C25 従来の攻撃プラットフォームがモバイルに変わりつつある現状と要因について

北崎 恵凡
JPAAWG / ソフトバンク株式会社

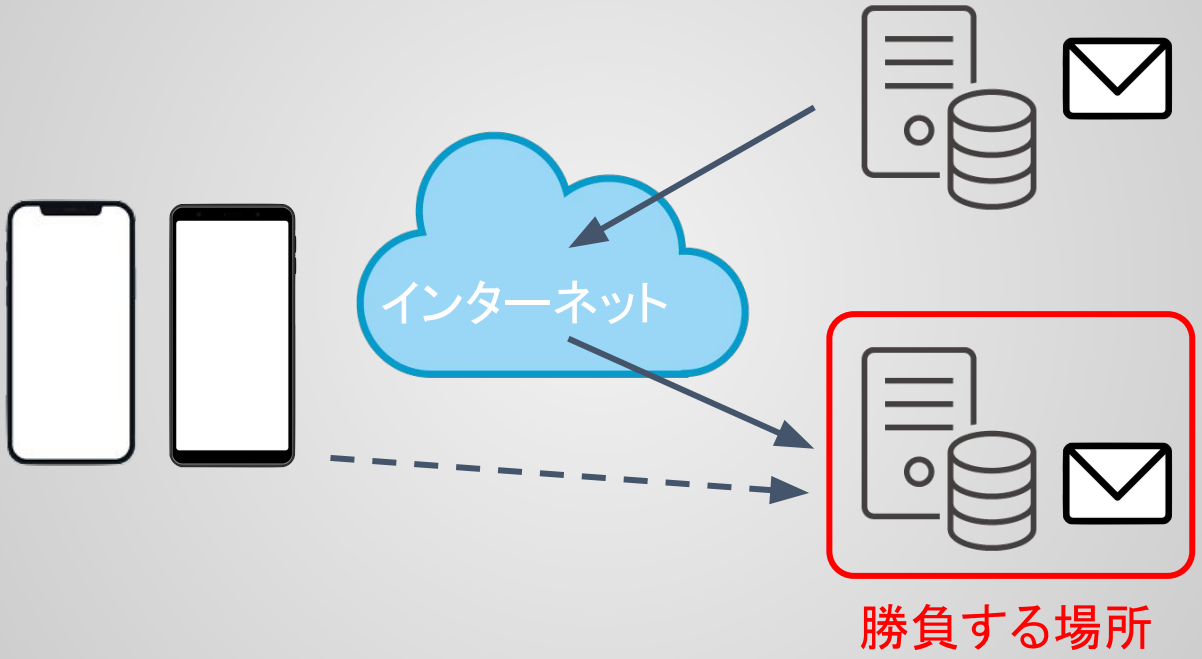
以前は.. Emotet（エモテット）

特徴
・EメールのURLリンク、添付ファイルで感染
・C&C通信でBotネットを構築
・Eメールでマルウェアを配信

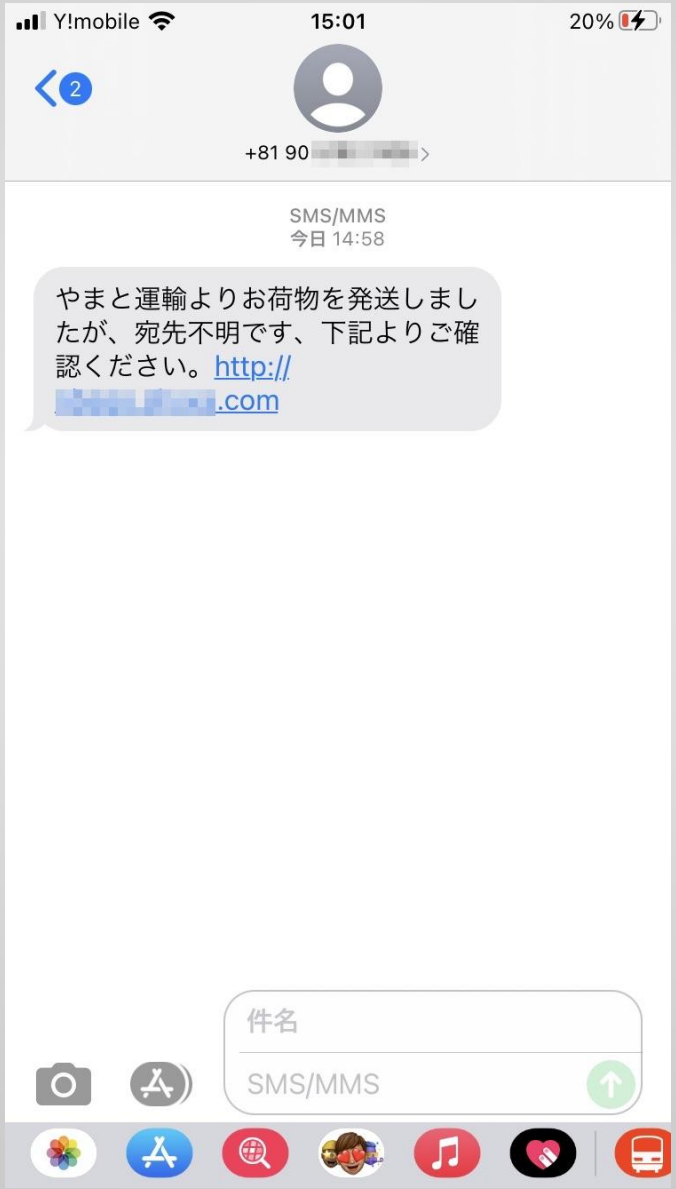
「Emotetのテイクダウン（停止措置）について」
2021年1月27日　EUROPOLによる攻撃基盤の停止
2021年4月25日　機能停止（ほぼ観測されていない）

