金融分野のサイバーセキュリティレポート

令和元年６月

金融庁

[目次]

はじめに

金融庁では、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の認識の下、2015 年７月、「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」という）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、金融を取り巻く環境は、デジタライゼーションの加速的な進展による伝統的な金融機関のビジネスモデルの変革の動き、非金融のプレイヤーの参入などにより、大きく変化してきている。こうした動きは、利用者の利便性を大きく向上させ、生産性を高める可能性がある一方、あらゆるシステムがネットワークに繋がることにより、これまで以上にサイバーセキュリティの確保が重要となってきている。

また、容易に国境を跨ぐサイバー攻撃に対しては、国際的に協調していくことが重要であり、我が国としてもこうした議論に積極的に貢献していく必要がある。更に、2020 年に開催が予定されている「2020 年東京オリンピック・パラリンピック競技大会」（以下、「2020 年東京大会」という）は、国際的にも最高度の注目を集めて開催される行事であり、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いる。このため、「2020 年東京大会」に向けて、更に金融分野におけるサイバー対策を強化していく必要がある。

デジタライゼーションの進展によりサイバー攻撃は複雑化・巧妙化してきており、的確に対処していくためには、経営層の適切な関与の下、自社の情報資産の把握やリスク評価、対応態勢の構築、インシデント発生に備えたコンティンジェンシープランの整備といった基礎的なサイバーセキュリティ管理態勢を構築するにとどまらず、セキュリティインシデントの監視・分析、脆弱性診断・ペネトレーションテストやサイバー演習の繰り返し等を通じて、絶えず実効性を向上させていくことが重要である。

このように、金融機関を取り巻く状況が大きく変化しサイバーセキュリティの一層の強化が必要となっていることに加え、政府全体の基本戦略である「サイバーセキュリティ戦略」が改訂（昨年7月）されたことを踏まえ、昨年 10 月、「取組方針」をアップデートした。

今事務年度、新たな「取組方針」に基づき、金融環境の大きな変化に対してフォワードルッキングに対応するとともに、金融機関のサイバーセキュリティ管理態勢の強化、情報共有の枠組みの実効性の向上、金融分野の人材育成の強化などを通じて、金融分野のサイバーセキュリティ対策の向上に取り組んできた。

本レポートは、今事務年度における取組みで把握した実態や共通する課題等をとりまとめ、公表するものである。新たな「取組方針」では、「金融分野全体のサイバーセキュリティ対策の強化を促すために、金融分野に共通する課題等について積極的に情報発信する」旨掲げており、本レポートの公表を通じて、当局、金融機関、関係機関等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繋げていくことを目的としている。

１．金融分野を巡るサイバーセキュリティの現状について

(1) 近年の脅威動向等

我が国では、これまでに、金融システムの機能が停止するような大規模なサイバーインシデントは発生していないものの、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。報道等によると、例えば、2018 年４月には、メキシコの中央銀行が提供する銀行間電子決済システムを利用していた同国の複数の銀行がサイバー攻撃を受け、少なくとも４億ペソ（約 2,000 万米ドル）が不正送金により窃取された。また、2018 年８月には、インド国内の銀行が、同国の ATM や SWIFT[1]環境に対するサイバー攻撃を受け、1,350 万米ドルの被害が発生している[2]。

国内金融機関においては、昨年度、分散型サービス妨害攻撃（DDoS 攻撃）、標的型攻撃、サーバ等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状況にある。攻撃対象としては、大手金融機関のみならず、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、実際に、中小金融機関の Web サイトが改ざんされ、不正なサイトに誘導された事案や暗号資産（仮想通貨）の流出事案などが発生しており、実効性のあるサイバーセキュリティ対策は急務となっている。

加えて、今後、クラウドサービスを対象とした攻撃が拡大することが予想される[3]など、金融分野においても、絶えず新たな脅威を把握・分析し必要な対策を講じていく必要がある。

(2) 政府全体の取組み

社会全体で、AI、Fintech などの知見や技術・サービスが社会に浸透し、サイバー空間が持続的に拡大する中、サイバーセキュリティの確保は、金融分野のみならず各分野の全ての主体の重要課題である。こうした基本認識の下、昨年７月、政府は「サイバーセキュリティ戦略」を改訂した。

