生き抜く力 No.18
2025 一般社団法人ＮＴＳセーフティ家計総合研究所

セキュリティに対する脅威に備える

上席研究員　博士（法学）　吉元利行

2026 年 1 月 29 日に独立行政法人情報処理推進機構 （Information-technology Promotion Agency, Japan 以下「IPA」という）が「情報セキュリティ 10 大脅威 2026」を公表しました。

個人の皆さんには、あまり関係ないと思われがちですが、パソコンやスマートフォン、タブレットなどを保有していない人はほぼいないと思われますので、大いに関係があります。特に、パソコンやスマートフォンの操作に不慣れな人（年齢は無関係です）は、いつの間にか財産的、精神的な被害者になることと同時に、知らないうちに加害者になる可能性もあります。どのような脅威があるのかを知って、その対策を知り、自衛に努める必要があります。

「情報セキュリティ 10 大脅威 2026」とは

「情報セキュリティ 10 大脅威 2026」は、2025 年に発生した社会的に影響が大きかった情報セキュリティの事故や攻撃の状況などから、IPA が脅威候補を選定し、情報セキュリティ分野の研究者、企業の実務担当者などからなる「10 大脅威選考会」が審議・投票を経て決定したものです。

「10 大脅威」には、「組織向け脅威」と「個人向け脅威」の 2 種類があります。

企業の場合は、企業の営業秘密や機密情報などを狙った標的型攻撃、金銭（身代金）を狙うランサム攻撃、システムの脆弱性を悪用した攻撃などが有名です。これに加え、DDoS（ディードス）攻撃という、ターゲットとなるサーバーやネットワークに膨大な負荷をかけ、「サービスを停止させること（＝利用不能にすること）」を狙うものがあります。この攻撃は、攻撃の停止と引き換えに身代金を要求する金銭狙いのほか、サービスを止めて経済的損失と信頼失墜を与える営業妨害、思想・抗議など政治的な不満を表明し、相手の活動を阻害する目的、相手への嫌がらせや、自分の実力を誇示し、身代金を狙う目的などたくさんの目的で実施され、これらのサイバー攻撃に対し、様々なセキュリティ対策が必要とされているのは周知のとおりです。

しかし、個人利用の場合、そのような攻撃の対象となる機密情報や財産等が大きくないため、あまり脅威を感じていない人が多いかもしれません。しかしながら、「個人向け 10 大脅威」の中には、「インターネットバンキングの不正利用」「クレジットカードの不正利用」「サポート詐欺（偽警告）による金銭被害」「スマホ決済の不正使用」「メールや SNS 等を使った脅迫・詐欺の手口による少額から多額の財産的損害が発生する脅威が半数を占めています。

【図表】情報セキュリティ 10 大脅威 2026［個人］

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	7年連続10回目
インターネット上のサービスへの不正ログイン	2016年	11年連続11回目
インターネットバンキングの不正利用	2016年	4年ぶり8回目
クレジットカード情報の不正利用	2016年	11年連続11回目
サポート詐欺（偽警告）による金銭被害	2020年	7年連続7回目
スマホ決済の不正利用	2020年	7年連続7回目
ネット上の誹謗・中傷・デマ	2016年	11年連続11回目
フィッシングによる個人情報等の詐取	2019年	8年連続8回目
不正アプリによるスマートフォン利用者への被害	2016年	11年連続11回目
メールやSNS等を使った脅迫・詐欺の手口による金銭要求	2019年	8年連続8回目

出典：IPA　https://www.ipa.go.jp/security/10threats/10threats2026.html

個人には、どのような被害があるか

警察庁の「令和 6 年における組織犯罪の情勢について」および「令和 7 年の犯罪の情勢」によると、令和 7 年に報告されたフィッシングメールの数は、245.4 万件です。その結果、2024 年、2025 年の被害状況被害状況は以下の通りです。

