Vol.2019-EIP-83 No.9
2019/2/15

金融機関におけるサイバーセキュリティに関するリスクマネジメントの考察

小梶顯義† 原田要之助‡

概要：金融機関のサイバーセキュリティに関するリスクは増大しているが，そのマネジメントに関する手法や標準は確立されていない．また，国際機関，国，公的機関，利用者等から金融機関に対するサイバーセキュリティ態勢を強化する要求も高まっている．これらの状況を踏まえ，本稿では，金融機関におけるサイバーセキュリティ態勢強化に対する期待や規制，リスクマネジメントの手法や動向についての研究結果を示す．また，そのうえで今後の金融機関におけるサイバーセキュリティに関するガバナンスについて考察する．

キーワード：金融機関，サイバーセキュリティ，リスクマネジメント，ISO/IEC31000，ISO/IEC27014

A consideration of risk management on cyber security in financial institutions

AKIYOSHI KOKAJI YONOSUKE HARADA

Abstract: Risks related to cyber security of financial institutions are increasing, but methods and standards related to their management have not been established. There is also a growing demand for strengthening the cyber security system for financial institutions from international institutions, countries, public institutions, users, and others. In view of these circumstances, this paper shows the results of research on the expectation, regulation and risk management methods and trends of strengthening the cyber security system at financial institutions. In addition, I will consider the future governance of cyber security in financial institutions.

Keywords: Financial institution, cyber security, risk management, ISO/IEC31000, ISO/IEC27014

1. はじめに

国際通貨基金（IMF）レポート [1]は，2018 年 6 月，金融機関は年間 11 兆円がサイバー攻撃によって失われていると公表した.この 11 兆円という金額は，世界の金融機関の純利益額（120 兆円）の 9%に相当する.また，最悪シナリオでは，38 兆円に達する可能性があるとも公表している.金融機関へのサイバー関連損失の 90%は，SWIFT（国際送金システム）やビジネスメール詐欺（BEC）による不正送金が原因である.これらのサイバーリスクを低減するために，産官学が連携して，規制や監督の枠組みの見直しやリスク評価の取り組みが必要であるとしている.

日本においては，日銀レポート [2]は，2015 年度以降，金融機関の約半数がサイバー攻撃を受け，また，1 割強に業務影響があったと公表している.

現在，国内外の金融業界，政府機関，公的機関等が金融機関のサイバーセキュリティに関する態勢の強化を期待しており，金融機関としても自らの態勢強化においてこのような動向を踏まえ，取り組む必要がある.

2. 金融機関に対する期待

2-1. 国際金融機関

サイバー攻撃は，容易に国境を跨ぎ，その影響は金融システム全体に波及するおそれがあり，国際的にもサイバーセキュリティの確保は重要課題となっている.

こうした中，G7 財務大臣・中央銀行総裁会議は，2015 年に「G7 サイバーエキスパートグループ」を設置し，サイバーセキュリティに関する議論を重ねた.その結果，国際的なサイバーセキュリティ対策の基本原則を示した「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 [3]」を 2016 年 10 月に，その評価に関する「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 [4]」を 2017 年 10 月に公表している.

加えて，2018 年 10 月には，より具体的な個別分野の重要テーマ に関する基本原則として「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 [5]」,「金融セクターにおけるサードパーティのサイバーセキュリティリスクマネジメントに関する G7 の基礎的要素 [6]」を公表し，サイバーセキュリティにおける侵入テストの高度化，サードパーティへの対応の重要性を提唱している.

また，バーゼル銀行監督委員会は，2018 年 12 月，「サイ

† 情報セキュリティ大学院大学
Institutions of Information Security
‡ 情報セキュリティ大学院大学
Institutions of Information Security

バー耐性管理の諸慣行 [7]」を公表し，ガバナンスと文化の構築，リスクの測定と準備の評価（予防，回復及び学習），コミュニケーションと情報共有，第三者との相互接続を提唱している.

2-2. 主要国

金融安定理事会（FSB）は，2017 年に G20 蔵相・中銀総裁会議の求めに応じて 各国,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，「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 [8]」(以下，FSB 報告書)を公表している.

