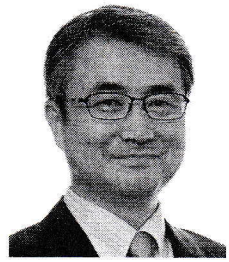
バングラデシュ中央銀行の不正送金事件とSWIFTのセキュリティ対策

日本の金融機関も含め、18年1月から安全基準の強制適用と外部検査の導入が始まる

2016年2月に不正な送金指図により、バングラデシュ中央銀行がニューヨーク連銀に預けてあった外貨準備から8100万ドルが盗み出されるという前代未聞の事件が発生した。この不正な送金指図にSWIFT（注1）が使われていたことを受け、SWIFTはこのほど新たな「セキュリティ対策フレームワーク」を導入し、すべてのSWIFTユーザーにその遵守を義務付ける措置をとった。本稿では、不正送金事件の概要とSWIFTの新たなセキュリティ対策について解説する。

麗澤大学
教授 **中島 真志**



過去最大の不正送金被害が発生

2016年2月にバングラデシュ中央銀行で8100万ドル（当時のレートで約93億円）の不正送金事件が発生した。具体的には、バングラデシュ中央銀行がニューヨーク連銀に保有している口座から、35回にわたり合計9億5100万ドルにもあたる不正送金が試みられた。このうち大半の送金は阻止されたが、4回分の合計8100万ドルについては、二つの中央銀行間の連絡の不備もあって、中継銀行（ドイツ銀行）を経由してフィリピンのリサール商業銀行の口座へ送金されてしまった。その後、カジノが保有するとされる多くの口座に分散して入金され、そこから引き出されて、資金の行方がわからなくなった。

これは、「単一のサイバー犯罪の被害額としては過去最大のもの」といわれており、翌月にはバングラデシュ中央銀行総裁が責任をとって辞任に追い込まれた。また、こうしたSWIFTを使った不正送金事件はこの1件だけにとどまらず、エクアドル、ベトナムなどの銀行でも同様のサイバー攻撃を受けていたことが明らかとなり、SWIFTのネットワーク全体の信頼性の問題として危機感が高まった。

約40年の歴史で初めて安全性が脅威にさらされる

不正送金事件を受けたＳＷＩＦＴの対策

国境をまたいだクロスボーダーの資金の受払いには、中央で集中的に決済を行う中央銀行のような存在がないため、お互いに契約を結んだ「コルレス銀行」が、お互いのために資金の受払いを行うのが一般的である。こうした国際業務を行う銀行の間において、国際的な送金メッセージの通信を行っているのがＳＷＩＦＴである。ＳＷＩＦＴは世界２００カ国以上に所在する１万１０００以上の金融機関を結んで、国際的な支払いメッセージの伝送サービスを行っている。こうした国際金融取引の中核にあって、日々、多額の国際資金移動に用いられているネットワークが不正送金に用いられたことは、世界の銀行に衝撃を与えた。

ＳＷＩＦＴは１９７７年の稼働開始以来、約40年の歴史を有するが、このようにＳＷＩＦＴの安全性が問題になったのは「ＳＷＩＦＴの歴史上で初めてのこと」であり、しかも中核的なサービスにかかわる問題だけに、ＳＷＩＦＴでは今回のサイバー攻撃の脅威をかなり深刻な問題としてとらえている（注2）。

不正送金の手口は四つのステップで巧妙に

ＳＷＩＦＴでは、今回の不正送金事件について、「ＳＷＩＦＴのネットワークやシステムの安全性が破られたわけではない」という点を強調しており、あくまでも「ユーザーの行内システム（ローカル環境）における安全対策の不備によるもの」としている。サイバー攻撃の対象となったいくつかの銀行は、規模、所在地、ＳＷＩＦＴへの接続方法、インターフェースなどはそれぞれ異なっているものの、「行内のセキュリティに脆弱な点があった」という点では共通していたものとされている。バングラデシュ中央銀行のシステムについても、①ファイアーウォールが不備であったこと、②パスワードが長期間変更されていなかったこと、③ＳＷＩＦＴとの接続に中古の安価なスイッチが利用されていたこと、などが指摘されている。

