総務省

JPAAWG 7th General Meeting in Sapporo

# 電気通信サービスの不適正利用対策

令和６年１１月
総合通信基盤局
電気通信事業部
利用環境課

黒田　凛奈

# 電気通信ツール悪用の変遷

# 特殊詐欺とは



- **特殊詐欺とは、被害者に電話**をかけるなどして対面することなく信頼させ、現金等をだまし取る犯罪をいい、手口が多様に存在。**令和5年の被害総額は約452億円（昨年から約80億円増）**。
- 実行犯が犯行の匿名性を確保するためには、**発信者の身元を特定されない方法**で電話をかける場合が多い。

## 特殊詐欺の手口

### オレオレ詐欺

親族、警察官、弁護士等を装い、親族が起こした事件・事故に対する示談金等を名目に金銭等をだまし取る（脅し取る）手口

### 預貯金詐欺

自治体や税務署の職員などと名乗り、医療費などの払い戻しがあるからと、キャッシュカードの確認や取替の必要があるなどの口実で自宅を訪れ、キャッシュカードをだまし取る手口

### キャッシュカード詐欺盗

警察官などと偽って電話をかけ「キャッシュカード(銀行口座)が不正に利用されている」等として、嘘の手続きを説明した上で、キャッシュカードをすり替えるなどして盗み取る手口

### 架空料金請求詐欺

未払いの料金があるなど架空の事実を口実とし金銭等をだまし取る（脅し取る）手口

### 還付金詐欺

税金還付等に必要な手続きを装って被害者にATMを操作させ、口座間送金により財産上の不法の利益を得る手口

### その他の手口

・融資保証金詐欺
・金融商品詐欺
・ギャンブル詐欺
・交際あっせん詐欺　　等

警察庁　特殊詐欺対策ページ　参照

# 電話悪用の手口について

- **電話悪用と対策はいたちごっこ。**犯罪者は、一つの手口をふさぐと次の手口に移っていく。

## 【携帯電話】 手軽に利用できる携帯電話を悪用した手口がまず発達


## 【電話転送】 電話転送サービスを悪用し、03番号等を表示させて信用させる手口が発達


## 【050IP電話】 050IP電話を悪用する手口が発達


最近では、海外経由の通信サービスなど、着信時に電話番号が表示されないものを悪用した犯行も確認されている。

# 総務省におけるこれまでの特殊詐欺対策について



特殊詐欺対策について、総務省は電話を所管する立場から、**以下の3本柱で、電話の悪用対策を実施**

**対策の柱①　携帯電話不正利用防止法（携帯電話利用者の本人確認）の執行**
**対策の柱②　犯罪収益移転防止法（電話転送サービス利用者の本人確認）の執行**
**対策の柱③　電話番号の利用停止措置の運用**

**①携帯電話不正利用防止法**の執行　（2006.4施行（レンタルは2008.12より対象））

- **携帯電話の契約時の本人確認**を義務付け
- 総務大臣は、本人確認義務を履行していないキャリアショップ等に対して是正命令を発出

**②犯罪収益移転防止法**の執行　（2008.3施行（電話転送は2013.4より対象））

- **電話転送サービス事業者等に対して、顧客等の本人確認**を義務付け
- 国家公安委員会からの意見陳述も踏まえ、総務大臣は、義務違反の事業者に対して是正命令を発出

**③電話番号の利用停止措置**の運用　（TCA 2019.9開始／JUSA 2022.12開始）

- 総務省から事業者団体（TCA・JUSA）への通知に基づき、県警等からの要請に応じて、特殊詐欺に利用された固定電話番号等の利用停止、悪質な利用者への新たな固定電話番号の提供拒否を実施。

# 「携帯電話不正利用防止法」の概要



## これまでの経緯

■ 平成17年4月、議員立法により「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律」が成立。（平成17年法律第31号）

■「レンタル携帯電話事業者による本人確認の厳格化等」を内容とする改正法が平成20年6月成立。同年12月から施行。

## 携帯電話不正利用防止法の概要

**◇ 契約者の管理体制の整備の促進 及び 携帯音声通信サービスの不正利用の防止のため、以下を措置**

**1．契約締結時・譲渡時の本人確認義務等**

・ 携帯電話事業者及び代理店に対し、① 運転免許証等の公的証明書等による契約者の本人確認とともに、② 本人確認記録の作成・保存（契約中及び契約終了後３年間）を義務付け。

**2．警察署長からの契約者確認の求め**

・ 警察署長は、犯罪利用の疑いがあると認めたときは、携帯電話事業者に対し契約者確認を求めることが可能。また、本人確認に応じない場合には、携帯電話事業者は役務提供の拒否が可能。

**3．貸与業者の貸与時の本人確認義務等**

・ 相手方の氏名等を確認せずにレンタル営業を行うことを禁止。 ① 運転免許証等の公的証明書等による契約者の本人確認とともに、② 本人確認記録の作成・保存（契約中及び契約終了後３年間）を義務付け。

**4．携帯電話の無断譲渡・譲受けの禁止**

・ 携帯電話事業者の承諾を得ずに譲渡することを禁止。

**5．他人名義の携帯電話の譲渡・譲受けの禁止**

# 050アプリ電話の契約時の本人確認の義務化



「ＳＮＳで実行犯を募集する手口による強盗や特殊詐欺事案に関する緊急対策プラン」（令和５年３月１７日犯罪対策閣僚会議決定）

特殊詐欺の犯行には、匿名での架電を可能とする様々な通信手段が利用されているところ、総務省、警察庁等の関連省庁が連携して施策を推進することにより、こうしたサービスの悪用防止対策を更に強化する。

⇨ これを受け、携帯電話不正利用防止法に基づく役務提供契約時の本人確認義務の対象とするため、携帯電話不正利用防止法施行規則（総務省令）を改正。（令和５年８月公布、令和６年４月施行）

※改正後の携帯電話不正利用防止法施行規則（抜粋）

（携帯音声通信役務）

第二条　法第二条第二項の総務省令で定める電気通信役務は、携帯電話端末又はＰＨＳ端末と接続される電気通信事業法施行規則（昭和六十年郵政省令第二十五号）第三条第一項第一号に規定する端末系伝送路設備に接続される移動端末設備（電気通信事業法（昭和五十九年法律第八十六号）第十二条の二第四項第二号ロに規定する移動端末設備をいう。）を用いることにより通話することを可能とするために電気通信番号規則（令和元年総務省令第四号）別表に掲げる音声伝送携帯電話番号又は特定ＩＰ電話番号を使用して提供される電気通信役務であって、その提供を受けようとする者と電気通信事業者（電気通信事業法第二条第五号に規定する電気通信事業者をいう。以下この条において同じ。）との間の契約に基づき提供されるものをいう。ただし、電気通信事業者と、当該電気通信事業者の提供する携帯音声通信に係る電気通信役務を利用して携帯音声通信に係る電気通信役務を提供する電気通信事業者であって当該電気通信役務に係る無線局を自ら開設していない者との間の契約に基づき当該者に対し提供されるものを除く。

# 「犯罪による収益の移転防止に関する法律」の概要

○　犯罪による収益の移転防止に関する法律（平成19年法律第22号）は、犯罪による収益の移転の防止を図り、国民生活の安全と平穏を確保するとともに、経済活動の健全な発展に寄与することを目的として制定（平成20年3月1日施行）。

○　特定事業者(※)に対して、顧客等の取引時確認、疑わしい取引の届出等を義務付け。

※ 金融機関、ファイナンスリース業者、クレジットカード業者、弁護士、司法書士、公認会計士等（特定事業者により義務等は若干異なる）。

総務省関係では、**電話受付代行業者**、**電話転送サービス事業者**、行政書士、独立行政法人郵便貯金・簡易生命保険管理機構が該当。

## 犯罪による収益の移転防止に関する法律の概要

### ◇ 特定事業者に対して、以下の事項について義務づけ。

#### 1．取引時確認義務

・ 運転免許証等の公的証明書等による顧客等の①氏名・名称、②住居・本店又は主たる事務所の所在地、③生年月日、④取引を行う目的、⑤職業・事業内容、⑥実質的支配者の確認を義務づけ。

・ マネー・ローンダリングに利用されるおそれが特に高い取引（ハイリスク取引）については、上記確認事項に加え、その取引が２００万円を超える財産の移転を伴うものである場合には「資産及び収入の状況」の確認も義務づけられている。

#### 2．確認記録の作成・保存義務

・ 取引時確認を行った場合には直ちに確認記録を作成し、当該契約が終了した日から７年間保存することを義務づけ。

#### 3．取引記録の作成・保存義務

・ 特定業務に係る取引を行った場合若しくは特定受任行為の代理等を行った場合には、直ちにその取引等に関する記録を作成し、当該取引又は特定受任行為の代理等が行われた日から７年間保存することを義務づけ。

#### 4．疑わしい取引の届出

・ 特定業務に係る取引について、①当該取引において収受した財産が犯罪による収益である疑いがあるかどうか、②顧客等が当該取引に関し組織的犯罪処罰法第10条の罪若しくは麻薬特例法第６条の罪に当たる行為を行っている疑いがあるかどうかを判断し、これらの疑いがあると認められる場合に、行政庁に対して疑わしい取引の届出を行うことを義務づけ。

