金融調査会　緊急提言２０２６
―　AI 時代に対応した金融分野のサイバーセキュリティ高度化に向けて　―

令和８年１１月１７日

１．　必要な政策対応

１－１．金融庁の足元の対応

AI 技術の進展に伴い、サイバー攻撃においても AI の活用が進み、攻撃の速度・規模・高度化が飛躍的に進展している。金融機関を取り巻くサイバー上の脅威はこれまで以上に深刻化しており、金融システムの安定性を確保するためには、金融機関におけるサイバーセキュリティ対策の強化を最優先課題として迅速に進める必要がある。

金融庁においては、本年４月以降、官民の連携強化を図るための会議の開催、金融機関等に対する短期的な対応の要請、昨今の不正アクセス事案を踏まえた注意喚起の発出などを通じて、金融機関の対応を促してきているが、足元のサイバーセキュリティ脅威の高まりを踏まえると、更に必要な対応を促していくべきである。また、中央機関等が主要システムを担っている協同組織金融機関については、短期的な対応の実施状況について、中央機関等とも連携してフォローアップを継続し、必要な改善を促すべきである。

１－２．中長期的な視点に立ったサイバーセキュリティ指針の策定

サイバー攻撃の態様は大きく変化しており、AI の活用により攻撃側の能力そのものが新たな段階に移行しつつあり、中長期的に深刻度を増すことが懸念される。このため、個別事案への対応のみならず、中長期的な視点から、金融分野全体のサイバーセキュリティ向上に向けた指針を官民が連携して策定する必要がある。特に、AI の活用を通じて、攻撃側のコストが劇的に下がっていることを踏まえ、金融業界全体でサイバーセキュリティコストを低減し、金融業界全体のサイバーセキュリティのレベルを上げていくために、たとえば、金融システム全体でのアーキテクチャの見直し、金融機関をまたいだシステムの共同化・標準化、金融機関自身の IT・ AI・セキュリティに係る知見の一層の向上、専門人材の確保、IT システムの受発注のあり方といった点について検討を行っていくことも重要である。くわえて、サイバーセキュリティの脅威は、機

密情報の流出に留まらない点も強く意識すべきである。金融システムは個人の生活・事業活動・社会全体の基盤であり、情報セキュリティの基本要素である、機密性（Confidentiality)、 完全性（Integrity)、 可用性（Availability）の全てを確保する必要性が高いことから、いかなる時でも金融システムの安定性が確保されるよう、冗長性を確保しレジリエンスを強化していくことが重要である。

金融庁は、金融業界、IT ベンダー及び関係省庁と連携し、AI 時代における金融機関等のサイバーセキュリティ対策の高度化の方向性を早期に示すべきである。その際、AI 時代にふさわしい金融機関のサイバーセキュリティのあるべき姿とともに、その実現に向けた進め方についても示すことで、金融機関における着実な進展を促すべきである。

１－３．二次被害の防止と被害者救済に向けた制度の在り方の検討

サイバー攻撃により、足もとで顧客情報の漏えいが相次ぐ中、実在の事業者や行政機関等を装った巧妙な不審メールや、他人になりすました金融サービスの悪用が今後さらに増加する可能性があることから、二次被害を防止するための対応を徹底するとともに、被害者の救済のための制度の実効性を高めていくことも重要である。

金融庁においては、警察当局とも密に連携し、引き続き、金融機関に対し、本人確認について IC チップ情報読取方式への早期の原則一本化や口座の不正利用について出金停止・凍結等の措置の迅速化を求めるほか、金融サービスの利用者に向けた注意喚起を行うべきである。また、最近のマネー・ローンダリングの手口を踏まえた金融事業者における対応状況についての実態把握を行うとともに、被害者の実効的な救済に向けた制度の在り方について検討を進めるべきである。

２．前例にとらわれない規模の予算措置など、共助・公助の強化を通じた実効性確保

金融庁は、金融機関において、サイバーセキュリティ対策の強化が適切に行われているかモニタリングするとともに、中長期的な視点で新たな対策や指針を示し、それらが金融機関において着実に実施され、その実効性が確保されることが重要である。

