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
（Ver. 3.0）

令和４年２月

金融庁

目次

１．はじめに

金融庁では、「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」（取組方針。2015 年 7 月に Ver. 1.0 を策定、2018 年 10 月に Ver. 2.0 にアップデート）に基づき、金融業界と連携して金融分野のサイバーセキュリティ管理態勢の強化に取り組んできた[1]。

取組方針（Ver. 2.0）では、2020 年東京オリンピック・パラリンピック競技大会（東京大会）を見据えたサイバーセキュリティの強化を新たな重要課題として位置付けていたが、1 年の延期を経て開催された東京大会は、金融機関やその顧客に被害を及ぼすサイバーインシデントは発生せずに終了した。

他方、取組方針を Ver. 2.0 にアップデートして以来、デジタライゼーションの動きは一層加速し、データの利活用の拡大や、新たなビジネスチャンスを捉えた新しいプレイヤーの金融分野への参入がさらに進んだ。加えて、新型コロナウィルス感染症の拡大は、リモートワークやオンラインでの商品やサービス提供の普及といった社会のデジタル化にも影響を与えたが、これらの非対面・非接触型の業務の脆弱性を狙ったサイバー攻撃や、ソーシャルエンジニアリングを用いた巧妙なサイバー攻撃も増加した（参考 1）。

前回のアップデートから約 3 年が経過し、金融分野のサイバーセキュリティを巡る状況が日々変化する中でサイバー空間における脅威は一層高まっている。これまでの取組みを振り返るとともに、新たな課題・脅威に対する対応方針を取組方針（Ver. 3.0）としてアップデートし、金融機関、金融サービス利用者及び関係機関と広く共有するため公表することとした。

（参考 1）国内の金融機関に対する主なサイバーインシデント事案（2018 年 10 月以後）

	時期	業態	概要
国内	2019 年 7 月	前払式支払手段発行者	認証設計の脆弱性を攻撃された不正利用
	2019 年 7 月	暗号資産交換業者	不正アクセスによる暗号資産の不正流出
	2020 年 7 月	証券会社	不正アクセスによる個人情報の漏えい
	2020 年 9 月	資金移動業者	認証設計の脆弱性を攻撃された不正出金
	2021 年 4 月	証券会社	不正アクセスによるオンライントレードシステムの停止
	2021 年 12 月	生命保険	認証設計の脆弱性を利用した不正出金[2]

[1] 金融庁ウェブサイト：https://www.fsa.go.jp/news/30/20181019-cyber.html

[2] 例えば、フィッシングと推測される手段で利用者の認証情報を不正取得し、利用者になりすまして架空口座を登録のうえ、契約者貸付手続を行い、架空口座に不正送金する事案が発生した。

２．現「取組方針（Ver. 2.0）」の進捗・評価

金融庁は、「サイバーセキュリティ戦略[3]」で示された政府全体の方針を踏まえ、取組方針（Ver. 2.0）に沿い、取組みを推進してきた。また、毎年の金融行政方針[4]等において、状況の変化に応じ、適時の方針の見直しを行ってきた。以下、2018 年 10 月以降の施策の進捗・評価を整理する。

（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

デジタライゼージョンの進展によって、金融機関に生じ得るサイバーセキュリティリスクを把握・分析するため、クラウドサービス、テレワーク等の利用状況やセキュリティ施策などに関して、国内外の金融機関や IT ベンダーとの対話を行ったほか、外部委託調査[5]を実施した。これらの対話等で得られた先進的な取組事例については、業界に共有し、金融機関に対して、新たなサイバーセキュリティリスクへの対応を促した。

一方、暗号資産取引やキャッシュレス決済などの新たな金融サービスが拡大する中で、セキュリティの不備を攻撃され、顧客資産が不正に送金される事案が複数発生した（下表参照）。

（表）近年の主なインシデントの例（暗号資産取引、キャッシュレス決済、クラウドサービス）

分野	インシデントの概要
暗号資産取引	暗号資産交換業者が外部ネットワークに接続されたホットウォレットで管理していた顧客の暗号資産が、外部からの不正アクセスによって流出する事案が複数発生した[6]。これに対し、2020 年 5 月に改正資金決済法が施行され、暗号資産交換業者は、原則、顧客の暗号資産を外部のネットワークに接続されていないコールドウォレットで管理する措置その他これと同等の技術的安全管理措置を講ずることなどが義務付けられた。
キャッシュレス決済	キャッシュレス決済については、認証設計の脆弱性を攻撃された不正出金が複数発生した。 ・ 2019 年 7 月には、流通系の前払式支払手段発行者において、新規のキャッシュレス決済サービスの提供を開始した直後から、リスト型アカウントハッキング[7]と推測される不正アクセスにより、不正利用が相次いで発生し、同年 9 月末にサービスを廃止した。 ・ 2020 年 9 月には、通信系の資金移動業者が提供するキャッシュレス決済サービスにおいて、悪意のある第三者が不正に入手した預金者の口座情報等をもとに当該預金者の名義で資金移動業者のアカウントを作成し、銀行口座と連携したうえで、銀行口座から資金移動業者のアカウントへ資金をチャージすることで不正な出金を行う事象が発生した。被害者がキャッシュレス決済サービス自体を利用していないにもかかわらず、自らの知らないところで悪意の第三者に自らの名義のキャッシュレス決済サービスのアカウントを作成され、銀行口座と連携されて不正出金された事案であった。

