特集

サイバーセキュリティ高度化への課題

金融分野における「取組方針」アップデートの狙い

環境変化への対応とPDCAでサイバーセキュリティ強化を図る

金融庁
総合政策局総合政策課
サイバーセキュリティ
対策企画調整室長
水谷 剛

金融庁
総合政策局総合政策課
サイバーセキュリティ
対策企画調整室
課長補佐 **平野 義隆**

近年のサイバー攻撃の高度化・複雑化に加え、デジタライゼーションの加速的な進展や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巡る環境は大きく変化している。こうした環境変化に伴う新たな課題に対応するため、金融庁は昨年10月に「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」をアップデートした。この取組方針に基づき、官民の緊密な連携を図り、サイバーセキュリティ強化に向けた取組みを進めていく。本稿では、アップデートした取組方針のポイントを解説する。

環境変化に対応して取組方針をアップデート

金融庁では、金融分野のサイバーセキュリティ確保の観点から、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」を策定・公表した。この取組方針に基づき、これまで官民が一体となって、金融分野のサイバーセキュリティに取り組んできた。

しかしながら、近年のサイバー攻撃の高度化・複雑化に加え、デジタライゼーションの加速的な進展、国際的な議論の進展、20年東京オリンピック・パラリンピック競技大会（オリパラ大会）の開催など、金融分野のサイバーセキュリティをとりまく状況は、15年の取組方針策定時から大きく変化している。また、これまでの取組みについても、PDCAを踏まえて改善していくことが重要である。こうした基本認識を踏まえ、昨年10月、金融庁では取組方針のアップデートを行い公表した。

デジタライゼーションの進展への対応

アップデートした取組方針では、対応すべき新たな課題として、①デジタライゼーションの加速的な進展、②国際的な議論の進展、③20年東京オリパラ大会の開催の3点を挙げている。

まず、金融分野では、すで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おり、今後においても、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予想される。一方、こうしたデジタライゼーションの進展により、図表のような新た

なリスクが顕在化することが考えられる。

今後、大手金融機関のみならず中小金融機関にとっても、こうしたデジタライゼーションの流れに対応していくことは不可欠となると考えられる。そして、その際にはデジタライゼーションに伴うリスクにしっかりと対応していくことが求められる。

〔図表〕　**顕在化することが考えられる新たなリスク**

- 新たなプレーヤーとの連携、既存業務の外部委託等の進展によるサードパーティー（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つながることにより、単一障害点を発端に連鎖的に影響が広範囲に及ぶリスク（最悪の場合は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・対応できなくなるおそれ

（出所）　金融庁「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」(18年10月)

このため、金融庁では、「デジタライゼーションの進展により具体的にどのようなサイバー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」などについて、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リスクへの対応策を金融機関に促していくとともに、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。

国際的議論やオリパラ大会も見据えた取組み

また、近年の世界的なサイバー攻撃の高度化・複雑化を受けて、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。Ｇ７財務大臣・中央銀行総裁会議では、15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。16年以降、サイバーセキュリティ対策の国際的な基本原則を示した「基礎的要素」を公表してきており、昨年10月には、「脅威ベースのペネトレーションテスト（ＴＬＰＴ）」および「サードパーティー（外部委託）」に関するＧ７の基礎的要素を策定・公表した。19年には、Ｇ７各国の当局が連携する大規模なサイバーインシデント（事件・事故）に対する国際的な合同演習の実施を予定している。

容易に国境をまた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、金融庁においては、今後とも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。

さらに、20年東京オリパラ大会の開催を控え、わが国の金融分野を含む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されていることから、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。昨年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である「サイバーセキュリティ戦略」が改訂され、新たな戦略のもと、20年東京オリパラ大会に向けて、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。こうした方針を踏まえ、金融庁では、20年東京オリパラ大会を見据えた金融分野の連携態勢を整備するため、関係省庁、日本銀行、業界団体、金融ＩＳＡＣやＦＩＳＣ等の関係団体との連携を一層緊密にし、大規模インシデント発生に備えた金融分野の危機管理態勢の構築に取り組んでいく。

ＰＤＣＡを踏まえた施策の推進

金融分野のサイバーセキュリティ対策のさらなる強化を図る

昨年10月に実施した「金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅲ）」の様子。

中小金融機関においては、依然として、サイバーセキュリティ対策の基礎となるリスク評価を実施していない先や、インシデント対応の基礎となるコンティンジェンシープラン（インシデント対応マニュアル）を整備していない先が見られた。リスク評価とは、まず保有する情報資産、ＩＴの利活用の状況を踏まえ、自組織のサイバーリスクを特定・評価するものであり、必要なサイバーセキュリティ対策を進めるうえでの基礎となるものである。中小金融機関については、こうした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。