特に、大手金融機関と比較して、中小金融機関等においては、専門人材や予算の不足が課題となっていることに加え、AI 時代においてサイバーセキュリティ対策に必要な投資や運用コストは今後も増加していくことが見込まれる。まずは金融機関による自助努力を基本としつつも、それだけで必要な対策を講じることには難しい面もある。このため、金融業界全体として相互に支え合う「共助」、政府による支援としての「公助」を一層強化していく必要がある。この際、不正アクセス等のサイバー事案が発生した際の初動対応から復旧に至るまで、自助・共助・公助の連携による実効的な対応体制の構築も重要である。特に、レジリエンスの確保という点からも、金融庁は、重大なサイバーセキュリティ事案が発生した際の対応方針を整理し、関係組織との連携を行うべきである。

金融 ISAC や業界団体等による情報共有は引き続き重要な取組であるが、情報の提供にとどまらず、共同での脅威分析、演習、対策支援及び人材育成等へと取組を発展させ、中小金融機関を含む業界全体の防御力向上につなげるべきである。

また、政府として、中小金融機関等を含めた金融業界全体のサイバーセキュリティ対策の実装を促進する観点から、これまでの前例には全くとらわれない規模での予算を措置すべきである。具体的には、金融庁において検査・モニタリングの一環として、金融機関に対し AI を活用した脆弱性診断を行うとともに、金融機関における脆弱性対応プロセスの高度化を促進し、業界全体のサイバーセキュリティ対応能力の強化を図るべきである。あわせて、金融庁が実施する業界横断的サイバー演習（Delta Wall）について、その対象や機会の拡充を図ることで、インシデント対応能力の向上のため、多くの金融機関、とりわけ預金取扱金融機関はすべての者が少なくとも年１回は何らかのサイバー演習に参加できる環境の整備を進めるべきである。また、こうした支援措置を、前述した指針と一貫した形で講ずることにより、短期的な取組と中長期的視点の取組を一体的に推進していくことも重要である。こうした取組を通じて、金融機関の職員が実践的な知見や経験を蓄積できる環境を整備し、AI やデジタル技術にも対応できる IT・サイバーセキュリティ人材の育成も促進すべきである。

政府は、不正アクセス事案の急増を受けた社会的不安の広がりにも留意すべきである。昨今の不正アクセス事案の特徴、それを踏まえた政府および金融機関の対応、今後起き得る事態やそれに対して個人・事業者が採り得る対策など、多くの人が理解できるように、より一層、簡潔・平易な普及啓発に努めるべきである。

３．金融行政における専門人材・知見の一層の強化・活用

上記で述べたとおり、足元、サイバーセキュリティ―についてのリスクは極めて高まっており、予算面も含めて必要なリソースの抜本的強化に取り組んでいくべきだが、サイバーセキュリティ以外にも、マネー・ローンダリング対策やAI・デジタル技術などをめぐり、金融業界を取り巻くリスクが複雑化・高度化する中、金融行政において、高度な専門性が求められる分野が拡大している。金融庁においては、これまでも、民間部門からの専門家を様々な形で採用してきたが、それについては引き続き、継続・強化していくべきである。

他方で、サイバーセキュリティなどについては民間部門においても専門人材は質量ともに十分とは言えず、それらの貴重な人材については、金融庁・財務局における採用という形以外にも、様々な形での官民の連携を通じ、実質的に政策形成に民間専門人材の知見を取り込んでいくことが重要である。

もとより、金融行政の中核は金融庁・財務局に継続的に勤務する職員が担い手であり、過去に提言を行っているとおり、金融庁・財務局職員の計画的育成について取り組むべきである。他方で、政府機関としてのリソースの確保には自ずと限界もあることから、協同組織金融機関の中央機関等、金融庁・財務局の外にある機関・人材との連携強化等も含め、金融行政の高度化に向けて、中長期的な組織・人員の在り方について検討を進め、専門性が求められる行政課題に持続的に対応できる体制整備の方向性を示すべきである。