総務省

# 電気通信サービスの
# 不適正利用対策

令和７年１１月
総務省
利用環境課

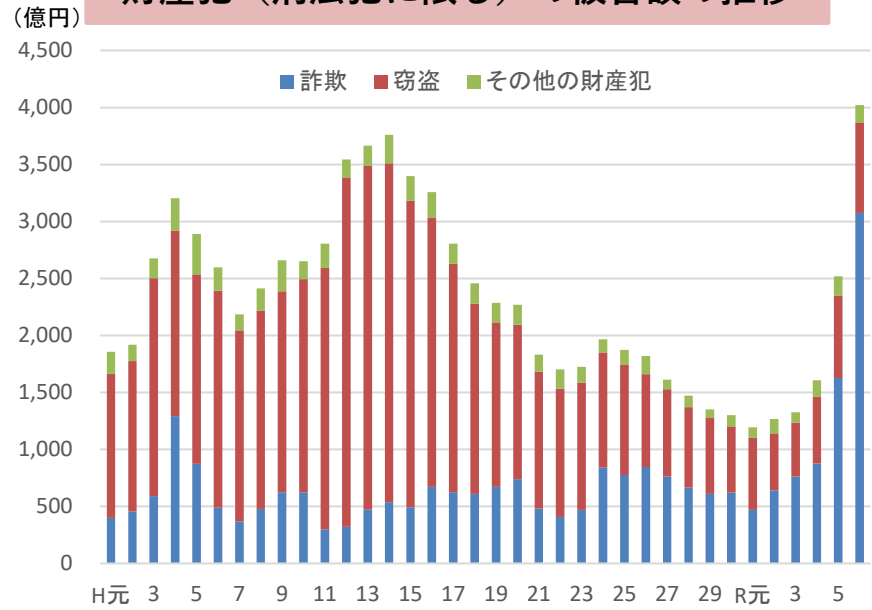
# 「国民を詐欺から守るための総合対策」の改定に当たって



## 現在の情勢

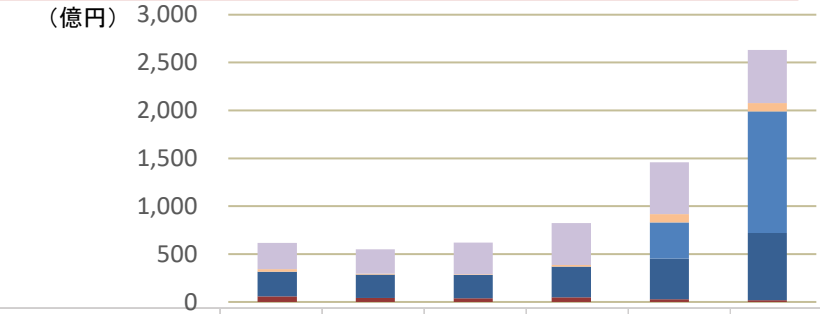
ＳＮＳやキャッシュレス決済の普及等が進む中で、これらを悪用した詐欺等の被害が加速度的に拡大する状況を受け、令和６年６月、「国民を詐欺から守るための総合対策」を策定し、官民一体となった対策を講じてきたところ、令和６年中の財産犯の被害額は4,000億円を超え、これは平成元年以来最も高かった平成14年当時の被害を上回る額であり、極めて憂慮すべき状況。その増分の大半を詐欺による被害額が占めており、詐欺への対策が急務。

### 財産犯（刑法犯に限る）の被害額の推移




| | R元 | R2 | R3 | R4 | R5 | R6 |
|---|---|---|---|---|---|---|
| 詐欺 | 469.5 | 640.1 | 763.0 | 876.8 | 1,625.8 | 3,074.7 |
| 窃盗 | 633.2 | 501.6 | 474.0 | 585.3 | 725.8 | 789.3 |

### 特殊詐欺、SNS型投資・ロマンス詐欺、不正送金事犯、クレジットカード不正利用事犯の被害額の推移




| | | R元 | R2 | R3 | R4 | R5 | R6 |
|---|---|---|---|---|---|---|---|
| 合計 | | 615.1 | 549.5 | 620.3 | 822.7 | 1,536.0 | 2,631.4 |
| カード不正利用 | | 274.1 | 253.0 | 330.1 | 436.7 | 540.9 | 555.0 |
| 詐欺 | 不正送金 | 25.2 | 11.3 | 8.2 | 15.2 | 87.3 | 86.9 |
| 詐欺 | SNS型投資・ロマンス詐欺 | | | | | 455.2 | 1268.0 |
| 詐欺 | 特殊詐欺（その他） | 256.7 | 242.6 | 242.5 | 323.9 | 422.8 | 704.4 |
| 詐欺 | 小計 | 281.9 | 253.9 | 250.7 | 339.1 | 965.3 | 2,059.3 |
| 特殊詐欺（詐欺盗） | | 59.1 | 42.6 | 39.5 | 46.9 | 29.8 | 17.1 |

※　令和６年の特殊詐欺及びＳＮＳ型投資・ロマンス詐欺の被害額は暫定値。
※　カード不正利用の被害額は、日本クレジット協会が集計したもの。

## 総合対策の改定

○　一層複雑化・巧妙化する詐欺等の被害から国民を守るためには、手口の変化に応じて機敏に対策をアップデートすることに加え、犯罪グループを摘発するための実態解明、犯罪グループと被害者との接点の遮断等の取組が必要。

