金融分野のサイバーセキュリティレポート

令和２年６月

金融庁
Financial Services Agency

[目次]

はじめに

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・公表した。

その後、金融分野のデジタライゼーションの進展、国際的な議論の進展及び東京2020オリンピック・パラリンピック競技大会（以下、「東京2020大会」という。）の開催などの状況変化を踏まえ、2018年10月、取組方針をアップデートし、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。

令和元事務年度は、東京2020大会を見据え平時におけるサイバーセキュリティ管理態勢、有事におけるインシデント対応能力の強化を通じて、金融機関のサイバーセキュリティ対策の実効性向上に取り組んだ。また、デジタライゼーションの進展や新型コロナウイルス感染症対策としてテレワーク等が拡大し、金融分野を取り巻く環境が変化する中、脅威情報の収集等を通じて、新たなサイバーリスク等の把握・分析に取り組み、積極的に金融機関の対応を促してきた。

IT技術の進化に応じて、金融機関のビジネスの変革が活発になる中、利用者の利便性の向上を図るためには、その前提として適切にサイバーセキュリティ対策を講じ、サービスの安全性（利用者保護）を確保することが重要である。

サイバー攻撃は引き続き複雑化・巧妙化しており、当局、金融機関、関係団体など官民が一体となって業界全体の対策向上に取り組んでいく必要がある。

本レポートは、令和元事務年度におけるこうした取組みで把握した実態や共通する課題等について公表するものである。

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

近年、国内では、企業や民間団体、官公庁等の業界を問わず、標的型攻撃による機密情報の窃取や、ランサムウェア[1]、DDoS 攻撃[2]等のサイバーインシデントが数多く発生している。

国内金融機関においては、これまでに金融システム全体が機能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、攻撃者が金融機関などを装った偽のウェブサイトに利用者を誘導し、不正送金やクレジットカード情報が窃取される等の被害が発生している。

海外の金融機関においては、2019 年３月に米国の大手金融持株会社がサイバー攻撃を受け、約１億人の個人情報が漏えいした。また、同年 12 月に英国の大手外貨両替会社がサイバー攻撃を受け、同社の外国為替サービスを利用する金融機関において顧客の注文を処理できないなどの影響が発生した。そのほか、同年 10 月に、国内外で、金銭を要求するいわゆる「脅迫文付き DDoS 攻撃」等のサイバーインシデントが発生した。

このようにサイバーインシデントは国内外のいたるところで発生しており、サイバーセキュリティを確保するために、より一層の対策強化が必要とされる状況である。

(2)国内金融機関のサイバーインシデントについて

国内金融機関に対する攻撃手法別の傾向としては、リスト型攻撃[3]や設定ミス等に起因した不正ログイン及び DDoS 攻撃に関する報告が多くを占めている。

一方、サイバーインシデントは、システムの本番環境に限らず、テスト環境でも発生しており、また海外拠点を経由した日本への攻撃事案も報告されている。

特に、リスト型攻撃手法による不正ログインや「脅迫文付き DDoS 攻撃」については、他金融機関においても同様のインシデントが発生する恐れがあることから、2019 年 10 月、金融機関に注意喚起を発出し、適切な認証方式による対策や DDoS 攻撃を受けた場合の態勢等の確認など、所要の対応を求めた。

業態毎の特徴としては、主に預金取扱金融機関、金融商品取引業者及び貸金業者において、不正ログインによる個人情報の窃取や DDoS 攻撃によるサービス提供の遅延等がみられた。また、暗号資産交換業者では、ホットウォレットの秘密鍵が不正に窃取され、多額の暗号資産が流出される被害が発生している。

こうした状況を踏まえ、今後も新たな脅威や脆弱性をタイムリーに把握・分析し、金融分野のサイバーセキュリティ管理態勢の強化を促していく必要がある。

(3)新型コロナウイルス感染症等によるサイバーセキュリティへの影響

新型コロナウイルス感染症が日本を含む世界各国で深刻な影響を及ぼす中、新型コロ

---

[1] 「ランサムウェア」とは、コンピュータウイルスの一種で、感染したコンピュータの利用制限やそのコンピュータを介してシステムのファイルが暗号化され、解除するために身代金を要求されることを指す。

[2] 「DDoS 攻撃」とは、Distributed Denial of Service の略で、分散型サービス妨害攻撃のことを指す。

[3] 「リスト型攻撃」とは、悪意を持った攻撃者が何らかの方法で入手したアカウント情報のリストを使用し、正規ユーザーを装ってログインしようとする攻撃手法のことを指す。

