BOJ Reports & Research Papers

金融システムレポート別冊シリーズ

Financial System Report – Annex

地域金融機関における サイバーセキュリティセルフアセスメント の集計結果（2022 年度）

日本銀行金融機構局
金融庁総合政策局

２０２３ 年 ４ 月

本レポートの内容について、商用目的で転載・複製を行う場合は、予め日本銀行金融機構局までご相談ください。転載・複製を行う場合は、出所を明記してください。

【本レポートに関する照会先】
日本銀行金融機構局考査企画課（csrbcm@boj.or.jp）

金融システムレポート別冊シリーズについて

日本銀行は、マクロ・プルーデンスの視点からわが国金融システムの安定性を評価するとともに、安定確保に向けた課題について関係者とのコミュニケーションを深めることを目的として、『金融システムレポート』を年 2 回公表している。同レポートは、金融システムの包括的な定点観測である。

『金融システムレポート別冊シリーズ』は、特定のテーマや課題に関する掘り下げた分析、追加的な調査等を行うことにより、『金融システムレポート』を補完するものである。本別冊では、2022 年度に日本銀行と金融庁が共同して地域金融機関向けに初めて実施した「サイバーセキュリティセルフアセスメント」の集計結果について、地域金融機関全体としてのサイバーセキュリティ管理態勢の概要と、今後の更なる態勢強化に向けたポイントを紹介する。

本別冊の要旨

サイバー攻撃が一層の高まりをみせ、サイバーセキュリティ管理態勢の整備や実効性の確保が重要な課題となっている。今般、日本銀行および金融庁は、サイバーセキュリティ管理態勢について、金融機関が他の金融機関対比での自組織の立ち位置や課題となる領域を特定する自己評価ツールを整備し、地域金融機関（地域銀行 99 先、信用金庫 254 先、信用組合 145 先）を対象に、初めてサイバーセキュリティセルフアセスメントの実施を求め、その集計結果を還元した。

集計結果から多くの地域金融機関では、サイバーセキュリティの確保を経営上の重要課題と捉え、態勢整備や技術対策に加え、コンティンジェンシープランに基づいた訓練の実施などサイバーセキュリティ対策の実効性向上に向けた取り組みを進めているが、サイバーセキュリティ人材の確保・育成やサードパーティリスクの管理といった課題を抱えていることが確認できた。

日本銀行および金融庁としては、地域金融機関がサイバーセキュリティ管理態勢の更なる強化に向けた取り組みを進めていくうえで、サイバーセキュリティセルフアセスメントが活用されることを期待するとともに、考査や検査、モニタリング、各種セミナー等を通じて、そうした取り組みを後押ししていく方針である。

I. サイバーセキュリティセルフアセスメントについて

1. 背景

最近のわが国の金融機関を取り巻く環境をみると、デジタル技術を活用し、モバイル端末向けのアプリケーションの開発[1]や FinTech 企業等の異業種との連携といった対顧客サービスの拡充に加え、リモートワークの導入[2]やクラウドサービスの活用[3]といった業務改革を推進する動きが進んでいる。他方、サイバー空間においては、複雑化・巧妙化したランサムウェア攻撃をはじめとして、組織化・洗練化されたサイバー攻撃が増加していることなどから、サイバー攻撃の脅威は一層高まっている。金融機関が、今後もデジタル技術を活用した顧客サービスの向上や業務の効率化に取り組んでいくうえで、サイバー攻撃の脅威の高まりを踏まえた、サイバーセキュリティ管理態勢の整備や実効性の確保は重要な課題となっている。

2. CSSA の目的

わが国の金融機関では、サイバーセキュリティの管理状況を確認するにあたって、大手金融機関では、国際的なフレームワーク[4]を活用した成熟度評価が行われている。一方で、地域金融機関では、これまで他の金融機関対比での自組織の立ち位置や課題となる領域を特定するツールが必ずしも広く用いられてこなかった。今般、日本銀行および金融庁は、地域金融機関を対象とした自己評価ツール（点検票）を整備し、「サイバーセキュリティセルフアセスメント（以下、CSSA）」を 2022 年度に初めて実施した。具体的には、地域金融機関に対し、CSSA の点検票に基づくサイバーセキュリティ管理態勢の自己評価を依頼し、集計結果を還元した。これにより、各地域金融機関において、自己評価に基づいて自組織の課題を認識したうえで自律的にサイバーセキュリティ対策の一層の強化に取り組むことを期待している。

3. CSSA の実施対象先金融機関

CSSA は、地域金融機関（地域銀行 99 先、信用金庫 254 先、信用組合 145 先）を対象に実施した[5]。なお、本取り組みは、環境変化を踏まえた設問の見直しを行いながら、2023 年

---

[1] 金融機関におけるアプリの提供状況等については、「金融機関におけるモバイルアプリの提供状況と管理体制について－アンケート調査結果から－」（金融システムレポート別冊シリーズ、2022 年 11 月）を参照。

[2] 金融機関におけるリモートワークの導入状況等については、「金融機関における在宅勤務の拡がりとシステム・セキュリティ面の課題－アンケート調査結果から－」（金融システムレポート別冊シリーズ、2020 年 10 月）を参照。

[3] 金融機関におけるクラウドサービスの活用状況等については、「クラウドサービス利用におけるリスク管理上の留意点」（金融システムレポート別冊シリーズ、2020 年 11 月）を参照。

[4] 例えば、米国連邦金融機関検査協議会（FFIEC）が策定したサイバーセキュリティアセスメントツール（CAT）を用いる事例がみられる。

[5] 金融機関による自己評価は 2022 年 7 月～8 月に実施。その後、同年 11 月に集計結果の還元を実施。

度以降も継続的に実施していくことを想定しているほか、保険、証券などの他の金融業態への活用も展望している。

4. CSSA の点検票の概要

CSSA の点検票は、日本銀行および金融庁が、金融情報システムセンター（FISC）の協力のもとで作成した。

設問は、全体を通して、自組織のサイバーセキュリティ管理態勢を網羅的に評価できるような構成とすることを目指し、米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワーク（CSF）をはじめ主要なサイバーセキュリティリスク管理の枠組みやアンケート調査の設問[6]などを参考に作成した（NIST CSF での 5 つの機能については後段の BOX1 を参照）。また、各設問は、国内の特定地域を中心にビジネスを展開する地域金融機関の規模や特性を踏まえるとともに、リモートアクセスやクラウドサービスの利用拡大など、システム環境の変化やランサムウェア攻撃の増加といった最近のサイバー攻撃の脅威動向を勘案している。なお、点検票は、地域金融機関自身が、自己評価に基づいて自律的にサイバーセキュリティ対策を強化することを促す目的で作成しているものであって、日本銀行または金融庁としてのベストプラクティスやミニマムスタンダードを示すものではないことに留意が必要である。

点検票における設問の主な論点は、以下のとおりである（図表 1、点検票は別紙参照）。

[6] 具体的には、国内金融機関で活用されている FISC の「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」、米国の The Cyber Risk Institute（CRI）が管理・更新しているサイバーリスクの評価の枠組み「CRI Profile」、日本銀行にて実施した「サイバーセキュリティに関するアンケート（2019 年）」、FISC にて実施した「令和 4 年度 金融機関アンケート」などを参考にしている。

