インタビュー

SBI EVERSPINの尹社長に聞く

サイバー攻撃、事前に防ぐ〜アプリの脆弱性に対応

聞き手
犬飼 優
金融財政ビジネス編集部

パソコンやスマートフォンによるインターネット取引が増える中、身代金要求型ウイルスの「ランサムウエア」などを使ったサイバー攻撃が急増している。SBIグループと韓国のAI基盤のセキュリティ企業、EVERSPINとの合弁会社「SBI EVERSPIN」が金融機関や一般企業を対象にしたサイバーセキュリティサービスを今年から本格的に始めた。尹慈明社長にセキュリティの重要性や実際にどのように防ぐかなどを聞いた。

尹　慈明 社長　（撮影:深澤　裕）

ランサムウエアが急増

――最近の金融取引の特徴は？

スマホをはじめとするモバイル端末の保有率上昇が背景となり、対顧客接点としてモバイルアプリの新規開発や機能拡充に注力する金融機関の動きが見られる。

現在、スマホは1人1台の「キーデバイス」。金融取引は、スマホのブラウザ経由で行うか、バンキングアプリを使うかのどちらかが多い。顧客が銀行店舗に出向く対面での時代と比べると、パラダイムシフトした。しかし、このようにネットで金融取引をする顧客が増えてきたために、サイバー空間での攻撃が非常に多くなってきている。

――サイバー攻撃にはどのようなものがあるのか？

直近だと、ランサムウエアによる被害が多い。警視庁の調査結果だが、2022年上半期は114件、下半期は116件、23年上半期は103件と、ランサムウエアの被害が依然として高水準で推移している。

ランサムウエアが狙うのはデータ。金融機関や企業のデータサーバーに入ってデータを盗み、身代金を要求したり、応じない場合は「データを流出する」と脅迫したりする。被害を規模別に見ると、大企業が3割、中小企業が6割、団体などが1割。業種別に分類した場合、製造業、サービス業が多いが、卸売・小売業、情報通信業など幅広い業種で被害が発生している（図表1）。

サイバーセキュリティ企業の米スプランクのリポートによると、過去1年間に大規模なサイバー攻撃を1回以上受けたことがあると回答した最高情報セキュリティ責任者（CISO）は90％に上る。さらに、83％の企業がランサムウエアによって身代金を支払っている。グローバルな調査だが、ランサムウエアは最も懸念すべきサイバー脅威の一つになっている。

身代金を支払ってデータやシステムを回復し、あるいは、機密情報の流出を防いだとしても企業評価が下がるリスクが付きまとう。

――ランサムウエアの攻撃方法は？

攻撃者はサーバーに侵入してデータを盗むことが最終目的だが、いろいろなシナリオを組み立てて攻撃してくる。例えば、不正に入手した認証情報を使ってログインする。ソフトウエアやシステムに脆弱性や欠陥がある場合は、それらを狙って攻撃する。あるいは、フィッシングメールを企業の従業員に送ってリンクを間違って押させ、そこから侵入する。

一度、攻撃が成功すると、すぐにシステム停止の被害が起きる。顧客情報が流出すれば顧客が被害を受け、企業価値も毀損する。情報等が改ざんされると、システム自体が混乱する。電子情報等が閲覧不可になるので、ネットによる情報が入ってこなくなる。フィッシング詐欺による不正送金など、実際の金融被害も起きる。

