金融分野のサイバーセキュリティレポートの視点

デジタライゼーションの進展と複雑化・巧妙化するサイバー攻撃への備え

金融庁は２０１８年10月、デジタライゼーションの加速的な進展など、金融分野の環境変化を踏まえ、「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」をアップデートした。新たな「取組方針」に沿った取組みにおいて、把握した実態や共通する課題などの認識を関係者間で共有し、サイバーセキュリティ対策の強化につなげていくため、今年６月、「金融分野のサイバーセキュリティレポート」を取りまとめ公表した。

金融庁　総合政策局
総合政策課
サイバーセキュリティ対策
企画調整室長
兼リスク分析総括課
水谷　剛

サイバーセキュリティ対策
企画調整室
兼リスク分析総括課
課長補佐
平野　義隆

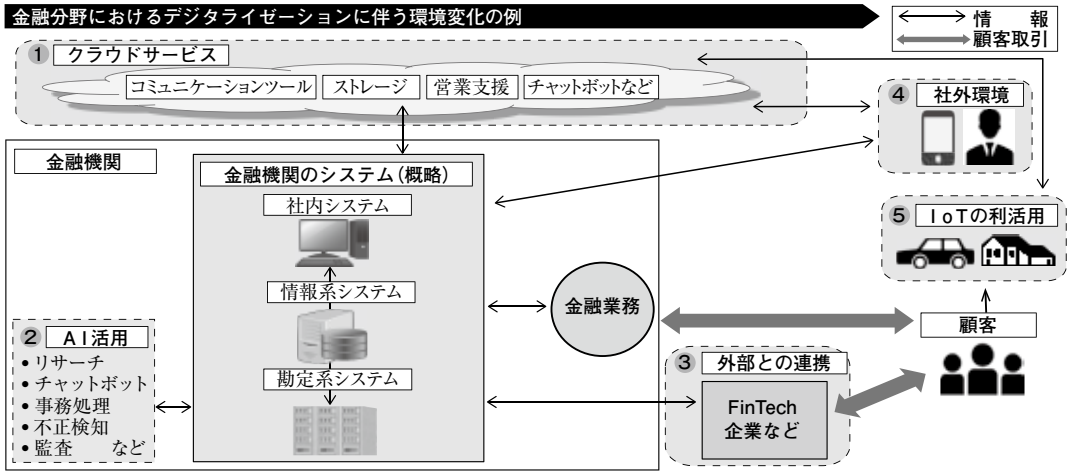
サイバーセキュリティの近年の脅威動向

金融庁は２０１５年７月、金融分野のサイバーセキュリティの確保は金融システム全体の安定のための喫緊の課題であるという認識のもと、「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」（以下、取組方針）を策定・公表し、これまで官民が一体となって、金融分野のサイバーセキュリティ強化に取り組んできた。近年、金融分野を巡るサイバーセキュリティの状況は、デジタライゼーションの加速的な進展、国際的な議論の進展などにより大きく変化している。また、来年の「２０２０年東京オリンピック・パラリンピック競技大会」（以下、20年東京大会）では、大会関係機関のみならず、重要サービスを提供する事業者もサイバー攻撃のターゲットとなる可能性が指摘されており、20年東京大会に向けてサイバー対策を強化していく必要がある。

このように、金融機関をとりまく状況が大きく変化していることなどを踏まえ、昨年10月に「取組方針」をアップデートした。さらに今年６月には、当局、金融機関、関係機関などの間で認識を共有し、金融分野のサイバーセキュリティ対策の強化につなげていくことを目的に、新たな「取組方針」に沿った取組みにおいて把握した実態や共通する課題などを取りまとめ、「金融分野のサイバーセキュリティレポート」として公表した。本稿では、「同レポート」のポイントを解説する。

近年のインシデント動向に関して、海外では金銭窃取を目的とした大規模なサイバー攻撃事例が発生しているが、国内金融

〔図表〕　金融分野におけるデジタライゼーションに伴う環境変化の例（銀行）



（出所）　金融庁

機関では昨年度、分散型サービス妨害攻撃（ＤＤｏＳ攻撃）、標的型攻撃、サーバーの脆弱性を突いた不正アクセスなどのサイバー攻撃が多く発生している。攻撃対象は、中小金融機関や暗号資産（仮想通貨）交換業者にまで拡大しており、今後は、クラウドサービスを対象とした攻撃が拡大することも予想されるなど、絶えず新たな脅威を把握・分析して必要な対策を講じていく必要がある。

