近年のサイバー攻撃事例から考え方の転換を迫られる金融分野のサイバーセキュリティ

吉川　浩史、齋藤　芳充

▌要　約▐

1. 近年の IT の発展によってサイバー攻撃の脅威は拡大している。組織的かつ高度な攻撃も登場し、経済・社会に重大な被害を及ぼすような事態が発生している。中でも金融はサイバー攻撃の標的となりやすく、世界的に見て攻撃件数が増加傾向にある。経済を支える基盤である金融には、重要インフラとしてサイバーセキュリティの向上が強く求められているが、日本の金融機関はサイバー攻撃に対する認識が十分ではないとの指摘がある。
2. 国外では金融機関に対するサイバー攻撃によって、大きな被害を受けた事例が存在する。100 以上の金融機関から計 10 億ドル以上を盗み出したカーバナック（Carbanak）や、不正取引への悪用を狙ってインサイダー情報を窃取した FIN4 といったサイバー犯罪集団の登場は、金融分野における新たな脅威となっている。また、政治的・思想的な理由からサイバー攻撃を行うアノニマス（Anonymous）が金融機関をターゲットとした大規模作戦を実行したことも確認されており、幅広い視野での警戒が必要である。
3. 日本の金融機関に対するサイバー攻撃の実態を見ると、法人全体の平均と比べて被害発生率が高くなっている。近年では標的が地銀・信金等の地域金融機関へとシフトしており、規模の大小や都市・地方を問わずサイバーセキュリティ向上が求められている。従来に比べて攻撃側の日本語能力が向上したことによって、巧妙な偽装メールを用いた手口が登場し、多数の被害が発生している点にも注意が必要である。
4. 金融分野に対するサイバー攻撃には、①攻撃対象の変化、②攻撃目的の多様化、③攻撃手法の高度化、④攻撃主体の変化という 4 つの変化が起きており、攻撃側が圧倒的優位に立つ基盤になっている。これを受け、サイバーセキュリティのあり方も、攻撃の完全防御からある程度の被害を前提とした損害最小化へと変化している。近年注目を集める FinTech を推進するためにも、金融機関は引き続きサイバーセキュリティ向上を意識することが求められる。

Ⅰ　サイバー空間におけるリスクの高まり

IT（情報通信技術）の発展に伴い、経済・社会活動の大部分がコンピュータやインターネットを通じて処理されるようになった。こうしたデータのやり取りによって仮想的な空間（サイバー空間）が形成されると、サイバー空間に対してデータの改ざん、窃取、破壊を行ったり、ネットワークを機能不全に陥れたりする行為（サイバー攻撃）が登場した。こうした行為への対応を目的として 2014 年 11 月にサイバーセキュリティ基本法[1]が制定され、その後「自由、公正かつ安全なサイバー空間」の創出、発展を目的としたサイバーセキュリティ戦略が政府によって策定された。

サイバー空間は、場所や時間の制約を受けることなく誰しもが容易に参加できるうえ、匿名性が高いために攻撃側が常に優位にあると言われている。さらに、攻撃側は 1 つの脆弱性を突くだけでよいのに対して、防御側は全ての脆弱性をカバーしなければならないという点も、攻撃側優位を確かなものにしている。最近では、国家レベルの組織的かつ極めて高度な攻撃者が登場し、経済・社会に重大な被害をもたらす事態が起きている。2015 年 12 月にウクライナで発生したサイバー攻撃による大規模停電はその一例であり、サイバー空間の脅威が、既に現実空間にまで及んでいることを示している。

また、IoT（Internet of Things[2]）化の進展は攻撃側にさらなる有利性をもたらすと考えられる。IPA（情報処理推進機構）は、2020 年までに家電、防犯機器、自動車、医療機器等、200 億個を超えるモノが IoT 化するとの予想を公表しており、ライフスタイルやビジネスを変革させるチャンスが拡大する一方で、サイバー攻撃の標的も増加していくことになる。

金融分野においては、インターネットバンキングやオンライン証券が登場した 2000 年前後から、サイバーセキュリティは重要なテーマであった。しかし、金融分野を狙った新しいサイバー攻撃の登場によって、金融機関に求められるサイバーセキュリティのあり方が変化してきている。

Ⅱ　サイバー攻撃の標的となる金融分野

金融分野は、その機能・サービスが社会・経済を支える基盤となっていることから、重要インフラ分野としてサイバー攻撃対策に万全を期すことが強く求められている[3]。なお、

1　サイバーセキュリティ基本法第 2 条によって、サイバーセキュリティが「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において、電磁的方式とする）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む）が講じられ、その状態が適切に維持管理されていることをいう」と定義された。

2　モノとインターネットが繋がって、ネットワークを介して情報の収集や制御が可能になること。

3　サイバーセキュリティ戦略では情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流の 10 分野を重要インフラとして位置づけた。その後、新たな分野の追加が検討され、化学、クレジット、石油が加わっている。

金融分野において現在想定されている脅威に関しては、金融庁によって類型化されたものが、対処していく範囲（スコープ）として公表されている（図表 1）。一般的に、金融機関は「そこにお金がある」ことが明らかであるため、他の産業に比べて経済的な利益を目的としたサイバー攻撃の標的となりやすい。さらに、重要インフラとしての社会に与える影響の大きさから、政治的・思想的理由によって狙われる可能性も高くなっている。しかし、日本の金融機関は、直接のサイバー攻撃を通じた顧客情報の漏えいや金銭の窃取による大規模な被害を経験したことがなく、基幹システムが隔離されたネットワーク環境下にあるという安心感から、サイバーセキュリティに対する認識が十分でないとの指摘がされている[4]。