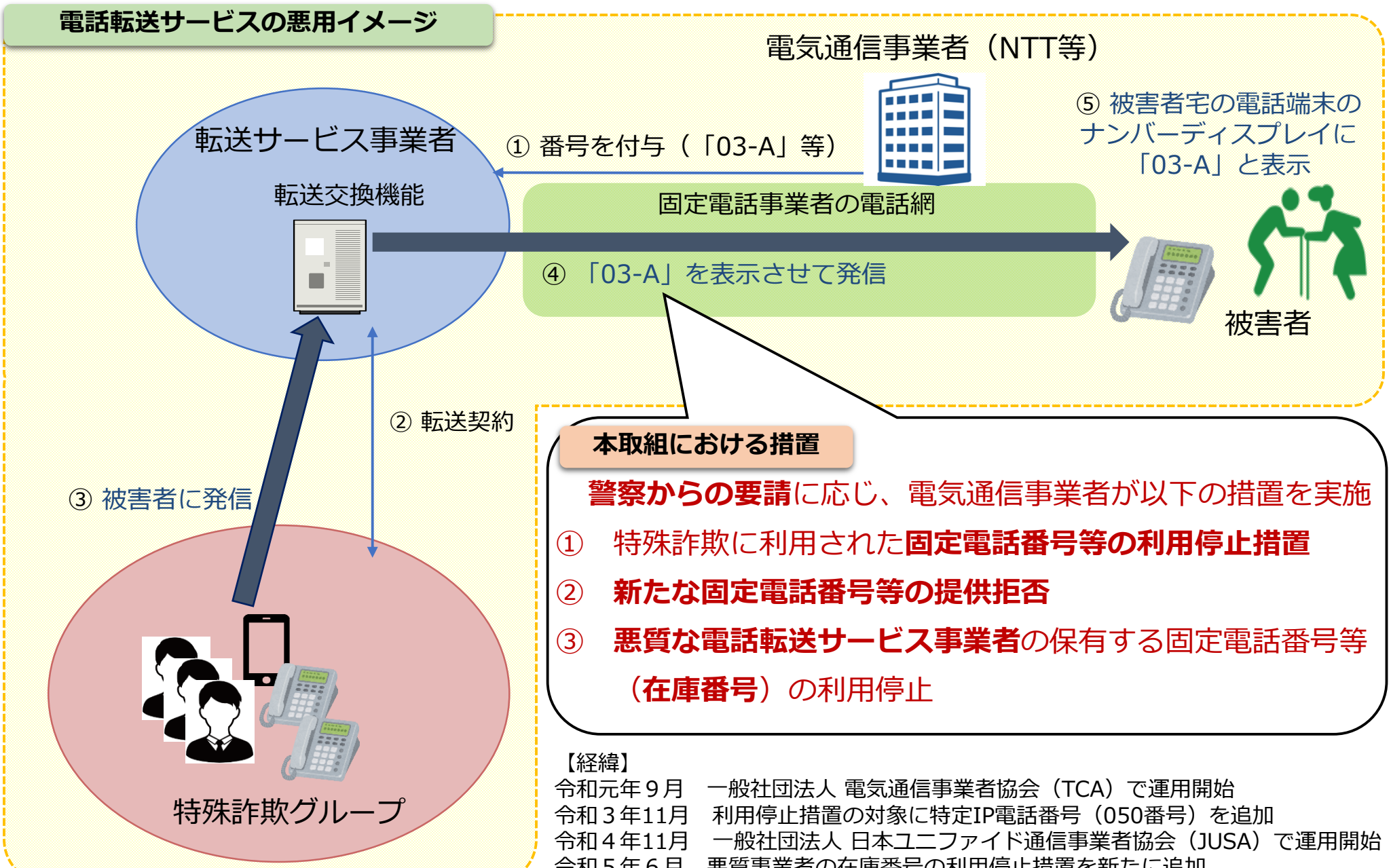
#### 5．取引時確認等を的確に行うための措置

・ ①取引時確認をした事項に係る情報を最新の内容に保つための措置を講ずるとともに、②使用人に対する教育訓練の実施、顧客管理措置の実施に関する内部規程の策定、顧客管理措置の責任者の選定等の措置を講ずるよう努めなければならない（努力義務）。

# 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



## 電話転送サービスの悪用イメージ




## 本取組における措置

**警察からの要請**に応じ、電気通信事業者が以下の措置を実施

① 特殊詐欺に利用された**固定電話番号等の利用停止措置**

② **新たな固定電話番号等の提供拒否**

③ **悪質な電話転送サービス事業者**の保有する固定電話番号等（**在庫番号**）の利用停止

【経緯】

令和元年９月　一般社団法人 電気通信事業者協会（TCA）で運用開始
令和３年11月　利用停止措置の対象に特定IP電話番号（050番号）を追加
令和４年11月　一般社団法人 日本ユニファイド通信事業者協会（JUSA）で運用開始
令和５年６月　悪質事業者の在庫番号の利用停止措置を新たに追加

# 高齢者向けナンバーディスプレイの無償化等

**NTT東西が、ナンバーディスプレイの無償化等の取り組み**を発表（2023/3/22）。

## ① 高齢者向けナンバー・ディスプレイ、ナンバー・リクエストの無償化

- ナンバー・ディスプレイの月額利用料（440円／月）及び工事費（2,200円）を無償化。
- ナンバー・リクエスト（※）の月額利用料（220円／月）及び工事費（2,200円）を無償化。

※　非通知でかけてきた相手に、電話番号を通知してかけ直すよう音声メッセージで応答するサービス。

- 70歳以上の契約者、または70歳以上の方と同居している契約者の回線。（申込制）
- 2023年5月1日より受付・適用開始。

## ② 電話番号の変更に関する工事費の無料化

- 特殊詐欺等の犯罪被害を受けるおそれがある場合、電話番号変更の工事費（2,750円）を無償化。
- 2023年4月1日より受付・適用開始

## ③ 特殊詐欺対策サービスの無料化

- 特殊詐欺対策サービス（※）の月額利用料（440円／月）および工事費（8,800円）を一定期間無料化（'23年5/1-'25年3/31。5000台限定。）。
- 2023年5月1日より受付・適用開始

※　通話録音機能付き端末に録音した通話録音データをクラウドに転送、特殊詐欺解析サーバにて解析し、特殊詐欺等の疑いがある場合には事前に登録した電話番号やメールアドレスに注意喚起を通知するサービス。

※　ナンバーディスプレイ加入者は月額利用料は無料。

# 政府の動き

# 国民を詐欺から守るための総合対策（概要）



※令和６年６月18日犯罪対策閣僚会議 資料抜粋

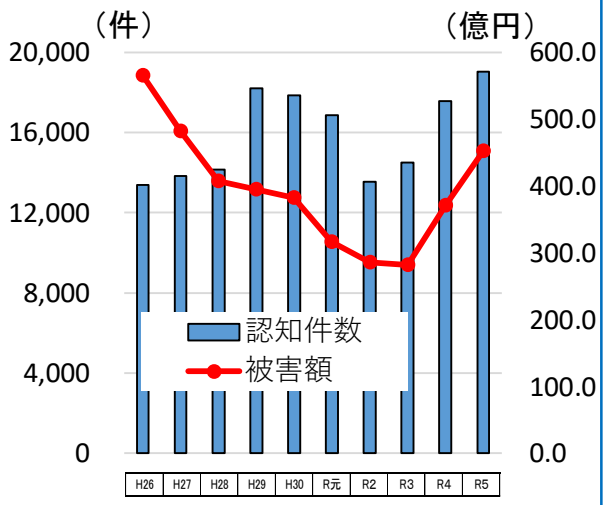
## 現在の情勢

特殊詐欺等に対しては、「オレオレ詐欺等対策プラン」（令和元年６月25日犯罪対策閣僚会議決定）及び「ＳＮＳで実行犯を募集する手口による強盗や特殊詐欺事案に関する緊急対策プラン」（令和５年３月17日犯罪対策閣僚会議決定）等に基づき官民一体となった対策を講じてきた一方で、令和５年中の詐欺被害は約1,630億円と前年から倍増。

近年、ＳＮＳやキャッシュレス決済の普及等が進む中で、これらを悪用した犯罪の手口が急激に巧妙化・多様化。それによって引き起こされる詐欺等の被害が、加速度的に拡大する状況。

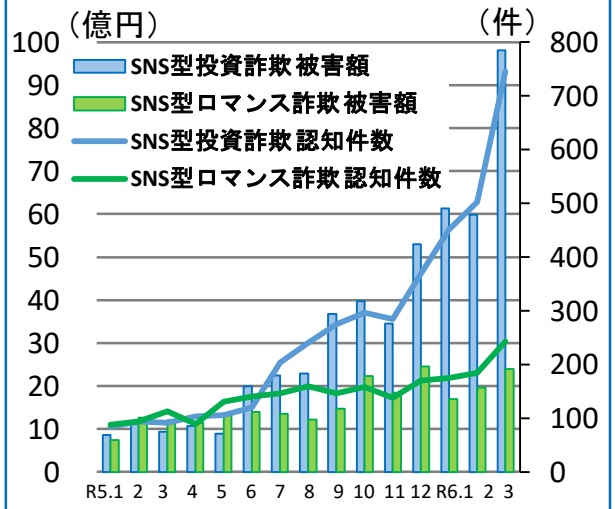
### 特殊詐欺

✓令和５年被害額は約452億円
✓前年から約80億円増加



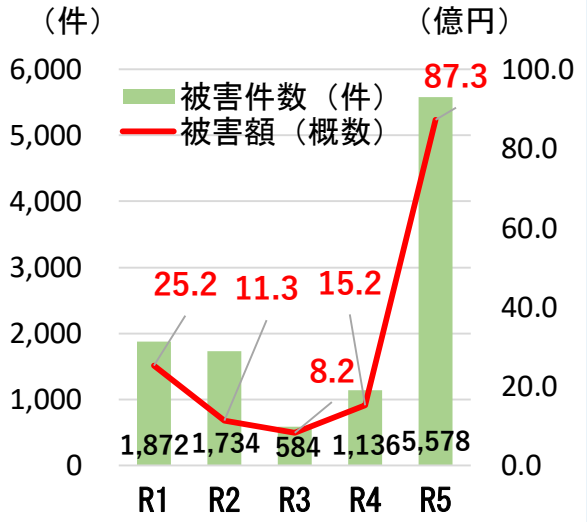

### ＳＮＳ型投資・ロマンス詐欺

✓令和５年下半期から急増
✓同年被害額は約455億円
✓令和６年１～３月被害額は約279億円




### フィッシングによる被害

✓インターネットバンキングに係る不正送金被害が急増(令和５年約87億円)




## 総合対策の策定

○　こうした情勢の中、変化のスピードに立ち後れることなく対処し、国民を詐欺の被害から守るためには、官民一体となって、一層強力な対策を迅速かつ的確に講じることが不可欠。

○　従来のプランを発展的に解消させ、特殊詐欺、ＳＮＳ型投資・ロマンス詐欺及びフィッシング等を対象に、総合的な対策を取りまとめ、政府を挙げて対策を推進。

# 「国民を詐欺から守るための総合対策」における主な施策



※令和６年６月18日犯罪対策閣僚会議 資料抜粋

## １.「被害に遭わせない」ための対策

### ＳＮＳ型投資・ロマンス詐欺対策

- **被害発生状況等に応じた効果的な広報・啓発等**
  - ○　不審なアカウントとのやり取りを開始する時など、詐欺の被害に遭う場面を捉えて利用者に個別に注意喚起を行うよう、ＳＮＳ事業者に要請
- **ＳＮＳ事業者等による実効的な広告審査等の推進**
  - ○　プラットフォーム上に掲載される広告の事前審査基準の策定・公表、審査体制の整備（特に、日本語や日本の社会等を理解する者の十分な配置）、広告出稿者の本人確認の強化等をＳＮＳ事業者に要請
  - ○　捜査機関から提供された「詐欺に使用されたアカウント」等の情報に着眼した、広告の迅速な削除等をＳＮＳ事業者に要請
- **なりすまし型偽広告の削除等の適正な対応の推進**
  - ○　なりすまし型の偽広告等に関し、ＳＮＳ事業者に対し、利用規約等に基づき、詐欺広告の削除等の措置を講ずるよう、事業者団体に通知
  - ○　インターネットで拡散する偽・誤情報や、なりすまし型偽広告への対応等について、国際的な動向を踏まえつつ、制度面も含む総合的な対策を推進
- **大規模プラットフォーム事業者に対する削除対応の迅速化や運用状況の透明化に係る措置の義務付け等**
  - ○　インターネット上の違法・有害情報への対応として、削除対応の迅速化や運用状況の透明化を大規模プラットフォーム事業者に義務付ける情報流通プラットフォーム対処法を速やかに施行するとともに、違法情報への該当性に関するガイドラインを迅速に策定
- **知らない者のアカウントの友だち追加時の実効的な警告表示・同意取得の実施等**
- **ＳＮＳの公式アカウント・マッチングアプリアカウント開設時の本人確認強化**
- **新たに開始された金融教育における被害防止に向けた啓発**
  - ○　金融経済教育推進機構（J-FLEC）による関係省庁と連携した金融経済教育の提供等を通じた金融リテラシーの向上

