資料１－３

ICTサービスの利用環境の整備に関する研究会
不適正利用対策に関するワーキンググループ
第１回 資料

SMS・スミッシングとは？

2024/2/26

株式会社マクニカ
角谷 沙歩子、塚田 晴史、丸山 一郎、鈴木 一実

Co.Tomorrowing

MACNICA ADD VNTR.

Agenda

1. マクニカのスミッシング撲滅活動
2. SMSとは？
3. SMSの利活用状況
4. SMSの配信経路
5. スミッシングとは？
6. スミッシング詐欺の拡大状況
7. 最近スミッシングの事例
8. スミッシング文面紹介
9. スミッシングの主原因はマルウェア感染端末
10. マルウェア感染端末のスミッシング配信のしくみ
11. マルウェア感染の原因と手口
12. マルウェア感染対策の例（ニュージーランドの場合）
13. 海外事例：スミッシング共通窓口による対策推進
14. 国内事例：通信事業者による迷惑SMSフィルタリング
15. 国内事例：通信事業者の新たな取り組み（RCSと共通番号）
16. まとめ

マクニカのスミッシング撲滅活動

技術・知見・経験を土台とし、深刻な社会課題の解決・被害の撲滅を目指した活動を推進しています。

フィッシング対策支援サービス

＜通信事業者向け＞
- 不正SMS検知分析
- 攻撃手法解析～プロファイリング
- 信号解析
- SMS-FW導入～建付け支援
- 対策運用全体の支援

＜エンタープライズ企業向け＞
- ブランド被害状況の調査
- 手口分析調査～対策立案
- 対策推進全体の支援

フィッシング対策協議会への参加

運営委員会

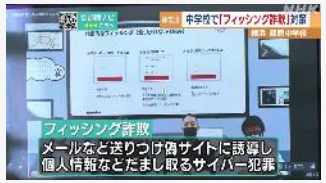
＜協議会での主な活動＞
- 業界横断ワークショップの企画・運営
- 対策ガイドライン作成（制度WG）
- 技術面の研究調査（学術WG）
- 協議会主催の勉強会／セミナー登壇

業界連携の推進

＜登壇＞
- フィッシング対策ワークショップ（全6回）
- クレジットカード協会
- JC3, JPAAWG
- 神川県警察シンポジウム
- 陸上自衛隊

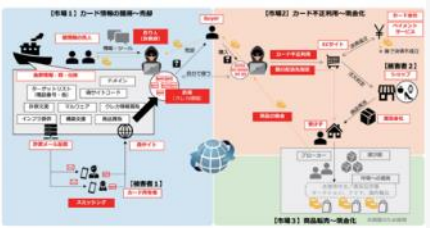
＜技術勉強会＞
- 企業の対策担当者・フィッシングハンターを含め技術で被害撲滅を推進・検討を行う会を主催

＜公共メディアで解説＞
- ニュースウォッチ9
- NHK あさイチ
- RKB毎日 ただいま!
- You Tube動画出演



専門知見の発信

手口・メカニズム・犯罪エコシステム・
対策フレームワークを解説
https://www.macnica.co.jp/business/security/security-reports/141702/