FSB 報告書によると，各国は，下表の通り国際的なガイダンス・基準を自国の金融機関に対する規制や監督上の慣行スキーム等に用いていると公表している.また，金融機関は特に ISO／IEC の国際規格を参照することが多い，としている.

主要国における動向は表 1 のとおりである.

表 1　自国の規制や監督上の慣行スキームに国際的なガイドライン・基準を用いた国と対象としたガイダンス・基準

国	活用した国際的ガイダンス･基準					
	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	■			■	■	
EC	■					■
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ヵ国)	19	6	4	11	17	15

（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 の図表 3 より筆者が作成）

なお，表 1 の活用した国際的なガイダンスや基準は以下の通りである.

・CPMI と IOSCO

BIS 決済･市場インフラ委員会(CPMI)と証券監督者国際機構(IOSCO)が，2016 年 7 月に公表した「金融市場のためのサイバー攻撃耐性に係るガイダンス」

・FFIEC

米国連邦金融機関検査協議会(FFIEC)が，2015 年 6 月に公表した「サイバーセキュリティアセスメントツール」（Cybersecurity Assessment Tool，CAT）.金融機関がサイバーセキュリティ対策を実施する際のアセスメント･ツールであり，サイバーセキュリティ態勢の成熟度を 5 段階で評価する.

・G7

2-1 で前述の「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」等

・ISACA(COBIT)

情報システムコントロール協会 (ISACA)と IT ガバナンス協会 (ITGI)が提唱している IT ガバナンスの成熟度を測るフレームワーク

・ISO/IEC

国際標準化機構，国際電気標準会議.国際的な標準である規格を策定.

・NIST

米国国立標準技術研究所(NIST)が，2014 年 2 月に公表した「重要インフラのサイバーセキュリティを強化するフレームワーク [9]」.大統領令に基づき，企業におけるサイバーセキュリティリスクの管理を支援するための，業界標準およびベストプラクティスをまとめた自主参加型の，リスクベースアプローチに基づくサイバーセキュリティ対策のフレームワークである.

2-3. 日本

（1）基本法

「サイバーセキュリティ基本法 [10]」は，2014 年 11 月にサイバーセキュリティに関する施策を総合的かつ効率的に推進するため，国家としての基本理念を定め，国の責務等を明らかにし，サイバーセキュリティ戦略の策定その他当該施策の基本となる事項等を規定している.さらに，2018 年 12 月，サイバーセキュリティに対する脅威が一層深刻化する中,我が国におけるサイバーセキュリティ の確保を促進し，2020 年東京オリンピック・パラリンピック競技大会の開催に万全を期すため，官民の多様な主体が相互に連携し，サイバーセキュリティに関する施策の推進に係る協議を行うための協議会を創設する等の措置を講ずるとしている.

また，2018 年 7 月に改訂した「重要インフラの情報セキュリティ対策に係る第 4 次行動計画 [11]」において，重要インフラサービスを安全かつ持続的に提供するという「機能保証」という考え方を、金融機関を含む重要インフラ事業者に提唱している.また,「機能保証」の実現に向けて，リスクマネジメント及びその態勢整備を推進すること，リスクベースの考え方により経営資源を適切に配分すること等

を提唱している.

(2) 関連省庁

(ⅰ) 総務省

総務省は，2017 年 12 月，サイバーセキュリティタスクフォースの下に「情報開示分科会」を開催し，本分科会において，民間企業のセキュリティ対策の情報開示に関する課題を整理し，その普及に必要な方策について検討し，「情報開示分科会報告書（案） [12]」を公表している.

この報告書案では,「セキュリティ対策の見える化」を通じて，民間企業の経営層が自社のセキュリティ対策の現状を認識し，他社の状況と比較することにより，さらに必要な具体的な対策を検討し，導入する「セキュリティ対策の好循環」が起こる環境の実現を提唱している.

また，情報開示にあたっては,「社内の情報共有」「契約者間などの情報開示」「社会に対する情報開示」の 3 段階にわけて，期待される取り組みを示している.

(ⅱ) 経済産業省

経済産業省は，2005 年 3 月,「企業における情報セキュリティガバナンスのあり方に関する研究会 [13]」において,「情報セキュリティガバナンス」を「コーポレートガバナンスとそれを支えるメカニズムである内部統制の仕組みを，情報セキュリティの観点から企業内に構築･運用すること」と定義し，企業における情報セキュリティガバナンスのあり方に関する研究会報告書，情報セキュリティ対策ベンチマーク，情報セキュリティ報告書モデル等を公表している.

