JPAAWG Japan Anti-Abuse Working Group

JPAAWG 7th C2-3

フィッシングに悪用されるドメイン名の過去と現在

フィッシングサイトへの誘導に使われるURLは、これまで利用者を騙すためにブランド模倣型の文字列が盛んに使われてきた。しかし、その手口は大きく変化し従来の考えでは対策のみならず検知も困難になっている。JPCERT/CCが提供するphishurl-listの分析結果をもとに実態を示し、検出～対策で考えるべき点を解説する。

富士通ディフェンス&ナショナルセキュリティ株式会社
谷口　剛
株式会社マクニカ ／ フィッシング対策協議会 学術研究WG
鈴木 一実

鈴木 一実

株式会社マクニカ / セキュリティエンジニア

- 2017~ 通信事業者向け国際セキュリティ支援に従事
  - SOC/SIRT立ち上げ支援、脅威分析、脅威ハンティング支援
- 2018~? スミッシングを発見し、同僚の丸山と共に対策にのりだす
- 現在　通信事業者、企業、公官庁、に対しスミッシング対策を支援中
- フィッシング対策協議会 WGメンバー

脅威分析を中心に何年経っても現場にいる主義。
趣味はスキー、ギター、DTM、DIY、居合。

- サイバー犯罪対策活動
  - 神奈川県企業サイバーセキュリティ対策官民合同プロジェクトメンバー
  - 神奈川県警サイバー防犯ボランティア
  - メディア出演解説　NHKニュースウォッチ９ NHKあさいち　RKB毎日放送タダイマ！

https://www.macnica.co.jp/business/security/mnc/phishing_report_202207.pdf

JPAAWG

谷口剛

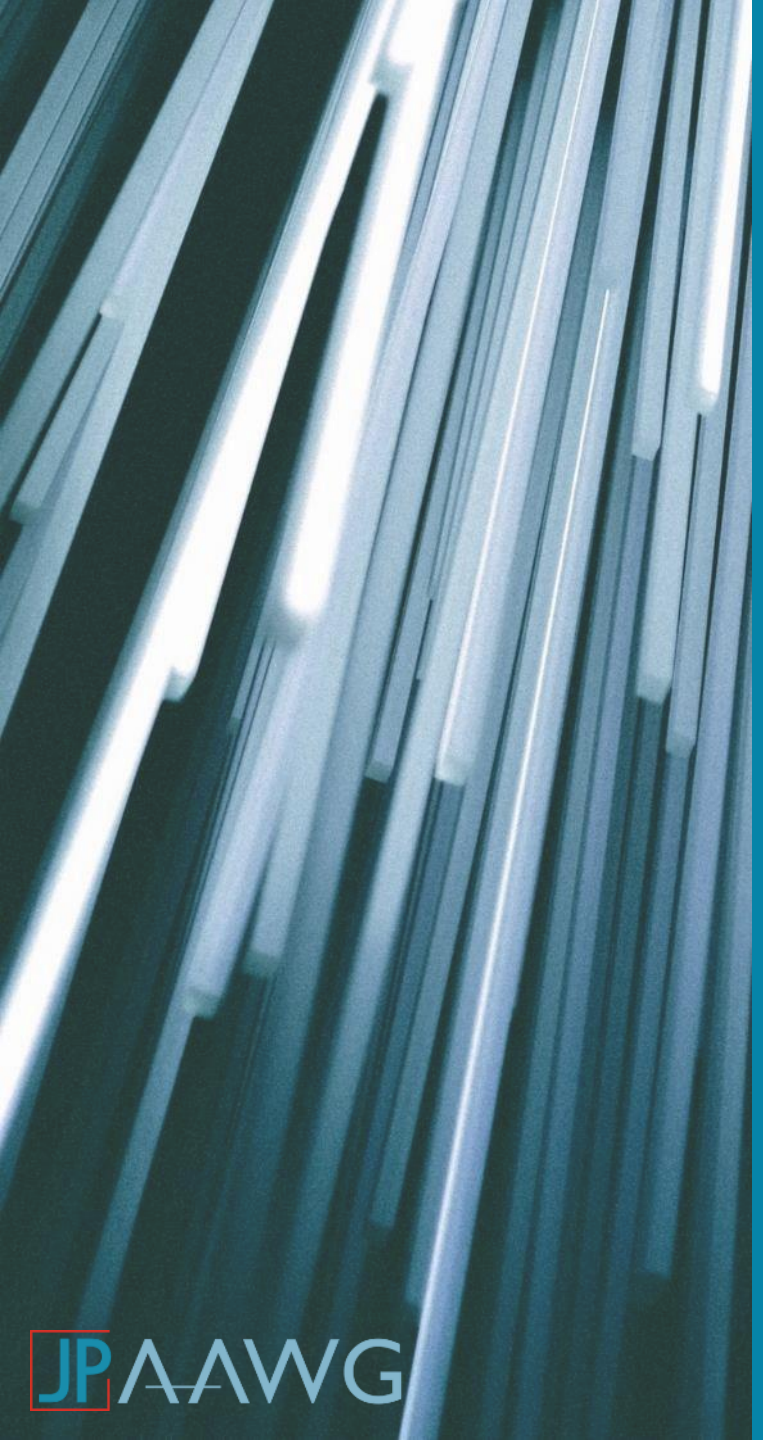
- 富士通ディフェンス＆ナショナルセキュリティ株式会社　研究員
  - 情報科学博士
- 2016 年からサイバーセキュリティの研究開始
  - 主に Passive DNS に基づく DNS 悪用検知が研究の中心
- 2023 年 2 月からマクニカ鈴木さんの紹介で学術研究 WG 参加
  - 2023 年 1 月の第 7 回フィッシング対策勉強会がきっかけ
- 過去の登壇
  - Black Hat Asia 2021, ACM ASIACCS 2021
  - CODE BLUE 2017 Day0 Special Track Counter Cyber Crime Track, CODE BLUE 2018, 2020, 2021, 2022
  - HITCON ENT 2024
- 3 日後に CODE BLUE 2024 登壇予定

JPAAWG

本講演の概要

- フィッシングに悪用されるドメイン名の過去と現在
  - 株式会社マクニカと富士通ディフェンス & ナショナルセキュリティ株式会社の共同レポート
  - https://www.macnica.co.jp/public-relations/news/2024/146000/
- 共同レポート作成の動機
  - パターン検知の終焉：2023 年秋には議論
  - 攻撃手法の変化に対する防御側認識のギャップ
- 攻撃者視点での防御
  - 過去のレポートや論文に欠けている視点：サブドメイン
  - 攻撃手法の正確な理解
  - 攻撃者の意図の理解

JPAAWG



パターン検知の終焉

The End of Pattern Matching

JP AAWG

攻撃手法の変遷 (2023 年秋議論)

