金融リテラシー講座

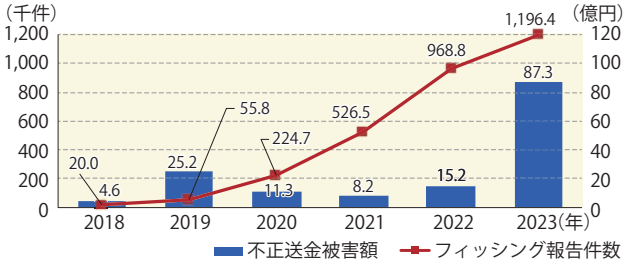
第6回 デジタル時代の金融犯罪への対抗策とは

調査研究部 総括研究員 **奥田 喜治**
（元北陸銀行システム統括部 ほくほくCSIRT担当）

1 あなたのセキュリティ対策は大丈夫?

最近は老若男女を問わずスマートフォンやパソコンを日常的に使用するようになり、フィッシング詐欺などインターネットによる金融犯罪は急増し、被害件数・金額とも過去最悪の水準に達しています（図表１）。

図表１ フィッシング報告件数・不正送金被害額の推移



出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」

まさに非常事態ともいえる状況ですが、みなさんは安全にITツールを利用できていますか。まずは以下のチェックリストで自己点検してみましょう（図表２）。

図表２ 金融犯罪リテラシー自己チェックリスト（10項目）

	A．メールに記載されたリンクを、疑わずにクリックしている。
	B．パスワードを複数のサービスで使い回している。
	C．不審なメールの添付ファイルを、相手先を確認しないまま安易に開いている。
	D．外出時などで、パスワードの入力が不要なフリーWi-Fiを利用している。
	E．ソフトウェアやシステムの更新通知を、無視している・気づかないことがよくある。
	F．取引先や社員の個人情報や重要な情報を、安易にメールやSNSで送信している。
	G．業務用パソコンやスマートフォンで、私用のSNSやショッピングサイトを頻繁に利用している。
	H．銀行やサービス提供会社を名乗る電話で、個人情報やパスワードなどの情報を伝えている。
	I．利用しているパソコンやスマートフォンに、セキュリティソフトを導入していない。
	J．金銭の支払い等の重要な取引において、相手先を十分に確認せずメールや電話による指示に従っている。

すべての項目に該当しないのが理想的ですが、「ついうっかり」というケースはありそうです。チェック数による危険度は次のとおりですが、いかがでしたか。

０～２項目	３～５項目	６～10項目
安　全	要 注 意	危　険

特に、**チェック項目Ａ・Ｂ・Ｃ・Ｅ・Ｊに該当する場合は、金融犯罪の被害を受ける可能性が非常に高い**と認識してください。

一般的に、犯罪者は被害者と比べて圧倒的に有利な立場にあると言われます。それは、犯罪者は相手の弱点を一つでも見つければ目的を達成でき、十分な時間をかけて入念に準備を行うことができるからです。

「彼を知り己を知れば百戦あやうからず」といいますが、本項では自らの状況を把握していただきましたので、次項では気をつけていただきたい金融犯罪を、チェックリストの項目とあわせて確認しましょう。

2 注意が必要な金融犯罪の手口

(1) フィッシング詐欺（図表３）

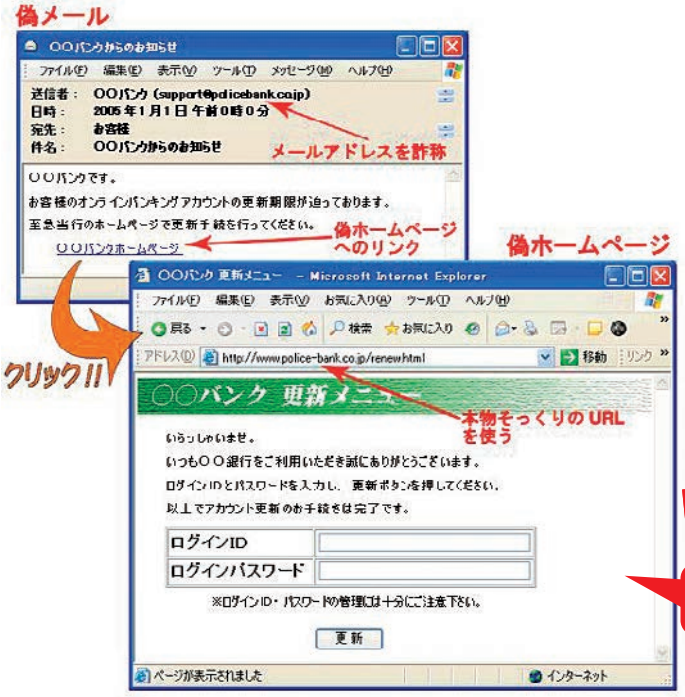
チェックリスト該当項目：Ａ・Ｃ

フィッシング詐欺は、金融機関など実在する組織を騙るメールを送りつけ、貼り付けたリンクをクリックさせて偽のホームページに誘導することで、クレジットカード番号やアカウント情報（ユーザIDやパスワードなど）の重要な情報を盗み出し、金銭等を窃取する詐欺のことです。

