

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

ともに挑む。
ともに実る。



竹内 司

Tsukasa Takeuchi

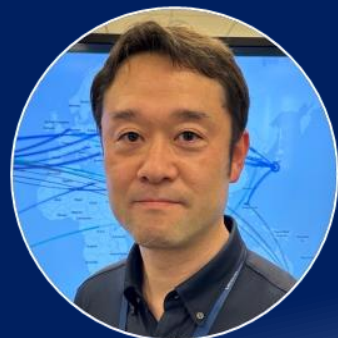
Cybercrime



遠藤 拓也

Takuya Endo

Technical



八子 浩之

Hiroyuki Yako

CSIRT

Engineer

西川 昌広 Masahiro Nishikawa

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

Technical team

近藤 一成 Kazunari Kondo

笹村 直樹 Naoki Sasamura

小山 昌樹 Masaki Koyama

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

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

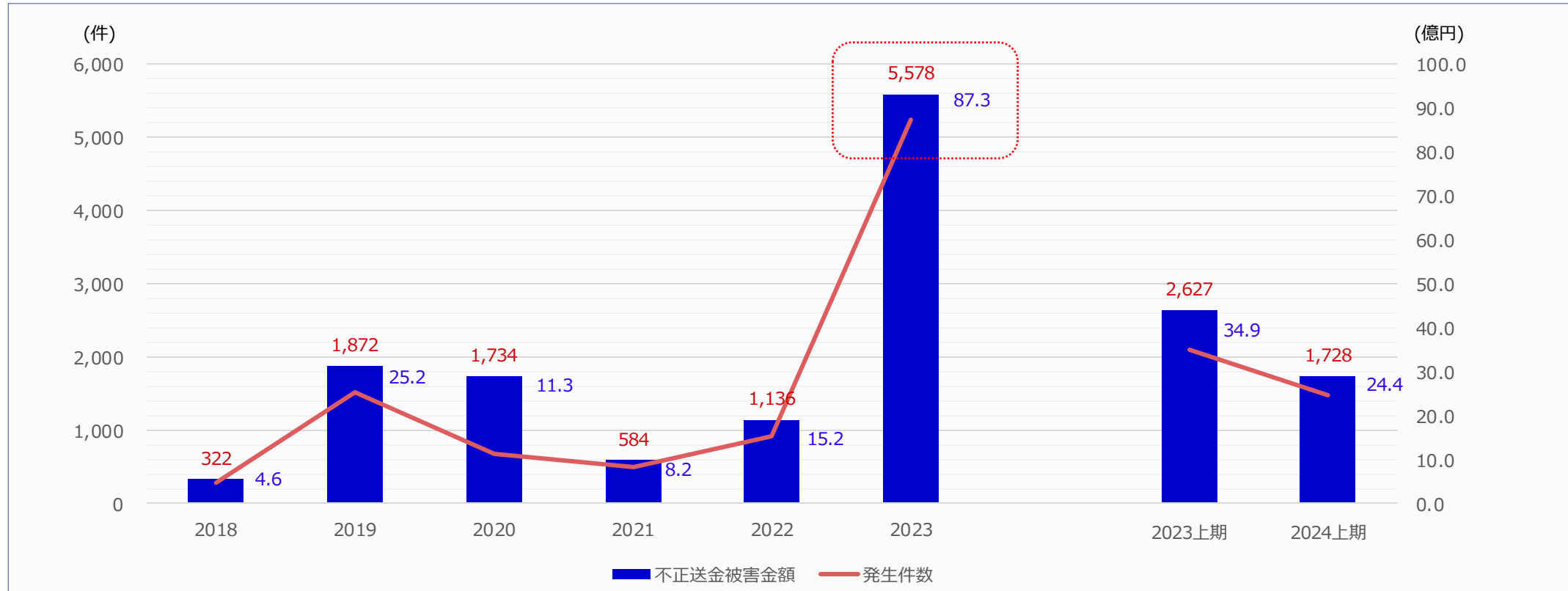
インターネットバンキングに係る
不正送金の発生件数

5,578件

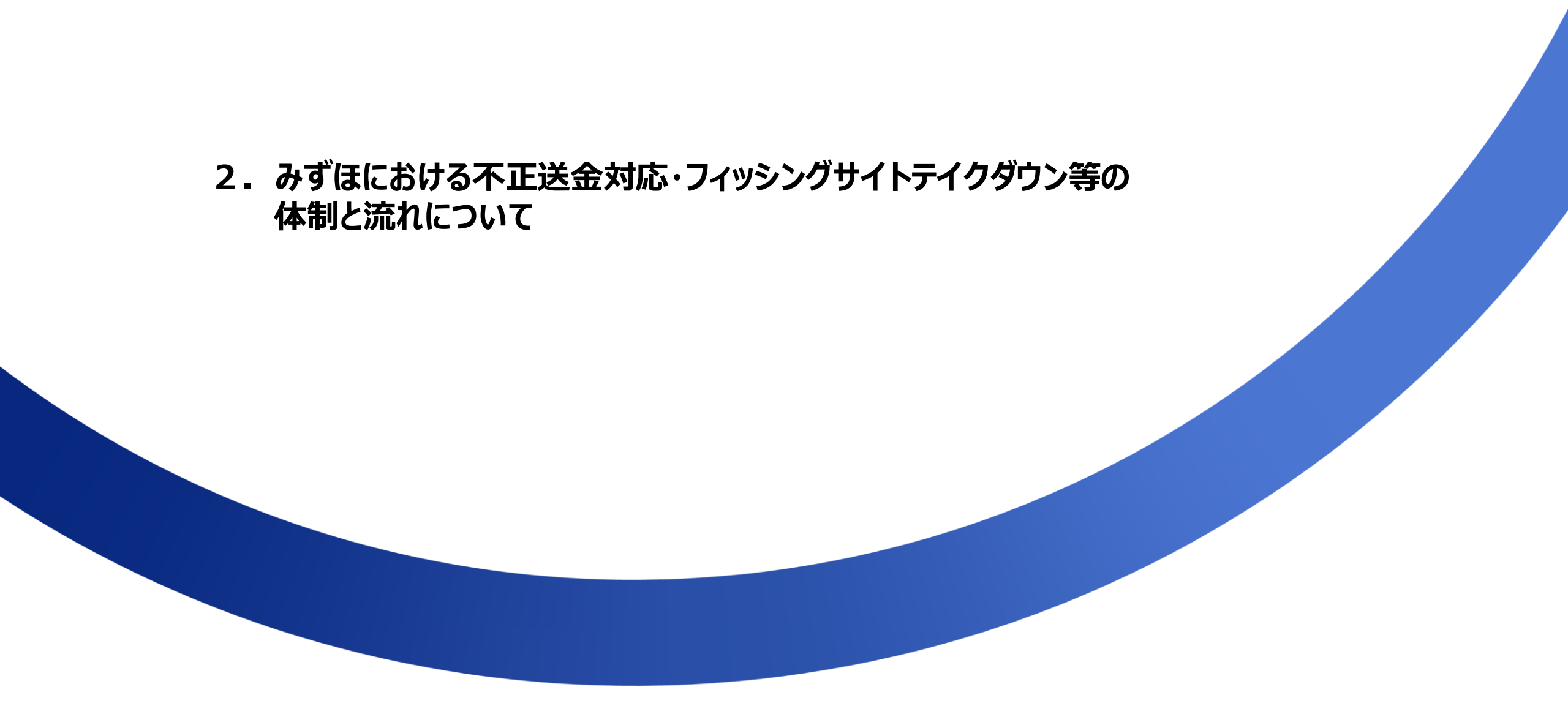
被害総額

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
説明させていただきます

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

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





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。



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
- TrendmicroやNetcraftなどセキュリティ事業者への申請
- IC3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?)	サイト特徴	・画面の作り込みが丁寧	URL例 hxxps://direct.mizuho-helpdisk.is hxxps://www.index-cr-mizu.cc hxxps://www.index-web-ib-mizuho.is hxxps://www.index-webib-mizuho.online
タイプ	リアルタイム	その他	・当行では2023年夏頃から大量発生 of グループ。邦銀では同グループによる被害を多数確認。 ・.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 ・立ち上げるURLの数は少ないが破壊力高 ・アプリを犯人側端末で乗っ取る手口多数	
(邦銀)出現頻度	高		Registrar (Registry) isnic.is.等	

みずほダイレクト

【パスワードや暗証番号の保管にご注意ください】
昨今、パソコンやスマートフォンのメモ帳や画像、メールソフトに保存していた暗証番号等が悪意のある第三者によって盗まれ、インターネットバンキングで不正送金されるケースが確認されています。大変危険ですのでご注意ください。

暗証番号が都度自動発行となり管理が必要ないことから、みずほダイレクトアプリ上で発行される「ご利用カード (アプリ版)」のご利用を推奨しております。利用方法などはみずほ銀行WEBサイトにてご確認ください。

セキュリティ対策は万全ですか?
より安心して利用するポイントを今すぐチェック!
[くわしくはこちら▶](#)

お客さま番号

次へ

・お客さま番号がわからない方はこちら (ご利用カード再発行)

・ログインパスワードをお忘れの場合はこちら

個人情報の取扱 | 規定
PCサイト | ヘルプ (注意事項等)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト

ログインパスワードを半角英数字で入力し、「ログイン」ボタンをクリックしてください。

本人確認

- お客さま番号
12341234
- ログインパスワード

ログイン

[ヘルプ](#)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト 本人確認

ご本人確認のため。

本人確認

- お客さま番号
12341234
- 名前
- 名前 (カナ)
- 生年月日
- 郵便番号
- 電話番号
- 都道府県
- 住所 (都市区)
- 第1暗証番号 (4桁の半角数字)

[ヘルプ](#)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト 本人確認

ご本人確認のため、SMS認証を入力してください。

本人確認

- お客さま番号
12341234
- SMS認証 (5桁の半角数字)

中止 次へ

[ヘルプ](#)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト 本人確認

ご本人確認のため、EMAIL認証用暗証番号を入力してください。

本人確認

- お客さま番号
12341234
- 認証用暗証番号 (半角数字5桁)

中止 次へ

[ヘルプ](#)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

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	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	URL例 hxxps://web.ib.mazizuzsfshodbank.co.jp. findhighpower.com/ hxxps://web.ib.mazizuzsfshodbank.co.jp. wowpalmbay.com	
タイプ	リアルタイム	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。 ・レジストラ:GMO、NameServer:A.SSHARE-DNS(Gname)を利用しており、比較的、落としやすい。		Registrar (Registry) GMO INTERNET,INC等
(邦銀)出現頻度	低				

みずほダイレクト

【パスワードや暗証番号の保管にご注意ください】
昨今、パソコンやスマートフォンのメモ帳や画像、メールソフトに保存していた暗証番号等が悪意のある第三者によって盗まれ、インターネットバンキングで不正送金されるケースが確認されています。大変危険ですのでご注意ください。

