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

【報告書】

2017 年 3 月 31 日

株式会社 NTTデータ経営研究所

目次

序論

情報システムは経営を支え、ビジネスを成功へと導く有効な手段である反面、システムトラブル、情報漏洩、ソーシャルネットワークサイトの風評被害によるレピュテーショナルリスクの増大等、会社経営そのものを揺るがす新たな脅威の原因となる可能性がある。

また、近年頻繁に発生している組織的なサイバー攻撃、外部委託先従業員による個人情報漏洩事故等の状況を踏まえ、各国の監督当局は規制を強化している。

我が国においても、2015 年 1 月に「サイバーセキュリティ基本法」が全面施行され、同年 4 月に金融庁が監督指針等を改正し、7 月には「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」を策定・公表している。

これを受けて、我が国金融機関においても、サイバーセキュリティは新たな重要課題であるとの認識のもと、IT ベンダ等の外部機関を利用した技術的対処や、サイバー攻撃を受けた場合のインシデント対応等サイバーセキュリティ対応態勢を構築してきている。

また、サイバーセキュリティリスクは、日々進化し、企業経営そのものに重大な影響を与える等、甚大な被害をもたらすものである。そのため、規程等の策定をはじめとする対応体制の整備、サイバー攻撃が与える影響度評価、サイバー攻撃時のインシデント対応手順の整備等をはじめとする、サイバーセキュリティ対応態勢の構築に取締役や執行役員等の経営陣（以下、経営層）の積極的な関与が求められる。

上記を踏まえ、本調査研究においては、様々なサイバーセキュリティリスクに備えるために、金融機関のサイバーセキュリティ対策における、組織的な判断及び意思決定等を行う経営層の関与のあり方に着目した。とりわけ、最高情報セキュリティ責任者（Chief Information Security Officer（CISO））、あるいは CISO と機能的に同じ役割を担う職責（以下、総称して「CISO 等」とする）が果たすべき役割・責任を、サイバーセキュリティ対策で先行する米国の事例や我が国の現況を通じて考察する。

エグゼクティブサマリー

CISO 等に期待される役割を調査するにあたり、サイバーセキュリティ対策で先行する米国の規制として、ニューヨーク州金融サービス局（以下、NYDFS）の「Cybersecurity Requirements For Financial Services」を調査した。加えて、CISO 等の役割に関する記載がみられる我が国の２つの規則・ガイドラインを調査した。

なお、米国の規制については、CISO 等の役割を定めた項目はないものの、サイバーリスク管理態勢の整備を求める規制であること等を踏まえ、NYDFS の規制に準ずるものとして、「Enhanced Cyber Risk Management Standards」（米国連邦準備制度理事会（以下、FRB）/米国通貨監督庁（以下、OCC）/米国連邦預金保険公社（以下、FDIC））も補完的に調査した。

これら調査を踏まえ、CISO 等に期待される役割を整理すると、以下の通りである。

（米国の規制）

- Cybersecurity Requirements For Financial Services（NYDFS）

【補完調査】

- Enhanced Cyber Risk Management Standards（FRB/OCC/FDIC）

（日本の規則・ガイドライン）

- サイバーセキュリティ経営ガイドライン（経済産業省）
- 産業横断サイバーセキュリティ人材育成検討会「第一期最終報告書」（産業横断サイバーセキュリティ人材育成検討会）

CISO 等に期待される役割

（役割 1）サイバーセキュリティ方針を策定する
（役割 2）サイバーリスクを評価し管理する
（役割 3）必要なリソースを見極め確保する
（役割 4）インシデントの発生に備えた準備、インシデント対応を指揮する

これらCISO等に期待される役割を踏まえ、CISO等の望ましい姿を考察するため、米国及び我が国金融機関のCISO等に対しインタビューを行い、CISO等の実務上の役割を確認した。

金融機関のCISO等に対するインタビュー結果を整理すると、以下の通りである。

（役割1）サイバーセキュリティリスク管理フレームワークの構築、リスク低減に関する助言
（役割2）サイバーセキュリティ方針の策定・見直し
（役割3）サイバーセキュリティ対応リソースの確保
（役割4）脅威情報の収集・共有
（役割5）取締役会等への報告

米国及び我が国におけるサイバーセキュリティの規制・ガイドライン等で定められたCISO等に期待される役割や、インタビューで得られたCISO等の役割を通じて、本調査を踏まえた我が国金融機関におけるCISO等の望ましい姿を考察した。

我が国金融機関におけるCISO等の望ましい姿の一例は、以下の通りである。

(1) 全社的なサイバーセキュリティリスク管理態勢の構築
(2) サイバーセキュリティを確保するための牽制機能の発揮
(3) 脅威情報の収集・分析スキームの構築
(4) 予算・リソースの確保のための経営層への働きかけ
(5) 専門技術を備えた人材の確保

本調査研究のアプローチ

本調査研究においては、我が国における金融機関のサイバーセキュリティ対策における経営層・CISO 等に期待される役割・責任のあり方を考察するため、以下の５つのステップにより実施した。

(1) 米国の規制に関する調査

サイバーセキュリティ対策が先行している NYDFS の「Cybersecurity Requirements for financial service companies」を調査（補完的に「Enhanced Cyber Risk Management Standards[1]」(FRB/OCC/米国 FDIC) も調査)。

(2) 我が国の規則・ガイドラインの調査

我が国のサイバーセキュリティ対策における規則・ガイドラインのうち、経営層・CISO 等の役割に関する記載のある以下の規則・ガイドラインを調査。

① 経済産業省「サイバーセキュリティ経営ガイドライン」

② 産業横断サイバーセキュリティ人材育成検討会「第一期最終報告書」

(3) CISO 等に期待される役割の抽出

米国の規制及び我が国の規則・ガイドラインの調査から、CISO 等に期待される役割を整理。

(4) CISO 等を設置する金融機関における取組

米国及び我が国金融機関へのインタビューを通じて、金融機関の取組や CISO 等の役割を確認。

（インタビュー対象先）

① 国内大手預金取扱金融機関

② 海外大手預金取扱金融機関

③ 海外大手証券会社

(5) 本調査を踏まえた我が国金融機関における CISO 等の望ましい姿の考察

米国及び我が国における規制・ガイドライン等で定められた CISO 等に期待される役割や、インタビューで得られた CISO 等の役割を通じて、我が国金融機関における CISO 等の望ましい姿を考察。

