

A2-5

15:00-15:45

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

小頭 秀行

KDDI株式会社

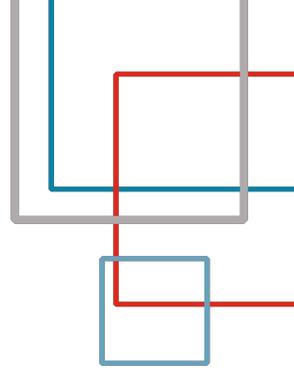
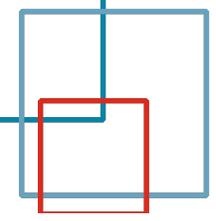
三谷 咲子

株式会社NTTドコモ

北崎 恵凡

ソフトバンク株式会社 / JPAAWG





登壇者紹介

(自己紹介)



SRE

ソフトバンク株式会社
ソリューション運用本部

プラットフォーム運用統括部
アプリケーション運用部
プラットフォーム運用課

北崎 恵凡

Kitazaki Ayachika

JPAAWG
運営委員

一般財団法人 インターネット協会
迷惑メール対策委員会 副委員長

一般財団法人 日本データ通信協会
迷惑メール対策推進協議会 構成員



KDDI株式会社
パーソナル事業本部 サービス統括本部
サービス開発3部 サービス1G
グループリーダー

小頭 秀行
KOTO Hideyuki

KDDI入社後、研究所に約10年間所属。
トラフィック制御・分析、
ネットワークの設計に関する研究に従事。

電子情報通信学会、IEEEを中心に活動。
3G/UMTS、4G/LTEに関する必須特許を考案。

その後、サービス企画部署に異動し、
SMSの機能拡張、迷惑対策強化、
RCS(+メッセージ)の立ち上げに参画。

自称「電番メッセージのエバンジェリスト」



株式会社NTTドコモ
営業本部 国際サービス戦略
国際サービス技術企画担当
危険SMS拒否設定導入・運用を担当

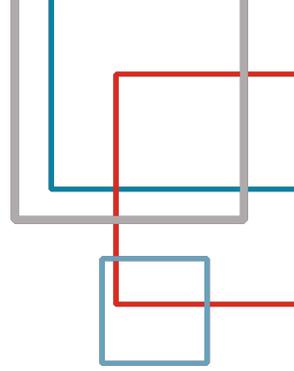
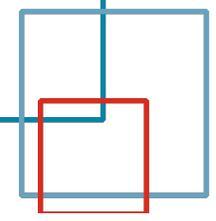
三谷 咲子
Mitani Sakiko

事前アンケート

法制度面 (2) 解釈・整備・後押し	外国からのメッセージを 受け付けない機能 効果は？	システム側での 対策方針は？
協力 (2) 情報提供・啓発	SMSは 危険なツール？	プラスメッセージの悪 質利用はある？
偽サイトへの誘導阻止 通報・テイクダウンは有 効？	研究テーマとしての SMS	

事前アンケート

法制度面 (2) 解釈・整備・後押し	外国からのメッセージを受け付け ない機能効果は？	システム側での対策方針は？
協力 (2) 情報提供・啓発	SMSは危険なツール？	プラスメッセージの悪質利用はある？
偽サイトへの誘導阻止 通報・テイクダウンは有効？	研究テーマとしてのSMS	



ふりかえり

SMSフィッシング

対策カンファレンス

2020

JPAAWG | JAPAN ANTI-ABUSE
WORKING GROUP

SMSフィッシングの最新の脅威情報を共有

携帯事業者、監督官庁、フィッシングハンターが集結

開催日時：2020年12月15日(火)



15:40-17:10

モバイル事業者のSMS対策向上委員会

北崎 恵凡

ソフトバンク株式会社 / JPAAWGメンバー

小頭 秀行

株式会社KDDI

田中 威津馬

株式会社NTTドコモ

田中 優成

株式会社アクリート 代表取締役社長

本田景輔

楽天モバイル株式会社

SMSフィッシング対策カンファレンス
2020.12.15 | ONLINE

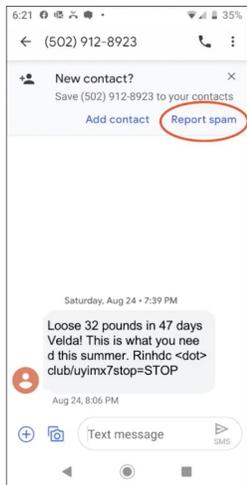


#jpaawg

海外での対策・取り組みの紹介

スパムレポーティング

Submission Method 1: Android Messages Integrated Spam Reporting

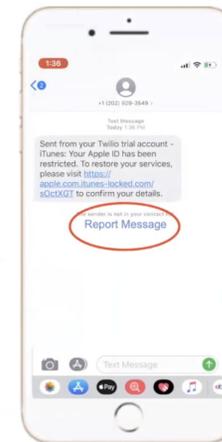


- Spam reports only goes to Google by Default
- Spam reports can optionally be forwarded to a carrier-defined short code (7726!)
- Messages forwarded to Cloudmark via SMPP bind
- Required operator to ask Google to configure carrier settings bundle option "spamForwardingNumber"

proofpoint Android Messagesアプリケーションにはワンクリックでレポートできる

Submission Method 2: Apple iOS SMS/MMS and Voice Spam Reporting

SMS/MMS Reporting



Voice Spam Call Reporting



proofpoint.

Apple iOSプラットフォームでは、

- 専用のショートコード (7726) を割り当て
- Android OS、iOSでサポート

海外での対策・取り組みの紹介

送信者表示名の詐称禁止

The screenshot shows the Twilio Help Center page for 'What is Alphanumeric Sender ID and how do I get started?'. The article explains that Alphanumeric Sender ID allows users to set their own business brand as the Sender ID when sending one-way messages. It notes that this feature is only available when sending messages to supported countries. A red box highlights the text: 'supported countries. Countries where pre-registered alpha sender IDs are required are currently not supported.' A red arrow points to this text with the Japanese text 'IDの事前登録が必要な国はサポート対象外' (Countries requiring pre-registration of IDs are not supported).

TP-OA: Transfer Protocol-Originating Address
(CgPA: Calling Party Address)

The screenshot shows the Twilio Help Center page for 'How do users opt out of messages sent with an Alphanumeric Sender ID'. The article states that since Alphanumeric Sender ID can only be used for one-way messaging, inbound messages sent to your Alphanumeric Sender ID will not be received by your Twilio Account. A red arrow points to this text with the Japanese text '返信は不可' (Reply is not possible). The article also states that customers receiving text messages with your Alphanumeric Sender ID should have opted in to your service and been informed on how to opt out. It recommends providing a clear description in your terms of service about how many messages they should expect to receive and how they can opt out. A red box highlights the text: 'Spoofing of brands or companies with Alphanumeric Sender ID is not allowed.' A red arrow points to this text with the Japanese text 'なりすましは禁止' (Impersonation is prohibited). The article also highly recommends offering your users the ability to opt out of receiving SMS messages from your service.

The screenshot shows the Twilio Help Center page for 'What countries does Twilio support Alphanumeric Sender ID?'. The article states that Twilio supports Alphanumeric Sender ID in the following countries. Currently Twilio does not support pre-register alpha sender ID. Countries where this is required are not supported. A table lists the supported countries and their alphanumeric support status. A red box highlights the entry for Japan, which is supported.