〇インターネットバンキング不正

2024 年 4,369 件、被害額 86.9 億円、2025 年 4,677 件、被害額 102,4 億円

〇クレジットカード不正

2024 年被害額 555.0 億円、2025 年被害額 510.5 億円※2025 年度被害額は、一般社団法人日本クレジット協会ホームページより引用

〇メールや SNS 等を使った詐欺のうち SNS 型投資詐欺、ロマンス詐欺

2024 年 10,237 件、被害額は 1,272 億円、2025 年 15,142 件、被害額 1,827 億円

金銭以外の被害も軽視できません

金銭的被害も大変ですが、非財産的な損害、重大な精神的なダメージを受けることがあります。例えば、DDoS（ディードス）攻撃などを受けて犯人からウイルス感染させられ、パソコン等を遠隔操作され、保有していたデータや映像や写真情報などを奪われ、世間に公開されるリスクがあります。遠隔操作される場合は、ターゲットに攻撃を仕掛ける手伝いをさせられることがあります。犯人が直接ターゲットを攻撃すると、自分の IP アドレス（ネット上の住所）から足がついてしまいます。そこで、犯人は誰かのデバイスを経由して攻撃を行うことで、捜査の手が自分以外に向くように細工するのです。そうなると、あなたが加害者扱いされてしまいます。

また、メールアカウントやサーバーが乗っ取られ、大量のフィッシングメールやスパムメールを世界中にばらまく拠点として使われてしまうことも考えられます。そうなると、あなたのメールアドレスがブラックリストに登録され、大切なメールが届かなくなったり、アカウントが停止されたりします。

どのような対策が必要か

他人に乗っ取られやすいのは、OS やソフトの更新を放置して脆弱性(セキュリティの穴)をつかれたり、パスワードが簡単すぎる場合、IoT 機器（防犯カメラ、ルーター等）の設定が初期状態のままであるなど、基本的な対策を怠っている場合です。

では、どのように対策すればよいのでしょうか。国や警察庁などが、国民を詐欺から守るための総合対策（案）などを取りまとめ、対策を進めていますが、個人としても、対策を講じて、自衛する必要があります。対策としては、大きく分けて、2 通りあります。

① パソコンやスマホでの基本対策

・OS やソフトウェア、ネットワーク機器等を最新の状態に保つこと。

作動するからといって、サポート期限が切れた OS を使い続けるのは、脆弱性を利用した攻撃を受けたり、ウイルスに感染する可能性があります。

【サポート期限が切れた主なOS】

パソコン・・・Windows8.1、Windows10、macOS 11 Big Sur、macOS 12 Monterey ChromeOSの初期のものなど

携帯電話・・・Android 11、iOS 16 以前（iPhone 8 / X 以前）

・OSを修正するアップデートは、こまめに実施すること。

（サポート期間中は、ネットワークを通じてセキュティ更新プログラムが配布され、基本的には自動的に適用される仕組みがある）

防犯カメラや室内カメラとの連携については、ファームウェアという機器を動かすためのソフトウェアは、メーカーからの更新プログラムを適宜「アップデート」する（できれば、「自動更新設定」をオンにしておく）こと。また、「外部からのアクセス許可」や「リモート管理」機能をオフにすること（設定が甘いと全世界に映像を公開しているのと同じ状態になります）。

・「画像の自動表示」をオフにすること。

フィッシングメールには、目に見えないほど小さな画像が含まれていることがあります。これを開くと「このメールアドレスは有効だ」と送信者に通知されてしまい、さらに攻撃が加速します。設定画面から「外部画像を表示する前に確認する」を有効にします。