[3] 「サイバーセキュリティ戦略」（平成 30 年 7 月 27 日閣議決定、内閣サイバーセキュリティセンターウェブサイト：https://www.nisc.go.jp/materials/index.html）

[4] 金融庁ウェブサイト：https://www.fsa.go.jp/policy/summry.html

[5] 「ゼロトラストの現状調査と事例分析に関する調査報告書」（金融庁ウェブサイト：https://www.fsa.go.jp/common/about/research/20210630.html）

[6] 中には事業者がサービスの拡大を図る反面、サイバーセキュリティ管理態勢等の整備が追い付いていない事例が認められた。

[7] 犯罪者が何らかの手段により他者の ID・パスワード等を入手し、これらの ID・パスワード等をリストのように用いて様々なサイトに不正ログインを試みる攻撃。

	上記のインシデントを踏まえ、金融庁において、2021 年 2 月に監督指針等を改正し、金融機関による不正防止策の実施、補償方針の策定・実施及び利用者相談に真摯に対応するための態勢整備等を監督上の着眼点として盛り込んだ。
クラウドサービス	2020年12月、クラウド型顧客関係管理ソリューションにおいて、複数の金融機関においてデータのアクセス権の設定不備により、クラウド上で管理する顧客情報等が第三者から閲覧された事案が発生した[8]。そのため、金融庁は、金融機関に対して、クラウド上で管理する情報のアクセス権限が正しく設定されているかを確認するよう注意喚起した。 また、金融分野においてクラウドサービスの利用が拡がる中、クラウド活用のベストプラクティスや適切なセキュリティ実装などに関して、クラウドサービス事業者との意見交換や外部委託調査[9]を通じて、金融機関等に対して、クラウド利用のメリットや留意点などの適切な理解及びセキュリティ実装を促した。

（２）国際的な議論への貢献・対応

サイバー攻撃は、国境を跨ぐため、それぞれの国においてサイバーセキュリティ施策を実施するだけでなく、国際的に協調して対応することが重要となる。そのため、金融庁は、G7 財務大臣・中央銀行総裁会議（参考 2）や、金融安定理事会（FSB）などにおけるサイバーセキュリティに関する国際的な議論に参画してきた[10]。

（参考 2）G7 財務大臣・中央銀行総裁会議におけるサイバーセキュリティに関する議論

G7 財務大臣・中央銀行総裁会議は、G7 サイバーエキスパートグループ（Cyber Expert Group、CEG）を設置し、金融分野のサイバーセキュリティ確保に関する議論を重ねてきた。CEG では、これまで、金融分野における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策定してきた（下表参照）。2021 年 11 月には、G7 財務大臣・中央銀行総裁会議において、サイバーセキュリティに関する議論が行われた[11]。

（表）G7 財務大臣・中央銀行総裁会議が公表した金融分野のサイバーセキュリティの基礎的要素[12]

基礎的要素	公表年月	概要
金融セクターのサイバーセキュリティに関する基礎的要素	2016 年 10 月	金融機関がサイバーセキュリティを講ずるうえで重要と考えられる基礎的要素
金融セクターのサイバーセキュリティの効果的な評価に関する基礎的要素	2017 年 10 月	金融機関のサイバーセキュリティに関するプラクティスの適切な実施・評価を行うことに焦点を当てた基礎的要素

[8] 金融機関以外にも、同様のソリューションを利用していた複数の地方自治体や、一般事業者においても、同様の事案（アクセス権の設定不備）と推測される被害が発生した。

[9] 「クラウドコンピューティングとサイバーセキュリティ等に関する調査報告書」（金融庁ウェブサイト：https://www.fsa.go.jp/common/about/research/20190611-2.html）

[10] 金融安定理事会（FSB）においては、2020 年に「サイバー事象への初動と回復に関する効果的な実務」、2021 年には「サイバー事象報告－既存のアプローチとより広い範囲での収斂に向けた今後のステップ」が公表されるなど、金融セクターにおけるサイバーセキュリティ確保に向けた議論が継続されている。このほか、バーゼル銀行監督委員会、証券監督者国際機構、保険監督者国際機構等においてもサイバーセキュリティに関する議論が行われている。

[11] 英国政府ウェブサイト：https://www.gov.uk/government/news/chancellor-chairs-g7-finance-track-meeting-on-cyber-security。このほか、G7 財務大臣・中央銀行総裁会議は、2020 年 10 月に、デジタル・ペイメントに関する G7 財務大臣・中央銀行総裁声明及びランサムウェアに関する附属文書を公表している（https://www.fsa.go.jp/inter/etc/20201014/20201014.html）。

[12] 金融庁ウェブサイト：https://www.fsa.go.jp/inter/etc/20161011-2.html、https://www.fsa.go.jp/inter/etc/20171020.html、https://www.fsa.go.jp/inter/etc/20181015/20181015.html、https://www.fsa.go.jp/inter/etc/20201130/contents.html

