

A13

フィッシングサイト判定補助
システム開発プロジェクト

吉村 颯泰
多田 楓菜

磯貝海玖亜
山田 珠音

川口 晴太郎
横内 郁弥

概要

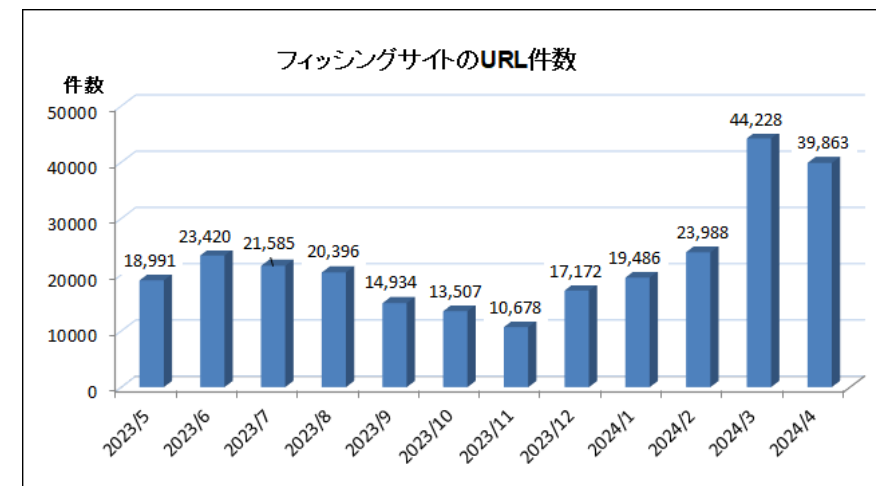
クライアント

日本サイバー犯罪対策センター（JC3）

背景

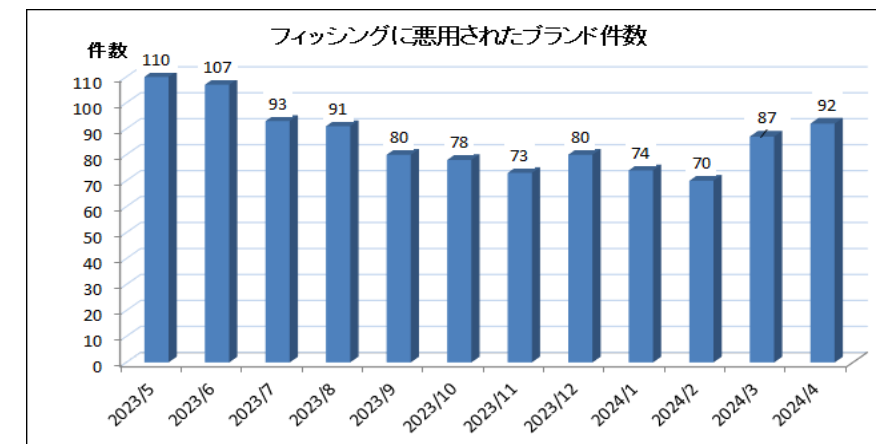
フィッシングサイトが近年急増

フィッシング対策協議会の月次報告書でフィッシングサイトの数を確認してみると近年で大きく増加している。



ブランドの悪用も増加

フィッシングに悪用されたブランドの件数も増加してきている。



背景

JC3がPredatorというシステムの開発



- ・ Predatorとは、フィッシングサイトを簡単に閉鎖できるというシステム。
- ・ 閉鎖できるサイトは、JC3がフィッシングサイトと特定したものだけ。
- ・ 特定されたフィッシングサイトとは利用者からの被害報告や怪しいと送られてきたもの