また，2016 年 12 月，独立行政法人情報処理推進機構（以下，IPA）とともに，大企業及び中小企業（小規模事業者を除く）のうち，IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象に，経営者のリーダーシップの下で，サイバーセキュリティ対策を推進するため,「サイバーセキュリティ経営ガイドライン [14]」を公表している.

当ガイドラインでは，サイバー攻撃から企業を守る観点で，経営者が認識する必要のある「3 原則」，及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」をまとめている.なお，2017 年に，経営者が認識すべき 3 原則は維持しつつ，経営者が CISO 等に対して指示すべき 10 の重要項目について改定している.

2018 年 5 月の第 2 回「産業サイバーセキュリティ強化へ向けたアクションプラン [15]」において,「経営・現場双方の課題に応えるサイバーセキュリティ経営強化パッケージ」のなかで，企業経営者に対するサイバーセキュリティ経営を促す仕組み『３STEP アプローチ』 を提言している.

そこでは，まずリスク管理の一環として，サイバーセキュリティ対策を位置づけ，コーポレート・ガバナンス・システムに関するガイドラインのとりまとめに向け，サイバーセキュリティを位置づけるとしている.さらに，サイバーセキュリティへの経営層の関与を，上場企業で行われている「取締役会の実効性評価」の評価項目へ組み込むことを促進すること，その評価については外部専門家と連携すること等を推奨している.

(ⅲ) 金融庁

金融庁は，2015 年 7 月，金融分野のサイバーセキュリティの確保は金融システム全体の安定のための喫緊の課題であるとの認識の下,「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 [16]」を公表している。方針として、サイバーセキュリティに係る金融機関との建設的な対話と一斉把握、金融機関同士の情報共有の枠組みの実効性向上、業界横断的演習の継続的な実施、金融分野のサイバーセキュリティ強化に向けた人材育成等の 5 点をあげている.

また，2018 年 7 月，政府全体の基本戦略である「サイバーセキュリティ戦略」改訂を受けて，改定している.そのなかで，デジタライゼーションの加速的な進展を踏まえた対応や G7 財務大臣・中央銀行総裁会議をはじめとするサイバーセキュリティに関する国際協調の議論に対して，各国当局と連携しつつ貢献･対応していく等が重要としている.

また，金融機関に対して，更なる経営の関与，侵入テストの高度化，リスクアセスメント等の取組強化に関する以下のレポートを公表している.

- 「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 [17]」
- 「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 [18]」
- 「『FFIEC Cybersecurity Assessment Tool に関する調査研究』調査報告書 [19]」
- 「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 [20]」

(3) その他機関

(ⅰ) 金融情報システムセンター

公益財団法人金融情報システムセンター（以下，FISC）は，2015 年 6 月,「金融機関等コンピュータシステムの安全対策基準・解説書（第 8 版追補改訂） [21]」を発刊し，金融機関などにおける「サイバー攻撃対応」と「クラウド利用」を二大テーマとし，基準の新設や追加・修正を実施している.

2018 年 3 月に金融機関コンピュータシステムの安全対策基準を第 9 版として改定し，システムリスクアセスメントにおけるリスクベースアプローチ導入，クラウド利用や FinTech の拡大等によるサードパーティーリスクに応じた

外部機関に関する統制基準の整理等を主眼においた改定を実施している.

（ii）一般社団法人日本経済経団体連合会

一般社団法人日本経済経団体連合会（以下，経団連）は，2018 年 3 月,「経団連サイバーセキュリティ経営宣言 [22]」を宣言し，「Society 5.0」に向け，あらゆる場面でＩＴとの融合が進む一方，サイバー空間の秩序や安全に脅威を与える，著しい悪意を持った行為も多発している.いまやすべての企業にとって価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題とし，企業に対しても同様の宣言を推奨している.

