JPAAWG 8th General Meeting

MNOキャリア4社のスミッシング対策について

docomo	株式会社NTTドコモ	齋藤 森史
KDDI	KDDI株式会社	尾谷　真知子
Rakuten Mobile	楽天モバイル株式会社	本田 景輔
SoftBank	ソフトバンク株式会社	松崎 達彦

Agenda

- 自己紹介
- メッセージビジネストレンド
- スミッシング対策啓蒙活動
- 能動検知とスミッシングのトレンド
- 感染端末の減少、SMS配信ガイドラインについて

株式会社NTTドコモ
コンシューマサービスカンパニー
マーケティング戦略部　コミュニケーションサービス担当　担当課長

齋藤 森史

- NTTドコモに入社後、スマートフォン製品の品質管理や商品企画、ハードウェア関連の要素技術探索や導入などの業務に従事。スマホの黎明期から最近まで、様々なプロダクトとともに駆け抜ける。
- 2024年からドコモメール/プラスメッセージ/SMSのサービス主管業務に従事。現在も国内の迷惑SMS対策に奔走

※昨年のJPAAWGで登壇した弊社　三谷よりバトンをうけ
　極度の緊張のもと本日に臨んでいます。

KDDI株式会社
事業創造本部　メッセージサービス戦略部　事業企画グループ

尾谷　真知子

電番メッセージ（SMS/RCS）のプロダクト担当
2023年より、電番メッセージ事業に参画。迷惑対策やB2C事業拡大に従事。

※本日は急遽弊社小頭が欠席となり申し訳ございません。

本田 景輔

楽天モバイル株式会社

情報セキュリティガバナンス推進本部

•

2000年頃より電気通信サービスを利用した不正事案（ABUSE）対策関連業務に携わる。

•2018年より楽天グループ（株）にて情報セキュリティガバナンス部門に従事。

•2020年より楽天モバイル（株）情報セキュリティガバナンス推進本部長を兼務。

ソフトバンク株式会社
コミュニケーションサービス開発本部

松崎 達彦

・モバイルシステム開発導入業務
・2021年よりSMS/メール系業務
  - 迷惑SMS判定機能の導入を担当
  - スミッシングや迷惑メールと格闘中

メッセージトレンド

KDDI株式会社　小頭 秀行

電番メッセージによるB2C配信

KDDI

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「RCS」**

【携帯電話番号】
0A0-BCDE-FGHJ

電番メッセージの市場規模

KDDI

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、歯医者の予約、宅配便の連絡、クーポン取得　など
- 日本の市場規模は**24年度で約250億円**

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　24年度

40億円 → 250億円

6年で約6倍

どのようなユースケース・業種

日本での利用用途

- **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**

主な用途		主な業種
認証		情報通信
重要なお知らせ	×	不動産
予約の事前連絡		医療
督促		金融

要するに

KDDI

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

企業・自治体など

【携帯電話番号】
0A0-BCDE-FGHJ

✓
- 便利でコスパもよいので、沢山使われている
- B2C市場全体はCAGR+30%成長が継続

→ 市場＆用途の拡大は止まっていない

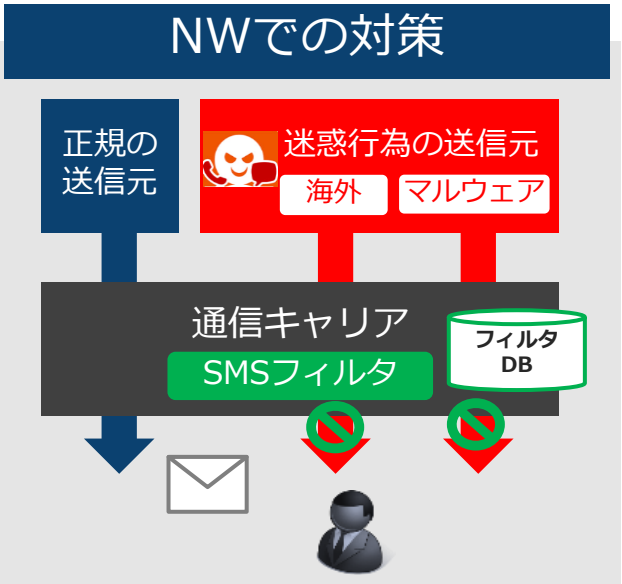
✕
- 送信元のなりすまし
- 電話番号だけで（勝手に）送れる

→ 便利で伸びているからこそ、悪用も増えている

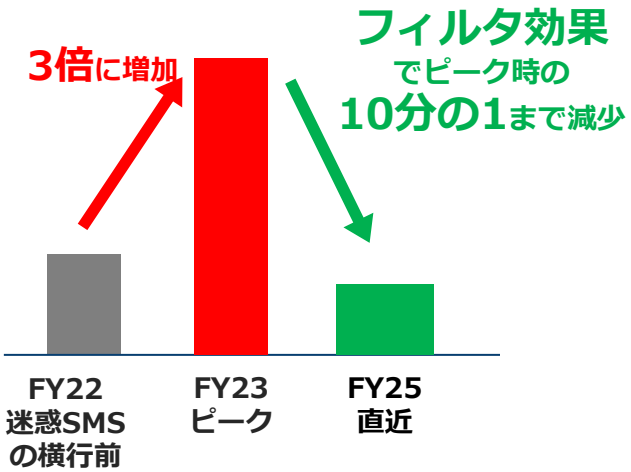
迷惑SMS向けの対策

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



お客様からの迷惑申告数



フィルタを
チューニングしながら
運用・改善

お客様を守りつつ、
SMSの価値を維持する

SMS共通番号/共通ショートコードとは

KDDI

SMS専用の番号「SMS共通番号」

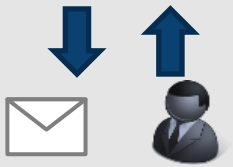
- **携帯電話キャリア4社で制定、統一化（全てのMNO＆MVNOで利用可能）**
- **キャリアが利用企業を審査し、番号を払い出し**
- **共通番号宛に、お客様からの上りメッセージ＝双方向のやり取りも可能**

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



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

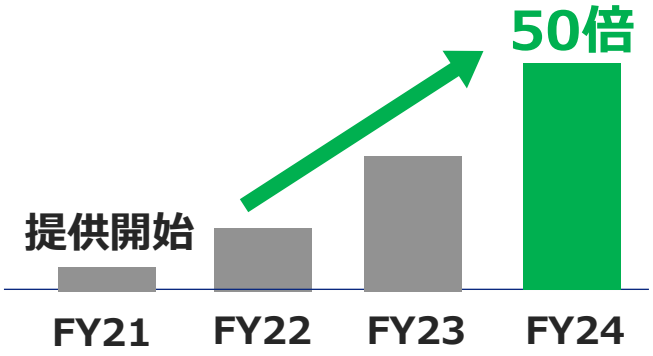
SMS共通番号/ショートコードによる課題解決

KDDI

- 「SMS共通番号」は**提供開始から3年で50倍に拡大**
- 企業・自治体・お客さまの認知拡大に向け、MNO4社が連携した
  「共通番号のキャリア統一サイト」を公開
  → **送信元の確からしさをMNO4社が証明・認定**し、信頼性を高める

普及状況

開始から3年が経ち、普及期へ



認知拡大

SMS共通番号のキャリア統一サイトを一般公開

https://japansms.com/

KDDI

RCS/プラスメッセージでの「公式アカウント」
・安心・安全な送信元として、利用企業を全て・事前に、キャリアが審査
・アプリ上で簡単に見分け表示する為の企業ロゴ＆チェックマーク