図表 1 CSSA の点検票における設問の主な論点

項　目	設問数	論点
サイバーセキュリティに関する経営層の関与	4	サイバーセキュリティに関する経営方針や経営計画、経営層への定期報告、随時報告など
サイバーセキュリティに関するリスクの把握と対応	4	サイバー攻撃の把握、情報収集、リスク評価、リスクへの対応方針の決定など
サイバーセキュリティに関する監査	3	監査対象、監査結果の報告先、指摘事項に対する改善の実施状況の確認
サイバーセキュリティに関する教育・訓練	1	サイバーセキュリティに関する注意喚起・教育・訓練の実施状況
新たなデジタル技術の評価	2	新たなデジタル技術の導入に際するリスク評価の体制など
資産管理	3	システム管理簿の整備状況、ハードウェア、ソフトウェアの管理状況など
アクセス管理	2	重要なシステムへのアクセス権、リモートアクセスの管理状況など
データ保護	2	データ保護（暗号化、伝送制限）、バックアップ対策など
監査証跡(ログ)の管理	1	重要なシステムの監査証跡(ログ)に関する規定
システムの脆弱性に関する管理・対応	4	脆弱性診断やペネトレーションテストの実施状況、パッチ適用方針など
サイバー攻撃に関する技術的な対策	3	端末、境界、Webサイト・インターネットバンキングシステムにおける技術的な対策
サイバーインシデントの検知	2	監視・分析等の実施状況、モニタリング内容
サイバーインシデント対応・業務復旧の態勢	6	サイバーインシデント発生時の対応要員、対応ルール・手順の整備など
サードパーティ等の管理	5	サードパーティ管理状況、クラウドサービスに対する安全対策など
合　計	42	（うちFISCアンケートとの共通設問3問を含む）

以下では、自己評価の集計結果に基づき、地域金融機関全体としてのサイバーセキュリティ管理態勢の概要と、今後の更なる態勢強化に向けたポイントを紹介する。なお、自己評価結果には、地域金融機関のセキュリティに関する技術的な情報が多く含まれることから、本レポートでは集計結果の開示にあたっては、地域金融機関のセキュリティ確保にも配慮している。

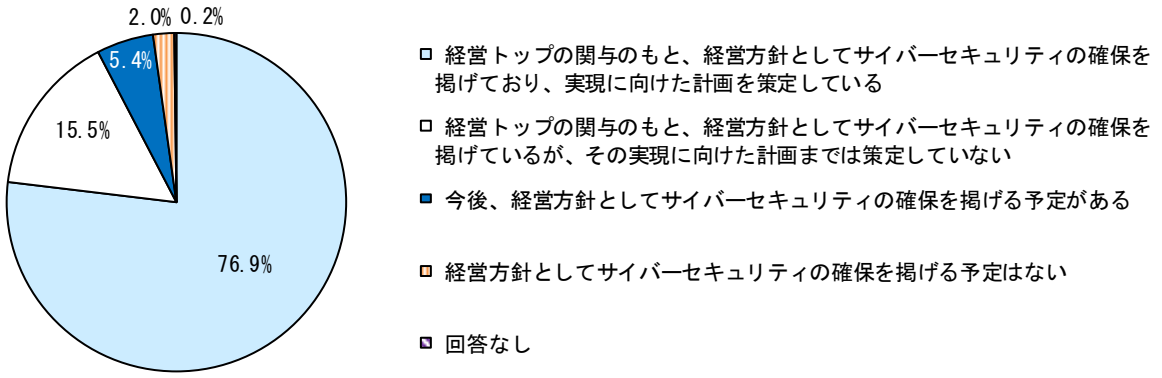
II. サイバーセキュリティセルフアセスメントの集計結果概要

1. 経営層の関与

経営方針の策定とその実現に向けた態勢

対顧客サービスの拡充や業務改革の推進といったデジタル化戦略を推進するにあたっては、その戦略内容を踏まえたサイバーセキュリティ管理態勢の整備について、経営トップの関与のもと、経営資源の投入を含む具体的な計画を策定し、計画的に取り組むことが重要である。サイバーセキュリティに関する経営方針・計画の策定状況をみると、8 割弱の先が、経営トップの関与のもと、経営方針としてサイバーセキュリティの確保を掲げ、実現に向けた計画を策定していると回答している（図表 2）。

図表 2 サイバーセキュリティの経営方針・計画



次に、自組織のサイバーセキュリティを統括する責任者についてみると、9 割強の先が役員と回答している（サイバーセキュリティのガバナンスモデルについては後段の BOX2 を参照）。内訳については、システムリスクを所掌する役員[7]（CIO[8]）が約 8 割となっており、一部大手行で任命される事例がみられるサイバーセキュリティを専門に担う役員（CISO[9]）が置かれている先は 7%弱となっている（図表 3）。

サイバーセキュリティに関し、経営層に定例的に報告している内容についてみると、自組織のサイバーインシデントや対策状況が高い一方で、他社事例については自組織と比べて低いとの回答となった（図表 4）。経営層に対し、他社のサイバーインシデント事例を含め最近の脅威動向に関する情報を広く報告し、自組織の対策状況の点検に繋げていくことが重要である。なお、他社事例に関しては、報道情報に加え、業界団体、官公庁などから無償で収集す

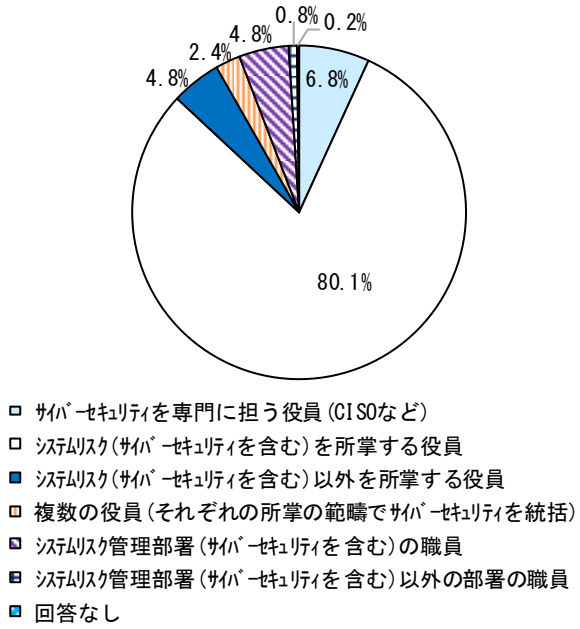
[7] 本レポートでは、執行役員などの従業員役職者は便宜上「役員」に含めている。

[8] Chief Information Officer の略。

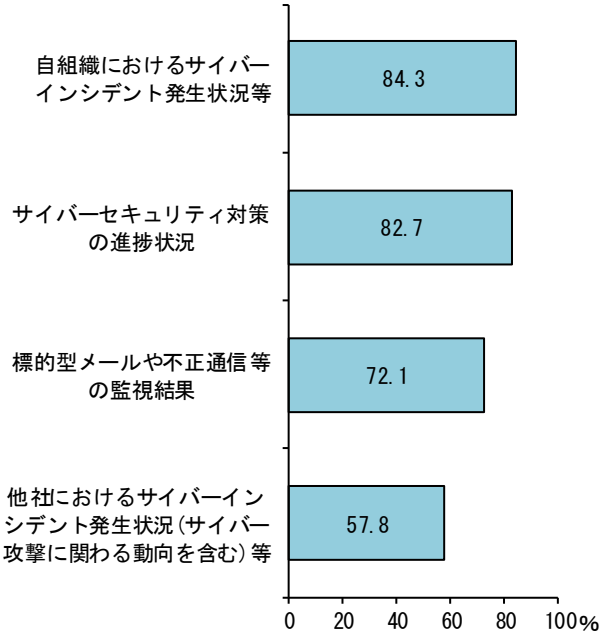
[9] Chief Information Security Officer の略。

ることが可能である。

図表 3 サイバーセキュリティの統括責任者



図表 4 サイバーセキュリティに関し、
経営層へ定例報告している内容



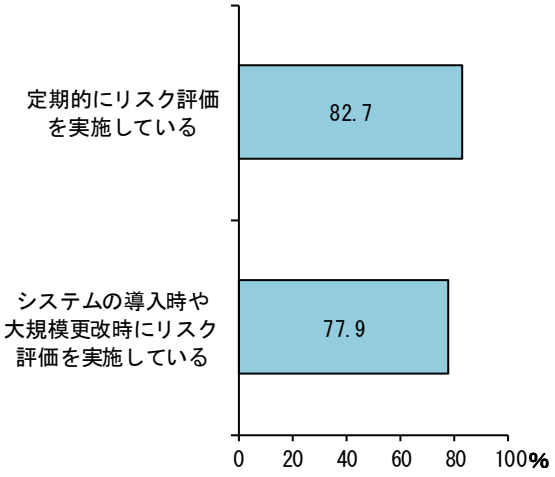
サイバーセキュリティに関するリスク評価の実施

自組織が利用する重要なシステム[10]に対しては、サイバーセキュリティに関するリスク評価を、適時適切に行うことが重要である。リスク評価の実施状況をみると、定期的に実施している先や、システムの導入時や大規模更改時に実施している先が多かった（図表 5）。

