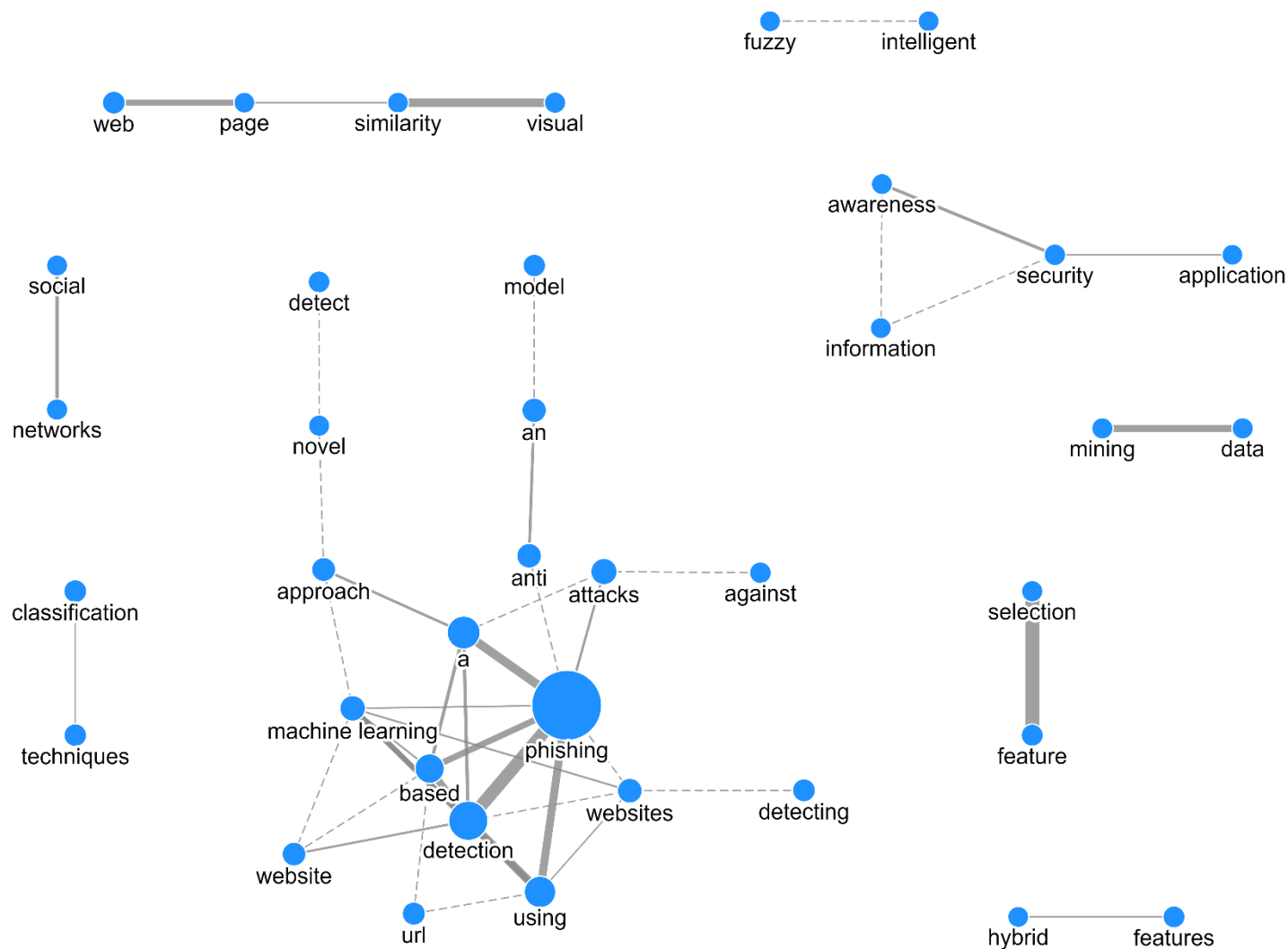
iapp

”phishing”が含まれている773論文タイトル内の名詞を使ってテキストマイニング





# IEEE Xploreから



情報学広場：情報処理学会電子図

+

ipsj.ixsq.nii.ac.jp/ej/?action=pages\_view\_main&active\_action=repository\_view\_main\_item\_snippet&meta=フィッシング&count=20&order=0&pn=1&st=1&page\_id=13&block\_id=8