お客様による評価

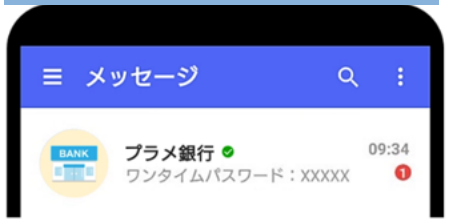
KDDI

・お客様の受け止め方について、UIUX調査（定性）を実施
・「SMS共通番号」よりも「RCS公式アカウント」の方が好ましい、との結果

SMS共通番号

▲
・電話番号のみだと、確からしさが不明
・共通番号を知らない

RCS公式アカウント

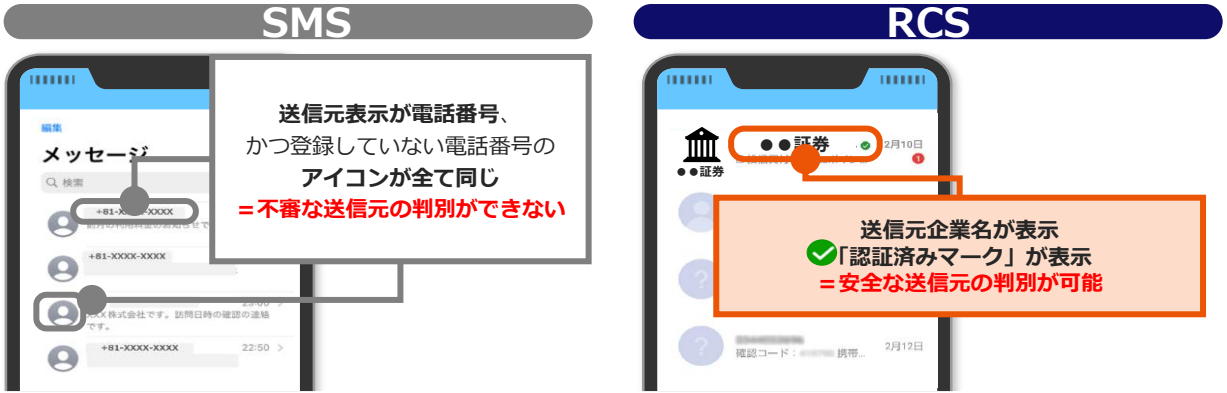


✓
・企業ロゴがあり分かりやすい
・チェックマークもあり、安心

KDDI

SMSでは不審な送信元の判別ができない

➡ RCSでは送信元企業名と認証済み表記により、安全な送信元の判別が可能

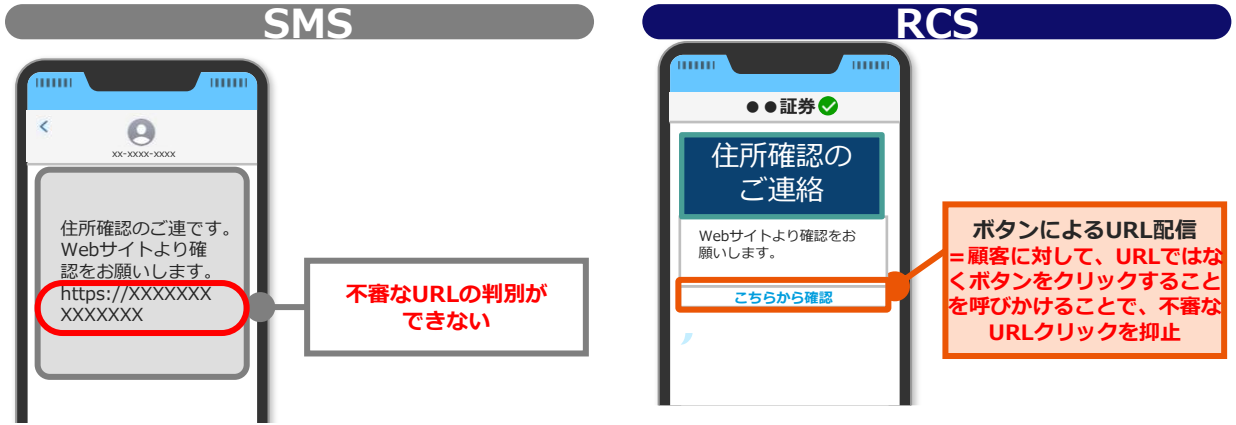


KDDI

SMSでは不審なURLの判別できない

➡ RCSでは、**ボタンによるURL配信が可能。**
URLではなくボタンをクリックすることを呼びかけることで、
不審なURLクリックを抑止

※認証済みマークやボタンの表示は、携帯キャリアが審査し承認した送信元のみが設定可能



おわりに

・通信キャリアにて、各種迷惑対策を強化中
　NW側：SMSフィルタのチューニング。但し、完全には防ぎきれない。
＋「SMS共通番号」「RCS公式アカウント」でホワイトな送信元を明示。
→ お客様と企業を、電話番号で安心安全に繋ぐ

NWフィルタ

共通番号・公式アカウント

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

Rakuten Mobile

スミッシングに関するユーザ向け注意喚起・啓発活動について

楽天モバイル株式会社　本田 景輔

スミッシング対策とユーザ向け注意喚起・啓発活動

- 楽天モバイルの迷惑SMSフィルタリングサービスの提供は2024年7月。
- 一定の効果はあるものの、フィルタをかいくぐるスミッシングの手口は巧妙化。
- 各種媒体によるフィッシング・スミッシングに関する注意喚起は継続して実施する必要がある。

「スミッシング対策入門（2022年」）

https://network.mobile.rakuten.co.jp/guide/security/cyber-bousai2022/

「迷惑SMS拒否設定（2024年」）

https://network.mobile.rakuten.co.jp/service/sms-filter/

事例①：ノベルティ（クリアファイル）の無償提供による啓発

- セキュリティ啓発を主旨としたノベルティを制作
- 詐欺対策の一つとしてフィッシング
- イベント等で無償配布

事例②：シニア向けセキュリティ啓発の動画およびクイズ

Rakuten Mobile

- 楽天シニアが提供するスマホ教室というサービスの中で、シニア向けの啓発施策を2024年3月にリリース
- 3つのトピックに対してそれぞれのトレーニングビデオとクイズを提供している。

事例③：セーフティ教室の開催

Rakuten Mobile

- 近隣の公立中学校を訪問し、セキュリティ部門社員による講義を実施
- 先述のクリアファイルを配布し、コンテンツに連動した内容でオンラインでの詐欺に対する啓発を行った

迷惑SMSの昨今のトレンドと“能動通知”の取組

株式会社NTTドコモ　齋藤 森史

キャリアによる迷惑SMS対策の全体像（ドコモの事例）

docomo

■ キャリアは通信の秘密を守りながら、お客さまの申告や同意に基づいて迷惑SMS対策を実施

Smishing発生の背景

通信事業者は送信元やSMSの内容に関わらず メッセージを届ける必要があり、検閲不可

憲法第21条第2項に規定される「通信の秘密」により、
キャリアはSMSの内容を検閲することができない

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。

海外ルートやマルウェア感染した
スマホからなりすましが発生

2022年では、フィッシング対策協議会に報告された
フィッシング詐欺[1]は**約970,000件**にまで膨れ上がっている[2]

キャリアによる対策例[3]

お客さまからの申告や同意をいただくことにより、以下のなりすまし対策を実施

業務面	・迷惑行為の送信元への、利用停止措置 ※お客さまからの申告が措置の法的根拠となる
アプリ面	・端末側でブロックや警告を実施 ※お客さま側でのインストール/設定が必要
ネットワーク面	・キャリアのシステムで迷惑SMSを検知して、お客さまへ届く前にブロック ※お客さまから事前に同意を取得して実施