### フィッシング対策

- **送信ドメイン認証技術（ＤＭＡＲＣ等）への対応促進**
  - ○　利用者にフィッシングメールが届かない環境を整備するため、インターネットサービスプロバイダー等のメール受信側事業者や、金融機関等のメール送信側事業者等に対して、送信ドメイン認証技術の計画的な導入を要請
- **フィッシングサイトの閉鎖促進**
- **フィッシングサイトの特性を踏まえた先制的な対策**
  - ○　フィッシングサイトが有する、１つのＩＰアドレス上に複数のサイトが構築されるなどの特性を踏まえ、いまだ通報がなされていないフィッシングサイトを把握して、ウイルス対策ソフトの警告表示等に活用するなどを検討

### 特殊詐欺等対策

- **国際電話の利用休止申請の受付体制の拡充**
  - ○　国際電話番号を利用した詐欺の被害を防止するため、国際電話の利用休止を一括して受け付ける「国際電話不取扱受付センター」を運営する電気通信事業者に対して、申請受付体制の更なる拡充を要請
- **ＳＭＳの不適正利用対策の推進**
  - ○　ＳＭＳの悪用を防止するため、ＳＭＳフィルタリングの活用の拡大等を推進
- **携帯電話を使用しながらＡＴＭを利用する者への注意喚起の推進**

# 「国民を詐欺から守るための総合対策」における主な施策



※令和６年６月18日犯罪対策閣僚会議 資料抜粋

## ２.「犯行に加担させない」ための対策

- **「闇バイト」等情報に関する情報収集、削除、取締り等の推進**
- **青少年をアルバイト感覚で犯罪に加担させない教育・啓発**

## ３.「犯罪者のツールを奪う」ための対策

- **本人確認の実効性の確保に向けた取組**
  - ○　携帯電話等の契約時の本人確認をマイナンバーカード等を活用した電子的な確認方法へ原則一本化
- **金融機関と連携した検挙対策の推進**
  - ○　金融機関において、詐欺被害と思われる出金・送金等の取引をモニタリング・検知する仕組み等を構築するとともに、不正利用防止の措置を行い、疑わしい取引の届出制度の活用をはじめ、不正な口座情報等について警察へ迅速な情報共有を実施
- **電子マネーの犯行利用防止対策**
  - ○　詐取された電子マネーの利用を速やかに発見するためのモニタリングの強化、発見した場合の電子マネーの利用の停止、警察への情報提供の体制について検討
- **預貯金口座の不正利用防止対策の強化等**
  - ○　法人口座を含む預貯金口座等の不正利用を防止するための取引時確認の一層の厳格化等の推進
- **暗号資産の没収・保全の推進**

## ４.「犯罪者を逃さない」ための対策

- **匿名・流動型犯罪グループに対する取締り及び実態解明体制の強化**
- **ＳＮＳ事業者における照会対応の強化**
  - ○　ＳＮＳ事業者に対し、捜査機関からの照会への対応窓口の日本国内への設置、迅速な照会対応が可能な体制の整備等を要請
- **海外拠点の摘発の推進等**
- **法人がマネー・ローンダリングに悪用されることを防ぐ取組の推進**
  - ○　実態のない法人がマネー・ローンダリング等の目的で利用されることを防ぐための新たな方策について検討
- **財産的被害の回復の推進**
  - ○　被害回復給付金支給制度及び振り込め詐欺救済法のきめ細やかな周知など効果的な運用の促進

# 犯罪対策閣僚会議（第39回会合）岸田総理大臣指示



近年、ＳＮＳやマッチングアプリを通じたやり取りで相手を信頼させ、投資等の名目で金銭をだまし取る、ＳＮＳ型投資詐欺、ＳＮＳ型ロマンス詐欺が急増しています。著名人になりすました偽広告によって、被害者を誘い込む手口も広く見られ、社会的な問題となっています。キャッシュレス決済の普及等の中で、拡大するフィッシング被害や手口を変化させながら拡大する特殊詐欺も深刻であり、危機感を持って対応しなければなりません。

このような状況を踏まえ、国民の大切な財産を守り抜くため、また、安心して投資できる環境を確保するとともに、国民生活に不可欠なツールとなっている、ＳＮＳやキャッシュレス決済などの健全性・信頼性を確保するため、この度、政府として初めて詐欺全般に特化した総合対策を取りまとめました。

各位にあっては、本対策に基づき、様々な手口を踏まえた広報啓発やＳＮＳでの警告表示、闇バイト情報に関するサイバーパトロール、そして、**携帯電話契約時などにおけるマイナンバーカードを用いた本人確認の厳格化**や犯罪収益のより的確な没収のための法改正を含む暗号資産対策、海外拠点の摘発を始めとする徹底的な取締りなど、被害に遭わせない、犯行に加担させない、犯罪者のツールを奪う、犯罪者を逃さないための対策を総合的に推進してください。

特に国民を被害に遭わせないため、ＳＮＳ事業者による実効的な広報審査や情報流通プラットフォーム対処法の速やかな施行、警察等からの通報への迅速な対応を含む偽広告の削除の推進など、偽広告への対策を抜本的に強化してください。

また、経団連などとも連携して、**フィッシングを防止するための送信ドメイン認証技術**や金融機関、ＥＣサイト等での次世代認証技術**の導入・促進を強力に進める**ほか、未把握のフィッシングサイトに係るウイルス対策ソフトを通じた警告など、**技術的なアプローチも強化してください**。

国民を詐欺から守るため、民間事業者に社会的責任を果たしていただくよう強く働きかけることを含め、強い決意をもって本対策に基づく取組を徹底するようお願いいたします。

## 1「被害に遭わせない」ための対策

### (2) フィッシングによる被害実態に注目した対策

#### ア フィッシングサイトにアクセスさせないための方策

##### (ア) 送信ドメイン認証技術（DMARC等）への対応促進

フィッシングメール等によるインターネットバンキングに係る不正送金やクレジットカードの不正利用の被害が深刻な状況であることを踏まえ、利用者にフィッシングメールが届かない環境を整備するため、インターネットサービスプロバイダー等のメール受信側事業者や、金融機関、ＥＣ事業者、物流事業者、行政機関等のメール送信側事業者等に対して、送信ドメイン認証技術（ＤＭＡＲＣ等）の計画的な導入を検討するよう、総務省が実施した実証結果も踏まえつつ、引き続き働き掛けを行う。

※参考　その他フィッシング対策関係新規施策

(ｲ)　フィッシングサイトの閉鎖促進

令和５年２月、フィッシングによるなりすましの被害に遭っている事業者等に対し、ホスティング事業者等へフィッシングサイトの閉鎖を働き掛けるよう要請した。引き続き、フィッシングサイトの閉鎖を推進するため、なりすまされている事業者等に対して閉鎖依頼の実施を要請するとともに、関係団体やサイバー防犯ボランティアとの連携を強化し、より幅広い主体が閉鎖依頼を実施する環境を整備する。

(ｳ)　パスキーの普及促進

次世代認証技術の１つであるパスキーについて、既に採用している事業者等における効果等を踏まえ、金融機関やＥＣ加盟店等のサービスにおける採用や、当該サービスの利用者に対する利用を働き掛けるなど、普及を促進する。

# 国民を詐欺から守るための総合対策　SMS対策関係部分抜粋



## １「被害に遭わせない」ための対策

### (3) 特殊詐欺等の被害実態に注目した対策

#### ア　被害に遭わない環境の構築

##### (イ) 犯人からの電話を直接受けないための対策

###### ⑧ SMSの不適正利用対策の推進

ＳＭＳを悪用するフィッシング詐欺（スミッシング）や、ＳＭＳを契機とする架空料金請求詐欺等の被害が相次いでいることから、一部の電気通信事業者がデフォルトオンで提供しているＳＭＳフィルタリングの活用を拡大するとともに、スミッシングメッセージの申告受付やＳＭＳ対策に係る周知・啓発を推進する。

また、スミッシングメッセージの大部分が、マルウェアに感染したスマートフォン等の端末から発信されているという分析結果を踏まえ、ＳＭＳフィルタリングにより得られたデータを分析し、マルウェア感染端末の特定・警告を行う取組を推進する。

さらに、ＳＭＳ配信に関わる関係事業者において、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確実に正規のものと分かる形で配信されるよう、効果的な対策を実行する。

# 国民を詐欺から守るための総合対策　本人確認関係部分抜粋

## ３「犯罪者のツールを奪う」ための対策

### （1）犯罪者グループ等が用いる電話に関する対策

#### ア　本人確認の実効性の確保に向けた取組

携帯電話や電話転送サービスの契約時の本人確認において、本人確認書類の券面の偽変造による不正契約が相次いでいることから、犯罪収益移転防止法、携帯電話不正利用防止法に基づく非対面の本人確認手法は、マイナンバーカードの公的個人認証に原則として一本化し、運転免許証等を送信する方法や、顔写真のない本人確認書類等は廃止する。**対面でもマイナンバーカード等のＩＣチップ情報の読み取りを犯罪収益移転防止法及び携帯電話不正利用防止法の本人確認において義務付ける。**また、そのために必要なＩＣチップ読み取りアプリ等の開発を検討する。さらに、公的個人認証による本人確認を進める。