世界的には、金融分野において 2015 年で約 8,289 万件の情報セキュリティ事象が検知されており、前年比で約 30%の大幅な増加となっている（図表 2）。この数値は検知されたもののみを反映しているため、検知をすり抜けた攻撃の存在を考えると、実際の状況はこれを上回っていると思われる。情報セキュリティ事象による被害では各種情報漏えいの経験が多く報告されているが、金融機関に存在する金銭を直接狙ったサイバー攻撃によって大きな損害を被ったケース等も既に確認されている（図表 3）。セキュリティベンダーのカスペルスキー（Kaspersky）は「世界で起きていることはいずれ日本でも起こる」として、サイバー攻撃に対する注意喚起を行っており[5]、日本の金融機関は国外の攻撃事例を踏まえつつサイバーセキュリティ向上の取り組みを進めていく必要がある。

次節では、金融分野を狙ったサイバー攻撃の中でも、今後のサイバーセキュリティのあり方を考えるうえで重要と思われる事例を取り上げ、詳しく説明する。

図表 1　金融分野のサイバーセキュリティとして対処していくスコープ

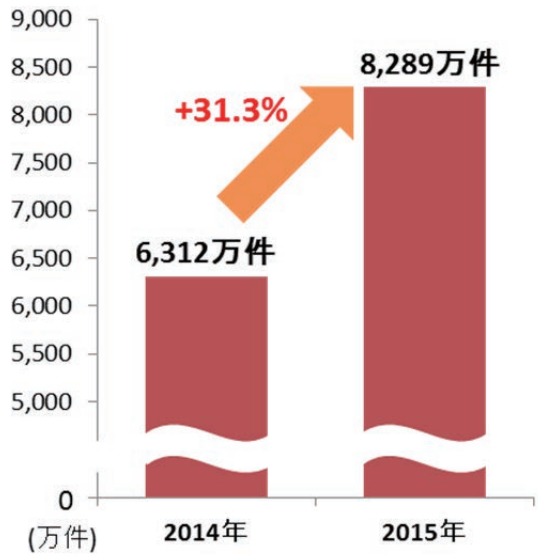
<table>
<tr><th>攻撃者の動機</th><th>対　象</th><th colspan="2">脅　威</th><th>関連する既存のリスク管理体制</th></tr>
<tr><td rowspan="2">社会秩序の混乱</td><td rowspan="3">金融機関</td><td rowspan="2">金融機関・金融インフラの機能停止</td><td>金融機関が直接サイバー攻撃から攻撃されるもの</td><td rowspan="2">業務継続（BCM）等</td></tr>
<tr><td>人的(故意・過失を問わない内部者)に、システムがマルウェア(注)に感染させられ、機能停止に陥るもの</td></tr>
<tr><td rowspan="3">経済目的</td><td rowspan="2">機密漏洩</td><td>金融機関が直接サイバー攻撃から攻撃されるもの</td><td rowspan="2">情　報セキュリティ管理等</td></tr>
<tr><td>人的(故意・過失を問わない内部者)に、システムがマルウェアに感染させられ、サイバー空間から機密漏洩</td></tr>
<tr><td>顧　客</td><td>不正送金等の不正取引</td><td>金融機関のコンピュータがマルウェアに感染して不正送金等の不正な取引がなされるもの</td><td rowspan="2">顧客保護等</td></tr>
<tr><td colspan="2"></td><td>顧客のコンピュータがマルウェアに感染して、顧客の意志に反した指示が金融機関になされるものや、フィッシング詐欺等</td></tr>
</table>

（注）　マルウェアとは、悪意のあるソフトウェアの総称。
（出所）金融庁資料より野村資本市場研究所作成

[4] 金融情報システムセンター「金融機関におけるサイバー攻撃対応に関する有識者検討会報告書（2014 年 2 月 26 日）」参照。
[5] カスペルスキー ウェブサイト（https://blog.kaspersky.co.jp/kaspersky-lab-predictions-2016-japan-asia/9893/）参照。

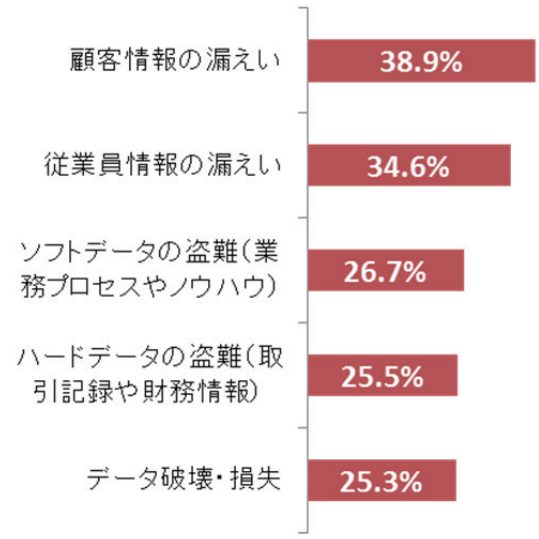
図表 2　金融機関において発生した情報セキュリティ事象

情報セキュリティ事象の検知件数



（出所）IBM, “Cyber Security Intelligence Index”より野村資本市場研究所作成

情報セキュリティ事象による被害の経験



（出所）PwC, “The Global State of Information Security Survey”より野村資本市場研究所作成

図表 3　国外での金融分野を狙ったサイバー攻撃の事例

発生月	発生国	被害内容
2014 年 1 月	韓　国	クレジットカード会社 3 社から、内部者によって約 8,500 万件の個人情報が盗まれる
2 月	英　国	銀行から約 2 万 7,000 件の個人情報が盗まれる
6 月	米　国	銀行からハッカーによって約 8,300 万件の個人情報が盗まれる
12 月	米　国	企業の経営層や法律事務所、コンサルティング会社等 100 社以上でメールが監視され、未公表情報が流出していたことが発覚
2015 年 1 月	エクアドル	銀行間決済ネットワークからの不正な送金指示によって 1,200 万ドルが盗まれる
2 月	露・米等	金融機関の送金システムに侵入され、不正な送金指示によって、2013 年からの 2 年間で 10 億ドルが盗まれていたことが発覚
8 月	米　国	上場企業の未公表情報を盗み、不正取引で 1 億ドル以上の利益を得ていた犯罪グループが摘発される
2015 年末	ベトナム	銀行間決済ネットワークからの不正な送金指示（1,000 万ユーロ分）があったが、未遂に終わる
2016 年 2 月	ﾊﾞﾝｸﾞﾗﾃﾞｼｭ	銀行間決済ネットワークからの不正な送金指示によって 8,100 万ドルが盗まれる
5 月～6 月	世界各国	複数の金融機関のウェブサイトが DDoS 攻撃を受け、閲覧できない状態となる