ナウイルス感染症に便乗したサイバー攻撃や、新型コロナウイルス感染症への対策として導入が進んでいるテレワーク環境を狙ったサイバー攻撃などが数多く発生している。

【図表１：新型コロナウイルス感染症に便乗したサイバー攻撃の事例】

項番	攻撃分類	事例
1	メール・SNS 等を用いた標的型攻撃	世界保健機関（WHO）や国立感染症研究所等の公的機関による給付金の配布を騙り、メールや SNS を用いてEmotet等のマルウェアへの感染やフィッシングサイトに誘導する。
2	フィッシングサイト	マスクの販売や政府機関の公式ホームページに似せた偽サイトにて、クレジットカード情報や個人情報の窃取を行う。
3	マルウェア	新型コロナウイルス感染症への対策に役立つアプリケーションを装って、クレジットカード情報や個人情報の窃取を行う。
4	ランサムウェア・DDoS	医療機関や政府機関、研究所等に対して機能停止を狙った攻撃を行う。
5	テレワーク環境を狙った攻撃	在宅ワークやリモートアクセス環境を狙って情報の窃取を行う。

（資料）金融庁

上表のとおり、新型コロナウイルス感染症に便乗したほとんどのサイバー攻撃は従来の攻撃手法が用いられているが、これまでの攻撃動向をみると、時々刻々と変化する世の中の環境に応じて、攻撃対象や標的型メール本文の内容等を随時変更しているといった特徴がある。このため、金融機関においても、タイムリーにサイバー脅威を把握し適切に対応してくことが求められる。

これまでのところ、国内金融機関では、新型コロナウイルス感染症の感染防止を含めたシステムの業務継続対策として、例えば、テレワーク及び交代勤務制・時差出勤やスプリット・オペレーション[4]を実施するなど、安全を確保しながら業務を継続してきており、重大な問題は発生していない[5]。

新型コロナウイルス感染症の影響を受けて、「新しい生活様式」が進む中、金融分野においても、テレワークを活用した新しい働き方や金融サービスの電子化が一層進展することが想定されるため、こうした環境変化を踏まえ、セキュリティ対策にも留意していく必要がある。

[4] 「スプリット・オペレーション」とは、業務を２つ以上のチームに分けて遂行し、同時感染を回避する手法のことを指す。

[5] サイバーインシデントではないが、2020 年３月に一部金融機関において、新型コロナウイルス感染症を発端とする株価変動等により、想定を超えた取引量に起因したシステム障害が発生。「金融機関のシステム障害に関する分析レポート」（令和２年６月公表）を参照

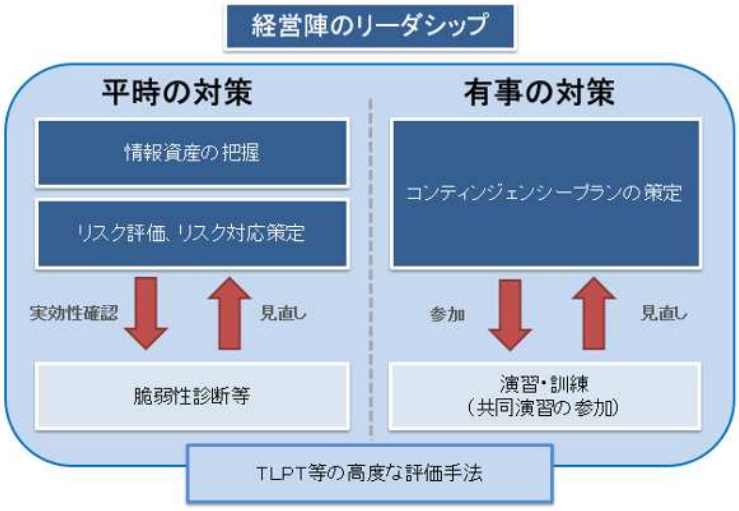
２．金融分野のサイバーセキュリティ強化に向けた取組み状況

(1) 金融機関のサイバーセキュリティ管理態勢の強化

これまで、金融機関のサイバーセキュリティ対策について、平時の対策・有事の対策の２つの観点から強化に取り組んできた。令和元事務年度は、それらの観点について、金融機関との対話や演習を通じて、金融機関のサイバーセキュリティ対策の実効性向上を促してきた。