TLPT[13]に関する基礎的要素	2018年10月	脅威動向の分析を踏まえた攻撃シナリオに基づく実践的な侵入テスト（TLPT）を実施するうえで重要な基礎的要素
金融セクターにおけるサードパーティのサイバーセキュリティリスクマネジメントに関する基礎的要素	2018年10月	金融機関の外部委託先等、サードパーティとの関係で生じるサイバーリスクに関する基礎的要素
サイバー演習計画に関する基礎的要素	2020年11月	金融セクターにおいてサイバー演習計画を立案するための効果的プラクティスの基礎的要素

（３）東京大会への対応

オリンピック・パラリンピック大会は世界的に注目を集めるイベントであり、過去にも、大会関係者等に対する多数のサイバー攻撃が観測されている。東京大会を契機にサイバー攻撃が増加するおそれに備え、金融分野を越えて、大会組織委員会、関係省庁、重要サービス事業者、関係団体等によるサイバー攻撃の脅威動向等に関する情報共有を強化した。

具体的には、内閣サイバーセキュリティセンター（NISC）が、2019年4月に設置した「サイバーセキュリティ対処調整センター」に、重要サービス事業者として金融機関、その所管省庁として金融庁も参加し、情報共有システム（JISP[14]）を利用して脅威情報等の共有を強化するとともに、演習においてインシデント対応の確認を行った。

さらに、金融分野における業態を跨いだ関係者相互の円滑な情報連携の促進を目的として、2019年6月に金融庁に「サイバーセキュリティ対策関係者連携会議」を設置し、大規模なインシデント発生時の連携手順を整備するとともに、情報共有体制を検証する訓練を金融セプター[15]等と実施した。

結果として、東京大会は、関係者の努力の成果もあり、金融機関やその顧客に被害を及ぼすインシデントが発生しないまま無事終了した。ただし、将来のサイバー攻撃の脅威への対応として、金融機関においては、東京大会における経験等を活かし、2025年日本国際博覧会（大阪・関西万博）の開催等も見据えて、その実効性の確保・向上に継続的に取り組む必要がある。

（４）金融機関のサイバーセキュリティ管理態勢の強化

①　大手行等

３メガバンクについては、米国大手行等の好事例やグローバルな脅威動向を踏まえ、(a)グループ・グローバルでの一元的な管理態勢や、(b)サイバーレジリエンスの強化[16]への取組状況などについて、検査・モニタリングの中で検証を行ってきた。2021事務年度は、日本銀行と共同で検証を実施した。

３メガバンク以外の大手行、新たな形態の銀行等については、アンケートを通じたモニタリングを実施し、そのうち、経営層の関与やリスク認識に改善の余地があると

[13] Threat-Led Penetration Testingの略。対象企業ごとに脅威分析を行い、個別にカスタマイズしたシナリオに基づき現実の脅威を再現した上で、より実戦的に行う「脅威ベースのペネトレーションテスト」を指す。

[14] Japan cyber-security Information Sharing Platformの略。

[15] セプターとは、重要インフラ事業者等の情報共有・分析機能等を担う組織であり、金融分野では、銀行等、証券、生命保険、損害保険の４つが該当。

[16] 例えば、サイバーインシデントからの復旧・回復のための対応能力の強化のため、TLPTの実効性の向上や、大規模サイバーインシデントを見据えた対応等の取組みが挙げられる。

考えられる一部の銀行について、意見交換を通じて課題認識を共有し、自主的な改善を促した。

② 地域金融機関

地域銀行、信用金庫、信用組合等の地域金融機関については、東京大会において想定されるリスクを見据えて、基礎的なサイバーセキュリティ管理態勢の整備[17]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た。そのため、(a)脆弱性診断の実施、(b)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、(c)監視・分析状況の整理とその結果に基づいた対策強化を要請し、地域金融機関の取組みを財務（支）局や業界団体と連携してフォローアップし、サイバーセキュリティ管理態勢の実効性向上を促してきた。あわせて、リスクが高いと考えられる金融機関に対して検査を実施し、判明した課題の改善を促した。

また、サイバーセキュリティ管理態勢の高度化を支援することを狙いとして、サイバーセキュリティの取組みに進展がみられる複数の地域金融機関に対してアンケート及び意見交換を実施し、業界団体を通じて傘下金融機関に好事例の還元を行った。

③ その他の業態

証券会社や外国為替証拠金取引業者については、基礎的なサイバーセキュリティ管理態勢の整備状況を検証したほか、不正アクセス事案の増加を踏まえて自主点検等を要請した[18]。また、不正アクセス対策を含むサイバーセキュリティ管理態勢に問題があると考えられる先に対しては検査・モニタリングで重点的に検証し、必要に応じて改善を促した。

大手保険会社については、サイバーセキュリティ管理態勢について、ヒアリングを通じたモニタリングを実施した。加えて、保険募集人・代理店については、保険商品を販売する代理店において顧客の個人情報を保有するため、業界団体とも連携して、代理店のサイバーセキュリティ強化に取り組んだ。