＋

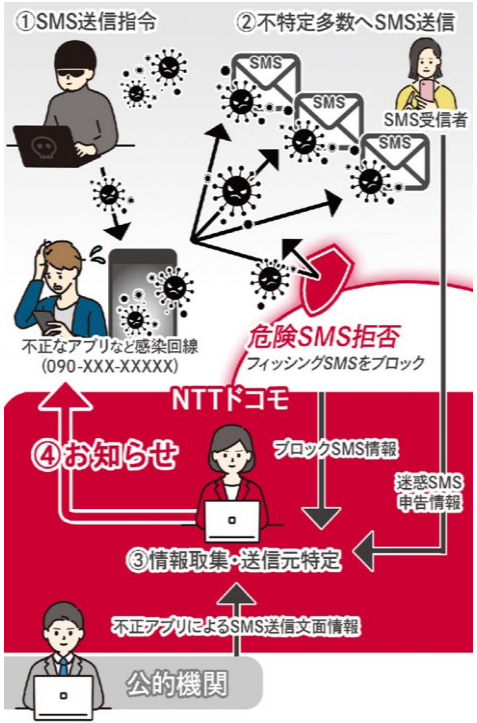
マルウェア感染疑いのお客様への能動通知

1. 実在する組織を騙って、クレジットカード番号などの個人情報を詐取することにより金銭を盗み取る詐欺
2. フィッシング対策協議会の月次報告書（https://www.antiphishing.jp/report/monthly/）をもとに算出。SMS以外の配信手段（Email等）に届いたフィッシング詐欺の件数も含む
3. ドコモの例であり、各キャリアごとに対策内容は異なる

ドコモの対策例：危険SMS拒否設定とマルウェア感染が疑われるお客様への能動通知

docomo

■ドコモでは“危険SMS拒否設定”という迷惑SMSをお客様に届かせない仕組みを運用しています。
■更に、お客様の携帯電話がフィッシング詐欺の踏み台にされている可能性を検知した際にお客さまへご連絡を行う能動通知施策（意図せぬ迷惑メッセージ送信に関するお知らせ）を昨年度より開始しました



意図せぬ迷惑メッセージ送信に関するお知らせ

概要

お客さまの携帯電話が知らないところでフィッシング詐欺の踏み台にされている可能性をお知らせし、ご確認と削除のお願いを実施します。

お申し込み　：不要（オプトアウト方式）
月額使用料　：無料
提供開始日　：2024年7月1日～

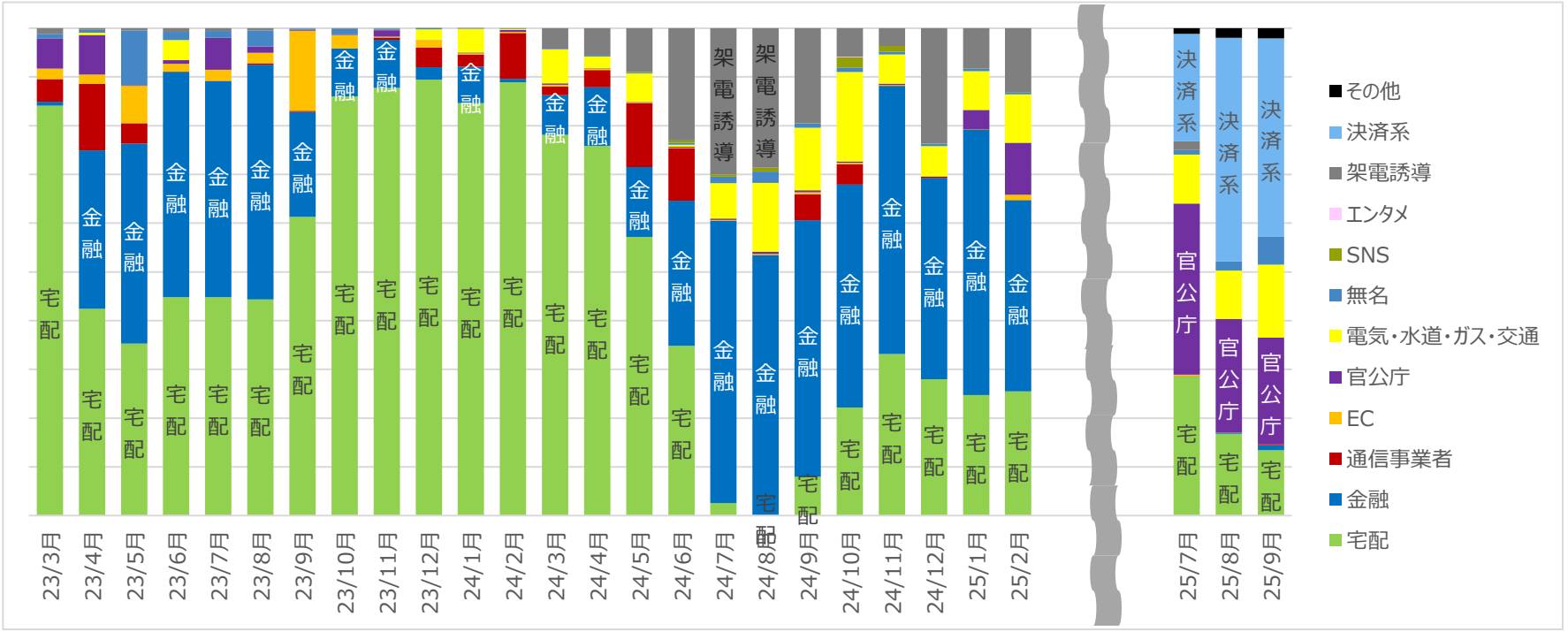
【お客様に届くお知らせのイメージ】
ご利用中の回線において、不正なコンテンツ等のインストールを促したり、個人情報を盗み取ろうとする危険なメッセージの送信行為が確認されました。お客さまの意図しない送信行為が行われている可能性があります。身に覚えのないアプリがインストールされていないかのご確認、および削除をしていただきますようお願いいたします。