COUNTRY	ALPHANUMERIC SUPPORT
Afghanistan	No
Albania	Yes
Algeria	No
Japan	Yes

▶ 日本はサポート対象

法律・規制の問題

架空・不当請求メール
規制法:無し

特定商取引法
対象:通販メール等
(管轄:消費者庁)

特定電子メール法
対象:広告宣伝メール
(管轄:総務省)

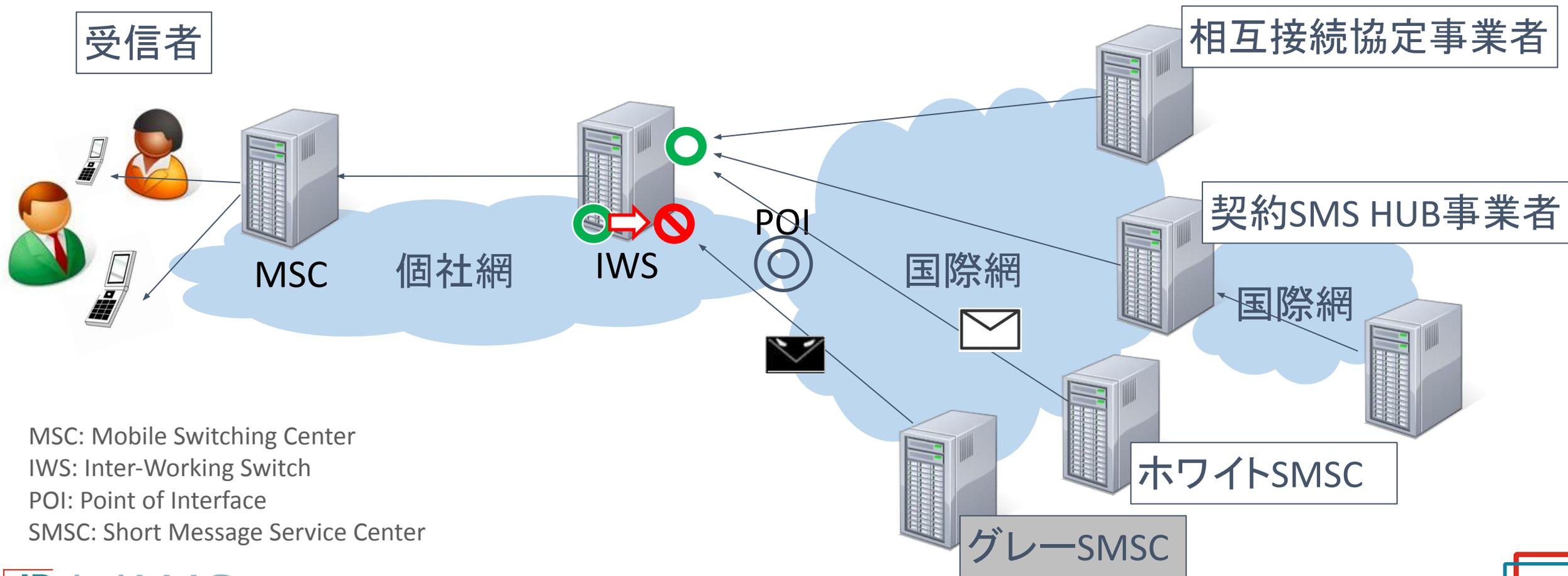
SMSを含む

刑法
対象:詐欺行為等
(管轄:警察庁)

事前アンケート

法制度面 (2) 解釈・整備・後押し	外国からのメッセージを受け付けられない機能効果は？	システム側での対策方針は？
協力 (2) 情報提供・啓発	SMSは危険なツール？	プラスメッセージの悪質利用はある？
偽サイトへの誘導阻止 通報・テイクダウンは有効？	研究テーマとしてのSMS	

ネットワーク側での対策



SMSフィッシング (SMiShing スミッシング)



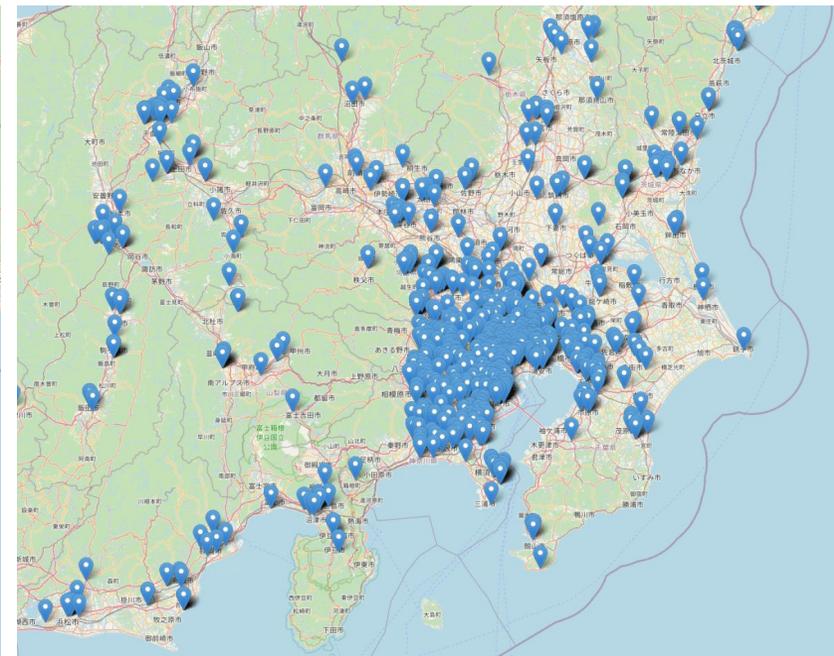
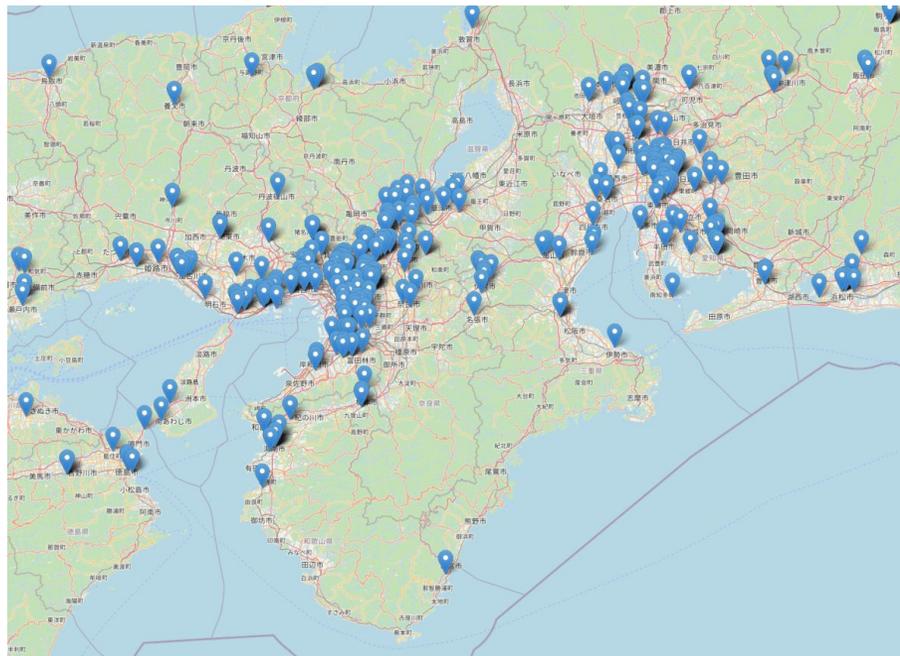
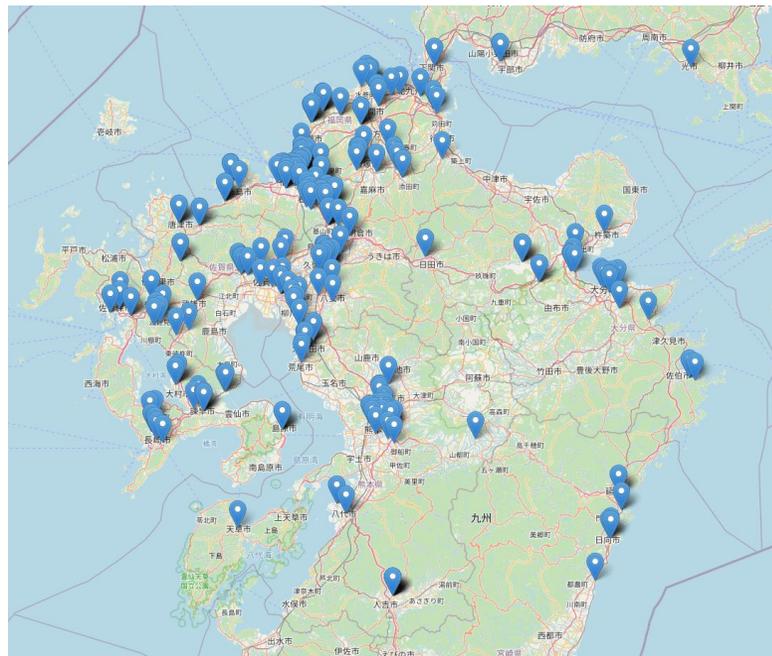
MoqHao (モクハオ)

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)

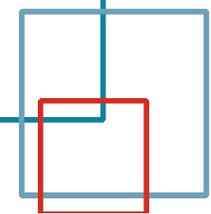


日本にもかなり進行している

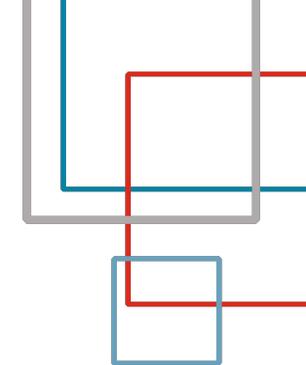


独自調査(2021/6/24) ・ ・ C2はUA (ccTLD)





フィッシングハンターからのお願い！ 『見分けようとしなさい！』



■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](https://www2.cr.mufg.jp.ttakasua4[.]tokyo)

■「http」か「http**s**」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](#)(シーズ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

AVTOKYOフィッシング語らナイト！

2022年の フィッシング詐欺 トレンド	フィッシング詐欺犯は 一体どんな人（人達） が行っているの？	迷惑SMS対策機能って ぶっちゃけ 使い物になるの？
技術的に フィッシング詐欺は 防げるのか	クレジットカードって どれだけ安心なの？	フィッシング啓発や 注意喚起で大事な 事ってあるの？
日本のフィッシング 詐欺被害率って 高いの？	サイト閉鎖 (テイクダウン) って やっぱり大変？	最新の手法って どんなのがあるの？

SMSフィルター機能の導入

ドコモからのお知らせ

いいね!

