# 不正送金に係るフィッシング犯行グループの観測と〈みずほ〉の対策

**みずほ銀行 / Mizuho Bank**

**みずほフィナンシャルグループ / Mizuho Financial Group**

サイバーセキュリティ統括部/Cyber Security Management Department
Tsukasa Takeuchi, Takuya Endo, Hiroyuki Yako

2025年1月22日

ともに挑む。ともに実る。
MIZUHO

# 発表者紹介 (発表順)

MIZUHO

ともに挑む。
ともに実る。

**竹内　司**
**Tsukasa Takeuchi**

Cybercrime

**遠藤　拓也**
**Takuya Endo**

Technical

**八子　浩之**
**Hiroyuki Yako**

CSIRT

## Engineer

**西川　昌広　Masahiro Nishikawa**

## Technical team

近藤　一成　Kazunari Kondo
笹村　直樹　Naoki Sasamura
小山　昌樹　Masaki Koyama

## Cybercrime team

森　三千代 Michiyo Mori
堀口　健　Ken Horiguchi
中島　陵太　Ryota Nakashima
中野　嘉寿美　Kasumi Nakano
久世　拓海　Takumi Kuze

## Automation Measures

大迫　結花　Yuka Osako
土井　優大　Masahiro Doi

## Special thanks

浅谷さん　Asatani-san
常盤さん　Tokiwa-san

## 発表の概要

本発表では、みずほ銀行におけるフィッシング対応の課題とその解決策について説明します。

### 背景

・多数の金融機関でフィッシングによる被害が発生。みずほ銀行もターゲットになっている。
・不正送金のモニタリングやフィッシングサイトのテイクダウンによる被害抑止を実施中。
　それでも、被害は発生してしまう状況。

### 課題

・犯人のアクセスをモニタリングし即時停止するのも限界があり、フィッシングサイトの発見が急務
・フィッシング対応にはやらなければならない作業も多く、対応の人手にも限界がある

### 対策

・できるだけ早く、正確に、フィッシングサイトを検知をする
→マルウェア使い偽SMSをばらまくフィッシングアクターを監視
・対応を一部自動化する
→サイトの検知からテイクダウンまでを自動化

アジェンダ

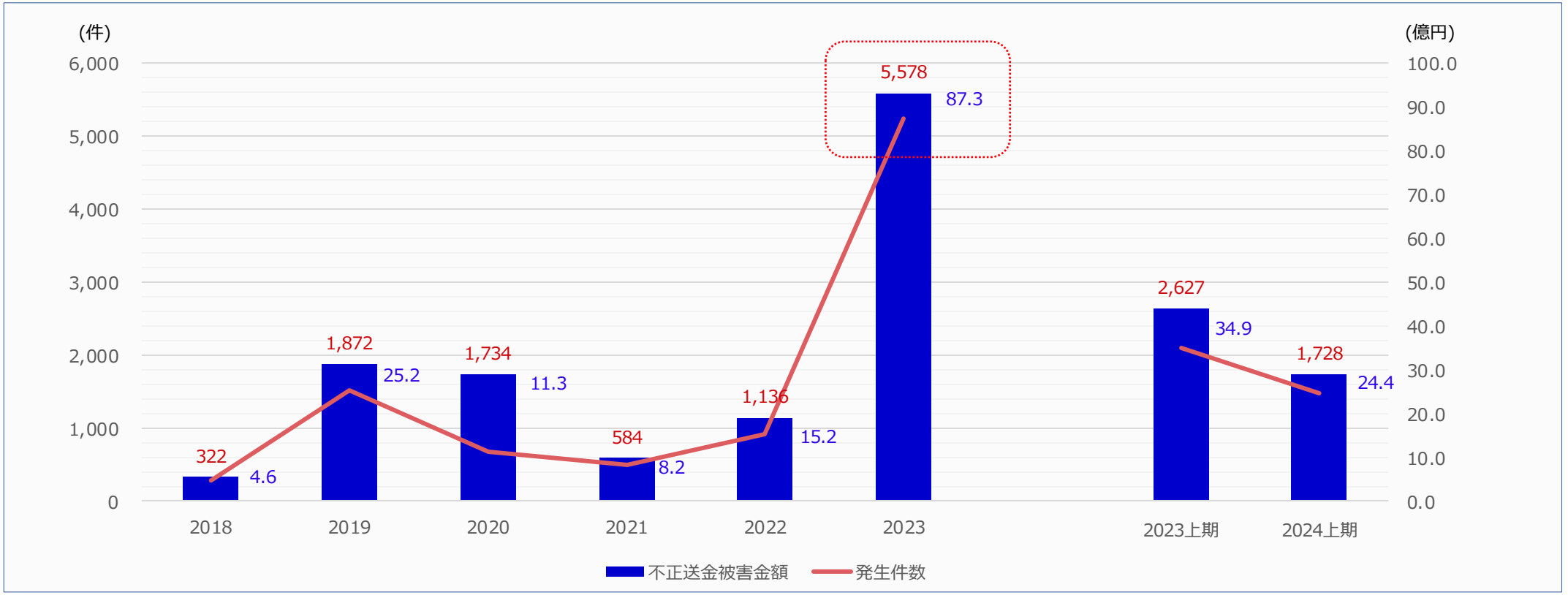
1. 国内におけるフィッシング被害の状況
2. みずほにおける不正送金対応・フィッシングサイトテイクダウン等の体制と流れについて
3. みずほを狙うフィッシングについて
4. 偽SMSを送信する犯行グループが使用するマルウェアについて
5. フィッシングサイトの早期検知の試みについて
6. みずほの自動化の取り組みと今後の方向性について

# １．国内におけるフィッシング被害の状況

# 国内におけるフィッシング被害の状況

| 2023年 | インターネットバンキングに係る不正送金の発生件数 | 5,578件 | 被害総額 | 約87億3,130万円 |
|---|---|---|---|---|

・2024年も不正送金被害は前年に近いペースで増加。金融機関ごとに多寡はあれど、相応に被害が発生している状況。
・これまで狙われたことがない金融機関もターゲットになることがあり、フィッシングへの対応が遅れると大きな被害が発生していると思われる。
・一方、フィッシング対策は特効薬のようなものはなく、様々な対策を複数組み合わせ運用していく必要がある。
その対策の1つとして、参考事例を次頁以降で解説する。




【警察庁:令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について】より

# ２．みずほにおける不正送金対応・フィッシングサイトテイクダウン等の体制と流れについて

まずは、詳細内容に入る前に、内容をわかりやすくするため、
あまり外部でお話しすることのない、銀行内の各部の役割などを
説明させてください

# みずほにおける不正送金対応・フィッシングサイトテイクダウン等の体制と流れについて

みずほには、不正送金の対応・対策に関わる主な部署として、3つの部署と2つのセンターがある。
1.インターネットバンキングとそのモニタリングを実施する部署(みずほダイレクト所管部署)とそのコールセンター
2.顧客への注意喚起や補償等を検討する金融犯罪対策部署(コンプライアンス部門)とそのコールセンター
3.フィッシングサイトの対応やサイバー犯罪対応を横断的に実施するサイバーセキュリティ統括部

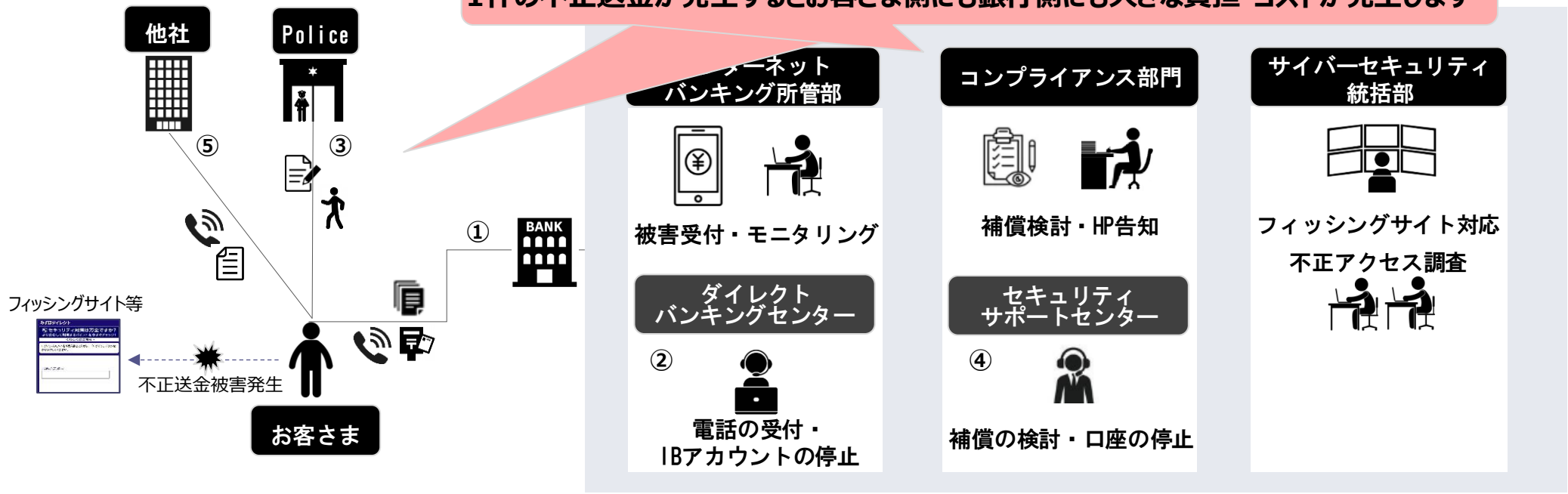
みずほにおける不正送金発生時の受付・対応イメージ
① コールセンター(ダイレクトバンキングセンター)からお客さまに架電(またはお客さまからコールセンターに入電)
② お客さまにて入出金や口座の状況を確認。不審な送金がある場合、お客さまに詳細なヒアリングをダイレクトバンキングセンターにて実施。
③ ②と並行して、お客さまから警察への相談を実施。
④「不正送金であること」が確定すると、コンプライアンス部門のセキュリティサポートセンターに所管が移り、補償有無の検討と更に詳細な調査を実施。
⑤ 上記①～③と並行して、お客さまは、パスワードや暗証番号などの漏洩の可能性がある場合、他社(他行やクレジットカード会社)にも連絡を実施。

# みずほにおける不正送金対応・フィッシングサイトテイクダウン等の体制と流れについて

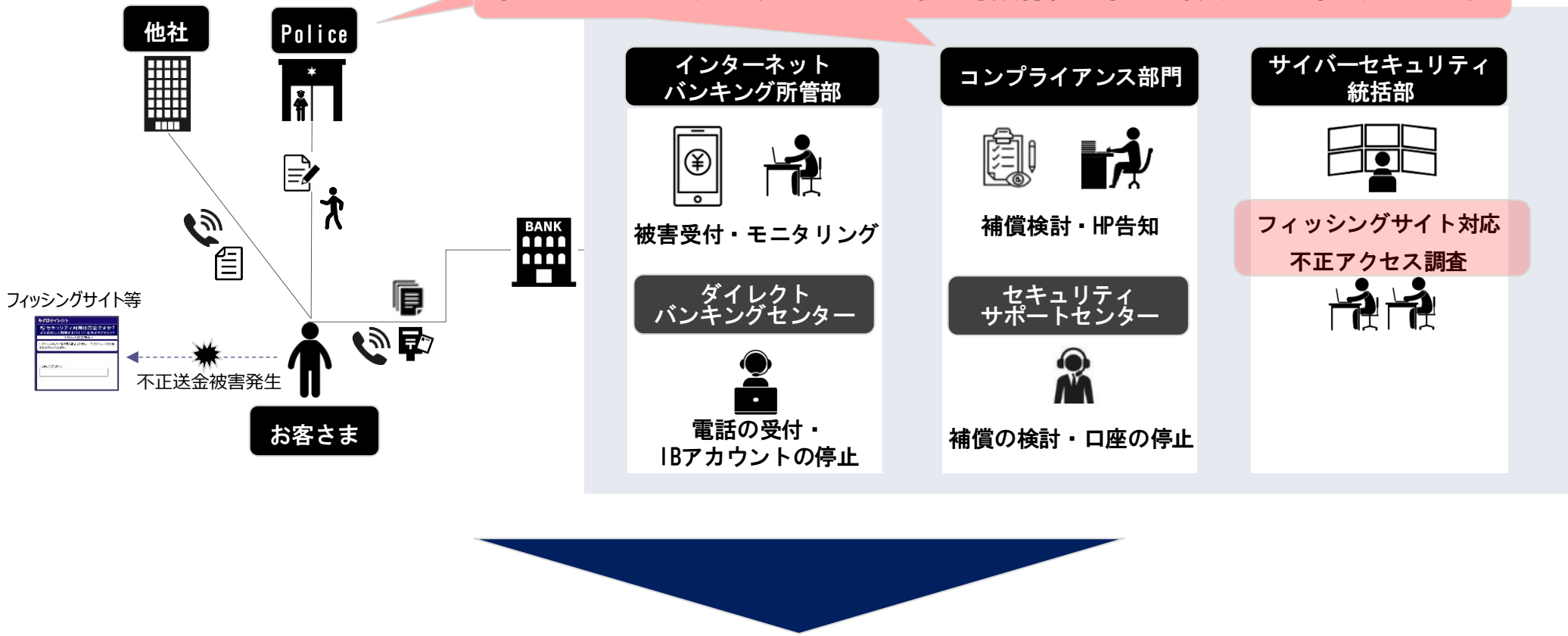
みずほには、不正送金の対応・対策に関わる主な部署として、3つの部署と2つのセンターがある。
1.インターネットバンキングとそのモニタリングを実施する部署(みずほダイレクト所管部署)とそのコールセンター
2.顧客への注意喚起や補償等を検討する金融犯罪対策部署(コンプライアンス部門)とそのコールセンター
3.フィッシングサイトの対応やサイバー犯罪対応を横断的に実施するサイバーセキュリティ統括部

みずほにおける不正送金発生時の受付・対応イメージ
① コールセンター(ダイレクトバンキングセンター)からお客さまに架電(またはお客さまからコールセンターに入電)
② お客さまにて入出金や口座の状況を確認。不審な送金がある場合、お客さまに詳細なヒアリングをダイレクトバンキングセンターにて実施。
③ ②と並行して、お客さまから警察への相談を実施。
④「不正送金であること」が確定すると、コンプライアンス部門のセキュリティサポートセンターに所管が移り、補償有無の検討と更に詳細な調査を実施。
⑤ 上記①～③と並行して、お客さまは、パスワードや暗証番号などの漏洩の可能性がある場合、他社(他行やクレジットカード会社)にも連絡を実施。

**1件の不正送金が発生するとお客さま側にも銀行側にも大きな負担・コストが発生します**



# みずほにおける不正送金対応・フィッシングサイトテイクダウン等の体制と流れについて




そのため、いうまでもなく、その不正送金の原因(の1つ)となるフィッシングサイト(フィッシングの犯行)をつぶさなければなりません

Projection Only

Projection Only

# みずほにおける不正送金対応・フィッシングサイトテイクダウン等の体制と流れについて

フィッシングサイトの対策について、大きく、検知・対応(テイクダウン)・管理に分類すると以下のようなことを実施中。

## 検知

- フィッシング対策ベンダー
- SNSの監視(Xなど)
- 脅威インテリジェンスツール
- JC3などの外部機関
- イントラ環境不審メール監視
- Post Blog
- IPアドレス/ドメイン監視
- URLScan(ブランド監視含む)
- 顧客WEB窓口(からの通報)
- マルウェアの通信の監視

## 対応

**外部**

- スクリーンショットやソースの取得
- ホスティング事業者への連絡
- ドメイン登録事業者への連絡
- Google Safe-Browsingなどブラウザ事業者への申請
- TrendmaicroやNetcraftなどセキュリティ事業者への申請
- JC3などへの連携

**内部**

- フィッシングサイトの分析
- ダミーアカウントの投入
- 不正アクセスの分析
- 関係部署連絡
- 顧客告知
- フィッシングメール/SMSの(現物)確認
- (ブラックリストの登録)
- (モニタリングルールの変更/強化)

