2.『国民を詐欺から守るための総合対策』の策定

要約

- 国内外で科学技術を悪用した特殊詐欺によって被害が拡大していることから、フィッシングなどを対象に『国民を詐欺から守るための総合対策』が策定された。
- 本総合対策では、送信者ドメイン認証技術やパスキーの導入推進、本人確認でのマイナンバーカードによる公的個人認証への原則一本化などがあげられている。

策定の背景

信頼とは様々な社会活動・経済活動を円滑に行うために不可欠なものであり、安全・安心な社会を支える基盤です。しかし、近年ではその信頼を逆手にとり、相手をだまして財産を奪い取る詐欺が増えています。そのような事案に対して政府は対策プランを策定し、官民一体となった対策を講じてきました。

しかしながら、官民をあげた対策に応じて特殊詐欺の手口も変化しています。その要因の一つとして急速に発展している科学技術の悪用があげられます。それにより、犯罪の手口が急激に巧妙化・多様化し、引き起こされる被害も拡大している状況が見受けられます。

このことは日本だけでなく国際的にも問題となっており、2023 年に水戸で行われた G7 茨城水戸内務・安全担当大臣会合においても共通の課題として認識が共有されました。また、2024 年にはロンドンで国際詐欺サミットが開催され、G7 以外の国を含むより広い枠組みで国境を越える組織的詐欺に協働して対処していくことが確認されました。

これらの背景を踏まえて、特殊詐欺、SNS 型投資・ロマンス詐欺、フィッシングを対象に、『国民を詐欺から守るための総合対策』(以降、本総合対策)(*1)が策定されました。

総合対策の概要

本総合対策は以下の章立てとなっています:

章題	内容
「被害に遭わせない」ための対策	①SNS 型投資・ロマンス詐欺、②フィッシング、③特殊詐欺等のそれぞれの被害実態に注目した対策について。
「犯行に加担させない」ための対策	主に「闇バイト」に関する対策について。
「犯罪者のツールを奪う」ための対策	携帯電話や預貯金口座、暗号資産、空き家等に関する対策について。
「犯罪者を逃さない」ための対策	犯罪グループの存在を見据えた取締り・実態解明や適正な科刑の実現、マネー・ローンダリング対策、財産的被害の回復について。

出典:『国民を詐欺から守るための総合対策』(*1)を基に大和総研作成

対策の具体的な内容

本総合対策の中では、利用者などに対する注意喚起や啓発、実効的な広告審査や偽広告の削除、無登録業者による偽広告の掲載が違法となり得る旨の明確化、取締り及び実態解明の促進や適正な科刑の実現といった、様々な場面、レイヤー、粒度での対策案があげられています。その中には情報技術に関わるものも含まれています。

(*1) 犯罪対策閣僚会議『国民を詐欺から守るための総合対策』(令和 6 年 6 月 18 日)

次に、フィッシングへの対策として、送信ドメイン認証技術（SPF、DKIM など）やパスキーがあげられました。送信者ドメイン認証技術とは、IP アドレスや電子署名を基に送信元の正当性を確認する技術です。また、パスキーとは、パスワードを使わずに認証する技術です。具体的な技術は以下の表のとおりです：

技術	概要
SPF	Sender Policy Framework の略。 送信元サーバーの IP アドレスから送信元の正当性を確認する仕組み。
DKIM	DomainKeys Identified Mail の略。 電子メールに付加された電子署名により送信元と本文の正当性を確認する仕組み。
DMARC	Domain-based Message Authentication, Reporting, and Conformance の略。 SPF または DKIM での認証に利用したドメイン名と表示上の送信元ドメインが一致するかを確認する。 一致しない場合には指定の操作が行われ、認証結果を送信側が受け取る仕組み。
BIMI	Brand Indicators for Message Identification の略。 DMARC での認証に成功したメールにロゴを表示させる技術。 オプションでロゴについての証明書を指定可能。
VMC	Verified Mark Certificate の略。 BIMI で表示されるロゴについての証明書。 ドメイン認証に加え、ロゴの商標登録、公証人や弁護士などによる申請者自身の確認などが求められる。
パスキー	パスワードの代わりに、アクセス先とアカウントに紐付いた公開鍵に対応する秘密鍵で生成した署名によって認証を行う技術。 ドメイン情報が一致しないと認証できないため、フィッシング耐性が高い。

出典：『国民を詐欺から守るための総合対策』を基に大和総研作成

なお、SPF/DKIM/DMARC については DIR SOC Quarterly vol.6 2023 autumn(*1)の『DMARC の導入にかかわる動向』で、パスキーについては vol.5 2023 summer(*2)の『パスワード不要の新しい認証方式「パスキー」』でそれぞれ取り上げています。たとえば、Gmail でロゴを表示させるためには VMC が必須となっています(*3)。また、au やメルカリ、任天堂といった企業では既にパスキーでの認証に対応しています。

他に、「犯罪者のツールを奪う」「犯罪者を逃さない」ための対策が記載され、契約などにあたっての本人確認があげられました。預貯金口座の開設や携帯電話の契約などの際には犯罪収益移転防止法(*4)や携帯電話不正利用防止法(*5)で本人確認することが定められています。この本人確認における本人確認書類の券面の偽変造が相次いでいるため、非対面で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一本化し、運転免許証などを送信する方法や顔写真のない本人確認書類などは廃止するとしています。また、対面であっても、IC チップ情報の読み取りを義務付けるとしています。

最後に

本総合対策は政府や地方自治体だけではなく、民間事業者の協力を得て推進するものとされています。そのため、これを基に各業界のガイドラインにセキュリティ対策として反映されることが予想されます。

本総合対策であげられた対策は特定の業界におけるものも含まれるため、必ずしも読者の皆さまの業界に当てはまるとは限りません。しかし、対策方法から逆説的に犯罪の手口がうかがえますので、私的な防犯対策としても一度読んでおくと良いでしょう。

（DIR SOC Quarterly 執筆者一同）

(*1) DIR SOC Quarterly vol.6 2023 autumn［第 3 部 1.］

(*2) DIR SOC Quarterly vol.5 2023 summer［第 3 部 2.］

(*3) Google Help『BIMI を使用してメールにブランドロゴを追加する』

(*4) 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）

(*5) 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（平成 17 年法律第 31 号）