資料43－１－２

悪性Webサイトの検知技術・共有手法の実装可能性検証に係る調査ご報告

2023年4月28日

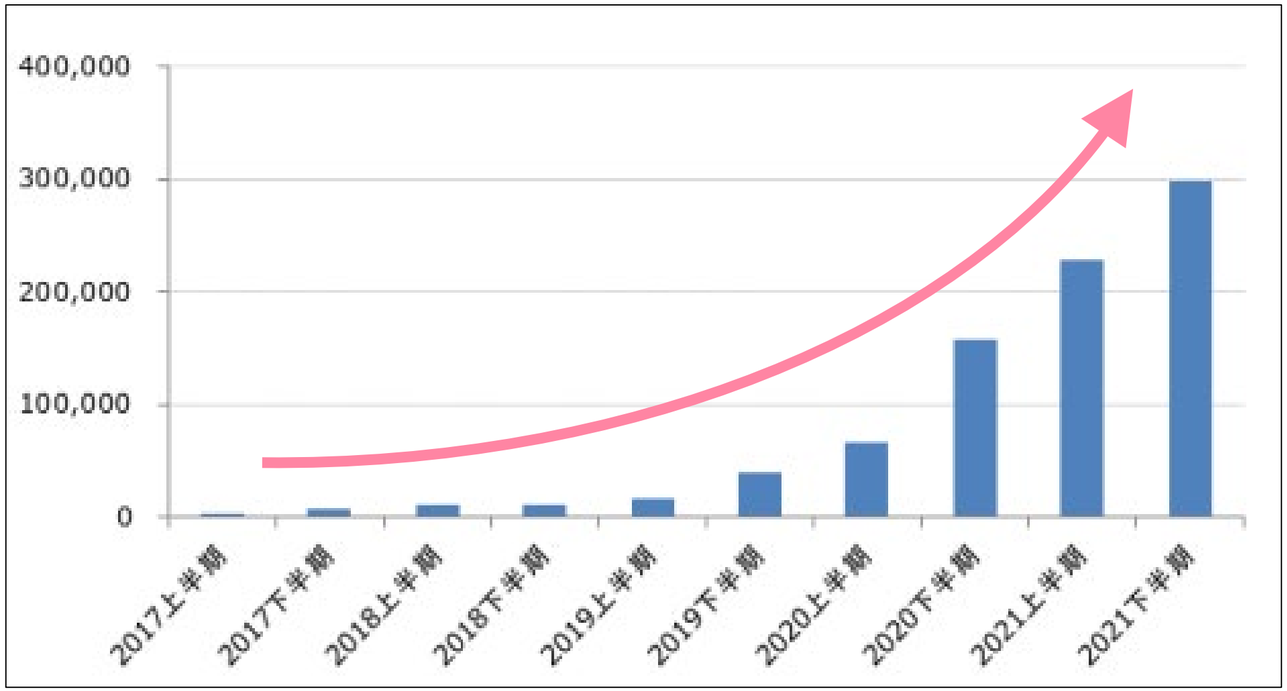
NTTコミュニケーションズ株式会社

目次

1. 背景・目的

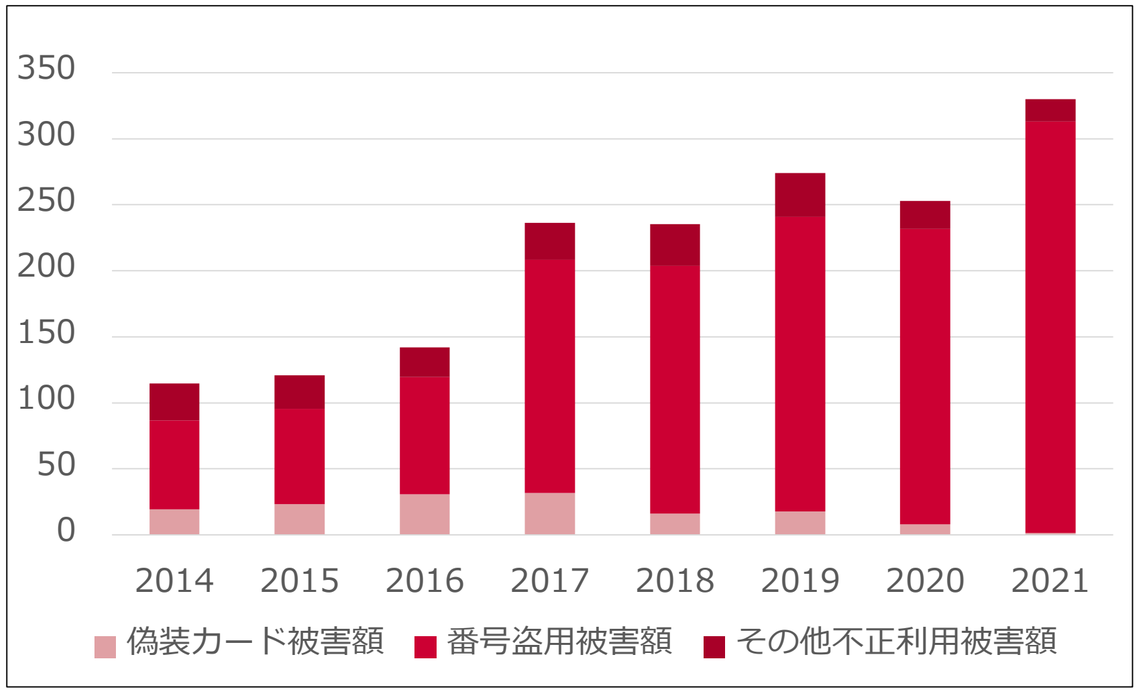
昨今、フィッシングサイト等を用いたサイバー攻撃の増加により、インターネット利用者の被害も増加傾向にある。国内の悪性Webサイト対策強化のため、本調査では悪性Webサイトを早期に検知し、実効的な対策へ早期に反映するための仕組みに関する調査・および検知結果を活用し継続的な対策を講じるための必要事項や課題の整理を図った。

国内のフィッシング報告件数



フィッシング対策協議会／フィッシングレポート
https://www.antiphishing.jp/report/phishing_report_2022.pdf

