BIS 決済・市場インフラ委員会および証券監督者国際機構による市中協議報告書
「金融市場インフラのためのサイバー攻撃耐性に係るガイダンス」
Guidance on Cyber Resilience for Financial Market Infrastructures

エグゼクティブ・サマリー[1]（仮訳）

○ 目的：本文書の目的は、金融市場インフラ（FMI[2]）に対し、ガイダンスを提供することによって FMI のサイバー攻撃耐性を強化することである。FMI の安全かつ効率的な運営は、金融安定及び経済成長を維持・促進するためには極めて重要である。適切に管理されない場合、FMI は流動性の歪みと信用損失のような金融ショックの原因になりうるほか、それらのショックが国内・国際金融市場に伝播していくチャネルになりうる。この意味では、サイバー攻撃耐性を含む FMI のオペレーション上の耐性レベルは、金融市場および経済の全体におけるサイバー攻撃耐性を創造する決定的な要素になりうる。

○ 概要：本ガイダンスは、「主要なリスク管理要素」5 項目および「リスク管理を効果的に機能させる要素」3 項目を解説する章で構成されている。「主要なリスク管理要素」とは、ガバナンス（governance）、特定（identification）、防御（protection）、検知（detection）、対応と復旧（response and recovery）であり、「リスク管理を効果的に機能させる要素」とは、テスト（testing）、状況認識（situational awareness）および学習と進化（learning and evolving）である。サイバー攻撃耐性に係る目標を達成するためには、FMI が各分野に横断的に取組むことで相互に強化されるため、総合的に検討するべきである。

○ FMI 原則との関係：本文書は、CPMI-IOSCO 「金融市場インフラのための原則」（FMI 原則）のうち、主に、ガバナンス（原則 2）、包括的リスク管理制度（原則 3）、決済のファイナリティ（原則 8）、オペレーショナル・リスク（原則 17）と FMI 間リンク（原則 20）に対する補足的なガイダンスを提供するものである。本ガイダンスは FMI 原則の枠を超えた追加的な規則を設定するものではなく、サイバー攻撃による脅威が金融安定に与えるリスクを限定的とするべく、FMI がサイバー攻撃耐性を強化するために取組むべき準備や手段の詳細を提供するものである。

○ 関係者・市場等との関連性：本ガイダンスは、FMI を直接的な対象としているが、FMI が参加者や関係者に対して積極的に働き掛け、サイバー攻撃耐性に係る目的と対応に対する理解と支持を促進することは重要である。金融システムの緊密な相互リンクおよび相互依存性を踏まえると、FMI 単独のサイバーセキュリティ実務が適切であっても、必ずしも市場全体のサイバー攻撃耐性を確保できる訳ではない。特に、市場全体のサイバ

[1] 専門用語については p.23 の用語集を参照。
[2] 本ガイダンスにおける「FMI」とは、2012 年 4 月に CPMI-IOSCO が公表した FMI 原則と同様に、システミックに重要な資金決済システム、証券集中振替機関（CSD）、証券決済システム（SSS）、清算機関（CCP）及び取引情報蓄積機関（TR）を指している。

ー攻撃耐性は FMI 単独だけではなく、FMI と相互に連結している他の FMI やサービスプロバイダー、参加者におけるサイバー攻撃耐性にも依存している。

○ 協力：FMI とその関係者がそれぞれサイバー攻撃耐性を強化しようとする場合、有効な解決には、相互の協力が必要不可欠であろう。FMI 及びその関係者は、こうした協力の成果を、個別または総合的な戦略的計画に踏まえるべきである。サイバー攻撃耐性に係る戦略の設計について強調していく努力は、タイムリーかつ効率的により強化された戦略の構築をもたらしうる。システムやプロセスの設計時および見直し時に、サイバー攻撃耐性に係る高い目標を織り込むことによって、より強固なサイバー攻撃耐性を構築することができる。FMI におけるサイバー攻撃耐性は、金融市場の安定というより広い目的をサポートするものであるほか、清算・決済のプロセスにおける相互依存性の大きさを踏まえると、当局間の協力が、適切な場合において、当局による FMI やその関係者に対するオーバーサイトおよび監督の方向の整合性を考慮する上での一助となる可能性があることを認識しながら、当局間において協調することは重要である。また、金融監督当局と FMI は、テクノロジー企業やその他の企業に対し、効率的かつ実効的なソリューションを特定・策定するための協力を呼びかけることが必要となろう。

○ ガバナンス：FMI が直面する他のリスクを有効に管理することと同様に、健全なガバナンスは重要である。サイバー・ガバナンスとは、サイバーリスクを管理するための取組みを、FMI 自身が構築、導入およびレビューする取組みを指している。有効なガバナンスは、広く金融安定という目的を支えると共に、FMI におけるオペレーションの安全性および効率性を優先した、明瞭かつ包括的なサイバー攻撃耐性の枠組みから始めなければならない。この枠組みでは、サイバー攻撃耐性の目標を定め、かつサイバーリスクを管理するための人員、プロセス、テクノロジーに対する要求を明確にしなければならない。また、この枠組みは、関係者間のタイムリーなコミュニケーションと協力を含むものでなければならない。さらには、FMI の経営陣や役員の役割や責務が明確に決められていることが重要である。経営陣や役員は、全てのスタッフや関連サービスプロバイダーがサイバー攻撃耐性に重要な責任があると認識するカルチャーを創り出す義務がある。この章では、FMI のサイバー攻撃耐性に係る枠組みの基本的要素や、FMI のガバナンスに係る取組みのあり方などを纏めている。