政府全体としては、昨年７月に改訂された「サイバーセキュリティ戦略」を踏まえ、重要インフラ事業者の対策強化のため、「災害対応」や「データ管理」の強化などに取り組んでいる。さらに今年４月には、「サイバーセキュリティ基本法」に基づき、官民の多様な主体が相互に連携して情報共有を行う「サイバーセキュリティ協議会」（注１）を設立した。金融分野においても、政府全体の取組みに積極的に協力していく。

デジタライゼーションの加速的進展を受けた対応

昨今のデジタライゼーションの加速的な進展に伴う環境変化について、①クラウドサービス、②ＡＩやＲＰＡ（注２）、③外部連携（外部委託）、④外部接続、⑤ＩｏＴ（注３）――の五つの観点に整理し、大手金融機関等へのヒアリングを通じて、サイバーセキュリティ上の課題・リスクへの対応策などについて把握・分析を行った（図表）。

⑴大手金融機関におけるデジタライゼーションの利用実態

大手金融機関では、クラウドサービスやＲＰＡなどの分野では相応に活用が進んでいる状況が見られた。

クラウドサービスについては、クラウドサービスに係る専門チーム（注４）を設置し、ノウハウなどの蓄積を進めながら段階的に進めてきているが、基幹システムなど業務継続が必須な重要システムについては、セキュリティや可用性を外部に転嫁しない姿勢を堅持しており、クラウドサービスの対象外としている。

ＡＩやＲＰＡについては、特に既存業務の自動化に注力している状況にあり、ＡＩを推進するには、データやアウトプットへの信頼性の確保や顧客への説明責任が重要という意見が多い。

外部連携（外部委託、協業など）については、当局の「監督指針」などを基準にしたチェックリストなどを作成し、委託内容の重要性に応じて追加の対策（サービスレベル契約、業務継続計画、監査権（実地調査権））を講じている。

社外環境（外部からのモバイル端末などによるアクセス）やＩｏＴを利用したデータの利活

用については、一部の金融機関での利活用にとどまっている状況にある。

⑵デジタライゼーションの進展に伴うサイバーリスク

クラウドサービスについては、セキュリティ面のみならずサービス内容・責任範囲の理解、利用者の責任領域における各種設定などの管理が不十分な場合、サービス停止、情報漏洩などのインシデント、法令違反（コンプライアンス）などのリスクにつながっていくおそれがある。大手金融機関ではこうしたリスクを可視化するため、CASB（Cloud Access Security Broker）の活用、クラウドサービスのログを自社システムで監視・分析することなどに取り組んでおり、これらリスクを適切に管理しながら利用を進めていくことが重要である。また、今後、クラウドサービスの利活用が進むことにより、特定のクラウドベンダーへの集中リスクが高まっていくことが想定されており、当局としても金融機関のクラウドサービスの利用状況などの把握・分析に取り組む必要がある。

デジタライゼーションの進展に基づく外部依存度の高まりにより、これまで各社が構築していたセキュリティ対策の外側（サプライチェーンを含む）に大きなリスクが生じる可能性がある。一方で、あらゆるサイバー攻撃を事前に防御することは困難であり、侵入されることを前提とした対策（多層防御や監視・検知など）がより重要である。また、重要な外部委託先も含めたBCPの整備と演習・訓練を通じた実効性の向上を図っていく必要がある。

国際的議論への貢献と20年東京大会への備え

G7財務大臣・中央銀行総裁会議では、サイバーセキュリティに関する国際協調を進めるため、15年に「サイバーエキスパートグループ」を設置し、サイバーセキュリティに関する議論を重ねてきた。昨年10月には、「脅威ベースのペネトレーションテスト」および「サードパーティのサイバーリスクマネジメント」に関する基礎的要素を策定・公表した。グローバルに業務を展開している金融機関は、こうした国際的な動きを踏まえ、サイバーセキュリティ対策の高度化に向けた取組みを進めていくことが重要である。さらに今年6月には、G7諸国が連携し、クロスボーダーの大規模なサイバーインシデントの発生を想定した合同演習を実施した。本演習への参加を通して得た知見や教訓を国内外における今後の取組みにつなげていくことが重要である。