クレジットカード不正利用被害額統計（単位：億円）



※日本クレジット協会の情報を基に作成
https://www.j-credit.or.jp/information/statistics/download/statistics_domestic_2021.pdf

被害最小化のため**早期検知・対策**が求められる

2. 調査スコープ

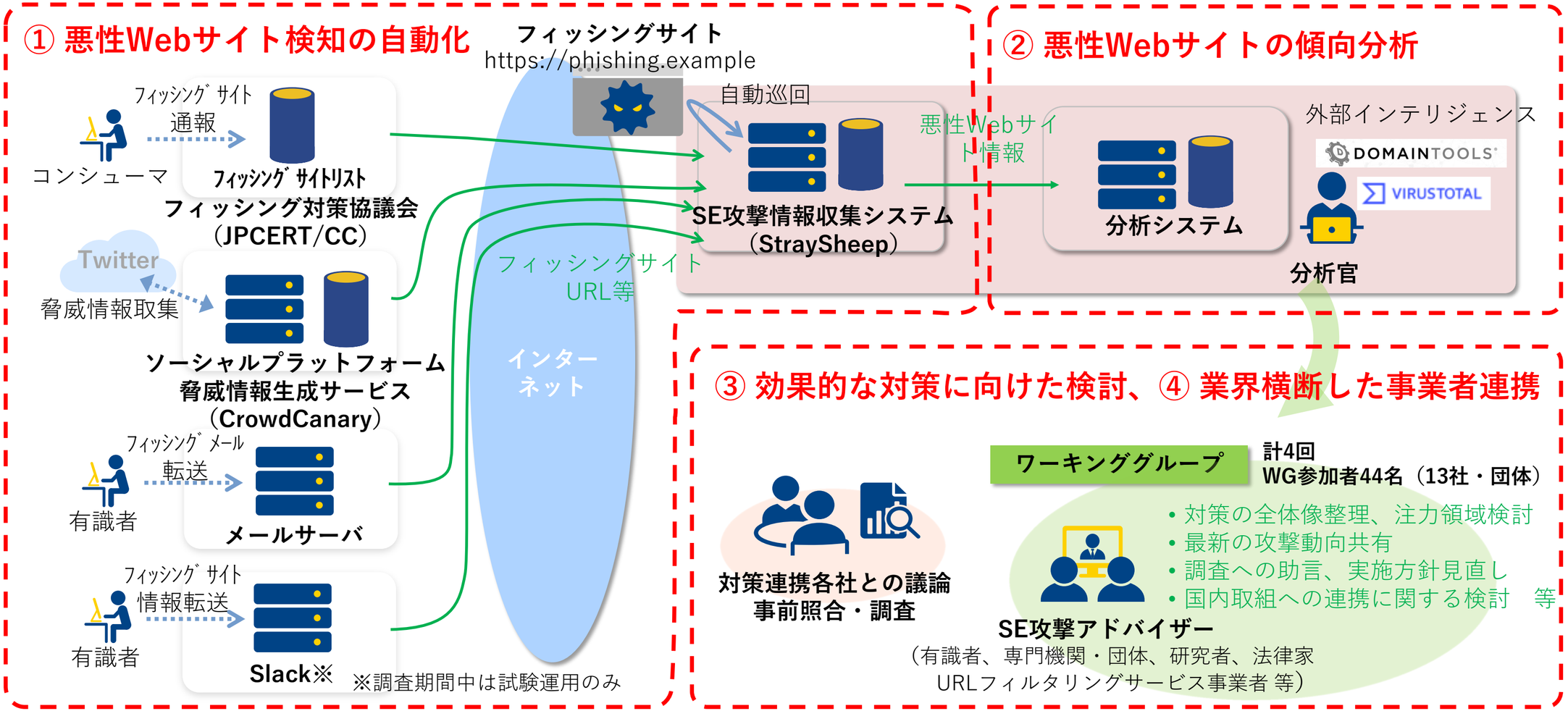
本調査のスコープは「フィッシング詐欺ビジネスプロセス分類」の誘導段階におけるメール/SMSがばらまかれた後の悪性Webサイトの早期検知・早期対策を主眼とした。

分類	攻撃段階と対策の観点	対策等の取り組み（例）
計画	攻撃者がメール/SMSをばらまく計画の妨害	• フィッシングキットの収集・共有、活動事例の事前把握
調達	攻撃者のインフラ調達を妨害	• インフラ提供事業者側でサービス利用者の評価
構築	攻撃者のフィッシングサイト構築妨害	• 悪性IPモニタリング、CTログ調査等 • フィッシングキットを基にした脅威ハンティング • ネットワーク管理者等への連絡、テイクダウン
誘導	攻撃者のメール/SMSばらまき無効化	• 迷惑メール・SMSフィルターの調整・強化 • 送信ドメイン認証（メール）
誘導	メール/SMS受信後のユーザ通知	• フィッシング詐欺行為の存在を認知させる取り組み • メール・SMSや誘導先Webサイトの内容を解析し危険判定 • URLをクリックした際の検知・アラート（エンドポイントのURLフィルタリング） • Webブラウザでの警告表示強化 • テイクダウン
詐取	IDパスワードを盗まれた際の早期発見	• 注意喚起：公式アプリ・ブックマークの重要性 • 具体的な攻撃事例／被害事例の業界横断した積極的共有 • ユーザへのバッドプラクティスの積極的な注意喚起
収益化	攻撃者の悪用を緩和	

フィッシング対策協議会「フィッシング詐欺ビジネスプロセス」分類
https://www.antiphishing.jp/news/collabo_20210316.pdf

