BOJ Reports & Research Papers

金融システムレポート別冊シリーズ

Financial System Report – Annex

IT の進歩がもたらす金融サービスの新たな可能性とサイバーセキュリティ

日本銀行
金融機構局
2016 年 3 月

【本レポートに関する照会先】
日本銀行金融機構局考査企画課（csrbcm@boj.or.jp）

（金融システムレポート別冊シリーズについて）

日本銀行は、マクロ・プルーデンスの視点からわが国の金融システムの安定性を評価するとともに、安定確保に向けた課題について関係者とのコミュニケーションを深めることを目的として、『金融システムレポート』を年２回公表している。同レポートは、金融システムの包括的な定点観測である。

『金融システムレポート別冊シリーズ』は、特定のテーマや課題に関する掘り下げた分析、追加的な調査等を不定期に行い、『金融システムレポート』を補完するものである。本別冊では、近年の IT（情報技術）の進歩がもたらす金融サービス分野の新たな可能性と、金融機関に求められるサイバーセキュリティの確保について取り上げる。

（本別冊の要旨）

近年、企業は、IT の進歩を積極的に活用することで、多様で変化の激しい顧客ニーズへの対応力を飛躍的に高めることが可能になっている。そうした働きの金融サービス分野における表れが FinTech（フィンテック）であり、伝統的な金融機関に該当しない担い手が、IT を活用して格段に高い利便性や大幅なコスト削減を実現しつつ、新たな付加価値を持つ金融サービスを提供している。

金融機関内および金融機関間でこれまで構築されてきたシステムは、精緻な機能設計と連動性の高さ、取引の安全性などに特徴があるが、上述の環境変化の中で、投資額の大きさや維持管理、変更作業の重さが意識されるようにもなっている。金融機関にも、IT の進歩を活用して、金融サービス分野で新たな付加価値を創出するチャンスがある。ただ、金融機関にとっての IT 戦略は、FinTech の取り込みに限定されるものではなく、サービスの高度化、顧客との接点の拡充、マーケティング力の強化、業務プロセスやコスト構造の革新、顧客情報の能動的な分析・管理など、経営戦略と表裏一体をなすものである。明確な戦略のもとでの IT 活用、システム開発の力が競争力を左右する要素の一つになっていくと考えられる。

また、IT 活用にあたっては、インターネットを通じる取引の信頼性や安全性の確保、具体的には、サイバーセキュリティの確保が前提条件となる。サイバー攻撃の目的毎に異なる金融システムへの影響度合いや、「ネットワーク」と「外縁部」に着目した対応が重要である。体制面では、経営陣の積極的な関与、サイバー攻撃を受けた後の迅速な影響範囲の特定・対応、幅広い情報の収集と共有が求められる。

日本銀行は、以上の認識のもと、IT 技術やその金融面の活用について研究と情報発信を行うとともに、個別金融機関の実情に応じた IT 戦略の策定やサイバーセキュリティの強化を促していく。

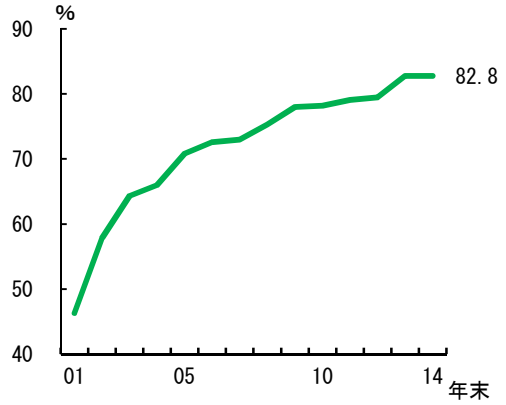
１．IT の進歩がもたらす金融サービス分野の新たな可能性

（１）インターネットの利用拡大とその含意

近年、インターネットの利用が一層拡大しており、わが国での普及率は 2014 年末で 8 割を超えているとの調査結果もみられる（図表 1）。

この背景には、CPU やメモリなどの性能向上や価格低下、通信回線の高速・大容量化、さらにはスマートフォンやタブレットなどのモバイル端末の急速な普及（図表 2）といった IT の進歩がみてとれる。また、ソフトウェアやデータを必要なときに必要なだけ利用できるクラウドサービスなど、関連するサービスが拡充されてきたことも、インターネットのさらなる普及に寄与している。

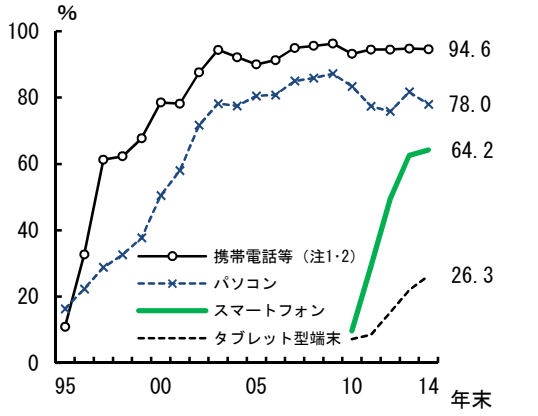
図表１　わが国のインターネットの人口普及率の推移



（注）人口普及率は、通信利用動向調査の回答者（世帯毎ではなく各世帯構成員毎）に占めるインターネット利用者の割合。

（資料）総務省

図表２　情報通信端末の世帯保有率の推移



（注 1）携帯電話、PHS、携帯情報端末（09 年末～12 年末）、スマートフォン（10 年末以降）を含む。

（注 2）95 年末から 97 年末までは、携帯電話と PHS を併用している世帯が二重計上されている。なお、98 年末時点の併用世帯の割合は 8.5%。

（資料）総務省

この間、モバイル端末の普及により、通勤・通学時や外出先など、人々がインターネットを手軽に利用できる機会が格段に増加した。また、インターネット経由でダウンロードできる様々なアプリケーション[1]を利用することで、端末の用途が飛躍的に拡大した。