Phishing attacks in Japan

Subdomain abuse (legitimate URLs) → Subdomain abuse (random string)

Smishing attacks in Japan

DDNS abuse → Combo squatting → Random string

- 防御側に認識されて 5 ～ 20 年以上経過した手法を積極的に使うのか？
- 各社が検知していた範囲では、ランダム文字列に移行している感触

対策に対する課題感（共同レポートの動機）

- **防御側が知っていることは攻撃側も知っている**
  - 攻撃側は検知回避に想像以上にストイック

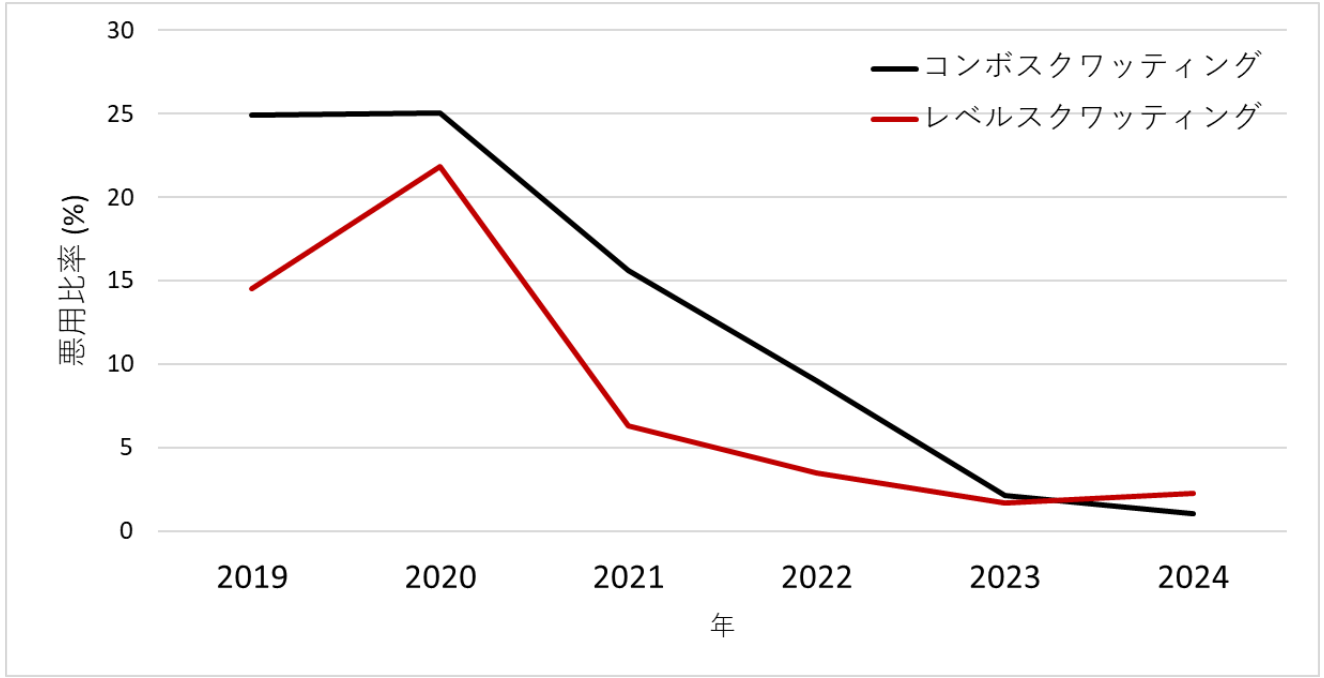
- **注意喚起は説明しやすい (特徴的な) 事例に限られる**
  - 最近の攻撃ではブランド模倣は少数派
  - にもかかわらず、メディアなどでは最近でもブランド模倣への注意喚起
    - ・・・実際の詐欺メールにはブランド模倣なんてほぼ入っていないですよね？
    - ・・・実際、どのくらいブランド名が模倣されている？
    - ・・・短縮が増えた気がする？
    - ・・・デタラメな文字列も散見する？
    - ・・・ユーザのリテラシーに頼るのには限界？？

<u>的確な防御のためには、的確な現状把握が不可欠</u>

- 前スライドのタイムラインを phishurl-list で確認 (エビデンス)

単純なブランド模倣の終焉

- コンボスクワッティング：ブランド名を含むドメイン
  - Ex. www.login-macnica.co.jp
- レベルスクワッティング：サブドメインに正規 URL (ブランド名)
  - Ex. www.macnica.co.jp.example.com
- 2023 年からほぼ見られなくなった



※レポートの図 12 と図 14 を統合

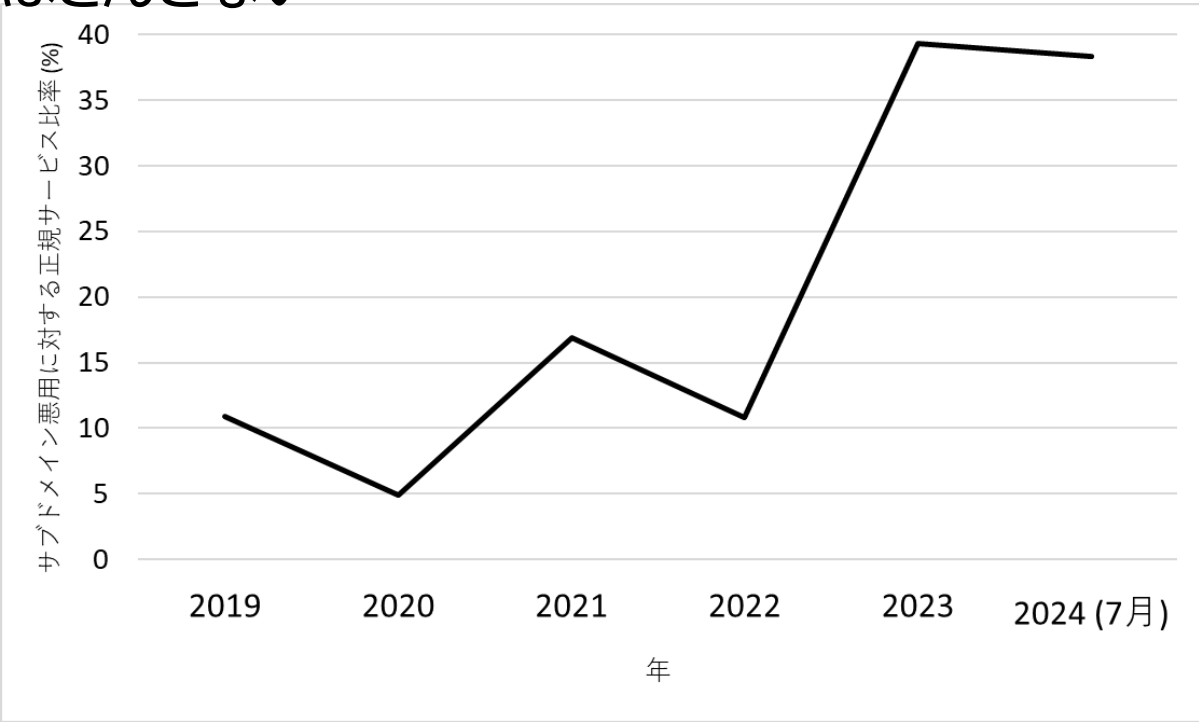
攻撃者の意図と今後の方向性

- URLでブランドを模倣しようがしまいが、URLを見ないでクリックしてしまう
  ↓
- 利用者（詐欺ターゲット層）の特徴から、ブランド名は重要ではない
- セキュリティフィルタ回避上もブランド名を入れたくない