3. リスクマネジメントや情報セキュリティガバナンスマネジメントに関する動向

3-1. リスクマネジメントに関する定義

リスクは，ISOGuide73:2009 の定義において，リスクを「目的に対する不確かさの影響（Effect of uncertainty on objectives）と定義されている.影響とは，“期待されていることから，良い方向及び・又は悪い方向に逸脱することであり，リスクについて好ましい方向か否かにかかわらず，目的達成には，好ましくない影響をもたらすリスクをとることも必要である”と定められている.即ち，リスクが機会ともなることが認識されている.

リスクマネジメンメントの手法については，ルールベースアプローチ，リスクベースアプローチ等があるが，以下の通り，昨今では，特にサイバーリスクにおいては，リスクベースが提唱されることが多い.

金融庁は，ルール・ベースのアプローチは、2007 年に公表した「金融規制の質的向上：ルール準拠とプリンシプル準拠 [23]」と題するホームページのなかで、“ある程度詳細なルールや規則を制定し，それらを個別事例に適用していくこと”と定義している.また, 2018 年に公表した「マネー・リンダリング及びテロ対策資金供与対策に関するガイドライン [24]」において，リスクベースアプローチを“金融機関等が，自らのリスクを特定・評価し，これを実効的に低減するため，当該リスクに見合った対策を講ずること”と定義している.

また，前述の G7 の「金融セクターにおけるサードパーティのサイバーセキュリティリスクマネ ジメントに関する G7 の基礎的要素」において，金融機関は，サードパーティに関連するサイバーリスクを特定・評価・監視し， リスクベースアプローチを用いてサードパーティのサイバーリスクを管理すべきであるとしている.

更に，後述する ISO/IEC27014 においても，原則 2 としてリスクベースのアプローチを採用することとしている.その理由として,「情報セキュリティのガバナンスは，リスクベースの決定に基づいている必要がある.許容できるセキュリティの量の決定は，競争上の優位性の喪失，コンプライアンスおよび責任のリスク，業務の中断，評判の低下，および財務上の損失など，組織のリスク選好度に基づいて決定する必要がある.」としている.

3-2. リスクマネジメントの変遷

日本では，阪神大震災をきっかけにクライシスマネジメントの観点から，危機管理の規格が作られ，これをもとにリスクマネジメントを追記する形で，リスクマネジメント規格が作られた．国際的には，クライシスマネジメントは自然災害だけではくリスクマネジメントを中心に規格化が進んでいる.

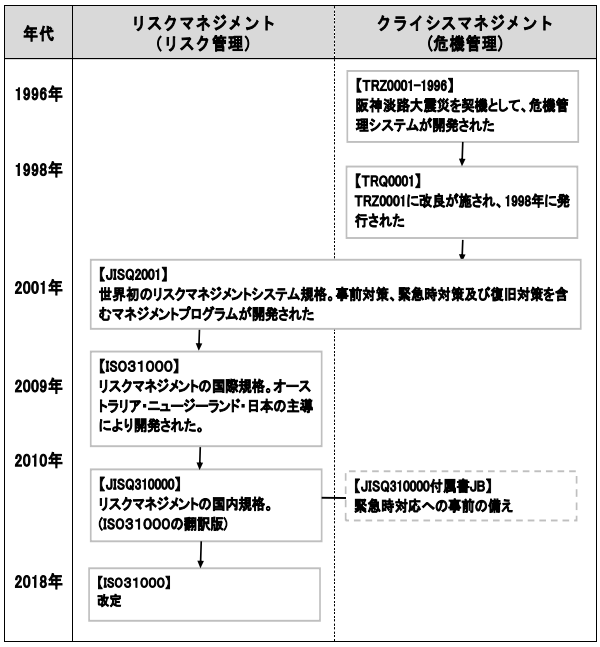

図 1　リスクマネジメントの変換

3-3. 主なリスクマネジメントモデル

（1）ISO/IEC31000

前述の FSB 報告書のとおり，各国や国際機関の規制・ガイダンス，監督上の慣行においては，ISO／IEC の国際規格が参照されることが多いため，ここでは，リスクマネジメントを規格している ISO/IEC31000 **[25]**について述べる.

ISO/IEC31000 では，リスクマネジメントを 3 つの要素，「原則」「枠組み」「プロセス」から構成するとしている.

