特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

6 金融分野におけるサイバーセキュリティを巡る国際的な議論の動向

応用 一般

河田雄次　金融庁

金融に関する国際的な議論の枠組み

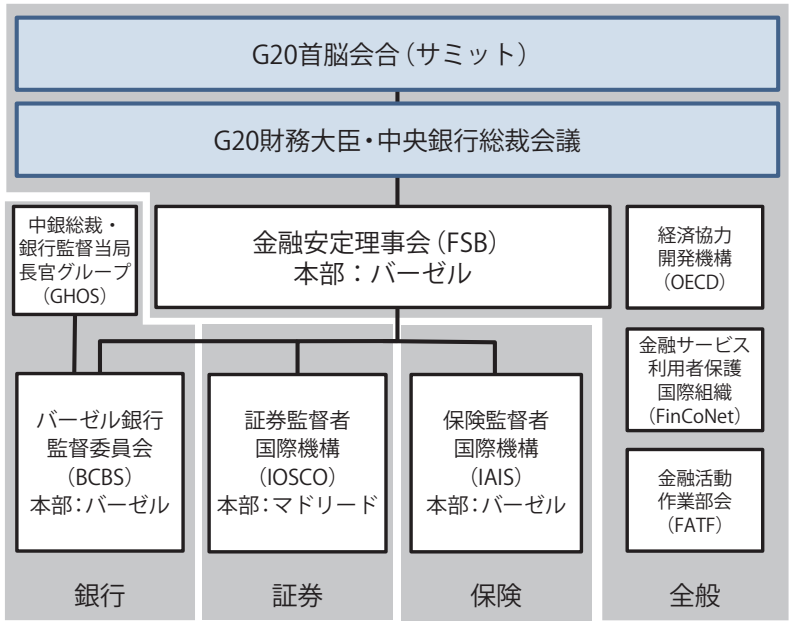
金融分野における幅広い世界共通の課題にかかる国際的な議論は，「国際経済協調の第一のフォーラム」である G20 をはじめとするさまざまな場において行われている．具体的な議論の紹介の前に，本稿では，まずその概観を整理したい（図 -1）．

G20

G20 とは，2008 年のリーマン・ショックに端を発する金融危機をきっかけに，危機対応や規制監督の改革等について，それまでの G7（日本，米国，英国，ドイツ，フランス，イタリア，カナダ）を超えた新興国を含む幅広いメンバで議論するために設置された，20 カ国・地域（G7 の主要 7 カ国に加え，アルゼンチン，オーストラリア，ブラジル，中国，インド，インドネシア，メキシコ，韓国，ロシア，サウジアラビア，南アフリカ，トルコ，欧州連合）からなる国際フォーラムである．2008 年の第 1 回 G20 首脳会合以降，G20 は国際経済協力に関する「第 1 のフォーラム」として定例化されている．

近年では，年 1 回の首脳会合（以下，サミット）と，年数回の財務大臣・中央銀行総裁会議が開催され，サイバーセキュリティのほか，国境を越えて広く利用されるような新たな形態のデジタルマネーであるグローバル・ステーブルコインへの金融規制監督の在り方，新型コロナウイルス感染症への対応施策の協調，サステナブルファイナンス，クロスボーダ決済の改善，金融包摂等が幅広く議論されている．

後述する金融安定理事会や基準設定主体がとりまとめた報告書や指針，基準等は，G20 サミットや G20 財務大臣・中央銀行総裁会議の共同声明で国際合意として盛り込まれる場合も多い．



■図 -1　国際的な議論の枠組み―文献 1）を参考に作成

金融安定理事会（FSB）

金融安定理事会（Financial Stability Board，以下FSB）は，1997年に発生したアジア通貨危機の経験を踏まえて1999年のG7での合意に基づき設立された金融安定化フォーラムを前身とする国際組織であり，リーマン・ショックを契機に，メンバをG20の財務省・中央銀行・監督当局や他の国際組織などに拡大・改組する形で2009年に設立された．FSBは，G20からの要請に基づき，国際的な金融システムの安定に資する取り組みを行うとともに，基準設定主体における作業の調整等を行う．

G20の節で挙げた通り，さまざまなテーマについて検討を行っているが，サイバーセキュリティに関しては，2017年以降，取り組みを本格化させている．

基準設定主体

金融分野では銀行や証券，保険などのセクタ別に，規制監督に関する国際原則，指針や基準等を策定する基準設定主体（Standard Setting Bodies，以下SSB）と呼ばれる国際組織が存在する．具体的には，銀行規制監督に関するバーゼル銀行監督委員会（Basel Committee on Banking Supervision，以下BCBS），証券市場規制監督に関する証券監督者国際機構（International Organization of Securities Commissions，以下IOSCO），保険規制監督に関する保険監督者国際機構（International Association of Insurance Supervisors，以下IAIS），マネー・ローンダリングおよびテロ資金供与対策（以下，マネロン等対策）に関する金融活動作業部会（Financial Action Task Force，以下FATF）等である．