▼「身に覚えのないアプリ」の確認および削除方法の案内

フィッシングSMSのトレンド：騙られたジャンル推移　（過去の中長期スパン）

docomo

■ 過去猛威を振るってきた宅配騙りの件数が減少し、官公庁や決済系が増加



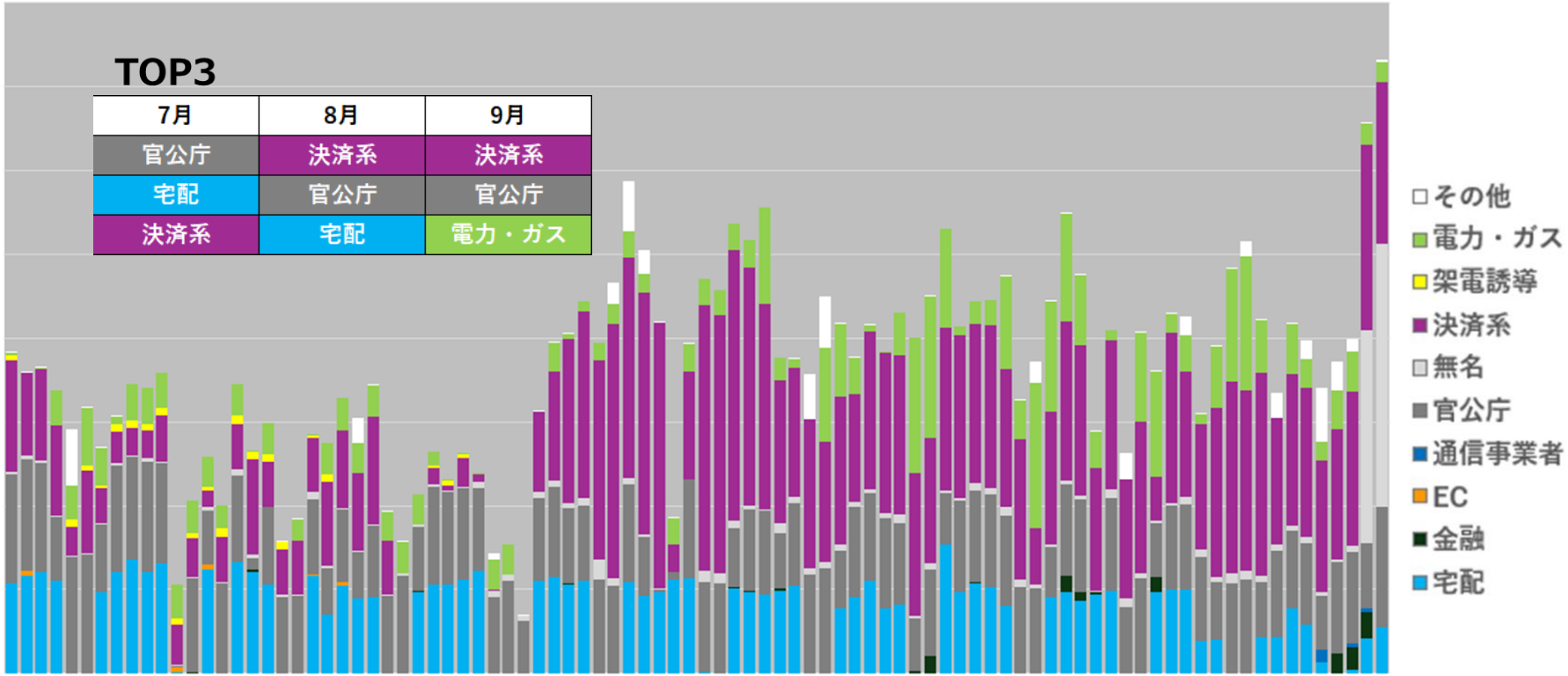
※ドコモ回線宛に対し分析

フィッシングSMSのトレンド：騙られたジャンル推移（直近のスパン）

docomo

■ 直近は官公庁・決済系・宅配・電力・ガスなどを騙ったスミッシングが多発しており、日々流量も変化

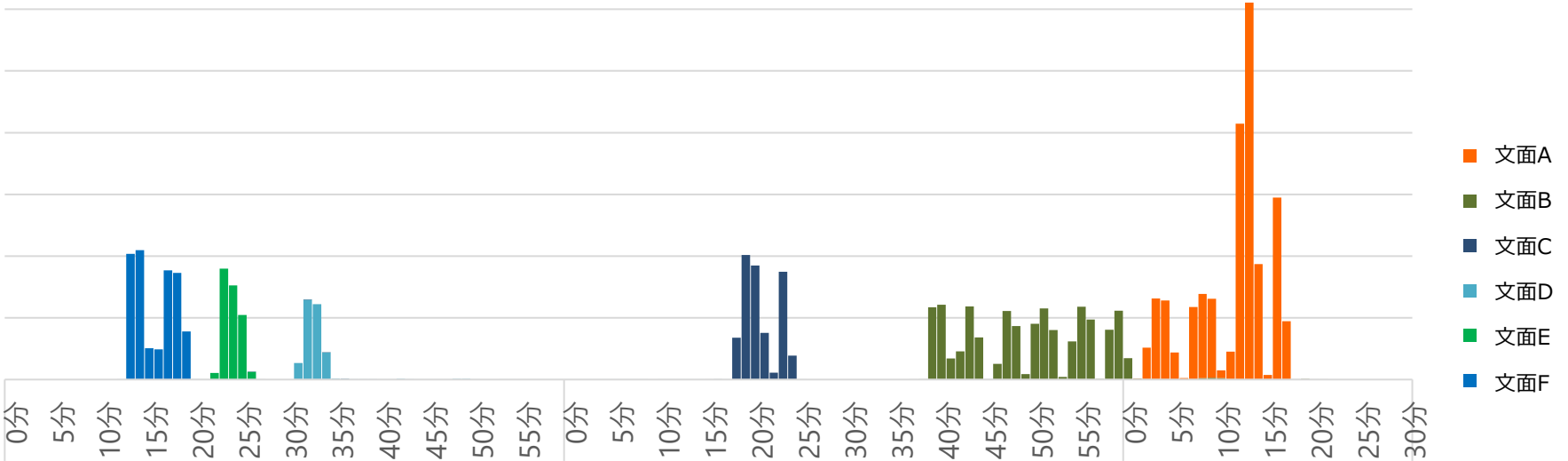
Smishing　騙られた企業・サービス別　直近の検知数推移



フィッシングSMSのトレンド：以前の攻撃傾向

■ 以前は同じフィッシングSMS文面が一定時間大量に送信される傾向が見られた

過去ある日の攻撃例：Smishing文面の短時間変化(宅配騙り)

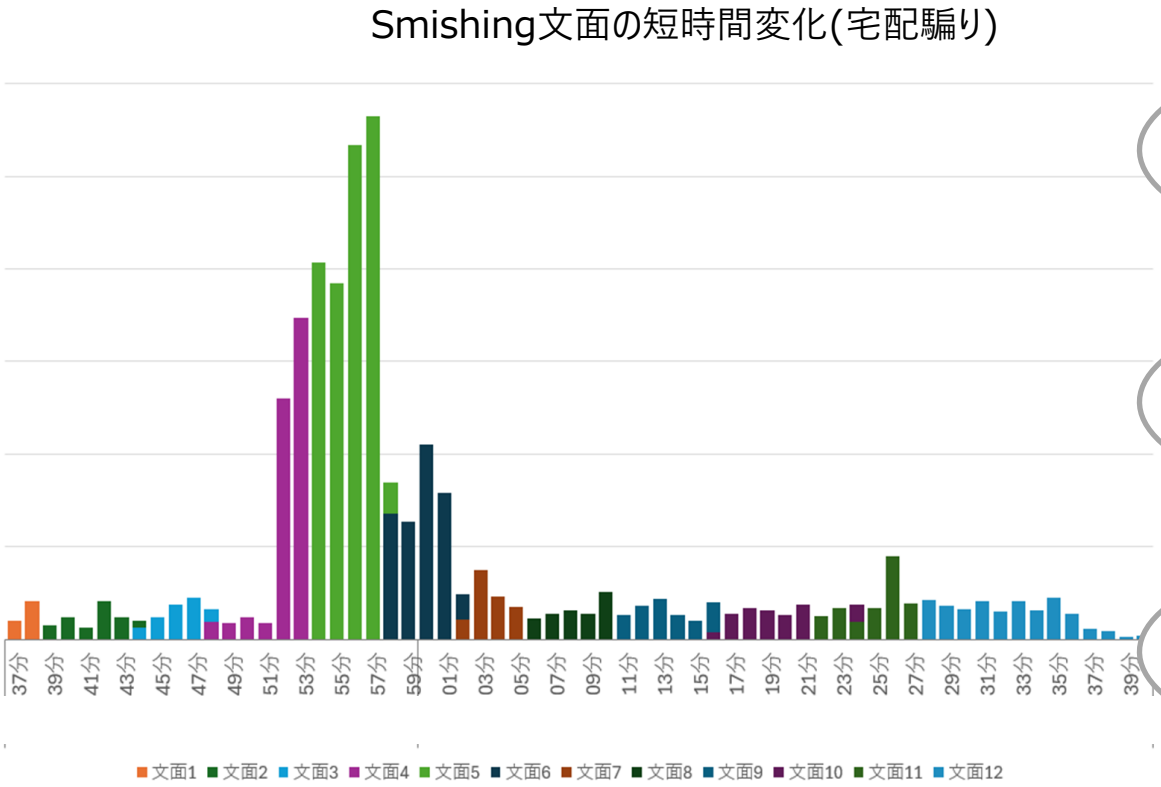


※ドコモ回線宛に対し分析

フィッシングSMSのトレンド：直近で観測されている攻撃傾向

docomo

- 現在は以前に比べ短時間で文面が変わる傾向が見られる
- AI等により多くのフィッシング文面が作成できるようになったことで、スミッシングが巧妙化している可能性が示唆される



