資料１－４

Androidマルウェアによるスミッシングの状況

2024年2月26日

トビラシステムズ株式会社

柘植 悠孝

TOBILA SYSTEMS

2023年10月期末時点

トビラシステムズ会社概要

トビラシステムズ株式会社（東証スタンダード 4441）

トビラシステムズは、特殊詐欺犯罪の被害を0にすることを目指しています

- 社名　トビラシステムズ株式会社*
- 証券コード　東証スタンダード 4441
- 設立年月日　2006年12月1日（**創業 2004年4月1日**）
- 本社所在地　愛知県名古屋市中区錦二丁目5-12
  パシフィックスクエア名古屋錦 7F
- 代表者　代表取締役社長　明田篤（創業者）
- 従業員数　99人（うち技術52人）※2023年10月末時点
- 拠点　**東京**、名古屋

明田　篤　トビラシステムズ株式会社　代表取締役社長

愛知県出身。祖父が原野商法（ほとんど価値のない土地を『別荘地として値上がりする』などと偽って、高額で売りつける商法）にひっかかり、助けたいという思いで、プロダクトを開発。今では、利用者数1,500万人以上。アントレプレナー表彰制度である「EY Entrepreneur Of The Year 2020 Japan」ファイナリスト

*:トビラシステムズ株式会社ホームページ https://tobila.com/

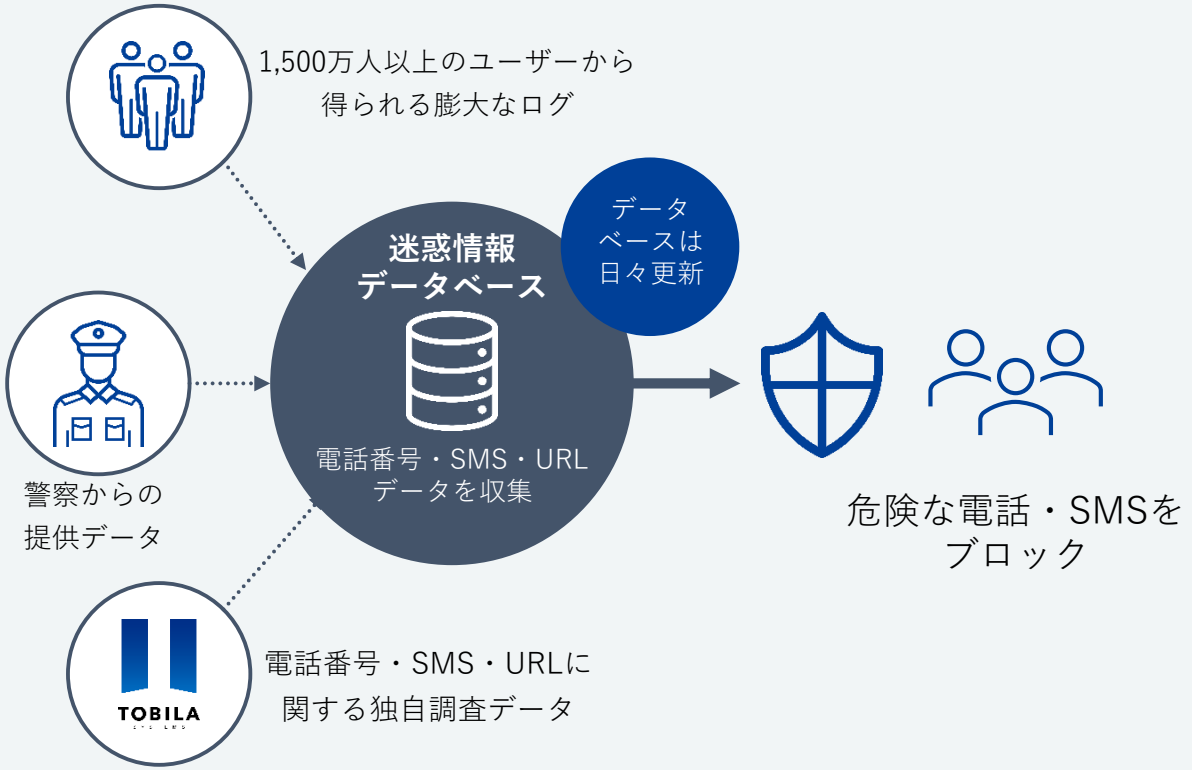
社会課題に向けたアプローチ：「迷惑情報データベース」

- 危険な電話に出てしまう、受信したSMSに反応してしまう、危険なURLを触ってしまうことが被害に合うきっかけとなる
- 電話番号・SMS・URLを収集した「迷惑情報データベース」を日々更新し、危険な電話番号・SMSに記載されているURL等をブラックリスト化することで、当社サービスの利用者を危険から守る仕組みを提供

