2023 年度消費者・事業者懇談会　発言要旨

テーマ：「インターネットに関する消費者トラブルについて
～フィッシング被害防止に向けて～」

日時：2023 年 11 月 15 日（水）午後１時 30 分から午後３時 30 分まで
場所：愛知県自治センター　４階　大会議室

１　開会

２　挨拶（愛知県 県民文化局 県民生活部 県民生活課長）

３　内容

（１）基調説明

①『最近のフィッシング報告状況』

（一般社団法人 JPCERT コーディネーションセンター（フィッシング対策協議会事務局））

・（一社）JPCERT コーディネーションセンターは、1995 年から活動しているコンピューターセキュリティーインシデントに対応する民間の機関で、主に経済産業省や内閣官房からの委託予算で活動している。また、サイバーセキュリティに関する事象が発生した場合に、国内外の関係者との連絡調整を行う関係機関として長年活動しており、サイバーセキュリティ基本法上の「サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関」として、政令指定法人として指定されサイバーセキュリティ協議会の事務局や、その他にもフィッシング対策協議会の事務局を担っている。

・JPCERT は、インシデントの報告窓口を設けており、2022 年４月から 2023 年３月の１年間の報告件数は昨年から増加し、フィッシングサイトの報告が 68.12%と大きな割合を占めていた。

・JPCERT は、フィッシング対策協議会が受け付けたフィッシングの報告により、フィッシングサイトの閉鎖調整やフィッシングサイトにアクセスした際に警告表示を出せるよう URL 共有を行っている。

・また、緊急情報としてフィッシング対策協議会の Web ページ等に、一般への影響度が高い場合については、フィッシングメールの文面とフィッシングサイトの画像を掲載しているほか、直近のフィッシングの傾向については月次報告書という形で、毎月公開している。その他、事業者向けや一般利用者向けにフィッシング対策ガイドラインを公表している。

・フィッシングで詐称される分野として、EC サイトや様々な種類のクレジットカード会社、銀行、ETC サービス、キャッシュレス決済、旅行サイト、マイナポイント事務局、宅配便の不在通知等がある。

・クレジットカードの不正利用額については、年々大きくなっており、また、今年は銀行を騙るフィッシングによる不正送金被害額が上半期だけで過去最多となっている。

・2020 年に消費者委員会から「フィッシング問題への取組に関する意見」として、「早急に取り組むべき事項」①フィッシングメールの受信防止対策の普及促進および効

果検証、②不正アクセス禁止法等に基づく取り締まりの強化、③消費者への注意喚起の一層の強化、④関係行政機関の連携強化が対策を所管する、警察庁、総務省、経済産業省、消費者庁に対して示された。

・フィッシング対策協議会が対象としているフィッシングとは、実在する組織を騙って、ユーザーネーム、パスワード、アカウント ID 、ATM の暗証番号、クレジットカード番号といった個人情報を詐取する行為であり、不正アクセス禁止法上における「フィッシング行為」を指す。

・フィッシング詐欺は、基本的に犯罪者が不正契約を通してメールのインフラや、フィッシングサイトを作った上で、偽のメールを送り、偽メールを受信した方が、メールのリンクをクリック、もしくはタップしてしまうことでフィッシングサイトに誘導されて、そこで情報を搾取される流れとなる。

・フィッシングの例として、同一文面でブランド名と署名欄だけ変更したフィッシングメールの大量配信、URL に飾り文字などが含まれたフィッシングメール、URL の偽装等がある。

・消費者へのアドバイスとして、フィッシングメールやフィッシングサイトは、本物のメールやサイトをそのままコピーして、見た目は分からないことが多いので、焦らせる内容でも慌てずに、そのメールやショートメッセージの文面から直接アクセスせず、スマートフォンであれば、普段使っているアプリもしくは、ブラウザの場合は正しいサイトをブックマーク、お気に入りに登録してそこからアクセスする。

・カード情報、口座情報、暗証番号、認証コード等の入力を求められたらフィッシングを疑い、一度立ち止まる。

・怪しいと思ったら「件名」や「本文」内の文字列で検索する。また、サービス提供事業者へ直接確認する。

・ID やパスワードが不正利用される際に気づけるように、多要素認証の併用等のセキュリティ機能を強化する。

・フィッシングメールは一度来始めると止まらないため、可能であればメールアドレスを変更する。また、フィッシングメールをフィルターするメールサービスを利用する。

・差出人のメールアドレスを書き換えることは簡単にできるので、例えば jpcert.or.jp というところから来たメールが本物とは限らない。そこで、なりすましメール対策とて、メールの受信側で、フィッシングメールかどうかを判断して、利用者の受信トレイに届かないようにする送信ドメイン認証技術がある。