企業の側からみると、これらを活用することで、店頭での応対などに比べ、遥かに多くの、幅広い顧客に対して、多様なサービスを提供することが可能に

[1] 目的に応じて利用されるソフトウェア（アプリケーション・ソフトウェア）。

なっている。

また、クラウドサービスやオープンソース・ソフトウェア[2]を利用することで、サーバなどのシステム基盤の構築やアプリケーションの開発に要する時間や費用を大幅に節減できるようになった。この結果、企業は、インターネットを活用したサービスを、より早く、より安く提供することが可能になっている。

このように、近年の IT の進歩を積極的に活用することで、企業は、多様で変化の激しい顧客ニーズへの対応力を飛躍的に高めることが可能となっている。

（２）金融サービス分野の変化

金融機関における IT の活用状況

わが国の金融機関[3]は、インターネットが普及する前から、IT の進歩を積極的に活用し、業務のシステム化やネットワーク化を進めてきた。具体的には、1960 年代以降、他の多くの産業に先駆けてコンピュータ・システムを導入し、窓口事務や勘定処理を含む後方事務、顧客情報管理や市場・国際業務、リスク管理業務などをシステム化するとともに、本支店間や金融機関間のネットワーク化を推進し、拡充してきた[4]。また、地域銀行では、1990 年代後半以降、ハードウェアの一層の性能向上や仮想化技術[5]のさらなる普及などを背景に、勘定系システムを中心にシステムの共同化が急速に進展した（図表 3）。

これらの金融機関内および金融機関間のシステムは、精緻な機能設計と連動性の高さ、取引の信頼性・安全性に特徴があり、確実かつ効率的な事務処理に大きな役割を果たしてきた。また、地域銀行のシステム共同化は、自社のシステム要員を削減しつつ、システムの安全性（機密性）や安定性（可用性）、業務継続能力を向上させた（図表 4）。これらの有用性は失われていないが、一方において、後述するような IT の飛躍的進歩、FinTech（フィンテック）の登場といった環境変化の中で、勘定系システムに代表される既存システムの投資額の大きさ、維持管理の重さや仕様変更などにかかる柔軟性・迅速性の欠如がより強く意識されるようにもなっている。

---

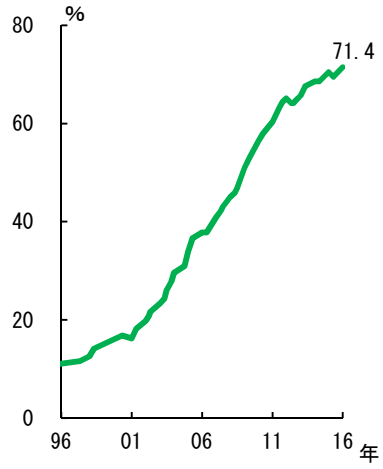
[2] ソースコードを広く無償で公開し、誰でも扱えるようにしたソフトウェア。

[3] 本稿では、主として預金取扱金融機関を想定している。

[4] 例えば、1973 年に全国銀行データ通信システム（全銀システム）が稼働を開始し、オンライン処理による金融機関間の内国為替取引が可能となった。その後も同システムは増強を続け、1990 年頃までには、全国へのリアルタイム送金や各種の自動引落・振込が可能となった。

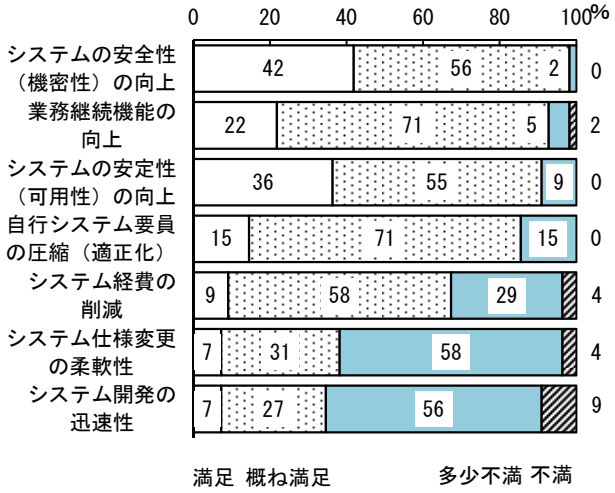
[5] コンピュータ資源をハードウェアの構成によらずに論理的に分割または統合する技術。

図表 3　地域銀行における勘定系システムの共同化率



（注）勘定系システムの開発または運用を他の金融機関と共同で外部委託している地域銀行を共同化先と定義。
（資料）日本銀行

図表 4　勘定系システムの共同化に対する満足度



（注 1）2009 年に地域銀行を対象に実施したアンケート結果より抜粋。
（注 2）勘定系システムを共同化している 55 先が回答。
（資料）日本銀行

このほか、金融サービスを提供する取引チャネルについても、ATM 網の拡大と高機能化を推進し、業務の効率化と顧客の利便性向上を図ってきた。また、1990 年代後半以降、相次いでインターネット・バンキングの提供を開始し[6]、その利用可能時間を漸次拡大してきた。近年では、専用のアプリケーションを提供し、モバイル端末でも使い勝手の良いかたちでインターネット・バンキングを利用可能とする動きが広がってきている。

もっとも、現在のインターネット・バンキングは、総じて取引チャネルの一つとして、「窓口や ATM を通じて提供してきたサービスを、インターネット経由でも提供する」との位置付けにとどまっており、「インターネットならではの柔軟、便利で安価なサービスを提供する」事例はまだ少ないように窺われる。