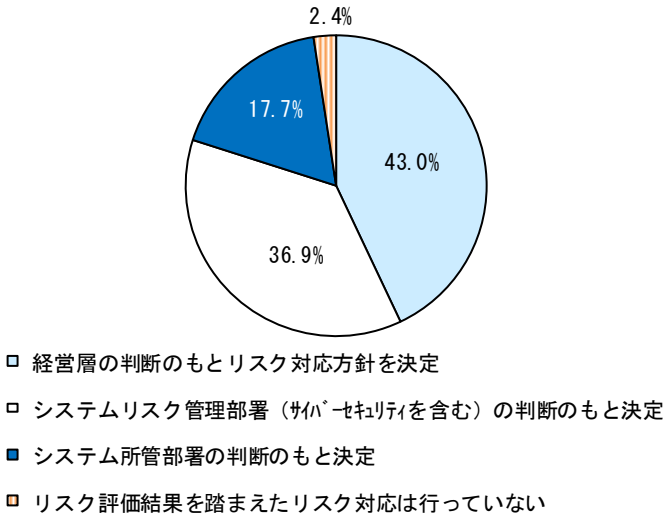
リスク評価を踏まえた、対応（低減、回避、移転、受容）の決定や対応方針の優先順位の決定については、経営層の関与のもとで組織的に行われることが重要である。決定者についてみると、システムリスク管理部署やシステム所管部署が判断している先が多く、経営層が判断している先は４割強であった（図表 6）。

[10] 今回の CSSA では、「重要なシステム」とは、「勘定系や顧客情報を扱うシステムなど自組織として業務運営上特に重要と認識しているシステム」と定義。

図表 5 重要なシステムのサイバーセキュリティに関するリスク評価の実施状況



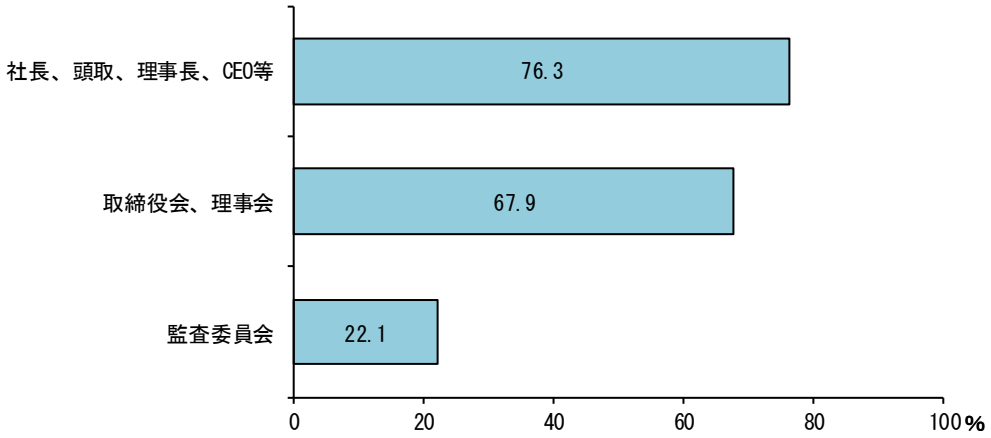
図表 6 リスク評価を踏まえた対応方針の決定者



サイバーセキュリティに関する監査

サイバーセキュリティに関する監査結果の報告先についてみると、大半の先が経営層に報告している（図表 7）。サイバーリスクは金融機関の経営上の重要課題の一つであることを踏まえると、今後はサイバーセキュリティの監査について、経営層が監査結果を認識することにとどまらず、監査部門が監査指摘事項の改善策の実施状況を被監査部門に確認することなどを通じ、所謂「第３線部門としての機能」を発揮することが重要である。

図表 7　サイバーセキュリティに関する監査結果の報告先



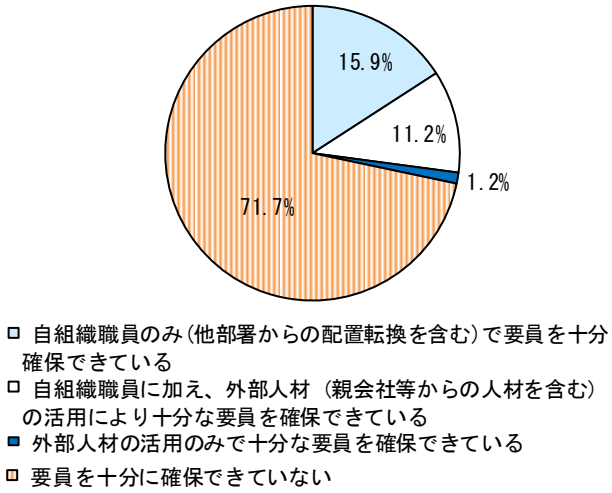
サイバーセキュリティ人材の確保の態勢

デジタル技術を活用した対顧客サービスの拡充や業務改革を進めるにあたり、同時に、それにより生じ得るサイバーセキュリティに関するリスクを評価・管理できる人材の確保が重要である。こうした人材の確保の状況をみると、７ 割強の先が要員を十分に確保できていな

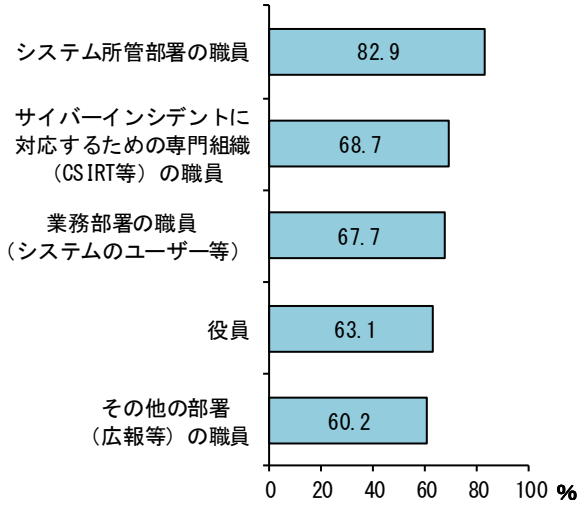
いと回答している（図表 8）。

サイバーセキュリティ人材の不足感が強い中にあって、各先とも、内部職員の育成のほか、外部専門業者の活用など組織態勢の強化に向けて複線的に取り組んでいる。そうした人材の育成・強化策の一つである e-learning（ビデオ、書面等含む）によるサイバーセキュリティに関する意識啓発の対象者をみると、システム所管部署の職員を対象に含めている地域金融機関が 8 割を上回っているものの、役員やその他の職員を対象とする先は 6～7 割にとどまっている（図表 9）。今後、システム所管部署にとどまらず、経営層、業務部署、広報その他部署などの幅広い層への研修等を通じて、組織全体としてのサイバーセキュリティ人材の育成や知識の底上げを図ることが期待される。