---

[1] 本規制は、未だ施行されていないため、2016 年 10 月に公表されたパブリックコメント案に基づいて調査を実施。

1. 米国におけるサイバーセキュリティに関する規制等

「Cybersecurity Requirements For Financial Service Companies」

① 本規制の背景・目的

NYDFS が、ニューヨーク州に拠点を持つ金融機関が遵守しなければならないサイバーセキュリティ管理に係る規制を策定し、2017 年 3 月より適用されている。

本規制は、金融機関の情報システムと顧客情報の保護を促すことを目的としている。

② 本規制の対象金融機関

本規制は、ニューヨーク州内に拠点を持つ金融機関が対象となる。ただし、以下のいずれかに該当する金融機関は、本規制のうち、CISO の設置、ペネトレーションテストと脆弱性診断（Vulnerability assessments）の実施、監査の実施をはじめとする 9 項目が除外される。

・従業員が 10 名未満

・過去 3 年間それぞれの年間総売上（Gross annual revenue）が 500 万ドル未満

・年度末の資産規模（Total assets）が 1,000 万ドル未満

③ 本規制の概要

本規制は、サイバーセキュリティプログラムの策定、サイバーセキュリティ方針の策定、CISO の設置、非公開情報の暗号化等を金融機関に求めている。

本規制の内容を要約すると、以下の通り。

(ア) サイバーセキュリティプログラムの策定

自社の情報システムの機密性、安全性、可用性を守るため、リスク評価の結果に基づき、以下の機能を実現させるよう、サイバーセキュリティプログラムを策定しなければならない。

ⅰ)非公開情報や情報システムに対する社内外の脅威の特定

ⅱ)防御システムの利用や、情報システム保護のための方針や手順の実行

ⅲ)サイバー攻撃の検知

ⅳ)検知された事案による影響を低減させるための対応

ⅴ)サイバーインシデントからの復旧

ⅵ)当局への報告

(イ)サイバーセキュリティ方針の策定

情報システムと非公開情報の保護のため、リスク評価の結果に基づき、経営層の承認をとった上で、以下の分野を含む方針や手続きを明文化し維持しなければ

ならない。

ⅰ)情報セキュリティ

ⅱ)データの統制と分類

ⅲ)資産リストの作成と危機管理

ⅳ)アクセスコントロールとアカウント管理

ⅴ)業務継続と自然災害からの復旧計画

ⅵ)業務システム

ⅶ)システムとネットワークのセキュリティ

ⅷ)システムとネットワークの監視

ⅸ)システム・アプリケーション開発と品質保証

ⅹ)物理セキュリティと環境管理

ⅺ)顧客データのプライバシー

ⅻ)ベンダやサードパーティサービスプロバイダの管理

ⅹⅲ)リスク評価

ⅹⅳ)インシデント対応

(ウ) 最高情報セキュリティ責任者（CISO：Chief Information Security Officer）の設置

金融機関は、サイバーセキュリティプログラムの監督と実行、サイバーセキュリティ方針の適用に責任をもつCISOを設置しなければならない。CISOは、金融機関、その関連会社、またはサードパーティサービスプロバイダから指名すること。

関連会社またはサードパーティサービスプロバイダから指名する場合には、金融機関は以下を実施しなければならない。

ⅰ)本規制の要求事項を遵守する責任を持つ

ⅱ)サードパーティサービスプロバイダに対して指示命令や監督を行う責任を有する人材（Senior member）を、金融機関の中から指名しなければならない

ⅲ)この章での要求事項を守るべく金融機関で適用されているサイバーセキュリティプログラムについて、サードパーティサービスプロバイダにおいてもその適用を求めること

CISOは取締役会、またはそれと同等の統制を行う会議体(governing body)に対し、年1回以上、書面による報告を行わなければならない。そのような会議体がない場合は、CISOは上席役員(Senior officer)に随時報告を行わなければならない。

その際、CISOは、サイバーセキュリティプログラムと重要なサイバーセキュリティリスクについて、以下の内容を含む報告を行わなければならない。

ⅰ)非公開情報の機密性、情報システムにおける完全性とセキュリティ
ⅱ)サイバーセキュリティ方針とその手続(procedures)
ⅲ)重要なサイバーセキュリティリスク
ⅳ)サイバーセキュリティプログラムの有効性
ⅴ)影響を及ぼした重要なサイバーセキュリティ事案

(エ)ペネトレーションテスト[2]及び脆弱性診断(Vulnerability assessments)の実施

自社のリスク評価の結果に基づき特定された情報システムリスクに対して、年１回ペネトレーションテストを実施しなければならない。また、自社の情報システムにおける既知の脆弱性の特定のため、半年に１回脆弱性診断を実施しなければならない。

(オ)監査証跡の取得

金融取引など業務に関するログや、サイバー攻撃の検知、対応等のログを、監査証跡として保存しなければならない。ログは、最低５年は保持しなければならない。

(カ)アクセス権限の管理

リスク評価の結果に基づき、非公開情報を保有する情報システムに対し、アクセス権限を制限しなければならない。

(キ)アプリケーションのセキュリティの維持

サイバーセキュリティプログラムには、自社におけるアプリケーションのセキュアな開発を維持するための手続きや基準などを盛り込まなければならない。この手続きや基準は、年１回以上、または必要に応じてCISOがレビュー、評価、修正を行わなければならない。

(ク)リスクアセスメントの実施

定期的に情報システムのリスク評価を実施しなければならない。また、情報システム、非公開情報、業務の変化に対処するため、必要に応じ、評価の見直しを行わなければならない。

リスク評価に際しては、以下を含む方針と手順を作成しなければならない。

ⅰ)サイバーセキュリティリスクや脅威の評価と分類の基準

---

2 ネットワークに接続されている情報システムに対し、既知の技術を用いて侵入を試みることにより、情報システムに脆弱性がないかを検証するテスト

ⅱ)情報システムや非公開情報の安全性、機密性、可用性の評価の基準
ⅲ)リスク評価の結果に基づき、特定されたリスクを低減させるか、受け入れるかを決めるための要件

(ケ)サイバーセキュリティ人材とインテリジェンスの確保

自社、子会社、サードパーティサービスプロバイダのサイバーセキュリティ人材を確保し、自社のサイバーセキュリティリスクの管理や、(ア)で挙げた機能の実現を担わせなければならない。そのような人材には、現時点でのサイバーセキュリティリスクを把握できるよう、研修などを受けさせなければならない。

(コ)サードパーティサービスプロバイダのセキュリティ方針の評価

サードパーティサービスプロバイダが保有、またはアクセス可能な情報システムや非公開情報の保護に関する方針や手続きを定めなければならない。方針や手続きは、リスク評価をベースにして、以下を盛り込まなければならない。