3. 調査の全体像

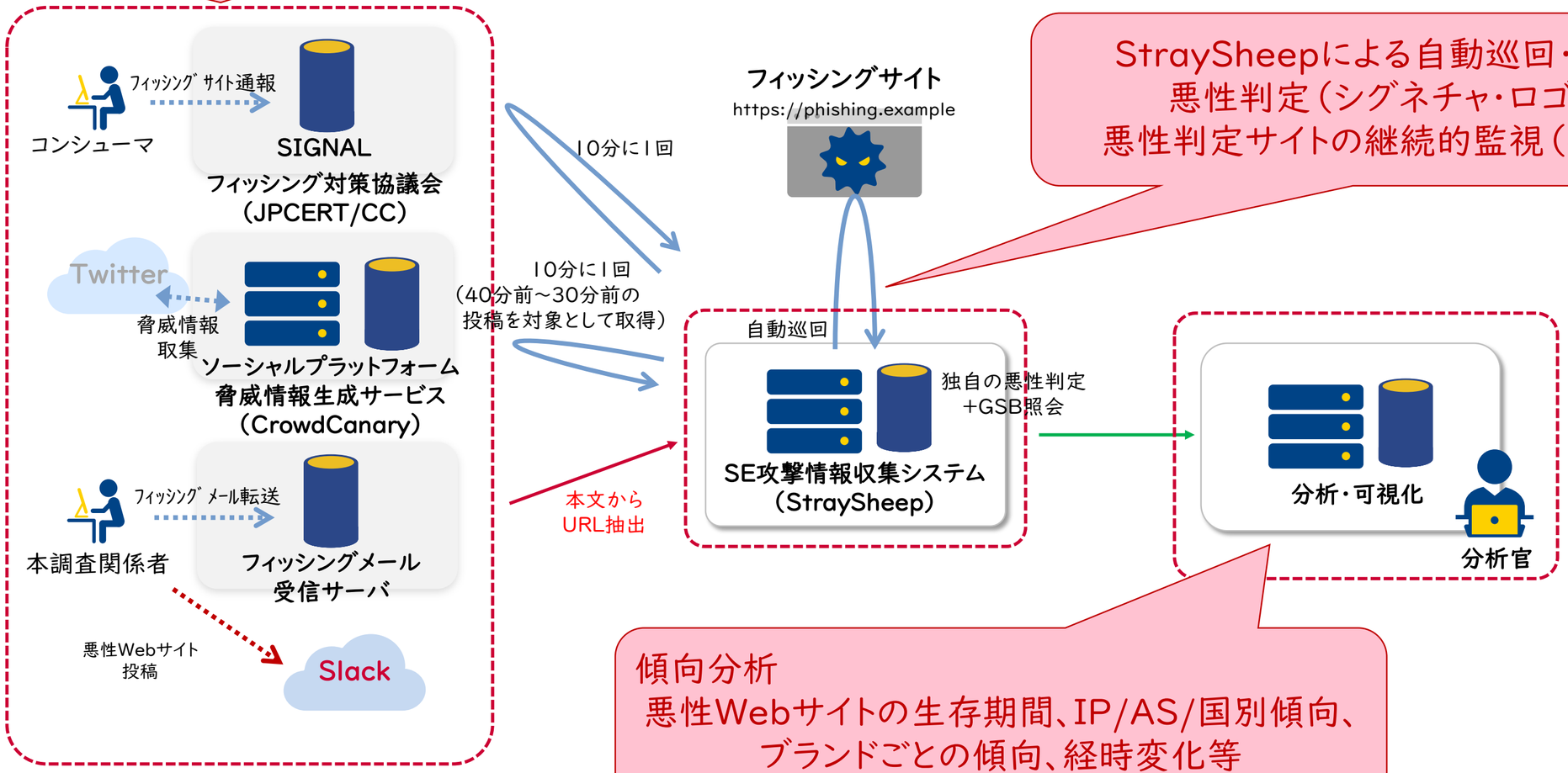
ソーシャルエンジニアリング（以降SE）により誘導される悪性Webサイトの早期検知・対策に向け、検知の自動化（①）、収集した悪性Webサイトの傾向分析（②）セキュリティサービス提供事業者や専門機関との連携（③）、有識者を含むワーキンググループ議論（④）を実施した。



3. 調査の全体像

①悪性Webサイト検知の自動化～②悪性Webサイトの傾向分析

フィッシング対策協議会（SIGNAL）、Twitter投稿、フィッシングメール有識者等からの投稿など、複数のソースからシードURLを収集



StraySheepによる自動巡回・悪性判定
悪性判定（シグネチャ・ロゴ検知）
悪性判定サイトの継続的監視（死活監視）

傾向分析
悪性Webサイトの生存期間、IP/AS/国別傾向、
ブランドごとの傾向、経時変化等

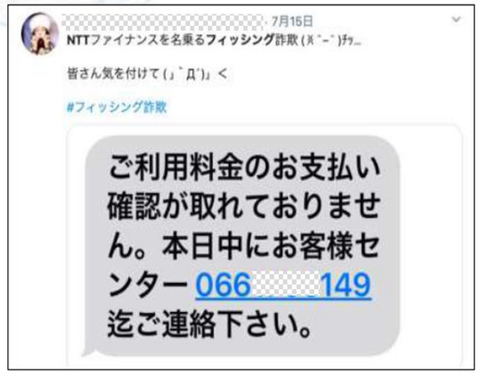
（参考）調査システム

フィッシングサイトの自動巡回、Twitterからの悪性Webサイト情報の収集（シード情報の収集、自動巡回・悪性判定）においては、NTT社会情報研究所が開発したソーシャルエンジニアリング攻撃（SE攻撃）関連技術を活用。