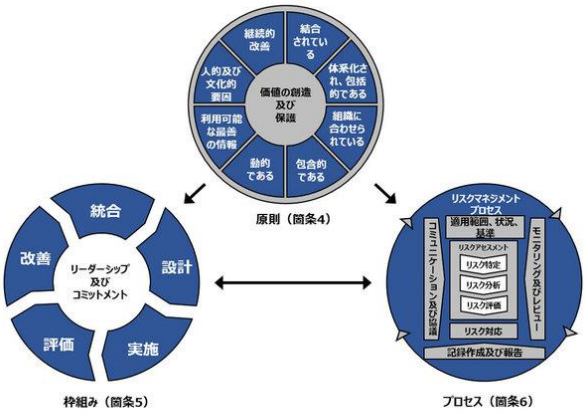

図 2　ISO/IEC31000　リスクマネジメント

「原則」は，リスクマネジメントをどのような組織において行う場合にも遵守すべき事項を示した方針であり，上図の通り 8 つの原則がある.

また「プロセス」はより現場に近い活動を指す一方，「枠組み」はそうした「プロセス」が組織の目的達成(例:経営理念やミッション，中長期目標や計画)と適切にリンクするような設計や導入，見直しにつながるための活動を指している.

なお，リスクアセスメントの手法は，ISO/IEC30100 [26]において詳細に補完している.

(2) COSO　ERM

米国のトレッドウェイ委員会組織委員会(COSO)が公表している内部統制フレームワークであり，原型は 1992 年に発行された内部統制フレームワークであり，COSO キューブと呼ばれる考え方である [27].

その後，2004 年に改定され，経営や戦略の視点からリスク許容度を設定・コントールすること，個々のリスクをポートフォリオの観点から統合管理することを提唱し，COSO ERM フレームワークと呼ばれるようになった.

また，2017 年に改訂し，ERM の位置付けを図 3 のように捉え，5 つのカテゴリから構成するとしている.

図 3　COSO　ERM　Aligning Risk with Strategy and Performance の図 5 より筆者が作成

また，5 つのカテゴリは，さらに 23 の原則から構成されている.主な原則は表 2 の通りである.

表 2　COSO　ERM における主な原則

カテゴリ	代表的な原則
リスクガバナンス，文化	取締役会など組織の機関設計やトップの倫理感
リスク，戦略，及び目標設定	組織の戦略策定におけるリスクマネジメント
実行上のリスク	リスクマネジメントを支える「リスク特定」「リスク分析」「リスク評価」「リスク対応」
リスク情報，コミュニケーションと報告	組織が認識したリスクに関する情報の報告・共有
リスクマネジメントパフォーマンスのモニタリング	上記活動が適切に行われているかどうかのモニタリング

(3) リスクアペタイトフレームワーク

2000 年代後半の世界的な金融危機以後，金融機関のコーポレートガバナンス強化の議論の一環として提唱された概念である.

金融庁は，金融行政方針（2015 年） [28]において，リスクアペタイトフレームワークの注釈として，自社のビジネスモデルの個別性を踏まえたうえで，事業計画達成のために進んで受け入れるべきリスクの種類と総量を「リスクアペタイト」として表現し，これを資本配分や収益最大化を含むリスクテイク方針全般に関する社内の共通言語として用いる経営管理の枠組みとしている.

また，FSB は，2013 年 12 月に，「金融安定理事会実効的なリスクアペタイトフレームワークの諸原則 [29]」を公表している.

3-4. 情報セキュリティガバナンス

ISO/IEC にて規格されている情報セキュリティガバナンス(ISO/IEC27014)について述べる.

(1) 経緯

ISO/IEC 27014 [30]は,経済産業省が 2009 年に公表した「情報セキュリティガバナンス導入ガイダンス [31]」を基に国際提案し，2013 年に発効されたものである.また，2015 年 7 月に JIS で発効されている.なお，現在，規格改定中である.