暗証番号が都度自動発行となり管理が必要ないことから、みずほダイレクトアプリ上で発行される「ご利用カード（アプリ版）」のご利用を推奨しております。利用方法などはみずほ銀行WEBサイトにてご確認ください。

セキュリティ対策は万全ですか？

より安心して利用するポイントを今すぐチェック！
[くわしくはこちら▶](#)

お客さま番号

次へ

・お客さま番号がわからない方は[こちら（ご利用カード再発行）](#)
・ログインパスワードをお忘れの場合は[こちら](#)

個人情報取扱 | 規定
PCサイト | ヘルプ（注意事項等）

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト

ログインパスワードを半角英数字で入力し、「ログイン」ボタンをクリックしてください。

本人確認

- お客さま番号
12341234
- ログインパスワード

ログイン

[ヘルプ](#)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト 本人確認

ご本人確認のため、第1暗証番号、第2暗証番号を入力してください。

本人確認

- お客さま番号
12341234
- 第1暗証番号（4桁の半角数字）
- 第2暗証番号（6桁の半角数字）
- ご登録メールアドレス

中止 次へ

[ヘルプ](#)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

MIZUHO みずほ銀行

One MIZUHO

【みずほ総合口座・みずほマイレブ・みずほダイレクト・みずほビット・カードローン】 口座開設情報のご入力

旧字等があり、漢字変換出来ない場合は、入力可能な新字をご入力ください。

フリガナ（全角カタカナ）【必須】

(例) ミスホ タロウ
姓 名

生年月日（半角）【必須】
西暦 年 月 日

郵便番号（半角）【必須】
ご自宅の郵便番号をご入力ください。
(例) 100-0011
 -

自宅の郵便番号をご入力ください。

都道府県【必須】
お選びください▼

市区町村・番地（全角）【必須】
ご自宅の住所を番地までご入力ください。
(例) 千代田区内幸町1-1-5

(注) 本人確認書類の住所に合わせて入力訂正をお願いします。

アパート・マンション名（全角）
例) みずほビル101 ○○様方

団地・アパート名・棟号・室号および様方までご入力ください。

携帯電話番号（半角）【必須】
 - -

お申込日
2024年04月11日

支店番号（半角）【必須】
(例) 012

口座番号（半角）【必須】
(例) 1234567

おなまえ（全角）【必須】
(例) みずほ 太郎
姓 名

「おなまえ」欄は、本人確認書類上の氏名をご入力ください。

次へ▶

[このページをクリアする▶](#)

みずほダイレクト【インターネットバンキング】

[この画面のヘルプ](#)

ご本人さま以外によるお取引を防止するため、認証用暗証番号(半角数字5桁)をご登録いただいているメールアドレスにお送りしました。本画面を閉じずに、電子メールに記載の認証用暗証番号(半角数字5桁)をご入力ください。
※電子メールが到着するまで、数分程度お時間がかかる場合がございます。

■ワンタイムパスワード追加認証

認証用暗証番号(半角数字5桁)

戻る 中止 次へ

登録メールアドレス **tanakiyo@gmail.ne.jp**

※電子メールの送信元メールアドレスは「send_mail@e-mail.mizuhobank.co.jp」となります。受信拒否設定をされている場合は、当該メールアドレスを許可のうえ、再度お取引を行ってください。

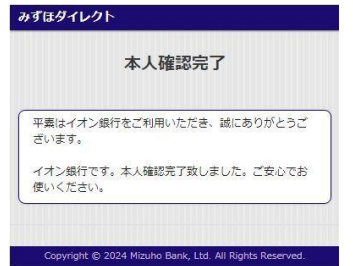
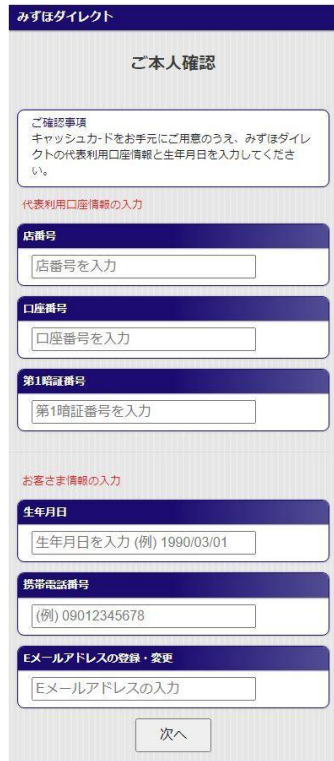
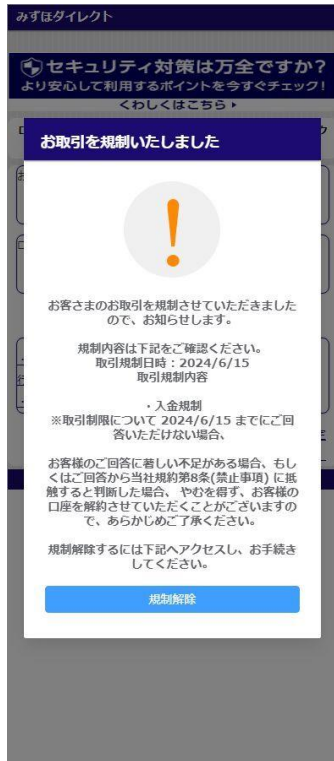
※ご登録のメールアドレスで電子メールが受け取れない場合は当行ホームページよりみずほダイレクトへログインいただき、「各種手続き」メニューの「メールアドレス変更」で変更のうえ、再度お取引を行ってください。

※ご本人さま以外が操作した可能性があるメールアドレス変更については、変更後一定時間以内はお取引を受け付けできない場合があります。なお、電話での利用停止・再開をご案内させていただくこともありますので、あらかじめご了承ください。

Copyright (c) 2024 Mizuho Bank, Ltd. All Rights Reserved.

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)	サイト特徴	<ul style="list-style-type: none"> 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) 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 	URL例	hxxps://feyusb6.duckdns.org hxxps://gfpbq452s.duckdns.org		
タイプ	リアルタイム	その他	<ul style="list-style-type: none"> アプリを犯人側の端末に紐づけ乗っ取る手口が多数 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 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 当行では緊急的に対処実施 			Registrar (Registry)	duckdns.org等
(邦銀)出現頻度	高						



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)	サイト特徴	<ul style="list-style-type: none"> 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) 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 	URL例	hxxps://uv2r90.duckdns.org hxxps://mzgel01.duckdns.org
タイプ	リアルタイム	その他	<ul style="list-style-type: none"> 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。 	Registrar (Registry)	duckdns.org等
(邦銀)出現頻度	高				

The screenshots show the following steps in the phishing process:

- Security Warning:** A message asking if security measures are complete, with a 'Login' button.
- Login Screen:** Fields for card number and PIN, with a 'Login' button.
- Card Management:** A screen for managing the 'MIZUHO' card, including fields for card number and PIN.
- Confirmation Screens:** A series of screens for updating personal information, including fields for name, date of birth, address, and phone number.
- Security Enhancement:** A screen showing a progress indicator (4%) for security enhancement, with a 'Next' button.
- SMS Authentication:** A screen for SMS authentication, with a field for the authentication code and a 'Send' button.
- Final Confirmation:** A screen for final confirmation of SMS authentication, with a 'Send' button.

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	サイト特徴	<ul style="list-style-type: none"> 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 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 	URL例	hxxps://cdshyj.com hxxps://dizichina.com Hxxps://qigehangmo.com
タイプ	リアルタイム	その他	<ul style="list-style-type: none"> 2022年9月頃～被害を及ぼしていたと考えられる 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) 	Registrar (Registry)	Gname.com Pte. Ltd.等
(邦銀)出現頻度	高				

■PCサポート詐欺
ウイルス感染等の画面を表示させ電話の案内により不正に送金される手口。画面に表示された番号には電話せず、ブラウザの強制終了、パソコンの再起動をしてください。

■通販サイトの「返金手続き」詐欺
通販で購入した商品が届かず「返金手続き」を装ってキャッシュレス決済や振込で送金させられる手口。返金手続きと称した送金・振込の依頼にはご注意ください。

万一、暗証番号等を入力した場合、専用ダイヤル(0120-324-358)に直ちにご連絡ください。受付時間9時～17時

🔒セキュリティ対策は万全ですか?
より安心して利用するポイントを今すぐチェック!
くわしくはこちら▶

お客さま番号
[入力欄]
次へ

・お客さま番号がわからない方はこちら(ご利用カード再発行)
・ログインパスワードをお忘れの場合はこちら

個人情報の取扱い | 規定
PCサイト | ヘルプ(注意事項等)

みずほダイレクト

お客さま番号
1234123

ログインパスワード
[入力欄]

ログイン キャンセル

ログインパスワードをお忘れの場合はこちら

ヘルプ(注意事項等)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト 秘密の質問

秘密の質問にお答えください。

秘密の質問
お客さま番号
1234123
今日の晩ご飯は?
[入力欄]

次へ

ヘルプ

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト ご本人確認

ご本人確認のため、店番号、口座番号、第1暗証番号、生年月日、電話番号、ワンタイム認証で利用するメールアドレスを入力してください。

ご本人確認
お客さま番号
1234123
店番号 (3桁の半角数字)
[入力欄]
口座番号 (7桁の半角数字)
[入力欄]
第1暗証番号 (4桁の半角数字)
[入力欄]
生年月日 (西暦6桁の半角数字)
[入力欄]
電話番号 (半角数字)
[入力欄]
ワンタイム認証で利用するメールアドレス
[入力欄]

次へ

ヘルプ

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト SMS認証

09001231234に認証コードを送信しました。SMSをご確認のうえ、認証コードを入力してください。

SMS認証
お客さま番号
1234123
認証コードの入力
[入力欄]

次へ

ヘルプ

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト ご本人確認

ご本人確認のため、第2暗証番号を入力してください。

ご本人確認
お客さま番号
1234123
第2暗証番号 (6桁の半角数字)
[入力欄]

次へ

ヘルプ

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト

認証用暗証番号(半角数字5桁)をご登録いただいているメールアドレスにお送りしました。本画面を閉じずに、電子メールに記載の認証用暗証番号(半角数字5桁)をご入力ください。
※電子メールが到着するまで、数分程度お待たせがかかる場合がございます。

ワンタイムパスワード追加認証
お客さま番号
1234123
登録メールアドレス
tanakiyoo@yahoo.co.jp
認証用暗証番号 (5桁の半角数字)
[入力欄]

次へ

ヘルプ

※電子メールの送信元メールアドレスは「send_mail@e-mail.mizuho-bank.co.jp」となります。
※ご登録のメールアドレスで電子メールが受け取れない場合は「各種手続き」メニューの「メールアドレス変更」で変更のうえ、再度お振込のお手続きを行ってください。
※ご本人さま以外が操作した可能性があるメールアドレス変更については、変更後一定時間以内はお取引を受け付けできない場合があります。なお、電話での利用停止・再開をご案内させていただくこともありますので、あらかじめご了承ください。