資金移動業者や前払式支払手段発行者については、顧客データの不適切な取扱いや、認証設計の脆弱性を突いた不正出金が発生したことを踏まえ、利用者情報管理態勢の整備状況や取引のリスクに見合った堅牢な認証方式を導入しているか等を検査・モニタリングで確認した。

暗号資産交換業者については、課題となっていたサイバーセキュリティ管理態勢の整備状況等について、検査・モニタリングにより、各社の状況を確認したほか、脆弱性診断の実施や、演習・訓練の実施を通じたサイバーインシデント発生時のコンティンジェンシープランの実効性の向上を促した。その結果、インシデント発生時における対応手順の整備に進捗が認められた。

監査法人については、公認会計士・監査審査会による検査等を通じて各法人のサイバーセキュリティ対策の状況を確認したほか、監査報告書の提出や企業情報の管理に影響を与え得るシステムに対して、サイバー攻撃や障害が発生した場合に、金融庁及

[17] 例えば、内部規程の整備やコンティンジェンシープランの策定など。
[18] 金融庁ウェブサイト：https://www.fsa.go.jp/news/r2/shouken/20200917.html

び日本公認会計士協会への報告を求めるルールを整備した。

（５）情報共有の枠組みの実効性向上

日々変化するサイバーセキュリティリスクについて、個々の金融機関が単独で調査・把握するには限界があるため、金融機関においては、必要に応じ、共助機関である金融ISAC[19]が支援している、技術的な課題への対応、ベストプラクティスの提供、最新のサイバー攻撃の動向や脆弱性情報の分析等についての知見を積極的に活用することが有効である。金融 ISAC を介した共助の取組みを促進するため、金融庁は、これまで、脆弱性情報の分析、インシデント対応の支援及びサイバーセキュリティ対策関係者連携会議での情報共有などの面で、金融 ISAC と緊密に連携してきた。

脅威情報の収集・分析については、金融機関において引き続きその能力を高める必要がある。このため、金融庁は、今後とも、金融機関同士の緊密な連携による情報共有の活発化を図るため、金融 ISAC の活動を積極的に支援するほか、地域に根付いた近隣の金融機関によるサイバーセキュリティに関するコミュニティ活動[20]についても後押しする。

また、公益財団法人金融情報システムセンター（FISC）が主催するセキュリティ実務担当者を対象としたサイバーセキュリティ研修や、経営層・マネジメント層を対象とした講演会において、金融庁から講師を派遣し、サイバーセキュリティの強化に向けた啓発や人材育成の支援に貢献した。加えて、FISC の安全対策基準が足許のリスク動向や脅威動向をタイムリーに反映するよう、金融機関で発生したインシデントの分析結果を定期的に FISC と共有するなど、共助の取組みを通じて金融業界のサイバーセキュリティ管理態勢の高度化を促した。

（６）金融分野の人材育成の強化

金融機関が、より効率的で付加価値の高いサービスを提供するためにデジタライゼーションを追求する中、サービスや業務の安全性を維持するために、サイバーセキュリティの確保は、経営上の重要な課題となっている。経営層は、サイバーセキュリティに関するリスクを正しく認識し、リーダーシップを発揮して施策を進める必要がある。

金融庁は、経営層、実務担当者層など、幅広い階層における人材育成を促進するため、財務（支）局、金融 ISAC、FISC、その他の業界団体等が主催するセミナーに講師を派遣し、サイバーセキュリティの強化に関する講演[21]を行った。また、振り込め詐欺やインターネットバンキング不正送金などの金融犯罪撲滅に向けた取組みとして、都道府県警察、財務（支）局、地域金融機関及び業界団体と連携して会議を実施し、最新の犯罪手口や防犯への取組事例等について知見の共有を図った。

さらに、金融機関のサイバーセキュリティ管理態勢を適切にモニタリングするうえで、

[19] 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。ISAC は Information Sharing and Analysis Center の略。

[20] 例えば、共同センターを利用している金融機関同士や近隣地域の金融機関同士による勉強会や情報共有を目的とした連絡会を定期的に開催している事例などが見られる。

[21] 例えば、サイバー攻撃の脅威動向、モニタリングを通じて得られたベストプラクティスの還元、サイバーセキュリティ演習を通じて得られた共通課題、経営層向け意識啓発等について取り扱った。

当局自身もサイバーセキュリティに関する知見を継続的に高めていく必要がある。このため、金融庁内の監督・モニタリング部門の職員を対象とした、金融機関のサイバーセキュリティに関するセミナーを実施したほか、金融機関のサイバーセキュリティ管理態勢を効率的にモニタリングするためのプロセスや視点をまとめたハンドブックを作成し、財務（支）局と共有した。引き続き、こうした取組みを通じ、人材育成に取り組む必要がある。

３．新たな「取組方針（Ver. 3.0）」

サイバー攻撃の脅威の増大をはじめとする、金融分野を取り巻く新たな状況に対応するため、今後、特に、以下の 5 つの項目に焦点を当てる。なお、これらの項目は、今後の情勢の変化等を踏まえ、適時に見直しを行う。

また、新たな取組方針（Ver. 3.0）を実施するに当たっては、日本銀行、関係省庁等（NISC、警察庁、公安調査庁等）、関係機関（金融 ISAC、FISC 等）、海外当局等と緊密に連携して対処していくことが重要である。