迷惑情報データベースの強み

- 警察から、犯罪や攻撃に使われたとみられる電話番号・URLのデータ提供を受けていること
- 利用者から電話番号・SMSに関するフィードバックを受けられる体制
- 当社調査チームにより、日々最新のデータが反映

利用者から利用者が多くなるほどデータが蓄積され、データベースの精度が高まる循環システムを確立



迷惑情報フィルタ事業のサービス内容

- 迷惑情報データベースを活用し、「モバイル向け」・「固定電話向け」・「ビジネスフォン向け」に展開
- 電話を全方位からカバーしており、迷惑情報データベースの月間利用者数は1,500万人以上

モバイル向け

あんしんセキュリティ

auブロック

280 blocker

- 主に通信キャリアのアプリとして提供
- 迷惑電話、迷惑SMSをブロック
- 不快な広告をブロック

固定電話向け

コミュファ光

eo光 HIKARI

auひかり

ケーブルプラス

- 外付け型、機器内蔵、ネットワーク網まで様々なタイプでサービス展開
- 不要な営業電話や詐欺電話をブロック

ビジネスフォン向け

トビラフォン Biz

トビラフォン Cloud

Talk Book

- 法人向けサービス
- 電話業務の効率化やDXを促進

アジェンダ

- 会社概要

1. 国内SMSフィルタリングの2レイヤー

2. スミッシングと不正送金被害の状況

3. スミッシングにおける送信元

- Androidマルウェアによるばらまきの割合
- iOSのマルウェア

4. Androidマルウェア

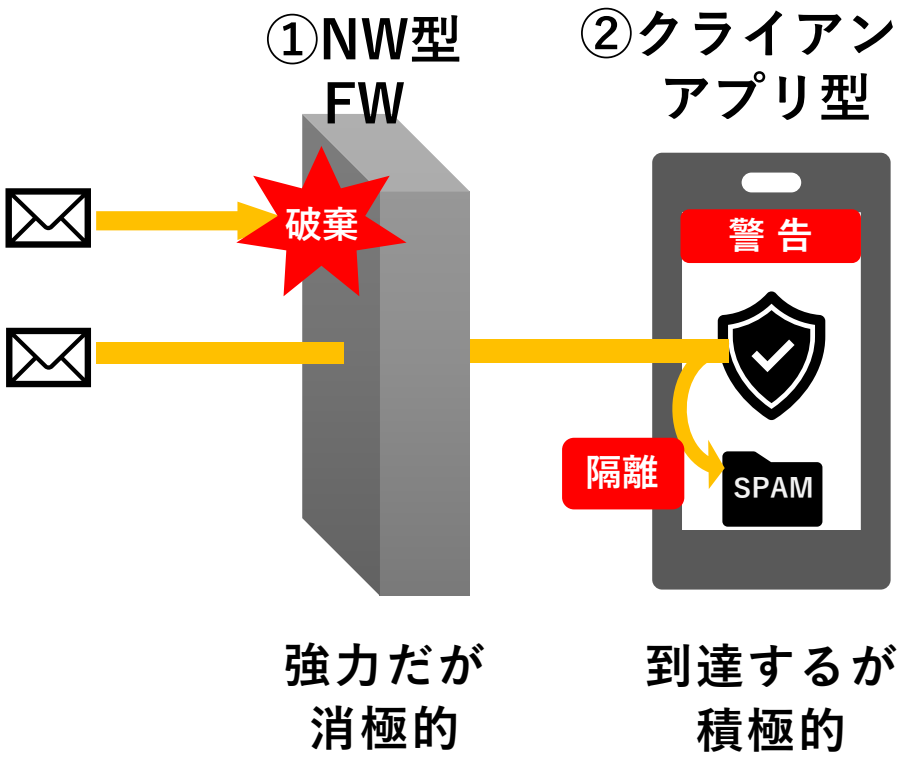
- 2大Androidマルウェア
- インストールの流れ
- 初回起動時の権限取得
- ばらまき時間の傾向

