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（2023 年度）

日本銀行金融機構局
金融庁総合政策局
2024 年 4 月

【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、2023 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

わが国金融機関においては、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が重要な課題となっている。日本銀行および金融庁は、2022 年度に続き、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、サイバーセキュリティセルフアセスメントを実施した。

今次集計結果から、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、技術・組織両面での対策の導入により、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着実に進めているが、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については、なお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. はじめに

わが国の金融機関では、デジタル技術を活用した新規ビジネスの開拓や FinTech 企業等の異業種との連携を通じた対顧客サービスの拡充のほか、クラウドサービスを活用した業務改革を推進する動きが進んでおり[1]、この結果、金融機関におけるサイバー空間との接続点が拡大している。一方、サイバー空間では、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引き続き高水準となっていることから、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。

今般、日本銀行および金融庁は、地域金融機関を対象に、2022 年度[2]に続き第二回目となる「サイバーセキュリティセルフアセスメント（以下、CSSA）」を実施した。対象先には、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求め、その集計結果を還元した[3]。各地域金融機関においては、自己評価に基づいて自組織の課題を認識したうえで、サイバーセキュリティ対策の一層の強化に自律的に取り組んでいくことを期待している。

CSSA の点検票は、国内外における主要なサイバーセキュリティリスク管理の枠組み[4]を参考に作成している。前回との比較では、国内外の金融機関を取り巻く環境変化も踏まえ、より先進的な対策に関する設問を追加したほか、地域金融機関の意向も踏まえたうえで、見直しを行っている。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。

---

[1] クラウドサービスの利用状況については、「金融機関におけるクラウドサービスの利用状況と利用上の課題について －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、2024 年 1 月）を参照。

[2] 2022 年度の状況等については、「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）」（金融システムレポート別冊シリーズ、2023 年 4 月）を参照。

[3] 対象先は、地域銀行 99 先、信用金庫 254 先、信用組合 145 先（前回同様）。自己評価は 2023 年 7 月～8 月に実施。その後、同年 11 月に集計結果を還元。なお、第 2 回目となる 2023 年度は、地域金融機関のほか、保険・証券といった他の金融業態に対しても実施（金融庁ホームページ参照）。

[4] 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」、FISC にて実施した「令和 5 年度 金融機関アンケート」などを参考にしている。

今回の点検票における主な論点は、以下のとおりである（図表 1、点検票は別紙参照）。

図表 1 点検票の主要項目

大項目	中項目	設問数	論点
ガバナンス	サイバーセキュリティに関する経営層の関与	5	サイバーセキュリティに関する経営方針、経営計画、経営層への定例報告、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	7	サイバー攻撃の把握、情報収集、リスク評価、参考としているガイドライン、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
	サイバーセキュリティ人材の確保・育成	3	サイバーセキュリティ人材について、機能別の確保状況、確保の取り組み、育成の取り組み
識別	デジタル技術の評価	1	デジタル技術の導入に伴うサイバーセキュリティ上の脅威の認識と対策状況
	資産管理	4	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、管理簿で管理している情報など
防御	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
	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
	不正送金・フィッシングの脅威への対応	1	不正送金、フィッシング攻撃への対策の実施状況
	ゼロトラスト化	1	ゼロトラスト・アーキテクチャの導入状況
	システムの脆弱性に関する管理・対応	6	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、パッチ適用の判断基準など
	サイバー攻撃に関する技術的な対策	5	端末、境界、Webサイト・インターネットバンキングシステム、モバイルアプリにおける技術的な対策、先進的対策の導入状況
検知	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
	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
対応・復旧	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
サードパーティ関連	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	55	うちFISCアンケートとの共通設問5問を含む

（注）前回から追加した論点には下線を付している。

II. CSSA の集計結果概要

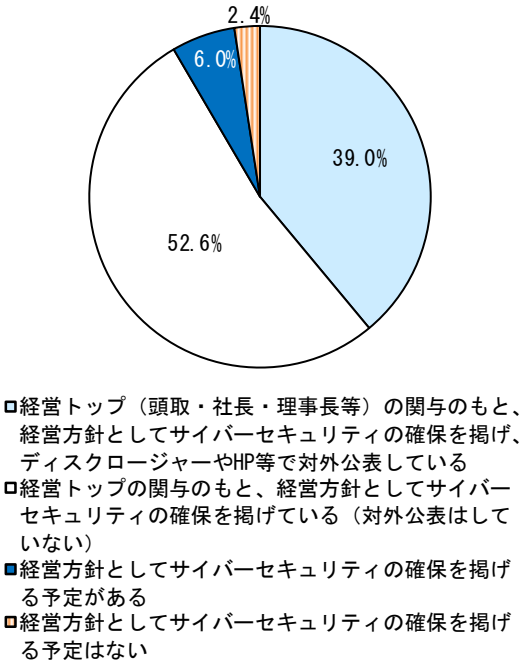
以下では、自己評価の集計結果に基づき、地域金融機関全体としてのサイバーセキュリティ管理態勢の概要と、今後の更なる態勢強化に向けたポイントを紹介する。なお、自己評価結果には、地域金融機関のセキュリティに関する技術的な情報が多く含まれることから、本レポートでは集計結果の開示にあたっては、地域金融機関のセキュリティ確保にも配慮している。

1. 経営層の関与

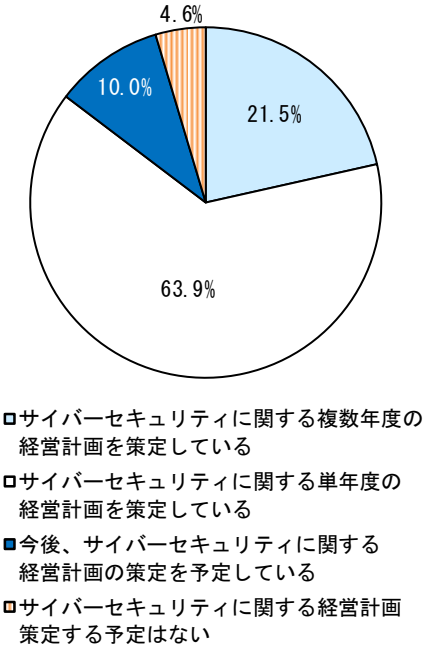
経営方針・経営計画の策定、統括責任者の役割

地域金融機関において、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り、自組織のサイバーリスクを踏まえた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、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の策定状況をみると、殆どの先が、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ているが、経営方針を定めていない先が 8%程度みられた（図表 2）。また、サイバーセキュリティに関する経営計画については、15%程度の先がこれを策定していなかった（図表 3）。経営方針を定めたうえで、具体的な計画を策定して取り組むことが重要である。