ⅰ)サードパーティサービスプロバイダの特定とリスク評価
ⅱ)サードパーティサービスプロバイダに求める最低限のサイバーセキュリティに関する要求事項
ⅲ)サードパーティサービスプロバイダのサイバーセキュリティ対策の妥当性の評価手順
ⅳ)サードパーティサービスプロバイダに対する定期的な評価

なお、サードパーティサービスプロバイダに対するガイドラインには、以下を盛り込まなければならない。

ⅰ)重要なシステムや非公開情報へのアクセスを制限するため、多要素認証などによるアクセス制御の方針
ⅱ)非公開情報を移動、または保存する際の暗号化の方針
ⅲ)サードパーティサービスプロバイダが保有する自社の情報システムや非公開情報に影響が及ぶ、インシデント発生時の自社への通知
ⅳ)サードパーティサービスプロバイダが方針や手続きを遵守する契約や保証

(サ)多要素認証の実施

リスク評価の結果に基づき、非公開情報や情報システムに対する不正アクセスを、多要素認証やリスクベース認証などを用いて効果的に制御しなければならない。同等もしくはより安全なアクセスコントロールの利用について、CISOが書面にて承認しない限り、多要素認証は、外部から内部ネットワークに対するあらゆるアクセスに対して適用しなければならない。

(シ)データ保有の制限

サイバーセキュリティプログラムに、業務上必要のなくなった非公開情報の定期的な処分の方針や手続きについて盛り込まなければならない（法律等により保管が求められている情報は除く)。

(ス)研修とモニタリングの実施

権限が与えられたユーザの活動、権限のないアクセス履歴、非公開情報の改ざんをモニタリングする方針や手続きを定めなければならない。また、リスク評価の結果、特定されたリスクについて、全従業員に周知させるため定期的に研修を行わなければならない。

(セ)非公開情報の暗号化

暗号化する非公開情報の範囲を決定しなければならない。なお、暗号化以外に有効な手段であるとCISOが認めた場合には、代替可能である。決められた範囲での暗号化やその代替手段の有効性について、CISOは年1回以上レビューをしなければならない。

(ソ)インシデント対応計画の策定

以下を盛り込んだ計画を策定しなければならない。

ⅰ)サイバーセキュリティイベントへの対応における組織内手続き
ⅱ)インシデント対応計画の目標
ⅲ)役割や責任、意思決定の権限レベルの定義
ⅳ)内部・外部との情報共有
ⅴ)情報システムの脆弱性の改善に対する要求事項の特定
ⅵ)インシデントとその対応に関する説明書類の作成と報告
ⅶ)今後のインシデントに備えた対応計画の評価と改善

④　本規制において CISO 等に期待される役割

本規制では上述の通り５項目(P９　参照)について、経営層への報告を CISO 等に求めている。当該５項目とこれらに関連する他の要請事項を、タスクごとに整理すると、本規制における CISO 等に期待される役割は、以下の通り。

項番	分類	CISO 等に期待される役割
1	サイバーセキュリティ計画・方針の策定	サイバーセキュリティプログラムの策定を指揮する。
2		情報システムを保護するためのサイバーセキュリティ対策の方針や手順の作成を支援する。
3	サイバーセキュリティリスク評価	リスク評価に関する方針や手順の作成を支援する。
4		日々進化するリスクに合わせた定期的な方針や手順の見直しを支援する。
5	セキュリティ技術の導入	非公開情報の暗号化方式や代替方式の検討､暗号化を行う情報の選定を支援する。
6		非公開情報や情報システムのアクセスに対する多要素認証やリスクベース認証などを用いて効果的に制御する。
7		非公開情報が不要となった場合の管理に関する方針や手順の策定を支援する。
8	情報システムの開発に関する計画の策定	アプリケーションのセキュアな開発を維持するための手続きや基準を定期的にレビューする。
9	インシデント対応	検知されたインシデントの影響を低減するための対応を指揮する。
10		サイバーセキュリティ事案の復旧を指揮する。
11		インシデント対応に関する説明書類の作成を支援する。
12	人材の確保・研修	サイバーセキュリティに必要な人材を確保する。
13		研修を定期的に行う仕組みを構築する。
14	関係当局への報告	サイバーセキュリティプログラムを当局に報告する。
15		重要なサイバーインシデントを当局に報告する。

（参考）Enhanced Cyber Risk Management Standards

① 本規制の背景・目的

FRB、OCC、FDIC により、2016 年 10 月にパブリックコメントに付されたサイバーセキュリティ管理に関する規制である。

本規制は、大規模金融機関を対象としたサイバーリスク管理基準であり、各金融機関にサイバーリスク管理のフレームワークの策定を求めている。他のリスク管理と同様、サイバーリスクをシステムリスクの一部ではなく、重要なリスク管理の 1 つとして扱うことが求められている。

② 本規制の対象金融機関

本規制では、以下のいずれかに該当する金融機関が対象となる。

・500 億ドルの連結資産を有するすべての米国の銀行持株会社
・米国の資産総額 500 億ドル以上の外国銀行の米国事業（現地法人のほか、支店を含む）
・総資産が 500 億ドル以上の貯蓄貸付組合