ソーシャルプラットフォーム脅威情報生成サービス（CrowdCanary）

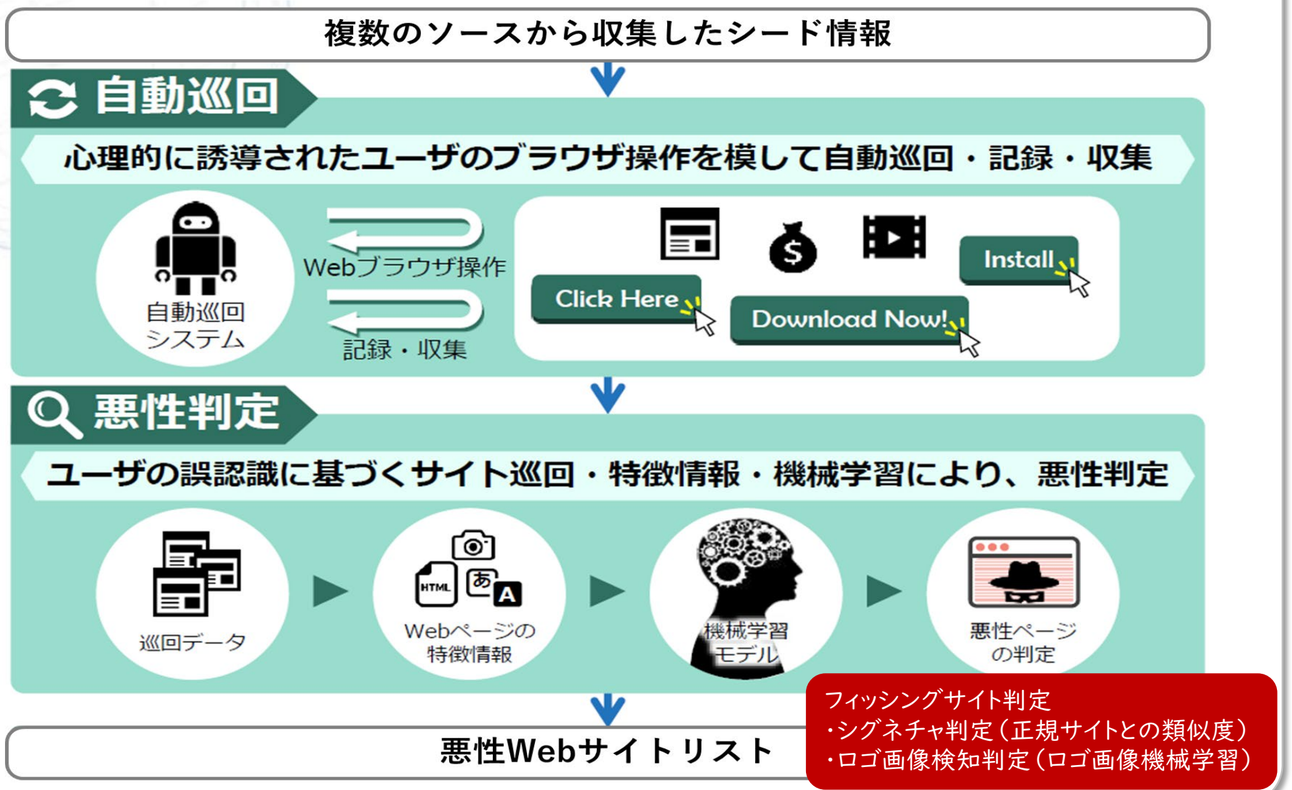
Twitter上の広範囲のユーザの投稿から、フィッシング攻撃への関連性が高いURLとドメイン名を含んだユーザの報告を早期かつ高精度に抽出するシステム

悪性サイト等に関するユーザー投稿の例



SE攻撃情報収集システム（StraySheep）

SE攻撃の特徴を考慮し「自動Webブラウザ操作によるWebサイト情報収集」、「Webサイトの複数の特徴量を活用した機械学習による悪性判定」を実施するシステム



4. 調査の結果

本調査期間中における悪性Webサイトの自動巡回・悪性判定結果、傾向分析結果のサマリ

①悪性Webサイト検知の自動化

巡回

- **シード収集連携：3**
  - Twitterキーワード収集：CrowdCanary
  - フィッシング対策協議会：SIGNAL
  - フィッシングメール
- **累計シード取集数/ユニークURL数※：**
  51,447件/26,488件（※日単位で重複排除）

SIGNAL：11,675/10,336件
Crowd Canary： 38,486 / 16,486件
Phishingメール：1,206/557件

悪性判定

- **累計悪性Webサイト検知数/悪性Webサイト検知率（ユニーク）※：**
  27,459件/47.5%（※日単位で重複排除）
  PC：24,559件
  IOS：16,738件 / Android：11,977件
- **Google Safe Browsing未登録URL：**
  9,070件（72.1%）
- **検知可能なロゴ・シグネチャ件数**
  Signature：75件 / ロゴ検知：353件
- **これまで検知したブランド数：88件**

②悪性Webサイトの傾向分析

- **悪性Webサイト死活監視数：755件**
  （2023年2月27日の死活監視巡回分）
- **稼働中の悪性Webサイト数：843件**
  （2023年2月27日に悪性判定されたURL数合計）

- **傾向分析を実施した際の観点**
- 傾向分析
  - ✓悪性Webサイトの生存期間
  - ✓IP/AS/国別傾向
  - ✓ブランドごとの傾向
- 深堀分析の観点：
  - ✓悪性Webサイトの経時変化
  - ✓URLの構造
  - ✓証明書の使いまわし
  - ✓悪性Webサイト構築によく使われるサービス（DuckDNS 等）
  - ✓悪性Webサイトで窃取される情報

