FSB（金融安定理事会）による“各国及び国際機関の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報告書”概要

平成 30 年 12 月 7 日
佐志田晶夫
（公益財団法人日本証券経済研究所）

FSB（金融安定理事会）による“各国及び国際機関の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報告書”概要

要約

デジタル技術の発達と利用の拡大・高度化が進む中で、サイバーリスクが増大していることを背景に、金融部門でのサイバーセキュリティ強化の重要性が国際的に高まっている。このため、G20 蔵相・中銀総裁会議の求めに応じて FSB（金融安定理事会）は、2017 年に各メンバー法域・国際機関の規制・ガイダンス、監督上の慣行に関する調査を行い、2017 年 10 月に報告書を公表している。本稿はその概要を紹介するもの。

調査対象は、金融部門のサイバーセキュリティ対応に関するメンバー法域と国際機関の公表された規制・ガイダンスや監督上の慣行。非公表のものや自主規制団体によるものは含まない。全法域がなんらかの対応を行っており、部門別では全 25 法域が銀行部門、24 法域が FMI（金融市場インフラ）に対応、この分野の重要性が示唆される。取引執行施設、保険業はそれぞれ 19、資産運用業は 18、証券業は 16 が対応しているが、年金基金は 8 に止まる。

公表された規制・ガイダンスの数は監督上の慣行よりも多いが、監督上の慣行には非公表なものもある。規制、監督スキームの開発では国際機関等が公表したガイダンスや基準が参考にされ、CPMI-IOSCO のガイダンスと ISO／IEC の国際規格が参照されることが多い。なお、20 法域が国家的なサイバーセキュリティ戦略・方針を公表、その多くは、防衛、教育、成長と技術革新、パートナーシップと協調、国際的なパートナーとの協働などのテーマを含む。

25 法域から合計で 85 規制スキームと 35 監督上の慣行スキームが報告されている。85 規制スキームの内で 29 がオペリスクを、56 はサイバーセキュリティ／IT リスクを対象としている。部門別では取引執行施設や FMI はサイバーセキュリティ／IT リスクでの対応の比率が高い。

規制スキームが対象に取上げているトピックは、ガバナンス（ボードと上級経営陣の役割等）、サイバーセキュリティ担当の専門性・独立性、リスク評価、訓練、システムアクセス管理、テスト、復旧、サードパーティーとの接続、規制上の報告などである。

監督上の慣行スキームでは、銀行部門が 16 法域、FMI は 12、資産運用業では 10、証券業と取引執行施設は 9、保険業は 8 で、年金基金は 4。監督スキームが取り上げたトピックは、監督チームの専門性、ガバナンス、方針と手順、リスク評価プロセス、データセキュリティ、テスト、過去のインシデントの影響度、当局によるコミュニケーション、情報共有などがあった。

サイバーセキュリティ対応に実効性がある基準や慣行を列挙すると、CPMI-IOSCO の FMI に関するガイダンス、プリンシプルベースや比例的な監督（金融機関の特質、規模、複雑さ、リスクプロファイルと比例）、ボードと上級経営陣の役割（経営陣の説明責任、ボードでの認

識、CISO（最高情報セキュリティ責任者）の任命）、リスク管理の独立性、当局と規制対象機関のコミュニケーション、協調と情報共有（脅威インテリジェンス、サイバーインシデント対応、ベストプラクティス）、サイバーセキュリティ要件の特定と更新、外部委託のリスク管理、システミックリスク評価などがあった。

また、サイバーセキュリティに対する監督上の手段では、金融機関のサイバー・ロードマップのレビュー、業界全体の準備状況演習、サードパーティーの監査と評価、金融機関の自己評価、ペネトレーションテスト（システムへの侵入テスト）やレッド（攻撃）チーム演習を含むテスト、過去のサイバーインシデントのレビュー、サイバーセキュリティのテーマレビュー、懸念される特定分野への助言やガイドライン、行政上の処罰などが挙げられた。

国際機関・組織では、バーゼル委員会（BCBS）、決済・市場インフラ委員会 CPMI）、G7 サイバーエキスパートグループ（CEG）、IOSCO（証券監督者国際機構）、経済協力開発機構（OECD）がガイダンスを公表している（CPMI と IOSCO は共同）。

主な例としては下記が挙げられる。

・CPMI-IOSCO「金融市場インフラのためのサイバー攻撃耐性（レジリエンス）に係るガイダンス」2016 年 7 月

・G7CEG「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」2016 年 10 月

なお、G7CEG は活動を継続しており、FSB 報告書の公表後にも以下を公表している。

「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 G7 の基礎的要素」2017 年 10 月、「脅威ベースのペネトレーションテスト」及び「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 の基礎的要素について」2018 年 10 月。

FSB（金融安定理事会）による“各国及び国際機関の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報告書”概要

公益財団法人日本証券経済研究所
特任リサーチ・フェロー佐志田晶夫

Ⅰ．はじめに

本稿では、FSB（金融安定理事会）が 2017 年 10 月に公表した“各国及び国際機関の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報告書 (1)”の概要を、図表を中心に紹介したい。昨年 3 月にドイツで開催された G20 蔵相・中銀総裁会議では FSB に、サイバーセキュリティへの効果的な実務慣行を特定するための第一歩として“我々の国・地域内における既存の関連する公表されている規制や監督上の慣行、及び既存の国際的なガイダンスに関する現状調査”を求めた(2)。報告書はこの求めに応じたものである。

報告書公表後も FSB のサイバーセキュリティ関連のプロジェクトは継続されており、最近では、サイバーセキュリティ関連の用語集が市中協議を経て公表された(3)。2019 年の FSB の作業計画では、サイバーインシデントへの金融機関の対応と復旧に関する実効的な慣行の開発プロジェクトが予定され、2019 年半ばに進捗状況の報告を行うこととなっている。

こうした動きの背景には、主要国間のサイバーリスクとサイバーセキュリティの重要性に関する認識の共有がある。2016 年の G7 伊勢志摩サミットでは、“サイバーに関する G7 の原則と行動”が公表され(4)、2017 年の 7 カ国財務大臣・中央銀行総裁会議声明(5)では“金融サービスのデジタル化が拡大し、サイバーの脅威が進展している状況において、各金融機関及び金融

---

1 本件については金融庁の HP、https://www.fsa.go.jp/inter/fsf/20171018.html 及び FSB の HP http://www.fsb.org/wp-content/uploads/P131017-2.pdf を参照。

2 財務省 HP“20 か国財務大臣・中央銀行総裁会議声明（仮訳）（2017 年 3 月 17-18 日 於：ドイツ・バーデン=バーデン）”を参照。https://www.mof.go.jp/international_policy/convention/g20/170318.htm

3 サイバー用語集については、http://www.fsb.org/2018/11/cyber-lexicon/ 参照。FSB の 2019 年の作業計画は、FSB 総会のプレスリリース http://www.fsb.org/2018/10/fsb-reviews-financial-vulnerabilities-and-deliverables-for-g20-summit/ および 2018 年 11 月 28 日公表の FSB の年次報告でのサイバーリスクに関する記述を参照。http://www.fsb.org/2018/11/implementation-and-effects-of-the-g20-financial-regulatory-reforms-fourth-annual-report/

4 外務省 HP G7 伊勢志摩サミット https://www.mofa.go.jp/mofaj/files/000160315.pdf 参照。

5 財務省 HP“7 カ国財務大臣・中央銀行総裁会議声明（仮訳）（2017 年 5 月 12-13 日 於：イタリア・バーリ）”参照。https://www.mof.go.jp/international_policy/convention/g7/cy2017/g7_170513.pdf

セクターレベルにおけるサイバーセキュリティの評価のための効果的な手法を追求することは重要”として、G7 サイバーエキスパートグループ（G7CEG）に活動を指示している。G7CEG は、“2015 年の立ち上げ以来、多様な参加者と高いレベルの相互共有と信頼を構築し、サイバーセキュリティに関する国際協調のための固有のプラットフォームを提供”したとされている。G7CEG の活動は継続しており、今年は「脅威ベースのペネトレーションテスト」及び「サードパーティのサイバーリスクマネジメント」に関する報告書が公表されている(6)。

本稿で紹介する FSB の報告書の構成は図表 1 のとおりであり、各国・法域及び国際機関による規制やガイダンスを集約して、どんな点が重視されているかを概観している。また、報告書の付属資料で、各法域の回答の要旨がそれぞれ 1～3 ページ程度でまとめている。

図表1：FSBサイバーセキュリティ報告書の目次

要旨
1. FSBメンバー法域での規制、ガイダンス及び監督上の慣行
1. 1 はじめに
1.2 報告された規制、ガイダンス及び監督上の慣行
1. 2. 1 一般的な規制およびガイダンス
1. 2. 2 オペレーショナルリスクに対処する規制及びガイダンス
1. 2. 3 サイバーセキュリティ及び／またはITリスクを対象とした規制及びガイダンス
1. 2. 4 監督上の実務
1. 3 報告された将来計画
1. 4 報告された実効的な慣行
2. 国際機関によるガイダンス及びその他の活動
2. 1 国際機関が発行したガイダンス
2. 2 国際機関によるその他の公表物
2. 3 将来の計画
付属資料A：追加の図表
付属資料B：既存の各国及び国際的なガイダンス及び基準についての用語集
付属資料C：FSBの調査に対する各法域の回答の要約集

なお、最近の日本の動きとしては、金融庁が「金融分野におけるサイバーセキュリティ強化に向けた取組方針」を 2018 年 10 月に更新、新たな課題と対応を整理している(7)。こうした動きについては本稿の末尾で簡単に紹介する。

---

6 金融庁 HP：“「脅威ベースのペネトレーションテスト」及び「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 の基礎的要素の公表について”を参照 https://www.fsa.go.jp/inter/etc/20181015/20181015.html