ご不在でしたので、荷物を持ち帰りました。
こちらでご確認ください。
https://t.co/XXXXXXXXX

お客様が外出されていたため、荷物は当社の営業所で保管しています。
https://t.co/YYYYYYYYY

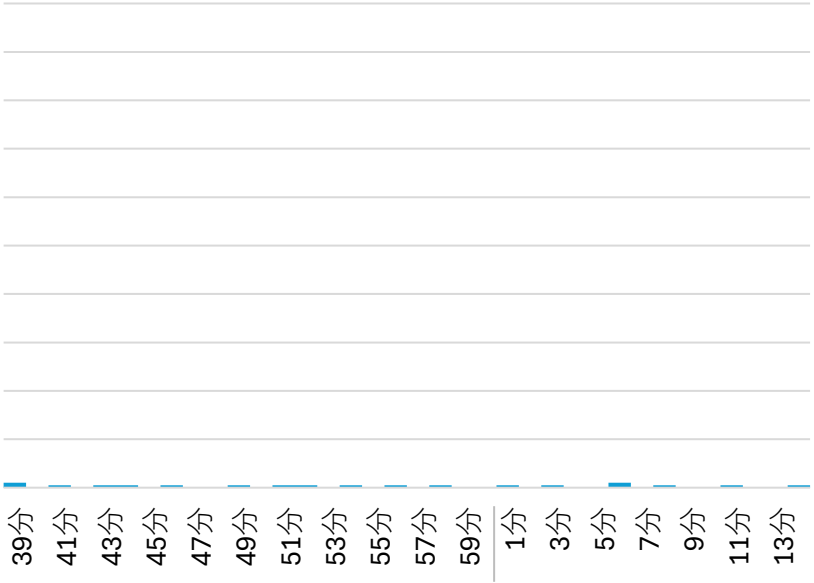
お荷物の配達を再調整しています。新しい配達日時をご確認ください。
https://t.co/ZZZZZZZZZ

※ドコモ回線宛に対し分析

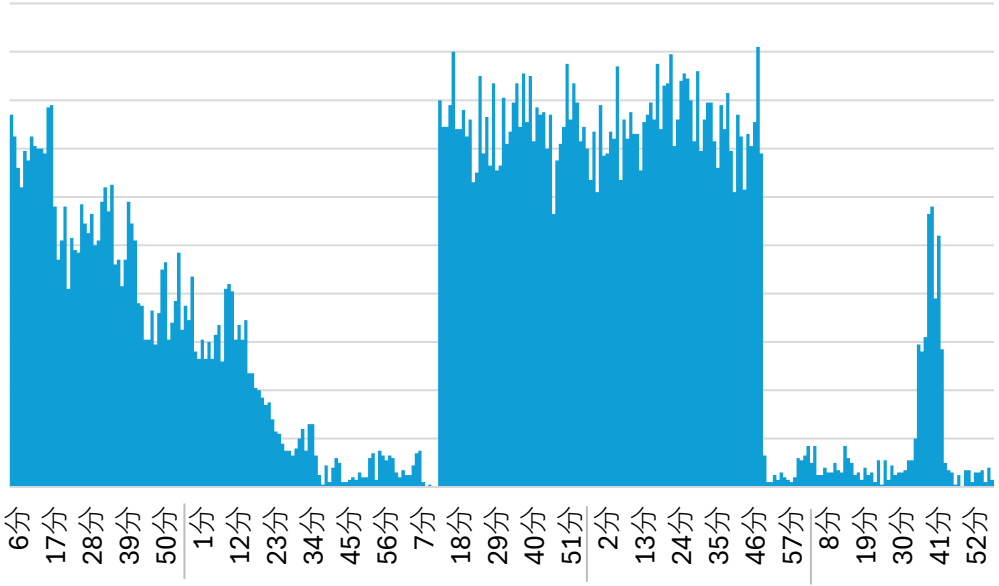
フィッシングSMSのトレンド：直近で観測されている攻撃傾向

docomo

新規文面パターン数(9月上旬のある1日)



新規文面パターン数(10月中旬のある1日)



※ドコモ回線宛に対し分析　※縦軸は2つのグラフで同じ縮尺を利用

参考：JC3様の注意喚起

■ JC3（日本サイバー犯罪対策センター）様からもこうした状況を踏まえた注意喚起が実施されています(10/28付)

あなたのスマートフォンが犯罪のインフラに（2025年更新版） ～生成AIにより巧妙化する偽SMS～ | 脅威具体例 | 脅威情報 | 一般財団法人日本サイバー犯罪対策センター（JC3）

更なる対策としての“能動通知”

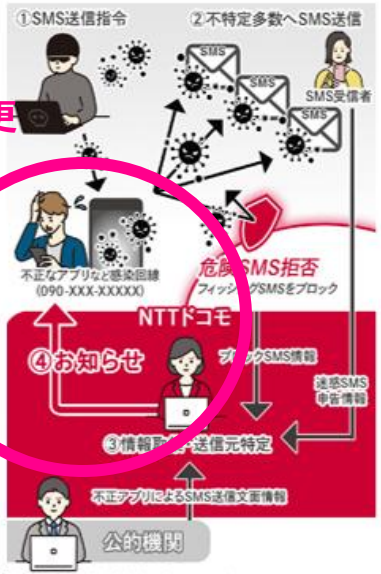
docomo

ドコモの対策例：危険SMS拒否設定とマルウェア感染が疑われるお客様への能動通知

docomo

■ドコモでは“危険SMS拒否設定”という迷惑SMSをお客様に届かせない仕組みを運用しています。
■更に、お客様の携帯電話がフィッシング詐欺の踏み台にされている可能性を検知した際にお客さまへご連絡を行う能動通知施策（意図せぬ迷惑メッセージ送信に関するお知らせ）を昨年度より開始しました

能動通知による更なる取り組み



意図せぬ迷惑メッセージ送信に関するお知らせ

概要
お客さまの携帯電話が知らないところでフィッシング詐欺の踏み台にされている可能性をお知らせし、ご確認と削除のお願いを実施します。

お申し込み　：不要（オプトアウト方式）
月額使用料　：無料
提供開始日　：2024年7月1日～

【お客様に届くお知らせのイメージ】
ご利用中の回線において、不正なコンテンツ等のインストールを促したり、個人情報を盗み取ろうとする危険なメッセージの送信行為が確認されました。お客さまの意図しない送信行為が行われている可能性があります。身に覚えのないアプリがインストールされていないかのご確認、および削除をしていただきますようお願いいたします。