新規登録 | ログイン

情報処理学会

Information Processing Society of Japan

電子図書館

お知らせ

※**ユーザ登録は無料です。**

情報学広場に掲載されているコンテンツには有料のものも含まれています。  
有料コンテンツをご購入いただいた場合でも、領収書の発行はいたしておりません。  
クレジットカード会社様からの領収書/請求書をもってかえさせていただいております。  
本電子図書館のご利用にあたっては「情報処理学会電子図書館利用規約」をご遵守下さい。

**複写および転載をされる方へ**

一般社団法人情報処理学会では複写複製および転載複製に係る著作権を学術著作権協会に委託しています。当該利用をご希望の方は、**学術著作権協会**が提供している複製利用許諾システムもしくは転載許諾システムを通じて申請ください。尚、本会会員（賛助会員含む）および著者が転載利用の申請をされる場合については、学術目的利用に限り、無償で転載利用いただくことが可能です。ただし、利用の際には予め申請いただくようお願い致します。

※情報処理学会発行の刊行物に掲載されている製品名等は、各社の商標または登録商標です。

WEKO

トップ

ランキング

フィッシング

検索

詳細検索

☐ 全文検索

☒ キーワード検索

Language

日本語

検索結果

1 - 20 of 118 items

チェックしたアイテムをExport

実行

表示順

出版年（降順）

表示数

100

The latest issue of the following contents can be found on J-Stage. Please click on the following link:

[Journal of Information Processing\(JIP\)](#)

[Bioinformatics\(TBIO\)](#)

[System LSI Design Methodology\(TSLDM\)](#)

[Computer Vision and Applications\(CVA\)](#)

