米国サイバーセキュリティの最新動向

グローバルリサーチ研究所代表
青木　武
あおき・たけし　慶大卒。99年米ニューヨーク大学経営学修士（ＭＢＡ）取得。信金中金総合研究所ニューヨーク駐在主任研究員等を経て、09年7月米国内にグローバルリサーチ研究所（ＩＧＲ）を設立。http://www.igrlc.com/

C10pと称するサイバー攻撃団体が、Progress Software社のMOVEitというファイル転送システムの発見される前の脆弱性をついた「ゼロデイ攻撃」により、多くの企業、金融機関、政府等を襲った。少なくとも91の企業等が攻撃を受け、この中には少なくとも15の金融機関が含まれている。今回のようなゼロデイ攻撃は、ディフェンス（ソフトウエア等の開発者や利用者側）側が脆弱性を見つける前にサイバー攻撃側が相手の脆弱性を先に見つけ、攻撃を仕掛ける方法である。よって、通常の方法では防ぎようがない。サイバーセキュリティも新しい考え方に切り替える必要がある。

1　ゼロデイ攻撃とゼロトラスト

これまで、多くのサイバー攻撃は「一番弱い部分」である人間、つまり企業の従業員や顧客をターゲットにしたフィッシング攻撃、既に明らかになっているソフトウエアの脆弱性を攻撃する方法が主流であった。これらが引き続き主流であることに違いないが、上記の通り、攻撃者以外の誰もまだ発見していない脆弱性が見つかり、それが攻撃されるゼロデイ攻撃も脅威となっている。ソフトウエアを利用している企業からすれば、まだパッチもされていない脆弱性が攻撃されるため、防ぎようがない。さらに、金融機関の場合は、金融機関本体ではなく、利用しているＩＴ企業等が攻撃され、被害を受けるケースも多い。例えば、モンタナ州のクリアウォーター・クレジットユニオンは、本体のシステムではなく、サードパーティベンダーが攻撃されたと顧客に説明している。その結果、社会保障番号の末尾４桁、名前、口座番号、電子メールアドレスおよび電話番号が漏洩したと発表している。さらに、大手金融ＩＴベンダーのＦＩＳも攻撃の対象になっていた。同社を利用している一部の銀行において、顧客の情報が漏洩した懸念がある。このほか、CU*Answersというクレジットユニオン向けベンダーも攻撃を受けており、クレジットユニオンが影響を受けている。

フロリダ州のシティナショナル銀行も３・６万人分の社会保障番号等が漏洩したと報告している。サウンド・ファイナンシャル・バンコープもＳＥＣに対して、ベンダーがMOVEitを利用していたことから、１・６万人分の情報が漏洩したと報告している。

先述の事例の場合、Progress社はＳＱＬインジェクション（アプリケーションの脆弱性により、本来の意図ではない命令文が注入されること）に関する三つの脆弱性を発見し、既にパッチをリリースしている。

Clopはこれまで50以上の組織にランサム請求をしており、そのうち25％は金融機関であるという。また、運転免許センターのような政府機関からも個人情報を盗んでいる。オレゴン州では、州が発行している運転免許の90％に当たる３５０万の運転免許証の情報が漏洩している。金融機関から個人情報が漏れたことにより、今後、漏洩対象者のカードや口座がなりすまされるリスクがあり、注意が必要となっている。

　このような、まだ見つかっていない脆弱性に対応するためには、ゼロトラストと呼ばれるサイバーセキュリティ対策が重要であると考えられている。コロナウイルスに例えれば、今までのサイバーセキュリティは水際対策、つまり国内（企業内）にウイルスが入らないように境界を防衛しようとする試みである。一方、コロナで明らかになった通り、水際対策には限界があり、日本も水際対策を強化して鎖国状態であったにも関わらず、２０２２年８月ごろのコロナ感染状況は世界でもトップクラスであった。一方、コロナウイルスは既に国内にまん延しているという前提で、国民のほとんどがワクチンを接種すれば、実質的な感染者は少なくなるはずである。ゼロトラストはこうした考え方に似ており、「企業内に攻撃者は侵入している」という前提の下、対策を行う方法である。ゼロトラストは、２０１０年にフォレスターリサーチが提唱し、その後、米国国立標準技術研究所（ＮＩＳＴ）も「基準８００―２０７」をリリースしている。ゼロトラストはその名の通り、「何も信用しない」という意味であるが、今までのサイバーセキュリティのように外部との境界（水際）を防衛するという発想ではなく、「攻撃者は既に侵入しており、その攻撃の被害を最小限にする」ということが前提となっている。具体的なプラクティスは以下の通りとなる。

●重要な情報資産は常に暗号化する。これにより、漏洩したとしても被害がないようにする。もっとも、量子コンピューターが将来的に発達すれば、漏洩した情報が暗号化されていても、将来的に量子コンピューターで暗号が解読されるというリスクはある。こうしたことから、暗号化も今後は量子コンピューターでも解けない暗号にしていく必要があると思われる。