○　令和６年12月に決定した「いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策」と統合するとともに、金融・通信に関するサービス・インフラの悪用を防止するための対策や、架空名義口座を利用した新しい捜査手法の検討等の新たな取組を追加して従来の総合対策を改定し、政府を挙げた詐欺等に対する取組を抜本的に強化。

# 「国民を詐欺から守るための総合対策2.0」における主な施策

犯罪対策閣僚会議決定
（令和7年4月22日）



## 1 SNS型投資・ロマンス詐欺対策 ／ 2 特殊詐欺対策

### （1） 犯行準備段階への対策

○ 携帯電話不正利用防止法上、契約時における本人確認が義務付けられていないデータ通信専用SIMについて、悪用実態を踏まえ、電気通信事業者に対して契約時における実効性のある本人確認の実施を働き掛けるとともに、契約時の本人確認の義務付けを含め検討。

○ 犯罪実行者募集情報の削除等の取組を促進するほか、犯罪グループの人的基盤となり得る非行集団等からの少年の離脱に向けた取組等犯罪への加担を防止するための取組を推進。

### （2） 着手段階への対策

○ 詐欺に誘引するダイレクトメッセージ等が被害者等の端末に届く前にフィルターする取組や利用者が詐欺に誘因するダイレクトメッセージ等を受信した際に警告表示を行う取組を推進。

○ 契約変更等の機会も活用しながら、国際電話サービスを利用しない設定があることを一層強く国民に周知。また、将来的には、国際電話サービスを利用しない者に対する優遇措置等、国際電話を必要としない人への利用休止を促すような効果的な対策の導入を検討。

○ 迷惑電話、迷惑SMS等の受信を防止又は受信した際の警告を行う有料のサービスについて、事業者に対し、無償化を含めた効果的な措置を要請するとともに、被害防止機能向上のためより効果的な方策を検討し、その普及や有効性の向上を図る。

○ 発信者番号の表示が官公庁等の電話番号に偽装されている手口について、国民に注意喚起を実施するとともに、関係事業者と連携して効果的な対策を検討し、速やかに実施。

### （3） 欺罔段階への対策

○ 変化する欺罔の手口について、迅速・的確にその特徴や被害者層、具体的に講じるべき対策等を明らかにした上で、訴求対象・訴求内容と合致する広報啓発の手段を選定するなど、効果的な広報啓発を実施。

### （4） 金銭等の交付段階への対策

○ インターネットバンキングの初期利用限度額の適切な設定、インターネットバンキングの申込みがあった際や利用限度額引上げ時の利用者への確認や注意喚起等の取組を推進。

○ 預金取扱金融機関や暗号資産交換業者によるモニタリングの強化や、暗号資産交換業者への不正送金防止に係る取組を推進。

○ 預金取扱金融機関間において不正利用口座に係る情報を共有しつつ、速やかに口座凍結を行うことが可能となる枠組みの創設について検討。預金取扱金融機関と暗号資産交換業者における情報連携・被害拡大防止に係る取組を推進。

○ 犯罪者グループの上位被疑者の検挙、犯罪収益の剥奪等を図るとともに、口座の悪用を牽制するため、捜査機関等が管理する架空名義口座を利用した新たな捜査手法や関係法令の改正を早急に検討。

### （5） 犯行後の捜査段階における対策

○ 匿名性の高い通信アプリをはじめとする犯罪に悪用される通信アプリ等について、被疑者間の通信内容や登録者情報等を迅速に把握するために効果的と考えられる手法について、諸外国における取組を参考にしつつ、技術的アプローチや新たな法制度導入の可能性も含めて検討。

○ 通信履歴の保存の在り方について、電気通信事業における個人情報等保護に関するガイドライン改正や保存義務付けを含め検討。

○ 仮装身分捜査を、令和７年１月に制定した実施要領に基づき適正に実施し、詐欺や強盗等の犯人の検挙、被害の抑止を推進。

# 「国民を詐欺から守るための総合対策2.0」における主な施策



## 3 ID・パスワード等の窃取・不正利用対策

### （1） フィッシングサイトへの対策

○ フィッシングサイト判定の高度化・効率化のために生成AIを活用し、閲覧防止措置や警告表示による対策の効率化を図るなど、フィッシングサイトへの対策を推進。

### （2）・(3） ID・パスワードやクレジットカード情報の不正入手・利用対策

○ 悪用のおそれのあるクレジットカード情報を国際ブランド各社に提供する枠組みを活用するほか、ECサイトの脆弱性を悪用したクレジットカード情報窃取対策の実施について、カード会社がEC事業者に対して適切に指導を行うよう監督。

○ なりすましメールの対象となる事業者に対し、関係省庁が連携し、メールのなりすまし防止技術（DMARC）の導入推進のため、必要に応じたフォローアップや受信拒否を要求するポリシーでの運用の働き掛けを実施。

### （4） マネー・ローンダリングや現金化への対策

預金取扱金融機関等によるモニタリングの強化、EC加盟店等との情報連携等(1･2(4)等再掲)

### （5） 犯行後の捜査段階における対策

○ インターネットバンキングに係る不正送金等の実行時に、一般家庭からのアクセスに偽装するための踏み台として家庭用インターネット通信機器が悪用されていることから、その実態を調査・分析し、悪用実態を踏まえた対策を実施。