また、東京 2020 大会の開催を見据え、金融機関全体のサイバーセキュリティ態勢の把握及び底上げに取り組んだ。

【図表２：平時・有事の対策の考え方】



（資料）金融庁

① 平時のサイバー対策

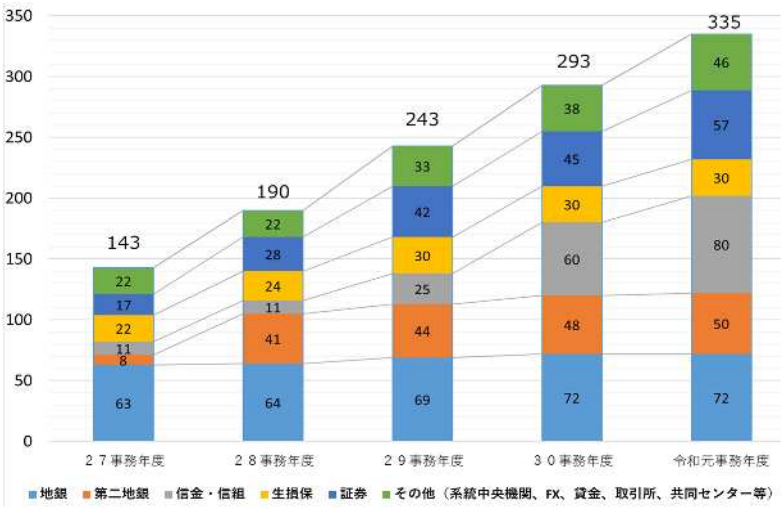
ア. 中小金融機関等

これまで、中小金融機関については、実態把握（対話によるモニタリング）を通じて、基礎的なサイバーセキュリティ管理態勢の整備状況[6]を検証してきており、平成 30 事務年度から、新たな目線としてセキュリティインシデントの監視・分析状況や脆弱性診断の実施状況などを加え、実態把握を行っている。

令和元事務年度は、業界全体の底上げの観点から、基礎的なサイバーセキュリティ管理態勢の整備の遅れが懸念される先を中心に、実態把握を行った。

[6] 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

【図表３：業態別実態把握先の推移（実態把握先の累計（２巡目含む））】



（資料）金融庁

○ 地域銀行・信用金庫・信用組合

地域銀行、信用金庫、信用組合の各業態について、基礎的なサイバーセキュリティ管理態勢の整備に遅れが懸念される先を中心にリスクベースで対象先を抽出して実態把握を行い、基礎的な態勢整備に向けた取組状況を確認するとともに、サイバーセキュリティ対策の実効性の検証を行った。

実態把握の結果、一部の先では、経営陣も積極的に関与して取組計画に基づく管理、モニタリングを行うなど、自主的に強化を図っている状況がみられたものの、依然として基礎的な態勢整備に課題[7]がある先もみられた。

これらの先については、対話を通じて直接的に取組加速を要請するとともに、金融庁と財務局が一体となって取組状況をフォローアップし、各先の課題解消に向けて、経営陣が主体となった取組みの推進態勢の整備を促進している。

○ 証券会社等

証券会社等については、これまで実態把握を行っていない地域証券会社、FX 業者、PTS 業者[8]のうち、リスクプロファイルにより態勢整備の遅れが懸念される先に対して実態把握を行った。その結果、取組みが進展している金融機関が増えている一方、依然として取組みの進展が停滞状態の先もみられた。

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、自主的にサイバーセキュリティ管理態勢の強化等を図っている。一

[7] 実態把握でみられた課題は以下の通り
・取組計画の進捗状況のモニタリング等において、経営の関与がみられない。
・リスク評価が形式的な実施に留まり、残存リスクの特定ができていないなど、自社のリスクが経営に正しく伝わっていない。
・コンティンジェンシープランを策定したものの、その実効性を検証するプロセスが整備されておらず、プランが自組織に即した内容となっていない。

[8] 「PTS 業者」とは、Proprietary Trading System の略で、私設取引システムのことを指す。

方、信用金庫・信用組合と同様に、基礎的な態勢整備が未だ途上の段階にある先もみられた。また、基幹システム系ネットワークとインターネット環境とを物理分離していることに安心して、両ネットワーク間のデータのやり取りに関する規程が整備されていない先や、ウェブサイトの管理を外部委託先に一任している中、脆弱性等の対応状況を把握していない先がみられた。これらの先については、対話を通じて直接的に取組加速を要請するとともに、金融庁と財務局が一体となって取組状況をフォローアップし、各先の課題解消に向けて、経営陣が主体となった取組態勢の整備を促進している。

○ 資金決済事業者（前払式支払手段発行者、資金移動業者）等

資金決済事業者について、令和元事務年度に発生した不正利用等の事案を受けて、主要なスマートフォン決済サービスを営む事業者に対し、サイバーセキュリティ対策の実態の把握を行った。その結果、リスクに応じた利用者認証方式や不正取引の監視体制等に課題がある先もみられた。

これらの先については、対話を通じてセキュリティ対策の向上を促すとともに、事業者に向けた注意喚起[9]を行い、業態全体のサイバーセキュリティ管理態勢の整備を促進している。

イ. 大手金融機関等

これまで、大手金融機関については、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、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[10]に、定期的な対話を通じて、継続的に議論を重ねてきた。

令和元事務年度は、３メガグループ等については対話の中で、サイバー攻撃の複雑化・巧妙化、国際的な動向等を念頭に、高度化が期待されるグループ・グローバルでの管理態勢の高度化、TLPT[11]の活用状況を中心に確認した[12]。また、信託銀行やネット銀行等については、相対的にリスクの高いと思われる金融機関に対して、アンケートを通じたオフサイトモニタリングを実施した。