## 管理

- フィッシングサイト件数の把握
- メール/SMSのばら撒き状況の監視
- フィッシングサイトの死活監視
  →Domain Statusの確認
  携帯端末からの閲覧可否確認

**サイバーセキュリティ統括部**

フィッシングサイト対応
不正アクセス調査

# みずほにおける不正送金対応・フィッシングサイトテイクダウン等の体制と流れについて

フィッシングサイトの対策について、大きく、検知・対応(テイクダウン)・管理に分類すると以下のようなことを実施中。

## 検知

- フィッシング対策ベンダー
- SNSの監視(Xなど)
- 脅威インテリジェンスツール
- JC3などの外部機関
- インターネット環境不審メール監視
- Post Blog
- IPアドレス/ドメイン監視
- URLScan(ブランド監視含む)
- 顧客WEB窓口(からの通報)
- マルウェアの通信の監視

## 対応

**外部**

- スクリーンショットやソースの取得
- ホスティング事業者への連絡
- ドメイン登録事業者への連絡
- Google Safe-Browsingなどブラウザ事業者への申請
- TrendmaicroやNetcraftなどセキュリティ事業者への申請
- JC3などへの連携

**内部**

- フィッシングサイトの分析
- ダミーアカウントの投入
- 不正アクセスの分析
- 関係部署連絡
- 顧客告知
- フィッシングメール/SMSの(現物)確認
- (ブラックリストの登録)
- (モニタリングルールの変更/強化)

## 管理

- フィッシングサイト件数の把握
- メール/SMSのばら撒き状況の監視
- フィッシングサイトの死活監視
  →Domain Statusの確認
  携帯端末からの閲覧可否確認

**24/365で対応が必要、やることも多く結構大変・・・**

サイバーセキュリティ統括部

フィッシングサイト対応
不正アクセス調査

# ３．みずほを狙うフィッシングについて

# みずほを狙うフィッシングサイト

フィッシングサイトを立ち上げ不正送金を行うグループは複数あると考えられている。
サイトの作りに少しずつ違いがあり、不正送金の手口等にもそれぞれ違いや特徴がある。
例：・フィッシングサイトの作りは誤字等が目立ち雑な犯行グループ
・サイトデザインに凝り研究熱心な犯行グループ
・Eメールで誘導するグループ、SMSで誘導するグループ…etc
中でもSMSを使用し多額の不正送金を今も成功させているグループ3は厄介な存在であり、対策が急務であった。

【2024年の中から例示】 *：日本サイバー犯罪対策センター

| グループ | JC3*における分類 | 狙っていたことが確認された銀行 | メインの配信インフラ | 銀行以外 |
|---|---|---|---|---|
| グループ１ | CP29 | みずほ銀行、三菱UFJ銀行、PayPay銀行、三井住友銀行 | Eメール | Apple、auID、メルカリ、ETC、くらしTEPCO |
| グループ２ | UKN 432 | みずほ銀行 | Eメール | |
| グループ３ | BP1 | みずほ銀行、三菱UFJ銀行、三井住友銀行 | SMS | auID、ドコモ、くらしTEPCO |
| グループ４ | CP20 | みずほ銀行、GMOあおぞらネット銀行、三菱UFJ銀行、楽天銀行、りそな銀行、ソニー銀行 | Eメール | Amazon、マスターカード、メルカリ、楽天カード |

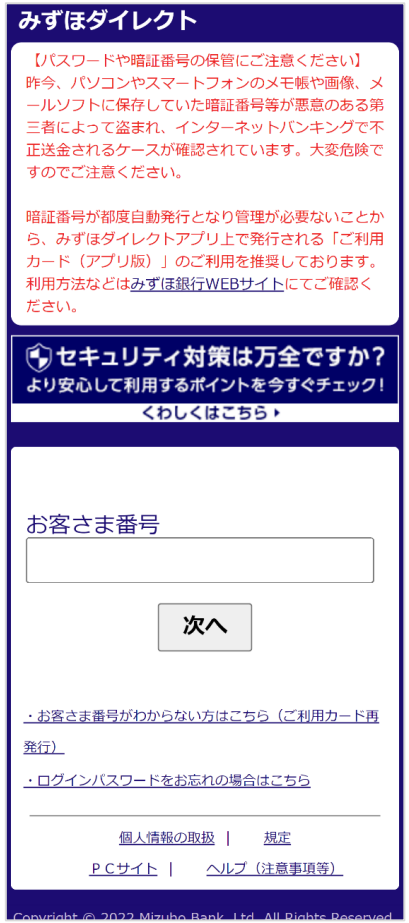
次頁以降、発生時期順に各グループ毎、サイトの詳細をご説明

# みずほを狙うフィッシングについて_グループ1_CP29(2024年 3月、6月頃)

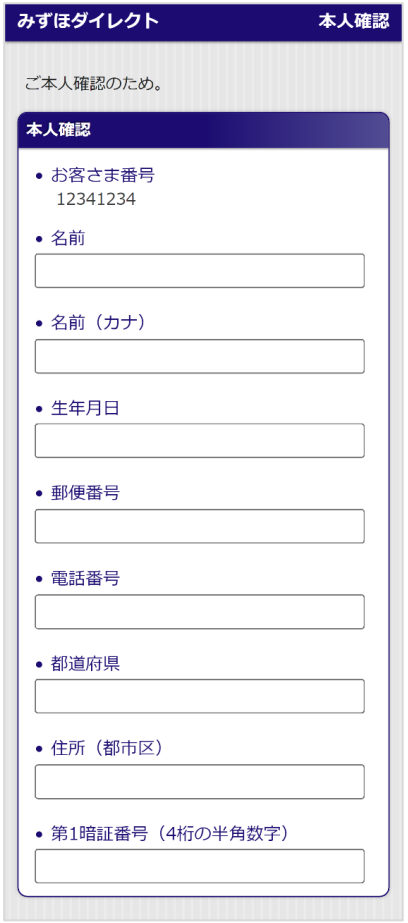
| | |
|---|---|
| 主なばら撒き方法 | Eメール（SMSも?） |
| タイプ | リアルタイム |
| (邦銀)出現頻度 | 高 |

| | |
|---|---|
| サイト特徴 | ・画面の作り込みが丁寧 |
| その他 | ・当行では2023年夏頃から大量発生のグループ。邦銀では同グループによる被害を多数確認。<br>・.infoや.net等のドメインから「.is」をメインで使用するようになった<br>・立ち上げるURLの数は少ないが破壊力高<br>・アプリを犯人側端末で乗っ取る手口多数 |

| | |
|---|---|
| URL例 | hxxps://direct.mizuho-helpdisk.is<br>hxxps://www.index-cr-mizu.cc<br>hxxps://www.index-web-ib-mizuho.is<br>hxxps://www.index-webib-mizuho.online |
| Registrar (Registry) | isnic.is.等 |







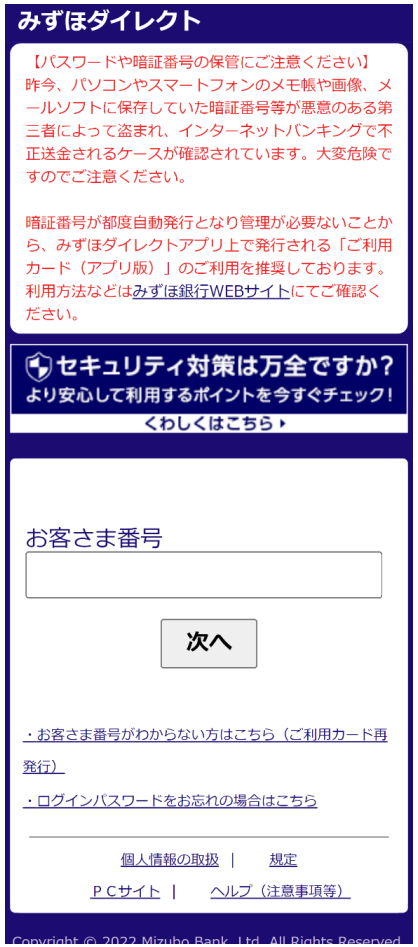


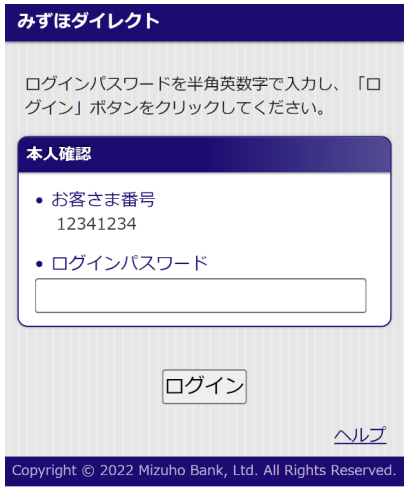
# みずほを狙うフィッシングについて_グループ2_UKN432(2024年 4月頃)

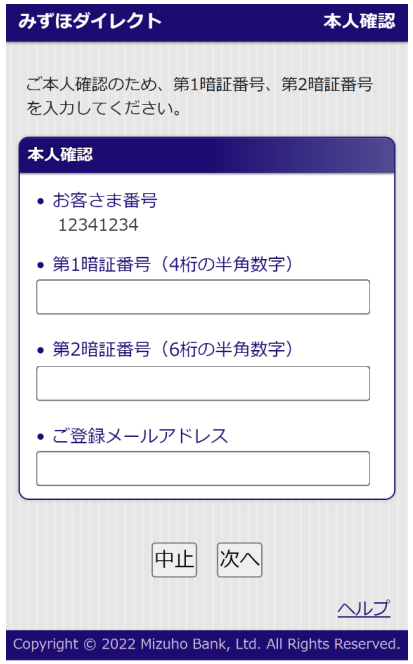
| | |
|---|---|
| 主なばら撒き方法 | Eメール |
| タイプ | リアルタイム |
| (邦銀)出現頻度 | 低 |

| | |
|---|---|
| サイト特徴 | ・インターネットバンキングの実際の応答をチェックしページが遷移するリアルタイム型 |
| その他 | ・4/11発生の新グループ。類似グループは他にあるがサイト構築のコードが異なるため犯行グループは別と想定。<br>・レジストラ:GMO、NameServer:A.SSHARE-DNS(Gname)を利用しており、<br>比較的、落としやすい。 |

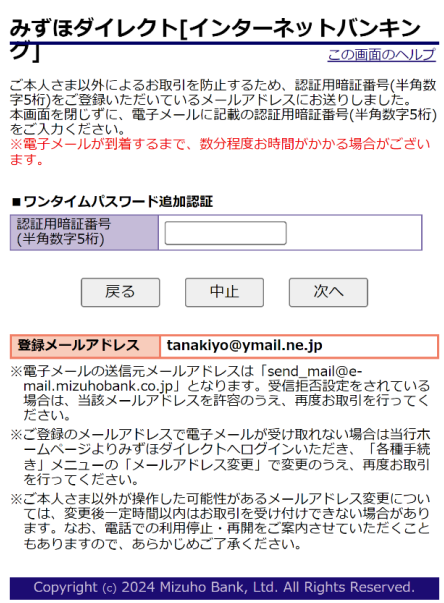
| | |
|---|---|
| URL例 | hxxps://web.ib.mazizuzsfshodbank.co.jp.findhighpower.com/<br>hxxps://web.ib.mazizuzsfshodbank.co.jp.wowpalmbay.com |
| Registrar (Registry) | GMO INTERNET,INC等 |





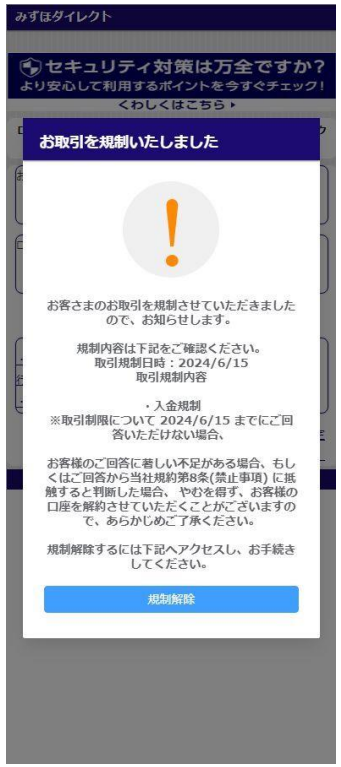


# みずほを狙うフィッシングについて_グループ3_BP1(2024年 6月頃)

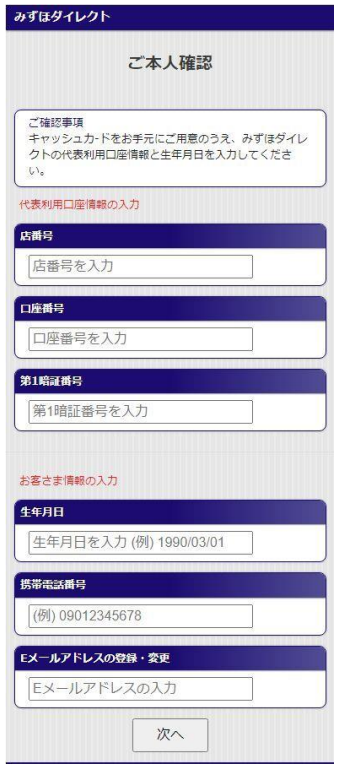
| | |
|---|---|
| 主なばら撒き方法 | SMS(MW:KeepSpy) |
| タイプ | リアルタイム |
| (邦銀)出現頻度 | 高 |

| | |
|---|---|
| サイト特徴 | ・無料でサブドメインを生成可能なduckdnsを使用(大量生成可能且つ落ちにくい)<br>・フィッシングサイトトップ画面に「！」マークを表示し、GSB等を回避する手法を取る |
| その他 | ・アプリを犯人側の端末に紐づけ乗っ取る手口が多数<br>・ダイレクトへの登録済メールアドレスを犯人のものへ変更<br>・某銀行で猛威を振るい、2023年前後、大規模な不正送金被害が発生したといわれている<br>・当行では緊急的に対処実施 |

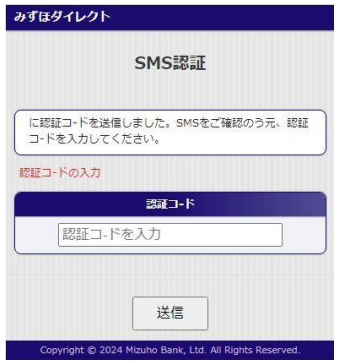
| | |
|---|---|
| URL例 | hxxps://feyusb6.duckdns.org<br>hxxps://gfpbq452s.duckdns.org |
| Registrar (Registry) | duckdns.org等 |



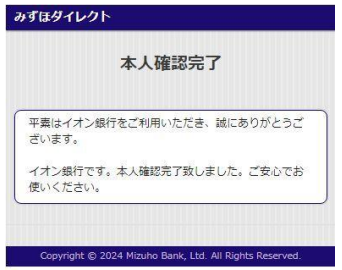












# みずほを狙うフィッシングについて_グループ3(再)_BP1(2024年 6月頃)

| | |
|---|---|
| 主なばら撒き方法 | SMS(MW:KeepSpy) |
| タイプ | リアルタイム |
| (邦銀)出現頻度 | 高 |

| | |
|---|---|
| サイト特徴 | ・無料でサブドメインを生成可能なduckdnsを使用(大量生成可能且つ落ちにくい)<br>・フィッシングサイトトップ画面に「！」マークを表示し、GSB等を回避する手法を取る |
| その他 | ・前頁続き。第2暗証番号を取る画面がなかったが、アプリ乗っ取り対策を当行が実施したためか、即時送金できるよう第2暗証番号の画面を用意してきた。 |