# 総務省の動き

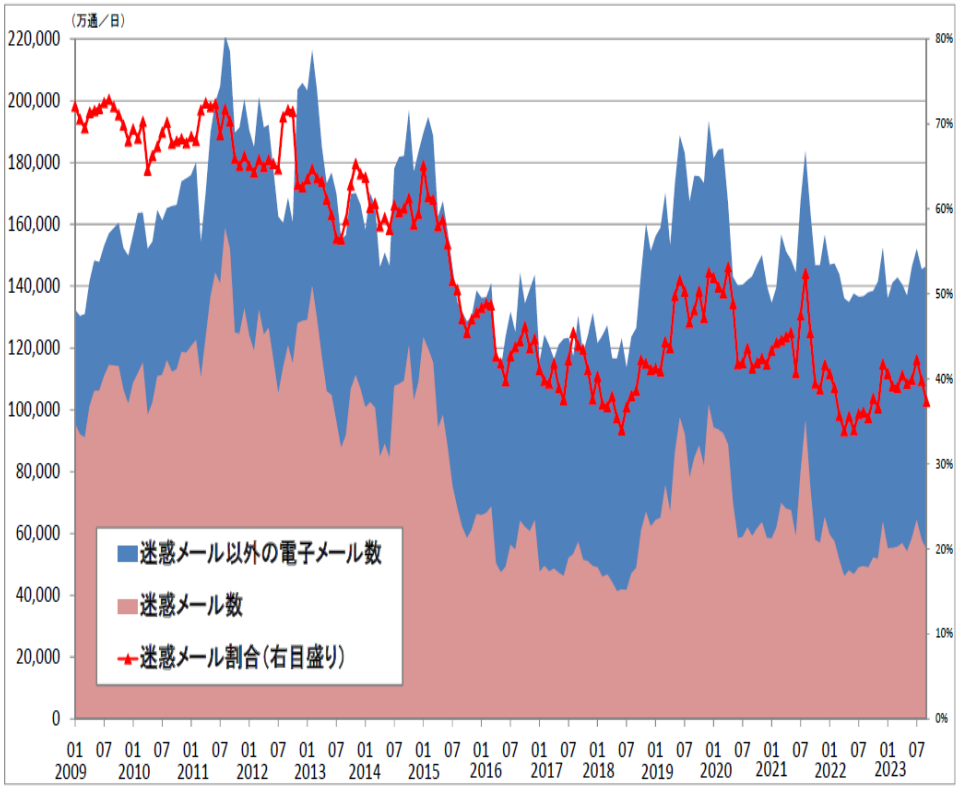
# 迷惑メール対策

# 我が国における迷惑メールの現状①



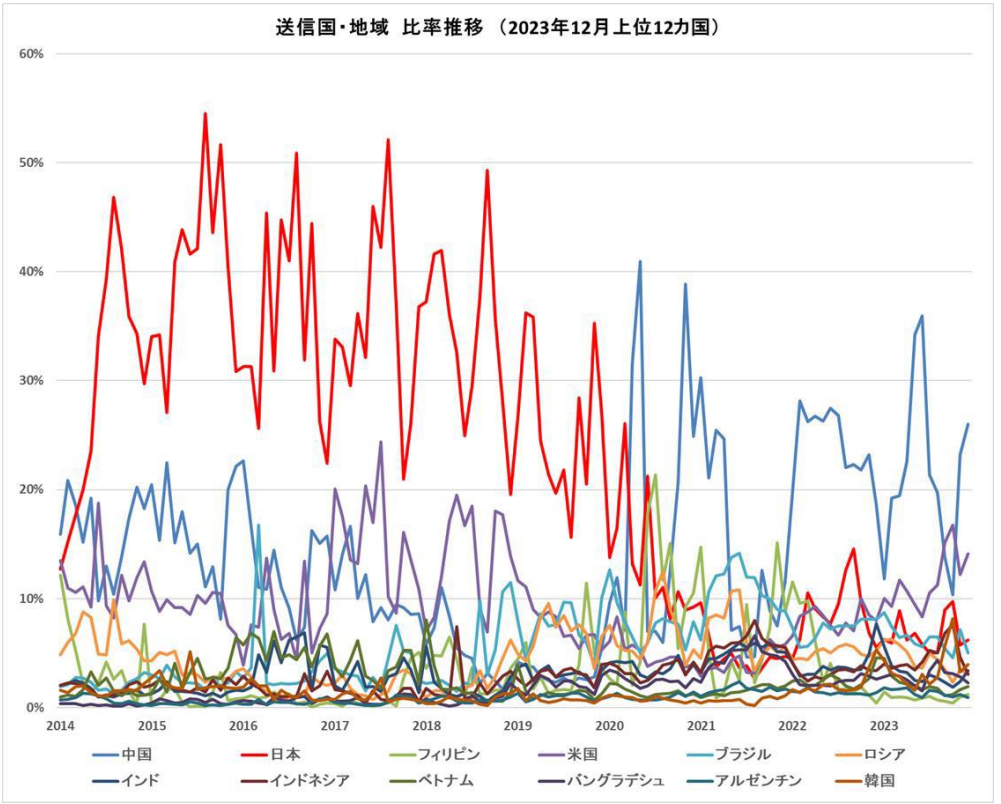
○　我が国の電気通信事業者が受信した電子メール中、迷惑メールが占める割合は現在は約４割前後。
○　国内着の迷惑メールの送信国は、中国が最多。

＜国内ISPにおける迷惑メール数・割合の推移（2023年9月時点）＞




出典：電気通信事業者10社の協力により、総務省がとりまとめ

＜国内着の迷惑メール送信国・地域の推移＞

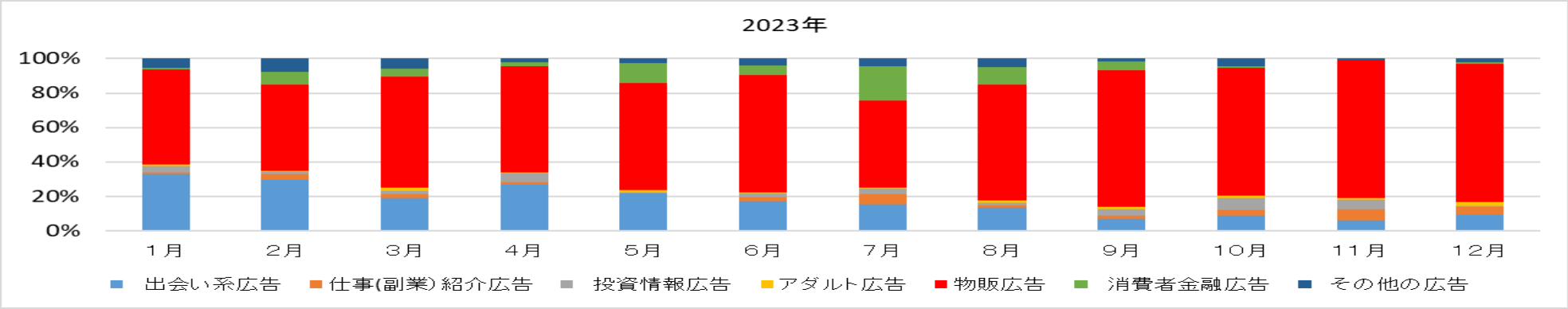



出典：一般財団法人日本データ通信協会迷惑メール相談センター調べ
（センターのモニター機で受信した情報を分析したもの）

# 我が国における迷惑メールの現状②

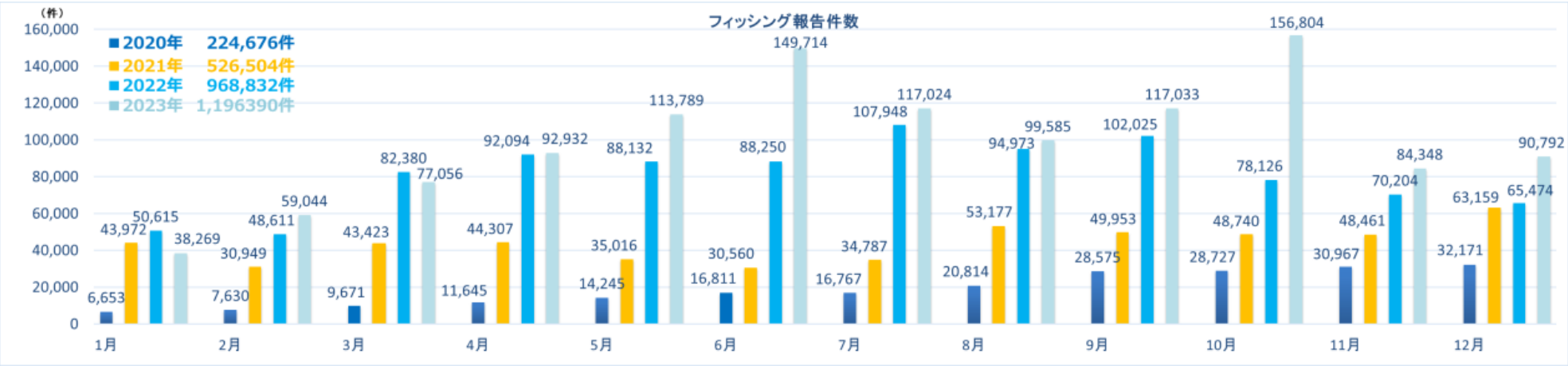
○　迷惑メールのうち、出会い系サイトや物販の広告宣伝を内容とするものが多くを占めている。
○　フィッシング報告件数は増加傾向。

**＜迷惑メールの広告宣伝内容別の構成比率＞**




出典：一般財団法人日本データ通信協会迷惑メール相談センター調べ（相談センターのモニター機で受信した情報を分析したもの）

**＜フィッシング情報の報告件数＞**



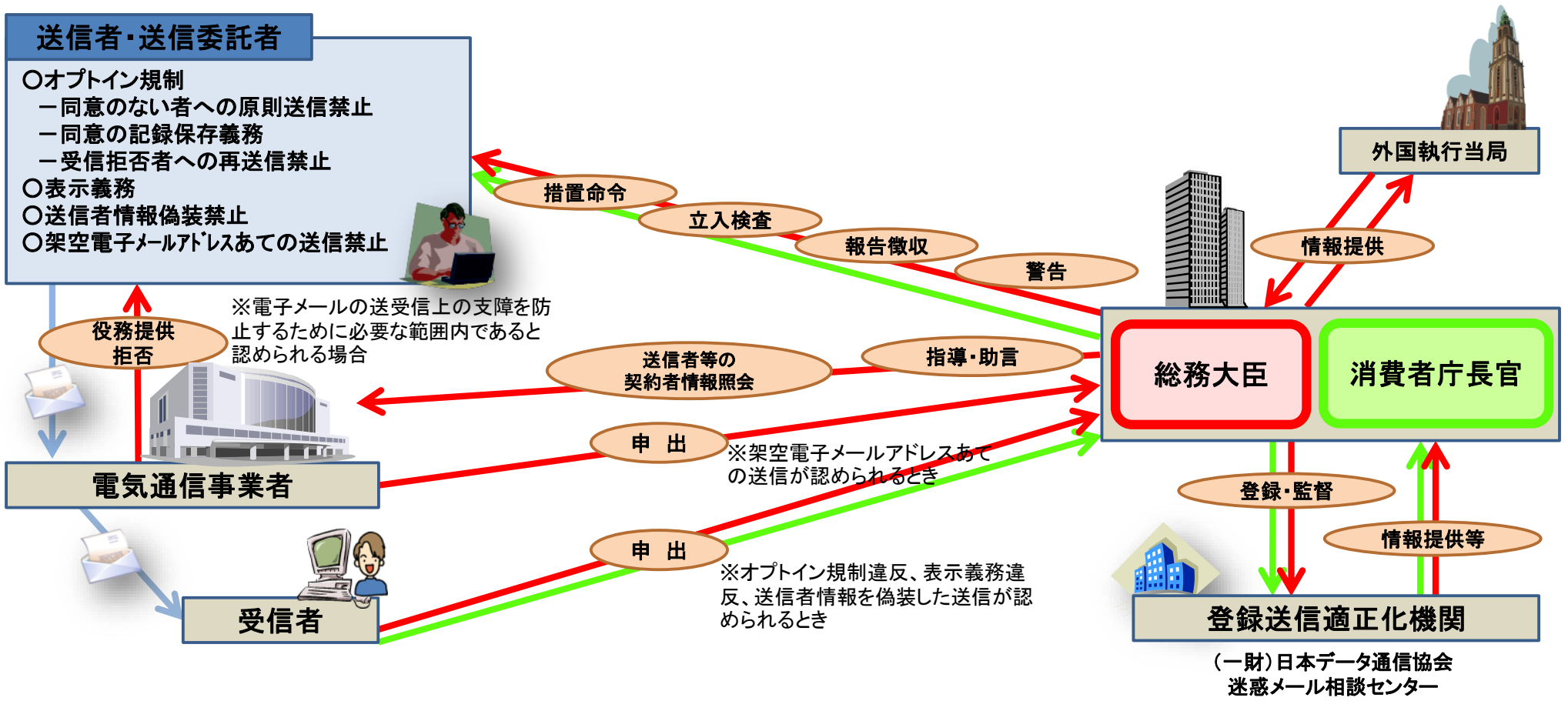

出典：フィッシング対策協議会「フィッシング報告状況」（https://www.antiphishing.jp/news/info/）　をもとに、迷惑メール対策推進協議会事務局が編集

