2024.11.12 金融財政事情 掲載

サイバーセキュリティー確保に向けた新たなガイドラインの要諦

サードパーティーを含めたエコシステム全体で対策の強化を

金融庁総合政策局リスク分析総括課
IT サイバー・経済安全保障監理官　齊藤 剛
サイバーセキュリティ対策企画調整官　三浦 俊
IT サイバー・経済安全保障監理官室 総括補佐　木澤 浩亮

金融分野のサイバーセキュリティーの確保は、金融機関の経営および金融システム全体の安定に関わる喫緊の課題だ。そこで金融庁では 10 月４日に監督指針等を一部改正するとともに、「金融分野におけるサイバーセキュリティーに関するガイドライン」（以下、GL）を策定した。本稿ではこの狙いや概要について、パブリックコメントで寄せられた意見も交えて解説する[1]。

規模・業態を踏まえてリスクに応じた対応を

各業態の監督指針・事務ガイドライン（以下、監督指針等）では今回の改正まで、サイバーセキュリティーに関する記載は、2015 年の改正で追加した 10 項目にとどまっていた。しかし、近年のサイバー攻撃の脅威の動向や国内外の情勢、当庁の検査・モニタリングの経験を踏まえると、金融機関が直面するサイバーリスクが顕著に台頭し、必要なリスク管理態勢と現状の差が拡大しているとみられる。

当庁はこの差を解消するため、講演や寄稿、検査・モニタリングなどのあらゆる機会を通じて金融機関と対話し、対応を促してきたが、こうした監督上の期待を明確化することが、金融機関のみならず、サードパーティーを含めたエコシステム全体のサイバーセキュリティー向上のために有益だと考えた。そこで監督指針等を改正するとともに、新たに GL を策定した。

GL の策定に当たっては、国内外のフレームワークを参考にするとともに、当庁の検査・モニタリングで発見した事項等を盛り込んだ。GL では、特定、防御、検知、対応・復旧についての項目に加え、こうしたフレームワークにおいて近年重要な要素とされる経営陣のリーダーシップを含むガバナンス、サードパーティーリスク管理に関す

[1] 詳細は金融庁ウェブサイトにて公表している GL に加え、「コメントの概要及びコメントに対する金融庁の考え方」も参照。

る着眼点を盛り込んでいる。

また GL では、各領域において「基本的な対応事項」と「対応が望ましい事項」を明確化した（図表）。金融機関の規模・特性は多様であり、「基本的な対応事項」および「対応が望ましい事項」の双方について一律の対応を求めるものではない。金融機関自らを取り巻く事業環境や経営戦略、リスク許容度等を踏まえ、サイバーセキュリティーリスクを特定・評価し、それに見合った低減措置を講ずる「リスクベース・アプローチ」が求められることを GL に明記している。

〔図表〕　ガイドラインで明確化した事項

基本的な対応事項	• いわゆる「サイバーハイジーン」と呼ばれる事項、その他の金融機関等が一般的に実施する必要のある基礎的な事項
対応が望ましい事項	• 金融機関等の規模・特性等を踏まえると、インシデント発生時に、地域社会・経済等に大きな影響を及ぼし得る先において実践すべきと考えられる取り組み • 他国の当局または金融機関等との対話等によって把握した先進的な取り組み等、大手金融機関および主要な清算・振替機関等が参照すべき優良事例

（出所）「金融分野におけるサイバーセキュリティに関するガイドライン」から筆者作成。

なお、規模や業態などの要素だけで GL 記載事項の該否を考えるべきではない。脅威環境などによってリスクは変動し得る点に留意が必要だ。

改正後の監督指針等および GL は、公表日（10 月４日）から適用を開始した。特定の期限までに対応を促す性質のものではないため、経過措置は設けていない。当庁のモニタリングに当たっては、GL への対応については金融機関で重要性・緊急性に応じて優先順位を付けた上で、リソースの制約を踏まえ、リスク低減措置に取り組むべきであることに留意することとしている。この優先順位の付け方は一意に存在するものではなく、各金融機関で検討が必要だ。

前述のとおり GL ではリスクベースでの対応が求められるものの、サイバーリスクは金融機関の経営に重大な影響を及ぼしかねないトップリスクの一つであるため、金融機関においては、その管理態勢の整備および実効的な運営が喫緊の課題となる。金融機関を取り巻く脅威動向やリスクを踏まえると、形式的な体制整備ではなく、ガバナンスを含めたサイバーセキュリティー管理態勢が、現実にどの程度有効に機能するかという観点からの実質的な対応が求められる。