（１）モニタリング・演習の高度化

国家の関与が疑われるような組織化・洗練化されたサイバー攻撃[22]や複雑化・巧妙化するランサムウェア攻撃の増大[23]等に対応するため、金融機関の規模・特性やサイバーセキュリティリスクに応じて検査・モニタリングを実施し、サイバーセキュリティ管理態勢を検証するほか、公助の取組みである金融庁主催の演習を通じて個別金融機関及び金融業界全体のインシデント対応能力の向上に取り組む。また、検査・モニタリングで得られた金融機関に共通する課題や好事例については、業界団体を通じて傘下金融機関に還元することで、金融業界全体のサイバーセキュリティの高度化を促す。

なお、金融庁と日本銀行のモニタリングの連携強化の枠組み[24]の中で、サイバーセキュリティに関するモニタリングにおいても効率化・高度化を図ることができるものについては一層の連携強化に取り組む。

①　サイバーセキュリティ管理態勢の検証

（a）大手行等

グローバルに業務を展開している 3 メガバンクについては、サイバー攻撃の脅威動向の変化や海外大手金融機関における先進事例を参考にしたサイバーセキュリティの高度化に着目しつつ、通年検査においてサイバーセキュリティ管理態勢を検証する。また、その他の大手金融機関（新たな形態の銀行を含む）については、各社のビジネスモデル及びそのリスク特性を踏まえ、リスクベースでのモニタリングを通じて検証する。

---

22 「サイバーセキュリティ戦略」（令和 3 年 9 月 28 日閣議決定）、8 頁。

23 「サイバーセキュリティ戦略」（令和 3 年 9 月 28 日閣議決定）、9 頁。

24 「金融庁・日本銀行の更なる連携強化に向けた取り組み」（令和 3 年 3 月 22 日、金融庁ウェブサイト：https://www.fsa.go.jp/news/r2/20210322/20210322.html
日本銀行ウェブサイト：https://www.boj.or.jp/announcements/release_2021/rel210322c.htm/）。

（b）地域金融機関

地域金融機関については、組織化されたサイバー攻撃やランサムウェア攻撃の増大など、金融機関がリスク管理を高度化すべき範囲が拡大している中で、サイバーセキュリティに関する基礎的な管理態勢の実効性を向上させるために、継続的な取組みが必要である。

こうした状況を踏まえ、リスクが高いと考えられる金融機関に対する検査の実施を含め、サイバーセキュリティ管理態勢の実効性を検証する。

（c）その他の業態

証券会社や外国為替証拠金取引業者については、サイバーセキュリティに関する基礎的な取組みにおいて進捗が認められる一方、不正アクセス等による被害も複数発生していることを踏まえ、引き続き、検査・モニタリングを通じて、サイバーセキュリティ管理態勢を検証する。

保険会社についても同様に、インシデントの発生状況等を踏まえ、引き続き、検査・モニタリングを通じ、リスクベースでサイバーセキュリティ管理態勢を検証する。

資金移動業者や前払式支払手段発行者については、事業者及び必要に応じてその親会社等と対話を行ってグループ全体のビジネスモデルを的確に把握するとともに、ビジネスモデルに応じ、サイバーセキュリティ管理態勢の整備を促す。

暗号資産交換業者については、検査・モニタリングを通じて、顧客の暗号資産及び個人情報の保護などを重点的に検証し、サイバーセキュリティ管理態勢の整備を促す。

監査法人については、監査における IT の活用が一層普及・進展しており、大手監査法人のみならず準大手・中小監査法人においてもこうした IT の活用が進められている現状を踏まえ、引き続き、検査・モニタリングを通じてサイバーセキュリティの状況を確認する。

② サイバーセキュリティに関する自己評価の促進

金融機関は、それぞれの規模・特性に応じ、サイバーセキュリティ管理態勢を整備し、実効性を確保する必要があるが、これまで、他の金融機関対比での自組織の位置付けや改善すべき領域を特定するツールが必ずしも広く用いられてこなかった。

このため、地域金融機関向けのサイバーセキュリティに関する自己評価ツールを日本銀行及び FISC と共同で整備するとともに、地域金融機関の自己評価結果を収集・分析し、その結果を還元することで、地域金融機関のサイバーセキュリティ管理の自律的な高度化を促す。

金融庁においても、地域金融機関のサイバーセキュリティ管理態勢を把握するうえで、上記の分析結果をモニタリング上の参考とする。

また、地域金融機関以外の業態についても、各業態の特性等に応じた自己評価ツールの活用を検討する。

③　サイバーセキュリティ演習の高度化

2016 年以降、サイバーセキュリティ演習（Delta Wall）を実施し、参加金融機関に加え、業界団体を通じて非参加金融機関にも演習で認められた課題や好事例を還元することで、金融分野全体のインシデント対応能力の向上を促してきた[25]。金融機関自身による演習では、演習の品質や水準の確保において限界があるため、今後も、同演習は金融分野全体のサイバー攻撃へのインシデント対応能力を向上させる重要なツールである。サイバー攻撃の脅威動向、我が国の金融機関におけるインシデントの状況、他国の演習で参考となる事例等を踏まえ、個別金融機関及び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ため、引き続き、演習の高度化に努める。