ツイート

「危険SMS拒否設定」(無料)の提供について(2022年3月22日更新)

2022年1月13日

平素は弊社商品・サービスをご利用いただき、誠にありがとうございます。

ショートメッセージ(以下、SMS)を用いて行われるフィッシング詐欺対策を目的に、危険なサイトのURLや電話番号が含まれるSMSを自動で拒否する「危険SMS拒否設定」(以下、本機能)を、2022年3月24日(木)(予定)に提供開始します。

2022年3月24日(木)

サービス 2022年

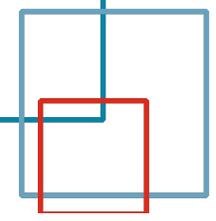
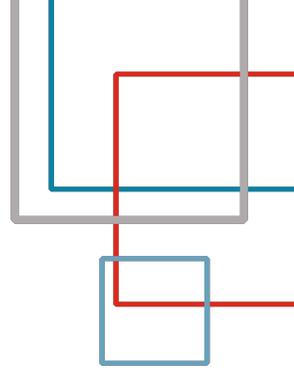
迷惑SMS対策機能(無料)を提供開始

掲載日: 2022年6月2日

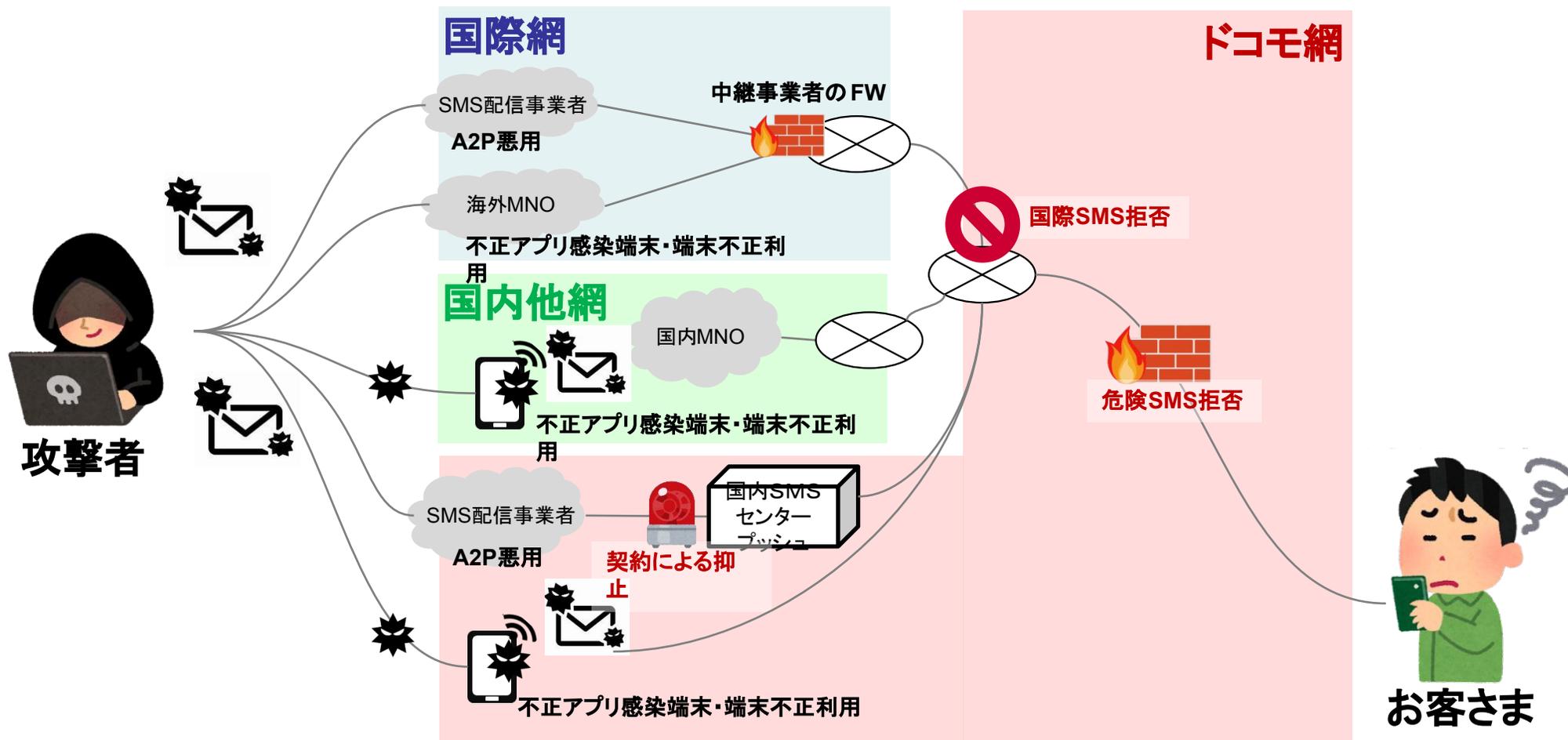
ソフトバンクは、ショートメッセージ(以下、SMS)を利用して行われるフィッシング詐欺対策を目的に、迷惑SMS対策として「なりすましSMSの拒否」、「URLリンク付きSMSの拒否」および「迷惑SMSフィルター」の新機能(無料)を2022年6月23日(木)から提供開始予定です。また、これまで提供してきた「電話番号メール拒否・許可」に、アルファベットでの入力指定を追加します。

ソフトバンクは、これまでもさまざまな迷惑メール対策や、なりすましメールへの注意喚起などを行ってきましたが、新たな迷惑SMS対策機能を提供することで、フィッシング被害の未然防止や拡大抑止に取り組みます。今後もお客さまに安心・安全にサービスをご利用いただけるよう、引き続き対策強化に努めていきます。

2022年6月23日(木)