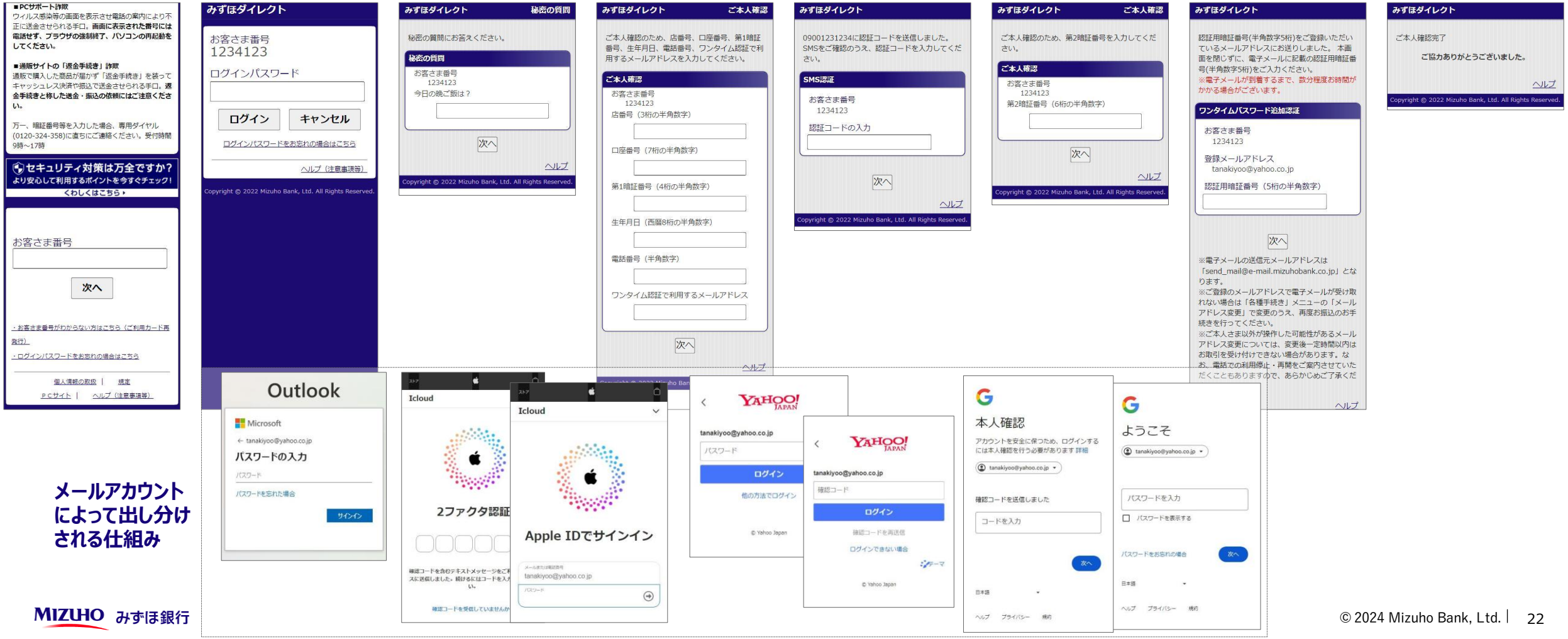
| | |
|---|---|
| URL例 | hxxps://uv2r90.duckdns.org<br>hxxps://mzgel01.duckdns.org |
| Registrar (Registry) | duckdns.org等 |

# みずほを狙うフィッシングについて_グループ4_CP20(2024年 8月頃)

| | |
|---|---|
| 主なばら撒き方法 | Eメール |
| タイプ | リアルタイム |
| (邦銀)出現頻度 | 高 |

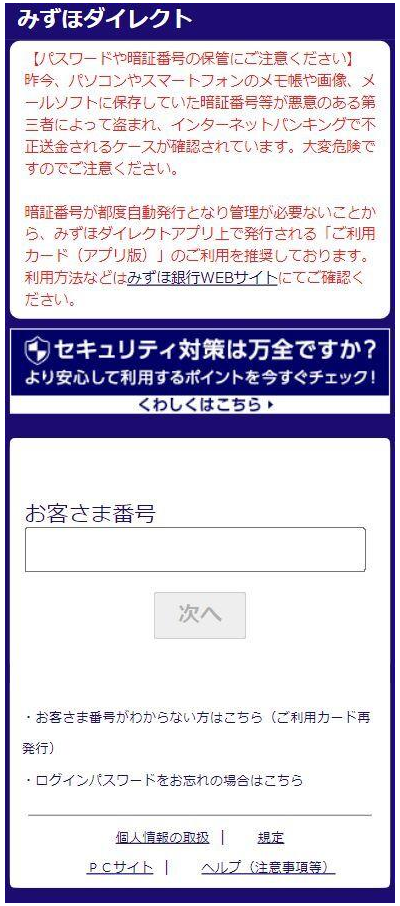
| | |
|---|---|
| サイト特徴 | ・元々窃取情報貯め込み型がメインの犯行グループだったが、2023年ごろからリアルタイム型を併用<br>・メールOTPの詐取を目的に、メールアカウントの乗っ取りを狙った新規画面を追加 |
| その他 | ・2022年9月頃～被害を及ぼしていたと考えられる<br>・ドメインは様々な文字列を使用(長いものから短いものまで) |

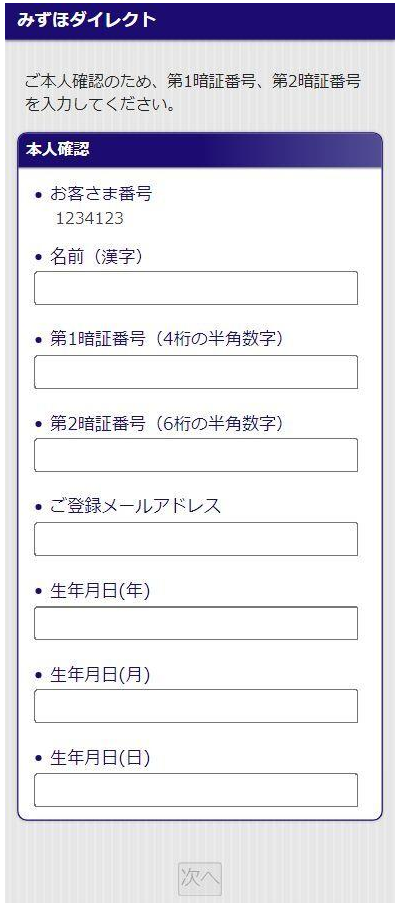
| | |
|---|---|
| URL例 | hxxps://cdshyj.com<br>hxxps://dizichina.com<br>Hxxps://qigehangmo.com |
| Registrar (Registry) | Gname.com Pte. Ltd.等 |

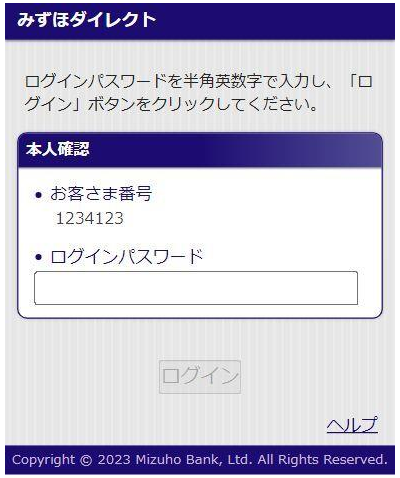


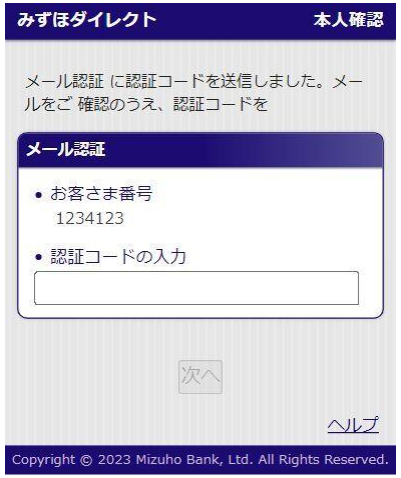

**メールアカウントによって出し分けされる仕組み**

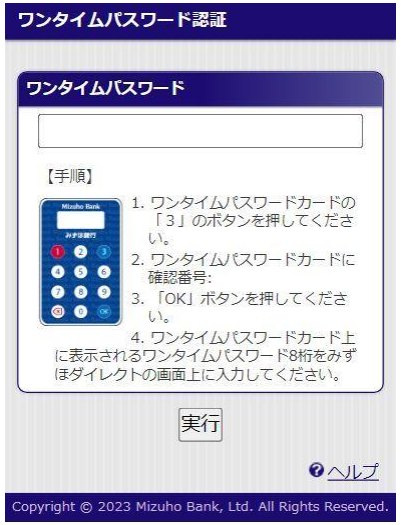
# 参考：本原稿作成中に発生したBP5_2024年12月

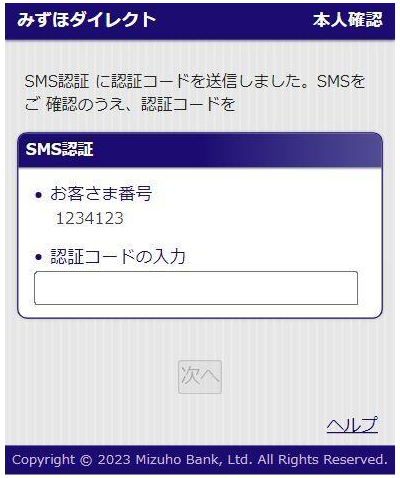


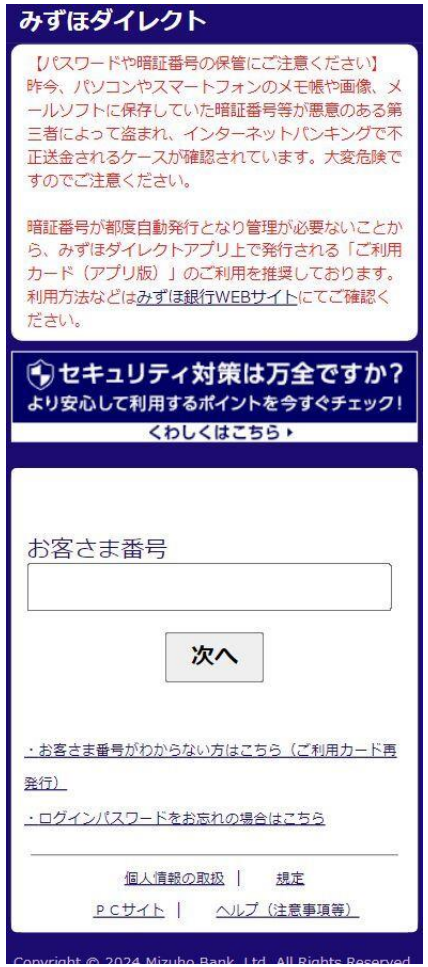



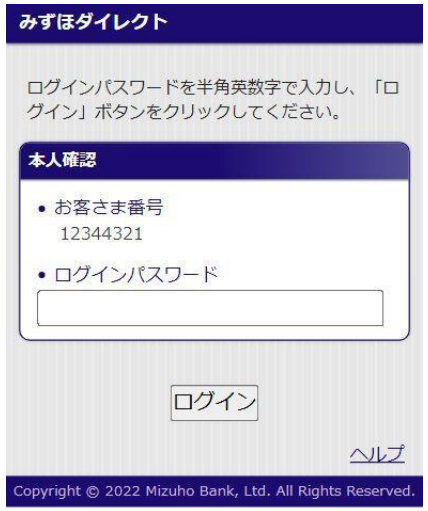



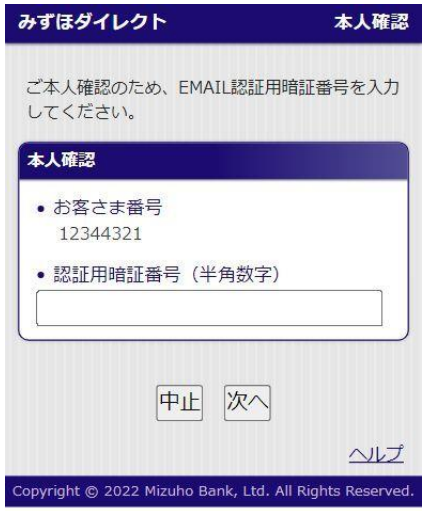



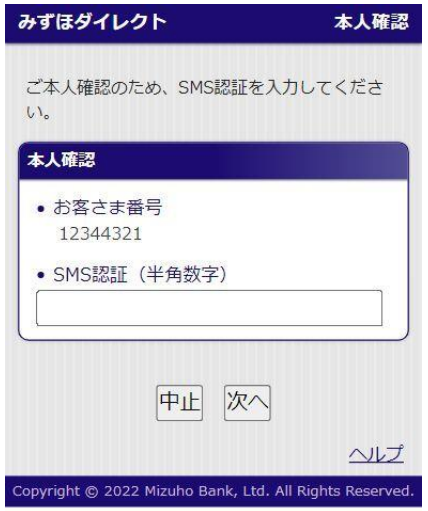



# 参考：本原稿作成中に発生したCP29_2024年12月




Projection Only

Projection Only

Projection Only

Projection Only

Projection Only

【課題】

・犯人のアクセスをモニタリングし即時停止するのも限界がある

・やらなければならない作業も多く、対応の人手にも限界がある

【対策】

・できるだけ早くフィッシングサイトを検知をする

・対応を一部自動化する

【課題】

・犯人のアクセスをモニタリングし即時停止するのも限界がある

・やらなければならない作業も多く、対応の人手にも限界がある

【対策】

・できるだけ早くフィッシングサイトを検知をする

・対応を一部自動化する

# ４．偽SMSを送信する犯行グループが使用するマルウェアについて

# 調査のMotivation

- **背景**
  - フィッシングに対する被害額は年々増加する中、特に**銀行を騙ったSMSによるフィッシング被害が非常に深刻**な状況
  - 当該手口による**フィッシングサイトの早期検知**が求められている。
  - X(旧：Twitter)上にて善意のフィッシュハンターによる投稿を頼りにフィッシングサイトの検知、テイクダウン対応をしており、**他社(他行)を頼りにする体制**には不安定さを感じていた。

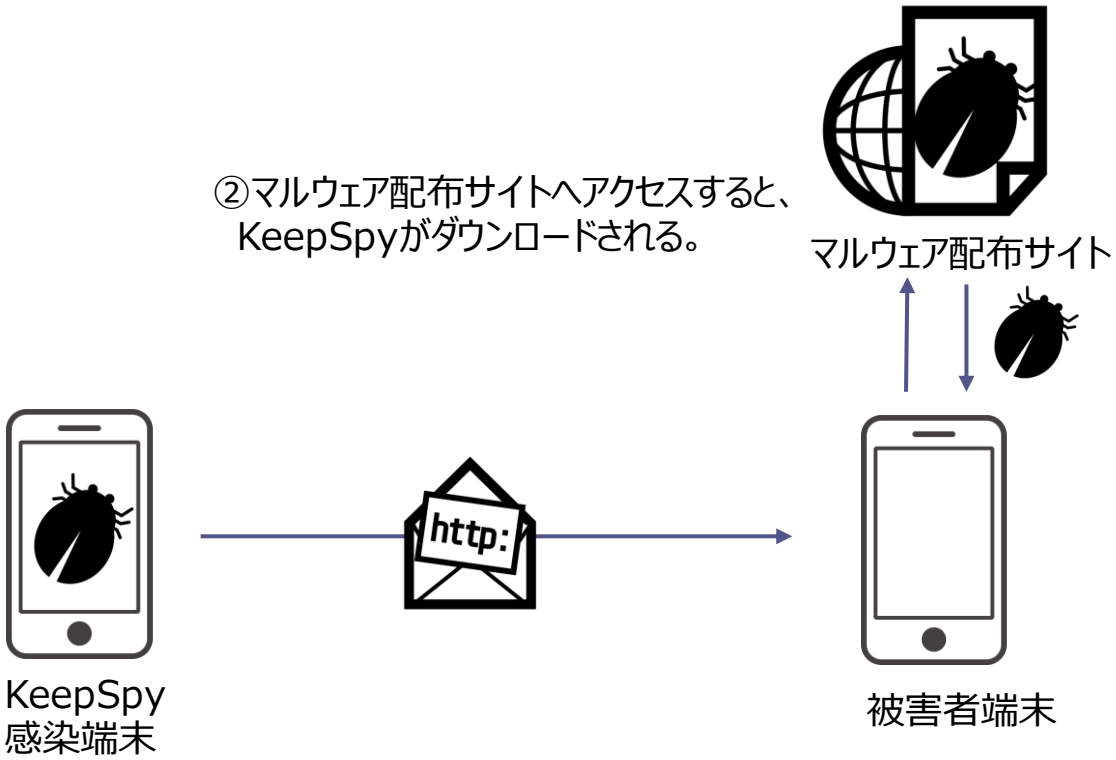
- **目的**
  - 銀行を騙るSMSのばらまきに使用される**KeepSpyの解析**、及び**フィッシングサイトを調査**し、フィッシングサイト立ち上げの早期検知を目指す。



