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）

○ 背景：金融市場インフラ（FMI[2]）の安全かつ効率的な業務運営は、金融の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、金融システム及び経済全体における攻撃耐性の決定的な要素となりうる。

○ 目的：本文書（本ガイダンス）の目的は、FMI に対し、そのサイバー攻撃耐性を強化するためのガイダンスを提供することである。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）及び FMI 間リンク（原則 20）に関連して、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の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及び手段の詳細を補足的に提供するものである。

○ 概要：本ガイダンスは、「主要なリスク管理要素」５項目及び「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）及び学習と進化（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。

○ 広範な関連性：本ガイダンスは、FMI を直接的な対象としているが、FMI がその参加者やその他の利害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。金融システムにおける緊密な相互接続を踏まえると、FMI のサイバー攻撃耐性は、FMI と相互に接続している他の FMI、サ

[1] 専門用語については別添 A 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。

ービスプロバイダー及び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 とその利害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。サイバー攻撃耐性に係る戦略の設計について協力していく努力は、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。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おいて考慮すべきである。FMI におけるサイバー攻撃耐性は、金融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及び監督の方向の整合性を考慮する上での一助となるであろう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解決策を特定・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、FMI 自身が構築、実施及びレビューするための取組みを指している。有効なガバナンスは、広く金融の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及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。この枠組みは、サイバー攻撃耐性に係る戦略により導かれるとともに、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、利害関係者との効果的な協力が可能となるようタイムリーなコミュニケーション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文化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及び優先順位をもって不正アクセスから守られるべき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利害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、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に、先進的なサイバー攻撃耐性及び情報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及び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。

○ ２時間以内の業務再開（以下、２時間の RTO または 2hRTO という。）：金融の安定は、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（disruption）発生後２時間以内に重要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。重要な業務を２時間以内に再開する能力如何にかかわらず、障害に対処する場合、FMI は自身又はそのエコシステムに対するリスクが増幅しないよう、障害発生日の終了までに決済が完了することが不可欠であることを勘案した上で、再開を行うかどうか判断する必要がある。また、FMI は再開目標が達成できないシナリオに対する計画も立てるべきである。金融監督当局は、サイバー攻撃耐性に係る目標の達成に当たり FMI が直面する難題を認識しているが、現状及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実施可能な選択肢となりうるとも認識している。[3] さらに、再開の目標を策定する根拠は、その達成に向けた課題に左右されるべきではない。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諸要素は、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。健全なテスト体制は、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

[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、BIS 決済・市場インフラ委員会による報告書「FMI のサイバー攻撃耐性」セクション 4.3.3 参照。

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特定･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利害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に伴って効果的な管理が可能となるような、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。

○ 本ガイダンスの適用：本ガイダンスの実施に当たって、FMI は、リスクベース･アプローチを採用することが期待される。FMI は、適用される法令及び規則と整合的に本ガイダンスを実施する必要がある。組織上の違いと共に、適用される法令及び規則によって、望ましい結果を達成するために本ガイダンスがどのように採用されるかが決定される。FMI は、関係する利害関係者と協働して、サイバー攻撃耐性の向上のために本ガイダンスを考慮したうえで、必要な措置を迅速に講じるべきである。また、FMI は、本ガイダンスの公表後 12 か月以内に、本ガイダンスの第６章において議論された２時間以内の業務再開という目標を確保するため、対応能力を向上させる具体的な計画の策定を行うべきである。