金融機関を標的としたサイバー攻撃等の動向について

佐々木　稔[1)]

概　　要

近年、サイバーセキュリティに対する脅威の増大が声高に叫ばれている。

国家レベルでは、日本政府が来年の東京オリンピック・パラリンピック競技大会を見据えて取組みを加速させており、国際的には選挙への介入や通信機器の安全性などが大きな問題として取り上げられている。

他方、個別のサイバーセキュリティ事案のレベルでは、SNS からの情報漏洩事案が世界的に大きく報じられ、日本国内では今年に入って百万件単位の情報漏洩事案が複数公表されてはいるものの、そもそもそのような事案の詳細まで公になることは決して多くなく、そのため、脅威が実際にどのようなものであるかというイメージが湧きにくいという実情もあろう。

そこで、本稿では、金融機関のサイバーセキュリティに対する脅威のイメージをつかみ、そのリスクを理解するため、公表情報を収集し、日本を含む世界の金融機関において実際に確認されたサイバー攻撃事案等を整理する。

また、SWIFT[2)]ネットワークをはじめとする銀行間決済システムが悪用された不正送金事案が多数確認されている状況を踏まえ、SWIFT が行っている取組みについても説明する。この取組みの中で SWIFT が SWIFT ネットワーク利用組織に対して実施を求めている対策は、SWIFT に関連しないシステムのセキュリティを確保する上でも参考にできる内容が多く、それを理解することは SWIFT ネットワークを利用していない金融機関にとっても有益であろう。

キーワード：サイバーセキュリティ、サイバー攻撃、SWIFT、不正送金、暗号資産

[1)] 金融庁金融研究センター研究官。本稿は筆者の個人的見解であり、金融庁および金融研究センターの公式見解ではない。

[2)] Society for Worldwide Interbank Financial Telecommunication の略で、国際金融取引を行うためのネットワークシステム等を提供する組織。日本語では「国際銀行間通信協会」などと訳される。提供するネットワークシステム等そのものを指す場合もある。本稿では便宜上、組織を指す場合は「SWIFT」と表記し、提供するネットワークシステムを指す場合は「SWIFT ネットワーク」と表記する。SWIFT ネットワークは国際金融取引を行う上でのデファクトスタンダードのような位置付けにあり、近年は新技術を活用したより利便性の高いシステムの研究・開発が行われているものの、依然として世界中の金融機関等で利用されている。

目次

１．はじめに

近年、サイバーセキュリティに対する脅威がますます増大していると言われている。

国内では、日本政府が、2020 年の東京オリンピック・パラリンピック競技大会等の重要イベントに向けて取組みを加速させている。

国際的には、選挙への介入をはじめとする国家によるサイバー攻撃、一部の通信機器の安全性、欧州の GDPR（General Data Protection Regulation、一般データ保護規則）をはじめとする各国・地域の規制強化等が話題になっており、各政府による活発な動きが見られている。

個別のサイバーセキュリティ事案に目を向けると、2018 年には、海外の大手 SNS や大手ホテルチェーンからの大量の情報漏洩があり、国内では複数の暗号資産交換所[3)]から多額の暗号資産が流出した。2019 年に入ってからも、海外の大手金属メーカーがランサムウェア[4)]に感染し業務影響が生じた事案や、大手パソコンメーカーへのサプライチェーン攻撃[5)]によりユーザーへマルウェア[6)]が配布された事案が発生し、国内ではファイル転送サービスや大手自動車販売店からの百万件単位の情報漏洩（漏洩懸念含む）が明らかになっている。

このような状況の中、金融庁では、2015 年 7 月に策定した「金融分野におけるサイバーセキュリティ強化に向けた取組方針」を 2018 年 10 月にアップデートし[7)]、2020 年の東京オリンピック・パラリンピック競技大会やデジタライゼーションの進展等を踏まえつつ、中小金融機関の底上げや大手金融機関の一層の高度化に向けた取組みを進めている。

金融業界における足もとの動きの 1 つとしては、サイバーリスクを経営上のトップリスクの 1 つとして明確に位置付ける金融機関が増えてきたことが挙げられる。2019 年 3 月に一般社団法人日本経済団体連合会（以下、「経団連」という）が「経団連サイバーセキュリティ経営宣言[8)]」を公表して以降、大手銀行グループが相次いで「サイバーセキュリティ経営宣言」を策定し、経営課題としての認識を明確にした。2019 年 4 月に行われた米国議会の公聴会においても、

---

3) 暗号資産交換業者名とその提供するサービス（一般的に「取引所」や「販売所」と言われているもの）名が異なる場合があるが、本稿ではより一般的に使用されている後者の名称を使用することとし、それらを「暗号資産交換所」と表記する。

4) 身代金を要求するマルウェア（「マルウェア」については脚注 6 参照）。英語表記は「ransomware」で、「ransom（身代金）」と「software（ソフトウェア）」を組み合わせた造語。

5) 標的を直接攻撃するのではなく、標的の属するサプライチェーンを利用して行う攻撃の総称。広義と狭義の 2 通りの意味があり、広義には、標的の取引先等を攻撃し、そこを足掛かりにして標的を狙う攻撃、狭義には、標的の使用しているソフトウェア等の製品の製造元を攻撃してマルウェア等を仕込み、その製品を標的に使用させることでマルウェアに感染させるなどの攻撃を意味する。ここでは後者の意味で使用している。

6) 悪意あるソフトウェア。英語表記は「malware」で、「malicious（悪意ある）」と「software（ソフトウェア）」を組み合わせた造語。

7) https://www.fsa.go.jp/news/30/20181019-cyber.html

8) 経団連が取り組むアクションプランを掲げたもの。取り組むべき項目を下記の 5 つに分けて示している。
1. 経営課題としての認識
2. 経営方針の策定と意思表明
3. 社内外体制の構築・対策の実施
4. 対策を講じた製品・システムやサービスの社会への普及
5. 安心・安全なエコシステムの構築への貢献
(http://www.keidanren.or.jp/journal/times/2018/0322_02.html)

米国大手金融機関の CEO が「サイバーセキュリティは世界の金融システムにとって最大のリスクである」と証言するなど、サイバーリスクがトップリスクであるということはもはや世界中の金融機関の共通認識になりつつある。

このように、サイバーセキュリティに対する脅威が増大し、サイバーリスクの重要性が高まっていることは疑いようのない事実であるものの、他方、近年の金融機関のサイバーセキュリティに対する脅威については、国内で発生した大規模な暗号資産交換業者へのサイバー攻撃が広く報じられたものの、公になっている事案は決して多くなく、詳細までは公表されないケースも多いため、実際に脅威がどのようなものであるか、なかなかイメージしにくいという実情もあろうかと思われる。

そこで、本稿では、金融機関のサイバーセキュリティに対する脅威のイメージをつかみ、そのリスクを理解するため、国内外の一般メディア・専門メディア・セキュリティベンダーのレポート等から収集した、金融機関を標的としたサイバー攻撃等に関する情報を整理する。

また、SWIFT ネットワークをはじめとする銀行間決済システムが悪用された不正送金事案が多数確認されている状況を踏まえ、そのようなサイバー攻撃への対策の考え方の一例として、SWIFT が行っている取組みについても説明する。

２．金融機関を標的としたサイバー攻撃事案等

本章では、筆者が国内外の一般メディア・専門メディア・セキュリティベンダーのレポート等から収集した金融機関を標的としたサイバー攻撃等に関する情報[9)]を整理する[10)]。対象は、筆者が金融庁でサイバーセキュリティ関連業務に従事し始めた 2017 年 10 月から 2019 年 5 月までに公表された情報とする。

まずは、２．１節において、収集したサイバー攻撃事案等の情報を一覧化する。その後、２．２節以降で、一覧表に挙げた事案のうち、攻撃手口等の情報が相応に公表されている事案について、それらの内容を詳述する[11)]。なお、当然のことながら、本章に記載したサイバー攻撃事案等は、世界中の金融機関で発生したサイバー攻撃事案等を網羅しているわけではなく、あくまで氷山の一角に過ぎない。また、公表情報のみを情報源としたため、詳述と言いながらも、内容が断片的である場合がある。

---

9) 海外情報については、原則として英語で公表されている情報を収集した。なお、本稿の対象は特定の金融機関が標的となった事案等（一部、サイバー攻撃ではないサイバーセキュリティ事案も含む）とし、金融機関の顧客や特定の暗号資産等が標的となった事案（金融機関を装った個人へのフィッシング（脚注 29 参照）、個人の暗号資産ウォレットからの不正流出、暗号資産へのいわゆる「51%攻撃」等）は対象外とした。また、具体的な金融機関名や被害状況が明らかでない情報（セキュリティベンダーが公表する被害が顕在化していない攻撃情報等）や、金融機関との関連が不明瞭な情報（特定のデータベース上で特定の金融機関の顧客のものとみられる情報が公開されていた等）についても対象外とした。

10) 原文は英語等の外国語が多いため、本稿では適宜日本語に仮訳しているが、その正確性を保証するものではない。原文については参考文献あるいは表１中の「主な公表情報」を参照のこと。３章の内容についても同様。

11) 対象期間中に発生した大規模事案の１つとして日本の Coincheck 事案があるが、攻撃手口を含め国内の一般メディアで広く報じられており、改めて本稿で詳述する必要はないと考えるため、詳述しない。

２．１　サイバー攻撃事案等一覧

表 1　金融機関を標的としたサイバー攻撃事案等一覧

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
1	2017 年 10 月	遠東國際商業銀行	台湾	銀行	SWIFT ネットワークが悪用された不正送金	約 6,000 万米ドル（約 67 億円[15]） （うち約 5,950 万米ドルは回収済）	参考文献参照	２．２節
2	2017 年 10 月	NIC Asia Bank	ネパール	銀行	SWIFT ネットワークが悪用された不正送金	約 4 億 5,000 万ルピー（約 5 億円） （うち約 4 億ルピーは回収済）	参考文献参照	２．３節
3	2017 年 11 月	上光証券（現北洋証券）	日本	金融商品取引業者	情報漏洩（攻撃手口非公開）	83 名分の顧客情報（名前、住所、電話番号、メールアドレス）	https://www.hokuyo-sec.co.jp/notice/news/pdf/apology20171120.pdf	-
4	2017 年 12 月	TIO Networks（PayPal 子会社）	カナダ	資金移動業者	情報漏洩（攻撃手口不明）	約 160 万人分の顧客情報（名前、連絡先、口座番号、社会保障番号、ユーザー名、パスワード等）	https://www.bleepingcomputer.com/news/security/paypal-says-1-6-million-customer-details-stolen-in-breach-at-canadian-subsidiary/	-

12) 筆者が確認した情報の中で最も早く公開された情報の公開月。表中の「主な公表情報」に記載した情報の公開月とは必ずしも一致しない。
13) 詳述しない事案については、複数ある情報のうち、基本的に情報量が最も多いと思われるものを記載した。
14) 原則として金融庁の定義に便宜的に当てはめたが、海外の金融機関については相応しくない可能性がある。「暗号資産交換所」、「中央銀行」等、金融庁の定義に沿わない名称も一部使用している。
15) 「公表／報道月」当時のレートによる。以降も同様。

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
5	2017年12月[16]	アメリカの15の銀行・信用組合[17]	アメリカ	銀行、信用組合	デビットカード等の処理システムが悪用されたATMからの不正出金	平均約50万米ドル（約5,600万円）	参考文献参照	2．4節
		ロシアの銀行3行[17]	ロシア	銀行	ロシア国内の銀行間決済システムが悪用された不正送金	平均約120万米ドル（約1.3億円）		
6	2017年12月	Bitfinex	香港	暗号資産交換所	DDoS攻撃[18]によるサービス利用不可（複数回発生）	12/7に約3時間、12/12～13に約12時間	https://www.hackread.com/bitfinex-cryptocurrency-exchange-hit-by-ddos-attacks/	-
7	2017年12月	Youbit[19]	韓国	暗号資産交換所	ホットウォレット[20]からの不正送金	約170億ウォン（約19億円）相当の暗号資産	参考文献参照	2．5節
8	2017年12月	東海日動パートナーズ中国四国（東京海上日動火災保険子会社の保険代理店）	日本	保険会社	利用していたメールサービスへの不正アクセスによる情報漏洩	約5,400人分の顧客情報（名前、住所、電話番号、メールアドレス、生年月日、性別、証券番号、車のナンバー、銀行口座情報、健康情報）	https://tnp-cs.com/news/info/224/	-

16) これらの各事案は2016年5月から2017年11月まで断続的に発生。同一の攻撃者グループによるものとされているため、まとめて記載している。
17) 個別の金融機関名は不明。
18) Distributed Denial of Service attackの略で、分散した大量のコンピュータから一斉にアクセスすることなどにより処理能力以上の負荷をかけ、標的のサービスを正常に提供できないようにする攻撃。日本語では「分散型サービス妨害攻撃」と訳される場合がある。DoS攻撃（脚注26参照）の一種。
19) サイバー攻撃が発生した2017年12月当時の名称。
20) インターネットに接続された状態のウォレット。インターネットに接続されているため、外部からのサイバー攻撃にさらされやすい。これに対し、インターネットに接続されていない状態のウォレットのことを「コールドウォレット」という。

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
9	2017 年 12 月	Globex bank	ロシア	銀行	SWIFT ネットワークが悪用された不正送金	約 5,500 万ルーブル（約 94 万米ドル、約 1 億円）（一部は阻止し、被害を約 10 万米ドルに抑えた）	https://www.reuters.com/article/us-russia-cyber-globex/russias-globex-bank-says-hackers-targeted-its-swift-computers-idUSKBN1EF294?feedType=RSS&feedName=technologyNews	-
10	2018 年 1 月	Zaif	日本	暗号資産交換所	利用者口座への不正アクセスによる不正出金、不正取引（攻撃手口非公開）	不正出金 37 件、不正取引 137 件（金額非公開）	https://corp.zaif.jp/info/8265/	-
11	2018 年 1 月	Bancomext	メキシコ	銀行	SWIFT ネットワークが悪用された不正送金	約 1 億 1,000 万米ドル（約 112 億円）（送金先銀行の始業前に全額回収し、最終的には被害無し）	https://www.zerohedge.com/news/2018-05-29/mexican-bank-foils-110-million-cyberheist	-
12	2018 年 1 月	Coincheck	日本	暗号資産交換所	取引所システムへの不正アクセスによる不正送金	約 580 億円相当の暗号資産	https://corporate.coincheck.com/2018/03/08/46.html	-
13	2018 年 1 月	ABN AMRO、ING Bank、Rabobank	オランダ	銀行	DDoS 攻撃によるオンラインサービス利用不可	約 3 時間～1 日半[21]	参考文献参照	2．6 節