<参考>善意のフィッシュハンターの投稿

# KeepSpyについて

- **概要**
  - 主にAndroidデバイスをターゲットにしたモバイルマルウェア。
- **感染経路**
  - 主に通信事業者を騙るSMSに記載されたリンクからマルウェア配布サイトへ誘導し、正規のセキュリティソフト等がダウンロード可能であるかのように偽装し、被害者にダウンロード及びインストールを促す事で感染させる。

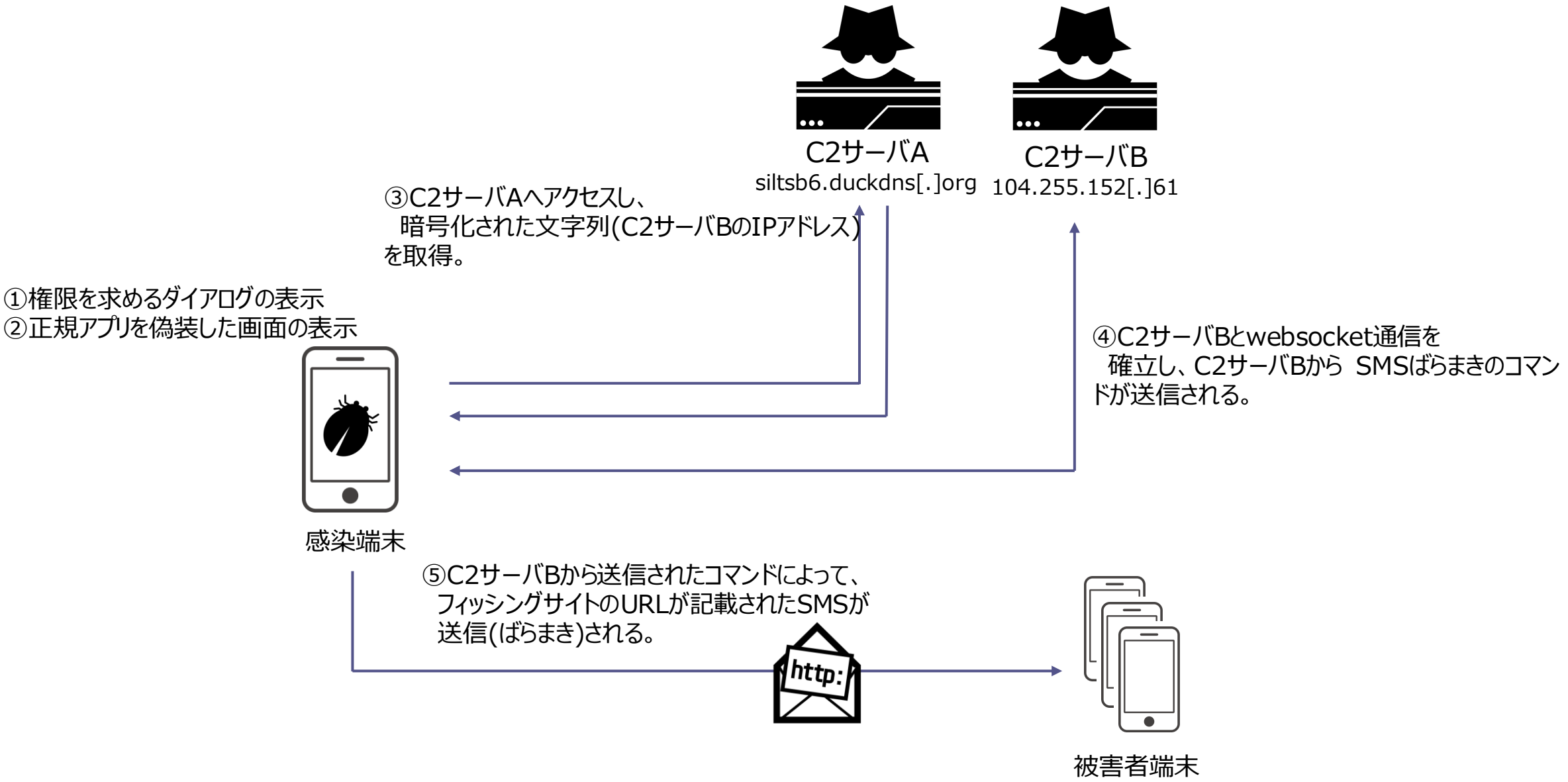



＜例＞ドコモを騙り、セキュリティソフトをインストールさせる。

## 解析に利用したKeepSpy検体

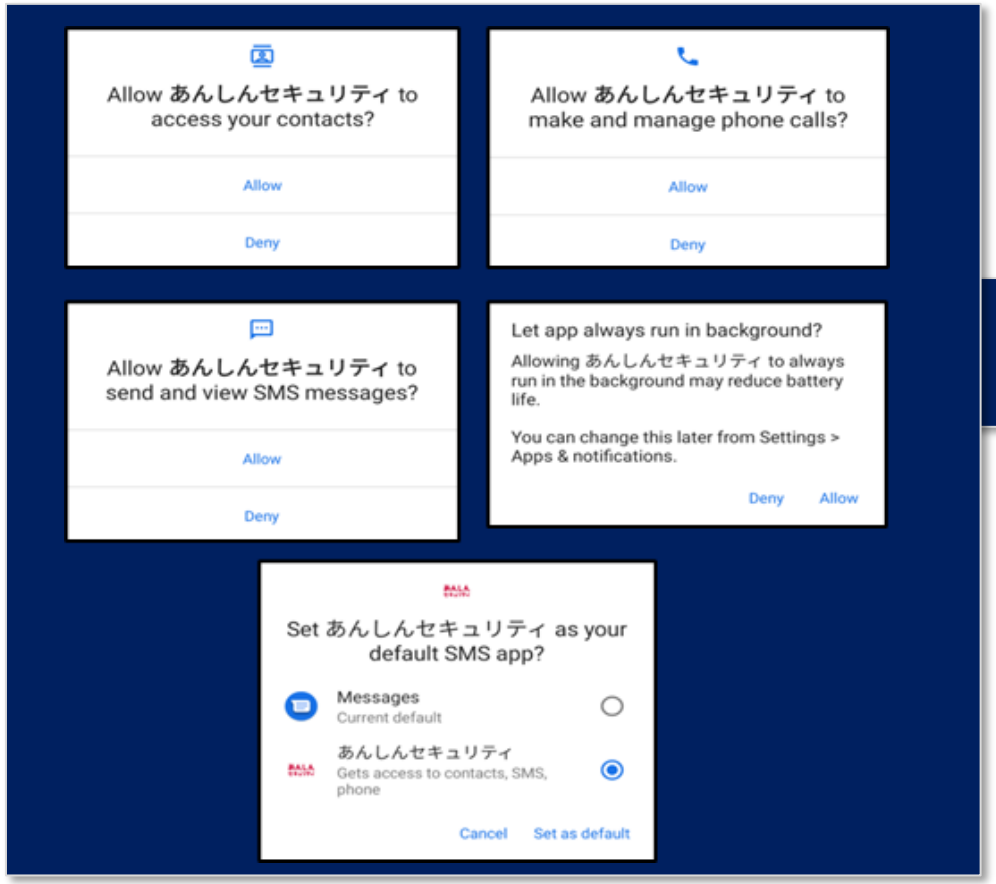
| 項目 | 値 |
| --- | --- |
| **ファイル名** | DOC2024.apk |
| **ハッシュ値(SHA256)** | 66b118b5c63a3c8e30941b2e620211d04febbb21e3c90feb1f283b0b598fb46c |
| **アイコン画像** |  |
| **First Submission (VirusTotal)** | 2024-05-09 02:23:38 UTC |

# <解析結果：全体像>KeepSpy感染からSMS送信までの仕組み



# <解析結果：詳細>KeepSpyの画面上の挙動について

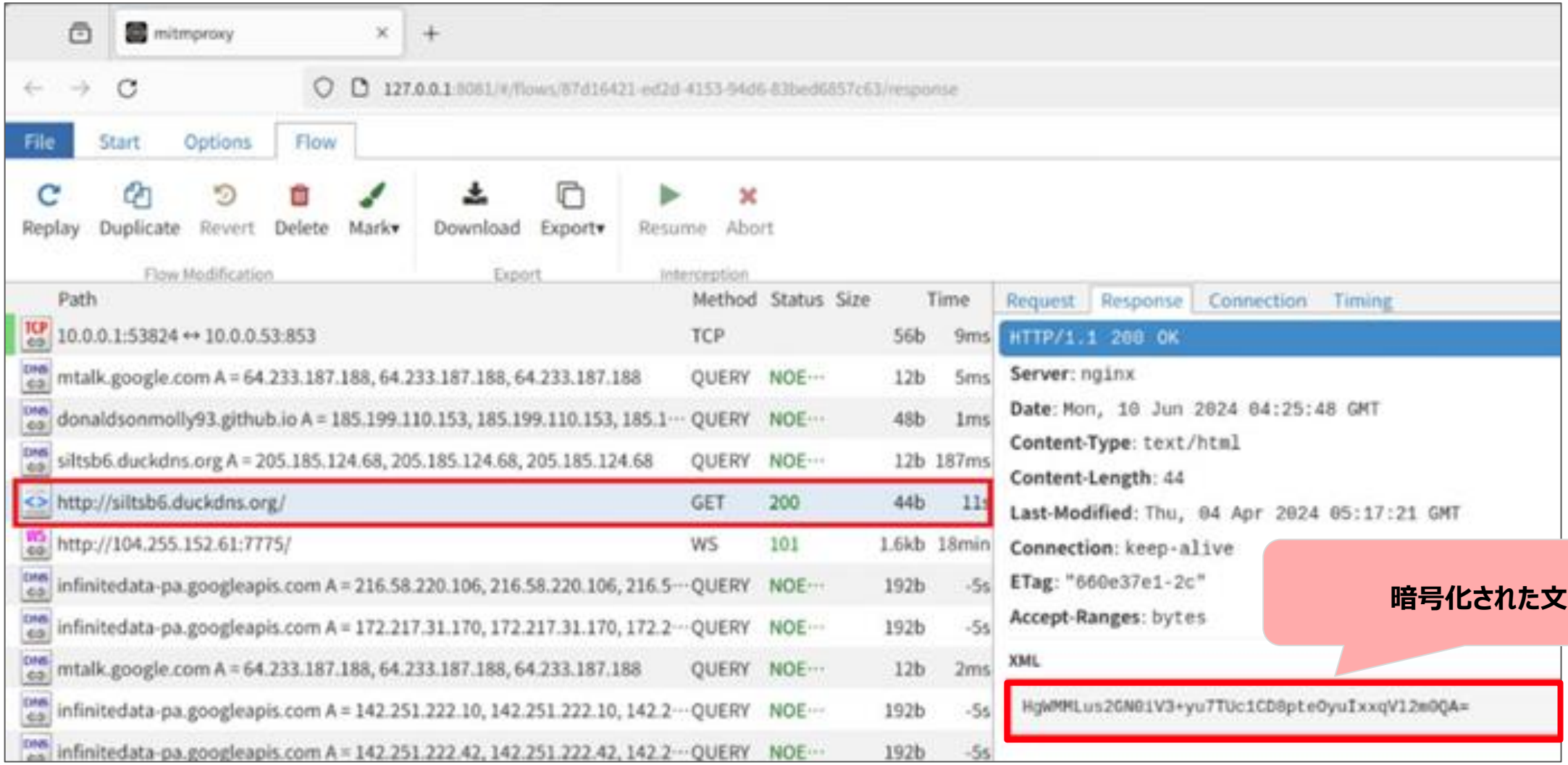
①権限を求めるダイアログの表示
・連絡先へのアクセス
・通話の管理
・SMSメッセージの送信と表示
・SMSアプリの変更
・バックグラウンドでの常時実行




②偽装元の「あんしんセキュリティ」の画面のようなものが表示される。
なお、どこをタップしても動作に変化無し。

# KeepSpyの動的解析

③C2サーバAへアクセスし、 暗号化された文字列(C2サーバBのIPアドレス) を取得。



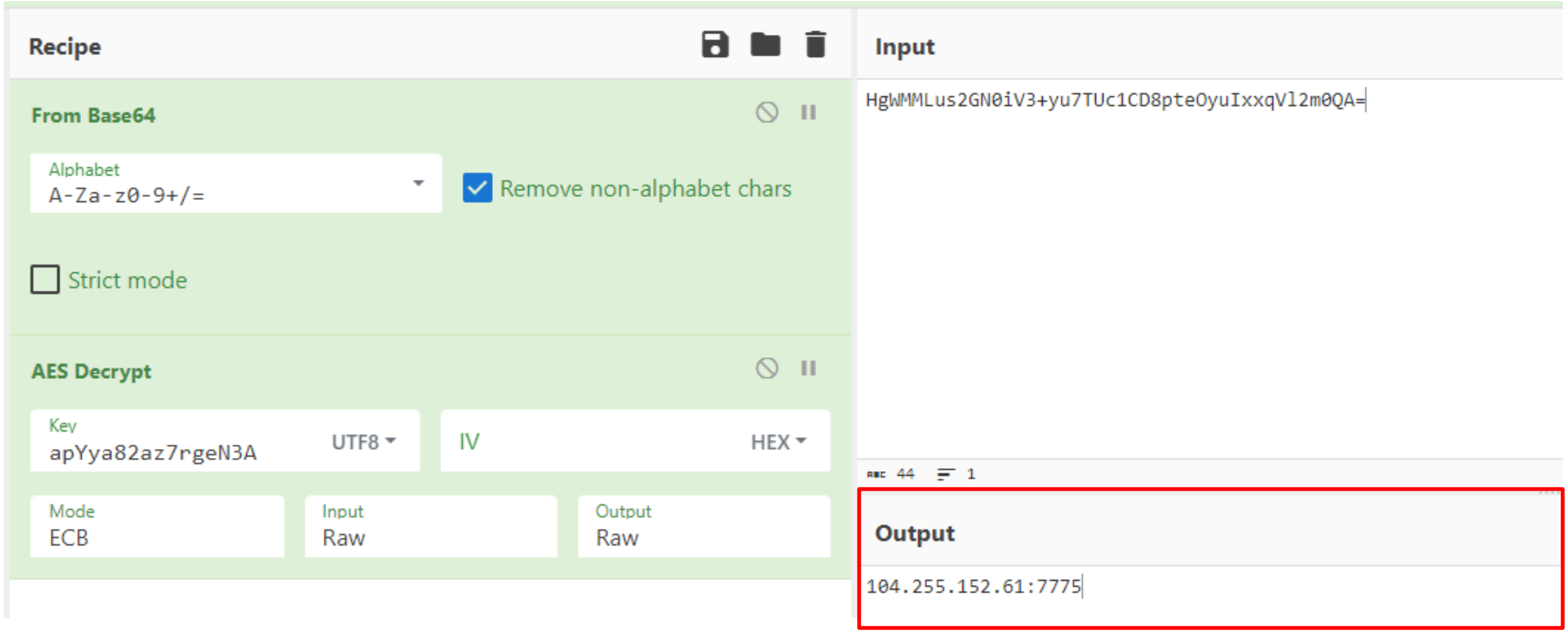
# C2サーバBのIPアドレス復号について

- Base64とAESにより、C2サーバAから受け取った文字列を復号し、C2サーバBのIPアドレスを取得
- 暗号化方式や秘密鍵は難読化されてソースコード上にハードコードされている。

```
public static String gjqbrbweff(String str) {
    try {
        byte[] decode = Base64.decode(str, 2);  ←Base64デコード
        Cipher cipher = Cipher.getInstance(f4411bkrdrfezfl);  ←"AES/ECB/PKCS5Padding"(暗号方式)
        String str2 = f4412dwygyiog;  ←"apYya82az7rgeN3A"(鍵)
        String str3 = f4416wxyvgvzr;  ←"0"(パディング用:)
        int length = str2.length();
        if (length < 16) {
            StringBuilder sb = new StringBuilder();
            sb.append(str2);
            for (int i = 0; i < 16 - length; i++) {
                sb.append(str3);
            }
            str2 = sb.toString();
        }
        Charset charset = f4413fwpstitn;
        cipher.init(2, new SecretKeySpec(str2.getBytes(charset), f4415hepjaxvtj));
        return new String(cipher.doFinal(decode), charset);  ←最終的な復号のタイミング
    } catch (Exception e) {
        e.printStackTrace();
        String str4 = f4414gjqbrbweff;
        Log.e(str4, str4 + e);
        return null;
    }
}
```