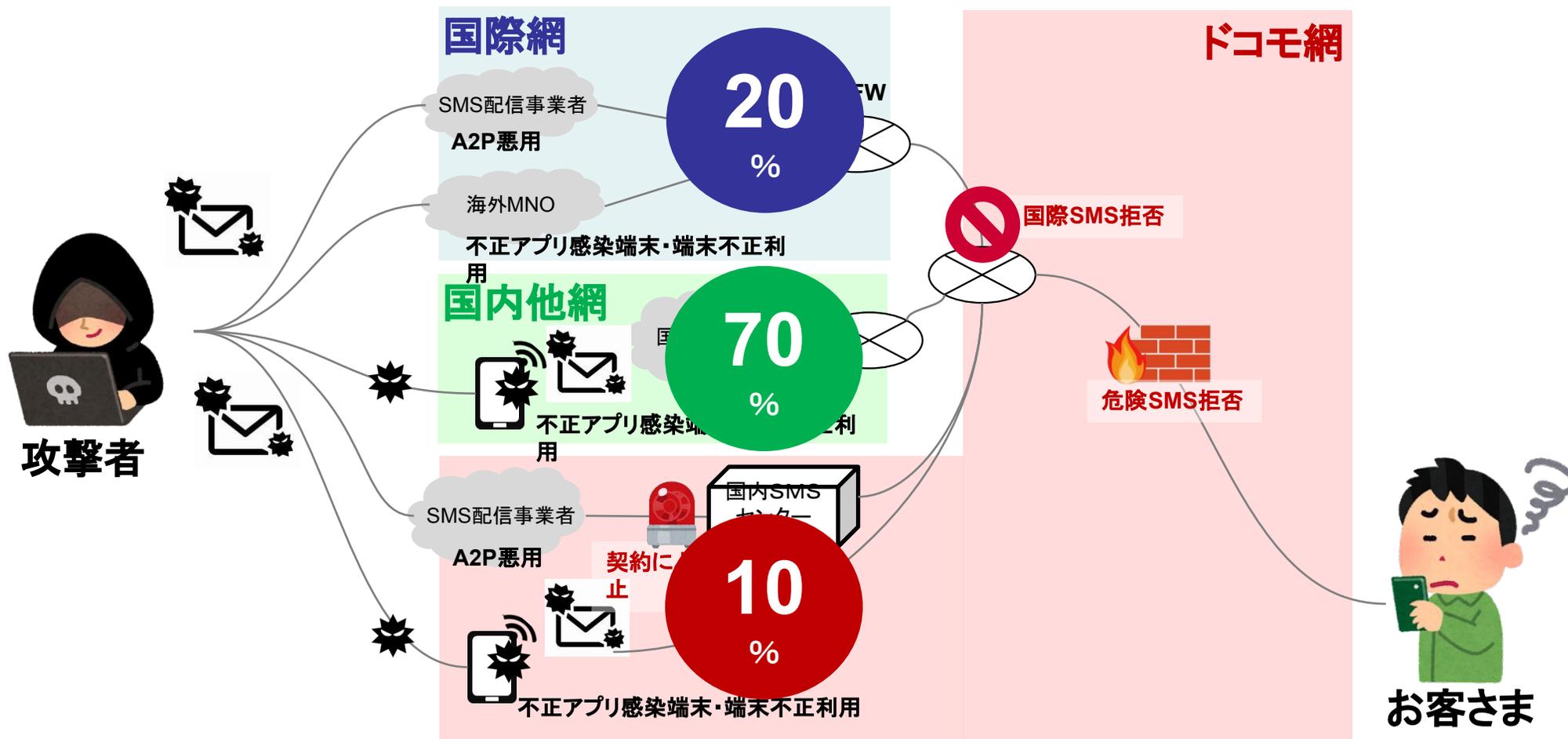
- 
- 
- 個別同意
 - 包括同意

攻撃者はあらゆるルートを使ってSmishingをばらまいている



どのルートが多いの？

※2022/8-10月に危険SMS拒否により検知した通数により算出



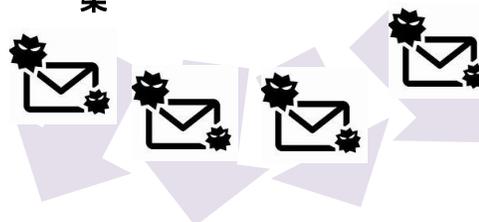
国内ルートがなぜそんなに多いの？



不正アプリ感
染



フィッシングサイ
ト



不正アプリ感染端末から
最大**200**通/日・端末
フィッシングSMSがばらまかれる

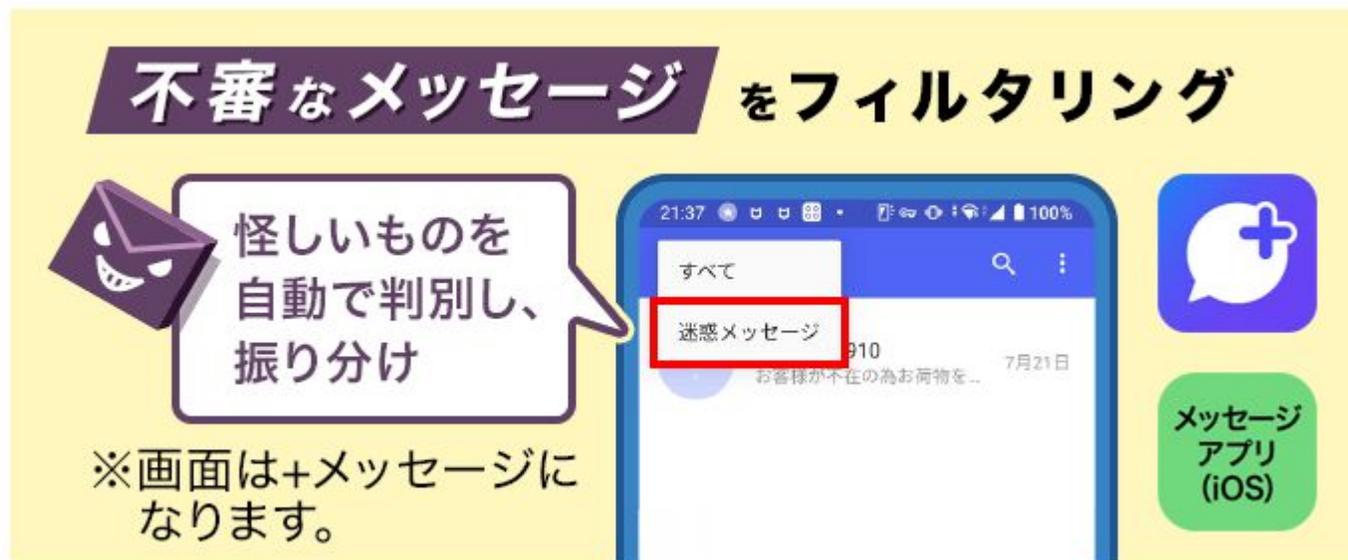


もし、1,000台感染すると
最大**20万**通/日

多層防御によりお客さまの被害を抑止！



あんしんセキュリティ(迷惑SMS対策) 2022年10月27日提供開始!



危険な詐欺SMSだけでなく、
迷惑SMSも強力フィルタ!

ご利用料金

月額220円(税込み)[初回60日間無料]

対応機種

Android™ OS 6.0以降

iOS 14以降

*一部機種を除く

※すべての迷惑SMSを正確に判定することを保証するものではありません。

「危険SMS拒否」と「あんしんセキュリティ(迷惑SMS対策)」って何が違うの？

	危険SMS拒否	迷惑SMS対策
申込	不要(初期値ON)	必要
アプリ	不要	必要
料金	無料	有料
対応機種	すべて	iOS14以上(一部機種除く) Android6.0以上(一部機種除く)
防御方法	ドコモネットワーク上でブロック(破棄)	お客さま端末上でフォルダ分け
防御対象	フィッシング詐欺等の危険なSMS	フィッシング詐欺等の危険なSMS ・迷惑なSMS
送信者への通知	エラー通知	通知なし
特徴	ドコモにて収集した既知の危険なSMSを届く前にブロック	AI技術を駆使し、日々変化する悪意あるSMSをより短時間・広範囲にフィルタリング

iPhoneのメッセージアプリで、SMSにもリアクションが付けられるけど、SMSとしてテキスト送信されている(=SMS送信料がかかる)

iPhone側



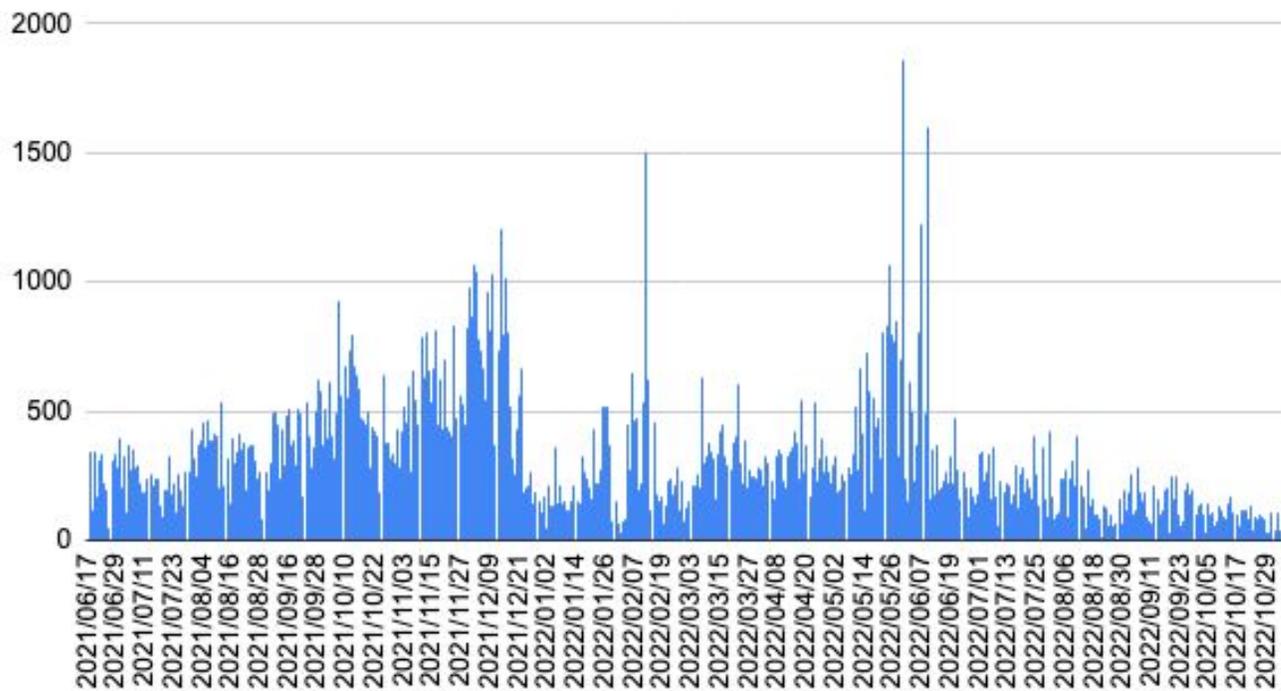
(リアクションを削除)