こうした中、今事務年度、政府全体として、重要インフラ事業者の対策強化のため、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」[4]を改定し、「災害対応」や「データ管理」の強化等に取り組んだ。「金融分野」が我が国の重要インフラ分野の１つであることを踏まえ、当局も公益財団法人金融情報システムセンター（以下、「FISC」という）等の関係機関とも連携し、政府全体の取組みに適切に対応していく。

また、本年４月、「サイバーセキュリティ基本法」が改正され、国の行政機関、重要インフラ事業者、サイバー関連事業者等官民の多様な主体が相互に連携し、サイバーセキ

---

[1] 銀行間の国際金融取引に係る事務処理の機械化、合理化及び自動処理化を推進するため、参加銀行間の国際金融取引に関するメッセージをコンピュータと通信回線を利用して伝送するネットワークシステムのこと（全銀協ウェブサイト）。

[2] NISC「サイバーセキュリティ 2019」の「2 重要インフラ分野等におけるサイバーセキュリティに関する情勢」を参考に記載。

[3] Fire Eye の年次脅威レポート「2019 年、そしてこれからのサイバー・セキュリティ」を参考に記載。

[4] 重要インフラ事業者等が事業を営む際の基準である「安全基準等」に規定されることが望まれる事項を整理・記載した指針（サイバーセキュリティ対策本部において決定）。

ュリティに関する施策の推進に係る協議を行うため、「サイバーセキュリティ協議会」が設立された。金融分野からは、金融 CEPTOAR[5]（銀行等、証券、生保、損保）のほか、金融 ISAC[6]等も参加しており、政府全体の情報共有態勢の強化に向けて、当局も積極的に協力していく。

２．金融分野のサイバーセキュリティ強化に向けた取組み状況

新たな「取組方針」では、近年の金融分野の環境変化を踏まえた課題として、(1)デジタライゼーションの加速的な進展を踏まえた対応、(2)国際的な議論への貢献・対応、(3)2020年東京オリンピック・パラリンピック競技大会等への対応、を取り上げるとともに、これまでの進捗・評価を踏まえた施策の推進として、(4)金融機関のサイバーセキュリティ管理態勢の強化、(5)情報共有の枠組みの実効性向上、(6) 金融分野の人材育成の強化、を重要テーマとして取り組むこととしている。以下では、今事務年度おける各施策の進捗状況や実績・共通する課題等を取りまとめた。

(1) デジタライゼーションの加速的な進展を踏まえた対応

昨今のデジタライゼーションの加速的な進展が金融サービスに与える影響についての実態を踏まえ、どのようなサイバーリスクが発生するか、そのリスクが金融機関や金融セクター全体にどのような影響を与えるか、そのリスクへの対応策等について把握・分析に取り組んだ。

具体的には、まずは、IT ベンダー、コンサルタント等の外部有識者へのヒアリングを通じて知見を収集し、金融機関との対話に向けて、デジタライゼーションの領域を大きく①クラウドサービス、②AI（RPA[7]）、③外部連携（外部委託）、④外部接続（社外環境）、⑤IoT[8]、の５つの観点に整理した。

