第72回（平成30年８月24日）

○的井総務課長　大変お待たせいたしました。定刻となりましたので、会議を始めます。

本日は、加藤委員が御欠席です。

それでは、以後の委員会会議の進行につきましては、堀部委員長にお願いいたします。

○堀部委員長　ただいまから、第72回個人情報保護委員会を開会いたします。

議題１、個人を狙ったサイバー攻撃に対する注意喚起について、事務局から説明をお願いいたします。

○事務局　それでは、議題１、個人を狙ったサイバー攻撃に対する注意喚起について、説明させていただきます。

昨今、不正アクセスによる個人情報の流出が増えており、クレジットカード情報の不正利用等の被害が増加している現状において、事業者のみならず個人から直接個人情報が流出しているケースも数多く存在していることから、委員会として個人に対しても注意喚起を行うものです。

まず、不正アクセスによる個人情報の流出状況について説明させていただきます。

当委員会に報告のあった不正アクセスによる個人データの漏えい等事案の報告ですが、件数、人数ともに増加傾向にあります。また、不正アクセスによる個人データの流出については、誤送付や紛失等、他の要因と違い二次被害につながる可能性が高いことが特徴です。二次被害の代表例として、クレジットカード情報の不正利用が挙げられますが、クレジットカード協会の公表資料によりますと、クレジットカード情報の不正利用額は年々増えているとのことです。

委員会としましては、事業者に対する不正アクセスにより個人データの漏えいが判明した際には、ヒアリングや場合によっては立入検査を行い、事実関係の詳細を確認の上、適切な対応を促すとともに、適切な再発防止策の策定、実施を確認しています。

その一方で、委員会に報告がない部分で、個人が直接サイバー攻撃を受け、不正に個人情報を取得されているケースがあることが分かっています。個人を狙ったサイバー攻撃といえば、フィッシングやマルウェアが代表的であり、いずれも昔からある攻撃ではありますが、時代の進化とともに攻撃方法が多様化してきています。詳しくは後ほど説明いたしますが、例えばバンキングトロージャンと呼ばれるマルウェアは、その名のとおりインターネットバンキングをターゲットとしていました。しかし、最近ではクレジットカード会社のサイトを狙うケースが増えています。また、スマートフォンの普及に伴い、スミッシングと呼ばれるスマートフォンを対象としたフィッシングも増えています。さらに、ダークウェブ等が出現し、一度流出した個人情報や攻撃方法が流通することで、個人情報の流出が新たな個人情報の流出を生むというサイクルができているという状況があります。

個人情報の流出のサイクルについてですが、第一段階として、攻撃者は、個人に対してはフィッシングやマルウェアによって、事業者に対してはＳＱＬインジェクションなどの不正アクセスによって、ＩＤ、パスワード、メールアドレス、クレジットカード情報等を

不正に取得します。この段階では攻撃者には何のメリットもないため、攻撃は次の段階に移行します。

次の段階として、個人に対しては事業者から不正に取得したメールアドレスを使って新たなフィッシング等を仕掛ける一方で、事業者に対してはクレジットカード情報の不正利用やポイントの不正利用という形で金銭的な利益を得ます。また、ダークウェブ等を通じて、不正に取得した個人情報を売却するといった形で利益を得ることもあります。

この二段階で一連の攻撃となりますが、結果としてダークウェブ等では個人情報や攻撃方法が流通することとなり、そこにある個人情報や攻撃方法を購入、閲覧した者が新たな攻撃者となります。新たな攻撃者は、不正に取得した個人情報を使い、先ほどの攻撃と同様、更なる個人情報の不正取得や、クレジットカード情報の不正取得を行います。その結果、個人情報流出のサイクルが拡大していくことになります。

この状況を踏まえ、個人や事業者から流出した個人情報の流出のサイクルを食い止めるためには、これまでどおり事業者に対し適切な指導を行っていく一方で、個人に対しても注意喚起を行っていく必要があります。そのため、今回個人に対する注意喚起として、「個人を狙ったサイバー攻撃に関する留意事項」という文書を起案いたしました。

資料１「個人を狙ったサイバー攻撃に関する留意事項」をご覧ください。

委員会としましては、事業者に対する不正アクセスにより個人データの漏えいが判明した際には、ヒアリングや場合によっては立入検査を行い、事実関係の詳細を確認の上、適切な対応を促すとともに、適切な再発防止策の策定、実施を確認しています。その一方、委員会に報告がない部分で、個人が直接サイバー攻撃を受け、不正に個人情報を取得されているケースがあり、注意が必要ですという導入になっております。

「１．個人を狙ったサイバー攻撃の例」として、最近増加していると報道されているマルウェアの代表例としてバンキングトロージャン、フィッシングの代表例としてスミッシングを挙げました。

まずバンキングトロージャンですが、感染すると、正規サイトにアクセスした利用者のパソコンに「にせ画面」を表示させ、クレジットカード情報等の個人情報を収集します。名前のとおり、もともとはインターネットバンキングがターゲットにされていましたが、最近ではクレジットカード会社のサイトが狙われるようになっております。

次のページをご覧ください。

スミッシングとは、事業者を装った攻撃者からショートメッセージがスマートフォンに送られ、メール本文中のＵＲＬにアクセスすると、事業者の公式サイトに酷似した「にせサイト」が表示され、スマートフォン用アプリをインストールすると、スマートフォンの個人情報が抜き取られるものです。