③ 本規制の概要

本規制は、サイバーリスク[3]管理態勢の整備にかかる要件を定めたものであり、具体的には、

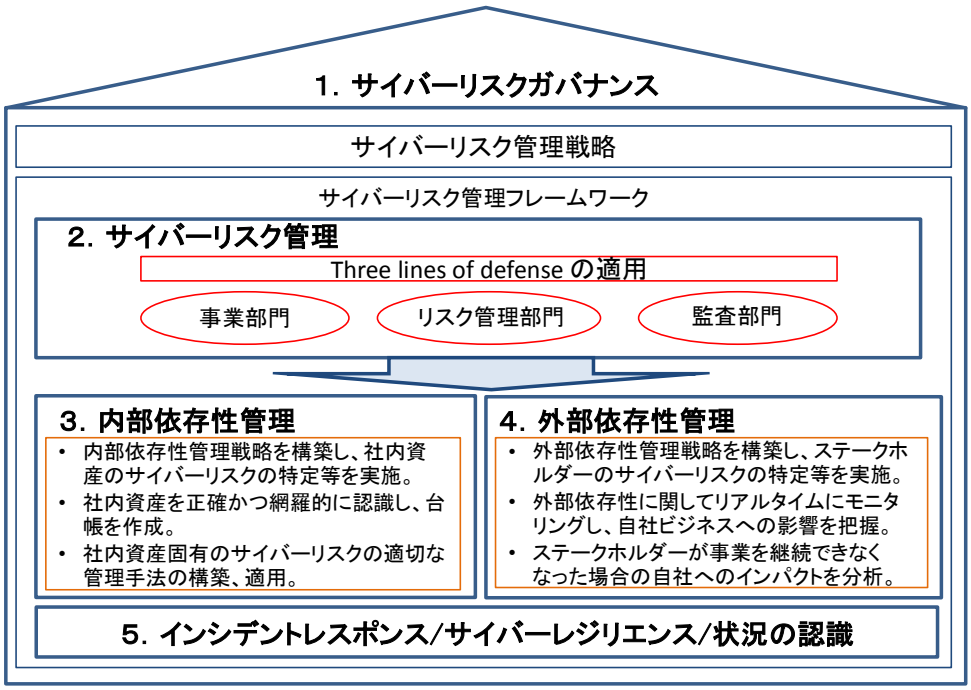
（ア）サイバーリスクガバナンスの策定
（イ）サイバーリスク管理
（ウ）内部依存関係の管理
（エ）外部依存関係の管理
（オ）インシデント対応、サイバーレジリエンス、及び状況認識の高度化

の 5 つから構成される。

これら 5 つの関係性を概念図として整理すると、図表 1 の通り。

[3] 当該規制では、金融機関が管理すべきリスクカテゴリーの１つとして「サイバーリスク」（Cyber Risk）という用語を用いている。このため、本項ではこの記載にならい、当該規制が想定する管理すべきリスクカテゴリーを表す用語として「サイバーリスク」を用いる。なお、本報告書における「サイバーリスク」と、本項以外の箇所で記載している「サイバーセキュリティリスク」は同義である。

〔図表１〕



本規制の内容を要約すると、以下の通り。

（ア）**サイバーリスクガバナンス**

ⅰ)全社的な「サイバーリスク管理戦略」を作成し、経営層の承認を得る

ⅱ)経営層は、全社的なサイバーリスクの選好と許容の範囲について、業務の特性に応じた管理、承認を行う

ⅲ)経営層は、サイバーリスク管理フレームワークの改善を担う責任者を設置する

ⅳ)サイバーリスクを監査する責任者を、ビジネスラインから独立した形で設置する

ⅴ)「サイバーリスク管理戦略」の達成をサポートすべく、「サイバーリスク管理フレームワーク」を構築する

（イ）**サイバーリスク管理**

サイバーリスク管理については、「three lines of defense[4]」を適用し、事業部門、リスク部門、監査部門の三者で実施する。

i)事業部門

- 各部門で日々の業務に関連するサイバーリスクを評価
- CEO を含む幹部層に自部門のサイバーリスクに関する情報を共有
- 「サイバーリスク管理フレームワーク」に準拠した管理を行う

ⅱ)リスク管理部門

- 全社的なサイバーリスクの管理の責任を負う
- 1 つ以上の事業部に影響があるサイバーリスクへの対応の検討、分析
- 適切な独立性、水準、権限、リソース、経営層との連携を保ち、レポートラインは他の部門から独立させ明確化する

ⅲ)監査部門

- 「サイバーリスク管理フレームワーク」が法律や制度、企業の規模と複雑性、リスクと合致しているものになっているか評価する
- サイバーリスク管理の評価を監査計画に組み込んだ上で、業務部門やリスク管理部門が策定した方針・手順等と、経営層が承認した「サイバーリスク管理フレームワーク」が合致しているか評価する

（ウ）**内部依存関係の管理**

対象は、金融機関内部の資産（従業員、データ、施設・設備など）である。

ⅰ)全社的な内部依存性に関連するサイバーリスクを減らすため、業務の有効性を継続的に評価し改善する

ⅱ)「サイバーリスク管理戦略」の達成のため、内部資産やビジネス機能を正確かつ網羅的に認識する

ⅲ)資産に対して固有のサイバーリスクを認識できるよう、適切な管理態勢を構築、運用する

（エ）**外部依存関係の管理**

対象は、金融機関がサービスを提供するために依存している、組織外部の関係者（ベンダ、サプライヤ、顧客、その他の外部組織）である

ⅰ)全社的な外部依存性に関連するサイバーリスクを減らすため、業務の有効性を、継続的に評価し改善する

---

[4] 金融機関のリスク管理を 3 つの階層で実施するものであり、一線はビジネスラインによるオペレーションの遂行、二線は一線のモニタリング、三線は独立した立場での評価を行う

ⅱ）「サイバーリスク管理戦略」の達成のため、全ての外部委託先に対してリアルタイムなモニタリングを可能とする

ⅲ）外部委託先に対するサイバーリスクを認識できるよう、適切な管理態勢を構築、運用する

（オ）**インシデント対応とサイバーレジリエンス[5]、状況認識**

ⅰ）サイバー攻撃に直面した場合でも、重要な業務が継続できるよう、サイバーレジリエンス能力を高める。業務環境の変化を踏まえ、信頼に足る予測、分析、対応により効果的な状況認識に努める

ⅱ）インシデント対応とサイバーレジリエンスの効果的な統制、戦略、能力を構築、維持し、発生する障害を想定することにより、その対応、復旧を行う

ⅲ）ＲＴＯ[6]の確立に加え、復旧やレジリエンスの計画により、システムを通じて影響が広がるマルウェア、データ破壊やシステムの可用性に対する脅威に対処する

ⅳ）相互依存性のある他の重要インフラ事業者（エネルギー、通信）に対するサイバー攻撃によって、自社が混乱を招く可能性を考慮し、自社の中核業務を継続するための戦略を策定・実施する

ⅴ）安全なオフラインのストレージに重要データを格納しておくための手順を準備する

ⅵ）業務が停止した場合に備え、他の企業やサービスプロバイダにビジネス機能ごと移管させる計画を作成する

ⅶ）顧客へのサービスの提供に影響を与えるような、破壊的なサイバーインシデントに焦点を当てたテストを実施する。また、マーケットや決済システム、清算機関、メッセージサービス等との相互接続の観点からもテストを実施する