背景

Predatorで閉鎖できるサイト数は限りがある

閉鎖できるサイトは、JC3がフィッシングサイトと特定したものだけ
今では利用者が見つかるか、被害に合わないを見つけられない。



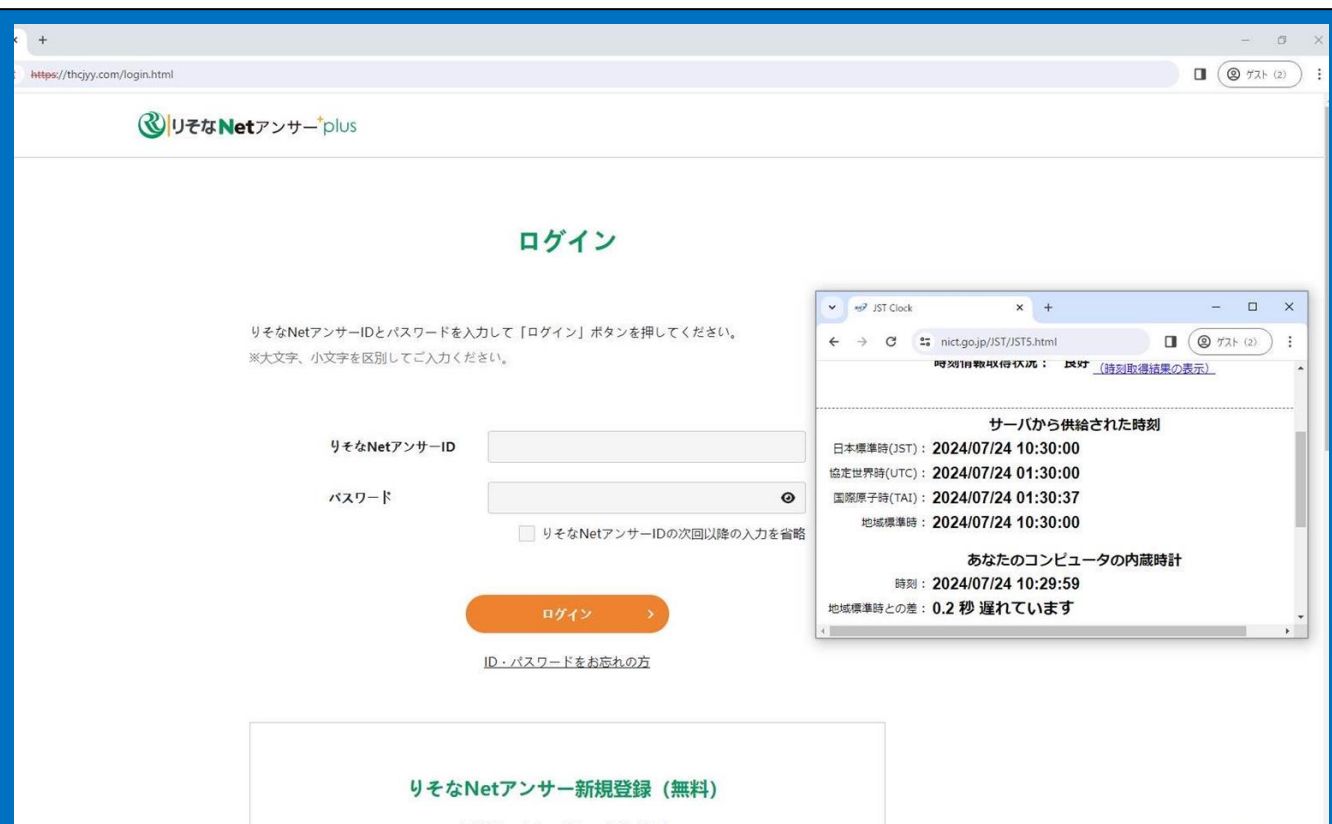
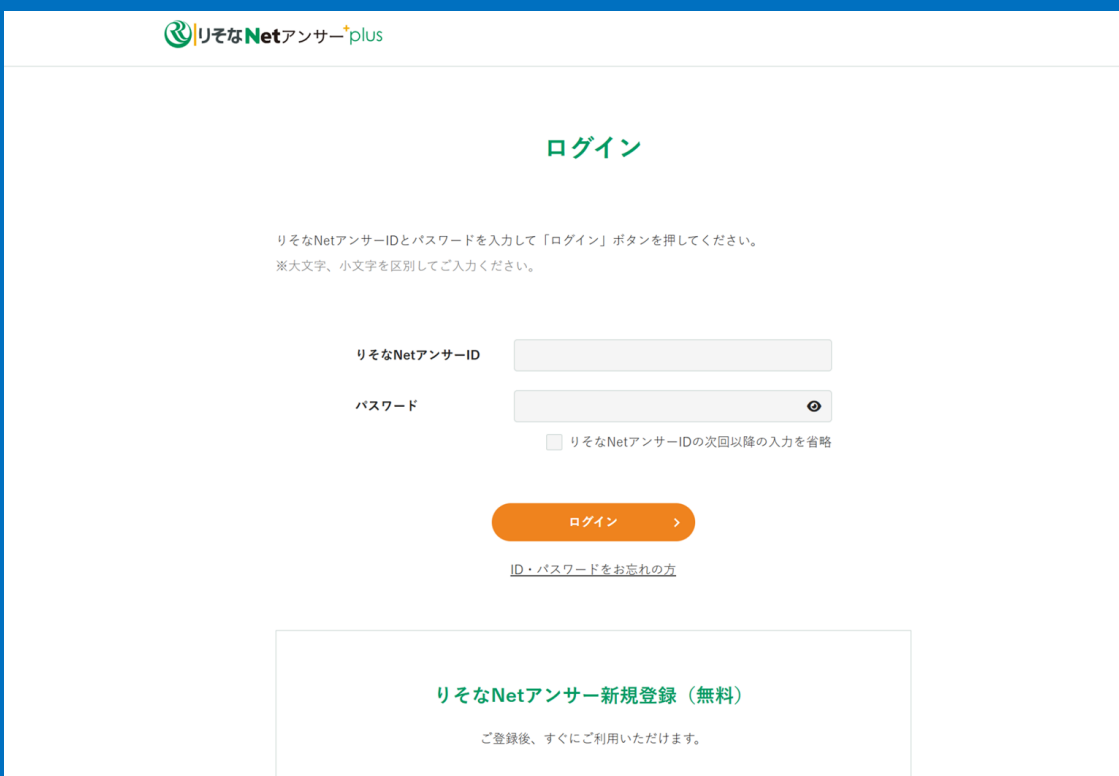
課題：フィッシングサイトの搜索