図表 2 サイバーセキュリティの経営方針

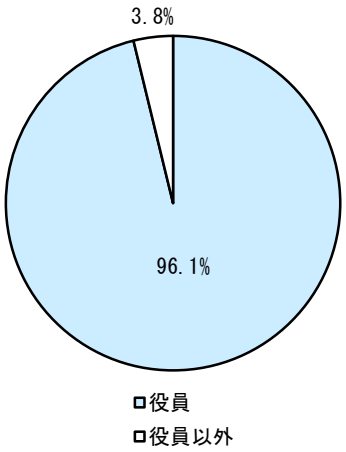


図表 3 サイバーセキュリティの経営計画

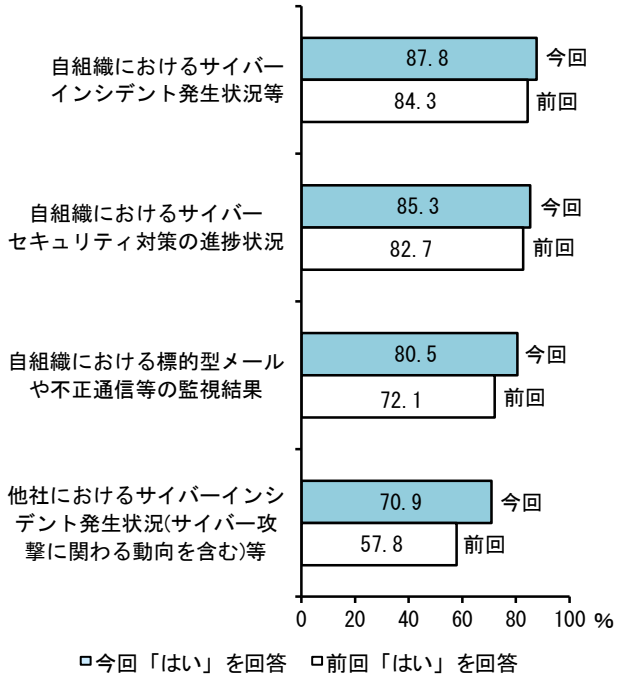


自組織のサイバーセキュリティを統括する責任者についてみると、殆どの先が役員となっていた（図表 4）。次に、サイバーセキュリティを統括する責任者に定例報告している内容についてみると、自組織におけるサイバーインシデントの発生状況やセキュリティ対策の進捗状況が高くなっていた。また、他社におけるサイバーインシデント事例の報告については、前回比改善し、7 割強の先が実施していたが、自組織にかかる報告と比べて実施した割合が低い（図表 5）。経営層に対しては、他社事例を含め、最近の脅威動向に関する情報を広く報告し、自組織の対策状況の点検に繋げていくことが重要である。

図表 4 サイバーセキュリティの統括責任者



図表 5 サイバーセキュリティに関し、
統括責任者に定例報告している内容

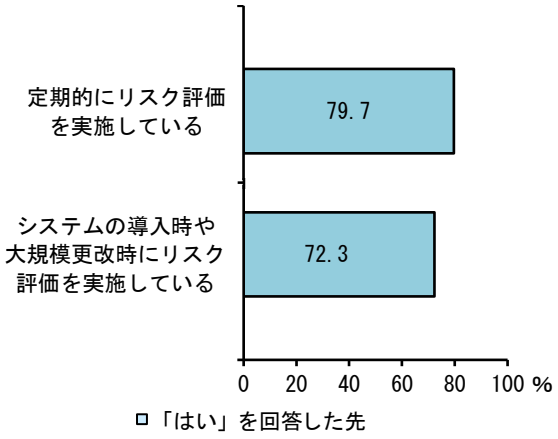


リスク管理と経営層の関与

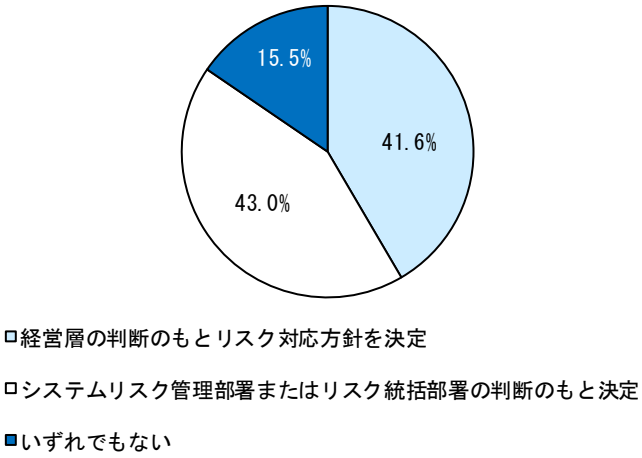
自組織が利用する重要なシステム[5]については、経営層が主導してサイバーセキュリティに関するリスク管理を行うことが重要である。リスク評価の実施頻度をみると、定期的に実施している先が 8 割弱、システムの導入時や大規模更改時に実施している先が 7 割強となっていた（図表 6）。他方、リスク評価を踏まえた、対応方針（低減、回避、移転、受容）や優先順位の決定についてみると、経営層の判断のもとで決定している先は 4 割強にとどまった（図表 7）。

[5] 今回の CSSA における「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 6 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頻度