[21] ABN AMRO はニュースリリースで正確な時間を公表。ING Bank および Rabobank は正確な時間の公表がなかったため、それぞれの公式 Twitter への障害連絡の投稿時刻から推定（障害発生連絡の投稿時刻から障害復旧連絡の投稿時刻までの時間とした）。詳細は２．６節を参照のこと。

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
14	2018 年 2 月	Bitgrail	イタリア	暗号資産交換所	不正送金（攻撃手口不明）	約 200 億円相当の暗号資産	https://medium.com/@bitgrailvictims/the-bitgrail-exchange-ruling-a-win-for-cryptocurrency-exchange-users-50df6c383571	-
15	2018 年 2 月	Punjab National Bank	インド	銀行	顧客と内部犯行者の共謀により SWIFT ネットワークが悪用された不正融資	約 21 億米ドル（約 2,268 億円）	参考文献参照	2．7節
16	2018 年 2 月	ロシアの銀行[22]	ロシア	銀行	SWIFT ネットワークが悪用された不正送金	約 3 億 3,950 万ルーブル（約 6.5 億円）	https://www.reuters.com/article/us-russia-cyber-swift/hackers-stole-6-million-in-attack-on-swift-system-russian-central-bank-says-idUSKCN1G00DV	-
17	2018 年 2 月	City Union Bank	インド	銀行	SWIFT ネットワークが悪用された不正送金	150 万米ドル、30 万ユーロ（合計約 2.1 億円） （うち少なくとも 50 万米ドル、30 万ユーロは回収済）	https://www.reuters.com/article/us-city-union-bank-swift/indias-city-union-bank-ceo-says-suffered-cyber-hack-via-swift-system-idUSKCN1G20AF	-
18	2018 年 3 月	Bank Negara Malaysia	マレーシア	中央銀行	SWIFT ネットワークが悪用された不正送金	不明 （不正送金は全て阻止し、最終的には被害無し）	http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4651&lang=en	-

[22] 個別の金融機関名は不明。2017 年中に発生した 1 件のサイバー攻撃事案に関する情報としてロシア中央銀行が公表したもの。

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
19	2018 年 4 月	Coinsecure	インド	暗号資産交換所	不正送金（攻撃手口不明）	約 300 万米ドル（約 3.2 億円）相当の暗号資産	https://www.reuters.com/article/us-crypto-currencies-india/indias-coinsecure-exchange-says-3-million-worth-of-bitcoins-stolen-	-
20	2018 年 4～5 月	Banorte を含む 5 行	メキシコ	銀行	メキシコ国内の銀行間決済システムが悪用された不正送金	約 3 億ペソ（約 17 億円）	参考文献参照	2．8節
21	2018 年 5 月	Banco de Chile	チリ	銀行	SWIFT ネットワークが悪用された不正送金およびワイパー型マルウェア[23]感染によるデータ破壊	・不正送金：約 1,000 万米ドル（約 11 億円） ・システム停止：テレフォンバンキング等の一部サービス	https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075	-
22	2018 年 5 月	Rabobank、ABN AMRO	オランダ	銀行	DDoS 攻撃によるオンラインサービス利用不可	約 6～9 時間[24]	https://nltimes.nl/2018/05/28/ddos-attacks-target-dutch-banks	-

[23] データを破壊するマルウェア（「マルウェア」については脚注 6 参照）。語源は英語の「wipe（(コンピュータ等からデータ等を）消す)」。ランサムウェア（脚注 4 参照）がデータを暗号化し、復号化の対価として金銭を要求するのに対し、ワイパー型マルウェアはデータを破壊するため、復号化できない。
[24] それぞれの公式 Twitter への障害連絡の投稿時刻から推定（障害発生連絡の投稿時刻から障害復旧連絡の投稿時刻までの時間とした）。

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
23	2018 年 5 月	Bank of Montreal、Simplii Financial（Canadian Imperial Bank of Commerce 子会社）	カナダ	銀行	マイページへの不正ログインによる情報漏洩および身代金要求	・Bank of Montreal：約 5 万人分の顧客情報（個人情報、口座情報） ・Simplii Financial：約 4 万人分の顧客情報（個人情報、口座情報）	参考文献参照	2．9節
24	2018 年 6 月	Bitfinex	香港	暗号資産交換所	DDoS 攻撃によるサービス利用不可	約 3 時間	https://www.cnbc.com/2018/06/05/cryptocurrency-exchange-bitfinex-briefly-halts-trading-after-cyber-attack.html	-
25	2018 年 6 月	Coinrail	韓国	暗号資産交換所	不正送金（攻撃手口不明）	約 400 億ウォン（約 40 億円）相当の暗号資産	https://www.hackread.com/bitcoin-falls-korean-exchange-hack-attack/	-
26	2018 年 6 月	Instinet Europe Limited（野村ホールディングス子会社である Instinet Incorporated（米）の子会社）	イギリス	金融商品取引業者	不正アクセスによる顧客情報漏洩（攻撃手口非公開）	非公開	https://www.nomuraholdings.com/jp/news/nr/holdings/20180614/20180614.pdf	-

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
27	2018 年 6 月	Liberty	南アフリカ	保険会社	メールシステムへの不正アクセスによる顧客情報漏洩	不明	https://www.businesslive.co.za/fm/fm-fox/2018-06-21-liberty-hack-the-biggest-breach-yet/	-
28	2018 年 6 月	Bithumb	韓国	暗号資産交換所	不正送金（攻撃手口不明）	約 350 億ウォン（約 35 億円）相当の暗号資産（当社は後に被害額を約 190 億ウォンへ引下げ）	https://jp.cointelegraph.com/news/bithumb-details-still-sketchy-after-30-mln-hack	-
29	2018 年 7 月	Bancor	イスラエル	暗号資産交換所	不正送金（攻撃手口不明）	約 2,350 万米ドル（約 26 億円）相当の暗号資産（うち 1,000 万米ドル相当は即座に回収済）	https://japan.cnet.com/article/35122471/	-
30	2018 年 7 月	PIR Bank	ロシア	銀行	ロシア国内の銀行間決済システムが悪用された不正送金	100 万米ドル（約 1.1 億円）程度（少なくとも約 92 万米ドル）	参考文献参照	２．１０節
31	2018 年 7 月[25]	The National Bank of Blacksburg	アメリカ	銀行	デビットカード処理システムや勘定系システムが悪用された不正出金	約 240 万米ドル（約 2.6 億円）	https://krebsonsecurity.com/2018/07/hackers-breached-virginia-bank-twice-in-eight-months-stole-2-4m/	-

[25] 事案発生は 2016 年 5 月と 2017 年 1 月の 2 回。被害額は 2 回分の合計額。

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
32	2018 年 8 月	Krungthai Bank、Kasikornbank	タイ	銀行	情報漏洩（攻撃手口不明）	・Krungthai Bank：約 12 万人分の顧客情報（オンラインでローン申請を行った顧客の情報） ・Kasikornbank：約 3,000 社分の顧客情報（保証状取引のある法人顧客の名前、電話番号）	https://www.bangkokpost.com/news/security/1513410/kbank-ktb-targeted-in-cyber-attacks	-
33	2018 年 8 月	Cosmos Cooperative Bank	インド	銀行	デビットカード決済システムが悪用された ATM からの不正出金および SWIFT ネットワークが悪用された不正送金	約 9 億 4,400 万ルピー（約 15 億円）	参考文献参照	２．１１節
34	2018 年 8 月	Banco de España	スペイン	中央銀行	DoS 攻撃[26]によるウェブサイトアクセス不可	丸 1 日以上（日曜日に攻撃が開始し、月曜日は 1 日中利用不可）	https://www.bankinfosecurity.com/bank-spain-hit-by-ddos-attack-a-11430	-
35	2018 年 8 月	Banco del Estado de Chile（BancoEstado）	チリ	銀行	顧客情報漏洩（複数回発生、攻撃手口不明）	合計約 25 万人分の顧客情報	https://www.chiletoday.cl/two-hacks-in-two-days-at-bancoestado/	-
36	2018 年 9 月	Zaif	日本	暗号資産交換所	不正送金（攻撃手口非公開）	約 70 億円相当の暗号資産	https://prtimes.jp/main/html/rd/p/000000094.000012906.html	-

[26] Denial of Service attack の略で、標的のサービスを正常に提供できないようにする攻撃。処理能力を上回る負荷をかける「フラッド型」と、システムの脆弱性を悪用する「脆弱性型」がある。日本語では「サービス妨害攻撃」と訳される場合がある。

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
37	2018 年 9 月	福島信用金庫	日本	信用金庫	訪問者への詐欺行為を行う不正画面が表示されるようにウェブサイトが改ざん	確認されていない	https://www.nikkei.com/article/DGXMZO360588840T01C18A0000000/	-
38	2018 年 10 月	State Bank of Mauritius India	インド	銀行	SWIFT ネットワークが悪用された不正送金	約 14 億 7,000 万ルピー（約 23 億円） （うち大半が回収済で、実際の被害額は約 1 億 9,000 万ルピー）	https://mumbaimirror.indiatimes.com/mumbai/crime/fraudsters-duped-sbm-by-hacking-swift-system-cops/articleshow/66189808.cms	-
39	2018 年 11 月	HSBC Bank USA	アメリカ	銀行	クレデンシャルスタッフィング攻撃[27]による顧客情報漏洩	当行のアメリカ顧客の 1%（推定約 1 万 4,000 人）未満の顧客情報（名前、住所、電話番号、メールアドレス、生年月日、口座番号、口座種類、口座残高、取引履歴、支払先口座情報、取引明細）	https://oag.ca.gov/system/files/Res%20102923%20PIB%20MAIN%20v3_1.pdf	-
40	2018 年 12 月	PayPay	日本	前払式支払手段発行者	漏洩したクレジットカード情報を悪用した不正利用	不明	https://piyolog.hatenadiary.jp/entry/20181218/1545164396	-

[27] 漏洩したユーザーアカウントの認証情報を利用し、オンラインサービスに対して自動的にログインを試行する攻撃。英語表記は「credential stuffing attack」で、直訳は「認証情報詰込み攻撃」。いわゆる「リスト型攻撃」を自動化した攻撃。

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
41	2019 年 1 月	Cryptopia	ニュージーランド	暗号資産交換所	7 万 6,000 以上のウォレットへの不正アクセスによる不正送金	約 1,600 万米ドル（約 17 億円）相当の暗号資産	https://jp.cointelegraph.com/news/new-analysis-suggests-16-million-in-crypto-stolen-in-cryptopia-hack	-
42	2019 年 1 月	Redbanc	チリ	銀行間 ATM ネットワーク	業務用パソコンへのマルウェア感染	被害無し（被害発生前に検知）	参考文献参照	２．１２節
43	2019 年 1 月	Cryptopia	ニュージーランド	暗号資産交換所	約 1 万 7000 のウォレットへの不正アクセスによる不正送金	約 18 万米ドル（約 2,000 万円）相当の暗号資産	https://jp.cointelegraph.com/news/report-new-zealand-cryptopia-exchange-hack-continues	-
44	2019 年 1 月	Metro Bank	イギリス	銀行	電話網の通信プロトコルの脆弱性[28]を悪用した SMS 傍受により認証を突破され不正送金	不明（最終的には被害無し）	https://www.vice.com/en_us/article/mbzvxv/criminals-hackers-ss7-uk-banks-metro-bank	-

[28] 「SS7」あるいは「共通線信号 No.7」と呼ばれる通信プロトコルに存在し、トラフィックが暗号化されず、正規のコマンドと不正なコマンドの判別ができず、発信元に関係なく全てのコマンドが処理されてしまうという脆弱性。

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
45	2019 年 1 月	State Bank of India	インド	銀行	保護されてない状態で顧客情報が保存されており大量の顧客情報へのアクセスが可能	「SBI Quick サービス（SMS 等のテキストメッセージによる取引情報取得サービス）」利用者数百万人へ送信された、電話番号、口座残高、取引履歴等を含む過去２ヵ月分のテキストメッセージ	https://techcrunch.com/2019/01/30/state-bank-india-data-leak/	-
46	2019 年 2 月	Bank of Valletta	マルタ	銀行	（おそらく SWIFT ネットワークが悪用された）不正送金	約 1,300 万ユーロ（約 16 億円）（うち約 1,000 万ユーロは回収済）	参考文献参照	２．１３節
47	2019 年 2 月	CI Banco	メキシコ	銀行	ランサムウェアへの感染	約 1 日半の間、国内の銀行間決済システムから切断され、取引が制限	https://expansion.mx/empresas/2019/02/14/ci-banco-restablece-operaciones-tras-el-ciberataque	-
48	2019 年 3 月	DragonEX	シンガポール	暗号資産交換所	顧客のウォレットおよび交換所自らのウォレットへの攻撃による不正送金	約 700 万米ドル（約 7.7 億円）相当の暗号資産（20 種類）	https://cryptogo.jp/news/hacking-damage-at_dragonex-and-biki-com/	-
49	2019 年 3 月	BiKi.com	シンガポール	暗号資産交換所	顧客アカウント情報およびパスワードの改ざん	一部顧客（詳細不明）	https://cryptogo.jp/news/hacking-damage-at_dragonex-and-biki-com/	-
50	2019 年 4 月	Bithumb	韓国	暗号資産交換所	内部犯行者のハッキングによる不正送金	約 21 億円相当の暗号資産	https://coinpost.jp/?p=77358	-