一般的には，こうしたSSBにより策定された国際基準そのものは各メンバ国を法的に拘束するものではないが，各国の法規制が国際的に整合性のとれたものとなるよう，メンバ国をはじめとする世界各国で幅広く取り入れられている．

G7

G7は主要7カ国からなる国際フォーラムであり，主要先進国としての共通の価値観を共有する点が特徴である．

サイバーセキュリティに関しては，2015年にG7サイバーエキスパートグループを設置している．当該グループは，金融セクタにおけるサイバーセキュリティの現状分析や，G7各国間の連携を目的として活動を行っている．

その他，G7は，フェイスブック等によりリブラ構想が公表された2019年にとりまとめたグローバル・ステーブルコインに関する報告書や，2021年にとりまとめた中央銀行デジタル通貨に関する共通原則など，適宜，重要なテーマに関して検討グループを組織して検討を行っている．

最近の議論の動向

近年，金融機関等に対するサイバー攻撃の脅威が増し，金融システムの安定等にも影響を与えかねないことを踏まえ，前章で挙げたG20やFSB，SSB，G7のそれぞれでサイバーセキュリティに関する議論が積極的に行われている．

本章ではFSBおよびG7における最近の主な公表物を中心に，その内容を紹介したい（図-2）．

サイバーセキュリティ

ドイツ議長下の2017年3月G20財務大臣・中央銀行総裁会議での声明を受けて，FSBは，G20メンバ国における金融分野のレジリエンス向上へ向けたクロスボーダでの協力を強化する第一歩として，各国金融当局やSSB等のサイバーセキュリティ関連の規制監督上の取り組みについてサーベイを実施した．そして，その結果を同年10月のG20財務大臣・中央銀行総裁会議に提出し，「金融セクターのサイバーセキュリティにおける規制・ガイダンス・監督上の慣行に関するストックテイク報告書」とし

て公表した．

報告書は，各法域のサイバーセキュリティに関する規制監督枠組みは，既存の国際基準や指針等にある程度基づいているものの，法域内および法域間で多くの差異が見られることを指摘している．

国際的に一貫した規制監督体制の構築へ向けて，グローバルな対話を促進するために，まずサイバーセキュリティやサイバーレジリエンスに関する用語の共通理解を図る必要性が認識された．

そのため，翌 2018 年のアルゼンチン議長下では，FSB は，FSB や SSB，各法域の官民等でのサイバーレジリエンス向上へ向けた取り組み支援を目的として，関連する重要な用語をとりまとめ，同年 11 月に「サイバー用語集」として公表し，G20 サミットへ提出した．用語集は市中協議等でのフィードバックを踏まえたものであり，金融分野におけるサイバーセキュリティに関する政策立案等に有用な 50 超の用語から構成されている．

この後，サイバーインシデントからの復旧・回復といったレジリエンス向上へ向けたさらなる取り組みとして，2019 年の日本議長下では，FSB は，サイバーインシデントへの初動と回復（Cyber Incident Response and Recovery）に関するベストプラクティスのとりまとめに着手した．その後，進捗報告書を同年 6 月の G20 財務大臣・中央銀行総裁会議に，最終報告書を 2020 年 10 月の G20 財務大臣・中央銀行総裁会議に提出し，「サイバー事象の初動・回復対応の効果的な実務」として公表した．

報告書は，主に金融機関向けのプラクティス集であり，金融機関が自らの組織の規模や複雑性，リスクに基づいて適切なものを選択できるように，広範なプラクティスをとりまとめた形となっている．具体的には，①ガバナンス，②計画・準備，③分析，④影響緩和，⑤復旧・回復，⑥連携・情報共有，⑦

FSBにおける関連する文書	
2017	フィンテックによる金融安定上のインプリケーション
2017	金融セクタのサイバーセキュリティにおける規制・ガイダンス・監督上の慣行に関するストックテイク報告書
2018	サイバー用語集
2019	クラウドサービス利用における第三者サービスへの依存：金融安定への影響に関する考察
2020	サイバー事象の初動・回復対応の効果的な実務
2020	アウトソーシング・サードパーティに関する規制・監督上の論点（ディスカッション・ペーパー）
2021	アウトソーシング・サードパーティに関する規制・監督上の論点（市中協議に寄せられた意見の概要）
2021	サイバー事象報告－既存のアプローチとより広い範囲での収斂に向けた今後のステップ