さらに、ショートメッセージ（SMS）により誘導するスミッシング（図表４）や、QRコードを悪用するクイッシングを含め、手口は複雑かつ巧妙化しています。

特に最近は生成AIを活用してメール文面の精度を高

図表３　メールによるフィッシングのイメージ図



出典：富山県警察ホームページ

図表４　典型的なスミッシング（SMS）

めており、油断していると正当なメールとの判別が困難になっています。犯罪者側の技術の向上により、フィッシングの被害が増えているのが実情なのです。

次のようなメール等を受信した場合はフィッシングを疑い、個人情報や認証情報等の重要な情報を絶対に入力しないでください。

- メールの件名や本文に【緊急】【重要】等の表記があり、恐怖心や緊張感を煽り、クリックを促す。
- 見知らぬ相手から、リンクへのクリックや添付ファイルの開封を求められる。
- 官公庁、銀行やカード会社等を騙り、パスワードやクレジットカード番号等の入力を要求する。

（2）SNS型投資詐欺（図表５）

チェックリスト該当項目：A・B・F・G・J

投資詐欺は古典的な詐欺手法ですが、スマートフォンの普及に伴いSNS型投資詐欺が急増しており、2023年には被害額が約278億円に達しました。

被害者の約７割は男女とも50代以上の比較的余裕がある世代であり、その手口が非常に巧妙なため、１件あたりの被害額が1000万円を超えるなど、被害が高額になるケースも多いのが特徴です。

SNS型投資詐欺は、著名人やインフルエンサーのアカウントを偽装して高収益な投資案件をSNSで勧誘したり、投資アプリやプラットフォームへ誘導するなどして金銭を窃取する手法が主流です。

SNSやメールにて投資勧誘を受けた際、次の事項に関し少しでも違和感がある場合は、お金を振り込む前に、迷わず手を止めて警察等に相談してください。

- 投資先が実在しているか、国の登録業者かどうか。
- 「必ずもうかる」「あなただけ」等の文言に注意。
- 投資を勧める「著名人」がなりすましでないか。
- 投資に関係する暗号資産やアプリ等が実在するか。
- 振込先の口座に不審な点がないか。

図表５　SNS型投資詐欺の画面イメージ

出典：警察庁ホームページ

（3）カード情報や個人情報を悪用する犯罪

チェックリスト該当項目：A・B・C・D・H

サブスクリプションの定着等に伴い、カード情報をインターネットに入力することへの抵抗感が薄らいできました。その結果、以下の手口などで、カード情報等の重要情報を詐取される被害が続出しています。

●事例A【フリーWi-Fi利用による情報盗用】

カフェでフリーWi-Fiを利用中にネットショッピングをしたところ、通信が暗号化されておらず、通信内容を傍受した犯罪者がカード情報を入手。その後、クレジットカードが不正利用されて多額の被害を受けた。

●事例B【偽の通知と気付かず情報を登録】

クレジットカード会社を装った偽のポイント還元キャンペーンの案内メールを受け取り、メール内のリンクからログインし、カード番号やセキュリティコードを入力したところ不正利用されてしまった。

この犯罪の特徴は、多様な手口で日常生活に入り込み、本人が犯罪を認識しないまま金銭などを詐取されてしまうことです。**人間の不注意や知識の乏しさという隙を突く手法ですので、注意が必要です。**被害にあわない、または被害に早く気付くために、以下の点を日頃からこころがけましょう。

- 正規のカード会社は、カード番号や暗証番号、セキュリティコードを直接尋ねることはないので、怪しい要求には応じない。
- ネットショッピング時には、信頼できるサイトであることを確認する。（URLの「https://」と公式マークの有無をチェック）
- 毎月のカード利用明細を確認し、不審な取引があれば迅速にカード会社に連絡する。