#	公表／報道月[12]	サイバー攻撃事案等が発生した金融機関			概要	具体的な被害	主な公表情報[13]	本稿での詳述
		名称	国／地域	業態[14]				
51	2019 年 5 月	Binance	マルタ	暗号資産交換所	フィッシング[29]やマルウェア等の攻撃によるホットウォレットからの不正送金	約 44 億円相当の暗号資産	https://jp.cointelegraph.com/news/binance-discovered-a-large-scale-security-breach	-
52	2019 年 5 月	First American Financial	アメリカ	保険会社	システム設計の不備により大量の顧客情報がウェブサイト上で閲覧可能	顧客情報（銀行口座番号、銀行取引明細、送金領収書、社会保障番号、運転免許証、ローン情報、納税情報等）の記載された約 8 億 8500 万件の文書ファイル	https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/	-

（資料）各事案に関する公表情報（参考文献あるいは表中の「主な公表情報」参照）より作成

[29] 利用価値のある個人情報（銀行口座情報やクレジットカード情報等）を盗むためにインターネット上で行われる詐欺行為。金融機関等を装った偽サイト（フィッシングサイト）を用意して標的をそのサイトへ誘導し、盗みたい情報を入力させる手口が一般的。

２．２　遠東國際商業銀行（台湾）の事案

〈事象〉

2017 年 10 月 3 日（火）、台湾の遠東國際商業銀行において、SWIFT ネットワークが悪用され、7 件の不正な送金指示により、約 6,000 万米ドル（約 67 億円）がカンボジア、スリランカ、アメリカの銀行へ送金されたことが判明。

なお、その後の各国の警察当局等の協力により、カンボジアへ送金された約 5,700 万米ドル、アメリカへの約 100 万米ドル、スリランカへの約 160 万米ドルについては回収されている。

〈攻撃手口〉

攻撃の流れは以下の通り。

① バックドア[30]が仕込まれた添付ファイルとオンライン上の PDF ファイルへのリンクが付いたメールをある支店の行員へ送信する。
② 行員が添付ファイルを開くと業務用パソコンがマルウェアに感染し、外部からの遠隔操作が可能となる。
③ ウイルス対策機能を停止させる。
④ ネットワーク内を探索し、特権アカウント[31]情報を窃取する。
⑤ 窃取した特権アカウントにより、SWIFT 取引システム[32]へ侵入する。
⑥ 正規の送金電文を解読し、その電文上の取引金額と送金先口座の情報のみを書き換え、不正な送金電文を複数作成する。
⑦ 不正な送金電文を SWIFT ネットワーク経由で発信し、不正送金を実行する。
⑧ システムをランサムウェアに感染させ、侵入の痕跡や不正送金の取引記録を暗号化する。そのほかにも、このランサムウェアは、本来の目的である不正送金を隠す役割も果たした。

〈攻撃者〉

不正送金先の口座の一部や使用されたマルウェアが過去に使用されたものと一致したことから、2016 年 2 月のバングラデシュ中央銀行における不正送金事案[33]（以下、「バングラデシュ

---

30) 正規の手順を踏まずにシステム内部へ侵入できる裏口。

31) 一般ユーザーには与えられていない特別な権限を付与されたアカウント。本稿では管理者権限を付与された「管理者アカウント」と特に区別しない。

32) SWIFT ネットワークへ接続し SWIFT ネットワーク経由の取引を行うための当行のシステム。SWIFT が提供する SWIFT ネットワークではなく、あくまで SWIFT ネットワークを利用する組織側に管理責任がある。SWIFT ネットワークと区別するため、本稿ではこのように表記する。

33) 2016 年 2 月、バングラデシュ中央銀行がサイバー攻撃を受け、SWIFT ネットワーク経由で不正な送金電文が送信され、フィリピンの銀行へ約 8,100 万米ドルが不正に送金された事案。金融機関に対するサイバー攻撃事案の代表例として言及されることが多く、本章記載の事案も含め、その後も類似事案が多数明らかになっている。攻撃は特定の国家の支援を受けるサイバー攻撃者グループによるものとされている。攻撃の流れは以下の通り。

① 行員へメールによる攻撃を仕掛ける。
② 銀行ネットワークにマルウェアが感染し、外部からの遠隔操作が可能となる。
③ ネットワーク内を探索し、特権アカウント等を窃取する。
④ SWIFT 取引システムにもマルウェアを感染させる。
⑤ SWIFT 取引用の認証情報を窃取する。

※次頁へつづく

中銀事案」という）と同じ攻撃者グループによるものではないかとの見方がある。

〈攻撃が成功した要因〉

台湾の金融当局は、当行のシステム管理体制の不備を 2 点指摘した。

1 点目は、一般職員にも特権アカウントが付与されていたため、一般職員から特権アカウントと認証情報が窃取されてしまったことである。アカウント情報が盗まれた際の被害を最小限に抑えるため、業務上必要となる最小限の権限のみを付与することは基本的なセキュリティ対策の 1 つであるが、当行ではこの対策が行われていなかった。

2 点目は、SWIFT 取引システムがその他のシステムと物理的に隔離されておらず、業務上の利便性のために接続されていたことで、メールによって当行のシステムへ侵入した攻撃者がネットワーク内を移動し、最終的に SWIFT 取引システムにまで侵入されてしまったことである。バングラデシュ中銀事案を受け、台湾の金融当局は同年 9 月、所管の銀行に対し、SWIFT 取引システムを他のシステムから物理的に隔離することを求めていたにも関わらず、当行では物理的に隔離していなかった。

２．３　NIC Asia Bank（ネパール）の事案

〈事象〉

2017 年 10 月 19 日（木）、ネパールの NIC Asia Bank において、SWIFT ネットワークが悪用され、31 件の不正な送金指示により、約 4 億 5,000 万ルピー（約 5.0 億円）が中国（香港含む）、日本、マレーシア、シンガポール、トルコ、アメリカ、イギリス、ドイツ等の銀行へ送金されたことが判明。

なお、その後の各国当局等の協力により、約 4 億ルピーについては回収されている。

〈攻撃手口〉

攻撃の流れは以下の通り。

① 行員へ攻撃を仕掛ける。
② 行員の業務用パソコン（SWIFT 取引とその他の業務の兼用）がマルウェアに感染し、外部からの遠隔操作が可能となる。
③ 特権アカウント情報を窃取する。
④ 不正な送金電文を SWIFT ネットワーク経由で発信し、不正送金を実行する。

このとき、④は 5 日間の祝日期間中に行われており、これは検知や対応を遅らせるためだと考えられる。

なお、本事案との関係性は不明であるが、当行は不正送金が発生した前日に DoS 攻撃も受けていた。

〈攻撃者〉

手口の類似性から、バングラデシュ中銀事案と同じ攻撃者グループによるものではないかと

※前頁からのつづき
⑥ 不正な送金電文を SWIFT ネットワーク経由で発信し、不正送金を実行する。
⑦ 送金の痕跡の削除や残高の改ざんを行う。

の見方が一部にあるが、内部犯行の可能性も排除されていない。

〈攻撃が成功した要因〉

ネパール中央銀行は、SWIFT 取引端末でメールの確認ができてしまうという脆弱性を突かれたためと指摘している。当行自身は、SWIFT 取引システムと顧客情報や残高を管理する銀行の中核システムは異なると話しているものの、メールを含むその他の業務を行う行員のパソコンから SWIFT 取引システムへもアクセス可能だったものとみられる。

このほか、以下のように、当行のセキュリティ対策や体制面の不備が多数指摘されている。

- ネパールでは一般的に業務時間外は SWIFT 取引システムを停止させるにも関わらず、当行は起動したままであったこと。
- システムへのアクセスに通常の ID とパスワードしか使用されておらず、ワンタイムパスワード等の強度の高い認証方式が採用されていなかったこと。
- SWIFT 取引システムに遠隔操作機能が備わっており、アクセス経路が複数あったこと。
- 経営陣の中に IT 責任者がおらず、IT 部門が重要な意思決定に参加できていなかったこと。
- ネパールの銀行業界の慣習として、システムが監査対象になっておらず、対策が不十分であることを見抜けなかったこと。

また、本事案を受けて当行が行った唯一の事後改善策が、SWIFT 取引の運用を担っていた 6 名の担当者を異動させたことであったが、その運用チーム自体が元凶なのではなく、IT 部門長と副部門長という上位の役職が空席になっており、ノウハウの不十分な下位の役職者により運営されていたことが問題であるとの指摘もある。

２．４　アメリカ、ロシアの銀行等の事案

〈事象〉

2016 年 5 月から 2017 年 11 月にかけ、アメリカの 15 の銀行・信用組合とロシアの銀行 3 行において、クレジットカードやデビットカードの処理システム（以下、「カード処理システム」という）や国内の銀行間決済システムが悪用され、金銭が盗まれる事案が断続的に発生した。これらは全て同一の攻撃者グループによって行われたサイバー攻撃だとされている。

アメリカの 15 の銀行・信用組合の大半は地域銀行で、カード処理システムが悪用され、平均で約 50 万米ドル（約 5,600 万円）の被害が発生した。

ロシアでは、ロシア国内の銀行間決済システム（Automated Work Station Client of the Russian Central Bank、AWS CBR）[34]（以下、「AWS CBR」という）が悪用され、平均で 120 万米ドル（約 1.3 億円）の被害が発生した。

なお、金銭だけでなく、資金決済システムに関する文書も盗み出されており、この攻撃者グループが今後も資金決済システムを悪用したサイバー攻撃を仕掛ける可能性がある。

---

[34] ロシア中央銀行の運営する決済システム（日本の全国銀行データ通信システム（以下、「全銀システム」という）に相当するシステムだと思われる）へ接続し、取引を行うための各銀行のシステムだと思われる。

〈攻撃手口〉

攻撃の流れは以下の通り。

① 何らかの方法で銀行システムへ侵入する。
② 正規のペネトレーションテスト[35]ツール等を利用し、システム内部を探索する。
③ 内部システムの管理用コンピュータへのアクセス権を獲得する。
④ マルウェアの形跡を削除する。
⑤ システム内の偵察、脆弱なアプリケーションの探索、脆弱性の悪用、特権の昇格[36]等を行い、ドメイン[37]管理者権限を獲得し、ネットワークを支配する。
⑥ 銀行員の活動を監視し、不正取引の実行方法を習得する。

（カード処理システムを悪用する場合）

⑦ 正当な銀行口座を開設し、カードを作成する。
⑧ 当該口座の貸越限度額やクレジットカードの利用限度額の制限を解除する。
⑨ 出し子が ATM から出金する。

（AWS CBR を悪用する場合）

⑦ 送金処理の途中で、正当な送金指示電文の送金先を攻撃者グループの口座（送金 1 件毎に別の口座を用意）へ書き換えた上で送信することにより、不正送金を実行する。
⑧ 不正送金の処理結果通知を、不正に書き換える前の本来の送金指示電文に基づく内容へ書き換えることにより、検知されにくくする。
⑨ 出し子が ATM から出金する。

〈攻撃者〉

ロシア語を話す攻撃者グループであるとみられている。

〈攻撃から守るための推奨事項〉

本事案を分析したセキュリティベンダーは、外部からのログインの禁止、ユーザーへの必要最小限の権限付与、ソフトウェア等のタイムリーなアップデート、IDS（Intrusion Detection System、侵入検知システム）の導入等を推奨している。

２．５　Youbit 等の韓国の暗号資産交換所において 2017 年に発生した事案

〈事象〉

2017 年 12 月 19 日（火）、韓国の暗号資産交換所 Youbit において、取引資産の約 17%にあたる約 170 億ウォン（約 17 億円）相当の暗号資産が不正に送金されたことが判明。同交換所は同日、破産を申請した。

同交換所は 2017 年 4 月（当時の名称は「YAPIZON」）にも、当時の取引資産の約 37%にあたる約 55 億ウォン（約 5.5 億円）相当のビットコインを盗まれており、その際、顧客のビットコ

[35] 実際にシステムへの侵入を試みることでシステムの安全性を検証するテスト。「ペネトレーション（penetration）」は侵入の意。
[36] 本来は特権を持たないユーザーが一時的に特権を取得すること。
[37] ネットワーク上の複数のコンピュータからなる特定のグループ。

インを一律 37%減額する形で被害を顧客に転嫁し、議論を呼んだ。その後、当時の被害者へ毎月一定額を補償してきたが、まだ全額の補償は完了していなかった。

なお、韓国では 2017 年に暗号資産交換所へのサイバー攻撃が多数発生しており、Youbit（YAPIZON）の 2 件に加え、6 月には Bithumb から約 3 万 6,000 人分の情報が漏洩し、9 月には Coinis から約 21 億ウォン相当の暗号資産が盗まれたことが明らかになっている。

〈攻撃手口〉

各事案と手口が個々に紐付けられているわけではないものの、韓国の暗号資産交換所へのサイバー攻撃の手口としては、一般的に以下のような流れとされている。

① 暗号資産交換所の職員へメールを送信する。メールの内容は、交換所・金融機関・国家機関等を装ったものや、入社願書や採用募集を装ったもの、税金関連を装ったもの等が確認されている。

② 職員がメールの添付ファイルやリンクを開くと、その業務用パソコンがマルウェアに感染し、遠隔操作が可能となる。

③ 個々の攻撃目的に合わせた追加のマルウェアのダウンロード等を行い、特権アカウントや暗号資産口座の認証情報を窃取する。

④ それらの認証情報を利用し、ホットウォレットから不正送金を実行する。

〈攻撃者〉

Youbit（YAPIZON）、Bithumb 、Coinis の 4 事案について、韓国国家情報院は、特定の国家による攻撃であると断定している。また、複数のセキュリティベンダーも、各社が分析した 2017 年の一連の韓国暗号資産交換所への攻撃について、バングラデシュ中銀事案と同じ攻撃者グループによるものである可能性が高いとしている。

〈攻撃が成功した要因と攻撃から守るための推奨事項〉

一般的に、暗号資産交換所は小規模な業者が営んでいることが多く、多数の顧客情報や多額の暗号資産を保有しているにも関わらずセキュリティ水準が低いと言われており、攻撃者に狙われやすいと指摘されている。

これらの事案を分析したセキュリティベンダーは、ソーシャルエンジニアリング[38]や最新の脅威動向に関する研修の継続的な実施、サンドボックス[39]により添付ファイルやリンクが悪意あるものであるか否かを判別できる高度なマルウェア防御・検知ソリューションの導入、全ての主要システムへの二要素認証の実装等を推奨している。