・この技術を活用するためには、受信側のメールサーバーが対応し、正規のドメインを持っている事業者が、送信者側のサーバーへ必要な情報を公開、検証する必要があるため、登場人物がそれぞれ対応できるよう、この技術の普及啓発を行っている。

・また、BIMI と呼ばれる正規メールにブランドアイコンを表示する技術もあり、Gmail や Yahoo！メールでは、正規メールには送信ドメイン認証を利用している会社のブランドアイコンやマークが表示されるようになっている。

・経済産業省、警察庁および総務省が連名で、クレジットカード会社等に対し、送信ドメイン認証技術の導入をはじめとするフィッシング対策の強化を要請しており、現在、業界を挙げてフィッシング関する対応を進めている。

②『株式会社ジェーシービーでのフィッシング対策について』
（株式会社ジェーシービー）

・株式会社ジェーシービーは、日本で唯一の国際クレジットカードブランドを運営する企業で、ブランド事業、加盟店事業、カード事業の大きく３つを行っている。
・今回話をするフィッシング対策については、国際ブランドの JCB としてではなく、株式会社ジェーシービー自社の範囲で行っている対策となるのであらかじめ御承知いただきたい。
・フィッシングの事例として、旧 Twitter の偽アカウントを使って JCB の偽キャンペーンを展開し、そこにアクセスするとカード番号を入力させるといった、ソーシャルメディアフィッシング、弊社の MyJCB と言われるポータルサイトの偽サイト、JCB を騙るフィッシングメール等がある。
・偽サイトは正規のサイトを丸々複製しているので、本物と見分けがつかない。また、URL を確認するように言われるが、そもそも何が正しい URL なのか消費者は分かっていないため難しい。
・最近検知した事例では、リアルタイムフィッシングと呼ばれるものがあり、ワンタイムパスワードの入力を求める Web サイトが増え、ログイン ID、パスワードの窃取のみでは不正ログインが出来なくなった事から、不正犯はフィッシングサイトに入力された情報をリアルタイムでモニターし、ログイン ID、パスワードに加え、ワンタイムパスワードを窃取してくることもある。
・弊社のフィッシング対策として、①送信ドメイン認証によるフィッシングメール対策、②フィッシングサイトの閉塞処理によるフィッシングサイト対策、③利用者への注意喚起を行っている。
・これら対策により、今年の JCB のフィッシングサイトの検知件数は、昨年と比較して大幅に減っている。
・実際に万が一、不審メールの中の偽サイトに暗証番号等を入力してしまった際は、第三者によるカード不正の利用の恐れがあるため、基本的には、紛失と同じ扱いで連絡してほしい。
・弊社の方で、カードの利用停止、不正利用が確認できた際にはカードの差し替え、実際に利用覚えがないものについては、請求せず決済自体を止めるといった対応を行っている。
・弊社の決済内容については、24 時間 365 日モニタリングをしており、いつもと違う利用の仕方、いつも違う場所の決済、深夜帯の決済、いつもより高額の決済等、いつもと違う決済事項が行われると、怪しい決済として一旦止め、ヒアリングを行った上で決済する等の対応をしている。
・また、利用者には、明細を毎月見ていただき、利用覚えのない明細があったときには連絡してほしい。弊社は全てチェックしており、状況を確認し、利用覚えなしとして決済事項を取り消しする等の対応も行っている。

（２）情報提供（愛知県 県民文化局 県民生活部 県民生活課）

ア　愛知県消費生活モニターアンケートの結果について

年に一度、愛知県消費生活モニターを対象にアンケートを実施しており、今年度は「なりすましメールや SMS によるフィッシング」をメインテーマに実施したので、そ

の結果を抜粋して紹介する。

（「フィッシングの認知度について」、「なりすましメールやSMSの受信状況について」、「なりすましメールやSMSへの対応について」等について結果を紹介。そのほか、アンケート結果の詳細は以下を参照。
【 https://www.pref.aichi.jp/soshiki/kenminseikatsu/monitor-en5.html 】）