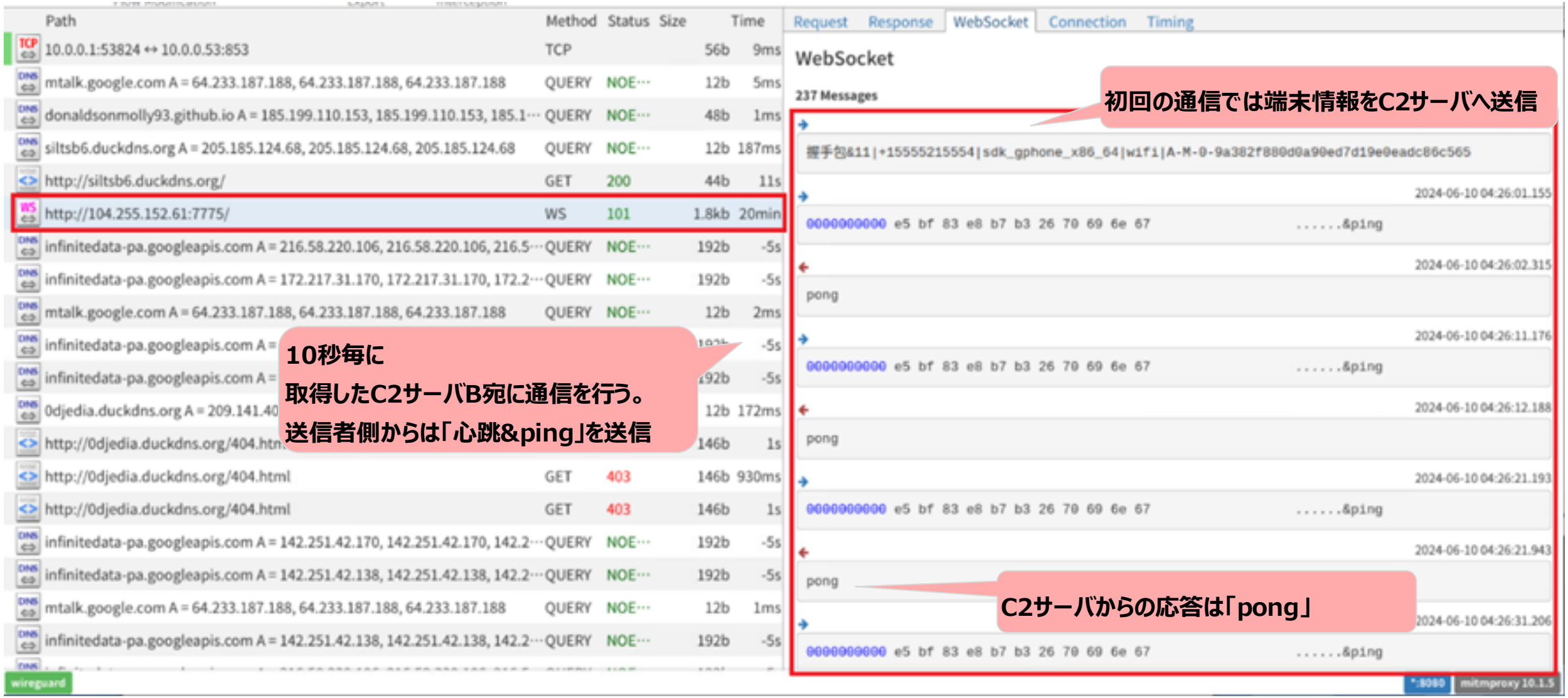
# C2サーバBのIPアドレス復号について

CyberChefによる復号結果は以下の通り



# KeepSpyの動的解析

④C2サーバB(http[:]//104.255.152[.]61:7775/)とwebsocket通信を確立し、C2サーバBからコマンドを受信



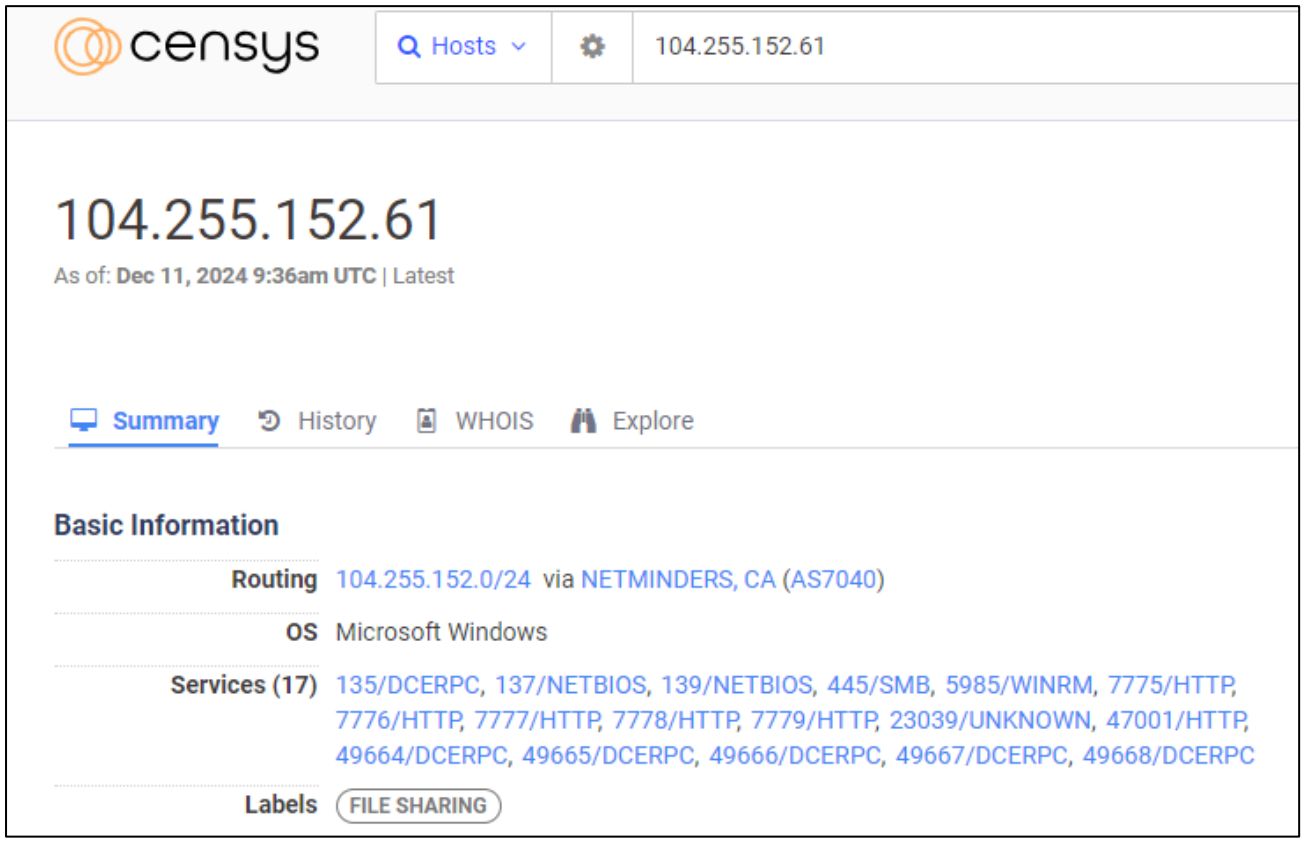
## KeepSpyの機能

C2サーバBから受信する可能性のあるコマンドは以下の通り。
(動作検証は行っていないため、具体的な動作は未確認)

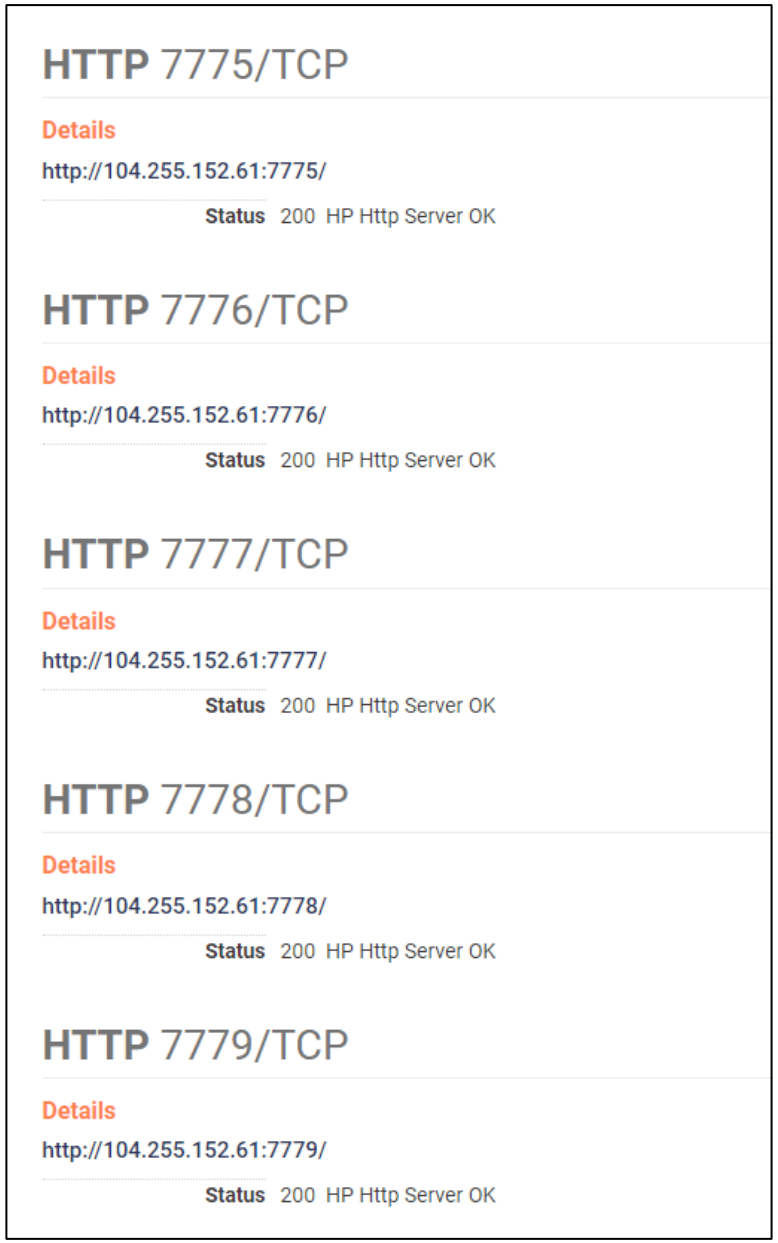
| コマンド名 | 日本語訳 |
|---|---|
| 通讯录 | 電話帳 |
| 收件箱 | 受信箱 |
| 拦截短信&open | テキストメッセージ傍受 |
| 拦截短信&close | テキストメッセージ傍受 |
| 发信息& | メッセージ送信 |
| 清除短信& | SMSを削除 |
| 普通通知栏& | 通常の通知バー |
| 通知栏& | 通知バー |
| 应用列表& | アプリケーションリスト |
| 更新& | 更新 |

# KeepSpyのC2サーバBについて

Censys※で確認した結果は以下の通り。
7775の他,7776,7777,7778,7779が空いており、7775~7779ポートの応答は
すべて”HP Http Server OK”と同様
→**<u>7776~7779ポートからも同様のコマンドが返信される</u>**ものと思われる。



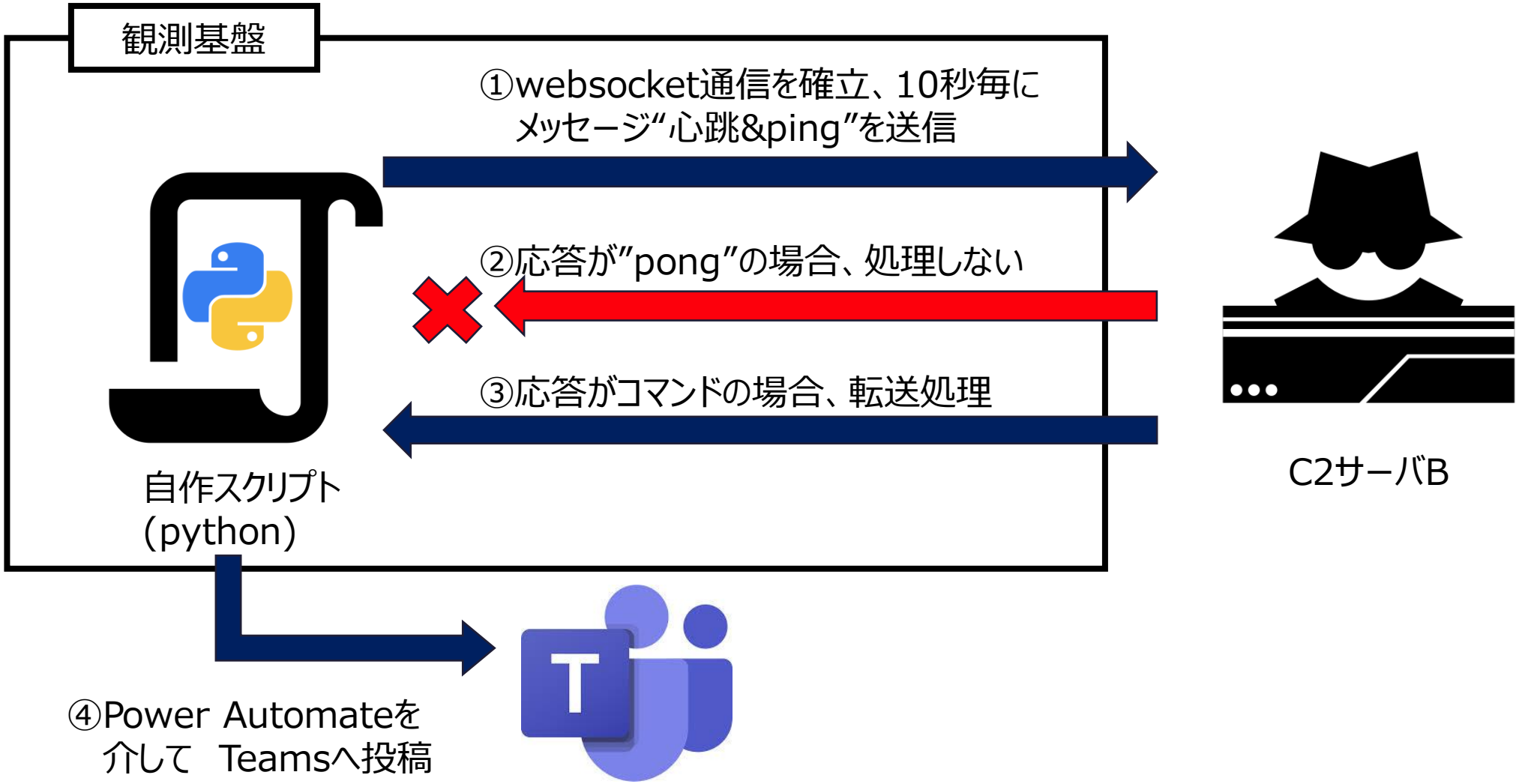

※https://search.censys.io/hosts/104.255.152.61



# 偽SMS観測基盤の構築

C2サーバBへの通信の内容が判明したので、C2サーバBからSMSばらまきコマンドを取得する方法を検討

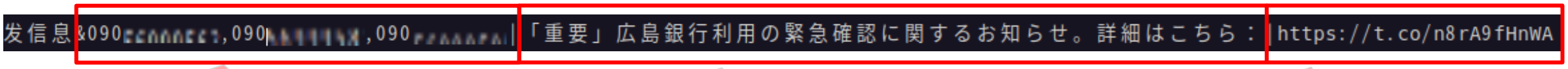
C2サーバBからSMSばらまきコマンドを受信した場合にTeamsへ通知する観測基盤を構築



