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　　礒貝海玖亜　　川口　晴太郎
多田　楓菜　　山田　珠音　　横内　郁弥

概要

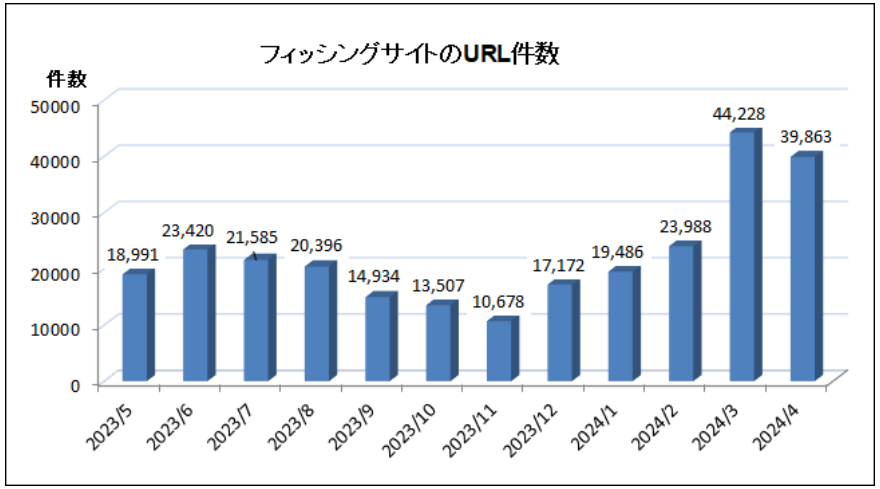
クライアント

日本サイバー犯罪対策センター（ＪＣ３）

背景

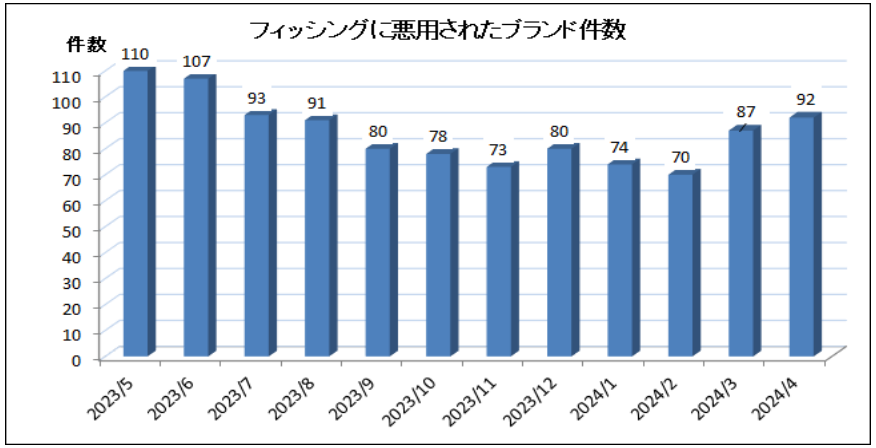
フィッシングサイトが近年急増

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けるか、被害に合わないと見つけられない。

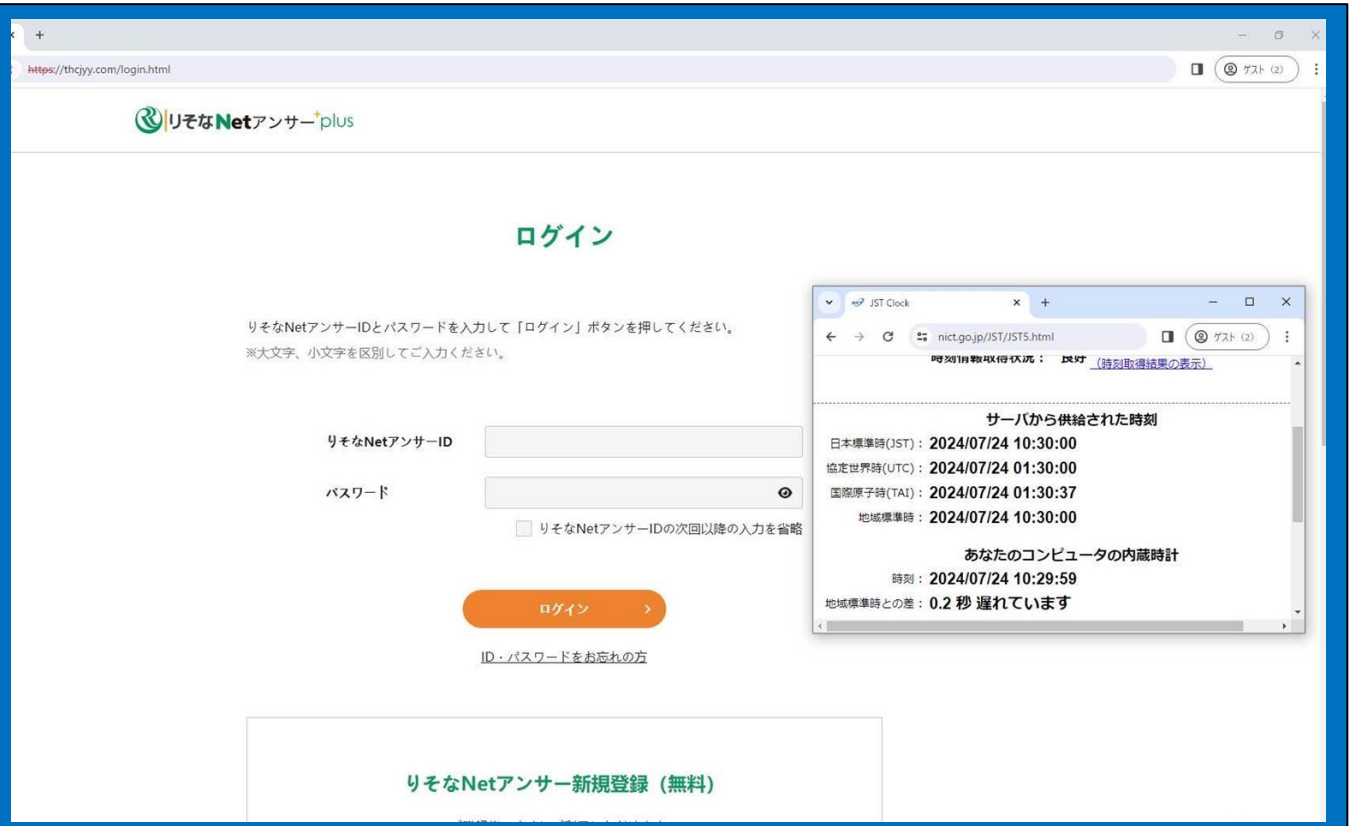