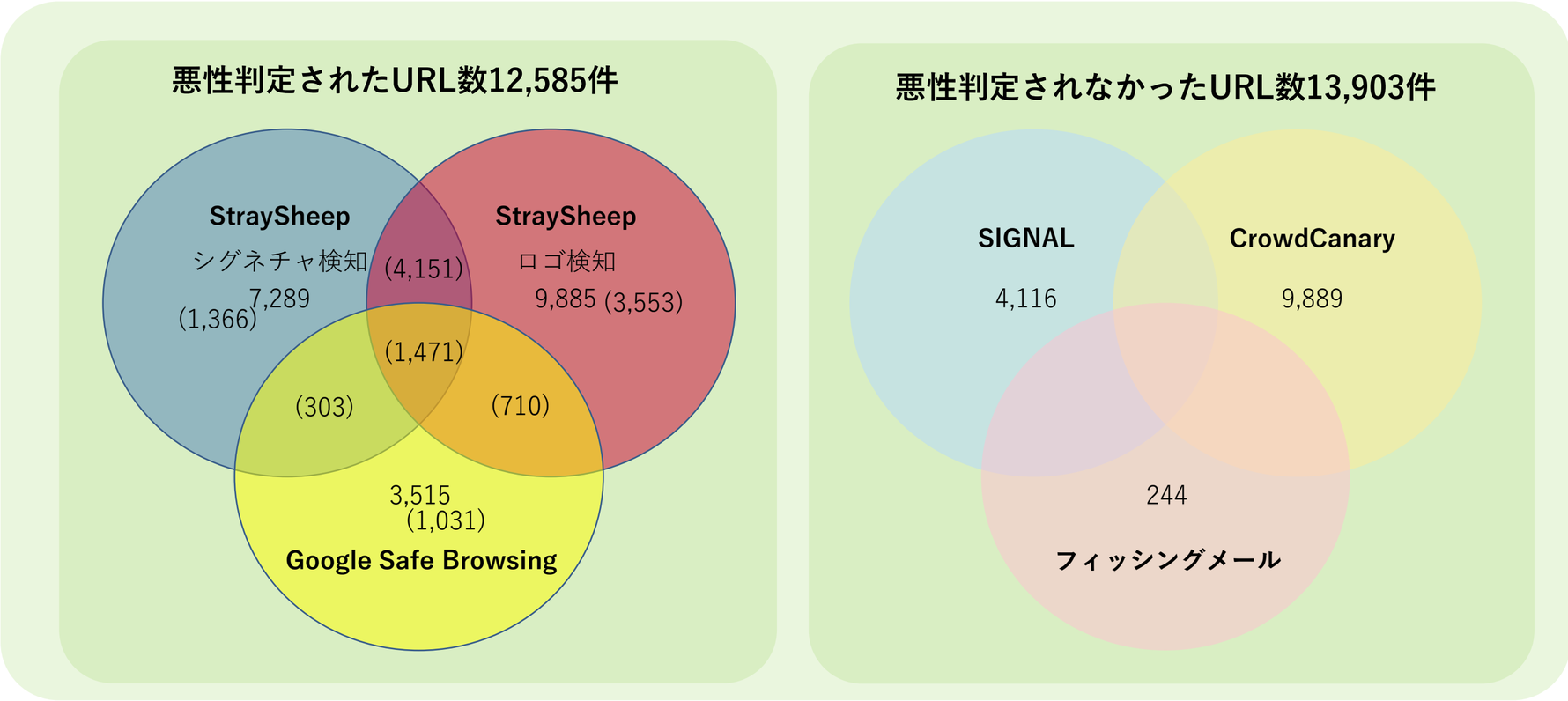
（集計期間：11月1日～2月28日）

①悪性Webサイト検知の自動化
巡回・悪性判定結果

調査期間における悪性Webサイト検知数とGoogle Safe Browsingの検知結果との比較結果を記載。

- 悪性判定されたURLのうち72.1%は構築システムのみで検知したURL（Google Safe Browsingに未登録）

全体26,488件（日単位で重複排除）



（集計期間：11月1日～2月28日）

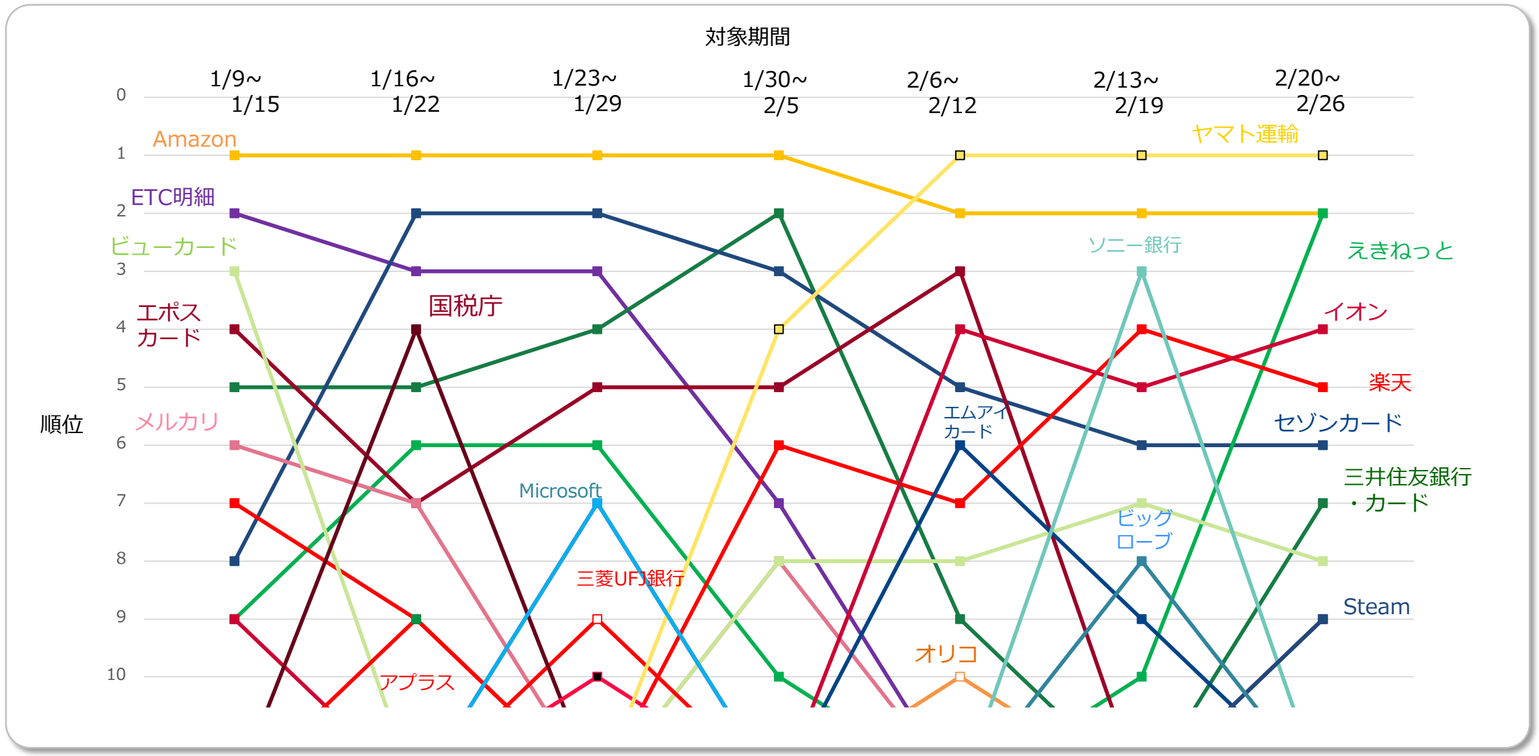
②悪性Webサイトの傾向分析

最近の狙われやすいブランドとその推移（集計期間：1/9~2/26）

クローラーで悪性判定されたURLについて、紐づくブランドの上位10件の集計結果を記載。

- 「Amazon」を騙る悪性Webサイトが多く、またカード会社など金融系も継続して上位に位置した
- 集計期間前半は「ETC明細」「ビューカード」、後半は「ヤマト運輸」が上位に位置した