・ウイルスソフトを必ず導入すること。

新しいウイルスに対応するため、ウイルス対策ソフト等を導入するだけでなく、パターンファイルを更新するとともに、定期的にウイルススキャンを実行することが重要です。

・なりすましメールの警告や外部送信時の宛先確認など、視覚的な注意喚起機能のあるメールサービスを採用すること。

② 個人としての対応

・メールに記載されているリンクを安易にクリックしないこと。

リンクにアクセスし、クレジットカード情報やID/パスワードなどを入力しないように気を付けること。

メール内のボタンではなく、ブラウザのブックマークや公式アプリからログインする。

・送信元アドレスのドメインを確認すること。

表示名が例えば、「Amazon」でも、アドレスがamazon-support@xyz.com など変なドメインでないか確認する。

・急かす内容のメッセージは常に疑うこと。

「24時間以内に停止します」「不正ログインがありました」といった不安を煽る言葉はフィッシングの常套手段です。

・IDとパスワードの適切な設定と管理を行うこと。

メールアドレスや特定のIDを繰り返し使用しない。取引パスワードは、各取引ごとに数字＋英文字（大小）＋特殊記号を使い、13文字以上にし、使い回ししない。

・二要素認証やパスキーを利用すること。

二要素認証を設定すれば、パスワードが盗まれても、スマホへの認証コードなどがなければログインできない。また、パスキーが使用できるときは、パスキーを利用する。

・SNSなどのプロフィールの公開は、最小限にとどめること。

一般公開をやめて、友達の範囲内など、公開対象を絞る。

“なりすまし”に注意する

最近は、AIを活用して、フィッシングメールを作成したり、著名人などになりすましてテレビ通話を通じた勧誘なども行われており、より巧妙な詐欺を仕掛けてきています。他人に相談させる時間を与えない、金銭の支払いが絡む話をする、投資による金儲けの話をするような勧誘については、家族や信頼できる第三者に相談することが必要です。

正当な金融機関・担当者であれば、家族に相談することを止めることはありません（金融機関の金融サービスについての説明義務等が定められています）。

フィッシングで銀行預金を送金されたり、クレジットカードで買い物されても、本人にカード情報などの安全管理義務違反などの過失があると判断されれば、本人負担となります。十分に注意しましょう。

現在、当研究所の「#From Red To White:)」というブログサイトに、「偽メール・偽サイトなどに騙されないために」というシリーズで、各種注意事項や対策を連載中です。個別の詳しい対策は、こちらも参考にしていただけますと幸いです。

活動状況（講師派遣）

【過去３年以内の実績】　※五十音順

【教育関係など】
神奈川県立相模田名高等学校
（株式会社 TAP 経由）
神田外語大学
潤徳女子高等学校
女子美術大学付属高等学校
学校法人中越学園中越高等学校
（アドバンスパートナー株式会社経由）
東京家政大学板橋キャンパス
東京コミュニケーションアート
専門学校
東京都立東久留米総合高等学校
（定時制・株式会社 TAP 経由）
東京都立永山高等学校
東京都立農業高等学校
東京都立雪谷高等学校
（株式会社 TAP 経由）
豊島岡女学園高等学校

【行政機関など】
労働者協同組合労協センター事業団
いたばしひとり親家庭相談窓口
佐賀県子ども家庭課
栃木県庁こども政策課
横浜市青葉区地域福祉活動拠点
「ふれあい青葉」
横浜市金沢区能見台ケアプラザ
横浜市左近山地域ケアプラザ
横浜市新栄地区ケアプラザ
横浜市菅田地域ケアプラザ
横浜市反田地域ケアプラザ
横浜市都筑区役所生活支援課
横浜市東本郷地域ケアプラザ
横浜市保土ヶ谷区 NPO 法人リロード
横浜市緑区山下地域ケアプラザ
横浜市南希望が丘地域ケアプラザ
よこはま北部ユースプラザ

【その他】
青森県消費生活センター
一般社団法人　金融財政事情研究会

ゆきちと A1（えいいち）
当法人のマスコットキャラクターです。

【講演／取材のご依頼　※リモート対応もご用意しております】
講演／取材のご依頼がございましたら、下記 URL より、お問い合わせメールに「講演／取材の問い合わせ」とご記載のうえお送りいただくか、下記ご連絡先までお問い合わせください。

【寄付のお願い】
私どもの活動にご賛同いただける方からのご寄付を随時受け付けております。
詳しくはホームページをご覧ください。

【PRTIMES 掲載】
私どもの広報活動をプレスリリースにて随時配信しております。
詳しくはホームページをご覧ください。

PRTIMES

生き抜く力　2026.3　No.18
≪編集・発行・ご連絡先≫
一般社団法人 ＮＴＳセーフティ家計総合研究所　（担当：北村）
〒108-0023　東京都港区芝浦３－１６－２０　芝浦前川ビル４階
TEL　（０３）６４５９－４７７０　FAX　（０３）３４５７－１６３０
URL：https://nts-safety.com　Mail：nts_kskn@nts-hd.co.jp