金融セクターにおける集団的なサイバーインシデントへの対応及び復旧に関する G7 の基礎的要素（仮訳）

序論と概要

サイバーリスクは、急速なデジタル・トランスフォーメーション、脅威主体の高度化、世界的な緊張の高まり、地政学的動向、及び金融機関、その他の重要な経済分野、各国経済間の情報通信技術（ICT）の相互接続性の高まりによって増大し続けている。重大なサイバーインシデントはますますグローバルな性格を持つようになっているため、効果的なサイバーインシデントへの対応と復旧は、これまで以上に集団的な取組が重要となる。この取組には、国内及び国境を越えた、金融当局、金融機関及び関連するサードパーティのサービス提供者間の協力、ならびに政府当局（例えば、法執行機関、サイバーセキュリティ機関）を含む他のセクターの関係者との協力が含まれる。サイバーインシデントへの対応と復旧のアプローチをグローバルに調整する法域が増えるほど、広範なサイバーインシデントに対してより効果的に対応できる。広範な協力を促進するために、G7 サイバー・エキスパート・グループ（G7 CEG）は、集団的なサイバーインシデントへの対応と復旧（「**CCIRR**」）の基礎的要素を策定した。

公式なものであれ自発的なものであれ、申合せで確定した協調的な CCIRR アレンジメント（以下、「**CCIRR アレンジメント**」という。）は、重要な利点をもたらす。当該利点は、状況認識の向上、適切かつ法的要件に合致したより効果的で適時の情報共有、CCIRR アレンジメントのメンバー（以下、「**メンバー**」という。）間の相互信頼の向上、緩和策の共同開発と普及、危機時のコミュニケーションにおける誤解や対立のリスクの低減を含んでいる。協調的な対応と復旧の取組は、インシデントの影響をより効果的に抑え、金融システムの安定に貢献し、公共の信頼の強化に役立つ。

「金融セクターにおける CCIRR に関する G7 の基礎的要素」は、金融分野を超えて、CCIRR アレンジメントの策定及び改善の指針となり得る、拘束力のないハイレベルな原則である。これらの基礎的要素は、規制上の期待ではなく、むしろ、異なるアプローチ間のより一層の収れんと互換性を促進すると同時に、各法域内の固有の市場と規制に基づき、国や分野、または組織的なニーズに合わせた柔軟性確保と調整を可能にすることを目的としている。

「金融セクターにおける CCIRR に関する G7 の基礎的要素」は、3 つの包括的な柱から構成される。

I. CCIRR アレンジメントの**策定**
II. CCIRR アレンジメントの**運用**
III. CCIRR アレンジメントの**維持及び検証**

基礎的要素の柱は、金融安定理事会（FSB）が公表したサイバーインシデントへの対応及び復旧の実務と同じ構造を有しており、3つまたは4つの要素で構成される。

I. CCIRR アレンジメントの策定

CCIRR アレンジメントは、ガバナンス体制、CCIRR のための調整プロトコル、及び対応計画が他の関連する枠組みとどのように相互作用するかを明確に規定する。

要素1：ガバナンス

明確化された目的、適用範囲、適切なグループ構成、及び規定された役割を伴う、強固なガバナンスを確立する。

ガバナンスは、CCIRR アレンジメントの策定、運用、維持及び検証のための基本的な指針を示すために重要である。強力なガバナンスは、効果的な意思決定を可能にし、共通の目標を達成するための鍵となる。

目的への合意は、CCIRR アレンジメントの明確な方針、目的及び焦点を提供することに役立つ。目的は、全てのメンバーが CCIRR アレンジメントについて達成することを理解し、メンバーが効果的に、行動を調整し、業務の優先順位付けを行えるようにする。また、目的は、進捗状況を評価できる測定可能な目標が定められている場合には、より良い意思決定が可能となる。

CCIRR の対象となるインシデントの種類を含め、メンバー間での共通の理解を確保することが不可欠であるため、適用範囲はもう一つの重要な要素である。適用範囲は、CCIRR アレンジメントの閾値（発動基準を含む）、及び発動する場合にどの側面を対象とするか（例えば、技術情報の交換、対外コミュニケーションの調整、金融安定の維持手段に係る議論）を規定し得る。適用範囲は、また、想定されるメンバーのスキルセット（例えば、サイバーセキュリティ/デジタル・オペレーショナル・レジリエンスの専門家、ビジネスの専門家、事業継続管理者）や役職のレベルを含め、想定されるメンバーを決定する上で大きな影響がある。