○ ３メガグループ等

グループ・グローバルの管理態勢について、各社は、グループ会社（海外拠点を含む）の重要なシステムのリスク評価や主要グループ会社を対象とした詳細なサイバーセキュリティ能力成熟度評価を行うなど、グループ・グローバルベースの一元的な管理態勢の高度化に取り組んでいる。

各社とも、サイバーセキュリティ対策の弱いグループ会社や外部委託先が攻撃されるリスクを踏まえ、アクセスコントロールの強化、サイバーレジリ

[9] 「キャッシュレス決済機能を提供する事業者の皆様への注意喚起」（令和元年８月６日公表）（https://www.fsa.go.jp/policy/shikinkessai/01.pdf）

[10] ３メガバンク、大手証券、大手生損保、ゆうちょ銀行と定期的な対話を実施

[11] 「TLPT」とは、Threat-Led Penetration Testing の略で、脅威ベースのペネトレーションテストのことを指す。

[12] 特に、保険会社に対しては、協会と連携して、代理店のサイバーセキュリティ強化に取り組んだ。

エンスの高度化等を通じて、引き続きグループ・グローバルでの一元的な管理態勢の強化を図っていくことが期待される。

また、TLPT については、各社ともサイバーセキュリティの実効性を向上させるために活用しており、特に、３メガは、銀行以外の主要グループ会社にも対象を拡大させている。

こうした中、各社は、TLPT をより実効性のあるものとするため、各種ガイドライン[13]に準拠することに加え、国際的なフレームワーク[14]を活用して、攻撃側（レッドチーム）による攻撃シナリオの評価や防御側（ブルーチーム）によるインシデント対応能力の評価等の高度化を行うこと、また、こうした取組みに必要となる、より高度な専門人材の育成を継続することが期待される。

○ 信託・ネット銀行等

信託銀行やネット銀行等については、これまでにアンケート等によるサイバーセキュリティ管理態勢のモニタリング[15]を実施しており、各行とも基礎的なサイバーセキュリティ管理態勢は概ね整備している状況であった。こうした中、東京 2020 大会の開催も見据え、令和元事務年度は相対的にリスクの高いと思われる金融機関[16]に対して、アンケートを通じたオフサイトモニタリングを実施した。

その結果、全般的に基礎的なサイバーセキュリティ管理態勢は維持していることを確認するとともに、サイバーセキュリティの高度化に向けた取組みを推進している先がみられた。しかしながら、一部銀行については、経営陣が主体となった取組推進やリスク認識に改善の余地がみられたため、意見交換を通じて課題を共有し自主的な改善活動を促した。

② 有事のサイバー対策

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、防御に加えて攻撃を受けた後の対応が重要となる。

サイバー攻撃に的確に対応するためには、演習を通じて、現在の対応態勢や手順が十分であるかを確認するなど、PDCA サイクルを回しつつ、インシデント対応能力を向上させることが有効である。

こうした認識の下、金融庁では、毎年、金融機関の対応能力強化を図るため、「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。

---

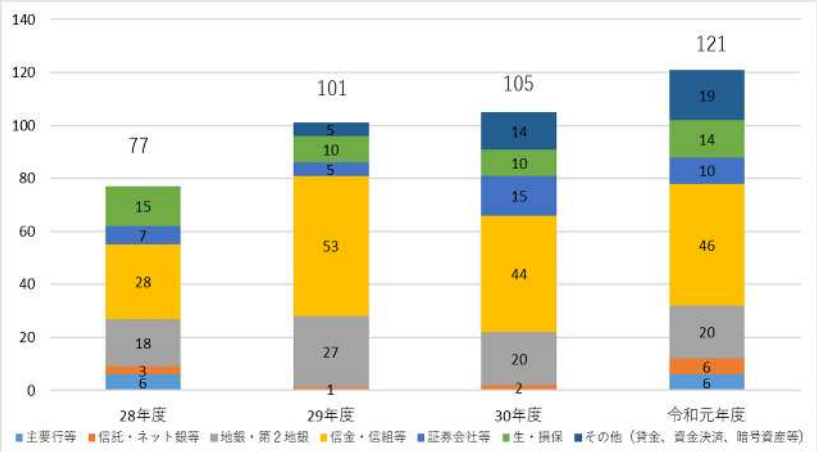
[13] 「脅威ベースのペネトレーションテストに関するＧ７の基礎的要素」、公益財団法人金融情報システムセンター（FISC）の「金融機関等における TLPT 実施にあたっての手引書」