そのため、現在特定されているフィッシングサイトから得られる情報で
新たなフィッシングサイトを見つけ出すシステムの提案

背景

引用： [りそなNetアンサー | りそなカード《セゾン》 | りそなカード](#)

フィッシングサイト判別方法



背景

引用： [りそなNetアンサー | りそなカード《セゾン》 | りそなカード](#)

正しいサイト

The screenshot shows the official login page for risonaNet Answer Plus. The page has a clean, professional layout with a white background and blue accents. At the top left is the logo. The main heading is "ログイン" (Login). Below it, there is a short instruction in Japanese: "りそなNetアンサーIDとパスワードを入力して「ログイン」ボタンを押してください。 ※大文字、小文字を区別してご入力ください。" (Enter your risonaNet Answer ID and password and click the "Login" button. Please distinguish between uppercase and lowercase letters when entering). There are two input fields: "りそなNetアンサーID" and "パスワード". Below the password field is a checkbox for "りそなNetアンサーIDの次回以降の入力を省略" (Omit input for next time and onwards). An orange "ログイン" button with a right arrow is positioned below the fields. At the bottom, there is a link: "ID・パスワードをお忘れの方" (If you have forgotten your ID or password). At the very bottom, there is a green box with the text "りそなNetアンサー新規登録 (無料)" (New registration for risonaNet Answer (free)) and "ご登録後、すぐにご利用いただけます。" (After registration, you can use it immediately).

フィッシングサイト

The screenshot shows a phishing site that mimics the official login page. The URL in the browser is "https://thcjy.com/login.html". The page layout is identical to the official site, including the logo, "ログイン" heading, instructions, input fields, checkbox, and "ログイン" button. However, there are several red flags: the URL is suspicious, and there is a small inset window in the bottom right corner. This window is titled "時刻情報取得状況" (Time Information Acquisition Status) and shows a comparison of server and local times. The data is as follows:

サーバから供給された時刻	
日本標準時(JST)	2024/07/24 10:30:00
協定世界時(UTC)	2024/07/24 01:30:00
国際原子時(TAI)	2024/07/24 01:30:37
地域標準時	2024/07/24 10:30:00

