第 18 回　決済システムフォーラム

2018 年 2 月
日本銀行決済機構局
浜野　隆

決済インフラのサイバーリスクに関する国際的な議論

目　次

１．　国際的な議論の流れの概観

（１）歴史的経緯

1990 年　CPSS 発足（2014 年に CPMI に改組）

1998 年　主要国中銀が SWIFT に対する国際協調オーバーサイトの枠組みを構築

2001 年　CPSS が「資金決済システムのためのコアプリンシプル」、CPSS/IOSCO が「証券決済システムのための勧告」を公表

2004 年　CPSS/IOSCO が「清算機関のための勧告」を公表

2007 年　SWIFT の国際協調オーバーサイトのための基準（High Level Expectations）を策定

グローバル金融危機（2009 年～）

2010 年　CPSS/IOSCO が上記国際基準の包括的な見直しに着手

2012 年　CPSS/IOSCO が「金融市場インフラのための原則（PFMI）」を公表

2014 年　CPMI が「金融市場インフラのサイバーレジリエンス」報告書を公表

バングラデシュ中銀不正送金事件（2016 年 2 月）

SWIFT がカスタマー・セキュリティ・プログラムを開始（2016 年 5 月）

2016 年　CPMI/IOSCO が「金融市場インフラのサイバーレジリエンスガイダンス」を公表

2017 年　CPMI が「大口資金決済システムのエンドポイントセキュリティ」に関する市中協議（9～11 月）

2018 年～　**各種の取組みが実施フェーズへ**

（２） サイバーセキュリティ・サイバーレジリエンスに関する国際基準の潮流

・サイバー攻撃の増加・高度化を受けて、多くの国際基準設定主体がサイバーリスクへの取組みを強化。

・決済インフラのサイバーリスクへの取組みは、主として国際基準設定主体である CPMI と IOSCO が担っているほか、SWIFT のユーザーセキュリティ強化策は、主要国中銀の国際協調オーバーサイトの枠組みの下で進められている。

・決済インフラの国際基準においては、サイバーリスクは比較的新しい概念。

—— 「コアプリ」（2001 年）、「証券決済システムのための勧告」（同年）、「清算機関のための勧告」（2004 年）には、サイバー攻撃、サイバーリスクといった用語はみられない。

・2012 年公表の「FMI 原則」では、オペリスクの顕現化の要因として、「サイバー攻撃」に明示的に言及。

・サイバーリスクへの対処策については、「サイバーセキュリティ」の語が使われるが、決済インフラについては、その一内容である「サイバーレジリエンス」が強調されることが多い。

・サイバーレジリエンスは業務継続計画（BCP）に近い概念であり、当日中の決済の結了が求められる決済インフラにとって特に重要性が高い。

⇒　決済インフラには、「サイバーリスクの顕現化回避」と「迅速な復旧（決済の結了）」が求められる。

・わが国政府のサイバーセキュリティ戦略でも、重要インフラのサイバーセキュリティを重視。

サイバーセキュリティ戦略本部「サイバーセキュリティ 2017」（平成 29 年 8 月 25 日）抜粋 2.2 重要インフラを守るための取組み 「・・・・・重要インフラサービスを安全かつ持続的に提供できるよう、重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、情報セキュリティ対策に関する取組を推進・・・・・」

・国際的な議論では、決済インフラのサイバーリスクは、オペレーショナルリスクの一場面と位置づけられるのが一般的であり、「FMI 原則」もオペレーショナルリスクの一環として整理。

・もっとも、サイバー攻撃の特殊性から、通常のオペレーショナルリスクとは異なる配慮が必要となり得る。例えば、CPMI「サイバーレジリエンス報告書」（2014 年）は、「サイバー攻撃には、物理的な攻撃とは別の対処が必要」と指摘。

> Given their sophistication, range of motivations and pervasive scope, cyber attacks can present unique challenges to FMIs' operational risk management frameworks. In some cases, the risk management and business continuity protocols used in the event of physical attacks are ineffective or could actually exacerbate a cyber attack.