図表 8　新たなデジタル技術導入により生じ得るサイバーセキュリティに関するリスク評価が可能な人材の確保状況



図表 9　e-learning（ビデオ、書面等含む）による啓発の対象者



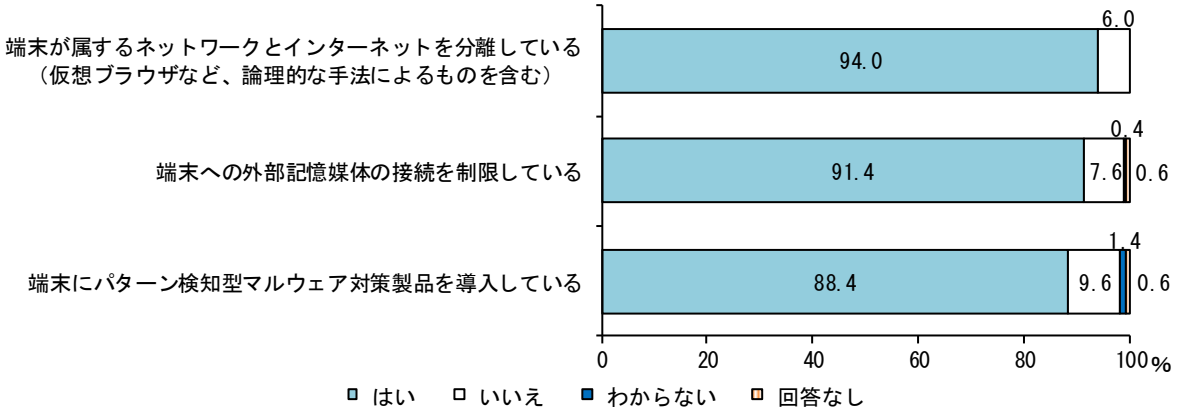
2. リスクへの構え

サイバー攻撃への技術的対策

OA 端末[11]のサイバー攻撃対策についてみると、インターネットとの分離、外部記憶媒体の接続制限、パターン検知型マルウェア対策製品の導入といった対策が進んでいる（図表 10）。今後、デジタル化施策を一段と推進していく場合、脅威動向の変化に目配りしつつ、新しいリスクに応じたサイバーセキュリティ対策の高度化に取り組んでいく必要がある。

[11] 今回の CSSA では、「OA 端末」とは、「職員が文書作成等で標準的に用いる端末」と定義。

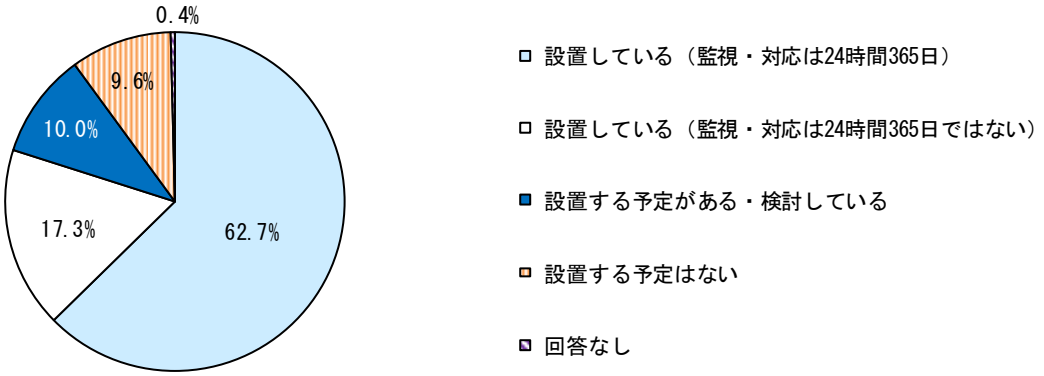
図表 10 OA 端末のサイバー攻撃対策



サイバーインシデントの監視・分析態勢

サイバーインシデントを早期に検知し、迅速に対応するためには、セキュリティ関連の監視・分析等を行う組織（SOC[12]）を設置することが重要である。そうした組織の設置状況をみると、約 8 割の先で設置されており、常時の監視・対応を行っているとの回答は 6 割を超えていた（図表 11）。今後も、常時化（24 時間 365 日）を含め、検知・対応の迅速化が期待される。

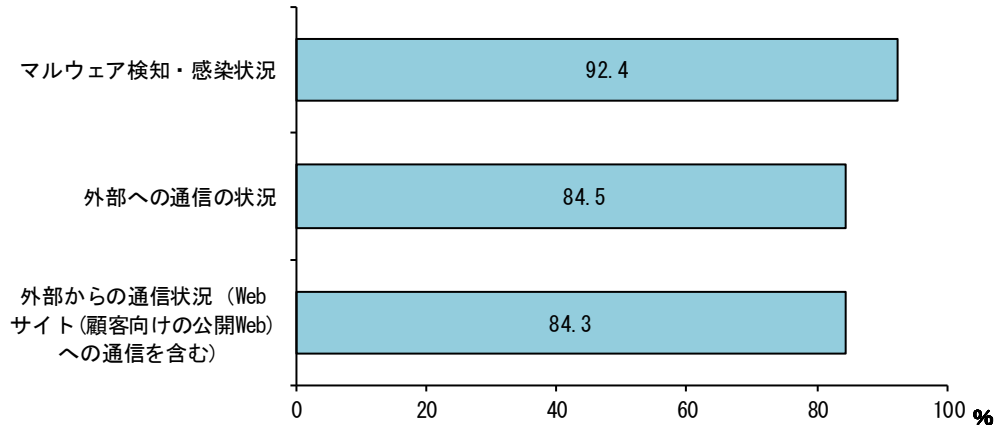
図表 11 セキュリティ関連の監視・分析等を行う組織（外部委託含む）の設置状況



また、SOC 等サイバーセキュリティの監視部署でのモニタリング対象をみると、マルウェア検知・感染状況や外部との通信状況を監視・分析しているとの回答が 8 割を超えていた（図表 12）。今後も、監視する対象システム等の拡充を含め、モニタリングの一層の高度化が期待される。

[12] Security Operation Center の略。ネットワークやサーバ、ファイアウォール等の機器への攻撃状況など、セキュリティ関連の監視・分析等を行う組織。

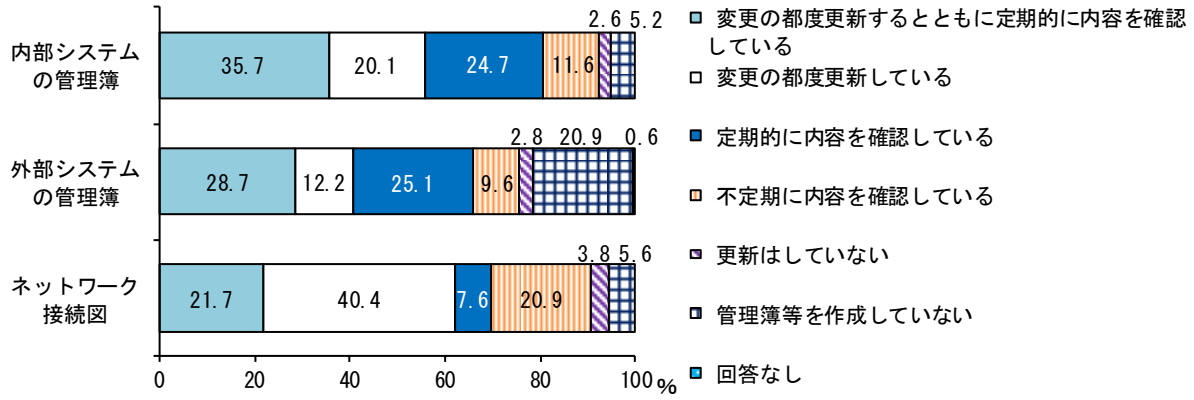
図表 12 SOC 等サイバーセキュリティの監視部署でのモニタリング対象



システム資産の管理、脆弱性への対応

サイバーインシデントの発生原因としては、システムの OS やソフトウェアの脆弱性（vulnerability）を悪用した攻撃が多くみられる。まず、組織としてシステム資産の管理が適切に行われているかという観点から、管理簿等の整備状況をみると、内部システム[13]と比べて外部システム[14]の更新・確認の頻度が低くなっていた（図表 13）。自らが提供する対顧客サービスや内部の重要情報を格納するシステムについては、外部システムであっても自組織におけるシステムとして認識し、管理簿等を作成するほか、内容を最新化しておくことで、システムの脆弱性調査や保守契約の管理などを迅速かつ正確に実施できるようにすることが重要である。