みずほダイレクト

ご本人確認完了

ご協力ありがとうございました。

ヘルプ

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

Outlook

Microsoft
← tanakiyoo@yahoo.co.jp
パスワードの入力
パスワード
パスワードを忘れた場合
サインイン

iCloud

2ファクタ認証
Apple IDでサインイン
メールアドレスは既定のまま
tanakiyoo@yahoo.co.jp
パスワード
[入力欄]

YAHOO! JAPAN

tanakiyoo@yahoo.co.jp
パスワード
ログイン
他の方法でログイン
© Yahoo Japan

tanakiyoo@yahoo.co.jp
確認コード
ログイン
確認コードを再送信
ログインできない場合
© Yahoo Japan

本人確認
アカウントを安全に保つため、ログインするには本人確認を行う必要があります 詳細
tanakiyoo@yahoo.co.jp
確認コードを送信しました
コードを入力
次へ
ヘルプ プライバシー 規約

ようこそ
tanakiyoo@yahoo.co.jp
パスワードを入力
パスワードを表示する
パスワードをお忘れの場合
次へ
ヘルプ プライバシー 規約

メールアカウント
によって出し分け
される仕組み

みずほダイレクト

【パスワードや暗証番号の保管にご注意ください】
 昨今、パソコンやスマートフォンのメモ帳や画像、メールソフトに保存していた暗証番号等が悪意のある第三者によって盗まれ、インターネットバンキングで不正送金されるケースが確認されています。大変危険ですのでご注意ください。

暗証番号が都度自動発行となり管理が必要ないことから、みずほダイレクトアプリ上で発行される「ご利用カード（アプリ版）」のご利用を推奨しております。利用方法などはみずほ銀行WEBサイトにてご確認ください。

セキュリティ対策は万全ですか？
 より安心して利用するポイントを今すぐチェック！
[くわしくはこちら](#)

お客さま番号

次へ

・お客さま番号がわからない方はこちら（ご利用カード再発行）
 ・ログインパスワードをお忘れの場合はこちら

[個人情報取扱](#) | [規定](#)
[PCサイト](#) | [ヘルプ](#)（注意事項等）

みずほダイレクト

ご本人確認のため、第1暗証番号、第2暗証番号を入力してください。

本人確認

- お客さま番号
1234123
- 名前（漢字）
- 第1暗証番号（4桁の半角数字）
- 第2暗証番号（6桁の半角数字）
- ご登録メールアドレス
- 生年月日(年)
- 生年月日(月)
- 生年月日(日)

次へ

みずほダイレクト

ログインパスワードを半角英数字で入力し、「ログイン」ボタンをクリックしてください。

本人確認

- お客さま番号
1234123
- ログインパスワード

ログイン

[ヘルプ](#)

Copyright © 2023 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト **本人確認**

メール認証に認証コードを送信しました。メールをご確認のうえ、認証コードを

メール認証

- お客さま番号
1234123
- 認証コードの入力

次へ


[ヘルプ](#)

Copyright © 2023 Mizuho Bank, Ltd. All Rights Reserved.

ワンタイムパスワード認証

ワンタイムパスワード

【手順】



- ワンタイムパスワードカードの「3」のボタンを押してください。
- ワンタイムパスワードカードに確認番号:
- 「OK」ボタンを押してください。
- ワンタイムパスワードカード上に表示されるワンタイムパスワード8桁のみずほダイレクトの画面に入力してください。

実行

[ヘルプ](#)

Copyright © 2023 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト **本人確認**

SMS認証に認証コードを送信しました。SMSをご確認のうえ、認証コードを

SMS認証

- お客さま番号
1234123
- 認証コードの入力

次へ

[ヘルプ](#)

Copyright © 2023 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト

【パスワードや暗証番号の保管にご注意ください】
 昨今、パソコンやスマートフォンのメモ帳や画像、メールソフトに保存していた暗証番号等が悪意のある第三者によって盗まれ、インターネットバンキングで不正送金されるケースが確認されています。大変危険ですのでご注意ください。

暗証番号が都度自動発行となり管理が必要ないことから、みずほダイレクトアプリ上で発行される「ご利用カード（アプリ版）」のご利用を推奨しております。利用方法などはみずほ銀行WEBサイトにてご確認ください。

セキュリティ対策は万全ですか？
 より安心して利用するポイントを今すぐチェック！
[くわしくはこちら](#)

お客さま番号

次へ

[・お客さま番号がわからない方はこちら（ご利用カード再発行）](#)
[・ログインパスワードをお忘れの場合はこちら](#)

[個人情報の取扱](#) | [規定](#)
[PCサイト](#) | [ヘルプ（注意事項等）](#)

Copyright © 2024 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト

ログインパスワードを半角英数字で入力し、「ログイン」ボタンをクリックしてください。

本人確認

- お客さま番号
12344321
- ログインパスワード

ログイン

[ヘルプ](#)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト **本人確認**

ご本人確認のため、EMAIL認証用暗証番号を入力してください。

本人確認

- お客さま番号
12344321
- 認証用暗証番号（半角数字）

中止 **次へ**

[ヘルプ](#)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト **本人確認**

ご本人確認のため、SMS認証を入力してください。

本人確認

- お客さま番号
12344321
- SMS認証（半角数字）

中止 **次へ**

[ヘルプ](#)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

みずほダイレクト **本人確認**

ご本人確認のため。

本人確認

- お客さま番号
12344321
- 登録メールアドレス
- 生年月日
- 郵便番号
- 電話番号
- 都道府県
- 住所（都市区）
- 第1暗証番号（4桁の半角数字）

中止 **次へ**

[ヘルプ](#)

Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

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

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。



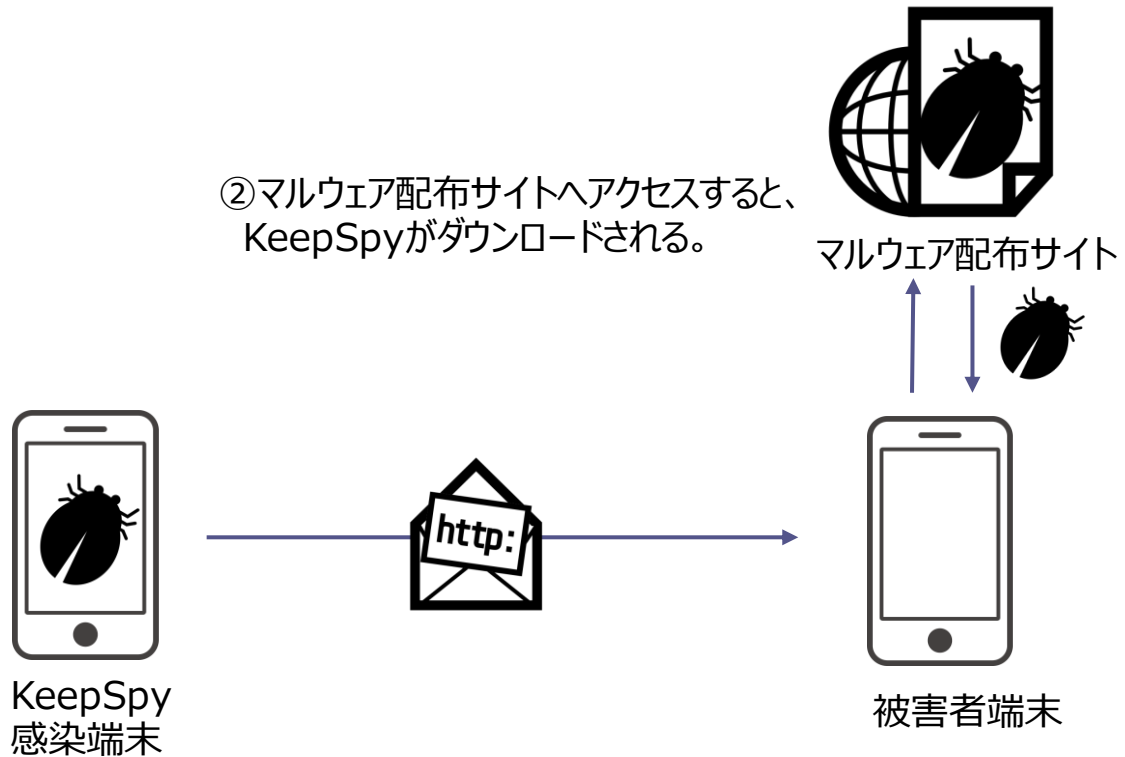
<参考> 善意のフィッシュハンターの投稿

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。



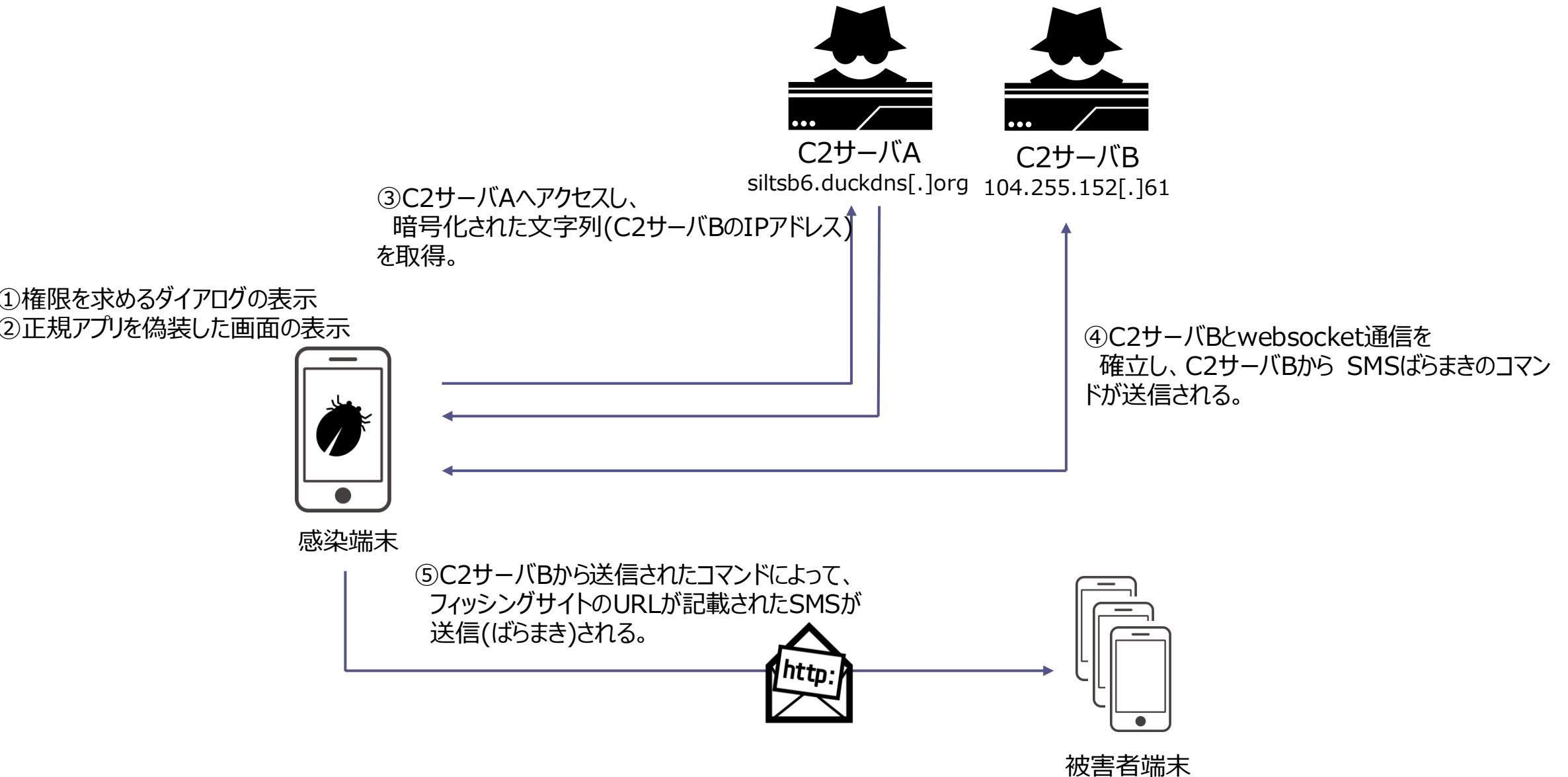
- ①KeepSpy感染端末から、マルウェア配布サイトのURLが記載されたSMSが被害者端末へ送信される。