システムメンテナンスのお知らせ

AM2:00頃～AM5:00頃はシステムメンテナンスのためアクセスしにくい場合がありますが、ご理解のほどお願いいたします。

**システムメンテナンスのお知らせ（2022-10-21）**

下記時間帯におきまして、情報学広場のシステムメンテナンスを行います。  
システムメンテナンス中は、サイトを停止いたします。

【作業期間】  
2022年 11月9日（水） 14:00-17:00

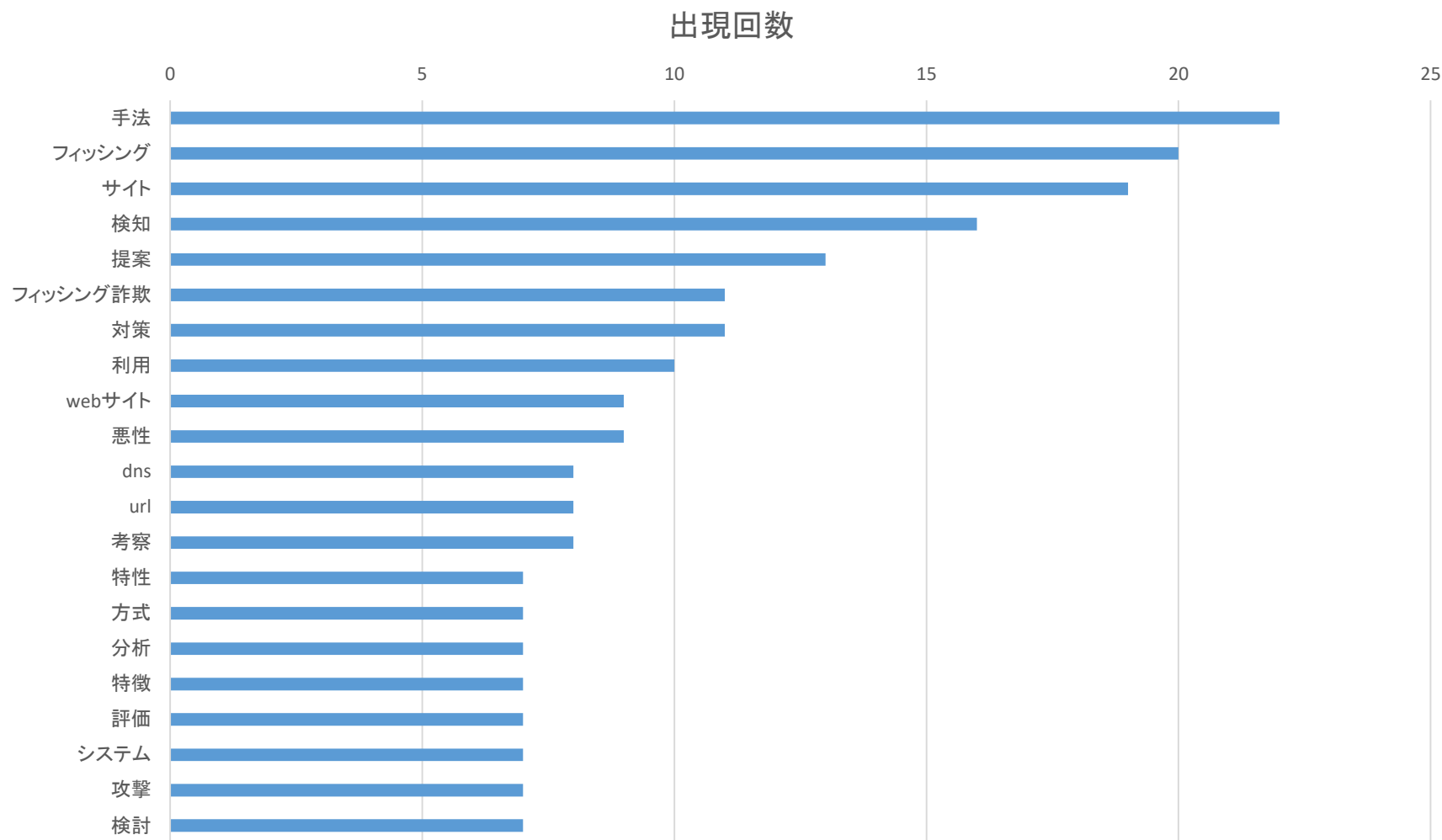
ご利用の皆さまには大変ご不便をおかけしますが、ご理解賜りますようお願い申し上げます。