7 金融庁 HP：“「金融分野におけるサイバーセキュリティ強化に向けた取組方針」のアップデートについて” を参照。https://www.fsa.go.jp/news/30/20181019-cyber.html

報告書の内容に入る前に、報告書の問題意識を確認するため、基本的な概念であるサイバーセキュリティおよびサイバーレジリエンス（回復力、耐性）が、各 FSB メンバーによってどう用いられているかを紹介しておきたい（より詳しくは本稿末を参照）。

・サイバーセキュリティ
香港：サイバー攻撃から保護または防御する能力であり、攻撃とは組織の IT システムとネットワークを標的として、途絶、無能化、破壊するか、悪意を持って IT システム／ネットワークを制御し組織のデータの完全性を破壊、あるいは情報を盗むことを指す。
インド：サイバー攻撃を防ぎサイバーレジリエンスの向上を意図する方法、手段およびプロセス。サイバーレジリエンスは、サイバー攻撃に備えて対応し、サイバー攻撃の間も業務を継続し復旧する能力。
イタリア：攻撃の開始が物理的なものか論理セキュリティ侵害によるものかに関わらず、情報システム資産とコミュニケーションネットワークを、あらゆる非物理的な攻撃から守るために用いられる管理および組織的な手段と方法（人的、技術的等）。

・サイバーレジリエンス
CPMI-IOSCO（決済・市場インフラ委員会 - 証券監督者国際機構）：サイバー攻撃を予期し、耐性を備え、封じ込め、迅速に復旧する FMI(金融市場インフラ)の能力。
オーストラリア：サイバー攻撃に備え対処し、復旧する能力。サイバーセキュリティは、連関する脅威からデジタル資産を護ることの実践。レジリエンスは、単に攻撃を防ぎ、対処する以上のものであり、そうしたイベントの最中でも業務を運営し適応・復旧する能力も考慮する。

Ⅱ．メンバー法域の規制・ガイダンスと監督上の慣行の概観

今回の調査は、金融部門のサイバーセキュリティ対応に関して、各国の政府当局が公表している規制・ガイダンスや監督上の慣行が対象であり、公表されていないものは含まない。監督上の慣行では、使用されているが非公表のものがあり、それらは報告書には含まれていない。

また、自主規制団体や地方政府（州など）が制定したものも本報告書には含まれない。このため、監督上の慣行では、実際に用いられている慣行を完全には捉えていない。また、報告書の情報は、各法域の異なる規制およびビジネス環境という文脈で考えるべきである。

FSB メンバー法域の全てが、少なくとも金融部門の一部のサイバーセキュリティに関する規制・ガイダンスか監督上の慣行を公表している。25 法域のすべてが規制または監督により銀行部門に対応、FMI には 24 法域が対応しており、これらの分野の重要性が示唆される。また、19 法域が取引執行施設と保険業、18 法域が資産運用業、16 法域が証券業のサイバーセキュリティに取り組んでいる。一方で、年金基金については 8 法域に止まる。

規制・ガイダンスと監督上の慣行で公表された情報を比べると（図表 2）、規制・ガイダンスの方がかなり多いが、これは前述のように監督上の慣行は公表された情報が少ないということであり、実施されている監督上の慣行が少ないことを必ずしも意味しない。過半数の法域が、サイバーセキュリティに関する将来計画の立案を考えている（図表 2 の右端列参照）。

図表2：サイバーセキュリティについての各国で公表された情報

メンバー法域	国家的戦略	規制／ガイダンス							監督上の慣行							将来計画
		FMI	取引執行施設	銀行	保険	証券業	資産運用	年金基金	FMI	取引所	銀行	保険	証券業	資産運用	年金基金	
アルゼンチン		■		■							■					✔
オーストラリア	✔	■	■	■	■	■	■	■	■							✔
ブラジル	✔	■	■	■	■	■	■							■		✔
カナダ	✔	■	■	■	■	■	■									
中国	✔	■	■	■	■	■	■			■	■		■	■		✔
EU	✔	■	■	■	■	■					■					✔
フランス	✔	■	■	■	■	■	■	■	■		■	■				✔
ドイツ	✔	■	■	■	■	■	■	■								✔
香港	✔	■		■	■	■	■		■		■		■	■		✔
インド	✔	■	■	■	■						■					
インドネシア		■		■		■	■		■		■		■			✔
イタリア	✔	■	■	■	■		■		■	■						
日本	✔	■	■	■	■	■	■		■	■	■	■	■			
韓国		■	■	■	■		■		■	■	■	■		■		✔
メキシコ		■	■	■	■	■	■	■	■	■	■	■	■	■		✔
オランダ	✔	■									■	■		■	■	✔
ロシア	✔	■	■	■							■					✔
サウジアラビア		■		■	■											✔
シンガポール	✔	■	■	■	■	■	■		■	■	■	■	■	■		✔
南アフリカ	✔			■												✔
スペイン	✔	■	■	■												✔
スイス	✔	■	■	■	■	■	■									
トルコ	✔	■	■	■		■	■	■	■	■	■		■	■	■	
英国	✔	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
米国	✔	■	■	■	■	■	■	■	■	■	■	■	■	■	■	✔
合計	20	24	19	24	18	16	17	7	12	9	16	8	9	10	4	18

出所：FSB報告書の表1より作成

■ 該当する法域

各法域では、金融部門のサイバーセキュリティに関する規制および監督スキームの開発に際して、各国当局や国際機関が公表したガイダンスや基準を参考にしている。主な機関・組織を一覧で示すと以下の通りであり、とりわけ CPMI-IOSCO のガイダンスと ISO／IEC の国際規格が多くの法域で参照されている（図表 3 参照）。

CPMI-IOSCO：「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」
米国 NIST（国立標準技術研究所）：「サイバーセキュリティフレームワーク」
ISO(国際標準化機構）／IEC（国際電気標準会議）：27000 シリーズ
ISACA（情報システムコントロール協会）：COBIT（Control OBjectives for Information and related Technology）
FFIEC（米国連邦金融機関検査協議会(8)）
G7 サイバーエキスパートグループ(注 5 参照)

図表3：既存の各国または国際的なガイダンス・基準を自法域の規制および／または監督上の慣行スキームに用いている法域

メンバー法域	諸国または国際的なガイダンス・基準を反映	ガイダンス・基準を発行した機関					
		CPMI-IOSCO	FFIEC	G7	ISACA（COBIT）	ISO-IEC	NIST
アルゼンチン	✔		■	■	■	■	■
オーストラリア	✔	■					■
ブラジル	✔	■			■	■	
カナダ	✔	■	■		■	■	■
中国	✔	■			■	■	
EU	✔	■					■
フランス	✔	■	■				■
ドイツ	✔	■				■	
香港	✔	■	■		■		■
インド	✔	■			■	■	■
インドネシア	✔				■	■	
イタリア	✔	■		■		■	
日本	✔	■				■	■
韓国	✔					■	
メキシコ	✔	■		■	■		■
オランダ	✔	■			■	■	■
ロシア	✔	■				■	
サウジアラビア	✔	■				■	■
シンガポール	✔	■		■		■	■
南アフリカ	✔	■					
スペイン	✔	■					
スイス	✔						■
トルコ	✔				■	■	
英国	✔	■				■	■
米国	✔	■	■		■	■	■
合計	25	19	6	4	11	17	15

出所：FSB報告書の付属資料A、表6より作成

■ 該当する法域

なお、図表 2 の左端列で示されているように、20 法域が金融部門における対応に加えて、国家的なサイバーセキュリティ戦略、方針またはより広く適用される枠組みを公表している。その多くには、防衛、教育、成長と技術革新、パートナーシップと協調、国際的なパートナーとの協働などのテーマが含まれている。報告書の BOX を要約すると以下の通り。

8 金融庁の委託調査：「『FFIEC Cybersecurity Assessment Tool に関する調査研究』調査報告書」（委託先：株式会社 NTT データ経営研究所）2016 年 3 月を参照。 https://www.fsa.go.jp/common/about/research/20160815-1/01.pdf

（参考）国家的なサイバーセキュリティ戦略（報告書 BOX2 より）
防衛：報告された戦略のかなりの部分が、サイバー脅威に対する国家的防衛についてである。各法域は、政府システムと重要な国家インフラを守る行動を特定していることが多い。

教育：多くの法域が教育を対象とする戦略を報告している。これは、市民のサイバー問題に対する認識を高めることと関連して報告されている。

成長と技術革新：いくつかの法域は、成長と技術革新、研究と開発、そして科学と技術を対象にしている。ある法域は、公的および民間部門の両方の国家的な需要に応える人材と、将来の脅威と挑戦に対応し打ち克つ専門性の育成・供給への強い願望を示している。

パートナーシップと協調：実効的なパートナーシップと協調の重要性を多数の法域が強調。頻繁に報告されるのは公的部門と民間部門のパートナーシップである。また、パートナーシップを連邦政府外部の重要なサイバーシステムを守る手段としている法域がある。別の法域は、相互信頼の基礎となる情報共有のプラットフォームを作る行動を概説している。

国際的なパートナーとの協働：多くの法域が国際的なパートナーとの協働の概要を述べている。ある法域は、国際協力に焦点を当てた具体的な戦略を報告。ある法域は、集団的なセキュリティを強化する国際的な行動の重要性を指摘。別の法域は、国際法の執行を強化する行動を具体的に報告している。

Ⅲ．報告された規制・ガイダンスと監督上の慣行

1．法域／部門別の概況

メンバー法域からは 85 の規制・ガイダンススキームと 35 の監督上の慣行スキームが報告された（図表 4）。規制・ガイダンスは、規制対象機関に要件を課すかガイダンスを提供するもので、監督上の慣行は、監督当局が規制対象機関の監督や検査で用いる慣行である。