# 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。



# 官民連携：迷惑メール対策推進協議会



○　迷惑メール対策に係る最新の情報共有、対応方策の検討、対外的な情報提供などを行うことを目的に、2008年11月、迷惑メール対策に関する関係者が幅広く集まり、「迷惑メール対策推進協議会」を設立。

○　現在では送信ドメイン認証技術の普及促進活動を中心として、調査研究や情報提供を随時実施。

## 構成

○　座長：新美育文 明治大学名誉教授
　　事務局：一般財団法人日本データ通信協会 迷惑メール相談センター

○　構成員：53名（2024年４月現在）

　　電気通信事業者、広告事業者、セキュリティベンダー、学識経験者、関係省庁（総務省、消費者庁、警察庁）等

○　送信ドメイン認証技術の普及その他の技術的課題に関し、方針案の作成、基礎的資料の作成等を行うため「技術ＷＧ」を設置（主査：櫻庭 秀次　電気通信大学 協力研究員）

## 主な活動

○　送信ドメイン認証技術の普及促進

○　「送信ドメイン認証技術導入マニュアル」の発行

○　「迷惑メール白書」の発行


迷惑メール白書

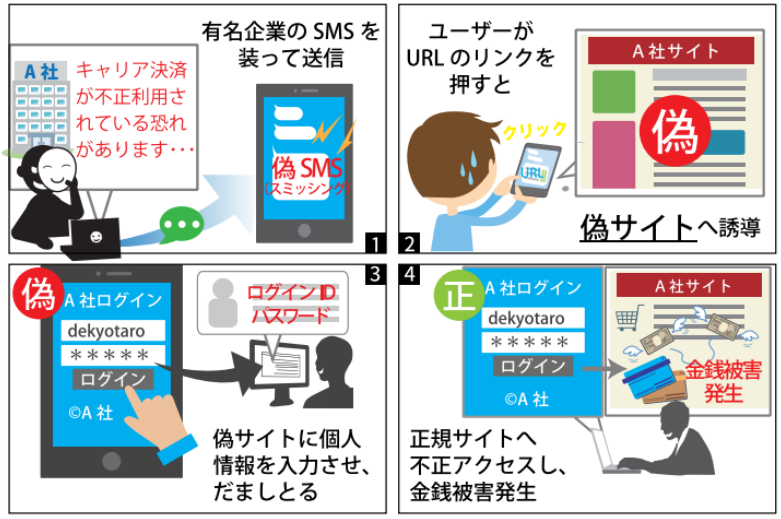

送信ドメイン認証技術
導入マニュアル

# （参考）フィッシングメールの危険性等に関する広報






〈SMSを利用したフィッシング詐欺の一般的な流れ〉

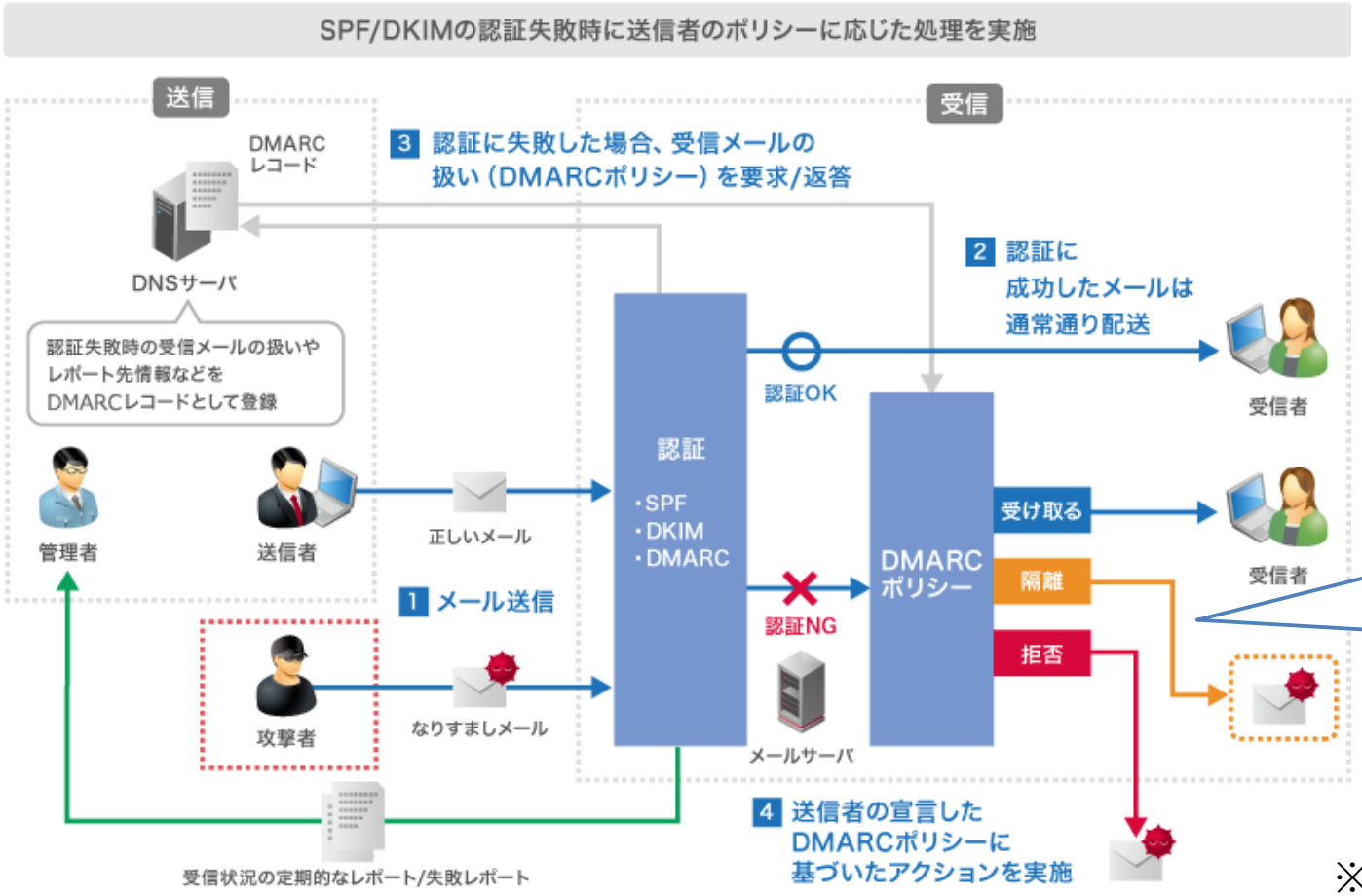


# 技術面の対策：送信ドメイン認証技術（DMARC）

○　DMARCは、送信側と受信側が協調し、総合的に送信ドメイン認証を行う技術であるため、受信者に表示される送信者アドレスの詐称に対応可能であることから、フィッシングメール対策に有効。

○　「国民を詐欺から守るための総合対策」（令和６年６月18日）においても、フィッシングメール対策として、DMARCの普及が求められている。

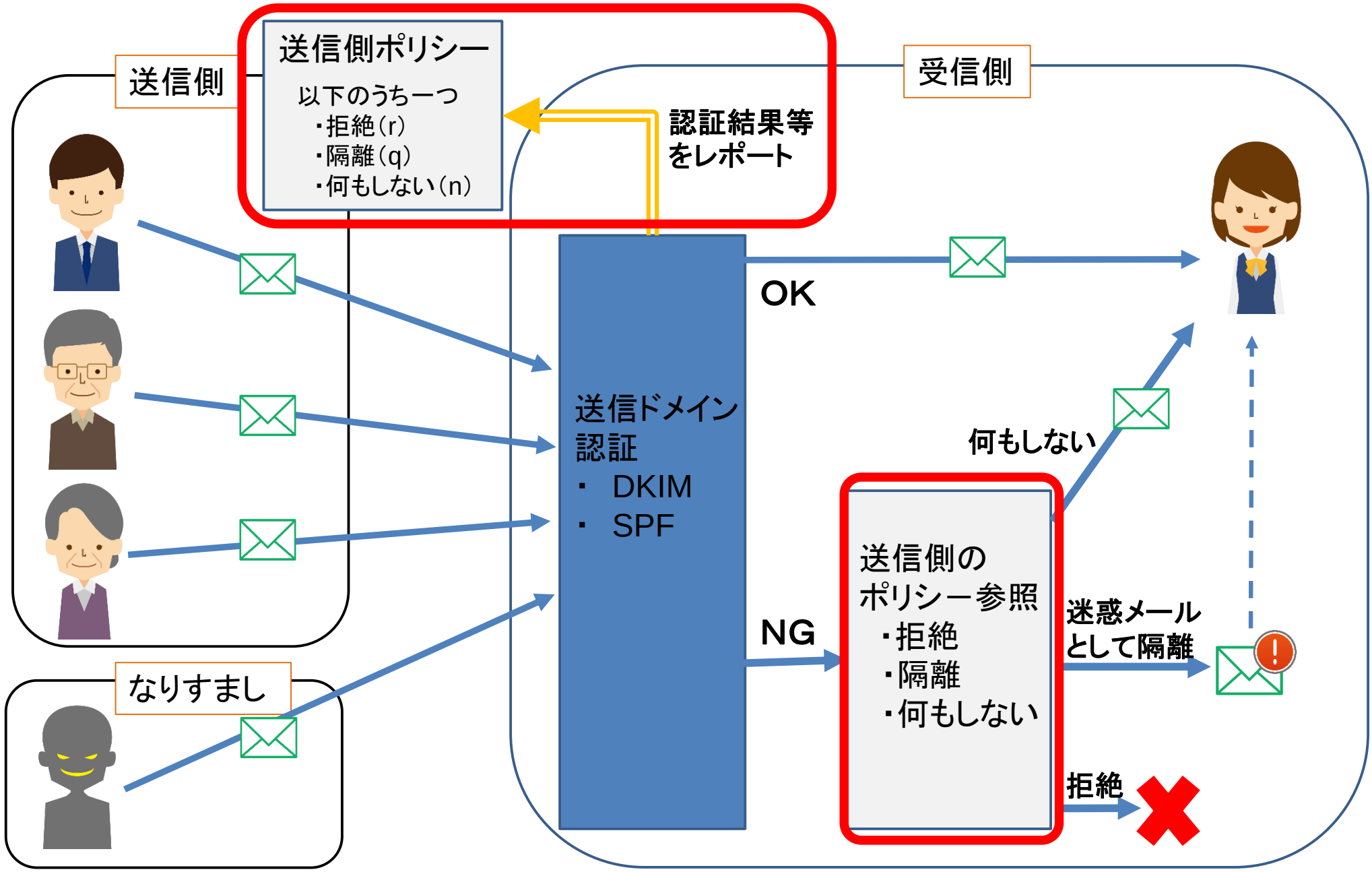
図3：DMARCの仕組み




送信側のポリシーに基づき、
① none（受け取る）
② quarantine（隔離）
③ reject（拒否）
のいずれかを実施

※IIJホームページより引用

# DMARCの概要図


送信側
送信側ポリシー
以下のうち一つ
・拒絶（r）
・隔離（q）
・何もしない（n）
認証結果等
をレポート
受信側
OK
送信ドメイン
認証
・ DKIM
・ SPF
何もしない
送信側の
ポリシー参照
・拒絶
・隔離
・何もしない
迷惑メール
として隔離
NG
拒絶
なりすまし