## 4 治安基盤の強化等

○ 犯罪グループの首謀者等の検挙、警察・検察におけるサイバー人材の育成の更なる推進、警察庁・都道府県警察間の連携強化等のため、態勢の充実強化を推進。

○ スマートフォン端末等の解析能力の強化、捜査に必要な情報収集の効率化のため、警察・検察の装備資機材の充実強化を推進。

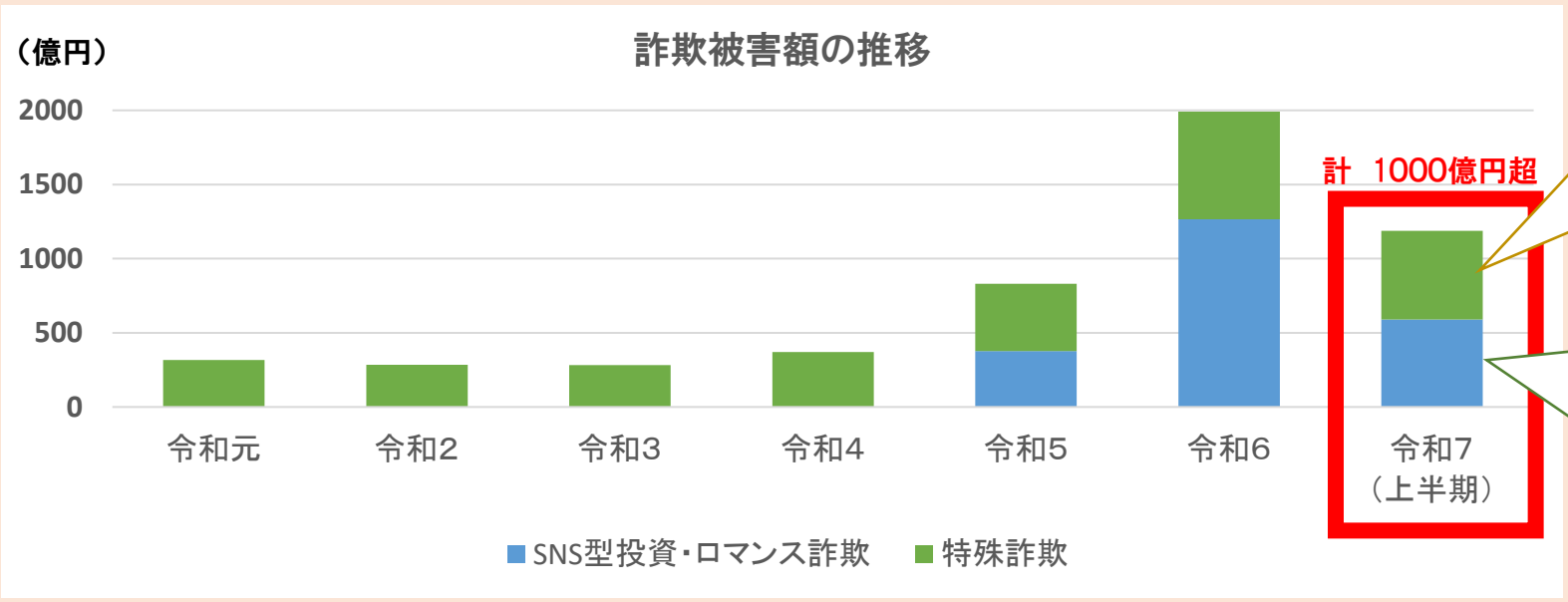
○ 外国機関と連携し、詐欺等対策や邦人保護の取組のほか、情報技術解析の高度化を推進。

○ 地方創生の交付金を活用した防犯カメラの設置等地域防犯力の強化に資する取組への支援を行うなど、防犯対策の強化を推進。

○ 詐欺等のほか、組織的な窃盗や強盗、違法・悪質なホストクラブ営業やスカウト行為、薬物密売、オンラインカジノ等多岐にわたる資金獲得活動に着目した取締り等を推進し、匿名・流動型犯罪グループの資金源への対策を推進。

# 詐欺被害の現状



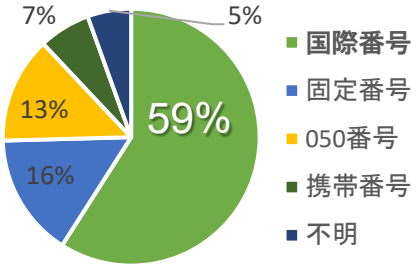



**特殊詐欺**
**597.3億円**
**（前年同期比+162%）**
✓ 電話での接触が全体の約8割

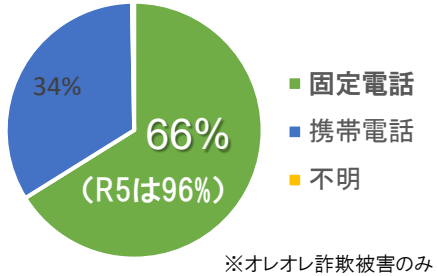
**SNS型投資・ロマンス詐欺**
**590.8億円**
**（前年同期比-11%）**
✓ SNSで募集し、LINEへ移行

