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

平成３０年１０月

金融庁

[目次]

１.「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」のアップデートについて

(1) アップデートの背景

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、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。

こうした中、デジタライゼーションの動きが加速的に進展しており、新しいプレイヤーの金融分野への進出や情報の利活用の進展により、金融業は抜本的な変革が起こりつつある。このような動きは、利用者利便を飛躍的に向上させ、我が国経済の生産性を高める可能性がある一方、金融に関わるあらゆるビジネス・業務がデジタル化され、あらゆるシステムがネットワークに繋がることで、サイバーセキュリティに係るリスクがより一層高まっていくおそれがある。このため、デジタライゼーションが進展する社会において、金融サービス利用者の安全性や我が国の金融システムの安定性を確保しつつ、利用者の利便性や金融業における生産性を向上させていくためには、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。

近年、国内外においてサイバー攻撃の高度化・複雑化によりサイバーセキュリティに係るリスクが一層高まっている状況にある。海外では、2016 年には海外の中央銀行における国際的な送金システム（SWIFT）の不正操作による不正送金事案[1]、2017 年には世界各国においてランサムウェア[2]に感染する大規模な事案[3]が発生するなど、世界的にサイバー攻撃の脅威が深刻化してきている。このような状況を受けて、国際的にもサイバーセキュリティの確保が重要なテーマとなっており、Ｇ７財務大臣・中央銀行総裁会議などにおいて、金融分野のサイバーセキュリティに関する国際的な議論が行われている。こうした国際的な議論に対して、我が国としても積極的に貢献・対応していくことが必要である。

また、国内金融分野におけるサイバー攻撃の動向については、大手金融機関のみならず中小金融機関や仮想通貨交換業者にまでその裾野が拡大しており、その手法も、分散型サービス妨害攻撃（DDoS 攻撃）、標的型攻撃、サーバ等の脆弱性等を突いた不正アクセスなど多様化している。こうした中、我が国では、「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）の開催を控え、金融分野を含む我が国の重要インフラ事業者等がサイバー攻撃のターゲットとなる可能性が指摘[4]されており、大規模インシデントの発生に備え、官民一体となった危機管理態勢の構築が求められている。また、本年７月には、政府全体のサイバーセキュリティに関する基本方針

---

[1] バングラディシュ中央銀行において国際的な送金システム(SWIFT)端末がマルウェアの感染により不正操作され多額の資金が不正送金（約 8,100 万ドル）された事案（同様の事案が台湾、ネパール等でも発生)。

[2] 「Ransom（身代金)」と「Software（ソフトウェア)」を組み合わせた造語。感染すると、パソコンのデータを暗号化し使用不能等にしたのち、元に戻すことと引き換えに身代金を要求する不正プログラムの総称。

[3] 2017 年５月、世界 150 ヵ国以上において、WindowsOS のパソコンやサーバが「WannaCrypt」と呼ばれるランサムウェアに感染する事案が発生。また、同年６月には、欧米をはじめとする世界各国において、ランサムウェア「Petya」に感染する事案が発生。

[4] 「サイバーセキュリティ戦略」によると、ロンドン大会では、膨大な数のサイバー攻撃があったとされるほか、リオデジャネイロ大会や平昌大会においても、相当数のサイバー攻撃が行われ被害を受けたとの報道がある。

である「サイバーセキュリティ戦略」が改訂され[5]、新たな戦略の下、2020 年東京大会に向けて、政府一丸となって、金融分野を含めた重要インフラ事業者等のサイバーセキュリティ対策に取り組むこととされている。

このように、金融分野のサイバーセキュリティを巡る状況が大きく変化する中、実効性のあるサイバーセキュリティ管理態勢の構築に向けて、今般、金融庁として、新たな課題への対応方針や現「取組方針」の進捗・評価を踏まえた今後の取組み方針を明確化し、金融機関、金融サービス利用者及び関係機関と問題意識を共有するため、「取組方針」のアップデートを実施することとした。