引用元　https://www.ipa.go.jp/security/announce/20191202.html

以前は..



SMSフィッシング (SMiShing、スミッシング)



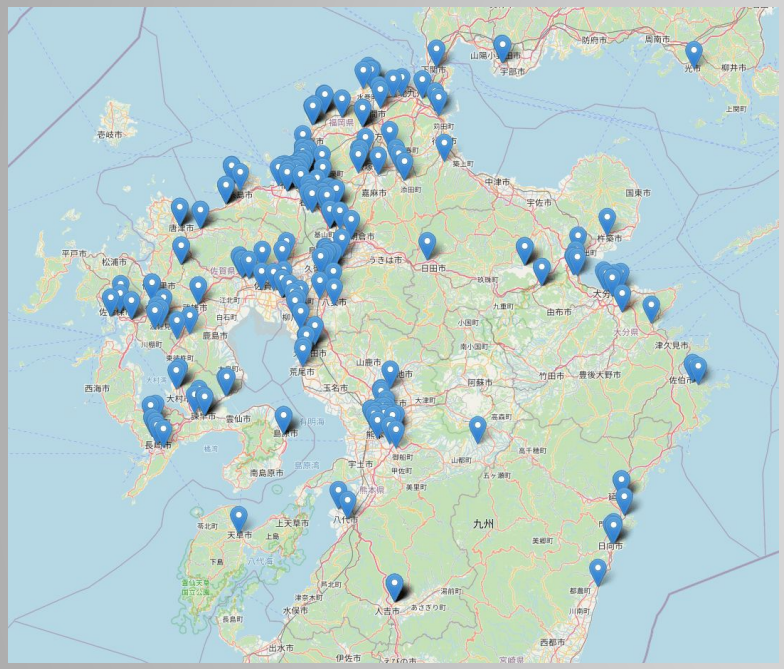
MoqHao（モクハオ）

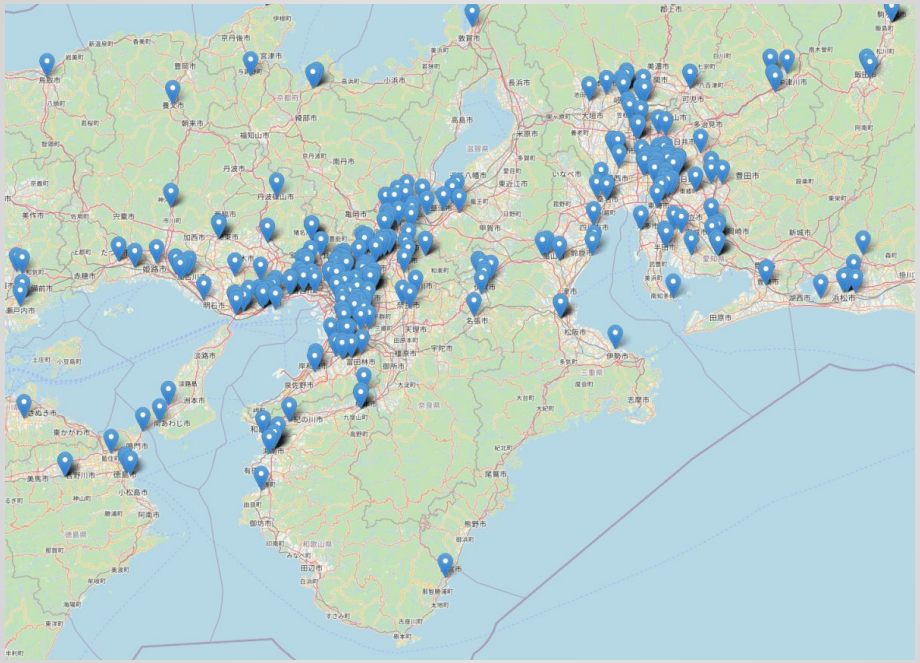
特徴

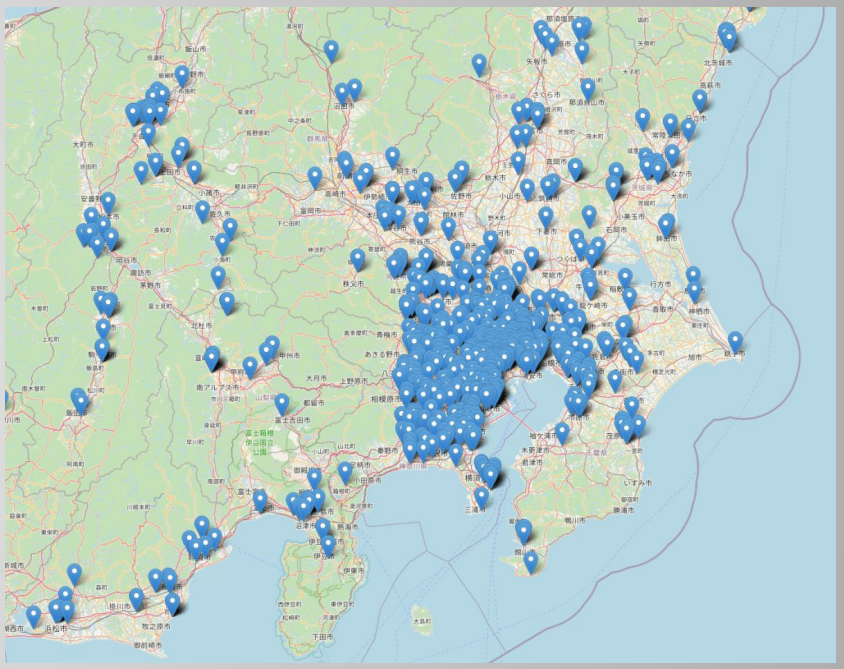
・スマートフォン（Android OS）に感染
・C&C通信でBotネットを構築
（C&C通信を観測）
・SMSでマルウェア（apkファイル）を配信
（SMS大量送信を観測）