・こうした配慮から、CPMI/IOSCO は、FMI 原則を補完する観点から、サイバーレジリエンスに関するガイダンスを策定・公表（2016 年）。

・また、近時は、決済インフラのエコシステム全体のサイバーセキュリティへの関心が高まりをみせており、CPMI は、エンドポイントセキュリティに関する取組みを進めている（2016 年～）。

２． サイバーリスクに関する国際基準の概要

（１）「金融市場インフラ（Financial Market Infrastructures）のための原則」

（位置付け）

・CPMI/IOSCO の「金融市場インフラのための原則」（FMI 原則）は、システム上重要な資金決済システム（SIPS）、証券決済システム（SSS）、証券集中保管機関（CSD）、清算機関（CCP）、取引情報蓄積機関（TR）に適用されるほか、他の決済インフラの安全性・効率性のための指針ともなる。

―― FMI向けの24の原則と、中央銀行・市場監督者等の関係当局向けの5つの責務により構成。

・わが国では、FMI 原則は、金融庁の監督指針や日本銀行の「オーバーサイト基本方針」の基盤。

日本銀行「日本銀行による金融市場インフラに対するオーバーサイトの基本方針」（2013 年 4 月実施）

金融庁「清算・振替機関等向けの総合的な監督指針」（2013 年 12 月～。累次改定）

（FMI 原則におけるサイバーリスク）

・FMI原則は、従来の決済システムに関する国際基準を包括的に見直したものであり、これまでの基準運用の経験のほか、グローバル金融危機から得られた教訓やその後の店頭デリバティブ市場における金融市場インフラ面での改革などを踏まえ、多くの点で従来の基準に比べ要求水準を引き上げる内容。

・オペレーショナルリスク に関する原則17は、業務継続体制の底上げの観点から、「枢要なITシステムについては、障害発生から2時間以内の復旧を可能とすること」を明記。

・FMI 原則は、オペレーショナルリスクの要因の一つとして、「サイバー攻撃」に明示的に言及。

> ***Identifying sources of operational risk***
>
> 3.17.2. An FMI should actively identify, monitor, and manage the plausible sources of operational risk and establish clear policies and procedures to address them. （中略）an FMI should assess the evolving nature of the operational risk it faces on an ongoing basis (for example, pandemics and **cyber-attacks**), so that it can analyse its potential vulnerabilities and implement appropriate defence mechanisms.

（２）CPMI サイバーレジリエンス報告書

（位置付け）

・CPMI は、2014 年に「サイバーレジリエンスに関する報告書（Cyber resilience in financial market infrastructures）」を公表。

・同報告書は、FMI に対するサイバー攻撃の増加・高度化を踏まえて、FMI の直面するサイバーリスクの現状とそれへの対応力を調査・分析。

・基本的な問題意識は、FMI はサイバー攻撃を受けても、「早期に復旧し、当日中に決済を完了する必要がある」というもの。

・同報告書は、FMI 原則 17 に加えて、当局の協調的な行動とガイダンスの必要性を示唆。

（報告書の概要）

・金融市場インフラ（FMI）は、サイバー攻撃を受けた場合にも「FMI原則」が求める「2時間以内の復旧」、および「当日中の決済の完了」を確実にする観点から、以下の3つの側面で対応。

（1） サイバーレジリエンスの射程（サイバーリスクのシナリオ）として、①情報の機密性に対する侵害、②FMI が提供するサービスの可用性に対する侵害、③FMI の中核的な情報やシステムの正統性に対する侵害を想定。

（2） サイバーセキュリティのガバナンスは、IT技術に関するものに止まらずに、人員、手続、関係者とのコミュニケーションをカバー。

（3） サイバーレジリエンスを確保する手段として、サイバー攻撃の発生を防止し、検知し、攻撃後の復旧のための様々な手段を装備。

（３）CPMI/IOSCO「サイバーレジリエンスガイダンス」

・ CPMI/IOSCO は、FMI 原則を補完する観点から、2016 年 6 月に「サイバーレジリエンスに関するガイダンス（Guidance on Cyber Resilience for Financial Market Infrastructure）」を公表。