２．６　ABN AMRO 、ING Bank、Rabobank（オランダ）の事案

〈事象〉

2018 年 1 月、オランダの ABN AMRO、ING Bank、Rabobank の 3 行が断続的に DDoS 攻撃を受け、

[38] システムへ侵入するための秘密情報を、情報通信技術を使わず、人の心理的な隙などにつけ込んで窃取する手法。

[39] 未確認のソフトウェア等が悪質な挙動を伴うものかどうかを実際に実行して確認するために使用する、外部へ影響を与えないよう隔離して構築された仮想環境。

ウェブサイトやインターネットバンキング等が利用不可となった。

ABN AMRO はニュースリリースにて、1 月 27 日（土）20 時から 28 日（日）0 時 15 分頃まで、および、28 日（日）12 時から 14 時頃までの間、ウェブサイトやインターネットバンキング等のサービスが利用不可であったと公表している。

ING Bank は当行公式 Twitter へ、28 日（日）22 時 08 分にオンラインバンキングが利用不可である旨、29 日（月）0 時 17 分に復旧した旨それぞれ投稿しており、また、1 月 30 日（火）にも、18 時 04 分にウェブサイトとアプリが利用不可である旨、18 時 48 分に復旧した旨それぞれ投稿している。

Rabobank は当行公式 Twitter へ、29 日（月）0 時 46 分にモバイルバンキングやインターネットバンキング等が利用不可である旨、30 日（火）14 時 14 分に復旧した旨それぞれ投稿している。

なお、同じタイミングで、オランダの政府機関も DDoS 攻撃を受けていた。

〈攻撃手口〉

逮捕された容疑者は、「stresser」と呼ばれる DDoS 攻撃製品をダークウェブ[40]上で購入、1 週間で 50 ユーロを支払い、50～100Gbps[41]のデータを送信した。

実際の攻撃は、「IoTroop[42]」というマルウェアに感染した IoT 端末により構成されたボットネット[43]から行われたとの見方がある。

〈攻撃者〉

容疑者として 18 歳のオランダ人の少年が逮捕されている。オランダでは本事案発生の数日前、ロシアのサイバー攻撃者グループによる米民主党へのサイバー攻撃に関する情報をオランダの諜報機関からアメリカに対し共有したことが広く報じられており、本事案発生当初は、それに反発したロシアによるサイバー攻撃だとの見方が多かった。

逮捕された少年とメディアとのやりとりから、少年はハッカーとして自身が認知され名声を博することを求めていたことが明らかになっている。サイバー攻撃を行った動機として、「僕が（サイバー攻撃を）行ったにもかかわらず、他の全員が狂ったようにロシアを非難するのを見るのがおもしろかった」と述べている。また、銀行を狙った動機としては、「銀行は適切なセキュリティ対策を実施しておくべきだからだ」と話している。

なお、この少年は本事案発生の約 4 ヵ月前にも、banq というオランダの銀行に対してサイバー攻撃を行っており、オランダ国内では既に名前が知られていた。

---

40) 一般的な検索サイトからは見つけることができず、専用の閲覧ソフトを使わなければアクセスできない、匿名性の高いウェブサイト。漏洩した個人情報やサイバー攻撃用のツール・サービス等が売買されている。

41) 「bps」は bit per second の略で、1 秒間に流れるビット数（データ量）を示す単位。

42) セキュリティベンダーCheck Point 社が 2017 年 10 月に発見した、IoT 端末に感染しボットネット化するマルウェア（「ボットネット」については脚注 43 参照）。それにより構築されたボットネットを意味する場合もある。同じく IoT 端末をボットネット化する「Mirai」よりも非常に早いペースで感染が広がっており、潜在的な危険性がより高いとみられている。

43) マルウェアに感染し悪意ある者に乗っ取られた多数のボットで構成されたネットワーク。「ボット（bot）」とはロボット（robot）の短縮形であり、本来は悪い意味は持たないが、サイバーセキュリティの文脈では、「マルウェアに感染し悪意ある者に乗っ取られたコンピュータ」の意味で使用されることが多い。

２．７　Punjab National Bank（インド）の事案

〈事象〉

インドのPunjab National Bankにおいて、共犯者である当行行員がSWIFTネットワークを悪用し、宝石商を営む首謀者の会社のダイヤモンドの原石輸入用資金の調達という名目で不正にLetter of Undertaking[44]（以下、「LoU」という）が発行され、首謀者の会社がそれに基づく不正な融資を受けた。2011年から2017年の7年間に、このような不正取引が少なくとも150件行われ、被害額は約21億米ドル（約2,268億円）に及んだ。

〈攻撃手口〉

明らかになっている攻撃の流れは以下の通り。

① 首謀者の経営する会社がダイヤモンドの原石輸入代金支払用の資金調達のためとしてLoUの発行を依頼する。

② 共犯者である当行の副マネージャーと担当者の2名は、基幹システムと連携していないSWIFT取引システムを悪用（担当者が取引内容を入力、副マネージャーが取引を承認）し、Axis Bank、Allahabad Bank、Union Bank of India（いずれもインド）の海外支店へLoUを不正に発行する。ここで、本来であれば、当該取引を基幹システムへもマニュアルで入力しなければならないところ、入力せず。そのため、帳簿には現れないまま、不正な取引が行われる。

③ 当行のLoUを受け、Axis Bank、Allahabad Bank、Union Bank of Indiaの海外支店が首謀者の会社に対し融資を実行する。

〈攻撃者〉

インドで宝石商を営む首謀者をはじめ、首謀者の会社の関係者や当行の行員など、多数が共犯者として逮捕されている。なお、首謀者は現在国外へ逃亡中である。

〈攻撃が成功した要因と攻撃から守るための推奨事項〉

インド国内の銀行関係者らは、攻撃が成功した要因として、当行の基幹システムがSWIFT取引システムとシステム的に連携しておらず、マニュアルによる入力が求められていたため、SWIFT取引システムとその他のシステムとの間で不整合がないかシステム的に検証することが不可能であったことを挙げている。

2016年のバングラデシュ中銀事案発覚後、インド中央銀行はインド国内の銀行に対し、自行の内部システムがSWIFT取引システムと正しく統合されていること確認すること、特に、基幹システムとSWIFT取引システムをシステム的に連携させることを指示していたにも関わらず、当行は資金移動を伴わない取引についてはシステム的に連携していなかった。インド国内の民

[44] ここでは、ある銀行（A銀行とする）の顧客が他の銀行（B銀行とする）の外国支店から現地通貨建ての短期資金調達を行えるよう、A銀行が発行する保証状のことをいう。顧客はその保証に基づいて資金調達を行い、現地の輸入元に対して代金を支払う。類似のものとしてLetter of Credit（信用状）があるが、信用状は発効日・有効期限・輸入商品等を詳細に規定した上で輸入者から輸出者への期限内の正しい代金支払いを銀行が保証するのに対し、このLoUはそのような詳細な条件まで規定しないため、悪用しやすかったと言われている。

間銀行は両システムをシステム的に連携させているものの、当行を含め、インドの国営銀行のほとんどは連携できていないと言われている。

ほかにも、SWIFT 取引に必要なパスワードが適切に管理されておらず、複数人の間で共有されていたことも問題視されている。

これら全体の背景として、そもそもインドの金融機関にはリスク、特にオペレーショナルリスクを管理する企業文化が欠如しているとの指摘がある。

システム専門家らは、年１回のシステム監査を行うことや、適切なガバナンスとリスク管理のための UEBA[45]等の新技術の活用を提案している。

２．８　メキシコの銀行５行の事案

〈事象〉

2018 年 4 月中旬から 5 月上旬にかけ、Banorte を含むメキシコの銀行 5 行において、メキシコ中央銀行が運営するメキシコ国内の銀行間電子決済システム（Interbanking Electronic Payment System、SPEI）[46]（以下、「SPEI」という）が悪用され、何百件もの不正な送金指示により合計約 3 億ペソ（約 17 億円）が他行へ送金された。その後、攻撃者グループは、即座に数十の支店から現金を引き出した。

〈攻撃手口〉

攻撃の流れは以下の通り。

① 当行システムのセキュリティの脆弱性を利用して当行内部のシステムへアクセスする、あるいは、行員への攻撃により彼らの認証情報を窃取し、その後の攻撃の足掛かりとする。

② 認証情報を窃取しながらシステムの内部深くまで侵入し、SPEI 取引システム[47]へアクセスする。

③ SPEI 取引システムの送金依頼者の妥当性チェック処理の不備を利用し、実際には存在しない架空口座を送金元に設定し、攻撃者グループの管理する偽名口座へ送金を実行する。このとき、毎日何百万件にも上る多数の送金や何百万ペソにも上る高額な送金が処理される SPEI の中で不正送金が目立たぬよう、1 件 1 件の送金金額は少額（数万から数十万ペソの範囲内）に抑える。

④ 当行が不正送金に検知する前に速やかに出し子が出金する。

なお、攻撃者グループが何百件もの不正送金を出金するためには、長期に渡り何百人もの出し子を雇い訓練する必要があり、相応の資金が必要になるが、出し子一人あたり 5,000 ペソ程度あれば十分であったとみられている。

---

[45] User and Entity Behavior Analytics の略で、ユーザーやエンドポイントなどの活動に見られる振る舞いを AI や機械学習のような技術を用いて継続的に分析すること（「エンドポイント」については脚注 57 参照）。これにより、不審な活動のリスクスコアやリスクが高いと分析した要因を可視化し、セキュリティ運用を支援する。

[46] 日本の全銀システムに相当するものだと思われる。

[47] SPEI へ接続し SPEI 経由の取引を行うための各銀行のシステム。SPEI システムそのものではなく、あくまで SPEI を利用する組織側に管理責任があることに留意。

〈攻撃が成功した要因〉

メキシコの金融機関のシステムのネットワーク構造および SPEI 取引のセキュリティ監視が、ずさんで安全ではなかったと指摘されている。指摘されている具体的な問題点は以下の通り。

- 多くのネットワークが強固なアクセス管理機能を備えていなかったため、侵害された行員の認証情報により多数のシステムへアクセスできてしまったこと。
- ネットワークが十分にセグメント化されておらず、最初の侵入さえできれば、その後はシステムの内部深くまで侵入できてしまい、SPEI 取引システムまでアクセスできてしまったこと。
- 銀行内部のネットワークを流れる取引データが必ずしも常に保護されておらず、取引の追跡やデータの操作ができてしまったこと。
- SPEI 取引システムに不備があり、適切な取引妥当性チェックが行われず、不正取引を見逃してしまったこと。

また、金融機関に限らず、メキシコ全体として、そもそもサイバー攻撃に関する知見や情報が十分に共有されていないことが大きな問題であり、あらゆる組織がより協力していく必要があるとの指摘もある。

なお、本事案を受け、メキシコ中央銀行は、SPEI へ接続するメキシコの銀行が最低限遵守すべきサイバーセキュリティスタンダードを確立させるため、資金決済に係る方針と管理の強化を行った。

２．９　Bank of Montreal、Simplii Financial（カナダ）の事案

〈事象〉

2018 年 5 月頃、カナダの銀行である Bank of Montreal、Simplii Financial（Canadian Imperial Bank of Commerce 子会社のネット銀行）において、ウェブサイトから顧客情報等を表示する各顧客専用のページ（いわゆるマイページ）へ不正ログインされ、それぞれ約 5 万人分、約 4 万人分の氏名・生年月日・住所・電話番号・口座番号・パスワード・秘密の質問と回答・社会保険番号・口座残高等の顧客情報が漏洩し、同月 27 日（日）、個人情報を盗んだ攻撃者グループから、盗んだ顧客情報を公開されたくなければ 100 万カナダドル（約 8,500 万円）相当のリップル[48)]を支払うよう脅迫を受けた。なお、2 行は本事案を受けて必要なセキュリティ対策等を行った上で、リップルの支払いは拒否した。

〈攻撃手口〉

判明している攻撃の全体の流れは以下の通り。

① 2018 年 1 月頃、Bank of Montreal のウェブサイトへの攻撃に成功。Bank of Montreal は侵害されたウェブサイトを修正したが、その後、再度攻撃に成功する。

② 2 月から 5 月にかけて、Bank of Montreal と Simplii Financial を装ったフィッシングサイトを設け、実在する顧客の口座情報を不正入手する。この情報は、銀行のウェブサ

48) 暗号資産の１つ。

イトの認証の仕組みを分析するためのテストデータとして使用したとみられる。なお、この時点では2行以外のカナダの銀行への攻撃に向けたフィッシングサイトも用意していた。

③　5月前半、Simplii Financialのウェブサイトへの攻撃に成功する。

④　5月27日（日）4時36分、攻撃者は2行へメールを送信し、ウェブサイトをハッキングし顧客情報を窃取したことを告げ、身代金を支払わなければ顧客情報を公開すると脅迫する。また、そのメールでは、ウェブサイトの認証に使用されるセッションクッキー[49]の弱点と、パスワードを忘れた顧客用のパスワードリセットページを悪用した攻撃手口についても説明していた。