（出所）各種報道資料より野村資本市場研究所作成

Ⅲ 金融分野を狙ったサイバー攻撃の事例

１．世界 100 の金融機関から 10 億ドルを盗んだカーバナック

サイバー犯罪グループのカーバナック（Carbanak）は経済的な利益獲得を目的に、標的型攻撃（Advanced Persistent Threat、APT）と呼ばれる手法で、2013 年から 2 年間にわたりロシアや米国を中心に 100 もの金融機関に攻撃を仕掛け、10 億ドルを盗み出したとされている[6]。彼らはロシアやウクライナ、中国のサイバー犯罪者で構成される多国籍グループであるとの見方が報告されており、国際刑事警察機構（インターポール）や欧州刑事警察機構（ユーロポール）による共同捜査が行われているが、未だ逮捕の報道は出ていない。

具体的な手口は、次の通りである。

１）事前準備

カーバナックは、事前準備としてダークウェブから銀行の従業員のコンピュータへのアクセス権限を購入していたと見られている。ダークウェブとは一般的なインターネットブラウザではアクセスできないウェブサイトを指し、通信を匿名化するソフトウェアを用いることで閲覧が可能となる。ダークウェブ上には、拳銃や違法薬物、偽造書類、違法賭博等を取り扱うサイトが多数存在しており、サイバー攻撃用のハッキングツール、サイバー攻撃によって盗まれたアカウント情報やコンピュータのアクセス権の売買を行う闇市場も確認されている。オンラインサービスのアカウント情報は 1～10 ドルで販売されており[7]、このアカウント情報に含まれているメールアドレスのアカウントをハッキングして情報収集を行う。オンラインサービスのパスワードをメールアドレスのログイン情報にも使い回している場合、メールアカウントへの侵入を容易に許してしまうこととなる。

２）侵入・感染

メールアカウントから交友関係や職務関係に関する情報を収集すると、標的を定めて通常業務のやりとりに偽装させたフィッシングメールを送信する。このメールの添付ファイルを開いたコンピュータはマルウェアに感染し、カーバナックの監視下となって、外部から秘密裏に操作可能な状態となる。このコンピュータは外部からの不正操作によって行内ネットワーク上にあるコンピュータへ次々とフィッシングメールを送信し、感染を拡大させる。

---

6 カスペルスキー ニュースリリース（2015 年 2 月 18 日）参照。

7 なお、ダークウェブ上の闇取引ではビットコイン等の仮想通貨が用いられることが多いという。（トレンドマイクロ ウェブサイト参照。）

３）潜伏・実行

感染が送金システムの担当者にまで達したことがわかると、カーバナックはシステム担当者の日々の業務画面を監視して送金手順に関する情報収集を行う。送金作業の手順を把握した後は、秘密裏に担当者のコンピュータを遠隔操作し、通常の作業手順を装って不正送金を実行する。

カーバナックはこの一連の作業を 2～4 か月程かけて行い、1 度に最大で 1,000 万ドルを窃取した。金融機関の不正取引検出システムが顧客口座の金銭の動きのみを監視対象としていることに目をつけたカーバナックは、金融機関の内部手続きを模倣する手口によって既存のセキュリティをすり抜けることに成功している。

カスペルスキーはこの事件について、「金融機関を狙ったサイバー犯罪活動が新たな段階に入り、標的を金融機関の利用者から銀行自体に移し、直接攻撃して金銭を窃取し始めた」と述べており、サイバー犯罪の転換点として捉えている。

2016 年 2 月には、金融機関ではなく企業の経理部門を標的としてカーバナックが再び活動を始めたことが報告されており、企業の口座ログイン情報を窃取して口座の保有者情報を改竄し、現金を引き出すといった手口が確認されている[8]。

２．上場企業のインサイダー情報を不正取得していた FIN4

セキュリティベンダーのファイア・アイ（FireEye）が発表したレポート[9]によると、FIN4 は遅くとも 2013 年半ばから企業のインサイダー情報を得るために関係者のメールアカウント情報を窃取していた犯罪グループである。米国を中心に 100 社以上の企業が標的となり、そのうち 3 分の 2 以上がヘルスケア・製薬業界の企業、残りは M&A に関する助言を行うコンサルティング会社や法律事務所であったとされている。FIN4 がヘルスケア・製薬業界を重点的に狙った理由は、臨床試験の結果や規制に関する決定等によって株価が大きく変動するためだと考えられている。実際に FIN4 は、医薬品開発や保険料率、係争中の訴訟といった情報にアクセスしていたことがわかっている。

具体的な手口は次の通りである。

１）ログイン情報の窃取

M&A や IR に関する偽造文書が添付されたフィッシングメールを標的の企業へ送付する。この文書を開くとメールアカウント情報の入力を求める偽のログイン画面が表示され、入力したアカウント情報は FIN4 に窃取されて監視下に入ることとなる。偽造文書の多くは、実際の M&A 案件で使用された文書を元に作成されており、フィッシングメールの内容にも受信者の興味を引き付けるような工夫がされていたことがわかっている（図表 4）。

[8] カスペルスキー ニュースリリース（2016 年 2 月 29 日）参照。
[9] ファイア・アイ「ウォール街をハッキング？市場をもてあそぶ FIN4 グループ」参照。