図表 13 システムの管理簿等の整備状況

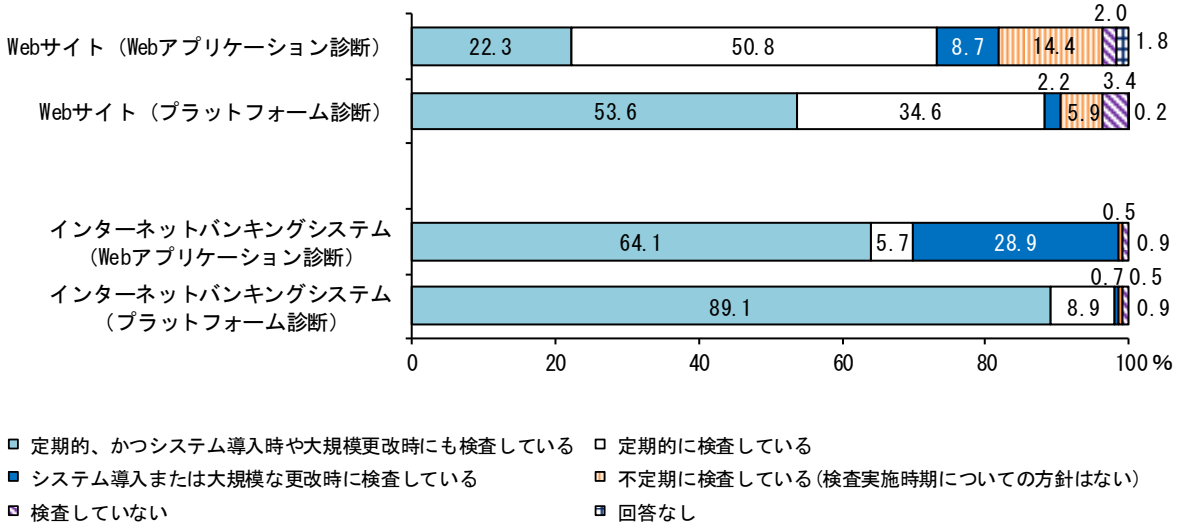


[13] 今回の CSSA では、「内部システム」とは、「自組織内で運用しているシステム」と定義。

[14] 今回の CSSA では、「外部システム」とは、「自組織の外部で運用しているシステム（クラウドを含む）」と定義。

脆弱性が新たに判明する可能性もあることから、システム導入時の脆弱性診断に加え、導入後も診断を継続的に実施することが重要である。脆弱性診断等の実施状況についてみると、多くの先でシステム導入後も継続的に実施されている（図表 14）。また、脆弱性診断の実施に加え、自組織における検知・監視態勢を整備・確立している先においては、ペネトレーションテスト[15]や脅威ベースのペネトレーションテストを実施し、客観的な目線から検知・監視態勢の実効性の確認を行うことも重要である。

図表 14 脆弱性診断等の実施状況

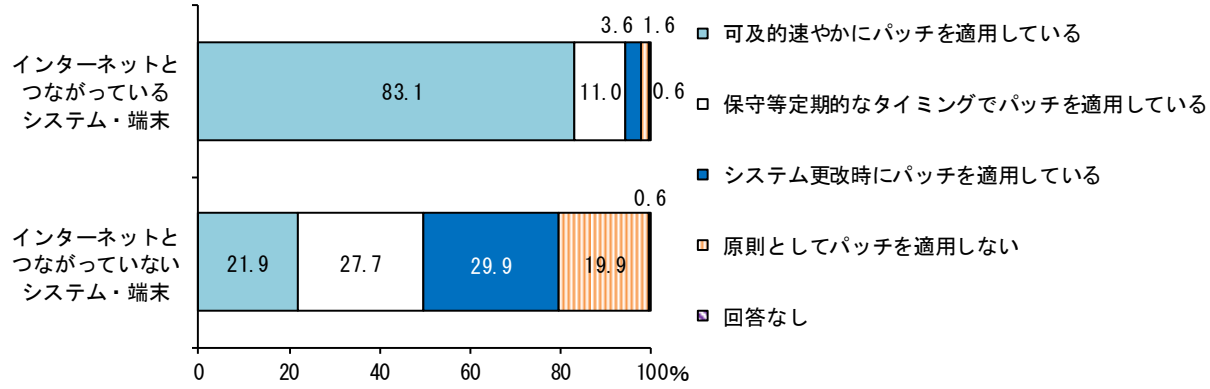


（注）診断等の実施には、外部にシステム運用を委託している場合の同先での診断等の実施状況を確認している場合も含む。

このほか、自組織のシステムで深刻な脆弱性が判明した場合の対応としては、セキュリティパッチ（脆弱性修正プログラム）を迅速に適用することが重要である。そうした場合のパッチの適用方針をみると、インターネットと接続しているシステムでは 8 割以上の先が可及的速やかに適用している一方、インターネットと接続していないシステムでは、ほぼ半数の先が、システム更改時に適用するか、原則としてパッチを適用しないとの対応であった（図表 15）。攻撃の蓋然性を勘案したリスクベースでの対応を基本としつつ、最近のサイバーインシデント事案を踏まえ、閉域網を過信することなく、パッチ適用の要否を検討することが重要である。

[15] 今回の CSSA では、「ペネトレーションテスト」とは、「擬似的なマルウェアを利用したり、脆弱性･設定不備等を悪用したりするなど擬似的な攻撃を仕掛けることで、侵入･改ざんの可否や検知の可否、対応の迅速性･適切性を検証するテスト」と定義。