サイバー攻撃は、以下のような四つのステップで行われたものとみられている。第一に、ユーザーのローカル環境にマルウエアなどを使って侵入が行われた。第二に、ユーザーのローカル環境のシステム内に、マルウエアが一定期間にわたって潜み、送金権限者の認証情報（ＩＤとパスワード）など、不正送金を行うために必要な情報を入手した。第三に、入手した認証情報を使ってＳＷＩＦＴのシステムにログインし、不正な送金のメッセージを送った。第四に、ユーザーのローカル環境において、不正送金を送った痕跡を消しておいた。バングラデシュ中央銀行では、取引履歴がプリントアウトできないように改竄されており、不正の発見が遅れることになった。

事件発生後のＳＷＩＦＴの対応

ＳＷＩＦＴでは事件が明らかになって以降、以下のような四つの対策をとってきた。ＳＷＩＦＴでは、こうした対策を進めるうえで、ＳＷＩＦＴのみの対応では十分ではなく、金融業界内の協力が不可欠であるとして、「ユーザー全体としての対応」が必要である点を強調している。

①顧客安全プログラム（16年5月）

ＳＷＩＦＴは5月に「顧客安全プログラム」（ＣＳＰ、注3）を導入した。これは、(a)ユーザー間の情報交換の改善、(b)ＳＷＩＦＴ提供のツールの向上、(c)安全ガイドラインの向上、(d)不正検出の向上、(e)外部業者によるサポートの向上という5本柱による対策である。そしてユーザーに対して、①ＩＤやパスワードなどの認証情報の管理の厳格化、②ＳＷＩＦＴ接続機器に対するインターネット接続の制限、③ＳＷＩＦＴへのインターフェースのバージョンのアップデートの励行、④ＳＷＩＦＴの不正利用があった場合の早期の報告などを求めた。なお、ＳＷＩＦＴのルールでは、ＳＷＩＦＴのサービスで不正利用があった場合には、ただちにＳＷＩＦＴに報告することが求められている。

②専門部署の立ち上げ（16年7月）

ＳＷＩＦＴは7月にサイバー

セキュリティの専門部署である「顧客安全情報活動チーム」を立ち上げた。このチームには、複数のサイバーセキュリティの専門会社も参加している。

〔図表１〕　日次検証レポートの概要

アクティビティ・レポート（日々の送受信の合計額）		リスク・レポート（大口の支払いや異常なメッセージ）
●メッセージ・タイプごと ●通貨ごと ●国ごと ●相手行ごと	●１日の合計件数 ●１日の合計金額 ●最大額の取引 ●平均的な取引件数・金額との比較	●最も金額の大きい取引 ●最も合計額が大きい相手行 ●新しい取引相手との取引

③ＲＭＡの利用キャンペーン（16年8月から）

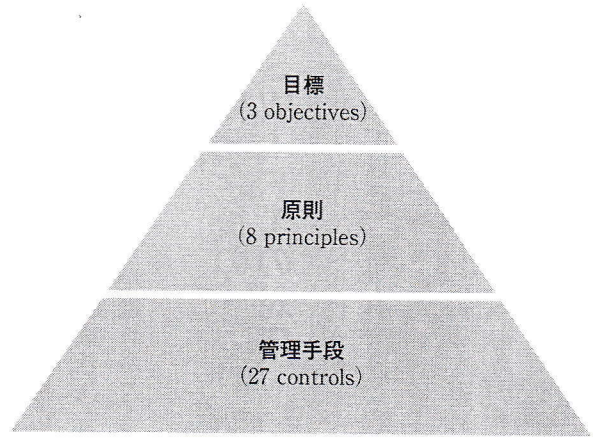
ＳＷＩＦＴは８月以降、メッセージの送受信のフィルター機能である「ＲＭＡ」（注４）を第一線の防御として利用することを、ユーザーに呼びかけている。ＲＭＡは、送受信する相手行や各行とやりとりするメッセージのタイプを選択・制限することができるフィルター機能であり、これを使うことによって、迷惑メッセージや不正な支払いを防止することが可能になる。

④日次検証レポート（16年12月から）

ＳＷＩＦＴにおける日々の取引の集約データを提供し、それによりメッセージの送受信の検証や異常なパターンの検出を可能とする日次のレポートが、12月から導入される。このレポートは独立したチャンネルを通じてユーザーに届けられるため、送金部署以外の独立した部署がレポートを受け取って検証することが可能となっている。セキュリティが破られた場合には、ローカルなシステム上の支払いデータや照合データが変更されてしまうことが多いため、こうした証拠隠滅への対策となる。