近年の金融分野における主なサイバー攻撃事案等

動機	対象	主な攻撃手法	事案の概要
政治的な信条	金融機関	✓ DDoS攻撃によるWebサイト等のサービスの停止	◆ 国内の金融機関や金融庁等、複数の組織のWebサイトに対してDDoS攻撃による被害が発生。また、標的となった組織と同一のWebホスティング会社を利用する金融機関にも影響
情報の窃取		✓ メール等による標的型攻撃 ✓ サーバ等に対する不正アクセス	◆ 国内金融機関のメールサーバに対して不正アクセスが発生し、顧客の氏名、住所、口座番号等の顧客情報が漏えい（2016年9月） ◆ 国内金融機関のWebサイトに対して不正アクセスが発生し、顧客のIDや氏名、住所、生年月日等の顧客情報が漏えい（2017年7月） ◆ 金融機関のWebサイトがサイバー攻撃により改ざんされ、当該Webサイトを閲覧した利用者が悪意のある外部サイトに誘導されるとともにマルウェアをダウンロードさせられる事案が発生
金銭目的		✓ 金融機関自身への攻撃による不正送金	◆ バングラデシュ中央銀行で国際的な送金システム(SWIFT)に利用されているPCが遠隔操作され、不正に多額の資金が窃取（2016年2月）（その後同様の事案が台湾、ネパール等でも発生） ◆ 仮想通貨交換業者において、外部からの不正アクセスにより、仮想通貨の大規模な不正流出が発生（2018年1月、9月）
		✓ 金銭を目的としたDDoS攻撃	◆ 複数の金融機関が、期日までに身代金としてビットコインを支払わなければDDoS攻撃を仕掛ける旨の脅迫メールを受信するとともに、短時間のDDoS攻撃による被害も発生（2017年6月、9月）
	顧客	✓ 顧客PCのマルウェア感染	◆ インターネットバンキング利用者のIDやパスワードを窃取するマルウェアが発生。最近では仮想通貨取引所の利用者もターゲットとするマルウェアも確認

【出典】各種公表資料等より作成

(2) 現「取組方針」に関する進捗・評価

金融庁では、2015 年に「取組方針」を公表後、同方針に沿って、官民が一体となって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みを推進してきた。以下では、現「取組方針」で示された各方針の進捗・評価について整理[6]する。

① サイバーセキュリティに係る金融機関との建設的な対話と一斉把握

2015 年の「取組方針」公表以降、地域金融機関を中心に、証券会社、保険会社等の幅広い業態にわたる 200 先を超える金融機関に対しサイバーセキュリティ対策に係る実態把握を実施[7]してきた。

サイバーセキュリティ対策が進んでいる金融機関は、サイバーセキュリティを重大

[5] 「サイバーセキュリティ戦略」においては、2020 年東京大会に向けた態勢の整備（「サイバーセキュリティ対処調整センター」（政府オリンピック・パラリンピック CSIRT）の構築）や多様な主体の情報共有・連携の推進などが盛り込まれている。

[6] 現「取組方針」においては、①サイバーセキュリティに係る金融機関との建設的な対話と一斉把握、②金融機関同士の情報共有の枠組みの実効性向上、③業界横断的演習の継続的な実施、④金融分野のサイバーセキュリティ強化に向けた人材育成、⑤金融庁としての態勢構築の５つの方針を示している。このうち、⑤金融庁としての態勢構築については、金融庁内部において情報・知見を一元的に集約し、組織横断的に企画調整を行う「サイバーセキュリティ対策企画調整室」を 2015 年 7 月に設置済であるので、ここでは①～④の進捗・評価について整理する。

[7] 平成 28 事務年度までに、地方銀行、第二地方銀行については、全行の実態把握を実施済。

なコーポレートリスクの一つとして捉え、経営陣の強いリーダーシップにより、サイバーセキュリティに着眼したリスク評価の実施、対応態勢の構築（組織態勢・技術的対策）、コンティンジェンシープランの整備・継続的な演習等への参加、サイバーセキュリティに関する監査の実施といったフレームワークをシステム部門のみならず、関係部門（経営企画、法務、広報、各業務部等）も含めて構築している。加えて、新たな脅威の発生など、外部環境の変化に応じて定期的にリスク評価を見直す等、PDCA サイクルを循環させている。

一方、サイバーセキュリティを単にシステム部門などの担当部署が対応すべきリスクとして捉えている金融機関では、依然として、サイバーセキュリティ対策の基礎となるサイバーセキュリティに着眼したリスク評価が不十分であり、自組織のどこにサイバーセキュリティに係るリスクがあるか特定できていない状況にある。また、技術的な対応については担当部署や外部委託先に任せきりな傾向にあり、インシデント発生時のコンティンジェンシープランも未整備の状況にある。

