金融セクターのサイバーセキュリティの効果的な評価（Assessment）に関するＧ７の基礎的要素

要旨

サイバーセキュリティのリスクは継続的に拡大しており、金融セクターにおけるサイバーセキュリティの強化に向けてたゆまぬ努力が必要であることを踏まえ、Ｇ７は、ここにサイバーセキュリティの効果的な評価に関する基礎的要素（fundamental elements）を策定する。

2016 年 10 月、Ｇ７は「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」（以下、「Ｇ７ＦＥ」）を公表した。この「Ｇ７ＦＥ」は、民間主体、当局、及び金融セクターにおける効果的なサイバーセキュリティのプラクティスを提供するものである。その目的は、民間・公的主体がサイバーセキュリティの方針・運用のフレームワークを策定・実施することを促し、金融システムのレジリエンス（サイバー攻撃への耐性やダメージからの回復）をより強化することにある。「Ｇ７ＦＥ」は、民間・公的主体がそのリスク管理や組織文化を踏まえ、サイバーセキュリティに関するアプローチを確立しようとするにあたって、その基礎を提供するノンバインディングで俯瞰的な土台である。

「効果的な評価に関するＧ７の基礎的要素」は、「Ｇ７ＦＥ」に示されたプラクティスの適切な実施・評価を行うという点に焦点をあて、「Ｇ７ＦＥ」の有効なプラクティスを促進しようとするものである。「Ｇ７ＦＥ」は、本文書のパートＡ（望ましいアウトカム）及びパートＢ（評価・検証プロセス）を用いることにより、最大の効果が発揮される。具体的には、

・　パートＡは、対策が進んだ主体に見られる５つの**特徴**（**Desirable Outcomes**）を示したものであり、同時に対策が遅れている主体にとってはいわば目標となり得るものである。この Desirable Outcomes は、「Ｇ７ＦＥ」を土台とし、サイバーセキュリティ向上のためのたゆまぬ努力を金融機関等に促しつつ、サイバーセキュリティ対応能力の有効性を評価するための手掛かりを提供するものである（「何を目指すのか」）。

・　パートＢは、評価者が、各主体におけるサイバーセキュリティの強化・推進の進捗状況を評価すべくそのアプローチを決定する際に活用でき

る、５つの**評価要素**(Assessment Components)から成る。この評価要素は、サイバーセキュリティの評価の質を向上させることや、改善プロセスの継続性を保つことを目的としている。この評価要素はまた、評価の範囲・実施、評価結果のコミュニケーションに対して信頼性を付与するものである。同時に、この評価要素は、サイバーセキュリティ評価が効果的であることを説明し、サイバーセキュリティ評価を後押しするものである（「どのように目指すのか」）。

Desirable Outcomes（パートＡ）	評価要素（パートＢ）
１．Ｇ７ＦＥが定着している	１．明確な評価目的の設定
２．組織的な意思決定にサイバーセキュリティの視点が組込まれている	２．メソドロジー・期待値の設定・コミュニケーション
３．Disruption が発生し得るものであるということが認識されている	３．ツールキットの多様性、ツール選択プロセス
４．柔軟なサイバーセキュリティ・アプローチが採用されている	４．明確な結果報告・具体的な改善措置
５．セキュリティ重視の行動を促す組織文化がある	５．評価の信頼性・公平性

「効果的な評価に関するＧ７の基礎的要素」（以下、「基礎的要素」）は、サイバーセキュリティにとって重大なリスク管理上の意思決定にかかる社内外の検討を促進する有用なツールとしての役割を果たす。これらは、例えば取締役会の議論・取締役会による監督に好影響を与えるものである。本「基礎的要素」は子細にわたるもの（prescriptive）ではなく、各主体、監督当局及び独立した評価者のいずれをも啓発しようとするものである。本「基礎的要素」は、規制上の検査・考査、自己評価、及び独立したサードパーティによる検証においても活用できる。さらに、本「基礎的要素」は、当局間及びセクター間のコミュニケーションを促進させ、サイバーリスク管理の有効なプラクティスにかかる技術的・組織文化的なコミュニケーションを活発にさせるであろう。

