

新生活シーズン、個人情報を狙う「フィッシング詐欺」に注意

～詐欺SMSは3.2倍増、SIMスワップ詐欺やインターネットバンキング不正送金被害も～

トビラシステムズ株式会社（本社：愛知県名古屋市、以下「トビラシステムズ」）は、進学や就職、一人暮らしや引っ越しなどが増えやすい新生活シーズンの今、個人情報を狙う「フィッシング詐欺」や関連する犯罪について注意喚起を行います。当社の独自調査データとともに、手口の事例と対策をお伝えします。

■変化の多い新生活シーズン、個人情報の管理に注意

新生活シーズンとなり、進学や就職、一人暮らしや引っ越しなどが増えやすい時期です。生活環境の変化に伴い、様々な手続きや、新生活に必要な買い物なども増えやすくなります。この時期に改めて注意したいのが、個人情報の管理です。中でも、個人情報詐取の代表的な手口「**フィッシング詐欺**」は最も身近な犯罪の一つであり、日頃の対策が重要です。

【新生活シーズンに注意したい場面の例】

- ・新生活に必要な買い物をしたタイミングで、宅配事業者やEC事業者をかたるSMSが届いた
- ・引っ越し前後のタイミングで電力会社や水道局をかたるSMSが届いた
- ・クレジットカードや銀行口座を作ったタイミングで金融機関をかたるSMSが届いた
- ・一人暮らしを始め、インターネットを契約したタイミングで通信事業者をかたるSMSが届いた

フィッシング詐欺SMSの文面例

配達先にてご不在を確認し、荷物を持ち帰りました。お早めにご連絡を。[URL]

Amazon荷物の配送先住所が間違っています。クリックして住所を更新してください。[URL]

【重要】お客様の三菱UFJ銀行取引における重要な確認について。詳細はこちら:[URL]

App Storeには自動更新料金があり、購読をキャンセルします:[URL]

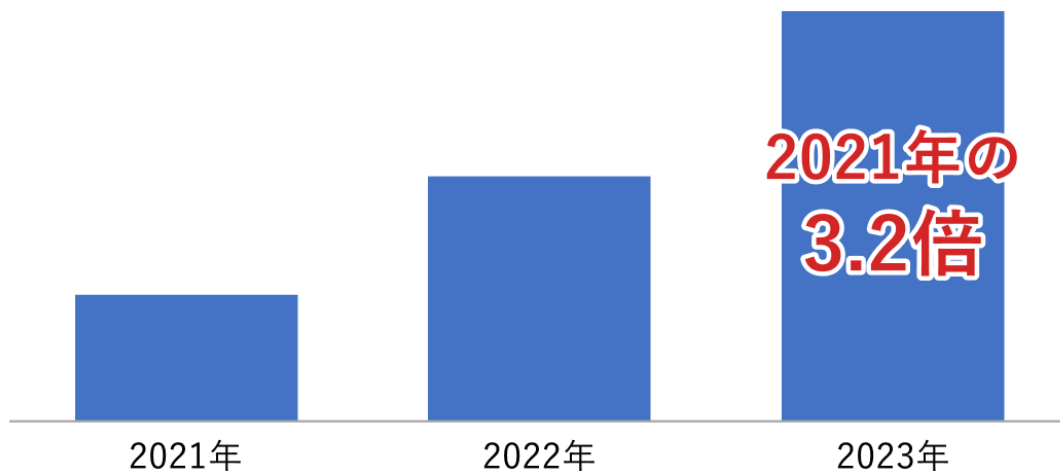
SoftBank - お読みください。重要なお知らせ。[URL]

【TEPCO】お客様ID: 471 先月の電気代が未払いのため、電力サービスを停止します。[URL]