あなたのコンピュータの内蔵時計	
時刻	2024/07/24 10:29:59
地域標準時との差	0.2 秒 遅れています

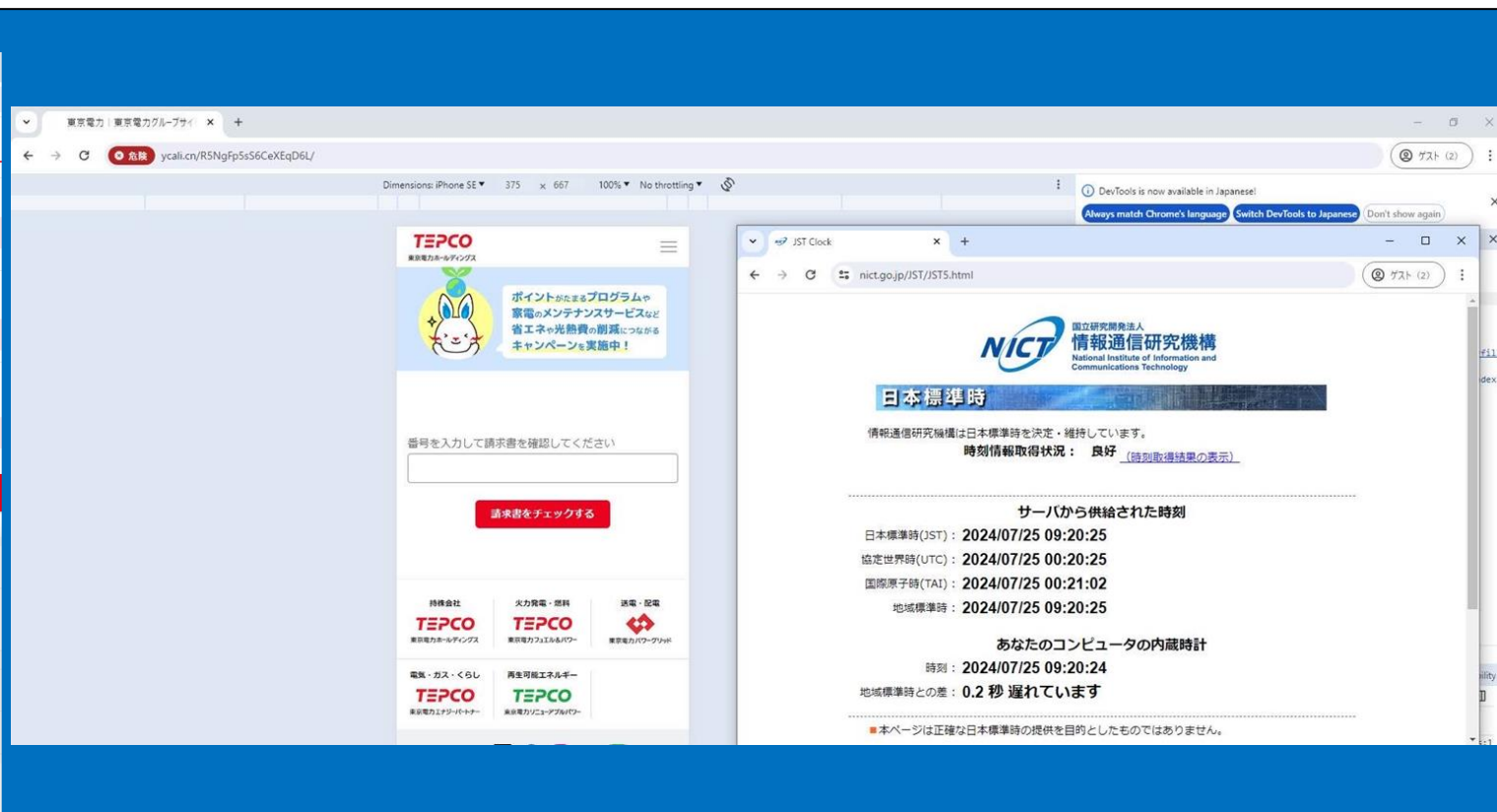
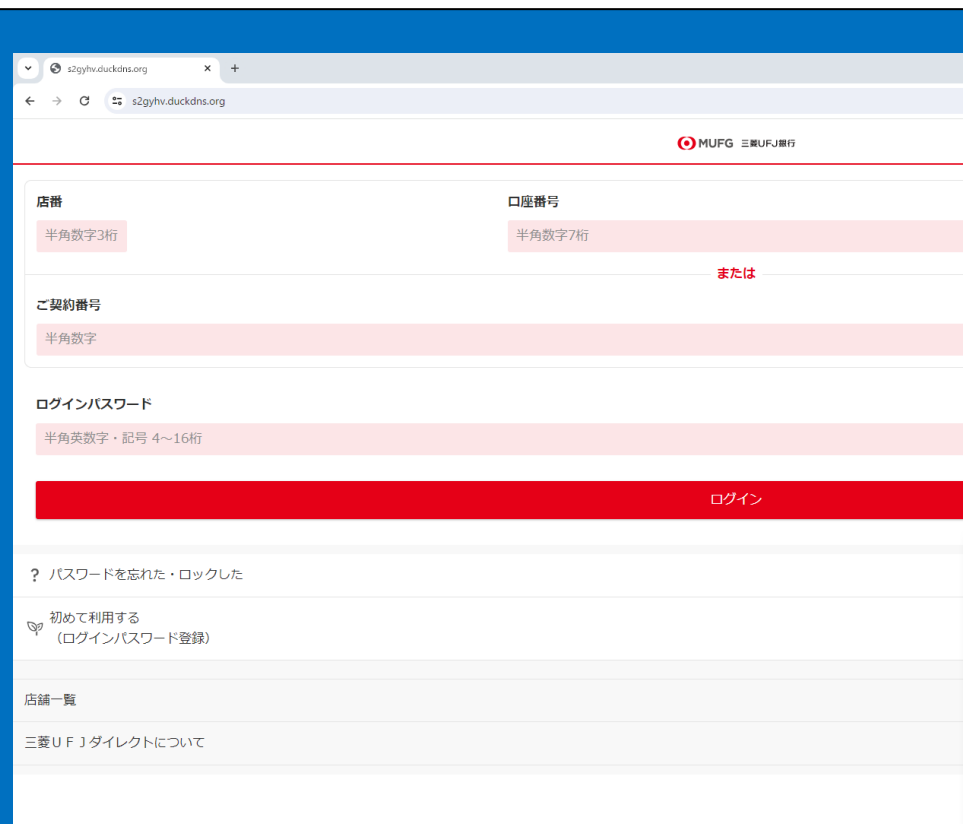
The time difference of 0.2 seconds is a clear indicator of a phishing attempt. At the bottom of the page, there is a green box with the text "りそなNetアンサー新規登録 (無料)" (New registration for risonaNet Answer (free)).