G7における関連する文書・取り組み	
2016	金融セクタのサイバーセキュリティに関するG7の基礎的要素
2017	金融セクタの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
2018	脅威ベースのペネトレーションテストに関するG7の基礎的要素
2018	金融セクタにおけるサードパーティのサイバーリスクマネジメントに関するG7の基礎的要素
2019	合同演習
2020	サイバー演習計画に関するG7の基礎的要素
2020	ランサムウェアに関する附属文書

■図 -2　FSB および G7 における議論の動向―公表情報をもとに作成

改善の 7 領域における計 49 項目のプラクティスから構成されている．

その後，2021 年のイタリア議長下で，FSB は，金融当局向けの取り組みを開始した．具体的には，金融機関から当局へ提出されるサイバーインシデント報告を対象に，グローバルに調和を図ることが可能な領域を特定するために，各法域の規制報告枠組みについてサーベイを実施した．その結果を同年 10 月の G20 財務大臣・中央銀行総裁会議に提出し，「サイバー事象報告―既存のアプローチとより広い範囲での収斂に向けた今後のステップ」として公表した．

当局が金融機関や金融システム全体のリスクを評価する上で，サイバーインシデント報告は重要なツールである．サイバー攻撃の脅威がクロスボーダ・クロスセクタである一方，報告書は，多くの共通点が見られるものの，各国のサイバーインシデント報告には，報告対象とされるサイバーインシデントのスコープや，インシデントの深刻さやインパクトを測る手法，報告期限，報告された情報の用途に関して，法域間・セクタ間で差異が見られることを指摘している．

報告書は，今後取り組むべき内容として，①サイバーインシデントに関して当局が最低限必要とする情報の特定，②法域間・セクタ間で共有されるべき共通の情報の種類の特定，③共通用語の作成の 3 点を挙げており，FSB は，サイバーインシデント報告のグローバルな調和を図るためのさらなる作業を検討中である [2]．

G7 においては，2015 年に設置された G7 サイバーエキスパートグループ（以下，エキスパートグループ）が，サイバーセキュリティに関するベストプラクティスをとりまとめた内容を公表している．

具体的には，エキスパートグループは，2016 年 10 月，金融機関がサイバーセキュリティ対策を講ずる上で重要と考えられる「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」を公表した．翌 2017 年 10 月には，前年の基礎的要素に示したプラクティスの適切な実施・評価を行う点に焦点をあてた「金融セクターの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」を公表した．さらに，2018 年 10 月には，サイバー脅威情報の分析を踏まえた実践的な侵入テストに関する「脅威ベースのペネトレーションテストに関する G7 の基礎的要素」，金融機関における第三者委託先のリスク管理に関する「金融セクターにおけるサードパーティのサイバーリスクマネジメントに関する G7 の基礎的要素」を公表した．また，2019 年 6 月には，大規模なサイバーインシデントの発生を想定した合同演習を実施し，G7 諸国を中心としたクロスボーダの連携を確認した．そして 2020 年 11 月には，演習計画を立案・実施するための指針として「サイバー演習計画に関する G7 の基礎的要素」を公表した．

エキスパートグループでは，引き続き，演習を通じて得られた知見や教訓を踏まえ，G7 金融当局間の連携手順の改善など，国際的な連携の強化に向けた議論が進められている [3]．

第三者委託

サイバーセキュリティ対策を含む，金融機関のレジリエンス向上に関連したトピックとして，第三者委託先の管理や業務継続性の確保などが挙げられる．近年，IT を活用して新たな金融サービスを提供するフィンテックの台頭やそれに伴う新たな事業者の参入，金融機関間および金融機関と外部の委託先との間の相互接続（たとえば，クラウドコンピューティングやフィンテック事業者を通じた相互接続）の拡大，国際的に活動する大手クラウド事業者への集中リスクの高まりなどを背景に，金融機関における業務継続性の確保について国際的に関心が高まっている．特に，フィンテックを積極的に推進してきた欧州や英国を中心に積極的に議論が進められている．

FSB では，早くからこの点に関してリスク評価を

進めており，2017 年 6 月に公表したフィンテックに関する規制監督上の含意をとりまとめた報告書では，当局間のクロスボーダでの協力が必要とされる最重要項目として，金融機関が利用するクラウドなどの第三者委託先に起因するオペレーショナル・リスク管理を挙げている．なお，金融分野における国際的な議論では，第三者委託については，外部委託（Outsourcing）を含む，金融安定や金融機関にリスクをもたらす，あらゆる第三者との関係（Third-party relationships）を念頭に議論される場合が多い．