引用元　https://blog.trendmicro.co.jp/archives/27635

日本にもかなり進行している

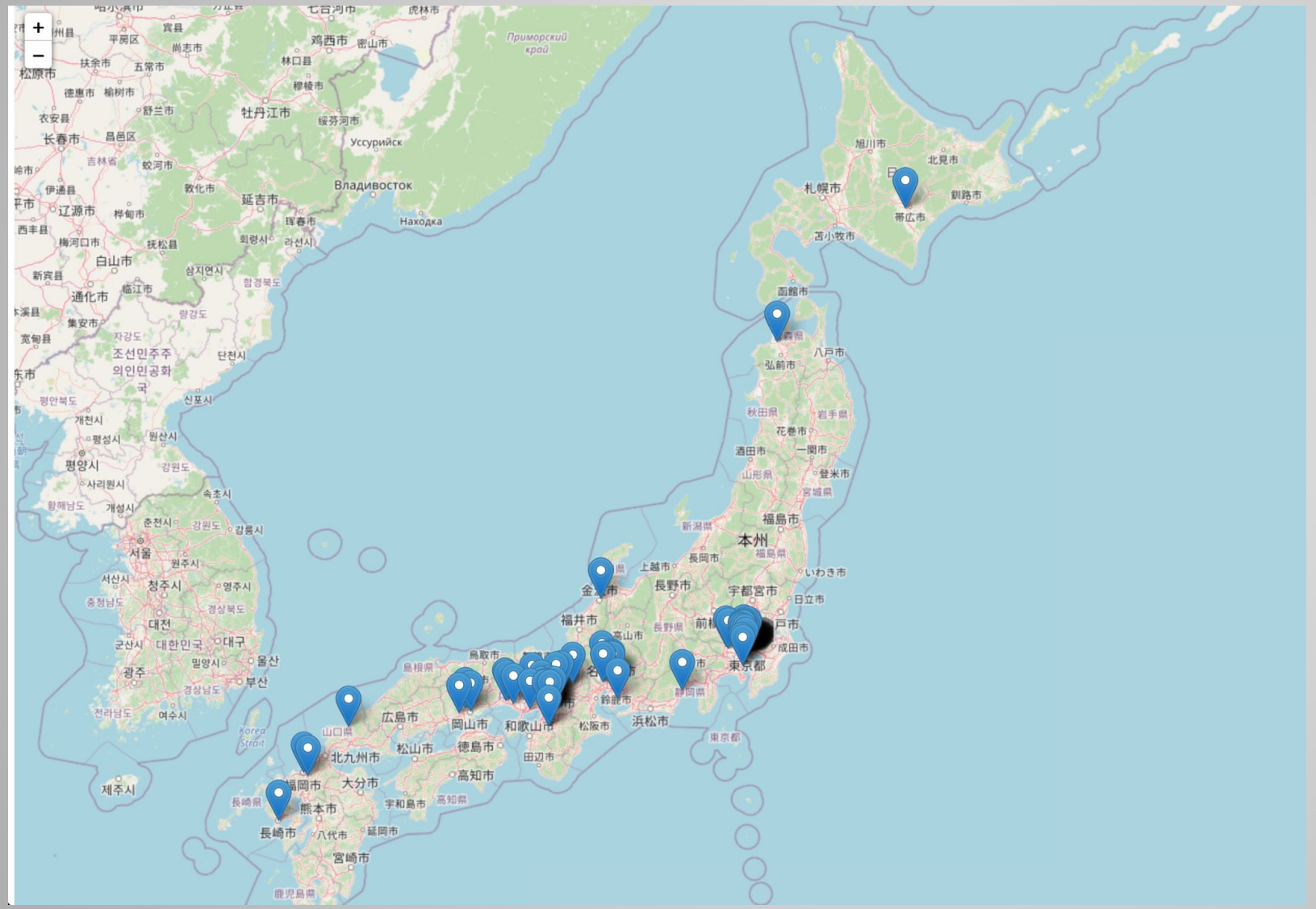