金融サービス分野への新規参入の動き

一方、このところ、IT ベンチャー企業などが提供する新たな金融サービスが注目を集めている。これらの多くは FinTech と呼ばれ、決済・送金サービス、融資サービス、投資仲介サービス、個人向けの資産管理サービスや資産運用サービス、小規模な企業に対する各種管理業務の支援サービスなど、様々な分野で新しいサービスが生み出されている（図表 5）。

[6] このほか、2000 年代に入ると、インターネット専業銀行も登場した。

図表 5　FinTech の事例

サービス分野	事例
決済・送金サービス Payment/Remittance	・ インターネットを利用することで、クレジットカード決済などを、24 時間 365 日、リアルタイムで、安価に行うことを可能とするサービス。 ・ モバイル端末を簡易なカード読み取り機として用い、その導入費用を安価または無料にすることで、小規模企業や個人企業でもクレジットカード決済の取り扱いを可能とするサービス。 ・ モバイル端末の機能（電話、電子メール、ソーシャル・ネットワーキング・サービス＜SNS＞）を用いて、国際送金を含む個人間（P2P）の送金などを、いつでもどこでも、リアルタイムで、安価に行うことを可能とするサービス。 ・ ビットコインにも利用されているブロックチェーンの技術を用いて、既存の決済インフラなどの刷新を目指す企業も登場。
融資サービス lending	・ インターネット上で貸し手と借り手を募り、資金貸借を実現するためのプラットフォームを提供（その際、借り手の信用力評価も実施）するサービス。専ら個人や中小企業の小口の借入ニーズと、投資の小口分散化のニーズに対応。 ・ ネット・ショッピングやクレジットカードの利用に伴う取引情報や決済情報、売り手企業に対する利用者の評価など、金融機関がこれまであまり用いなかったデータを基に、スコアリング・モデルなどで自動的に審査を行うことで、小口や緊急の借入ニーズなどに、安価に、スピーディに対応するサービス。
投資仲介サービス Equity Finance	・ インターネット上でベンチャー企業の資本性資金（equity）の調達ニーズと、個人投資家の運用ニーズを募り、マッチングする（クラウド・ファンディング）ためのプラットフォームを提供するサービス。従来、専ら限られた関係者間で行われていたエンジェル投資（創業後間もない企業への資金供給）を、より多くの企業や投資家に開放。
個人資産管理サービス Personal Finance Management	・ 本人の許諾を得て、インターネットを通じて多数の金融機関の口座情報などを自動的に集約（アカウント・アグリゲーション）し、総額や増減、評価損益、目標金額に対する達成状況を自動計算するなど、（小口の）個人の資産を分かり易く管理することを可能とするサービス。
個人資産運用サービス Retail Investment	・ ソフトウェアによる完全自動処理でコストを抑えることで、小口の個人資産運用に対しても、投資助言サービス、投資一任サービスを安価に提供。 ・ 例えば、①個人投資家が予め設定したリスク許容度などに基づき、一定のアルゴリズム（ロボアドバイザー）を用いて中長期の資産運用のポートフォリオを組成するサービス、②不特定多数の個人投資家が、投資戦略や先行きの見通しを互いにシェアするためのサービス（ソーシャルトレーディング）など。
小規模企業向けの管理業務支援サービス Business Tools	・ 売掛金データと入金データのマッチング・自動消し込み、銀行・カード情報の自動取得や人工知能を用いた自動仕訳による経理事務の効率化、給与の自動計算・給与明細のウェブ化・労働保険手続きの連動処理による給与・保険事務の効率化など、各種の管理事務をソフトウェアによる自動処理やクラウドサービスの利用により安価に提供。小規模企業の各種管理事務の効率化に寄与。

FinTech は、金融機関がこれまで提供してきた金融サービスと比べると、以下の点で大きく異なっている。

第一は、主として多数顧客を対象としたサービス提供における利便性、汎用性の高さである。インターネット、さらにはモバイル端末のアプリケーションをより積極的に活用することにより、広範な顧客と直接接する機会を獲得する

とともに、顧客の求めに応じて「いつでも、どこでも、リアルタイムで」サービスを提供することができる。

第二は、コスト競争力の強さである。従来に比べ格段に安価にサービスを提供することで、これまで不採算とされてきた個人や小規模な企業に対する小口の金融サービスを充実させることが可能となっている。具体的には、プログラムによる自動処理を基本とすることで事務処理コストを引き下げているほか、サービスの提供チャネルをインターネットに特化させ、クラウドサービスやオープンソース・ソフトウェアを積極的に活用することで、ネットワーク基盤の構築・運用コストやシステムの開発・運用コストを大幅に削減している。このように社外の資産・サービスを積極的に活用することは、準備期間を短縮し、機動的にサービスを提供できる強みにもなっている。

第三は、新たな付加価値の創出である。インターネットで得られる多様かつ膨大な情報を自動収集・分析することにより、これまでの金融機関と異なるデータや手法を用いて、リスク評価やプライシングの見直し、新たな顧客ニーズの掘り起こしを試みる動きがみられている。例えば、ネット・ショッピングやクレジットカードの取引情報や決済情報、売り手企業に対する利用者の評価などを、借り手の信用力評価や借入需要の開拓などに活用した融資サービスは、既に少なからぬ事例がみられているほか、GPS による位置情報、検索情報、SNS の情報などを活用した新たな金融サービスも模索されている。また、ブロックチェーン[7]などの新たな技術を活用して、貿易金融や決済の安全性・効率性を大幅に高めることなども検討されている。

以上のとおり、IT の進歩を積極的に取り入れて、格段に高い利便性や大幅なコスト削減を実現しつつ、従来の金融機関にはない付加価値を持つ金融サービスを提供していることが、FinTech の特徴といえる。