▼「身に覚えのないアプリ」の確認および削除方法の案内

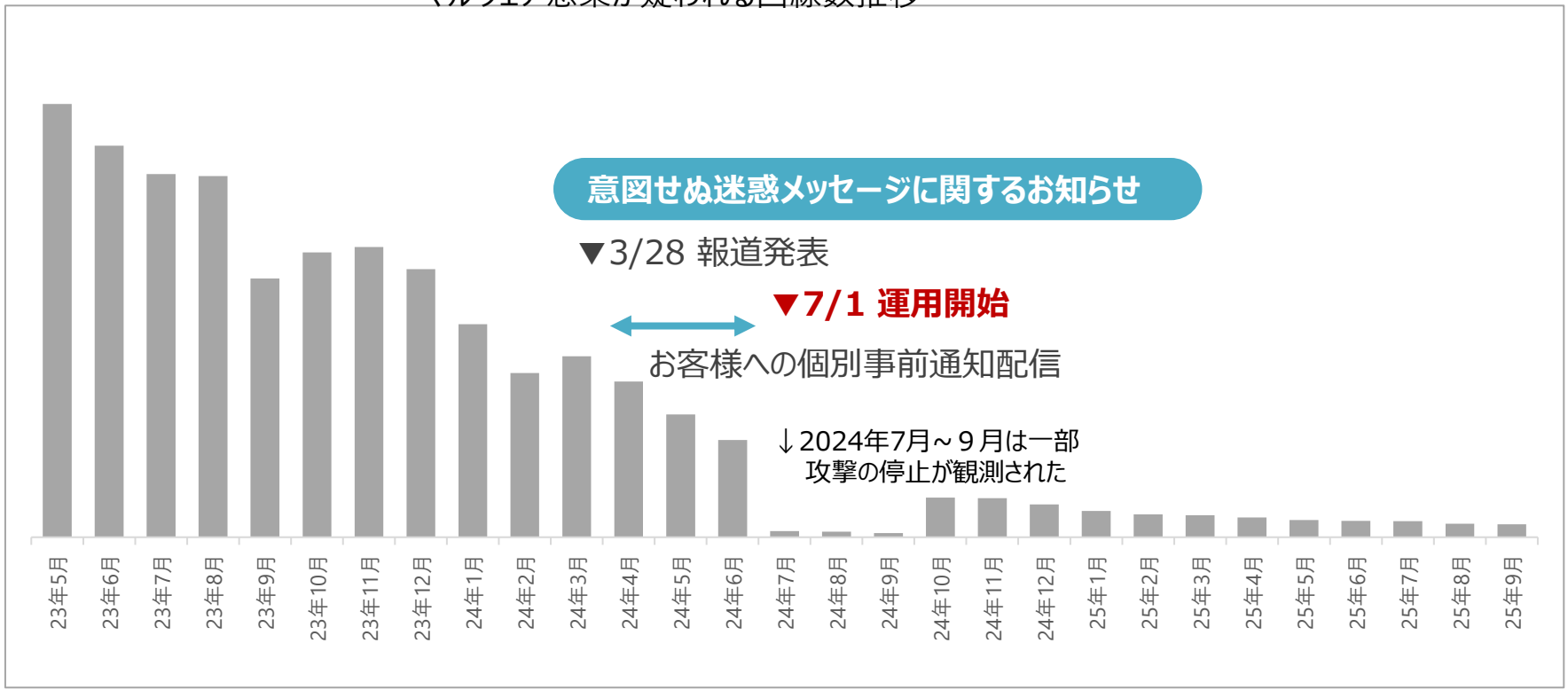
13

能動通知の効果：マルウェア感染ドコモ回線推移

docomo

- マルウェアに感染しフィッシングSMSを送信していると思われるドコモ回線数は減少傾向
- 一方で直近の数か月は回線数の減少度合いは小さくなっている

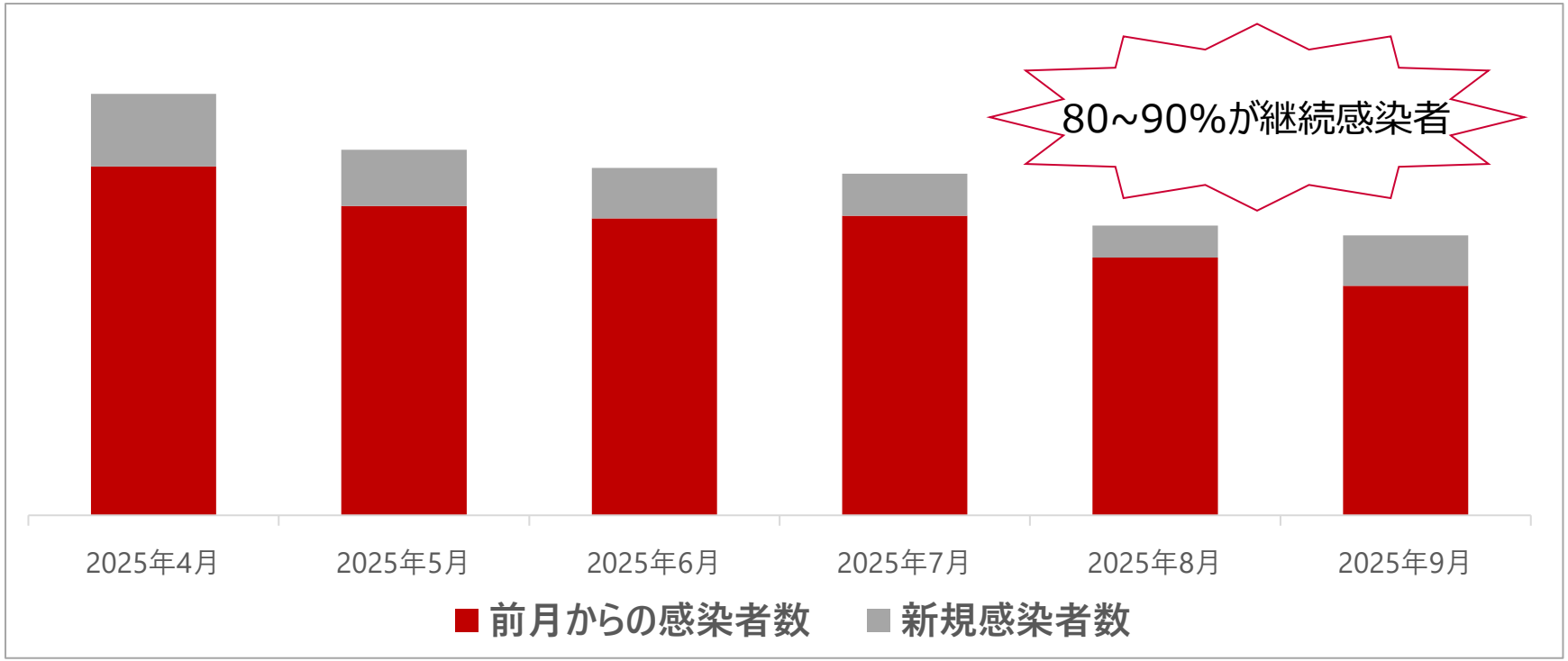
マルウェア感染が疑われる回線数推移



能動通知の効果：直近のマルウェア感染ドコモ回線の内訳

■ 感染者数全体は減少傾向にあるものの、お知らせを受け取った後も継続してマルウェアに感染し続けている端末が一定存在

マルウェア感染が疑われる回線数推移（新規・既存内訳）

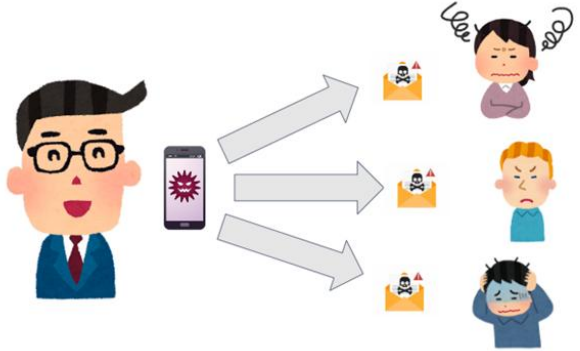


感染端末の減少、SMS配信ガイドラインについて

ソフトバンク株式会社　松崎 達彦

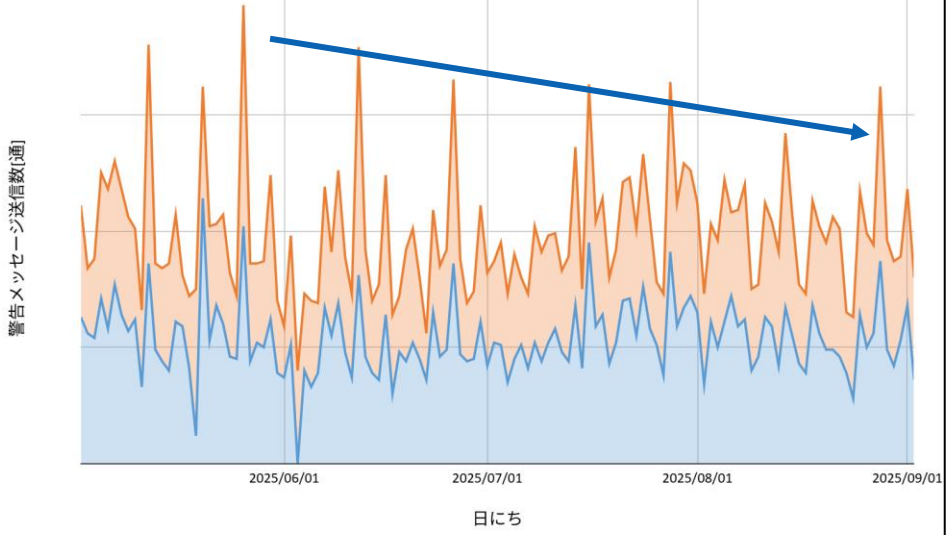
＜マルウェア感染へのアプローチ＞

SMSを大量送信しているお客様へ、1日の送信閾値を超えた場合にお知らせSMSを送信する。



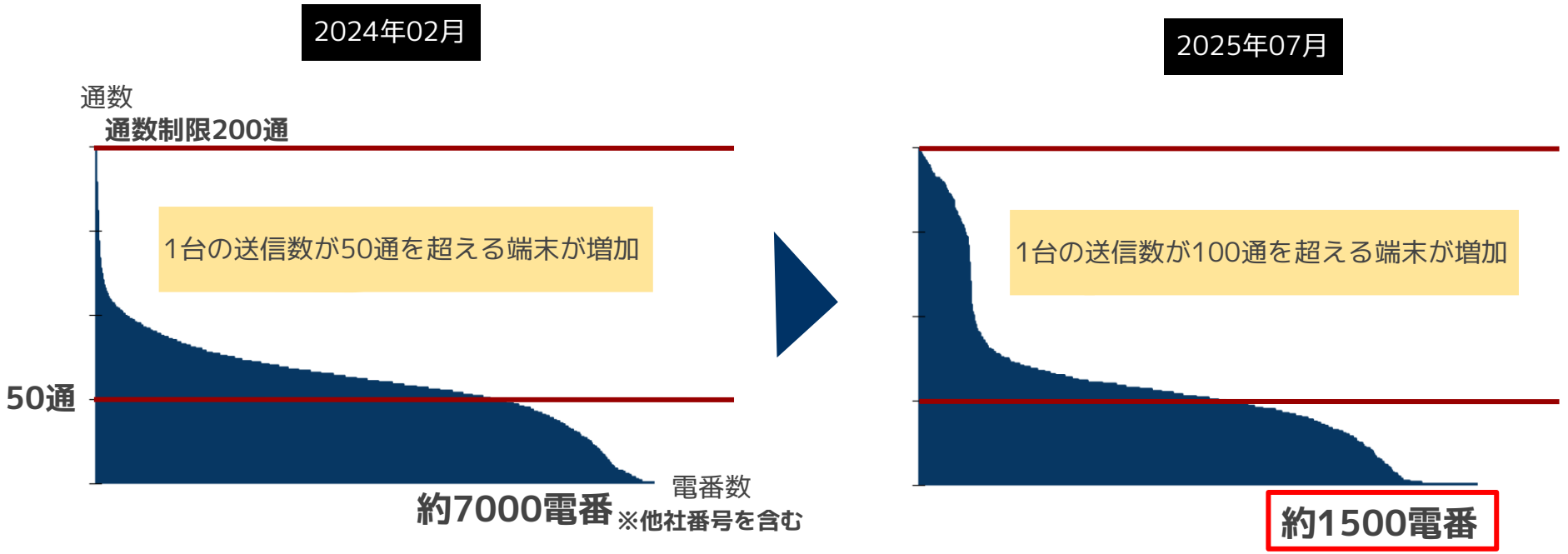
マルウェア感染端末等からのSMS送信はバックグラウンドで行われる為、送信側のユーザが気付いていないケースが多い