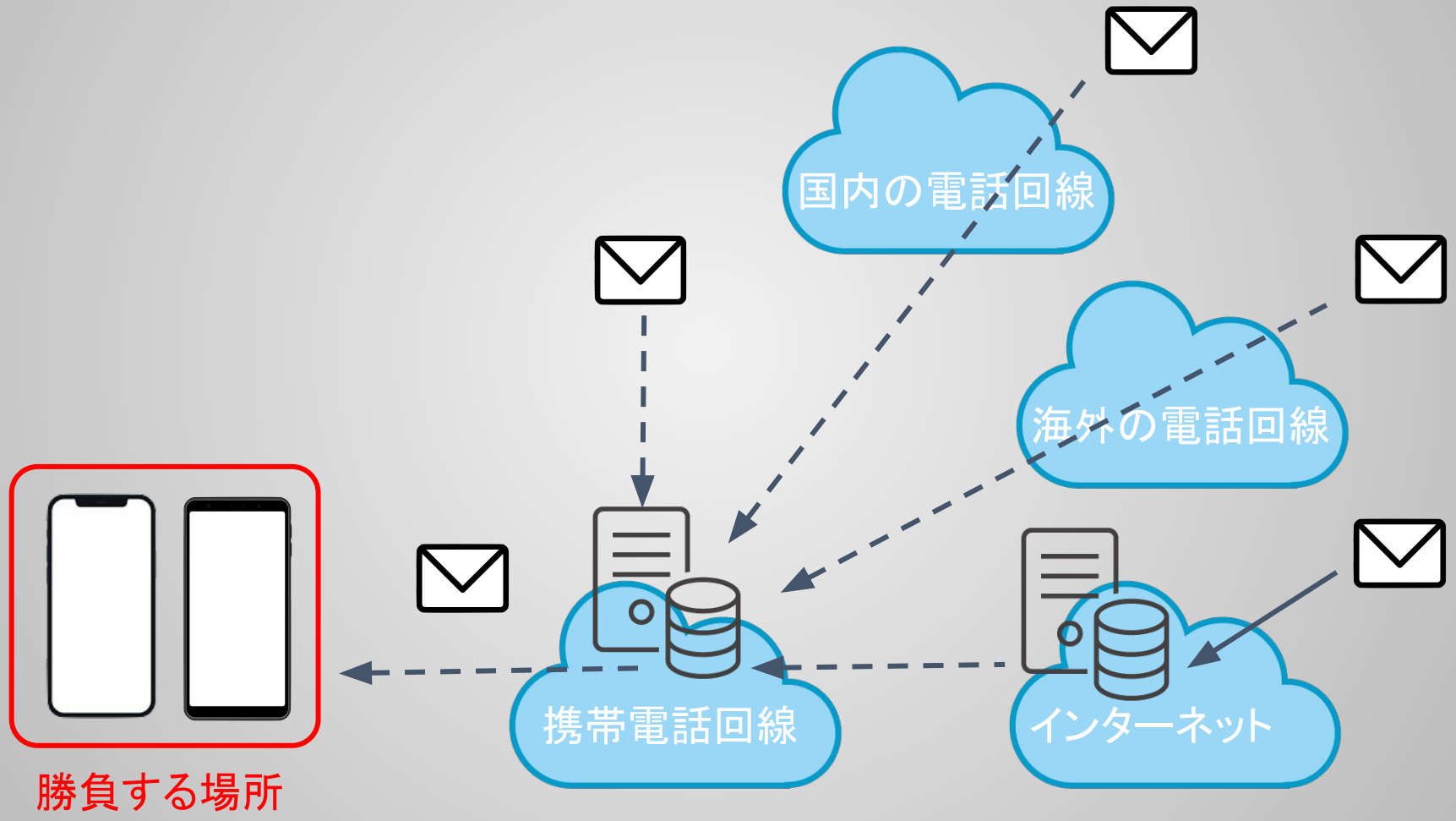


引用元 https://team-cymru.com/blog/2021/08/11/moqhao-part-1-5-high-level-trends-of-recent-campaigns-targeting-japan/

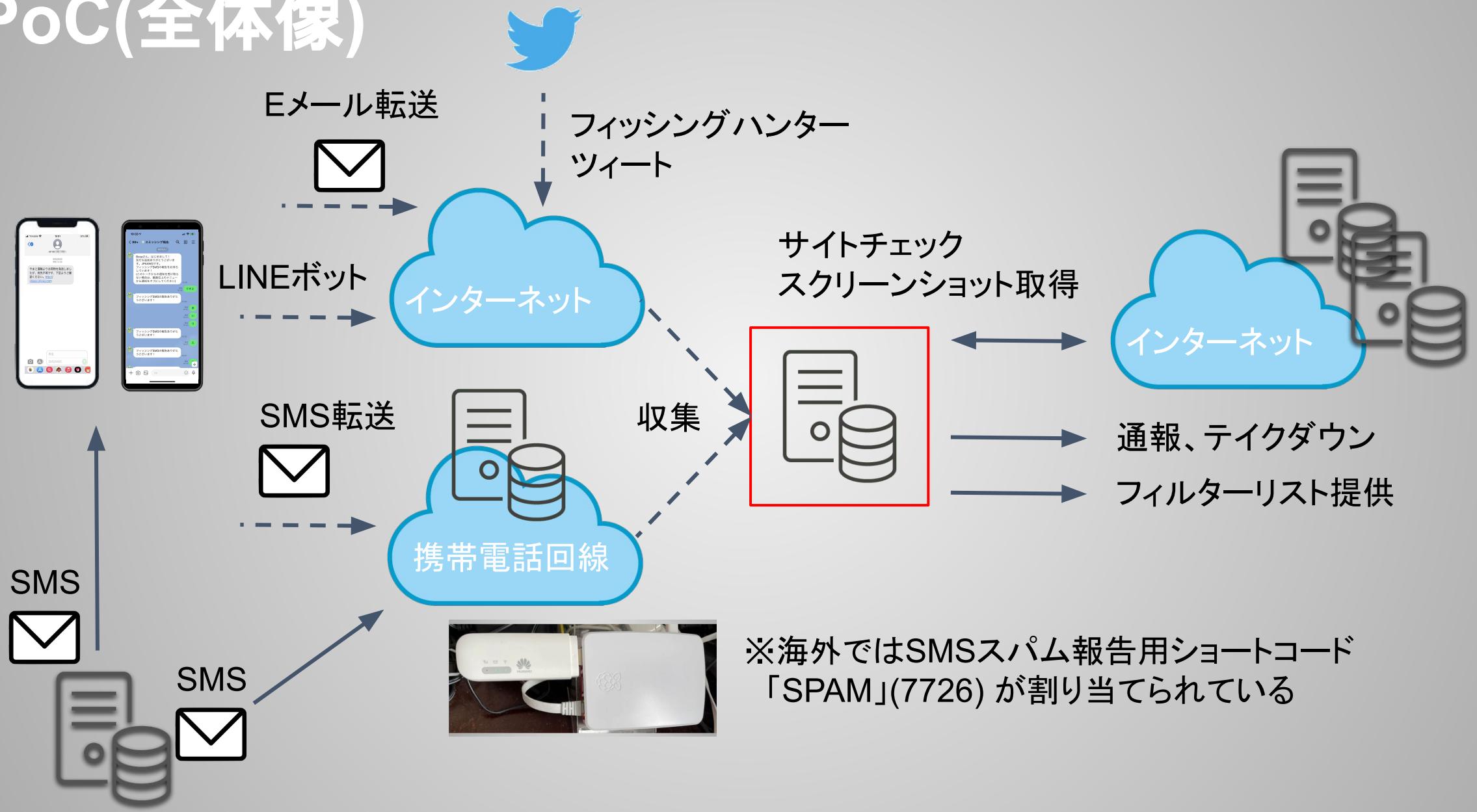
独自調査　‥C2はUA (2021/6/24)