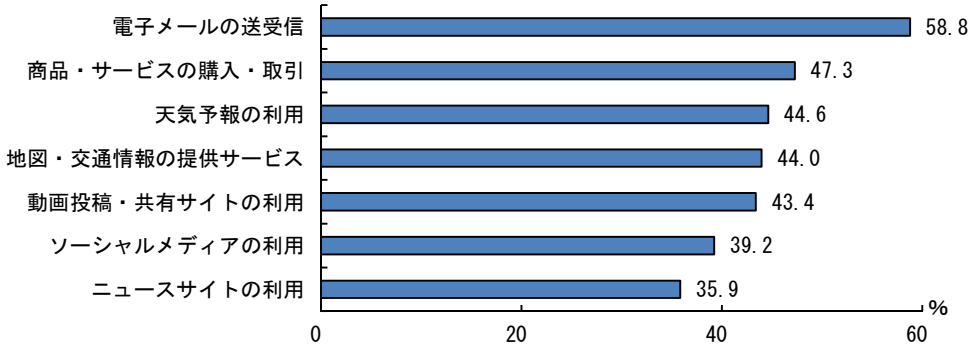
（３）金融サービス分野の新たな可能性と金融機関の課題

前掲図表 1 でみたとおり、インターネットの普及率は既に 8 割を超えている。利用するサービスの内容は、電子メール、天気予報や地図・交通情報、動画投稿・共有サイトなど様々である（図表 6）。経済取引での利用状況をみても、「商品・サービスの購入・取引」にインターネットを利用する人の割合は、20 歳代から 50 歳代では既に 5～7 割に及んでいる（図表 7 の①）。また、60 歳以上の利

[7] 一部の仮想通貨に使用されている、取引記録を共有・分散保存する技術。

用率は、相対的に低位ではあるが、年々上昇している（同②）。

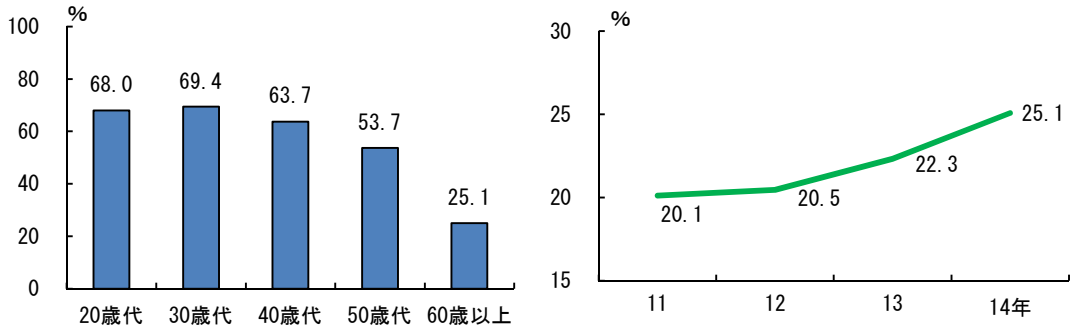
図表 6　過去 1 年間にインターネットで利用した人の割合（2014 年、全世代計）



（注 1）インターネットの利用者のうち、インターネットで上記の各機能・サービスを利用した人の割合を、調査の回答者全体に占めるインターネット利用者の割合に乗じて算出。
（注 2）電子メールの送受信は、メールマガジンの購読を除く。
（資料）総務省

図表 7　過去 1 年間にインターネットで商品・サービスの購入・取引を行った人の割合

① 世代別（2014 年）　② 60 歳以上（時系列）



（注）インターネットの利用者のうち、インターネットで「商品・サービスの購入・取引」を行った人の割合を、調査の回答者全体に占めるインターネット利用者の割合に乗じて算出。
（資料）総務省

モバイル端末の普及により、人々は日々の生活の中でより手軽にインターネットを利用できるようになった。また、データの入力方式も、キーボードやマウスから、画面タッチ、さらには音声入力などへと、より直感的な操作が可能となる方向に変化してきている。インターネットでのサービス提供に注力する企業は、「いかに利用者にストレスを感じさせずにサービスを利用してもらうか」を重視して、画面の構成や遷移などの面でもユーザーインターフェイス[8]の工夫を競い合っている。インターネットを通じた様々なサービスは、今後も、世代

[8] コンピュータとその利用者の間で、情報をやり取りするための仕組み。

を問わず、利用者にとって一層使いやすいものになっていくと考えられる。

現在、金融システムにおける FinTech の位置付けは必ずしも大きいものではない。ただ、インターネットで提供されるサービスが今後も拡充し続けていくとみられる中で、インターネットを主軸に据えて展開する FinTech の潜在力が、業態や地域の垣根を容易に越えて波及し得るものであることには留意が必要である。

金融機関にも、近年の IT の進歩をより積極的に活用することで、こうした趨勢への対応力を高めつつ、金融サービス分野で新たな付加価値を創出するチャンスがある。その際、システム上、そうしたサービスを現在稼働しているシステムとは別のものとして、業務提携や企業買収などの形で「外付け」することは、現実的な選択肢の一つとなり得る[9]。しかし、やや長い目でみれば、「高価」で「重い」既存のシステムを、活かすべき長所は活かしつつも、いかに顧客ニーズの変化に柔軟かつ機動的に対応し得るシステムへと見直していくことができるかが重要である。IT 戦略は、提供するサービスの高度化、顧客との接点や販売チャネルの拡充、マーケティング力の強化、業務プロセスやコスト構造の見直し、顧客情報の能動的な分析・管理など、金融機関の経営戦略と表裏一体のものとなっている。IT の進歩を常時フォローし、明確な経営戦略のもとでの IT の活用やシステム開発を進めていく力を有するかどうかが、金融機関の競争力を左右する要素の一つになっていくと考えられる。もちろん、IT の活用が広がるほど、相対・対面型のカスタマイズされた金融サービスの付加価値が認識される面もある。こうした側面も含め、サービスの内容やチャネルのあり方を検討していくことが重要と考えられる。