この異常発見のためのツールには、２種類のレポートがある（図表１）。一つは「アクティビティ・レポート」であり、日々のメッセージの送受信の合計額について通知するものである。一日のデータをまとめて簡単にみられるようにした一覧表（スナップ・ショット）を作成することにより、異常パターンを検出しやすくする。二つ目は「リスク・レポート」であり、大口の支払い、異常なメッセージ、これまで使われていない支払いルートの利用など、異常な行動パターンについて通知するもの

〔図表２〕セキュリティ対策フレームワークの構成



〔図表３〕　セキュリティ対策フレームワークの目標と原則

三つの目標	八つの原則
１．ユーザー環境の安全性確保	①インターネット接続の制限 ②基幹システムと一般的なＩＴ環境との隔離 ③攻撃対象領域と脆弱性の縮小 ④物理的な安全性の確保
２．アクセスの制限	⑤認証情報の漏洩防止 ⑥ＩＤの管理と権限の分離
３．不正の検出と対応	⑦システムや取引情報における異常行動の検出 ⑧事故発生時の対応や情報共有の方針策定

である。これにより、特異な送金相手や異常な送金パターンを早期に特定することができる。

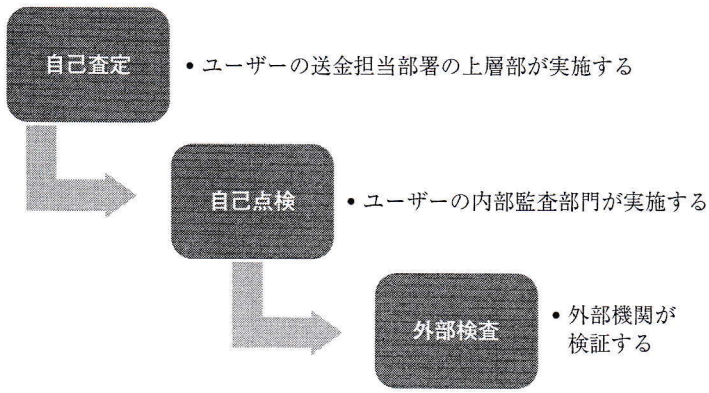
「セキュリティ対策フレームワーク」の導入

ＳＷＩＦＴは、こうした種々の対策に加えて、さらなる本格的な対策として「セキュリティ対策フレームワーク」を導入することを9月末に公表した。このフレームワークでは、すべてのＳＷＩＦＴユーザーに「コア安全基準」を強制適用することとしており、この基準に適合していることを毎年、ＳＷＩＦＴに対して示すことが必要とされる。また、この安全基準を満たしていないユーザーについては、その組織名を対外的に公表するという、やや強硬的なアプローチをとっている点が特徴である。

セキュリティ対策フレームワークは、①三つの目標、②八つの原則、③27の管理手段によって構成されている（図表2、3）。27の管理手段のうち、16が「強制適用」であり、11は適用が望ましいとされる「勧告ベース」である。

同フレームワークでは、上記のような安全対策を①自己査定、②自己点検、③外部検査という3段階のプロセスによって達成するものとしている。つまり、ユーザー部署がまず自己チェックを行ったうえで、次に社内の内部監査部門が点検を行い、最終的には、外部機関がさらにチェックを行うこととされている（図表4）。

〔図表4〕 セキュリティ対策フレームワーク達成のための三つのプロセス



〔図表5〕 セキュリティ対策フレームワークの実施スケジュール

2016年10月末	フレームワークの詳細をユーザーに通知
2016年11～12月	各国からのコメント期間
2017年3月	フレームワークの最終版の公表
2017年4月～	各行での自己査定のスタート
2018年1月～	強制適用の開始（外部検査のスタート）

このフレームワークに関する詳細を10月末にユーザーに通知し、年末までの2カ月間は、各国のユーザーグループからのフィードバックを受ける期間とする。そのうえで、17年3月末までに最終版を公表し、すべてのユーザーにその遵守を義務付けることとしている。

これを受けて、17年4月からは各ユーザーにおける自己査定がスタートすることになる。また、安全基準の強制適用と外部検査は18年1月から開始される（図表5）。各ユーザーの安全基準の遵守状況（コンプライアンス・ステータス）については、取引相手の銀行に対して開示される。これは、各ユーザーが、相手行のリスクに応じて取引関係を継続するかどうかを決めるようにするためである。