■詐欺 SMS が増加傾向、2021 年から 3.2 倍に

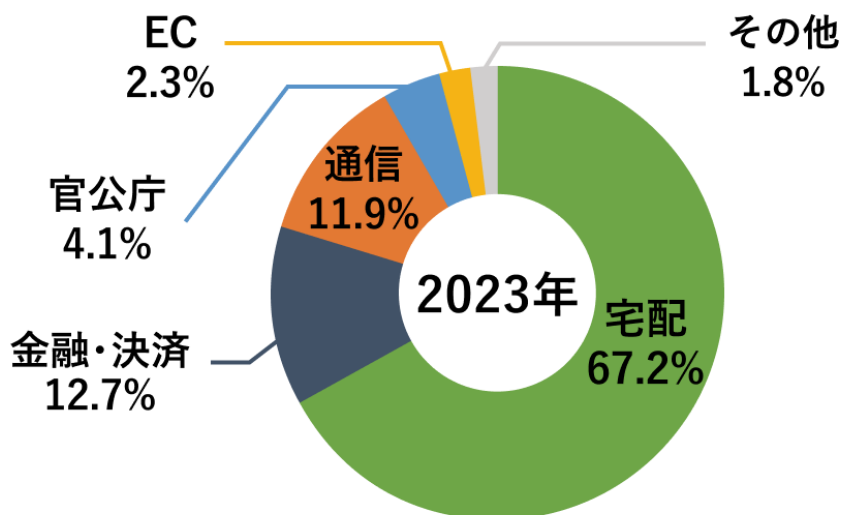
フィッシング詐欺をはじめとする詐欺 SMS が増加しています。トビラシステムズの調査で、2023 年に確認された詐欺 SMS の件数は、前年比で約 1.7 倍、**2021 年比で約 3.2 倍**に増加しています。

詐欺SMS件数推移 (トビラシステムズ調べ)



また、2023 年に最も多く確認されたフィッシング詐欺の SMS (スミッシング) の手口割合は、**1 位は宅配事業者、2 位は金融・決済サービス、3 位は通信事業者をかたる手口**となっています。いずれも生活に身近なサービスであり、特に新生活シーズンにはサービスの契約や更新、利用機会も増えやすいため、改めてご注意ください。

スミッシング手口の割合 (トビラシステムズ調べ)



■フィッシング詐欺による被害事例

フィッシング詐欺で個人情報を詐取されることにより、様々な犯罪に巻き込まれる可能性があります。フィッシング詐欺によって起こりうる被害の事例を紹介します。

○ID・パスワード、クレジットカード情報などの悪用

フィッシング詐欺では、企業やブランドを装ったフィッシングサイト（偽サイト）で個人情報の入力を促され、詐取される場合があります。

【詐取される情報の例】

- ・ID となりうる情報（アカウント名、メールアドレス、携帯電話番号、口座番号など）
- ・パスワード
- ・SMS 認証コード
- ・クレジットカード情報（カード番号、カード名義人、有効期限、セキュリティコード、3D セキュアパスワードなど）
- ・個人に関するプライベートな情報（氏名、住所、生年月日、基礎年金番号など）

フィッシングサイトの例（トビラシステムズ調べ）

The image shows two examples of phishing websites. The left screenshot is a fake Amazon login page (amazon.co.jp) with fields for 'メールアドレスまたは携帯電話番号' and 'Amazonのパスワード', a 'パスワードを表示' checkbox, and a 'ログイン' button. The right screenshot is a fake TEPCO payment page (くらしTEPCO web) with fields for 'カード名義人', 'カード番号', '有効期限', and 'セキュリティコード', and a '料金支払い' button.

個人情報を詐取されると、利用するサービスへの不正ログインやクレジットカードの不正利用などの被害を受ける可能性があります。また、詐取された個人情報が犯罪グループ間で売買され、さらに悪用される危険もあります。

○身分証明書の偽造

個人情報の詐取を目的としたフィッシングサイトの中には、ID やパスワードに加え、身分証明書の画像アップロードを求められるものもあります。

【詐取される身分証明書の例】

- ・運転免許証
- ・健康保険証
- ・マイナンバーカード
- ・パスポート

フィッシングサイトの例 (トビラシステムズ調べ)

厚生労働省
Home

個人番号カード前面：

個人番号カードを正しくアッ...

基本的な個人情報：

名前

携帯電話

個人番号

送金銀行コード

補助金を受け取るための給付金勘定...