- 今後の方向性
  - 短縮 URL (SNS)
  - 正規サービス (Dynamic DNS など)
  - ユニコード、飾り文字

正規サービス悪用が急増

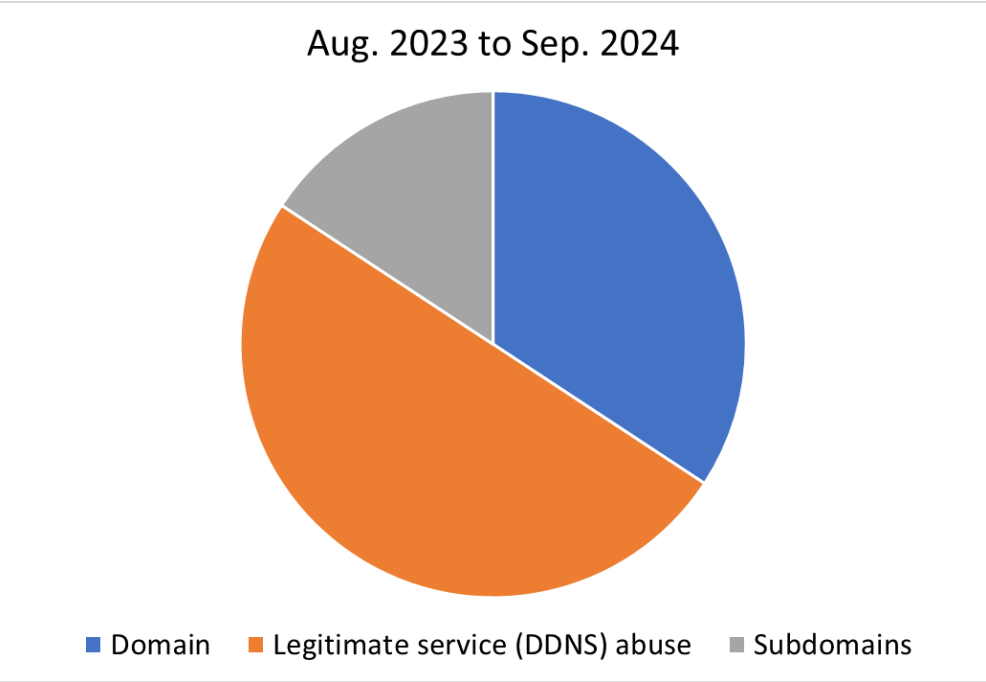
- Ex. https://f2ksvq9j.duckdns.org
  - 2024/07/03 14:46:00 (phishurl-list)
- 2023 年に 40% に急増した流れを 2024 年も引き継いでいる
- phishurl-list に関連した過去のレポートで正規サービス悪用について触れているものはほとんどない

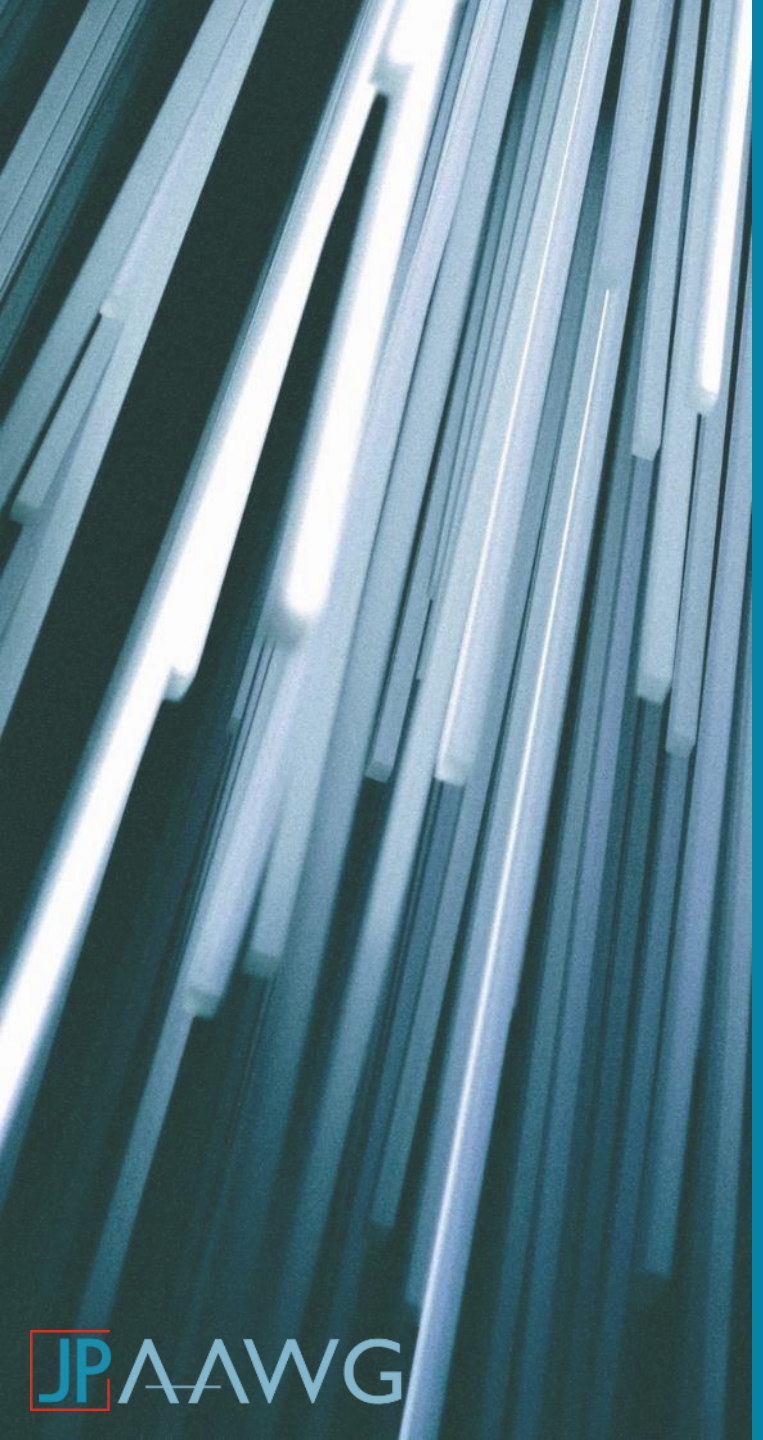


※レポートの図 9 から比率のみ抽出

PhishTankでは・・・

- Cisco が運営するフィッシング URL 共有サイト
  - 日本だけでなく、世界のフィッシング URL が検証可能
- 正規サービス悪用は全体の 50% 程度、サブドメイン悪用の 75% 程度
  - phishurl-list の倍近い悪用
  - 日本ではまだ独自ドメインを登録して攻撃している印象