[14] MITRE 社の ATT&CK 等が想定される。

[15] 平成 28 事務年度及び平成 29 事務年度に実施

[16] 2017 年度以降に新規設立・業態変更した先、直近でサイバー攻撃被害状況のあった先等を抽出

【図表４：業態別サイバー演習参加社数推移（年度別）】



（資料）金融庁

令和元事務年度は、東京 2020 大会に向けた、大規模インシデントの発生に備え、業界全体の底上げの観点から継続的に参加している中小金融機関に加え、金融サービスへの影響が大きい大手金融機関が参加したほか、本演習の対象となっていなかった業態（資金移動業者、前払式支払手段発行者、監査法人等）を追加し、121 社（約 2,000 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規程類の見直しを実施・予定しているほか、社内及び外部組織との情報連携の強化に関する対応を実施・予定しており、本演習を通じて対応態勢の改善が図られている。

一方で業態別では、大手銀行、地域銀行、保険会社は全般として対応が概ねできていたものの、復旧対応や顧客対応に課題が一部みられた。その他の業態については事案の分析及び対応の優先度に関する判断（トリアージ）、顧客からの問合せ増加を見据えた顧客対応、インシデント発生に関する再発防止策の検討など、全体的に改善の余地がみられた。

本演習結果を踏まえ、引き続き改善の余地がみられた業態のインシデント対応能力の向上を図っていく必要があるほか、対応が概ねできていた業態については、シナリオに対する金融機関内での深度ある議論が求められるような形式とするなど更なる高度化を図っていく。

なお、サイバー演習については、金融庁のほか、NISC(内閣サイバーセキュリティセンター)、一般社団法人金融 ISAC（以下、「金融 ISAC」という。)、業界団体が多様な演習を実施しており、こうした演習への参加を通じてインシデント対応能力の更なる向上を図っていくことが重要である。

【金融業界横断的なサイバーセキュリティ演習（Delta Wall）について】

金融庁では、2016 年から毎年 10 月に金融業界全体のインシデント対応能力の底上げを図ることを目的に「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。過去４回実施し、平成 28 年度は 77 先、平成 29 年度は 101 先、平成 30 年度は 105 先、令和元年度は 121 先の金融機関等が参加した。

➢Delta Wall
サイバーセキュリティ対策のカギとなる「自助」、「公助」、「共助」の３つの視点（Delta）＋防御（Wall）

〇本演習の特徴は以下の通り

・インシデント発生時における金融機関内外の情報連携に係る対応態勢や手順の確認を目的
・経営層や多くの関係部署（システム部門、広報、企画部門等）が参加できるよう、自職場参加方式で実施
・民間の専門家の知見や攻撃の実例を踏まえたサイバーリスクの洗い出しを行うことにより、金融機関が陥りやすい弱点が浮き彫りとなり、参加者が「気づき」を得ることができる内容
・参加金融機関が PDCA サイクルを回しつつ、対応能力の向上を図ることができるよう、具体的な改善策を示すなど、事後評価に力点
・本演習の結果（全体的課題や良好事例）は、参加金融機関以外にも業界全体にフィードバック
・過去の演習実績を踏まえ、より実効性の高い演習方法・内容等を検討し、継続的に改善を実施

③ 東京 2020 オリンピック・パラリンピック競技大会の開催を見据えた管理態勢の強化

東京 2020 大会は、国際的な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、金融機関を含む重要インフラ事業者等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、金融機関のサイバーセキュリティ管理態勢の強化に向けて、平時の対策としてサイバー攻撃で端緒となることの多い既知の脆弱性にしっかり対処しておくこと、有事の対策としてサイバー攻撃が発生した際に適切なインシデント対応ができるようにしておくことなど、これまで整備してきた基礎的なサイバーセキュリティ管理態勢[17]の実効性を向上させておくことが何よりも重要である。加えて、インシデントの発生を早期に検知し迅速なインシデント対応につなげるためには、自社の情報資産等の監視・分析状況を整理しておくことも重要となる。

ア. 基礎的なサイバーセキュリティ管理態勢の実効性向上

[17] 特に、信用金庫・信用組合では、業界団体の協力のもと、平成 30 事務年度になってリスク評価・コンティンジェンシープランを策定した先が多かった。

こうした認識のもと、地域銀行、信用金庫・信用組合に対し、2020 年３月末までに、①脆弱性診断の実施、②演習・訓練によるコンティンジェンシープランの実効性向上、③監視・分析状況の整理・対策強化、を実施するよう要請するとともに、各協会と連携して、その取組みを支援してきた。

その結果、多くの金融機関は、脆弱性診断の実施、演習・訓練への参加、監視・分析状況の整理を対応期日（2020 年３月末）までに完了した。特に、信用金庫・信用組合業界全体では、平成 30 事務年度において、脆弱性診断の実施が１割程度、外部演習への参加が６割程度にとどまっていたところ、いずれも９割以上に大きく増加した。ただし一部の金融機関ではその対応に遅れがみられた。こうした先については、引き続き、協会と連携しフォローしていく。