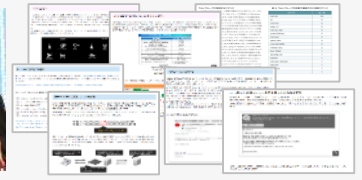


英語版もリリース（2023/5月）

技術調査・対策技術の創出・技術活用

セキュリティ研究センター

セキュリティドメインチーム



テレコムセキュリティチーム

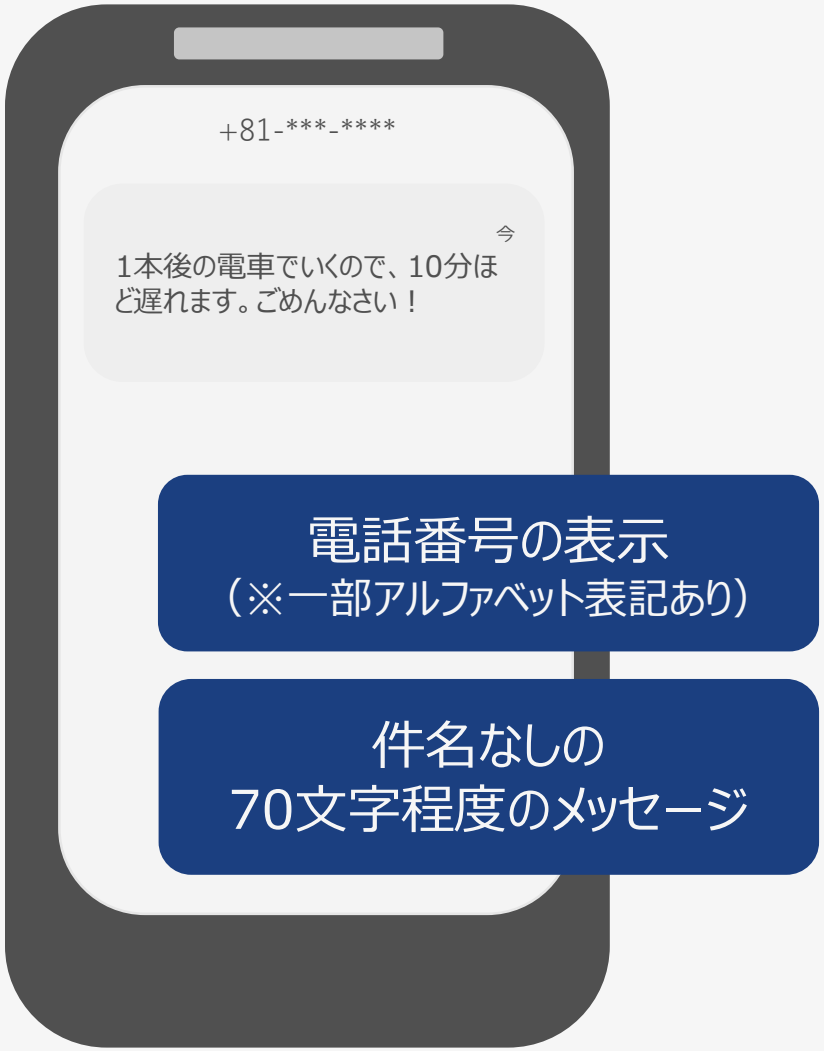
博士

侍

- 国内スミッシングの定量分析
- アクタープロファイリング
- マルウェア解析
- 犯罪コミュニティ調査
- モバイル脅威分析
- サイバー犯罪対策
- 各種検知技術
- 社外共同研究

SMSとは？

ショートメッセージサービス（Short Messaging Service）の略語です。



SMSの4つの特徴

- すべての携帯電話に含まれる機能、アプリ不要で利用可能
- 電話番号で送受信可能
- スマホ画面にポップアップして着信をお知らせ
- リンクや電話番号にタッチすれば、サイト閲覧・電話につながる

タイムリーに受領され、次へのアクションがとりやすい

出典：NTTコムオンライン　2024/2/1開催セミナー資料参照
増加するSMSフィッシング！その最新動向と企業が取るべき対策とは？
を参考に弊社作成

SMSの利活用状況

SMSは、①携帯端末から発信　②SMS配信事業者から発信　があり、特に後者、
企業が発信するSMS通数は年々増加しています。SMSの利点を活かし、様々な業界・用途で活用されています。