## 観測実施の結果

C2サーバBからSMSばらまきコマンドを受信することに成功！
1日に1~2回程度、7775~7779の5ポートからSMSばらまきコマンドを受信

11/27(水)に送信されたSMSばらまきコマンドの例：




**送信先電話番号**　**メッセージ**　**フィッシングサイトのURL**

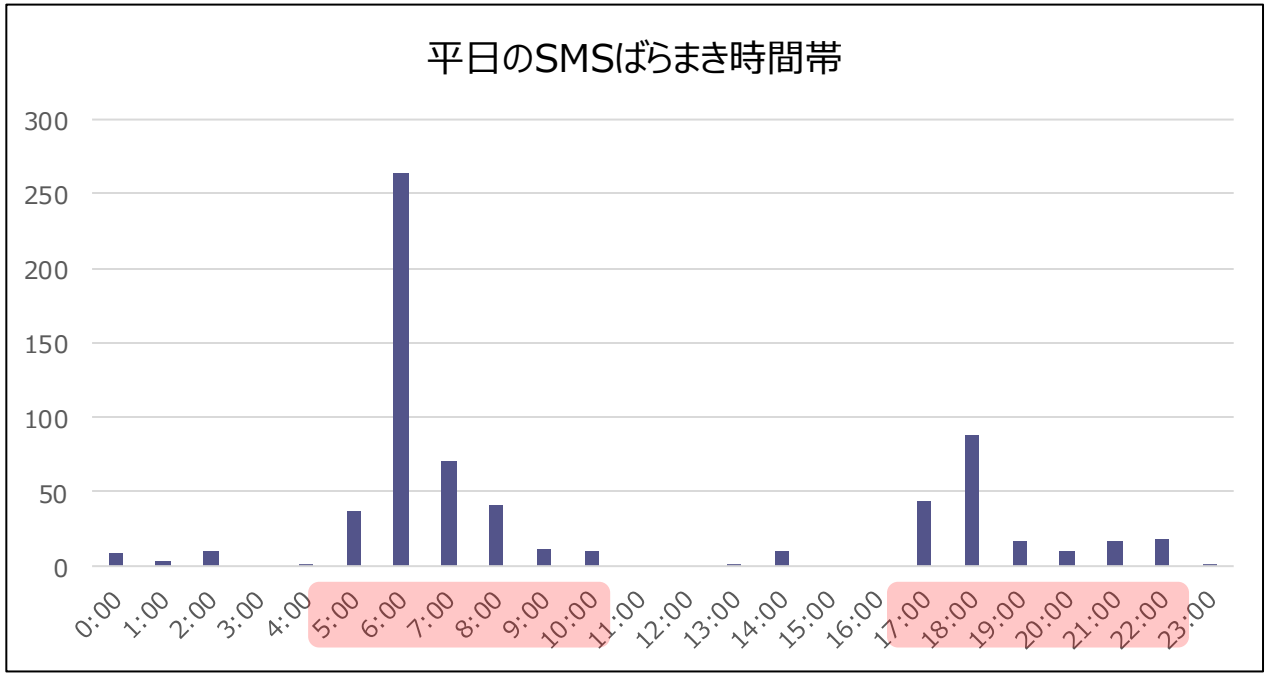
Teams投稿(C2サーバのポート番号とリダイレクト先も付与)：

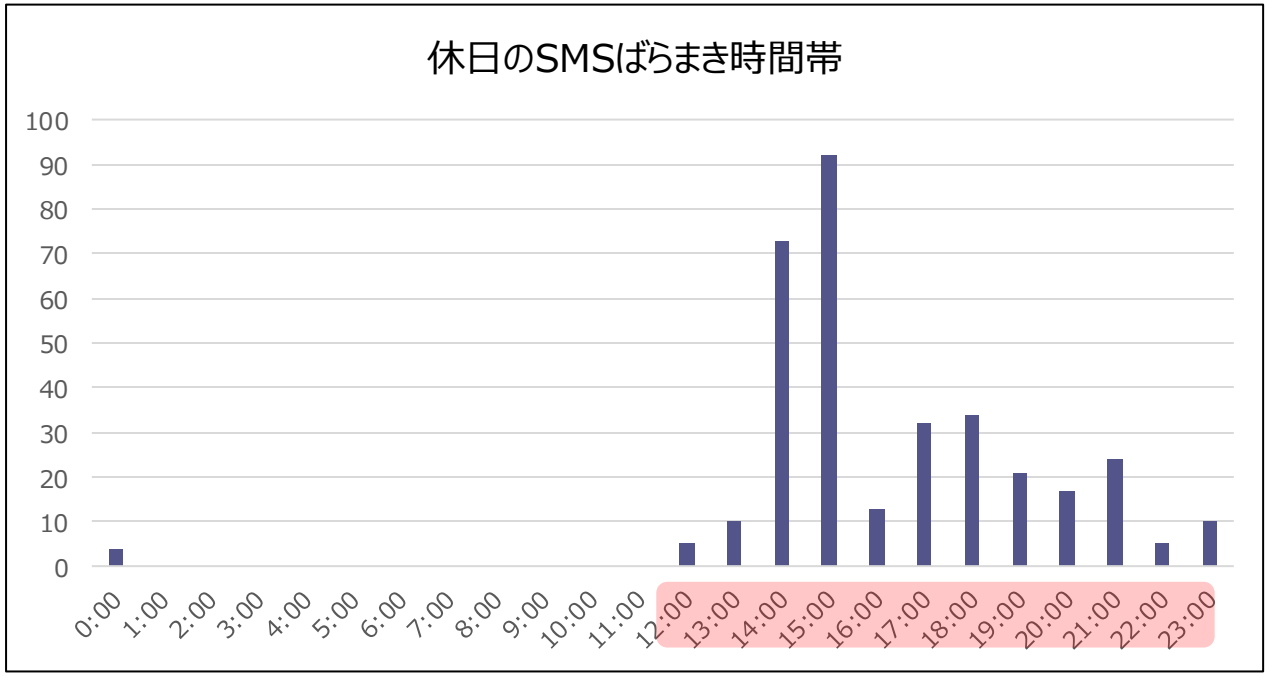

**結果**

みずほ銀行がターゲットとなった場合に速やかにフィッシングサイトのテイクダウン対応が可能。ターゲットとなった他行へ通知も可能。

# SMSばらまきコマンドの特徴(配布時間帯ついて)

- **観測期間**：2024/06/19 ~ 2024/12/11
- **観測ポート**：7775~7779の5つのポート
- **結果**
  - 平日：**6:00~7:00 or 17:00~18:00**が多い。
  - 休日：**14:00、15:00**が多く、午後の配信がほとんど。
- **考察**
  - SMSを閲覧することが可能な時間帯を狙っている可能性がある
  - 平日：1日の仕事開始、終了の時間
  - 休日：午前に用事を済ませ、午後に休憩しているタイミング？



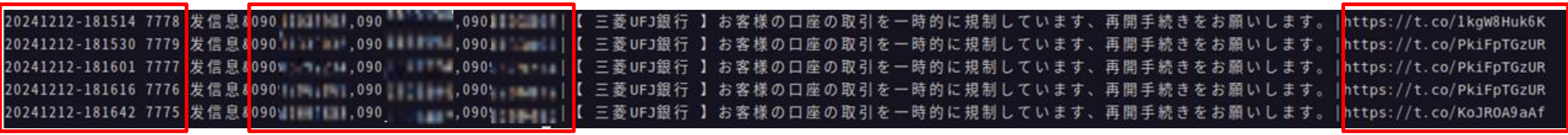
## SMSばらまきコマンドの特徴(ポート毎)

- 各ポート毎にSMSばらまきコマンドの差異があるか調査
  - 回数：各ポートから**一日1~2回程度**
  - 時間帯：同一の時間帯に**各ポートから一斉に送信**される。
  - 電話番号：同一の時間帯に同じ番号はなく、**すべて異なる電話番号**
  - URL：短縮URLは複数存在。短縮URLからの遷移先URLは概ね同一(時間経過によって遷移先URLが変わる場合もある)

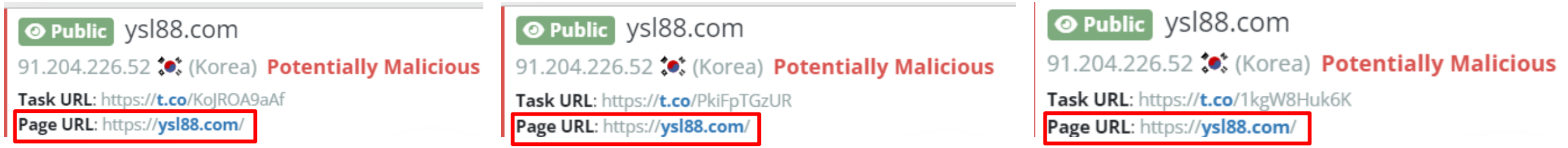
**同じ時間帯に各ポートからコマンドが送信される**

**SMSの送信先はすべて異なる**

**短縮URLは複数存在する。**




例:12/12(木)：送信されたSMSばらまきコマンド




例: 12/12(木)：短縮URLからの遷移先

# ５．フィッシングサイトの早期検知の試みについて

## 本調査の前提について

- **対象フィッシングサイト**：BP1(SMSばらまきを行うアクター)のフィッシングサイト
- **調査対象期間**：2024/4 ~ 2024/10
- **調査データ**：JC3が保有するフィッシングサイトに関するデータ、インターネット上の公開データ等
- **調査内容**
  - ターゲットのブランド名(会社名)
  - フィッシングサイトのサーバ証明書

## BP1が騙るブランド名(会社名)の統計

- 集計方法：BP1のフィッシングサイトのFQDN数を集計
- ターゲットとなった会社をランキング形式で表記(分類できないものを除く)
  - 被害額が大きいとされる**三菱UFJ銀行が上位**。
  - **地方銀行も狙われる**。
  - 2024年4月～8月までは**5,000以上**のFQDNがあるが、**9月以降は減少**

| 順位 | 4月(FQDN数) | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 |
|---|---|---|---|---|---|---|---|
| 1位 | 三菱UFJ銀行(4862) | 三菱UFJ銀行(4198) | 三菱UFJ銀行(4442) | 三菱UFJ銀行(5331) | 三菱UFJ銀行(1678) | 三菱UFJ銀行(613) | りそな銀行(688) |
| 2位 | docomo(1226) | docomo(2663) | みずほ銀行(1884) | TEPCO(53) | 北海道銀行(1074) | 静岡銀行(16) | 三菱UFJ銀行(610) |
| 3位 | KDDI(617) | TEPCO(33) | docomo(1076) | 東京ガス(5) | りそな銀行(971) | りそな銀行(8) | 北國銀行(135) |
| 4位 | TEPCO(12) | | りそな銀行(263) | りそな銀行(2) | 岩手銀行(507) | TEPCO(8) | 南都銀行(7) |
| 5位 | | | 三井住友銀行(58) | 福岡銀行(1) | 関西みらい銀行(417) | 南都銀行(2) | TEPCO(4) |
| 6位 | | | 三井住友 カード(28) | 七十七銀行(1) | 三井住友銀行(233) | | 名古屋銀行(2) |
| 7位 | | | TEPCO(5) | | イオン銀行(189) | | |
| 8位 | | | | | ライフカード(106) | | |
| 9位 | | | | | TEPCO(33) | | |
| 10位 | | | | | JCB(2) | | |
| 合計 | **6717** | **6894** | **7756** | **5393** | **5210** | **647** | **1446** |

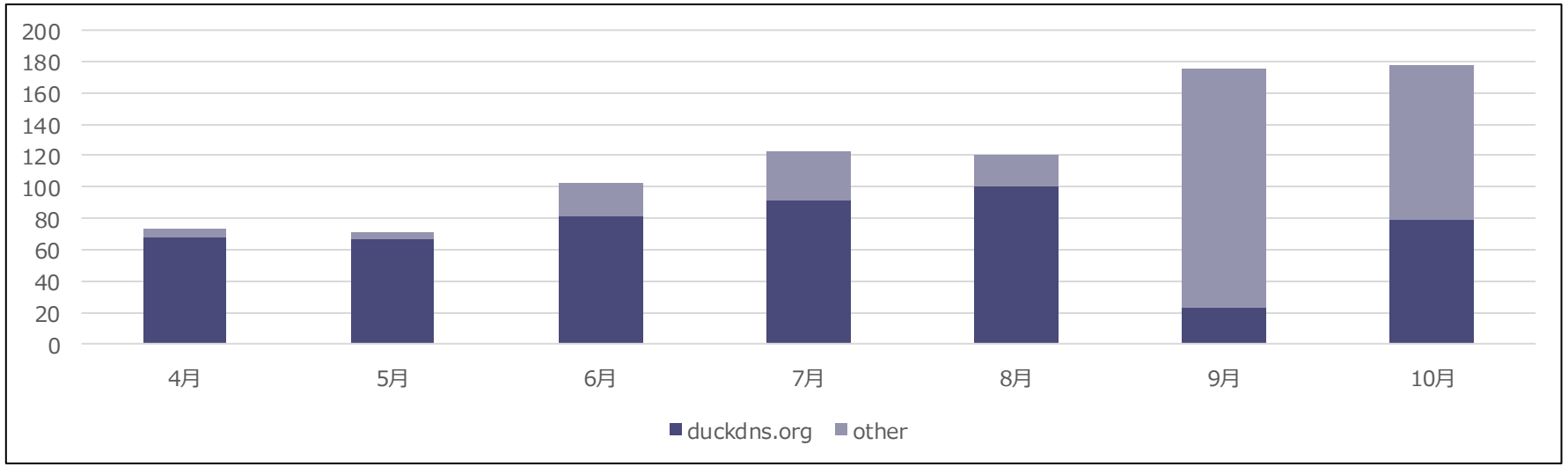
# BP1が発行するサーバ証明書について

- BP1によるサーバ証明書の発行数ついては以下の通り

| | 4月 | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 |
|---|---|---|---|---|---|---|---|
| 発行数 | 73 | 71 | 102 | 123 | 121 | 176 | 178 |

  - サーバ証明書の発行数は**上昇傾向**
  - フィッシングサイトのFQDN数と比較し、**サーバ証明書の発行数は少ない**

- サーバ証明書の発行数がFQDN数より少ない原因についての調査結果
  - 4月~8月：CNが[subdomain].duckdns.orgの証明書を持つフィッシングサイトの**割合が高い**。
  - 9月~10月：CNが[subdomain].duckdns.orgの証明書を持つフィッシングサイトの**割合が低い**。




BP1が発行するサーバ証明書の発行数(duckdnsとそれ以外)

## BP1が発行するサーバ証明書について

- サーバ証明書の発行数がFQDN数より少ない原因についての調査結果
  - CNが[subdomain].duckdns.orgのサーバ証明書について、**SAN（Subject Alternative Name）に複数のフィッシングサイトのドメインが登録されている**ことが多い。

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:60:05:14:83:68:d6:3a:08:35:87:47:4a:5a:1c:9b:ea:b4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 295815)
            commonName                = R11
            organizationName          = Let's Encrypt
            countryName               = US
        Validity (Expired)
            Not Before: Jul 31 20:24:50 2024 GMT
            Not After : Oct 29 20:24:49 2024 GMT
        Subject:
            commonName                = 307ebru4p.duckdns.org
```