２．サイバーセキュリティの重要性

金融機関が長年大事にしてきた取引の信頼性や安全性は、顧客との相互信頼

[9] 金融審議会・金融グループを巡る制度のあり方に関するワーキング・グループによる報告書（2015 年 12 月）では、金融グループにおける IT・決済関連業務の取り扱いに関し、銀行持株会社や銀行が、認可を受けて、「銀行が提供するサービスの向上に資する業務又はその可能性のある業務」を行うための子会社等への出資を行うことを可能とすること（金融関連 IT 企業等への出資の容易化）、決済関連のシステム事務などの業務（従属業務）を営む銀行の子会社・兄弟会社の収入依存度規制（親銀行グループからの収入が総収入の 50%以上であることなど）について、銀行のシステム管理や ATM 保守などの業務に関しては収入依存度の下限を引き下げるなどの柔軟化を図ること（銀行グループ内外の決済関連事務等の受託の容易化）が提言されている。

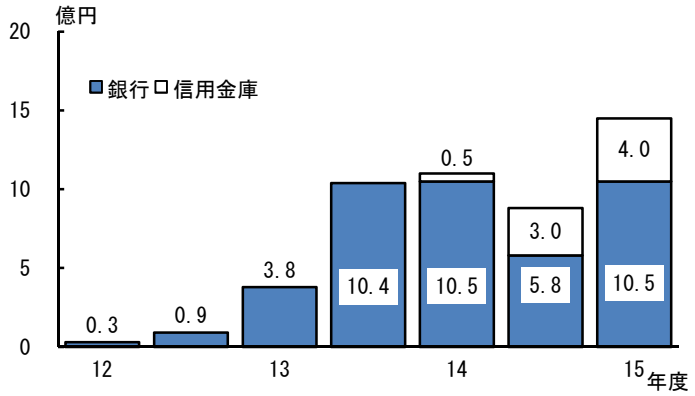
の基礎をなすものである。金融分野では、いかに便利・安価であろうと、セキュリティが十分でないサービスは存続が難しい。今後、金融機関が IT の進歩を積極的に取り込み、付加価値の高いサービスを創出していくうえで、取引の信頼性や安全性を確保していくこと、すなわちサイバーセキュリティの確保は、競争力や成長性の重要な前提となるものである。

以下では、まず、わが国の金融機関および金融市場インフラ[10]（以下、「金融機関等」）に対するサイバー攻撃と金融業界の対応状況を概観する。次に、サイバーセキュリティの確保に向けて、金融システムの安定確保の観点からみた留意点と、金融機関に求められる体制整備について整理する。

（１）わが国の金融機関等へのサイバー攻撃と金融業界の対応状況

わが国の金融機関等に対するサイバー攻撃の発生状況をみると、インターネット・バンキングを悪用した預金などの不正な払い戻しが 2013 年度以降に急増している（図表 8）。攻撃手法も、ID・パスワードを不正に入手し、顧客に成りすまして不正な払い戻しを行う方法のほか、近年では、顧客のパソコンに予め感染させたマルウェア[11]を用いて、顧客の支払指図を改ざんするといった方法も用いられるようになっている。

図表 8　インターネット・バンキングによる預金などの不正払い戻し金額の推移



（注）半期ベース。
（資料）全国銀行協会、全国信用金庫協会

[10] 資金決済システム、証券集中保管機関、証券決済システム、清算機関および取引情報蓄積機関を指す。

[11] 不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪意のあるコード（コンピュータプログラム）の総称。ウィルス、ワーム、トロイの木馬、スパイウェア、キーロガー、バックドア、ランサムウェアなどが含まれる。

これに対し、全国銀行協会では、金融機関や顧客に対し、セキュリティ対策ソフトの無償配布や利用促進、基本ソフトウェアの最新化といったマルウェアへの感染防止策の徹底や、ワンタイムパスワード[12]や 2 経路認証[13]の導入と利用促進など、認証方法の強化を推奨している。このほか、金融機関の中には、支払指図の改ざんの有無を確認するための取引認証[14]の導入と利用促進、顧客の端末がウィルスに感染していないかどうかを金融機関の側で監視する対策などを講じている先もみられる。

また、DDoS 攻撃[15]などにより、ホームページやインターネット・バンキングのサービス提供に支障が生じる事例も散見されている。こうした状況のもと、大手金融機関やインターネット専業銀行を中心に、システムや通信回線の処理能力の増強、専門業者との連携強化などの対策に取り組む先が増えつつある。

これまでのところ、標的型攻撃[16]など外部からのサイバー攻撃により、わが国の金融機関等から大規模な情報流出が生じた事例はみられていない。もっとも、わが国全体でみれば、サイバー攻撃による情報漏えい事件が少なからず発生している。それらも踏まえ、多くの金融機関等では、マルウェアによる攻撃への対策などに取り組むとともに、情報管理の一層の厳格化を図っている。

これらの対応に加え、金融機関等では、セキュリティ面の脅威に対応する特別組織（CSIRT[17]）を設ける動きや、攻撃の影響・被害が生じた場合の詳細なコンティンジェンシー・プランを整備する動き、社内の訓練を実施・拡充する動きが広がっている。さらに、社外の関係者との間で、サイバーセキュリティにかかる情報共有や、サイバー攻撃を想定した合同訓練に取り組む動きも増えてきている。