攻撃者視点での防御

Defense considerations from Actor’s viewpoint

JP AAWG

この URL はどの悪用手法ですか？

- https://www.eki-net-members.o05uvl0[.]cn/
  - 2022/03/01 11:48:00 (phishurl-list)

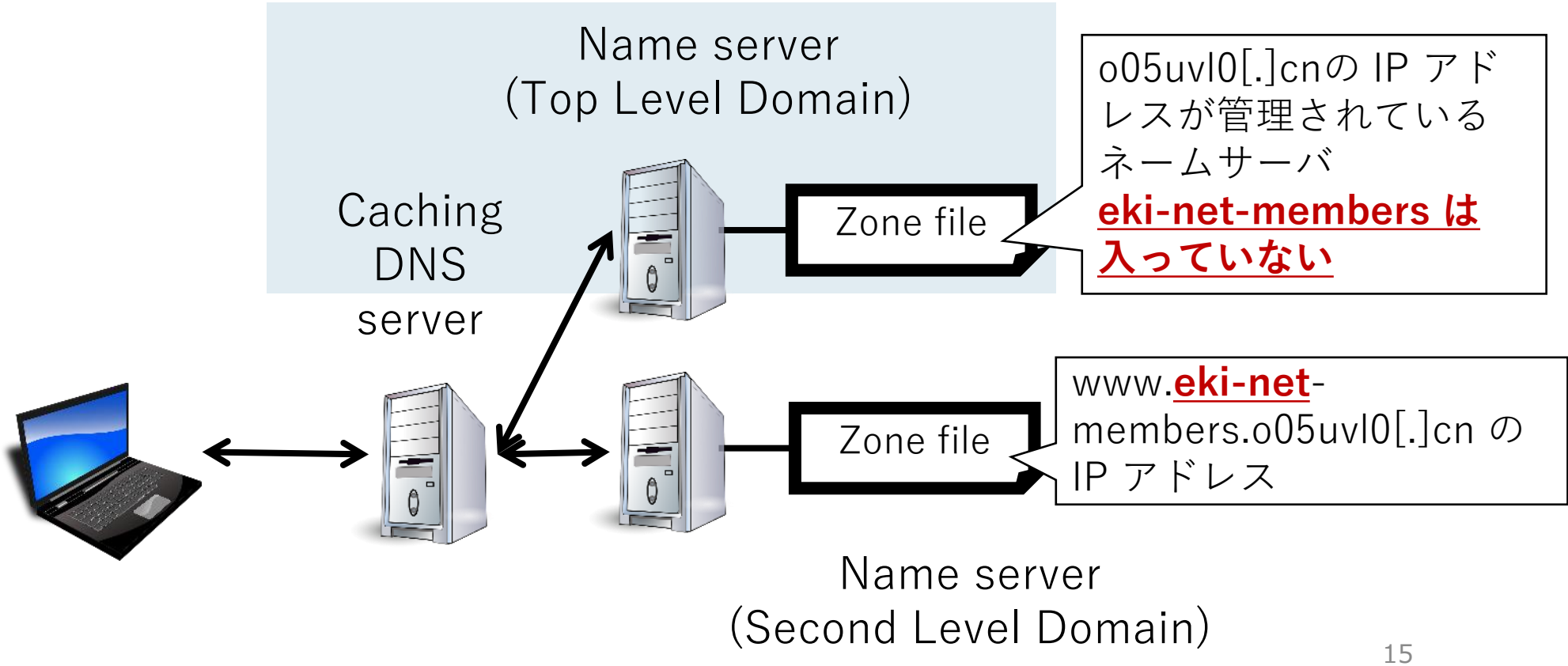
コンボスクワッティングではありません

- https://www.**eki-net**-members.o05uvl0[.]cn/
  - 2022/03/01 11:48:00 (phishurl-list)
- コンボスクワッティング
  - ドメインスクワッティングの一種で**ドメインを実際に登録する**
  - 防御側が探しやすいところにデータが存在
  - 定義：**ドメイン**にブランド名が含まれる
- 過去のレポートでは FQDN をただの文字列とみなしているものが多い