## 特殊詐欺における電話対策の必要性

### 特殊詐欺に利用された番号（R6）



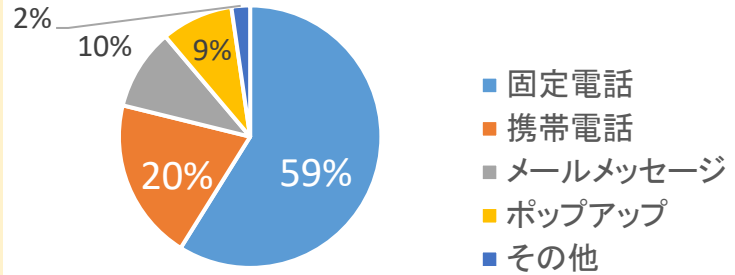

### 被害者の電話（R6）




※オレオレ詐欺被害のみ

## 特殊詐欺の接触手段の全体の約8割は電話

### 被害者への接触方法（R6）




※警察庁資料抜粋

# これまでの不適正利用対策

**高度化・多様化した電気通信サービスが国民各層に広く普及・浸透**

- IoTやAI、５G等の進展、ネットワーク仮想化技術の普及、スマートフォンやタブレット端末等の普及

**電気通信サービス市場における競争の激化**

- 光回線・携帯電話回線の卸売を受けたさまざまな事業者の参入、利用者獲得競争の激化
- サービス・料金体系の複雑化、利用者から行政機関に寄せられる苦情相談件数の高止まり

**犯罪に悪用される情報通信ツールの多様化及び増加**

- 不適正対策の推進の必要性

## ➢ 主な電話の不適正利用対策（特殊詐欺対策）

**携帯電話不正利用防止法（携帯電話契約時の本人確認義務）**

070, 080, 090
R6.4より、足のつかない
050アプリ電話を対象に追加

被害者宅

**犯罪収益移転防止法（電話転送契約時の本人確認義務）**

足のつかない
PC／電話

電話転送
事業者

交換機

03番号等
を表示し
信用させる

被害者宅

**特殊詐欺に利用された固定電話番号等の利用停止等スキーム**

総 務 省

電話番号
の指定

TCA事業者
（NTT東西等）

TCA

利用停止

悪質
事業者

卸契約

事業者 JUSA

卸契約

利用停止

事業者 悪質

卸契約

## ➢ 主な迷惑メール・不正SMS対策（フィッシング対策・スミッシング対策）

**特定電子メール法（事前同意なしの広告宣伝メール送信禁止）**

**送信ドメイン認証技術の普及・啓発(DMARC導入に向けた周知)**

**官民連携（迷惑メール対策推進協議会等）**




**SMSの不適正利用対策に係る検討**

- マルウェア感染端末の特定・警告の推進
- スミッシングメッセージの申告受付の推進
- SMS関連事業者による業界ルールの策定
- 迷惑SMS対策に係る周知啓発の推進

# 最近の不適正対策WGの動き（第7回～第10回）



## 背景

**いわゆる「闇バイト」犯罪の増加**

- ✓ 携帯電話の不正SIM転売が報告

**特殊詐欺被害の深刻化**

- ✓ 特殊詐欺の入り口の8割が電話
- ✓ 国際電話の悪用も急増

**犯罪行為の巧妙化、高度化**

- ✓ 青少年が生成AIを悪用した自作したプログラムで携帯電話を不正契約

## 検討項目

**（1）携帯電話本人確認のルール**

1 SIMの不正転売
2 法人の代理権（在籍確認）
3 他社の本人確認結果への依拠
4 追加回線
5 上限契約台数
6 データSIM

**（2）特殊詐欺、闇バイト等対策**

1(1) 固定電話の対策
1(2) 携帯電話・SMS・メールの対策
2 既存番号へのスプーフィング（なりすまし）
3 海外電話番号による詐欺電話

令和7年4月から6月まで、計4回の議論を経て、上記検討項目について検討を実施し、9月に報告書をとりまとめ

# 1. 詐欺電話対策

# 国際電話の利用休止の普及、詐欺携帯電話・詐欺メールの受信防止



○　総務省では、令和7年4月23日に、TCA((一社)電気通信事業者協会)に対して、固定・携帯電話、SMS及びメールを悪用した特殊詐欺等に対する対応に関して、要請を発出。

1　固定電話への国際電話サービスを悪用した詐欺等への対策

　新規、移転、切り替え時の契約変更時等の機会を捉えて、国際電話サービスを悪用した詐欺の可能性を説明し、契約の必要性の確認をすることや、国際電話サービスを利用しない者に対する優遇措置等、国際電話を真に必要としない人に対して利用休止を促すような効果的な措置を検討すること。

　また、国際電話不取扱センターの体制強化を通じた国際電話サービスを休止する体制の整備、キャパシティ向上を見据えた運用改善等を検討すること。

2　携帯電話への電話サービスを悪用した詐欺等への対策

　詐欺に誘引する電話について、国際電話発の詐欺電話を含む被害の未然防止に向けて、利用者に提供する迷惑電話対策サービスの無償化を含むより効果的な措置を検討すること。

3　SMS、電子メールサービスを悪用した詐欺等への対策

　詐欺に誘引するSMS、電子メールについて、被害の未然防止に向けて、利用者に提供する迷惑SMS、迷惑メール対策サービスの無償化を含むより効果的な措置を検討すること。

4　注意喚起・周知活動

　固定・携帯電話、SMS及び電子メールの利用者に対して、詐欺に巻き込まれる危険性について、効果的な注意喚起や周知活動を行うこと。

# 迷惑電話対策相談窓口「でんわんセンター」の設立



○ 令和7年6月10日、総務省請負事業として、迷惑電話対策相談に関する「でんわんセンター」を設立。
○ 業務内容は、迷惑電話に関する相談受付業務、相談内容の分析、分析を踏まえた電話の不適正利用対策の周知広報や啓発等。
○ 国際電話不取扱受付センターとも連携することで、国際電話を休止したい方の申込の円滑化も図っていく。