グループ構成に関して、メンバーの候補は、公的セクターと民間セクターの両方に存在し得る。公的セクターにおいては、メンバーの候補は、それぞれの組織の目的（例えば、金融機関の監督、金融安定の維持、またはサイバーセキュリティの向上など）

に応じて決定され得る。公的セクターの役割である金融監督、オーバーサイトまたは破綻処理と、潜在的に果たし得る役割である調整役または触媒的な推進役の両者をCCIRR アレンジメントにおいて区別しておくことは、信頼性の高い環境でメンバーが円滑な情報共有するうえで有益であり得る。

民間セクターからのメンバーの候補には、金融セクターにおいて極めて重要な金融機関及び関連するサードパーティのサービス提供者の双方の代表者が含まれ得る。例えば、規模や相互接続性の程度及び提供されるサービスと金融セクターの機能との関連性などの要素が、関連要素となり得る。すべてのメンバーの指定された最新の連絡先を保持することは有益である。インシデント発生時のより広範な協力を促進するために、他の関連するフォーラムの最新の連絡先リストを維持することも有益である(「要素3:他の枠組みとの相互運用性」も要参照)。グループの規模に関しては、対象範囲と機敏性のバランスをとることが有益である。大規模なグループは、より広い対象範囲をカバーし、サイバーインシデントの間に主要な利害関係者が排除されるリスクを低減する。逆に、小規模なグループは、積極的な参加を奨励し、より高い機密性を維持しながら、迅速な調整と意思決定を通じて高い機敏性を実現できる。

最後に、ガバナンス体制は、意思決定プロセス、リーダーシップ(例えば、議長の交代)、内部の事務局、危機対応調整チームまたは技術的支援などの主要な支援機能、ならびにこれらの機能を維持するための規則など、業務の進め方ならびに主要な組織的側面及び役割を規定することもできる。

要素2:調整プロトコル

効果的な CCIRR アレンジメントを確保するための仕組み及び手続を確立する。

CCIRR アレンジメントには、インシデント発生時に体系的な対応を可能にする、明確で制度化された規則、仕組み及び手続(「**調整プロトコル**」)が含まれる。また、CCIRR アレンジメントは、これに定められたガバナンスと整合的な対応及び復旧の方略を定めることができる。

調整プロトコルには、特に、CCIRR アレンジメントの適用範囲と整合的な発動、エスカレーションとデスカレーション及び解除のための明確な基準、発動条件又は閾値を含めることができる。これらの基準には、(拘束力のない)定量的基準及び定性的基準の双方を含めることができる。

さらに、調整プロトコルは、適切な場合に機密性や匿名性を確保する情報共有のアレンジメント、ならびにグループ活動を強化する他のツールの利用を通じて、内部のコミ

ュニケーションおよび調整を支援できる。例えば、調整プロトコルは、メンバーが情報を収集・共有・統合・抽出するための情報交換プラットフォームならびに会議ツール及び警戒システムを活用し得る。さらに、調整プロトコルでは、メンバー組織間で最高の意思決定レベルまで情報をエスカレーションする必要があるシナリオを考慮できる。

既存の調整枠組みを活用してカスタマイズすることにより、調整プロトコルの設計に役立てることができる。

要素3：他の枠組みとの相互運用性

円滑な調整を確実なものとし、他の関連するフォーラムとの相乗効果を促進する。

サイバーインシデントの影響範囲はメンバーに限定される可能性が低いため、他の関連するフォーラムとの調整及び相互運用性を確保することは有益であり得る。そのような調整及び相互運用性のための対応計画は、複数のフォーラム間での責任の重複及び、目標あるいは優先事項の相反を見出し、その問題を潜在的に緩和し得る。