ウェブサイトから顧客情報を盗んだ攻撃の詳細な手口については以下の通り。

i. 別途用意しておいたフィッシングサイト（上記②）から入手した実在する複数の口座番号を使用し、2行の口座番号の採番の仕組みを分析するとともに、クレジットカード番号や携帯電話等の各種識別番号が有効な番号であるかどうかを判別するためのアルゴリズム[50]を利用し、実在するであろうと考えられる口座番号の候補を大量に生成する。

ii. 生成した口座番号の候補を、パスワードを忘れた顧客向けのパスワードリセットページへ入力する。このとき、2行のパスワードリセットページでは、口座番号入力後に秘密の質問に回答する必要があったが、ウェブサイトが口座番号入力後に認証情報を含むクッキーを生成する仕組みになっていたため、このクッキーを利用し、本来は認証されたユーザーしかアクセスできない秘密の質問の変更ページへアクセスし、秘密の質問の回答を任意に変更する。

iii. 再度パスワードリセットページへアクセスし、口座番号とiiで変更した秘密の質問の回答を入力し、パスワードリセットを行う。これにより顧客の認証情報が揃い、ログインが可能となる。

iv. 実在する顧客になりすまし、2行のウェブサイトへログインし、顧客情報を窃取する。

v. iからivまでのプロセスを自動化し、顧客情報を効率的に窃取する。なお、Bank of

---

[49] セッション（session）IDを格納するクッキー（cookie）。
「セッション」とは、通信を開始し終了するまでの一連のやりとりの単位。訪問者がウェブサイトへアクセスし、一連の処理を行い、離脱するまでを1セッションと数える。
「クッキー」とは、ウェブサイト（ウェブサーバ）が訪問者（ウェブブラウザ）を識別するための情報。最初にウェブサーバが発行し、ウェブブラウザへと渡し、ウェブブラウザが次にウェブサイトへアクセスした際、そのクッキーをウェブサーバへ渡すことにより、ウェブサーバは訪問者を前回の訪問者と同じであると識別でき、訪問者は前回のアクセスの続きとしてアクセスできる。
例えば、マイページ等のログインした訪問者しかアクセスできないウェブサイトの場合、最初のログイン時に、ウェブサーバがその後の一連のセッションで使用するセッションIDを発行し、クッキーへ格納して（これが「セッションクッキー」）ウェブブラウザへと渡し、次に訪問者がマイページ内のコンテンツへアクセスする際、ウェブブラウザがそのセッションクッキーをウェブサーバへ渡すことで、ウェブサーバはその訪問者をログイン認証済の訪問者として識別でき、訪問者は都度ログイン認証を行わずともアクセスできる。
このように、クッキーはウェブサイト訪問者の利便性向上のために使用されるが、その中身を分析することにより訪問者のアクセス履歴等がわかることから、個人情報として扱う国もあり、近年、個人情報保護の観点から話題に上ることが多い。

[50] 特定の問題を解決するための計算方法や処理手順。

Montreal はこの段階で異常を検知し、パスワードリセットの回数に一定の制限をかけたものの、攻撃者はパスワードリセット回数を 1 つの IP アドレスあたり 2 回に抑えつつ、異なる 500 の IP アドレスから分散して行うことにより、この制限を回避した。

〈攻撃者〉

Bank of Montreal はカナダ国外からの攻撃だとの認識を示している。また、攻撃者からのメールの送信元はロシアを示唆するアドレスであったが、これは誤解させることを意図したものである可能性があり、本当にロシアに存在する攻撃者グループからの攻撃であったかどうかは不明。

〈攻撃から守るための推奨事項〉

本事案を分析したセキュリティベンダーは、以下のような対策を推奨している。

- システムを常時監視すること。
- ソフトウェアの定期的なアップデートおよびパッチ適用を行うこと。
- 多要素認証等によるログインプロセス強化、パスワードリセット後の一定の取引不可時間の設定、秘密の質問としてより細かく具体的な質問（例えば、「直近のクレジットカードの請求額は？」、「平均給与は？」、「(ローンを借りている場合、) ローン残高は？」など、顧客と銀行のみが知り得るような質問）の追加を行うこと。
- M&A 等の際、古いシステムを移行あるいは繋ぎ合わせて利用し続けるのではなく、セキュリティを考慮した新システムを構築すること。
- 行内の部署間で協力して独自のセキュリティ情報を収集すること（本事案の場合、パスワードがリセットされた顧客へ連絡を取っていれば、より早く攻撃を検知できた可能性があり、顧客からの苦情をパスワードリセットの攻撃と関連付けることができれば、パスワードのリセット直後に不正が行われるというパターンを明らかにできた可能性がある)。

２．１０　PIR Bank（ロシア）の事案

〈事象〉

2018 年 7 月 3 日（火)、ロシアの PIR Bank において、AWS CBR が悪用され、100 万米ドル（約 1.1 億円）程度（少なくとも約 92 万米ドル）がロシア大手行の 17 口座へ不正に送金された（当行はその翌日に検知)。なお、その資金のほとんどは当行の回収前に出金された。

〈攻撃手口〉

攻撃の流れは以下の通り。

① 2018 年 5 月下旬、当行の地方支店の 1 つで使用されていたサポート期限切れのルーター（ソフトウェア「Cisco IOS 12.4」を搭載した「Cisco 800 シリーズ」と呼ばれるルーター）から侵入する。このルーターを利用すれば、当行の内部ネットワークへ直接アクセス可能であった。なお、このように地方支店のネットワークを利用して攻撃する手口は、この攻撃者グループ（後述の通り、「２．３　アメリカ、ロシアの銀行等

の事案」と同じ攻撃者グループ）が少なくとも過去に 3 回使用したことのある手口であった。

② 基幹システムのネットワークへ侵入し、長期間潜伏しながら、PowerShell[51]等を利用し、場合によっては攻撃の自動化も行いつつ、AWS CBR へアクセスする。

③ AWS CBR から不正な送金指示を送信することにより、ロシア大手行の口座へ不正送金を行う。

④ 出し子が ATM から即座に出金する。

⑤ 多数のコンピュータの OS からログを削除する。

なお、当行は不正送金が行われた翌日の夕方に不正送金に気付き、当局へ資金移動の停止を依頼したものの、停止は間に合わなかった。

また、攻撃者は、さらなる攻撃のため、攻撃者側のサーバへ接続し新たなコマンドを実行可能にするプログラムを当行のネットワーク内に残していたが、これは本事案への対応中に検出され削除された。

〈攻撃者〉

ほかの攻撃者グループの攻撃に悪用されたことのない AWS CBR を悪用していること、脆弱な地方支店のネットワークからを侵入していること、PowerShell を利用していること等の特徴から、「２．３　アメリカ、ロシアの銀行等の事案」と同じ、ロシア語を話す攻撃者グループによるものとみられている。

〈攻撃から守るための推奨事項〉

本事案を分析したセキュリティベンダーによると、この攻撃者グループは脆弱なルーターから侵入することが多いため、まずはルーターのファームウェア[52]のアップデート要否を確認し、ブルートフォース攻撃[53]に対する脆弱性を検証し、設定変更の必要性をタイムリーに検知することが必要であるとしている。

２．１１　Cosmos Cooperative Bank（インド）の事案

〈事象〉

2018 年 8 月、インドの Cosmos Cooperative Bank において、デビットカード決済システムおよび SWIFT ネットワークが悪用され、約 9 億 4,400 万ルピー（約 15 億円）が不正に盗まれた。

---

51) マイクロソフト社が開発した、システム管理者向けに設計されたコマンドラインシェル（https://docs.microsoft.com/ja-jp/powershell/scripting/getting-started/getting-started-with-windows-powershell?view=powershell-6）。コマンド（命令）を入力することで、さまざまな動作を行うことができる。Windows OS に標準搭載されている正規のソフトウェアであるため、攻撃者に悪用されても、それが悪意ある動作なのか正常な動作なのかという判別が難しいとされる。そのため、近年は、PowerShell 等を利用し、実行ファイルを利用しない「ファイルレス攻撃」が増加していると言われている。

52) 電子機器内部に予め組み込まれ、内容が変更されることがほとんどなく、ハードウェアに密接に結びついて基本的な制御を行うソフトウェア。ハードウェアとソフトウェアの中間的な存在として「ファーム（堅固な）ウェア」と呼ばれている。

53) パスワード等の秘密情報に対して考え得るあらゆる組合せを試行することにより、秘密情報を解読したり不正にログインしたりする攻撃。日本語では「総当たり攻撃」と訳されることが多い。

11 日（土）、インド国内の ATM から 2,849 件の不正出金により約 2,500 万ルピーが、インド国外の 28 ヵ国の ATM から約 12,000 件の不正出金により約 7 億 8,000 万ルピーが盗まれ、13 日（月）、SWIFT ネットワークにより香港の恒生銀行へ約 1 億 3,900 万ルピーが不正送金された。

なお、その後、約 3 万 6,500 ルピーは回収されている。

〈攻撃手口〉

攻撃の流れは以下の通り。

① 何らかの方法により当行のシステムへ侵入する。

② ATM 関連システムに複数のマルウェアを感染させる。また、悪意ある ATM スイッチ[54]を立ち上げ、既存の ATM スイッチと基幹システムとの通信の一部を悪意あるスイッチへと迂回させる。それにより、不正取引が基幹システムへ送信されず、口座番号や口座状態等のチェックが行われなくなるとともに、基幹システムの代わりに悪意ある ATM スイッチが ATM 端末に対して取引を承認する偽の応答を返すことで、不正な出金が可能となる。

③ 複製した 450 枚の偽造カードを使用し、インド国内外で ATM から一斉に出金する。

④ システム内を移動し、SWIFT 取引システムを侵害し、3 件の不正送金を行う。

⑤ 攻撃の全ての証跡を削除する。

〈攻撃者〉

インド警察当局は出し子のうち 7 人を逮捕しているが、その背後にいる攻撃者グループが何者であるかは判明していない。なお、出し子 7 人のうち 4 人は、2018 年 2 月の City Union Bank の事案にも関与しており、その際にも ATM から不正に出金していた。

一方で、本事案を分析したセキュリティベンダーは、他のセキュリティベンダーの分析も引用しつつ、バングラデシュ中銀事案と同じ攻撃者グループである可能性を指摘している。

〈攻撃が成功した要因と攻撃から守るための推奨事項〉

インド警察当局によれば、インドの一部の協同組合銀行（Cooperative Bank）と異なり、当行は優れたサイバーセキュリティポリシーとフレームワークを採用しており、全てのシステムが PCI DSS[55]に準拠するとともに、顧客データの保護のための独自のデータセンターおよび SOC[56]を保有していた。警察は、「SOC でも気付けない攻撃の手口というのは驚くべきものだ」と、攻撃が非常に高度なものであったことを示唆している。

本事案を分析したセキュリティベンダーは、

- 取引内容に加え、ユーザー・システム・ネットワークそれぞれの挙動がどのような状

---

54) 「スイッチ」とは、異なるネットワーク間をつなぐネットワーク機器。ここでいう「ATM スイッチ」は、各 ATM 端末と基幹システム等の当行システムや各地域・国・国際間のネットワークとを繋ぎ、取引の送信および通信経路の決定を担っている。

55) Payment Card Industry Data Security Standard の略で、加盟店やサービスプロバイダーにおいてクレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準。国際カードブランド 5 社(American Express、Discover、JCB、MasterCard、VISA)が共同で設立した PCI SSC(Payment Card Industry Security Standards Council)によって運用・管理されている。
（https://www.jcdsc.org/pci_dss.php）

56) Security Operation Center の略で、システムを監視し、システムに対する脅威の検出・分析・対応等を行う組織。

態であれば正常であるかということを定義することにより、そこから逸脱する異常を検知できるようにすること、

- システムのあらゆる部分を適切に連携させることで、進行中の攻撃を検知できるようにすること、

が非常に重要であると指摘しており、そのためには、

- エンドポイント[57]やネットワークを含むシステム環境の可視化、
- SWIFT 等のサードパーティを含む組織内外の様々なエンティティに跨る異常を互いに繋ぎ合わせ補完し合うこと、

が鍵になるとしている。

２．１２　Redbanc（チリの銀行間 ATM ネットワーク）の事案

〈事象〉

2018 年 12 月下旬、チリ国内の全ての銀行の ATM が相互接続するネットワークを提供する組織である Redbanc がマルウェアに感染した。監視システムがネットワーク内の異常な振る舞いを検知し、攻撃が未然に防がれたため、ATM ネットワークへ影響は生じなかった。

〈攻撃手口〉

Redbanc が検知するまでの攻撃の流れは以下の通り。巧妙なソーシャルエンジニアリングの手法が使用されている。

① 攻撃者グループのフロント企業である人材会社が、LinkedIn[58]に企業のシステム開発者を募る偽の求人広告を掲載し、攻撃の標的とするに相応しい人物が応募してくるのを待つ。
② Redbanc の従業員が応募する。
③ Redbanc の従業員に対し、Skype を利用して現地語であるスペイン語による面接を行い、その場で、採用に必要な申請書を作成するためのツールを装ったマルウェアをインストールし実行するよう依頼する。
④ Redbanc の従業員が業務用パソコンへマルウェアをインストールする。このとき、マルウェアはウイルス対策ソフトに検知されず、正常にインストールできた。
⑤ マルウェアが感染した Redbanc の業務用パソコンに関する情報を収集し、外部にある攻撃者のサーバへ送信する。この段階で Redbanc の監視システムが異常を検知した。

〈攻撃者〉

使用されたマルウェアが過去に使用されたものと一致したことから、バングラデシュ中銀事案と同じ攻撃者グループによるものとみられている。

---

57) ネットワークに接続された端末やシステム機器の総称。
58) ビジネス用の SNS で、人材の採用やビジネスパートナー等とのコンタクトを取ることが可能。

２．１３　Bank of Valletta（マルタ）の事案

〈事象〉

2019 年 2 月 13 日（水）、マルタの Bank of Valletta において、11 件の不正な送金指示により、約 1,300 万ユーロ（約 16 億円）がイギリス、アメリカ、チェコ、香港の銀行へ送金されたことが判明。

また、この不正送金を受け、被害の極小化およびシステムの点検のため、当行はほぼ丸 1 日間に渡り、支店・インターネットバンキング・カード決済を含む全業務を停止した。マルタ国内の銀行取引の約半分のシェアを占める最大手行である当行の業務停止により、マルタ経済は大きな影響を受けた。特に、翌日に年金支給日を控えていたこともあり、必要に応じて中央銀行が小切手を発行するなどのコンティンジェンシープランが政府と中央銀行により策定された。

なお、その後、約 1,000 万ユーロについては回収されている。

〈攻撃手口〉

攻撃の流れは以下の通り。

① 2018 年 10 月頃、開くとシステムへのアクセス権を与えてしまうよう細工されたリンクあるいは偽文書を添付し、公式なレターヘッドを使用してフランスの金融市場庁（Autorité des marchés financiers）を装ったメールを当行へ送信する。
なお、このとき、マルタの別の銀行である HSBC Malta やフランスの組織へも同様のメールを送信したとみられている。

② 当行の行員がメールの添付ファイルを開き、攻撃者がアクセス可能となる。
なお、同様のメールが送られた HSBC Malta へは侵入できなかった。

③ PowerShell Empire[59]という正規のツールを利用し、システム内を移動し探索する。

④ 不正送金を行う。

〈攻撃者〉

攻撃に利用されたシステムインフラや攻撃コード等から、2013 年から 2015 年の約 2 年間で世界 30 ヵ国、100 の金融機関から約 10 億ドルを盗んだ攻撃者グループ[60]と関連があるとの見方がある。