その後，FSB は，クラウドサービスを対象に，その金融安定上のリスクについてさらに検討を行った結果を，2019 年 12 月に「クラウドサービス利用における第三者サービスへの依存：金融安定への影響に関する考察」として公表した．報告書は，金融機関によるクラウドサービスの利用は金融安定上の喫緊のリスクではないと結論づけているものの，第三者委託に関する規制や監督実務の妥当性評価等の必要性を指摘している．

FSB は，こうしたリスク評価結果を踏まえ，次に規制監督上の論点について検討を進めた．その結果を，2020 年 11 月に「アウトソーシング・サードパーティに関する規制・監督上の論点（ディスカッション・ペーパー）」として公表し，広く一般からコメントを募る市中協議を行った．

報告書では，第三者委託の増加は，個社レベルではスケーラビリティやオペレーショナル・レジリエンスの向上，コスト削減等のメリットをもたらす一方で，金融当局等にとっては，特に，①金融機関と第三者委託先との契約に関する実務的な課題，②クロスボーダに起因する監督上の課題，③第三者委託先の集中化に起因する金融システム上の課題という 3 点の課題をもたらし得ると指摘している．

①の実務的な課題とは，（1）当局のリソースや IT スキルの不足のほか，（2）金融機関が第三者委託先との契約へ規制監督上の要件を盛り込むことが実務的には困難であり，監査権やデータへのアクセス権，情報取得権が不十分，（3）金融機関のオペレーションにかかるサプライチェーンが長く複雑であるため，二次受けや三次受け等含めたサプライチェーン全体に渡るリスクを特定し管理することが困難，といった課題を指す．

②のクロスボーダの課題とは，（1）監督管轄権が海外の事業者まで及ばない場合や，（2）データ守秘義務の基準等が異なるために当局間の情報共有や金融機関による統一的なデータ管理が困難，（3）第三者委託先が破綻した際に第三国にある重要なデータ等の回収が困難，などの課題を指す．

③の集中化による課題とは，クラウドなど，少数の第三者委託先による寡占市場が生じることで，特定のサービス事業者が単一障害点となり，特定サービスの障害が多くの金融機関に影響を与え得ることを指す．こうした課題を踏まえ，報告書は，金融当局，金融機関，第三者委託先の間でのグローバルな対話の必要性を指摘している．

その後，FSB は，市中協議等でのフィードバックをとりまとめたものを，2021 年 6 月に「アウトソーシング・サードパーティに関する規制・監督上の論点（市中協議に寄せられた意見の概要）」として公表した．

報告書では，前年の報告書で指摘した，監査権やアクセス権，情報取得権の制約，重要サービスにおける集中リスク，規制監督や業界慣行の法域間の相違，データローカライゼーション要件，サイバーセキュリティ・データセキュリティ，専門人材の不足などの課題については，市中協議でおおむね支持されたことを報告している．

また，こうした課題に対処する解決策の案として，（1）事業者に求める事業継続計画・災害復旧計画やサイバーセキュリティ対策，金融機関による事業者の選定やモニタリング，事業者から徴求すべき情報の標準化，事業者との契約の雛形などの第三者委託に関するグローバルスタンダードの策定，（2）定義や用語の統一，（3）金融機関が共同で行う共

同監査や第三者認証の活用，（4）第三者委託先への依存関係の把握，（5）国際協調や官民連携の促進などが挙げられたことを報告している．

今後，FSB は，定義や用語の統一のほか，第三者委託に関する監督上の期待事項のとりまとめを進めていく方向である[2]．

SSB においても活発に議論が進められており，たとえば，BCBS は，サイバー攻撃や自然災害などの発生時における銀行の重要な業務の継続性確保について，2021 年 3 月に，「オペレーショナル・レジリエンスのための諸原則」を公表した．これは，大規模なシステム障害やサイバー攻撃の脅威の増大，パンデミックなどのリスク環境の変化を踏まえ，未然防止策を尽くしてもなお業務中断が生じ得ることを前提に，自行だけでなく，第三者委託先から ATM や窓口等の顧客接点までのエンドツーエンドで，業務中断の影響が許容水準内に収まるよう包括的な態勢整備を求めるものである．

具体的には，①ガバナンス，②オペレーショナル・リスク管理，③事業継続計画とテスト，④組織内外の相互連関性の特定，⑤第三者への依存度の管理，⑥インシデント管理，⑦サイバーを含む ICT セキュリティ対応という 7 つの原則からなる．