一方、国内では、20年東京大会という国際的なビッグイベントを控え、今年4月に「サイバーセキュリティ対処調整センター」を設立し、官民関係者の情報連携態勢を整備するなど、政府全体の取組みが進んでいる。金融分野においても、日本銀行、業界団体、金融ISACやFISCなどとの連携を一層緊密にし、金融分野の危機管理態勢の構築に取り組む必要がある。このため今年6月には、金融分野の各関係団体と連携し、「サイバーセキュリティ対策関係者連携会議」を立ち上げた。今後、連携会議を活用し、20年東京大会を見据えた大規模インシデント発生時の連携態勢について、官民の関係団体との間で連携手順を共有するとともに、演習などを通じて実効性を確認していく。

サイバーセキュリティ管理態勢の強化

⑴平時のサイバー対策

①中小金融機関等

中小金融機関等については、これまで業態全体の底上げに取り組んできたところであるが、直近では基礎的なサイバーセキュリティ管理態勢の整備に加え、その実効性を高めていくことが大きな課題となっている。こうした基本認識を踏まえ、実態把握や業界との対話を実施した。

〈地域銀行〉

地域銀行については実態把握が一巡しており、前回実態把握時に取組みが遅れていた先を中心に実態把握を実施したが、全般的に課題を解消し、経営陣も積極的に関与して取組計画を策定して対策を進めているほか、銀行間の共助も進展している状況が見られた。一方、新たな目

線として把握した、脆弱性診断・ペネトレーションテストの実施状況については、意識的に診断を実施しているのは一部にとどまっており、必要性が十分浸透していない状況だった。

〈信金・信組〉

信金・信組については、比較的規模の大きな先であっても、リスク評価やインシデント対応といった基礎的態勢は整備途上の段階にあり、脆弱性診断・ペネトレーションテストは、地域銀行以上に浸透していない状況であった。当局としては、このような状況を踏まえ、信金・信組については、20年東京大会までに適切なサイバーセキュリティ対策を完了させることを目標に、強化に向けた方針（注5）を策定した。こうした取組みを通じて、今年度、大部分の信金・信組がリスク評価を実施し、コンティンジェンシープランを策定したものの、今後は、リスク評価に基づく必要なサイバーセキュリティ対策の実施、脆弱性診断などを通じた実効性の確保が課題となる。

②証券会社等

証券会社等については、中小・地域証券会社、ＦＸ業者、ＰＴＳ（注6）業者、投資運用業者等に対して実態把握を行ったところ、取組みが進展している金融機関が増えている一方、信金・信組同様に依然として取組未着手・停滞状態の先が多く見受けられ、基礎的な態勢は整備途上の段階にある。

③暗号資産（仮想通貨）交換業者

昨年10月には、日本仮想通貨交換業協会（以下、ＪＶＣＥＡ）を認定資金決済事業者協会として認定し、各業者はＪＶＣＥＡが制定した自主規制規則・ガイドラインに基づき、態勢整備に取り組んでいる。また、脆弱性診断・ペネトレーションテストも、各社が必要性を認識して対策を講じている状況である。さらに、多額の暗号資産の流出事案を受け、全業者より暗号資産を管理するウォレット（注7）の管理方法についてもヒアリングを行った。

④大手金融機関

３メガバンクについては、海外の最新動向を踏まえたさらなる高度化に向けて、自組織の取組計画を策定し取組みを推進している。一方で、サイバー攻撃の複雑化・巧妙化、国際的な動向等を踏まえると、司令塔となるＣＩＳＯ（注8）の機能強化などを通じて、グループ・グローバルでの一元的な管理態勢のさらなる高度化が期待される。３メガ以外の大手金融機関（大手証券、大手生損保、ゆうちょ銀行）については、サイバーセキュリティ態勢の強化に継続的に取り組んでいるものの、規模やグローバル展開の程度によって、グループ・グローバルでの一元的な管理態勢や、脆弱性対応に改善の余地があり、継続的な改善・高度化が期待される。

⑤監査法人

大手および準大手監査法人について、金融機関の取組みを参考に実態把握と対話を実施した。大手監査法人は、専門の人員や部署を設け、所属するグローバルネットワークと連携が図られている状況が見受けられるが、準大手監査法人は、サイバーセキュリティ対策への取組みが十分に進んでいない状況が見受けられた。