こうした傾向は、特に中小金融機関に顕著であり、基礎的なサイバーセキュリティ管理態勢の整備により、業界全体の底上げを図っていくことが大きな課題となっている。このため、信用金庫・信用組合業態については、平成 29 事務年度に、金融庁も後押しし、信用金庫・信用組合のそれぞれの協同組織中央機関・業界団体が連携のうえ、リスク評価の手引書やコンティンジェンシープランのひな型を策定し、傘下金融機関に還元した。今後は、信用金庫・信用組合のそれぞれの協同組織中央機関・業界団体による適切な支援の下、各信用金庫・信用組合において、自らの特性を踏まえ、当該ひな型も活用し、態勢整備を加速させていく必要がある。

一方、地方銀行、第二地方銀行については、基礎的なサイバーセキュリティ管理態勢の構築が一定程度進んでおり、今後、サイバー攻撃に対するサイバーセキュリティ対策の実効性を確保していくことが課題となる。

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[8]。こうした中、３メガバンクでは、サイバーセキュリティ対応能力をもう一段引上げるため、より高度な評価手法として「脅威ベースのペネトレーションテスト」[9]の活用を進める等、一層の高度化に向けて相応の進展がみられたところである。

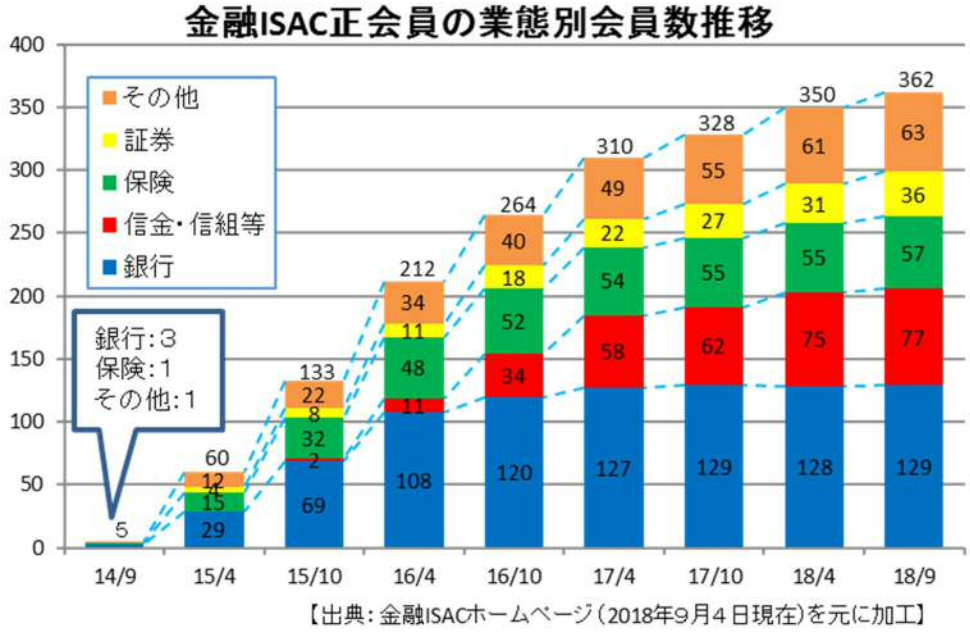
また、平成 29 事務年度には、金融庁において海外大手金融機関の取組みについて現地でのヒアリングを含め調査・分析を行い、３メガバンクとの間で海外の先進的な取組みを踏まえた対策の必要性について認識の共有を図った。国際的なサイバー攻撃の脅威の高まりに応じて、海外大手金融機関は対策を一層高度化させており、今後もこうした取組みを参考にすることにより、国内大手金融機関の対策のもう一段の高度化を図っていく必要がある。

[8] 平成 29 事務年度より、大手保険会社との間でも、サイバーセキュリティ管理態勢、人材育成・教育や保険代理店の対策状況等について定期的に対話を実施している。

[9] 金融機関に対する脅威動向の分析を踏まえて作成した攻撃シナリオに基づく実践的な侵入テスト。

② 金融機関同士の情報共有の枠組みの実効性向上

金融機関の取組みを向上させ、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」、金融庁等の当局の支援である「公助」だけではなく、金融機関同士で情報共有・分析を行う「共助」が非常に有効となる。「共助」態勢の確立に向けて、一般社団法人 金融 ISAC[10]（以下、「金融 ISAC」という）等の情報共有機関を活用した情報共有や取組みの高度化（脆弱性情報の迅速な把握・防御技術の導入等）の意義について、金融機関に対して周知してきた結果、金融 ISAC への加盟が着実に進捗してきている。