---

[12] 一定時間ごとに自動更新され、しかも一度しか使うことができないパスワード。

[13] 振込・振替取引の際に、例えば、パソコン（第一経路）で取引データを作成し、スマートフォン（第二経路）で承認を行うことで取引を成立させる認証方式。

[14] 取引の都度、顧客がトークンを操作するなどして取引内容を入力し、それによって生成されるワンタイムパスワードを添付して取引電文を送信する仕組み。

[15] 大量の（または不正な）通信により、標的とするコンピュータや通信回線の機能（サービス）を停止または著しく低下させる攻撃（DoS 攻撃）のうち、インターネット上に分散する複数の機器から同時に攻撃するもの。DoS は Denial of Service、DDoS は Distributed Denial of Service の略。

[16] 特定の組織に狙いを絞り、その組織の内部情報について入念な調査を行ったうえで、様々な手法により行う攻撃。

[17] Computer Security Incident Response Team の略。

（２）金融システムの安定確保の観点からみた留意点

このように、わが国の金融業界でも、サイバーセキュリティの確保に向けた様々な取り組みが行われている。もっとも、サイバー攻撃の手法が複雑・巧妙化しているほか、海外では、大規模な情報漏えいや金銭被害、重要業務の停止に至る事例がみられている（図表 9）。今後、わが国の金融業界でインターネットが一層積極的に活用される可能性も展望すると、金融機関等はさらに取り組みを強化していく必要がある。

図表 9　海外の金融機関におけるサイバー攻撃の被害事例

時期	発生国	内容
2011 年	米国	大手金融機関が不正アクセスを受け、30 万以上の顧客のクレジットカード情報が漏えい。
2012 年	イタリア、ドイツ、オランダ、米国等	60 以上の金融機関で総額 60 億円相当以上の不正送金が発生。
2013 年	韓国	複数の大手金融機関等がマルウェアに感染し、多数のオンライン端末や ATM が利用不能に。
2013～2014 年	ロシア、米国、ドイツ、中国等	約 100 の金融機関がマルウェアに感染し、不正送金や ATM からの現金自動払出しなどにより、総額 1 千億円相当以上の被害が発生。
2014 年	米国	大手金融機関がマルウェアに感染し、8 千万以上の顧客の情報が漏えい。

（資料）各種公表情報

また、サイバー攻撃の影響は、攻撃を受けた個々の金融機関にとどまらず、顧客の取引や他の金融機関の業務、ひいては金融システムにも及ぶ可能性がある。金融取引や決済などのプレゼンスの大きい先を中心に、こうしたシステミックなリスクがもたらす他者への影響も踏まえてサイバーセキュリティの確保に取り組む必要がある。

サイバーセキュリティの確保に取り組むうえで、金融システムの安定確保の観点から特に留意を要するのは、以下の 2 点である。

サイバー攻撃の目的と金融システムへの影響

サイバー攻撃を、その目的で分類すると、（ア）金銭の窃取を狙うもの、（イ）情報の窃取を狙うもの、（ウ）攻撃対象の企業などの業務の妨害・停止を狙うものの 3 つに大別できる。そして、サイバー攻撃が金融システムに与える影響は、これらの攻撃目的によって異なり得る。

まず、（ア）金銭の窃取を狙う攻撃は、顧客預金などの不正な払い戻しを企図したものが多く、また（イ）情報の窃取を狙う攻撃は、顧客に関する重要情報を狙うものが中心であると考えられる。したがって、これらの攻撃は、損害賠償や調査・対策に要する費用などを通じ、事後的に金融機関等の財務などに影

響を及ぼす可能性がある[18]。

次に、（ウ）業務の妨害・停止を狙う攻撃については、攻撃対象となった金融機関等だけでなく、その金融機関等の業務を通じて様々な取引を行う個人や企業、他の金融機関等の業務にも幅広く影響する可能性、ひいては金融システムにも影響を及ぼす可能性がある。また、こうした影響は、攻撃を受けた直後から発生し、攻撃が終了した後も継続する可能性がある点にも留意が必要である。

一般に、金融取引に関する事務処理、なかでも資金決済や証券決済、金融市場取引に関する事務処理には、厳格な時限性や適時性が求められる。また、一つの取引や決済が行われることを前提に、他の取引や決済が行われる――すなわち、取引や決済が連鎖する――ことが少なくないことから、ある取引や決済が予定どおりに処理されない場合、その影響が急速かつ広範に広がる可能性もある。業務の妨害・停止を狙う攻撃の影響が、攻撃開始からごく短時間のうちに発生・拡大する可能性があることもあわせて考えると、対応の緊急性が高いということも、重要な留意点である。

「ネットワーク」と「外縁部」に着目した対応の重要性

上述のとおり、金融分野では、多数の取引や決済が連鎖することが多い。また、国内外の本支店やシステムセンター、事務処理センターなど、個々の金融機関等の内部における複数の拠点間、あるいは複数の金融機関等の間に張り巡らされたコンピュータ・ネットワークを用いて、様々な事務が処理されている。このため、サイバーセキュリティの確保にあたり、金融機関等は、攻撃対象となるシステムや事務、関連する取引や決済、部署や拠点、ひいては自社そのものが、他とどのように繋がっているか、という「ネットワーク」に着目し、対応を検討・実施していくことも重要である。

具体的には、個々の金融機関等がサイバー攻撃を受けた場合、その影響が様々な「ネットワーク」を通じて、どの程度の強さや範囲で伝播する可能性があるかを考える必要がある。例えば、ある金融機関等がサイバー攻撃で業務停止に陥った場合、その金融機関等の取引や決済が多額であったり、多数の相手先を伴うものであったりすれば、金融システムに大きな影響を与える可能性がある。したがって、そうした金融機関等には、より強固な対応が必要である。