次に、大手金融機関等へのヒアリングを実施し、課題・リスク等への対応策等について把握・分析を行った。

---

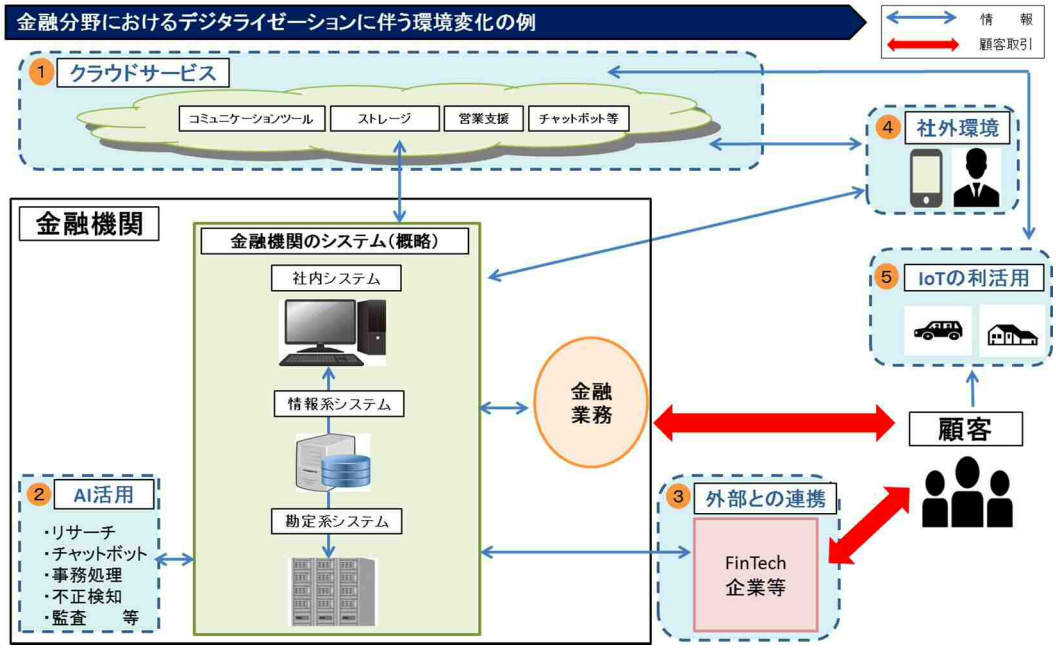
[5] CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response の略。重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織のこと。金融分野では、銀行等、証券、生保、損保の４つが該当（事務局は各協会）。

[6] 我が国の金融機関によるサイバーセキュリティに関する情報の共有及び分析を行い、金融システムの安全性の向上を推進することにより、利用者の安心・安全を継続的に確保することを目的として設立（2014 年８月）された一般社団法人（Information Sharing and Analysis Center）。

[7] Robotic Process Automation の略。

[8] Internet of Things の略。

【図表１：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）】



（資料）金融庁

① 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について

デジタライゼーションの活用状況に関して、大手金融機関では、特に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みられた。

クラウドサービスについては、多くの大手金融機関ではクラウドサービスに係る専門チーム[9]を設置し、ノウハウ等の蓄積を進めながら段階的に進めてきている。これにより、金融セクター全体を俯瞰すると、大手クラウドベンダーへの集中は高まってきている状況にあり、今後、知見の集積により、更に集中が進む可能性があると考えられる。他方で、金融機関のシステムのうち、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（RPA）については、大手金融機関では特に既存業務の自動化（RPA）に注力している状況にある。AI を推進するにあたっては、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。このため、既に AI が使われている領域についても、アウトプットが導き出される過程がブラックボックス化しないよう、結論部分に関しては人が関与しているケースがみられた。

外部連携（外部委託、協業など）については、外部委託先の業種・種別に拘わらず、原則、当局の「監督指針」や FISC の「金融機関等コンピュータシステムの安全対策基準」に沿って基準やチェックリストを策定し、定期的な評価を通じて遵守状況を確認し

[9] 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・利用サポート等を行うチームのこと。

ている。加えて、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等によるアクセス）については、会社貸与のモバイル端末等の活用に留まり、職員の私物端末の活用を認めているのは一部の金融機関のみであった。

IoTを活用しデータを収集するサービスを提供しているのは、ごく一部の金融機関に留まり、現時点では本格的な利活用には至っていない状況にある。

② デジタライゼーションの進展に伴うサイバーリスク等について

大手金融機関では、適切にリスクを管理するため、ノウハウ・専門人材の確保などを進めつつ、基本的には、これまでのサイバーセキュリティのフレームワーク[10]に沿ってセキュリティ対策を講じている。他方で、デジタライゼーションによりシステムが一層複雑化してきており、情報資産の網羅性の確保やリスクコントロールが一層重要となってきている。このため、大手金融機関では、CASB（Cloud Access Security Broker）の活用やクラウドサービスのログを自社で監視・分析するなどの取組みがみられた。