<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。



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

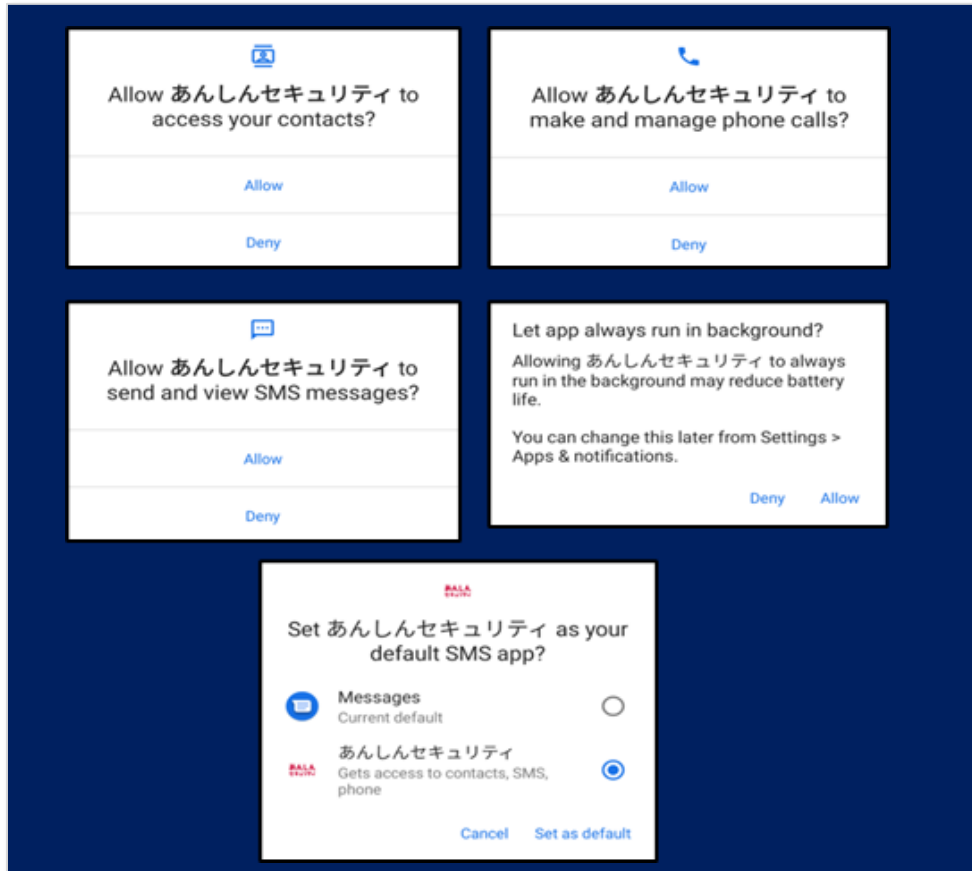
<解析結果：全体像>KeepSpy感染からSMS送信までの仕組み



<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。



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。

The screenshot shows the mitmproxy interface with a list of intercepted flows. The flow for `http://siltsb6.duckdns.org/` is highlighted with a red box. The details pane on the right shows the response body containing a base64-encoded string.

Path	Method	Status	Size	Time
10.0.0.1:53824 ↔ 10.0.0.53:853	TCP		56b	9ms
mtalk.google.com A = 64.233.187.188, 64.233.187.188, 64.233.187.188	QUERY	NOE...	12b	5ms
donaldsonmolly93.github.io A = 185.199.110.153, 185.199.110.153, 185.1...	QUERY	NOE...	48b	1ms
siltsb6.duckdns.org A = 205.185.124.68, 205.185.124.68, 205.185.124.68	QUERY	NOE...	12b	187ms
http://siltsb6.duckdns.org/	GET	200	44b	11s
http://104.255.152.61:7775/	WS	101	1.6kb	18min
infinitedata-pa.googleapis.com A = 216.58.220.106, 216.58.220.106, 216.5...	QUERY	NOE...	192b	-5s
infinitedata-pa.googleapis.com A = 172.217.31.170, 172.217.31.170, 172.2...	QUERY	NOE...	192b	-5s
mtalk.google.com A = 64.233.187.188, 64.233.187.188, 64.233.187.188	QUERY	NOE...	12b	2ms
infinitedata-pa.googleapis.com A = 142.251.222.10, 142.251.222.10, 142.2...	QUERY	NOE...	192b	-5s
infinitedata-pa.googleapis.com A = 142.251.222.42, 142.251.222.42, 142.2...	QUERY	NOE...	192b	-5s

Response details:

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 10 Jun 2024 04:25:48 GMT
Content-Type: text/html
Content-Length: 44
Last-Modified: Thu, 04 Apr 2024 05:17:21 GMT
Connection: keep-alive
ETag: "660e37e1-2c"
Accept-Ranges: bytes
XML
HgWMM1Lus2GN01V3+yu7TUc1CD8pte0yuIxxqV12m0QA=
```

暗号化された文字列

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("AES/ECB/PKCS5Padding"); ←"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 = f4414gjqrbrbweff;
        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

The screenshot displays the CyberChef interface with the following configuration:

- Recipe:** From Base64
- Alphabet:** A-Za-z0-9+/=
- Remove non-alphabet chars:**
- Strict mode:**
- AES Decrypt:** Key: apYya82az7rgeN3A, UTF8, IV, HEX
- Mode:** ECB
- Input:** Raw
- Output:** Raw

The **Input** field contains the Base64 string: `HgwMMLus2GN0iV3+yu7TUc1CD8pte0yuIxxqV12m0QA=`

The **Output** field contains the decoded result: `104.255.152.61:7775`

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

Path	Method	Status	Size	Time
10.0.0.1:53824 ↔ 10.0.0.53:853	TCP		56b	9ms
mtalk.google.com A = 64.233.187.188, 64.233.187.188, 64.233.187.188	QUERY	NOE...	12b	5ms
donaldsonmolly93.github.io A = 185.199.110.153, 185.199.110.153, 185.1...	QUERY	NOE...	48b	1ms
siltsb6.duckdns.org A = 205.185.124.68, 205.185.124.68, 205.185.124.68	QUERY	NOE...	12b	187ms
http://siltsb6.duckdns.org/	GET	200	44b	11s
http://104.255.152.61:7775/	WS	101	1.8kb	20min
infinitedata-pa.googleapis.com A = 216.58.220.106, 216.58.220.106, 216.5...	QUERY	NOE...	192b	-5s
infinitedata-pa.googleapis.com A = 172.217.31.170, 172.217.31.170, 172.2...	QUERY	NOE...	192b	-5s
mtalk.google.com A = 64.233.187.188, 64.233.187.188, 64.233.187.188	QUERY	NOE...	12b	2ms
infinitedata-pa.googleapis.com A =
infinitedata-pa.googleapis.com A =
0djedia.duckdns.org A = 209.141.40...
http://0djedia.duckdns.org/404.htm...
http://0djedia.duckdns.org/404.html	GET	403	146b	930ms
http://0djedia.duckdns.org/404.html	GET	403	146b	1s
infinitedata-pa.googleapis.com A = 142.251.42.170, 142.251.42.170, 142.2...	QUERY	NOE...	192b	-5s
infinitedata-pa.googleapis.com A = 142.251.42.138, 142.251.42.138, 142.2...	QUERY	NOE...	192b	-5s
mtalk.google.com A = 64.233.187.188, 64.233.187.188, 64.233.187.188	QUERY	NOE...	12b	1ms
infinitedata-pa.googleapis.com A = 142.251.42.138, 142.251.42.138, 142.2...	QUERY	NOE...	192b	-5s

初回の通信では端末情報をC2サーバへ送信

**10秒毎に
取得したC2サーバ宛に通信を行う。
送信者側からは「心跳&ping」を送信**

C2サーバからの応答は「pong」

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)

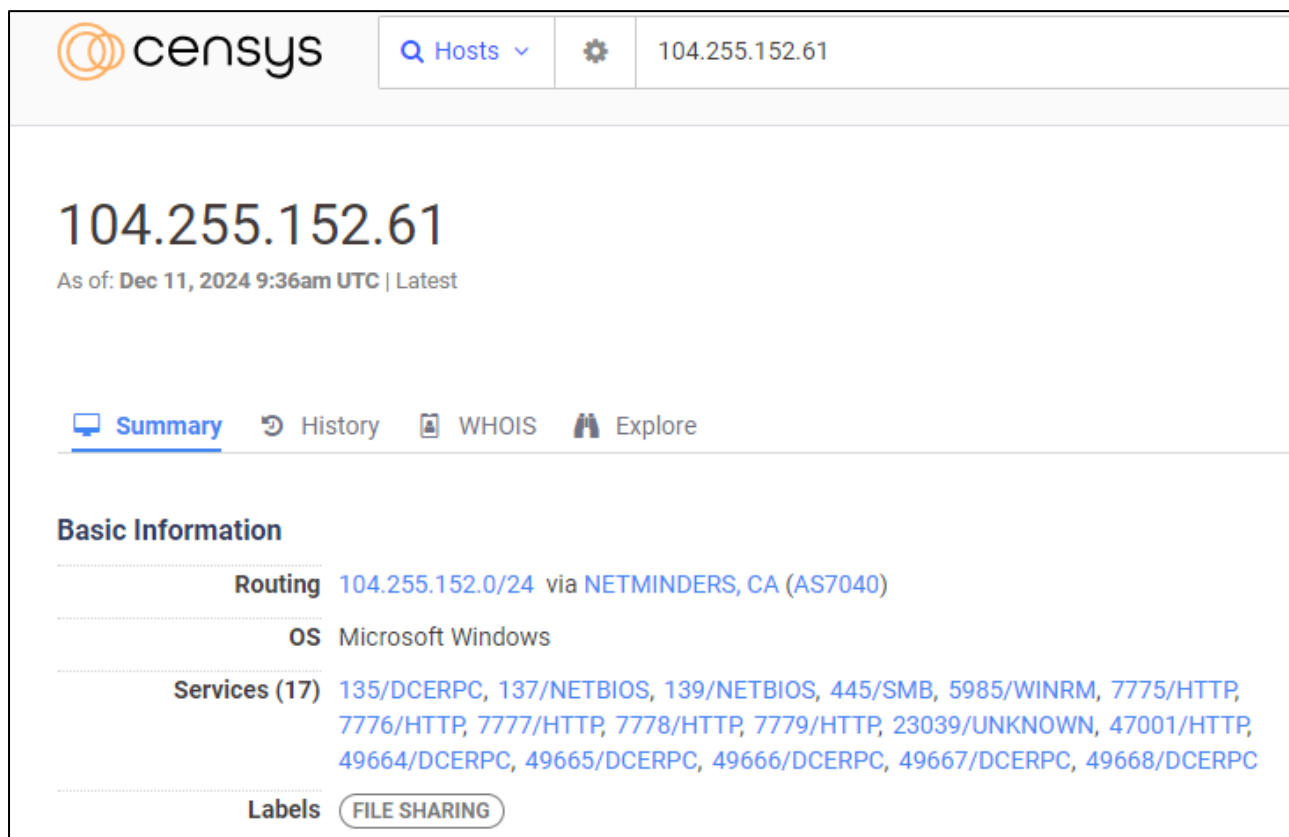
コマンド名	日本語訳
通讯录	電話帳
收件箱	受信箱
拦截短信&open	テキストメッセージ傍受
拦截短信&close	テキストメッセージ傍受
发信息&	メッセージ送信
清除短信&	SMSを削除
普通通知栏&	通常のお知らせバー
通知栏&	通知バー
应用列表&	アプリケーションリスト
更新&	更新

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

→**7776~7779ポートからも同様のコマンドが返信される**ものと思われる。



The screenshot shows the Censys search interface for the IP address 104.255.152.61. The main heading is "104.255.152.61" with a timestamp "As of: Dec 11, 2024 9:36am UTC | Latest". Below this, there are navigation tabs for "Summary", "History", "WHOIS", and "Explore". The "Basic Information" section is expanded, showing the following details:

- Routing:** 104.255.152.0/24 via NETMINDERS, CA (AS7040)
- OS:** Microsoft Windows
- Services (17):** 135/DCERPC, 137/NETBIOS, 139/NETBIOS, 445/SMB, 5985/WINRM, 7775/HTTP, 7776/HTTP, 7777/HTTP, 7778/HTTP, 7779/HTTP, 23039/UNKNOWN, 47001/HTTP, 49664/DCERPC, 49665/DCERPC, 49666/DCERPC, 49667/DCERPC, 49668/DCERPC
- Labels:** FILE SHARING

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

HTTP 7775/TCP

Details

<http://104.255.152.61:7775/>

Status 200 HP Http Server OK

HTTP 7776/TCP

Details

<http://104.255.152.61:7776/>

Status 200 HP Http Server OK

HTTP 7777/TCP

Details

<http://104.255.152.61:7777/>

Status 200 HP Http Server OK

HTTP 7778/TCP

Details

<http://104.255.152.61:7778/>

Status 200 HP Http Server OK

HTTP 7779/TCP

Details

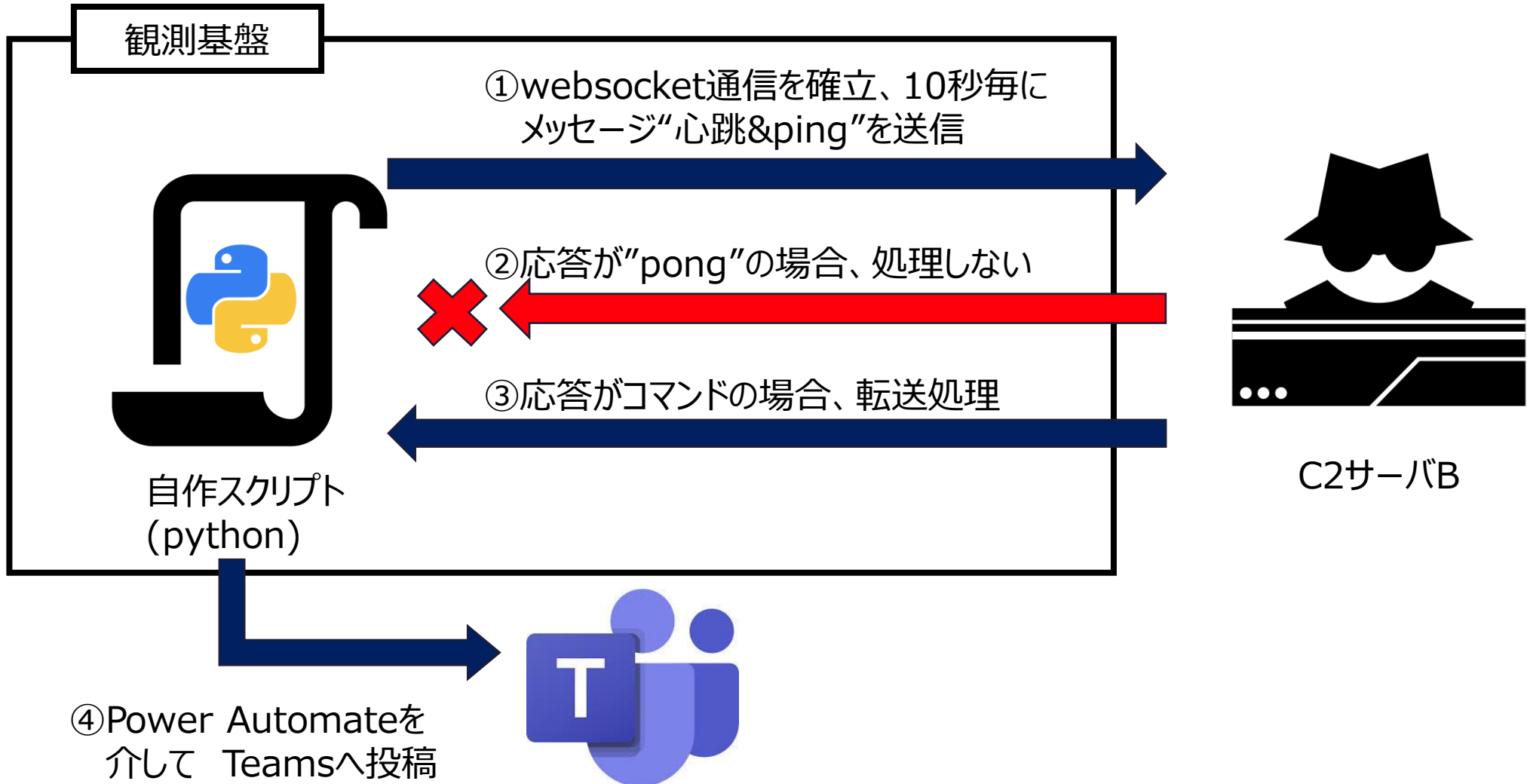
<http://104.255.152.61:7779/>

Status 200 HP Http Server OK

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：

发信息 &09055000000,090... 「重要」広島銀行利用の緊急確認に関するお知らせ。詳細はこちら：<https://t.co/n8rA9fHnWA>

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)：

M通 keepspy注意報

昨日 7:10

本文：「重要」広島銀行利用の緊急確認に関するお知らせ。詳細はこちら：(ポート:7775) 電話番号：090 ,090 090 短
縮URL：https://t.co/n8rA9fHnWA 遷移先：https://liveidc.net/

C2サーバBのポート番号

リダイレクト先

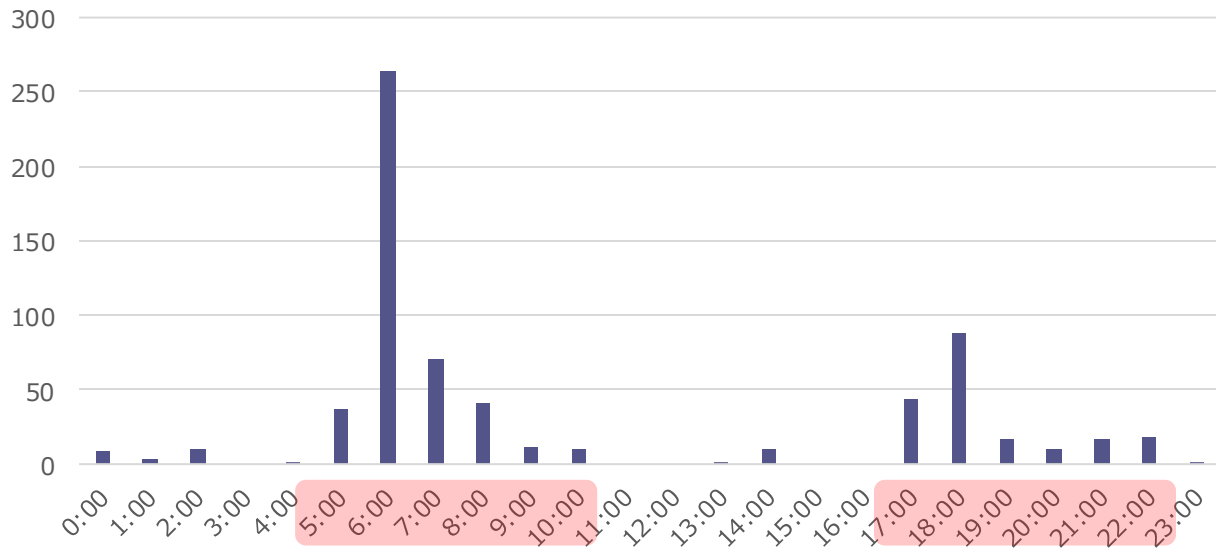
結果

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。

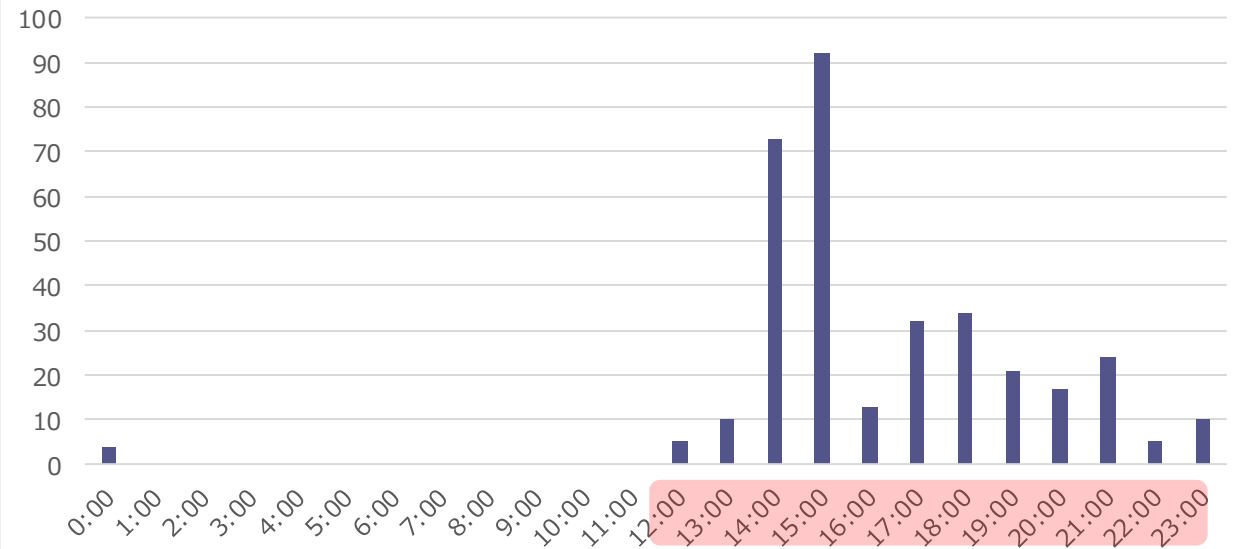
SMSばらまきコマンドの特徴(配布時間帯について)

- 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：午前中に用事を済ませ、午後に休憩しているタイミング？

平日のSMSばらまき時間帯



休日のSMSばらまき時間帯



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。