図表 4　FIN4 が経営幹部に送ったフィッシングメールの例

件名	従業員による貴社に関する告発文の投稿について

株式掲示板に、従業員を名乗るユーザー（FinanceBull82）から、貴社の役員報酬と役員の能力に関する告発文が投稿されています。この文章で示されている具体例の中には、まだ検討中の未公表情報が含まれている可能性があります。
従業員にも意見を述べる権利があるのはもちろん承知しておりますが、顧客として、このことが将来のビジネスに悪影響を及ぼすのではないかと危惧しております。この投稿が行われる前に、何らかの方法で彼の不満をくみ取ってやるべきだったのではないでしょうか。
掲示板へのリンクは次のとおりです（2 番目の投稿が告発文です）。
http://(偽のログインページへの URL)/

当該従業員と話をしていただけますか。
よろしくお願いします。
××　××

（出所）ファイア・アイ資料をもとに野村資本市場研究所作成

２）情報網の拡大

FIN4 は、手に入れたメールアカウントを不正に操作して、新たな標的へとフィッシングメールを送付する。この段階で送られるフィッシングメールは、実在するアカウントから既存のやり取りに対する返信の形式をとっており、通常のメールとの区別が極めて困難なものとなる。

３）情報の窃取・隠ぺい工作

ログイン情報の窃取とフィッシングメールの送信を繰り返して情報網を拡大し、インサイダー情報の不正入手を行う。乗っ取ったアカウントに対しては、サイバー攻撃に関する指摘・注意を行う単語[10]を含んだ電子メールを自動削除するようなフィルタリングを設定し、攻撃の発覚を遅らせようと工作していたこともわかっている。一連の手口はマルウェアの感染を伴わないことから、アンチウィルスソフトウェア等による検知が難しく、被害の発覚を遅らせる要因となった。

FIN4 は、不正に入手したインサイダー情報に基づく不公正取引で多額の利益を得たとみられており、ファイア・アイは SEC と FBI に対して情報提供を行っている。しかし、このグループが摘発されたという事実はまだ確認されていない。

似たような事例として、米国でプレスリリース配信会社のシステムに侵入してインサイダー情報を入手し、5 年間にわたって不公正取引を続けて 1 億ドル以上の利益を得たグループの存在が明らかになっており、2015 年 8 月に摘発されている[11]。このグループは、高レバレッジの証券 CFD（Contract For Difference）取引[12]を通じて不公正

[10] 例として「hacked（ハックされている）」、「phish（フィッシング）」、「malware（マルウェア）」といった単語が紹介されている。
[11] 米 SEC プレスリリース（2015 年 9 月 14 日）参照。
[12] 少額の証拠金を預託し、有価証券や有価証券指数等を対象資産として取引する差金決済取引のことを指す。

取引を行っていたことがわかっている。証券 CFD 取引は、取引所へ発注される名義がカバー先や取扱会社となることから個別の投資家の動きが掴みにくく、不公正取引の温床となる懸念が日本でも指摘されている[13]。

これらのサイバー攻撃は、インサイダー情報の窃取を通じた不公正取引が、金融商品市場の信頼性・公平性に対する新たなリスクとして顕在化していることを示している[14]。

３．金融機関に対する大規模攻撃を宣言したアノニマス

先に述べた 2 グループが経済的な利益を目的とした犯罪グループ（Criminals と呼ばれる）であるのに対して、アノニマス（Anonymous）は政治的・思想的な理由によってサイバー攻撃を行うグループ（Hacktivists と呼ばれる）である。彼らは階層的な指揮系統を持たない緩い繋がりの組織であり、その時々の発案者の思想に賛同する不特定多数のメンバーがサイバー攻撃を実行する。2016 年 5 月にはイカロス作戦（OpIcarus）と称して、金融機関に対する大規模攻撃を宣言し（図表 5）、いくつかのウェブサイトを閲覧できない状態にした（「TANGODOWN」という単語を使用）とツイッター上等で報告を行っている（図表 6）。同年 6 月からは証券取引所を攻撃対象に加えた次の作戦（Project Mayhem）を実行している。一連の作戦において、日本銀行と東京証券取引所等のウェブサイト[15]が標的リストに含まれていたが、現時点で攻撃報告は確認できていない。

図表 5　ウェブサイトに掲載された声明文（抜粋）

銀行をシャットダウンせよ #OpIcarus

…軍需産業、金融機関、政府の諜報機関やその他の組織は、密かに連合を形成して、腐敗と強欲にまみれているということが、ウィキリークスとアノニマスによって明らかとなった。この連合は権力を永続化しようと、ビルダーバーグ・グループや CFR といったシンクタンクを司令塔として、IMF や FRB、世界銀行を通じて影響を及ぼしている。合衆国大統領や内閣は彼らの傀儡であり、アノニマスの思想・作戦の広がりや、影の権力者の存在が暴かれることを阻んでいる。では影の権力者はどこにいるのか。それは、NY 証券取引所とイングランド銀行を中心としたグローバル金融システムの中である。

…影の権力者たちはイカロスのように太陽に近づきすぎたために、翼は燃え落ち、彼らが依存するシステムも崩壊の時が迫っている。我々は、今一度この構造を破壊して帝国の中枢を討たなければならない。今こそはるか大きな目標であるグローバル金融システムに立ち向かう時である。…

（出所）OpIcarus ウェブサイトより野村資本市場研究所作成

[13] 日本証券業協会「証券 CFD 取引ワーキング・グループ最終報告書」（2010 年 3 月 16 日）参照。
[14] 日本においては、サイバー攻撃によって未公表情報を盗み出した場合、金商法 166 条で規定される内部者に該当しないため、インサイダー取引規制の適用外になるのではないかという指摘もある。（2015 年 1 月 27 日産経ニュース）
[15] 東京証券取引所、福岡証券取引所、JASDAQ、名古屋証券取引所、大阪証券取引所（大阪取引所）、札幌証券取引所の名前がリストに含まれていた（うち東京証券取引所、JASDAQ、大阪取引所は合併前の URL）。