【図表２：大手金融機関のヒアリングを通じて把握した取組事例】

事 項	取組事例
① クラウド	・専門チーム(CCoE)を設置。知見・人材を蓄積し、クラウドに関する設計ガイドライン・管理基準を制定 ・CASB(Cloud Access Security Broker)を導入するとともに特に重要なクラウドベンダーの通信ログを自社で監視・分析 ・クラウドベンダーとの契約において秘密鍵の自社での管理、情報漏えい事案による秘密保持契約に対してリスクに応じた賠償責任の定めを求めている ・オンプレミスのシステムとは必要な知識が異なることを踏まえ、クラウドの専門人材育成を強化
② AI(RPA)	・AI導入ガイドラインを策定し、倫理的に不適切にならないよう留意するポイント、成果物の権利義務の帰属、学習データ等に関する知的財産権を明確化 ・システム子会社の有識者を中心にAICoE(AIに係る専門チーム)を構築
③ 外部連携	・委託先のKPI/KRIとして実損発生件数/顧客情報漏えい件数を設定し、経営陣に対して報告 ・情報漏えい事案懸念の場合の報告期限を明確化するとともに、サイバー事案の報告を義務付け ・年次で契約サービス等の棚卸しを実施
④ 社外環境	・MDM(Mobile Device Management)などツールを導入しセキュリティを管理
⑤ IoT	・個人が特定できないよう、収集データはプライベートクラウド等に分散して保存

（資料）金融庁

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

[10] 米国国立標準技術研究所（NIST）の「Cybersecurity Framework」や米国連邦金融機関検査協議会（FFIEC）の「CAT（Cybersecurity Assessment Tool）」。

報漏えい等のインシデント、法令違反（コンプライアンス）などのリスクに繋がっていくおそれがある。こうした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等の把握・分析に取り組む必要がある。

AI については、各社とも公平性・透明性（ブラックボックス化）・セキュリティなどのリスクを認識しており、利用基準等をガイドライン等により明確化し、利活用を進めていくことが重要である。

また、外部委託に関して、海外ではよりサプライチェーン（ベンダーなどの製品調達先等）を重視する動きもあり、グローバルで活動する金融機関において、委託先管理・調達管理の高度化が課題となっている。

社外環境からのアクセスや IoT に関しては、現時点では、限定的な利用となっているが、利活用を進めるにあたっては、端末の適切な管理、アクセスコントロールやデータの分散保存など、必要なセキュリティ対策を講じていくことが重要である。

デジタライゼーションの進展による外部依存度の高まりにより、各社が構築していたセキュリティ対策の外側（サプライチェーン含む）に大きなリスクが生じる可能性があり、外部委託を含め委託内容に応じた適切な対策が求められる。

一方で、あらゆるサイバー攻撃を事前に防御することは難しく、実際にクラウドサービスや外部委託先へのサイバー攻撃も発生しており、侵入されることを前提とした対策がより重要である。外部委託先を含めた情報資産の把握、リスク評価、入口・内部・出口対策（多層防御）に加え、監視・検知機能の強化、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。当局としては、国際的な動向も踏まえつつ、金融機関のデジタライゼーションの進展状況に応じて、サイバーセキュリティに関する適切なリスク管理が行われているか、モニタリングしていく。

(2) 国際的な議論への貢献・対応

金融システムはグローバルに相互接続されているため、G７や G20 といった国際的な場でも、協調してサイバーセキュリティ確保に取り組むための議論を進めている。G７財務大臣・中央銀行総裁会議では、2015 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。2018 年 10 月には、G７財務大臣・中央銀行総裁会議が「脅威ベースのペネトレーションテスト」及び「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については、こうした国際的な動きを踏まえて、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。

また、G７諸国がクロスボーダーに連携して実施する、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。

(3) 2020 年東京オリンピック・パラリンピック競技大会等への対応

2020 年東京大会にあたっては、大会関係機関への攻撃のみならず、重要サービスを提供する事業者も大会運営の妨害や社会的な混乱を狙ったサイバー攻撃のターゲットとなる可能性が指摘されている。実際、過去のオリンピック・パラリンピック競技大会においては、電力システムを狙ったサイバー攻撃情報を受けてマニュアル操作に切り替えた事案や大会に関わる公共事業を請け負った建設会社のウェブサイトから個人情報が漏洩した事案が発生した[11]。こうした事案に加え、近年サイバー攻撃が益々複雑化・巧妙化していることを踏まえ、2020 年東京大会に向けて、金融分野も例外ではなく、更にサイバーセキュリティ対策を強化していく必要がある。特に対策の弱い金融機関への攻撃を足掛かりに業界全体に影響が拡大する事態も十分に想定しておく必要がある。