Android側

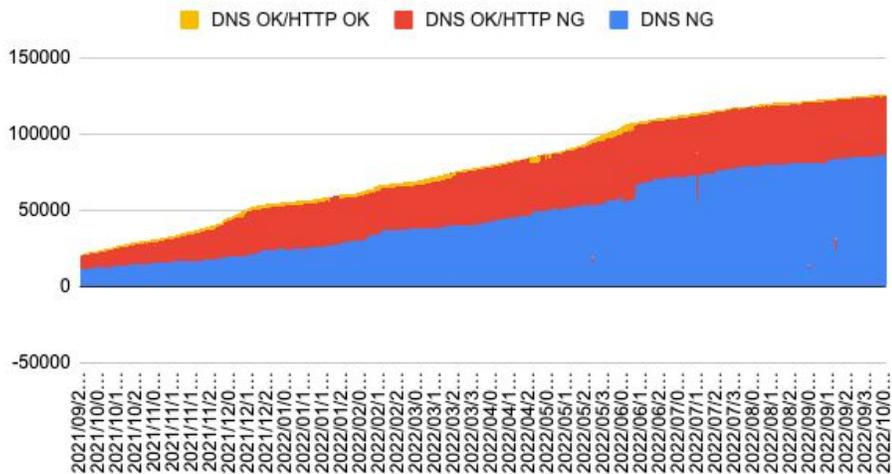


見覚えのないSMS通信料は、これが原因の場合もあるのでご注意ください。

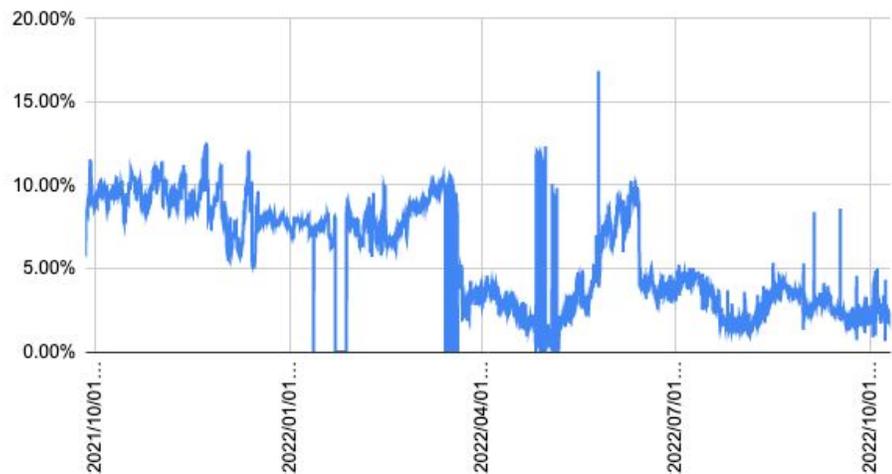
フィッシングURL報告件数(Twitter)



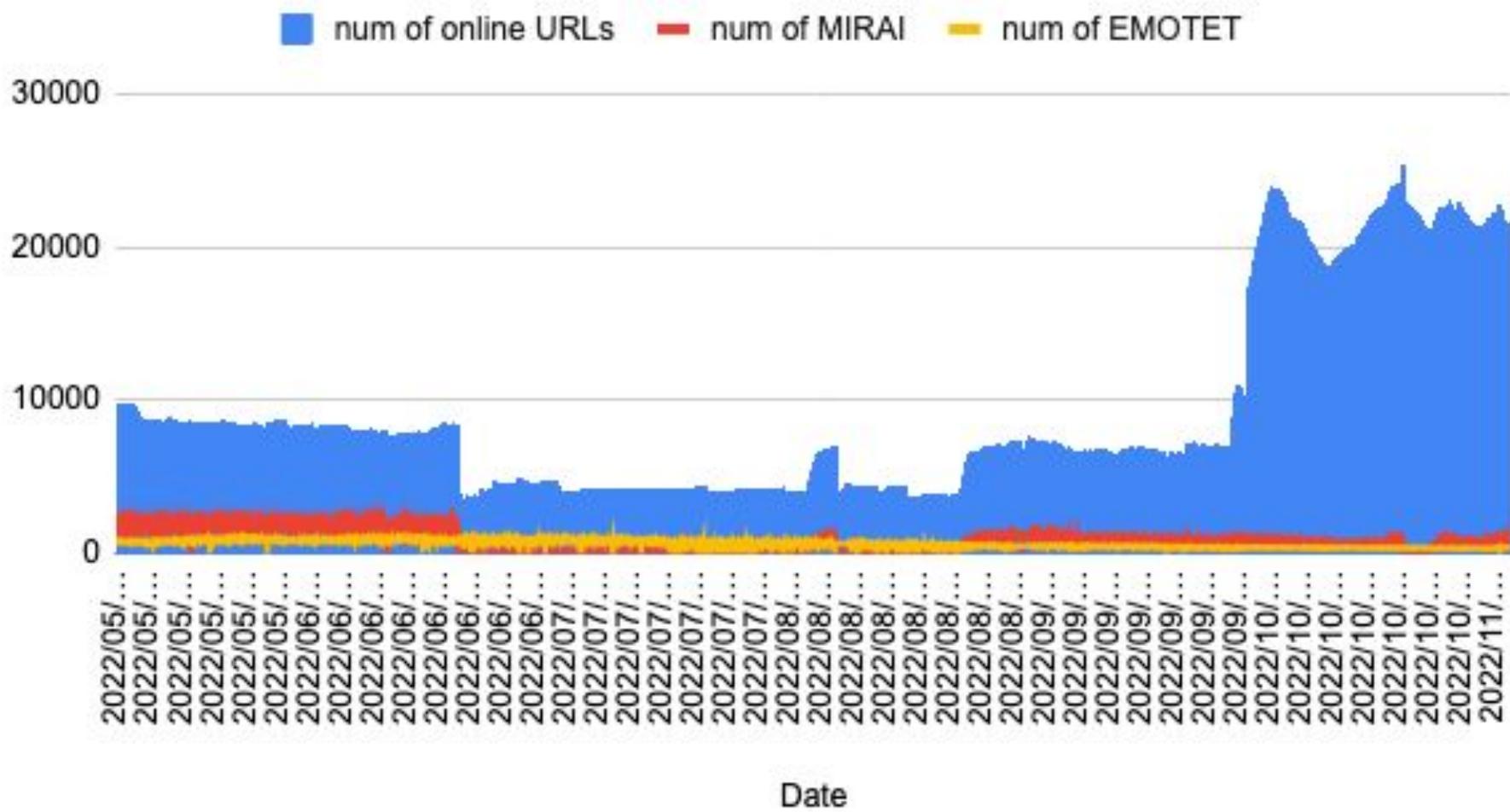
フィッシュサイト稼働状況(Twitter)



稼働率(Twitter)



URLhaus online URLs



Top > “インシデント”の一覧 > JPCERT/CCが確認したフィッシングサイトのURLを公開



中井 尚子 (Shoko Nakai)