国内アグリゲーターとキャリア・アグリゲーターのSMS送信数
（日本国内における消費者向けSMS送信市場）

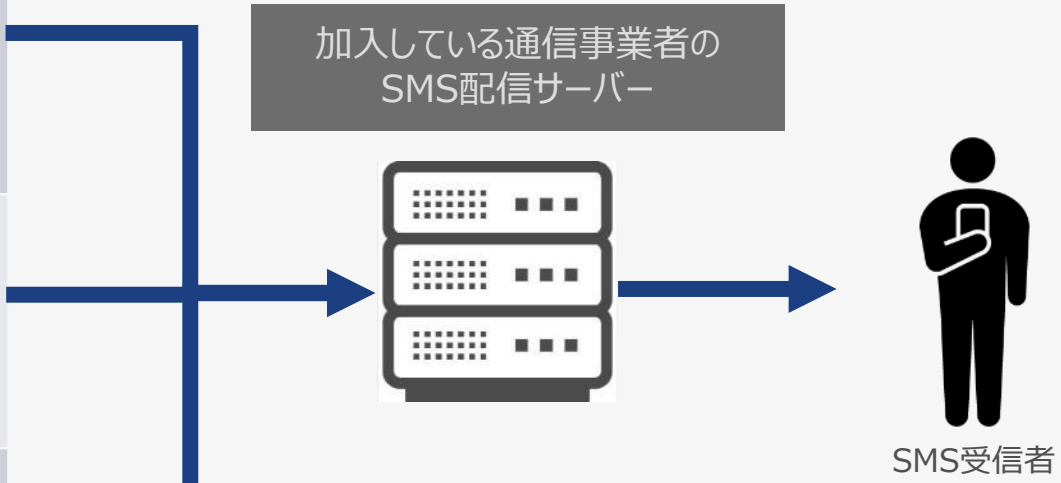
利用用途例

出典：ミックITリポート2024年1月号「2023年度に急ブレーキがかかるも2028年度まで成長期が続くA2P-SMS市場」より。
デロイト トーマツ ミック経済研究所株式会社

SMSの配信経路

配信経路は、①国内携帯電話端末、② 国内SMS配信事業者、③海外通信事業者　の3つのルートがあり、
利用者がSMSを受信する前には**必ず加入している通信事業者のSMS配信サーバーを経由**します。

配信経路	送信元番号の表示 
①国内携帯電話端末	携帯電話番号 （090~ 080~ 070~など）
②国内SMS配信事業者	国内固定電話番号 キャリア共通番号 （03~ 0120~ 0005~など）
③海外通信事業者	海外電話番号 アルファベット ランダムな英数字など



スミッシングとは？

フィッシング（Phishing）行為の一種であり、**SMS Phishing**から生まれた造語です。

クレカ番号や口座番号など
個人情報などを釣り上げる
釣り＝Fishingが語源の造語

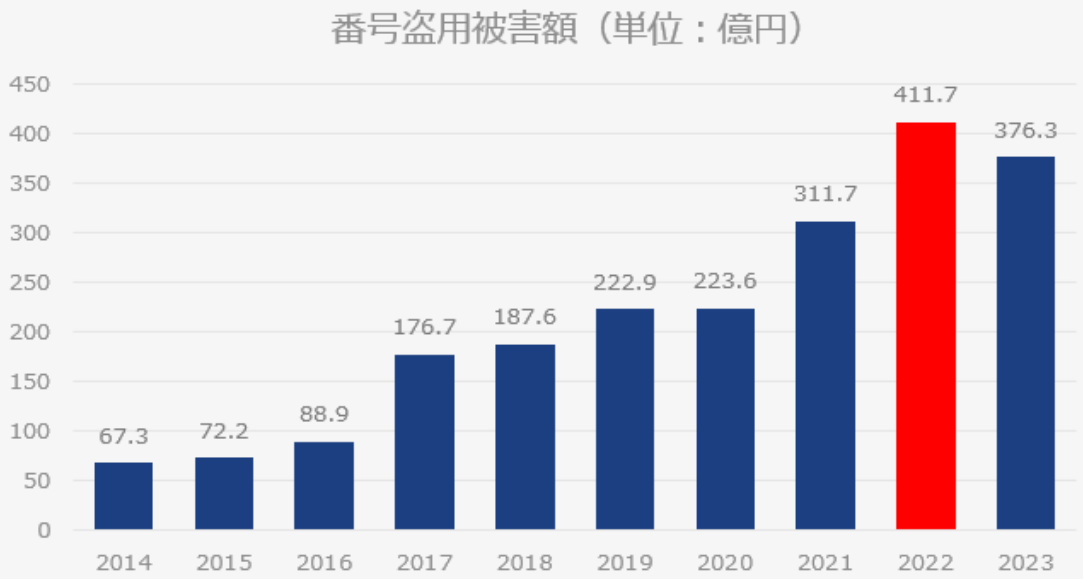
その釣りをSMSを使って行う事を
SMS Phishing（略してスミッシング）と呼ぶ