# 2. フィッシングメール対策

# フィッシング詐欺対策について

## 典型的な手口

「電子メール」から「偽サイト」に誘導し、「個人情報」を詐取する

**メール**

○○様

三菱UFJダイレクトをご利用いただきありがとうございます。

口座の安全を確保するため、お客様の口座が一時凍結されました。

下記のURLから再開手続きを設定下さい。

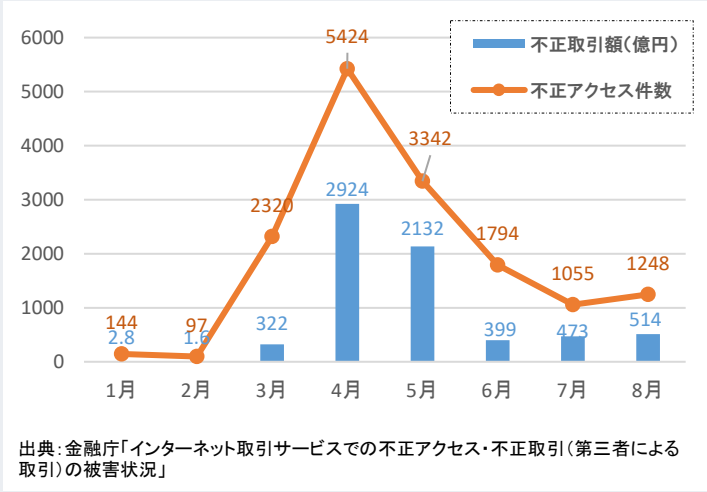
ここをクリック

**ログイン画面**


**詐取されたパスワード等を犯罪に悪用**

## 被害の広がり

証券口座の乗っ取り被害が拡大しており、補償が課題に




出典：金融庁「インターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害状況」

**9月1日** 文書により、主要通信4団体に対して対策強化を要請

**9月22日** 通信4団体との意見交換会を実施

# フィッシングメール対策の強化に関する要請



○　総務省では、令和7年9月1日に、4通信事業者団体に対して、生成AIを用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところ、フィッシングメール対策の強化に関して、要請を発出。

(1)フィルタリングの判定技術の向上や迷惑メール判定における AI の活用等、メールの フィルタリングの精度の一層の向上を積極的に図ること。また、迷惑メールのフィルタリ ング強度を適切に設定するなどして、高度化するフィッシングメールに対応可能なメール フィルタリングを目指すこと。

(2)なりすましメール対策として有効な DMARC の導入や DMARC ポリシーの設定(隔離、拒 否)を行うこと。送信側だけでなく受信側についても、適切な DMARC ポリシーに基づく処 理やレポート送信を設定すること。また、ドメインレピュテーション、BIMI、踏み台送信 対策等の更なる対策の導入を積極的に検討していくこと。

(3)提供しているフィッシングメール対策サービスについて、様々な利用者層に向けた一 層の周知・啓発を行うこと。

# フィッシングメール対策の強化等に関する意見交換



○　9月1日に発出した要請等の内容について、同月22日には、意見交換会を実施。
○　意見交換会では、総務省より、通信事業者に対して、フィッシングメール対策、特殊詐欺対策等について、改めて必要な対策を行うよう要請。