悪性判定されたURLに紐づくブランド上位10件の推移



②悪性Webサイトの傾向分析

死活監視により悪性Webサイトの変化を早期に検知した例

下記のシードURLにおいて、悪性Webサイトの死活監視により、Google Safe Browsing未登録サイトを早期に検知ができていることを確認。

- シードURL：hxxps://www.ekl-net.co.jp-jrmnjk74l5x.cn

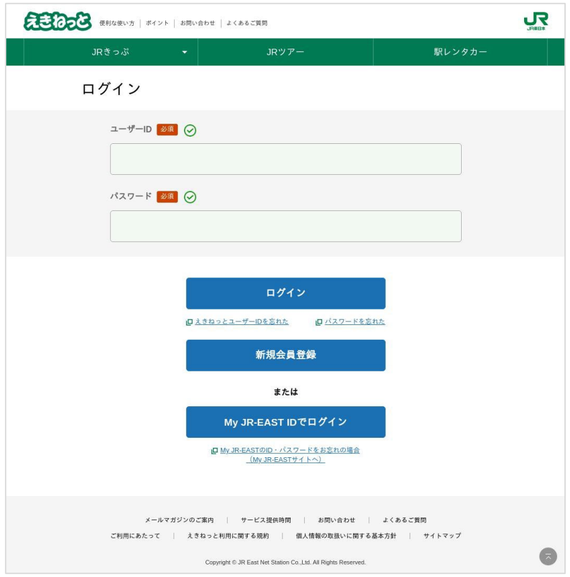
シード収集日：11月20日
TwitterよりURLを抽出
（抽出キーワード：phishing）

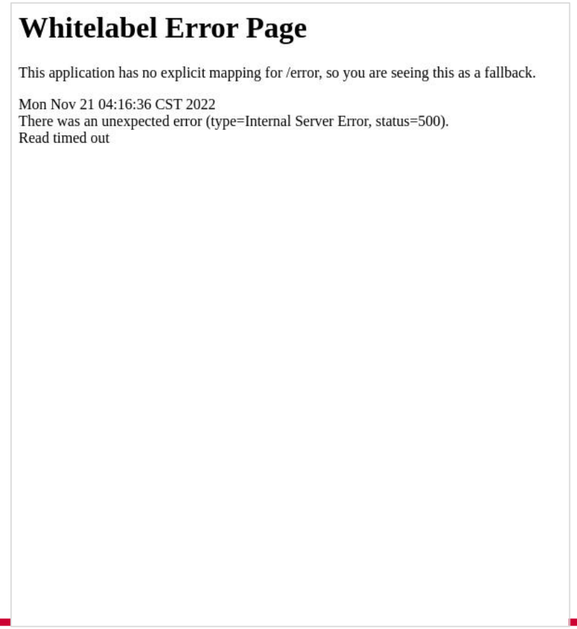
2022年
11月　1　…　20　21　22　23　24　時間軸（日）

GSB登録

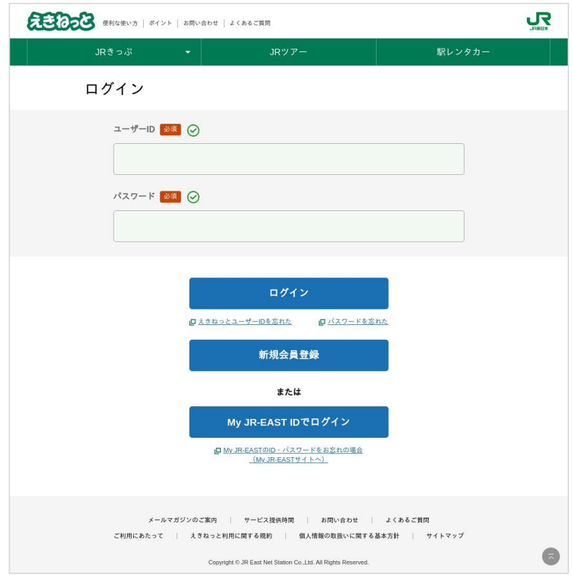
※Google Safe Browsing登録なし

日々巡回・死活監視





えきねっと正規サイトへ
リダイレクト



②悪性Webサイトの傾向分析

同一IPアドレスでターゲットを変えつつ攻撃する例

日々巡回の結果より、ターゲットブランドの異なる悪性Webサイトが下記の同一IPアドレスに集約されていることを確認。

- IPアドレス：115.144.69.127

日々巡回

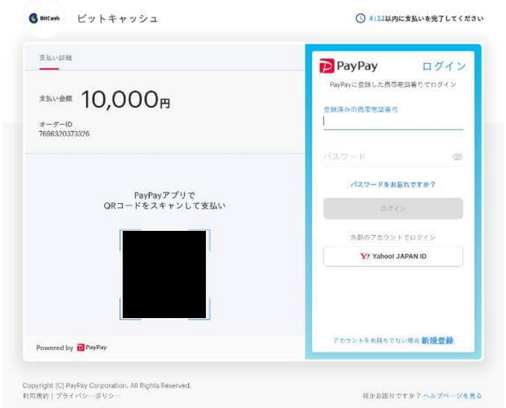
2022年12月　　2023年1月

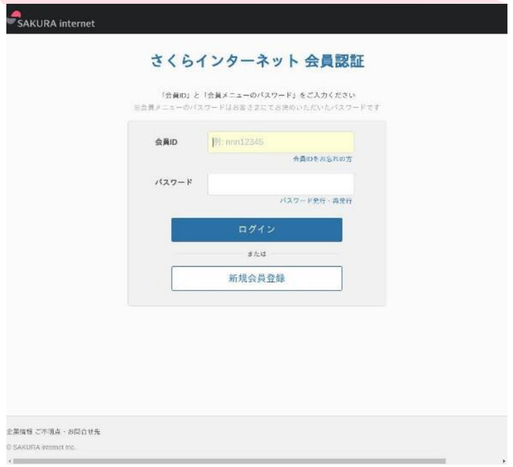
… 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 …