マクニカHP　https://www.macnica.co.jp/business/consulting/columns/140841/

スミッシング詐欺の拡大状況

フィッシング詐欺が深刻な社内問題となる中で、SMSを悪用したスミッシングが注目を集めています。

＜クレジットカードの番号盗用被害額＞
スミッシングがトリガーとなって発生している可能性が考えられます。
2022年は411億円、2023年は376億円の被害が申告されています。



日本クレジット協会　「日本のクレジット統計」
P34 クレジットカード不正利用被害の発生状況　よりマクニカ作図

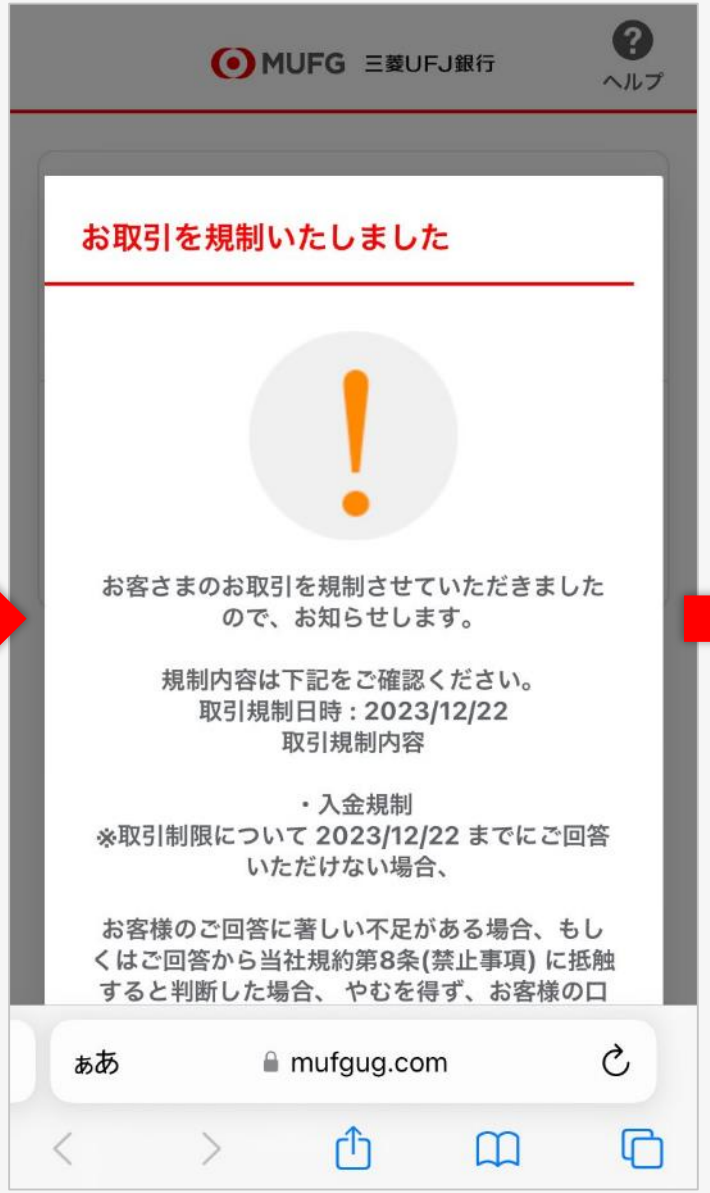
＜インターネットバンキングに関わる不正送金被害額＞
フィッシングによるものと思われる不正送金の被害額も
2023年には、80億円を超えています。

警察庁
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）

最近スミッシングの事例 2023/12/22

- SMSに記載されたリンクから
  詐欺ページにアクセスさせます。
- 銀行口座利用に必要な情報を
  用意されたサイトに入力させ、抜き取ります。

【重要】三菱UFJ銀行お知らせ、お客様の銀行取引を一時的に規制しています、ご本人様確認が必要となります。
hxxps://mufgug.com



フィッシングハンター@NaomiSuzuki_氏のツイートより
文面・画像を引用
https://twitter.com/NaomiSuzuki_/status/1738201373907521851