また，IOSCO では，2021 年 10 月に「外部委託に関する原則」を公表した．これは，過去に公表した「市場仲介業者の外部委託に関する原則」および「取引所業務の外部委託に関する原則」を統合した上，近年の動向を踏まえて内容を更新し適用範囲を拡大したものである．

本原則は，外部委託の定義，重大性（Materiality）及び不可欠性（Criticality）など外部委託における基本的な考え方に関する記述と，①外部委託先の選定プロセスとモニタリング，②外部委託先との契約，③情報セキュリティ，業務の回復力，事業継続性，災害復旧の確保，④秘密保持，⑤特定の外部委託先への集中，⑥外部委託先のデータ，事業所，人員へのアクセスおよび関連する検査権限，⑦外部委託契約の解除の 7 分野に関してそれぞれ定めた 7 つの原則からなる．

ランサムウェア・暗号資産

最後に，サイバーセキュリティに関連したその他のトピックについても紹介したい．金融分野では，犯罪収益のマネロン等対策やサイバー保険など，サイバーセキュリティを取り巻くトピックに関しても積極的に議論が行われている．

たとえば，ランサムウェアについては，近年，その被害の拡大とともに，対策の必要性について国際的に関心が高まっている．2020 年 10 月の G7 財務大臣・中央銀行総裁会議は，ランサムウェアに関する附属文書を公表した．これは，G7 の文書としては異例ながら，業界に対して直接働きかける文言となっており，ランサムウェア攻撃の脅威が増している点に懸念を示している．

また，ランサムウェアへの対処としては，①自らが被害を受けない，②たとえ被害を受けても身代金を支払わない，③被害を受けずとも身代金の支払いに利用されない，という 3 点が考えられるところ，文書は，特に③の身代金の支払いに利用されてはならないという点を強調している．具体的には，ランサムウェアの身代金として暗号資産が利用される場合が多いことに触れつつ，金融機関に対して，身代金の支払いを防止すべく，FATF 勧告や国内法令等に基づき，マネロン等対策にかかる義務を確実に実施することを求めている．

FATF は，2019 年 6 月に暗号資産に関する FATF 基準を最終化し，マネロン等対策に関する FATF 基準が暗号資産にかかる金融活動にも適用されることを明確にしている．その後，新たな FATF 基準の各国での実施状況や残された課題等をとりまとめた報告書を公表している．その中でも，2021 年 7 月に公表された「暗号資産・暗号資産交換業者に関する FATF 基準についての 2 回目の 12 カ月レビュー報告書」は，ランサムウェア攻撃による犯罪収益が匿

名性を高めるツールなどを介して資金洗浄される危険性を指摘しているほか，各国での新たな FATF 基準に基づくマネロン等対策の必要性を強く指摘している．

なお，FATF は，2021 年 10 月に，「暗号資産及び暗号資産交換業者に対するリスクベース・アプローチに関するガイダンス」を公表して，新たな FATF 基準に関する考え方を詳細に記したガイダンスを 2 年ぶりに更新した．ガイダンスは，暗号資産やマネロン等対策を行う規制対象の定義など FATF 基準の適用範囲を明確化したほか，ステーブルコインに関する考え方，仲介業者を利用せずに個人間で行われる取引のリスクおよびリスク低減策，仲介業者の登録・免許付与，国際的な監督協力等をまとめている．FATF は，今後とも，暗号資産に関するモニタリングを継続していくこととしている．

今後に向けて

本稿では，金融分野におけるサイバーセキュリティを巡る国際的な議論の動向について概説した．金融機関等へのサイバー攻撃の脅威が増し，金融システムの安定等にも影響を与えかねないことから，G20 や FSB，SSB，G7 等のさまざまな場において積極的に議論が行われている．議論の中では，サイバーセキュリティ対策のほか，用語の統一，規制報告枠組み，第三者委託，犯罪収益や暗号資産など多面的な観点から議論が行われている．引き続き，各国の金融当局が連携して，課題解決に向けた議論をグローバルに深めていくことが望まれる．

本稿で示された内容や意見は，筆者個人のものであり，金融庁の公式見解を表すものではない．

参考文献
1）金融庁：金融庁の 1 年（2020 事務年度版）（2021）．
2）FSB：Promoting Global Financial Stability - 2021 FSB Annual Report（2021）．
3）金融庁：金融分野のサイバーセキュリティレポート（2020）．

（2022 年 1 月 17 日受付）

■河田雄次　yuji.kawada@fsa.go.jp

慶應義塾大学大学院理工学研究科基礎理工学専攻修了．2015 年から（株）三菱総合研究所主任研究員，2016 年から 2018 年まで日本銀行に出向し欧州中央銀行とのブロックチェーン共同調査に従事．2020 年から現職．