参加者

・総務省

・事業者団体：
　電気通信事業者協会
　テレコムサービス協会
　日本インターネットプロバイダー協会
　日本ケーブルテレビ連盟

・事業者：
　NTTドコモ
　KDDI
　ソフトバンク
　楽天モバイル

意見交換会の様子

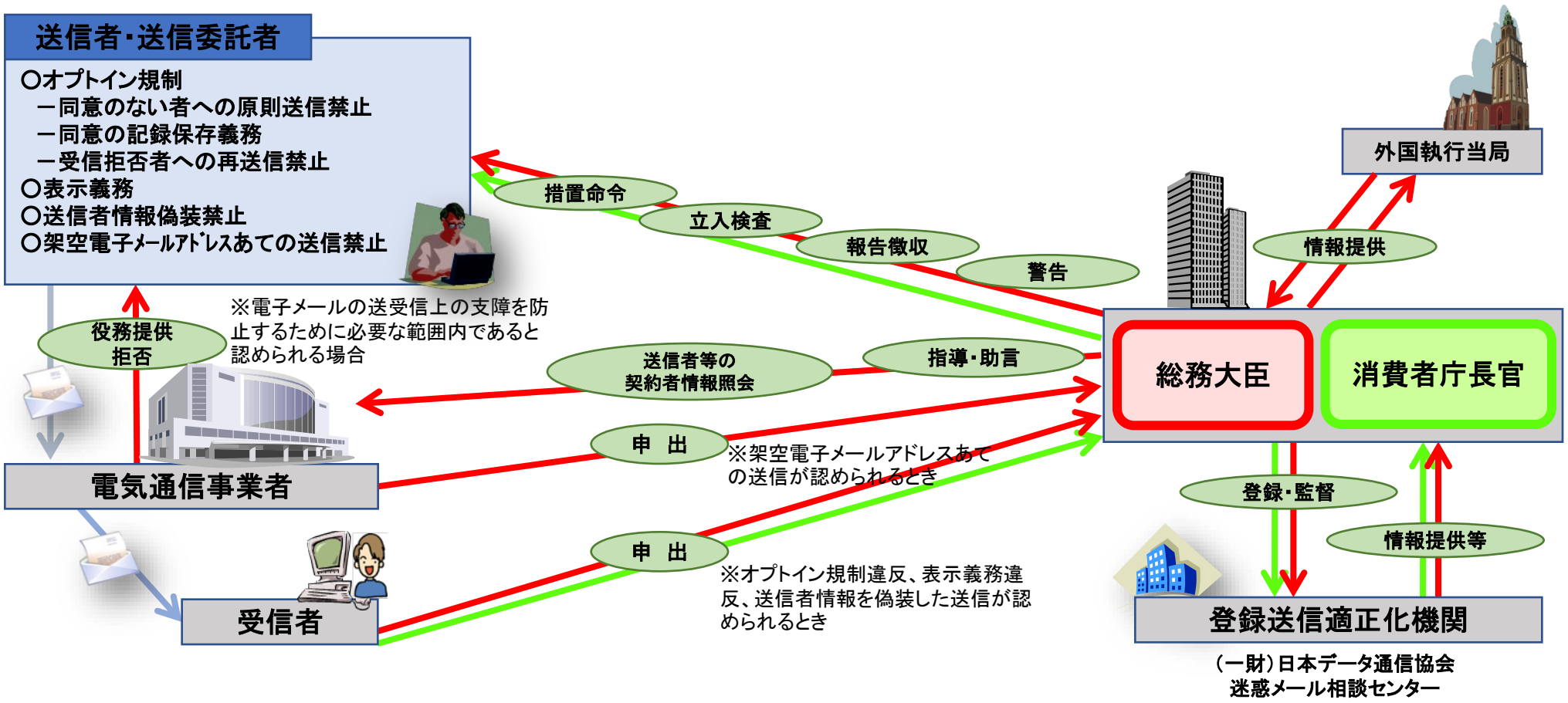
# 3. スミッシング（SMS）対策

# 制度面の対策：特定電子メール法※

※特定電子メールの送信の適正化等に関する法律（平成14年法律第26号）

○　電子メールによる一方的な広告宣伝メールを送り付ける「迷惑メール」が社会問題となったことから、広告宣伝メールの送信者に対して、原則としてあらかじめ送信の同意を得た者以外の者への送信禁止（オプトイン規制）を始めとする規制を定めている。

○　総務省及び消費者庁の共管として、迷惑メールの受信者からの通報や登録送信適正化機関のモニター機の観測結果等を踏まえて、送信者に対する警告等の行政指導を随時実施している。



# 不適正利用対策に関するワーキンググループについて



■ 令和６年２月から「不適正利用対策に関するワーキンググループ」を開催し、特殊詐欺やフィッシング詐欺等のICTサービスの不適正利用への対処に関し、最近の動向等を踏まえ、専門的な観点から集中的に検討を実施。

| | 論　点 |
|---|---|
| ①　特殊詐欺対策 | 1.　特殊詐欺被害が引き続き深刻な状況。**「足のつかない電話」の発生抑止のため、本人確認書類の偽変造への対応など、本人確認の実効性の向上※に関して取り組むべき事項はあるか。**<br>※非対面契約でのマイナンバーカードの公的個人認証の活用等<br>2.　特殊詐欺に悪用された電話番号の**利用停止スキーム**が効果をあげていることから、本スキームの**適用事業者の拡大**※に向けて取り組むべき事項はあるか。⇒電気通信番号制度に係る検討と合流<br>※業界団体に加盟していない事業者等 |
| ②　SMSによるフィッシング詐欺（スミッシング）対策 | 1.　SMSを利用したフィッシング詐欺（スミッシング）の被害が拡大する中、スミッシングメッセージの**発信元※への警告など、実効性ある対応策はあるか。**<br>※マルウェアに感染したスマートフォンの利用者など |

**構成員**

| | | |
|---|---|---|
| 座長 | 大谷　和子 | 株式会社日本総合研究所 執行役員 法務部長 |
| | 沢田　登志子 | 一般財団法人　ECネットワーク　理事 |
| | 鎮目　征樹 | 学習院大学　法学部教授 |
| | 辻　秀典 | デジタルアイデンティティ推進コンソーシアム(DIPC) 代表理事 |
| | 中原　太郎 | 東京大学大学院法学政治学研究科教授 |
| | 仲上　竜太 | 日本スマートフォンセキュリティ協会(JSSEC) 技術部会 部会長 |
| | 星　周一郎 | 東京都立大学 法学部 教授 |
| | 山根　祐輔 | 片岡総合法律事務所　弁護士 |