（２）新たなリスクへの備え

2018 年の取組方針（Ver. 2.0）のアップデート以降も、金融分野におけるデジタル化は進展し、金融機関を取り巻く環境は様々な側面で変化している。

ビジネス面においては、フィンテック企業等の新たなプレイヤーの参入により金融サービスの担い手が多様化するとともに、各プレイヤーがそれぞれの強みを連携し、キャッシュレス決済サービスなど[26]利便性の高い新たなサービスを展開している。

また、システム面においては、クラウドサービスの利用が浸透し、金融機関の中には基幹系システムをクラウドサービスに移行する動きが見られるほか、外部委託の拡大、サプライチェーンの複雑化等も進んでいる。

このように、金融機関において、IT を活用した利用者利便の向上や経営の効率化が推進される一方、連携サービスや外部委託の拡大、サプライチェーンの複雑化・グローバル化に伴いリスク管理の難度は増しており[27]、昨今のインシデントや今後想定されるリスク[28]を踏まえ、適切な対応を講ずる必要がある。

①　キャッシュレス決済サービスにおける安全性の確保

キャッシュレス決済サービスは、一部事業者の利用者が数千万人に至るなど、国民生活のインフラとして重要性が高まる一方、認証設計の脆弱性に起因した不正出金が発生しており、セキュリティの確保が重要な課題となっている。

金融商品・サービスの企画・設計段階から、セキュリティ要件を組み込む「セキュリティバイデザイン」を実践し、サービス全体の流れの中で、連携先も含めて脆弱性を洗い出し[29]、リスクに見合った堅牢な認証方式を導入することが重要である。

---

[25] 演習規模を拡大（2016 年度は 77 先、2017 年度は 101 先、2018 年度は 105 先、2019 年度は 121 先、2020 年度は 114 先、2021 年度は 150 先が参加）するとともに、演習方法の高度化（例えば、銀行業態の演習シナリオをブラインド化、実際のテレワーク環境下での演習参加、技術的な課題への対応を確認）を図った。

[26] キャッシュレス決済サービスのほか、例えば、スマートフォンのアプリを利用することにより、キャッシュカードを用いることなくATM で取引することが可能となるスマホATMサービスなどもある。

[27] 例えば、外部委託先の拡大やグローバル化により、サプライチェーンが複雑に連鎖するようになってきており、サプライチェーンでインシデントが発生した場合に、金融サービスに及ぼす影響の範囲、程度の予測やその対策が難しくなっている。

[28] 例えば、新たなプレイヤーとの連携、既存業務の外部委託等の進展によるサードパーティリスクや、特定の事業者や技術への依存度が高まることによる集中リスク（例えばクラウドサービス）等。

[29] 例えば、キャッシュレス決済のアカウント作成から銀行口座との連携、チャージ、決済・送金までのサービスの始点から終点まで検証する等。

さらに、万が一、利用者等に被害が生じた場合も、速やかな被害回復を行う態勢を整備するなど、利用者保護の観点から適切な措置を講じることも肝要である。

金融庁においても、金融 ISAC 等との連携を強化し、金融機関に共通するリスク（システムの脆弱性等）の把握を行い、必要に応じ、被害の拡大を防ぐために金融機関に対して迅速に注意喚起し、対策を促すなど、プロアクティブな対応を行う。

② クラウドサービスの普及等への対応

金融機関でクラウドサービスの利用が拡大する中、クラウドサービスの特性や仕様の理解不足等に起因するアクセス権限の設定不備による顧客情報の漏えいなど、多くの金融機関に影響を及ぼす事案が発生した。金融機関は、クラウドサービスの利点[30]を活かすうえで、クラウドサービスの仕様、特性に伴うリスクも適切に評価し、システム稼働の安定性や顧客情報の適切な管理を確保する必要がある。過去のインシデントを踏まえると、金融機関がクラウドサービスを活用するうえで、サイバーセキュリティが確保されているかを確認するためには、例えば、インシデント発生時のコンティンジェンシープランの整備や演習の実施を通じて、システムの可用性やデータの機密性を確認することが有効である。

金融庁においても、金融機関のクラウドサービスの利用実態やそれに伴うサイバーセキュリティ管理態勢[31]の把握を進めるほか、クラウドサービス事業者との対話を行う（参考 3）。

加えて、クラウドサービスに限らず、外部委託の拡大やサプライチェーンの複雑化・グローバル化等によって、サイバーセキュリティを確保するうえで不可欠である IT 資産の脆弱性管理の難度が増していることを踏まえ、金融機関における脆弱性管理態勢のさらなる強化を促す。

（参考3）クラウドサービスへの対応例

- サイバーインシデント発生時における金融機関とクラウドサービス事業者とのコミュニケーションや、クラウドサービス事業者からの金融機関や金融機関の顧客に対する情報提供の強化[32]などに関して、クラウドサービス事業者と対話を行う。
- 外部からの侵入を前提とした境界型セキュリティの手法には限界[33]があるため、アクセスの信頼性を常に検証する「ゼロトラスト[34]」の考え方に基づいた施策が考えられるが、こうした考え方に基づいた取組みで他の金融機関の参考になる事例があれば業界全体に還元する。