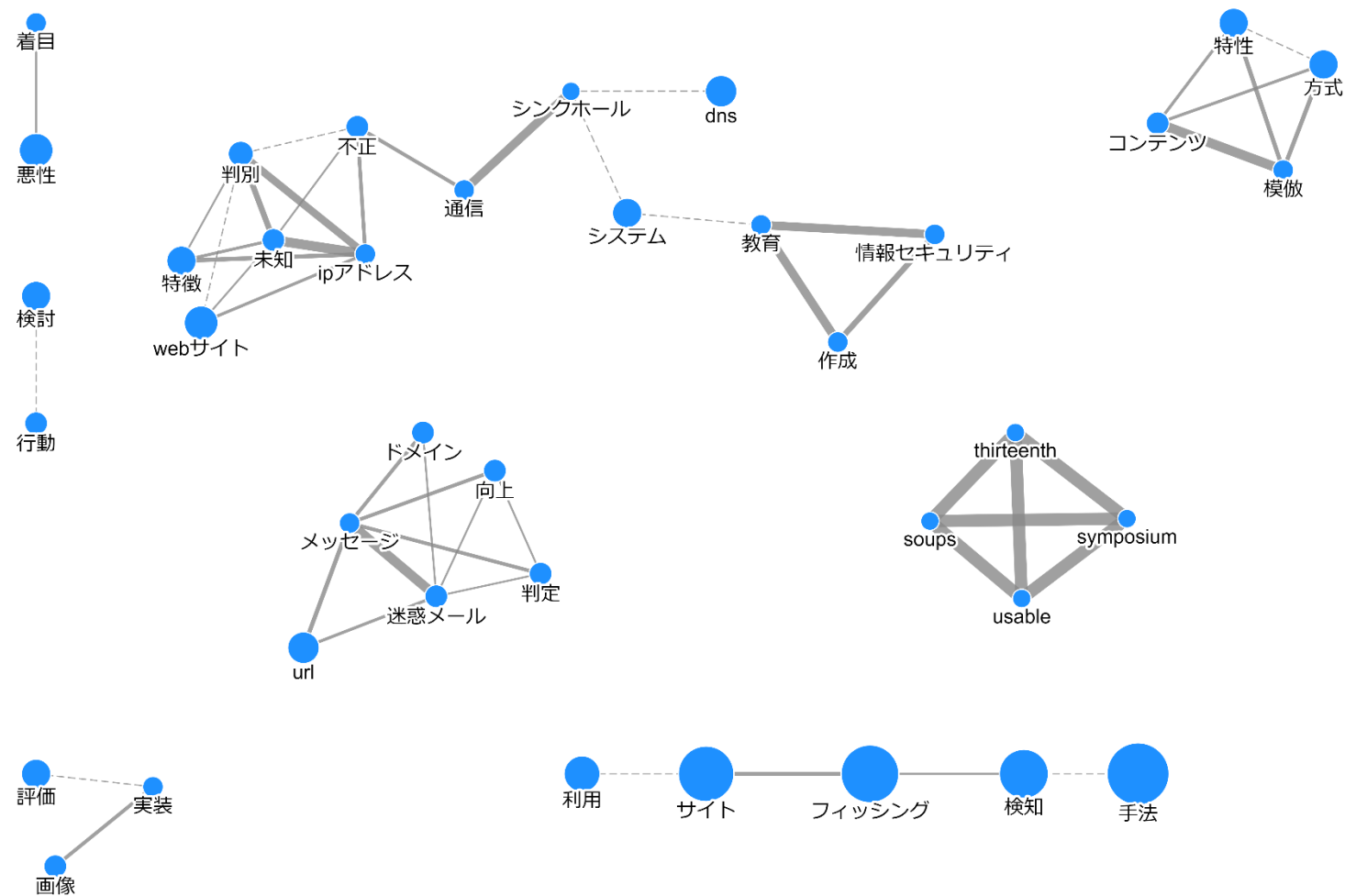
フィッシング対策協議会

f Anti-Phishing Japan

「フィッシング」が含まれている(重複を除いた) 94論文タイトル内の名詞を使ってテキストマイニング







# なんとなくの傾向（私見）



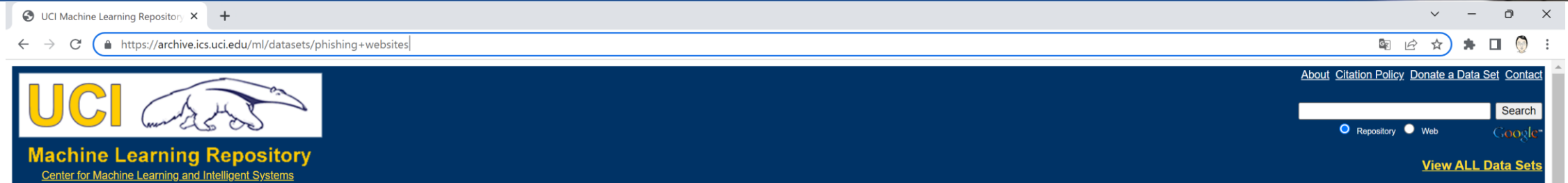
- これだけでは何とも言い難いものの・・・
- フィッシングサイトやフィッシングメールの検出に着目した論文が多そう
- 海外では単体要素（ドメイン等）への着目より、説明変数が多い機械学習が主流か
- Language Barrier（英語vs日本語）もありそう
- DMARC関連論文を検索してみたところ、（あまり関係なさそうなのも含んで）IEEEで21本、IPSIで16本
- 対策事業者と研究者の間にはギャップがあるかも
- （傾向とは違うが）そもそもフィッシングというキーワードがいまい？



# 研究用リソース

---

# UCI Phishing Websites Dataset



Check out the [beta version](#) of the new UCI Machine Learning Repository we are currently testing! [Contact us](#) if you have any issues, questions, or concerns. [Click here to try out the new site.](#)

## Phishing Websites Data Set

Download: [Data Folder](#), [Data Set Description](#)

**Abstract:** This dataset collected mainly from: PhishTank archive, MillerSmiles archive, Google's searching operators.

|                            |                |                       |      |                     |                   |
|----------------------------|----------------|-----------------------|------|---------------------|-------------------|
| Data Set Characteristics:  | N/A            | Number of Instances:  | 2456 | Area:               | Computer Security |
| Attribute Characteristics: | Integer        | Number of Attributes: | 30   | Date Donated        | 2015-03-26        |
| Associated Tasks:          | Classification | Missing Values?       | N/A  | Number of Web Hits: | 212564            |