送信数が削減　＝　マルウェア感染端末の削減

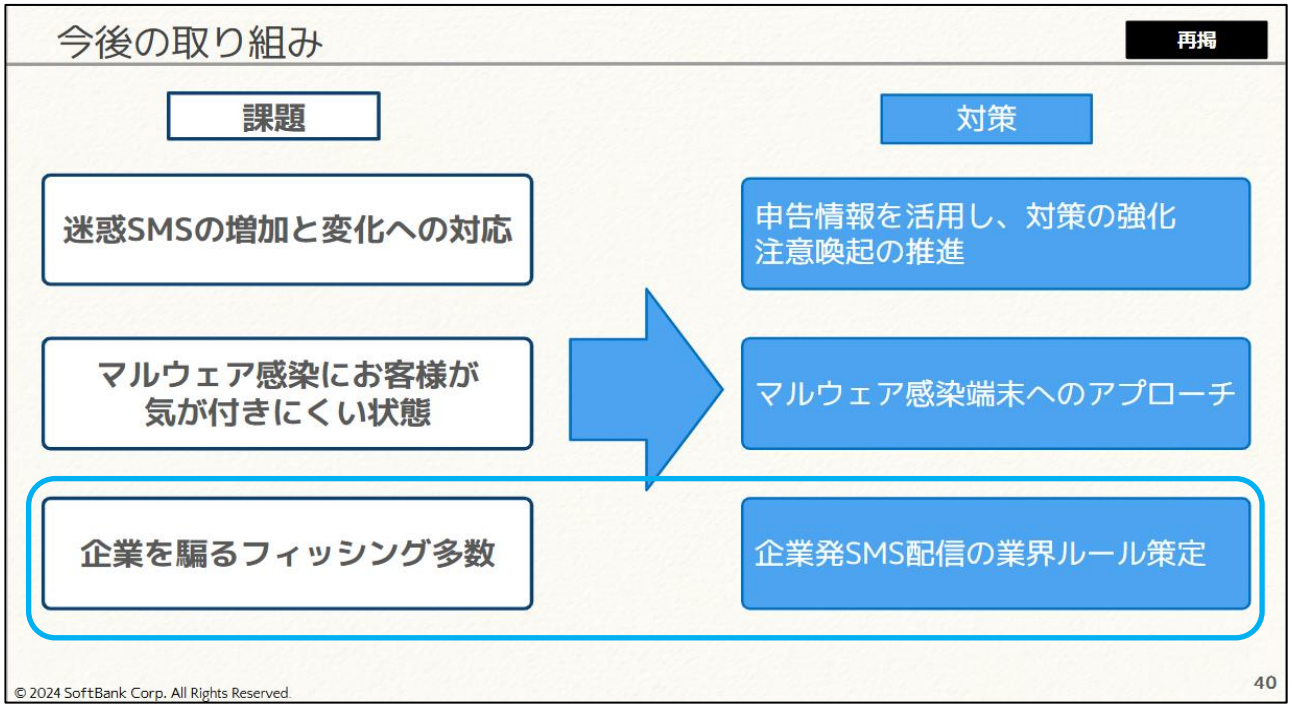


約80%のマルウェア感染端末の削減

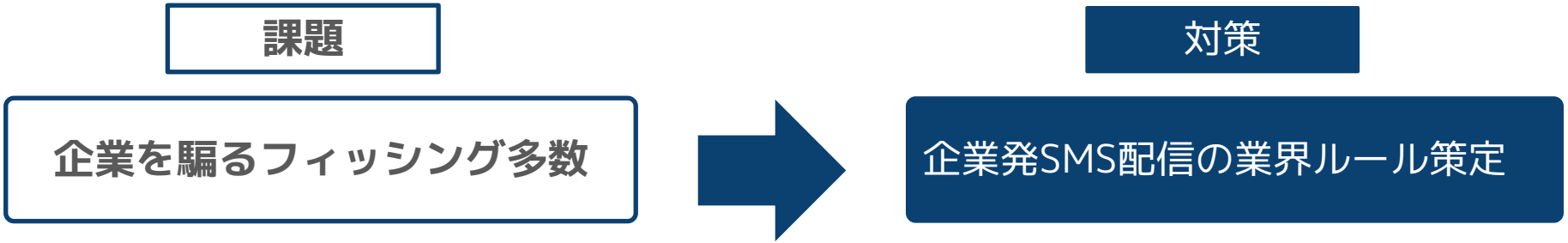
※ソフトバンク調べ



正しいSMSを判定しやすくするために業界ルールの策定



2024年11月
JPAAWG



項目	概要
目的	SMSを信頼できる通信手段として利用できるようにするために、 SMS発信元の明確化・透明化のための業界ルールを策定する

企業発SMS配信の業界ルール策定

SoftBank

＜配信企業＞
SMS配信をスミッシングと判断されないように確実に届けたい。

＜キャリア＞
企業を騙る迷惑SMSが多数存在する為、正しいSMSを判断することが困難。

＜お客様＞
正しいSMSを判断することが困難。

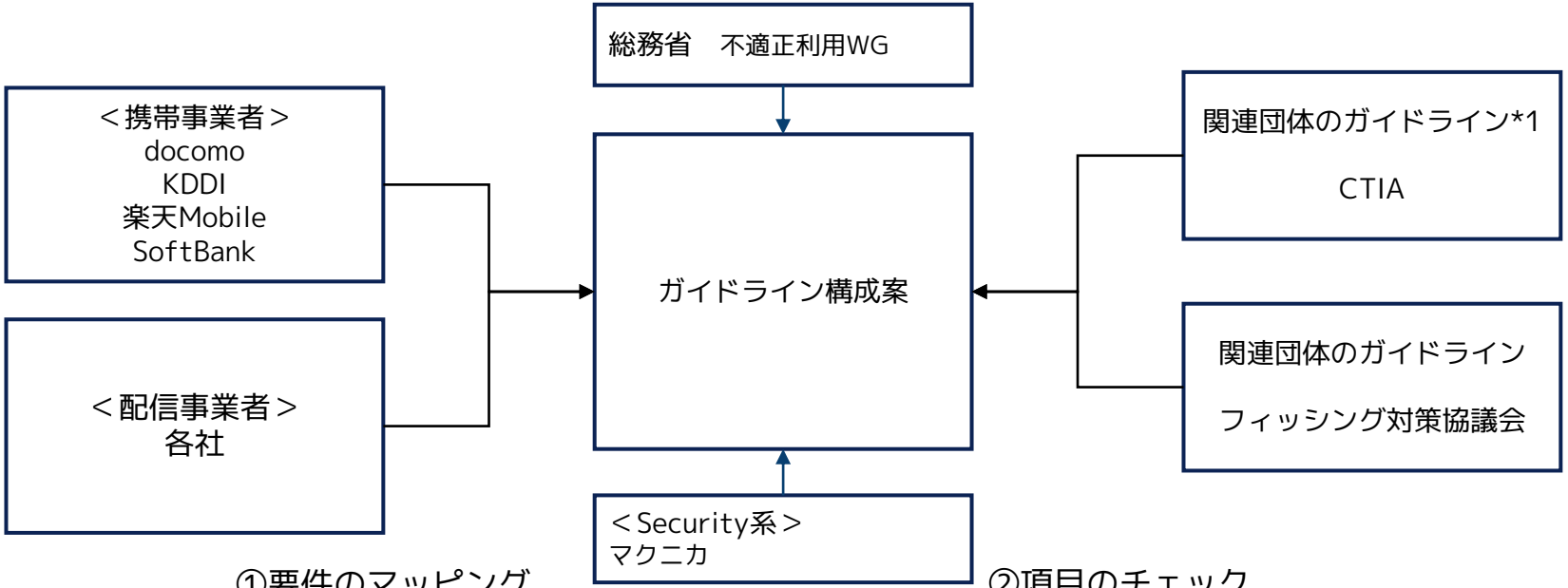
＜業界ルール策定(案)＞

・配信者の特定：共通番号利用を促進

・配信者の判別：共通番号をユーザへ開示

・配信内容：無償短縮URLは利用しない。など

SMS配信ガイドライン検討体制



①携帯事業者要件、配信事業者様要件を、ガイドライン構成案にマッピングする
②ガイドライン（CTIA、対策協議会）の項目に対して、ガイドラインでの検討漏れをチェックする

*1 CTIAのガイドラインからSMS配信に関連する２つを対象とする
- CTIA Short Code Monitoring Handbook
- Messaging Principles and Best Practices

SMS配信ガイドライン：ガイドライン構成

大項目	中項目	小項目
1．はじめに		
	1.1. ガイドラインの目的	
	1.2. 用語集	
2．SMS信頼性確保のために守ること		
	2.1. 送信者の適正管理	2.1.1. 払い出し可能な共通ショートコードの規定
		2.1.2. 払い出し先利用企業の確認
		2.1.3. 共通ショートコードから利用企業の特定
		2.1.4. 共通ショートコードの消費者への周知
	2.2. メッセージの適正運用	2.2.1. 利用者同意の適切な取得
		2.2.2. メッセージの送信頻度と送信時間
		2.2.3. 配信停止機能の提供
		2.2.4. メッセージコンテンツの適合性
		2.2.5. メッセージコンテンツのURL/電話番号利用
	2.3. セキュリティと不正防止	2.3.1. 不正行為の防止
		2.3.2. コンプライアンス違反への対応
	2.4. 利用者保護とプライバシー	2.4.1. 消費者保護と申告受付
		2.4.2. データ保護とプライバシー
参考文献		

さらなるスミッシング対策検討(案)

SoftBank

①SMS配信ガイドライン1.0公開

②送信元ホワイトリスト化(共通ショートコードなど)

③②と合わせて送信内容のホワイトリスト化

Appendix

- CTIAが実施している、事業者がガイドラインを遵守しているかのモニタリングについて教えて下さい。
  - モニタリングの対象は何でしょうか：全てのSMS、Non-Consumer SMSのみなど
  - モニタリングはSMS配信経路のどこで行いますか
  - モニタリングの許諾を、消費者からえているのでしょうか。
- コンプライアンス違反への対処について教えて下さい
  - CTIAがコンプライアンス違反を見つけた場合は、送信元である企業に対して、直接警告を行うのでしょうか。
  - コンプライアンス違反で対処を行うのは、年間何件くらいになりますか。