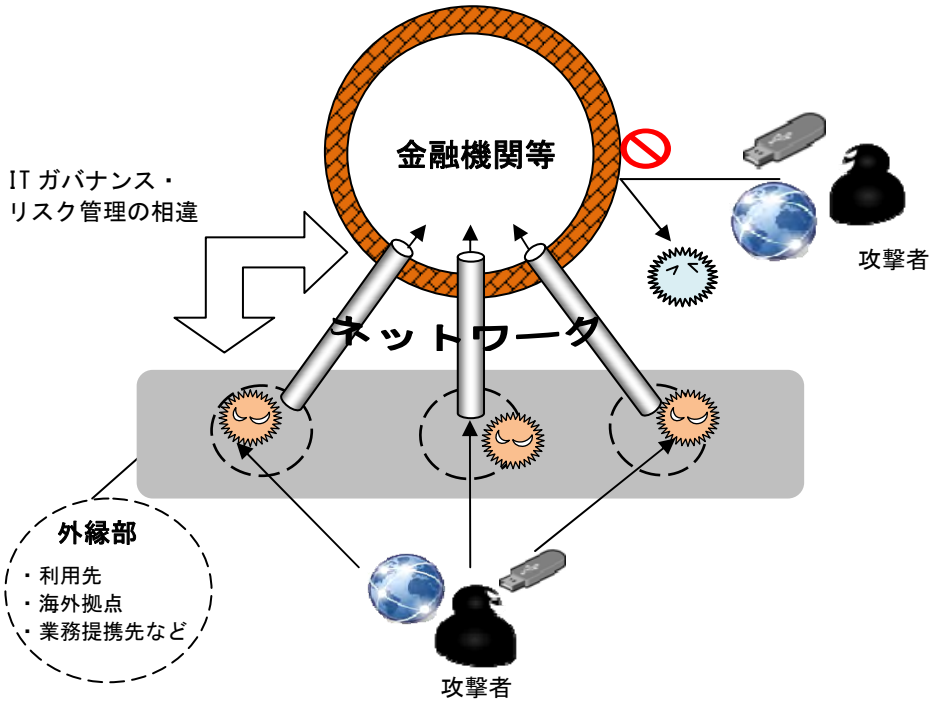
また、「ネットワーク」の「外縁部」にも着目する必要がある。「外縁部」とは、IT ガバナンスやリスク管理が異なり得る組織や人、システム、業務などが

[18] このほか、金融機関等の評判への影響も生じ得る（（ウ）についても同様）。

繋がる「境目」に当たる部分である。

例えば、（ア）金融市場インフラやシステム共同センターの利用先金融機関、（イ）国際的に業務を展開している金融グループの海外拠点（特に、ガバナンスが異なり得る海外現地法人など）、（ウ）コンピュータ・ネットワークを接続した、金融グループ外の業務提携先の企業などが考えられる（図表 10）。

図表 10　「ネットワーク」と「外縁部」（例）



（ア）では、金融市場インフラやシステム共同センターのシステムや組織がサイバー攻撃対策を講じている場合でも、個々の利用先金融機関の対策が不十分であれば、そうした利用先が受けたサイバー攻撃の影響が、「ネットワーク」を通じて、金融市場インフラやシステム共同センター、他の利用先金融機関に波及する可能性がある。

同様に、（イ）では、海外拠点のリスク管理が――国内とはシステムの構成や利用方法、ひいてはリスク管理方法が異なり得ることなどもあって――不十分であった場合、（ウ）では、提携先企業のリスク管理が不十分であった場合、海外拠点や提携先企業で生じたサイバー攻撃の影響が、「ネットワーク」を介して国内拠点や金融グループ内部に波及してくる可能性がある。

ＢＯＸ　サイバー攻撃の目的別にみた「外縁部」

「ネットワーク」の「外縁部」には、本文で示したもの以外にも、様々なものがある。ここでは、サイバー攻撃の目的別に、「外縁部」を例示する。

（金銭の窃取を狙った攻撃）

金銭の窃取を狙った攻撃は、金融機関の勘定系システムにある「預金元帳データベース（DB）」の不正な書き換え、より具体的には、預金元帳に記載されている個別の預金口座の残高を不正に増減させることを企図した攻撃である。

かつては、金融機関の職員が、窓口で本人確認を行い、預金者が記入した支払指図を基に、金融機関が管理する端末などを用いて預金元帳の書き換えを行っていた。これに対し、インターネット・バンキングでは、本人認証のためのID・パスワードの管理や、支払指図の作成・送信などを行うパソコンやモバイル端末の管理は、預金者が行っている。預金者のリスク管理の内容・水準は、金融機関のそれとは異なり得るため、預金者は、預金元帳の書き換えに関する事務フローやコンピュータ・ネットワークの「外縁部」に相当する。インターネット・バンキングを悪用した不正送金は、「外縁部」である預金者のリスク管理の脆弱性を狙った攻撃といえる。

セキュリティ対策ソフトの無償配布は、預金者による端末のリスク管理を、金融機関のリスク管理水準に引き上げることを目的とした施策であり、ワンタイムパスワードなどは、窓口事務と異なり非対面で行う本人確認の確実性をより高めるための工夫といえる。また、預金者の端末のウィルス感染状況を金融機関側で監視する対策などは、ガバナンスが異なる預金者に対して、金融機関と完全に同一のリスク管理を求めることの限界を踏まえ、金融機関側でのリスク管理を一段と強化する工夫である。いずれも、「外縁部」が内包するリスク管理の脆弱性に対して様々な対策を講じることで、「ネットワーク」全体でみたリスク管理の強化を図る取り組みといえる。