CCIRR アレンジメントは、情報共有が適切かつ合意されたプロトコルに従って管理された状態であることを確保しつつ、インシデント時により広範な協力を促進するために、適切な場合には、国内外の他のフォーラムとの連携を規定できる。共通の用語集、標準化された情報共有テンプレート、または他のフォーラムに参加するオブザーバーの指名などを通じて整理された枠組みは、調整を強化できる。さらに、メンバーが同時に発動している複数の枠組みに参画している場合、各メンバーは、スタッフレベルでの資源配分を考慮できる。連絡窓口を一元化する場合には、様々な関連フォーラムに参加する際であっても一元的な危機管理を行える。この場合、ボトルネックや単一障害点に起因するリスクをもたらし得るが、適切な事前計画と人員配置を通じて対処できる。

全般的な準備体制と調整を強化するために、CCIRR アレンジメントは、セクター横断的かつ国際的なシナリオに適用可能な手続を含み得る。

II. CCIRR アレンジメントの運用

CCIRR アレンジメントは、強靭な対応手段と方法を規定し、明確で効果的かつ適時の危機時のコミュニケーションを準備する。

要素4：対応と復旧のためのツール及び方法

想定される対応と復旧のツール及び方法を事前に特定し規定し確立する。

インシデント時には、効果的かつ適時な対応と復旧が極めて重要である。すべての状況を予測できるわけではないが、起こり得るシナリオとその潜在的影響を考慮することにより、調整プロトコルに使用可能なツールと方法の準備、組み込み、即時使用が可能になる。これらの対応と復旧のツールと方法では、以下を考慮することができる。

- 重要な業務/重要な金融サービスへの影響：方法及びツールは、不可欠なサービスの障害を最小限に抑え、重要な業務の安全な復旧を確実にするように設計され得る。
- 関連するサードパーティのサービス提供者のリスク：対応及び復旧措置は、関連するサードパーティのサービス提供者から発生したインシデントに適応させる必要があり得る。そのような危機は、より急速に拡大し、波及し得るためである。
- 切断、再接続及びデータの復元：ベストプラクティスは、システムの安全な切断及び再接続、ならびにデータの信頼できる復元の指針となり得る。

FSB の「サイバーインシデントへの対応と復旧のための効果的な実務」は、想定される対応及び復旧のためのツール及び方法のための有用な参考資料である。

要素５：危機時のコミュニケーション

インシデントが発生した場合に関連するステークホルダーへの適時かつ効果的なメッセージの発信を確保するためにメンバー間で危機時のコミュニケーション戦略を確立し、誤情報や偽情報、及び顧客とのコミュニケーションを管理するための戦略を準備する。

インシデント後の明確で効果的かつ適時な危機時の対外コミュニケーションは、市場とその参加者へのさらなる影響を防ぐために重要である。コミュニケーション戦略は、対外コミュニケーションの一般的なルールを事前に規定できる（例えば、声明を発表する前にメンバーに通知すること、または本人の同意なく他のメンバーについてコミュニケーションすることを控えることなど）。さらに、危機時のコミュニケーションを調和させる範囲（例えば、時期、テンプレート、共通する要素を共有するためのプラットフォーム）を規定できる。異なるシナリオを事前に準備することにより、インシデント時の明確で効果的かつ適時のコミュニケーションを促進できる。危機時のコミュニケーション戦略は、適切な対象者への伝達に適したツールやメディアを駆使した危機時のコミュニケーションを策定・発信するための主要な役割と責任を定め、割り当てることができる。CCIRR アレンジメントにコミュニケーションの専門家を直接参加させることは、危機時のコミュニケーションを CCIRR に確実に含めるために推奨される。

要素６：CCIRR アレンジメントのレジリエンス

代替的な解決策を用意し、CCIRR のための十分なリソースを確保することにより、CCIRR アレンジメントのレジリエンスを確保する。

情報及び通信システムが遮られる危機時（例えば、通信遅延または停電）には、対応及び復旧のためのツール及びコミュニケーション手段も損なわれ得る。メンバーは、技術的な代替手段や機能縮小モードなどによる最小限のレベルの調整を確保するために、代替ツールや回避策を実装することにより、危機のシナリオに備えることができる。

平時にこれらの代替手段を定期的に検証することは、その有効性の維持に役立つ。

Ⅲ. CCIRR アレンジメントの維持及び検証

定期的な検証、演習及び継続的な改善は、CCIRR アレンジメントを強化する。さらに、CCIRR アレンジメントは、確立された信頼関係及び脅威インテリジェンスによって支えられる場合、より効果的に機能する。