全ての法域が少なくとも 1 つの規制・ガイダンスがあると報告しているのに対して、監督上の慣行は 6 法域が報告していない。報告数はまちまちだが、何を別のスキームとするか、一つのスキームとするかは各法域に委ねられている。このため数の違いから何らかの結論を導くのは難しい。部門別では、銀行と FMI を対象とするものが多く年金基金は少ない。

2．規制・ガイダンスの全般的な状況

メンバー法域が報告した 85 の規制・ガイダンスの内で、79 が最終化・公表されたものであり、内 9 は、修正案や精緻化案が公表されている。6 は、まだ草案である。部門別では、銀行部門と FMI には、ほとんどの法域で規制・ガイダンスが導入され、保険業、取引執行施設、資産運用業と証券業にも過半数の法域が規制・ガイダンスを実施している（図表 5 参照）。

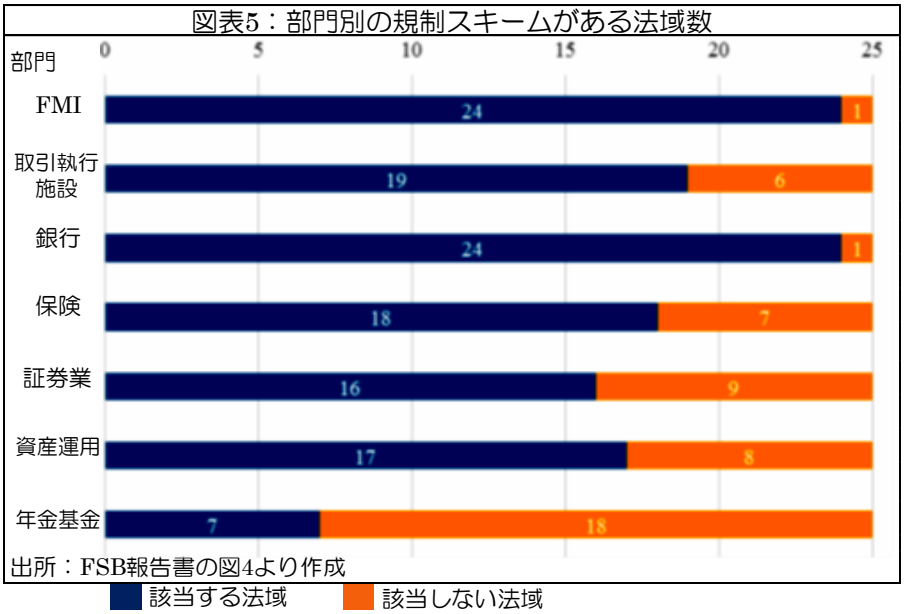
図表4：法域毎の規制及び監督スキームの状況

メンバー法域	法域数		部門						
	規制／ガイダンス	監督上の慣行	FMI	取引執行施設	銀行	保険	証券業	資産運用	年金基金
アルゼンチン	1	1	■		■				
オーストラリア	3	1	■	■	■	■	■	■	■
ブラジル	4	1	■	■	■	■	■	■	
カナダ	3	0	■	■	■	■	■	■	
中国	6	2	■	■	■	■	■	■	
EU	10	2	■	■	■	■	■		
フランス	2	1	■	■	■	■	■	■	■
ドイツ	7	0	■	■	■	■	■	■	■
香港	3	2	■		■	■	■	■	
インド	3	1	■	■	■	■			
インドネシア	4	2	■		■		■	■	
イタリア	7	2	■	■	■	■		■	
日本	1	1	■	■	■	■	■	■	
韓国	1	1	■	■	■	■		■	
メキシコ	5	3	■	■	■	■	■	■	■
オランダ	1	1	■		■	■		■	■
ロシア	1	1	■	■	■				
サウジアラビア	1	0	■		■	■			
シンガポール	1	1	■	■	■	■	■	■	
南アフリカ	1	0			■				
スペイン	1	0	■	■	■				
スイス	3	0	■	■	■	■	■	■	
トルコ	3	4	■	■	■		■	■	■
英国	3	3	■	■	■	■	■	■	■
米国	10	5	■	■	■	■	■	■	■
合計	85	35	24	19	25	19	16	18	8

出所：FSB報告書の表2より作成

■ 該当する法域

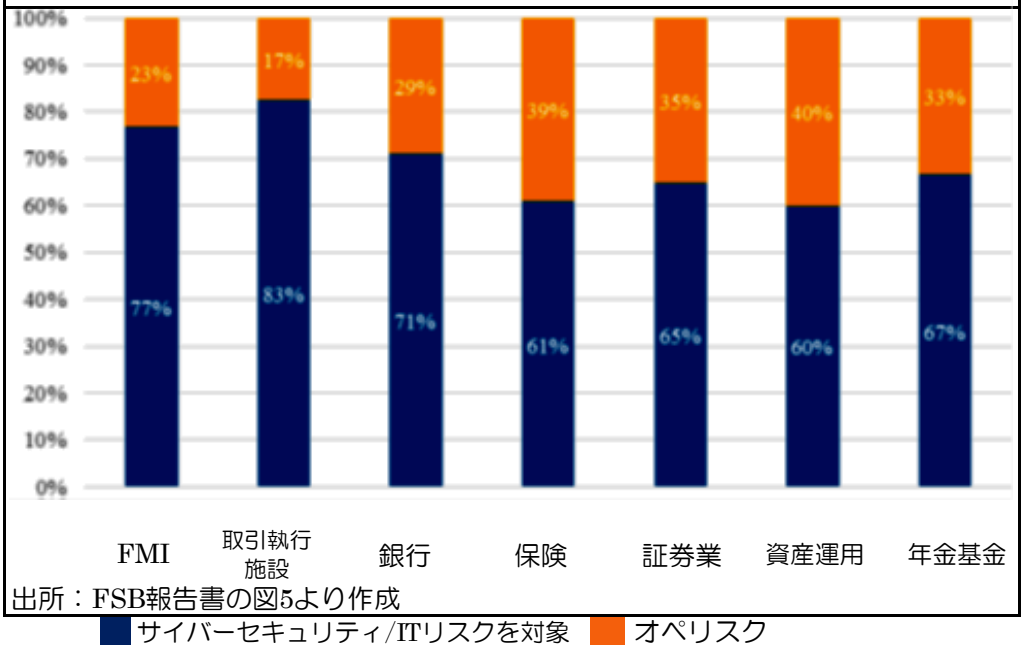
図表5：部門別の規制スキームがある法域数



今回の調査では、規制・ガイダンスはオペリスク全般が対象なのか、サイバーセキュリティ／IT リスクが対象かを尋ねている。全 85 の内 29 の規制スキームがオペリスクを、56 はサイ

バーセキュリティ／IT リスクが対象。部門別では取引執行施設と FMI でサイバーセキュリティ／IT リスクが対象である比率が高く、保険業、資産運用業、証券業は低い（図表 6 参照）。

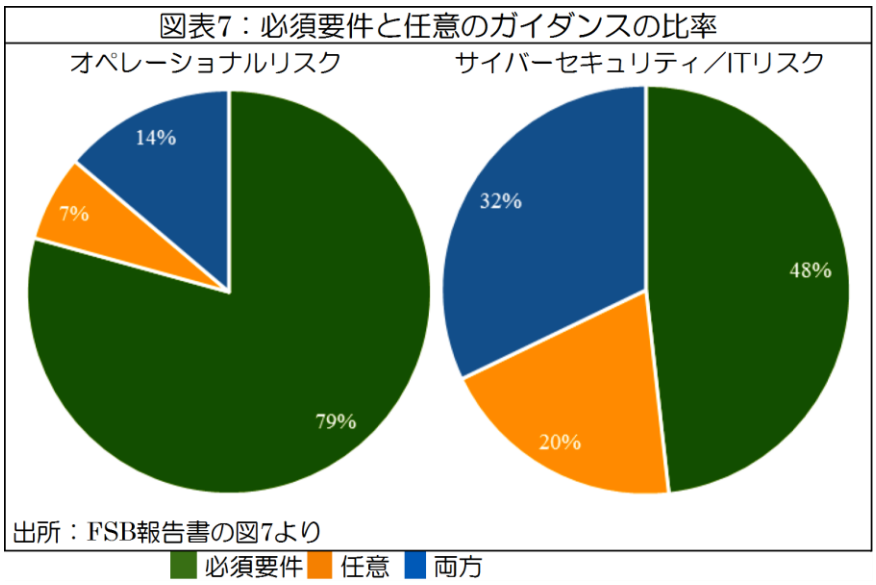
図表6：サイバーセキュリティ/ITリスクを対象とする規制スキームの部門別状況



出所：FSB報告書の図5より作成

また、規制スキームが必須の要件か、必須要件とガイダンスの組合せか、任意なガイダンスのみなのかを尋ねている。オペリスクを対象とした規制スキームでは大半が必須要件か必須要件とガイダンスの組合せで、ガイダンスのみは 7%に止まる。これに対してサイバーセキュリティ／IT リスク対象とした規制スキームでは、必須要件は 48%と半数に達せず、32%が必須要件とガイダンスの組合せ、ガイダンスのみが 20%だった。

図表7：必須要件と任意のガイダンスの比率



出所：FSB報告書の図7より

3. オペレーショナルリスクに対処する規制・ガイダンス

オペリスクを対象とした規制・ガイダンスは、プリンシプル・ベースか比例的な特性を持ち、規制対象機関が達成すべき目的が特定されている。例えば、ある情報システム管理スキームでは、情報システムセキュリティの定期的な評価の実施、深刻なシステム障害でも業務を継続するためのバックアップ手順が利用可能なこと、どんな場合でも情報の完全性と機密性が保たれることが特定されている。

他のスキームでは、各機関特有のリスクやビジネスモデルの複雑さ、特質と規模を考慮に入れた比例性のプリンシプルを反映し、適切で実効的な管理により規制対象機関に裁量の余地を与えているものもある。また、情報処理システムに関して実効的なプロセスと内部統制メカニズムを持つべきだとするスキームもある。