(2) 原則とプロセス

ISO/IEC 27014 では，以下 6 点を原則として定義している．

1：組織全体の情報セキュリティを確立する
2：リスクベースのアプローチを採用する
3：投資決定の方向性を設定する
4：社内外の要件への準拠を確保する
5：セキュリティに配慮した環境を育む
6：事業成果に関連して業績を見直す

また，プロセスは図 4 および表 3 の通り定義している．

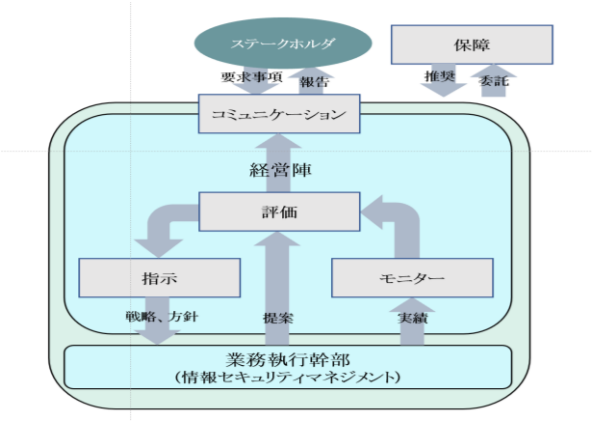

図 4　ISO/IEC 27014 のプロセス

表 3　ISO/IEC 27014 のプロセスの定義

プロセス	ISO/IEC27014 における定義
評価	現在のプロセスと計画された変更に基づいて現在および将来のセキュリティ目標の達成を考慮し，将来の戦略目標の達成を最適化するためにどこで調整が必要かを決定する
指示	経営陣が情報セキュリティの目的および実行する必要がある戦略について指示を与える
モニター	経営陣が戦略的目標の達成を評価することを可能にする
コミュニケーション	経営陣と利害関係者がそれぞれのニーズに適した情報セキュリティに関する情報を交換する
保証	経営陣が独立した客観的な監査，レビュー，または認証を依頼する

4. 今後のサイバーセキュリティのリスクマネジメントに関する考察

4-1. 概要

今後の金融機関におけるサイバーセキュリティのリスクマネジメントについて，前述の金融機関に対する期待，リスクマネジメントや情報セキュリティガバナンスの動向を踏まえ，情報セキュリティのガバナンスの規格である ISO/IEC27014 に基づき考察する．

4-2. 金融機関に期待されている事項の整理

２章で前述した期待事項を，内容毎に分類すると，「経営全般に関する事項」「リスクアセスメントに関する事項」「技術的対策に関する事項」「情報開示，情報共有に関する事項」「第三者活用に関する事項」に分類することできた.特に重要なことは以下の通りである．

「経営全般に関する事項」については，経産省にあるサイバーセキュリティ経営ガイドラインや取締役会運営に関する事項等があげられる．

「リスクアセスメントに関する事項」としては，まず.リスクベースアプローチの考え方を浸透させることが期待される.そのためには，リスクアペタイトなどのリスクベースのフレームワークを採用すること，FISC で推奨されているリスクベースアプローチの導入を徹底すること等があげられる.その上で，ISO/IEC31000 が示すようなリスクマネジメントを実施することがあげられる．

「情報開示，情報共有に関する事項」としては，総務省情報開示分科会報告書（案）に基づく情報開示，一層の外部との情報共有を進めていくことがあげられる．

「第三者活用に関する事項」については，取締役会の実効性評価における活用等があげられる

4-3. ISO/IEC27014 に基づく取組モデル

4-2 で整理した期待事項を ISO/IEC27014 のプロセスに適用，整理することで，よりガバナンスが発揮されるようモデル化を試みる．

なお，ISO/IEC27014 の評価・指示・モニターについては期待事項の「経営全般に関する事項」「リスクアセスメントに関する事項」，コミュニケーションは「情報開示，情報共有に関する事項」，保証は「第三者活用に関する事項」を適用することで整理する．

（1）評価・指示・モニター

ベースとして，経済産業省「サイバーセキュリティガイドライン [14]」や金融庁「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 [16]」に基づいた態勢を構築することが前提となる．

その上で，上場企業においては，コーポレートガバナンスコード，同・システムについて，今後，東京証券取引所や総務省から提唱される内容に基づき取り込むこと，さらに経済産業省の提唱内容に基づき取締役会実効性の評価項目にサイバーセキュリティに関する評価項目を追加すること等が重要な見直し事項としてあげられる．

更に，「リスクベース」に基づくサイバーセキュリティリスクに関するリスクマネジメントを実施することが期待さ

れる.