また、20年東京オリパラ大会の開催に関連して想定されるリスクを見据えて、リスク評価に基づく対策を進めることによりその実効性を高めていくことが重要である。このため、業界団体等との対話や実態把握などを進めることにより、態勢整備の加速を促し、効果的に業態全体の底上げを図っていく。

大手金融機関については、わ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。こうしたなか、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き上げるため、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（ＴＬＰＴ）の活用を進めるなど、一層の高度化に向けて相応の進展が見られる。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などを踏まえ、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ことにより、サイバーセキュリティ対策の一層の高度化を促していく。

②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、日々進化するあらゆるサイバー攻撃を検知し防御することには限界があり、攻撃を受けたあと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することにより、対応能力を向上させることが有効である。

こうした認識のもと、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ことを目的として、「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（囲み記事参照）。今後とも、金融機関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ための重要なツールとして継続的に実施していく。

③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、自らのリスク評価に基づき必要なサイバーセキュリティ対策を実施する「自助」の取組みが重要であることは言うまでもない。ただ、サイバー攻撃が高度化・複雑化する中で、こうした「自助」を効果的・効率的に進めていくためにも、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、金融分野のサイバーセキュリティ強化に向けた対策を、①平時のサイバー対策（サイバー攻撃への備え）、②インシデント対応（インシデント発生時の適切な対応）、③情報共有、④人材育成――に区分して概説する。

①平時のサイバー対策

15年の取組方針公表以降、金融庁は、中小金融機関を中心に200先を超える金融機関に対してサイバーセキュリティ対策に係る実態把握を実施するとともに、3メガバンクや業界団体との対話を進めてきた。

ためには、新たな課題への対応に加え、15年に策定した取組方針に基づくこれまでの取組みのＰＤＣＡを踏まえて施策を推進することが重要である。以下では、

融ＩＳＡＣ等の情報共有機関を活用した「共助」の意義について、引き続き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、地域における情報共有を推進していく。

④金融分野の人材育成の強化

サイバーセキュリティ人材については、金融分野のみならずわが国全体として不足が指摘されており、人材の確保のほか、サイバーセキュリティへの理解の促進やスキル向上が重要な課題となっている。加えて、金融機関のサイバーセキュリティ対策を進めるためには、「経営層」の意識改革が不可欠であるが、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いえない状況にある。これまでの金融庁の実態把握においても、金融機関におけるサイバーセキュリティ対策の進み具合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いる。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。

このため、金融庁では、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など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啓発を進めるとともに、金融分野の人材育成の強化に継続的に取り組んでいく。

みずたに つよし
95年大蔵省入省。金融庁総務企画局企業開示課課長補佐、滋賀大学経済学部准教授、滋賀県湖南市総合政策部理事などを経て、18年7月から現職。リスク分析総括課を兼務。
ひらの よしたか
03年金融庁入庁。16年総務企画局政策課サイバーセキュリティ対策企画調整室係長、17年7月から現職。リスク分析総括課を兼務。

金融業界横断的なサイバーセキュリティ演習の実施

昨年10月、取組方針に基づき、特に中小金融機関のインシデント対応能力の底上げを図ることを目的に、金融庁主催による3回目の「金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅲ）」を実施した。今回の演習は、銀行、協同組織金融機関、保険、証券、貸金業者に加え、昨今の脅威動向を踏まえ、新たな業態としてＦＸ業者、仮想通貨交換業者を対象に追加し、計１０５社が参加した。

本演習は机上演習と呼ばれるものである。演習を通じてインシデント発生時における金融機関内外の情報連携に係る対応態勢や手順が十分であるかを確認することを目的として、民間の専門家の知見や攻撃の実例分析などを参考にしつつ、金融機関が見逃しやすい弱点を浮き彫りにし、参加者が「気づき」を得られる内容で実施している。また、経営層や多くの関係部署が参加できるよう、会場集合方式ではなく、自職場参加方式を採用している。

今回の演習は10月22日～26日に、業態別にシナリオを変えて5日間に分けて実施した。10月22日に実施した地方銀行・第二地方銀行向けの演習では、前回までの演習結果における成熟度を踏まえ、より実践的で難易度の高い、シナリオの骨子を事前開示しないブラインド方式を採用した。

今後、参加金融機関がＰＤＣＡサイクルを回しつつ対応能力の向上を図れるよう、演習結果の事後評価を還元するとともに、業界全体にフィードバックすることによって、業界全体の底上げを図っていく。