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（仮訳）

サイバー攻撃の巧妙化や頻度・執拗さの増大により、サイバーリスクはより危険度が高まるとともに多様化しており、グローバルに相互接続された金融のシステムや、これらシステムを運用・サポートする機関に大きな支障を生じさせるおそれがある。以下のノンバインディングで俯瞰的な「基礎的要素」はこうしたリスクに対処するためのものであり、金融セクター内の民間・公的主体が、自身の業務や脅威の状況、金融セクター内における役割、法規制にあわせて調整することができるように策定されている。

本「基礎的要素」は、個々の金融機関が、自らのリスク管理や企業文化に関する認識を踏まえた上で、サイバーセキュリティ・ストラテジーやその運用のためのフレームワークを策定・実施するにあたり、その土台としての役割を果たす。また、本「基礎的要素」は、個々の金融機関が、業務や脅威を巡る環境の変化に応じてサイバーセキュリティ・ストラテジーとフレームワークを体系的に見直していく、というダイナミックなプロセスに向けて、その手順を提供するものである。一国の、または国を跨る当局も、本「基礎的要素」を自身の政策、規制・監督上の取組みのガイドとして利用することができる。民間・公的金融機関と当局は、本「基礎的要素」を踏まえつつ、協働していくことにより、国際的な金融システムにおけるサイバーセキュリティやレジリエンス（サイバー攻撃への耐性やダメージからの回復力）を全般的に強化することができる。

要素１：サイバーセキュリティ・ストラテジーとフレームワーク（Cybersecurity Strategy and Framework）

国内外及び業界における標準やガイドラインを適切に踏まえ、自らが対峙するサイバーリスクに対応したサイバーセキュリティ・ストラテジーとフレームワークを構築・維持すること。

サイバーセキュリティ・ストラテジーとフレームワークを作成する目的は、サイバーリスクをいかに統合的・包括的かつ効果的に特定、管理、軽減させるのか、を明確化することにある。金融機関は、その特性、規模、複雑性、リスクプロファイル、企業文化を踏まえ、サイバーセキュリティ・ストラテジーとフレームワークを構築すべきである。各国の当局は、金融セクター内の各主体と当局の間において、または金融セクターが依存する他のセクターとの間において、あるいは他国との関係において、サイバーの脅威や脆弱性を踏まえどのように協調するのか、を示す金融セクター全体のサイバーセキュリティ・ストラテジーとフレームワークを構築することもできる。

要素２：ガバナンス（Governance）

サイバーセキュリティ・ストラテジーとフレームワークを実施し、管理し、有効性を確認する役職員の役割・責任を明確化し、これらの手順を促進することにより、

アカウンタビリティを確保すること。また、当該役職員に対し、十分なリソース、適切な権限、経営陣等（例えば、企業にあっては取締役会、当局にあっては幹部）へのアクセスを付与すること。

ガバナンスの構造は、責任の所在や報告・エスカレーションのラインを明確化することによって効果的なものとなり、アカウンタビリティが強化される。また、効果的なガバナンスは、競合する目標を解決し、部署間やＩＴ・リスク管理関連の活動におけるコミュニケーションを円滑化するものである。自らのミッション・戦略に沿って、取締役会（あるいは公的機関や当局における同様の組織）は、自身のサイバーリスク許容度を設定するとともに、サイバーセキュリティ計画の作成や実施を監督し、その有効性を確認すべきである。

要素３：リスク管理の評価（Risk and Control Assessment）

相互接続関係や依存度、外部委託の状況も踏まえ、機能・業務・製品・サービスを特定し、それらの重要性に優先順位を付した上で、それぞれのサイバーリスクを評価すること。経営陣によって設定された許容度の範囲内で、こうしたリスクを統御・管理するため、システム、方針、手順そして訓練を含めた管理手法を確定・実施すること。

金融機関のリスク管理の一環として、それぞれの機能・業務・製品・サービスをサポートする職員、業務プロセス、技術、基礎データに由来するサイバーリスク（あるいは、管理手段が欠如しているサイバーリスク）を評価することが理想的である。その上で、金融機関は、隠れたサイバーリスクまでも含め、特定されたリスクに対して統御・管理が存在し有効であることを確認・評価すべきである。ある行動をとらないことにより、リスクを回避・排除することも統御メカニズムに含まれる。また、統御メカニズムには、リスク管理によりリスクを軽減することや、リスクを共有・移転することも含まれる。リスク管理の評価においては、自らの機能・業務・製品・サービスから生ずるサイバーリスクを評価することに加え、自らが他の金融機関や金融セクター全体にもたらすサイバーリスクについても適切に検討すべきである。当局は、金融のシステムにおける重要な経済機能をマッピングすることにより、「単一障害点」や集中リスクを特定するためのリスク管理を行うべきである。金融セクターの重要な経済機能は、預金取扱、貸出、支払にとどまらず、トレーディング、クリアリング、セトルメント、カストディにも及ぶ。

要素４：モニタリング（Monitoring）

サイバーインシデントを速やかに検知し、ネットワークのモニタリング、テスト、監査、演習等を通じて種々の管理手段の有効性を定期的に評価する、体系的なモニタリングプロセスを構築すること。