ⅷ）業務の状況と、サイバーセキュリティ態勢の状況を把握した上で、サイバー事案に対して、迅速に対応できる態勢を構築する

---

[5] サイバー攻撃への耐性やダメージからの回復力。

[6] Recovery Time Objective（目標復旧時間）。事業が中断した際に、「いつまでに事業を復旧するか」という目標時間を表す指標。

④　本規制と CISO 等の役割

本規制には、CISO 等の役割を定めた項目はないものの、サイバーセキュリティに関するリスクガバナンスやリスク管理を求める規制であること等を踏まえ、NYDFS の規制に準ずるものとして、補完的に調査した。

その上で、本規制における、CISO 等の役割と関係性が高いと考えられる項目を参考までに整理すると、以下の通り。

分類	CISO 等に期待される役割
リスク管理戦略の立案	全社的な「サイバーリスク管理戦略」を作成し、経営層の承認を得る。
	「サイバーリスク管理戦略」の達成をサポートすべく、「サイバーリスク管理フレームワーク」を構築する。
	サイバーリスク管理フレームワークを改善する。
リスク管理部門における実務	全社的なサイバーリスクの管理の責任を負う。
	1 つ以上の事業部に影響があるサイバーリスクへの対応方法の検討、分析の実施を支援する。
	適切な独立性、水準、権限、リソース、経営層との連携を持ち、レポートラインは他の部門から独立させ明確化する。

2. 我が国におけるサイバーセキュリティに関する規則・ガイドライン等

(1) サイバーセキュリティ経営ガイドライン

① 本ガイドラインの背景・目的

企業の経営者を対象として、サイバー攻撃から企業を守るために、経済産業省、独立行政法人情報処理機構が 2015 年 12 月に策定したものである。また、2016 年 12 月に改訂されている。

② 本ガイドラインの概要

本ガイドラインは、経営者のサイバーセキュリティに必要な認識として、「サイバーセキュリティ経営の３原則」を整理している。また、CISO 等の情報セキュリティ対策の責任者となる担当役員が実施すべき「サイバーセキュリティ経営の重要１０項目」を整理している。

項番	分類	CISO 等に期待される役割
1	サイバーセキュリティ対策フレームワークの構築	サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
2	サイバーセキュリティ方針の策定	サイバーセキュリティリスクの認識、組織全体での対応の策定（セキュリティ方針）
3	リスク管理	サイバーセキュリティリスク管理体制の構築
4		サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
5	サイバーセキュリティ対応リソースの確保	サイバーセキュリティ対策のための資源（予算、人材等）確保
6	外部からの情報収集	情報共有活動への参加を通じた攻撃情報の入手とその有効活用
7	インシデント対応手順	緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施
8	インシデント対応／関係当局への報告／顧客等への開示	被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備
9	外部委託先との連携	系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握
10		IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保

(2) 産業横断サイバーセキュリティ人材育成検討会「第一期最終報告書」

① 本報告書の背景・目的

経団連が、「サイバーセキュリティ対策の強化に向けた提言」を公表（2015 年 2 月 17 日）。同提言で重要視している人材育成を推進するため、「サイバーセキュリティに関する懇談会」のメンバーであった日本電信電話株式会社、日本電気株式会社、株式会社日立製作所の 3 社が事務局となり、重要インフラ分野を中心とした企業 48 社（金融機関を含む）による「産業横断サイバーセキュリティ人材育成検討会」を設置した（2015 年 6 月 9 日）。

本検討会では、2015 年 6 月から 2016 年 6 月（第一期）の 1 年間において、産業界共通の情報システム部門を対象とした人材定義を取りまとめ、「第一期最終報告書」を公表している。

② 本報告書の概要

本報告書で取りまとめられた、「産業横断人材定義リファレンス（機能と業務に基づくセキュリティ人材の定義）」では、サイバーセキュリティ対策に必要となる主要な機能を 14 項目に整理している。また、その業務を担う役割を、「管理職」、「セキュリティ担当職」、「担当職」、「監査・個人情報保護」の 4 つに整理し、役割に紐付く担当者に細分化している。

これら機能を担当別に、要求知識「必須」、「あると良い」、「なくても良い」の 3 段階、業務区分「業務責任を負う」、「業務責任者を支援・補佐する」、「業務を担当する」、「業務担当者を支援・補佐する」、「業務内容を理解する」の 5 段階で評価している。

③ 本報告書において CISO 等が担う役割

「産業横断人材定義リファレンス（機能と業務に基づくセキュリティ人材の定義）」において、CISO 等に期待される役割として、「管理職である CISO、CRO、CIO 等」に関する業務のうち、業務区分が「業務責任を負う」、「業務責任者を支援・補佐する」に該当する業務を抽出した。（図表 2 参照）

なお、本報告書は、ヒアリングにより作成されているため、産業界における CISO 等の実態に近いものと考えられる。

［図表 2］

項番	分類	CISO 等に期待される役割
1	全社のサイバーセキュリティ戦略の統括	サイバーセキュリティ対策に関する全社的統括
2	セキュリティ対策計画の策定	コンプライアンス、ガバナンス及びリスクマネジメントの観点に基づくセキュリティ対策
3		・セキュリティ対策に係る実施計画の企画立案 ・規程、ルールの策定
4		・各事業に対する IT 導入、構築運用改善計画の企画立案 ・ガイドライン、マニュアルの策定
5	セキュリティ技術の導入	・システムセキュリティの観点に基づく機能改善・実施計画の企画立案 ・システム構成に関するセキュリティ機能改善計画の策定
		・ユーザビリティの観点に基づく機能改善、実施計画の企画立案 ・エンドポイント及び UI に関するセキュリティ機能改善計画の策定
6	情報に関する対策の導入	・情報資産保護活動における ICT 環境改善計画の策定 ・情報資産の保護基準や保護方法の改善、情報漏洩保険の導入検討
7		・情報資産保護活動における ICT 運用改善活動の策定 ・情報資産の棚卸
8	システム構築に関する計画の策定	・ライセンス管理を踏まえたリプレース計画の企画立案 ・固定資産管理、ソフトウェア会計管理
9	インシデント対応計画の策定	災害対策に関する ICT 環境改善計画の策定
10		災害対策及び災害発生時に関する稼働計画の策定
11		・ICT 環境における事業継続計画の策定 ・サイバーセキュリティ保険の導入の検討

3. 調査結果からみたCISO等に期待される役割の抽出

これまで、米国におけるサイバーセキュリティに関する規制、我が国のサイバーセキュリティの規則・ガイドラインにおける、CISO等に期待される役割を整理してきた。

これらを踏まえ、今回調査対象とした３つの規制・ガイドライン（加えて、補完的に調査した「Enhanced Cyber Risk Management Standards」）に共通する、CISO等に期待される役割を整理すると、以下の４つに大別できる。