多くのオペリスクスキームは、規制対象機関が対処すべき要素を列挙している。

・ガバナンス：ボードと上級経営者の役割についての指摘が多い。あるスキームでは、リスク管理と内部統制機能に関してガバナンスは、分離され独立した内部監査機能を含め、十分な権限、独立性、資源、およびボードへのアクセスがあることを確実にすべきだとしている。

別のスキームでは、リスクの監視と管理および経営判断の通知のため、ボードが活用す明確なリスクアペタイト・ステートメント（承認と保持をボードが行う）に支えられたビジネス戦略と、明確に定義され透明で整合的な責任体系を伴う明瞭な組織構造を含んだ、頑健なガバナンス取決めを求めている。

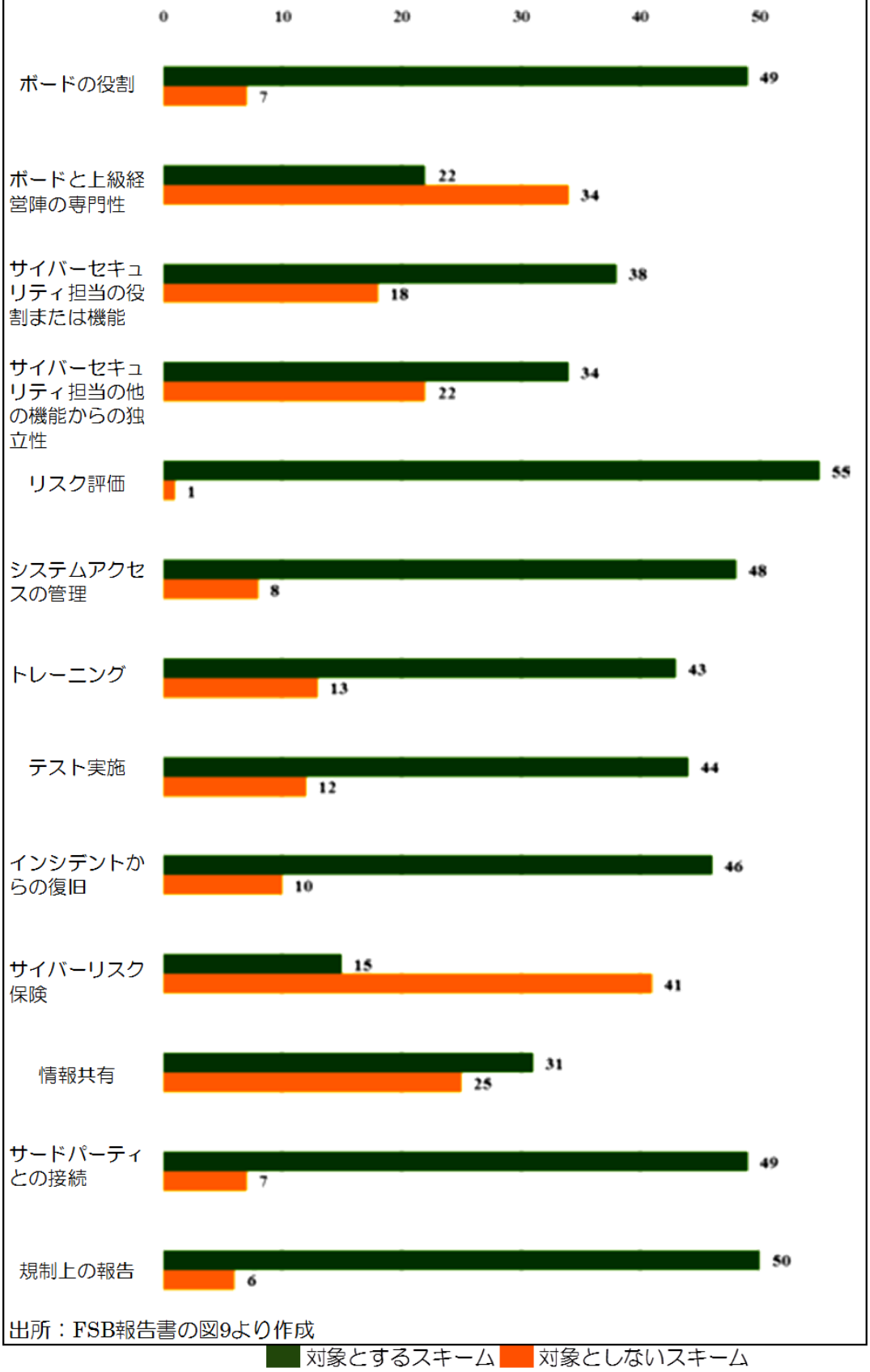
・リスク評価とリスク管理：あるスキームは、オペリスク・イベント、具体的には、システムと IT に関連するプロセスやインフラの不具合に、適切に対処するリスク管理枠組みを求めている。他のスキームは、決定的に重要なインフラについて、物理的なリスクおよびサイバーセキュリティリスクの双方を含むリスク評価を要請。別のスキームは、金融機関がビジネスの特質、規模、複雑さと比例して、その安全性および健全性と整合的な、頑健なリスク管理、財務上およびオペレーショナルな管理の枠組みを持つべきだとしている。

・その他の要素：オペリスクに対処する方針、プロセスおよび管理の確立、デジタル攻撃の防止および脆弱性の検知と削減、機密情報を含む情報の保護、情報システムのセキュリティテスト、バックアップサイトとディザスターリカバリー（障害・被害からの復旧）、事業継続計画、オペレーショナルイベントの規制当局への通知、運営の手順とシステムの独立したレビュー、サードパーティー・リスクなどが共通している。

4. サイバーセキュリティ／IT リスクに対処する規制・ガイダンス

56 の規制・ガイダンススキームがサイバーセキュリティ／IT リスクを対象とし、その内の 41 は、既存の各国または国際的なガイダンスや基準を取り入れている。調査では規制スキームがどんな特定の要素に対処しているかを尋ねている（図表 8 参照）。

図表8：特定トピックを含むサイバーセキュリティ／ITリスク規制スキーム数



出所：FSB報告書の図9より作成

図表 8 でまとめた情報をトピック毎に整理すると以下の通り。

規制スキームで取り上げられた特定のトピックの概要
・ボードおよび上級経営陣の役割と専門性
56規制スキーム中49スキームとかなり多くが、ボードや金融機関の全般的監督に責任を担う他の者のサイバーセキュリティでの役割に対応。これには、サイバーセキュリティ方針と戦略枠組みの承認、委任された機能についてのボードの説明責任、ボードに提供されるべき情報、リスク管理の役割、十分な人員および技術的、財務的な資源の割当てを含む。 一方、ボードや上級経営陣の専門性に対応しているスキームは56中22と半分以下である。専門性に対応したスキームには、ボードがリスク委員会および監査委員会に適切な質問を尋ねる能力、ボードによる専門家の雇用、サイバーリスクに関するボードの訓練などが含まれている。
・サイバーセキュリティについての役割
38規制スキームが、CISO（最高情報セキュリティ責任者）のようなサイバーセキュリティに責任を持つ役割または機能の創設に対応。この役割はしばしば必須のものである。34スキームがサイバーセキュリティ機能の他の業務からの独立性に対応している。
・システムアクセスの管理
48規制スキームが対応。適切なセキュリティ許可のある者のみにアクセスを制限。無許可のネットワークアクセスを自動的に検知しブロックする。追跡可能性を確実にするためにITシステムへのアクセス権限を持つ人員を特定して人数を制限し監視する能力やアクセス記録の保管と監視。
・訓練
43規制スキームが対応。顧客や技術スタッフ、非技術スタッフなどを含む訓練と教育の対象者の決定やスタッフのテスト。訓練の種類としてはサイバーセキュリテイの認識および攻撃や重大な懸念発生シナリオへの反応が含まれる。重大な懸念シナリオには、フィッシングやソーシャル・エンジニアリングなどによる被害、eメールやリムーバブルメディア経由のデータの喪失あるいはソーシャルメディアへの機密または私有情報の意図しない投稿などが含まれる。
・テスト
44規制スキームが対応。ハードウエアとソフトウエアの脆弱性検査、ペネトレーションテスト、システムの運用開始前のテスト、事業継続方針とディザスター復旧計画のテストおよびサイバーインシデント対応計画のテストを含む。
・インシデントからの復旧
46規制スキームが対応。シナリオ計画やコミュニケーション計画などの復旧計画。業務運営再開までに要する時間の特定およびサービス再開についての規定、サイバーセキュリティ・インシデント後のシステムの完全性の保証、喪失したか破損したデータの復旧、バックアップサイトなどの事項を含む。
・サイバーリスク保険
15規制スキームのみと最も対応が少ない。その内容では、こうした保険が、財務的な負担の軽減を提供したり、途絶の影響を削減したりするため、利用の検討をすべきと示唆するものが多い。
・情報共有
31規制スキームが対応。これには、通知の要否についての当局による決定と当局へのサイバーセキュリティや脅威情報の通知、同業者間での情報共有の要請、内部的な利害関係者への伝達を含むインシデント管理プロセス、金融機関の間での情報共有のプラットフォーム、金融部門の情報共有組織への参加、などが含まれる。
・サードパーティ接続
49規制スキームが対応。サードパーティやベンダーから生じるリスクの管理、外部委託方針およびリスクの特定、管理と監視を含む外部委託の管理、ITサービスの外部調達の前に行うリスク評価、サードパーティのサイバーレジリエンス計画のレビューとオンサイト評価を含む。また、サードパーティとの接続のリスク分析、外部委託契約で必要な条件、サードパーティ・サービス提供者の選定と監視の際のデュー・デリジェンスなどを含んでいる。
・規制上の報告
50規制スキームが対応。インシデントの特質やインシデント後にとられた措置、再発防止策などを含むインシデント報告。報告された情報の当局による使用。インシデント報告の時間的枠組み、セキュリティ違反や脆弱性、対応措置とその結果の年次報告が含まれている。