なお、その他の金融機関[18]に対しても、別途アンケート等を通じて、脆弱性診断の実施等の要請に相当する事項について確認した。要請に相当する３つの事項については、特段の課題はみられなかったが、今後も必要に応じて取組み状況の把握やフォローを行っていく。

イ.要請対応やアンケートを通じて把握した事例や実効性向上への課題

脆弱性診断については、外部公開 Web サイト（自社のサブサイトやグループ会社のサイトを含む）やリスクの高い内部環境領域といった対象範囲を特定した上で、計画的に診断を実施している良好事例がみられた。一方、診断で検出された脆弱性への対策が必要と認識しながら、リスク認識が不十分なため対策の意思決定に時間がかかっている事例もみられた。

演習・訓練については、外部団体主催の演習や内部訓練を複数回行い、コンティンジェンシープランの見直しにつなげている良好事例がみられた一方、演習参加にとどまり、振返り等を実施せず、課題の洗い出しや改善につなげられていない事例もみられた。

監視・分析については、インシデントを早期検知し、速やかに分析する態勢を整備している良好事例がみられた一方、ログを取得はしているものの、平時における確認や分析には至っていない事例がみられた。

また、外部委託管理の観点では、契約時に脆弱性診断や監視等について明確化しておらず、脆弱性診断の実施ができない、あるいはセキュリティ対策の状況の開示を拒否される事例などがみられた。このため、各金融機関は、必要に応じて、委託先との役割・責任分担等を改めて契約書にて明確化する等、外部委託先の管理状況を見直すことが重要である。

2020 年３月、新型コロナウイルス感染症の影響により東京 2020 大会の延期が発表されたが、サイバーリスクはむしろ高まっており、各金融機関は、上記事例も参考にして、引き続き、経営陣の強いリーダーシップのもと、サイバーセキュリティ管理態勢の実効性の維持・向上に取り組むことが重要である。特に、今回の要請を受けて初めて脆弱性診断や演習を実施した金融機関は、今後もこうした取組みを定期的に実施していくことが必要である。

[18] 都市銀行、信託銀行、その他銀行、資金決済事業者、証券、生損保、貸金業者など

④ デジタライゼーションの加速的な進展を踏まえた対応

金融庁では、平成 30 事務年度、デジタライゼーションの領域を大きく５つの観点[19]に整理した上で、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・分析した。

令和元事務年度は、国内外の金融機関や IT ベンダー等にヒアリングを行い、クラウドサービスを中心にデジタライゼーションの進展状況等の把握・分析に引き続き取り組んだ。

ア. クラウドサービス全般

国内金融機関におけるクラウドサービス利用は拡大しており、クラウドサービス導入率は 50%を超えている状況[20]にあり、特に、銀行業態についてはほとんどの先が既に導入している。利用用途としては、電子メールや社内情報共有、営業支援システムが多いものの、基幹業務システムをパブリッククラウド上に構築する動きも出てきている。

こうした中、国内金融機関においては、クラウドサービスに起因する大規模なサイバーインシデントはこれまで報告されていないものの、2019 年３月には米国の大手金融持株会社において、クラウドサービスの設定不備に起因するサイバーインシデントが発生している。

通常、利用するクラウドサービスの提供形態（SaaS[21], IaaS[22]等）によって責任分界点は異なるが、クラウドサービス利用者側の責任の範疇において適切に設定・管理・運用することが求められる。このため、スキルのある人材確保[23]やサービスの変化に合わせた継続的なスキルアップが必要である。

大手金融機関では、利用するクラウドサービス業者が提供する研修の受講、認定資格保有者数の目標設定、新サービスについての説明会実施やサービス提供事業者が主催するイベントへの参加などを通して、新サービスの早期活用、継続的なスキルアップを図っている取組みがみられた。また、各クラウドサービスやサードパーティ製のツールを活用し、設定不備や誤設定をシステム的に検知・是正できる仕組み・ツールの導入が進んでいる状況であった。

イ. 新たなセキュリティモデルへの転換

従前のセキュリティモデルでは、信頼できる内部（社内）ネットワークと信頼できない外部（社外）ネットワークとで境界を設け、内部ネットワークであれば全て信頼できるという境界による防御を意識したセキュリティ対策が一般的であった。

しかしながら、クラウドサービスの利用により情報が社外に置かれるようにな

[19] ①クラウドサービス、②AI（RPA）、③外部連携（外部委託）、④外部接続（社外環境）、⑤IoT

[20] 公益財団法人金融情報システムセンター（FISC）の「令和元年度金融機関アンケート調査結果」（金融情報システム（令和元年 11 月号））によると、平成 30 年度の国内金融機関のクラウドサービス利用率は「52.9%」であった。