受取申請

SAGAWA

Web再配達受付サービス

ご利用案内

本人限定受取
本人確認書類としてご利用可能なもの 2020年4月1日の「犯罪による収益の移転防止に関する法律施行規則」改正に伴い、同日から、特定事項伝達型の本人確認書類を、顔写真がはり付けられているものに限定しました。これにより、健康保険証など顔写真がはり付けられていないものは、特定事項伝達型を受け取る際の本人確認書類としてご利用できませんのでご注意ください。ご本人様を確認できる書類として、以下のアップロードください。

不在票情報

営業所番号
7151

お問い合わせ送り状No.①
3543-7634-6731

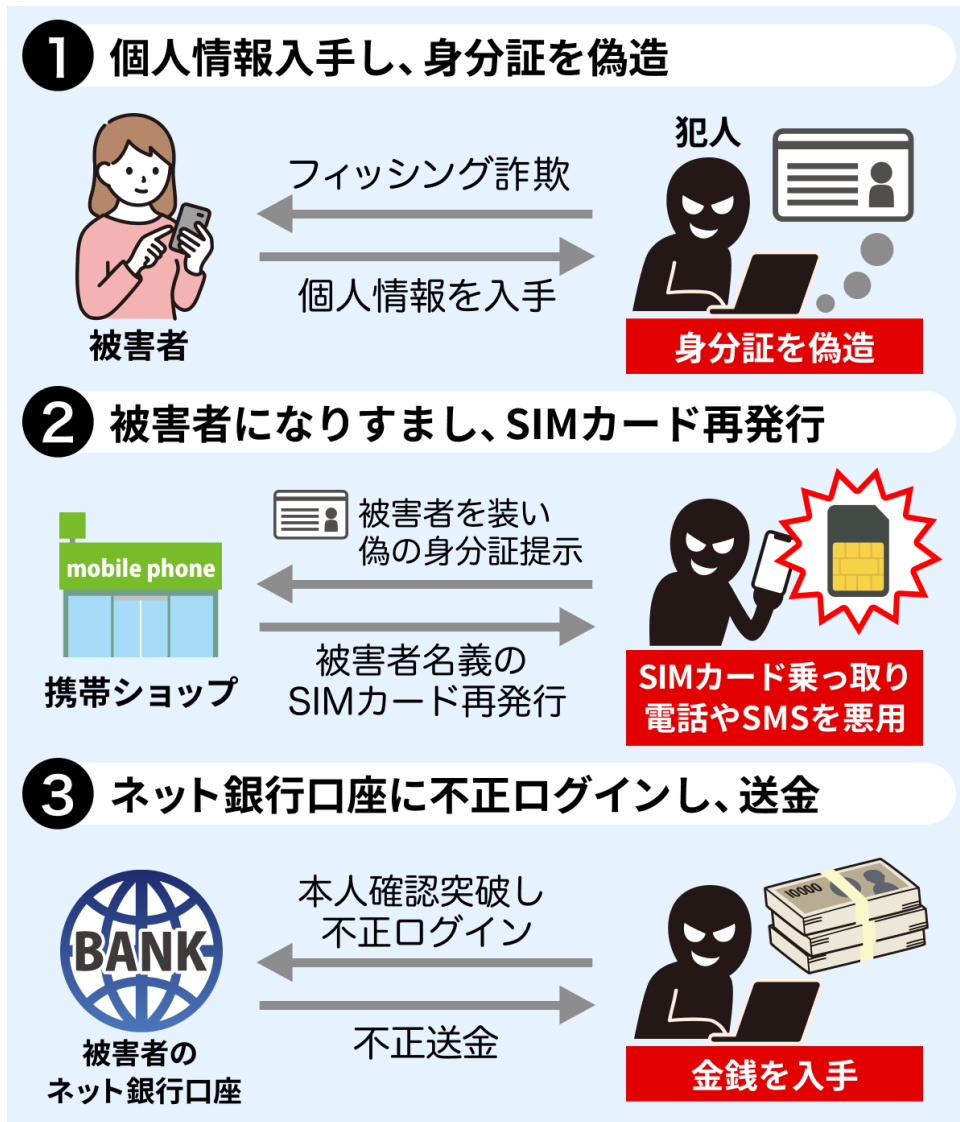
本人確認書類

・マイナンバーカード (個人番号カード) ・運転免許証 ・旅券 (パスポート)