３．SWIFT の取組み

前章の一覧表に整理した通り、銀行等（中央銀行・信用組合・銀行間決済システム含む）において発生した事案 28 件のうち半数以上が、SWIFT ネットワーク等の銀行間決済システムが悪用された事案となっている。

各事案から得られた教訓は〈攻撃が成功した要因〉や〈攻撃から守るための推奨事項〉に記

[59] 主にペネトレーションテスト（脚注 35 参照）等で利用される、無料でダウンロードできるオープンソースのセキュリティツール。パスワードの抽出、特権昇格、ネットワーク探索等、様々な機能がある。

[60] 最近では世界 40 ヵ国から約 12 億ドルを盗んだとする推計もある。（参考：https://blog.kaspersky.co.jp/billion-dollar-apt-carbanak/6879/）

載した通りであるが、銀行間決済システムが悪用された不正送金事案が多数確認されている昨今の状況を踏まえ、そのようなサイバー攻撃への対策の考え方の一例として、SWIFT が行っているセキュリティ強化に向けた取組みである「Customer Security Programme」（以下、「CSP」という）について説明する。また、CSP を成す複数の施策のうち、SWIFT が SWIFT ネットワーク利用組織（以下、単に「利用組織」という）に対して実施を求めているセキュリティ対策である「Customer Security Controls Framework」（以下、「CSCF」という）について、個別に説明する。CSCF は、SWIFT に関連しないシステムのセキュリティを確保する上でも参考にできる内容が多く、SWIFT ネットワークを利用していない金融機関にとっても有用であると思われる。

CSP、CSCF の内容を説明に先立ち、それらが適用される範囲について、概念図を示しておく（図 1）。

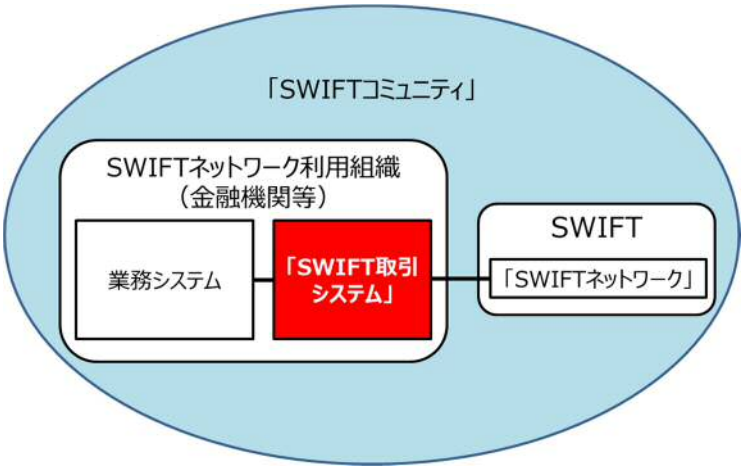

図 1　利用組織と SWIFT の関係

（注 1）図中の角丸四角形は組織、四角形はシステムを表す。

（注 2）CSP は 「SWIFT コミュニティ[61)]」に適用され、
CSCF は利用組織内の「SWIFT 取引システム」に適用される。

３．１　Customer Security Programme（CSP）

SWIFT では、2016 年 2 月に発生したバングラデシュ中銀事案をはじめとする SWIFT ネットワークに対するサイバー脅威の高まりを受け、同年、セキュリティ強化策（＝CSP）の検討を開始。その後、利用組織と連携しつつ内容を固め、2017 年に正式版をリリースした。

CSP は、「自組織（You）」、「相手先（Your Counterparts）」、「自組織の属する社会環境（Your Community）」という 3 つの領域から構成されている。これらは、まずは自組織を保護しセキュリティを確保すること、次に、自組織と相手先との関係性の中の不正行為を防止し発生した不正行為を検知すること、そして、自組織の属する社会環境の中で常に情報を共有し将来のサイ

61) SWIFT が使用している表現で、SWIFT ネットワークの利用組織だけでなく SWIFT 自身も含めた SWIFT 関係者全体を指す。

バー脅威からの防御に備えること、を意味する（図 2）。

図 2　CSP のイメージ

（出所）SWIFT ウェブサイトより

1 つ目の「自組織を守りセキュリティを確保すること」とは、つまり、自組織内の SWIFT 関連のシステムインフラ[62]を保護し、適切な人員・ポリシー・プラクティスを配置・適用することである。SWIFT はその支援のため、既存のセキュリティガイダンスに基づきつつ、最新のサイバー脅威やインシデント等のインテリジェンスも考慮し、利用組織が必ず実装すべきセキュリティ管理項目（3．2 節にて説明する CSCF における必須管理項目）を策定した。

2 つ目の「自組織と相手先との関係性の中の不正行為を防止し発生した不正行為を検知すること」とは、利用組織が強固なセキュリティ対策を適用することは当然必要であるものの、他方で攻撃者も非常に洗練されているため、実際にサイバー攻撃の標的になってしまった場合のことを想定しておく必要があり、その際、自組織と相手先との関わりの中におけるセキュリティリスクの管理も非常に重要になるということである。これにはさらに、自組織が侵害された場合と、相手先が侵害された場合という 2 つの場合がある。

自組織が侵害された場合、その事実を検知できるよう、SWIFT では、特にリソースの限られる小規模な組織を支援するため、SWIFT ネットワーク上の取引データを日次で還元する新たなツールの提供を開始した。これにより、高額あるいは異常な取引を二次的に確認することが可

[62] 前章で使用した「SWIFT 取引システム」（脚注 32 参照）に同じ。本章の中の CSP あるいは CSCF の内容説明に係る記述は基本的に SWIFT の英語による説明の仮訳であるため、SWIFT の使用する用語に応じ、「SWIFT 関連のシステムインフラ」、「SWIFT インフラ」、「SWIFT 関連アプリケーション」、「SWIFT 関連コンポーネント」、「SWIFT 環境」、「SWIFT システム」、「SWIFT メッセージングインターフェース」と、表現にブレがあるが、いずれの用語も「SWIFT ネットワークへ接続し SWIFT ネットワーク経由の取引を行うための当行のシステム」という意味では同じであるため、本稿においては、これらは全て前章で使用した「SWIFT 取引システム」と同義であると理解して差し支えない。

能となるほか、利用組織内の取引データと照合させることで不正な取引を検知できるという。

相手先が侵害された場合、自組織がその相手先から不正なメッセージを受信する可能性があり、それに備える必要がある。また、そもそも相手先が信頼できる組織であるか否かを確認することが大前提であり、SWIFT は相手先との関係性を管理できるツールを提供している。

最後の「自組織の属する社会環境の中で常に情報を共有し将来のサイバー脅威からの防御に備えること」とは、特定の組織内の特定の場所で発生した事象が、世界中のどこか別の場所で容易に再現される可能性があるため、そのような情報を SWIFT コミュニティ内で共有し、攻撃された場合のための準備をしておく必要があるということである。

情報共有のため、利用組織は、自組織がサイバー攻撃の標的にされた場合あるいは侵害された疑いのある場合、速やかに SWIFT へ通知する必要があり、その情報は SWIFT が設置したインテリジェンス専門チームにより匿名化され、利用組織へ配布される。また、SWIFT は「SWIFT ISAC（Information Sharing and Analysis Centre）」と呼ぶ情報共有ポータルサイトを導入しており、その場で詳細情報の共有が可能となっている。

利用組織は攻撃に備え、そのように共有される脅威情報やセキュリティのアップデート情報に基づきタイムリーに対応するとともに、必ず実装すべきセキュリティ管理項目を確実に充足することが求められている。

３．２　Customer Security Controls Framework（CSCF）

CSCF の策定は、CSP の中核となる施策である。CSCF は 3 つの「目的」と、それぞれの目的の中の優先度の高い事項として 8 つの「原則」が示されており、それらを支えるものとして 27 の詳細な「管理項目」が存在する（図 3）。なお、CSCF は毎年見直しが行われており、2019 年版への改定においては、当初推奨管理項目であった 3 項目が必須管理項目へと引き上げられるとともに、新たな推奨管理項目として 2 項目が追加され、管理項目は全 29 項目となっている。

図 3　CSCF の全体構成

（資料）SWIFT ウェブサイトより作成

目的と原則の具体的内容と対応関係はそれぞれ次の通り（表 2）。

表 2　CSCF の目的と原則

（資料）SWIFT ウェブサイトより作成

（注）左側の 3 項目が 3 つの目的、中央の 8 項目が 8 つの原則。

目的と原則を支える 29 の管理項目は、19 の必須管理項目（表 3）と、10 の推奨管理項目（表 4）に分類される。SWIFT は利用組織に対して 19 の必須管理項目の遵守を求めており、実際に遵守できているか否かを確認するため、年 1 回利用組織が自己査定を行い、毎年年末までにその結果を SWIFT へ提出することを求めている。2018 年以降に行われる自己査定においては、必須管理項目のうち一部でも遵守できていない組織が認められた場合には、SWIFT はその事実をその組織を所管する当局へ通知するとしており、そのことによりある種の強制力を持たせている。

表 3　CSCF 必須管理項目

必須管理項目	目的
1. インターネットへのアクセス制限と重要システムの一般 IT 環境からの保護	
1.1 SWIFT 環境の保護	利用組織内の SWIFT インフラを組織内の一般 IT 環境や外部環境における侵害から保護する
1.2 OS の特権アカウント管理	OS の管理者アカウントの配布と使用を制限し管理する
2. 被攻撃対象と脆弱性の低減	
2.1 内部データフローのセキュリティ確保	組織内の SWIFT 関連アプリケーションとオペレータ PC との間のデータフローの機密性・完全性・真正性を確保する

必須管理項目	目的
2.2 セキュリティのアップデート	ベンダーからのサポートの確保、必須のソフトウェアアップデートの適用、リスク評価を踏まえたタイムリーなセキュリティアップデートの適用により、組織内の SWIFT インフラにおける既知の技術的脆弱性の発生を最小化する
2.3 システムの強化	システムの強化により、SWIFT 関連コンポーネントのうちサイバー攻撃の対象となり得る部分を減らす
2.6 オペレーターセッションの機密性と完全性	組織内の SWIFT インフラと接続する双方向のオペレーターセッションの機密性・完全性を確保する
2.7 脆弱性スキャン	定期的な脆弱性スキャンプロセスおよびスキャン結果に基づく対応プロセスを実装することにより、組織内の SWIFT 環境における既知の脆弱性を特定する
3. 物理環境のセキュリティ確保	
3.1 物理セキュリティの確保	機密性の高い設備・職場環境・システム設置場所・保管場所への不正な物理的なアクセスを防止する
4. 認証情報漏洩の防止	
4.1 パスワードポリシー	効果的なパスワードポリシーを実装し実行することにより、一般的なパスワード攻撃に対する十分な耐性を確保する
4.2 多要素認証	多要素認証を実装することにより、認証要素が単一であることが原因で SWIFT システムへアクセスされてしまうことを防止する
5. 個人認証管理と特権の分離	
5.1 論理的アクセス管理	オペレーターアカウントに応じた必要最小限のアクセスの許容・最低限の権限付与・職務の分離というセキュリティの原則を実行する
5.2 トークン管理	接続型ハードウェア認証トークンを使用している場合、その適切な管理・追跡・使用を徹底する
5.4 物理的・論理的なパスワード保管	物理的および論理的に記録されたパスワードを保護する
6. システムまたは取引の記録に対する異常の検知	
6.1 マルウェアからの保護	組織内の SWIFT インフラをマルウェアから確実に保護する
6.2 ソフトウェアの完全性	SWIFT 関連アプリケーションの完全性を確保する
6.3 データベースの完全性	SWIFT メッセージングインターフェースのデータベースの完全性を確保する

必須管理項目		目的
	6.4 ログ取得と監視	セキュリティイベントを記録し、組織内の SWIFT 環境における異常な挙動やオペレーションを検知する
7. インシデント対応および情報共有に関する計画		
	7.1 サイバーインシデント対応計画	サイバーインシデント管理のための一貫性のある効果的なアプローチを確保する
	7.2 セキュリティ訓練と意識啓発	定期的なセキュリティ訓練および啓発活動を行うことにより、全職員がセキュリティを確保する責任を意識し全うするよう徹底する

（資料）SWIFT ウェブサイトより作成

表 4　CSCF 推奨管理項目

推奨管理項目		目的
1. インターネットへのアクセス制限と重要システムの一般 IT 環境からの保護		
	1.3A 仮想化基盤の保護	SWIFT 関連コンポーネントを搭載する仮想化基盤および仮想マシンのセキュリティは、物理システムと同水準の確保する
2. 被攻撃対象と脆弱性の低減		
	2.4A バックオフィスのデータフローのセキュリティ確保	バックオフィス（またはミドルウェア）のアプリケーションと SWIFT インフラと接続するコンポーネントとの間のデータフローの機密性・完全性・相互真正性を確保する
	2.5A 外部送信されるデータの保護	セキュアゾーンの外へ送信される SWIFT 関連データの機密性を確保する
	2.8A 重要業務の外部委託	重要業務を外部委託することで生じるリスクから組織内の SWIFT インフラの保護する
	2.9A 決済業務の管理	取引の相手方を正当で承認された相手先のみとし、かつ、取引は通常業務で想定される範囲内に制限する
	2.10A アプリケーションの強化	SWIFT の認証を受けたメッセージングおよび通信のインターフェースや関連アプリケーションの強化により、SWIFT 関連コンポーネントのうちサイバー攻撃の対象となり得る部分を減らす
5. 個人認証管理と特権の分離		
	5.3A 職員の身元調査プロセス	身元調査により、組織内の SWIFT 環境を運用するスタッフの信頼性を確保する
6. システムまたは取引の記録に対する異常の検知		
	6.5A 侵入検知	組織内の SWIFT 環境へ接続するネットワーク、あるいは、SWIFT 環境の内部にあるネットワーク上の異常を検知・防止する

推奨管理項目		目的
7. インシデント対応および情報共有に関する計画		
	7.3A ペネトレーションテスト	ペネトレーションテストにより、セキュリティ設定の妥当性を検証しセキュリティ対策の不備を特定する
	7.4A シナリオベースのリスク評価	想定されるサイバー攻撃シナリオに基づき、組織のリスクおよび態勢を評価する