金融 ISAC では、情報共有に留まらずワーキンググループ活動を通じたリソースの共有、地方でのカンファレンス開催など、様々な活動に取り組んできており、その果たす役割は大きくなってきている。一方で、一部の業態[11]では加盟が停滞しており、引き続き、「共助」の有効性について浸透を図り、金融業界の共助態勢の確立に努めていくことが課題である。また、一部の中小金融機関からは、金融 ISAC への加盟は地理的・人的・金銭的に難しいとの意見も聞かれ、こうした現状を踏まえ、例えば、地域内の連携など[12]の取組みについても検討していく必要がある。

③ 業界横断的演習の継続的な実施

金融庁では、特に中小金融機関のインシデント対応能力の向上を図るため、2016 年より、毎年「金融業界横断的なサイバーセキュリティ演習」（Delta Wall[13]）を実施してきた。本演習には、2016 年に 77 金融機関、2017 年に 101 金融機関が参加し、演習に向けた準備、演習への参加及び演習結果のフィードバックを通じて、インシデント

[10] 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）。

[11] 信用金庫・信用組合、中小証券会社において未加盟の先が多い。

[12] 例えば、「新潟県金融機関サイバーセキュリティ対策情報連絡会（2018 年 2 月 22 日設立）」や「サイバーセキュリティ Day in 広島－サイバー空間をみんなで守ろう－（2018 年 4 月 10 日開催）」等の共助の取組みがみられる。

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

対応能力の向上を図った[14]。また、演習結果については、演習に参加していない金融機関の取組みに活用してもらうために、共通する傾向や課題等についてとりまとめ、業界全体に還元した。

一部の金融機関では、迅速かつ的確にインシデントに対応するための工夫を行う良好事例[15]が認められたものの、総じてシナリオで提示された攻撃への対応に目が行きがちであり、シナリオで掲示された攻撃の裏で別の攻撃を受ける可能性を考慮した監視強化の実施等、インシデント発生時におけるより広い視野での対応に課題が認められた。サイバー攻撃へ迅速・的確に対応するためには、予め想定される様々な行動を洗い出し、対応手順等の規程類に具体化し、外部演習等への参加を通じて継続的に内容をブラッシュアップしていくことが重要である。

サイバーセキュリティ演習については、これまでの演習結果を踏まえ、より実効性の高い演習方法・内容等を検討し、官民が一体となってインシデント対応の向上に努めていくことが重要である。

④　金融分野のサイバーセキュリティ強化に向けた人材育成

金融庁では、2016 年度に全国の財務（支）局において、サイバーセキュリティワークショップ[16]を開催したほか、金融機関向けの講演等の機会を捉えて、継続的に経営層へのサイバーセキュリティ対策の重要性の啓発などに取り組んできたところである。また、公益財団法人金融情報システムセンター（以下、「FISC」という）においても、2017 年度より中小金融機関を中心としたワークショップを各地域で開催しており、金融庁とも連携して、サイバーセキュリティに係る各種対策・整備の考え方に対する理解の向上やスキルアップに取り組んでいる。

こうした取組みの結果、一定程度金融機関におけるサイバーセキュリティへの意識や理解の高まりがみられるものの、特に中小金融機関においては、依然として経営層の意識やサイバーセキュリティ対策の理解が十分とは言えない状況にある。また、金融分野のみならず日本全体としてサイバーセキュリティ人材の不足が指摘されている。

金融機関のサイバーセキュリティ対策を強化するためには、「経営層」の意識改革が不可欠である。あわせて、サイバーセキュリティ人材の確保、サイバーセキュリティへの理解の向上やスキルアップも重要となる。このため、金融 ISAC や FISC 等とも連携し、業界全体で人材育成等に取り組む必要がある。

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について

(1) 基本的な考え方

上述のとおり、これまで金融分野のサイバーセキュリティ対策の強化に向けて、現「取組方針」に基づく取組みを推進してきた。しかしながら、デジタライゼーションの加速的な進展、2020 年東京大会等の開催、国際的な議論の進展など、金融分野のサイバーセキュリティを取り巻く状況は、2015 年の「取組方針」策定時から大きく変化している。