課題：フィッシングサイトの捜索

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

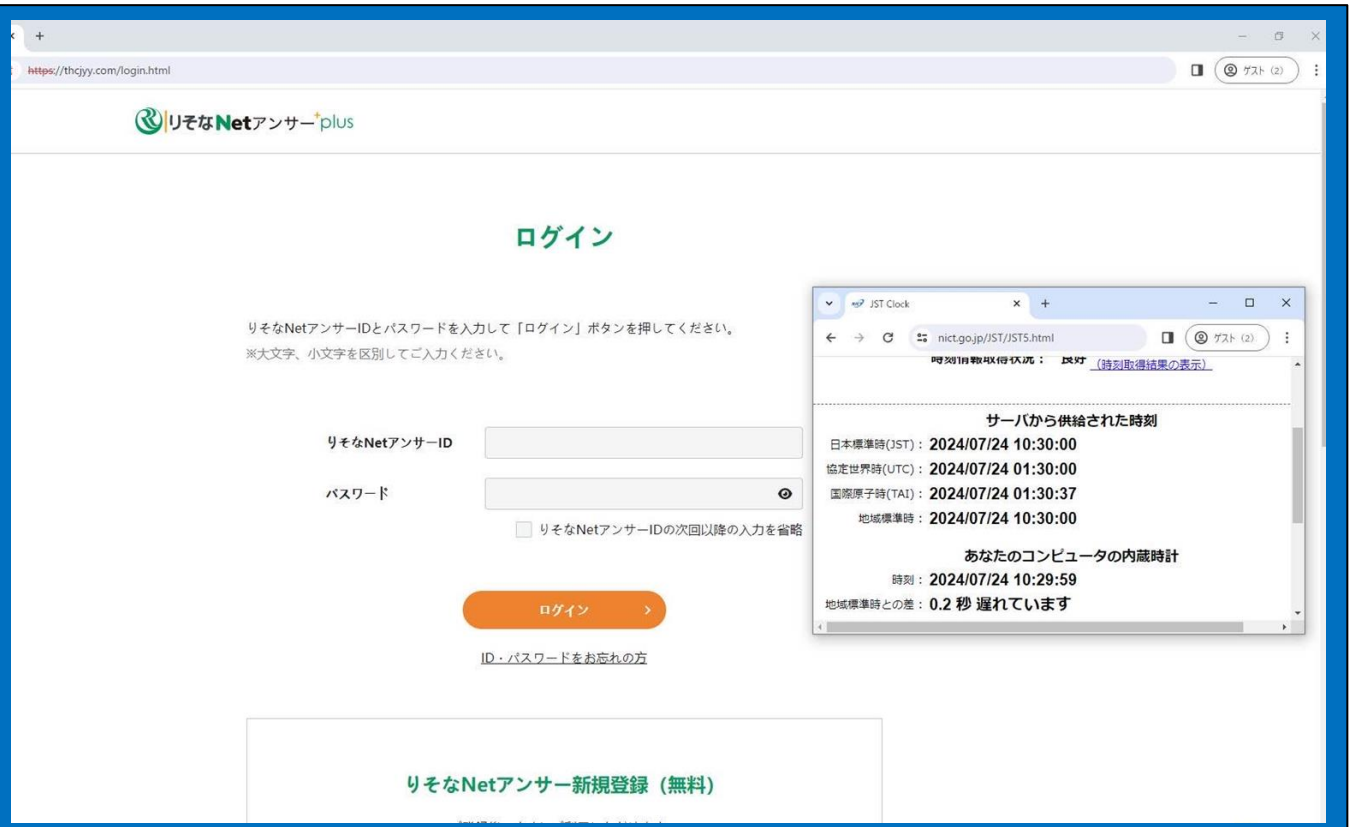


背景

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

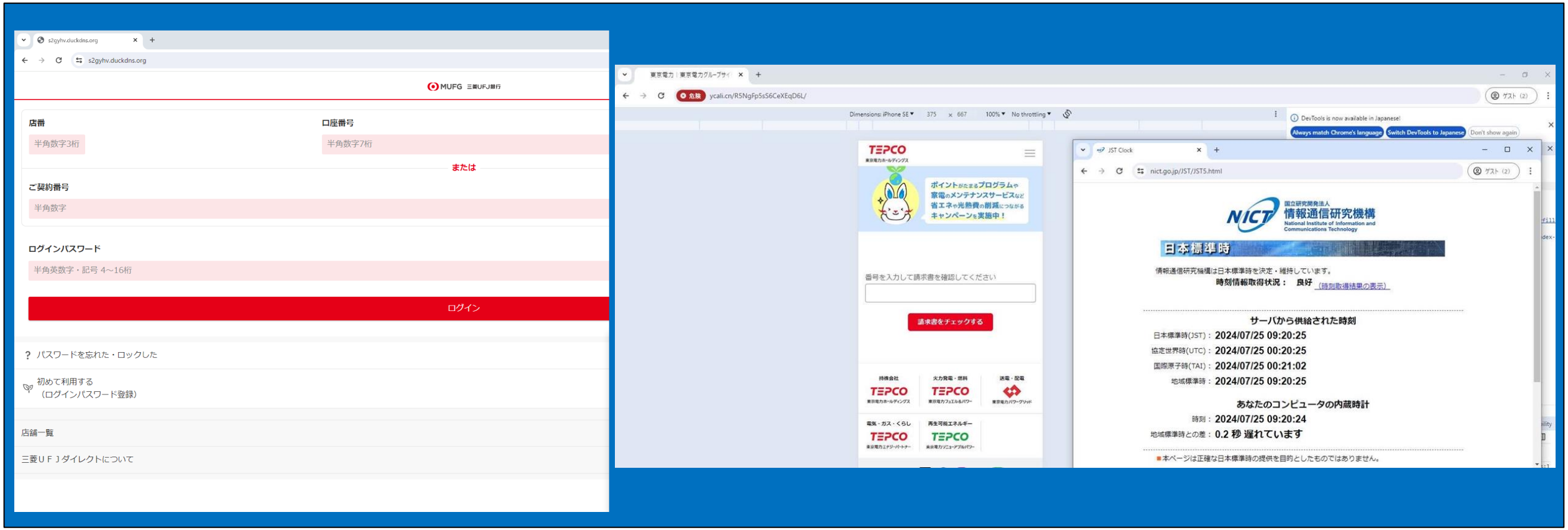
フィッシングサイト



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

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みる