（資料）SWIFT ウェブサイトより作成

（注）推奨管理項目の各項目番号には、末尾に「A」が付与されている。

ここで、前章で詳述した 12 事案のうち、SWIFT ネットワークをはじめとする銀行間決済システムが悪用された 8 事案について、それぞれの〈攻撃が成功した要因〉または〈攻撃から守るための推奨事項〉と CSCF の各管理項目を照らし、CSCF の管理項目を遵守することでこのようなサイバー攻撃をどれほど抑止できる可能性があるのか検証する（表 5）（２．１２節の事案は攻撃が成功していないため省略）。

表 5　各事案と CSCF 管理項目との対応関係

節	金融機関名	悪用されたシステム	攻撃が成功した要因・攻撃から守るための推奨事項	対応する CSCF の管理項目等
２．２	遠東國際商業銀行	SWIFT ネットワーク	〈攻撃が成功した要因〉 ・ 一般職員にも特権アカウントが付与されていたため、一般職員から特権アカウントと認証情報が窃取された ・ SWIFT 取引システムがその他のシステムと物理的に隔離されていなかったため、メールによって当行のシステムへ侵入した攻撃者がネットワーク内を移動し、最終的に SWIFT 取引システムにまで侵入された	・5.1 論理的アクセス管理、1.2 OS の特権アカウント管理 ・1.1 SWIFT 環境の保護

節	金融機関名	悪用されたシステム	攻撃が成功した要因・攻撃から守るための推奨事項	対応する CSCF の管理項目等
2．3	NIC Asia Bank	SWIFT ネットワーク	〈攻撃が成功した要因〉 ・ SWIFT 取引端末でメールの確認ができた ・ ネパールでは一般的に業務時間外は SWIFT 取引システムを停止させるにも関わらず、当行は起動したままであった ・システムへのアクセスに通常の ID とパスワードしか使用されておらず、ワンタイムパスワード等の強度の高い認証方式が採用されていなかった ・ SWIFT 取引システムに遠隔操作機能が備わっており、アクセス経路が複数あった ・ 経営陣の中に IT 責任者がおらず、IT 部門が意思決定に参加できていなかった ・ ネパールの銀行業界の慣習として、システムが監査対象になっておらず、対策が不十分であることを見抜けなかった	 ・1.1 SWIFT 環境の保護 ・無し ・4.2 多要素認証 ・1.1 SWIFT 環境の保護 ・7.1 サイバーインシデント対応計画 ・無し
2．4	アメリカ、ロシアの銀行	クレジットカードやデビットカードの処理システム、ロシア国内の銀行間決済システム	〈攻撃から守るための推奨事項〉 ・ 外部からのログインの禁止 ・ ユーザーへの必要最小限の権限付与 ・ ソフトウェア等のタイムリーなアップデート ・ IDS（侵入検知システム）の導入	 ・1.1 SWIFT 環境の保護 ・5.1 論理的アクセス管理、1.2 OS の特権アカウント管理 ・2.2 セキュリティのアップデート ・6.5A 侵入検知
2．5	Youbit、その他の暗号資産交換所	交換所システム	〈攻撃から守るための推奨事項〉 ・ソーシャルエンジニアリングや最新の脅威動向に関する研修の継続的な実施	 ・7.2 セキュリティ訓練と意識啓発

節	金融機関名	悪用されたシステム	攻撃が成功した要因・攻撃から守るための推奨事項	対応する CSCF の管理項目等
			・サンドボックスにより添付ファイルやリンクが悪意あるものであるかどうかを判別できる高度なマルウェア防御・検知ソリューションの導入 ・全ての主要システムへの二要素認証の実装	・6.1 マルウェアからの保護 ・4.2 多要素認証
2．7	Punjab National Bank	SWIFT ネットワーク	〈攻撃が成功した要因〉 ・ 基幹システムが SWIFT 取引システムとシステム的に連携しておらず、不整合がないかシステム的に検証することが不可能であった ・ SWIFT 取引に必要なパスワードが適切に管理されておらず、複数人の間で共有されていた ・ オペレーショナルリスクを管理する企業文化が欠如していた 〈攻撃から守るための推奨事項〉 ・ 年 1 回のシステム監査を行うことや、適切なガバナンスとリスク管理のための UEBA 等の新技術の活用	・2.4A バックオフィスのデータフローのセキュリティ確保 ・5.1 論理的アクセス管理、5.4 物理的・論理的なパスワード保管 ・7.4A シナリオベースのリスク評価 ・CSCF に基づく自己査定
2．8	メキシコの銀行 5 行	メキシコ国内の銀行間決済システム	〈攻撃が成功した要因〉 ・ 多くのネットワークが強固なアクセス管理機能を備えていなかったため、侵害された行員の認証情報により多数のシステムへアクセスできた ・ ネットワークが十分にセグメント化されておらず、最初の侵入さえできれば、その後はシステムの内部深くまで侵入できてしまい、SPEI 取引システムまでアクセスできた ・ 銀行内部のネットワークを流れる取引データが必ずしも常に保護され	・5.1 論理的アクセス管理、1.2 OS の特権アカウント管理 ・1.1 SWIFT 環境の保護 ・2.1 内部データフローのセキュリティ

節	金融機関名	悪用されたシステム	攻撃が成功した要因・攻撃から守るための推奨事項	対応する CSCF の管理項目等
			ておらず、取引の追跡やデータの操作ができた ・ SPEI 取引システムに不備があり、適切な取引妥当性チェックが行われず、不正取引を見逃した	確保、6.2 ソフトウェアの完全性、6.3 データベースの完全性 •2.4A バックオフィスのデータフローのセキュリティ確保、2.9A 決済業務の管理
2．10	PIR Bank	ロシア国内の銀行間決済システム	〈攻撃から守るための推奨事項〉 ルーターのファームウェアのアップデート要否を確認し、ブルートフォース攻撃に対する脆弱性を検証し、設定変更の必要性をタイムリーに検知すること	2.2 セキュリティのアップデート、2.7 脆弱性スキャン
2．11	Cosmos Cooperative Bank	SWIFT ネットワーク	〈攻撃から守るための推奨事項〉 ・ 取引内容に加え、ユーザー・システム・ネットワークそれぞれの挙動がどのような状態であれば正常であるかということを定義することにより、そこから逸脱する異常を検知できるようにすること ・ システムのあらゆる部分を適切に連携させることで、進行中の攻撃を検知できるようにすること	•6.4 ログ取得と監視 •2.4A バックオフィスのデータフローのセキュリティ確保
2．13	Bank of Valletta	SWIFT ネットワーク	不明	-

（資料）SWIFT ウェブサイトより作成

表 5 からわかる通り、一部を除き、SWIFT ネットワーク以外のシステムが悪用された事案を含め、各事案の〈攻撃が成功した要因〉または〈攻撃から守るための推奨事項〉には、それぞれ対応する CSCF の管理項目が存在している。つまり、仮に攻撃を受ける前にこれらの項目を遵守できていたとすれば、被害を抑止できた可能性が高い。CSCF は過去の SWIFT ネットワークが悪用された事案等を踏まえて策定されているため、このことはある意味当然ではあるものの、

利用組織の中には必須項目が遵守できていない組織も存在しており、そのような組織においては、このようなサイバー攻撃事案が世界中で継続的に発生していることおよび被害抑止のためには CSCF が有用であることを改めて認識した上で、早急に対応することが求められる。

４．まとめ

ここまで、金融機関を標的にしたサイバー攻撃事案等および SWIFT の取組みという事実に基づく情報を整理してきたが、本章では、２章に挙げた 52 の事案の分析を簡単に行った上で、筆者の個人的見解を述べる。

まず、52 の事案からは、以下のようなことが読み取れる。

① 目的別に見ると、金銭目的の事案（最終的に被害が無かったものも含む）が 35 件と全体の 7 割弱を占めている（図 4）。

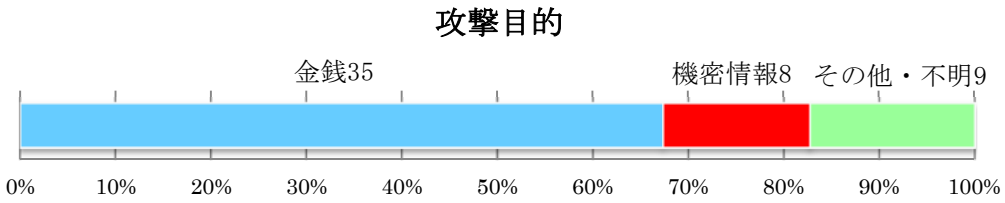

図 4　攻撃目的別割合

（注 1）各データラベル内の数値は件数を示す。

（注 2）金融機関の不備による情報漏洩は「その他・不明」に分類。

② 業態別に見ると、銀行等（中央銀行・信用組合・銀行間決済システム含む）が標的となった事案が 28 件と過半数を占め、暗号資産交換所が 17 件と続き、その他が 7 件となっている（図 5）。

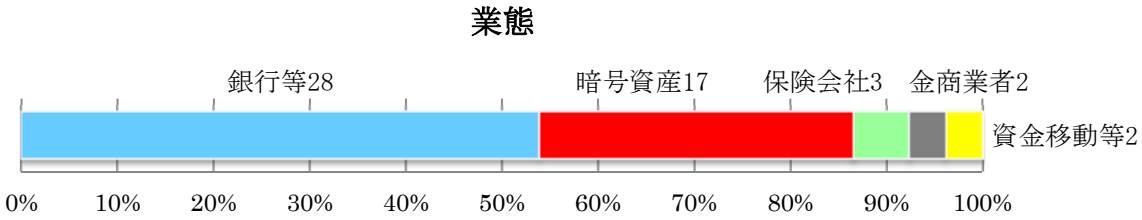

図 5　業態別割合

（注 1）各データラベル内の数値は件数を示す。

（注 2）「銀行等」には、中央銀行・信用組合・銀行間決済システムを含む。

③　攻撃種類を見ると、不正送金等（不正出金・不正融資含む）が 32 件と 6 割超を占め、DoS 攻撃（DDoS 攻撃含む）が 5 件、不正ログインが 3 件と続く（図 6）。

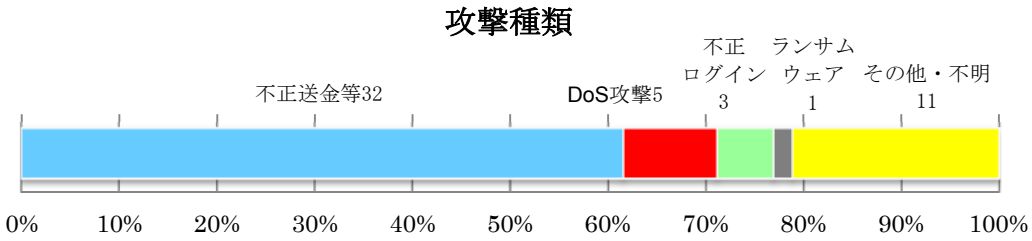

図 6　攻撃種類別割合

（注 1）各データラベル内の数値は件数を示す。

（注 2）「不正送金等」には、不正出金・不正融資を含む。

（注 3）「DoS 攻撃」には、DDoS 攻撃を含む。

（注 4）金融機関の不備による情報漏洩は「その他・不明」に分類。

金融機関を標的にする目的はやはり金銭の窃取が多く、攻撃者グループは送金を取扱う銀行あるいは暗号資産交換所を狙っている。銀行等から金銭を盗む方法としては、国際送金が多い。SWIFT ネットワークを利用し銀行自身の口座の入出金により行う国際送金は、２．２節の遠東國際商業銀行の事案のように、攻撃者にとっては高額の資金を効率的に盗むことができる方法であるが、近年は、２．１１節の Cosmos Cooperative Bank の事案のように、より検知されにくいよう、少額の送金を多数繰り返す方法も見られる。また、暗号資産交換所は一般的に規模が小さくセキュリティも脆弱であることが多いと言われているとともに、暗号資産はマネーロンダリングを行いやすいこともあり、攻撃者にとって恰好の標的となっており、国内外のどこかの交換所から毎月のように暗号資産が盗まれているような状況にある。

このような、SWIFT をはじめとする銀行間決済システムや暗号資産交換所を狙った攻撃を行う攻撃者グループは限られており、特定のグループが様々な攻撃に関与していると言われている。そのため、２章で詳述した通り、その攻撃手口には細かな差異はあるものの、広義の攻撃手口は非常に似通っていると言える。攻撃者がまず金融機関の職員へ悪意あるメールを送り、職員がそれを開封しマルウェアに感染、攻撃者による遠隔操作が可能となり、正規のツール等を利用しながら金融機関内部のネットワーク内を探索、SWIFT ネットワーク等の銀行間決済システムやブロックチェーンへ接続し送金を行うためのシステムへアクセスし、そこから不正な送金を実行、事前に手配した出し子が送金先の金融機関からが出金し、不正送金の形跡は削除あるいは改ざんして立ち去る、というパターンが多い。

SWIFT はその利用組織がこのような攻撃から自組織の SWIFT 取引システムを守ることができるよう CSCF を策定したが、このような攻撃パターンは、SWIFT ネットワークに限らず、その他のシステムが悪用された場合についても共通する部分が多いため、CSCF はそのようなシステム

に対しても少なからず参考にできる部分があろうと考えられる。本稿で示した攻撃事例や CSCF を 1 つの参考情報としつつ、自組織が同様の攻撃を受けた場合に事前に検知し被害を防止できる対策が取れているか、検証してみるのもよいのではないだろうか。

既存の攻撃手口を知り、その対策を実施することは当然重要であるが、他方、攻撃者グループは金融機関の対策状況を踏まえて次々と新たな攻撃手口を考え出し、対策を乗り越えてくることが十分に考えられるため、そのような点も考慮した上で、自組織の置かれた環境のサイバーセキュリティに対する脅威の動向を日々収集・分析し、必要に応じて追加の対策を行うなどの柔軟な対応も重要になる。その点、CSCF に関して言えば、SWIFT が最新のインテリジェンス等を考慮して毎年継続的にアップデートしていくため、利用する金融機関としては、それに遅れることなくタイムリーに対応していくことが重要になる。加えて、前章の表 5 の通り、推奨管理項目を遵守していれば被害が抑止できた可能性がある事例もあるため、必須管理項目に限らず、推奨管理項目も含めて遵守できるよう対応することが望ましい。