```
20241212-181514 7778 发信息 090 11111111,090 11111111 【三菱UFJ銀行】お客様の口座の取引を一時的に規制しています、再開手続きをお願いします。 https://t.co/1kgW8Huk6K
20241212-181530 7779 发信息 090 11111111,090 11111111 【三菱UFJ銀行】お客様の口座の取引を一時的に規制しています、再開手続きをお願いします。 https://t.co/PkiFpTGzUR
20241212-181601 7777 发信息 090 11111111,090 11111111 【三菱UFJ銀行】お客様の口座の取引を一時的に規制しています、再開手続きをお願いします。 https://t.co/PkiFpTGzUR
20241212-181616 7776 发信息 090 11111111,090 11111111 【三菱UFJ銀行】お客様の口座の取引を一時的に規制しています、再開手続きをお願いします。 https://t.co/PkiFpTGzUR
20241212-181642 7775 发信息 090 11111111,090 11111111 【三菱UFJ銀行】お客様の口座の取引を一時的に規制しています、再開手続きをお願いします。 https://t.co/KoJR0A9aAf
```

例:12/12(木)：送信されたSMSばらまきコマンド

Public ysl88.com
91.204.226.52 🇰🇷 (Korea) **Potentially Malicious**
Task URL: <https://t.co/KoJR0A9aAf>
Page URL: <https://ysl88.com/>

Public ysl88.com
91.204.226.52 🇰🇷 (Korea) **Potentially Malicious**
Task URL: <https://t.co/PkiFpTGzUR>
Page URL: <https://ysl88.com/>

Public ysl88.com
91.204.226.52 🇰🇷 (Korea) **Potentially Malicious**
Task URL: <https://t.co/1kgW8Huk6K>
Page URL: <https://ysl88.com/>

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

- **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**

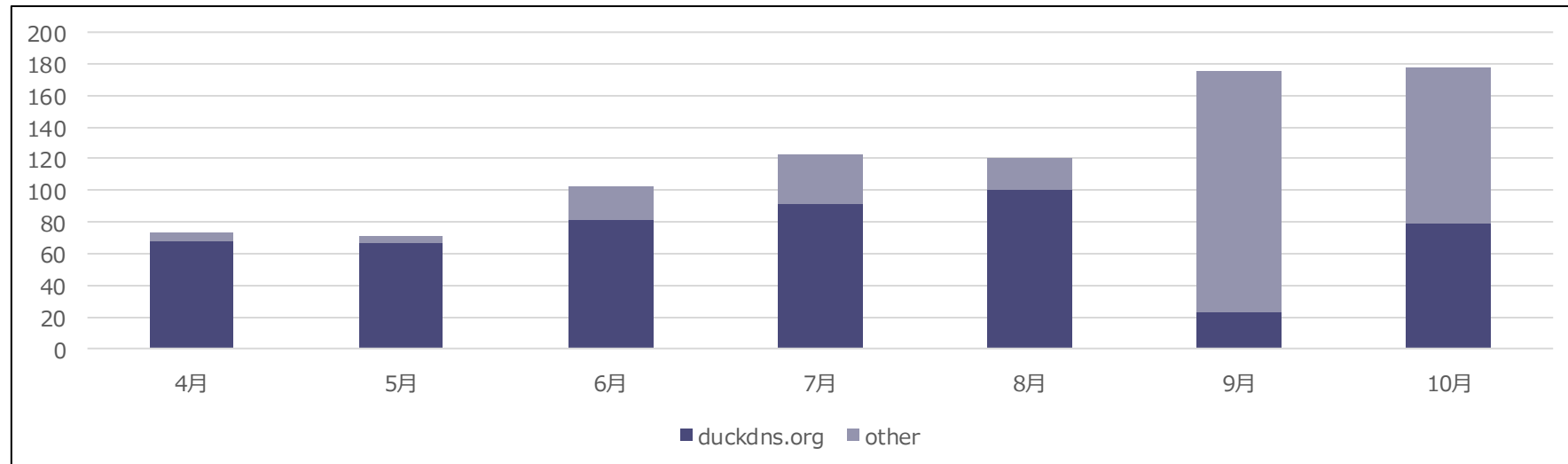
順位	4月(FQDN数)	5月	6月	7月	8月	9月	10月
1位	三菱UFJ銀行(4862)	三菱UFJ銀行(4198)	三菱UFJ銀行(4442)	三菱UFJ銀行(5331)	三菱UFJ銀行(1678)	三菱UFJ銀行(613)	りそな銀行(688)
2位	docomo(1226)	docomo(2663)	みずほ銀行(1884)	TEPCO(53)	北海道銀行(1074)	静岡銀行(16)	三菱UFJ銀行(610)
3位	KDDI(617)	TEPCO(33)	docomo(1076)	東京ガス(5)	りそな銀行(971)	りそな銀行(8)	北國銀行(135)
4位	TEPCO(12)		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に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。

• 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れる。
- 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)

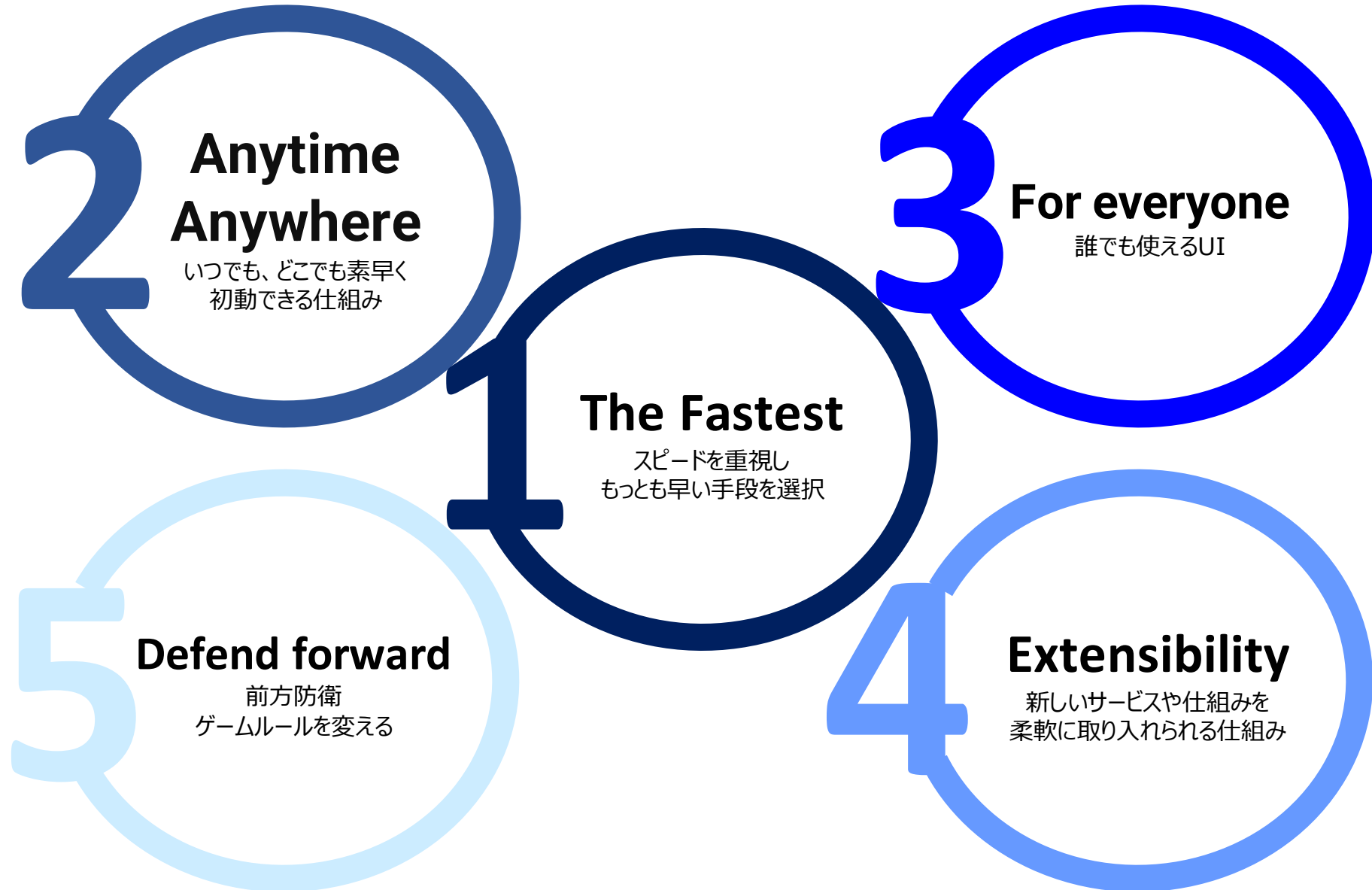
4章_Summary

- 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

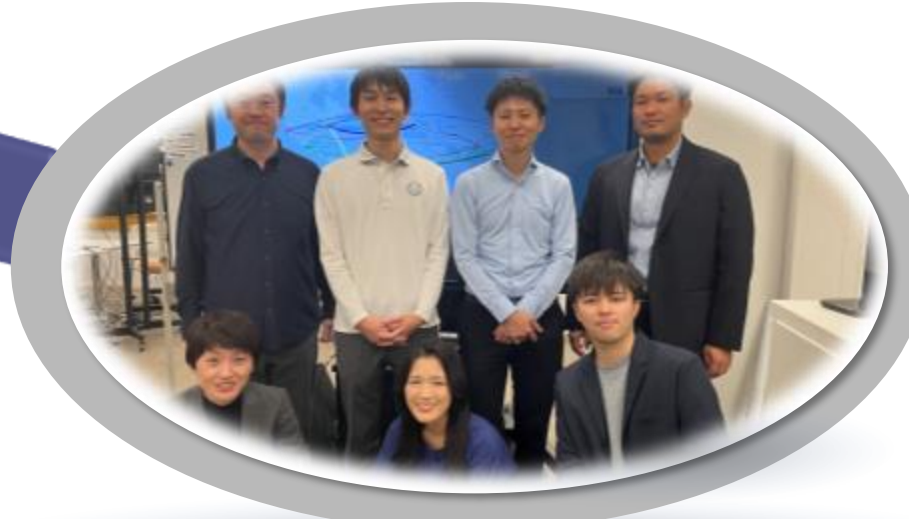
- 月毎のフィッシングサイトの数を集計
- 月毎のサーバ証明書の発行数を集計
- 2024年4月~8月の期間ではDuckDNSが多用されており、発行されるサーバ証明書のSANに複数のFQDNが登録されている。