効果的なモニタリングは、既設定のリスク許容度を金融機関に遵守させるとともに、既存の管理における弱点をタイムリーに強化・修正することの手助けとなる。テスト・監査のプロトコルは、金融機関と当局の双方に対して、基本的な保証（*assurance*）のためのメカニズムを提供する。金融機関やそのサイバーリスク・プロファイルの特性、統御環境にもよるが、テスト・監査機能は、サイバーセキュリ

ティ計画を実行・管理する責任者から適切に独立しているべきである。当局は、検査・考査、オンサイトその他の監督上の手段、金融機関のテスト結果の比較分析、公的・民間部門共同の演習を通じて、個々の金融機関の相対的なリスクプロファイルと能力のほか、金融セクター全体にかかるサイバーの脅威や脆弱性をより適切に理解することができる。

要素５：インシデント発生時の対応（Response）

インシデント発生時に、以下のような対応をタイムリーにとること。
(a)サイバーインシデントの特性、範囲、影響を評価すること。
(b)インシデントを封じ込め、その影響を軽減すること。
(c)内外の関係者（司法当局、規制当局、その他の当局に加え、必要に応じ、株主、外部委託先サービスプロバイダー、顧客）へ通知すること。
(d)必要に応じて、共同でインシデント対応を図ること。

金融機関は、リスク管理の評価の一環として、効果的なインシデント対応をとることができるよう、インシデント対応方針や他の管理手法を実行しておくべきである。これらの管理手法においては、とりわけ、意思決定の責任の所在を明確にし、エスカレーションの手順を定め、内外の関係者とのコミュニケーションプロセスを構築すべきである。金融機関や当局が、あるいはこれらの主体が共同で行う演習は、より効果的なインシデント対応につながるものである。演習を行うことで、金融機関と当局は、とりうる意思決定が互いの能力 ― 重要なもの、そうでないものも含めた機能・サービス・業務を維持する能力 ― にどのような影響を与えるのかを把握することができる。

要素６：復旧（Recovery）

脆弱性等の改善作業を継続しつつ、速やかに業務を再開すること。具体的には、以下のような対応をとること。
(a)インシデントによる有害な痕跡を除去すること。
(b)システムやデータを正常に復旧し、平常状態を確保すること。
(c)悪用された脆弱性をすべて特定し、軽減すること。
(d)同様のインシデントから防御するため、脆弱性を改善すること。
(e)内外との適切なコミュニケーションを確保すること。

業務の安定性・完全性が確保された後は、重要な経済機能とその他の機能との優先順位付けや、関係当局が設定した目標を踏まえ、迅速かつ有効に業務復旧を行うべきである。金融機関と当局とが、重要な機能・プロセス・業務の復旧にあたり、互いに助け合うことができれば、金融セクターにおける信認の維持は著しく強化される。インシデントが発生する前に、資金調達などの重要な業務・プロセスに関するコンティンジェンシープランを策定し、テストを行っておくことは、より迅速かつ有効な復旧につながり得る。

要素７：情報共有（Information Sharing）

防御の強化や被害の最小化、状況認識の向上や広汎な知識の習得のため、脅威、脆弱性、インシデントの発生、発生時の対応に関する、信頼性の高い実践的なサイバーセキュリティ情報を、内外の関係者（金融セクター内外の金融機関及び当局を含む）とタイムリーに共有すること。

テクニカルな情報 ― 脅威に関する情報や、脆弱性が悪用された際の詳細情報等 ― を共有することにより、金融機関は自らの防御手段をアップデートし、攻撃者の最新の手口を習得することができる。金融機関の間で、または金融機関と当局の間で、あるいは当局の間で、攻撃者が金融セクター全体の脆弱性をどのように悪用する可能性があり、それが重要な経済機能に大きな支障を生じさせ金融の安定を脅かす可能性を持っているのか、についての広範な知見を共有することで、共通の理解を深めることができる。情報共有は重要であることから、金融機関と当局は、情報共有の阻害要因を特定し、それに対処すべきである。

要素８：継続的な学習（Continuous Learning）

サイバーリスクの変化に対処し、資源を割当て、ギャップを特定・改善し、教訓を活かすため、サイバーセキュリティ・ストラテジーとフレームワークを定期的かつ必要に応じて見直すこと（見直しに際しては、ガバナンス、リスク管理の評価、モニタリング、インシデント対応、復旧、情報共有の要素を含むこと）。

サイバーに関する脆弱性・脅威は、それらに対処するためのベストプラクティスや技術標準が進化するのと同じように、急速に進化している。新しいタイプの金融機関や製品・サービスが登場し、外部委託先サービスプロバイダーへの依存度が高まっていくにつれて、金融セクターの構成も時間の経過とともに変化する。金融機関のサイバーセキュリティ・ストラテジーとフレームワークは、金融セクター全体のそれと同じく、脅威やその統御環境の変化に対応し、利用者の意識を向上させ、効果的に資源を配分するために、定期的な見直しとアップデートを必要とする。エネルギーや通信などのその他のセクターは外部依存の対象である。したがって、金融機関と当局は、自らの見直しプロセスの一環として、こうしたセクターの動向を考慮に入れるべきである。