⑵有事のサイバー対策

①中小金融機関等

金融庁では、毎年、特に中小金融機関のサイバー対策の向上を図るため、「金融業界横断的なサイバーセキュリティ演習（Delta Wall）」を実施している。昨年10月には、昨今の脅威動向を踏まえ、新たな業態としてＦＸ業者、暗号資産交換業者を追加し、１０５社（約１４００名）が参加して演習を実施した。事後評価を重視した本演習を通じて対応態勢の改善が図られた一方で、全体の傾向として、インシデント対応時における委託先との連携や顧客対応などが不十分といった課題や、インシデント対応に必要な人員が確保できていないといった課題が認められた。次回の演習では、20年東京大会で想定されるリスクを意識した演習シナリオなどにより、金融分野全体の対応能力の向上を図っていく。

②大手金融機関

大手金融機関については、Ｇ７諸国の当局による合同演習に参画するなど、大規模なインシ

デントに対するわが国金融システム全体の対応能力の向上に取り組んだ。海外大手金融機関のベストプラクティスなどを踏まえ、対応能力のより一層の高度化を図る観点から、「ＴＬＰＴ（脅威ベースのペネトレーションテスト）」（注９）などの高度な評価手法を活用・促進した。ＴＬＰＴは、自組織にとっての脅威情報を収集し、攻撃手段を調査・分析する、いわゆる「脅威インテリジェンス」を活用することに大きな特長があり、こうした特長を踏まえ、テストの深度をさらに深めていくことが期待される。

情報共有の実効性向上や人材育成の強化の必要性

これまで、金融ＩＳＡＣなどの情報共有機関を活用した「共助」の意義について、機会をとらえて金融機関に周知してきたところ、金融ＩＳＡＣの加盟金融機関数は着実に増加してきている。他方、中小金融機関にとっては、金融ＩＳＡＣへの加盟が地理的・人的・金銭的に難しいとの意見があることも踏まえ、「共助」の取組みの第一歩となるよう、地域内の情報共有も推進していく必要がある。このため、ＦＩＳＣが開催している「サイバーセキュリティワークショップ」を通じて地域連携の強化に取り組んだ。

また、実効性のあるサイバーセキュリティ管理態勢を構築するためには、サイバーセキュリティに係るリスクを組織全体での対応が必要なコーポレートリスクとして認識し、対策を進めることが極めて重要である。そこで、財務（支）局とも連携し、金融機関の経営層向けのセミナーなどを各財務局において開催し、地域金融機関の経営層の意識改革や金融機関同士の共助の活動に貢献してきた。今後は、地域における状況を踏まえ、こうした取組みをほかの地域にも展開していくことが重要である。

当局における今後の取組み

デジタライゼーションの進展により、金融機関のビジネスモデルの革新、プラットフォーマーと呼ばれる非金融プレイヤーの参入など、金融分野をとりまく環境は急速に変化している。また、サイバー攻撃が一層複雑化・巧妙化するなか、20年東京大会などの国際的なイベントを控え、金融分野を含む重要サービスを提供する事業者に対するサイバー攻撃のリスクの高まりが指摘されている。このため、20年東京大会までに、官民が一体となって、金融業界全体のもう一段のサイバーセキュリティ対策の強化に取り組んでいく。

（本稿において意見にわたる部分は筆者らの個人的見解であり、所属する組織の見解を示すものではない）

（注）１　金融分野からは、金融ＣＥＰＴＯＡＲ（銀行等、証券、生保、損保）のほか、金融ＩＳＡＣなどが参加。
２　Robotic Process Automationの略。
３　Internet of Thingsの略。
４　一般的にＣＣｏＥ（Cloud Center of Excellence）と呼ばれ、組織横断的にクラウドサービスの知見集積・利用サポートなどを行うチームのこと。
５　①経営層の意識啓発・目標の共有、②取組状況の確認、フォローアップ、③リスクベースで対象先を増やした実態把握――の三つを柱とする。
６　ＰＴＳ（Proprietary Trading System）：私設取引システム。
７　秘密鍵を保管する場所。
８　Chief Information Security Officerの略。最高情報セキュリティ責任者。
９　Threat-Led Penetration Testingの略。

みずたに　つよし
95年大蔵省入省。金融庁総務企画局企業開示課課長補佐、滋賀大学経済学部准教授、滋賀県湖南市総合政策部理事などを経て、18年７月から現職。
ひらの　よしたか
03年金融庁入庁。16年総務企画局政策課サイバーセキュリティ対策企画調整室係長、17年７月から現職。