背景

引用：[りそなNetアンサー](#) | [りそなカード《セゾン》](#) | [りそなカード](#)

フィッシングサイト

似ているサイトはたくさん存在している



背景

フィッシングサイト



The screenshot shows a web browser window with the address bar containing the URL `z7t7d.ankongb.cn/caonima=hrdl1o4.co.jp`. A large grey L-shaped arrow points from the address bar to the text "URLの違い" (Difference in URL). Below this, the legitimate website URL `www.kuronekoyamoto.co.jp` is displayed. A security overlay from Cloudflare is present, showing a "検証中..." (Checking...) status with a circular progress indicator and the Cloudflare logo with the text "クラウドフラアライバンスご契約条件". Below the overlay, a message reads: "www.kuronekoyamoto.co.jp では、続行する前に接続のセキュリティを確認する必要があります。" (On www.kuronekoyamoto.co.jp, you need to check the security of the connection before proceeding.)

URLの違い

`www.kuronekoyamoto.co.jp`

あなたが人間であることを確認します。これには数秒かかる場合があります。

検証中...  クラウドフラアライバンスご契約条件

www.kuronekoyamoto.co.jp では、続行する前に接続のセキュリティを確認する必要があります。

背景

判定方法

- ・ サイトのURL
- ・ 日本語や文字が変な場所
- ・ サイトのデザインの違い 等

が挙げられる

このフィッシングサイトの判定はボランティアができる範囲ではないためやはり我々のシステムは怪しいサイトを出すまでである

目的・目標

目的

フィッシングサイトを判定補助を行う

目標

「地域性」「ネットワークの分布」「攻撃対象」の要素でスコアリングし怪しいかどうかを提示する

目標

要素でスコアリングし怪しいサイトを提示

「地域性」「ネットワークの分布」「攻撃対象」
3つの要素でスコアリングし怪しいサイトを提示する。

URL	IPアドレス	国名	カテゴリ	スコア
https://amazon.ff16998.com/OzgJHg	172.1.0.1	日本	amazon	10
https://guqnfzj.tqhmu.cn/caonima	10.0.0.1	アメリカ	メルカリ	9
https://smbc.investpro.jp/vpasslogin/index.html	192.168.1.1	日本	三井住友カード	8
https://cntmkt.awwhfcjfls.com/OzgJHg	172.6.0.1	ドイツ	メルカリ	7
https://icloud.apple-itudin.cphlb.cn/sign-insetup	72.16.0.1	日本	apple	7

進捗説明

要素 1

1. ネットワーク分布（同一ネットワーク部）の観点

フィッシングサイトのIPアドレスからCIDRを取得し含まれるIPアドレスの中にどれだけフィッシングサイトが存在するか

大体フィッシングサイト1つから得られるIPアドレスは200～65000個近くあり、その中で50個に1つの割合で存在している

そのため、同一ネットワーク部の中でフィッシングサイトとして活用されているIPアドレスは2%である。しかし、現在活用されていないIPアドレスが今後フィッシングサイトとして使用される可能性もある。

進捗説明

要素 1

1. ネットワーク分布（同一ネットワーク部）の観点

同一であれば2点

同一でなければ1点

で表す。

進捗説明

要素 2

2. 地域性 (MAP) の観点

フィッシングサイトが誕生しやすい・封鎖されにくい裏には対応が悪いレジストラが隠れている。そのレジストラからIPアドレスを購入したり、テイクダウンがされなかったりとするためそのレジストラ付近に集まる。

そのためフィッシングサイトが密集している地域はそれだけフィッシングサイトの可能性が高い。

進捗説明

要素2

2. 地域性 (MAP) の観点

300km以内に10個以上で赤くなるようにした

10以上	高いとみなし	3点
5～9	中とみなし	2点
1～4	低とみなし	1点

進捗説明

要素 3

3. 攻撃対象（トレンドグラフ）の観点

攻撃対象がフィッシングサイトのトレンドのものと一致しているかを見る

現在のトレンドはAmazonであり、直近100件の内70件が一致していた

そのため、フィッシングサイト全体の70%が最新のトレンドに埋め尽くされている。そのため、怪しいサイトがトレンドの攻撃対象だった場合高確率でフィッシングサイトである。