スミッシングの文面紹介

2023年10月30日

メール・SMSの文面例

SMS 文面の例

【三菱UFJ銀行】お知らせ、お客様の銀行口座の取引を一時的に規制しています、必ずご確認ください。https://muf[redacted].com

https://www.antiphishing.jp/news/alert/mufgbank_20231030.html

2023年04月10日

メール・SMSの文面例

SMS 文面の例

【三井住友信託ダイレクト】必ずご回答ください／お取引目的等の確認のお願い。https://rb.gy/[redacted]

https://www.antiphishing.jp/news/alert/smtb_20230410.html

2019年07月08日

メール・SMSの文面例

【EPOS】お客様のエポスカードが不正利用の可能性があります。本人認証設定をお願いします。
http://www.epos-●●●●.com

https://www.antiphishing.jp/news/alert/eposcard_20190708.html

税金のお支払い方法に問題があります、更新してください：https://www.td[redacted].net/WbqFUa2494

【国税庁8月12日】未払い税金お支払いのお願い。ご確認ください。https://cutt.ly/[redacted]

お客様が不在の為お荷物を持ち帰りました。こちらにてご確認ください 1kr[redacted]com?us9ia

【重要なお知らせ】SoftBank未払い料金お支払いのお願い。
http://fhmwt.[redacted].xyz

【利用停止予告】NTTドコモ未払い料金お支払いのお願い。
https://bit.ly/[redacted]

【auからの重要なお知らせ】ご利用金額が設定した金額を超えました。ご確認が必要です。
https://bit.ly/3[redacted]

https://www.antiphishing.jp/report/consumer_antiphishing_guideline_2023.pdf

受け取った方の**不安を煽る文面**で
確認を急ぐ内容が多くみられます。

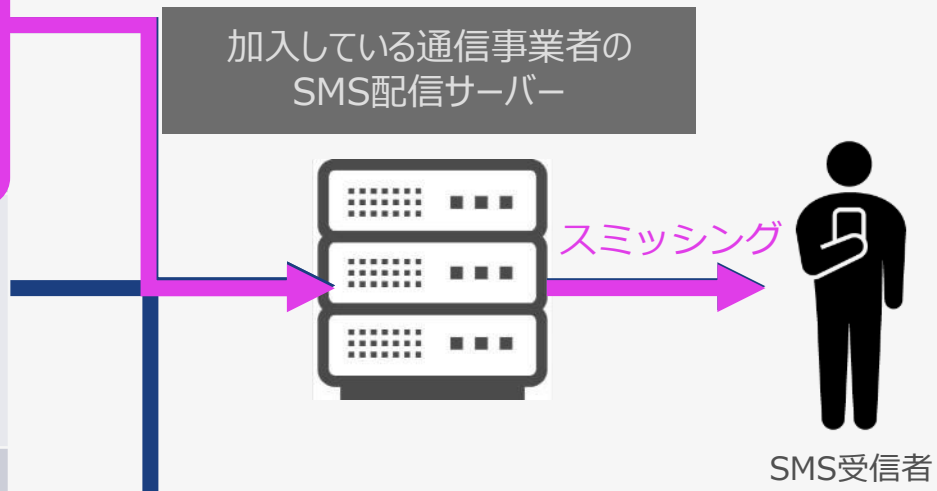
スミッシングの発信源はマルウェア感染端末

一昔前は海外通信事業者からのスミッシング発信が多かったが、現在は、マルウェア感染した端末が主な発信源となっており、国内発信のスミッシング比率が高くなっています。

スミッシングの分布比率※	配信経路	送信元番号の表示 
99%	①国内携帯電話端末	携帯電話番号 (090~ 080~ 070~など)
	②国内SMS配信事業者	国内固定電話番号 キャリア共通番号 (03~ 0120~ 0005~など)
1%	③海外通信事業者	海外電話番号 アルファベット ランダムな英数字など