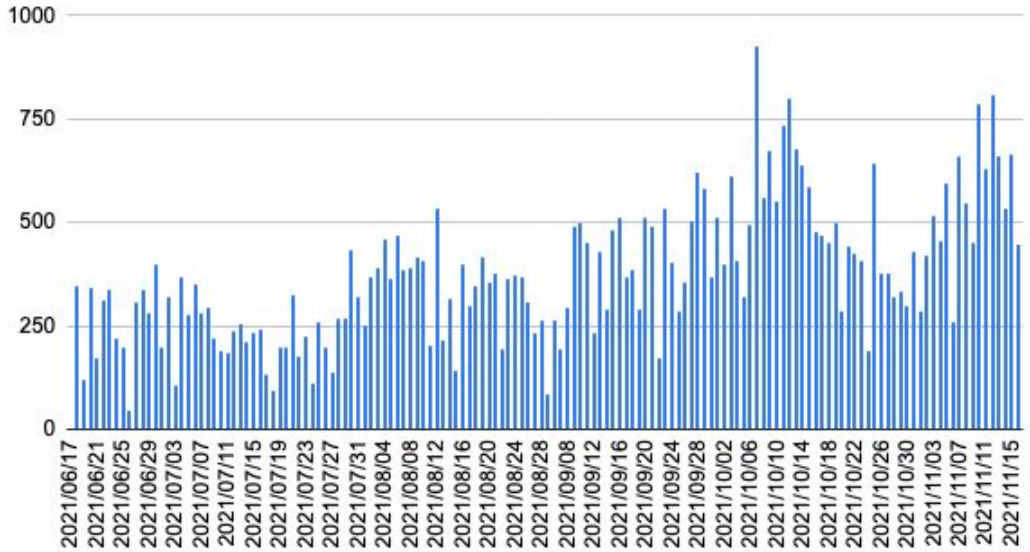
課題



PoC(全体像)

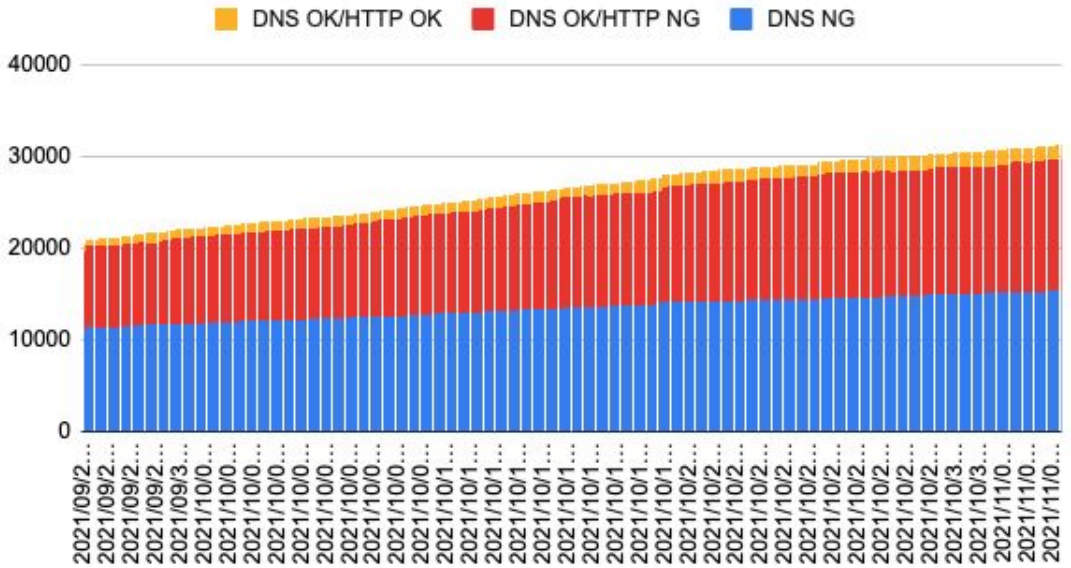

Eメール転送
フィッシングハンター
ツィート
LINEボット
インターネット
サイトチェック
スクリーンショット取得
インターネット
SMS転送
収集
通報、テイクダウン
フィルターリスト提供
携帯電話回線
SMS
SMS
※海外ではSMSスパム報告用ショートコード
「SPAM」(7726) が割り当てられている

フィッシングURL報告件数(Twitter)