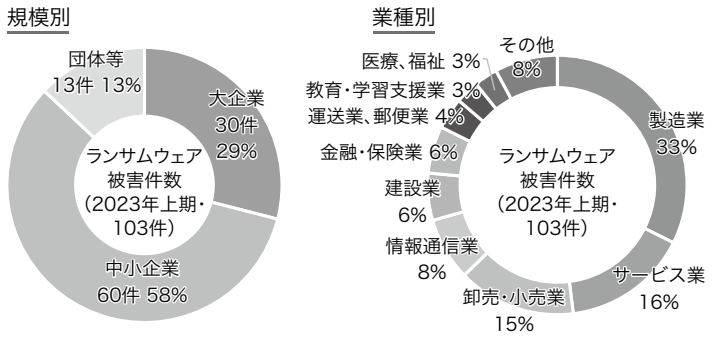
――攻撃が成功した場合の企業の対

応は？

事故対応として記者会見を行ったり、広告宣伝、新聞広告、テレビコマーシャルで謝罪する場合もある。

また、役所に事故原因や被害の範囲を調査して、報告をしなければならない。社内にサイバーセキュリティの専門家がいれば、原因をすぐに分析し、報告資料を作成できるが、大概の中小企業はそういった専門家がいないことが多い。

〈図表1〉企業・団体規模別被害状況（日本）



（出所）警視庁「令和5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」

企業は、自社がサイバー被害を受けた場合の予算を確保していないことが多い。まずは、そういった費用をどこかから調達しないといけない。また、個人情報が流出した場合、顧客からのクレームが来る。流出した個人情報が悪用された場合は、その補償も問題となる。法律専門家に相談し、どこまで顧客に補償していかないといけないかを考える必要がある。コンサルティング会社にサイバーセキュリティ専門のインシデント対応の相談もしないといけないかもしれない。

――個人へはどういった攻撃があるのか？

フィッシング詐欺が増えている。フィッシングサイトに誘導するメールにリンクが張られている。偽サイトとは気付かず、本物の金融機関のサイトと思い、そこにＩＤとパスワード（ＰＷ）を入れてしまう。個人情報がそのまま流出し、それを使って攻撃者が金融機関の本物のサイトに入り、攻撃者が不正送金をして、金融被害が出てしまう。

スマホのアプリでも、偽アプリをインストールさせて、そこにＩＤとＰＷを入れさせ、個人情報を悪用して、金融被害を与える手法も出てきている。

直近ではやっているものとしては、遠隔操作ソフト、アプリがある。犯罪者がモニタリングをしながら「やり方を教えます」と言って操作させる。操作内容を録画させ、被害者のスマホ情報、ＰＣ情報を盗む、もしくは、遠隔操作で不正な行為をさせる。高齢者らデジタル弱者がターゲットになることが多い。

被害が起こる前に守る

――サイバー攻撃を防ぐ方法は？

事前予防と事後対策の二つの側面があるが、われわれはどちらかというと、（攻撃の被害が出ない）事前予防に重点を置いている（図表2）。

まずは、攻撃の予兆を検知する方法で、ハッキング攻撃が実際にされているかどうかをモニタリングで検知する。

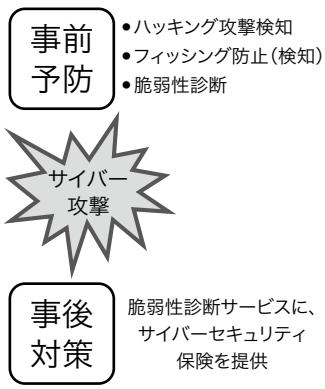
二つ目は、（金融機関のアプリを使う）個人客を保護するためにフィッシング防止、不正アプリなどを事前に検知する。

三つ目は、サイバー攻撃はソフトウエアあるいはシステムの脆弱性が狙われるので、この脆弱性を診断し、改善する。

――攻撃の予兆をどうやって検知するのか？

クライアントのサイトやアプリにセキュリティモジュールを導入する。併せて、サーバー側でモニタリング画面を見られるようにし、ハッカー攻撃のログ（予兆探知）をリアルタイムに確認できるようなモニタリング画面を用意する。ログ記録があるので、どういった攻撃があったかが分かり、事前に対策ができる。例えば、攻撃が１００件あったけれども、セキュリティ部門の目標として50まで減らしましょうと、年間目標の数字を立てることもできるようになる。モニタリングがなければ、攻撃がどのようにされているかが分からない。そもそも何が起こっているかを可視化できる利点がある。