ドメインスクワッティングの探索範囲

https://www.eki-net-members.**o05uvl0[.]cn**/

ドメイン悪用探索範囲
特に新規登録ドメイン

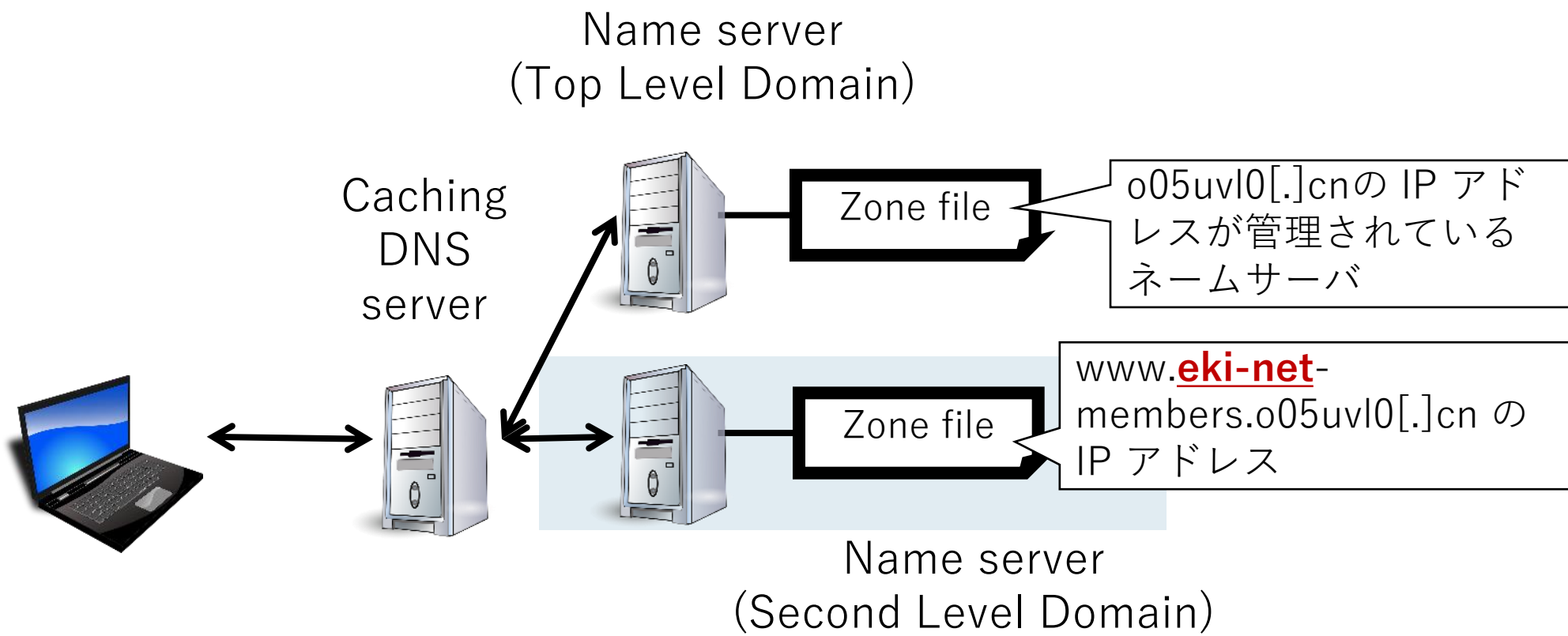


レベルスクワッティング (亜種) です

- https://**www.eki-net-members**.o05uvl0[.]cn/
  - 2022/03/01 11:48:00 (phishurl-list)
- レベルスクワッティング
  - サブドメイン悪用の一手法でドメインはなんでもよい
  - ドメイン所有者は好きな文字列をサブドメインとして運用可能
    - 悪意を持っている場合、正規 URL やブランド名も可能
  - **登録情報にサブドメインは含まれない**
  - **防御側から探しづらいところにデータが隠れる**
  - 定義：**サブドメイン**に正規 URL (レポートではブランド名も含むものに拡張)

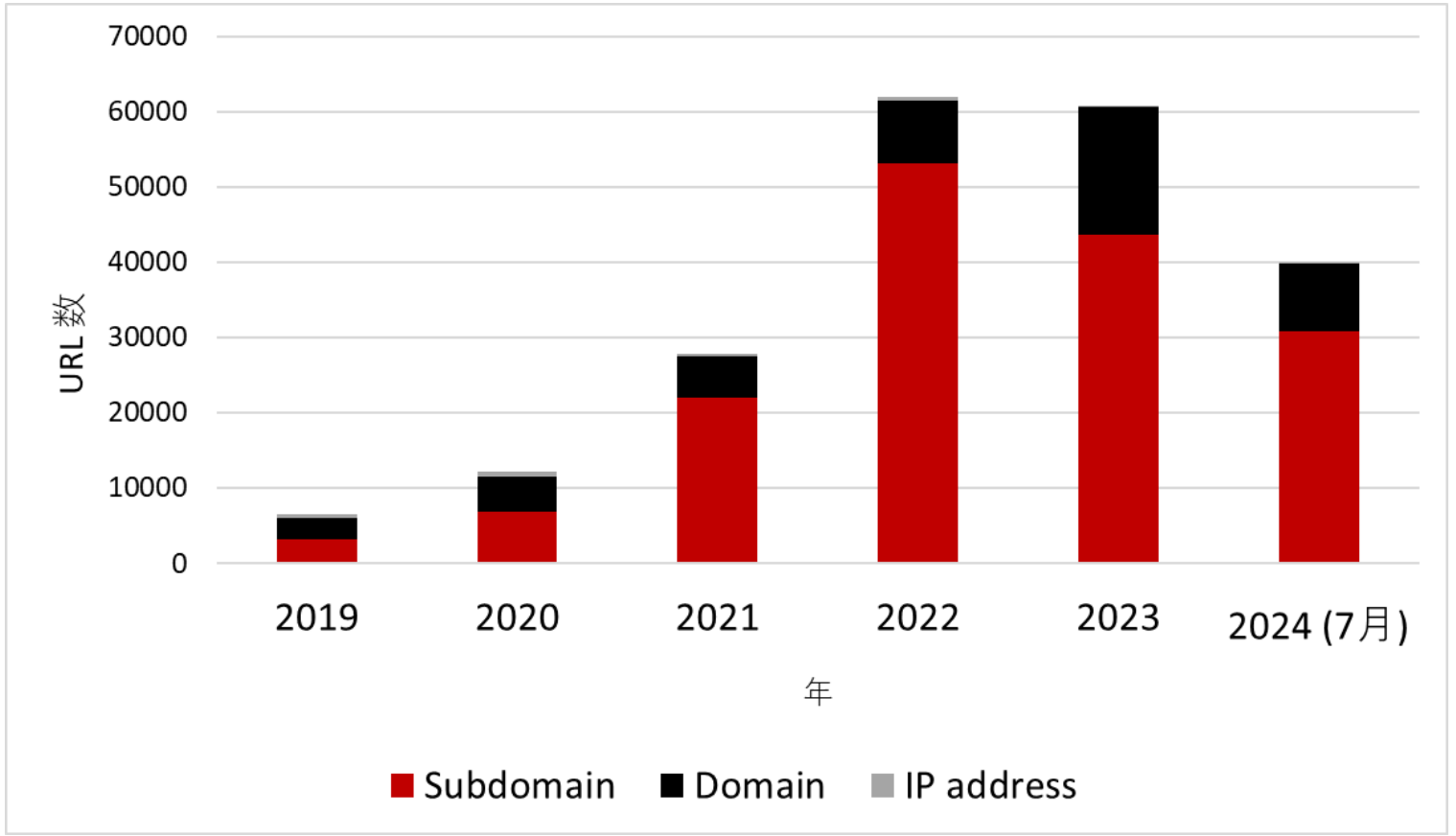
サブドメインはどこで管理されている？

https://www.eki-net-members.o05uvl0[.]cn/



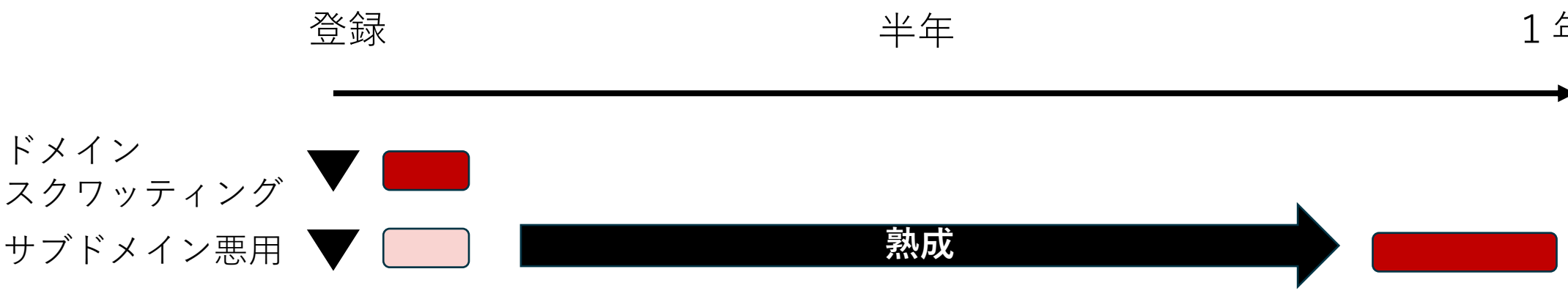
サブドメイン悪用が主流の時代

	2019	2020	2021	2022	2023	2024 (7月)
全 URL 数	0.6 万	1.2 万	2.8 万	6.2 万	6.1 万	4.0 万
サブドメイン比率	50%	57%	79%	86%	72%	77%



※レポートの図 3 と対応

攻撃者の意図



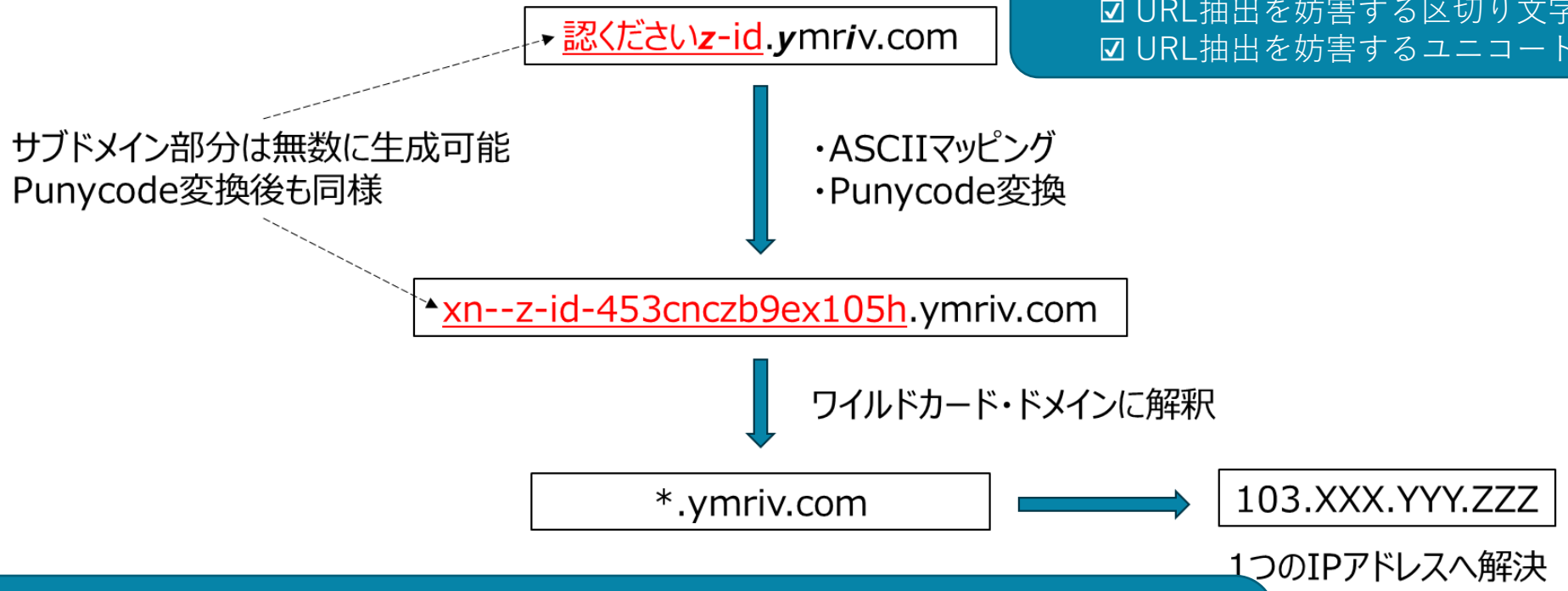
- ドメインスクワッティング
  - 防御側が探しやすい特徴的な文字列を登録情報に晒すので、登録してすぐ悪用
- サブドメイン悪用
  - ブランドと関係ない文字列で計画的に登録
  - エイジングフィルタ回避のため、10 ～ 12 カ月寝かせてから悪用
  - 登録の手間を省けるため、ワイルドカード機能を悪用してフィッシングメール一通ごとに別々の URL を生成するケースもあり (登録後すぐの悪用が多い)

サブドメインがワイルドカード

JPAAWG 6th 「2023年上半期におけるスミッシング状況と今後の対策の模索」鈴木(APC)・新藤(JC3)・・より

- どんなサブドメインでも詐欺サイトに誘導する

Androidではリンク成立するが、セキュリティフィルタではリンク識別が正しく行えない問題をついた攻撃手法
- ☑ URL抽出を妨害する区切り文字
- ☑ URL抽出を妨害するユニコード文字



① そもそも、セキュリティソフトではURL部分をうまく取り出せない
② かつ、ドメイン部分だけで探索してもフィッシング判定されない
③ にもかかわらず、サブドメインは何を指定してもフィッシングサイトに誘導
➡ SMSだけでなく、emailフィッシングでも観測され始めている