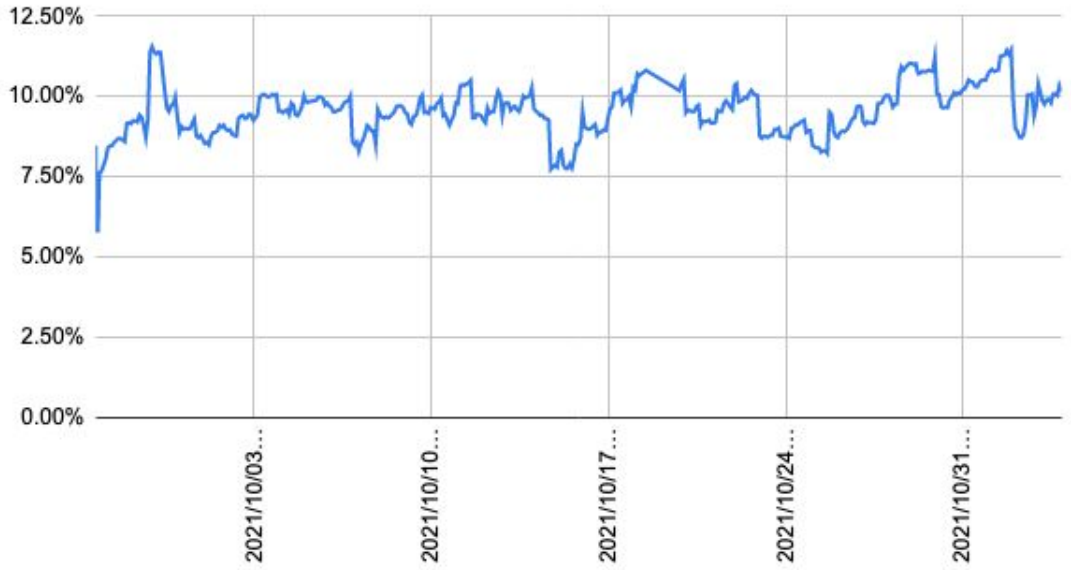


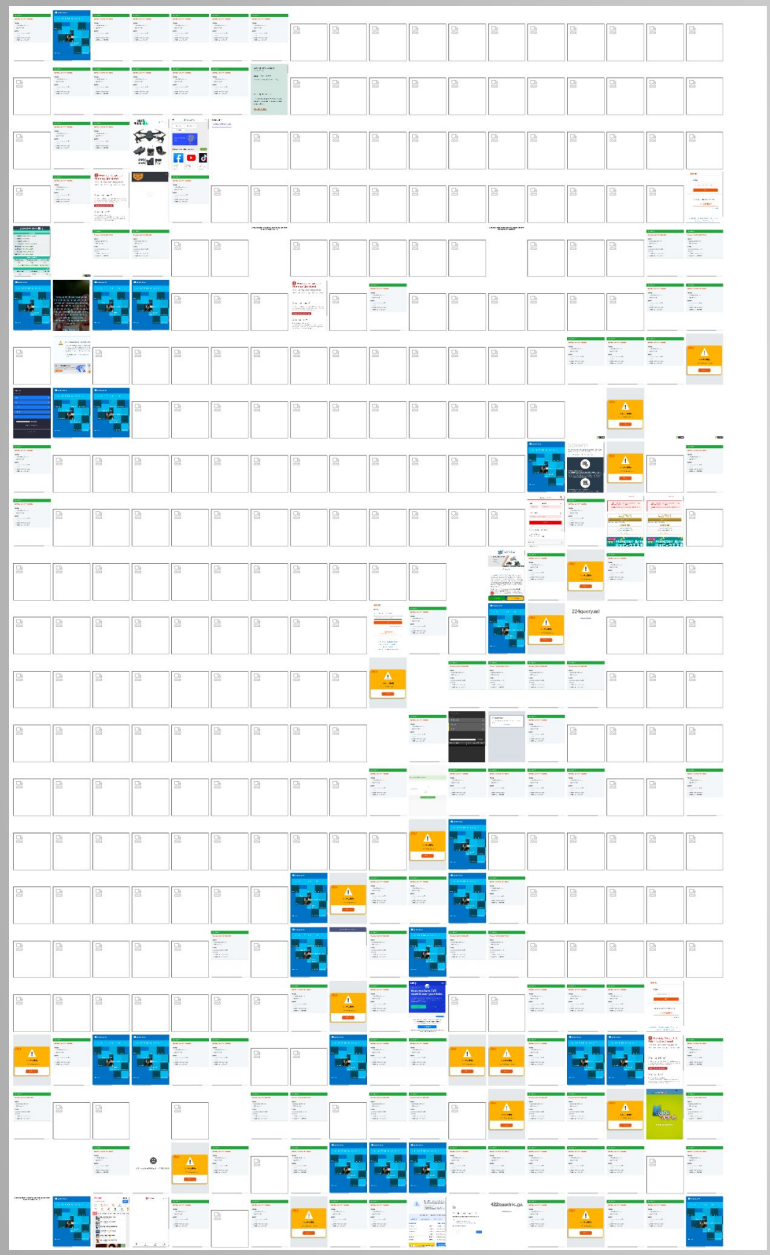
順位	ブランド名	登録件数
1	三井住友カード	2069
2	ドコモ	1867
3	ETC利用照会サービス	1312
4	PayPay銀行	548
5	SMBC/三井住友カード	468
6	SoftBank	357
7	au	349
8	メルカリ	338
9	ヨドバシカメラ	329
10	ビックカメラ	310
11	JCB	257
12	KDDI/au	186