[21] 「SaaS」とは、Software as a Service の略

[22] 「IaaS」とは、Infrastructure as a Service の略

[23] 自社で人材を確保できない場合には、マネージドサービスの活用という方法も考えられる。

り、従来の境界があいまいになってきている。また、働き方改革や新型コロナウイルス感染症等の環境変化により、テレワーク等外部から内部への接続ニーズ（グループ企業やサードパーティによる接続を含む）が高まることで、外部から内部への侵入リスクも高まっている[24]。

こうした中、大手金融機関の中には、たとえ内部であっても「全て信頼できない」とするゼロトラストを意識したセキュリティ対策（例えば、利用者やデバイスの認証・認可の高度化[25]など）に本格的に取り組む動きがみられる。

【技術的な取組事例】

●コンテナ・マイクロサービスに関する取組み

ビジネスの変化が早く不確実性の高い業種（特にインターネット系企業）では、クラウドサービスの活用において、コンテナ技術、マイクロサービスアーキテクチャなどの新技術を取り入れて、ユーザーの要望に対して素早く継続的に改善する取り組みが行われている。

➢コンテナとは
仮想化方式の１つ。１つの OS 環境の上に分離した空間を作成し、その分離された空間ごとに異なる OS 環境を実現しアプリケーションを実行できる技術。システム資源の負担は小さく可搬性は高い。

➢マイクロサービスアーキテクチャとは
ソフトウェア・アプリケーションを小さく、独立し、疎結合のサービスの組み合わせとして設計する方法。単位が小さくスピーディーに開発が可能になる他、それぞれが１つの独立したサービスとして構成されるため、相互に影響なく変更等も可能。

金融分野においても、既に資金移動業者にて本番環境で利用している事例がみられたほか、ネット銀行や地域銀行においてもこうした手法や技術を活用して勘定系システムをクラウドサービス上へ構築する動きがみられた。
新技術の導入にあたっては、IT ガバナンスを発揮した上で、新技術を適用するシステム案件の選定や適切な開発手法（アジャイル開発等）の選択、新技術に対応した体制（DevSecOps 等）の整備、新技術に精通した人材の育成・確保などを行っていくことが重要である。

➢新技術に精通した人材の育成・確保の必要性
新しい技術は機能追加のためのバージョンアップの頻度も高く、速やかに対応していくためには、開発時のみならず、リリース後も継続的な人材の育成・確保が必要となることに留意が必要。

加えて、コンテナ技術の脆弱性を狙ったサイバー攻撃が既に確認されており、サイバーセキュリティの観点での対応も必要である。例えば、新技術の特性や既存の技術との違いを考慮してリスク評価を行うことや、開発プロセスの早い段階から必要なセキュリティ対策に取り組むこと（セキュリティ・バイ・デザイン）が求められる。

[24] 仮に、社内へのアクセス用に VPN を構築しても、接続端末がマルウェアに感染した場合には、マルウェアが VPN を経由して社内に侵入し感染が社内に拡大するリスクがある。
[25] ゼロトラストを意識した認証の高度化として SDP（Software Defined Perimeter）が挙げられる。なお、認証の高度化の一つして二要素認証が利用されるが、トレンドマイクロ社「2019 年年間日本セキュリティラウンドアップ」によると、近年増加しているスミッシング（モバイル端末のメッセージサービス）を悪用してワンタイムパスワードを窃取する手口を応用し、クラウドサービスや VPN アクセスにおける二要素認証が突破される可能性が指摘されており、二要素認証なら安全と考えるのは危険である。

(2)関係団体・海外当局との連携を通じた取組み

① 情報共有の枠組みの実効性向上

金融業界全体のサイバーセキュリティを強化していくためには、金融機関自身の取組みである「自助」を前提としつつ、金融機関同士で情報共有・分析を行うなど連携した「共助」が非常に有効である。

金融庁として、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。

「共助」の取組みには、サイバーの脅威・脆弱性等の情報共有に加え、有効性の高いセキュリティ対策に係る情報共有やサイバーセキュリティ対策の提供などがある。これまで、サイバーの脅威・脆弱性等の情報共有、有効性の高いセキュリティ対策に係る情報共有については、金融 ISAC を中心に進められてきたが、今後、さらなるサイバーセキュリティ強化を図るためには、業界団体との連携等を一層充実させていくことにより、サイバーセキュリティ対策の提供を含めた「共助」を深化していくことが期待される。金融庁としては、引き続きこうした活動を積極的に支援していく。

② 大規模インシデント発生時の連携

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金融分野の関係者相互の円滑な情報連携ができるよう、2019 年６月にサイバーセキュリティ対策関係者連携会議（以下、「連携会議」という。）を立ち上げた。

連携会議を活用し、東京 2020 大会の開催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、連携手順の整備やサイバー演習等を通じた業界全体の連携態勢の強化を図ってきている。具体的には、連携会議立ち上げからこれまでに６回の会議を開催し、連携手順書の整備及びサイバー演習（Delta Wall Ⅳ）での確認、連携会議内で使用するシステムを情報共有システム（JISP）とすることに決定した。