(1)サイバーセキュリティ方針を策定する

サイバーセキュリティ方針を策定した後、策定した方針に準じた手続きの詳細化を図る。

CISO等は定められた手続きが遵守されているか定期的に評価するとともに、対応できるよう支援する。また、評価結果に応じてサイバーセキュリティ方針・手続きの見直しや経営層への報告が求められる。

(2)サイバーリスクを評価し管理する

脆弱性診断等のリスク評価手法、リスク評価に関する対応手順の策定、リスク許容度等を規定するサイバーセキュリティリスク管理フレームワークの構築が必要である。

CISO等は各事業部門がリスク低減策を実行するにあたり、技術的な対策の導入等を支援する。また、自社のみでなく外部委託先も含めた定期的なリスク評価を行う。リスク評価には、情報共有機関等からの脅威情報を入手し活用することが必要である。

また、リスク評価により顕在化したサイバーセキュリティリスクについては、改善に向けたCISO等の助言が必要である。さらに、自社におけるサイバーセキュリティリスクに関する情報を経営層に定期的に報告することが求められる。

(3)必要なリソースを見極め確保する

サイバーセキュリティリスク管理態勢を構築する上で、セキュリティ対策に必要なリソースを洗い出し、リソースが不足する場合には、CISO等は、経営層に予算等の割り当てを上申する等により必要なリソースの確保が求められる。なお、このリソースの確保には内部人材の育成も含まれる。

(4)インシデントの発生に備えた準備、インシデント対応を指揮する

インシデント対応においては、平時から対応手順の策定や対応態勢の構築が必要である。実際にインシデントが発生した場合には、CISO等はその影響を低減するため、

対応手順に則ったインシデント対応・復旧を指揮するとともに、重大なインシデントについて経営層・外部（当局・顧客）への報告・説明が求められる。

また、インシデント発生後における対応手順の有効性の検証や、定期的なサイバーセキュリティ演習等への参加を通じ、インシデント対応手順の見直しが必要である。

4. CISO 等を設置する金融機関における取組

我が国及び米国金融機関の CISO 等へのインタビューを通じて、実際のサイバーセキュリティに関する取組や CISO 等の役割を確認した。

(1) 国内大手預金取扱金融機関の取組

① サイバーセキュリティリスクの評価

CISO 等は、サイバーセキュリティリスクの評価に関して、リスクが顕現化するシナリオをセットし、顕現化するリスクの特性を評価した上で、当該シナリオの下でサイバーセキュリティを確保するために必要な施策を講ずる。

加えて、システム部門は特定の機能や製品には詳しいが、サイバーセキュリティの観点での検討が不足がちであることから、CISO 等は、新規 IT 導入時を含め事業部門に対するセキュリティの技術的観点からの助言を行っている。

② 脅威情報の収集

サイバーセキュリティを脅かす事象は広範囲に渡ることから、インシデントの検知に関しては、社内のリソースに留まらず外部のインテリジェンスを活用する体制が求められる。CISO 等はこうした体制整備の責任を担う。

③ インシデント発生時の対応

インシデント検知後は、CISO 等はインシデントがもたらし得る影響評価の分析を指示し、当該サイバーセキュリティリスク低減策について協議した上で、CIO にその内容を報告しなければならない。

とりわけ、サイバー攻撃が発生し業務継続に重大な影響を及ぼし得ると判断される場合には、BCP の発動に関わるため、CRO に対しても影響評価の内容を報告し、対応策を直ちに協議しなければならない。

④ 海外当局によって異なる規制要件の差異を吸収

グループ全体としてのサイバーセキュリティ方針等の整備にあたって、海外の規制要件を充足することが必要となる。海外当局の要請には、大きな方向性に変わりはないものの、細部の規制要件は各国当局によってその厳格さが異なっている印象がある。したがって、グループ全体としてのサイバーセキュリティ方針の策定にあたっては、細部の規制要件を意識している。

⑤ 実効性あるリスク管理のため CIO の直下に CISO 等を設置

サイバーセキュリティリスク管理における CRO 等のリスク責任者と CISO 等の役割分担を考える際のポイントは、サイバーセキュリティ管理に対する専門的知見の多寡である。当社のサイバーセキュリティ担当部署は、CIO の直下で主にサイバーセキュリティ管理実務に習熟した者により構成された組織であり、リスクガバナンス

を巡る理論ではあくまで第一線の位置づけとなる。理論上、リスク管理部署が第二線としてその管理を担うべきではあるが、実効性あるリスク管理を行う上では、専門的な知見を有する者がその任にあたることが重要であり、現状の体制で実効性を確保できている。

⑥ 予算の確保

当社では、予算の承認権限は CIO が有しており、CISO 等はその権限を有していない。そのため、CISO 等がサイバーセキュリティ管理態勢整備に必要な予算案を作成し、CIO に伺いを立てている。

こうした枠組みであるものの、当社ではサイバーセキュリティ管理が経営上の重要課題の１つとして位置付けられているため、必要な予算を十分に確保できている。すなわち、サイバーセキュリティ管理のためのリソースを適切に配分できれば、実効性は十分に確保できる。

⑦ サイバーセキュリティ対策の浸透のための取組

グループ全体としてサイバーセキュリティ管理を更に実効性の高いものとするため、各海外拠点のスタッフとのコミュニケーションを密に図り、方針及び当該方針に基づいた事務手順の浸透に努めている。こうした取組のほか、米国金融機関においてサイバーセキュリティ管理の実務経験を積んだ者を専門家として採用し、体制を強化している。

⑧ サイバーセキュリティ方針の再編

サイバーセキュリティ方針の整備における課題は、サイバーセキュリティ管理にかかる大方針から手続きまでを包括的に取扱う形となっているサイバーセキュリティ方針の再編である。すなわち、大方針のみを新たな「サイバーセキュリティ方針」として位置付け、各種手続きを「規程」レベルに定め、各担当者が実行すべきより詳細な手順を「事務マニュアル」に定めることが必要と考えている。

(2) 海外大手預金取扱金融機関[7]の取組

① サイバーセキュリティリスクの管理

CISO 等には、各種オペレーションを担うビジネスラインから独立したリスク管理が求められている。当社では、CISO チームを設け、主に「第二線」の立場から、サイバーセキュリティ方針を含むサイバーセキュリティ管理に必要なフレームワークの整備、サイバーセキュリティ管理にとって脅威となる事象とその事象が業務に与える影響を評価している。こうしたことから、CISO チームは、IT 専門家・サイバー