〈図表2〉



――ハッキング対策をしてセキュリティが破られることは？

金融アプリなどに入っているセキュリティコードは通常は一つで、ハッカーが攻撃する際、時間をかければ、セキュリティコードが解析され、侵入され得る。

ＥＶＥＲＳＰＩＮ社はＡＩ基盤の技術を活用し、このセキュリティコードを毎日替える。ハッカーが攻撃してセキュリティコードを分析しても、侵入しようとした段階ではすでにコードが替えられている。また最初から分析が必要になる。これが延々と続き、ハッカーに時間を与えない。ハッキング攻撃は通常、時間をかけて行われるが、セキュリティコードが替わるため、セキュリティが破られることはまずない。

――フィッシング詐欺に対しては？

アプリへの対策だ。当社は、公式ストアに登録されている正規アプリの情報を毎日欠かさず収集し、今では２０００万以上の正規アプリをリスト化している。このデータベースを基に、端末にあるアプリが正規アプリであるか否かを照合する。正規アプリでない場合は、不正アプリになる。これを検知してメッセージを出し、モニタリング画面にも表示する。既存ではブラックリスト方式（ブラックリストを使って不正アプリを照合する）の対策が多いが、それでは新しく出てくる不正アプリが検知から漏れてしまう。

――技術者はどのような構成か？

ＥＶＥＲＳＰＩＮ社のホワイトハッカーらが対応する。技術チームは、攻撃者観点で研究する「ハッキング技術チーム」と、防御者観点の「セキュリティ技術チーム」の二つに分かれている。前者は、脆弱性診断サービスを対象に、実際のリアルサービスを一切の情報がない中でサーバーまで侵入可能かをテストする「模擬ハッキング」（ペネトレーションテスト）を行う。模擬ハッキングでセキュリティが破られれば、それを基に企業にどのような対策をすればよいかを助言できる。

なお事後対策として万が一、サイバー攻撃に遭ったときの費用をカバーするため、保険会社（ＳＢＩ損保）と共同で、脆弱性診断とセットになったサイバーセキュリティ保険も無料で提供している。

信頼なくせば事業継続は困難

――日本企業のセキュリティ対策をどう見ているか？

とりわけウエブサイトの対策に注力している印象がある。モバイルのアプリはセキュリティとして割と新しい分野だ。アプリをどう守るか、アプリにどうサイバー攻撃が行われるかは、最新の動きの中で出ている課題なので、対策を講じる段階まで来ていないのではないか。

ハッキングされる時も、フィッシングされる時も、犯罪者のターゲットは銀行口座や住所、電話番号、名前、ＳＮＳなどの個人情報だ。それらを盗まれれば、各人の状況が全部筒抜けになってしまう。

モニタリングの結果に基づいた事前の予防が不要なケースでは、別の形でのセキュリティ対策でもいいが、予兆検知によって防げる範囲は想像以上に広い。企業としてどのように情報を効率よく守っていくのかということに尽きると思う。

――サイバー対策で重要な点は？

攻撃により大きな被害が発生する事実を認識することだ。経済被害が出なかったとしても、個人情報の流出は企業価値の毀損につながる。ガバナンス上、企業の経営者がどう考えるか。個人情報が流出するというニュースは多く、被害が出れば、謝罪会見や引責辞任もあり得る。一番怖いのは、信頼を失うことだ。個人情報を流出させた企業に、もう一度情報を預けたいのかを考えると、顧客離れにもつながりかねない。信頼をなくしては事業を続けることは難しい。

セキュリティの予算は、「守り」の予算なので、（経営者は）消極的に考えがちだが、仮に企業価値が毀損した場合、その金額は決して小さくない。セキュリティを強化し、顧客に安全・安心を与えることで、結果として事業へも注力できるのではないかと思う。

【ＥＶＥＲＳＰＩＮ】韓国のＡＩ基盤のセキュリティ企業。偽アプリを検知するFake Finder は韓国の金融機関45社以上に採用され、人口では８割に当たる約４３００万人の金融取引をカバーしている。