Ⅳ．監督上の慣行

監督上の慣行に関して法域毎の状況をみると、銀行部門は 25 法域中 16 法域が対応しているが、FMI では 12 で過半数をやや下回る。資産運用業では 10、証券業と取引執行施設はそれぞれ 9、保険業は 8 である。規制スキームと同様に年金基金では 4 と少ない。

いくつかの法域には複数の監督スキームがあり、25 法域合計で 35 監督スキームが報告されている。各法域と部門別の状況を整理すると図表 9 の通りである。なお、35 スキームの内 28 が、既存の各国および国際的なガイダンスや基準に基づいていると回答されている。

図表9：各法域の個別の監督上の慣行スキーム

法域／スキーム	部門							
	FMI	取引執行施設	銀行	保険	証券業	資産運用	年金基金	その他
アルゼンチン			■					
オーストラリア	■							
ブラジル						■		■
中国1		■			■	■		■
中国2			■					
EU1								■
EU2			■					■
フランス	■		■	■				
香港1	■		■					
香港2					■	■		
インド			■					
インドネシア1	■				■			
インドネシア2			■					
イタリア1	■							
イタリア2		■						■
日本	■	■	■	■	■			■
韓国	■	■	■	■		■		
メキシコ1	■	■	■		■	■		
メキシコ2	■		■					■
メキシコ3				■				
オランダ			■	■		■	■	■
ロシア			■					
シンガポール	■	■	■	■	■	■		■
トルコ1	■							
トルコ2			■					
トルコ3								■
トルコ4	■	■			■	■	■	
英国1	■							
英国2			■					■
英国3		■	■	■	■	■	■	■
米国1	■							■
米国2			■					■
米国3				■				
米国4	■	■			■	■	■	■
米国5	■	■						
合計	16	10	18	8	9	10	4	15

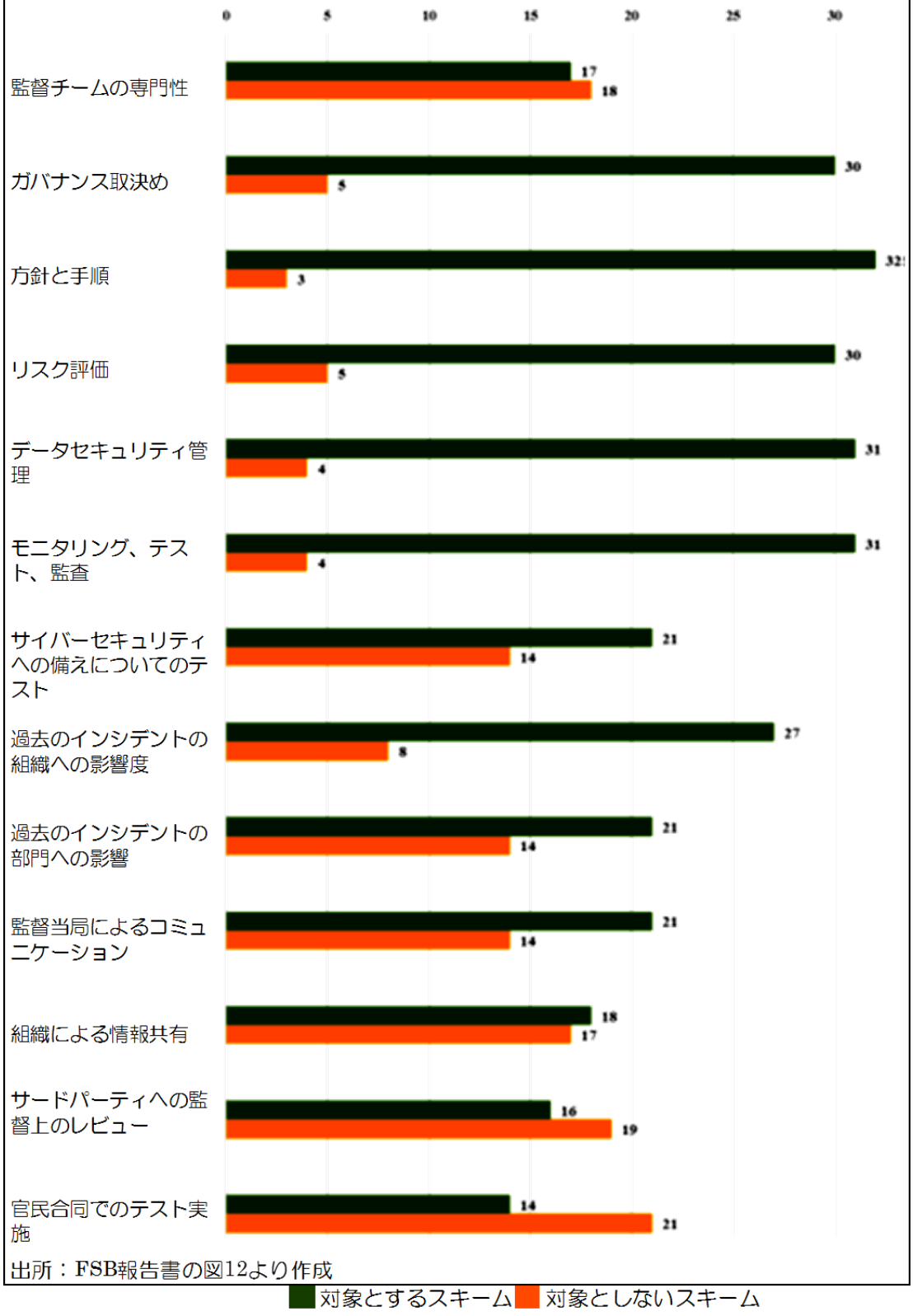
出所：FSB報告書の表5より作成

■ 該当する法域

（注）部門別“その他”は、その他信用提供機関、支払いサービス提供者、格付け会社等。

調査では監督上の慣行が対処している特定の要素について尋ねている。図表 10 は各法域からの回答（合計 35 スキーム）の内容を整理したもの。

図表10：特定トピックを含む監督上の慣行スキーム数



出所：FSB報告書の図12より作成

図表 10 でまとめた情報をトピック毎に整理すると以下の点通り。

監督上の慣行スキームで取り上げられた特定のトピックの概要
・監督チームの専門性
17のスキームが対応。サイバーセキュリティに関する詳細な知識、適切な経験、専門家としての資格、技能と継続的な訓練、外部専門家の雇用およびITでの経歴などに言及。
・ガバナンス取決め
30のスキームが組織のサイバーセキュリティに関するガバナンス取決めのレビューに対応。これには、情報セキュリティへの責任に関する独立した役割、ITに関連した意志決定に関する責任と義務の明確さ、サイバーセキュリティに関するガイダンスと戦略設定でのボードの構造と関与を含む。
・方針と手順
32のスキームがサイバーセキュリティに関する方針と手順に対応。これには、サイバー脅威インテリジェンスの共有とインシデント対応、機密情報保護の手順と情報セキュリティ方針の検証、サイバーリスクおよび複雑さと比例していてボードが承認したサイバーセキュリティ方針が実施されているか、を含む。
・リスク評価プロセス
30のスキームが対応。リスク評価プロセスが実効的か、定期的なリスクの特定と監視のプロセス確立、ITリスク評価の結果が適切に活用されているか。リスク評価の定期的な当局への提出。リスク評価が脅威とサイバーリスクへの脆弱性についての適切なデータ収集に支えられているかの検証を含む。
・データセキュリティ管理
31のスキームが対応。データバックアップと復旧方針、データの追跡可能性、認証と承認および監視と記録の蓄積などを含む。
・モニタリング、テストおよび監査
31のスキームが対応。脅威の監視と監査証跡、ペネトレーションテストと脆弱性検査が定期的に適用されているか、コンピューターウィルスおよび悪意のあるコードを検知する手段の利用手順などを含む。
・監督当局によるテスト／監督当局へのテスト結果の提出
21のスキームが対応。いくつかの監督当局は、業界全体の演習とともに、金融機関へのペネトレーションテストを実施するか、または金融機関にペネトレーションテストの評価結果の提出を要請している。
・過去のインシデントの組織および金融部門への影響度
27のスキームが対応。また、21のスキームではある金融機関へのインシデントの影響が、他の金融機関または金融部門に及ぼす潜在的な影響を評価するインシデント・レビューに対処している。いくつかの監督当局は、金融部門の安定に危害を及ぼしかねない障害に対する金融部門全般の対応を組織するメカニズムについて報告している。これには、コミュニケーション計画、同じインシデントが他所で起きたか、部門全体にどんな影響があったか確認するためのある金融機関のインシデントの事後フォローを含む。
・監督当局によるコミュニケーション
21のスキームが対応。問題への対応手段には、共有すべき情報の基準、他の国内および国際的な当局との窓口の確立と法の執行、情報共有の覚書および法域全体でのインシデント対応枠組みを含む。
金融機関による情報共有
18のスキームが対応。これには、金融機関から当局への報告がタイムリーだったか及び金融機関がサイバー脅威インテリジェンス共有の方針と手順を持っているかに関するレビューと、金融機関に情報共有組織への参加を促すことを含む。
・サードパーティへの監督上のレビュー
16スキームが対応。サードパーティとはサイバーセキュリティに影響を及ぼすベンダーなど。ときには監督当局は外部パートナーの施設で実地に重要なIT活動のレビューを行う。サービス提供者へのアクセスは、適用される法令で直接、または外部委託契約にアクセス権限を含むように要請することで得られる。
・官民合同でのテスト実施
14のスキームが対応。こうした演習のいくつかは金融部門内部やその一部で実施されているが、他の演習には部門横断的で複数の極めて重要なインフラ部門を含み、複数の法域が関与したものもあった。