# 総務省におけるDMARCの普及促進に向けた取組

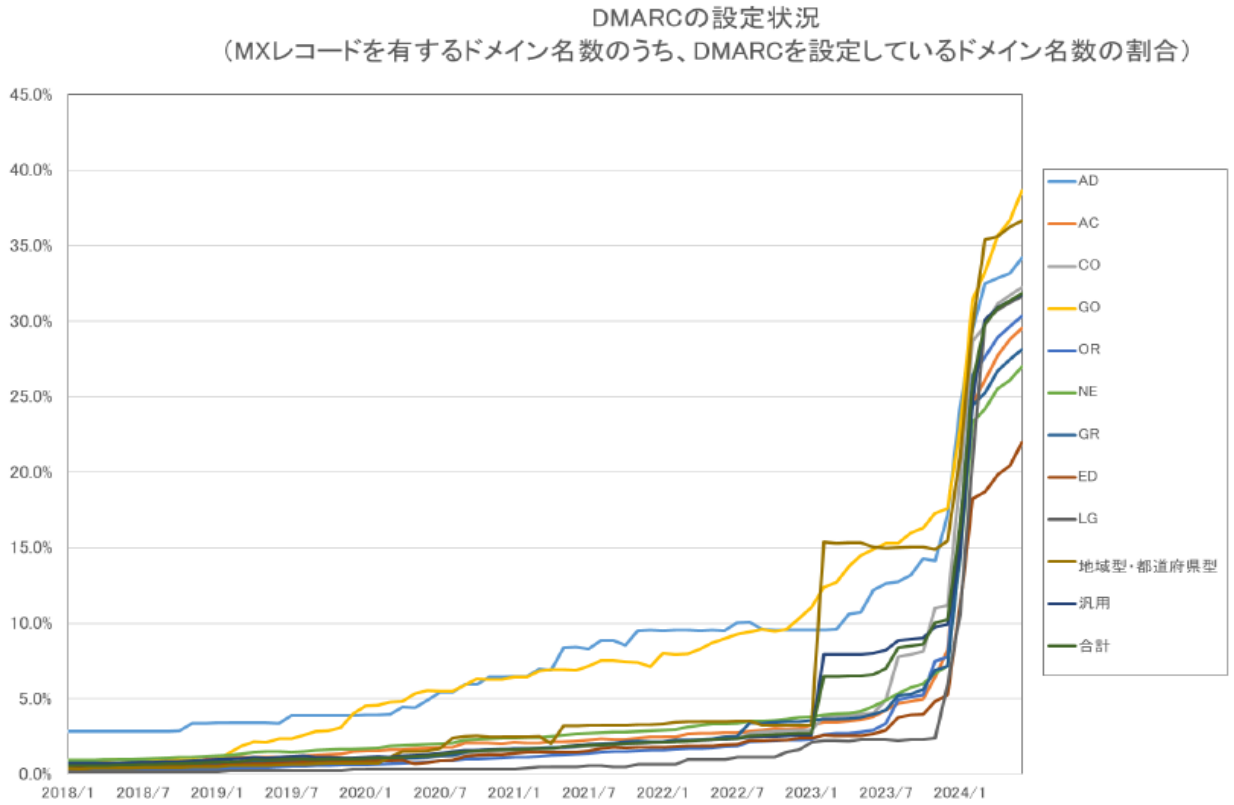


○　総務省では、関係省庁や通信事業者との協力により、送信ドメイン認証技術の普及促進に取り組んでいる。

・　令和３年５月、消費者行政第二課から物流団体連合会及び全銀協に対しDMARC導入の依頼文を送付

・　令和５年２月、経産省・警察庁と連名で日本クレジット協会に対してもDMARC導入の依頼文を送付。

・　NISCが令和５年７月４日に改訂した統一基準群「政府機関等の対策基準策定のためのガイドライン」において、DMARCの取扱強化を含め、迷惑メール対策の技術的な動向を踏まえた対策を追記。




△△△.ad.jp　JPNIC会員
△△△.ac.jp　大学など高等教育機関
△△△.co.jp　企業
△△△.go.jp　政府機関
△△△.or.jp　企業以外の法人組織
△△△.ne.jp　ネットワークサービス
△△△.gr.jp　任意団体
△△△.ed.jp　小中高校など初等中等教育機関
△△△.lg.jp　地方公共団体

# NISCガイドラインへの盛り込み



### 6.2.2 電子メール

**目的・趣旨**

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいするなどの機密性に対するリスクの他、悪意ある第三者等によるなりすまし等、電子メールが悪用される不正な行為の被害に電子メールを利用する職員等が巻き込まれるリスクもある。これらの問題を回避するためには、適切な電子メールサーバの管理が必要である。

なお、本款の遵守事項のほか、6.2.1「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

**遵守事項**

(1) 電子メールの導入時の対策

(a) 情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。

(b) 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。

(c) 情報システムセキュリティ責任者は、電子メールのなりすましの防止策を講ずること。

(d) 情報システムセキュリティ責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずること。

**【 基本対策事項 】**

＜6.2.2(1)(b)関連＞

6.2.2(1)-1 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下を例とする職員等の主体認証を行う機能を備えること。

a) 電子メールの受信時に限らず、送信時においても不正な利用を排除するためにSMTP 認証等の主体認証機能を導入する。

＜6.2.2(1)(c)関連＞

6.2.2(1)-2 情報システムセキュリティ責任者は、以下を全て含む送信ドメイン認証技術による電子メールのなりすましの防止策を講ずること。

a) DMARC による送信側の対策を行う。DMARC による送信側の対策を行うためには、SPF、DKIM のいずれか又は両方による対策を行う必要がある。

b) DMARC による受信側の対策を行う。DMARC による受信側の対策を行うためには、SPF、DKIM の両方による対策を行う必要がある。

6.2.2(1)-3 情報システムセキュリティ責任者は、必要に応じて、S/MIME 等の電子メールにおける電子署名の技術による電子メールのなりすましの防止策を講ずること。

6.2.2(1)-4 情報システムセキュリティ責任者は、職員等が機関等外の者と電子メールを送受信する場合には、政府ドメイン名を取得できない場合を除き、政府ドメイン名を使用した電子メールアドレスが利用される機能を備えること。

＜6.2.2(1)(d)関連＞

6.2.2(1)-5 情報システムセキュリティ責任者は、以下を例とする電子メールの盗聴及び改ざんの防止策を講ずること。

a) SMTP によるサーバ間通信を TLS により保護する。

b) S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用する。



（解説）

- **遵守事項 6.2.2(1)(a)「不正な中継」について**

不正な中継が行われると、迷惑メールの送信等に悪用される問題がある。これにより、電子メールサーバや通信回線のリソースが消費されて運用に支障をきたす、不正な中継を行う電子メールサーバとして他の電子メールサーバ等から接続や電子メールの転送を拒否される、又は迷惑メールの受信者からの苦情や問合せへの対応が必要になるなどの問題が生じるおそれがある。これらを回避するため、電子メールの不正な中継を行わないように電子メールサーバを設定することが必要である。送信元の電子メールサーバの IP アドレスによる制限や送信元又は宛先のメールアドレスのドメイン名による制限を行うなど、中継を許可する電子メールは必要最小限とすることが望ましい。なお、当該設定においては、多重防御の考えに基づき、メール中継サーバを含む全ての電子メールサーバにおいて実施することが望ましい。特にメール中継サーバを設置する場合には、送信元の電子メールサーバの IP アドレスによる制限等の対策をファイアウォールによる通信制限のみに依存するのではなく、メール中継サーバでも講じることで、ファイアウォールの設定ミスが発生した場合でも多重防御による効果が期待できる。

- **遵守事項 6.2.2(1)(d)「サーバ間通信の暗号化」について**

相手先サーバが暗号化に対応していない状況も考慮しなければならない。自らが送信側となる際には、相手先が暗号化に対応可能であることを確認し、確認が取れた場合には以降の通信を暗号化することが求められる。また、自らが受信側となる際には、相手先からの接続要求時に暗号化の機能に対応していることを示すことが求められる。

暗号化された通信の監視については、「(解説) 遵守事項 5.2.1(3)(a)(イ)「監視するデータが暗号化されている場合は、必要に応じて復号」について」を参照のこと。

また、電子メールクライアントと電子メールサーバ間の通信の暗号化についても併せて対応することが望ましい。

- **遵守事項 6.2.2(1)(d)「対策を講ずること」について**

技術的な事情等により対策に時間を要する場合は、「インターネット通信のセキュリティ強化と利用者に対する配慮について」（平成 29 年 7 月 10 日　内閣官房内閣サイバーセキュリティセンター事務連絡）に基づいて、計画的に対策を推進することが求められる。

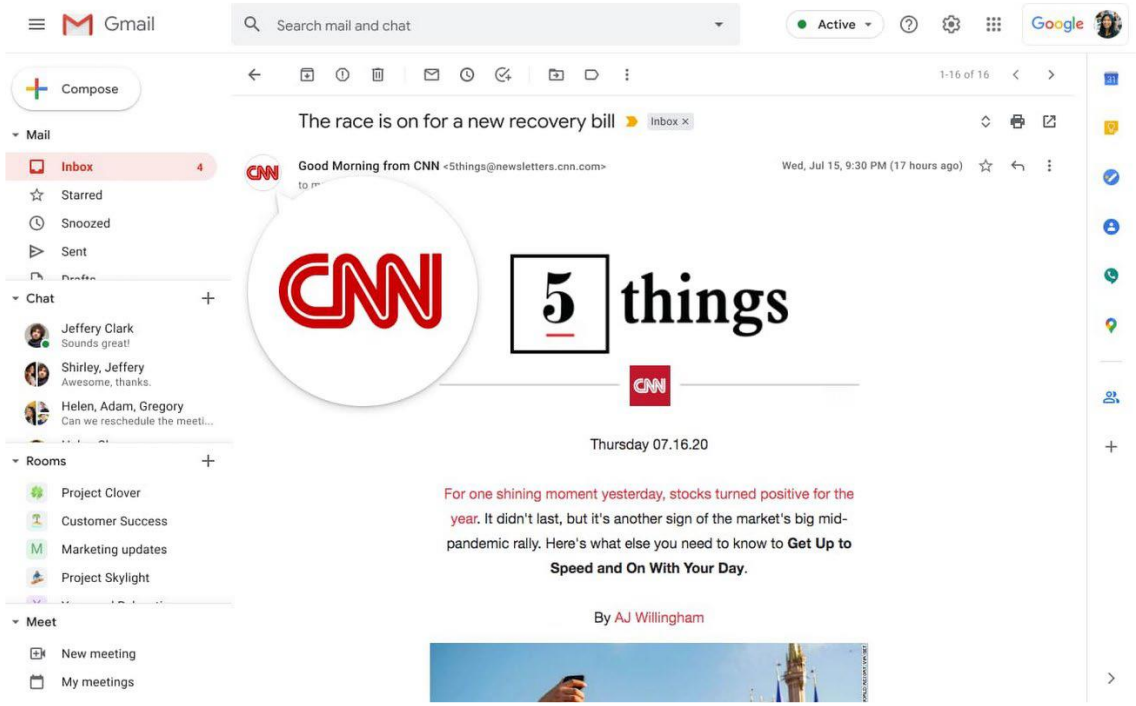
# （ご参考）BIMI



メール受信者が正規のメールであるかを判断できるよう、メールサービス事業者が送信ドメイン認証技術を用いて、受信者側でイメージ表示する機能を提供。

具体的には、BIMI (Brand Indicators for Message Identification)がIETF(Internet Engineering Task Force)に提出されており、まだ正式な仕様ではないものの、幾つかのメールサービスプロバイダで利用可能になっています。