続いて、「２．個人情報を不正に取得された場合の影響」、その次のページには「３．対策」を記載しております。

対策については、これまでさんざん言われておりますとおり、不審なメールの添付ファ

イルを開かないであるとか、不審なＵＲＬのリンク先へアクセスしない、ということしかないのですが、このように攻撃方法を具体的に図示し、身近に感じてもらうことで注意喚起を図れればと考えております。

また、個人に対するサイバー攻撃については、対策を講じていたつもりでも、実際に被害に遭わないと気がつかないという問題点があります。そのため、日頃からクレジットカードの利用明細を確認し、不正利用が疑われるようであれば、できるだけ早くクレジットカード会社へ連絡するよう促すという注意喚起も記載しております。

最後に、４として、関連情報が掲載されているページのリンクを貼っています。

サイバー攻撃がますます多様化、高度化している状況において、専門機関との連携は必要不可欠ということで、１つ目はＪＰＣＥＲＴが事務局を務め、フィッシング対策情報が掲載されているフィッシング対策協議会の消費者への注意喚起ページを挙げました。また、２つ目にはＩＰＡが国民向けに開設している情報セキュリティ安心相談窓口、３つ目には主にマルウェア対策の情報が掲載されているＪＣ３の情報提供ページを挙げております。

なお、当委員会ウェブページの掲載場所ですが、「ご注意ください！」の部分、「お知らせ　注意情報」の部分、「くらしと個人情報　気をつけて！　～個人情報にかかる注意喚起～」の部分を考えております。

説明は以上になります。御審議のほどよろしくお願いいたします。

○堀部委員長　ありがとうございました。

ただいまの説明につきまして、御質問、御意見をお願いします。

大滝委員、どうぞ。

○大滝委員　今、説明いただきましたように、事業者だけではなくて個人を狙ったサイバー攻撃は非常に多様なものになってきていて、クレジットカードの不正利用等の被害が増えてきているということが考えられると思います。

私のスマホにも、ここでいうとスミッシングと言われているようなものに近いものが時々送られてきており、不用意にＵＲＬにアクセスしてしまうようなことが日常的に起こる可能性もあるのではないかと思っています。そういう意味で、個人情報の流出を止めていく、被害を最小限に抑えていくという意味で、当委員会としてこういった形で個人に対しても注意喚起を図っていく、それから、専門の団体とも協力しながら前に進めていくということは大切なことだと思いますので、是非前に進めていただければと思います。

○堀部委員長　ありがとうございました。

ほかにいかがでしょうか。

手塚委員、どうぞ。

○手塚委員　今、大滝委員からもお話があったように、説明でもバンキングトロージャンやスミッシングというような話、それと、企業等では特に標的型攻撃でいろいろと対策を打って、演習等もやっているような時代になっているわけです。

そういう中で、特に個人というものに対しての攻撃は非常に個人差が出るところで、や

はり弱いところに影響が出てくる。個人情報保護委員会として、個人情報の取扱いという視点から言うと、まさにその弱いところに対してどういうふうに対応していくかということが非常に重要なテーマとであり、そこを所管する委員会としては非常に重要な役目を持っていると考えています。

そうは言っても、これらの分野は他のいろいろな組織で今までも対応してきていますので、委員会の一組織だけでやるのではなく、他のセキュリティの専門の機関とうまく連携することが非常に重要だと思っています。

先ほども名前が挙がりましたけれども、ＪＰＣＥＲＴ／ＣＣとか、ＩＰＡ、更にはＩＣＴ-ＩＳＡＣというような電気通信事業者系の非常に先端的なところを走っているところとか、警察系ではＪＣ３等があるわけで、是非そういうところとうまく連携して、この委員会でのノウハウをためるのと併せて人的交流も将来的には必要になるのではないかな、というような気もしますので、そういうところを深く検討していただいて、この個人情報の分野をしっかりと当委員会が支えていくというふうになればいいなと思っております。

○堀部委員長　ありがとうございました。

ほかにいかがでしょうか。

これまで御発言がありましたように、個人情報を狙ったサイバー攻撃が非常に増えておりまして、種類も多様化、高度化してきております。対象は事業者ばかりではなくて、個人を狙っているというところがありますので、当委員会といたしましては、手塚委員の御指摘のようにサイバーセキュリティの専門機関とも連携しながら、事業者ばかりではなく個人に対しても注意喚起を行うことが重要であると考えますので、こういう形で留意事項を掲載して、今後も引き続きこれを進めていく必要がありますので、対応については今後ともよろしくお願いしたいと思います。

ありがとうございました。

本日の議題は以上です。本日の会議資料につきましては、準備が整い次第、委員会のホームページで公表してよろしいでしょうか。

（「異議なし」と声あり）

○堀部委員長　そのようにさせていただきます。

本日の会議は閉会といたします。今後の予定につきまして、的井総務課長から説明をお願いします。

○的井総務課長　次回の委員会でございますが、９月12日水曜日の14時30分から開催の予定でございます。

本日の資料につきましては、ただいまの御決定どおりに取扱いをさせていただきます。

本日は誠にありがとうございました。