（情報の窃取を狙った攻撃）

情報の窃取を狙った攻撃では、オリジナルのDBだけでなく、その一部または全部を複写したファイルやDBも、攻撃者にとって価値があり、攻撃対象になり得る。したがって、複写したファイルなども含め、重要なデータの保管場所とその管理方法（パスワードの設定や暗号化の有無など）、アクセス可能な端末や役職員などを把握することが、リスク管理の出発点となる。

重要なデータの保管場所についての「外縁部」をみると、例えば、システム

センターのサーバに格納されたオリジナル DB は厳格に管理されている一方で、営業店や本部の各部署ではリスク管理が徹底されず、共用パソコンのハードディスクに、複写ファイルなどがパスワードや暗号化措置を施さないまま格納されている事例がみられる。また、営業店の窓口端末、スイッチやルーターなどのネットワーク機器などに、重要なデータがファイルやシステムログの形で保存されることがあるが、そうしたデータの存在（リスクの所在）が認識されていないケースもみられる。これらに対し、データのフローを把握し、重要情報を保存する可能性のあるシステム・機器を特定することが、まずもって重要である[19]。

このほか、重要なデータにアクセス可能な外部委託先なども、ガバナンスやリスク管理が委託元の金融機関等と異なるという意味で「外縁部」に該当する。この場合、外部委託先のリスク管理が、委託元である金融機関が求める内容・水準となっているかを、契約に基づく定期報告や監査などで確認していく必要がある。

（業務の妨害・停止を狙った攻撃）

業務の妨害・停止を狙った攻撃では、攻撃対象の重要システムと連動するシステムや、攻撃対象の重要業務の前提となる付随業務などが「外縁部」になり得る。

例えば、多くのシステムの運行を管理する管理サーバのリスク管理が不十分で、サイバー攻撃によってこれが停止した場合、勘定系システムを含む多くのシステムの稼働にも支障が生じることが考えられる。また、図表 9 に示した 2013 年の韓国の事例は、ATM やインターネット・バンキングを含む金融機関の広範なサービス提供に重大な支障が生じたものであるが、この主因は、プログラムの修正や機能追加を行う「パッチ」を管理するシステムがウィルスに感染し、同システムから配信されるパッチを介して、大量のパソコンやサーバへウィルスの感染が広がったことだとされている[20]。

このため、業務の停止・妨害を狙ったサイバー攻撃に関しては、重要なシステムや業務を直接狙った攻撃に加え、それらと関係の深い連動システムや付随

---

[19] 日本銀行金融機構局「重要な顧客情報のセキュリティ強化に向けて――コンピュータ・システムのリスク管理上の留意点――」（2015 年 1 月）を参照。

[20] 金融業界以外では、例えば、2015 年 6 月にポーランドの航空会社で発生したフライトの大量欠航・遅延も、類似の事例である。これは、LOT ポーランド航空の地上システムがサイバー攻撃を受けたことが原因で、航空管制などに用いる飛行計画の発行という付随業務に支障が生じ、結果として、ワルシャワ・ショパン空港発の多数のフライトが不能となったものである。

業務を狙った攻撃なども想定して、対策を講じる必要がある。

（３）金融機関等に求められる体制整備

サイバーセキュリティを確保するため、金融機関等の体制面の取り組みとしては、以下の諸点が重要である。

第一は、経営陣の積極的な関与である。システム化の進展や必要な知識・ノウハウの高度化により、サイバーセキュリティの確保に向けた取り組みには、相応の経営資源の投入が必要になっている。また、サイバー攻撃を受けた場合、システムの復旧対応や事務処理の代替策の検討・実施、顧客・広報対応など、全社的な対応が求められる。これらの取り組みや対応が不十分な場合には、企業の信用・ブランドが損なわれるリスクもある。

第二は、（リスクの未然防止に加えて）事後対応のための体制整備である。サイバー攻撃を受けた場合に、その影響範囲をいかに早期に把握し、対応できるかによって、被害の大きさは大幅に異なり得る。攻撃手法が複雑・巧妙化する中で、サイバー攻撃を予め完全に防御することは、手法の面でも経営資源の制約の面でも困難である。したがって、攻撃の影響や被害を極力抑制する観点から、攻撃に即応する専門部署の設置や、コンティンジェンシー・プランの策定といった体制整備が求められる。

第三は、サイバーセキュリティに関する幅広い情報の収集と共有である。サイバー攻撃の手法や規模は多種多様であり、時間の経過とともに変化していく可能性もある。また、同種の攻撃手法が、国から国へ、ある業種から別の業種へ、ある組織から別の組織へと伝播しながら、繰り返し使われることも少なくない。このため、情報の収集や共有にあたっては、社外の動向にも十分に目配りし、必要に応じて、高度なノウハウを有する社外組織と連携するなどの対応を継続していくことが求められる。

３．おわりに

日本銀行は、以上のような問題意識のもと、先端的な IT の動向やその金融面の活用状況についてフォローするとともに、セミナーやワークショップの開催、論文の公表などを通じ、金融機関の創意工夫、とりわけイノベーションへの取

り組みをサポートしていく[21]。また、考査・モニタリングでは、個々の金融機関の経営戦略を踏まえながら、IT 活用の戦略に関する意見交換を行うとともに、サイバーセキュリティにかかるリスク管理の充実を促していく。

[21] 日本銀行では、これまでも同様のサポートを行ってきている。例えば、2000 年に、「金融機関における情報セキュリティの重要性と対応策――インターネットを利用した金融サービスを中心に――」（日本銀行調査月報 2000 年 5 月号）を公表。最近では、2014 年から 2015 年にかけて、「IT を活用した金融の高度化に関するワークショップ」を開催し、その報告書を公表（2015 年 10 月）する一方、「2015 年度の考査の実施方針等について」（2015 年 3 月）で、サイバー攻撃に対する金融機関の対応状況を点検する旨を打ち出している。