5. 詐欺SMSモニター

- Appendix

1. 国内SMSフィルタリングの２レイヤー

現状の国内のSMSフィルタリングは
NW型とクライアントアプリ型の２つのレイヤーでの防御



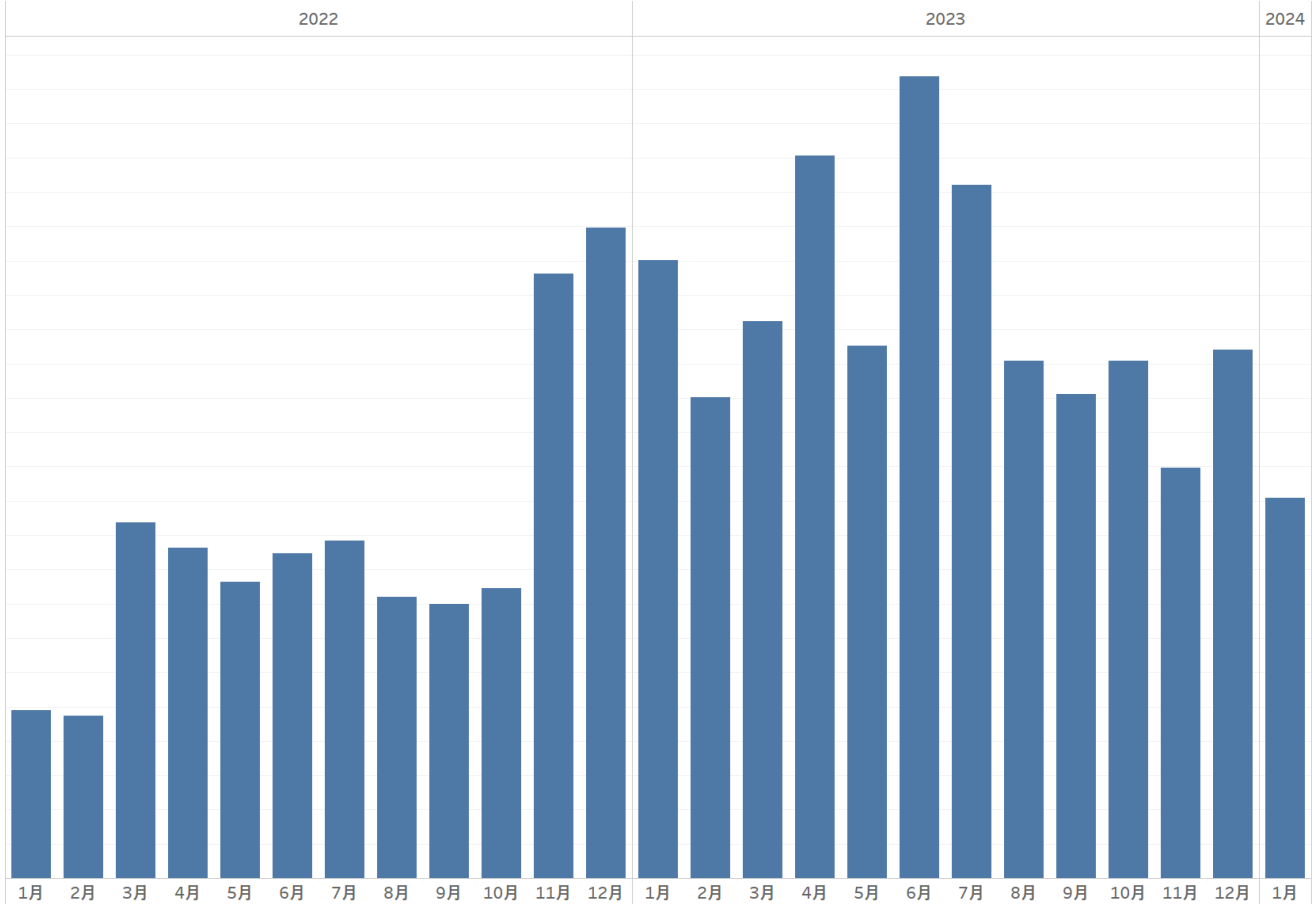
	フィルター動作	特徴
①NW型	破棄 端末に届かない	フィルターされたSMSをユーザーが確認できないため、誤検知影響は大きい
②クライアントアプリ型	警告または隔離 端末に届く	フィルターされたSMSでもユーザーが確認できるため、誤検知影響は小さい

