特集

中小企業を狙う新たなサイバー犯罪 急増するボイスフィッシングの実態と対策

警察庁サイバー警察局

Webでは+αの情報も読むことができます
ユーザ協会　D10062

インターネットバンキングに係る不正送金など、サイバー犯罪が増加しています。特に昨年は中小企業を標的にしたボイスフィッシングによる被害が顕著であり、今後も発生する可能性があるため早急な対策が求められています。そこで今回は、被害防止のため金融機関や関係団体、一般利用者などに対策情報を発信する警察庁サイバー警察局の根本 農史氏に、ボイスフィッシングを中心としたサイバー犯罪の動向と、実践的な対策法などについてうかがいました。

サイバー企画官
警視正
根本 農史氏

ボイスフィッシングによる企業への攻撃が増加中

2025年中のインターネットバンキングに係る不正送金（以下、不正送金）事犯の発生件数は4,747件で、被害額は過去最高の約104億円に達しました。中でも、銀行を装った電話と偽メールを組み合わせてフィッシング※1を仕かけ、法人口座から資金を不正に送金させる「ボイスフィッシング」による被害が深刻化しています。

「昨年の法人口座を狙った不正送金事犯発生件数は189件です。不正送金事犯全体（4,747件）の約4%に過ぎませんが、被害額は約47億円と、全体の45%超にも上ります。また、その大半がボイスフィッシングによる被害（143件、約45億円）です。ボイスフィッシングは2024年秋頃から目立ち始め、2025年3月には単月で約15億円の被害が発生しています。同年5月から10月までは、金融庁や全国銀行協会などと連携した注意喚起により一定の抑制が見られましたが、11月に再び大規模な被害が発生しています（図1参照）。また、1件当たりの平均被害額は単純計算で3,000万円超となります」（根本氏）

ボイスフィッシングの最大の特徴は、1件当たりの被害額の大きさです。法人口座では、1日当たりの送金限度額が高額であるケースも多く、残高がそのまま不正に送金されてしまうリスクがあります。中には、1社で4億円を超える被害に至った事例も報告されています。

ボイスフィッシングにみる巧妙な詐欺の手口

ボイスフィッシングは、銀行を装った電話から始まります（自動音声の場合もあります）。「顧客情報の更新が必要」「電子証明書の期限が切れるため更新が必要」などと不安をあおり、対応用のURLを送付するためとして担当者のメールアドレスを聞き出します。犯人はその場でフィッシングメールを送り、記載したURLから偽サイトへ誘導し、インターネットバンキングのIDやパスワードなどの情報を入力させます。犯人は入力確認と同時に口座へ不正アクセスし、自らの口座へ資金を不正に送金します（図2参照）。

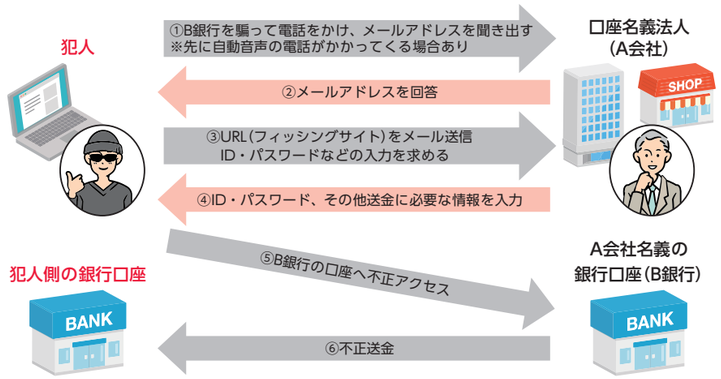
電話を切った時点で送金はすでに完了しているケースもあり、被害者側が打つ手はほとんどありません。銀行からの連絡で初めて被害に気づくケースも少なくないといいます。では、なぜこうした手口にだまされてしまうのでしょうか。ボイスフィッシングには、いくつかの巧妙な罠があると根本氏は指摘します。

「経理担当者は、メインバンクを名乗る電話というだけで警戒心が薄れがちです。加えて、犯人の口調は丁寧で知識も豊富なため、信頼してしまいやすいのです。さらに『すぐに対応しないと問題が生じる』といった言葉で緊急性をあおられ、その場で指示に従ってしまいます。着信から送金完了までわずか10分程度の場合もあるなど、担当者に考える余裕を与えない巧妙なシナリオこそが、ボイスフィッシングを成立させている要因です」（根本氏）