[14] 2018 年 10 月末、約 100 の金融機関が参加し３回目となる演習を実施する予定。
[15] 例えば、IT ベンダーに対して、システムを共同利用している他の金融機関で類似被害の発生がないかを確認した事例や情報漏えいにより顧客に二次被害が発生しないよう口座の不正な動きを監視した事例がみられた。
[16] 2016 年度に 10 財務（支）局で通算 23 回開催し、合計約 500 の金融機関が参加。

また、現「取組方針」に基づく取組みについても、進捗・評価を踏まえて改善していくことが重要である。

こうした基本認識の下、金融分野のサイバーセキュリティを取り巻く環境変化に伴う新たな課題に対応するとともに、これまでの取組みの進捗・評価を踏まえた金融分野のサイバーセキュリティ対策の更なる強化を図るため、今後、官民が緊密に連携を図り、以下の項目に取り組む。こうした取組みを通じて把握したサイバーセキュリティに関する課題等については、個別金融機関や業態全体に対する積極的な問題提起を通じて、関係者間での認識の共有を図り、具体的な改善を図っていく。また、金融分野や業態に共通する課題等については、定期的に取りまとめ、積極的な情報発信を通じて、金融分野全体のサイバーセキュリティ対策の強化を促していく。

なお、これらの項目については、テクノロジーの進展等により金融業のあり方が大きく変わりつつあることを踏まえ、適時に見直しを行っていく。

(2) 新たな課題への対応

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

金融分野では、既にインターネットを中核とした業務やサービスが相当程度普及している中で、今後、サイバー空間における技術革新やイノベーションが加速的に進展することが想定される。こうした動きは、既存の金融機関におけるフィンテック企業等との連携による新たな金融サービスの提供や非金融プレイヤーの金融業への参入などによる新しいビジネスモデルの創出、金融機関の IoT・AI の利活用やクラウドサービスの普及による業務面の IT 化・効率化、仮想通貨交換業や電子決済等代行業など新たな金融事業者の登場など、金融業におけるビジネス・業務のあり方に抜本的な変化をもたらしている。一方、こうしたデジタライゼーションの進展により、例えば、以下のようなリスクが顕在化することが考えられる。

デジタライゼーションの進展により想定されるリスク例(仮説)

- 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(外部委託)リスク
- ITシステムの停止がビジネスそのものの業務継続に直接影響を与えるおそれ(ITリスク管理から危機管理の視点)
- あらゆるシステムが繋がることにより、単一障害点を発端に連鎖的に影響が広範囲におよぶリスク(最悪の場合決済機能不全に陥ることも)
- 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)
- AI等のテクノロジーを悪用し、新たな攻撃手法を生み出すことで、既存の対策では検知・対応出来なくなるおそれ

このため、デジタライゼーションの進展が金融業に与える影響を把握し、具体的にどのようなサイバーセキュリティに係るリスクが発生しうるか、そのリスクが顕在化した場合に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・分析に取り組む。また、把握・分析した結果を踏まえ、新たな実効性あるサイバーセキュリティに係るリスクへの対応策を金融機関に促していく。また、こうした変化に対応した当局のモニタリングのあり方についても検討していく[17]。

② 国際的な議論への貢献・対応

サイバー攻撃は、容易に国境を跨ぎ、その影響は金融システム全体に波及するおそれがあり、国際的にもサイバーセキュリティの確保は重要課題となっている。

こうした中、Ｇ７財務大臣・中央銀行総裁会議では、2015 年に「Ｇ７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[18]。これまで、国際的なサイバーセキュリティ対策の基本原則を示した「金融セクターのサイバーセキュリティに関するＧ７の基礎的要素」（2016 年）及びその評価に関する「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Ｇ７の基礎的要素」（2017 年）を策定・公表してきた。加えて、本年 10 月には、より具体的な個別分野の重要テーマに関する基本原則として「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」、「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Ｇ７の基礎的要素」を策定・公表した。また、2019 年には、Ｇ７諸国の当局が連携して実施する、大規模なサイバーインシデントに対するクロスボーダーの合同演習が予定されている。

容易に国境を跨ぐサイバー攻撃に対しては、それぞれの国においてサイバーセキュリティ対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。このため、Ｇ７財務大臣・中央銀行総裁会議をはじめとするサイバーセキュリティに関する国際協調の議論に対して、各国当局と連携しつつ貢献・対応していく。