このリスクマネジメントを効率的，かつ有効に運営するためには，リスクそのものを「見える化」し，リスクの内容や程度を共有することが重要となる.そのためには，リスクシナリオに基づき具体的な被害状況を共有すること，ぐ想定される損失金額を具体的な金額で示すこと，またリスクや想定される被害を一覧化すること(ダッシュボード化)等が有効な手段になると考える.

また，適切性を維持するには，最新動向を常に掌握することも重要となる.そのためには，サイバーセキュリティに関するインテリジェンス人材の育成および外部情報機関との連携強化も必要となる.

上記をまとめると図 5 の通りとなる.

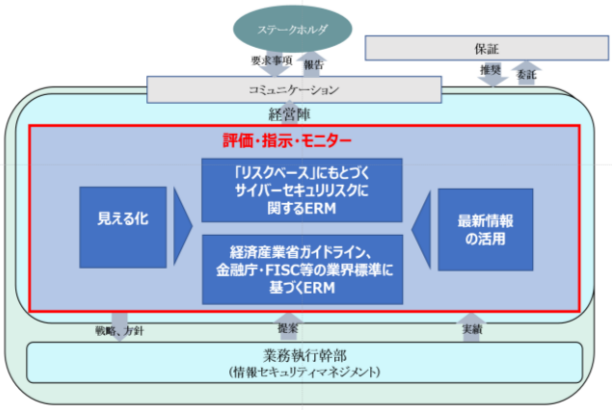

図 5　ISO/IEC 27014 評価・指示・モニターにおける想定される取組(ISO/IEC27014 より筆者が作成)

(2) コミュニケーション

主に株主を想定して狭義のコミュニケーションと幅広い関係者を想定した広義のコミュニケーションに分けて整理する.

狭義のコミュニケーションについては，総務省の報告書に基づく情報開示が上場企業を中心に求められるようになると考えられる.また，金融機関自身が積極的に経団連サイバーセキュリティ経営の宣言を強化することも必要になる.

広義のコミュニケーションを図るためには，「自助」「公助」だけでなく，「共助」による情報共有、即ち、双方向の情報共有がより重要となる.

これらの活動を進めていくには，金融 ISAC を始め，業界内交流や他業態交流の活性化もより重要になると考えられる.

上記をまとめると図 6 の通りとなる.

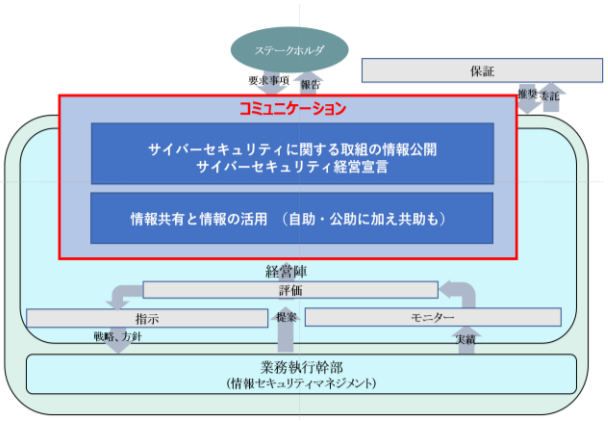

図 6　ISO/IEC 27014 コミュニケーションにおける想定される取組(ISO/IEC27014 より筆者が作成)

(3) 保証

外部活用による保証と金融機関内部の態勢強化に分けて整理する.

外部活用としては，経済産業省が「産業サイバーセキュリティ強化へ向けたアクションプラン」で示した通り，取締役会運営の評価について，第三者専門家を活用することがあげられる.

内部の態勢強化としては，内部監査の一層の活用，内部統制における 3 ラインディフェンスの導入や徹底等が有効と考えられる.

上記をまとめると図 7 の通りとなる.