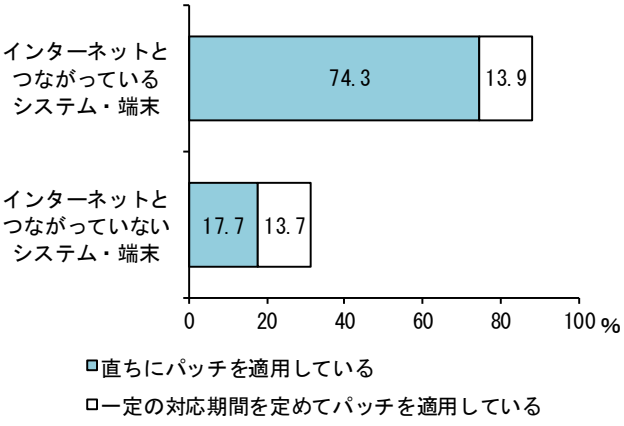
図表 7 リスク評価を踏まえた対応方針の決定者



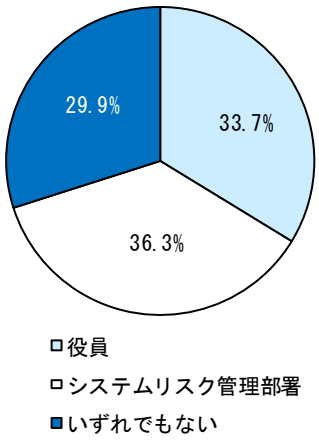
深刻な脆弱性が判明した場合、速やかにセキュリティパッチ（脆弱性修正プログラム）を適用することが大原則であるが、パッチを適用できない事情があるときは、経営層の承認のもと、リスク受容を決定することがある。深刻な脆弱性が判明した場合のパッチの適用方針をみると、インターネットと接続しているシステムでは、直ちにまたは一定の対応期間内で適用している先が 9 割弱となった一方、インターネット接続していないシステムでは、3 割強にとどまった（図表 8）。また、深刻な脆弱性に対して、セキュリティパッチを適用しないことの判断に役員が関与している先は 3 割強にとどまった（図表 9）。

最近のサイバーインシデントでは、関連会社や外部委託先の VPN 機器等の脆弱性を起因とし、自組織とインターネットで接続しない閉域網を経由したランサムウェア攻撃の被害を受けた事例がみられており、自組織がインターネットとつながっていないからといってリスクが低いとは言い切れない状況となっている。セキュリティパッチの迅速な適用を見送る場合、経営層の承認のもと、リスク受容を決定することが求められる。

図表 8 深刻な脆弱性が判明した場合のパッチの適用方針



図表 9 深刻な脆弱性に対してパッチを適用しない場合の承認者

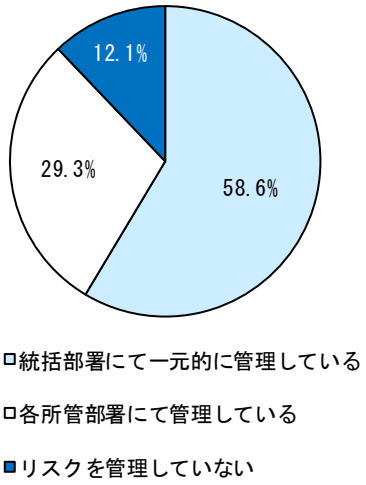


サードパーティリスクへの取り組み

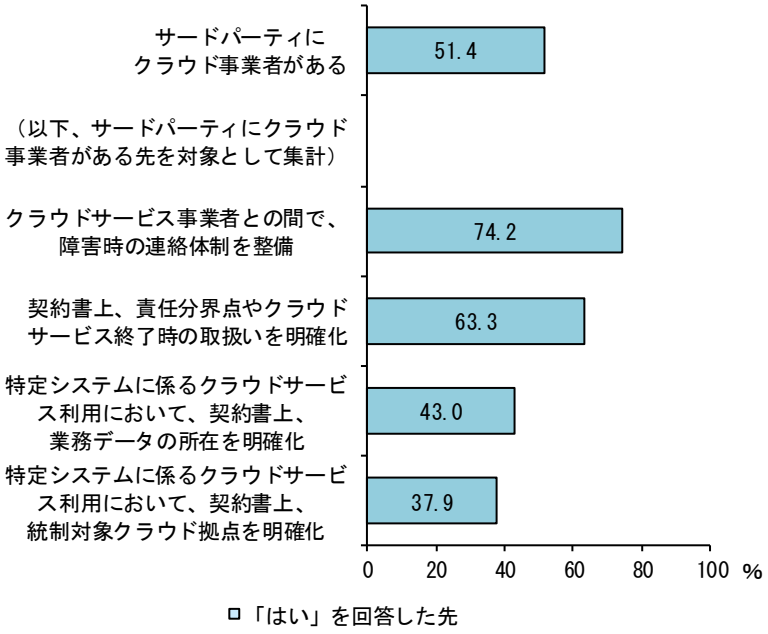
近年、デジタルビジネスを支えるサプライチェーンが広範かつ複雑化するなかで、サードパーティを適切に管理することの重要性が高まっている。管理の目線をそろえる観点からは組織横断的に対応することが望ましいが、重要なサードパーティ[6]のリスク管理状況をみると、統括部署にて一元的に管理している先は 6 割弱にとどまったほか、リスクを管理していない先も 1 割強みられた（図表 10）。

また、サードパーティが提供するサービスのうちクラウドサービスについては、半数以上の先がこれを利用していた。次に、同サービスの利用先がクラウド事業者との間で定めている事項についてみると、障害時の連絡体制、責任分界点やサービス終了時の取扱いについては、6～7 割の先がこれを定めていた。一方、業務データの所在や統制対象クラウド拠点を明確化している先は 3～4 割にとどまった（図表 11）。クラウド事業者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、重要な業務領域でクラウドを利用するのであれば、重要事項の内容を相手先と十分に確認し、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。

図表 10 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 11 クラウド事業者と契約等で定めている事項