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

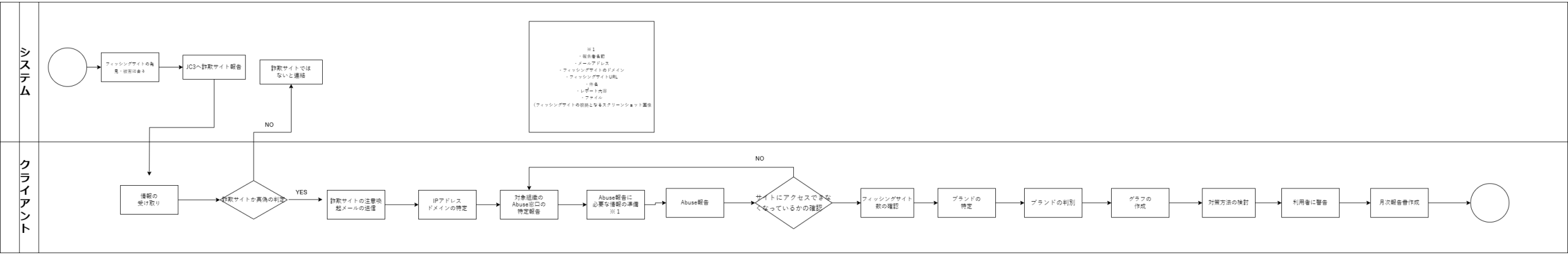
要素

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。

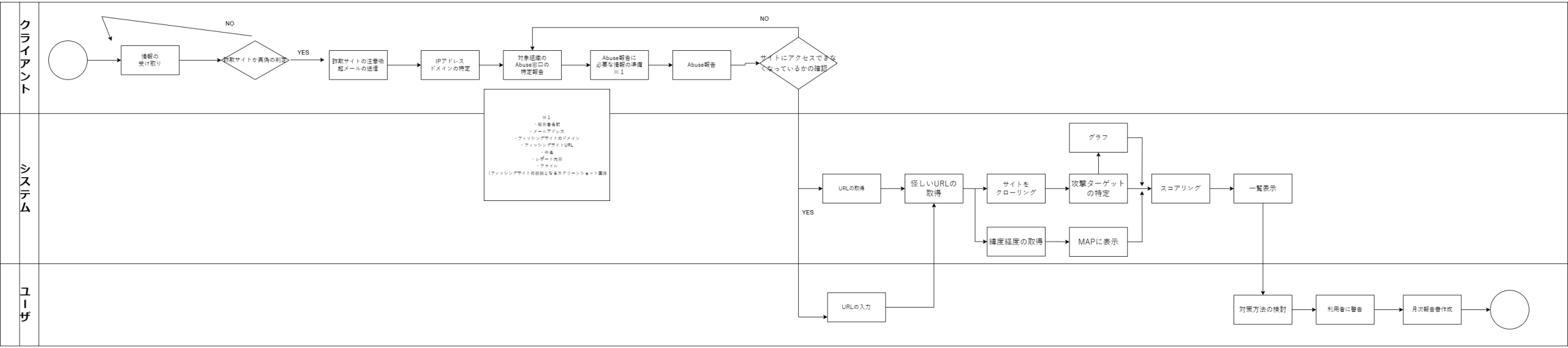
業務分析

業務フロー図


システム
クライアント
フィッシングサイトの発見・被害に合う
JC3へ詐欺サイト報告
詐欺サイトではないと連絡
※1
・販売者名前
・メールアドレス
・フィッシングサイトのドメイン