③ 2020 年東京オリンピック・パラリンピック競技大会等[19]への対応

「サイバーセキュリティ戦略」で示された政府全体の方針[20]を踏まえ、2020 年東京大会を見据え、金融分野の連携態勢を整備するため、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[21]）、金融 ISAC や FISC 等の

---

[17] 仮想通貨交換業者については、2017 年８月に金融庁内に「仮想通貨モニタリングチーム」を設置し、仮想通貨交換業者の登録審査・モニタリングや、仮想通貨（暗号資産）に係る情報の収集・分析等を行っている。また、本年８月、これまでの検査・モニタリングで把握した問題点等について「仮想通貨交換業者等の検査・モニタリング　中間とりまとめ」として公表した。

[18] Ｇ７のほか、FSB(Financial Stability Board)、SSG(Senior Supervisors Group)、IOSCO(International Organization of Securities Commissions)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。

[19] 我が国おいては、2020 年東京大会のほか、2019 年にはラグビーワールドカップ、G20 大阪サミットといった国際的なイベントが予定されている。

[20] 「サイバーセキュリティ戦略」では、「関係府省庁、大会組織委員会、東京都、競技会場のある地方公共団体、重要サービス事業者等、大会関係組織間でサイバーセキュリティに係る脅威情報を共有するとともに、事案発生時に大会関係組織が皆で力を合わせて対応するために国が調整役となるための組織である『サイバーセキュリティ対処調整センター（政府オリンピック・パラリンピック CSIRT)』の構築を推進し緊密に連絡調整を図るための態勢を整備する。」とされている。

[21] 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

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とともに、整備した態勢については大規模インシデント発生時の金融分野における危機管理態勢の仕組みとして活用していく。

また、サイバー攻撃に的確に対応していくためには、金融セクターにとってリスクとなりうる脅威情報をタイムリーに収集・分析し、プロアクティブに対応していくことが重要である。近年、サイバー攻撃が高度化・複雑化し、その被害が個別金融機関にとどまらず他の金融機関や金融システム全体に波及するおそれがある中、こうした情報共有の必要性は益々高まっている。特に、2020 年東京大会に向けて、サイバー攻撃の増加、各分野を跨るような攻撃や大規模インシデントの発生などが懸念されており、金融機関のインシデント情報のみならず、電力・通信等の他の重要セクター、サードパーティ（外部委託）や海外の動向等についても幅広く情報収集に取り組む必要がある。

これまで金融庁では、業界団体（CEPTOAR）を通じた情報提供[22]に関して、NISC から発信された情報に限らず、金融機関で発生したインシデントのうち、他の金融機関でも同様の被害が生じうる可能性がある場合には、積極的に注意喚起して所要の対応を求めてきた。こうした対応に加えて、2020 年東京大会に備え、金融庁として NISC 等とも連携しつつ、これまで以上に情報収集・分析能力（インテリジェンス）の強化を図り、必要に応じて金融機関に情報発信しプロアクティブな対応を促していく[23]。

(3) これまでの進捗・評価を踏まえた施策の推進

上述の新たな課題への対応に加え、現「取組方針」に基づくこれまでの取組みの進捗・評価を整理し、PDCA サイクルを回すことにより、金融分野のサイバーセキュリティ対策の更なる強化を図ることが重要である。

金融機関の業態・規模、システム構成やビジネスモデル等の特性に応じてサイバーセキュリティに係るリスクが異なるため、必要となるサイバーセキュリティ対策の深度に違いはあるものの、すべての金融機関において実効性のある態勢整備が求められる。そこで、これまでの取組みの進捗・評価に基づく残された課題等を踏まえ、金融分野のサイバーセキュリティ対策を加速させるため、金融機関のサイバーセキュリティ対策を、「平時のサイバー対策」（高度化・複雑化するサイバー攻撃への備え）、「インシデント対応」（インシデント発生時の適切な対応）に区分し、業態・規模・特性等に応じた対応を進めていく。

監査法人については、大手監査法人を中心に、IT を活用した監査の普及・深化を進めており、実効性や効率性を確保した深度ある監査の実現に資するものとして期待される。一方で、海外において監査法人を標的としたサイバー攻撃による被害の事例も発生している。サイバーセキュリティ問題は監査法人にとって経営上のリスクであり、サイバーセキュリティの強化を確実に行っていく必要がある。監査法人に対しては、サイバーセ