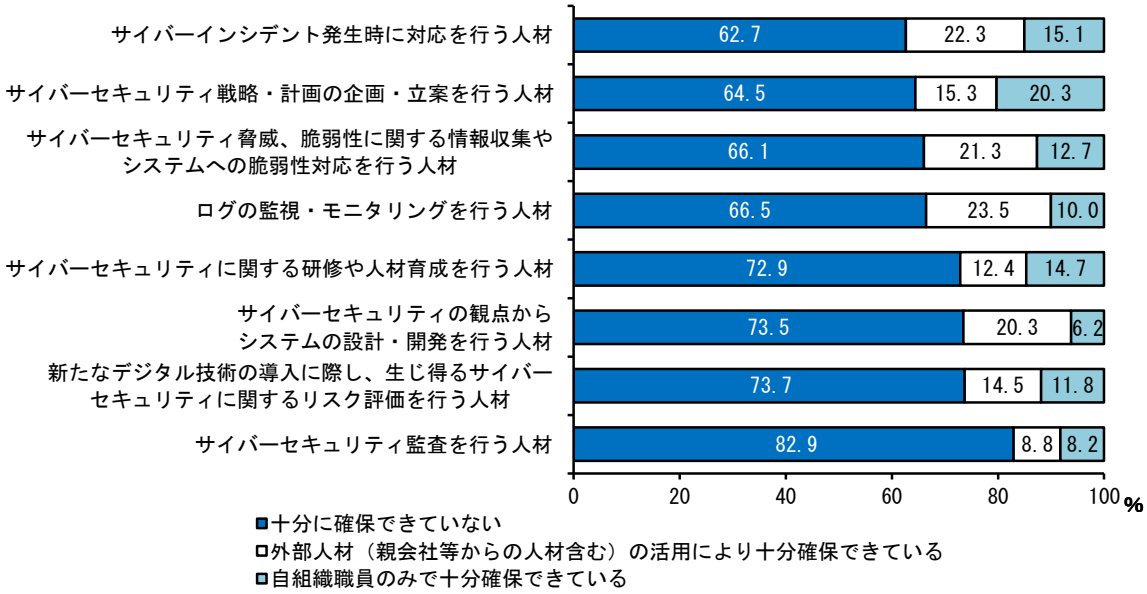


[6] 今回の CSSA における「重要なサードパーティ」とは、「自組織として業務運営上重要と認識しているサードパーティ」と定義。なお、「サードパーティ」とは、「自組織がサービスを提供するために、業務上の関係や契約等を有する他の組織」と定義（例：システム子会社、ベンダー等の外部委託先、クラウド等のサービス提供事業者、資金移動業者等の業務提携先など）。

サイバーセキュリティ人材の確保

サイバーセキュリティ人材の確保状況について、機能別に踏み込んで確認したところ、インシデント発生時の対応や戦略等の企画・立案といった自組織にとって重要な機能を優先しつつ、少ない自組織職員を外部人材で補完するかたちでの確保を図っている様子が窺われた。一方で、いずれの機能でも、人材が十分に確保できていないとの回答が大半を占めており、全体的に不足している状況となっていた（図表 12）。

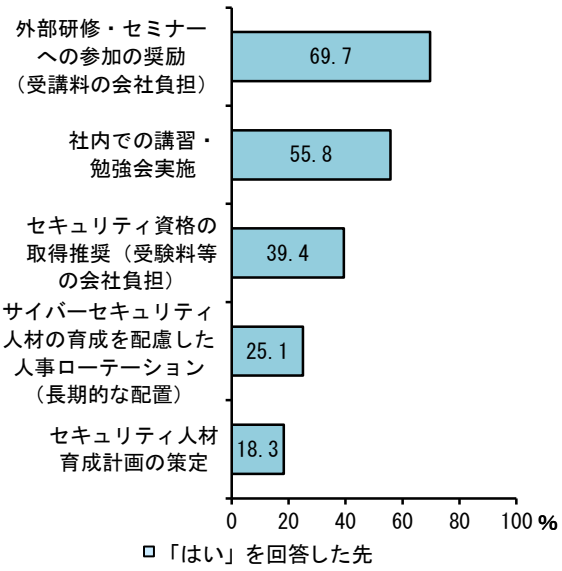
図表 12　機能別にみたサイバーセキュリティ人材の確保状況



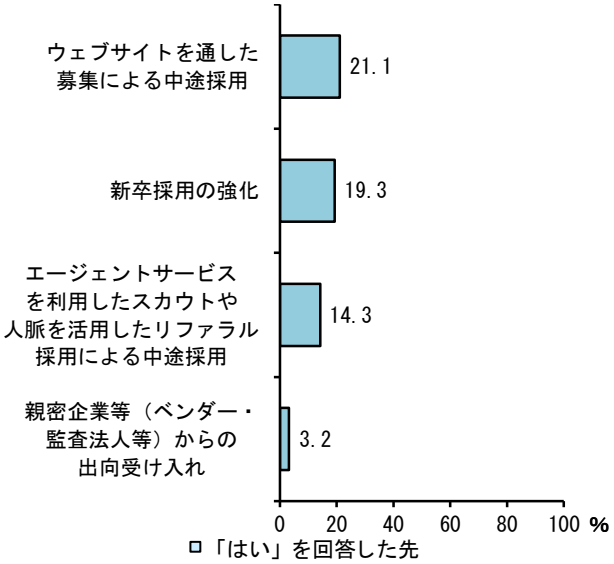
サイバーセキュリティの担い手確保に向けて、自組織における人材育成の取組状況をみると、外部研修・セミナー等への参加や社内での講習・勉強会の実施など即効性を意識して取り組む先が半数以上となっていた。他方、サイバーセキュリティ人材の育成に配慮した長期的な人事ローテーションやセキュリティ人材育成計画の策定など、中長期的に取り組む先は限定的となっていた（図表 13）。今後も、サイバーセキュリティ人材の不足が恒常化する可能性を念頭に置きつつ、中長期的な視点に立って、自組織内でのサイバーセキュリティ人材の底上げ・確保に取り組むことが重要である。この点、例えば、他の金融機関との間でサイバーセキュリティ対策に関する情報や知見の共有のほか、技術的対策に関する踏み込んだ情報連携や関連する業務遂行面での連携といった、業界横断的に連携・協力して実践力を高めていくような「共助」の視点に立った取り組みが期待される。

また、外部からのサイバーセキュリティ人材採用の取組状況についてみると、全体として、低調となっていた（図表 14）。この背景には、スキルのある専門人材が大都市圏に偏在しており、地方での採用が容易でないという事情が影響している可能性がある。