本資料のデータはクライアントアプリ利用者
(SoftBank, au, docomo)のSMSログに基づくもの

2. スミッシングと不正送金被害の状況

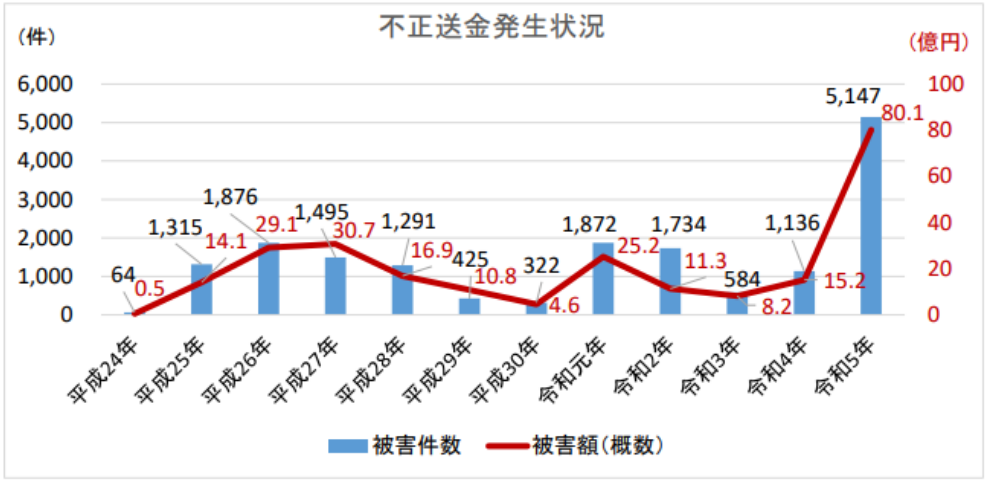
2022年11月からスミッシングが大幅に増加
2023年はフィッシング起因の可能性のある不正送金被害が急増

月ごとのスミッシング件数推移



2022年1月～2024年1月の当社サービス利用者のSMSデータより（実数非開示）

スミッシングによるものが全てとは言えないが
2023年（令和5年）は被害件数・被害額ともに5倍近くに増加



R5.12.25 警察庁・金融庁
フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（注意喚起）
https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf

Androidマルウェアによるばらまきの割合

当社の観測するスミッシングの9割以上はAndroidマルウェアによるばらまきSMS

送信元	割合	ブランド	文例
Androidマルウェア感染疑い携帯電話番号 約99.6%	56.3%	宅配事業者	お荷物のお届けに参りましたが、お留守でしたので、別の日に再配達します。hxxps://t[.]co/VISNI7X4fi
			お荷物のお届けに伺いましたが、ご不在でしたので、後日再度お伺いします。hxxps://t[.]co/hGchp8ko9s
			お荷物をお届けしようとした際、ご不在でしたので、後日再度お伺いします。hxxps://t[.]co/CNUTcweEaC
			お荷物をお届けしようとしましたが、ご在宅されていないため、保管いたしました。hxxps://t[.]co/I9VQxLSMrq
			お荷物をお届けに参りましたが、お留守でしたので、保管しています。hxxps://t[.]co/bTkHMI9ubP
			お客様がご不在でしたので、荷物を営業所に保管しています。hxxps://t[.]co/reOD7h28Cd
			お客様のご不在のため、荷物を指定の場所に保管しました。hxxps://t[.]co/ENNwbh8yOO
			お届けしようとした荷物がありますが、ご不在のため、後日お届けします。hxxps://t[.]co/b21m1jp0v6
			お届けに参りましたが、お客様がご不在でしたので、荷物を一時保管しています。hxxps://t[.]co/zyeSurkIsO
			お届け先でお客様をお見かけできず、荷物を持ち帰りました。hxxps://t[.]co/itovlpEhxc
			ご在宅を確認できず、荷物を持ち帰りました。後ほどお問い合わせください。hxxps://t[.]co/Ufdqfim5At
			ご不在でお受け取りができなかったため、荷物を局で保管しています。hxxps://t[.]co/su3jPGhB1u
			ご不在のため、お荷物を一時的に保管いたします。再配達をご希望の場合はご連絡ください。hxxps://t[.]co/vt9wXe0oof
			ご不在時の荷物は、再配達をご希望の場合はご連絡をお願いします。hxxps://t[.]co/zGJAUfnW7r
			配達に伺いましたが、ご不在だったため、荷物を局に戻しています。hxxps://t[.]co/iAMMFMFK7N
			配達の際、ご不在でしたので、荷物は安全な場所に保管しております。hxxps://t[.]co/jWyGEmlUU6
			配達時、お客様がお出かけ中でしたので、荷物を局に戻しました。hxxps://t[.]co/zzbodQpROJ
			配達時にお会いできなかったため、お荷物をセンターに戻しました。hxxps://t[.]co/U3WLnsqwjN
			本日、お荷物をお届けしようとしましたが、ご不在のため、持ち帰りました。hxxps://t[.]co/z2ynAXURUy
			本日、お客様がご不在だったため、荷物を営業所に持ち帰りました。hxxps://t[.]co/binxUIqK4N
	43.1%	SoftBank	[SoftBank]重要な情報、ご注意ください。hxxps://t[.]co/AtuML5C0x9
			[SoftBank]お読みください。重要なお知らせ。hxxps://t[.]co/vlUteP61u0
			[ソフトバンク]重要な情報、ご注意ください。hxxps://t[.]co/ihxeSphNIJ
			[ソフトバンク]お読みください。重要なお知らせ。hxxps://t[.]co/fXugLVdwqK
	0.005%	au	【重要なお知らせ】auサービスUua/vhr-18が制限されています。ご確認ください：hxxp://hqcig[.]aodx[.]cc
	0.18%	三菱UFJ銀行	三菱UFJ銀行お客様の銀行口座の取引を一時的に制限しています、ご確認が必要ですhxxps://entry11-bk[.]mufj-jp[.]is/
	0.005%	イオン銀行	イオン銀行、お客様の口座ご利用を一時停止しております、本人確認手続きをお願いします。hxxps://aeonabank[.]jp
数字列	0.35%	メルカリ	ご本人確認の手続きをお願いします。そうでないとアカウントが停止されます。hxxps://mercoai[.]infoメルカリ
ブランド名称文字列	0.005%	楽天カード	「楽天e-NAVI」不正利用，時間内に更新してください。hxxps://www-rakutan[.]com/