・フィッシングサイトURL
・件名
・レポート内容
・ファイル
（フィッシングサイトの根拠となるスクリーンショット画像
NO
情報の受け取り
詐欺サイトか真偽の判定
YES
詐欺サイトの注意喚起メールの送信
IPアドレス ドメインの特定
対象組織のAbuse窓口の特定報告
Abuse報告に必要な情報の準備 ※1
Abuse報告
サイトにアクセスできなくなっているかの確認
NO
フィッシングサイト数の確認
ブランドの特定
ブランドの判別
グラフの作成
対策方法の検討
利用者に警告
月次報告書作成

業務分析

業務フロー図

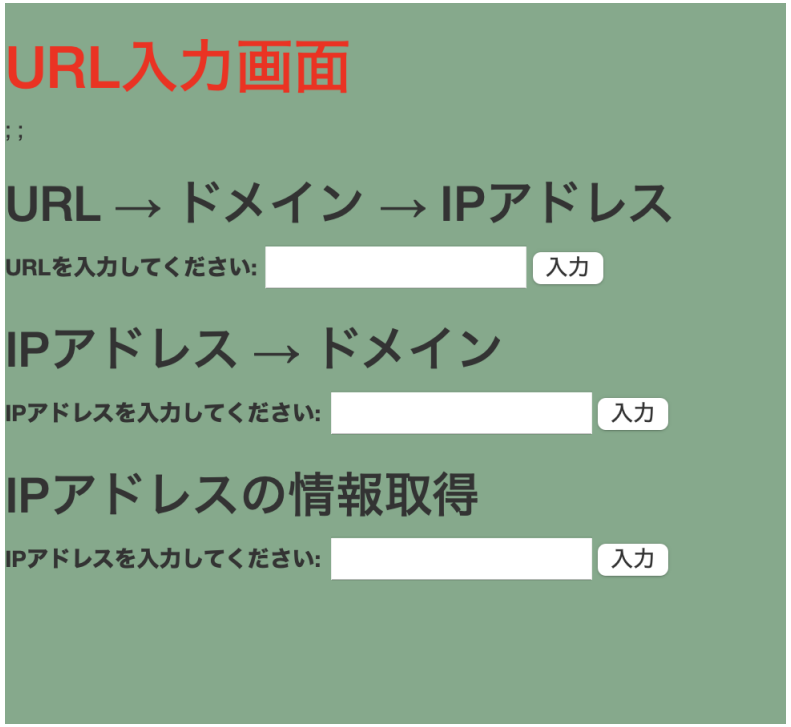

クライアント
システム
ユーザ
NO
情報の
受け取り
詐取サイトか真偽の判定
YES
詐取サイトの注意喚起メールの送信
IPアドレス
ドメインの特定
対象組織の
Abuse窓口の
特定報告
Abuse報告に
必要な情報の準備
※1
Abuse報告
NO
サイトにアクセスできなくなっているかの確認
※1
・報告者名前
・メールアドレス
・フィッシングサイトのドメイン
・フィッシングサイトURL
・件名
・レポート内容
・ファイル
（フィッシングサイトの原因となるスクリーンショット画像
YES
URLの取得
怪しいURLの
取得
サイトを
クローリング
攻撃ターゲット
の特定
グラフ
スコアリング
一覧表示
緯度経度の取得
MAPに表示
URLの入力
対策方法の検討
利用者に警告
月次報告書作成