要素７：検証と演習

CCIRR アレンジメント及び調整プロトコルの実効性を確保するため、定期的な検証及び演習を実施する。

CCIRR アレンジメント及び調整プロトコルの定期的な検証は、その有効性に寄与し、また、メンバーがその運用方法に精通するのに役立つ。さらに、検証は、ツール（代替手段を含む）及び起動/警戒ならびにその他のアレンジメントの側面が適切に機能するかを確認できる。

シミュレーション演習は、ストレス下を想定した現実的な検証と訓練を提供し、先見性と準備体制を強化するため、特に有益である。加えて、このような演習は、メンバー間の結束を強化し、調整プロトコルを含む CCIRR アレンジメントを精緻化する機会を提供する。その他の種類の演習(例えば、机上演習または運営体制の検証〈logistic test〉)も、広範なシミュレーション演習の準備を含め、有益となり得る。G7 CEG は、演習プログラムの設計におけるベストプラクティスに関するガイダンスを公表した。

検証及び演習の事後評価報告は、得られた教訓及び改善の余地のある領域を特定するために有益である。教訓は、適切な場合に、他のグループと共有することにより、学びを比較し、ベストプラクティスを共有し、共通の対応及び復旧の成果をもたらすこ

ともできる。

要素8：継続的改善

確立された CCIRR アレンジメントを継続的に改善し、メンバーの平時の活動を維持する。

CCIRR アレンジメント及びその基盤となるプロトコルの有効性を維持・向上させ、長期的な妥当性を確保するために、CCIRR アレンジメントとその基礎となるプロトコルを定期的に見直し、更新する(例えば、インシデント後の報告とその中で推奨される行動と修復措置に基づいて、過去のインシデントと演習から学んだ教訓を理解して取り入れ、政策、規制、要件の将来の進展を見越す)ことは有益である。体系化されたレビュー・プロセスは、これらの取組を支援し、危機ではない平時にも活動を維持するために重要である。改善の機会や将来的に開発する領域を見出すことにメンバーが関与することは、プロトコルに対する責任感の共有と方向性の一致を育む。これにより、プロトコルの改善と運用に積極的に貢献するメンバーの意欲と関与が増す。さらに、作業部会の設置（例えば、演習の設計と実施のため）、定期的な会合、または共同プロジェクトなど、平時における継続的な関与を促進する戦略は、グループの結束を維持し、継続的な妥当性を確保し、将来のインシデントに対する備えを強化するのに役立つ。

要素9：継続的な脅威インテリジェンス

脅威インテリジェンスの能力を構築・強化する。

脅威インテリジェンスに関連する CCIRR アレンジメントの内外での積極的かつ持続的な協力は、変化する脅威動向に対処する適応能力を維持するうえで重要である。脅威インテリジェンスと法域または産業セクターの特定部分に影響を及ぼす新たな動向（例えば、新技術が及ぼし得る影響）の情報を交換することは、メンバーが将来の脅威と困難に備えるうえで有益である。脅威インテリジェンスは、CCIRR アレンジメントのさらなる発展の指針となり、演習活動を活発化させ得る。

要素 10：信頼されるコミュニティ

メンバーの相互信頼関係を醸成し、維持する。

インシデント発生時の効果的な協力は、メンバーが互いを知り、信頼している場合に強力なものとなる。信頼できるパートナーのネットワークを育成し、人々が率直に話すことを快適に感じる環境を醸成するために、妥当かつ適切な場合には、データ/情報

を共有し機密性と匿名性を確保するための明確な規則を定めることが有益であり得る。これは、例えば、情報共有の取決め及び/または共有された情報の機密レベルを示す分類システム（例えば、TLP〈Traffic Light Protocol〉、チャタムハウス・ルール）を確立することにより達成できる。この分類システムは、情報共有に適用されるメンバーの各法域における法的制約またはその他の制約を考慮している。

危機時に機微情報を共有するために必要とされる信頼を育むために、演習、脅威インテリジェンスの交換、または平時における他の作業部会の活動などを通じて、定期的な接点を持つことも有益であり得る。特に、対面会議は、メンバー個人が互いをより深く理解し、コミュニケーションを強化することを可能にする。