2022/08/31

JPCERT/CCが確認したフィッシングサイトのURLを公開

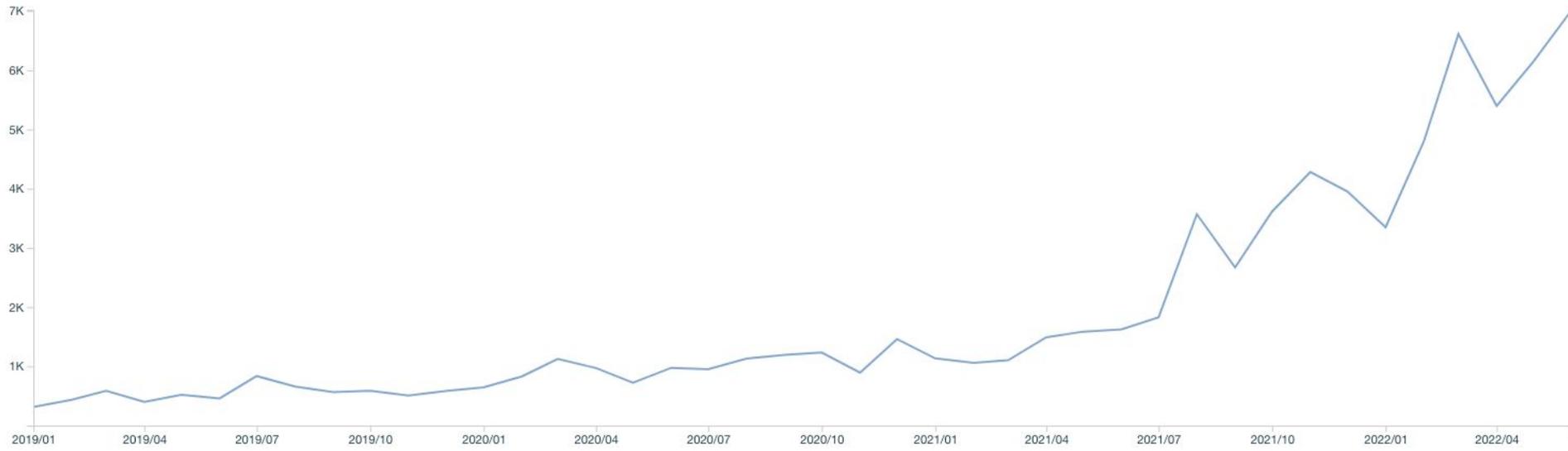
Phishing

ツイート

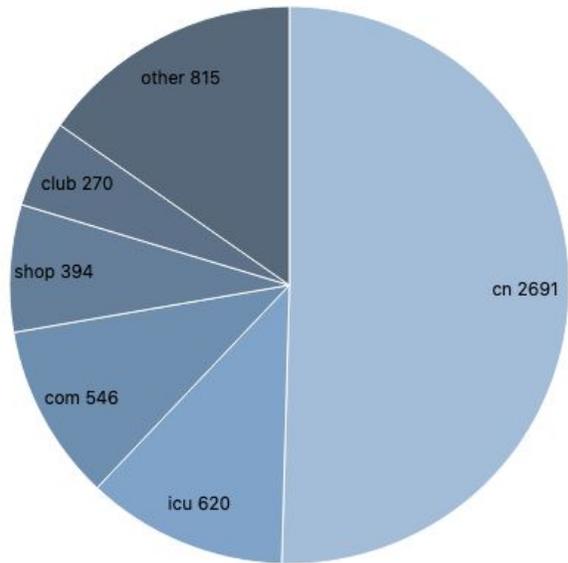
メール

前回公開した2021年度のフィッシングサイトドメインの傾向を紹介した [ブログ](#) を公開後、フィッシングサイト情報を提供して欲しいという要望を多くいただいたため、この度、2019年1月から2022年6月までのJPCERT/CCが確認したフィッシングサイトのURLデータを公開しました。フィッシングサイトのURLデータは、以下のGitHubレポジトリを通じて公開しています。

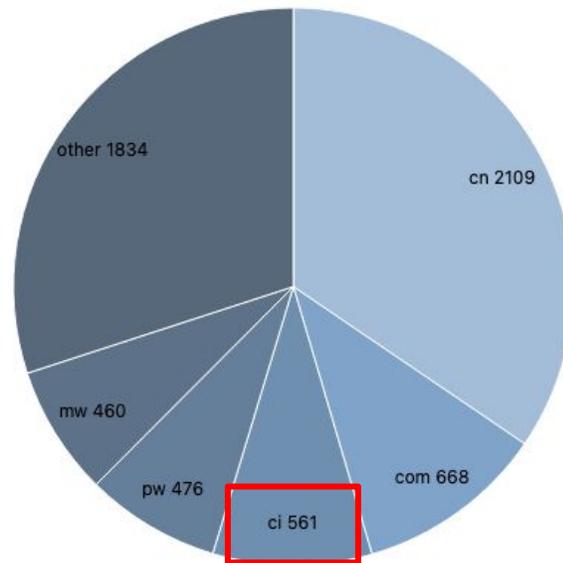
Total number of phishing URLs (per month)



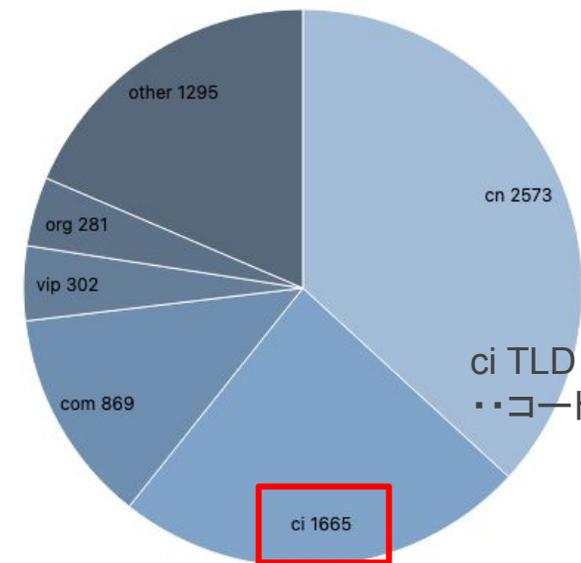
Top 5 Phishing URL TLDs (202204)



Top 5 Phishing URL TLDs (202205)



Top 5 Phishing URL TLDs (202206)



ci TLD
..コートジボワール

事前アンケート

法制度面 (2) 解釈・整備・後押し	外国からのメッセージを 受け付けない機能 効果は？	システム側での 対策方針は？
協力 (2) 情報提供・啓発	SMSは 危険なツール？	プラスメッセージの悪 質利用はある？
偽サイトへの誘導阻止 通報・テイクダウンは有 効？	研究テーマとしての SMS	

電番メッセージによるB2C配信

電番メッセージ： 携帯電話番号宛のメッセージ配信

- ・ スマホを持つ**全ての人に届く「SMS」**
- ・ 画像やファイル送信など**リッチに送れる「+メッセージ（RCS）」**



電番メッセージの市場規模

世界的な市場規模は2-3兆円

- ・ **全てのスマホ宛に送れるので、海外ではB2Cメッセージの主媒体**
- ・ 二段階認証に加えて、歯医者予約、宅配便の連絡、クーポン取得 など
- ・ 日本の市場規模は**21年度で約150億円**