- この特徴を用いてCTログからフィッシングサイトの早期検知が可能な状態であった。
- 2024年9月~10月の期間ではduckdns.orgのドメインが減少。

6. みずほの自動化の取り組みと今後の方向性について



不正送金班

01



02

Tech班(マルウェア解析)



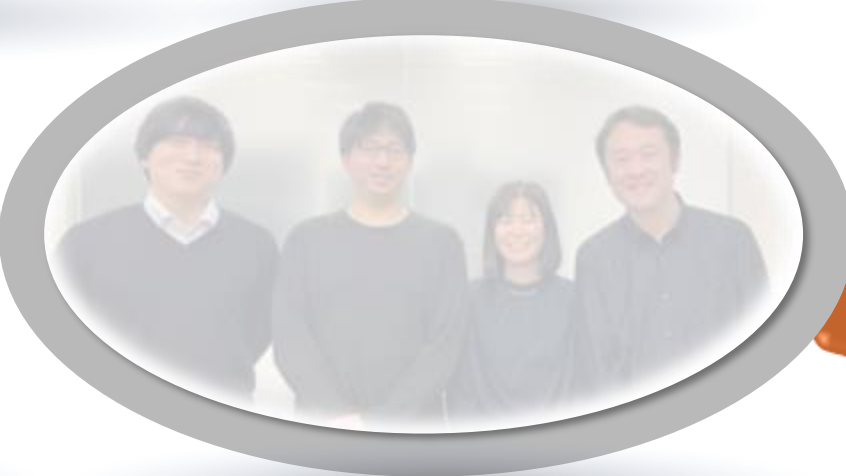
03

開発実装担当



04

自動化推進担当





投稿者: fake_sms

keepsy注意報

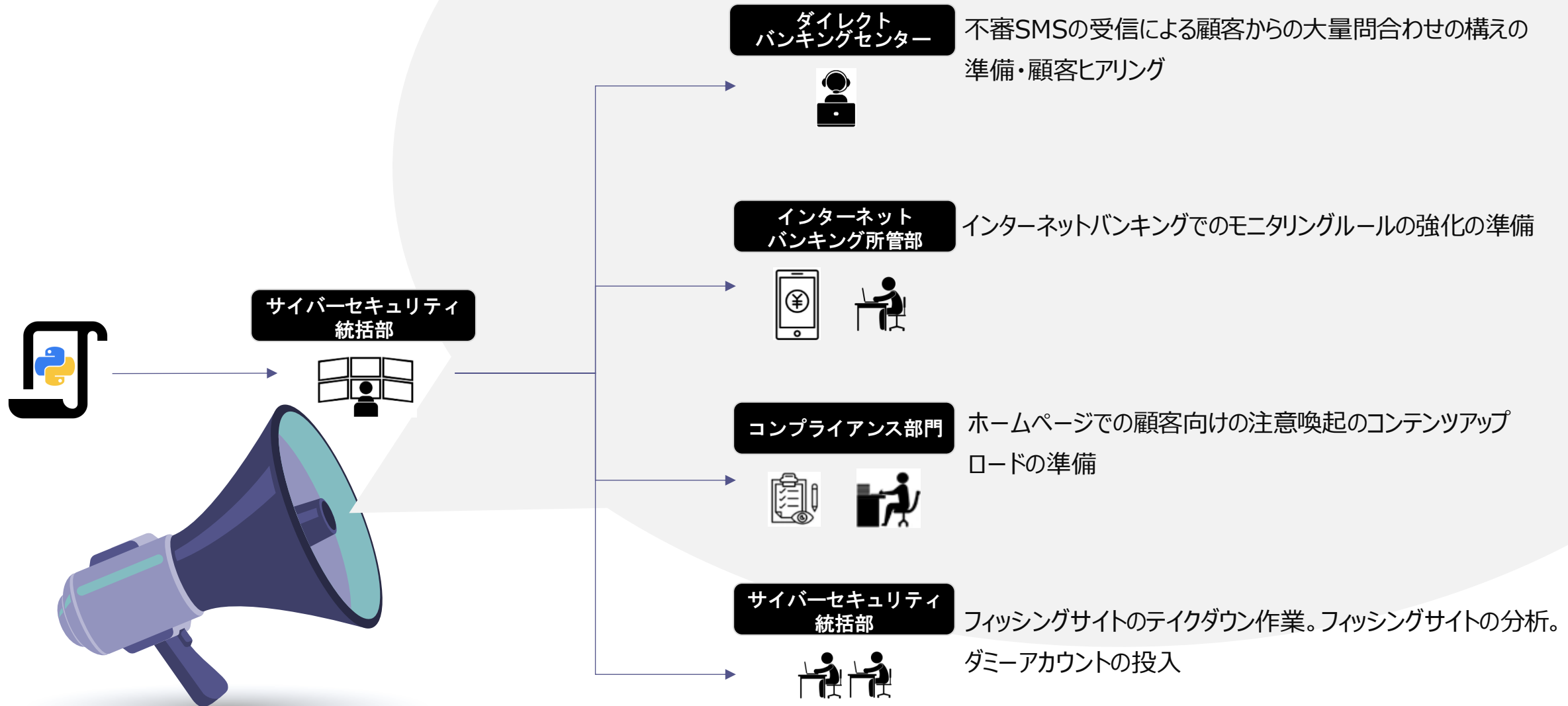
チャンネルに移動

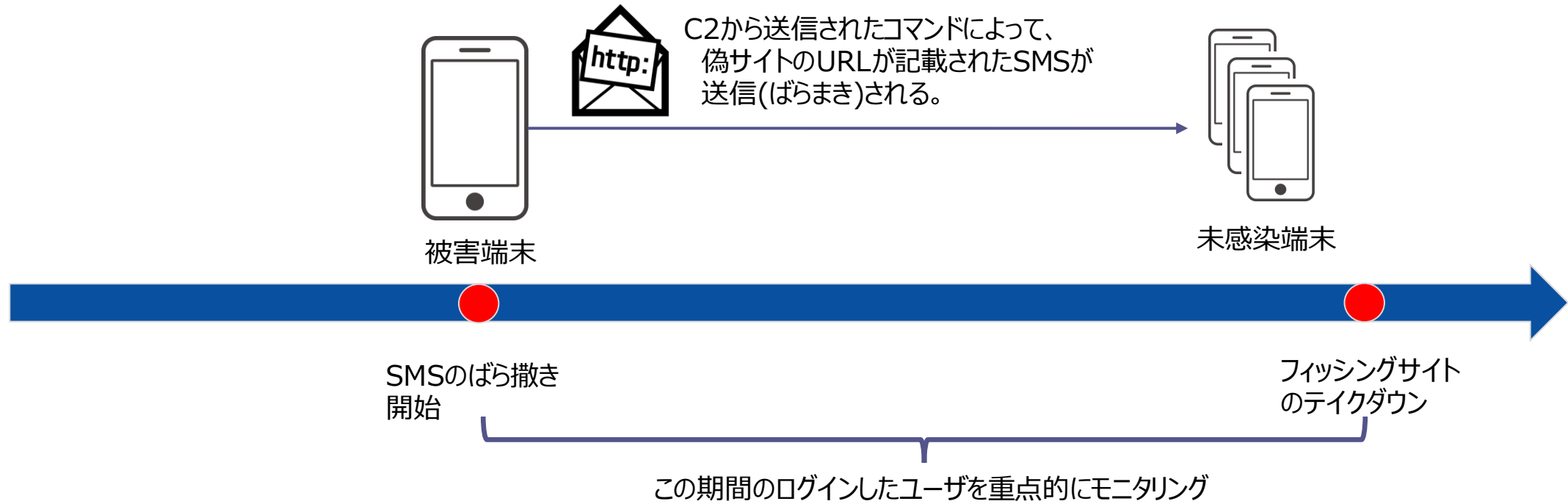


fake_sms 6/22 17:10

『みずほ銀行』お客様の口座の取引における重要な確認について。確認をお願い申し上げます。(ポート7779)
hxxps://3vdl430f.duckdns[.]org/








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






 みずほ銀行 梅本
2023年11月1日 19:33

みずほ銀行 @isnic
webibmizuhobanks.is on hold

 8 


1件の返信   



 yako(mizuho) 2023年11月1日

Registration Certificate  

webibmizuhobanks.is

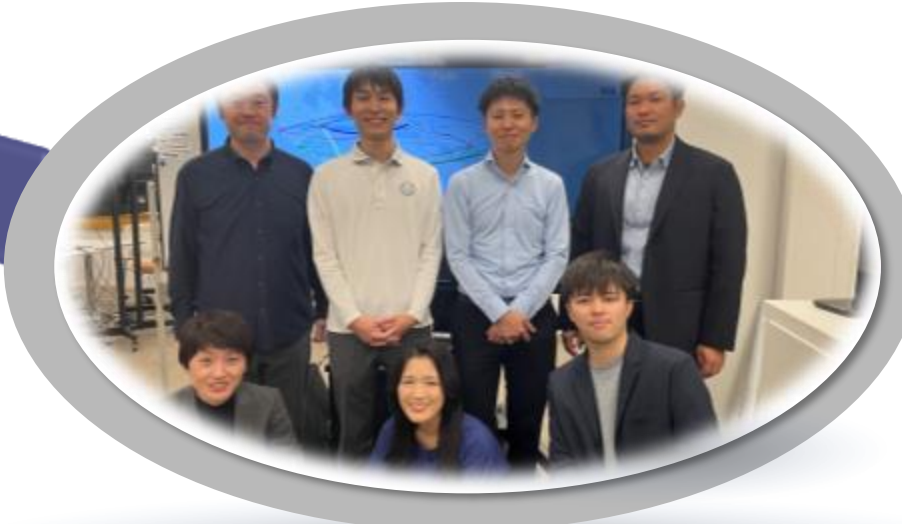
Domain: webibmizuhobanks.is
(This domain is on hold)

Country: FR
Registered: 1. November 2023
Expires on: 1. November 2024
Last change: 1. November 2023
DNSSEC: 
Not signed
Contacts:

 3 

不正送金班

01



02

Tech班(マルウェア解析)



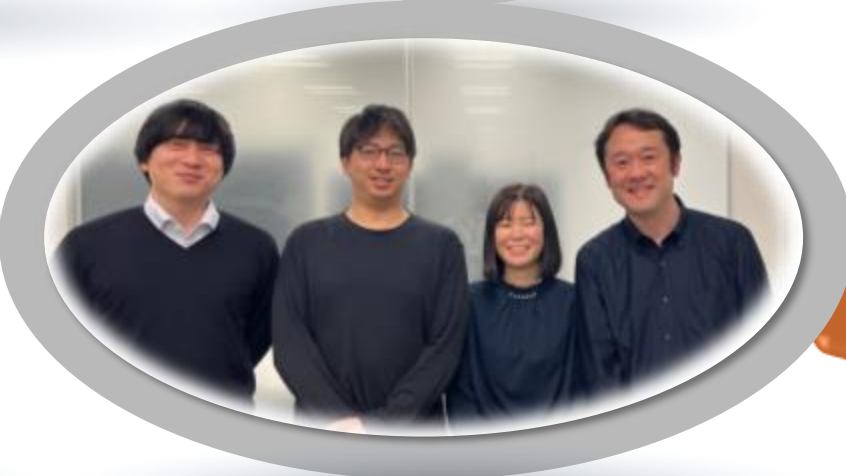
03

開発実装担当



04


自動化推進担当



当日投影のみ

 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

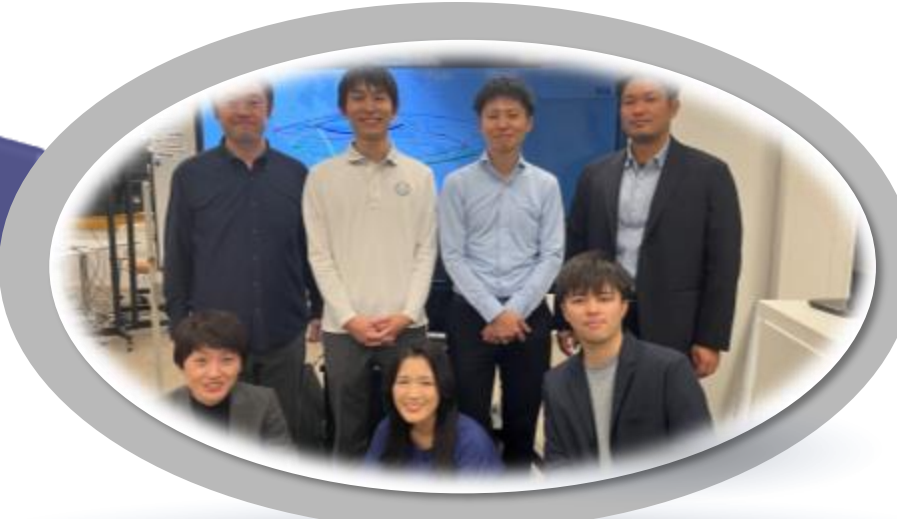
urlscan.ioのAPIでフィッシングサイトの画像が取れるかもしれないんですよ。検証しないとわからないですけど。
もし取れるようになるなら、手動でテイクダウンする前にサイトの画像を取れたら便利じゃないですか？

 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

不正送金班

01



02

Tech班(マルウェア解析)



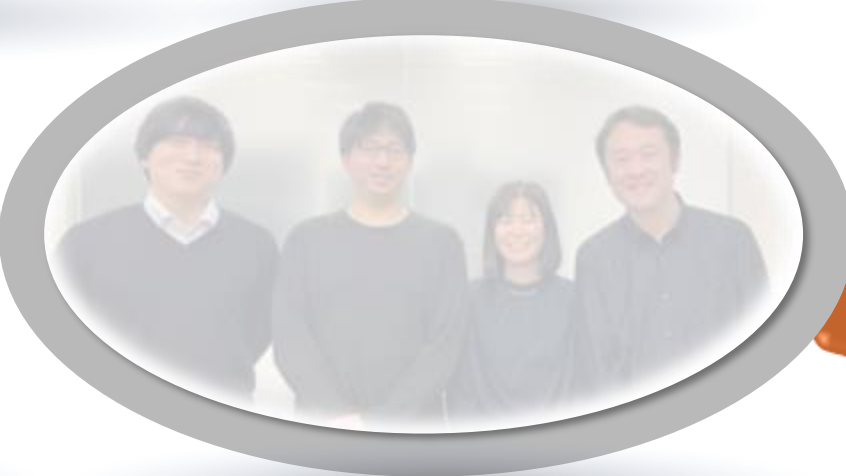
03


開発実装担当



04

自動化推進担当




 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、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あ

 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



Predator
Phishing site Researching data monitor



hiroyuki.yako ▾

[Detail](#) [Reload](#)

Management board

215

Total number of case

215

Total unsupported number

46


Number of registrations this month


0


Number of cases handled

46


Unsupported number

 Report CSV


 Stats Page

 Import File


Meta Data




Actor




Target




Abuse





Tasks









Status

 Bulk Create

 Progress Bar

 New Case

Show 20 ▾