パートＡ：効果的なサイバーセキュリティの特徴

以下の５つの Desirable Outcomes は、評価者から見て、サイバーセキュリティに関する知見・実施・管理に秀でた金融分野の主体に見受けられる特徴を述べたものである。サイバーセキュリティが多義的であることを踏まえ、これら特徴は幅広いものとなっている。

アウトカム１：Ｇ７ＦＥが定着している

「Ｇ７ＦＥ」は、サイバーレジリエンス強化の初期段階にある主体やより対策が進んだ主体のいずれに対しても、サイバーセキュリティの土台となる要素を提供するものである。

「Ｇ７ＦＥ」は、サイバーセキュリティという課題の特性を反映して、多岐にわたる内容となっている。効果的なサイバーセキュリティは、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維持し(「要素１」)、ガバナンス・プロセスを適応または強化すること（「要素２」）を各主体に求めている。同様に、適切なリスク管理によるリスクの軽減・統御メカニズムを含めたリスク管理のフレームワーク（「要素３」）やさらには効果的なモニタリング（「要素４」）も必要となる。破壊的なサイバーイベントに備えて、手順が明確化され定期的に訓練されたインシデント対応（「要素５」)・復旧(「要素６」)の手順が定着していることが必要である。最後に、情報共有（「要素７」）及び継続的な学習（「要素８」）は、「Ｇ７ＦＥ」の各要素を強化し、全般的なサイバーセキュリティの強化に資するものである。

アウトカム２:組織的な意思決定にサイバーセキュリティの視点が組込まれている

Ｇ７ＦＥの「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)」及び「要素２（ガバナンス)」にあるように、サイバーセキュリティを各主体の通常の意思決定過程に組み入れること（特に、早くからサイバーリスク管理を意思決定過程に含めること）は、各主体の組織全体にわたる戦略的なアウトカムに好影響を与える。サイバーセキュリティは、各主体の業務の中核的な運営プロセスから －概念的にも、設計上も、またオペレーション上も－ 切り離して考えるべきではない。むしろ、新た

な製品・サービスを開発する際や、既存の技術・インフラを活用する業務運営の有効性を評価する際には、サイバーセキュリティは戦略的な考慮を要する重要事項であると認識すべきである。

経営陣や取締役会が積極的に関与している主体では、経営陣や取締役会は、サイバーセキュリティ計画の作成、実施及びその有効性の確認を行っている。脅威・脆弱性に関する情報や自らのリスク選好を把握していれば、短期的にも長期的にも、取締役会・経営陣はリスク管理に関する意思決定・監督・アカウンタビリティを発揮できる。このように、取締役会・経営陣は、従来の法令遵守の観点を越えて、サイバーセキュリティ計画を促進する意思決定を行うことができる。

アウトカム３：Disruption が発生し得るものであるということが認識されている

Ｇ７ＦＥの「要素３（リスク管理の評価）」にあるように、多層防御は重要であり、資産やサービスの可用性（availability）、完全性、機密性を損ねるおそれを減少させる。しかしながら、対策が進んだ主体は、問題を一切引き起こさない環境を保証することなど出来ないことを認識している。各主体の重要な意思決定権者は、disruption（支障）が発生し得ると認識することによって、戦略的な投資選択とは、「Ｇ７ＦＥ」の各要素のバランスを追求するものであることを理解することができる。

こうしたバランスの重要性が理解できない主体は、境界防御（perimeter controls）に過度に依存するあまり、Ｇ７ＦＥの「明確化され定期的に訓練されたインシデント対応（「要素５」）」や「業務再開のための実行可能でテストされたコンティンジェンシープラン（「要素６」）」をおろそかにしてしまうかもしれない。

アウトカム４：柔軟なサイバーセキュリティ・アプローチが採用されている

セキュリティの弱点を突くサイバーの脅威・脆弱性は、いずれも変化・進化し続けている。このため、各主体は、自らのサイバーセキュリティ対応が絶え間なく変化する状況に対処できるよう、現状維持的な思考に陥ることなく、柔軟に順応していくことが必要である。