・同ガイダンスは、原則 17 を中心に、サイバーレジリエンスの観点から、FMI 原則を補完するもの。

（「サイバーレジリエンスガイダンス」の対象となる原則）
原則 17：オペレーショナルリスク
原則 2：ガバナンス
原則 3：リスクの包括的な管理のためのフレームワーク
原則 8：決済ファイナリティ
原則 20：FMI 間のリンク

・主たる問題意識は、FMI 原則により求められる「2 時間以内の復旧」と「当日中の決済の完了」（決済ファイナリティの確保）。

・同ガイダンスは、サイバーリスク管理面の要諦（primary risk management categories）として 5 つの項目、リスク管理の強化のための共通の方策（overarching components）として、3 つの項目を挙げている。

サイバーリスク管理面の要諦（primary risk management categories）

①「ガバナンス」

②「守るべき重要機能の特定（identification）」

③「保護対策（protection）」

④「サイバー攻撃の発見・検知（detection）」

⑤「対応と復旧（response and recovery）」～『2 時間以内の業務再開（resumption within two hours）』

リスク管理の強化のための共通の方策（overarching components）

①ストレステスト（testing）

②情報収集・状況把握（situational awareness）

③訓練・進化（learning and evolving）

・「2 時間以内の業務再開」は、FMI に対して、強度のストレス時（extreme but plausible scenarios）であっても 2 時間以内の業務再開（two-hour RTO）を求めるものであり、FMI は、本ガイダンスの公表から 12 か月以内（2017 年 6 月まで）に同目的の達成のための具体的な計画の策定を求められている。

（4）FMI 原則・ガイダンスの実施モニタリング

・CPMI/IOSCO は、2012 年 12 月、「FMI 原則の情報開示の枠組みと評価方法」を公表し、①各国の当局や FMI 自身が「FMI 原則」を適用して業務内容等を評価する際の具体的な手順、②そうした評価を行う上での前提となる FMI による情報開示のあり方を定めた。

・CPMI/IOSCO は「FMI 原則」の実施状況に関するモニタリングを３つのレベルで実施。

レベル 1 評価：FMI 原則の国内実施のための枠組み・関連法・規制・方針の整備状況の確認
レベル 2 評価：各国の枠組みの内容と FMI 原則との整合性の検証
レベル 3 評価：個別 FMI における実施状況の検証

・「サイバーレジリエンスガイダンス」を踏まえた FMI 原則の実施状況は、今後、レベル 3 評価などの対象となり得る。

３． 大口資金決済システムのエンドポイントセキュリティに関する CPMI の取組み

（位置付け）

・CPMI は、バングラデシュ中銀の不正送金事件等を踏まえ、大口資金決済システムのエンドポイントセキュリティ（endpoint security）の強化に関する方策・提言を検討するためにタスクフォース（Task Force on Wholesale Payments Security）を設置。日本銀行も TF に参加し、「基本戦略（strategy）」策定に参画。

（Task Force on Wholesale Payments Security のメンバー＜2017 年 9 月時点＞）

NY 連銀（共同議長）、ベルギー中銀（同）、FRB、欧州中銀、英中銀、蘭中銀、独ブンデスバンク、伊中銀、スイス中銀、豪州準銀、韓国中銀、シンガポール通貨庁、日本銀行

・同 TF は、2016 年夏に中銀・大手資金決済システム向けのサーベイ調査、2017 年 3 月に資金決済システムの運営者などとの官民ワーショップを開催して検討を進め、2017 年 9 年に大口資金決済システムのエンドポイントセキュリティ強化のための「基本戦略（strategy）」に関する市中協議文書を公表。