進捗説明

要素 3

3. 攻撃対象（トレンドグラフ）の観点

先月から

2割以上増えていたら	5点
2割以下の増加ならば	4点
変わらない場合は	3点
2割以下の減少ならば	2点
2割以上減少していたら	1点

進捗説明

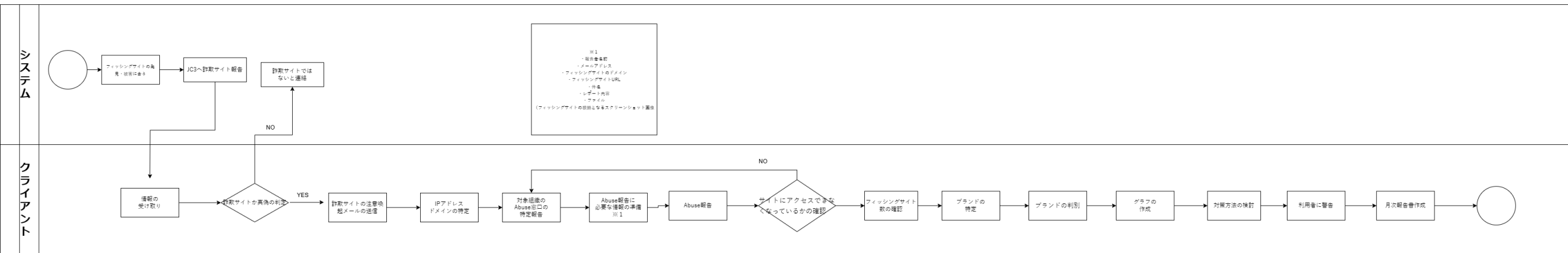
要素

1. ネットワーク分布（同一ネットワーク部）の観点
2. 地域性（MAP）の観点
3. 攻撃対象（トレンドグラフ）の観点

この3つの観点を参考に、さまざまな要素が確認出来たらそれだけフィッシングサイトの可能性が高いという風に捉えることができる。
より割合が高い3の観点ではフィッシングサイトの可能性がもっとも高いと言える。

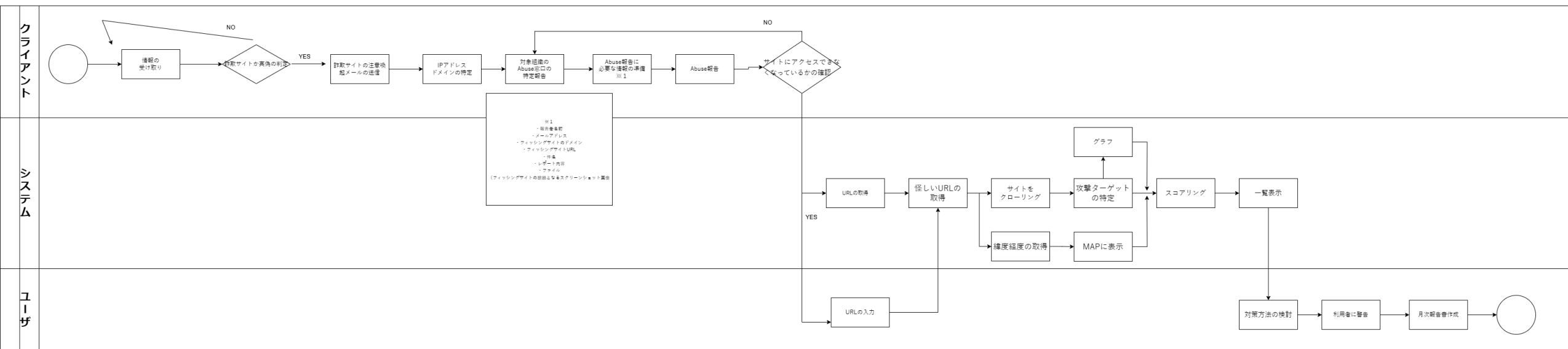
業務分析

業務フロー図



業務分析

業務フロー図



機能説明

入力画面

このシステムでなにをINするかというと
フィッシングサイトのURL

このURLはJC3がすでに特定してあるもの
(PredatorでURLは入手可能)

URL入力画面

URL → ドメイン → IPアドレス

URLを入力してください: 入力

IPアドレス → ドメイン

IPアドレスを入力してください: 入力

IPアドレスの情報取得

IPアドレスを入力してください: 入力

機能説明

一覧画面→ダッシュボード

入力したURLから得られる情報を分析して記載する

フィッシングサイトから取得したURL
そのURLのIPアドレス
Whoisで登録されている国名
攻撃ターゲット
3つの要素でスコアリングしたもの

URL	IPアドレス	国名	カテゴリ	スコア
https://amazon.ff16998.com/OzgJHg	172.1.0.1	日本	amazon	10
https://guqnfzj.tqhmu.cn/caonima	10.0.0.1	アメリカ	メルカリ	9
https://smbc.investpro.jp/vpasslogin/index.html	192.168.1.1	日本	三井住友カード	8
https://cntmkt.awwhfcjfls.com/OzgJHg	172.6.0.1	ドイツ	メルカリ	7
https://icloud.apple-itudin.cphlb.cn/sign-insetup	72.16.0.1	日本	apple	7