### Source:

Rami Mustafa A Mohammad ( University of Huddersfield, [rami.mohammad '@' hud.ac.uk](mailto:rami.mohammad '@' hud.ac.uk), [rami.mustafa.a '@' gmail.com](mailto:rami.mustafa.a '@' gmail.com))  
Lee McCluskey (University of Huddersfield, [l.mccluskey '@' hud.ac.uk](mailto:l.mccluskey '@' hud.ac.uk))

Fadi Thabtah (Canadian University of Dubai, [fadi '@' cud.ac.ae](mailto:fadi '@' cud.ac.ae))

### Data Set Information:

One of the challenges faced by our research was the unavailability of reliable training datasets. In fact this challenge faces any researcher in the field. However, although plenty of articles about predicting phishing websites have been disseminated these days, no reliable training dataset has been published publicly, may be because there is no agreement in literature on the definitive features that characterize phishing webpages, hence it is difficult to shape a dataset that covers all possible features. In this dataset, we shed light on the important features that have proved to be sound and effective in predicting phishing websites. In addition, we propose some new features.

### Attribute Information:

For Further information about the features see the features file in the data folder.

### Relevant Papers:

Mohammad, Rami, McCluskey, T.L. and Thabtah, Fadi (2012) An Assessment of Features Related to Phishing Websites using an Automated Technique. In: International Conference For Internet Technology And Secured Transactions. ICITST 2012 . IEEE, London, UK, pp. 492-497. ISBN 978-1-4673-5325-0

Mohammad, Rami, Thabtah, Fadi Abdeljaber and McCluskey, T.L. (2014) Predicting phishing websites based on self-structuring neural network. Neural Computing and Applications, 25 (2). pp. 443-458. ISSN 0941-0643

<https://archive.ics.uci.edu/ml/datasets/phishing+websites>

PhishTank | Join the fight against phishing

phishtank.org

PhishTank is operated by Cisco Talos Intelligence Group.

PhishTank® Out of the Net, into the Tank.

username

.....

Sign In

[Register](#) | [Forgot Password](#)

Home

Add A Phish

Verify A Phish

Phish Search

Stats

FAQ

Developers

Mailing Lists

My Account

## Join the fight against phishing

[Submit](#) suspected phishes. [Track](#) the status of your submissions.  
[Verify](#) other users' submissions. [Develop](#) software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

http://

Is it a phish?

### Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

| ID                      | URL                                                                                                                       | Submitted by            |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">7816128</a> | <a href="https://galiciahomebanking.galiciabaking.repl.co/">https://galiciahomebanking.galiciabaking.repl.co/</a>         | <a href="#">dms</a>     |
| <a href="#">7816127</a> | <a href="https://validacionbancaonline.josiwd.repl.co/">https://validacionbancaonline.josiwd.repl.co/</a>                 | <a href="#">dms</a>     |
| <a href="#">7816126</a> | <a href="https://ccgalicia.ccgalicla.repl.co/">https://ccgalicia.ccgalicla.repl.co/</a>                                   | <a href="#">dms</a>     |
| <a href="#">7816125</a> | <a href="http://coloursource.com.au/bt/ionos-1and1/40c1f234...">http://coloursource.com.au/bt/ionos-1and1/40c1f234...</a> | <a href="#">kkalmus</a> |
| <a href="#">7816124</a> | <a href="http://beta-exodes.com">http://beta-exodes.com</a>                                                               | <a href="#">DDay</a>    |
| <a href="#">7816122</a> | <a href="https://sunfores.top/exten/eoxodu/">https://sunfores.top/exten/eoxodu/</a>                                       | <a href="#">DDay</a>    |
| <a href="#">7816120</a> | <a href="https://unfortunateturbodebuggers.confirrmarrrrrrr...">https://unfortunateturbodebuggers.confirrmarrrrrrr...</a> | <a href="#">dms</a>     |
| <a href="#">7816119</a> | <a href="http://web.ib.mizuihaobank-japan.rest/client/index...">http://web.ib.mizuihaobank-japan.rest/client/index...</a> | <a href="#">ytakeda</a> |
| <a href="#">7816118</a> | <a href="http://web.ib.mizuihaobank-japan.rest/client/index...">http://web.ib.mizuihaobank-japan.rest/client/index...</a> | <a href="#">ytakeda</a> |
| <a href="#">7816117</a> | <a href="http://login.miizuhabunksdm.cyou/client/index_sp.p...">http://login.miizuhabunksdm.cyou/client/index_sp.p...</a> | <a href="#">ytakeda</a> |
| <a href="#">7816116</a> | <a href="http://login.miizuhabunksdm.cyou/client/index.php">http://login.miizuhabunksdm.cyou/client/index.php</a>         | <a href="#">ytakeda</a> |
| <a href="#">7816115</a> | <a href="https://bancobogotadc.3412244.repl.co/">https://bancobogotadc.3412244.repl.co/</a>                               | <a href="#">dms</a>     |
| <a href="#">7816112</a> | <a href="https://mizunhobank-servlet-logbnk0000000b-do.cyou...">https://mizunhobank-servlet-logbnk0000000b-do.cyou...</a> | <a href="#">ytakeda</a> |
| <a href="#">7816111</a> | <a href="https://mizunhobank-servlet-logbnk0000000b-do.cyou...">https://mizunhobank-servlet-logbnk0000000b-do.cyou...</a> | <a href="#">ytakeda</a> |
| <a href="#">7816110</a> | <a href="http://web.ib.mi.zuhobank-co-jp.cyou/client/index_...">http://web.ib.mi.zuhobank-co-jp.cyou/client/index_...</a> | <a href="#">ytakeda</a> |