図表 13 人材育成の取り組み



図表 14 人材採用の取り組み



2. リスクへの対策

ゼロトラストの考え方

従来、外部からの侵入をいかに防ぐか、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、境界防御型の対策に限界があるとの意識が広がっている。最近では「未知のマルウェアや脆弱性による自組織への侵入可能性は完全に排除できない」との前提のもと、自組織のインターネットに接続していない内部環境も含めて、アクセスの信頼性を常に検証することで企業の情報資産を保護すること（いわゆる「ゼロトラスト」の考え方に基づいた対策を講ずること）が重要となっている。

こうしたサイバーセキュリティ対策の変化を踏まえ、例えば、端末やシステムへのアクセス時における多要素認証の仕組みを導入するほか、内部に侵入された場合でも検知・対応が可能となるよう、振舞検知型マルウェア対策製品（EDR[7]を含む）の導入やセキュリティ関連の監視・分析等を行う組織（SOC[8]）の設置、脅威ベースのペネトレーションテスト[9]（TLPT）

---

[7] 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。

[8] 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。

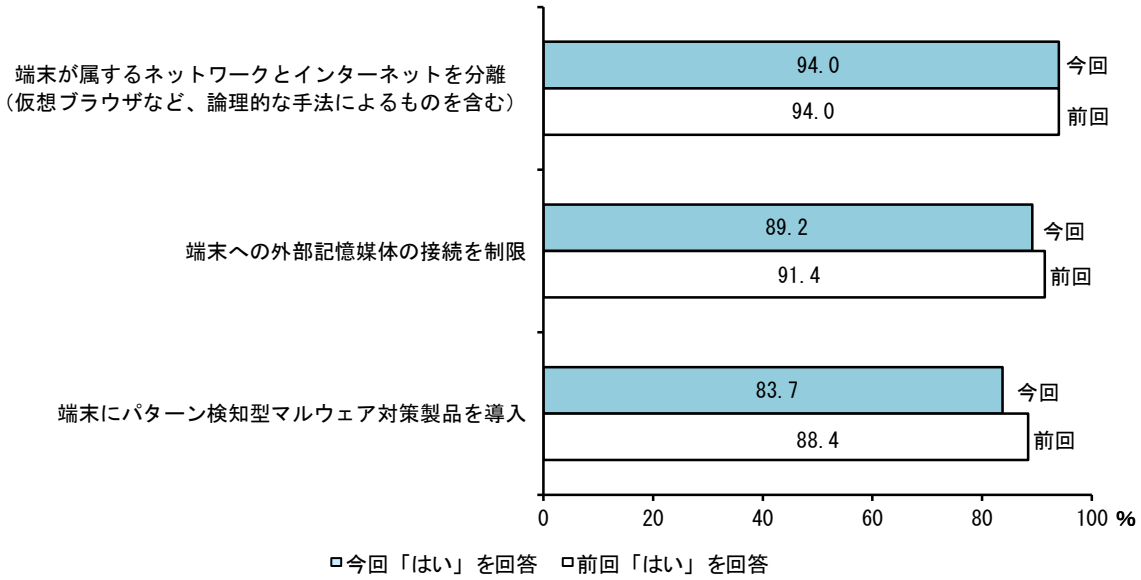
[9] 今回の CSSA における「ペネトレーションテスト」とは、「擬似的なマルウェアを利用したり、脆弱性･設定不備等を悪用したりするなど擬似的な攻撃を仕掛けることで、侵入･改ざんの可否や検知の可否、対応の迅速性・適切性を検証するテスト」と定義。また、「脅威ベースのペネトレーションテスト」とは、「自組織が抱えるリスクを個別具体的に分析したうえで、攻撃者が採用する戦術、手法を再現し疑似的な攻撃を仕掛けるこ

の実施、といった対策がより重要視されてきている。

OA 端末における対策

サイバー攻撃の侵入口となりやすい OA 端末[10]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は 8～9 割の先で実施されていた（図表 15）[11]。今後、デジタル化施策を一段と推進していく場合、多要素認証の仕組みや振舞検知型マルウェア対策製品（EDR 含む）の導入など、ゼロトラストの考え方を踏まえ、サイバーセキュリティ対策を強化していく必要がある（システムの脆弱性を悪用した攻撃への対策については、BOX1 参照）。

図表 15 導入している 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・分析等の態勢

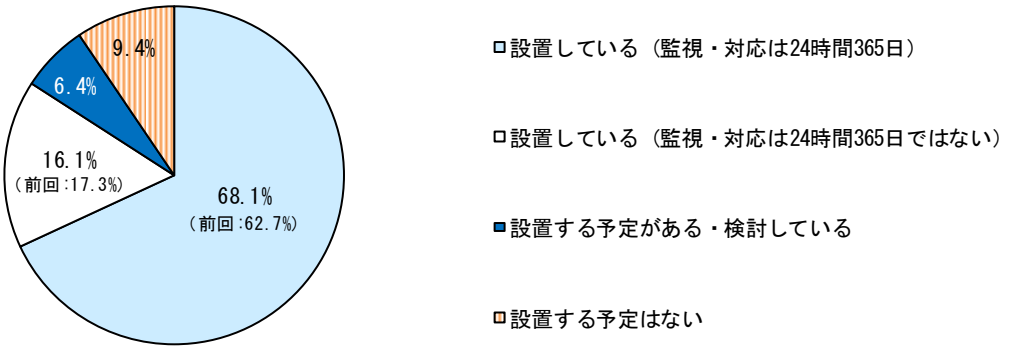
サイバーインシデントを早期に検知し、迅速に対応するためには、セキュリティ関連の監視・分析等を行う組織（SOC）を設置することが重要である。外部サービスの利用を含む SOC 等の設置状況をみると、これを設置している先は前回よりも増加して 8 割強となったが、2 割弱の先が常時監視（24 時間 365 日）ではなかった（図表 16）。今後、デジタル化施策により対顧客サービスの提供時間を拡大していくのであれば、提供時間に見合うかたちで常時監視（24 時間 365 日）による検知・対応の一層の迅速化が期待される。