イ　愛知県の消費生活相談の概要について

・2022年度に愛知県及び市町村の消費生活センター等に寄せられた消費生活相談は44,002件で、前年度に比べ1,591件（3.8%）増加した。2023年度直近６か月（４～９月）では21,594件で、前年同期に比べ727件（3.3%）減少した。直近６か月の相談で最も多かったのは、身に覚えのない架空請求などの「商品一般」に関するもので、次いで「化粧品」と続き、「賃貸アパート」、「健康食品」、「工事・建築」の順となっている。

・「フィッシング」に関する消費生活相談は、2022年度は627件で、前年度に比べ161件（34.5%）増加した。2023年度直近６か月（４～９月）については、310件と、前年同期に比べ、20件（6.1%）減少しているものの、ほぼ横ばいの件数で推移している。相談の主な内容としては、「通販サイトを騙るメールやSMSが、スマートフォンに届いた。記載されているURLにアクセスし、クレジットカード番号等を入力したあとに、身に覚えのない請求がきた。」などといった「販売方法」、「契約・解約」に関する相談や、「不在のため荷物を持ち帰ったとのメールが届いた。」、「クレジットカード会社から、不正利用が確認されたとメールが来ている。」などの「表示・広告」に関する相談、「携帯電話会社から『ご利用料金についてお知らせしたい』とのSMSが届いたので連絡したら、未払い料金があると言われた。」などといった「価格・料金」に関する相談が寄せられている。

・偽 SMS、メールにおいて騙られる事業者等は、通販サイトやフリマサイト、クレジットカード会社や金融機関、宅配便事業者、携帯電話会社、公共機関が多い。

（３）意見交換

① なりすましメールやSMSによるフィッシングについて疑問な点、不安な点について
② フィッシング被害防止に向けて必要な取組について
③ その他（業界や行政への質問、意見）

〇消費者

・フィッシングの可能性を感じた場合の真偽の見分け方について極めて難しいこと、また悪用されないように、知識をつけて自ら身を守らなければならないということが良く分かった。そのうえで、個人情報に係る漏えい原因について、さらに詳しく伺いたい。

・フィッシング行為に対するペナルティーの強化、あるいは消費者に対する関連社会教育の充実についてアドバイスがあればお願いしたい。

・インターネットバンキングやショッピングサイトを個人的にも利用する機会が多いので、フィッシングによる被害の実例、それに対する効果的な対策を教えてほしい。

〇消費者

・私もフィッシング等の迷惑メールが大量に送られてくるが、真偽を見分けるには電話で直接担当に確認する方法が有効だと思う。また、メールではなく郵便物は信用ができると思う。
・フィッシングの相手方の特定は、かなり難しいと思う。海外を経由すると犯罪をやりやすく、逆に検挙しづらいという現状があると思う。
・広報については、ｅラーニングという方法もあるが、被害に遭われる方は、高齢者が多いため、テレビが有効だと思う。愛知県の広報番組等で取り上げることも必要だと思う。

〇消費者

・私は、消費者関係の啓発ボランティアをしており、高齢者の方に勉強会等へ参加を呼び掛けているが、そんなことは既に知っていると、なかなか参加してくれない。どのようにすれば参加してくれるか悩んでいる。
・また、啓発する時に一番困るのは、参加者にできるだけ分かりやすく事例紹介をしたいけれど、新聞や警察も、あまり詳しい情報は教えてもらえない。新聞に書いてある程度の内容は、みんな知っていると言われてしまう。そのため、啓発活動として何をやったらいいか非常に悩んでいる。
・仮想通貨問題についても、近隣の都府県で被害の報告があり、愛知県では被害が報じられていないようだが実際はどうか。

〇消費者

・迷惑メールがよく来るが、迷惑メールか判断できるようアイコンがつく場合があると聞き、昔に比べると判断が楽になってきて少し安心をした。
・宅配便の SMS については、文面だけでは判断がつかないことがあり、対応に困っている。
・今日は、企業や県のフィッシングに対する取組について伺ったが、国の取組についても伺いたい。