図表 6　イカロス作戦において攻撃完了報告があった金融機関等

・アラブ首長国連邦中央銀行	・NYSE ユーロネクスト
・イラク中央銀行	・アテネ証券取引所
・サウジアラビア通貨庁	・カナダ証券取引所
・スイス中央銀行	・パナマ証券取引所
・タンザニア中央銀行	・フィリピン証券取引所
・フィジー連邦準備銀行	・ミュンヘン証券取引所
・フィリピン中央銀行	・ルーマニア証券取引所
・ベネズエラ中央銀行	・ロンドン証券取引所
・ベリーズ中央銀行	・HSBC
・ボストン連邦準備銀行	・JP モルガン・チェース銀行
・ポルトガル中央銀行	・中国工商銀行
・モンテネグロ中央銀行	・連邦住宅抵当公庫
・韓国銀行	…等

（出所）野村資本市場研究所作成

アノニマスの攻撃の殆どは、サーバーに大量のデータを送って処理を遅らせる DoS/DDoS 攻撃[16]と呼ばれるもので、被害はホームページの閲覧障害等の限定的なものに留まる。この攻撃に特殊な技術は必要なく、アノニマスが配布する攻撃ツールをダウンロードして使用することで容易に参加できる。最近では、DoS/DDoS 攻撃を陽動として用いることでセキュリティ担当者の注意をそらし、その間に他の攻撃を仕掛けるというケースが報告されている[17]。アノニマスには決まった指揮系統がないため、今後、ある標的を狙った犯罪グループが、もっともらしい思想でメンバーを扇動し、DoS/DDoS 攻撃を行う囮部隊として用いる可能性が危惧される。

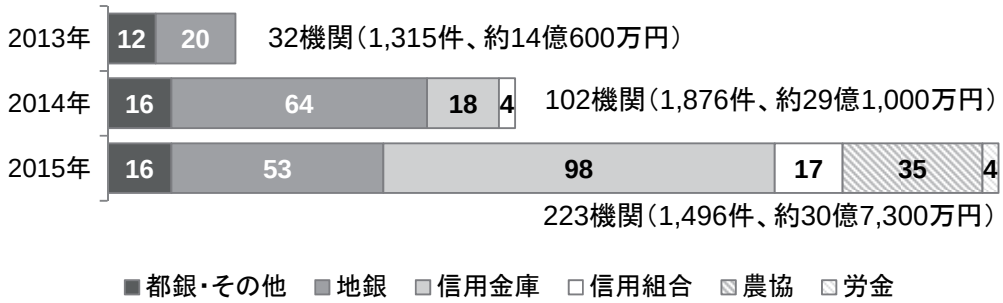
Ⅳ 日本におけるサイバーセキュリティ

これまで日本は、日本語が障壁となっていたために国外に比べるとサイバー攻撃の標的となる機会は少なかった。しかし、近年の自動翻訳サービスの精度向上やサイバー犯罪グループの多国籍化によって、言語の問題は解決されつつあると考えられる。潤沢な金融資産を持ちながら、これまで脅威に晒されなかったために欧米よりもセキュリティ意識が低い日本はサイバー攻撃の恰好の標的となり得る。

図表 7 は、金融機関別にインターネットバンキングによる不正送金被害の状況をまとめたものである[18]。2014 年に地銀の被害が拡大したことをきっかけに、被害件数・被害額が大きく増加している。2015 年には、信金・信組、農協や労金といった小規模金融機関の被害が大幅に増加した。こうした地域金融機関は、都銀に比べるとサイバーセキュリティ

[16] Denial of Service attack、Distributed Denial of Service attack の略。複数のコンピュータから行われる DoS 攻撃を DDoS 攻撃という。
[17] カスペルスキー ニュースリリース（2016 年 1 月 7 日）参照。
[18] 警察庁「平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について（2016 年 3 月）」参照。

図表 7　金融機関別インターネットバンキングに係る不正送金の被害



（出所）警察庁資料より野村資本市場研究所作成

に充てられる予算が少ないため、対策も手薄になってしまうケースもあると考えられ、その点をサイバー犯罪者が狙ったものと思われる。こうした事態を受け、金融機関はワンタイムパスワードや電子証明書の導入を進めているが、被害口座の多くは利用者自身がこうしたセキュリティ対策を導入していなかったことがわかっている。サイバー犯罪者は規模の大小や都市・地方を問わずに攻撃しやすい相手を標的としており、あらゆる金融機関が常にサイバー攻撃のリスクに晒されているということを金融機関自身とその利用者は意識する必要がある。

1．金融機関そのものを狙ったサイバー攻撃の状況

2016 年の調査では、法人の約 4 割が深刻なセキュリティインシデント[19]を経験していることが明らかになっており、金融は、全体平均に比べて発生率が高い分野の一つである（図表 8）。インシデント別に発生状況を見ると、全体平均よりも概ね高い数値が出ている中で、特にウィルス感染が多く報告されている。実害の発生状況では各種情報漏えいによる被害が多い（図表 9）。しかし、これらの数値はアンチウィルスソフトによる検知や