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、より実践的なテスト」と定義。

[10] 今回の CSSA における「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。

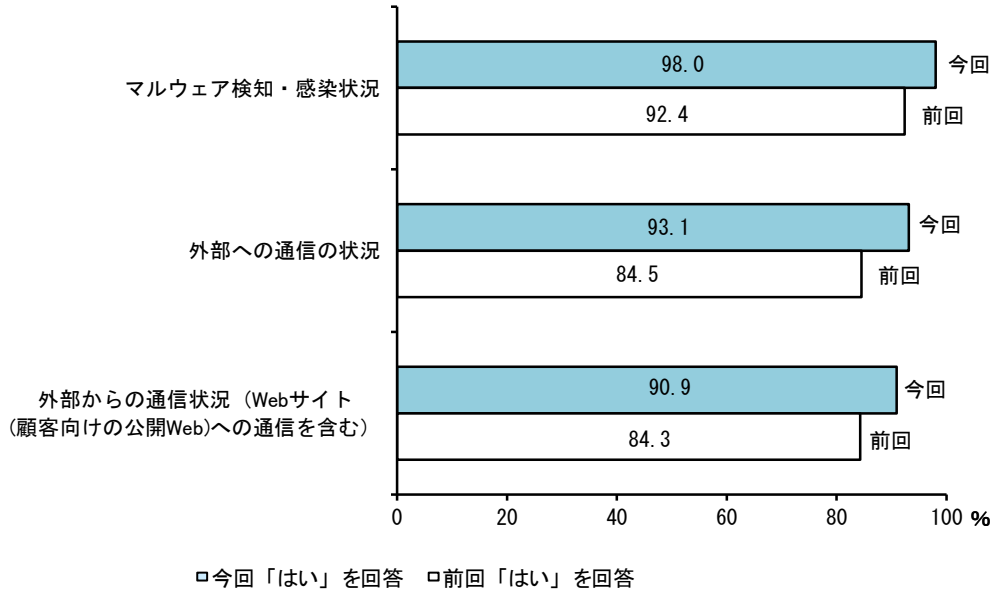
[11] 一部の対策は前回比で減少したが、その背景としては端末の VDI 化や EDR の導入などが進んでいることも可能性として考えられる。VDI（Virtual Desktop Infrastructure）： OA 端末のデスクトップ環境を仮想化して、サーバ上で稼働させる仕組み。

図表 16 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



SOC 等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など、境界防御を意識した監視・分析については、殆どの先が実施していた（図表 17）。今後も、デジタル化施策を一段と推進していく場合、インシデントの早期発見・早期対応（被害の拡大防止）の観点から、内部システムを含め監視する対象システム等を拡充するほか、自組織の内部に侵入されることや内部犯行（自組織の職員や外部委託先が不正な行為をすること）を想定し不審な挙動を監視するなど、モニタリングの更なる強化が期待される。

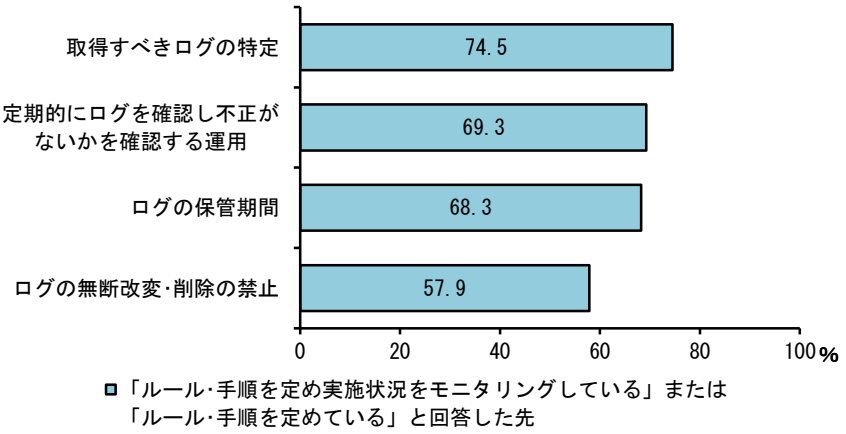
図表 17 SOC 等サイバーセキュリティの監視部署でのモニタリング対象



また、インシデントの検知やインシデントの影響範囲の調査、復旧対応の検討にあたってはシステムのログが必要不可欠であり、その正確性や網羅性を担保することが重要である。重要なシステムのログについて自組織内での取扱状況をみると、取得すべきログの特定、定期的なログの確認、ログの保管期間についてルールを定めている先は 7 割前後、ログの無断改変を禁止するルールを定めている先は 6 割弱にとどまった（図表 18）。内部犯行の抑止・

けん制も意識しつつ、重要なシステムのログの管理態勢を整備していくことが重要である。

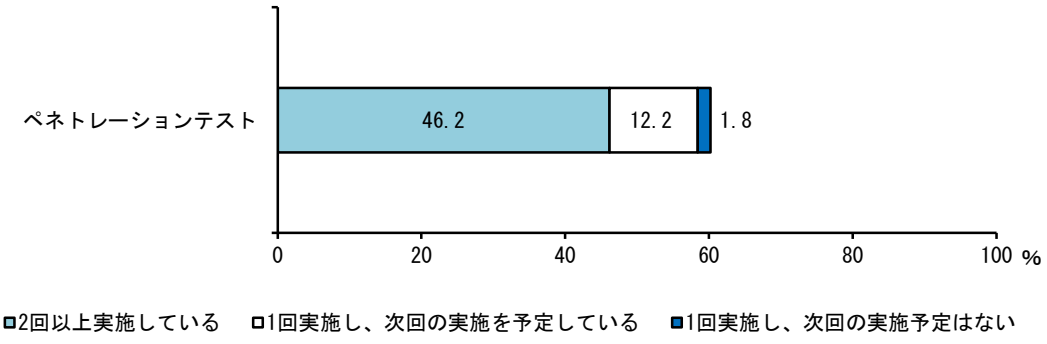
図表 18 重要なシステムのログ（監査証跡）について規定されている事項



検知・監視態勢の実効性の確認

自組織における検知・監視態勢を整備・確立したうえで、ペネトレーションテストや TLPT を実施し、第三者的な目線から検知・監視態勢の実効性の確認を行うことが重要である。テストの実施状況をみると、ペネトレーションテストを実施したことがある先は 6 割強となった（図表 19）。自組織の検知・監視態勢の実効性への課題を確認する観点から、ペネトレーションテスト等に取り組むことが期待される。