図表 15 深刻な脆弱性が判明した場合のパッチの適用方針

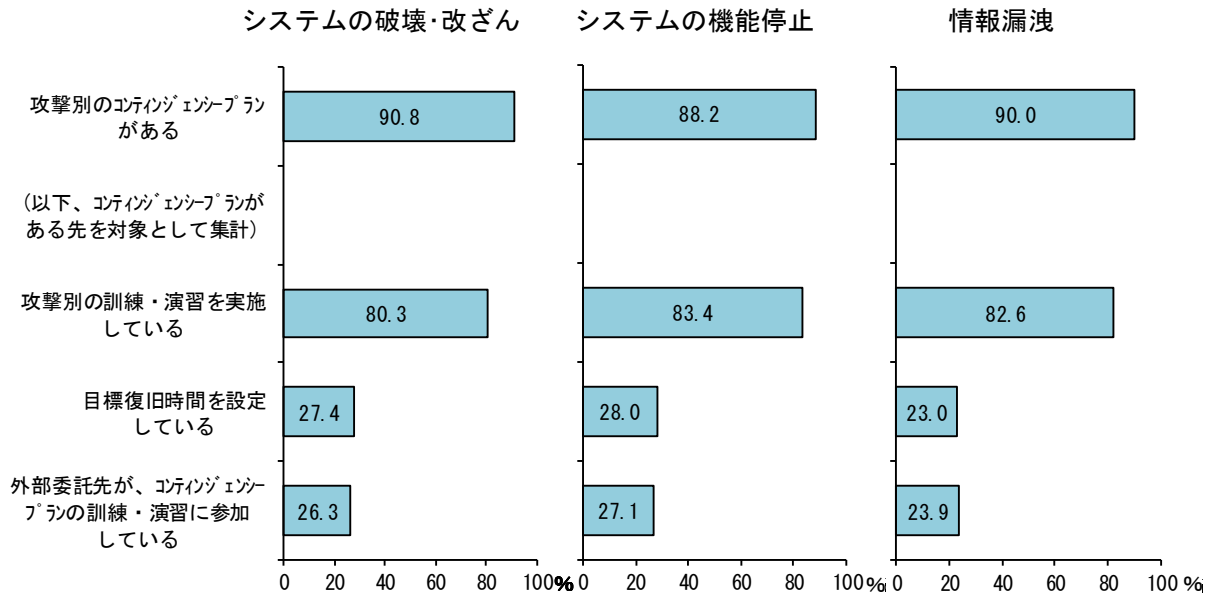


3. 有事への備え

コンティンジェンシープランの策定、訓練・演習の実施

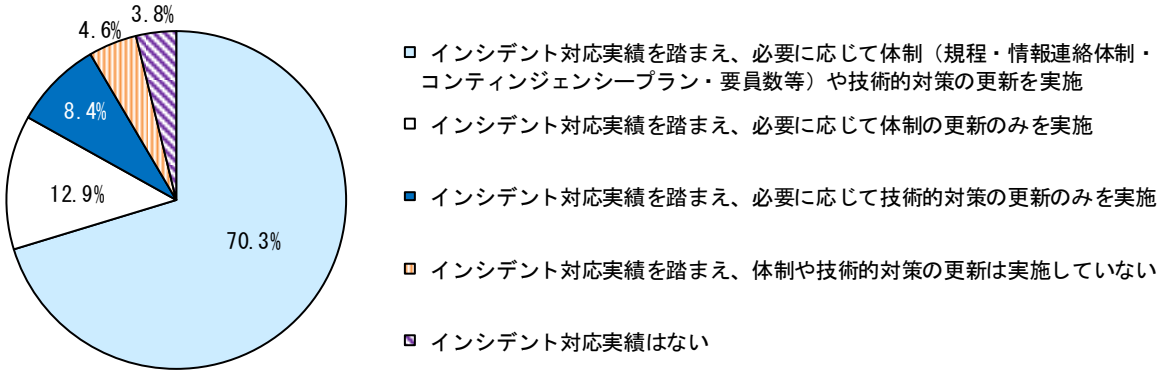
サイバーリスクが顕在化した場合を想定し、迅速な復旧を図ることが重要である。コンティンジェンシープランの整備状況をみると、大半の先がサイバー攻撃（被害）の別に応じてプランを整備している（図表 16）。今後は、業務への影響に応じて目標復旧時間を設定するとともに、外部委託先をはじめ重要なサードパーティに対するサイバー攻撃を想定した自組織のコンティンジェンシープランの整備および演習の実施など、コンティンジェンシープランの実効性を一層高めることが重要である（なお、復旧において重要となるバックアップデータの破壊・改ざん対策については後段の BOX3 参照）。

図表 16 サイバー攻撃（被害）に対応するコンティンジェンシープランおよび取組内容



また、サイバーインシデント対応や訓練・演習の実績を踏まえ、インシデント対応のための関連規程、情報連絡体制、コンティンジェンシープラン、要員数等の体制の見直しを図るとともに実効性を向上していくことも重要である。こうした取り組みについてみると、大半の先が実績を踏まえ、体制または技術的対策の更新に繋げていた（図表 17）。

図表 17 インシデント対応（訓練・演習を含む）実績を踏まえた体制の強化状況



サードパーティリスクへの取り組み

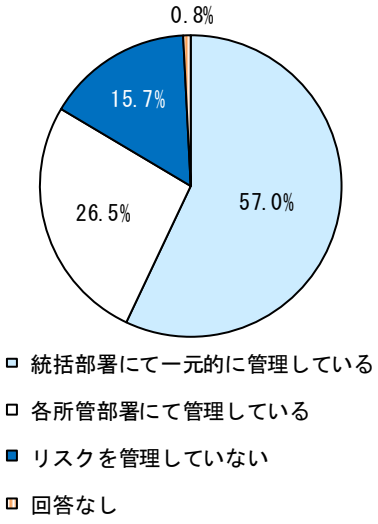
昨年、G7 がサードパーティに関するハイレベルガイダンスを公表するなど[16]、デジタルビジネスを支える広範かつ複雑なサプライチェーンを管理することの重要性が高まっている。重要なサードパーティ[17]に関するサイバーセキュリティのリスク管理状況をみると、半数以上の先で統括部署にて一元的に管理されている（図表 18）。

また、外部委託先とサイバーセキュリティに関する事項を契約等で定めているかについては、委託業務または提供サービス等におけるサイバーセキュリティ対策についての責任分界や、サイバーセキュリティのリスク管理責任者を定めていない先が少なからずみられた（図表 19）。サードパーティとの契約は先方の雛形に沿って締結されることが多いものと考えられるが、重要事項については、相手先と十分に確認を行い、追加的に書面のかたちで取扱いの明確化を図ることが重要である。

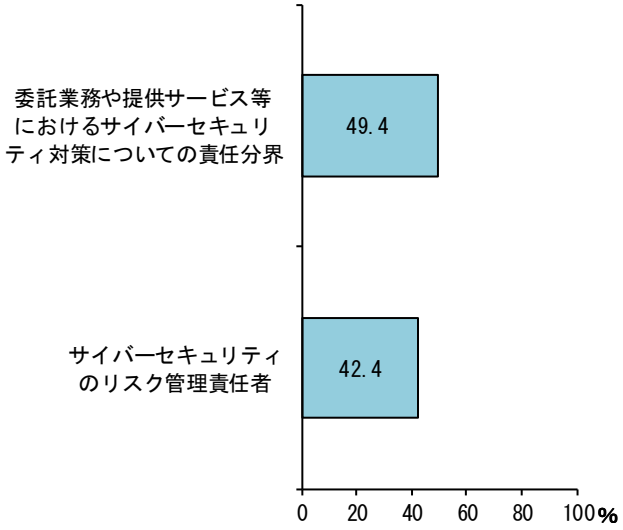
[16] G7 のサードパーティに関するハイレベルガイダンスについては、日本銀行または金融庁「G7 サイバー・エキスパート・グループによるランサムウェア及びサードパーティのサイバーリスクマネジメントに関する基礎的要素の公表について」（2022 年 10 月）を参照。

[17] 今回の CSSA では、「重要なサードパーティ」とは、「自組織として業務運営上重要と認識しているサードパーティ」と定義。なお、「サードパーティ」とは、「自組織がサービスを提供するために、業務上の関係や契約等を有する他の組織」と定義（例：システム子会社、ベンダー等の外部委託先、クラウド等のサービス提供事業者、資金移動業者等の業務提携先など）。