が該当（事務局は各協会）。

[22] 「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、平成 30 年 7 月 25 日サイバーセキュリティ戦略本部改定）に基づき実施。

[23] 「サイバーセキュリティ戦略」においては、「まずは国から率先して自ら保有している情報を適切に提供していく」とされている。

キュリティ対策の状況を確認し、下記の金融機関における取組みを参考にしながら態勢の充実を促していく。

また、金融分野全体のサイバーセキュリティの確保に向けた横断的施策として、「情報共有の枠組みの実効性向上」、「金融分野の人材育成の強化」に取り組む。

なお、金融機関のサイバーセキュリティ管理態勢に関する金融庁のモニタリング方法については、金融機関のサイバーセキュリティ管理態勢の整備状況やテクノロジーの進展等による金融サービスのあり方の変化を踏まえ、サイバーリスクに応じた効果的な手段を選択するなど、適時に見直しを行っていく。

① 金融機関のサイバーセキュリティ管理態勢の強化

ア. 平時のサイバー対策

中小金融機関については、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て、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。このため、協同組織中央機関・業界団体との対話を進めることにより、サイバーセキュリティに係るリスク評価やコンティンジェンシープランの整備を含めた態勢整備の加速を促し、効果的に業態全体の底上げを図る。実態把握やサイバーセキュリティ演習等で把握した業界全体に共通する課題等については、幅広く問題提起を行い、業界全体として必要な対応を促していく[24]。また、協同組織中央機関自身のサイバーセキュリティ対策についても確認を行い、必要な取組みを促していく。

個別金融機関に対する実態把握と対話については、基礎的なサイバーセキュリティ管理態勢の整備（経営陣の取組み、リスク管理の枠組み、技術的対策等の対応態勢、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、サイバーセキュリティに関する監査）に加え、例えば、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について踏み込んだ検証を行う。その際、信用金庫・信用組合については、各金融機関のリスクプロファイルを把握した上で、リスクベース・アプローチに基づき効果的に実態把握と対話を実施する。更に、特に取組みに遅れがみられるなど、サイバーリスクが高く自主的な改善が見込まれない先に対しては、必要に応じて立入検査も活用し、的確に対応していく。

このように、中小金融機関の基礎的なサイバーセキュリティ管理態勢の整備及びその実効性確保という課題に対して、協同組織中央機関・業界団体との対話、個別金融機関の実態把握、立入検査などの手法を効果的・効率的に連携させることにより確実に取組みを進めていく。

大手金融機関に対しては、グローバルに業務を展開していること等を踏まえ、海外大手金融機関のベストプラクティスや国際的な議論の動向を念頭に置いた対話を継続していく。金融庁としても、定期的に海外大手金融機関のベストプラクティスや国際的な議論の動向等について調査・分析を行い、優れた取組みについては対話の中で積極的に取り上げ、大手金融機関のサイバーセキュリティ対策のより一層の高度化を

[24] 平成 30 事務年度は、傘下金融機関に還元したリスク評価の手引書やコンティンジェンシープランのひな型を必要に応じて活用しつつ、傘下金融機関の基礎的なサイバーセキュリティ管理態勢の確保を後押しするような取組みを促す。加えて、傘下金融機関のセキュリティに関する脆弱性診断等の受検や脆弱性対応の実施について、どのように働きかけを行っているかを検証していく。

促していく。

イ.インシデント対応

サイバー攻撃が高度化・複雑化する中で、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。サイバー攻撃に的確に対応するためには、演習を通じて、コンティンジェンシープランに基づく対応を実践し、現在の対応態勢が十分であるかを確認するなど、PDCA サイクルを回しつつ、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、特に中小金融機関のサイバーセキュリティ対策の底上げを図るために「金融業界横断的なサイバーセキュリティ演習」（Delta Wall）を実施してきたところであり、サイバー攻撃へのインシデント対応能力を向上させるための重要なツールとして今後も継続的に実施していく。その際には、サイバー攻撃の実例分析・外部有識者の知見の活用等を通じて、業態・業務特性に照らして最も脅威となりうるサイバー攻撃を想定したより実践的な内容で実施する。加えて、例えば、共通インフラへの攻撃で影響が広範囲に及ぶことで、個別金融機関の対応のみならず業態全体としての対応が必要となる内容等を検討し、演習内容の一層の高度化に取り組む。また、演習参加業態や演習結果に係る事後評価基準については、サイバー攻撃の動向を踏まえ、必要に応じて見直しを行っていく。