Sがあることが重要！

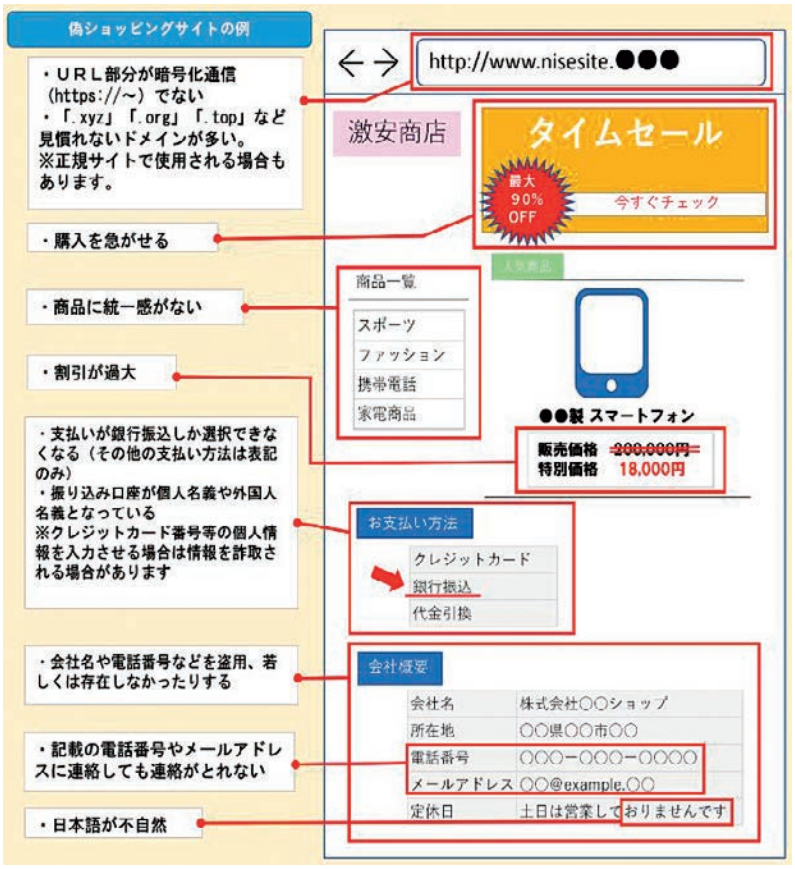
（4）ショッピング詐欺（図表６）

チェックリスト該当項目：A・D・E・G・J

インターネットショッピング等による詐欺を目的とした偽ウェブサイトを構築し、商品の注文・代金の振込を受けたうえで、商品を発送しない・偽物の商品を発送するなどのショッピング詐欺も急増しています。

また、**本物そっくりなコピーサイトを「見たことがある有名サイトだから大丈夫」という先入観から、怪しいと感じていながら入金し、被害に遭うケースも多発しています。**

図表６　ショッピング詐欺の特徴



出典：警察庁ホームページ

次の点に該当する場合は、いったんショッピングの操作を止めて、公式サイトを確認するまたは消費生活相談センターや警察等に相談しましょう。

- 正規ショップの価格よりも極端に安い。
- 販売会社の連絡先の記載がない。
- 日本語に違和感がある、なんとなく不自然だ。
- 支払方法が先払いかつ銀行振込のみ。
- 「品薄」等の表示により商品の購入を急がせる。