＜個人情報の漏えい原因について＞

〇一般社団法人 JPCERT コーディネーションセンター（フィッシング対策協議会事務局）

・個人情報の漏えい原因として、そのデータを持っている事業者が不正アクセスを受けて情報を盗み取られるケース、内部犯行として事業者の社員等がデータを持ち出すケース、消費者がアンケートサイト等でメールアドレスを登録し、そのサイトの管理が脆弱で流出するケース等が考えられる。
・メールアドレスを入力して、そのメールアドレスがリークされているかどうかをチェックできるサイトもあるので、自分のメールアドレスが大きい流出の中に含まれていないかを確認するのも一つの手段だと思う。

＜フィッシングによる被害の実例と効果的な対策について＞

〇一般社団法人 JPCERT コーディネーションセンター（フィッシング対策協議会事務局）

・フィッシングメールは、一度受信するようになった場合、メールアドレスは犯罪者がリストとして持っているので何度でも送られる。送信ドメイン認証技術はあるが、全てを排除することは出来ない。BIMI と呼ばれる仕組みにより正規メールにはブランドアイコンを付けることができるので消費者はこれを確認してほしい。

〇株式会社ジェーシービー

・インターネットバンキングやネットショッピングは、専用アプリがあれば、専用アプリを使い、決済の明細は常に確認してほしい。
・迷惑メールに対しては、フィルタリングし、仕分けをしてくれるアプリやサービスがあるため、利用するといいと思う。

〇愛知県警察本部サイバー犯罪対策課

・フィッシングによる被害として、インターネットバンキングについてのフィッシングが非常に増えており、今年は過去最高の被害額を出している。クレジットカードによる被害では、取得した ID やパスワードを使って何か購入されるが、インターネットバンキングによる被害では、預金が丸ごと移転させられてしまい、１回の送金で約 5,000 万円が架空口座に移動されたという報告もある。
・フィッシングによる被害相談を受け次第、速やかに警察庁を通して、各プロバイダーに情報提供し、赤字のポップアップを表示させて、「これは偽サイトです御注意ください」という警告画面を出すようにしている。
・電話でメールに書かれている内容を確認することは有効な手段、ただし、その時送られてきたメールに書かれている電話番号に電話をしてしまうと、犯罪者に繋がり言葉巧みに誘導して ID、パスワードを聞き出してしまう。そのため、連絡をするには別途インターネット上でブラウザを立ち上げて、その銀行の番号を検索して探すなど、何らかの別の方法で正しい電話番号を確認することが大切。
・郵便物については、すでに取引をしている銀行等からで、こちらの名前も記載されていれば、信頼がおけるものだと思う。ただし、ビラのように、ところ構わず投函されているものには、偽の住所や電話番号が書かれている場合もあるので気を付けてほしい。

＜消費者に対する関連社会教育の充実について＞

〇株式会社ジェーシービー

・フィッシングの被害にあう年齢層を調べてみると、高齢者か、意外と 20 代のような若い方が多い。若い方は、ID やパスワードを入力することが当たり前になっているので、抵抗感が少ないように思う。弊社としてもフィッシングに対する啓発を行っているが、特に高齢者や若い方へのアプローチをどうしていくか検討している。

〇愛知県県民生活課

・フィッシングを含め、消費者被害とその対処法について、学校や地域団体、事業者等の依頼に応じて、出前講座を実施している。開催する内容に応じ、県の消費生活相談員や、消費者教育コーディネーター、外部講師として弁護士等を派遣しており、消費者教育を推進している。

〇愛知県警察本部サイバー犯罪対策課

・啓発活動について、大学生のボランティアにお願いして、若い感性でフィッシングに関する動画を作成し、YouTube で公開している。高齢者に対しての啓発も検討し

ていきたい。
・被害に遭われた方に、所感を聞いて公表するということは、被害者心情を配慮して、今まであまりやってこなかったが、生の声があれば、より啓発が進むということであれば、検討していっても良いと思う。

＜フィッシング行為に対するペナルティーについて＞

〇愛知県警察本部サイバー犯罪対策課

・フィッシングサイトを、インターネット上に置くこと自体がすでに犯罪であり、またフィッシングメールを送ることそのものが犯罪であると、不正アクセス禁止法の中に明記されている。
・実際にフィッシングサイトを作った人間を検挙した事例は、全国的に見ても非常に少なく、その理由として、フィッシングサイトは多くが海外のサーバーに蔵置されており、犯人検挙のためには国際機関をとおした相手国の全面協力が必要で、非常に時間がかかるのが現状。
・これまで、出し子という末端の構成員を検挙して、そこから上に突き上げていくという捜査を行い、日本国内にいる中間管理職的な犯人を検挙した事例は多くある。
・サイバー犯罪以外の分野ではあるが、近年、インドネシア、タイ、フィリピンなどの海外に拠点を持っている犯罪者を移送して、日本で逮捕するということを順次進めており、海外にいれば、安全だという犯罪者の中での神話を崩していかなければならないと考えている。愛知県警においても、海外にいる犯罪者の検挙に向けて取り組んでいる。国際的な捜査の協力の枠組みが、今まで以上にできあがっている。