図表 18 重要なサードパーティ、また、それらが提供するサービス等のサイバーセキュリティに関するリスク管理状況



図表 19 外部委託先との契約等で定めている事項



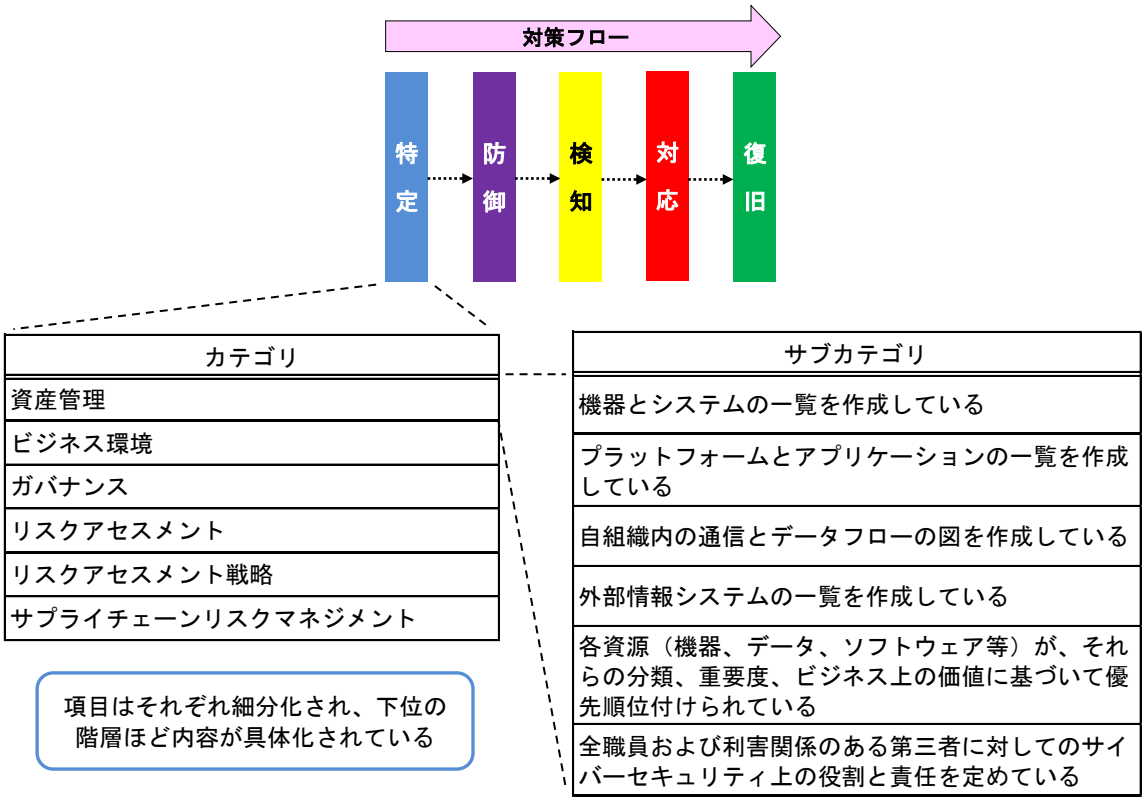
BOX1　NIST CSF における 5 つの機能

NIST CSF とは、米国国立標準技術研究所（NIST）が作成したサイバーセキュリティ対策のフレームワークであり、わが国でも、重要インフラをはじめ、幅広い業界で組織のサイバーセキュリティ態勢の測定や改善活動に活用されている。

NIST CSF では、サイバーセキュリティ対策において取り組むべき事項を関連する項目毎に整理するとともに、順序立てて示している。このうち、第一の項目は、以下、「5 つの機能」として最も基本的な 5 項目の要素に分類されている（図表 B1）。

また、各「機能」をさらに細分化した対策が、「カテゴリ」、「サブカテゴリ」として、下位の階層ほど内容が具体的に示されているため、取り組むべきサイバーセキュリティ対策を検討するうえで有用である。

図表 B1　NIST の CSF における 5 つの機能



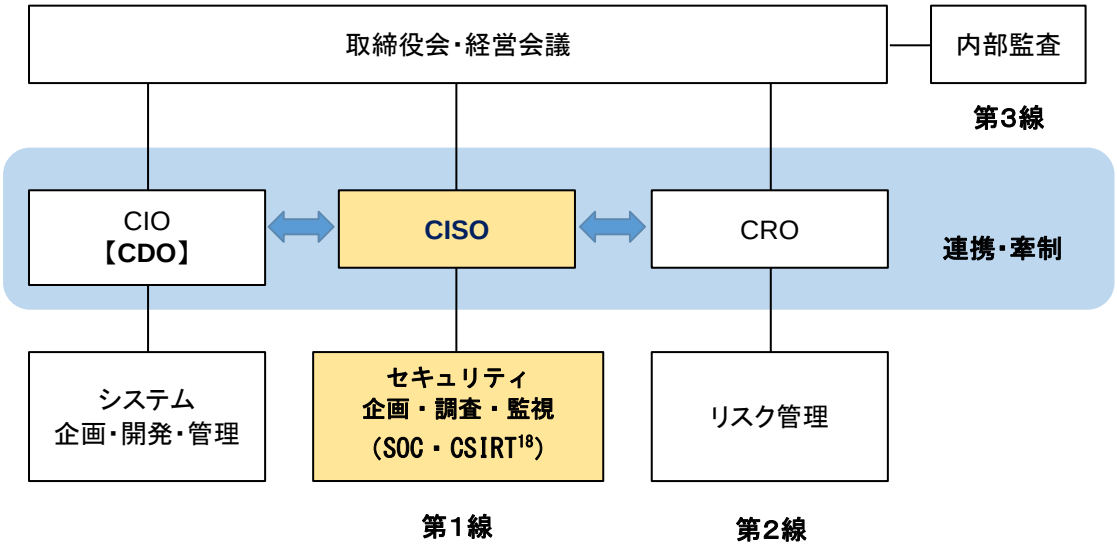
BOX2　サイバーセキュリティのガバナンスモデル

サイバーセキュリティを含むシステムリスクの管理態勢については、従来、システム部門の責任者である CIO（Chief Information Officer）が担っていたが、サイバーセキュリティの重要性が増していることから、近年、CIO から独立した CISO（Chief Information Security Officer）がサイバーセキュリティに関するリスク管理や各種対策を担うガバナンスモデルが海外で広がりつつあり、わが国でも大手金融機関の一部で採用事例がみられる（図表 B2）。

また、デジタルビジネスに戦略的に取り組むために、CDO（Chief Digital Officer）を設置する動きもみられているが、「攻め」と「守り」を両立する観点からも CDO の施策を検証する独立した CISO の重要性が高まっているといえる。

CISO はサイバーセキュリティの企画・調査・監視の機能を主に担うが、その際に、CIO・CDO および CRO（Chief Risk Officer）と密接に連携し、リスク認識の共有を図るとともに、実効的な施策を推進することが重要である。また、CISO の活動に対しては、第 2 線の CRO および第 3 線の内部監査が牽制機能を果たすことが重要である。

図表 B2　サイバーセキュリティ管理に関するガバナンスモデルの例



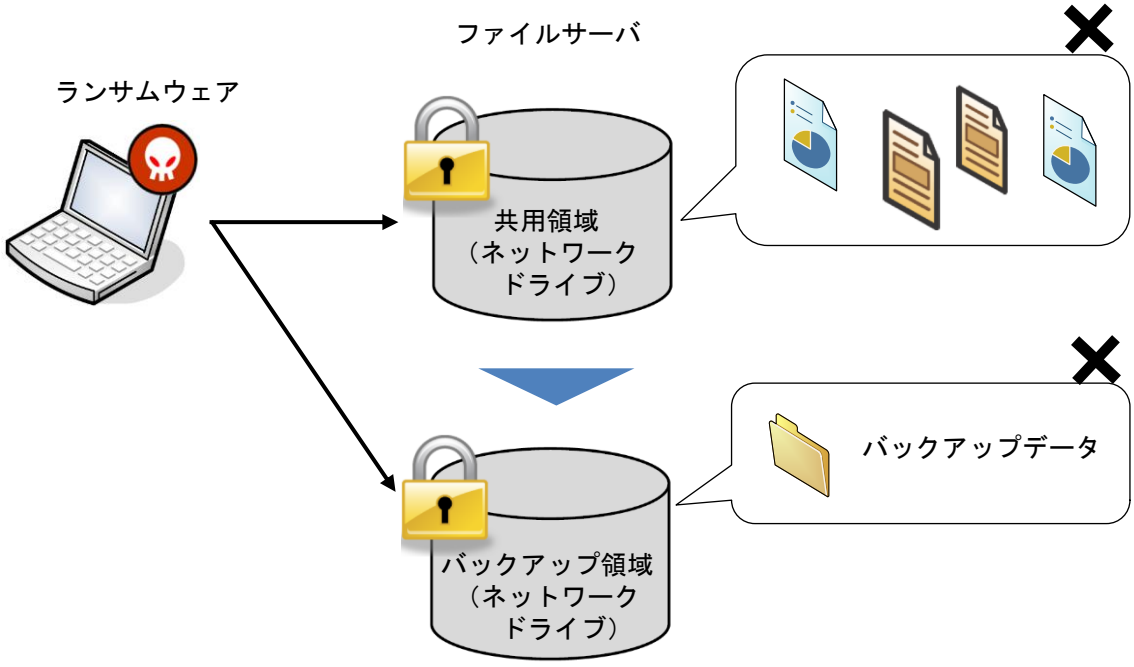
[18] Computer Security Incident Response Team の略。サイバーインシデントに対応するための組織。