※2024年1月31日のデータを集計　宅配事業者騙りの文例は非常に多いため一部を抜粋して記載

3. スミッシングにおける送信元

iOSのマルウェア

iOSアプリを用いたスミッシングは現時点では流行していないと思われる

iOSの仕様上、ユーザーの操作なしにSMSを送信する機能が公開されていないため
Androidのように、バックグラウンドでSMSを大量にばらまくアプリを開発できない。
そのためスミッシングのSMSばらまきの手段としては、iOSは対象にはされていないと思われる。

ただし、
最終的にアプリをインストールさせるものであるかは不明だが、
構成プロファイルのインストールに誘導し、
端末になんらかの害を及ぼす恐れのある攻撃を確認したことはある

SMS文例（2023年10月17日）

ローンの審査が承認されました。クリックしてローンを申請してください
hxxps://jp[.]btseloan[.]com

2大Androidマルウェア

現状2つのAndroidマルウェアによる攻撃が主流

①Moqhao(XLOADER)

ご不在のため荷物を営業所で保管しています。
受け取り日時をご指定下さい。hxxps://t[.]co/
●●●●●●●●●●

iOS -> Apple騙りフィッシング
Android -> マルウェアインストール誘導

②KeepSpy

・12月22日～2024年1月23日

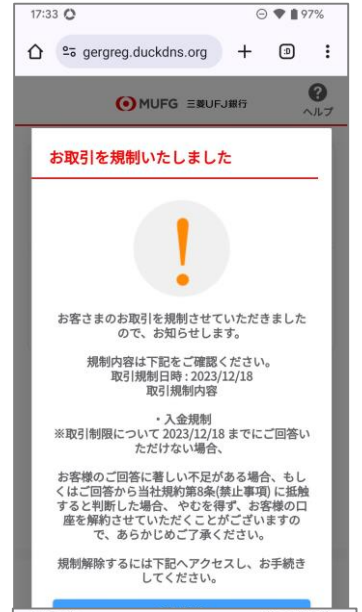
『三菱UFJ銀行』お知らせ - お客様の口座の取引における重要な確認について。ご確認ください。hxxps://t[.]co/●●●●●●●●●●