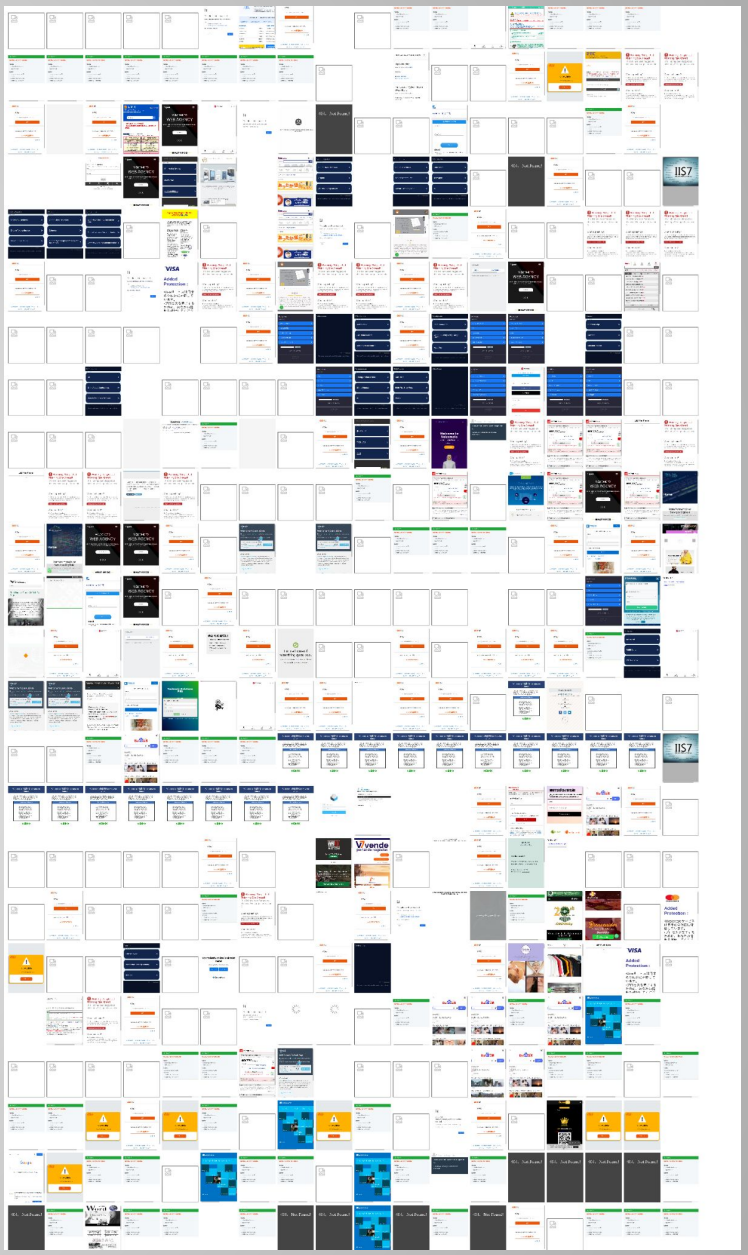
フィッシュサイト稼働状況(Twitter)



稼働率(Twitter)







フィッシングハンターからのお願い！
『見分けようとしない！』

■本物のURLと偽物のURLを見比べてみよう
＜パターン①：そっくり＞
本物：https://www.smbc-card.com/mem/index.jsp
偽：https://www.smbc-card.com.mem-index-jsp.vip
＜パターン②：正規ドメイン.～～～＞
本物：https://www2.cr.mufg.jp/~
偽：https://www2.cr.mufg.jp.ttakasua4[.]tokyo

■「http」か「https」かの違いで判断はできない

■TLD（トップレベルドメイン）での判断は危険
例1：mercarl[.]jp/secure_center/material（メルカリのフィッシングサイト）
例2：saison[.]updated[.]jp（セゾンカードのフィッシングサイト）

・本文に記載されたURLにはアクセスしない
・アクセスする際は登録済みのお気に入り等から


JP AAWG