Ⅴ．今後の計画、実効性のある慣行

1．今後の計画・課題

報告書によればオーストラリア、中国、EU、シンガポール、米国など 18 法域が金融部門のサイバーセキュリティに関する新たな規制・ガイダンスや監督上の慣行の策定を計画。

これらの計画で取り上げられる課題には、下記のものがある。

・金融部門のサイバーセキュリティの規制、ガイダンスおよび戦略の開発
・FMI のサイバーレジリエンスを評価するための自己評価演習
・サイバー脅威インテリジェンスに基づくサイバーレジリエンス・テスト実施ガイダンス
・情報技術リスク（サイバーを含む）の業界基準の開発と既存のガイダンスの更新
・コンピューター非常時対応チーム（セキュリティインシデント対応を含む CERT）設立

2．実効性のある慣行

サイバーセキュリティ対応に実効性があるとされた主な実務・慣行を列挙すると以下の通り。

・既存のガイダンスや基準：CPMI-IOSCO のガイダンスに多くの法域が言及。
・プリンシプルベース、リスクベースまたは比例的な監督：リスクの特定と評価、決定での健全な判断の適用。利用可能な監督及び規制の選択肢から最も適切な手段の決定。監督は、金融機関の特質、規模、複雑さおよびリスクプロファイルと比例的なものであるべき。
・ボードと上級経営陣の役割：経営陣の説明責任の重要性。上級経営者の重要性、ボードレベルのサイバーセキュリティの注意、認識、責任。CISO の任命。
・リスク管理の独立性：独立の技術的なリスク管理の重要性。
・方針と手順：規制対象機関はサイバーセキュリティ管理の方針、手順とプロセスを確立。

・当局と規制対象機関のコミュニケーション：効果的な規制・ガイダンスは、当局と規制対象機関との持続的な対話で一層、達成される。当局は規制対象機関が規制/ガイダンスに現実に適合するためには何が重要な問題なのかを、十分に理解しなければならない。
・協調と情報共有：法令執行当局を含む国内・海外当局との協調と情報共有および国際的組織との協働は効果的である。緊急時協調システムの確立と緊急時協調計画の改善も言及されている。脅威インテリジェンスやサイバーインシデントおよびベストプラクティス情報を含む当局と規制対象機関、金融機関同士の情報共有についても指摘あり。
・サイバーセキュリティ要件の特定と更新：より重要だと考えられる特定分野に対処する要件を含め、金融部門のサイバーセキュリティ要件を特定し更新。
・外部委託のリスク：外部委託リスクの強固な管理の重要性を指摘。

・監督上のサイバーセキュリティに対する手段としては以下が言及されている。

金融機関のサイバー・ロードマップのレビュー。サイバーリスク管理の適切性の評価に焦点を当てた検査を含む実地検査及びオフサイト、レビュー。業界全体の準備状況演習。サードパーティーの監査と評価。金融機関の自己評価、当局策定の手段（再現および測定可能なプロセス）

によるものを含む。ペネトレーションテスト、脆弱性テスト、レッドチーム（攻撃チーム）演習を含むテスト。サイバーインシデントを防ぎ検知するための金融機関の管理のレビュー。監督当局へのサイバーインシデントの通知。過去のサイバーインシデントのレビュー。
コンプライアンス・レビュー.特定分野の懸念の助言とガイダンス。行政上の罰金と罰則。

・システミックリスクの評価：クロスボーダーおよびクロスセクターの脅威と金融部門のシステミックリスクの評価の重要性が言及されている。

Ⅵ．国際機関によるガイダンスおよびその他の活動

1．サイバーセキュリティに関する国際機関から FSB への回答

FSB のサイバーセキュリティ調査には下記の国際機関・組織が回答している。

バーゼル委員会（BCBS)、グローバル金融システム委員会（CGFS)、決済・市場インフラ委員会（CPMI)、G7 サイバーセキュリティエキスパートグループ（G7CEG)、保険監督者国際機構（IAIS)、国際会計基準審議会（IASB)、国際通貨基金（IMF)、証券監督者国際機構（IOSCO)、経済協力開発機構（OECD)、世界銀行（WB）

BCBS、CPMI、G7CEG、IOSCO、OECD は、サイバーセキュリティに関するガイダンスを公表（CPMI と IOSCO は共同)、CPMI、IAIS、IOSCO、OECD は、その他のサイバーセキュリティ関連の文書を公表。また、BCBS、CPMI、G7CEG、IAIS、IMF、IOSCO、OECD、WB は、サイバーセキュリティについての作業を実施、あるいは計画している。

ガイダンスの対象は様々で、BCBS は電子バンキング、CPMI-IOSCO は FMI、G7CEG は金融部門の規制・監督対象機関全般、OECD は重要な情報インフラと全部門の経済・社会活動が対象。公表の時期も BCBS は 2003 年で CPMI-IOSCO と G7CEG は 2016 年である。

こうした違いにもかかわらず､各機関のガイダンスがカバーするトピックスは図表 11 のように整理ができ、内容的には共通性がある。

図表11：国際機関のガイドラインに含まれるトピックス

	BCBS	CPMI-IOSCO	G7CEG	OECD
ガバナンス	○	○	○	―
リスクの分析と評価	○	○	○	○
情報セキュリティ	○	○	○	○
セキュリティ管理とインシデント防御	○	○	○	○
専門性と訓練	○	○	○	○
監視、テストおよび／または監査	○	○	○	○
インシデント対応と復旧	○	○	○	○
コミュニケーションと情報共有	○	○	○	○
接続の監督	○	○	○	○
継続的な学習	―	○	○	○

出所：FSB報告書より筆者作成

2. 各国際機関が公表した主なガイダンス

①CPMI-IOSCO：「金融市場インフラのためのサイバー攻撃耐性（レジリエンス）に係るガイダンス」2016 年 7 月(9)

本ガイダンスの目的はサイバーレジリエンスを高めるための指針の提供であり、ガバナンス、特定（重要な機能や情報資産の優先順位付け）、防御、検知および対応と復旧など、FMI のサイバーレジリエンス枠組みに亘って対処すべきテーマを含む。ガイダンスは、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）および FMI 間リンク（原則 20）に関する補足的なガイダンスの提供を意図する。

ガイダンスに含まれる主な分野は以下の通り。

・サイバーレジリエンス枠組み：FMI は、広範な金融安定の目的を支持し運営の安全性と効率性の高度な優先度と一致する、明確で包括的なサイバーレジリエンス枠組みを持たねばならない。枠組みは、サイバーリスクを如何に効果的に特定し軽減し管理するか、サイバーレジリエンス目標とサイバーリスク許容度を如何に決定するかを明確にするべきである。
また、サイバーリスク管理の人員、プロセス及び技術的な要件の概要を説明し、適切な利害関係者と効果的に協調するための、タイムリーなコミュニケーションを含むべきである。

・ガバナンス：実効的なガバナンスは、明確で包括的なサイバーレジリエンス枠組みから始めるべきであり、レジリエンス枠組みを支える FMI のボードと上級経営陣の役割と責任が明確なことが不可欠である。接続するサービス提供者が FMI のサイバーレジリエンスに重要な責任を担い、全スタッフに認識される文化を造ることも、ボードと上級経営陣の責務である。

・リスク評価：FMI は、ビジネス機能と支援プロセスを特定しリスク評価をすべきである。特定されたビジネス機能と支援プロセスは重要度で分類され、FMI の保護、検知、対応と復旧の取組みにおける優先順位の指針となる。FMI は情報資産のリスク評価も行うべきである。

・IT セキュリティ：どの業務活動と支援する情報資産がセキュリティ侵害から保護されるべきか優先順位を特定することが重要である。サイバーレジリエンスは、FMI の資産とサービスの機密性、完全性と可用性を保護する、効果的なセキュリティ管理とシステム、プロセスデザインに依存している。

---

9 日本銀行 HP：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」の公表について、2016 年 7 月参照。
http://www.boj.or.jp/announcements/release_2016/rel160706a.htm/

・訓練：スタッフが、サイバーリスクを検知し対処する適切な認識と能力を、開発し維持する訓練を受けることを確実にする。異常な活動やインシデントを報告する訓練も受けるべきである。ハイリスク・グループは特定された情報セキュリティ訓練を受けるべきである。

・監視、テストおよび監査：継続的な監視能力を確立し、異常な活動やイベントを検知すべきであり、公知のおよび知られていない脆弱性の検知を目指すべきである。検知能力は、サービス提供者や信頼できるエージェントの誤ったアクセス、潜在的なインサイダーの脅威や他の高度な脅威活動にも対処するべきである。
サイバーレジリエンス枠組みの要素は、実効性判定のため厳格にテストされるべきである。テスト範囲は、脆弱性評価、シナリオに基づくテスト、ペネトレーションテストやレッドチームを用いたテストを含む。FMI のサイバーレジリエンス枠組みへの妥当性と準拠性は、独立したコンプライアンスプログラムと適格者による監査で定期的に評価・測定されるべきである。

・対応と復旧：FMI は、被ったダメージと共にインシデントの特質と程度を判定するため徹底した調査をすべきである。状況を抑え込み、更なる被害を防ぎ、対応計画に基づいて業務活動を回復するための復旧活動を開始するように、直ちに行動すべきである。
FMI は、重要な業務を 2 時間以内に再開できねばならず、この目標が達成できなかった場合のシナリオを計画し、重要な取引の処理を促進するため、再開と復旧活動を優先順位付けなければならない。また、極めて重要な人員、プロセスまたはシステムがかなりの期間利用できない状況についても計画しなければならない。