ID	Capture	Case	First seen	Actor	Target	Status	Reported by	Delete
5306		www-uc-co.99kwz.com	2024/11/29		[UCカード]		kasumi.nakano	
5305		michigan-cabin-rental.com	2024/11/29		[オリコカード]		auto	
5304		u5180.com	2024/11/28		[三菱UFJ銀行/MUFG]		masahiro.nishikawa	

Create new Case

×

Required

Case name

Optional

First Seen

Target

GSB

Type Phishing(みずほTarget)
 Unauthorized Use of Trademark(みずほTarget)
 その他
※GSB に申請する場合は申請する Type を選択してください

Ticket 申請しない Ticket が存在しない時に作成
に申請する場合は申請する Type を選択してください

Type Phishing(みずほTarget)
 Unauthorized Use of Trademark(みずほTarget)

URL
 アクセス先の HTML ソースを取得
 アクセス先のスクリーンショットを取得
※自動調査を有効にする場合、アクセス可能な URL を入力してください

FQDN
 FQDN のサーバ証明書を取得
 FQDN から IP 情報を取得
※自動調査を有効にする場合、FQDN 欄に有効な FQDN (xxx.com, yyy.co.jp など) を入力してください

Domain
 ドメインの Whois レコードを検索
※自動調査を有効にする場合、Domain 欄にドメイン名を入力してください

Actor

Survey Log



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. URLScan申請フォーム](#)

< 00. Predator申請フォーム ...

Predator 申請フォーム

Predator に申請するフィッシングURLとTargetを入力してください

こんにちは、浩之。このフォームを送信すると、所有者に名前とメールアドレスが表示されます。

* 必須

1. URL *

URLを複数入力する場合は、URLごとに改行してください

回答を入力してください

2. Target *

答えの選択

送信

Microsoft 365

< 01. GSB申請フォーム ...

GSB申請フォーム

Google Safe Browsing に申請したいフィッシングサイトのURLを入力してください。

こんにちは、浩之。このフォームを送信すると、所有者に名前とメールアドレスが表示されます。

* 必須

1. 申請URL *

- ① URLごとに改行してください
- ② スペースや不要な改行、デファングなどは削除・解除してから入力してください
- ③ 上限を100件前後を目途として、それを超える場合は処理完了後に新たに申請してください
- ④ 10件ずつ処理されるため、件数が多い場合は、申請を分けた方が申請が早くなる場合があります

回答を入力してください

2. 報告サイトの確認

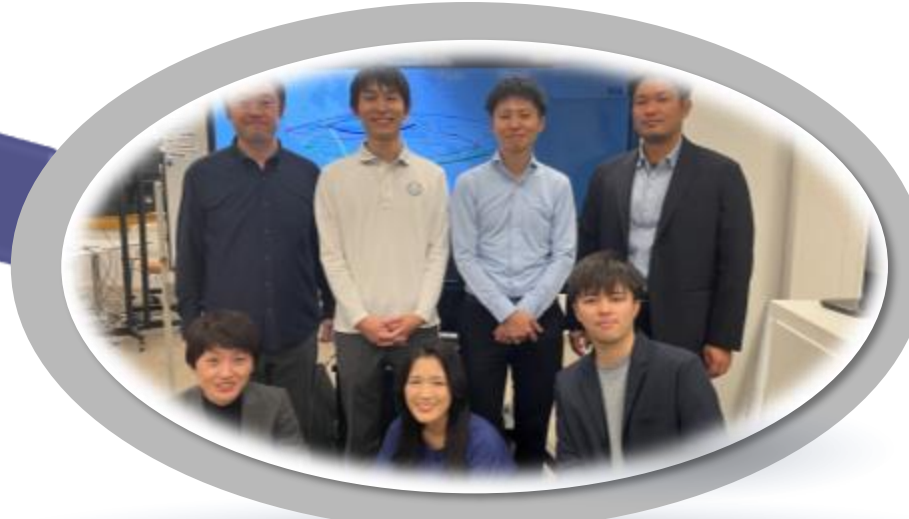
※みずほダイレクト以外のサイトを報告する場合は、以下をチェックしてください。
GSBに申請する文言を切り替えます。

みずほ関連/ログ使用等

当日投影のみ

不正送金班

01



02

Tech班(マルウェア解析)



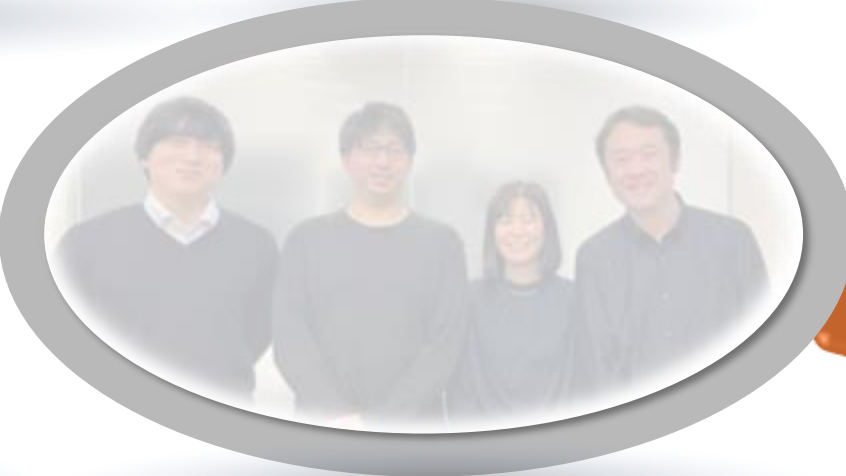
03

開発実装担当



04

自動化推進担当



JSAC2024

January 25-26, 2024

[TIMETABLE →](#)



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put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じた人的な交流、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ます、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

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)