Ｇ７ＦＥの「要素５（インシデント対応）」及び「要素６（復旧）」にあるように、disruption やストレスの下でも経済機能を維持し続けられるよう、各主体、セクター、セクター横断的、国際的なレベルのいずれにおいても、インシデント対応メカニズムは十分に整備されている必要がある。disruption が金融セクターに及ぼす影響は予測困難であることを踏まえれば、インシデント対応においては、柔軟性が必要である。Ｇ７ＦＥの「要素４（モニタリング）」と相俟って、結果を大きく左右するのは、disruption を速やかに特定し封じ込める敏捷性と経験である。これに関連して、サイバーセキュリティ計画の一環として、改善・学習が継続して進む環境を整えることに重点が置かれるべきである。

アウトカム５：セキュリティ重視の行動を促す組織文化がある

Ｇ７ＦＥの「要素７（情報共有）」及び「要素８（継続的な学習）」にあるように、スキル・行動に絶えず重点を置くことは、組織文化に効果的なサイバーセキュリティを組込むために重要である。

多くのサイバーセキュリティ・インシデントにおいては、手順の不備や人的要素が大きな原因となっている（脆弱なパスワードの活用、ソーシャルエンジニアリング、セキュリティに対する認識不足等）。効果的なサイバーセキュリティ・ストラテジーでは、技術的ソリューションと同じ程度に「人」・「プロセス」の視点が考慮され、投資決定に反映されている。エンドユーザー、従業員や経営陣をターゲットとする訓練・啓発も重要である。

個人がセキュリティと引き替えに利便性を求める世界では、攻撃者の技術の向上と同様に、人間心理の操作も大きな問題である。各人一人ひとりが果たすべき役割があることを理解することが重要である。サイバーセキュリティの効果は、従業員に対する働きかけ・教育を通じ、情報を安全に取扱わせることができるかどうかに左右される。サイバーセキュリティの訓練・啓発によって、技術的な知見の向上だけではなく、行動を変化させる機会も提供することができる。ルールの遵守を求めるよりも、むしろ目に見える本当の変化を目指し、組織文化を効果的に改善することこそが、効果的な訓練の目標である。一番の弱点は人間であるという常識を覆し、その代わりに、人間を最も価値ある資産とするのである。

パートＢ：効果的なサイバーセキュリティ評価の促進

「Ｇ７ＦＥ」を踏まえ、前記の Desirable Outcomes の達成を目指す主体にとっては、自身のサイバーセキュリティ計画の有効性を測定するために、定期的な評価を実施することが欠かせない。

サイバーセキュリティの評価とは、
（１）目指している水準と比較して達成度を判断し、
（２）フィードバックを実施し、要改善部分や改善措置を示すこと、
を目的として、サイバーセキュリティのプラクティスに関する情報を体系的に収集・レビュー・活用しつつ、個別の民間・公的主体または金融セクター全体を検証することを指す。

本「基礎的要素」は、金融セクターにおける各主体が、サイバーセキュリティ評価のフレームワークを構築・実施しようとする場合に検討すべき５つの俯瞰的な要素から構成されている。

要素１：明確な評価目的の設定

評価者は、評価者・被評価者のいずれにも明確な動機付けを与え、アカウンタビリティの向上を促すような評価となるよう、明確な目標を設定すべきである。明確に定義された目的は、継続的な改善・学習をもサポートすることができる。

評価の目的を設定することにより、評価範囲が確定する。評価範囲は、単一の主体（その一部または全部）にフォーカスする場合もあれば、セクター全体に及ぶ場合もある。また、評価範囲は、サイバーセキュリティの評価項目を明確にする。例えば、評価者は、「Ｇ７ＦＥ」のように一連の幅広いプラクティスに照らして評価する場合もあれば、その特定の項目に照らして評価を行う場合もある。

評価範囲を設定する際には、カバレッジ漏れを最小化するとともに、定量・定性双方の基準を組合せるなど、様々な評価要素が考慮される。評価範囲の設定にあたっては、相互依存性・サプライチェーンの関連性に照らして、包含・排除するものを決定しながら、評価の境界（perimeter）が

決定される。

評価目的を設定する際には、評価者は、評価が効率的・効果的に行われるような手法を検討する必要がある。それに加えて、複数の国にまたがる際には、法的なフレームワーク・規制における差異が考慮される。クロスボーダーの金融グループのような大規模な主体に対しては、複数の評価者が評価のアウトプットに対し関心を持つ。それぞれに利害とマンデートを持つ各評価者は、重要な相互依存性を特定し、前もって各自の責任を明確化し、相反する要求が避けられるよう、お互いに連携することが必要である。