（「エンドポイント」セキュリティの意義）

・大口資金決済システムの「エンドポイント」は、エコシステムの２つの主体（決済システムと通信ネットワーク、通信ネットワークとその参加者、決済システムとその参加者等）の間で、「支払指図の情報がやり取りされる際における接点」の意味。

・中央銀行は、自ら大口資金決済システム（中銀 RTGS システムなど）を運営するほか、民間大口資金決済システムの監督ないしオーバーサイトを行うことから、関与・関心が強い。

・「基本戦略」は、大口資金決済システムの重要性に鑑み、エンドポイントのセキュリティ強化により、エコシステム全体のサイバーセキュリティ・サイバーレジリエンスの向上を図ることを企図。

（「基本戦略（strategy）」の性格）

・「基本戦略」は、FMI 原則および関連するガイダンス（「サイバーレジリエンスガイダンス」など）のリスク管理面のトピックをカバーするが、これらの原則を代替するものではなく（the strategy is not intended to replace or supersede them）、適宜これらを補完するものとして勘案される（the scope of this strategy complements some of these principles and expectations, the strategy could be taken into account … where applicable and appropriate）。

―― 拘束力のある requirement よりも、「基本戦略（strategy）」というかたちで柔軟性の高いガイダンス（guidance）とすることを企図。

（対象範囲）

・対象は、大口資金決済システムや通信ネットワークおよびその参加者。

―― コルレス銀行ネットワークやリテール決済システムは射程外。

（「基本戦略」の内容）

・大口資金決済システム等のセキュリティのための「基本戦略」として、以下の７つのエレメント（element）を提案。

―― 大口資金決済システム毎に構造や決済の仕組みが異なることから、柔軟性に配意。

①リスクの特定・把握

- 運営者・参加者は、エンドポイントセキュリティに関するリスクの特定・把握に努めるべき。

②エンドポイントセキュリティの要件策定

- 運営者は、参加者の承認基準の中で、エンドポイントセキュリティの明確な要件（防止・検知・対応・情報共有等）を策定すべき。
- 各参加者は、必要に応じ、リスクベースのエンドポイントセキュリティの要件を独自に策定すべき。

③エンドポイントセキュリティ要件遵守の促進

- 運営者・参加者は、エンドポイントセキュリティ要件の遵守促進に資するプロセスを確立すべき。

④不正行為の防止・検知の向上のための情報・ツールの利用

- 運営者・参加者は、不正行為を適時に防止・検知する能力の向上に資する情報やツールの提供や利用を支援すべき。

⑤潜在的な不正行為への適時対応

- 運営者・参加者は、適時に不正行為に対応するための手順を整備するほか、十分なリソースを確保すべき。

⑥継続的な啓発・注意喚起・情報共有のサポート

- 運営者・参加者は、リスク自体やリスク管理にかかる継続的な啓発・注意喚起・情報共有に資する手続や慣行を整備するほか、十分なリソースを確保すべき。

⑦学習・発展・調整（前述①～⑥の取組みの継続）

- 運営者・参加者は、リスク自体やリスク管理をモニターし、その結果を踏まえ、エンドポイントセキュリティ要件の見直しや改訂を行うべき。
- 異なる決済システムの運営者・参加者の間で、エンドポイントセキュリティ強化に向けて協調すべき。
- 決済システム等の規制・監督・オーバーサイト当局は、リスク削減の戦略の進展に応じて、規制・監督上の目線（expectation）や評価プログラム等の見直しや改訂を行うべき。

（今後の進め方）

・CPMI は、市中協議終了後に、各エレメントへの対処の仕方に関する指針を作成する予定（CPMI plans to develop guidance for each element … on how they could approach each of seven element）。