（5）サポート詐欺

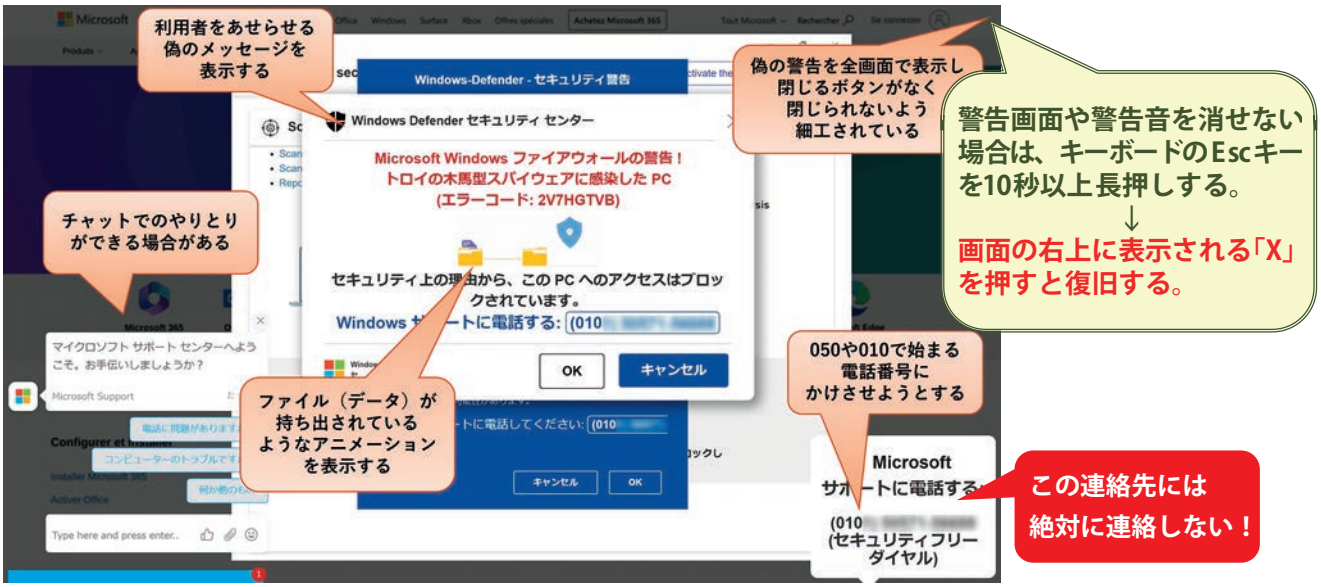
チェックリスト該当項目：A・C・G・H・J

みなさんはパソコンでのインターネット閲覧時に、突然セキュリティ警告画面や警告音が発生し、ウイルス感染等に対応するためのサポート窓口の連絡先が表示された経験はないでしょうか。

これはサポート詐欺の典型的な手口です。不安に駆られたユーザーは表示されている連絡先に電話し、通話先のサポート担当者から言われるままに操作することで、犯罪者からパソコンにウイルスを仕込まれ、金銭や個人情報を騙し取られます。

サポート詐欺では、犯罪者から少額のサポート費用をインターネットバンキングで支払うよう指示され、

図表７　サポート詐欺の画面イメージ



出典：IPA「偽セキュリティ警告（サポート詐欺）対策特集ページ」

自らは正確な金額を入力したにもかかわらず、遠隔操作により金額を改ざんされる（1,500円⇒150,000円など）ケースも増えています。

なおサポート詐欺の被害は、個人だけではなく企業でも急増していますので注意が必要です（特に企業のケースでは被害額が多額となることが多い）。

警告画面が表示されただけの段階（図表７）であれば、実際にはパソコンがウイルスに感染している可能性は低いので、慌てずに以下の対応をとりましょう。

- 表示されているサポート窓口には連絡しない。
- 【Esc】キーを10秒程度長押した後、画面右上に表示される「X」を押すと警告画面は消える。

またIPA（独立行政法人情報処理推進機構）がサポート詐欺の疑似画面を体験できるサイトを開設しているので、慣れるために閲覧されることをお勧めします。

●IPA・偽セキュリティ警告画面の閉じ方体験サイト

https://www.ipa.go.jp/security/anshin/measures/fakealert.html

3　デジタル時代の金融犯罪への対抗策

インターネット経由の金融犯罪は多岐にわたりますが、基本的な対策は概ね共通しています。以下の事項が実践できているか、あらためて確認してみましょう。

①パスワードの適切な運用
- パスワードを初期設定のままにしない。
- 推測されにくいパスワードを設定する。
  （「123456」「password」「123123」等は危険！）
- パスワードを使い回さない。
- パスキーや生体認証、多要素認証を利用する。
- パスワードを他人に教えない。

②情報リテラシー・モラルの向上
- SNS等に掲載されている情報を鵜呑みにしない。
- フリーWi-Fi利用時に、カード情報や個人情報等の重要な情報を入力しない。
- ソフトウェア等の更新通知は面倒でも確認し、セキュリティに必要な対応をとる。
- 本物を騙った偽の Web サイトや、個人情報を盗もうとするサイトがあることを知る。

③安易なファイル開封・サポート窓口への連絡はしない
- メール/SMS/SNSにおいて、安易にリンクやQRコードを開けたり、画面のボタンに不用意に触れない。
- 送付された添付ファイルをむやみに開けない。
- 案内として記載された電話番号には直接連絡しない。

④適切な報告・連絡・相談
- 金銭詐取の恐れがある場合、取引金融機関やカード会社および警察へただちに連絡する。
- 不審に感じた場合は自己判断で操作せず、デジタルに詳しい人や警察に相談する。

単独で高度な技術面での対策をとるのは困難ですが、安全性を過信せず、日常的に注意を払うことで大半の犯罪は回避できます。また、知人・企業内・警察等の外部の関係者と連携することで、平時・緊急時のトラブルにも落ち着いて対応できるでしょう。

プライベート・職場を問わず安全のための対策を実践し、周囲にもその意識をぜひ広めてください。

次回の金融リテラシー講座では、「キャッシュレス決済と利用のコツ」についてお伝えする予定です。