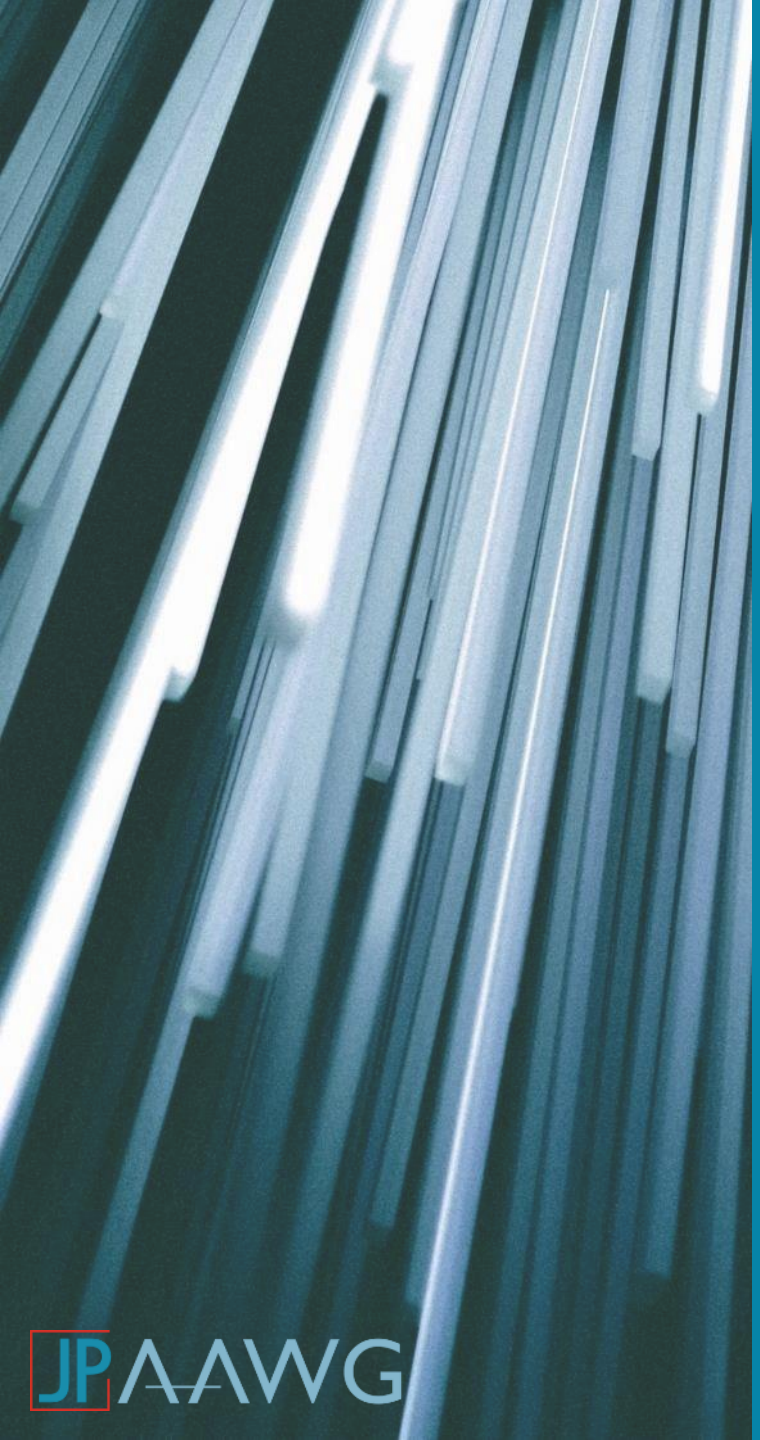
攻撃者からみたドメイン悪用

- 攻撃者は、「文字列あそび」をしているのではない
- 「サブドメイン悪用」は、文字列上の位置の問題ではない

↓

- ドメインがどのように動作し管理されているか、その仕組みに沿いながら、検知を回避する最適な手法を編み出している
- 結果、単純な文字列パターンマッチングでは判定できないフィッシングドメインが主流に