・CPMI は、市中協議期間中の 2017 年 11 月に官民ワークショップを開催し、民間決済システムの運営者との意見・情報交換を実施。

・市中コメントは、基本戦略の目的・方向性や個々のエレメントの内容について、総じて前向きな評価。

・CPMI は、市中コメントや上記ワークショップの成果を踏まえて、ガイダンスの策定作業に着手。

４．　SWIFT のユーザーセキュリティ強化策と国際協調オーバーサイト

（位置付け）

・2016 年 2 月初に発生したバングラデシュ中銀不正送金事件等を契機に、SWIFT ネットワークのみならず、SWIFT に接続する各ユーザーが十分なサイバーセキュリティを確保することの重要性が認識された。

・SWIFT は、全 SWIFT ユーザー（200 か国 11 千社程度）のサイバーセキュリティのレベル引上げを企図し、2016 年 5 月より CSP（Customer Security Programme）と呼ばれるユーザーセキュリティの強化の取組みを推進。

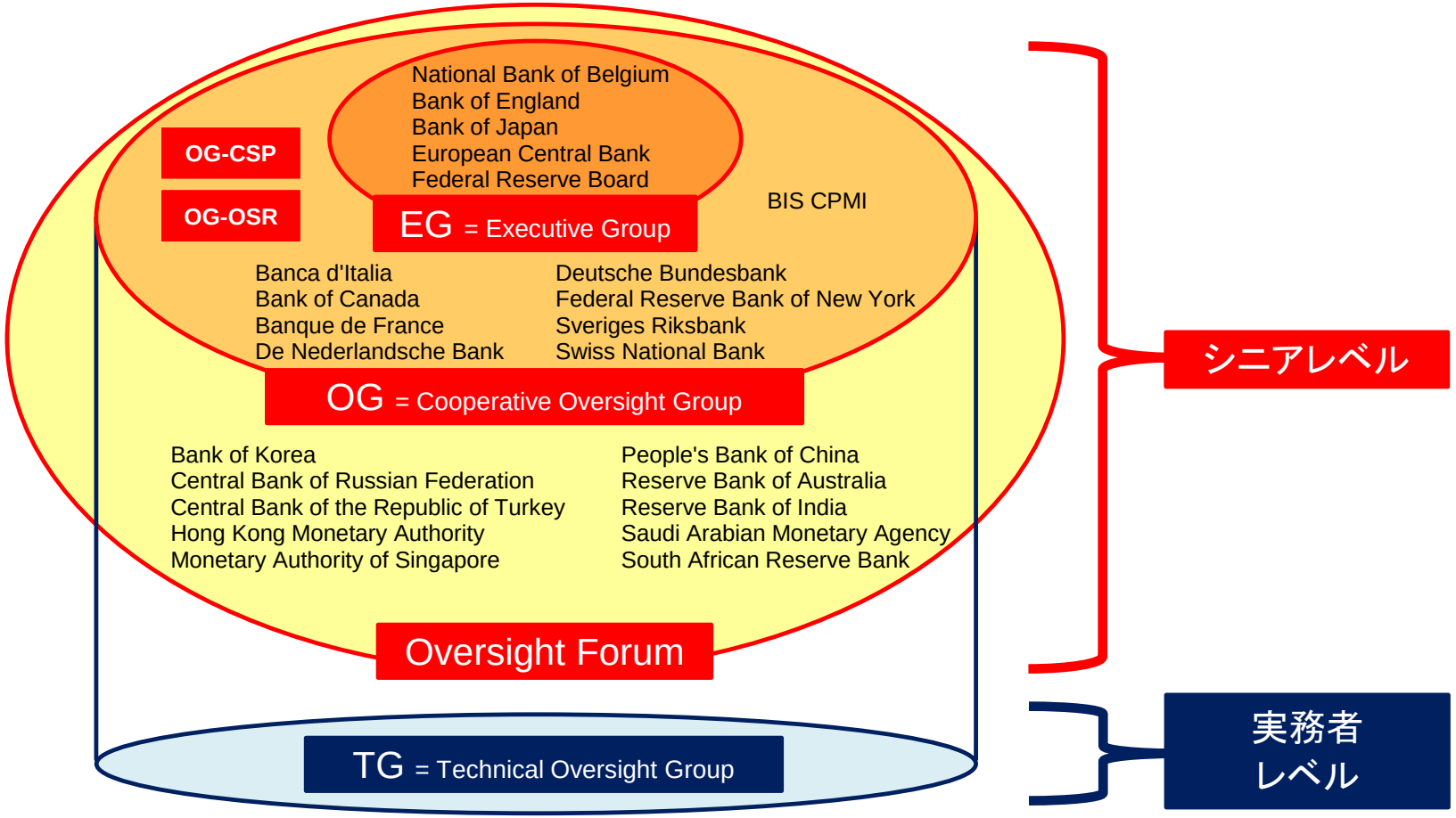
・日本銀行を含む主要国中銀は、SWIFT に対する国際協調オーバーサイトの一環として、CSP の取組みについて緊密に SWIFT と対話を重ね、その内容面・手続面の適正を担保。