今後は、行動計画[26]に基づく情報共有はもとより、情報共有システム（JISP）を利用したメンバー間での情報連携について、NISC 主催の演習に参加し、その有効性・実効性を確認していくほか、金融システム全体のインシデント対応能力の向上を図る観点から、サイバー演習（Delta Wall）において、連携会議メンバー間での情報連携の確認を行っていく。

③ 国際的な連携

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、連携してサイバーセキュリティ確保に向けた取組みを進めている。特に、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。同会議では、2016 年以降、サイバーセキュリティに関するベストプラクティスをまとめた「基礎的要素」を公表してきており、2018 年には「脅威ベースのペネトレーションテスト（TLPT）」に

[26] 重要インフラの情報セキュリティ対策に係る第４次行動計画（平成 29 年４月 18 日サイバーセキュリティ戦略本部決定）

関する基礎的要素が策定・公表された[27]。TLPT に関する基礎的要素の公表を踏まえ、金融庁として大手金融機関に TLPT の活用を促すとともに、公益財団法人金融情報システムセンター（以下、「FISC」という。）と連携を図り、国内金融機関が TLPT を実施する際の参考に資することを目的として「金融機関等における TLPT 実施にあたっての手引書」が FISC から 2019 年９月に公表された。

2019 年６月には、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、G７諸国の当局を中心としたクロスボーダーの連携を確認した[28]。引き続き、本演習の事後対応として、演習を通じて得られた知見や教訓を踏まえ、G７当局間の連携手順の改善など、国際的な連携の強化に向けた議論を進めている。

また、最近の国際的な議論[29]においては、クラウドサービスなどのサードパーティやサイバーインシデントからの復旧・回復といったレジリエンスの考え方が取り上げられている。こうした議論を含め国際的な動向を的確に把握・対応していくことが重要である。

３．当局の今後の取組み

新型コロナウイルス感染症の拡大に伴う外部環境の変化や 2021 年に延期された東京 2020 大会など、金融機関を取り巻くサイバーリスクは一層高まっている状況にある。こうした状況を踏まえ、金融機関においてはサイバーセキュリティの重要性を認識し、経営層のリーダーシップの下、サイバーセキュリティ対策に取り組んでいく必要がある。

今後当局としても、金融分野における更なるサイバーセキュリティ対策の強化を図っていくために、以下の取組みを重点的に推進していく。

○　金融分野の環境変化への対応

金融分野では、IT技術の利活用等によるデジタライゼーションが進展する中、新型コロナウイルス感染症への対応としてオンライン化・リモート化が加速しており、金融機関を取り巻く環境は大きく変わってきている。こうした新たな金融サービス・インフラの前提として、サイバーセキュリティの確保はますます重要な課題となってきている。

金融庁としては、こうした環境の変化を踏まえた新たなセキュリティに関する脅威の動向について、デジタライゼーションの進展を踏まえたサイバーセキュリティへの取組みとあわせて、積極的に情報収集を行い、必要な対応を促していく[30]。

---

[27] これまで４本の「基礎的要素」を公表

[28] 我が国からは、金融庁、日本銀行、金融 ISAC、大手金融機関等が合同演習に参加

[29] G20 の FSB（Financial Stability Board）等において議論されている。

[30] 本レポートとあわせて「金融機関の IT ガバナンス等に関する調査レポート」、「金融機関のシステム障害に関する分析レポート」を公表している。サイバーセキュリティ及びシステム障害分析に関しても、企業価値の創出を実現するための仕組みである IT ガバナンスの一環である。例えば、デジタライゼーションの進展や新しい生活様式への対応を進めるためには、IT ガバナンスの発揮に加え、適切な IT マネジメントの下、セキュリティに留意しつつ取り組むことが重要である。

○　金融機関のサイバーセキュリティ強化に向けた対応

中小金融機関に対しては、業界団体等との連携を通じた基礎的なサイバーセキュリティ管理態勢の実効性の維持・向上を促すとともに、サイバー演習によりインシデント対応能力の底上げを図る。また、各業態のサイバーセキュリティ対策の取組みに進展がみられる先との意見交換を通じてプラクティスを収集し、好事例を積極的に還元していく。

大手金融機関に対しては、国際的な議論の動向を念頭に、定期的な対話を通じて、グループ・グローバルベースでのサイバーセキュリティに関するリスク管理の高度化、TLPTの実効性向上を通じたサイバーセキュリティ対策のより一層の高度化を促す。また、海外において、破壊的なマルウェアの活動に対する警戒[31]が高まっており、検知の遅れにより長期間ネットワーク内で活動するリスク等を踏まえ、サイバーレジリエンスへの取組みについても対話を行う。

[31] 例えば、米国通貨監督庁（OCC）は、「Joint Statement on Heightened Cybersecurity Risk」（2020年1月16日）を発出している。