

不適正利用対策に関するワーキンググループ（第7回） ご説明資料

2025年4月21日
ソフトバンク株式会社

喫緊の課題である特殊詐欺等の各種犯罪に関しては
事業者としても重大な社会問題と認識



被害額：約720億円
認知件数：約21,000件
(2024年)

×



AIの利用など
犯罪手段の高度化

基本的な考え

不適正利用の防止に向け、携帯電話契約時の本人確認強化のみならず、利用者・SNS事業者等含む各方面からの対策が必要

「国民を詐欺から守るための総合対策」における主な施策

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
 - インターネット上で拡散する偽・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開鎖促進
- 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

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

出典：犯罪対策閣僚会議資料（2024年6月18日）

不適正利用防止に関する取組み

契約時本人確認に関する関係法令・業界自主ルールへの遵守のほか、
利用者のリテラシー向上に向けた各種取り組みを継続的に実施



不正契約防止

- 契約者本人確認書類を偽造・改ざんしたり、これらの書類を携帯電話の申し込みに使用することや、他人の名義で勝手に申し込みをした場合は、文書偽造罪（刑法第155条）や詐欺罪（刑法第246条）に触れる行為となります。
- 携帯電話申込時の本人特定事項（氏名・住居・生年月日）の虚偽申告や、自己名義携帯電話の無断譲渡、他人名義携帯電話の譲渡・譲受は、携帯電話不正利用防止法に違反する行為となります。
- 携帯電話申込時の連絡先や勤務先の電話番号は、必ず繋がる正しい番号を入力してください。審査時やお申し込み後に当社から確認の電話をする場合があります。

本書面と
ウェブサイトを **必ずご確認ください**



2025-03-19

特殊詐欺被害ゼロに向けたスマホの活用法。ソフトバンクと
警視庁戸塚警察署がセミナーを実施

ライフスタイル | ワイモバイル | シニア | シニアのスマホ利用 | 防犯



ご契約時の説明（重要事項説明）

各種コンテンツ提供、教室・セミナー開催等による周知

携帯電話の本人確認のルール関連

不適正利用の防止（契約の匿名性の排除、事後追跡性の確保等）のため、手口に合わせ、民民の契約において足りない部分を補完してきた認識



【法令・業界自主ルールで定められている事例】

- 犯罪利用の可能性のある回線の停止（契約者確認の求め）
- プリペイド携帯における本人確認
- データ回線における本人確認 等

- ・事業者は法令によらずとも、与信の観点から本人確認を行う必要がある
- ・犯罪の手口は変遷・多様化する



新たなルールの必要性がある場合、業界自主ルールでの対応を基本とし、
法令による規律は最小限にすべきと考える

検討事項

SIMの不正転売が増加し、詐欺への転用等の実態が指摘されている中、転売の防止に向けてどのような効果的な対策が考えられるか。

当社考え

- ・ 第一に、SIMの無断譲渡は違法であることの周知徹底が必要と考えます。
- ・ 総務省殿資料にあるような、犯罪利用可能性のある利用者の情報交換も対策案の一つと考えますが、下記のような点の整理が必要と考えます。
 - 警察からの提供情報の正確性の確保
 - 警察からの提供情報を正とした対応における、事業者側の免責
(例えば回線提供の拒否等へ活用した場合、役務提供義務に反しない整理等)

検討事項

法人の担当者が契約を行う場合における在籍確認の手法について、法令上の規定がなく、事業者によって異なる取扱いとなっている中、利用者視点に立ってどのような方策が考えられるか。

当社考え

- ・ 与信の観点から、既に法人の担当者の在籍確認が各事業者の運用として導入されているところであり、一定の対策は講じられているものと考えます。
- ・ これまでどおり本人確認の手法は個人契約に準じるものとし、法令での要件追加は不要と考えます。
- ・ なお、各事業者において必要書類が異なる点は、与信に関する各社の考え方によるところであり、法令等での統一化を図る必要はないものと考えます。

検討事項

携帯電話の契約時における他社の本人確認結果への依拠について、これまでの議論を踏まえ、利便性と不正対策のバランスの観点から、どのように考えるべきか。

当社考え

- 仮に依拠を許容する場合、本ワーキンググループの報告書における以下の記載に基づき、依拠先としては公的個人認証を行っている事業者に限定すべきと考えます。

過去の本人確認結果に依拠するに当たっては、依拠先の本人確認結果に依存することとなるため、保証レベルの低い本人確認結果に依拠することは、現行の法令に則った本人確認と同等の手続きがとられたとは必ずしもみなせないものと考えられる。従って、本人確認における保証レベルが高く、一定の手続きのもと継続的に最新の本人特定事項を取得可能な本人確認を実施することが望ましい。こうした本人確認方法は、例えば、公的個人認証による方法が考えられ、過去の本人確認結果の依拠方法としては、公的個人認証を用いて本人確認を行った結果に依拠するとともに、依拠先において多要素認証等の本人認証を実施する方法が考えられる。なお、過去の本人確認結果に依拠する方法については、事業者のニーズや本人確認の保証レベルとのバランス等を鑑みつつ、今後、総合的に検討することが適当である。

出典：不適正利用対策に関するワーキンググループ報告書（2024年11月29日）

検討事項

2回線目以降の回線契約時の本人確認について、法令上の要件が1回線目とは異なっている中、昨今の犯罪手口の巧妙化、高度化に対し、どのような効果的な対策が考えられるか。

当社考え

- 2回線目以降の回線契約時の本人確認について、法令上の要件が1回線目と異なっている点については一定の合理性があるものと考えます。
- 一方で、ID/PASSの詐取による不正契約事案を防止するためには、既存回線でのログイン必須化やワンタイムパスワードによる認証を取り入れる等、当人認証性を高めることが必要と考えます。

検討事項

上限契約台数について、本人確認が適切になされない場合に、大量不正契約に繋がる可能性があるが、利用者のニーズと不正対策のバランスの観点から、どのように考えるべきか。

当社考え

- 第一に本人確認の徹底、SIMの無断譲渡が違法であることの周知徹底、2回線目以降の本人確認における本人認証性の強化（ワンタイムパスワードによる認証等）が必要と考えます。
- 上限契約台数については、利用者の多様な利用用途に鑑み、過度な制約を設けることはふさわしくないとの基本的考えに則りつつも、業界自主ルールのほか各社が与信の観点から既に一定の制限を設けており、現行以上の追加的な規律や法令等による制度的担保までは不要と考えます。

検討事項

データSIMの本人確認について、法令上の要件が音声SIMと異なっている中、昨今の犯罪手口の巧妙化、高度化に対し、どのような効果的な対策が考えられるか。

当社考え

- データSIMについては、当社は業界自主ルールのもと音声SIMと同等の本人確認を実施しており、今後もこの取り組みを継続してまいります。