（SWIFT 国際協調オーバーサイトの枠組み）

・SWIFT は金融市場インフラそのものではないが、世界各地の重要な決済インフラ（一部の中銀の資金決済システムや CLS などの国際的な決済インフラ）が SWIFT のサービスに依存していることに鑑み、決済システムの円滑な運営、金融システムの安定の観点から、主要国の中央銀行による国際協調オーバーサイトを実施。

・SWIFT の国際協調オーバーサイトの体制は、ベルギー中銀をリード・オーバーシーアーとし、主要国 4 中銀（FRB、ECB、BOE、日本銀行）を加えた Executive Group（EG。シニアレベル）、G10 中銀で構成される Cooperative Oversight Group（OG。シニアレベル）および Technical Oversight Group（TG。実務者レベル）がその中核をなし、OG メンバーに新興国を含む 10 か国・地域の中銀を加えた情報共有・意見交換の場である SWIFT 協調オーバーサイトフォーラム（シニアレベル）を加えた 4 つの会議体により構成。日本銀行はその全ての会議体に参加。

＜国際協調オーバーサイト体制の概念図＞



（国際協調オーバーサイトの基準）

・SWIFT は、資金決済システムなどとは異なる性格を有するため、コアプリンシプル等の国際基準をそのまま適用することはできなかったことから、オーバーサイト中銀は、オーバーサイトのための基準として、2007 年に「High Level Expectations for the oversight of SWIFT」（HLE）を策定。

・HLE の内容は、一般化されたかたちで、FMI 原則の一部である Annex F(Oversight Expectations applicable to critical service provider)として取り込まれている。

＜High Level Expectations（HLE）の概要＞

HLE 1:リスクの特定・管理	・重要なサービスに関するオペレーショナルリスク・財務リスクを特定・管理 ・リスク管理プロセスの有効性を確保
HLE 2:情報セキュリティ	・情報の機密性・完全性、重要なサービスの可用性を確保するために、適切な方針・手続を策定し、十分な資源を投入
HLE 3:信頼性、レジリエンス	・重要なサービスの信頼性・レジリエンスを確保 ・業務継続・災害復旧計画により、早期の復旧を確保
HLE 4:技術面の企画・立案	・技術の利用に関する企画・立案、技術的な標準の選択のための手法を確立
HLE 5:ユーザーとのコミュニケーション	・ユーザーに十分な情報を提供し、透明性を確保

（SWIFT のユーザーセキュリティ強化策）

（１）Customer Security Controls Framework の概要

・SWIFT は、ユーザーが取り組むべきセキュリティ強化策の具体的な内容を定めた Customer Security Controls Framework を策定し、2016 年 10 月から 12 月にかけて全世界のユーザーへ意見照会を行ったうえで、協調オーバーサイトの枠組みの下で主要国中銀との対話を経て、2017 年 4 月に全世界の SWIFT ユーザーに配布。