経営陣の主体的関与でガバナンスの確立を

サイバーインシデントによる業務中断や機密情報の漏洩は、金融機関の事業・経営ならびに金融機関に対する信頼を揺るがしかねない重大な影響をもたらし得る。これは金融システムの不安定化をも招きかねない。

求められるサイバーセキュリティーの強化には、IT・システム部門だけではなく、各業務所管部や企画、広報、コンプライアンス、リスク管理、監査などの各部門間の連携が不可欠だ。技術的対策だけでなく、組織的な対策も推進するためには、経営者の認識とイニシアチブによるところが大きい。

GL でも、経営陣のリーダーシップの下でサイバーセキュリティーに関するガバナンスの確立が必要である点を明記した。例えば、経営陣が自らリーダーシップを発揮し、サイバーセキュリティー確保に向けた組織風土を醸成する必要性を記載した。

これには、経営陣が担当部署等の特定の部署あるいは特定の職員に対応を任せるのではなく、組織全体（部門、職員のレベルなどを問わず）として、サイバーセキュリティー管理態勢を構築・運用することが含まれる。担当部門が取締役会等に上程した内容を経営陣が受動的かつ形式的に追認している場合、経営陣の主体的関与が行われているとは一概に言い難いだろう。

また、人材育成に配慮した人事政策や、セキュリティー人材育成計画の策定の必要性について、GL では独立した節を設けて記載している。セキュリティー人材は金融分野以外でも逼迫しており、外部からの調達は容易ではない。こうしたなか、計画なく短期的な内部人材の配置転換を繰り返せば、人材の確保・育成はますます困難になろう。

事業継続の上でセキュリティーの確保は欠かせない前提であることを認識し、中長期的な視点で人材の確保・育成に取り組む必要がある。こうした対応は、経営陣が率先して関与しなければ実現は容易でないと思われる。

基本的な対策の実践が必要

GL には、基本的な対策として情報資産管理や脆弱性管理、定期的な脆弱性診断・ペネトレーションテストの実施、ID アクセス権管理などについての着眼点を記載した。これらは、過去の検査・モニタリングにおいて対策が不十分な事例が散見され、対応を促してきた事項でもある。

パブリックコメントでは、これらの実施頻度や程度・水準等に関する意見・質問が複数寄せられた。

その一つが情報資産の台帳をどの程度「最新の状態」に保てばよいのかという点である。これについては、リスクベースで判断すべきであり、例えば深刻な脆弱性が明らかになった場合に対応できるかという観点を考慮する必要がある。

また、脆弱性管理において、他のトラブルやコストを考慮してパッチ適用を速やかに実施しないことの是非についても質問が寄せられた。これもケースバイケースだ。深刻かつ機密性・可用性・完全性に重大な影響のある脆弱性であるにもかかわらず、他のトラブルがあることをもって代替的な低減措置なしにパッチ適用を否とするかについては慎重な検討が必要である。

なお、防御に関する技術的対策の運用・管理を外部ベンダーに委託する場合であっても、サイバーセキュリティーに関する最終的な責任を委託先に転嫁することはできない。委託先に対する統制・管理の責任が金融機関にあることを前提として、必要に応じて外部リソースを活用し、自組織のサイバーセキュリティーを補完・強化することが考えられる。

侵入を前提とした対応の強化が重要

リスク評価に当たっては、境界防御型セキュリティーが突破または迂回されるリスクや、内部不正などの脅威も考慮し、内部ネットワークセグメントに設置したシステムのリスクも対象とする必要がある。当庁は境界防御型セキュリティーの限界について、これまでさまざまな機会を通じて強調しており、GL でも明確化した。サードパーティーやサプライチェーン経由のものを含む内部不正のリスクが現実の脅威となっていることを踏まえた対応も欠かせない。

防御や検知だけでなく対応や復旧についても、さまざまなケースを想定しておくことが重要だ。サイバー攻撃か否かによって、そしてサイバー攻撃の種別によって、インシデント対応や復旧計画は異なると考えられる。

例えば、サイバー攻撃はシステム障害とは異なり、復旧や再接続時の再感染リスクの確認において対応に違いがあり得る。また、ウェブサイトのダウンを狙った DDoS 攻撃と、不正送金を引き起こす攻撃では、顧客対応の内容に違いが生じ得る。