●権限を必要最小限にする。19年のキャピタル・ワン（大手金融機関）のハッキング事案の際は、キャピタル・ワンのファイヤーウォールに何でもできるような権限が与えられていた。このため、元ＡＷＳ（アマゾン・ウエブ・サービス）職員に悪用され、情報が漏洩した。人にしてもシステムにしても、必要最小限の権限しか与えないことがゼロトラストでは重要であると考えられている。

●マイクロセグメンテーション：仮に侵入されたとしても、ネットワーク内に幾つも壁を設け、よそのセクションには移動できないように封じ込める。

●継続的に本人確認をする。ＡＰＩ（アプリケーション・プログラミング・インターフェース）の場合、正当な権限で入るが、その後、自分の権限を拡大して他の情報を盗む、といった手口が考えられる。本人確認、認証は最初だけでなく、継続的に行い、今利用している人が本当にその権限があって利用しているのかどうかを確認する必要がある。

●別環境にバックアップを設定する。ランサム攻撃で、バックアップも攻撃されればランサムを支払うほかに方法はなくなる。バックアップは別環境に安全に保管する必要がある。なお、サイバー用のバックアップは天災用のバックアップとは異なる。ウイルス等がないことを確認し、遮断された環境に保管する必要がある。

　もちろん、実際にこれらを実行することは、言うほど簡単ではない。それでも、サイバーセキュリティの考え方はゼロトラストの方向にシフトしており、クラウド・セキュリティ・アライアンス（ＣＳＡ）などのセキュリティ団体でもゼロトラストの話題やイベントが増えている。現実的に、上記の対応ができなければ、攻撃された金融機関等はランサムを支払わざるを得ないが、支払先が米国政府の制裁の対象になっていれば、金融機関等自身が政府から罰せられることになる。

　本件についても、社会保障番号を含む個人情報はファイル転送の際に暗号化されていたはずであり、実際にこれらの漏洩がエンドユーザーにどのような被害をもたらすのかは不明である。いずれにしても、情報が漏洩した個人に対しては、金融機関

は通知し、今後クレジットビューローの情報などに留意し、なりすまされてクレジットカード等が作成されないように注意を喚起する必要がある。現実問題として、今回のような脆弱性が発見される前のゼロデイ攻撃は防ぎようがなく、ましてやＦＩＳ社のようなトップクラスの大手金融ＩＴベンダーが攻撃された場合、同社を利用している中小零細金融機関は実質的に無力に近いように思われる。零細金融機関が熱心にＦＩＳ社のデューデリジェンスをしたところで、今回のような事態は想定できなかった可能性が高い。ゼロトラストの発想で、今後も同様のことが起きると想定し、暗号化の強度を高めることも検討に値するかもしれない。

２　サイバーセキュリティの最新情報

ウォール・ストリート・ジャーナル（ＷＳＪ）紙の主催でサイバーセキュリティのカンファレンスがオンラインで開かれ、その中で行われた専門家である Secure Anchor社ＣＥＯエリック・コール氏へのインタビュー内容を紹介する。同氏が最近の傾向として最も懸念していることは、サイバー攻撃の事業化である。サイバー攻撃は組織犯罪であり、企業のように従業員がいて組織的な攻撃をしている。また、生成ＡＩなどＡＩが発達していることから、フィッシングでＡＩが使われる。以前とは異なり、ＡＩで作成した電子メールは本物の上司からの電子メールと見分けがつかない。偽物の方がよくできていることもある。そうしたことから従業員向けのサイバー研修がいつも重要である。

このほか、ランサムウエアを脅迫に使うようになってきた。これまでランサム攻撃は企業のシステムを暗号化して、使えなくするという手口が中心であり、企業側にバックアップがあるかどうかが鍵であった。今は個人情報などを盗んで公開するぞと脅迫するという手口が増えてきた。例えば、ＥＵの市民の10万人分の個人情報が企業から漏れれば、当該企業はＥＵから２５００万ﾄﾞﾙの罰金を取られる。それを「１割の２５０万ﾄﾞﾙでいいよ」などとハッカーは要求してくる。政府は「ランサムを払うな」と言っているが、現実的には、企業にとってランサムを払わざるを得ない状況であることが多い。企業にとって、ランサムを払って、またやられる可能性はあるのか、というと、脅迫側もビジネスとして行っているので、通常は契約により12カ月などの契約期間中は再攻撃はしてこないことが普通であるという。企業はランサムを支払ってすぐに今のネットワークを修復し、１年以内に強化する必要がある。

ＡＰＩについては、攻撃者からすれば、入りやすい。プレミアムサービスでＡＰＩを分析したり、ペネトレーションテストを行い、分析ツールを買って評価すべきだ。ＡＰＩはセキュリティをあまりテストされていない傾向がある。