※DMARCのポリシーがquarantineあるいはrejectであった場合、BIMIレコードの参照を試み、BIMIレコードが存在する場合、BIMIレコードに示されたBrandIndicator(ロゴ)の存在場所を示すURIから、ロゴ情報を取得、メールクライアントで表示。



DMARCの積極的な導入を
お願いします。

# SMSの不適正利用対策

# 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 |

# 不適正利用対策に関するワーキンググループについて



## 開催状況

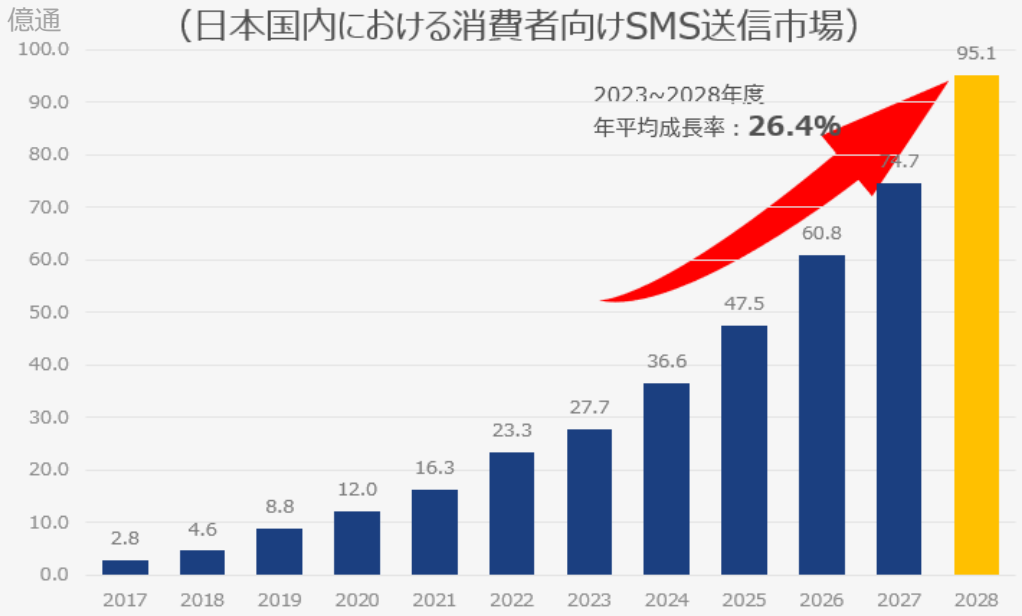
| | |
|---|---|
| 第１回（令和６年２月26日） | ○ICTサービスの不適正利用対策を巡る諸課題について<br>○SMSの不適正利用の実態について<br>・事業者ヒアリング：株式会社マクニカ、トビラシステムズ株式会社 |
| 第２回（令和６年３月14日） | ○SMS対策に関する関係者からのヒアリング<br>・事業者ヒアリング：NTTドコモ、KDDI、ソフトバンク<br>・オブザーバーからの報告：警察庁（サイバー警察局） |
| 第３回（令和６年４月15日） | ○SMS対策の方向性（案）について |
| | ○携帯電話不正利用防止法に基づく本人確認方法の見直し状況について<br>○本人確認に関する関係者ヒアリング<br>・オブザーバーからの報告：警察庁（刑事局）<br>・事業者ヒアリング：楽天モバイル |
| 第４回（令和６年５月15日） | ○本人確認に関する関係者ヒアリング<br>・有識者ヒアリング：デジタルアイデンティティ推進コンソーシアム<br>・事業者ヒアリング：イオンリテール、日本通信 |
| 第５回（令和６年６月６日） | ○携帯電話不正利用防止法に基づく本人確認方法の見直しに係る論点整理・意見交換 |
| 第６回（令和６年６月20日） | ○携帯電話不正利用防止法に基づく本人確認方法の見直しの方向性（案）について<br>○不適正利用対策に関するワーキンググループ中間とりまとめ（案）について |

# SMSの不適正利用対策について

## 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

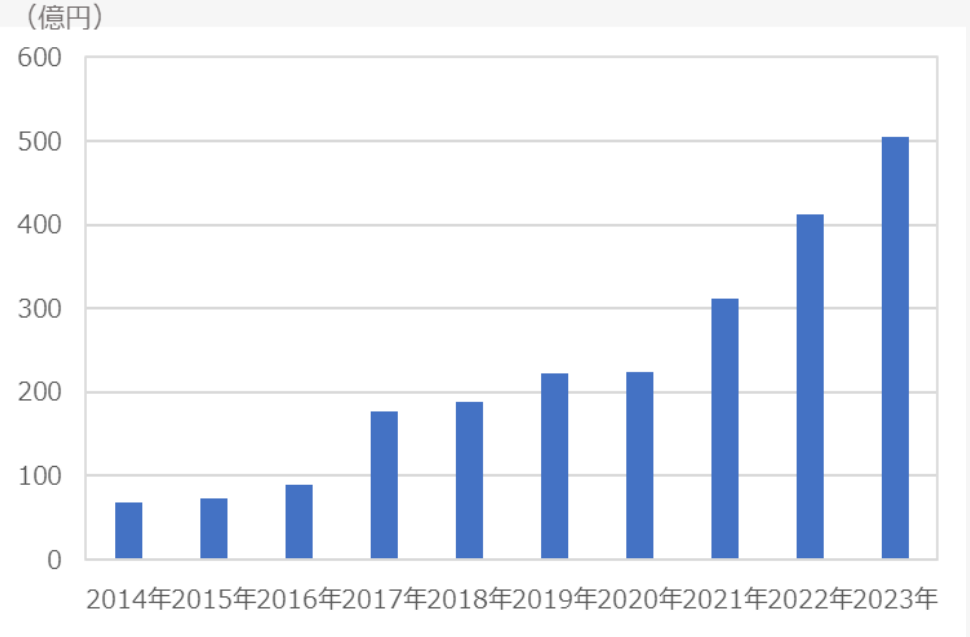

出典：ミックITリポート2024年1月号「2023年度に急ブレーキがかかるも2028年度まで成長期が続くA2P-SMS市場」より。
デロイト トーマツ ミック経済研究所株式会社

ADD VNTR.

# SMSの不適正利用対策について

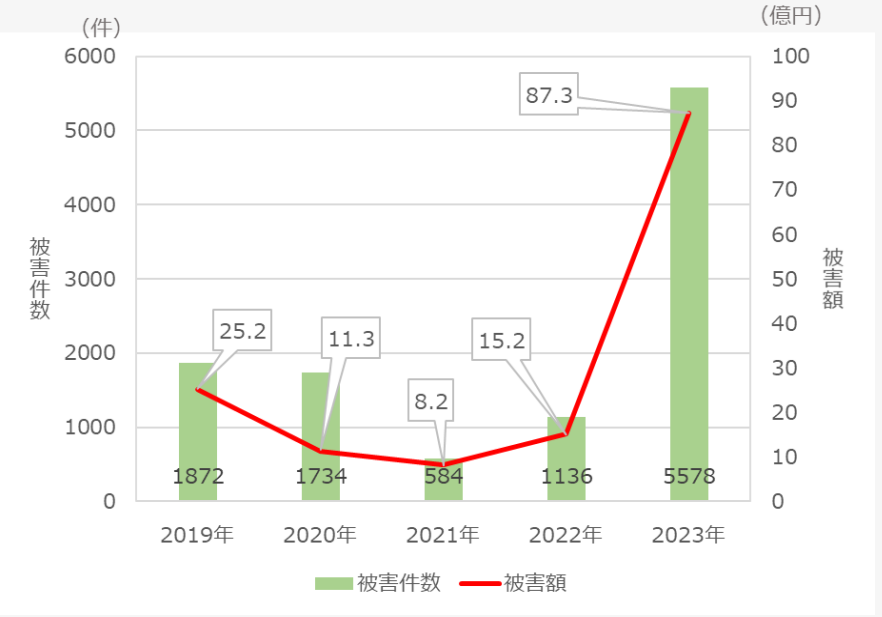
## SMSの犯罪利用

（一社）日本クレジット協会の調査では、令和5年のクレジット番号盗用被害額は約504.7億円に、また、警察庁の調査では、令和5年のインターネットバンキングに係る不正送金被害額は約87億円に及んでおり、被害は深刻なものとなっている。




クレジット番号盗用被害額の推移

※（一社）日本クレジット協会調査より




インターネットバンキングに係る不正送金被害額の推移

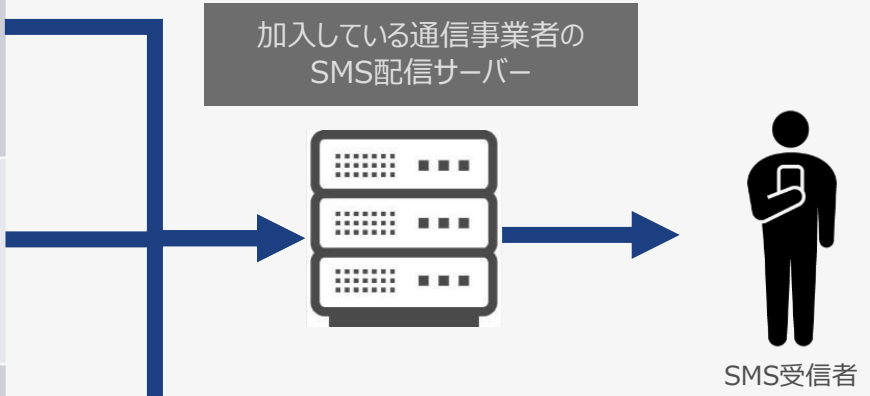
※国民を詐欺から守るための総合対策（概要）
（犯罪対策閣僚会議（令和６年６月18日決定）より

# SMSの不適正利用対策について

## 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。

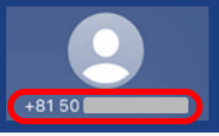
| 配信経路 | 送信元番号の表示  |
|---|---|
| ①国内携帯電話端末 | 携帯電話番号<br>（090~ 080~ 070~など） |
| ②国内SMS配信事業者 | 国内固定電話番号<br>キャリア共通番号<br>（03~ 0120~ 0005~など） |
| ③海外通信事業者 | 海外電話番号<br>アルファベット<br>ランダムな英数字など |