  - コンプライアンス違反があった場合、対象となる企業と違反の内容は公開されるのでしょうか。
  - 詐欺に使われる不正サイトのテイクダウン、番号の停止、口座への送信停止などの処置は行いますか
- Non-Consumer SMSの発信元番号について教えて下さい
  - 許可されている番号は、(1) 10桁のNANP（北米電話番号計画）、(2) 共通ショートコード、(3) テキスト対応トールフリー番号、(4) プロキシ番号の４つで、(2)(3)(4)は事前の許可が必要の理解で正しいですか。
  - アルファニューメリカル番号は許可されていないのでしょうか。
- 共通ショートコードに関して
  - 共通ショートコードの管理は、Common Short Code Administration (CSCA)が行うとあります。CSCAとはどのような組織でしょうか。
- メッセージの送信頻度や送信時間帯に関して教えて下さい
  - メッセージの頻度や送信時間帯に対して規定があります
- 7726へ申告について教えてください。
  - 申告内容を確認できるのは、CTIAでも確認可能でしょうか。
  - 迷惑申告が7726よりクライアントアプリが提供する申告が多いと聞いています。クライアントアプリ機能からの申告内容も確認可能でしょうか

- ガイドラインに関してサプライチェーンメンバを役割で規定する部分の質問

3.3. Messaging Ecosystem Roles

- Cloud-Based Providers, Connection Aggregators, Service Providers には、どの事業者が該当するか
  - 日本のSMS配信事業者は、Cloud-Based Providers と Connection Aggregators のどちらに該当するのか
  - 無線通信事業者は Service Providers に含まれるが、SMS配信事業者も含まれるのか
  - Cloud-Based Providers と Connection Aggregators の違いは何か

- Service Providers を対象とした規定は、無線通信事業者、SMS配信事業者の両方に当てはまるのか
  - 無線通信事業者とSMS配信事業者への規定の違いをどこで読み取ればよいのか

ロール	説明
Cloud-Based Providers	クラウドベースのプロバイダーは、オーバーザトップ IP 接続を使用するか、ワイヤレス メッセージングを含むワイヤレス キャリア ネットワーク サービスとの相互運用性を通じて、エンド ユーザーに音声やメッセージングなどのサービスを提供します。クラウドベースのプロバイダーの中には、ワイヤレス サービスにアクセスするための API を提供するものもあれば、スタンドアロン アプリケーションを提供するものもあります。
Connection Aggregators	コネクションアグリゲータは、複数のワイヤレスプロバイダーとのメッセージング接続など、企業顧客にさまざまな付加価値サービスを提供します。ICVとは異なり、接続アグリゲータは通常、キャリア間のピアリングトラフィックをサポートしていません。
Service Providers	サービスプロバイダーとは、ワイヤレスプロバイダー、MVNO、クラウドベースプロバイダー、CLEC など、10 桁の NANP 電話番号または短縮コードを使用して消費者または非消費者にメッセージングサービスまたはメッセージング関連サービスを提供する、セクション 3.3 で特定される当事者のいずれかを指します。