チャットＧＰＴのプライバシーについては、一般に言われている通り、懸念がある。しかし、それよりＳＮＳや検索エンジンの方がよほど個人情報を持っているので、現実的にはそちらの方を懸念すべきかもしれない。生成ＡＩの多くは個人をアバターとしか見ておらず、個人情報を追跡していないため、現実的なプライバシーの懸念は小さいという。一方、ユーザーは個人に関するデータをＳＮＳに無料で提供していることに問題意識を持つべきである。

サイバー対策に１００％の安全はない。まずはビジネスにとってのリスクを考える。それから、許容できるレベルのサイバーリスクを把握する。サイバーリスクはビジネスリスクであり、コストさえかければサイバーリスクは減らすことはできる。

フィッシングの多くは、ウィンドウズやマックＯＳを対象にしており、ｉＰａｄ等ではない。よって、電子メールはｉＰａｄやクロームブックで読むようにすれば間違えてクリックしてもリスクは低い。ｉＰａｄには失って困るデータを保存しない。他者と情報を共有するためには、ドロップボックスのようなファイルシェアは多要素認証が使えるため、電子メールより安全と言える。

攻撃者はセキュリティが弱い中小企業等を狙っている。中小企業は、システムはクラウドを利用すべきであり、自社内でやるべきではない。クラウドのリスクについては、クラウド業者はセキュリティの問題があれば顧客を失うことになるので、強力なセキュリティ対策を講じている。ゼロトラストなど、対策の有効性も証明されている。特に中小企業にとっては、クラウドは最善の方法とい

える。逆に、今はローテクの郵便や電話が脅威となっている。郵便を盗んだり、電話で国税局員になりすます手口がある。

３　ホワイトハウスもサイバーセキュリティを強化

バイデン政権は今年３月に国家サイバーセキュリティ戦略を発表しているが、７月13日にその実行計画を発表した。当該戦略には以下の五つの柱がある。

１　重要なインフラを守る：米国では、コロニアル・パイプラインへのランサム攻撃が記憶に新しいが、こうした重要なインフラを守るために必要な規制の強化が行われる。

２　攻撃者を混乱・解体させる：攻撃者はロシアや中国にいる場合が多く、実際にどこまで解体させられるのかは疑問もあるが、国として攻撃者に対して防衛だけでなく、より攻撃的になる、という意味と思われる。

３　セキュリティとレジリエンスの力を強化する：サイバー攻撃の基本は最も弱い者を攻撃する、ということになるが、それを防ぐために、強い者が弱い者を守れるような仕組みを作る、ということになる。金融機関にとっては、個人や中小企業など最も弱い者のサイバー攻撃を防ぐために何ができるのか、を検討する必要がある。また、個人情報の保護がより強化されると思われる。

４　将来に向けての投資：量子暗号対策やサイバー人材の育成に投資する。

５　同盟国とのパートナーシップを強化する。

米国では、金融は16の重要なインフラの一つに指定されている（金融以外は核関連施設、水、電力、ＩＴ、通信、運輸、食料、医療、政府、消防・警察、防衛、ダム、重要な製造業、化学、人が集まる場所）。ただし、金融機関に対しては、サイバー攻撃を受けた場合の36時間以内の報告義務等、既に厳しい規制がある。今後はソフトウエアの脆弱性のパッチマネジメント等をさらに強化する必要があるかもしれない。また、地政学リスクが増していることから、国家によるサイバー攻撃が特に懸念されている。一方、銀行では不正防止、マネロン対策、サイバーセキュリティの部門間の意思疎通が十分になされていないという問題も指摘されている。また、マネロン対策で行っている顧客の口座の資金の動きの監視について、ランサム関連の支払いの疑いがある場合は、その取引報告等をする必要が強化されると思われる。

７月13日に発表された実行計画においては、①官民を問わず、最も規模が大きく、最も能力があり、最も有利な立場にある主体が、サイバーリスクを軽減するための負担をより多く引き受けるようにすること②サイバーセキュリティへの長期投資を促進するインセンティブを高める―の二つの原則が定められている。アメリカンバンカー紙によると、ソフトウエアの脆弱性について、誰が責任を取るか、ということについて、上記の原則①である「最も規模が大きく、最も能力があり…」を適用する場合、銀行に関するサイバー事案であれば、銀行が責任を取らされる可能性が高い。さらに、ソフトウエアの成分表（ＳＢＯＭ）とも呼ばれる仕組みを導入し、ソフトウエアを構成しているコンポーネントを開示させることも計画に含まれている。米銀の多くは自前でソフトウエアを開発しているため、ＳＢＯＭを開示することが必要になる可能性がある。ＳＢＯＭの基準にはＳＰＤＸ、CycloneDXおよびＳＷＩＤが列挙されている。

欧州でも、ＤＯＲＡと呼ばれる規制が導入され、サイバーセキュリティが強化される方向にある。サイバー攻撃・サイバーセキュリティの状況は日々刻々と変化している。企業・団体は常に最近の動向について留意し、対策を行い、従業員や顧客を教育・啓蒙していく必要がある。