感染端末は、一般の個人が所有し、いたるところで日常利用しているため、対策が非常に難しい

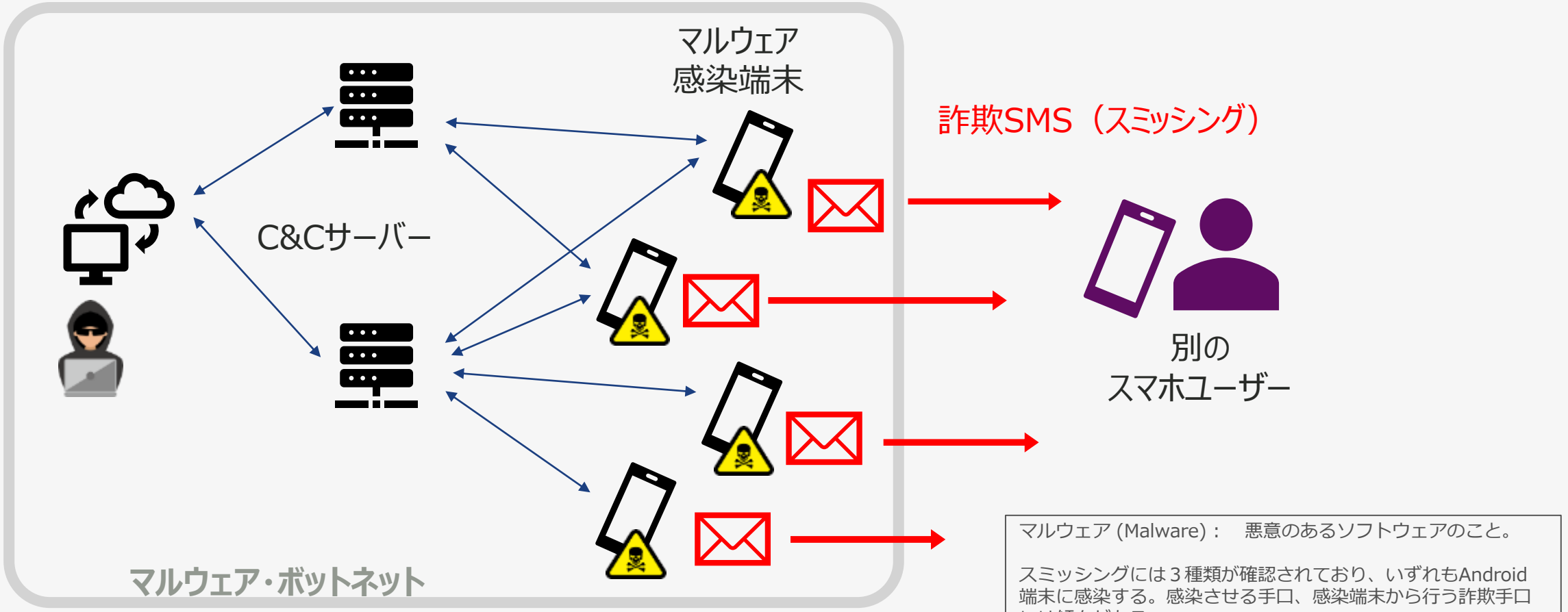
感染数の把握、端末の特定、無害化・・・などが急務である



※：NTTドコモ 三谷咲子様　2023/11/7 JPAAWG6登壇資料
携帯キャリアによるSMSフィッシング(スミッシング)対策の最新情報

マルウェア感染端末のスミッシング配信のしくみ

スマートフォンが、意図しない不正アプリ導入によりマルウェア感染し（本人は無自覚）、攻撃の踏み台にされています。



マルウェア (Malware)：　悪意のあるソフトウェアのこと。

スミッシングには３種類が確認されており、いずれもAndroid端末に感染する。感染させる手口、感染端末から行う詐欺手口には傾向がある。

マルウェア感染の原因と手口

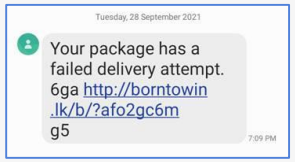
- フィッシングと同じ手口を使い、利用者を感染用のWEBサイトへ誘導、アクセスさせることでマルウェアに感染させます。
- WEBサイト側で端末を識別し、Android：不正アプリダウンロード、iPhone：Apple IDを搾取するページを表示します。
  - Android端末は正規ストア（Google Play）以外からのアプリ導入※を許容するため感染　※サイドローディングと言われる。
  - iPhoneはApp Storeが厳格かつサイドローディングが出来ないため、感染しない

代表的な事例：個人携帯発、不在通知を装う手口

フィッシングハンター@NaomiSuzuki_氏のツイートより文面・画像を引用
https://twitter.com/NaomiSuzuki_/status/1752182042291499460