× 送っている × 取替している × 小さい

ファイル
ファイルを選択 ファイル未選択

詐取された情報は、身分証明書の偽造に悪用される場合があります。偽造された身分証明書と、詐取された個人情報を組み合わせて悪用することで、被害者を装い携帯電話のSIMカードを再発行して電話やSMSを乗っ取る「SIMスワップ詐欺」や、犯罪グループが銀行口座を開設する際に悪用される危険があります。



(SIMスワップ詐欺のイメージ)

○インターネットバンキング不正送金被害

フィッシング詐欺で詐取された個人情報やインターネットバンキングの不正送金に悪用される可能性もあります。金融機関を装うメールやSMSからフィッシングサイトに誘導され、銀行口座の情報、インターネットバンキングのID・パスワード、ワンタイムパスワード等の入力を求められ、情報を詐取される場合があります。

警察庁の発表では、2023年におけるインターネットバンキングに係る不正送金事犯は、発生件数が5,528件、**被害総額は約86億円**で、いずれも過去最多となっています。なお、被害の多くはフィッシングによるものとみられています。

フィッシングサイトの例 (トピラスシステムズ調べ)

The image shows two examples of phishing login pages. The left page is for SMBC (三井住友銀行) and the right page is for MUFG (三菱UFJ銀行). Both pages mimic the official login screens with fields for branch/account numbers, passwords, and a login button.

SMBC (三井住友銀行) ログイン画面:

- 店番号・口座番号 (普通預金) / 契約者番号
- 店番号 / 口座番号
- ログイン暗証
- ログイン暗証とは? (ヘルプアイコン)
- ※ SMBCダイレクトの利用開始手続をされていないお客さまはキャッシュカード暗証番号を入力してください。
- ログイン暗証がお分かりにならないお客さまはこちら
- 画面が正しく表示されない場合はこちらをご確認ください。
- ログインでお困りのお客さまはこちら
- ログイン

MUFG (三菱UFJ銀行) ログイン画面:

- 店番 / 口座番号 (ヘルプアイコン)
- 半角数字3桁 / 半角数字7桁
- または
- ご契約番号 (ヘルプアイコン)
- 半角数字
- ログインパスワード (ヘルプアイコン)
- 半角英数字・記号4~16桁
- ログイン
- ? パスワードを忘れた・ロックした
- 初めて利用する

■フィッシング詐欺の対策

フィッシング詐欺の被害にあわないために、以下の対策を心がけてください。

<フィッシング詐欺の対策>

- 身に覚えのないメールやSMSが届いた場合、文面に添付されたURLに触らない
- 日頃利用するサービスは、公式アプリやブックマークしたサイトから情報を確認
- 迷惑SMS対策サービスを活用し、フィッシング詐欺などの不審なSMSを自動で遮断

詐欺 SMS の検知状況をリアルタイムに観測し可視化する「詐欺 SMS モニター」で、詐欺 SMS に関する最新情報をご確認ください。

詐欺 SMS モニター

<https://smon.tobila.com/>

■トビラシステムズについて



テクノロジーで社会課題の解決を目指し、特殊詐欺やフィッシング詐欺、グレーゾーン犯罪撲滅のためのサービスを提供しています。詐欺電話・詐欺 SMS 等の情報を収集・調査してデータベースを構築し、自動でフィルタリングする「迷惑情報フィルタサービス」は、固定電話、モバイル、ビジネス向けに展開し月間約 1,500 万人にご利用いただいています。

公式サイト：

<https://tobila.com/>

<本件に関する報道関係のお問い合わせ先>

トビラシステムズ株式会社

〒460-0003 愛知県名古屋市中区錦 2 丁目 5-12 パシフィックスクエア名古屋錦 7F

担当：管理部 広報 岩渕

TEL：050-3646-6670（直通）

FAX：052-253-7692

URL：<https://tobila.com/>