○ 特定：FMI のオペレーションに係る障害の発生は、金融の安定に悪影響を及ぼすことから、FMI が自らの最重要機能およびそれを支える情報資産を特定することが重要である。この章は、FMI が如何にビジネスのプロセス、情報資産、システムへのアクセス、外部依存性を特定し分類すべきかについて概説する。これにより FMI が、自身の内部状況、エコシステム内の企業との間のサイバーリスク、そして、サイバー攻撃耐性に係る仕組みを設計・導入する際にどのように関係者と調整しうるかという点についてより良く理解することに役立つ。

○ 防御：サイバー攻撃耐性は、自らの資産及びサービスの機密性、正確性及び利用可能性を保護する有効なセキュリティ・コントロールによって決められる。この章は、FMI に対し、先進的なサイバーセキュリティに沿った適切かつ実効的なコントロールの導入、潜在的なサイバーリスクによる影響を防止または限定するためのシステムとプロセスの設計を求めている。

○ 検知：異常事態の発生や、潜在的なサイバー攻撃の可能性を検知する FMI の能力は、堅固なサイバー攻撃耐性を構築するために不可欠な要素である。早期に検知することにより、FMI は潜在的なサイバー攻撃による侵害への対応策を講じるための有用なリードタイムを確保でき、実際の侵害に対する抑制策を積極的に講じることができる。不可視かつ高度に洗練された性質を持つサイバー攻撃による不正侵入が、複数のエントリー・ポイントに起きうることを踏まえると、広範囲に亘って異常な動きをモニタリングする優れた能力が必要である。この章では、FMI がサイバー事案の検知に用いるモニタリングとプロセスのツールについて概説する。

○ 対応と復旧：金融市場の安定性は、FMI が決済期限（遅くとも決済日の終了まで）に決済が完了できる能力に依存しうる。FMI は、例え極端であるが現実に起こりうるシナリオにおいても、サイバー攻撃による障害（cyber disruption）発生後 2 時間以内に不可欠な業務を安全に再開し、障害発生日の終了までに決済が完了できるよう、自身のシステムとプロセスを設計・テストすべきである。金融監督当局は、サイバー攻撃耐性に係る目標の達成にあたり FMI が直面する難題を認識しているが、現状および新興の実務とテクノロジーがその目標を達成するための確実な選択肢となりうるとも認識している[3]。さらに、再開の目標を達成する論理的根拠は、その達成に向けた難題に左右されるべきではない。業務継続計画は関連する目標を達成するためには欠かせない。この章では、FMI がサイバー攻撃を抑制し、再開及び復旧するためには如何に対応すべきかについてガイダンスを提供する。

○ テスト：サイバー攻撃耐性に係る枠組みの全ての要素は、枠組みの採用以後、その実効性について綿密にテストされなければならない。実効的なテスト体制は、サイバー攻撃耐性に関して定めた目標と現状の乖離を特定するための気づきをもたらす。また、FMI のサイバーリスク管理者に対し、信頼できる有意義なインプットを提供するものである。この章では、FMI のテスト・プログラムに含まれるべき分野やテスト結果が、如何にサイバー攻撃耐性に係る枠組みの改善に利用できるかについて、ガイダンスを提供する。

○ 状況認識：良好な状況認識は、サイバー攻撃を理解し、サイバー攻撃発生前に阻止する FMI の能力を強化させる。また、阻止できなかったサイバー攻撃についても、効果的に検知、対応、復旧させる能力を強化することができる。特に、サイバー攻撃による脅威

[3] CPMI による FMI へのインタビューを通じて得られた潜在的な解決策については、CPMI の報告書「FMI のサイバー攻撃耐性」セクション 4.3.3 参照。

の状況に対する鋭い認識は、FMI が自身の重要なビジネス機能の脆弱性をより良く理解し、適切なリスク削減策を採用することを促進することができる。この章では、サイバー攻撃による脅威の状況について如何に事前にモニタリングができるか、脅威に関する実用可能な情報の収集、有効活用を如何に行うか、また、これによりどのようにサイバー攻撃耐性の構築に関する有効なリスク評価、戦略の方向性、リソース配分、プロセス、手続き、コントロールを実施するかについて、ガイダンスを提供する。またこの章では、FMI 自身とエコシステムのサイバー攻撃耐性を強化するため、FMI が業界内外の信頼できる関係者との情報共有と協力に積極的に参加することの重要性についても強調している。

○ 学習と進化：最後の章は、サイバーリスクの進化やそれに伴うリスク回避策の変遷に連れて、適応性の高い枠組みを構築することの重要性を強調する。FMI は、組織の全ての職員レベルにおいて、サイバーリスクの認識を文化として植え付けることを目指すべきであり、サイバー攻撃耐性に係る方針の継続的な再評価と改善を示していくべきである。