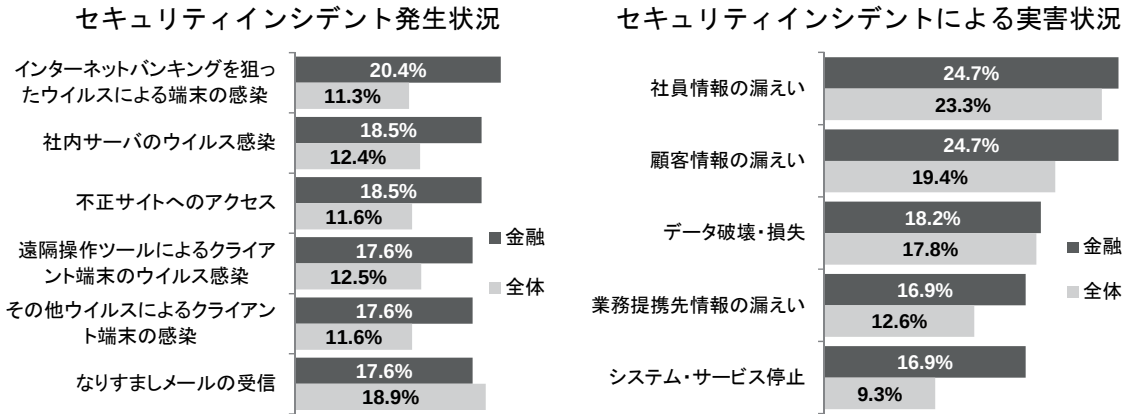
図表 8　深刻なセキュリティインシデント発生率上位 5 業種

順　位	業　種
1 位	中央省庁（57.8%）
2 位	**金融（49.1%）**
3 位	建設・不動産（48.1%）
4 位	都道府県庁（44.4%）
4 位	情報サービス・通信プロバイダ（44.4%）
―	全体（38.5%）

（出所）トレンドマイクロ「法人組織におけるセキュリティ対策実態調査」より野村資本市場研究所作成

[19] ビジネスに影響のある被害を伴うインシデントを指す。

図表 9　セキュリティインシデントの発生状況と実害の発生状況（金融上位 5 項目）



（出所）トレンドマイクロ「法人組織におけるセキュリティ対策実態調査」より野村資本市場研究所作成

ネットワーク監視等で認知された事象のみを反映した結果である。あくまでも氷山の一角であって、水面下ではこれ以上に深刻な被害が発生していることが予想される。

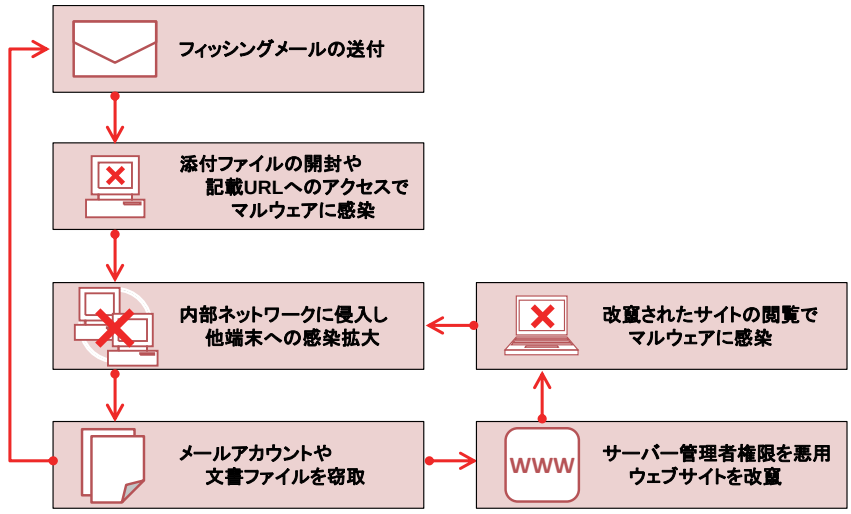
２．高度化したサイバー攻撃の登場

インシデントには、独立的に発生したものだけでなく、先に紹介した海外の事例にあるような特定の標的に特化させた標的型攻撃の過程で複合的に実行されたものも含まれていると考えられる（前掲図表 9）。日本をメインターゲットとする標的型攻撃が初めて確認されたのは 2014 年 10 月[20]のことで、「ブルーターマイト」と呼ばれている。ブルーターマイトは 2015 年 6 月時点で、銀行、金融サービスを含む少なくとも 300 以上の組織への侵入に成功したとみられている。この攻撃は標的の文書ファイル等機密情報の窃取を目的としており、既にエネルギー関連や防衛関連での流出事例が報告されている。2015 年の日本年金機構に対するサイバー攻撃もブルーターマイトによるものと考えられており、報告書[21]では、巧妙に偽装されたフィッシングメールが使われていたことが公表されている。メールの文章には業務に関連する内容が具体的に書かれており、偽装のレベルが個人の注意だけで開封を防ぐことが困難な域にまで達していることがわかる。

さらにブルーターマイトは、クラウドサービスを提供している情報通信業者のサーバー管理者権限の窃取に成功していることが判明している。この権限を悪用し、当該サーバーで運用されているウェブサイトに対して、閲覧者のコンピュータの脆弱性を突いてマルウェアを感染させるよう改竄し、新たな攻撃[22]の起点としていることも確認された（図表 10）。2015 年 5 月時点で、国内の数千のドメインがブルーターマイトの手中にあるとみられている。改竄によって埋め込まれた仕掛けの中には、ベンダーによる修正パッチがま

[20] カスペルスキー ニュースリリース（2015 年 8 月 20 日）参照。
[21] 日本年金機構「不正アクセスによる情報流出事業に関する調査結果報告（2016 年 8 月）」参照。
[22] 標的がよくアクセスするウェブサイトを改竄して待ち受けるこの手法は「水飲み場攻撃」と呼ばれる。

図表 10　ブルーターマイトの感染拡大経路



（出所）カスペルスキー資料より野村資本市場研究所作成

だリリースされていない未知の脆弱性（ゼロデイ脆弱性）を狙ったものもあり、感染の予防も難しくなってきている。

サイバー攻撃によってインサイダー情報を窃取し不正取引を行う手口は日本ではまだ確認されていないが、近いうちに起きる可能性は非常に高いと思われる。ブルーターマイトが機密情報の窃取に成功していることを考えれば、明らかになっていないだけで既に実行されている可能性もある。証券取引等監視委員会は、「わが国では米国と異なり、未公表の会社情報が大規模にハッキングされるおそれは殆どない」と述べているが[23]、認識を改める必要があるだろう。金融庁は 2013 年に、「公表前の情報を外部者が利用して取引が行われた場合、市場の公正性が著しく損なわれるおそれがある」との注意喚起を発出しており[24]、サイバー攻撃によるインサイダー情報の窃取が、市場の公正性・公平性を大きく傷つける脅威であることは間違いない。

