（仮訳）

サイバーセキュリティに関するニューズレター

2021 年 9 月 20 日

この数年、ランサムウェア攻撃等のサイバー脅威・事象は、個別金融機関の安全性と健全性、及び金融システムの安定性にリスクをもたらすといった銀行セクターへの懸念が高まってきている。新型コロナウイルス感染症の世界的な感染拡大を契機に、こうした懸念はさらに高まってきている。リモート勤務の導入や、デジタルな経路を通じた金融サービス提供の増加により、銀行が攻撃を受ける対象となる領域は拡大してきた。これは、益々巧妙化してきている悪意ある主体が、銀行システムへのより多くのアクセスポイントを持つことを意味する。銀行が共通して利用しているサードパーティソフトウェアやグループ内の事業者を含む、銀行のサードパーティへの標的型攻撃もまた、サイバーセキュリティ対策上、こうしたサードパーティへのオペレーション上の依存度を考慮に入れる必要があることの明確な警告となっている。ランサムウェアは、銀行業界が直面する主要なサイバーセキュリティ上の脅威の一つであり続けるだろう。その増大する重要性を鑑み、サイバーセキュリティは、中央銀行総裁・銀行監督当局長官グループが本年に承認した、バーゼル委の作業計画の重要な要素となっている。

バーゼル委は、2021 年 3 月 31 日に、オペレーショナル・リスクとオペレーショナル・レジリエンスに関連した、「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（原題：Revisions to the principles for the sound management of operational risk、以下『PSMOR』）」と、「オペレーショナル・レジリエンスのための諸原則（原題：Principles for operational resilience、以下『POR』）」という 2 つの文書を公表した。PSMOR は、サイバー脅威への脆弱性を含む、情報通信技術に関連したオペレーショナル・リスクをより適切に考慮に入れることも視野に入れて改訂された。加えて、POR で示されている通り、足もとの環境における銀行のオペレーショナル・レジリエンス（混乱時において重要な業務を継続できる銀行の能力を指す）の重要な構成要素は、アウトソーシングに起因する事象も含む、サイバー事象に対する強靭性である。そのような強靭性の獲得のためには、銀行は脅威や潜在的な破綻個所を特定し、これらから自らを守る必要がある。銀行はまた、混乱を伴う出来事が業務継続、特に重要な業務の継続に及ぼす影響を最小化するために、こうした出来事から回復し、学習するだけではなく、対応、適応を進めていかなければならない。

バーゼル委は、すべての銀行監督当局がその監督対象金融機関に対して、広く受け入れられている業界標準に沿ったサイバーリスク管理を行うために、有効性の確認を含めた、管理手段や効果的な慣行および枠組みの採用を推奨することが重要であると考えている。このようなアプローチを採用することで、銀行は、サードパーティに起因するものを含むサイバーリスクへのエクスポージャーを、よりよく特定、評価、管理し、軽減することが出来るようになる。これは、PSMOR と POR に則った取組みが進展する形で、サイバー脅威と事象に対するより高い強靭性を育むことにつながるだろう。さらに、このようなサイバーリスク管理のアプローチの利用を通じて、サイバーセキュリティ上の脅威と事象に対する銀行の取組みを強固にする。加えて、そのようなアプローチの利用は、当局による監督を円滑化し、監督当局の評価について法域間での一貫性を促進することに資する。

バーゼル委は基本的に、特定の手段、効果的な慣行あるいは枠組みを支持するということはないが、銀行が国際的に利用されていてかつ広く受け入れられている業界標準に沿った手段等を採用することについては歓迎する。これらの基準間でみられる内容や形式についての共通性には、主要なサイバーセキュリティ上の原則に現在盛り込まれている国際的なコンセンサスが表れている。業界標準に沿った手段、効果的な慣行および枠組みであって現在利用可能なものには、米国立標準技術研究所（National Institute of Standards and Technology：NIST）の「Cybersecurity Framework」、国際標準化機構（International Organization for Standardization：ISO）の「ISO2700X」、米 CIS（Center for Internet Security）の「Critical Security Controls」といったものが挙げられる。加えて、監督当局は銀行に対し、金融安定理事会が公表した「金融機関におけるサイバー事象の初動・回復対応のための効果的な実務のツールキット（Cyber Incident Response and Recovery toolkit）」や、「サイバー用語集（Cyber Lexicon）」といった資源の活用を促した方が良い。これらの手段、効果的な慣行および枠組みの多くは公開されており、銀行は無料で利用することができる。

バーゼル委は、現在の環境下において、銀行はサイバーセキュリティ上の脅威と事象に対する強靭性を向上させるよう、継続的に取り組む必要があると考えている。広く受け入れられている業界標準に基づいた手段、効果的な慣行と枠組みがより広く普及し、それにより効果的なサイバーリスク管理、入念なサイバー衛生慣行、サイバー脅威の特定と防衛の適切な手段や、対応・回復能力の強化といった基本的な要素が改善することを通じて、銀行のサイバーセキュリティの強化につながる。バーゼル委は、その作業計画に示されている通り、サイバー脅威に直面している銀行のシステムやデータの機密性、完全性、可用性の保護に資する、銀行のサイバーリスク管理と

強靭性の動向について監督と評価を継続する。バーゼル委は、個別銀行の安全と健全性を育み、潜在的な金融システム安定への影響を抑制するために、必要に応じて対応をとっていく。