要素２：メソドロジー・期待値の設定・コミュニケーション

評価者は、サイバーセキュリティ評価を実施するにあたり、既存のサイバーセキュリティガイダンス・フレームワークを考慮しながら、明確で測定可能な期待値を設定すべきである。こうした期待値は、評価の開始前に、対象となる主体に伝達し、その理解を得るべきである。

評価者は、あらかじめ定められた目的や被評価者の特性に合致したメソドロジーを選択する。サイバーリスクの複雑・ダイナミックな特性を考慮しながら、リスクベース・アプローチを採用することにより、メリハリの効いた（proportionality）評価を実現することができる。

要素３：ツールキットの多様性、ツール選択プロセス

サイバーリスクの複雑・多様な特性を踏まえれば、ツールキット（評価ツール・手法）のポートフォリオが多様であれば、効果的なサイバーセキュリティ評価が可能となる。ツールキットが多様であれば、その中で、それぞれの評価の成熟度やカバレッジの幅・深度に応じた手法を見つけることができる。ツールキットの多様性は、様々な状況に適した各種アプローチを評価者に与える。

サイバーセキュリティ評価のためのツールキットには次のものが含まれるが、これに限定されるものではない。

✓　机上レビュー、自己評価、オンサイトの検証、脅威ベースのペネトレーションテスト、深度ある技術的検証（deep dives）、テーマを絞

った評価、演習

各ツールは、様々に異なるプラクティスに対応するものであり、それぞれには長所・短所がある。複数のツールキットの活用や手法の組合せによって、単一の評価手法に過度に依存するリスクが最小化される。

目的に合ったツールキットを選択するプロセスが重要である。この選択プロセスでは、少なくとも次のような要素が考慮される。

✓ セクター全体から見た各主体の重要性・固有リスク、評価の特性・範囲、評価に費やされるリソース・時間、求められる保証水準

サイバーセキュリティの有効性を評価するためには、方針や手続きの見直しに加え、各主体のサイバーセキュリティ対応能力を積極的に実証するツールを選択することが、評価者には推奨される。

評価のためのツールキットは、常に評価の目的に合致するよう定期的に見直される。個々のツールの適用の可否は、定期的にモニターされ、脅威・業務環境の変化や手元のリソースに合わせて調整される。

要素４：明確な結果報告・具体的な改善措置

サイバーセキュリティ評価は、意思決定・行動の手助けとなる有益なアウトプットをもたらすべきである。このためには、結論が明確であるとともに、将来の行動につながるような具体的な改善措置や個々の課題を特定する必要がある。

主要な結論を出す際には、評価者は、確認されたプラクティス・達成度を整理し、事実から収集された期待値とのギャップや欠点を特定する。評価者は、関連するリスク等や、そのインプリケーションを提示する。全体として、評価のアウトプットは、被評価者にとって有用であり、その意思決定をサポートするとともに、持続的で著しい改善をもたらすようなフィードバックを生み出す。

要素５：評価の信頼性・公平性

しっかりとした評価のメソドロジーを用いれば、異なる評価者間の差異も小さくなり、手法の一貫性も確保することができる。メリハリを効かせることにより、評価は実践的で現実的なものとなる。

評価は、優れたスキルセット・知識を有する人材によって実施される。サイバーリスクの複雑・多様な特性を踏まえれば、関連業務または関連セクターに対する深い知見とともに、ＩＴまたはサイバーセキュリティにおける十分なバックグラウンドがあることが望ましい。個人であれ集団であれ、複数の領域をカバーできる評価者を確保できれば、有益な評価となり得る。さらに、進化する環境に遅れを取らないよう、評価者には、訓練や他の専門性の高い活動を通じて、求められるスキルセットを絶えず更新することが推奨される。

実際の評価や採用されたメソドロジーに対する独立したレビュー（評価者の評価）、評価者間の知見の共有、評価者に対する個別の評価を通じて、評価プロセスの質を保つことができる。評価主体にプロセスの透明性をもたらし、評価範囲・メソドロジー・結果に関する機密性を保証することにより、公平性・中立性が図られる。