・コミュニケーションと情報共有：サイバーレジリエンス枠組みは、関係者との効果的な協調を可能にするタイムリーなコミュニケーションを含まねばならない。FMI は監督・規制当局に、潜在的に重要またはシステミックなイベントを直ちに連絡しなければならない。
　大規模なインシデントへの部門全体の対応を促進するため、イベントやインシデントに際して信頼できるチャネルを通じた情報共有、自己のシステムと部門の参加者のシステムの検知・対応、再開と復旧を促進するタイムリーな情報の収集と交換を計画しなければならない。
　FMI は、積極的に情報共有グループに参加し、サイバー実務、サイバー脅威およびサイバー脅威に関する早期警戒指標の情報を提供し、評価しなければならない。

・継続的な学習：リスクの実効的な管理を可能にするため、サイバーリスクのダイナミックな性質とともに変化する、適応性のあるサイバーレジリエンス枠組み導入が重要である。FMI は、サイバーレジリエンスの状態の継続的再評価と改善を、組織のあらゆるレベルで行っていることを示すべきである。

・サードパーティーとの接続：FMI のサイバーレジリエンス枠組みは、FMI が参加者や他の FMI、ベンダー、ベンダーの製品やサービス提供者から被るサイバーリスクを、如何に定期的

にレビューし積極的に軽減するか考えるべきである。ガイダンスは、サードパーティーとの接続で生じるサイバーセキュリティ問題に対処する FMI の責任を定義している。

②G7CEG：「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(10)」
G7 の基礎的要素の目的（財務省（仮訳）を参照した）
「基礎的要素」は、個々の金融機関が、自らのリスク管理や企業文化に関する認識を踏まえた上で、サイバーセキュリティ・ストラテジーやその運用のフレームワークを策定・実施するにあたり土台としての役割を果たす。また、「基礎的要素」は、個々の金融機関が、業務や脅威を巡る環境の変化に応じてサイバーセキュリティ・ストラテジーとフレームワークを体系的に見直すダイナミックなプロセスに向けての手順を提供する。
一国の、または国を跨る当局も「基礎的要素」を自身の政策、規制・監督上の取組みのガイドとして利用できる。民間・公的金融機関と当局は「基礎的要素」を踏まえつつ協働し、国際的な金融システムにおけるサイバーセキュリティやレジリエンスを全般的に強化できる。

ガイダンスに含まれる主な分野
・サイバーセキュリティ・ストラテジーとフレームワーク：金融機関と当局は、サイバーセキュリティ・ストラテジーとフレームワークを、特定のサイバーリスクに適合させ、国際基準や国内及び業界の基準とガイドラインを適切に踏まえて構築し維持すべきである。戦略と枠組みは、金融機関の特質、規模、複雑さ、リスクプロファイルと文化に合わせるべきである。

・ガバナンス：金融機関と当局は説明責任を確保するため、サイバーセキュリティ・ストラテジーとフレームワークの実効性を実施、管理、監督する人々の役割と責任を定義し、促すべきである。十分な資源、適切な権限と統治機関（ボードまたは公的機関であれば上級職員）へのアクセスを付与すべきである。ボード等は、機関のサイバーリスク許容度を設定し、サイバーセキュリティプログラムに関する設計、実施および有効性を監督すべきである。

・リスク評価：金融機関と当局は、相互接続や依存度、サードパーティーの状況も踏まえ、機能、活動、製品とサービスを特定し、相対的な重要性を優先順位付けし、それぞれのサイバーリスクを評価すべきである。リスクを防御し、統治機関が設定した許容度内に管理するための制御手段（システム、方針、手順と訓練を含む）を特定、導入すべきである。
防御メカニズムには、特定の活動を行わないことによるリスクの回避や排除、リスクの制御や移転による軽減も含む。リスクと制御の評価では、当該機関が他の機関や金融部門全体に及ぼすあらゆるサイバーリスクを適切に考慮すべきである。

---

10 金融庁 HP：金融セクターのサイバーセキュリティに関する G7 の基礎的要素の公表について 2016 年 10 月を参照。
https://www.fsa.go.jp/inter/etc/20161011-2.html

・情報セキュリティ：理想的には、エンタープライズリスク管理プログラムの一部として、各機能・業務・製品・サービスを支える、人員や業務プロセス、技術及び基盤となるデータがもたらす本来的サイバーリスク（または、対応手段がないリスク）を評価すべきである。各機関は、特定されたリスクから防御する制御手段の存在と有効性を評価すべきである。

・訓練：訓練はサイバーリスクを防ぎ、管理するために可能な制御手段の一つである。

・監視、テストおよび監査： 金融機関と当局は、サイバーインシデントを迅速に検知する系統だった監視プロセスを確立し、徹底したネットワークの監視、テスト、監査、演習を含め、特定された制御の有効性を定期的に評価すべきである。
機関の特質とサイバーリスク・プロファイルおよび制御環境に応じて、テストと監査の機能は、サイバーセキュリティプログラムを導入し運営する責任がある者から、適切に独立していなければならない。徹底した検査、実地検査およびその他の監督メカニズム、当該機関のテスト結果の比較分析および官民合同の演習により、公的当局は、個々の機関の相対的なリスクプロファイルと能力とともに、部門全体のサイバー脅威と脆弱性をよりよく理解できる。

・インシデント対応と復旧：金融機関と当局は、タイムリーにサイバーインシデントの性質、範囲、影響を評価し、インシデントを抑え、影響を軽減し、内部・外部の関係者に伝え、必要な共同での対応活動について協調すべきである。
また、インシデントの有害な残滓の除去を含む継続的な是正を行いつつ、業務活動を責任を持って再開し、システムとデータの正常さを修復し正常な状態を確認し、悪用された全ての脆弱性を特定し軽減し、類似インシデントを防ぐために脆弱性を是正し、内部・外部に適切に伝達するべきである。

・情報共有：金融機関と当局は、防御を強化し被害を限定し、状況認識を向上させ学習を広げるため、脅威や脆弱性、インシデントと対応に関する、信頼性があり実用的なサイバーセキュリティ情報を、内部、外部の関係者（金融部門内外の機関と公的当局を含む）とタイムリーに共有すべきである。

・継続的な学習：サイバーリスクの変化に対処し、資源を配分し、ギャップを特定し改善し、教訓を活かすため、サイバーセキュリティ・ストラテジーとフレームワークを定期的かつ必要に応じてレビューすべきである。

③BCBS:「電子バンキングにおけるリスク管理の原則」2003 年 7 月(11)
ガバナンス、情報セキュリティ、セキュリティ管理、専門性、インシデントからの復旧、コミュニケーション、外部委託された業務についてまとめている。

④OECD は次の 2 つのガイダンス文書を公表している。

・「重要情報インフラの保護に関する理事会勧告（Recommendation of the Council on the Protection of Critical Information Infrastructures(12)）」2008 年 6 月

この勧告は、重要な情報インフラを保護する政策の開発に関して各国政府を支援するガイダンスを提供する。OECD は、多くの国では金融部門で活動するものは重要な情報インフラだとしている。なお、OECD は本勧告を見直す作業を行っている。

・「経済と社会の繁栄のためのデジタルセキュリティ・リスク管理に関する理事会勧告（Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity(13)）」2015 年 9 月

この勧告の目的は、政府、企業および個人が、デジタル信頼性を高めデジタル転換の利益を最大化するために、経済および社会的なリスクとしてのデジタルセキュリティへの対処を支援することである。本勧告は、企業のデジタルセキュリティ方針と政府の国家セキュリテイ戦略の開発を導くため、公的および民間組織の指導者と意思決定者に高いレベルの原則を提供する。また、各国の戦略に対するより詳細な公共政策ガイダンスも提供する。

3. 国際機関によるその他の文書と今後の計画

・サイバーセキュリティ関連でガイダンス以外に国際機関が公表した文書は下記の通り。

CPMI：2014 年 11 月、「FMI のサイバー攻撃耐性」報告書を公表。

IAIS：2016 年 8 月、「保険部門のサイバーリスク」報告書を公表。

IOSCO：2016 年 4 月、「証券市場におけるサイバーセキュリティ」報告書を公表。

OECD：サイバーセキュリティ関連で 8 つの文書を公表している。これらの文書は金融部門に焦点を当てたものではないが、複数の重要なトピックについて、デジタルトランスフォーメーションの文脈でのサイバーセキュリティなど経済・社会への影響といった広い観点を踏まえて対応するものである。

・各国際機関の今後の計画には以下が挙げられている（足元での動きを（）で若干補足）。

BCBS：今後の 2 年間で、サイバーリスクに関連した追加の方針および／または監督上の手段の開発を検討。

CPMI：IOSCO と共同ワーキング・グループで 2018 年末まで FMI のサイバーレジリエンスについて活動。CPMI - IOSCO のガイダンスの実施状況を監視し推進。ベストプラクティスと評

---

11 日本銀行 HP を参照：http://www.boj.or.jp/announcements/release_2003/data/bis0307b.pdf

なお、2018 年 12 月バーゼル委は、サイバーレジリエンスに関する各国の多様な実務を整理した“Cyber-resilience: range of practices”を公表している。 https://www.bis.org/bcbs/publ/d454.htm

12 https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/OECD_digital-security-risk-management_0.pdf

13 https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/OECD_digital-security-risk-management_0.pdf

価方法の情報共有を実施。2016 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・タスクフォース設立。銀行、FMI、その他金融機関が関連する（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」に関する市中協議文書、2018 年 5 月には「大口資金決済システムにおける不正リスクの削減」を公表）。
IOSCO：CPMI と共同で活動中。

G7CEG：2017 年 10 月に「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 G7 の基礎的要素」を公表。サードパーティリスク、非金融部門との協調について作業を進める予定（なお、2018 年 10 月に「脅威ベースのペネトレーションテスト」及び「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 の基礎的要素について」を公表）。