```
X509v3 Subject Alternative Name:
    DNS:00qfezzs.duckdns.org
    DNS:0iry10.duckdns.org
    DNS:0lkx9b.duckdns.org
    DNS:0ouqf4q.duckdns.org
    DNS:13tfxab.duckdns.org
    DNS:1c65z0.duckdns.org
    DNS:1cs6r0ow.duckdns.org
    DNS:1k4t8ew.duckdns.org
    DNS:2c6fwj7x3.duckdns.org
    DNS:2ez5zpq.duckdns.org
    DNS:307ebru4p.duckdns.org
    DNS:36o2rsez8.duckdns.org
    DNS:378vnxbx.duckdns.org
```

**SANに複数のFQDNがある。**
**この例では100個存在する。**

例：2024-07-31に発行された証明書

**結果まとめ**

DuckDNSが多用されるため、4月~8月の期間では、サーバ証明書の数に対してフィッシングサイトのFQDN数が多い傾向にある。

## CTログによる早期検知

- **考察**
  - DuckDNSを多用する理由は、**安価に大量のフィッシングサイトを構築し、防御側の対応コストをあげるため**と考えらえる。
  - サーバ証明書の発行の手間を軽減するため、**サーバ証明書のSANに複数のFQDNを登録し、1つのサーバ証明書を流用している**と考えられる。
  - サーバ証明書のSANを確認することにより、**サーバ証明書発行日のフィッシングサイトのFQDNを芋づる式に取得することが可能**

- **検証事項**
  - **CTログ**を利用し、BP1のフィッシングサイトに使用されるサーバ証明書の発行を検知できるか検証した。
  - 検索条件は以下の通り
    - SANのFQDN数が20以上
    - Issuer OrganizationNameがLet’s Encrypt
    - CNが*.duckdns.org

- **結果**
  - **4月～8月**では、duckdns.orgのドメインが多く、概ね**サーバ証明書が発行されたタイミングでフィッシングサイトの検知が可能**
  - **9月～10月**ではduckdns.orgのドメインが少なくなり、**フィッシングサイトの検知が困難**(BP1が対策を講じた可能性)

## 4章_Summary

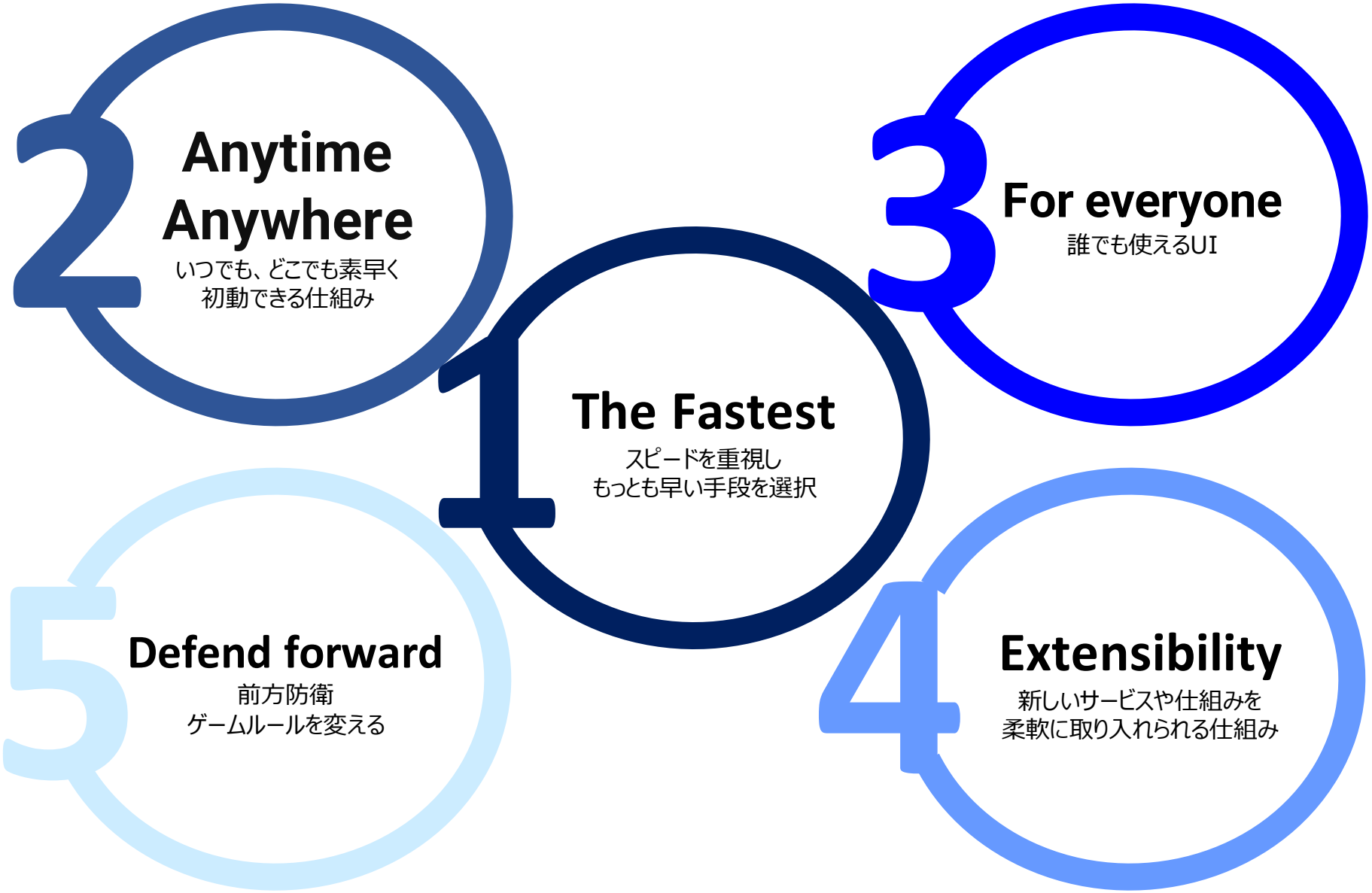
- KeepSpyの解析により、通信の内容を調査
- 観測基盤の構築によってSMSばらまきコマンドが観測でき、フィッシングサイトの早期検知、テイクダウン対応が可能に。
- SMSばらまきの情報(ターゲットの銀行とフィッシングサイトのURL)を他行へ共有することで、共助を実施。

## 5章_Summary

- 月毎のフィッシングサイトの数を集計
- 月毎のサーバ証明書の発行数を集計
- 2024年4月~8月の期間ではDuckDNSが多用されており、発行されるサーバ証明書のSANに複数のFQDNが登録されている。
- この特徴を用いてCTログからフィッシングサイトの早期検知が可能な状態であった。
- 2024年9月~10月の期間ではduckdns.orgのドメインが減少。

# ６．みずほの自動化の取り組みと今後の方向性について

# 私たちの取り組みのコンセプト



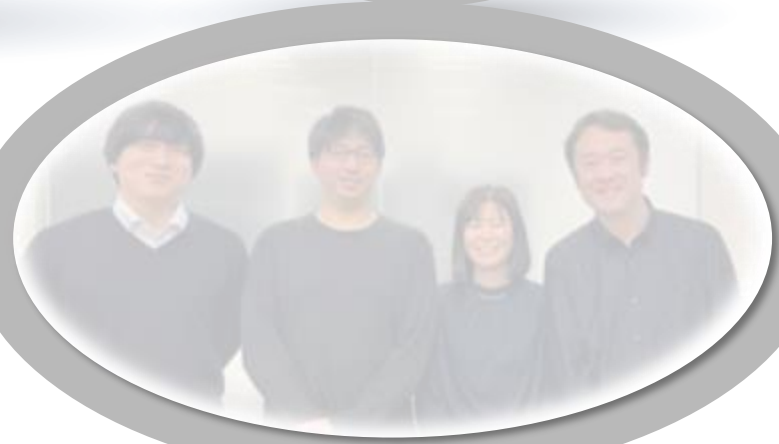
# The Fastest－ユーザ企業におけるLTMの業務活用

01 不正送金班

02 Tech班(マルウェア解析)

03 開発実装担当

04 自動化推進担当



# The Fastest－ユーザ企業におけるLTMの業務活用

# ユーザ企業におけるLTMの業務活用 - 注意喚起は最速で

サイバーセキュリティ統括部

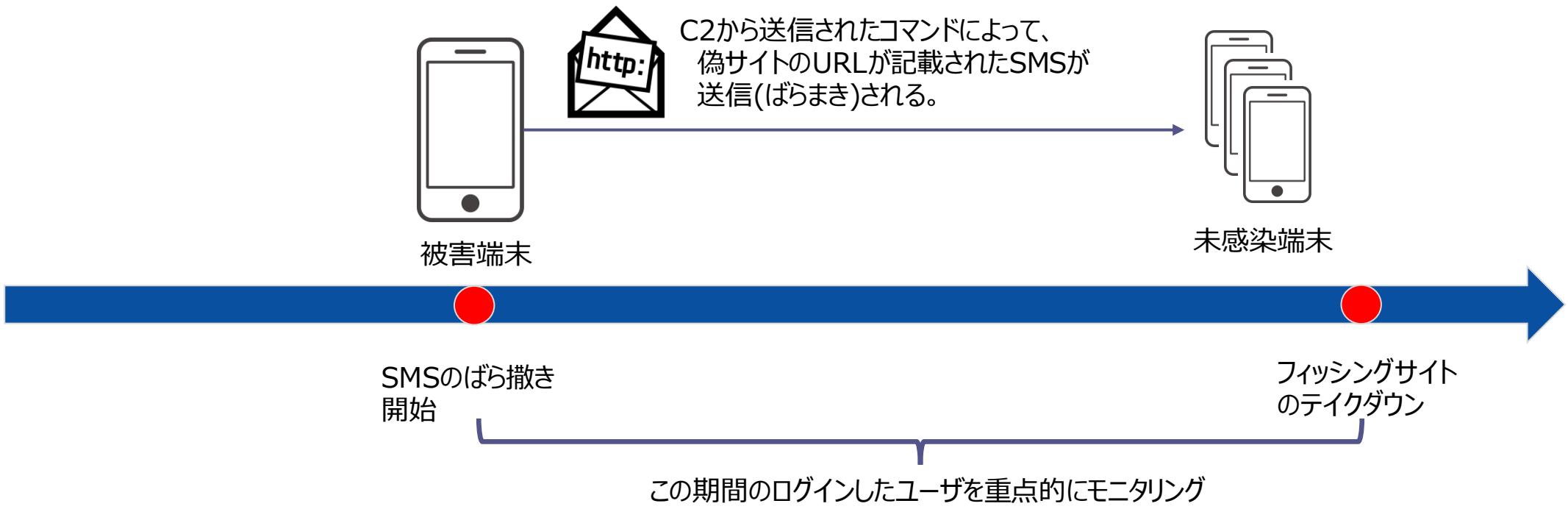
ダイレクトバンキングセンター
不審SMSの受信による顧客からの大量問合わせの構えの準備・顧客ヒアリング

インターネットバンキング所管部
インターネットバンキングでのモニタリングルールの強化の準備

コンプライアンス部門
ホームページでの顧客向けの注意喚起のコンテンツアップロードの準備

サイバーセキュリティ統括部
フィッシングサイトのテイクダウン作業。フィッシングサイトの分析。ダミーアカウントの投入

# ユーザ企業におけるLTMの業務活用




影響のあるユーザを分単位の誤差でトリアージし、モニタリングの強化を行うことが可能

# Anytime Anywhere - フィッシングは突然に

- フィッシング対応の課題としては、24/365でフィッシングサイトに備える必要あり
- 休日や夜間など担当者のリソースが少ないタイミングを狙われる初動に遅れが発生

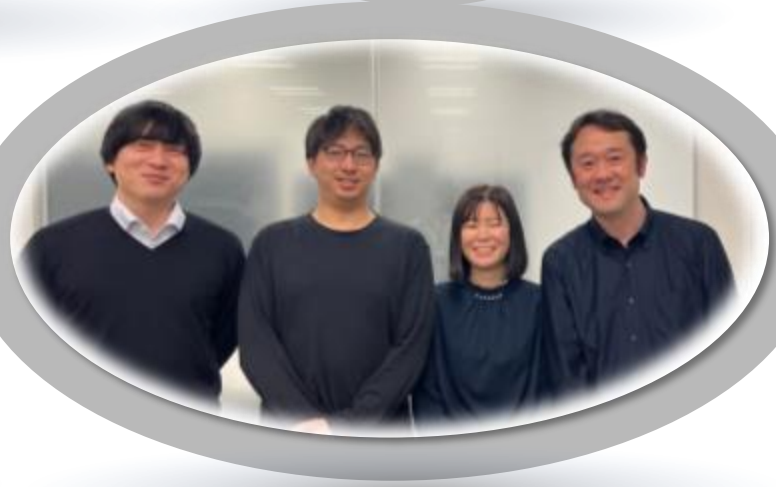
# Anytime Anywhere - 自動化だって楽じゃない

01 不正送金班

02 Tech班(マルウェア解析)

03 開発実装担当

04 自動化推進担当



# 当日投影のみ

# Anytime Anywhere – 何度でも

大迫 結花

今の無料版のurlscan.ioはどのタイミングで利用されていますか？
APIを利用できるPro版に変更されると聞きましたが…

森 三千代

もう少し先で利用開始できるよう予算確保に動いています！

竹内 司

urlscan.ioはテイクダウンの依頼を出した後に使っています
urlscan.ioでMalicious判定されるとGSBの効果が早くでる気がするから

土井 優大

urlscan.ioのAPIでフィッシングサイトの画像が取れるかもしれないんですよ。検証しないとわからないですけど。
もし取れるようになるなら、手動でテイクダウンする前にサイトの画像を取れたら便利じゃないですか？

竹内 司

おーそうなんだー。
そうすると、自動化に向けてもう一回業務フローを見直しましょう

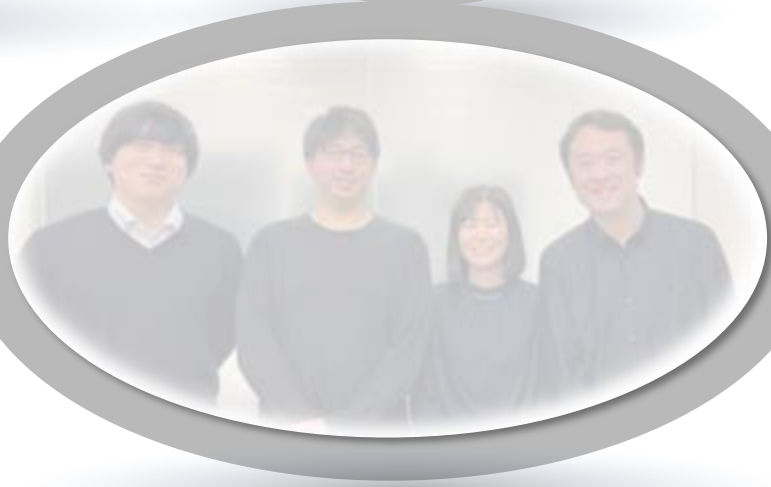
# Anytime Anywhere – 詳細フロー検討へ

01 不正送金班

02 Tech班(マルウェア解析)

03 開発実装担当

04 自動化推進担当



# Anytime Anywhere – 詳細フロー検討へ

西川 昌広