# SMSの不適正利用対策について

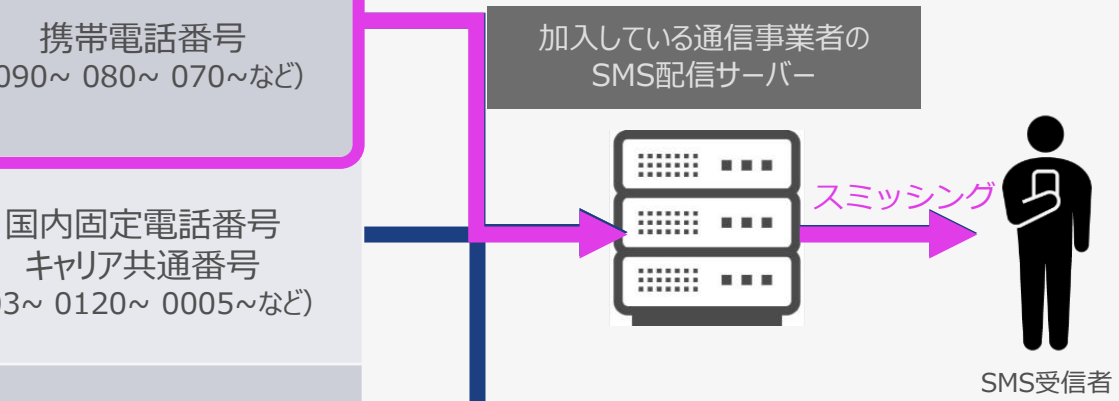
## スミッシングの発信源はマルウェア感染端末

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<br>(090~ 080~ 070~など) |
| | ②国内SMS配信事業者 | 国内固定電話番号<br>キャリア共通番号<br>(03~ 0120~ 0005~など) |
| 1% | ③海外通信事業者 | 海外電話番号<br>アルファベット<br>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

# SMSの不適正利用対策の方向性



## ①マルウェア感染端末の特定・警告の推進

- 通信の秘密の取扱いに留意した上で、通信キャリアが提供するSMSフィルタリングにおいて得られたデータを分析し、マルウェア感染端末の特定・警告を行う取組を進めることにより、マルウェア感染端末の利用者の損害の拡大の防止に加え、利用者の行動変容を促し、スミッシングメッセージの拡散を抑制する。

## ②スミッシングメッセージの申告受付の推進

- スミッシングメッセージ等の迷惑SMSを受け取った利用者から、さらに円滑に申告を受け付けられるようにしていくとともに、申告データを事業者横断で活用できるようにする仕組みを構築することにより、迅速な迷惑SMS対策ができるようにする。

## ③SMS関連事業者による業界ルールの策定

- SMS不適正利用対策事業者連絡会の枠組を活用し、SMSを利用する側の事業者を含め、関連する業界団体と連携することにより、SMS発信元の明確化・透明化に係る取組や、SMS認証代行事業者等の悪質事業者への対策などを盛り込んだ業界ルールを策定し、正規のメッセージがしっかり正規のものとわかる形で配信されるよう、効果的な対策を実行する。

## ④迷惑SMS対策に係る周知啓発の推進

- スミッシングの攻撃手法は時々刻々と変化をしていることから、官民が連携し、最新の対策方法に関する情報発信を行うとともに、キャリア共通番号の仕組みの周知広報やRCSの活用推進など、SMSに関する利用者のリテラシー向上につとめ、自主的な防衛を推進する。

# マルウェア感染端末の特定・警告の推進に関する法的整理



**第２章　対策の方向性**

**１　SMS フィルタリングサービスを活用したマルウェア感染端末の特定・注意喚起の推進**

不正 SMS メッセージのうち約 99%が、マルウェアに感染した個人端末から送信されている現状を踏まえると、マルウェア感染した端末及び回線を特定の上、同端末及び回線利用者への注意喚起を行うことが必要である。

これまで通信キャリアでは、迷惑 SMS 対策として、各社ごとにフィルタリング機能を提供していたところであるが、スミッシング被害がますます深刻化している状況を踏まえ、通信キャリアが、事業者自身の SMS フィルタリングサービスでブロックした SMS メッセージの通信内容等を用いて注意喚起すべきマルウェア感染端末を検知し、通信に係るログ情報に基づきマルウェア感染端末の利用者を特定した上で、特定した利用者に対して電子メールの送付等の方法により注意喚起を行うことが考えられる。

この取組を実施するに当たっては、SMS フィルタリングサービスでブロックした SMS メッセージの通信内容等を用いて注意喚起すべきマルウェア感染端末を検知し、通信に係るログ情報等と、通信キャリアが保有している契約者情報、通信履歴等を照合し、当該端末に係る通信回線の契約者及び連絡先を特定する行為は通信の秘密の窃用等に該当することから、これをどのように整理するかが論点となる。通信当事者の有効な同意がある場合には、通信当事者の意思に反しない利用であるから、通信の秘密の侵害には該当しないとされている。この点に関して、有効な同意があるとは、原則として、通信の秘密を取り扱うことに対する認識、認容がある場合をいい[18]、通常は、契約約款等に基づいた事前の包括同意のみの場合を含まない。ただし、次の場合には、例外的に、契約約款等による事前の包括同意であっても、有効な同意といい得る場合があるとされている[19]。

① 利用者が、事業者において通信の秘密を取り扱うことについて通常承諾すると想定し得るため、契約約款等による同意になじまないとはいえない場合であって、

② 利用者に将来不測の不利益が生じるおそれがない場合

[18] 同意の有効性に疑義を招かないためには、外形的にみても明確な同意を得ることが要求されることから、「個別具体的かつ明確な同意」が必要とされている。
[19] 「電気通信事業におけるサイバー攻撃の適正な対処の在り方に関する研究会　第三次取りまとめ」（平成 30 年 9 月 26 日公表）p.10