[See more suspected phishes...](#)

### New to PhishTank?

[Subscribe](#) to the PhishTank mailing lists.

What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.  
[Learn more...](#)

What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.  
[Read the FAQ...](#)

pan

[Friends of PhishTank](#)

[Terms of Use](#)

[Privacy](#)

[Contact](#)

PhishTank is operated by Cisco Talos Intelligence Group (Talos). Learn more about PhishTank or Talos

# JPCERT/CC Phishing URL dataset

GitHub - JPCERTCC/phishurl-list

github.com/JPCERTCC/phishurl-list/

https://github.com/JPCERTCC/phishurl-list

Product Solutions Open Source Pricing

Search Sign in Sign up

JPCERTCC / phishurl-list Public

Notifications Fork 6 Star 90

<> Code Pull requests Actions Security Insights

main 1 branch 0 tags

shu-tom Update README.md ✓ b69129a on 31 Aug 7 commits

|                   |                                          |              |
|-------------------|------------------------------------------|--------------|
| .github/workflows | Added script to create statistics page   | 2 months ago |
| 2019              | Added phishing url data 201901 to 202206 | 2 months ago |
| 2020              | Added phishing url data 201901 to 202206 | 2 months ago |
| 2021              | Added phishing url data 201901 to 202206 | 2 months ago |
| 2022              | Added phishing url data 201901 to 202206 | 2 months ago |
| .gitignore        | Added script to create statistics page   | 2 months ago |
| README.md         | Update README.md                         | last month   |
| index.html        | Updated statistic page                   | 2 months ago |
| statistic.py      | Added script to create statistics page   | 2 months ago |
| template.html     | Added script to create statistics page   | 2 months ago |

README.md

## Phishing URL dataset from JPCERT/CC

### Column details

- date: Date confirmed by JPCERT/CC
- URL: Entire URL of a phishing site

About

Phishing URL dataset from JPCERT/CC

Readme 90 stars 12 watching 6 forks

Languages

HTML 94.5%

Python 5.5%

# まとめ

---



- フィッシング・スミッシングが猛威を振るっている
- フィッシングはビジネス化され、エコシステムを形成している
- 利用者、事業者それぞれ異なるフィッシング対策
- 様々な観点でのフィッシング対策研究がおこなわれている
- しかし、フィッシングは減るところか増加傾向にある
- 対策検討に向けて研究コミュニティもぜひご協力ください



# ご清聴ありがとうございました

---

Special Thanks:

コンテンツをご提供いただいたフィッシング対策協議会学術研究WGの皆様  
タイトルをご提案いただいたソリトンシステムズの荒木様