BOX3　バックアップデータが破壊・改ざんされることを想定した対策

システムの破壊・改ざんの被害につながる攻撃として、システムのデータを暗号化し暗号解除の対価として暗号資産や金銭を要求する「ランサムウェア攻撃」が近年多く発生している。ランサムウェア攻撃を受けた場合の備えの一つとして、定期的に取得しているバックアップデータを用いて、システムを復旧する対策が有効である。

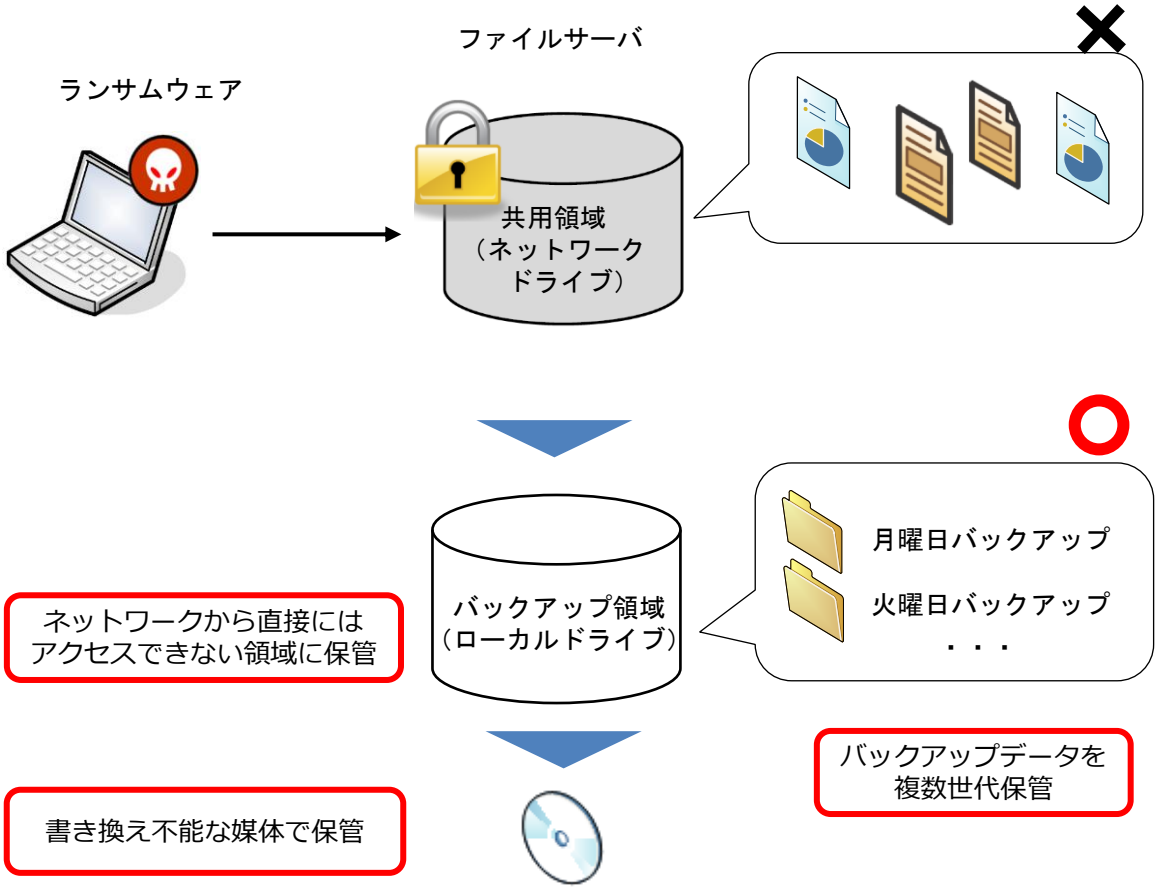
もっとも、あらかじめバックアップデータを取得していたものの、当該データの保管場所がランサムウェアに感染した機器からネットワークを介してアクセス可能であったため、バックアップデータも暗号化されてしまい、復旧が困難となったとの事例がみられる（図表 B3-1）。

図表 B3-1　ネットワークを介してバックアップデータも暗号化され得る場合のイメージ



業務復旧を早期に行う観点からは、バックアップデータが破壊・改ざんされないための対策を行うことが重要となる。この点、重要なシステムにおけるバックアップデータの破壊・改ざんを想定した技術的対策として、例えば、ランサムウェアの攻撃を回避する観点から、ネットワークから直接にはアクセスできない領域に保管する対策や書き換え不能な媒体で保管する対策がある。また、直近のデータも既に暗号化されているリスクに対処する観点から、バックアップデータを複数世代保管する対策などがある（図表 B3-2）。システムの重要性やシステム環境を踏まえ、適切な対策を行っておくことが重要である。

図表 B3-2　ランサムウェア攻撃などバックアップデータの破壊・改ざんを想定したバックアップデータの保管イメージ



また、取得したバックアップデータからの復旧が早急に行えるよう、あらかじめ手順を整備したうえで、復旧訓練を行うことで、復旧の実現可能性や復旧に要する時間を確認しておくなど、対策の実効性を確認することも重要である。

このほか、攻撃被害を受け、実際の復旧作業を行う際には、マルウェアに感染しているバックアップデータで復旧し、再度暗号化されてしまうことがないよう、あらかじめバックアップデータが安全なデータであることを確認したうえで復旧することが重要である。このため、バックアップデータをマルウェア対策製品でスキャンすることに加え、復旧を試みる段階で仮に原因が不詳である場合など、その時点では検知できないマルウェアに感染している可能性を考慮し、例えば、仮想環境や開発環境にて復旧を試行したうえで、安全なデータであることを確認するといった対応手順を確立しておくことが重要である。

III. 今後に向けて

金融機関によるデジタル技術を活用した対顧客サービスの拡充や業務改革を推進する動きが進むなかで、サイバー攻撃の脅威は一段と高まっている。各金融機関におけるビジネスの内容やデジタル技術の活用状況、システム構成によって、直面するサイバー攻撃の脅威には違いがあり、サイバーセキュリティの確保のために求められる取り組みも一律ではないものの、そうした脅威の高まりを踏まえて、今後もサイバーセキュリティ管理態勢の整備や実効性の確保に向けて取り組んでいくことが重要である。

この点、従来であれば、外部からのマルウェアの侵入をいかに水際で防ぐか、といった境界防御型の対策が重視されていたが、デジタル技術の活用に伴い、インターネットとの接続の拡大やサイバー攻撃の組織化・洗練化を受け、その対策として、最近では未知のマルウェアの侵入可能性は完全に排除できないとの前提のもと、性悪説に立って、組織のネットワーク内部も含め、多層的に対策を講じていくとの傾向が窺われる（この考え方は「ゼロトラスト」と呼ばれることもある）。こうした傾向を踏まえ、例えば、振舞検知型マルウェア対策製品（EDR[19] を含む）や端末ログイン時の多要素認証の仕組みといった対策の導入に加え、SOC による監視機能や ID・アクセス権管理、脆弱性対策[20]の高度化を計画的に推進していくことが期待される。

こうした状況を踏まえ、本取り組みは、環境変化を踏まえた設問の見直しを行いながら、2023 年度以降も継続的に実施していくことを想定している。

日本銀行および金融庁としては、地域金融機関がサイバーセキュリティ管理態勢の更なる強化に向けた取り組みを進めていくうえで、CSSA が活用されることを期待するとともに、考査や検査、モニタリング、各種セミナー等を通じて、そうした取り組みを後押ししていく方針である。

---

[19] Endpoint Detection and Response の略。端末やサーバの動作を監視することで不審な挙動（振舞い）を検知し、迅速な対応を支援する仕組み。

[20] システムの脆弱性や保守サービスの締結状況を把握したうえで、最新のパッチを適用する等の活動については「Cyber hygiene（サイバーハイジーン：サイバー空間の衛生管理）」と呼ばれることもある。