11

本件のケースについては、個別具体的な同意よりも事前の包括同意の方が、効果的であると考えられ、以下、マルウェアに感染している可能性が高い端末の利用者の特定及び注意喚起について、契約約款等に基づく包括的な同意を取得することで足りると解する余地があるか検討する。

①　契約約款等による同意になじむか

マルウェアに感染している端末については、知らぬ間に大量の SMS メッセージが送信されて高額の携帯電話料金が生じていること、場合によっては送信者が「詐欺師扱い」されるなど風評被害も生じ得ること等からすれば、マルウェアに感染している端末の利用者に対する注意喚起を通信キャリアが行うことは、一般的、類型的に見て、利用者における安心・安全な通信環境の確保に向けられた行為といえる。また、このような注意喚起を行うために、通信の秘密に当たる情報のうち、SMS フィルタリングサービスでブロックした SMS メッセージの通信内容等を用いて注意喚起すべきマルウェア感染端末を検知し、通信に係るログ情報（例えば、通信日時）[20]を元に、利用者の具体的な氏名及び連絡先を確認し、当該端末の利用者を特定する行為についても、一般的、類型的にみて、利用者における安心・安全な通信環境の確保に向けられた行為といえる。したがって、通常の利用者であれば、自らが利用している端末についてマルウェアに感染している可能性が高い場合には、注意喚起に必要最小限の範囲において通信キャリアが通信の秘密を利用することを承諾することが想定し得ることから、①の要件を満たすと解される[21]。

②　利用者において将来生じる不測の不利益を回避し得るか

注意喚起に関して利用される通信の秘密の対象、範囲は上記で述べたとおり明確であり、利用者に不測の不利益が生じる可能性は高くない。このような状況下で、以下のような条件を満たす場合には利用者が不測の不利益を被る危険を回避できると考えられる旨整理されていることを参考に、次の条件を満たす場合は、②の要件も満たすと解される[22]。

- a 注意喚起を希望しない者（オプトアウトした者）の利益が侵害されないような態勢を整える

[20] 本整理に基づいて、マルウェア感染端末の特定・注意喚起を実施する場合には、通信の秘密の問題を含むため、同意取得方法につき総務省に相談の上実施することが望ましい。
[21] 一例として、通信事業者のスミッシング対策検討におけるサンプル調査において、調査対象の８割以上の者の利用意向を確認した事例がある。
[22] 「電気通信事業におけるサイバー攻撃の適正な対処の在り方に関する研究会　第三次取りまとめ」（平成 30 年 9 月 26 日公表）p.13

12

- b 利用者が、一旦契約約款等に同意した後も、随時、同意内容を変更できる（設定変更できる）ようにする
- c 同意内容の変更の有無にかかわらず、その他の提供条件が同一である契約内容とする
- d 本件対策の内容とともに、注意喚起を望まない利用者は随時同意内容を変更できる（設定変更できる）こと及びその方法につき利用者に相応の周知を図る[23]

以上から、通信キャリアが提供する SMS フィルタリングサービスでブロックした SMS の通信通内容等を用いて注意喚起すべきマルウェア感染端末を検知し、通信に係るログ情報を利用し、マルウェア感染端末を使用している利用者を特定の上、個別に注意喚起を行う取組については、上述の条件を満たす場合には、契約約款等による包括同意であっても本件対策を行うための通信の秘密に属する事項の利用等について有効な同意であるということができ、有効な同意に基づいて実施するのであれば、通信の秘密の侵害に当たらないと整理することができる。

通信キャリアにおいては、本整理を参考にすることで、利用者の有効な同意を得た上でマルウェア感染端末を特定し、個別に注意喚起を行うことなど、利用者の損害の拡大防止を図り、スミッシングメッセージの拡散の抑制の取組が包括的に推進されることを期待する。[24]

**２　スミッシングメッセージの申告受付の推進**

ニュージーランドでは、政府においてスミッシングメッセージの申告を受け付け、その情報を元に対策を講じている。我が国においては、現在、国内キャリアや事業者団体を中心に、スミッシングメッセージの申告を受け付けているが、申告情報の横連携も限られているといった意見があった。これらを踏まえ、スミッシングメッセージ等の迷惑 SMS を受け取った利用者が、国内キャリア等へさらに円滑に申告をできるようにしていくとともに、国内キャリア等が保持する迷惑 SMS に係るデータを事業者横断で活用できるようにする仕組みを構築することにより、迅速で実効的な迷惑 SMS 対策を講じることが必要である。

[23] 利用者に対し、契約締結時に書面等を用いて明確に説明することが考えられる。また、既に契約している者に対しては、ウェブサイトへの掲載に加えて、電子メールや郵便等によってマルウェアに感染している可能性が高い端末の利用者に対して注意喚起をすることを周知するとともに随時同意内容を変更できる（設定変更できる）こと及びその方法を説明すること等が考えられる。
[24] 令和６年７月から(株)NTT ドコモにおいて、「意図せぬ迷惑メッセージ送信に関するお知らせ」の提供が開始された。

13

不適正利用対策に関するワーキンググループ報告書（令和6年 11 月 29 日）

# SMS関連事業者による業界ルールの策定



- 業界ルールの策定（ キャリア事業者、SMS配信事業者他で議論中）
  - 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・透明化のためのルールを記載予定
- 通信キャリアにおいて、共通ショードコード情報をまとめたサイトをリリース（2025年7月22日）
  - 共通ショードコード及びその利用企業名を照会可能

https://japansms.com/

ご清聴ありがとうございました