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）



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

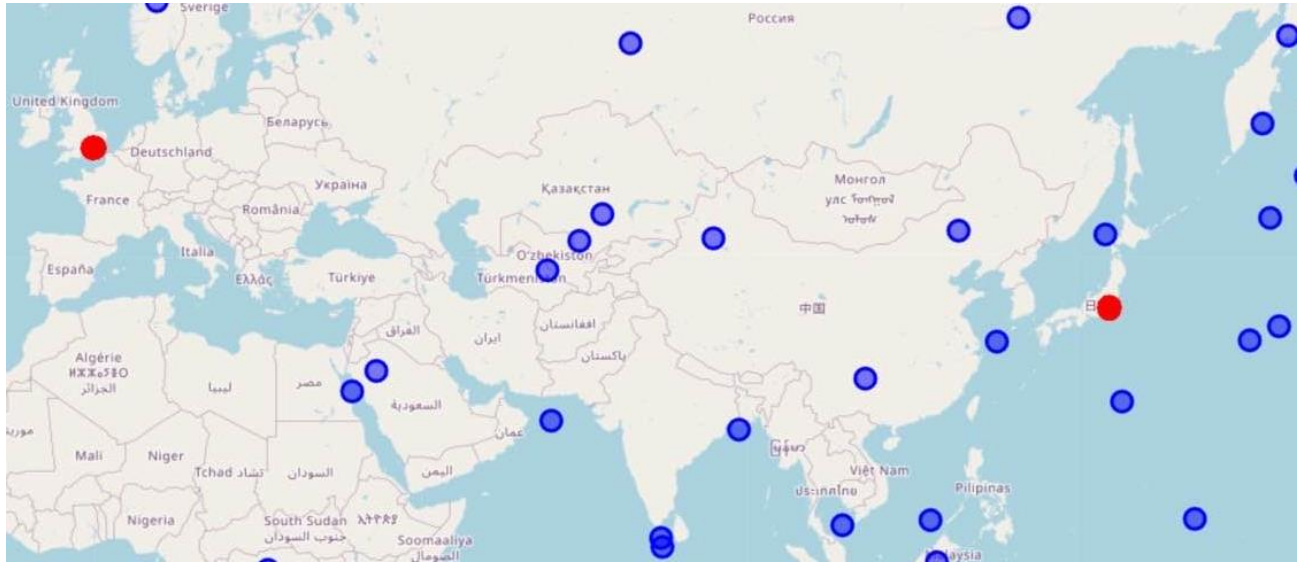
これは毎月出ている月次報告書で記載している、ブランドの増減やフィッシングサイトの増減等の情報分析業務の軽減につながる