2020 年東京大会を見据えた政府全体の動きとしては、本年４月に「サイバーセキュリティ対処調整センター」が設立され、官民関係者の情報連携態勢の整備がなされた。金融分野においても連携態勢を整備することが重要であり、関係省庁（内閣サイバーセキュリティセンター（NISC）等)、日本銀行、業界団体（CEPTOAR)、金融 ISAC や FISC 等の関係団体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、金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における相互の情報連携ができるよう、本年６月に「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、2020 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、演習等を通じて実効性を確認していく必要がある。

(4) 金融機関のサイバーセキュリティ管理態勢の強化

今事務年度は、サイバーセキュリティ対策を平時の対策・有事の対応の２つの観点から、これまでの実態把握等を通じて把握した業態毎の状況を踏まえ、金融機関等との対話や演習に取り組んだ。

① 平時のサイバー対策

ア. 中小金融機関等

これまで、中小金融機関等については、実態把握やサイバーセキュリティ演習等を通じて、業態全体の底上げを図ってきた。こうした中、直近では 2020 年東京大会において想定されるリスクを見据え、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。

今事務年度は、従来目線である基礎的なサイバーセキュリティ管理態勢の整備[12]を検証するとともに、新たな目線として、セキュリティインシデントの監視・分析状況

[11] 「リオ 2016 大会の振り返りと東京 2020 大会へ向けたサイバーセキュリティの取組み」（平成 29 年 7 月 19 日、公益財団法人東京オリンピック・パラリンピック競技大会組織委員会テクノロジーサービス局長　舘剛司）を参考に記載。

[12] ①経営陣の取組み、②リスク管理の枠組み、③技術的対策等の対応態勢、④コンティンジェンシープランの整備と演習を通じた実効性確保、⑤サイバーセキュリティに関する監査。

や脆弱性診断の実施状況などについて踏み込んだ検証を重点事項とし、実態把握を行った。

○　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[13]、当時の議論を踏まえて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進めており、自主的に強化を図っている状況がみられた。

また、態勢整備には、銀行間の共助態勢も有効活用されているのが特徴であり、金融 ISAC の共同演習等への参加をはじめとして、共同システム加盟行間の情報交換、共同検討会等の活動が行われている。

一方、新たな目線として、脆弱性診断・ペネトレーションテストの実施状況を把握したところ、金融機関自らが、セキュリティ診断業者に委託するなどして意識的に診断を実施しているのは一部に留まっており、実施基準も定められていないなど、その必要性が十分浸透していない状況であった。自社に潜む脆弱性を的確に把握し、2020 年東京大会に向けて脆弱性対応まで完了しておくことが必要である。

なお、地域銀行のうち、サイバーセキュリティ対策が進んでいる銀行については、大手金融機関の先進事例等を参考に、もう一段上のサイバーセキュリティ対策を実施することが期待される。

○　信金・信組

信金・信組については、2015 年の「取組方針」の公表から既に３年が経過したにもかかわらず、業態内上位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依然として整備途上の段階に留まっていた。こうした業態全体の停滞傾向は、サイバーリスクに対する経営陣の危機感が希薄であることに加え、専門の担当者もいない中で地域銀行のような共助態勢もなく試行錯誤していることが大きな要因となっている。また、脆弱性診断・ペネトレーションテストについては委託先任せで実施有無や実施範囲も把握しておらず、地域銀行以上にその必要性が十分浸透していない状況であった。地域銀行同様に、自社に潜む脆弱性を的確に把握し、2020 年東京大会に向けて脆弱性対応まで完了しておくことが必要である。

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、2020 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とし、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３点を柱とするサイバーセキュリティ態勢の強化に向けた方針を策定した。

本方針に基づき、今事務年度は業界団体等とも連携し、各信金・信組に対して、講演、セミナー等の機会を通じて、2020 年東京大会に向けた目標を共有し、本年

[13] 地方銀行の２巡目及び第二地方銀行の前回実態把握時に取組みが遅れていた先のフォローアップを実施。

３月までにサイバーセキュリティ対策の土台となるリスク評価・コンティンジェンシープランの策定を完了させるよう要請した。各信金・信組の取組状況については、アンケートを通じて確認するとともに、未実施先に対してフォローアップを実施することとしている。

さらに、信金・信組のサイバーセキュリティ対策の底上げを図る観点から、アンケート等を活用し、各信金・信組のリスクプロファイルを把握した上で、特に取組みが遅れている先に対して、リスクベースで対象先を増やした実態把握を通じて直接的に取組加速を要請した。