自動化するために最初のインプットとなる条件を整理したいです
検知サービスからのメールだけで良いでしょうか？

竹内 司

二つのサービスを利用していて、共にメールを受信しています。また手動で検知したURLを投入するパターンがあります。フィッシングのパターンとしても商品サービス毎に分類と、詐欺やロゴの不正使用もあるなど条件が複雑です…

西川 昌広

森 三千代

経営向けの報告にも投資詐欺のサイトの件数は入れていないからカウントは別にしたいなぁ

竹内 司

１か月以内に投稿したサイトのURLならば重複として処理しないとか、各サービスはグループ会社までは対応しないなど、条件が複雑すぎるので、いったん今の話を全て書き出してもらえますか？

西川 昌広

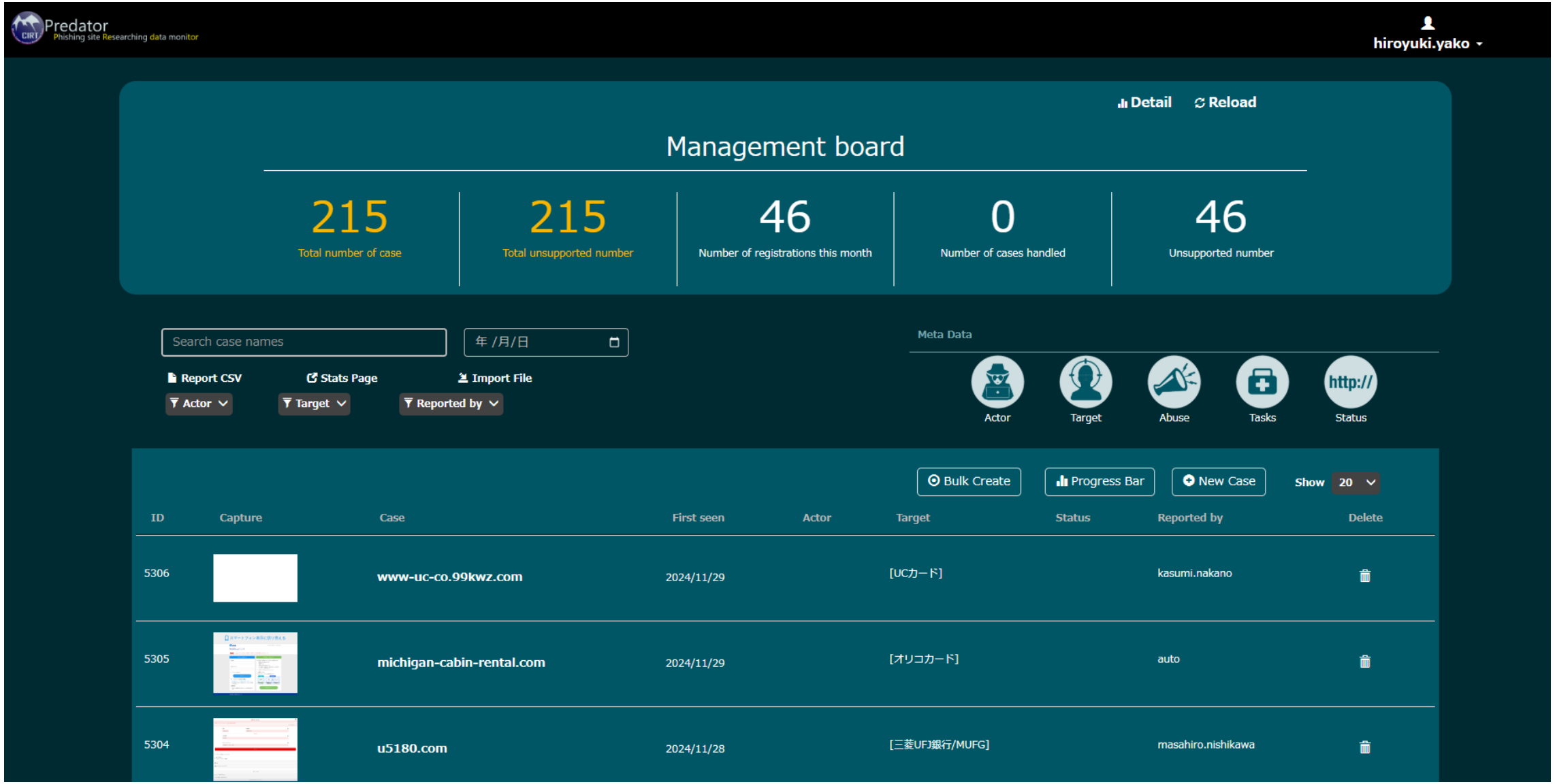
当日投影のみ

当日投影のみ

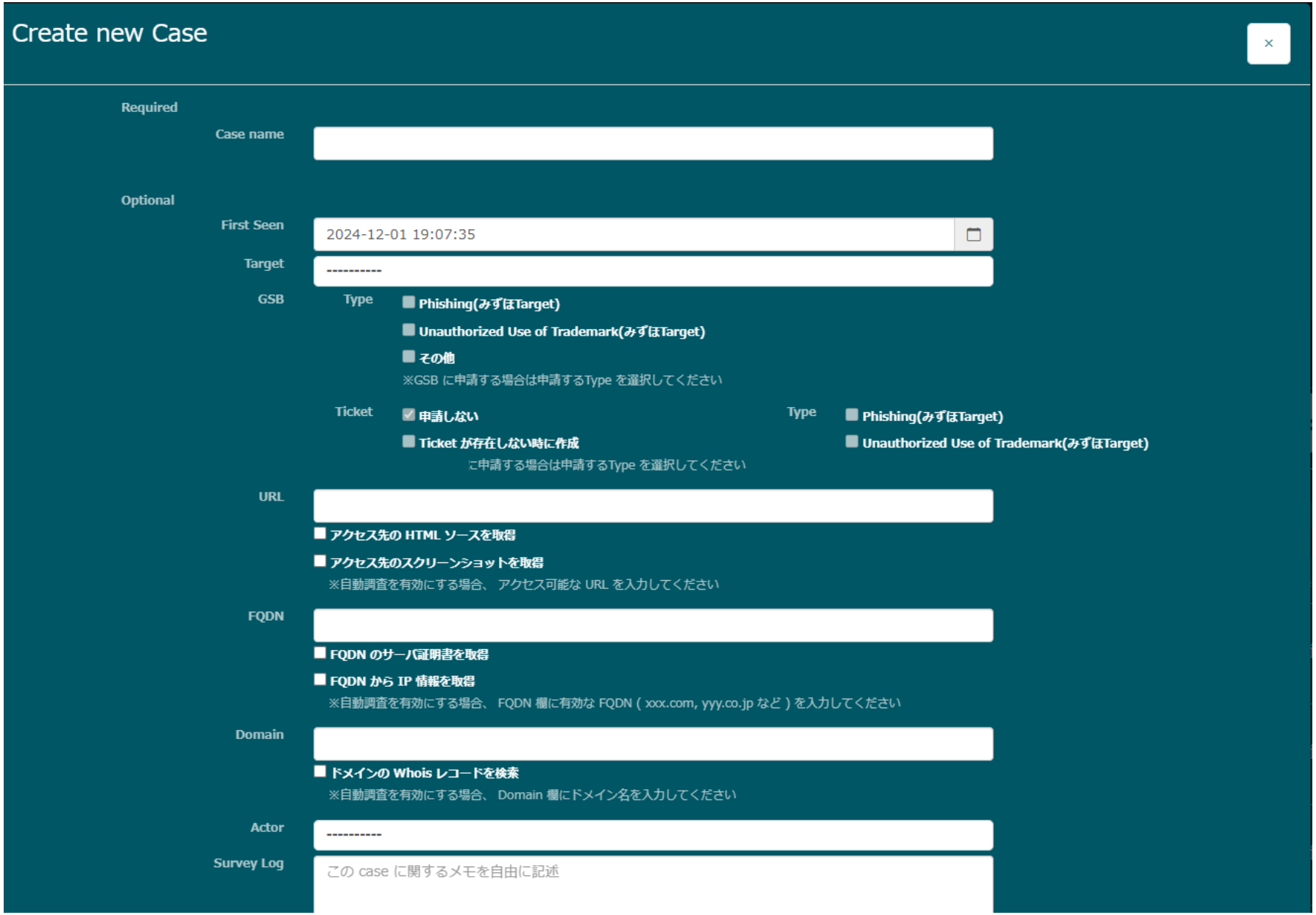
# 当日投影のみ

# 当日投影のみ

# For everyone – テイクダウン支援ツールのアップデート



# For everyone – テイクダウン支援ツールのアップデート

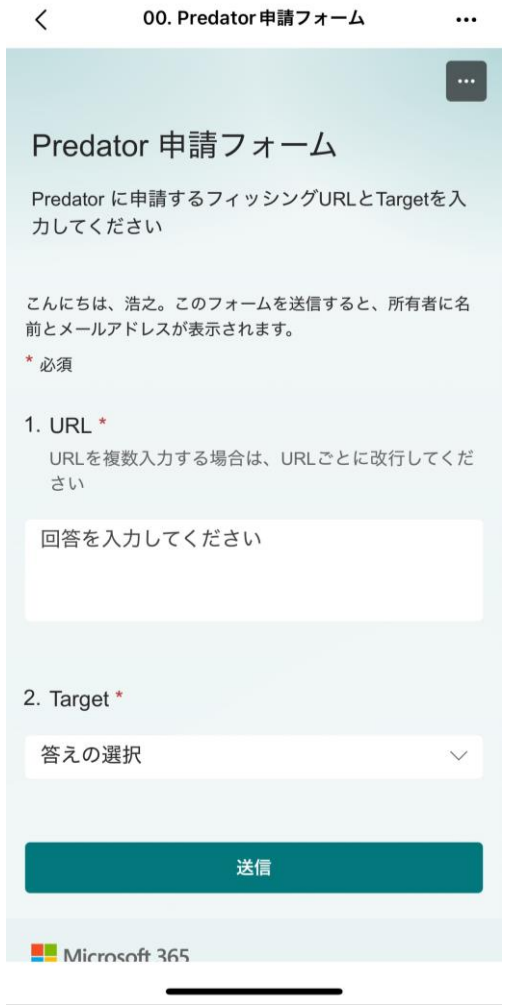


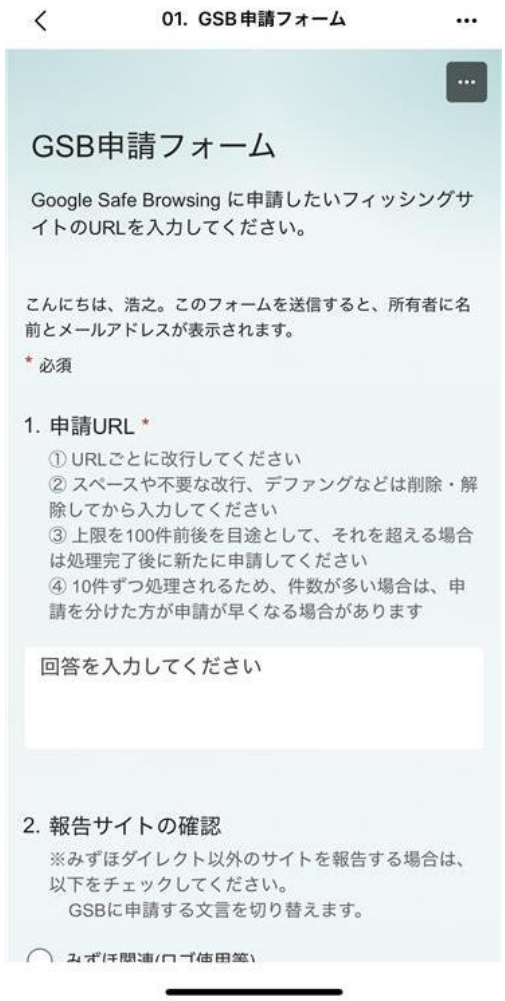
A air3_apps 9/30 10:04 編集済み

# README

## 各種フォーム

00. Predator申請フォーム
01. GSB申請フォーム
02. URLScan申請フォーム
03. 申請フォーム



# 当日投影のみ

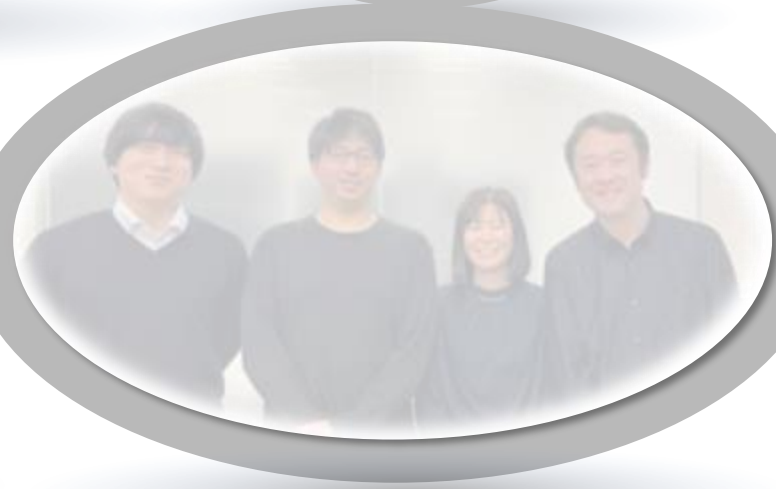
# Defend forward - Deceptionアプローチ

01 不正送金班

02 Tech班(マルウェア解析)

03 開発実装担当

04 自動化推進担当



# Defend forward - Deceptionアプローチ


## フィッシングサイトに対する Deceptionアプローチ

### Abstract

近年、フィッシングサイトの数が急増しており、状況が悪くなる一方である。彼らの主な目的はクレジットカード情報やオンライン口座の認証情報など「金の種」を狙うことがわかっている。

フィッシング攻撃に対する対応として、一般的には
1. テイクダウン
2. 一般ユーザーへの啓蒙
の２つ手段がある。しかし、ABUSEによるサイトのテイクダウンは報告先の対応に依存し、攻撃者のインフラの選択により大きな制限を受けることになる。一般ユーザーへの啓蒙も一朝一夕には進まない。

延々とテイクダウンを継続する対応は心が病んでいくため、上記以外の対応として何ができるか調査し、Deceptionのアプローチを試してみた。本講演では、２つの攻撃グループが作成したフィッシングサイトに対して行なったアプローチについて説明する。また、一連の作業において発生してきた問題と対策を共有する。

### Speaker

猪野 裕司

吉川 允樹

当日投影のみ

当日投影のみ

将来的には、フィッシングサイトの発見後速やかに対象のグループを分類、自動的にダミーのアカウントを投入する仕組みを構想中

## 自動化の更なる推進

- 大量発生時には管理業務（フィッシングサイトの件数やステータス管理）の負荷が高いため、フィッシングのステータス監視やその集計の効率化を図り、ダッシュボードとして経営層も閲覧可能な形に整理を行う。
- インプットとなるフィッシングサイトの情報収集源から自動的に収集する仕組みの強化やテイクダウンに必要なサービスへの連携拡大を追求。
- AIの活用により、フィッシングサイトの攻撃アクターグループの自動分類、フィッシングサイトの特徴の分析等に活用を想定。将来的にはより人間に近い「騙された振り作戦」の実行基盤を整備。

## 共同防衛の推進（≠情報共有）

- JSACでの発表内容は、フィッシングに苦しむ企業に対して、可能な範囲でノウハウを公開し、相互に効果が出た機能について共有・改善を行えるような連携を呼びかけたい。
- 研修制度や相互訓練等を通した人的な交流、フィッシングの防御技術の共有及び共同研究、相互のフィッシングサイトの観測とテイクダウンの取り組みへ発展させたい。特に官民連携が重要な分野であるため、積極的に働きかけていきたい。
- JC3や金融ISAC等のコミュニティに多大なる支援をいただいており、その発展に積極的に貢献する。単なる情報共有の組織ではなく、アクションができる組織として我々も積極的に参画していきたい。

# 終わりに

・不正送金モニタリングは必須ではあるが、限界があることから、フィッシングサイトの早期検知/テイクダウンなどを併せて実施
・対処するときは人的リソースに限界があることから対応の一部自動化を組み合わせる
・単独ではなく総力戦で

・マルウェア解析などの専門性を身に着けることで、ユーザー企業においても早期フィッシングサイト検知の仕組みを開発することが可能。

・自動化には複数の業務知識と専門性が必要。自分の専門分野だけでなく他のチームの業務分野まで踏み込める胆力とチームワークが必要。
・フィッシングと一緒に戦うために、志を同じくする組織・企業等と「アクション」に向けて積極的に活動していきたい。

# Appendix

## IoC

| value | type |
|---|---|
| 66b118b5c63a3c8e30941b2e620211d04febbb21e3c90feb1f283b0b598fb46c | SHA256 hash value of Keepspy |
| siltsb6.duckdns[.]org | Keepspy C2 Server A Domain |
| 104.255.152[.]61 | Keepspy C2 Server B IP Address |
| 104.255.152[.]62 | Keepspy C2 server B IP address (other C2 servers) |
| 104.255.152[.]85 | Keepspy C2 server B IP address (other C2 servers) |
| 104.255.152[.]86 | Keepspy C2 server B IP address (other C2 servers) |
| 104.255.152[.]100 | Keepspy C2 server B IP address (other C2 servers) |