・Customer Security Controls Framework は、SWIFT のサイバーセキュリティ確保のためにユーザーに求められる最低水準（baseline）を取りまとめたものであり、27 項目のセキュリティ管理策を網羅。このうち、16 が必須項目（mandatory control）、11 が勧奨項目（advisory control）とされ、ユーザーは全必須項目を充足することが期待されている。

Customer Security Controls Framework の概要

	必須項目（mandatory control）	勧奨項目（advisory control）
1. IT 環境へのアクセス制限	1.1 SWIFT 環境の保護 1.2 オペレーティング・システムの保護	-
2. 脆弱性の削減	2.1 内部データフロー・セキュリティ 2.2 セキュリティ・アップデート 2.3 システム強化	2.4 バックオフィスデータフロー・セキュリティ 2.5 外部送信データセキュリティ 2.6 オペレーターセッションの機密管理 2.7 脆弱性スキャン 2.8 重要な活動の外注 2.9 取引制限
3. 物理的安全性	3.1 物理的安全性	-
4. アクセスキー窃取の防止	4.1 パスワード・ポリシー 4.2 複数要素認証	-
5. 本人確認・入退出管理	5.1 入退出管理 5.2 トークン管理	5.3 人員採用プロセス 5.4 パスワードの管理方法
6. 非正規活動の検出	6.1 マルウェア対策 6.2 ソフトウェア対策 6.3 データベース対策 6.4 ログ管理・モニタリング	6.5 侵入検知
7. 危機対応計画・情報共有	7.1 サイバー事案対応 7.2 セキュリティ訓練	7.3 不正侵入テスト 7.4 シナリオリスク分析

（実効性の確保に向けた取り組み）

・SWIFT は、上記枠組みの実効性を担保する観点から、各ユーザーが、自己査定（self-attestation）を行い、その結果を SWIFT に報告するプロセス（Customer Security Attestation Process：CSAP）を策定し、主要国中銀との対話を経て、2017 年 5 月にユーザーに配布。

・同プロセスの下で、各ユーザーは、「必須項目」の充足の有無に関する自己査定を行い、その結果を SWIFT に報告。同報告内容は、SWIFT により集中的に管理され、報告者の了承を条件として、その取引相手である他のユーザーの閲覧に供される。

・2017 年末までに同自己評価を行っていないユーザーについては、2018 年 1 月以降、SWIFT がその名称を当該ユーザーの監督当局（local supervisor）に通知する扱い。2019 年 1 月からは、「必須項目」を充足していないユーザーも通知の対象となる。

（今後の取組み）

・上記のプロセスの下で、自己査定の結果の分析などにより、ユーザーセキュリティ向上が十分に達成されているか等を点検したうえで、課題やその対応策などについて、協調オーバーサイトの枠組みの下で、SWIFT と主要国中銀の間で対話が行われていく見込み。

（接続業者のセキュリティ強化策）

・一部のユーザーは、SWIFT の承認する接続業者（Service Bureau）を通じて間接的に SWIFT ネットワークに接続。

・Service Bureau については、そのシステム基盤等に一定のセキュリティ水準の充足を求める SIP（Shared Infrastructure Programme）と呼ばれる取組みが 2013 年から実施されており、接続業者についても Customer Security Controls Framework と同様のセキュリティ強化の取組みを実施。

５． 結び

・サイバーセキュリティ、サイバーレジリエンスに関する国際的な議論は、グローバル金融危機後に本格化、バングラデシュ中銀不正送金事件等を契機に大きく進展。

・今後とも、サイバーリスクの増加・高度化が続く中、サイバー攻撃の傾向の変化や IT 技術の進展などを受けて、決済インフラに求める事項や要求水準も変化し得る。

・決済インフラおよびユーザーは、FMI 原則などの国際基準や各種の取組みに照らし、間断なくサイバーセキュリティの状況・十分性について点検を行い、必要な対応を検討・実施していく必要がある。

・中央銀行は、FMI 原則の実施モニタリングや国際協調オーバーサイトの枠組みを通じて、同対応を後押し・支援していく。

以　　上