[7] Cybersecurity Requirements For Financial Service Companies(NYDFS)の対象先。

セキュリティ管理の専門家・業務継続計画に関する専門家によって構成されている。

（IT システムリスク・サイバーセキュリティリスク管理における役割分担）

部門	役割分担
第一線	業務システム、例えばデータセンター等において用いられるソリューションやアプリケーションの構築及びソリューションの維持に係るオペレーション、トレーダーによる市場取引にかかるオペレーション等、各種ビジネスプロセスの実行を担う者が該当する。
第二線	各種オペレーションを担うビジネスラインから独立した部署によるリスク管理である。この部署は CEO あるいは取締役会に報告義務を負う CRO の直下に置かれている。
第三線	内部監査による、第一線・第二線の機能検証を行う。

サイバーセキュリティ方針や規程の策定を含むリスク管理の枠組みの構築は、第二線が担う。第二線は、リスク選好フレームワークに則りリスク管理が行われているかをモニタリング（必要に応じて第一線からエビデンスを求め、確認することも含む）し、第一線におけるオペレーションに問題がある場合には改善を促す。

この点、特にサイバーセキュリティリスク管理に絞ると、リスク低減のための各種対応策の実行に必要な枠組みを構築するとともに、各ビジネスラインにおいて実行されたサイバーセキュリティリスク低減策を確認し、その内容に問題のある場合は、リスク管理部署が問題点を指摘し改善を求める。

② CISO 等が備えるべきスキルセット

CISO 等が有すべき能力として、IT 全般やサイバーセキュリティ管理に関する深い知見に基づき、全社的なサイバーセキュリティ戦略を推進することが重要である。すなわち CISO 等が扱う情報セキュリティ管理に関する内容は専門性の高いものであり、実際に IT インフラ構築・開発部門と緊密な連携を図り、適切な改善を求めるためには、構築中の IT システムにおいて用いられている技術を熟知しておく必要がある。

③ 米国規制が求める CISO 等のレポーティングライン

FRB、OCC 及び FDIC の規制（Enhanced Cyber Risk Management Standards）には、第一線・第二線の機能を明確化するとともに、サイバーセキュリティリスク管理の状況について CRO に報告すべき事項が盛り込まれている。この中で、CISO 等は、第一線の位置付けとなる IT インフラ構築・開発部門との間で直接のレポーティングラインを構成してはならないと理解している。これは、情報セキュリティ対策関連予

算が、他の IT インフラ構築に対する予算配分との関係で劣後し、戦略的に削減されてしまうことを、米国当局が懸念した背景があると考えられる。

④ 米国金融機関によって異なる CISO 等の組織構造における位置付け

米国における大手金融機関の情報セキュリティ管理機能は、主に、

・脆弱性・脅威への対応策の立案（あるいは第二線が立案した対応策のレビュー）、

・脆弱性・脅威に対する評価の実施、

・サイバーセキュリティリスクの低減に向けた対応策のモニタリング、

・上級管理者（Senior officer）への報告・当局向けの報告、

の４つである。

CISO 等には、「three lines of defense」でいう第一線と第二線の両方にまたがった機能がある中で、CISO 等をリスク管理側に置くべきか、IT インフラ開発部署に置くべきかについては金融機関によって区々である。このため CISO 等の考察にあたっては、規制が定める CISO 等が存在するか否かよりも、上述の“機能”が存在するかが重要である。

⑤ 米国における外部委託先の管理の強化

サイバーセキュリティ管理に関する規制には、外部委託先管理の強化も含まれている。具体的には、金融機関は業務委託先に対して自らの管理と同等の管理を求めるというものである。

(3) 海外大手証券会社[8]の取組

① サイバーセキュリティリスク管理の枠組み

CISO 等は、月１回開催されている会議体の議長を務めており、テクノロジーリスク管理に関するセキュリティ方針の策定を含む各種管理施策を承認している。会議体は各ビジネスラインの責任者・内部監査の責任者・コンプライアンス部門の責任者・各リージョンのテクノロジー部門のヘッドで構成される。CISO 等は、全社的なサイバーセキュリティリスク管理に必要な“枠組み”を整備する役割を担う。

② 各ビジネスラインに委ねられるセキュリティ対策

会議体で定められた方針に沿うことを前提に、サイバーセキュリティ管理のリスク低減策の立案・実行は各ビジネスラインが責任を有している。これは、自部門の運用実態を熟知している各部門の担当者にサイバーセキュリティ管理の実務を委ねた方が実効性が向上するからである。

---

8 Cybersecurity Requirements For Financial Service Companies(NYDFS)の対象先。

③　サイバーセキュリティ方針の改正

方針の改正は、

（ア）CISO 等が会議体において指示する場合

（イ）各ビジネスラインからの提案によって行われる場合

に大別される。

（ア）は複数のビジネスラインにまたがって共通の IT ソリューションを使用する等の理由により共通の管理規程が必要な場合に採られることが多く、（イ）はあるビジネスラインにおいて新規ビジネスを立ち上げるにあたって、新たなリスク管理上の対応を余儀なくされる場合に採られる。

④　脅威情報の収集

リスク管理の実効性を確保するため、特に防御を重視している。具体的には、テクノロジー部門のみならず各ビジネスラインにおけるサイバーセキュリティ担当者は、各国当局や IT ベンダ等がもたらす関連情報の収集・分析はもちろんのこと、その他あらゆるルートを通じて脅威の把握に努めている。とりわけ情報が公知になるタイミングで初めて把握するのでは、実効的なリスク管理を行う上では遅く、あらゆるルートを通じてできる限り早期に把握することが肝要である。

⑤　リスク評価

収集された脅威情報は全社的に共有され、テクノロジー部門及び各ビジネスラインのサイバーセキュリティ担当者間の議論によりリスク評価が行われる。

当社では、（ア）サイバーセキュリティの脅威となる事象がもたらすリスクの影響が当社 IT インフラまで広範囲に渡る場合、あるいは、（イ）インシデントの実行主体が、（ⅰ）各種のテロ活動等を支援する国家、（ⅱ）犯罪組織、（ⅲ）各種活動家のいずれかである場合、サイバーセキュリティリスクが更に高まると考えている。

⑥　インシデント対応

インシデント発生の疑いが検知された場合には、直ちに追跡し、発生の疑いがある場所及びインシデントの内容を明らかにする。

また、グローバルの各拠点において発生したインシデントを常時収集・分析するとともに、CISO 等はテクノロジー部門に対して、その結果を各ビジネスラインに還元し、PDCA サイクルの改善につなげている。