本稿では、金融機関を標的としたサイバー攻撃等の動向について、不正送金事案や SWIFT の取組みを中心に述べてきたが、これらはあくまでもサイバーセキュリティの 1 つの側面に過ぎず、それ以外の脅威や SWIFT 取引システム以外のシステムについても非常に重要であることは言うまでもない。そのため、このような金融機関を取り巻くサイバーセキュリティの多様な状況に関する情報収集・分析を絶えず行い、自組織のサイバーリスクを特定した上で、サイバーセキュリティ向上のための不断の取組みを行うことが求められる。

システム・サイバーセキュリティ用語集

（注 1）脚注にて説明した用語を掲載し、ページ番号はその脚注のあるページを示す
（注 2）鍵括弧書きの用語は本稿独自の意味で使用

参考文献

（1）２．２　遠東國際商業銀行（台湾）の事案（主なもの）

①FOCUS TAIWAN NEWS CHANNEL（2017.10.07）「Premier urges security review after Taiwanese bank hacked」（http://focustaiwan.tw/news/asoc/201710070007.aspx）

②FOCUS TAIWAN NEWS CHANNEL（2017.10.09）「CIB confirms suspect nabbed for hacking; US$500,000 unaccountable」（http://focustaiwan.tw/news/asoc/201710090016.aspx）

③Hiru News（2017.10.10）「Taiwan bank hack : Police expand investigations」（http://www.hirunews.lk/173081/taiwan-bank-hack-police-expand-investigations）

④Bloomberg（2017.10.12）「Sri Lanka Makes Arrests in $60 Million Taiwanese Bank Cyberheist」（https://www.bloomberg.com/news/articles/2017-10-12/sri-lanka-makes-arrests-in-60-million-taiwanese-bank-cyberheist）

⑤McAfee（2017.10.12）「Taiwan Bank Heist and the Role of Pseudo Ransomware」（https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/taiwan-bank-heist-role-pseudo-ransomware/）

⑥iThome（2017.10.12）「【遠銀遭駭追追追】遠銀被駭案，金管會初步調查：銀行未做好內控管理」（https://www.ithome.com.tw/news/117380）

⑦NOW NEWS（2017.10.13）「遠銀遭駭 襄陽分行電腦全中毒 惡意程式自動銷毀資料」（https://m.nownews.com/news/2624130）

⑧BAE Systems（2017.10.16）「Taiwan Heist: Lazarus Tools and Ransomware」（https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html）

⑨iThome（2017.10.17）「【遠東銀行遭駭追追追】權限控管超級重要！駭客入侵遠銀關鍵，就是這兩組帳密遭盜」（https://www.ithome.com.tw/news/117520）

（2）２．３　NIC Asia Bank（ネパール）の事案（主なもの）

①the kathmandu post（2017.10.23）「NIC Asia cash stolen in cyber heist」（http://kathmandupost.ekantipur.com/news/2017-10-23/nic-asia-cash-stolen-in-cyber-heist.html）

②Setopati（2017.10.23）「Rs 450m illegally transferred abroad from Nepali banks」（https://setopati.net/business/26733/Rs-450m-illegally-transferred-abroad-from-nepali-banks/）

③my Republica（2017.10.24）「NRB, NIC Asia Bank move to counter cyberattack」（http://www.myrepublica.com/news/29438/）

④THE NATION（2017.10.24）「NIC Asia cyber heist: Bank’s weakness helped criminals

to hack into its system」
(http://www.nationmultimedia.com/detail/asean-plus/30329996)
⑤the kathmandu post（2017.10.25）「Nepali banks ‘not prepared’ to ward off cyber threats」
(http://kathmandupost.ekantipur.com/news/2017-10-25/nepali-banks-not-prepared-to-ward-off-cyber-threats.html)
⑥CISO.in（2017.10.26）「Nepal bank comes under 'denial of service attack'」
(https://ciso.economictimes.indiatimes.com/news/nepal-bank-comes-under-denial-of-service-attack/61233325)
⑦the kathmandu post（2017.10.26）「NRB not keen on learning lessons from cyber heist」
(http://kathmandupost.ekantipur.com/news/2017-10-26/nrb-not-keen-on-learning-lessons-from-cyber-heist.html)
⑧ICT FRAME（2018.3.7）「Attackers Hacked Nepalese Bank’s Swift Server」
(https://ictframe.com/attackers-hacked-nepalese-banks-swift-server/)

（3）２．４　アメリカ、ロシアの銀行等の事案
Group-IB（2017.12）「MoneyTaker」

（4）２．５　Youbit等の韓国の暗号資産交換所において2017年に発生した事案（主なもの）
①朝鮮日報（2017.12.20）「韓国の仮想通貨取引所『ユービット』、ハッキング受け破産」
(http://www.chosunonline.com/site/data/html_dir/2017/12/20/2017122000657.html)
②ファイア・アイ（2017.10.01）「北朝鮮がビットコインに高い関心を持つ理由」
(https://www.fireeye.jp/company/press-releases/2017/north-korea-interested-in-bitcoin.html)
③Secureworks（2017.12.15）「Media Alert - Secureworks Discovers North Korean Cyber Threat Group, Lazarus, Spearphishing Financial Executives of Cryptocurrency Companies」
(https://www.secureworks.com/about/press/media-alert-secureworks-discovers-north-korean-cyber-threat-group-lazarus-spearphishing)
④朝鮮日報（2017.12.16）「ビットコイン関連のハッキング4件、全て北朝鮮が関与」
(http://www.chosunonline.com/site/data/html_dir/2017/12/16/2017121600415.html)
⑤中央日報（2018.2.6）「北朝鮮、仮想通貨ハッキング…韓国の取引所から数百億ウォン奪取」(https://japanese.joins.com/article/317/238317.html)

（5）２．６　ING Bank、Rabobank、ABN AMRO（オランダ）の事案（主なもの）
①SECURITY WEEK（2018.1.29）「Top Dutch Banks, Revenue Service Hit by Cyber Attacks」

(https://www.securityweek.com/top-dutch-banks-hit-cyber-attacks)

②Channel web (2018.1.29) 「ABN Amro, ING en Rabobank slachtoffer van DDoS-golf」
(https://www.channelweb.nl/artikel/nieuws/security/6289617/5226433/abn-amro-ing-en-rabobank-slachtoffer-van-ddos-golf.html)

③ABN AMRO (2018.1.29) 「Storingen door DDoS-aanvallen」
(https://www.abnamro.com/nl/newsroom/nieuws/2018/ddos-aanvallen.html)

④ComputerWeekly.com (2018.2.8) 「Teenager suspected of crippling Dutch banks with DDoS attacks」
(https://www.computerweekly.com/news/252434665/Teenager-suspected-of-crippling-Dutch-banks-with-DDoS-attacks)

⑤cyberscoop (2018.4.5) 「Mirai IoT botnet variant likely used in January DDoS attack against Dutch banks」
(https://www.cyberscoop.com/iot-botnet-dutch-banks-recorded-future/)

（6）２．７　Punjab National Bank（インド）の事案（主なもの）

①moneycontrol (2018.2.15) 「A freshly appointed official first noticed the fraud at Punjab National Bank」
(https://www.moneycontrol.com/news/business/economy/a-freshly-appointed-official-first-noticed-the-fraud-at-punjab-national-bank-2508727.html)

②BANK INFO SECURITY (2018.2.16) 「$1.8 Billion Fraud Case at PNB Raises Security Questions」
(https://www.bankinfosecurity.asia/18-billion-fraud-case-at-pnb-raises-security-questions-a-10657)

③REUTERS (2018.2.19) 「Eyes wide shut: the $1.8 billion Indian bank fraud that went unnoticed」
(https://www.reuters.com/article/us-punjab-natl-bank-fraud-insight/eyes-wide-shut-the-1-8-billion-indian-bank-fraud-that-went-unnoticed-idUSKCN1G200Z)

④BANK INFO SECURITY (2018.2.21) 「Mitigating the Insider Threat: Lessons From PNB Fraud Case」
(https://www.bankinfosecurity.com/mitigating-insider-threat-lessons-from-pnb-fraud-case-a-10674)

④Wikipedia (2019.5.7最終更新) 「Punjab National Bank Scam」
(https://en.wikipedia.org/wiki/Punjab_National_Bank_Scam)

（7）２．８　メキシコの銀行5行の事案（主なもの）

①REUTERS (2018.5.14) 「Thieves suck millions out of Mexican banks in transfer heist」

(https://www.reuters.com/article/us-mexico-cyber/thieves-suck-millions-out-of-mexican-banks-in-transfer-heist-idUSKCN1IF1X7)

②Zero Hedge (2018.5.29) 「Mexican Bank Foils $110 Million Cyber Robbery」
(https://www.zerohedge.com/news/2018-05-29/mexican-bank-foils-110-million-cyberheist)

③WIRED (2019.3.15) 「How Hackers Pulled Off a $20 Million Mexican Bank Heist」
(https://www.wired.com/story/mexico-bank-hack/)

（8）２．９　Bank of Montreal、Simplii Financial（カナダ）の事案（主なもの）

①BANK INFO SECURITY (2018.5.31) 「Two Canadian Banks Probe Alleged Exposure of Customer Data」
(https://www.bankinfosecurity.com/two-canadian-banks-probe-alleged-exposure-customer-data-a-11043)

②CBC (2018.5.31) 「Hackers threaten to reveal personal data of 90,000 Canadians caught in bank hack」
(https://www.cbc.ca/news/business/bank-hack-tuesday-1.4682018)

③INTSIGHTS (2018.6) 「Bank of Montreal & Simplii Breach: Timeline & Summary Report」

（9）「２．１０　PIR Bank（ロシア）の事案」（主なもの）

①Group-IB (2018.7.19) 「Group-IB is investigating a new daring attack by MoneyTaker: hackers try to steal $1 mln from the bank」
(https://www.group-ib.com/media/new-attack-moneytaker/)

②BANK INFO SECURITY (2018.7.20) 「Bank Hackers Exploit Outdated Router to Steal $1 Million」
(https://www.bankinfosecurity.com/bank-hackers-exploit-outdated-router-to-steal-1-million-a-11227)

（１０）２．１１　Cosmos Cooperative Bank（インド）の事案（主なもの）

①THE HINDU Business Line (2018.8.14) 「Cosmos Bank’s server hacked; Rs 94 cr siphoned off in 2 days」
(https://www.thehindubusinessline.com/money-and-banking/cosmos-banks-server-hacked-rs-94-cr-siphoned-off-in-2-days/article24687533.ece)

②BANK INFO SECURITY (2018.8.17) 「Police Investigate Cosmos Bank Hack」
(https://www.bankinfosecurity.com/police-investigate-cosmos-bank-hack-a-11379)

③SECURONIX (2018.8.27) 「Securonix Threat Research: COSMOS BANK SWIFT/ATM US$13.5 MILLION CYBER ATTACK DETECTION USING SECURITY ANALYTICS」

（https://www.securonix.com/web/wp-content/uploads/2018/08/Securonix_Cosmos-Bank-Report.pdf）

④BANK INFO SECURITY（2018.8.29）「Cosmos Bank Heist：No Evidence Major Hacking Group Involved」
（https://www.bankinfosecurity.com/cosmos-bank-heist-no-evidence-major-hacking-group-involved-a-11435）

⑤BANK INFO SECURITY（2018.9.21）「Seven Arrests in Cosmos Bank Heist」
（https://www.bankinfosecurity.com/seven-arrests-in-cosmos-bank-heist-a-11535）

（１１）２．１２　Redbanc（チリ）の事案（主なもの）

①trendTIC（2019.1.10）「[EXCLUSIVO] Así fue el intento de ciberataque a Redbanc en diciembre」
（http://www.trendtic.cl/2019/01/exclusivo-asi-fue-el-intento-de-ciberataque-a-redbanc-en-diciembre/）

②ZDNet（2019.1.16）「North Korean hackers infiltrate Chile's ATM network after Skype job interview」
（https://www.zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/）

③Gigazine（2019.1.22）「北朝鮮との関連が疑われるハッカー集団が『求人広告』を使って銀行間ネットワークを担う企業に侵入」
（https://gigazine.net/news/20190122-hackers-infiltrate-chiles-atm-network/）

（１２）２．１３　Bank of Valletta（マルタ）の事案（主なもの）

①TIMES OF MALTA（2019.2.13）「Watch: BOV hackers' €13m in transactions 'being reversed' - Muscat」
（https://www.timesofmalta.com/articles/view/20190213/local/watch-cyber-attack-on-bov-created-international-transactions-of-13m.701930）

②TIMES OF MALTA（2019.2.25）「How BOV hackers got away with €13 million」
（https://www.timesofmalta.com/articles/view/20190225/local/how-bov-hackers-got-away-with-13-million.702800）

③MALTACHAMBER.ORG.MT（2019.3.4）「BOV Hackers Were Planning Second Attack At A Later Stage - Reports」
（https://www.maltachamber.org.mt/en/bov-hackers-were-planning-second-attack-at-a-later-stage---reports）

④maltatoday（2019.3.11）「HSBC warned of BOV hackers last year」
（https://www.maltatoday.com.mt/news/national/93525/hsbc_warned_of_bov_hackers

_last_year#.XPnrl417mpb）

⑤TIMES OF MALTA（2019.5.9）「Bank of Valletta recovers €10m stolen by hackers, plice abroad establish source of attack」
（https://www.timesofmalta.com/articles/view/20190509/local/bank-of-valletta-recovers-10m-stolen-by-hackers-police-abroad-find-who.709547）

（１３）３．１　Customer Security Programme（CSP）

SWIFT（2019.6.12閲覧）「Customer Security Programme（CSP）- Programme description」
（https://www.swift.com/myswift/customer-security-programme-csp/programme-description?tl=en#topic-tabs-menu）

（１４）３．２　Customer Security Controls Framework（CSCF）

SWIFT（2019.6.12閲覧）「Customer Security Programme（CSP）- SWIFT Customer Security Controls Framework」
（https://www.swift.com/myswift/customer-security-programme-csp/security-controls?tl=en#topic-tabs-menu）

以上