このように、さまざまなケースを想定して、インシデント対応計画およびコンティンジェンシープランを策定する必要がある。それとともに、これらの実効性を定期的な演習・訓練によって確認し、技術面のみならず態勢面も継続的に改善することが重要である。

各金融機関の規模や特性、リスクが異なる以上、基本的な対応事項のそれぞれについて具体的な対応を一律に記載することは困難である。このため、基本的な対応事項のそれぞれについて自らの組織に必要な対応を考え、実践することが求められる。

管理が求められるサードパーティーリスク

昨今、サプライチェーンに由来するサイバーインシデントで金融機関の業務や顧客が影響を受ける事例が多発している。これを踏まえて GL では、サードパーティーリスク管理に係る対応事項を詳細に記載した。

サードパーティーリスク管理は、チェックリストを用いた形式的な確認によることが多いと考えられるが、リスク管理を実効的なものとしていくことが重要である。リスク管理の目線をそろえる観点からは、サードパーティーリスクを一元的に管理する統括部署の設置や、関係部署間の連携が重要だ。ライフサイクル管理（契約前のリスク評価・デューデリジェンス、期中のモニタリング、出口戦略など）も求められる。インシデントの発生を想定してコンティンジェンシープランを整備する際は、さまざまなシナリオの下で、サードパーティーのリスクも考慮することが必要である。

なお、特にサービス提供型のサードパーティーの場合、サードパーティーからの情報開示に制約があり、リスク管理が困難という意見もある。一般論として、このような場合には、サイバーセキュリティーの適切性・十分性について、契約書や第三者保証による報告書、サードパーティーから提供される報告書等を活用することが考えられる。さらに GL では、金融機関にサービスを提供するサードパーティーに対して、そのサイバーセキュリティーリスクを適切に管理するために必要な支援（リスク管理上必要とする情報の提供など）を金融機関が行うべきであることも示している。

業界団体や共助組織・中央機関の役割が大きい

特に規模が小さい金融機関において、最新の脅威や攻撃手法などの情報収集・分析や対応のノウハウ蓄積を単独で行うことには限界がある。そのために金融 ISAC などの「共助」の組織が設立され、技術的な課題への対応やベストプラクティスの提供、最新のサイバー攻撃の動向、脆弱性情報の分析、実践的な演習の実施等に関し、積極的な情報共有その他の協力が行われている。

また、協同組織金融機関の場合、中央機関による経営支援機能を活用することも考えられよう。中央機関には、サイバーセキュリティーに関する業務補完・支援の充実を通じて、業態内の相互扶助の充実を図ることが期待されている。

金融機関にとってサイバーセキュリティーは、競争分野ではなく協調分野だ。さらなる共助の余地があると考えられ、こうした共助組織、中央機関、業界団体やその活動の果たす役割は大きい。

仮に自らの組織のサイバーセキュリティーが強固なものであったとしても、他の金融機関の脆弱性が明らかとなれば、業界全体が標的とされ得るほか、業界全体の信頼が損なわれる事態に発展することもあり得る。サイバーセキュリティーは、業界、ひいては金融サービスの利用者、当局を含めたステークホルダーが、エコシステム全体

で強化すべく努める必要がある。

当庁としては、引き続き金融機関自らの努力による「自助」や業界の協力による「共助」、当局の支援による「公助」を組み合わせ、官民連携で知見とリソースを結集し、金融分野全体のサイバーセキュリティーの強化に邁進していく。

（本稿は 24 年 10 月時点の情勢に基づいている。また、本稿における意見に係る部分は筆者の個人的見解であり、所属組織の見解を示すものではない）

さいとう つよし
04 年金融庁入庁。保険監督者国際機構（IAIS）、総合政策局総務課国際保険規制調整官などを経て、21 年総合政策局サイバーセキュリティ対策企画調整室長。23 年7月から現職。

みうら しゅん
大手金融機関、コンサルティング会社を経て 09 年金融庁入庁。20 年7月から現職。サイバーセキュリティ企画グループ長として金融機関のサイバーセキュリティーに関する検査・モニタリングや金融業界横断的なサイバーセキュリティー演習を統括。

きざわ こうすけ
11 年財務省入省。金融庁監督局証券課、個人情報保護委員会事務局総務課国際室、経済協力開発機構（OECD）事務局デジタル経済政策課などを経て、23 年7月から現職。