V　サイバーセキュリティの今後

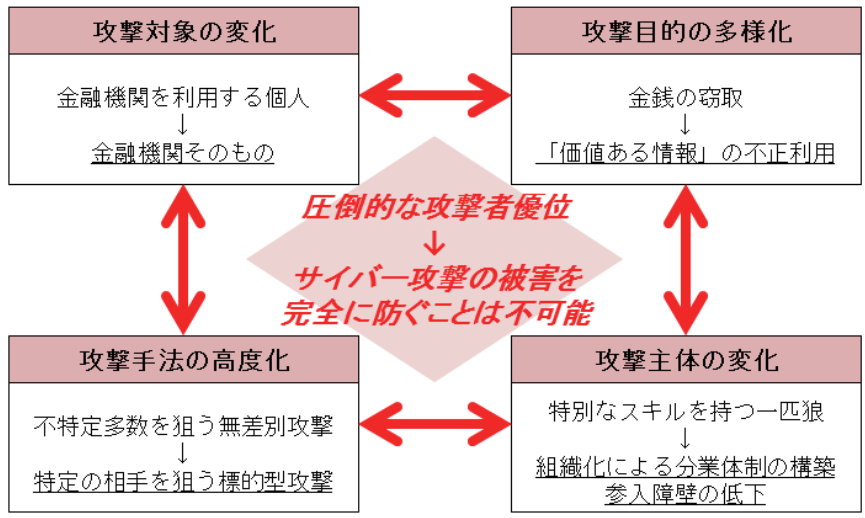
1．サイバー攻撃の変化

ここまで述べた事例から考えると、金融分野に対するサイバー攻撃には次のような変化が起きている（図表 11）。

第一は攻撃対象の変化である。これまで金融分野におけるサイバー攻撃は、インターネットバンキング利用者のログイン情報を窃取して口座から金銭を盗み出すといったもの

[23] 証券取引等監視委員会「証券取引等監視委員会の活動状況（2016 年 6 月）」参照。
[24] 金融庁「上場会社等が法定開示書類及び適時開示事項を自社ウェブサイト等に掲載する場合の留意事項について（2013 年 4 月）」参照。

図表 11　金融分野に対するサイバー攻撃の変化



（出所）野村資本市場研究所作成

が主流であって、金融機関はワンタイムパスワードや不正取引検出ソフト等を導入して対策を講じてきた。利用者への攻撃が難しくなったサイバー犯罪者は、このようなセキュリティ対策が行われていない口座に標的をシフトさせるだけではなく、一度に巨額の金銭を得られる可能性が高い金融機関そのものを狙って執拗な攻撃を行うようになっている。

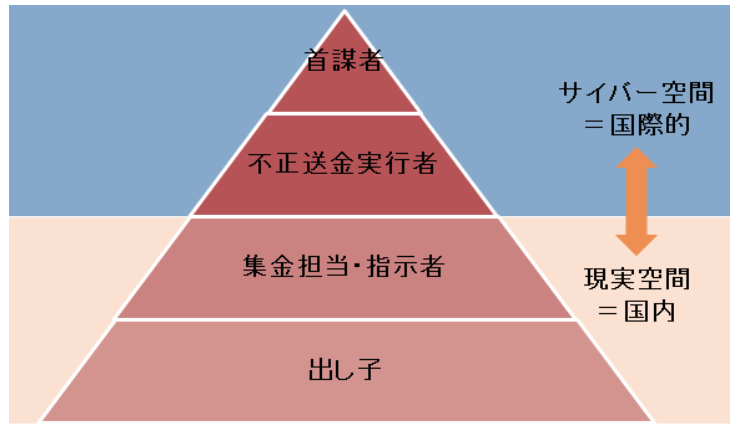
第二は攻撃目的の多様化である。金銭を直接窃取することを目的としたサイバー攻撃だけでなく、インサイダー情報や個人情報といった「価値のある情報」を狙った攻撃が確認され始めた。この攻撃を行った主体は、インサイダー情報を利用した不公正取引やダークウェブ上での個人情報の販売によって大きな利益を得たと考えられる。サイバー犯罪者の目的は金銭の窃取だけでなく、銀行や証券会社、保険会社が保有する「価値のある情報」の悪用によって不正利益を得ることにまで拡大してきている。金融機関側は守るべき情報が増え、セキュリティの確保がより難しい状況となっている。

第三は攻撃手法の高度化である。サイバー犯罪者の攻撃対象が個人から金融機関に移り、一度に得られる金銭的価値が増大することによって、一つの攻撃にかけられる労力が増し、攻撃内容も高度かつ執拗なものへと進化していった。フィッシングメールをただ闇雲にばらまくようなことはせず、事前の情報収集を行ったうえで標的のシステムやセキュリティの脆弱性を突くように個別にカスタマイズした攻撃[25]を行うようになっている。

第四は攻撃主体の変化である。サイバー犯罪者というと、映画やドラマでは特殊なスキルを持った一匹狼といったイメージで描かれることが多かった。しかし実際のサイバー犯罪者は組織化・ビジネス化しており、分業体制を構築して日々新しいサイバー攻撃を開発している。さらに、一部のサイバー犯罪者は自ら開発したハッキングツールをダークウェブ上で販売しており、特殊なスキルがなくとも悪意を持つ者であれば誰でもそれらを購入

