バングラデシュ中央銀行での不正送金事件の余波

2016年バングラデシュで、SWIFTを通じた巨額の不正送金事件が起きた。これは果たして対岸の火事なのだろうか？　事件を受けたSWIFTの対応は、「金融機関→ベンダー」という従来の外部委託管理のあり方に一石を投じている。

外縁部が狙われたサイバー銀行強盗

2016年2月4日木曜日の営業時間外に、バングラデシュ中央銀行のシステムにハッカーがマルウェアを利用して侵入した。そのハッカーは乗っ取ったアカウントを利用し、SWIFT[1)]を通じてニューヨーク連邦中央銀行宛に偽の送金指示を行い、フィリピンの銀行口座などへの不正送金に成功した。そこからカジノ等にお金が流れ、行方が分からなくなっている。

この事件は以下の点で特徴的だった。

1. 被害額が約8,100万ドルと史上最大級（送金の試みは10億ドル弱）
2. 最終的な標的は中央銀行（一般の銀行ではない）
3. 銀行のバックオフィス業務に精通した、精巧なマルウェアを使用
4. 詐欺の舞台が複数の国に跨っていた

事件は執筆時点では未解決であり、犯行の手口の詳細は分かっていないが、SWIFT利用者のネットワーク全体から見て、セキュリティの脆弱な「外縁部」が突破口として狙われた形であると言える。

SWIFTが講じた対策

SWIFTはこの事件を受けて迅速かつ積極的に行動を起こし、新しい「顧客セキュリティプログラム」[2)]を発表した。以下ではその中から2つの取り組みを紹介する。

1つ目は、SWIFT利用にあたって顧客が遵守すべき新たなセキュリティの枠組みである「顧客セキュリティフレームワーク」（CSF）の導入である。CSFは「必須」および「推奨」に分類された27のセキュリティコントロールから成る。個々のコントロールは国際基準に紐づいたものとなっており、事件の教訓が反映された内容と言える。

CSFの導入はいわば、今回の事件の発端となった外縁部のセキュリティレベルの底上げを狙ったものと捉えることができる。実際、本稿を執筆した時点で公表されているコントロールを見てみると、日本の金融機関にとって特に目新しいものはないようである。（念のため、自社の現状のコントロールとのギャップ分析を行い、必要に応じて対策を打つ必要があるだろう）

このCSFは「顧客保証フレームワーク」（CAF）によって裏打ちされている。CAFは、顧客が自身のセキュリティ遵守状況を対外的に「保証」するものだ。SWIFTの顧客はCSFの遵守状況を自己証明し、毎年報告する義務が生じる（2018年からの予定）。SWIFTを利用する日本の金融機関においても、SWIFTが要求するコントロール達成状況の自己評価のための準備を確実に進める必要がある。また、SWIFTは要求したコントロールが達成されているか、利用顧客をサンプリングし毎年監査を行う旨を表明している。この報告結果は専用サイト上で公開され、SWIFTでの取引相手が確認できるようになる。さらに利用規約上、報告結果を各国の規制当局に通知する権利をSWIFTが保持することを明言している[3)]。

2つ目は、インシデント、サイバーセキュリティに関する情報共有の強化である。バングラデシュでの事件後、ベトナムやエクアドルといった国でも以前に同様の事件が起きていたことが、メディアの報道により判明した。それまでSWIFTは同様の被害が発生していたことを把握していなかった。このため、SWIFTは自身に関連したインシデント情報の報告を改めて顧客に義務付け

NOTE

1) 国際銀行間通信協会（Society for Worldwide Interbank Financial Telecommunication）。SWIFTが提供するメッセージング・サービスは世界中の200以上の国家と地域で、11,000以上の金融機関等に利用されている。事件では、SWIFTが提供している銀行保有のAlliance Access systemのアカウントが乗っ取られ、不正な送金指示が可能となったと見られる。
2) Customer Security Programme（CSP）。SWIFTの顧客のセキュリティを守るためのプログラムとして発表されたもので、以下の5原則からなる。
①情報共有の改善
②SWIFTが提供するツール群の改善
③セキュリティガイドライン改善と保証フレームワークの提供
④正常取引パターンの把握／不正メッセージ検知への取り組み
⑤外部業者によるセキュリティサポート向上
今回はそのうち①③について取り上げ紹介した。
3) なお、英米ではこのSWIFTの姿勢を規制当局が後押しする動きがある。

た。この情報共有も、先述の遵守状況報告の対象とされたことから、以前よりも各金融機関の報告活動のインセンティブが上昇することが予想される。

また、SWIFT自身も有力な情報セキュリティ企業と契約を結んで技術面での対策強化を図っている。これにより、SWIFTにおける入手情報の理解度の向上が期待され、コミュニティ全体の情報共有レベルが上昇すると考えられる。

新たな協業態勢の幕開け

今回の事件が日本の金融機関に与えた示唆は2つあると考える。

1つ目は、日本の金融機関のグローバルな情報に関する情報共有、中でも情報の吸収力に関する懸念である。前述のように、今回の事件を機にSWIFTは情報共有を強化しようとしている。SWIFTからの情報提供は専用サイトを使って行われるが、そこに掲載される情報は基本的に英語である。日本の金融機関が英語の共有情報を吸収する能力は十分だろうか。国内の日本語での情報共有に懸念がないとしても、グローバルではどうだろうか。

今回のSWIFTの措置は日本の金融機関に大きな影響を与えるものではないと考えられるが、今後はセキュリティ等に関してより重要な情報が発信されることもあり得る。しかも、サイバーセキュリティに関する情報は迅速かつ正確な対応が求められるものが多い。日本の金融機関の中には、このグローバルかつ迅速・正確な情報吸収が不得意なところもあると想定され、効率的な対策を検討する必要があるだろう。

2つ目は、金融機関とサービス提供者の在り方についてである。今回の事件を受け、SWIFTは利用金融機関に対し、セキュリティ遵守とその遵守状況の報告を要求した。これは、共同システムにおいて「ベンダーから金融機関へ」セキュリティ遵守を要求し監査する形である。従来は、「（ユーザーである）金融機関からベンダーへ」統制活動やセキュリティ遵守について報告を要求し、監査を行ってきた。今回の流れは従来のものとは明らかに逆方向の動きである。これはいわばベンダーがイニシアティブを取った形であり、従来の外部委託管理に一石を投じたと言える。

昨今、金融サービスが高度化してきており、今後はフィンテック企業がサービス提供者として金融業界に進出してくることが予想される。彼らは時にはベンダーの立場にあるかもしれないが、時にはユーザーの立場をとるかもしれない。この場合、契約形態の複雑化が予想され、従来の動きに加え、特に「ベンダーから金融機関へ」の要求・監査形態が増えてくる可能性があると考えられる。

今回の事件は、セキュリティコントロールの方向性を変えた潮目のひとつなのかもしれない。特にSWIFTのようなグローバルネットワークを運用していくためには、従来のようにベンダーだけがセキュアな環境を保証するのではなく、ユーザーである金融機関も加わり、互いに協力してセキュアな環境を構築・維持していくことが求められるのではないだろうか。

（執筆協力：金融システムリスク管理部　塩入 崇史）

Writer's Profile

エリック・ファンドリッチ Eric Fandrich
金融システムリスク管理部
上級コンサルタント
専門は金融市場と金融機関のグローバル化研究
focus@nri.co.jp