時間軸（日）

American Express　bitcash　OCN　さくらインターネット　bitcash　お名前.com　American Express

※PayPayの正規支払画面



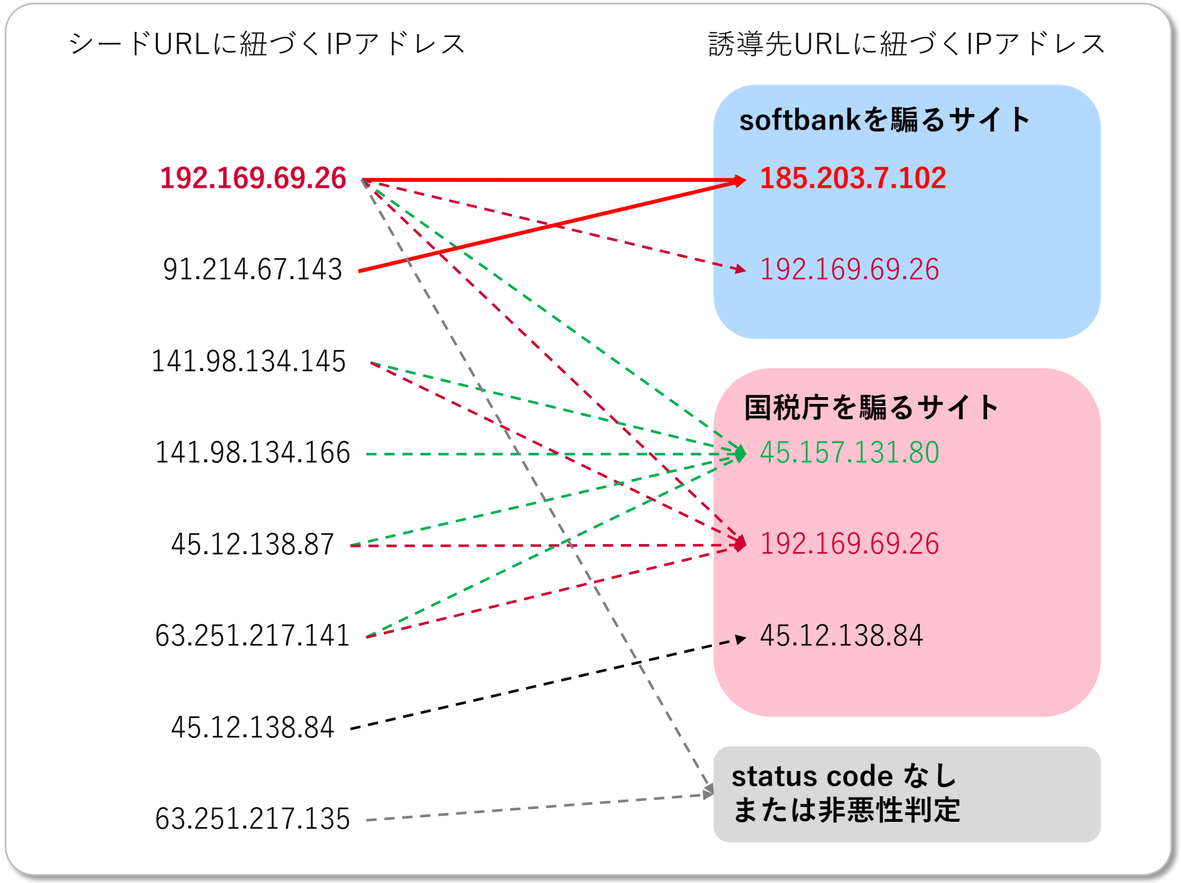


②悪性Webサイトの傾向分析

ダイナミックDNSサービスを利用したフィッシングサイト例（集計期間：12月19日のみ）

無償でサブドメインを利用できる特定のダイナミックDNSサービスを使った悪性Webサイトが散見される。このような悪性Webサイトでは、リダイレクトにより特定のIPアドレスや少数の誘導先URLへと集約される場合があることを確認。

特定のダイナミックDNSが利用されたiOS用クローラーでの巡回結果



紐づく悪性Webサイト数が多いIPアドレスのみに限定した際のサイト遷移（softbankを騙るサイトの例）

192.169.69.26に紐づくシードURL（131件）

（前略）
…
hxxp://umxnabefaa [.] duckdns [.] org
hxxp://ugeegzhgdx [.] duckdns [.] org
hxxp://uarynklvvq [.] duckdns [.] org
hxxp://txnyyesscu [.] duckdns [.] org
hxxp://tuejucopty [.] duckdns [.] org
hxxp://truwqyjwgy [.] duckdns [.] org
hxxp://trlqiydqna [.] duckdns [.] org
hxxp://timtpzgwgc [.] duckdns [.] org
hxxp://tfbaknyzla [.] duckdns [.] org
…
（中略）
…
hxxp://gjwxnnoser [.] duckdns [.] org
hxxp://fwbvpabaqz [.] duckdns [.] org
hxxp://fhbwnophac [.] duckdns [.] org
hxxp://ezxxaefdjk [.] duckdns [.] org
hxxp://etnvhhsjjv [.] duckdns [.] org
hxxp://ejajxpulqh [.] duckdns [.] org
hxxp://ecewpcxakn [.] duckdns [.] org
…
（後略）