[25] 問い合わせフォームから連絡を行って標的からの返信を待ち、やり取りの中でマルウェアを送る手法等が確認されている。

図表 12　インターネットバンキングの不正送金における犯罪組織の階層



（出所）野村資本市場研究所作成

してサイバー攻撃の基盤を構築することが可能であり、攻撃件数の増加要因となっている。

さらに、サイバー犯罪は場所に囚われることがないため、組織のメンバーの多国籍化が進んでおり、各国の法制度の違いや警察間の協力体制によっては追跡が困難になることも攻撃者にとって有利な状況に繋がっている。不正送金事件の報道を見ても、国内・国外を問わず、逮捕されているのは ATM 等で現金を実際に引き出す役の「出し子」と呼ばれる者たちが殆どである。こうしたサイバー犯罪組織は、図表 12 のような構造を持っていることが予想され、国外からサイバー空間上で犯行に及ぶ上位層は、複数サーバーの経由や通信暗号化等の技術を用いて隠蔽工作を行っているために、技術的・国際的な問題によって特定が困難になっているものと思われる。

これらの変化はサイバーセキュリティにおける攻撃者優位の構造をより強固なものとしており、サイバー攻撃による被害を完全に防ぐことを困難にしている。そのためサイバーセキュリティのあり方も、従来の攻撃させない・侵入させないという防御策から、感染や侵入を前提に、機密情報を持ち出させない・次の攻撃に繋げさせないといった被害の最小化を目指すものへと変わってきている。2015 年 7 月に金融庁が公表した「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」の中では「サイバー攻撃の手口の高度化・巧妙化が進み、どれだけあらかじめ対策を講じたとしても被害を受けてしまうことは生じ得る」として、ある程度の被害を前提とした対策の必要性を述べている。

2．次世代のサイバーセキュリティ

攻撃側と同様に、防御側にも変化が起きている。第 3 次ブームともいわれる人工知能（AI）の進化[26]とビッグデータ活用の波は、サイバーセキュリティの分野にも及んでおり、サイバー攻撃の検知・分析・対処という一連の作業を自動化させてセキュリティ向上に役

[26] 詳しくは、関雄太、佐藤広大、ラクマン ベディ グンタ「機械学習型人工知能とビッグデータの結合がもたらす金融サービス業の変化」『野村資本市場クォータリー』2016 春号を参照のこと。

立てようというソリューションが登場している。

サイバーセキュリティ・ベンチャーのサイランス（Cylance）[27]は、AI に約 5 億個のファイルやプログラム情報（マルウェアだけでなく、通常のファイルも含む）を読み込ませ、マルウェアに含まれる特徴を抽出させている。この特徴をもとにマルウェア検知のアルゴリズムを作成し、99%という高い検知率を持つセキュリティソフトの開発・提供を行っている。マルウェアかどうかは従来のアンチウィルスソフトのようにパターンファイル[28]との突合せではなく、マルウェア固有の特徴の有無で判定するため、未知のマルウェアであっても検知が可能であり、パターンファイルのデータベースを頻繁にアップデートする手間も必要ない。レコーデッド・フューチャー（Recorded Future）[29]はサイバー犯罪者の摘発にビッグデータ分析を活用することを提案している。4 年以上にわたってサイバー犯罪者が利用する 500 超のフォーラムでデータを収集し、74 万 2,000 のハンドルネームを追跡した結果、一見無関係と思われるアカウントの間でも活動スケジュールや話し方のパターンから関連性を発見でき、同一人物であることを特定することに至った[30]。活動スケジュールを詳しく調べれば、各国のタイムゾーンや休祝日と照らし合わせることで国籍の特定も可能であり、容疑者の絞り込みにも利用できると期待されている。サイランスとレコーデッド・フューチャーの技術は高い評価を受けており、米中央情報局（CIA）の立ち上げたベンチャーキャピタルであるインキューテル（In-Q-Tel）からの出資を受けている。

このように防御側で革新的な技術の活用が行われる一方で、こうした技術がサイバー犯罪者に悪用されるおそれもある。脆弱性の分析やフィッシングメールの送信、サーバーへの侵入等を AI が行うサイバー攻撃の自動化が実現すれば、攻撃の対象・件数は爆発的に増加するだろう。

３．日本の金融機関に求められるサイバーセキュリティの強化

日本では近年 FinTech が注目を集め、IT ベンチャー企業と金融機関との提携も進んでいる。インターネット上での金融サービスの提供が拡大することで、顧客の利便性向上等サービスの高度化が期待される一方で、提携先へのサイバー攻撃がネットワークを通じて金融システムにまで波及し、新たに導入される技術の未知の脆弱性がサイバー犯罪者に狙われるリスクが懸念される。金融機関が FinTech の活用を考える場合には、同時にサイバーセキュリティの確保を十分に考慮することが求められる。

世界では金融に対するサイバー攻撃による被害が拡大しており、米国の J.P.モルガン・チェース、バンク・オブ・アメリカ、シティバンク、ウェルズ・ファーゴ等は、サイバー

[27] https://www.cylance.com/
[28] 既知のマルウェアに特有のプログラムコードを登録したファイルのこと。
[29] https://www.recordedfuture.com/
[30] カスペルスキー ウェブサイト（https://blog.kaspersky.co.jp/math-catches-hackers/10374/）参照。

犯罪に対抗するために年間総額 15 億ドルもの費用を負担している[31]。日本の金融機関においても、サイバーセキュリティに対する意識向上と十分な態勢整備は喫緊の課題と言えよう。

2016 年 10 月には、金融庁主催によるサイバーセキュリティ演習が初めて実施される。80 の金融機関が参加するこの演習では、予め想定された攻撃シナリオに基づいて対応を行い、事後分析とフィードバックが行われる。これが日本の金融機関におけるサイバーセキュリティ意識向上のきっかけとなり、利便性と安全性を兼ね備えたより信頼性の高い金融システムの実現につながることを期待したい。

[31] "J.P. Morgan, Bank of America, Citibank And Wells Fargo Spending $1.5 Billion To Battle Cyber Crime," *Forbes*, Dec 13, 2015.