機能説明

グラフ

この機能で分かることは
フィッシングサイトのトレンド

今現在どんなフィッシングサイトが増えているかを
一目でわかるようにする

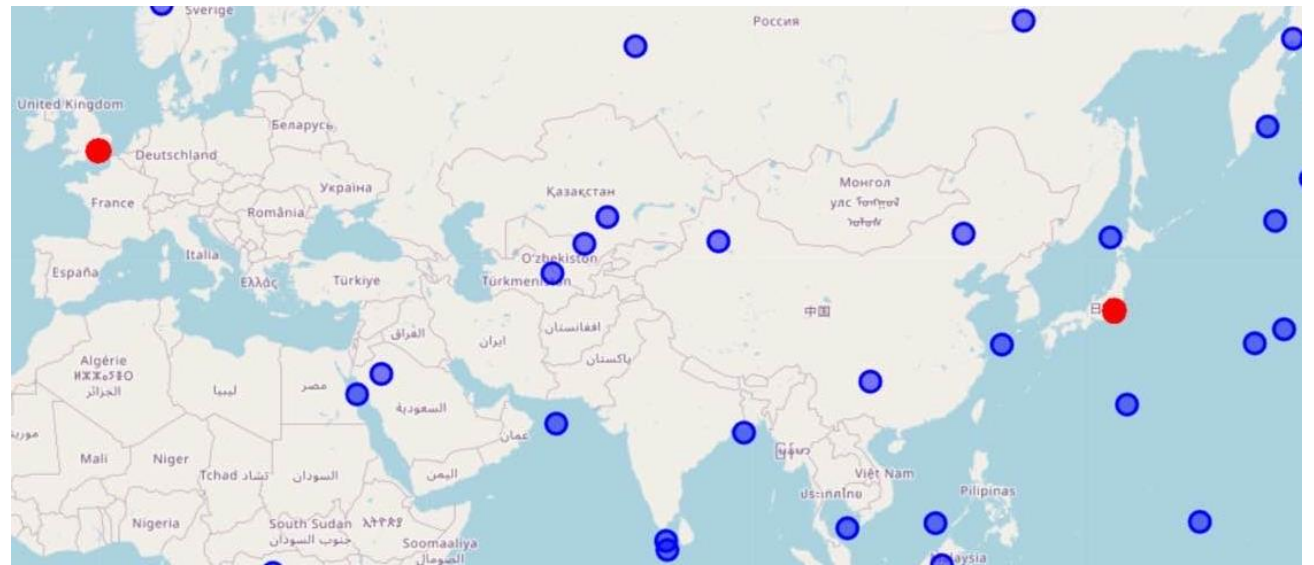
これは毎月出ている月次報告書に記載している、ブランドの増減やフィッシングサイトの増減等の情報分析業務の軽減につながる