図表 19 ペネトレーションテストの実施状況



不正送金やフィッシング攻撃に対する対策

このほか、金融機関の顧客を狙った攻撃として、銀行を騙った電子メールや SMS を通じて、インターネットバンキング利用者を偽のログインサイトに誘導し、ID やパスワード等の情報を窃取する、いわゆるフィッシングによるものとみられる不正送金の被害が急増している[12]。被害が発生してから対策を講じるのではなく、あらかじめ対策を進める必要がある。利用者に対する注意喚起のみならず、金融機関自身において、ログイン時・取引時の多要素認証の導入や、利用者に対するインターネットバンキングの利用状況の通知、フィッシングサイトの検知とテイクダウン手順の整備、送信ドメイン認証（SPF、DKIM、DMARC）[13]の導入などを計画的に進めることが重要である。

3. 有事への備え

被害拡大防止のための対応手順の整備

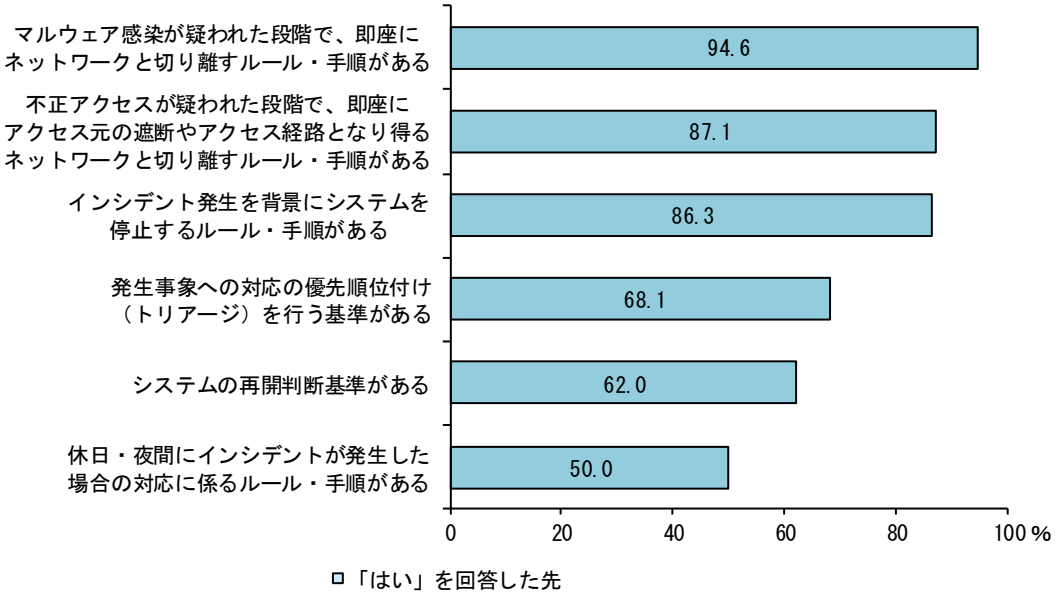
サイバーインシデントが発生した場合、発生事象を正確に把握したうえで、被害拡大防止のための対応を行いつつ、迅速な業務復旧を図ることが重要である。被害拡大防止のための対応手順の整備状況をみると、初動に関するルール・手順は大半の先が整備しているが、対応の優先順位付け（トリアージ）やシステムの再開判断基準、夜間・休日の対応手順については、これを整備している先が 5～7 割となった（図表 20）。インシデント発生時の状況を具体的に想定し、実践的なルール・手順の整備を図っていくことが重要である。

---

[12] 金融庁および警察庁連名で出された注意喚起「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）」（2023 年 12 月）を参照。

[13] SPF (Sender Policy Framework)： 電子メールの送信元ドメインが詐称されていないかを検査するための仕組み。DKIM (Domain Keys Identified Mail)：メールを送信する際に送信元が電子署名を行い、受信者がそれを検証することで、送信者のなりすましやメールの改ざんを検知できるようにする仕組み。DMARC (Domain-based Message Authentication, Reporting, and Conformance)：電子メールにおける送信ドメイン認証技術の一つであり、認証失敗時にどのようにメールを処理すればよいかを、送信者が受信者に対してポリシーと呼ばれるレコードを DNS 上で公開することで表明する仕組み。