防御側は上記を理解し、攻撃者の上を行く防御を考える必要がある



phishurl-list 分析

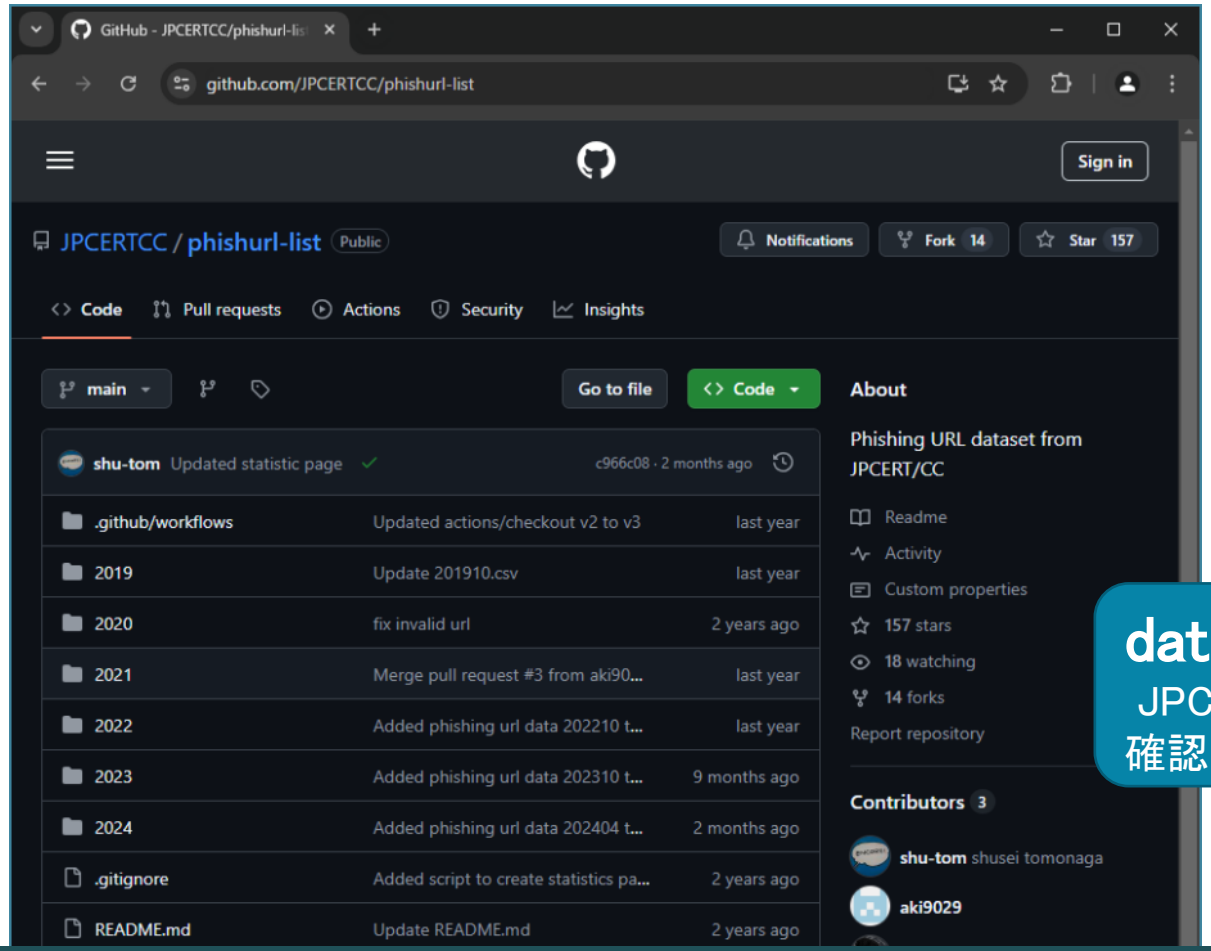
Analysis of phishurl-list

JPAAWG

phishurl-list について

- **phishurl-list はフィッシング攻撃の分析にとって非常によいデータ**

GitHubページ



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

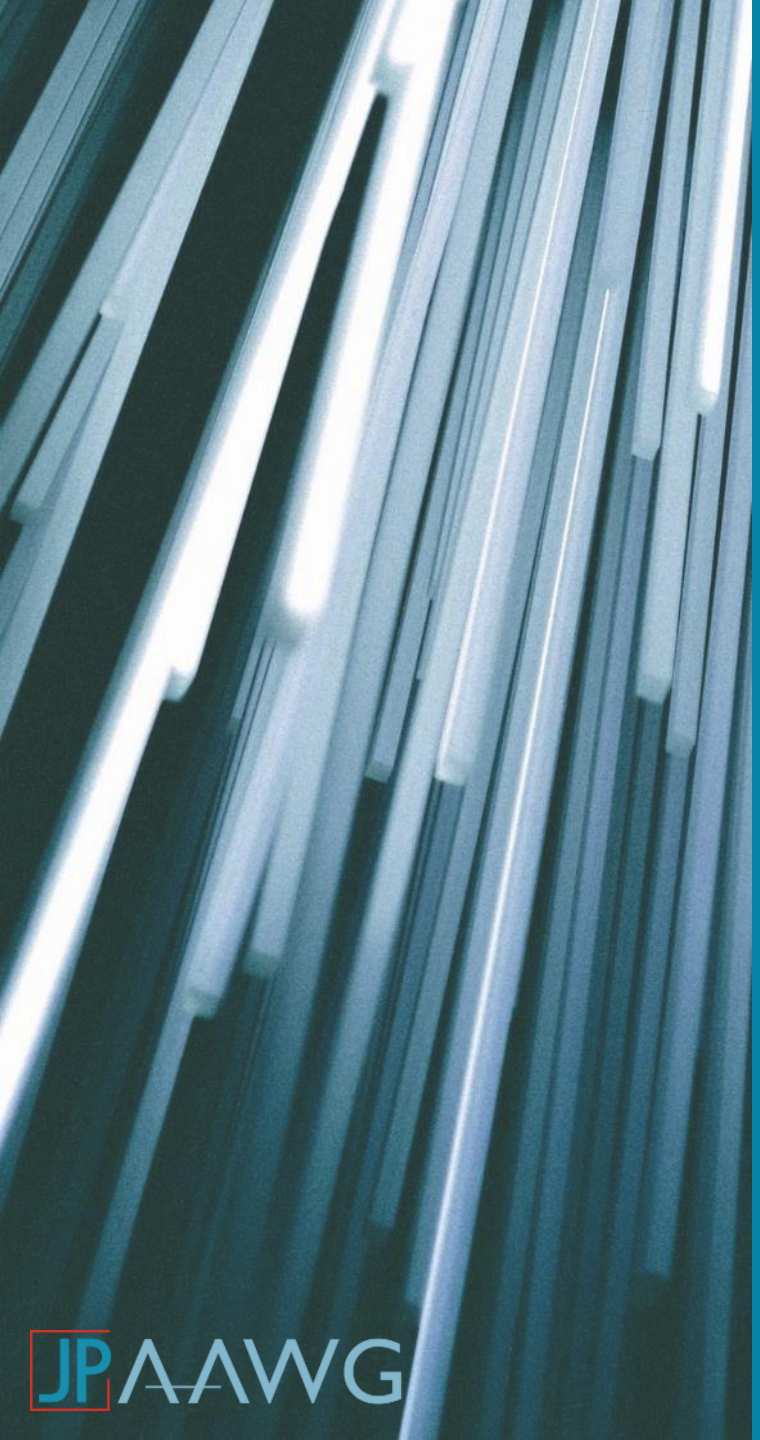
csvファイルの中身

phishurl-list の網羅性

- ただ、以下のような観点で網羅的ではないことは事前に認識すべき
  - フィッシング対策協議会が窓口 -> JPCERT/CC が確認、という流れの中で、窓口で受け付けられたが、確認前に落ちてしまうサイトも存在
    - 特にバラマキ系は攻撃の流れがかなり早く、サイトもすぐ落ちる
  - フィッシングハンターが検知したが、通報しないケースもあり
    - 特にスミッシングで多い傾向
  - Blind Spot に入っているサイトもかなりありそう

phishurl-list 分析ノウハウ

- **基本中の基本：FQDN を単純な文字列として分析してはダメ！**
- **まず Dynamic DNS を区別**
  - phishurl-list では、少なくとも duckdns.org と workers.dev は別扱い
  - 正規サイトがアカウントとして発行したサブドメインを分析しても意味はない
- **ドメインとサブドメインを分ける**
  - ccTLD の扱いに注意：Effective SLD が原則
    - .com.cn など
  - ドメインで分類した後、短縮 URL も区別 (文字列としては意味がない)
- **慣例的な www の扱い**
  - 基本的にはサブドメイン
  - www をつけてドメインスクワッティングにするパターンがあるので、レポートではドメイン悪用として分析
- **Description フィールドの活用**
  - 被害ブランドごとに URL の傾向が違うケースあり (特に eki-net, ETC)
  - 被害ブランドを限定した分析ができるように実装
- **DNS 悪性挙動の深掘り**
  - フィッシングサイトの稼働は短いため，phishurl-list をダウンロードした時点でほとんどのサイトにはアクセスできない
  - Passive DNS で IP アドレス (IP Geolocation でプロバイダまで) や、WHOIS コマンドで登録情報、登録から攻撃までの期間など、多角的に見た方がよりよい



まとめ

Conclusion

JP AAWG

まとめ

- 的確な防御のためには、的確な現状把握が不可欠
  - phishurl-listの活用
  - 感覚ではなく、俯瞰的・定量的に分析

- パターン検知の終焉
  - 単純なブランド模倣の終焉を phishurl-list で確認
  - 攻撃手法の変化（防御側の認識ギャップ）
    - 防御側に認識されて 5 ～ 20 年の手法は積極的に使わないだろう
    - ブランド模倣とは関係ない短縮 URL (SNS)
    - 正規サービス (Dynamic DNS など) 悪用
    - ユニコード挿入、ワイルドカード・サブドメイン

- 攻撃者視点での防御
  - 過去の分析調査で欠けている点：サブドメイン
    - ドメインとサブドメインでは管理されるネームサーバが異なる
    - 防御の観点では重要なのに分析者がほとんど気にしていない
  - 攻撃手法と攻撃者の意図の正確な理解が防御には重要

Thank you