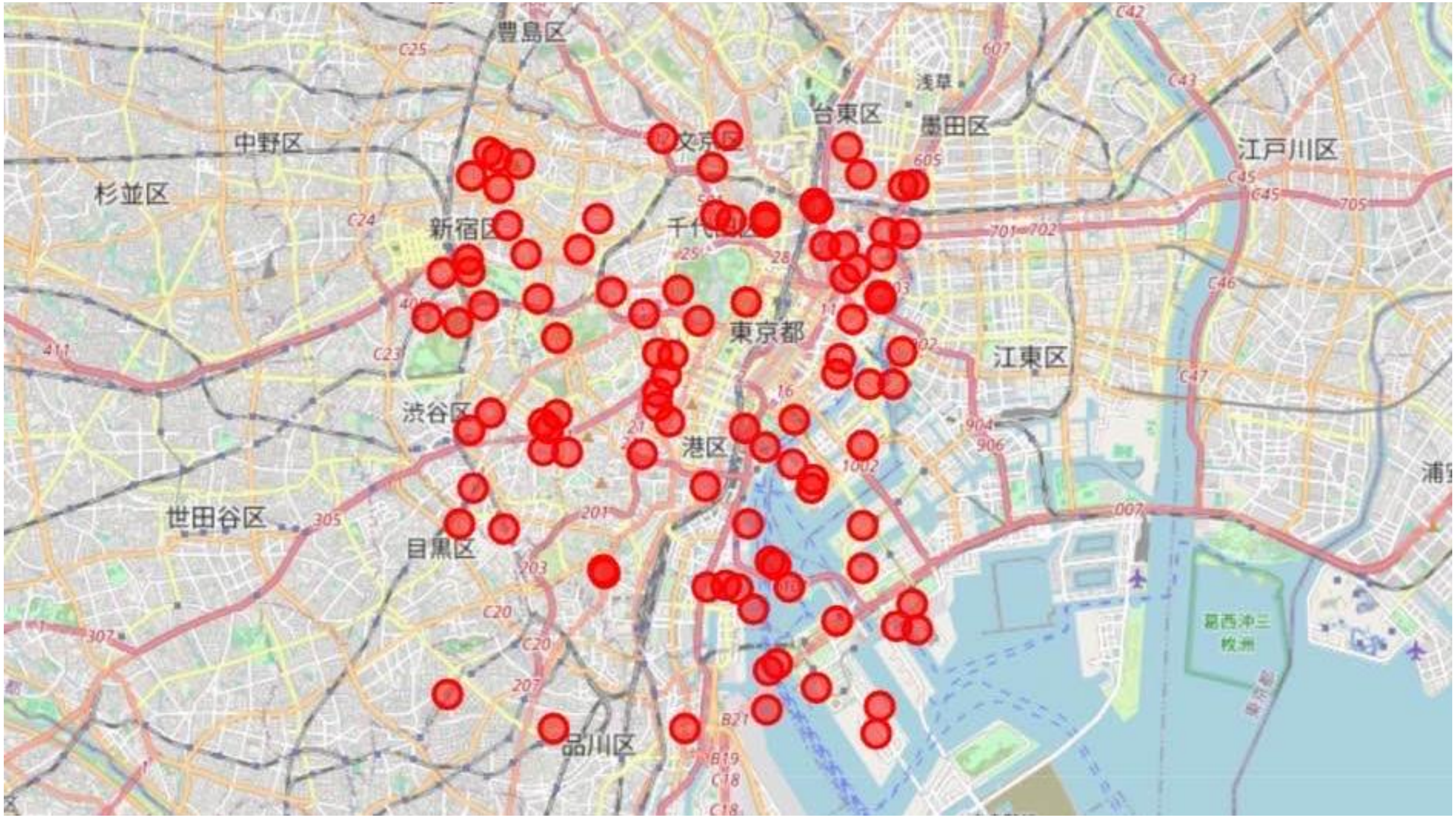
機能説明

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）




豊島区
中野区
杉並区
文京区
台東区
浅草
墨田区
江戸川区
新宿区
東京都
江東区
渋谷区
港区
世田谷区
目黒区
品川区

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）
礒貝 海玖亜（デザイナ）

○ 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、閉鎖できるようにな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

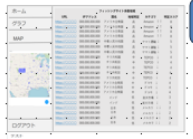
目標

「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

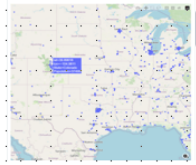
機能一覧

・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

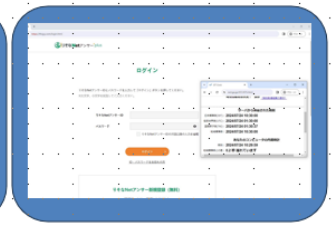
グラフ

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：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



✕ 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