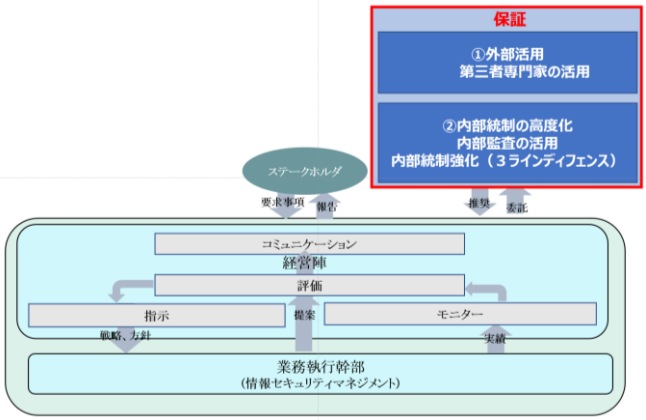

図 7　ISO/IEC 27014 保証における想定される取組(ISO/IEC27014 より筆者が作成)

5. まとめ

当報告では，金融機関におけるサイバーセキュリティに関するリスクマネジメントについて，ISO/IEC27014 のモデルに基づき，国際機関，国等の公的機関からの期待も踏まえ，方向感を整理した.

更なる研究，考察，体系化，具体化等が必要と考えているが，金融機関は今回の報告のような取組がより期待され

ると考える.

6. 今後の研究

今回の考察の全般について，先進金融機関の取組事例や国内外の各種動向等に関する研究を通して，見直し，具体化を重ねていきたいと考えている.

また，サイバーセキュリティに関連する「リスクアセスメント」について，ISO/IEC31000 を補完している ISO/IEC30100 にある各種手法や調査機関等が実施している調査結果等を参考にしながら，よりリスクを適切に「見える化」が可能となる手法やフレームワークを考案したいと考えている.

更に，コミュニケーションについては，特に海外の先進金融機関における情報公開の事例や国内外の各種動向に関する研究を通して，今後の国内金融機関が取り組むべき事項について体系化，具体化していきたいと考えている.

謝辞

本研究の調査や分析にご協力いただいた，原田研究室の先輩同僚の皆様に謹んで感謝の意を表します.

参考文献

[1] 国際通貨基金（IMF），“国際通貨基金（IMF）レポート,” 2018.

[2] 日本銀行, “日銀レポート,” 2017.

[3] G7,“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.

[4] G7,“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.

[5] G7,“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.

[6] G7,“金融セクターにおけるサードパーティのサイバーセキュリティリスクマネジメントに関する G7 の基礎的要素,” 2018.

[7] バーゼル銀行監督委員会，“サイバー耐性管理の諸慣行,” 2018.

[8] 金融安定理事会（FSB），“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,” 2018.

[9] 米国連邦金融機関検査協議会（FFIEC），“サイバーセキュリティアセスメントツール,” 2015.

[10] *サイバーセキュリティ基本法,* 2014.

[11] *重要インフラの情報セキュリティ対策に係る第４次行動計画,* 2018.

[12] 総務省，“情報開示分科会報告書（案）,” 2017.

[13] 経済産業省，“企業における情報セキュリティガバナンスのあり方に関する研究会,” 2005.

[14] 経済産業省，“サイバーセキュリティ経営ガイドライン,” 2016.

[15] 経済産業省，“産業サイバーセキュリティ強化へ向けたアクションプラン,” 2018.

[16] 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,” 2015.

[17] 金融庁，“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,” 2017.

[18] 金融庁，“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,” 2018.

[19] 金融庁，“『FFIEC Cybersecurity Assessment Tool に関する調査研究』調査報告書,” 2016.

[20] 金融庁，“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,” 2015.

[21] 公益財団法人金融情報システムセンター(FISC)，“金融機関等コンピュータシステムの安全対策基準･解説書（第 8 版追補改訂）,” 2015.

[22] 経団連，“経団連サイバーセキュリティ経営宣言,” 2018.

[23] 金融庁，“金融規制の質的向上 : ルール準拠とプリンシプル準拠,” 2007.

[24] 金融庁，“マネー・リンダリング及びテロ対策資金供与対策に関するガイドライン,” 2018.

[25] ISO/IEC, *ISO/IEC31000,* 2018.

[26] ISO/IEC, *ISO/IEC30100,* 2009.

[27] トレッドウェイ委員会組織委員会(COSO)，“COSO ERM,” 1992.

[28] 金融庁，“金融行政方針（2015 年）,” 2015.

[29] 金融安定委委員会（FSB），“金融安定理事会実効的なリスクアペタイトフレームワークの諸原則,” 2013.

[30] ISO/IEC, *ISO/IEC27014,* 2013.

[31] 経済産業省，“情報セキュリティガバナンス導入ガイダンス,” 2009.