iOS,Androidともに
三菱UFJ銀行騙りのフィッシング

・2024年1月26日～

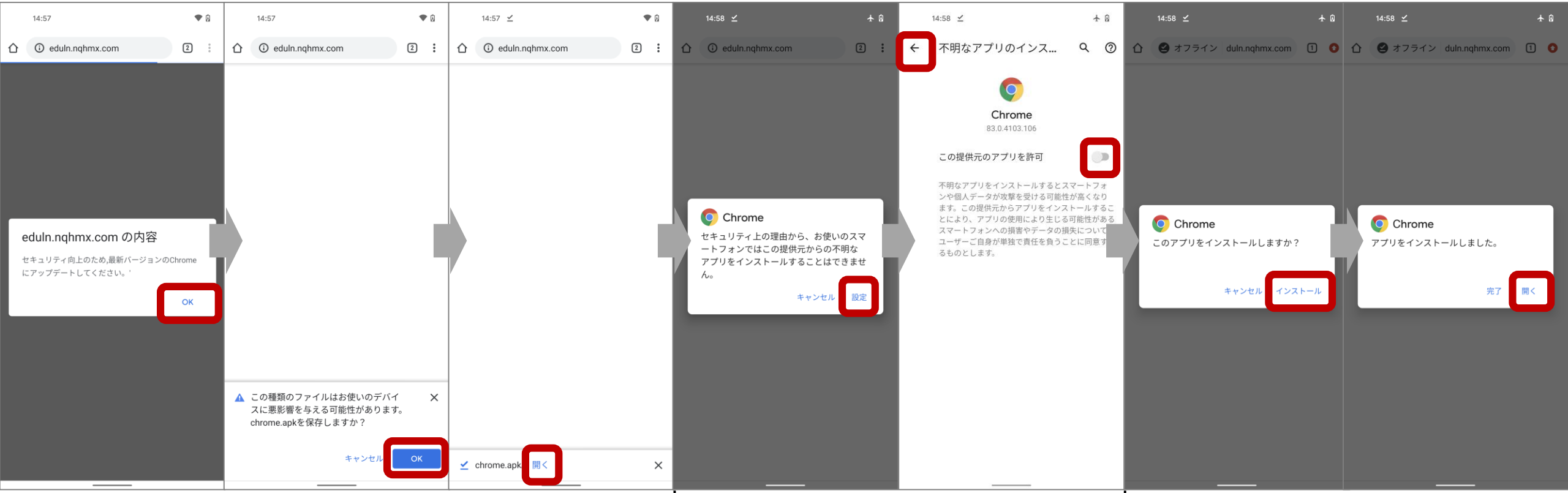
【ソフトバンク】お読みください。重要なお知らせ。hxxps://t[.]co/●●●●●●●●●●

iOS -> SoftBank騙り架空請求サイト
（Vプリカ4万円請求）
Android -> マルウェアインストール誘導



インストールの流れ

Moqhao(XLOADER)の例
Chromeブラウザを装うマルウェアをインストールさせる



過去にONに設定済みの場合はこの2画面分のステップは不要

初回起動時の権限取得

Moqhao(XLOADER)の例　初回起動時に各種権限を取得
攻撃者の指令によって同種のSMSをばらまくボットとなる

ばらまき時間の傾向

2023年12月度の日ごとのスミッシングの発生傾向

5. 詐欺SMSモニターについて

一般ユーザー向け注意喚起・啓発目的のWebサイトを制作
サイバーセキュリティ月間に合わせて限定公開(2024/2/1 – 3/18)