# SMSの不適正利用対策について

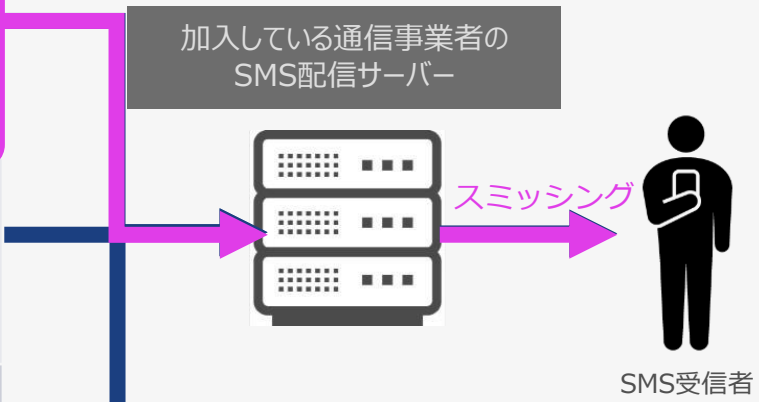
## スミッシングの発信源はマルウェア感染端末

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

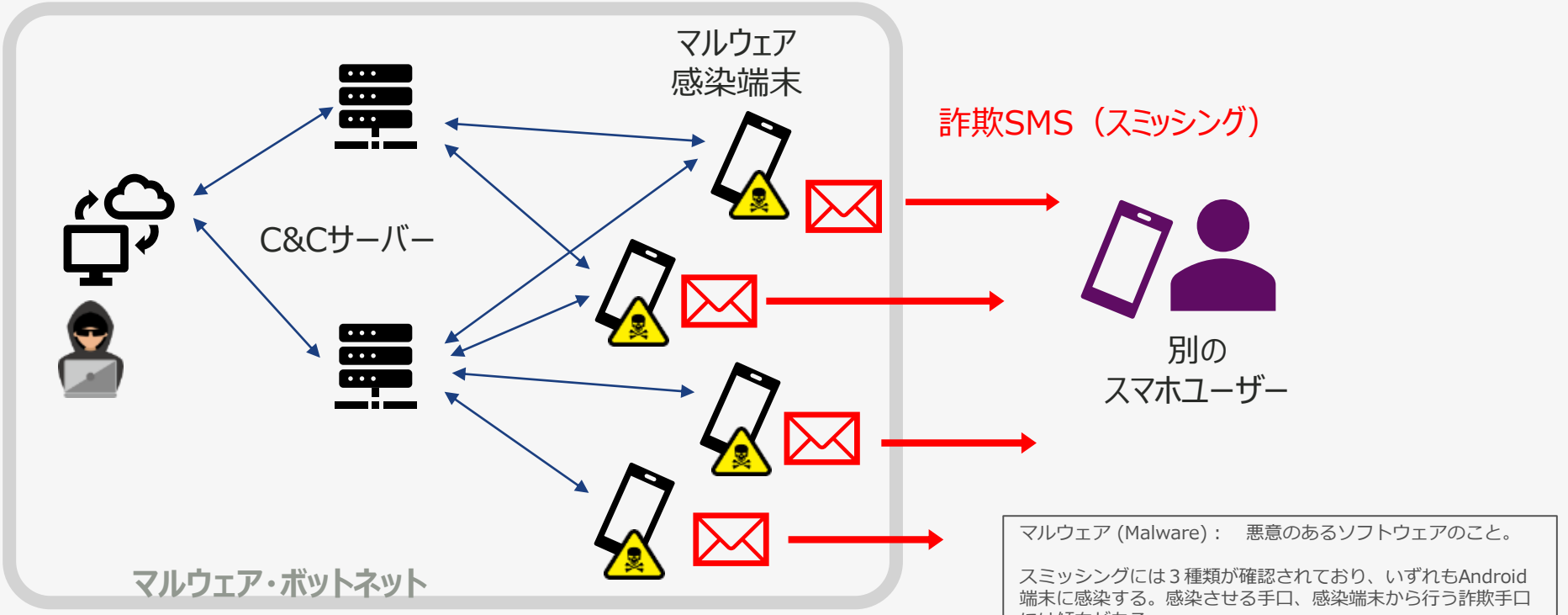



※：NTTドコモ 三谷咲子様　2023/11/7 JPAAWG6登壇資料
携帯キャリアによるSMSフィッシング(スミッシング)対策の最新情報

# SMSの不適正利用対策について

## 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。

# SMSの不適正利用対策について

## 不適正利用対策に関するワーキンググループ報告書（案）

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

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
- 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]

[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

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]

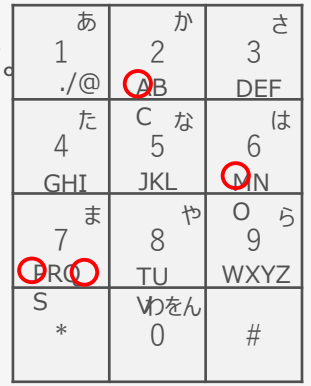
[23] 利用者に対し、契約締結時に書面等を用いて明確に説明することが考えられる。また、既に契約している者に対しては、ウェブサイトへの掲載に加えて、電子メールや郵便等によってマルウェアに感染している可能性が高い端末の利用者に対して注意喚起をすることを周知するとともに随時同意内容を変更できる（設定変更できる）こと及びその方法を説明すること等が考えられる。
[24] 令和６年７月から(株)NTT ドコモにおいて、「意図せぬ迷惑メッセージ送信に関するお知らせ」の提供が開始された。

13

# SMSの不適正利用対策について

## 海外事例：スミッシング共通窓口による対策推進

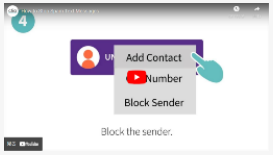
通信事業者横断のスミッシング申告として、Spam Reporting Service (7726) が広く使われています。




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

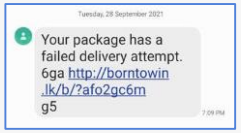
| 国 | イギリス | アメリカ | ニュージーランド |
|---|---|---|---|
| 運用主体 | Ofcom（情報通信省） | CTIA（携帯電話事業者の業界団体） | DIA（内務省） |
| 概要 | • 利用者は、不正SMSを受信したら7726に転送する<br>• iPhone/Androidの両方から利用可能で、使い方のYouTubeチュートリアルを公開<br>  | • 利用者は、不正SMSを受信したら7726に転送する<br>• iPhone/Androidの両方から利用可能で、使い方のYouTubeチュートリアルを公開<br>  | • Email/SMSに共通の不正申告サイトを設置している<br>• 利用者は、不正SMSを受信したら7726に転送する<br>• iPhone/Androidの両方から利用可能<br>  |
| 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 |

ADD VNTR.

# SMSの不適正利用対策について

## 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<br>  <br>② 被害者がリンクをクリック 不正サイトにアクセス<br>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<br>④ マルウェアが、スマートフォンから個人情報を取得<br>• 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<br>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<br>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**<br>DIAが緊急対策グループ設立<br>• CERT NZ、電気通信フォーラム、通信事業者と協力<br>最初の通報から3時間以内<br>**初動対応**<br>（感染者向け）<br>DIAが対応チームを作成、<br>• 通報からマルウェア感染被疑の600の電話番号を特定<br>• 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<br>（一般向け）<br>SNSの活用<br>• プレスリリースとメッセージ掲載<br>• 怪しいメッセージはSpam Reporting Service (7726) への通知を推奨<br>**根本対応**<br>Flubot マルウェアサーバを停止<br>• 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<br>• 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

# SMSの不適正利用対策について

## マルウェア感染対策の例（アメリカの場合）

**フィッシングのブロック**

米国Verizonでは毎月10億通以上の不正テキストメッセージをブロック。

（ユーザーが選択できるオプション）

・指定された電子メールアドレスまたはドメインからの全てのSMSをブロック。

・Webドメインからの全てのSMSをブロック。

・電子メールから送信される全てのSMSをブロック。

**ガイドラインに基づくSMS送信の要請**

米国ワイヤレス通信事業の業界団体であるCTIAは、SMSをビジネス利用するにあたり、

送信者である企業が守るべきベストプラクティスを “Messaging Principles and Best Practices”※ として公開。

※オプトインとオプトアウトについて記載

**Secure Messaging Initiative (SMI) の共同設立**

CTIAの活動で、通信事業者と政府機関がスパムの疑いのあるメッセージに関する情報を分析共有等を実施。

# SMSの不適正利用対策について

## 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。

| | NTTドコモ | au | ソフトバンク |
|---|---|---|---|
| ネットワーク側の対応 | 危険SMS拒否<br>2022/03開始<br>https://www.docomo.ne.jp/info/spam_mail/sms/ | 迷惑SMSブロック<br>2023/02開始<br>https://www.au.com/mobile/service/sms/filter/ | 迷惑SMS対策機能<br>2022/06開始<br>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<br>https://www.docomo.ne.jp/service/anshin_security/ | 迷惑メッセージ・電話ブロック<br>https://media2.kddi.com/meiwakublock/safecall/PC/PC.html | セキュリティOne<br>https://www.softbank.jp/mobile/service/security-one/ |

楽天モバイルは本年７月より「迷惑SMS拒否設定」の提供開始

ADD VNTR.




不適正利用対策に関するWG資料６－２より一部追記して作成

# 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、NTTドコモ・au・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

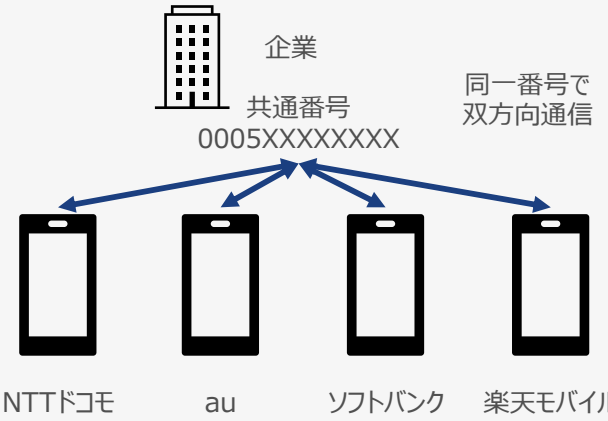
| 通信事業者 | NTTドコモ | au | ソフトバンク | 楽天モバイル |
|---|---|---|---|---|
| サービス名称 | ＋メッセージ | | | Rakuten Link |

ADD VNTR.

## キャリア共通番号（０００５）とは

通信事業者４社（NTTドコモ、au、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



# 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。

# SMS不適正利用対策事業者連絡会の立ち上げについて



| | |
|---|---|
| 目的 | SMS配信市場が著しく成長し、民間事業者だけでなく地方自治体等の公共機関においてもSMSを活用する機会が増えている一方で、SMSを悪用するフィッシング詐欺（スミッシング）の被害が増加していることを踏まえ、SMSに関わる主要事業者間で、定期的にSMSの不適正利用に係る情報を交換し、事業者間の自主的な対策を推進する。 |
| 活動内容 | ● SMSの不適正利用状況に関する**定期的な情報交換**<br>● SMSの不適正利用対策のための**事業者間の自主的な取組**の検討<br>● スミッシング詐欺対策に関する**利用者への周知広報**の検討 |
| 構成員 | ● 【携帯電話キャリア】 NTTドコモ、KDDI、ソフトバンク、楽天モバイル<br>● 【MVNO】テレコムサービス協会（MVNO委員会）<br>● 【SMS配信事業者】<br>NTTコムオンライン、メディア4u、アクリート、りーふねっと、AI CROSS<br>● 【セキュリティ関係】 マクニカ<br>● 【総務省】 利用環境課、番号企画室　（その他必要に応じて声かけ） |

ご清聴ありがとうございました