③ サイバーハイジーンの徹底

高度化するサイバー攻撃に対する防御として、高機能なセキュリティ製品を導入す

[30] 例えば、調達手続の簡易化、システム管理の効率性等。
[31] 例えば、リスクベースの冗長化設計やセキュリティ実装等。
[32] 例えば、金融機関が顧客対応や業務の継続・復旧に取り組むうえで必要かつ十分な情報が発信されているか等。
[33] 「サイバーセキュリティ戦略」（令和 3 年 9 月 28 日閣議決定）、8 頁。
[34] ゼロトラストとは、ネットワーク境界による静的なアクセスコントロールではなく、アクセスごとに動的に検証を行うなどの方法を用いたセキュリティの考え方。「ゼロトラストの現状調査と事例分析に関する調査報告書」も参照（金融庁ウェブサイト：https://www.fsa.go.jp/common/about/research/20210630.html）。

るなど技術的施策が有効であることは論を俟たない。その一方、インシデントの原因には、ソフトウェアの脆弱性へのセキュリティパッチの適用漏れなど、基本的な行動が徹底されていない事例も見られる。外部委託の拡大などにより、IT 資産管理の範囲が拡大し複雑化する中、安全性の高い IT 環境を維持するには、境界型セキュリティや特定のセキュリティ製品だけに依存することなく、風邪予防における手洗い、うがいなどの公衆衛生活動と同様に、IT 環境においても、例えば、IT 資産の適切な管理、速やかなセキュリティパッチ適用などの基本的な行動を組織全体に浸透させる取組み（いわゆるサイバーハイジーン）が重要であり、こうした取組みを金融機関に促していく。

④　サイバーレジリエンスの強化

サイバー攻撃が高度化・複雑化し、また、金融サービスの提供において、外部委託が拡大するとともに、サプライチェーンが複雑化・グローバル化していることを踏まえれば、事前にサイバーセキュリティリスクを全て洗い出したうえで施策を講じ、インシデントを未然に防止することは一層困難な状況となっている。サイバーセキュリティ管理の範囲は、インシデントの未然防止から、インシデント発生時の検知、特定、対応、業務の早期復旧や顧客影響の軽減といったレジリエンス（いわゆる復元力）の強化へと拡がっている。

そのため、金融機関においては、未然防止の施策に加え、インシデントによって業務が中断した場合も、業務や顧客への影響を許容水準内に収めるよう、訓練・テスト等を通じて、業務やサービスの強靭性・頑健性・冗長性を高めることが一層求められている。このため、金融庁では、インシデント発生時におけるサイバーレジリエンスの強化に向けた取組みを金融機関に促していく。

（３）サイバーセキュリティ確保に向けた組織全体での取組み

①　経営層の関与

サイバーインシデントによる業務の中断は、顧客に大きな影響を与え、ひいては金融機関の信頼に大きな影響を与えるものであり、サイバーセキュリティは IT・システム部門のみの問題ではなく、業務、企画、広報、コンプライアンス、リスク管理、監査などの他の部門、また、経営層から現場担当者まで、金融機関のあらゆる部門・階層での対応が求められる。そのため、組織全体でのサイバーセキュリティ管理の実効性を高めるためには、経営層の積極的な関与、リーダーシップの発揮が必要である。

金融庁では、引き続き、サイバーセキュリティの経営上の位置付けと組織としての対応を把握するとともに、サイバーセキュリティ管理の実効性向上のため経営層のリーダーシップの発揮を促していく。

②　セキュリティ人材の育成

サイバーセキュリティの確保のためには、IT・システム部門のみならず、経営層、業務部門、企画部門、広報部門、コンプライアンス部門、リスク管理部門、監査部門など、多様な部署の関与が必要であり、かつ、各部署で求められるサイバーセキュリ

ティの知見は異なる。定期的な人事ローテーションが存在する場合はそれを前提としたうえで、各部署に必要なセキュリティ人材を育成・配置する必要がある。例えば、自組織で知見が不足しているセキュリティ分野を洗い出し、人材育成計画を作成・実行するほか、内部の研修だけではなく、金融 ISAC 等のサイバーセキュリティの知見を高める外部の活動にも参加しやすい職場環境を整備するなど、計画的に組織全体でのセキュリティ人材の育成を図ることが期待される。特に、経営層の方針を踏まえ、具体的なサイバーセキュリティの立案と指揮を担う戦略マネジメント層や、研修や人材育成を担うセキュリティトレーナー、システムの開発・運用担当者については、育成に時間を要するため、計画的に取り組むことが重要である。

また、金融機関のサイバーセキュリティ管理態勢を適切にモニタリングしていくためには、金融庁自身もセキュリティ人材の確保・育成を強化することが不可欠である。そのため、金融庁としては、外部の専門人材の採用に加え、各役職に求めるスキルレベルを整理したうえで、計画的に、政府機関（NISC やデジタル庁等）や民間企業（セキュリティベンダーや IT 企業等）との人材交流や、IT・セキュリティ系の大学院への派遣など、IT・セキュリティ人材の育成を強化しており、引き続き、こうした取組みを推進していく。