Androidマルウェアを始めとしたスミッシングの情報をいち早く確認可能

①詐欺SMS件数のリアルタイムグラフ
ばらまきが発生しやすい、警戒すべき時間の傾向を可視化
一般のユーザーには見えにくいばらまきの波を伝える

②Androidマルウェア感染端末台数
ログ傾向をもとに、当社で観測するかぎりのマルウェア感染が疑われる台数を掲載

③知っていますか？
スミッシング送信者の多くは被害者（マルウェア感染者）であるということや、マルウェア感染手口についてコンテンツ化

④詐欺SMSギャラリー
最近のスミッシング文例

https://smon.tobila.com

Appendix

その他参考データ

生成AI活用？

12/25のMoqhaoのばらまきSMS 47種

クリスマスの宅配便不在連絡

明日、再配達を行う予定ですのでご在宅をお願いします。hxxps://t[.]co/ETLTOE3gNI

クリスマスプレゼントが明日になってしまう！
とあわててURLにアクセスしてしまう人も？

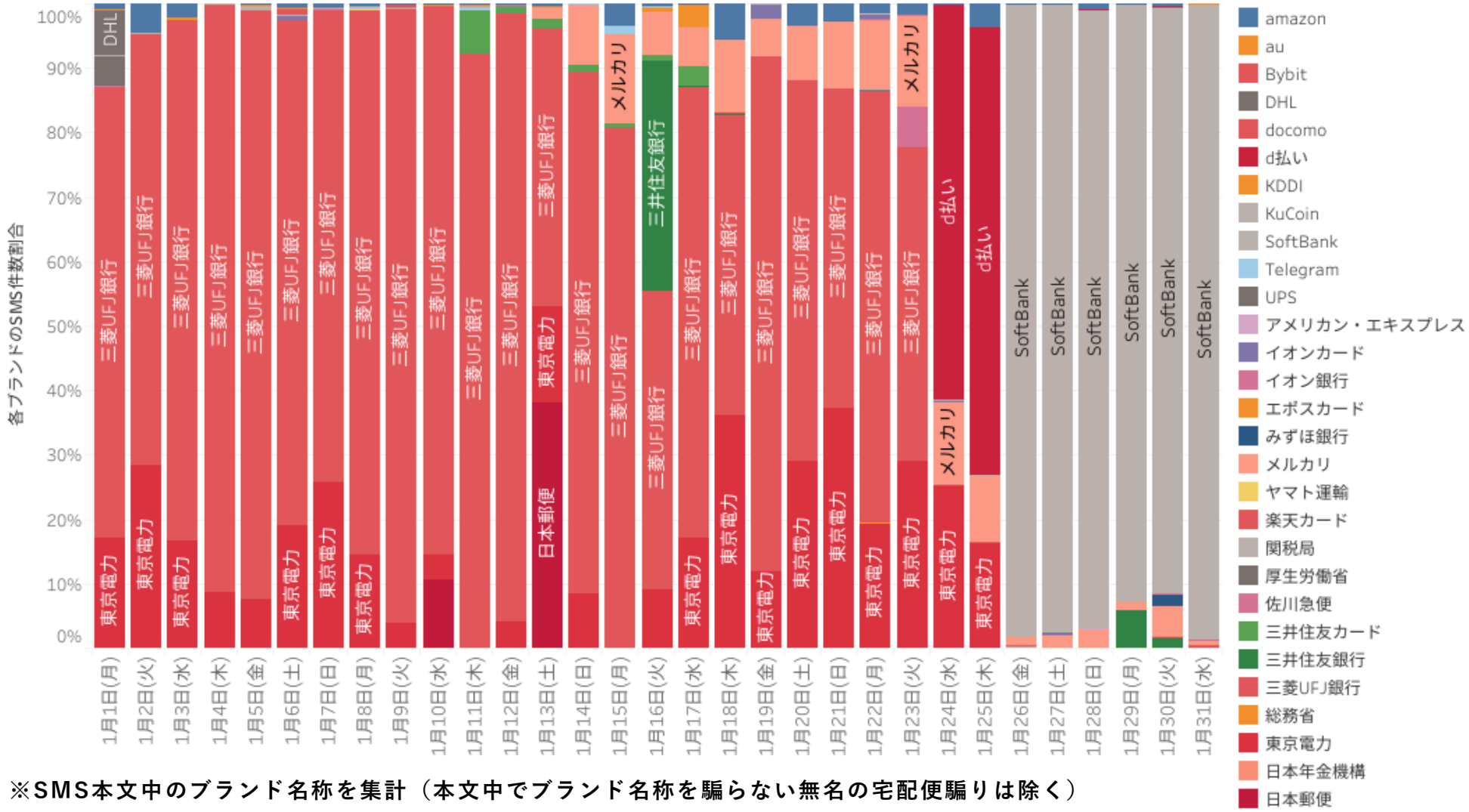
ここ最近（10/26～）は1日あたり数十種類の文種がほぼ毎日重複なく送信されている