＜仮想通貨問題等、新たな手口について＞

〇愛知県警察本部サイバー犯罪対策課

・サイバー犯罪は県の境目がなく、不正アクセスによって仮想通貨が盗まれてしまったという事例は、すでに愛知県内でも発生している。
・最近増えている手口として、サポート詐欺と呼ばれるものがある。パソコンが突然赤い画面になり「あなたのパソコンがウイルスに感染しました、これを元に戻して欲しければこちらに御連絡ください」とサポートセンターの番号が表示され、電話をすると犯罪者に繋がり、言葉巧みに情報を聞き出されお金を盗まれるというもの。
・画面が赤くなってもウイルスには感染してない場合があるので、冷静に判断いただき、警察等に通報してほしい。

＜フィッシングに対する国の取組について＞

〇中部経済産業局消費経済課

・クレジット会社に対する規制として、割賦販売法という法律がある。割賦販売法では、カード会社と加盟店において、クレジットカード番号の適切な管理、不正利用の防止といったセキュリティ対策を設けることが義務化されている。
・業界のガイドラインとして、一般社団法人日本クレジット協会が、クレジットカードセキュリティガイドラインを作っており、カード番号の適切な管理及び不正利用と防止の実務上の指針としている。
・2025 年の３月までに、原則全ての EC 加盟店にワンタイムパスワード等を義務づけ

るセキュリティ規格の導入を求めることとしている。

＜全体をとおして＞

〇公益社団法人全国消費生活相談員協会中部支部

・消費生活センターに寄せられる消費者トラブルの中で、最近はフィッシング詐欺や仮想通貨詐欺が、本当に多くを占めている。
・2020 年に、消費者委員会の委員をしており、「フィッシング問題への取組に関する意見」を出した。今日の会議を通して、取り締まりについて、やれることはやっていることが分かった。しかし、消費者に対する啓発は、まだ足りていないと感じる。
・フィッシング詐欺などの相談は事後の場合が多いため、スピード感を持って対応している。クレジットカード番号を入力してしまっていれば、まず先にカード会社へ連絡するようアドバイスし、その後に内容をフィードバックしてもらい、二次被害にならないような注意喚起をしている。
・フィッシングメールは、本文に個人名が書いていない。基本的に自分が契約している銀行やカード会社は必ず名前がつくため、判断の基準にしてほしい。
・私も消費生活相談員として啓発活動を行っているが、実際は啓発活動に参加してくれる人と被害に遭ってしまう人の格差がある。
・全国銀行協会や日本クレジット協会も、消費者のための Web サイトや動画等で啓発活動を行っているが、あまり知られていない。消費者一人一人に伝えられるよう啓発活動に力を入れてほしいと思う。
・啓発活動に事例が必要であれば、国民生活センターのサイトに掲載されているため確認するとよい。また、より詳しく知りたいときは、消費生活センターへ声掛けをしてほしい。

４　まとめ（愛知県 県民文化局 県民生活部 県民生活課長）

・JPCERT コーディネーションセンター様から、消費者が出来る対策についてアドバイスいただき、フィッシングメールが届いた時は、焦らず冷静に対応してほしい。
・全国消費生活相談員協会中部支部様の話にあったように、フィッシング被害について、不安に思った場合やトラブルが生じた場合は、すぐに最寄りの消費生活センター等へ相談してほしい。
・㈱ジェーシービー様の話から、フィッシング被害を減らすべく日々御努力されていることがよく理解できた。引き続き、関係各所と連携してフィッシング被害防止に向けた取組を続けていただきたい。
・県としても、消費者への情報提供や啓発を引き続き行うとともに、本日の懇談会で皆様からいただいた御意見や情報を、今後の消費者行政に役立てていきたい。

５　閉会