Globalでは
2-3兆円



人口や経済規模から
更なる成長の余地あり



18年度

21年度

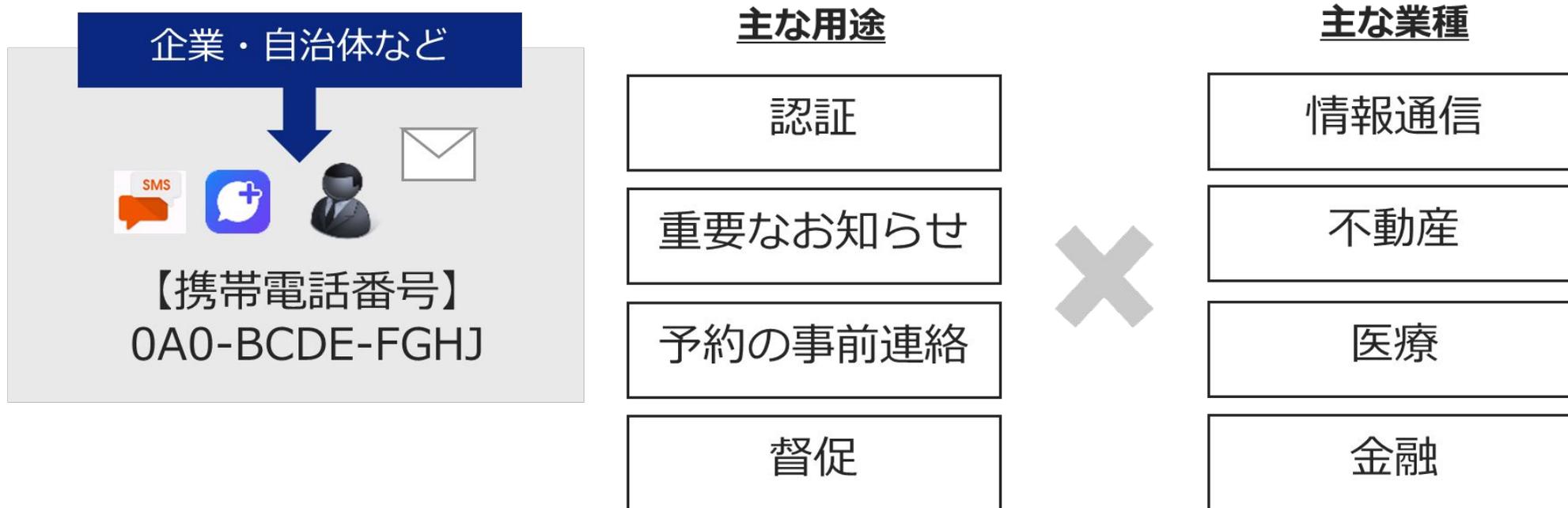
40億円 → 150億円

3年で約4倍

どのようなユースケース・業種

日本でのSMS利用用途

- ・ アプリやサービスの**認証** (OneTimePassword・二段階認証)
- ・ 重要なお知らせ・予約・督促などの**業務連絡用途が近年増加**



電番メッセージの特長

SMSの良さ

- ・ 手軽 : **電話番号**さえ分かれば送れる (配信の許諾は必要)
- ・ シンプル : **テキスト**文章のみ (良くも悪くも)
- ・ 本人性 : 携帯電話 (= 番号) はキャリアが**本人確認済み**

※「携帯電話不正利用防止法」に基づく本人確認

SMS

【携帯電話番号】
0A0-BCDE-FGHJ



課題

利便性

主に片方向

送信元が分かり難い

セキュリティ

詐称・なりすまし

機能拡充

1

SMS共通番号
+上り/双方向

2

迷惑対策

機能拡充①

SMS共通番号+上り/双方向

- ・ **SMS専用の番号「SMS共通番号」**を携帯電話キャリアで制定・統一化
- ・ キャリアが利用**企業を審査**し、番号を払い出し
- ・ 共通番号宛に、お客様からの上りメッセージ=**双方向のやり取り**も可能

SMS共通番号

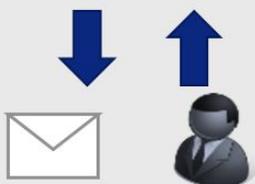
最小8桁～最大10桁
0005-ABCDEF

ドコモ

ソフト
バンク

au

楽天



※ 現時点ではドコモ、ソフトバンク、
KDDIで利用可能
楽天モバイルも準備中

特長

企業審査
→ なりすましを防止

専用の番号
→ 識別が容易

双方向のやり取り
→ 用途の拡大

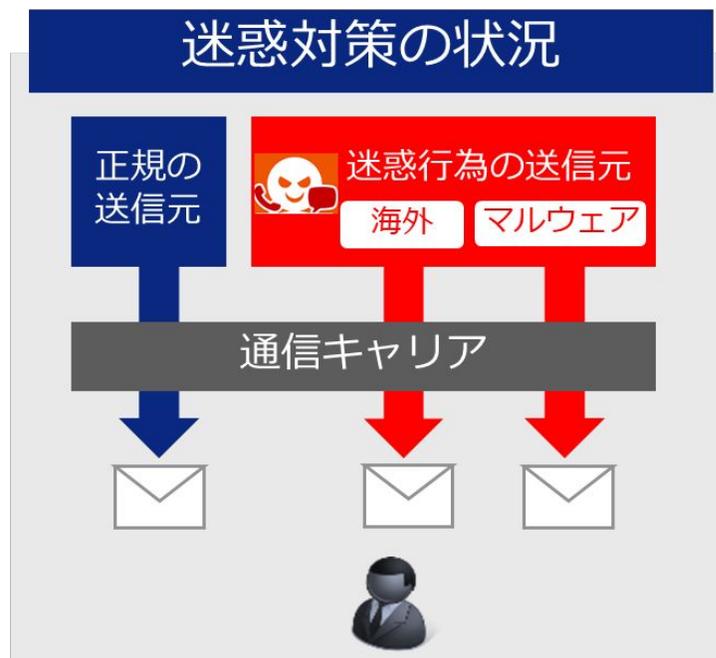
企業・自治体の
代表番号としての利用へ

機能拡充②

迷惑対策

- ・ **SMSの最大の課題は、詐称・なりすましの迷惑行為への対策**
 - ・ **そもそも、何故発生するのか？ 通信キャリアは根本対策しないのか？**
- **通信は、発生源や中身に関わらず、必ず繋げなければならない**

迷惑対策の状況



特長

主な発生源

- ・ 海外から（国際電話網）
- ・ マルウェア感染したスマホから

キャリアの対策

- ・ これまでの対策は「限定的」
- 憲法第21条第2項規定の「**通信の秘密**」

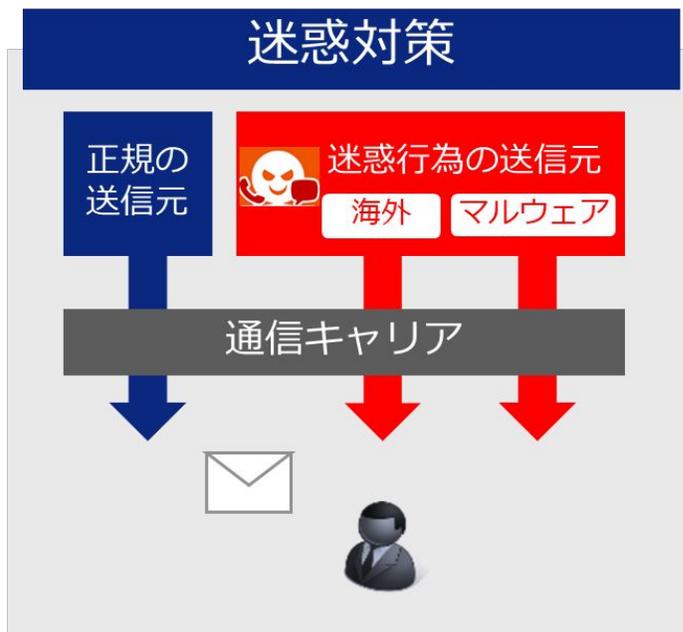
検閲は、これをしてはならない。
通信の秘密は、これを侵してはならない。

どのような内容であれ（犯罪行為だとしても）、公権力や、通信当事者以外の第三者が事前に把握したり、止めることを禁止

機能拡充② つづき

迷惑対策

- ・「通信の秘密」 通信キャリアは何もできないのか？ しないのか？
- **お客様からの申告や同意をいただくことにより、対策可能**



特長

業務的な対策

- ・ 迷惑行為の送信元への、利用停止措置
- ・ **お客様からの申告**があると、対応への法的根拠を得る

アプリでの対策

- ・ 迷惑な内容を受信する端末側での対策
ブロックや警告を実施
- ・ **お客様でのインストール**が必要

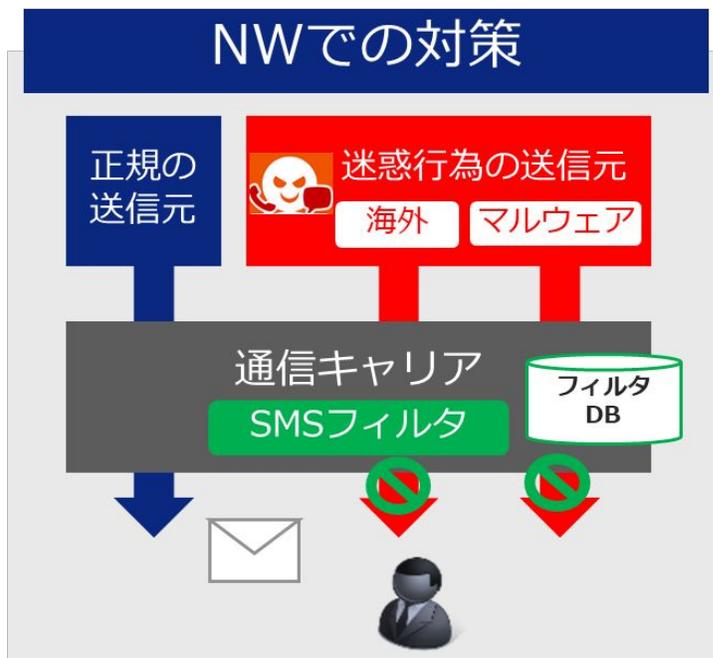
NWでの対策

- ・ お客様に届く前に事前にブロック
- ・ **お客様から事前に、個別かつ明確な同意**を取得

機能拡充② つづき

NWでの対策：SMSフィルタ

- ・ 通信キャリア側の設備で、内容を分析し、**迷惑と判定したSMSをブロック**
- ・ 全てのお客さまに「**デフォルトON**」「**無償**」で提供



特長

お客さまに届く前に、NW側で破棄

本機能が不要なお客様は任意でオプトアウト

フィルタ対象はお客様申告や警察などからの情報で更新

お客様を守りつつ、SMSの価値を維持する

SMSのまとめ

SMSは「手軽」「シンプル」「本人性」から**日本でも活用が拡大**

- ・主に「認証」「重要なお知らせ」で利用。さらには「広告」「販促」も。
- ・利用拡大の為、キャリア各社が**機能拡充**を実施
 - 「**共通番号を導入**」 → 企業の代表番号・双方向など利用シーン拡大へ
 - 「**セキュリティ・迷惑対策強化**」 → お客様がより安心安全に