マルウェア感染対策の例（ニュージーランドの場合）

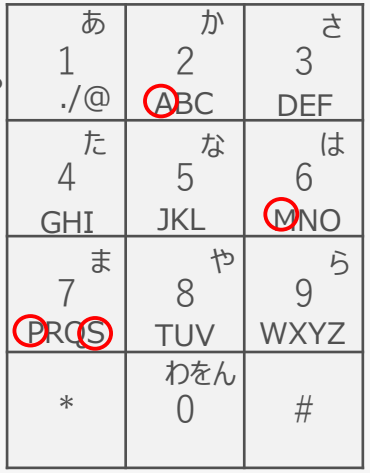
2021年9月に始まったFluBotマルウェアは、最初の9日間で11万件の通報があり、全通信事業者に大きな影響を与えました。
FluBotの被害は欧州全体に広がっており、**EC3と11か国の法執行機関の協力でサーバを停止**しました。

項目	内容
日時	2021年9月に発生、2022年5月にFluBotコントロールするサーバを停止
被害規模	内務省（DIA）の Spam Reporting Service（7726）は、最初の9日間で11万件以上の通報を受ける、最終的には70万通以上
攻撃対象	Androidスマートフォン（iOSでは、SMSのリンクをクリックするとフィッシングサイトへ誘導）
攻撃手法	① スミッシングを被害者のスマートフォンに送信  ② 被害者がリンクをクリック 不正サイトにアクセス  ③ 被害者のスマートフォンにマルウェアがダウンロードされる  ④ マルウェアが、スマートフォンから個人情報を取得 • 銀行ID、パスワード、クレジットカード情報、コンタクトリスト等 ⑤ コンタクトリストからスミッシングを送信して、被害が拡大  ⑥ マルウェアの除去のためには、工場初期化状態にリセットする
対策	**体制確立** DIAが緊急対策グループ設立 • CERT NZ、電気通信フォーラム、通信事業者と協力 最初の通報から3時間以内 **初動対応** （感染者向け） DIAが対応チームを作成、 • 通報からマルウェア感染被疑の600の電話番号を特定 • 24時間で所有者に400回の電話連絡を実施、マルウェア削除手順を通知 （一般向け） SNSの活用 • プレスリリースとメッセージ掲載 • 怪しいメッセージはSpam Reporting Service (7726) への通知を推奨 **根本対応** Flubot マルウェアサーバを停止 • ユーロポール欧州サイバー犯罪センター(EC3)＆11ヶ国の法執行機関の国際協力 • 2022年5月に実施

マルウェア文面は、Digital Messaging Landscape 2023 Operation Environment より引用

海外事例：スミッシング共通窓口による対策推進

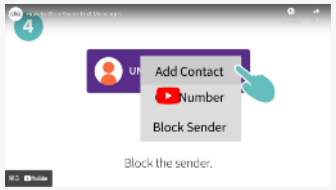
通信事業者横断のスミッシング申告として、Spam Reporting Service (7726) が広く使われています。



1．Spam Reporting Service とは

- 不正SMSを7726に転送すると、通信事業者を横断したSMSトラフィックを分析して、悪用を集約するサービス
- GSMAが2010年にパイロットサービスを開始、現在は個々の通信事業者が実施している
- 7726は、スマホのキーボードで SPAM にあたることから使われている

2．Spam Reporting Service のサービス提供例

国	イギリス	アメリカ	ニュージーランド
運用主体	Ofcom（情報通信省）	CTIA（携帯電話事業者の業界団体）	DIA（内務省）
概要	• 利用者は、不正SMSを受信したら7726に転送する • iPhone/Androidの両方から利用可能で、使い方のYouTubeチュートリアルを公開 	• 利用者は、不正SMSを受信したら7726に転送する • iPhone/Androidの両方から利用可能で、使い方のYouTubeチュートリアルを公開 	• Email/SMSに共通の不正申告サイトを設置している • 利用者は、不正SMSを受信したら7726に転送する • iPhone/Androidの両方から利用可能 
URL	https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/scams/7726-reporting-scam-texts-and-calls	https://www.ctia.org/consumer-resources/protecting-yourself-from-spam-text-messages	https://www.dia.govt.nz/Spam-Report-TXT-Spam