185.203.7.102に紐づく誘導先URL（99件）

hxxps://ykiufxzegx [.] duckdns [.] org/

hxxps://cdeafyjpaw [.] duckdns [.] org/

②悪性Webサイトの傾向分析

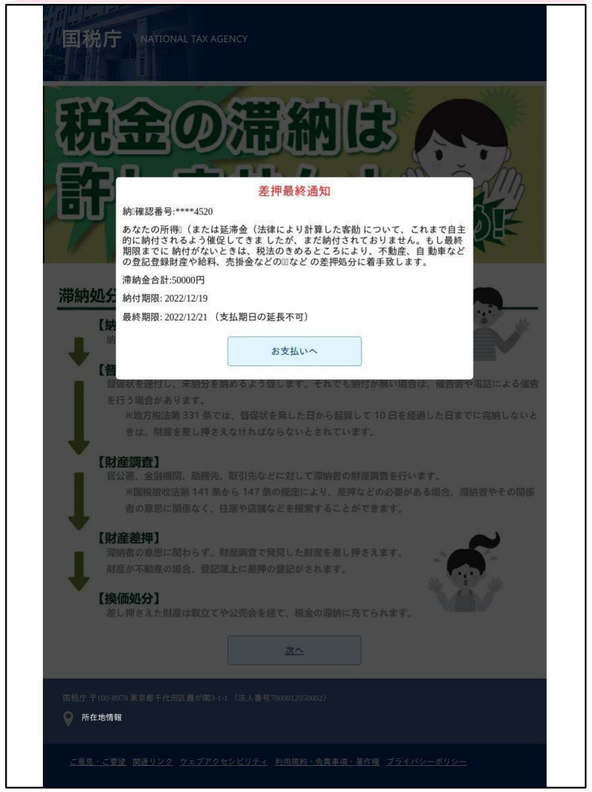
OS毎に異なる巡回結果：環境に応じてアクセス先を変動（クローキング）する例

悪性Webサイトによっては、ユーザーのアクセス環境に応じてページ遷移を変化させる挙動（クローキング）を取ることを確認。

PC用クローラーでは悪性判定だが、iOS用クローラーでは非悪性判定の例

シードURL：hxxps://wwwnta[.]jp[.]anankangkang[.]com/jp

PC用クローラー：悪性



iOS用クローラー：悪性ではない

iOS用クローラーでは
白紙の画面が表示される

PC用クローラーでは非悪性判定だが、iOS用クローラーでは悪性判定の例

シードURL：hxxps://amarzeon[.]com

PC用クローラー：悪性ではない

PC用クローラーでは
全く関係ない天気予報の正規サイトへ
リダイレクト

iOS用クローラー：悪性

調査結果のまとめ

	本調査の実施内容と主な成果	結果の再整理
①悪性Webサイト検知の自動化	■ 悪性Webサイトの巡回・悪性判定の自動化 • シード収集、悪性判定自動化や死活監視機能を含むシステムの構築・運用 • シード種別：3、収集したユニークなシード総数：26,488件 • 検知可能ブランドロゴ／シグネチャ件数：75件／353件 • 検知できたブランド数：88件 • 日時巡回により収集した悪性Webサイト数：12,585件 • 早期検知評価：Google Safe Browsing未登録URL 72.1％	■ 大量に生成される悪性Webサイトの実態把握 • 日々生成される大量のフィッシングサイトを確認 ➢ 影響度の高い悪性Webサイトを優先的に巡回するような機能（即時巡回、巡回対象の優先順位付け 等）の導入が必要 • アクセス環境に応じた悪性Webサイトの挙動変化を確認、有識者からの共有によりアクセス元の回線種別（固定回線かモバイル回線か）等様々な条件のクローキング技術について把握 ➢ 導入済みの複数OSを模し巡回する機能だけでなく、更なるシステム側の機能追加（モバイル回線の追加 等）が必要
②悪性Webサイトの傾向分析	■ 複数観点からの傾向分析を通した悪性Webサイトの攻撃実体の把握 • 狙われやすいブランドやその時系列変化の可視化 • 悪性Webサイトの死活監視による時系列変化の把握とサイトが再び立ち上がる挙動の検知 • 悪性Webサイトの死活監視によるIPアドレスに着目した基盤の使いまわし事例の可視化 • 特定のダイナミックDNSサービスを活用した悪性Webサイトにおけるシードと誘導先URLの関係性の可視化 • 複数種類のクローラーによる巡回結果を用いたクローキング事例の把握	■ 狙われやすいブランドや同じ特徴を持つ事例の可視化 • 攻撃者に狙われやすいブランドやIPアドレス・AS等の把握 • 複数のシードURLが単一の誘導先URLに紐づく悪性Webサイトの事例を確認 ➢ 攻撃者が利用するインフラ等の単位で攻撃を分類し、加えて被害実態と照らし合わせることで、攻撃の分類に応じた対策の優先順位付けへの活用が可能 ■ 既存対策と比較した早期検知の有効性確認 • 巡回・悪性判定の自動化による、広く利用される既存対策でカバーできていない悪性Webサイトの早期検知を確認 ➢ 既存対策（フィルタリングサービス等）との連携による悪性Webサイトへのアクセス抑止という対策への活用が可能

5．次ステップに向けた取り組み

今後は、前述の気づきをもとに収集した悪性Webサイト情報を対策に繋げる観点で、「巡回の高度化」による対策効果の大きい悪性Webサイトリストの生成や、商用サービス等と「アクセス実態調査」を実施した上で「対策試行」に取り組む。その知見をもとに「普及啓発・対策連携」を行う。

大量に生成される悪性Webサイトの実態把握

狙われやすいブランドや同じ特徴を持つ事例の可視化

既存対策と比較した早期検知の有効性確認

巡回の高度化

- 影響度の高い悪性Webサイトを優先的に巡回する機能の導入
- 最新のクローキング技術に併せて、モバイル回線追加などによるシステム巡回機能の追加実装

アクセス実態調査

- 検知した悪性WebサイトをURLフィルタリングサービスへ連携し、利用者のアクセス履歴（統計情報）をもとに悪性Webサイトに対する利用者のアクセス実態調査を実施

対策試行

- 検知した悪性WebサイトをURLフィルタリングサービスへ連携し、悪性Webサイトリストの有効性の評価を実施
- ブラウザの悪性Webサイト対策機能連携による早期対策
- 狙われやすい事業者や国内の専門機関等との連携による影響度に応じた悪性Webサイトのテイクダウン試行

普及啓発・対策連携

- 偽装されやすい業界団体や企業をはじめとした国内事業者間での連携方法や先行して対策を講じる企業の事例を含む参考資料の作成
- 一般国民目線で自衛に役立つ情報を周知啓発素材としてとりまとめ