こうした取組を通じて、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。今後、2020 年東京大会に向けて、リスク評価に基づき必要なサイバーセキュリティ対策を実施し、脆弱性診断等を実施することにより対策の実効性を確保していくことが必要である。

○　証券会社等

証券会社等については、実態把握未実施先のうち、中小・地域証券会社、FX 業者、PTS[14]業者、投資運用業者等に対して実態把握を行った。取組みが進展している金融機関が増えている一方、依然として取組未着手・停滞状態の先が多くみられた。

経営陣のリスク認識が高い先は、経営陣も積極的に関与して取組計画を策定し、自主的に強化等を図っている。一方、信金・信組同様、多くの先ではリスク評価の実施やコンティンジェンシープランの策定といった基礎的態勢は整備途上の段階にある。また、基幹システムとネットワーク環境とを分離していることに安心して、サイバーセキュリティのリスク評価とその結果明らかになる脅威への対策が停滞している先がみられた。

○　暗号資産（仮想通貨）交換業者

昨年 10 月に日本仮想通貨交換業協会（以下、「JVCEA」という）を認定資金決済事業者協会として認定し、情報連携を緊密に行ってきた。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、サイバー対策も含め態勢整備を図っているところである。第三者利用による脆弱性診断・ペネトレーションテストもこれまで一部の業者に留まっていたが、各社が必要性を認識し、対策を講じている状況である。

また、多額の暗号資産（仮想通貨）の流出事案を受け、全業者より暗号資産（仮想通貨）を管理するウォレット[15]の管理方法についてヒアリングを行った。

イ.大手金融機関

大手金融機関については、我が国金融システムの中核を担う３メガグループを中心に、これまで定期的な対話を通じて、継続的に議論を重ねてきた。

[14] PTS（Proprietary Trading System）：私設取引システム。
[15] 秘密鍵を保管する場所。

今事務年度、３メガバンクについては、米大手行の最先端の取組みやグローバルな動向を念頭に、定期的な対話を通じて、サイバー対策のもう一段の高度化の状況を確認した。また、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、対応能力のもう一段の引上げを促すために、業界内・他業態との比較分析等を行った。

３メガについては、海外の最新動向を踏まえた自組織の取組計画を策定し、高度化に向けた取組みを実施している。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[16]の機能強化、アクセスコントロールや脆弱性管理の強化等を通じて、グループ・グローバルでの一元的な管理態勢の更なる高度化が期待される。

３メガ以外の大手金融機関については、各々のリスク評価に基づいて、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一方で、各社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見られる先がみられた。より先進的な取組みを行っている他社事例や外部による評価の指摘事項等も参考にしつつ、継続的な改善・高度化が期待される。

ウ. 監査法人

監査法人に対しては、サイバーセキュリティ対策の状況を確認し、金融機関の取組みを参考にしながら態勢の充実を促していくこととしている。

今事務年度は、大手監査法人及び準大手監査法人について、実態把握と対話を実施した。大手監査法人においては、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みられるところ、準大手監査法人においては、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もみられた。

② 有事のサイバー対策

ア. 中小金融機関等

サイバー攻撃が複雑化・巧妙化する中で、あらゆるサイバー攻撃を速やかに捕捉し防御することには限界があり、攻撃を受けた後の対応が重要となる。このため、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）」を実施してきている。

今事務年度は、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（仮想通貨）交換業者を追加し、105社（約1,400名）が参加した。事後評価を重視した本演習を通じて、参加金融機関の多くがコンティンジェンシープラン等の見直しや社内外の情報連携の強化に向けた対応を実施するとしており、演習を通じて対応態勢の改善が図られている。一方で、業界全体の傾向として、例えば、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等が不十分な先が多い、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ることから、金融機関が継続して、PDCAサイクルを回しつつ、対応能力の向上を図っていくことが必要である。さらに、2020年東京大会を控え、2020年東京大会で想定されるリスクを意識した演習