【図1：ボイスフィッシングによる法人口座の不正送金被害件数・被害額】

出典：警察庁

【図2：法人口座における不正送金事犯の概要図】



出典：警察庁

ボイスフィッシングの三つの特徴と被害防止対策

ボイスフィッシングには一定の傾向が見られ、次の三つの特徴が見られた場合はその可能性が高いと根本氏は警告します。

「①発信元の番号が国際電話であること。②電話を受けると音声ガイダンスが流れ、その後オペレーターに切り替わること。③通話中にメールアドレスを聞き出され、URLリンク付きのメールが送られてくること。これらの特徴が一つでも見受けられると、ボイスフィッシングである可能性が高いです。このような電話を受けた場合は、いったん通話を切り、銀行へ連絡して事実関係を確認してください。また、メールに記載されたURLリンクには決してアクセスしないでください」（根本氏）

ボイスフィッシングの被害は、特に地方の中小企業で目立っています。人手不足による多忙などから、なりすましを見抜けず、指示通りに情報を入力してしまうケースが多いため、防御体制の弱さを理由に中小の事業所が狙われているようです。こうしたリスクへの対策として、最新のセキュリティ技術の導入も有効だと根本氏は指摘します。

「例えば、フィッシング耐性の高い認証方式であるパスキー※2や、メールの改ざんやなりすましを防ぐDMARC※3などを導入することで、防御力は大きく高まります。また、定期的にロールプレイを行い、攻撃を想定した対応手順を日頃から共有しておくことも重要です。また、インターネットバンキングの利用は、銀行の公式サイトや公式アプリからのみアクセスするなど、社内ルールの整備も効果的です」（根本氏）

では、万が一被害に遭ってしまった場合、企業はどのように対応すべきでしょうか。

「まずは直ちに銀行へ連絡してください。ボイスフィッシングは、不正送金後に被害が判明するケースが多く対応が難しいのですが、銀行側で送金を止められる場合もあります。また、同じパスワードをほかのサービスでも使い回している場合は、二次被害を防ぐためにも速やかに変更してください」（根本氏）

あわせて、最寄りの警察のサイバー犯罪担当部門への連絡も不可欠です。通話内容の記録や受信したフィッシングメールは削除せず、そのまま提供することで、捜査の進展につながります。

中小企業を狙うサイバー犯罪は、今後、AIの活用によってさらに高度化し、攻撃の精度や速度が一層高まると見られています。

「AIの犯罪利用はすでに始まっています。AIで作成された偽サイトや偽情報は、本物と見分けがつかないほど精巧で、被害リスクは一段と高まっています」（根本氏）

従来のフィッシングメールや偽サイトには、不自然な日本語や違和感のある表現が見られ、サイバー犯罪に詳しくない担当者でも見抜けるケースが少なくありませんでした。しかし、AIによって生成されたコンテンツは日本語も自然で、真贋（しんがん）の見極めはますます難しくなっています。

警察庁ウェブサイトのサイバー警察局のページ（下記URL）では個別事案への対策やサイバー空間をめぐる脅威の情勢などを掲載し、サイバー犯罪の手口や対策について紹介しているほか、啓発資料として活用できる「サイバー警察局便り」を公開しています。企業を守る対策の第一歩として、活用を検討してみてはいかがでしょうか。

※1 フィッシング：送信者を詐称したメールやSMSを送りつけ、貼り付けたURLリンクをクリックさせて偽のサイトに誘導することで、重要な情報を抜き出すこと。フィッシング目的のメールをフィッシングメール、サイトをフィッシングサイトという。
※2 パスキー：指紋認証や顔認証に代表される生体情報や、スマホなどのデバイス自体を鍵として認証に使用するもの。
※3 DMARC：メールの送信元が詐称されていないか、正規のサーバーから送られているものかを確認する送信ドメイン認証技術の一つ。

●概要
法人名：警察庁サイバー警察局
設立：2022年（令和4年）
所在地：東京都千代田区霞が関2-1-2
所掌事務：官民連携、人材育成などの基盤整備、各国との情報交換、サイバー事案の捜査指導、高度な解析への技術支援など
URL：https://www.npa.go.jp/bureau/cyber/index.html

関連記事もWebで！「フィッシング」
ユーザ協会　サイバーレジリエンス