また、安全基準を達成していないユーザーについては、監督当局に対して組織名を公表することとしている。こうしたやや強硬な手段がとられるのは、セキュリティは金融機関のネットワークにおける最も弱い部分で破られる可能性が高く、また一部が破られると、ネットワークを通じて金融業界全体に対しての脅威となるためである。

日本のユーザー約200社も対応が不可欠

このセキュリティ対策フレームワークは、前述のように全世界のすべてのＳＷＩＦＴユーザ

lに強制的に適用されるものである。したがって、わが国におけるＳＷＩＦＴユーザー（銀行、証券など約２００社）においても、今後、すべての先で自己査定・自己点検などの対応が求められることになる。また、安全基準の遵守状況が不十分である場合には、海外との取引関係に影響が出る可能性もある点には注意が必要である。

（注）1　Society for Worldwide Interbank Financial Telecommunication（ＳＷＩＦＴ）はベルギーに本部をおく協同組合として設立された。金融機関の金融取引に関するメッセージ通信「金融メッセージング・サービス」を国際的なネットワークを通じて提供している。詳細については、『ＳＷＩＦＴのすべて』（東洋経済新報社）を参照のこと。

2　今年9月にジュネーブで開かれたＳｉｂｏｓ（サイボス）でも、サイバーセキュリティが中心的なテーマとして、多くの議論がなされた。サイボスは、ＳＷＩＦＴが主催して世界各国の金融機関のトップやシステム関係者が一堂に会する、金融関係では最大級の国際会議である（今年の参加者は８３００名以上）。

3　Customer Security Programmeの略。

4　Relationship Management Applicationの略。通常のＲＭＡでは、対象メッセージのすべてに対して制御をかけることができる。メッセージのタイプを選択して制限をかける場合には、「ＲＭＡプラス」というオプション機能を利用する。

なかじま　まさし
81年一橋大学卒、博士（経済学）。日本銀行、国際決済銀行（ＢＩＳ）などを経て現職。著書に『決済システムのすべて』『証券決済システムのすべて』（以上、共著）、『ＳＷＩＦＴのすべて』『外為決済とＣＬＳ銀行』『入門 企業金融論』（以上、単著）などがある。

書架

『未来がみえた！』
筒井義信とチームみらい編著／プレジデント社 刊／1,200円＋税

地方創生が盛り上がりをみせているが、私にはやや不満がある。どうしても国主導で画一的なようにみえるからだ。地域は多様なのだから、各地域は自らの特性を生かして個性的な活性化の道を探るべきだ。本書はまさにそうした個性的な地域おこしの実例をニッセイ基礎研究所の有志が紹介したものである。

たとえば、北海道東川町では、「写真甲子園」が盛り上がっており、愛知県東栄町では伝統の「花祭」を通じて限界集落に人を呼び込んでいる。福岡県福岡市川端商店街では学会誘致に力を入れ、沖縄県久米島町では、海岸を離れるとすぐに水深が深くなるという地域特性を生かして、車エビの養殖などの深層水関連産業が勃興しつつあるといった具合だ。こうした元気な地域の事例を知ることは、地域創生という困難な政策課題に取り組みつつある多くの人々を勇気づけることになるだろう。

事例を目にして、私は次の3点を再認識した。第一は、だれが主役かだ。本書の紹介事例には地方自治体、ＮＰＯ、地域住民など多様な主体が参加している。つまり「国主導ではない」という特徴がある。地域の活性化はその地域自身が考え実践すべきものだということがわかる。

第二は、地域の個性を生かすことだ。各地域が伝統、歴史、地域的特性、地場産業などのそれぞれの地域ならではの特徴を生かして、活性化に取り組んでいる。このことは、他の地域の真似ではなく、自らの地域ならではの地域資源を発見していくことの重要性を示している。

第三は、やはり重要なのは「人」ということだ。紹介事例には必ずキーパーソンが存在する。そのキーパーソンが若干強引にでも方向性を示すことで、地域が導かれていくのだろう。

地域の活性化に関心をもつ多くの人に読んでほしい本である。

（法政大学大学院政策創造研究科教授　小峰 隆夫）