国内事例：通信事業者による迷惑SMS対応

通信事業者３社は、ネットワーク側で不正SMSのブロックを実施しています。
サービス利用の選択はオプトアウト方式で、ユーザはブロックを選択しない場合は、設定をオフに変更可能です。

	DOCOMO	KDDI	Softbank
ネットワーク側の対応	危険SMS拒否 2022/03開始 https://www.docomo.ne.jp/info/spam_mail/sms/	迷惑SMSブロック 2023/02開始 https://www.au.com/mobile/service/sms/filter/	迷惑SMS対策機能 2022/06開始 https://www.softbank.jp/mobile/info/personal/news/service/20220602a/
端末側の対応	あんしんセキュリティ https://www.docomo.ne.jp/service/anshin_security/	迷惑メッセージ・電話ブロック https://media2.kddi.com/meiwakublock/safecall/PC/PC.html	-

楽天モバイルはネットワーク側対応、端末側対応側共に未提供

国内事例：通信事業者の新たな取り組み（RCS、共通番号）

通信事業者はメッセージサービスの高度化のために、電話番号でリッチコンテンツを利用できるRCS、契約する通信事業者に関わらず共通の送信元番号を利用できるキャリア共通番号を提供しています。

RCSとは

RCS は、世界標準に基づき、SMSと同様に携帯電話番号で送ることができるメッセージサービス

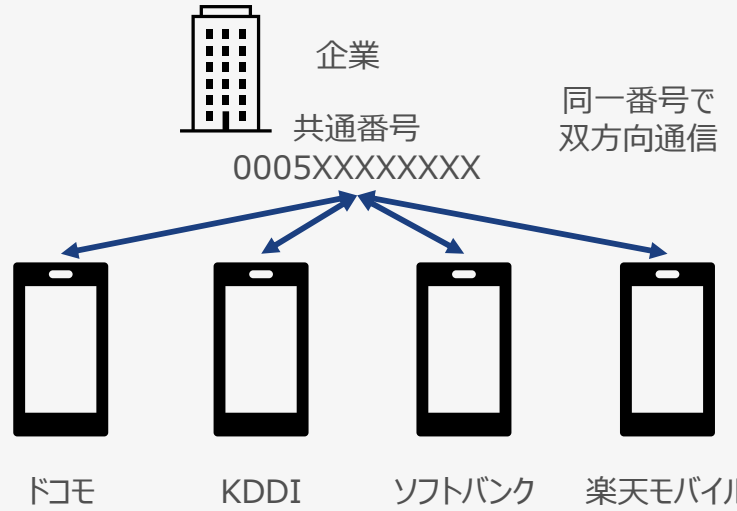
- 正式名称はRich Communication Service
- SMSより、多くの文字数を送付できる
- 公式マークを設定して、メッセージを発信できる
- テキスト以外に画像を送ったり、グループチャットが使える
- 日本では、ドコモ・KDDI・ソフトバンクが＋メッセージ、楽天モバイルがRakuten Link の名称でサービスを提供している
- Appleは、RCS Universal Profile を2024年後半にサポートする予定を表明

通信事業者	ドコモ	KDDI	ソフトバンク	楽天モバイル
サービス名称	＋メッセージ			Rakuten Link

キャリア共通番号（０００５）とは

通信事業者４社（ドコモ、KDDI、ソフトバンク、楽天モバイル）が管理する「0005」から始まる8～10桁の番号

- ユーザが契約している通信事業者に関わらず、送信番号として同じ番号が表示される（通信事業者での審査がある）
- 企業が事前にWebサイトなどで共通番号を公表することで、公表済の番号として携帯4社すべてのお客さまへSMSを届けられる
- 企業は、SMS送信サービス事業者と契約をして番号が割り当てられる



まとめ

1. SMSは**全てのスマートフォンが利用可能**で、**高い到達率・開封率を誇る**便利なメッセージサービス

2. SMSの利便性に**便乗して、スミッシング**が横行し、**大きな経済被害**でており、社会課題となっている

3. 更に**マルウェアによる拡散**が深刻化。感染数把握やスミッシング稼働状況などの把握・対策検討が急務

4. マルウエア感染はニュージーランドをはじめ、日本以外でも発生しており、**政府機関の協力で対策を講じた例**も存在、感染者への連絡や対応など対策アクションは参考になる

Co.Tomorrowing

MACNICA