⑦　取締役会等での報告

CISO 等は、取締役会や執行会議に対して、サイバーセキュリティリスク管理の状況を、他のカテゴリーのリスク（市場リスク・信用リスク等の金融リスク）と同様に、報告している。

⑧　予算措置

当社ではサイバーセキュリティリスク管理に必要な予算は、IT システム関連投資予算の中の１つとして取り扱われている。予算の優先順位付けは経営にもたらすリスクの多寡を踏まえ取締役会が決定する。CISO 等は予算の承認プロセスに関与するものの、専決権限を有していない。

⑨　CISO の経歴等

当社 CISO は、複数の金融機関でテクノロジー、ネットワーク等の関係に従事した後に入社している。リスク管理委員会のメンバーである。

5. 本調査を踏まえた、我が国金融機関における CISO 等の望ましい姿の考察

最後に、我が国及び米国におけるサイバーセキュリティの規制・ガイドライン等で定められた CISO 等に期待される役割や、インタビューで得られた CISO 等の役割を通じて、我が国金融機関における CISO 等の望ましい姿の一例を整理した。

(1) 全社的なサイバーセキュリティリスク管理の実行

CISO 等は、経営を揺るがすほど脅威のあるリスクとしてサイバーセキュリティリスクを取り扱うことが求められる。そのため、経営層が決定した、全社的なサイバーセキュリティに関するリスク評価、リスク許容度等に基づき構築されたサイバーセキュリティリスク管理フレームワークを踏まえ、CISO 等は、当該フレームワークに則った適切なリスク管理を行い、ビジネスラインにおけるリスク低減策に問題がある場合には、改善を促すことが求められている。

米国では、サイバーセキュリティリスクをコーポレートリスクと捉え、所管部署におけるリスク管理が適切に行われているか CISO 等が指揮・監督している。

他方、我が国では、サイバーセキュリティリスクはシステムリスクの一環として、主にシステム部門を中心にリスク管理が行われている。サイバー攻撃の高度化・複雑化が進む中、全社的にリスク管理が適切に実行される態勢の構築が望まれる。

(2) サイバーセキュリティを確保するための牽制機能の発揮

CISO 等は、全社的なサイバーセキュリティのリスクを許容可能な程度に低減し管理する立場にあることから、ビジネスラインあるいはシステムの開発・運用を行う部門から独立した立場から牽制機能を発揮すべきである。

例えば、米国では、各ビジネスラインの中にセキュリティ担当者を配置するケースが見られるが、このような組織体制をとっている場合は、各ビジネスラインが所管する情報システムのセキュリティ対策は、当該セキュリティ担当者によって実行される。そのため、CISO 等は、ビジネスラインから独立した「第二線」の立場から、全社的な視点でサイバーセキュリティ管理にとって脅威となる事象と業務に与える影響を把握できる。

我が国では、米国のような組織体制を採用しているケースは少ないものの、CISO 等が「第一線」へ牽制を働かせることが望ましいという点に変わりはない。

我が国の金融機関においては、システム部門を担う CIO が CISO 等を兼務するケースが多くみられるが、サイバーセキュリティリスク管理の実効性の観点から、CIO と CISO 等を分離し牽制機能を持たせる、あるいは CIO が CISO 等の役割を兼務する場合は、両面の役割・責任がバランスよく発揮できるよう、より上位の経営者や外部監査人等によるチェック機能を備えることが望まれる。

(3) 脅威情報の収集・分析スキームの構築

CISO 等は、金融 ISAC や JPCERT コーディネーションセンター等に代表される情報共有機関や、他の金融機関との情報連携を通じて、複数のルートから脅威情報を収集・分析することが望まれる。また、CISO 等は入手した脅威情報を、経営に大きな影響を与えるサイバーインシデントか判断し、その影響を未然に防止・低減する仕組みの構築が望まれる。

米国では、CISO 等の関与のもと、情報収集・分析を行う担当者が各国当局や IT ベンダ等を含め、複数のルートから積極的にサイバーセキュリティの脅威の把握に努めている。加えて、CISO 等自身も複数の企業での業務を経験し、他の企業における CISO 等と連携することも多い。

さらに、米国では、入手した脅威情報を基に、サイバーインシデントの攻撃主体等の情報により、リスクを評価し、脅威情報をインテリジェンス化することにより、サイバーセキュリティリスクを判断するスキームを構築している例もみられた。

一方、我が国では、脅威情報の入手先が限定的である金融機関が散見される。さらに、CISO 等による情報連携の機会も限られていることから、複数ルートからの脅威情報の収集スキームに CISO 等が積極的に関与することが望まれる。

また、我が国では、サイバーセキュリティを担う人材の不足等により入手した脅威情報を十分に分析できていない例もみられた。脅威情報をインテリジェンス化することにより、未然にサイバーセキュリティリスクの顕在化を防ぐことが可能となることから、CISO 等を中心とした情報分析スキームを構築することが望ましい。

(4) 予算・リソースの確保のための経営層への働きかけ

サイバーセキュリティリスクは、経営に甚大な影響を与える。したがって、CISO 等は、ビジネスを刷新するための情報システムへの新たな予算や、他の情報セキュリティの投資により、サイバーセキュリティに関する予算が劣後されないよう配慮することが求められる。

そのため、CISO 等は、情報セキュリティ管理について、必ずしも十分な専門的な知識を有しているとは限らない経営層に対して、サイバーセキュリティ対策の重要性を訴え、サイバーセキュリティリスクの低減策に必要な予算措置を講ずるよう働きかけることが求められる。

また、CISO 等は、平時から脅威の動向、全社的なサイバーセキュリティリスク、外部環境の変化等、サイバーセキュリティ管理について、取締役会や執行会議等で報告を行うこと等を通じて、経営層へサイバーセキュリティ対策の重要性を理解させることが必要である。

(5) マネジメント能力を備えた人材の確保

CISO 等は、全社的な情報セキュリティリスクを担当する責任者として、情報セキュ

リティリスク管理への深い知見や、関係部署の協力を得ながらサイバーセキュリティ戦略を推進する等、マネジメント能力を備えることが求められる。

米国における CISO 等には、我が国に比べて、概ね情報システムの開発や情報セキュリティリスク管理の実務経験等を背景に、全社的なサイバーリスク管理を担える者が多い。

こうしたことから、我が国においても、マネジメント能力を備えた人材の確保・育成が望まれる。