さらなる進化へ

プラス
+メッセージ 

+メッセージ 公式アカウント

企業・自治体とのやり取りが可能な「公式アカウント」

- ・安心・安全 : 利用企業を全て**キャリアが審査**
- ・便利 : 返信ボタン機能により、**双方向**のやり取りが簡単
- ・高い効果 : 開封率やクリック率(CTR)/遷移率(CVR)が高い

「公式アカウント」

安心・安全
 認証された企業を、
 ロゴや認証済みマークで
 分かりやすく



認証済み
 マーク

便利
 写真や動画も届いて、
 返信も簡単に



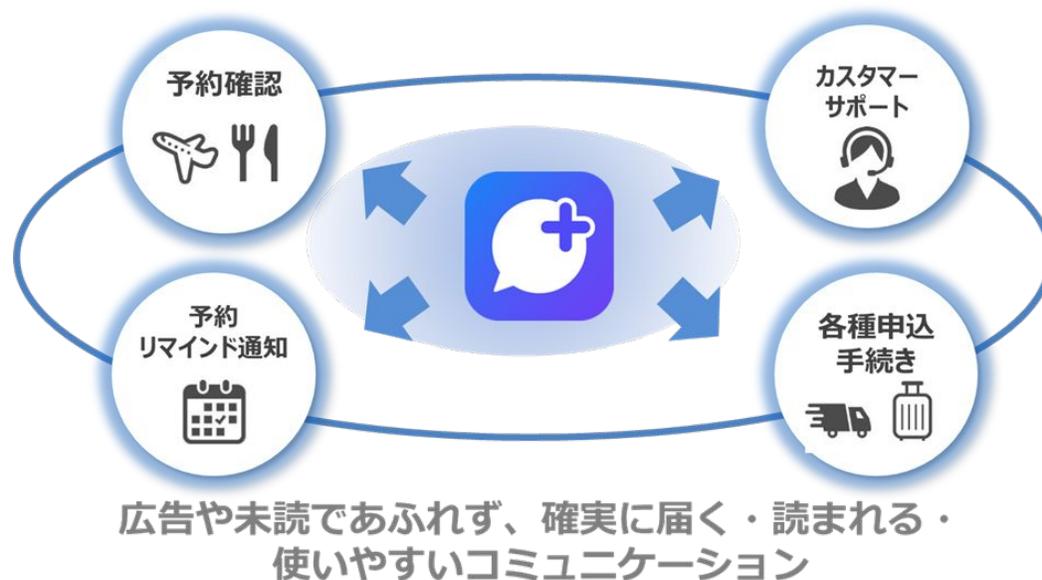
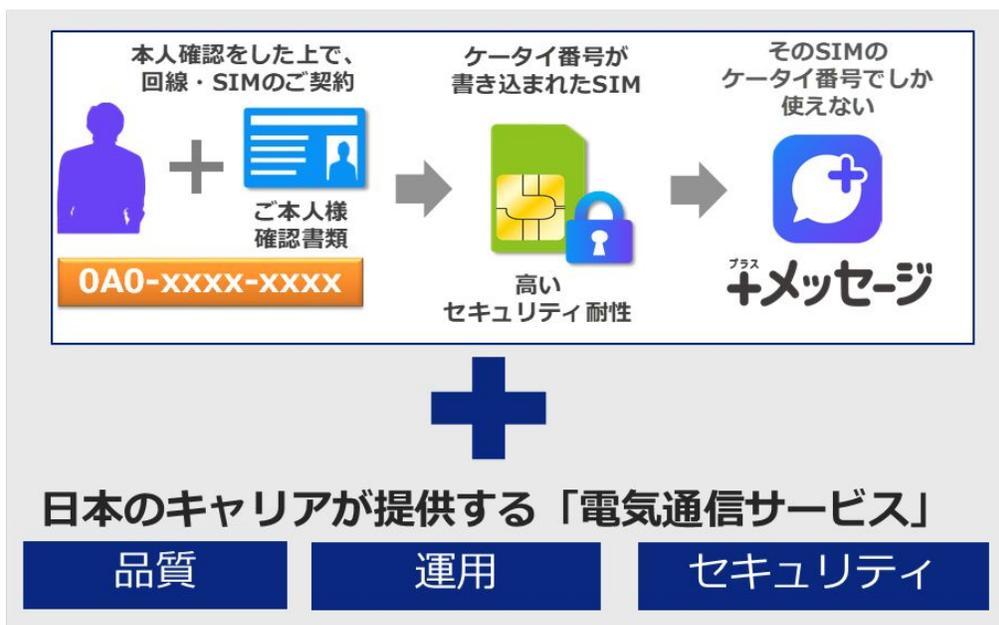
		 +メッセージ	SMS	メール
反応	開封率	高	計測不可	低
	遷移率 (CTR・CVR)	高	低	低
ボット機能連携		○	×	×
安心	お客様の 本人確認性	○	○	×
	アカウントの なりすまし防止	○	×	×

※+メッセージ利用者以外には自動的にSMSで送信可

+メッセージ キャリアとしての想い

通信キャリアによるUniversal・Public・Secureなメッセージングサービス

- ・ Universal : 国際標準準拠（GSMA標準であるRCS。欧米・中韓でも利用）
- ・ Public : PublicなIDである電番
- ・ Secure : キャリア運用のサービス・設備



+メッセージとJPKI連携

2022年7月~+メッセージアプリに、**JPKI機能を搭載**

- ・公式アカウントから、**マイナンバーカードの読み取りが可能に**
- ・**公的個人認証**により、さらに便利でセキュアな利用シーンへ

プラメ x JPKI



主な用途

オンライン手続き時の
本人確認

銀行口座開設
証券会社の証券口座開設
クレジットカード発行 など

本人限定メッセージ
(郵便物のデジタル化)

公共料金の案内
検診・予防接種の案内 など

銀行の預金残高通知
保険会社の保険証券・満期案内
クレジットカードの利用明細 など

電番メッセージ おわりに

電話番号をIDとして、お客様と企業を、便利に、**安心安全に繋ぐ**
通信キャリアが提供するUniversal・Public・Secureなサービス

- ・ 全てのお客様に到達可能で、シンプルな「SMS」
- ・ リッチなやり取りや、厳格な本人確認の時は「+メッセージ（RCS）」

SMS

手軽

シンプル

本人性



プラス
+メッセージ 

リッチ

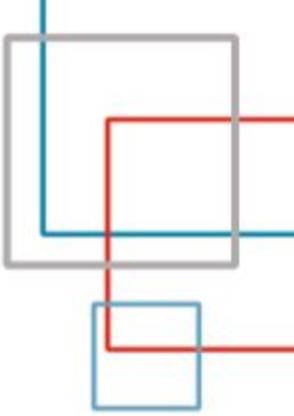
高い効果

JPKI



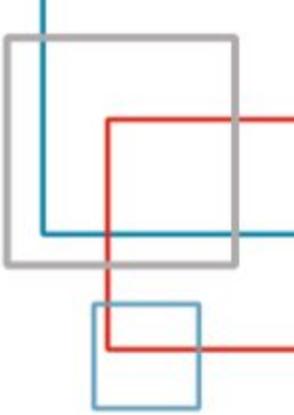
電話番号をキーに
安心・安全に繋がる世界へ

お客様と企業の
コミュニケーションのDX化を支援



パネルディスカッション





Q & A



事前アンケート

法制度面 (2) 解釈・整備・後押し	外国からのメッセージを 受け付けない機能 効果は？	システム側での 対策方針は？
協力 (2) 情報提供・啓発	SMSは 危険なツール？	プラスメッセージの悪 質利用はある？
偽サイトへの誘導阻止 通報・テイクダウンは有 効？	研究テーマとしての SMS	

ありがとうございました