IAIS:既存の保険コア原則（ICP）について検討中。サイバーセキュリティへのコア原則の適用に関する文書を 2018 年に公表する計画。

IMF：メンバー各国の政策を IMF がモニターする際の基礎となるサーベイランスシステムに関連して、サイバーリスクに関するパイロット作業を実施中。

OECD：デジタルセキュリティとプライバシーの改善について、この分野の統計指標の開発を通じて活動中。また、1997 年の「暗号政策に関するガイドライン」と 2008 年の「重要情報インフラの保護に関する理事会勧告」改訂を作業中。

WB:国際電気通信連合（ITU）とのパートナーシップで金融インフラのサイバーセキュリティの作業中。世銀グループ（WBG）は、各国政府のサイバーセキュリティ戦略の開発を支援。
NIST（米国国立標準技術研究所）のサイバーセキュリティ枠組みに基づく評価を行う「サイバーセキュリティ診断ツールキット」を開発。
各金融当局にサイバーインシデントに対処する役割を見出させるために、危機のシミュレーション演習を実施。新興市場諸国のサイバー犯罪との戦いのためのツールキットを開発。

以上

補論 1．サイバーセキュリティとサイバーレジリエンス（FSB 報告書 BOX1 より）

～FSB メンバーが報告したサイバーセキュリティとサイバーレジリエンスの定義の事例

・サイバーセキュリティ

アルゼンチン：5 つの関連し統合された情報セキュリティプロセス（認識、アクセス管理、保全と記録、管理と監視、インシデント管理）から構成されるサイクル。

中国：情報の収集、移送、交換および保管に際して、情報の有用性、機密性、無損傷性および非否認性を確保するために技術と管理を用いること。
サイバーセキュリティには、インターネットセキュリティ、システムセキュリティおよびコンテンツセキュリティを含み、全てのレベルのセキュリティ、即ち、物理的環境、インターネット、メインフレームシステム、デスクトップシステム、データ、アプリケーション、ディザスターバックアップ（障害を想定した備え）、セキュリティ管理および職員を対象としている。

香港：サイバー攻撃から保護または防御する能力。攻撃とは組織の IT システムとネットワークを標的として、途絶、無能化、破壊するか、または悪意を持って IT システム／ネットワークを制御し、組織のデータの完全性を破壊するかまたは情報を盗むことを指す。

インド：サイバー攻撃を防ぎサイバーレジリエンスの向上を意図する方法、手段およびプロセスである。サイバーレジリエンスは、サイバー攻撃に備え対応し、サイバー攻撃の間も業務を継続し復旧する能力である。

イタリア：攻撃が物理的なものかあるいは論理セキュリティ侵害によって開始されたものかに関わらず、情報システム資産とコミュニケーションネットワークをあらゆる非物理的な攻撃から守るために用いられる管理および組織的な手段と方法（人的、技術的等）。

サウジアラビア：メンバー組織の情報資産を内部および外部からの脅威から守る、手段、方針、セキュリティ概念、セキュリティ保護、ガイドライン、リスク管理アプローチ、行動、訓練、ベストプラクティス、保証および技術の集まり。

・サイバーレジリエンス

CPMI-IOSCO：サイバー攻撃を予期し、耐性を備え、封じ込め、迅速に復旧する FMI(金融市場インフラ)の能力。

オーストラリア：サイバー攻撃に備え、対処し、復旧する能力。サイバーセキュリティは、連関する脅威からデジタル資産を護ることの実践である。レジリエンスは、単に攻撃を防ぎまたは対処すること以上のものであり、そうしたイベントの最中でも業務を運営し、適応し復旧する能力も考慮する。

補論 2. 金融分野のサイバーセキュリティに関する日本での動き

サイバーセキュリティ基本法が 2015 年 1 月に施行されている。これに基づき内閣に「サイバーセキュリティ戦略本部」が、内閣官房に「内閣サイバーセキュリティセンター（NISC）」が設置された。金融庁が規制監督当局として金融分野のサイバーセキュリティを担当する。

・金融庁の取組み

金融分野のサイバーセキュリティに関する対応強化のため、金融庁は「金融分野におけるサイバーセキュリティ強化に向けた取組方針」を最近アップデートしている（注7参照）。

この背景として、デジタライゼーションの加速や金融業の抜本的な変革の動きにより、利便性向上や経済の生産性向上の可能性が期待される一方、サイバーセキュリティに係るリスクがより一層高まる恐れが指摘されている。実際、サイバー攻撃事案は高度化・複雑化している。

図表補論（1）：近年の金融分野における主なサイバー攻撃事案等

動機	対象	主な攻撃手法	事案の概要
政治的な信条	金融機関	✓ DDoS攻撃によるWebサイト等のサービスの停止	◆ 国内の金融機関や金融庁等、複数の組織のWebサイトに対してDDoS攻撃による被害が発生。また、標的となった組織と同一のWebホスティング会社を利用する金融機関にも影響
情報の窃取		✓ メール等による標的型攻撃 ✓ サーバ等に対する不正アクセス	◆ 国内金融機関のメールサーバに対して不正アクセスが発生し、顧客の氏名、住所、口座番号等の顧客情報が漏えい（2016年9月） ◆ 国内金融機関のWebサイトに対して不正アクセスが発生し、顧客のIDや氏名、住所、生年月日等の顧客情報が漏えい（2017年7月） ◆ 金融機関のWebサイトがサイバー攻撃により改ざんされ、当該Webサイトを閲覧した利用者が悪意のある外部サイトに誘導されるとともにマルウェアをダウンロードさせられる事案が発生
金銭目的		✓ 金融機関自身への攻撃による不正送金	◆ バングラデシュ中央銀行で国際的な送金システム(SWIFT)に利用されているPCが遠隔操作され、不正に多額の資金が窃取（2016年2月）（その後同様の事案が台湾、ネパール等でも発生） ◆ 仮想通貨交換業者において、外部からの不正アクセスにより、仮想通貨の大規模な不正流出が発生（2018年1月、9月）
		✓ 金銭を目的としたDDoS攻撃	◆ 複数の金融機関が、期日までに身代金としてビットコインを支払わなければDDoS攻撃を仕掛ける旨の脅迫メールを受信するとともに、短時間のDDoS攻撃による被害も発生（2017年6月、9月）
	顧客	✓ 顧客PCのマルウェア感染	◆ インターネットバンキング利用者のIDやパスワードを窃取するマルウェアが発生。最近では仮想通貨取引所の利用者もターゲットとするマルウェアも確認

【出典】各種公表資料等より作成

出所：金融庁「金融分野におけるサイバーセキュリティ強化に向けた取組方針」2018年10月

また、海外の経験を踏まえると、東京オリンピック・パラリンピック開催に向けて、金融分野を含む我が国の重要インフラ事業者等がサイバー攻撃のターゲットとなる可能性がある。

・このため、①デジタライゼーションの加速的な進展を踏まえた対応、②国際的な議論への貢献・対応、③2020年東京オリパラ大会等への対応、が必要とされている。

補論注 1：(参考)　サイバーセキュリティ基本法

http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000104#2

サイバーセキュリティ戦略の概要 2018 年 7 月

https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-zentaigaiyou.pdf

・これまでの進捗を踏まえ、新たな課題に対応する施策として以下が挙げられている。
①金融機関のサイバーセキュリティ管理態勢の強化
平時のサイバー対策～大手金融機関には海外大手金融機関のベストプラクティスも踏まえて対話を高度化。中小金融機関には業界団体を通じた底上げ、実態把握、立入検査。
インシデント対応～大手金融機関はG7諸国の当局が連携して実施する合同演習への参加を支援、「脅威ベースのペネトレーションテスト」等の高度な評価手法の活用を促す。中小金融機関では金融庁演習やNISC等の演習への参加。
②情報共有枠組みの実効性向上（金融ISAC、FISC等とも連携し「共助」促進）
③金融分野の人材育成の強化（「戦略マネジメント層」の育成・定着など）

（参考）サイバーセキュリティ関連の資料・情報
　金融庁はHPで、サイバーセキュリティ対策について紹介するとともに、国際的な動向などについての情報提供を行っている(注2) 内容は“金融庁の取組み”“金融業界横断的なサイバーセキュリティ演習”“国際的なサイバーセキュリティに関する取り組み”“委託調査”“監督指針等の改正について”である。

・業界横断的なサイバーセキュリティ演習では、参加企業・対象を広げ、業界毎のシナリオやブラインド方式を採用するなど、内容を強化して実施していることを紹介。
・国際的な取組みでは、G7CEGの報告を順次紹介している（2018年は「脅威ベースのペネトレーションテスト」及び「サードパーティーのサイバーリスクマネジメント」）。

・委託調査では、今までの成果として下記の報告書を掲載している。諸外国の動向やCISOの役割、各国で強化されてきている脅威ベースのペネトレーションテストなど、金融機関の対応強化に資するような資料提供が図られている(注3)。
「諸外国の「脅威ベースのペネトレーションテスト(TLPT)」に関する報告書」
「金融機関のサイバーセキュリティ対策における経営陣・CISO等に期待される役割・責任に関する調査研究」
「『FFIEC Cybersecurity Assessment Toolに関する調査研究』調査報告書」
「諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書」

補論注2：金融庁HP参照。　https://www.fsa.go.jp/policy/cybersecurity/index.html

補論注3：日本銀行からは下記の資料が公表されている。

金融システムレポート別冊：“サイバーセキュリティに関する金融機関の取り組みと改善に向けたポイント― アンケート（2017年4月）調査結果 ―”2017年10月 http://www.boj.or.jp/research/brp/fsr/fsrb171016.htm/

“第18回決済システムフォーラムの議事の概要”2018年4月（サイバーセキュリティやサイバー攻撃耐性（サイバーレジリエンス）の問題に焦点を当てている） http://www.boj.or.jp/announcements/release_2018/rel180418a.htm/