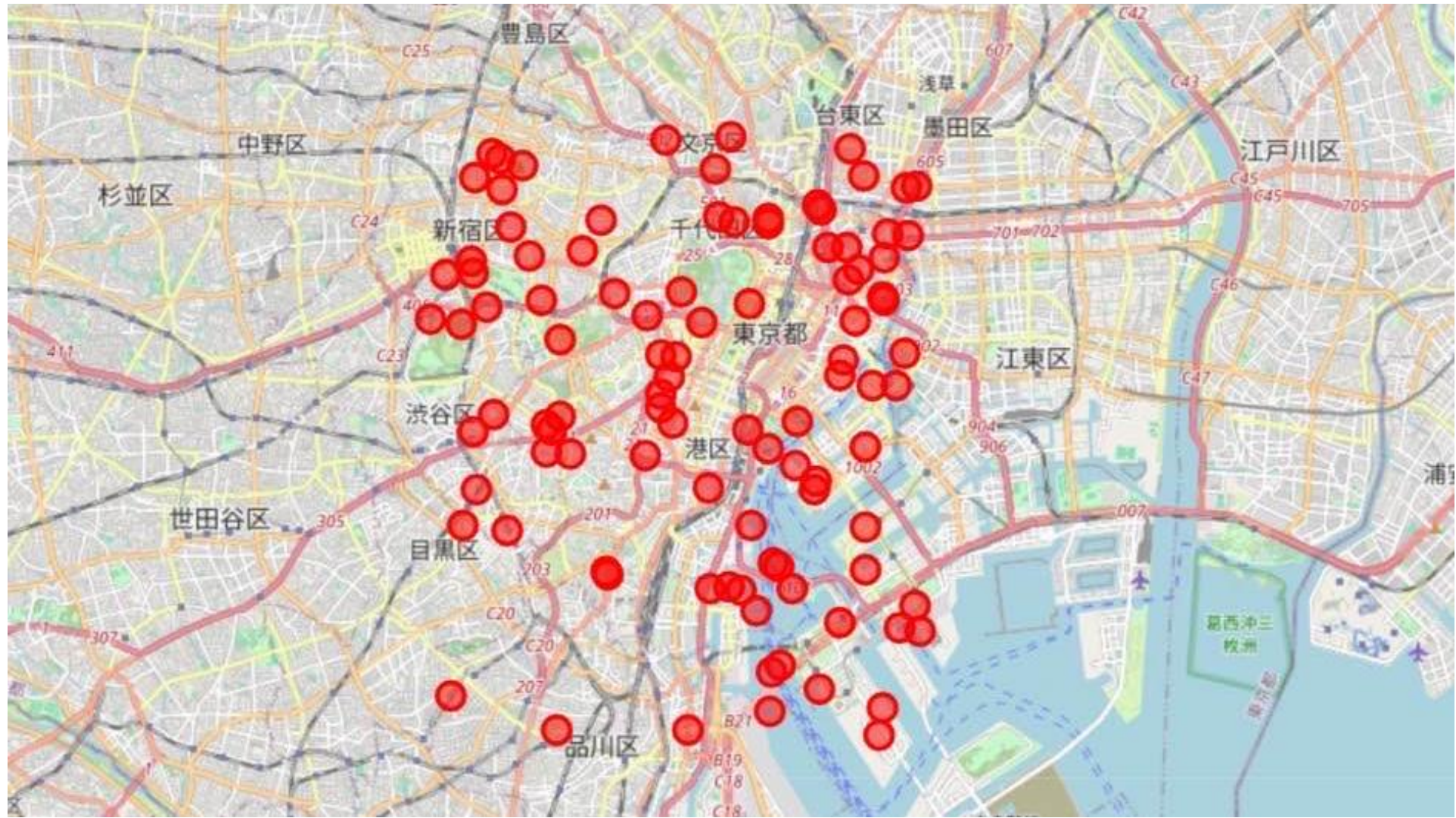
機能説明

MAP

点で表示させることでより正確な範囲

このURLはJC3がすでに特定してあるもの
(PredatorでURLは入手可能)





業務軽減

対応の悪いレジストラの特定

フィッシングサイトが誕生しやすい・封鎖されにくい裏には対応が悪いレジストラが隠れている。

その特定方法は一つ一つAbuse報告やテイクダウンを行ってその対応の速さ・正確さ・そもそも対応してくれるかという部分を見て判断するのだが、必然的にフィッシングサイトが多く存在する地域は対応が悪いレジストラがいるということになるので、一つ一つ見なくてもMAPで大まかに対応の悪いレジストラを特定できるようになる。

業務軽減

各情報の分析・収集

フィッシングサイトをテイクダウンするときや報告書に必要な情報の収集が楽になる

- ・ IPアドレスの入手するためにWhoisにドメインの入力が必要
- ・ 国名を入手するためにIPアドレスが必要→Whoisに入力
- ・ カテゴリ（攻撃対象）を入手するのに実際にサイトのアクセスが必要
- ・ フィッシングサイトの同一ネットワーク部を入手するためにCIDRが必要
CIDRを入手するためにWhoisにIPアドレスの入力が必要

システムの整合性

情報の整合性

実際に整合性を確かめるためURLを入力し、どのような結果が返ってくるか検証した

実際の正しいURLを入れたところ何件か高得点（8～10）
が出てしまったが基本的には4～6であった

これは地域制の観点でフィッシングサイト多数地域に入ったのが原因であるため、
実際は1～3の点数であるため整合性は取れている
逆にフィッシングサイトを入れたところ出てくる割合は半々くらいであった

ポスター

フィッシングサイト判定補助 システム開発プロジェクト

A13

○ メンバー・役割

吉村 颯泰 (プロジェクトマネージャ)
川口 晴太郎 (システム開発)
山田 珠音 (システム開発)
多田 楓菜 (システム開発)
横内 郁弥 (デザイナー)
磯貝 海玖亜 (デザイナー)

○ 開発環境

Python
php・HTML
MySQL

○ プロジェクト概要

フィッシングサイトの情報を集めて、閉鎖できるようにするために情報を提供するシステムの補助を行うシステムを開発した。
まず、クライアントであるJC3が特定しているフィッシングサイトのURLを解析し、グラフやマップを表示することが可能である。また、解析したURLから、IPアドレス・攻撃ターゲット・Whoisで登録されている国名、その情報に対してスコアリングすることができる。

○ プロジェクトの目標・目的

目的

フィッシングサイトの判定補助を行う

目標

「地域制」
「攻撃対象」
「ネットワーク分布」

の要素でスコアリングし怪しいかどうかを提示する

○ 成果物 概要

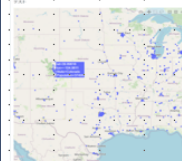
機能一覧

- ・MAP
- ・グラフ
- ・怪しいサイト一覧画面



サイト一覧

フィッシングサイト一覧画面
怪しいサイトと各種情報記載
スコアリング結果を一目で見れる



MAP

フィッシングサイトの位置を
確認できる
緯度経度を取得しMAPに記載



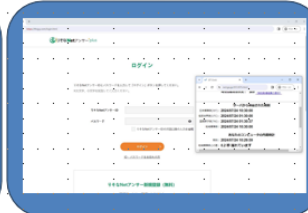
グラフ

フィッシングサイトの
攻撃ターゲットごとに
グラフがあるので増減を
確認できる

○ フィッシングサイトの判別方法 参考文献: リモネNetアンサー | リモネカード《セゾン》 | リモネカード



○ 正しいサイト



×フィッシングサイト

見た目だけで判断
するのは難しい

サイトのURL
日本がおかしな場所
サイトのデザインが違
うところで判断する

閲覧ありがとうございました