（４）関係機関との連携強化

①　NISC 等との連携

サイバー攻撃への対策においては、最新のサイバー攻撃の脅威動向や脆弱性情報を幅広く共有し、速やかに適切な防護策を講じることが重要である。金融庁は、引き続き、サイバーセキュリティの司令塔である NISC や金融 ISAC 等と緊密に連携し、脅威情報をタイムリーに収集・分析の上、積極的に注意喚起することで、金融機関に対してサイバー攻撃やシステムの脆弱性への迅速な対応を促す。また、サイバー攻撃の主体[35]や目的[36]が多様化し、脅威動向の把握が難しくなる中、情報収集・分析能力（インテリジェンス）をより強化するため、公安調査庁との情報連携も推進していく。

②　捜査当局等との連携

新技術を活用した新たな金融サービスが生み出される一方、金融犯罪においては、従来のインターネットバンキングに係る不正送金に加えて、暗号資産取引に関する匿名化技術を悪用し、ランサムウェア攻撃で身代金を暗号資産で要求するなど、新たなサービスや技術を悪用した犯罪が増加している。また、高度な技術を持たない悪意のある者へ、マルウェアや不正出金の手段などを組織的に提供するエコシステムが確立され、不正な収益獲得が可能となったと指摘されている[37]。

犯罪行為の誘因を下げ、サイバー攻撃を抑止する捜査当局の取組みを後押しするため、金融庁は、これまでも、警察庁等と緊密に連携し、例えば、インターネットバンキング・キャッシュレス決済による不正出金に関する注意喚起や、金融犯罪で利用さ

[35] 例えば、国家の関与が疑われるものや、国際的なハッカー集団等。
[36] 例えば、機密情報の窃取や、金銭の窃取等。
[37] 「サイバーセキュリティ戦略」（令和 3 年 9 月 28 日閣議決定）、9 頁。

れた暗号資産アカウントの凍結措置[38]に向けた業界団体との調整など、犯罪手口に即して、様々な対応を行ってきた。

引き続き、金融犯罪における手口の変化を注視し、注意喚起や啓発による防犯活動を業界団体等と連携して行う。あわせて、さらなる犯罪の抑止などに向けて、警察をはじめとする関係機関と緊密に連携し、金融犯罪の未然防止と被害拡大防止に取り組む。

③　国際連携の深化

国家の関与が疑われるような組織化・洗練化されたサイバー攻撃が増大しており、海外においては、国際的なハッカー集団による石油パイプラインへのサイバー攻撃といった市民生活に影響が及ぶ事態も発生している。そのため、改めて、サイバー攻撃に対して、各国当局との連携を強化する重要性が認識されている。

また、国際的に活動する大手クラウドサービス事業者の出現や、IT への依存の増大を踏まえ、金融分野のサードパーティリスクやオペレーショナル・レジリエンスに関する国際的な議論が高まっている[39]。また、FATF[40]においても、暗号資産に関する FATF 基準の実施を早急に行い、暗号資産がランサムウェアの身代金支払いのために利用されるリスクを低減すべきといった議論が行われている[41]。

金融庁としては、国境を跨ぐ脅威やインシデントに適切に対応するため、引き続き、こうした国際的な議論に参画し、海外当局と連携する。

（５）経済安全保障上の対応

安全保障の裾野が経済・技術分野に急速に拡大する中、経済安全保障への対応がより重要性を増しており、政府では、その重要分野の一つとして、基幹インフラの安全性・信頼性の確保について検討を進めている。

金融業については、国民生活や経済活動の基盤となる基幹インフラの一つであるとともに、大量の個人・企業の情報を保有する産業である。このため、経済安全保障の観点からは、金融業の保有するデータの適切な管理やサイバーセキュリティの強化に加えて、その機器・システムの利用や業務委託等を通じたリスクへの対処などに取り組む必要がある。

金融庁としては、その具体的な取組みについて、関係機関とも連携しつつ、引き続き適切に対応を行う。

---

[38] 例えば、銀行から暗号資産取引所の暗号資産アカウントに対して、サイバー犯罪などの犯罪収益が不正送金された場合、当該暗号資産アカウントを凍結する等。

[39] 例えば、金融安定理事会（FSB）による「サイバー事象への初動・回復対応の効果的な実務」（2020 年 10 月）や、バーゼル銀行監督委員会による「オペレーショナル・レジリエンスのための諸原則」及び「健全なオペレーショナル・リスク管理のための諸原則の改訂」（2021 年 3 月末）の公表など（金融庁ウェブサイト：https://www.fsa.go.jp/inter/fsf/20201022/20201022_2.pdf、https://www.fsa.go.jp/inter/bis/20210402/20210402.html）。

[40] FATF（金融活動作業部会）。マネーローンダリング・テロ資金供与対策の国際基準（FATF 勧告）を策定し、その履行状況について相互審査を行う多国間の枠組み。

[41] 「暗号資産・暗号資産交換業者に関する FATF 基準についての２回目の 12 ヵ月レビュー報告書」（2021 年 7 月）の公表、40 頁（金融庁ウェブサイト：https://www.fsa.go.jp/inter/etc/20210706/20210706.html）。