これを人間が毎日作り続けられるか・・・
生成AI活用？

お荷物の受け取りができなかったことをお知らせいたします。hxxps://t[.]co/rxwMXzM4SZ
お荷物の受け取りができなかったため、ご連絡をお待ちしております。hxxps://t[.]co/eRx8rDoPc5
お荷物は一時的に配送センターに戻されました。hxxps://t[.]co/7QTXIEoyio
お荷物は最寄りの郵便局に保管しております。hxxps://t[.]co/M7c4JdVMeI
お荷物をお持ちしましたが、ご在宅を確認できなかったため、後日再配達とさせていただきます。hxxps://t[.]co/uaCTCf6KHR
お荷物をお届けに上がりましたが、ご不在のため、再配達の手配をお願いいたします。hxxps://t[.]co/GFfQqkgcxZ
お客様がお出かけ中のため、配達予定の荷物を持ち帰りました。hxxps://t[.]co/qHKnjpu0SG
お客様がご在宅でなかったため、荷物を一時保管しています。hxxps://t[.]co/US14guGIpW
お客様がご自宅にいらっしゃらないため、荷物は当社にてお預かりしております。hxxps://t[.]co/YJLP7QKUkt
お客様がご自宅にいらっしゃらなかったため、荷物を後日に再配達いたします。hxxps://t[.]co/3F7cRz5VnO
お客様がご不在のため、本日の配達は延期となりました。hxxps://t[.]co/QMvzT9utIu
お客様が不在のため、荷物は一時的に当店でお預かりしております。hxxps://t[.]co/VyyggB5apK
お客様のご都合により、今日の荷物のお届けはできませんでした。hxxps://t[.]co/CmIfdNo8wi
お客様の荷物を指定の場所に配達済みです。ご確認をお願いします。hxxps://t[.]co/bIOauhopCU
お届けしようとしましたが、お客様がご不在のため、後日改めてお届けします。hxxps://t[.]co/Y5hc3e2Cvc
お届けに上がりましたが、ご不在でしたので後ほど再配達いたします。hxxps://t[.]co/s1sE6UImPR
お届け先に伺いましたが、お客様が不在でしたので、荷物は当社で保管しています。hxxps://t[.]co/YcIcXc3GBW
お届け先に到着しましたが、お客様がいらっしゃらなかったので、荷物を保管いたします。hxxps://t[.]co/1OkCQJHEaD
お届け先に到着しましたが、お客様がご不在だったため、荷物は保管いたします。hxxps://t[.]co/wWTfNt3wE7
お届け予定の荷物がございましたが、ご不在でしたので、後日に配達いたします。hxxps://t[.]co/KqbAb4wXVF
ご在宅を確認できなかったため、荷物を配送センターに保管しています。hxxps://t[.]co/jYXyHCq0Zm
ご指定いただいた場所にお荷物をお届けいたしました。ご確認ください。hxxps://t[.]co/kR2RBv9CTE
ご指定の時間にお伺いしましたが、お客様が不在だったため、荷物を保管します。hxxps://t[.]co/KdCbIwBqVc
ご指定の時間にお伺いしましたが、お客様が不在でしたので、荷物を持ち帰ります。hxxps://t[.]co/PMjq2MfZIu
ご指定の住所にお伺いしましたが、お会いすることができませんでした。hxxps://t[.]co/CibQjDonV4
ご指定の日時に配達に伺いましたが、お客様が不在でしたので、後日に改めます。hxxps://t[.]co/pLotZvmpsk
ご自宅に荷物をお届けしに上がりましたが、ご不在だったため、後日再配達します。hxxps://t[.]co/x2BmITYE9P
ご自宅に荷物をお届けしようとしましたが、お客様が不在だったため、保管します。hxxps://t[.]co/1VmFvOUzx2
ご自宅に伺いましたが、ご不在のため、荷物は後日に改めてお届けします。hxxps://t[.]co/tBVGrwImHs
ご不在のため、お荷物を近隣のコンビニエンスストアに預けています。hxxps://t[.]co/qWB1xvsuH7
ご不在の際にお荷物をお届けしましたので、再配達のご依頼をお待ちしております。hxxps://t[.]co/MKyfDHZayK
ご不在の際にお届けした荷物は、後日に再配達いたします。hxxps://t[.]co/F1Y0v3PEJY
ご不在の際に配達に伺いましたが、荷物を保管しております。hxxps://t[.]co/hCEJCoZtW0
再配達のご希望日時をお知らせください。hxxps://t[.]co/94wAo2hzta
配送ドライバーが訪問しましたが、応答がありませんでした。hxxps://t[.]co/hwO6ixss3j
配送の際にご在宅を確認できず、お荷物を持ち帰りました。hxxps://t[.]co/4yeK02skBr
配達に伺いましたが、お客様がご不在でしたので、荷物を持ち帰ります。hxxps://t[.]co/ubQDmn6397
配達に伺いましたが、お客様が不在でしたので、荷物は当店でお待ちしております。hxxps://t[.]co/d2Ru3w9RrV
配達に伺いましたが、ご不在でしたので、荷物は当店に戻りました。hxxps://t[.]co/skPu8o5Ouk
配達予定日時にご不在でしたので、配達を保留しております。hxxps://t[.]co/TNKgI59sNO
不在票をポストに入れましたので、お手数ですがご確認ください。hxxps://t[.]co/qQ4jouZVCJ
本日の配達が不可能でした。再配達のご要望を承ります。hxxps://t[.]co/vAyLuKm5L0
本日の配達は、お客様のご都合で持ち帰りとなりました。hxxps://t[.]co/IhzmmV5u4s
本日の配達はご不在のため、明日に再配達を予定しております。hxxps://t[.]co/aURp49S4CE
本日はお会いできず、荷物を持ち帰りました。再配達のご依頼をお願いいたします。hxxps://t[.]co/ZcZjMQMQLU
明日、もう一度お届けに伺いますのでご在宅をお願いいたします。hxxps://t[.]co/XMex46SVga
明日、再配達を行う予定ですのでご在宅をお願いします。hxxps://t[.]co/ETLTOE3gNI

日ごとブランド割合

2024年1月度の日ごとスミッシングのターゲットブランド割合



※SMS本文中のブランド名称を集計（本文中でブランド名称を騙らない無名の宅配便騙りは除く）

EOF