[16] CISO(Chief Information Security Officer)：最高情報セキュリティ責任者。

シナリオや参加対象先の拡大により、金融分野全体の対応能力の向上を図っていく必要がある。

イ.大手金融機関

大手金融機関については、G７諸国の当局が連携して実施す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我が国金融システム全体の対応能力の向上に取り組んだ。また、海外大手金融機関のベストプラクティスや国際的な動向を踏まえ、対応能力のより一層の高度化を図る観点から、「TLPT[17]（脅威ベースのペネトレーションテスト）」等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、所謂「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、テストの深度を更に高めていくことが期待される。

また、昨年、公表された「TLPT に関するＧ７の基礎的要素」等を踏まえ、現在、FISC において、「TLPT 実施にあたっての手引書」の策定作業を行っている。当局としては、こうした動きと緊密に連携していくとともに、各金融機関における TLPT の活用・促進に取り組む必要がある。

(5) 情報共有の枠組みの実効性向上

これまで、金融 ISAC 等の情報共有機関を活用した「共助」の意義について、機会を捉えて、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。また、昨年度から新たにトライアル会員制度を導入したところ、多くの金融機関の正式加盟に繋がっており、中小金融機関の「共助」参加への第一歩として機能しているものと考えられる。

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」に関して、当局や金融 ISAC、一般財団法人日本サイバー犯罪対策センター（JC3）より講師を派遣し、地域連携の強化に取り組んだ。

平成 30 年度においては、全国各地で 12 回開催し、241 社（293 名）が参加したが、前年度に比べて、信金・信組や地域証券の参加が増えるなど、中小金融機関においても、相応にサイバーセキュリティ対策への関心や共助の意識の高まりがみられた。今後は、こうした活動への参加をきっかけに、例えば、近隣の金融機関との情報共有活動など、具体的な取組みに繋げていくことが期待される。一方で、極端に参加者が少ない地域もあり、「共助」に対する意識に差がみられた。

金融分野における「共助」の果たす役割は年々大きくなってきている。新たに政府全体の「サイバーセキュリティ協議会」や金融分野の「サイバーセキュリティ対策関係者連携会議」も設立されたことを踏まえ、当局としては、金融機関の「自助」を前提とした「共助」の重要性について、引き続き機会を捉えて周知していくことが必要である。

[17] Threat-Led Penetration Testing の略。

(6) 金融分野の人材育成の強化

金融機関が、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、単なる技術上のリスクにとどまらず組織全体での対応が必要なビジネスリスク・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り、そのためには経営層の意識改革が不可欠となる。

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等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を促した。一部地域においては、金融 ISAC と連携して経営層も参加するワークショップ形式でのセミナー開催といった取組みを実施し、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た。今後、地域における状況を踏まえ、こうした取組みを他の地域にも展開していくことが重要である。

当局においても、各業界との意見交換会、金融 ISAC や FISC 等の関係機関の主催するセミナー等での講演、財務（支）局におけるモニタリングの機会を捉えて、経営層に対してサイバーセキュリティへの意識づけを進めてきた。この結果、サイバーセキュリティへの意識の高まりが一定程度みられるものの、2020 年東京大会に向けて、さらなる意識改革を進め、経営層のリーダーシップの下、サイバーセキュリティに係るリスクを重大なビジネスリスク・コーポレートリスクの一つとして捉えて取組みを進めることが重要である。

３．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、金融分野を取り巻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・巧妙化する中、今後「2020 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、今後当局として、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を図っていくため、以下の取組みを重点的に推進していく。

○　デジタライゼーションの進展を踏まえた対応

今事務年度実施したヒアリング結果等を活用し、金融機関の規模・特性を踏まえつつ、デジタライゼーションの進展状況等の把握に取り組む。また、こうした領域は進展が非常に速い分野であることを踏まえ、金融機関のみならず、非金融プレイヤーを含む様々な主体から積極的に情報を収集し、金融分野に対してサイバーセキュリティの観点から必要な対応をプロアクティブに促していく。

○　2020 年東京オリンピック・パラリンピック競技大会に向けた対応

2020 年東京大会に向けて、実態把握や対話等を通じた各金融機関のサイバー対策の強化、脆弱性診断・TLPT や演習等を通じたサイバー対策の実効性向上に取り組む。また、2020 年東京大会に係る政府全体の取組みに対して、積極的に貢献するとともに、先般立ち上げた「サイバーセキュリティ対策関係者連携会議」等を活用し、金融 ISAC や FISC 等とともに、金融分野における大規模インシデントへの対応を含む「共助」、「公助」態勢の強化を推進する。