こうした演習は、金融庁のみならず、NISC や金融 ISAC 等でも実施しており、それぞれの演習が金融機関の目的・成熟度に応じた多彩な選択肢となるように、関係者との連携を強化していく。

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への参加を支援することにより、クロスボーダーで、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を図る。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、「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の活用を促すことにより、対応能力の一層の高度化を図る。

② 情報共有の枠組みの実効性向上

サイバーセキュリティの確保は、まずは保有する情報資産、IT 技術の利活用の状況を踏まえ、自組織のサイバーセキュリティ上のリスクを特定し、必要なサイバーセキュリティ対策を進める「自助」の取組み[25]が前提となる。こうした「自助」に加えて、サイバー攻撃が高度化・複雑化する中で、金融機関同士で情報共有・分析を行う「共助」の果たす役割が非常に大きくなってきている。

このため、金融庁として、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、金融機関に周知していくことに加え、金融 ISAC への加盟が地理的・人的・金銭的に難しいとの一部中小金融機関の意見も踏まえ、金融 ISAC や FISC 等とも連携し、「共助」の取組みの第一歩となるよう、地域内の情報共有を推進していく。具体的には、現在、金融 ISAC や FISC では地域での活動に力を入れており、こうした活動が中小金融機関の「共助」態勢への参画に繋がるよう、金融庁としても、財務（支）局

[25] 「自助」の取組みを促進するための金融分野の人材育成の強化に向けた取組みについては③に記載。

等とも連携を図りながら、積極的に支援していく。加えて、FISC においても、会員向けにサイバーインシデントに関する情報共有の取組みを進めており、金融庁としても後押ししていく。

また、「サイバーセキュリティ戦略」において、従来の枠を越えた情報共有・連携体制の構築が掲げられており、サイバーセキュリティに係るリスクが拡大していることを踏まえ、重要インフラ事業者（銀行等、証券、生保、損保）以外の金融関連の業界団体等との連携を強化し、業界内での「共助」の取組みを促していく。

更に、NISC からの情報提供や他の金融機関で発生したインシデントを踏まえた注意喚起などの「公助」についても、デジタライゼーションの進展等を踏まえ、新たなサイバーセキュリティに係るリスク等の発生を迅速に把握するため、これまで以上に幅広く情報収集・分析を行い、金融分野への積極的な情報発信を通じて金融機関のプロアクティブな対応を促す。

③　金融分野の人材育成の強化

サイバーセキュリティ対策を進めていく上では、経営層の積極的な関与が非常に重要であり、「サイバーセキュリティ戦略」においても、「経営層の意識改革」が掲げられている。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、

・技術・システム部門の対応→管理・組織としての対応
・現場の問題→経営の問題
・IT リスクの領域→危機管理・リスク管理の領域

として認識した上で、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。これまでの金融庁の取組みにおいても、サイバーセキュリティ対策を進めている金融機関と、経営層の関与度合いには大きな相関関係があることが判明しており、金融分野のサイバーセキュリティの底上げのためには、経営層の意識向上が必須である。

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を各地域で開催するとともに、金融 ISAC や FISC 等の関係機関の主催するセミナー等にも積極的に講師を派遣し、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るとともに、金融分野の人材育成の強化に継続的に取り組む。

また、「サイバーセキュリティ戦略」では、経営層と実務者層・技術者層の橋渡しをする人材である「戦略マネジメント層」の育成・定着が掲げられている。今後、金融分野においても、NISC 等とも連携して、海外や他分野の優良事例等[26]を収集・還元することにより、金融機関における「戦略マネジメント層」の育成・定着を促していく。

更に、金融機関のサイバーセキュリティ対策の向上のためには、財務（支）局を含

[26] 海外大手金融機関のベストプラクティスでは、サイバーセキュリティに関する専担者（CISO：Chief Information Security Officer）を中心としたリスク管理を実施しており、国内大手金融機関においても専担者（CISO）設置の動きがみられる。

む監督当局の知見を強化していくことも重要である。監督当局の人材育成に向けて、関係部署とも連携し、専門研修の実施、外部研修の受講に加えて、専門大学院への継続的な職員の派遣等に取り組むことにより、サイバーセキュリティに関する情報収集・分析能力や金融機関のモニタリング能力の強化を図る。