図表 20 被害拡大防止のためのルール・手順の整備状況

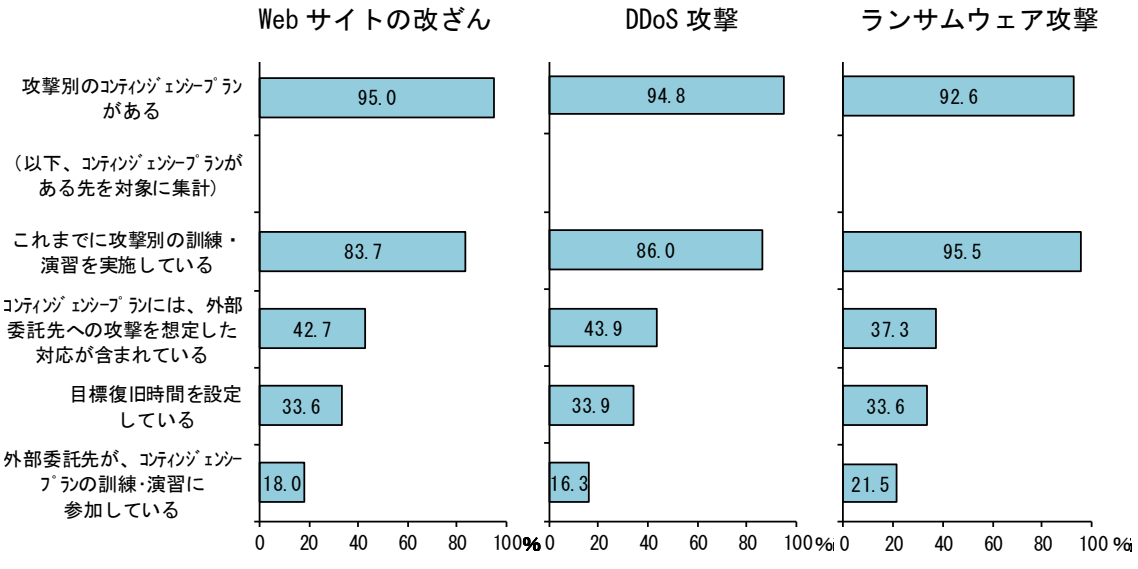


□「はい」を回答した先

コンティンジェンシープランの策定、訓練・演習の実施

コンティンジェンシープランの整備状況をみると、サイバー攻撃別に応じてプランを整備するとともに、訓練や演習を行っている先が大半となっていた（図表 21）。もっとも、外部委託先への攻撃を含めたコンティンジェンシープランの整備や訓練・演習への外部委託先の参加、目標復旧時間を設定している先は半数以下となった。外部委託先が攻撃を受け自組織に影響が及ぶ可能性への考慮や、自組織のシステム環境を踏まえた現実性のある目標復旧時間の設定など、実践的なコンティンジェンシープランを整備することが重要である。

図表 21 サイバー攻撃別のコンティンジェンシープランの有無および取組内容



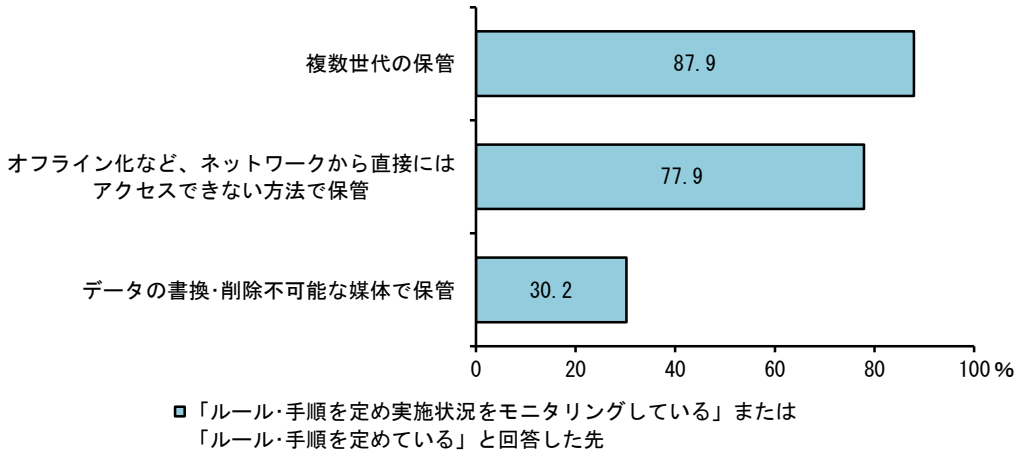
□「はい」を回答した先

ランサムウェア攻撃を想定したバックアップデータの保護

近年多く発生している「ランサムウェア攻撃」を受けた場合の対応としては、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、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事例がみられている（BOX2 参照）。

重要なシステムにおけるバックアップデータの破壊・改ざんを想定した対策状況をみると、複数世代の保管やネットワークから直接にはアクセスできない方法での保管を中心に、データの保護対策を講じている先が大半となった（図表 22）。ランサムウェア攻撃を受けた場合の業務復旧を早期に行う観点から、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である[14]。

図表 22 重要なシステムにおけるバックアップデータの破壊・改ざんを想定した対策

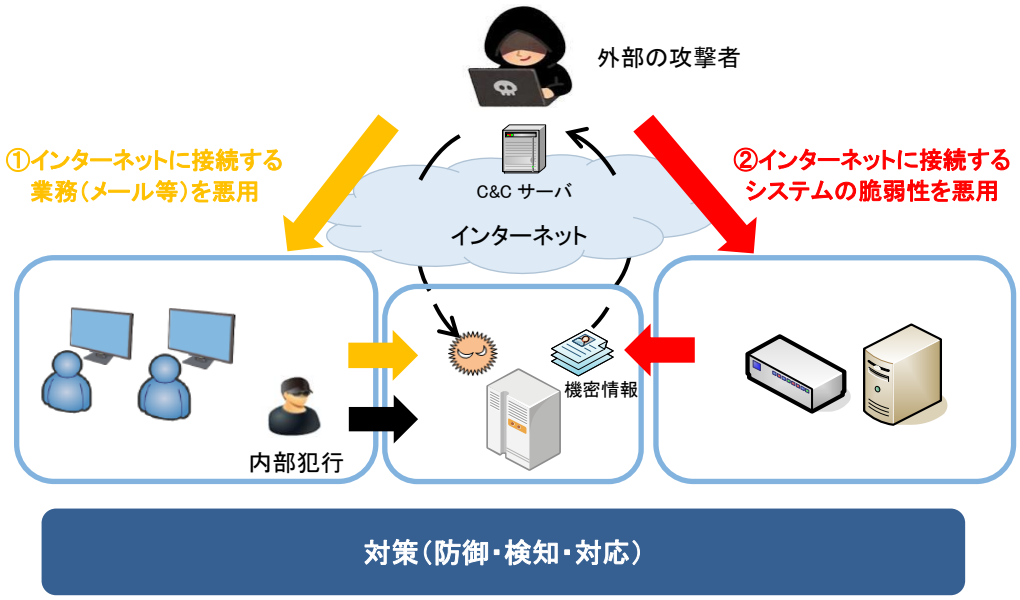


[14] バックアップデータが破壊・改ざんされないための対策を行うことの重要性については、「地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2022 年度）」（金融システムレポート別冊シリーズ、2023 年 4 月）の BOX3 を参照。

BOX1　脆弱性を悪用した攻撃への対策

攻撃者による外部からの主な侵入経路としては、①Web サイトへのアクセスやメールをはじめとした OA 端末の業務を標的とした攻撃のほか、②インターネットに接続するシステム（アプライアンス等の機器を含む）の脆弱性を悪用した攻撃がある（図表 B1-1）。ここでは後者の対策について整理する（OA 端末への攻撃対策については、本文（Ⅱ章 2 節の「OA 端末における対策」）を参照）。

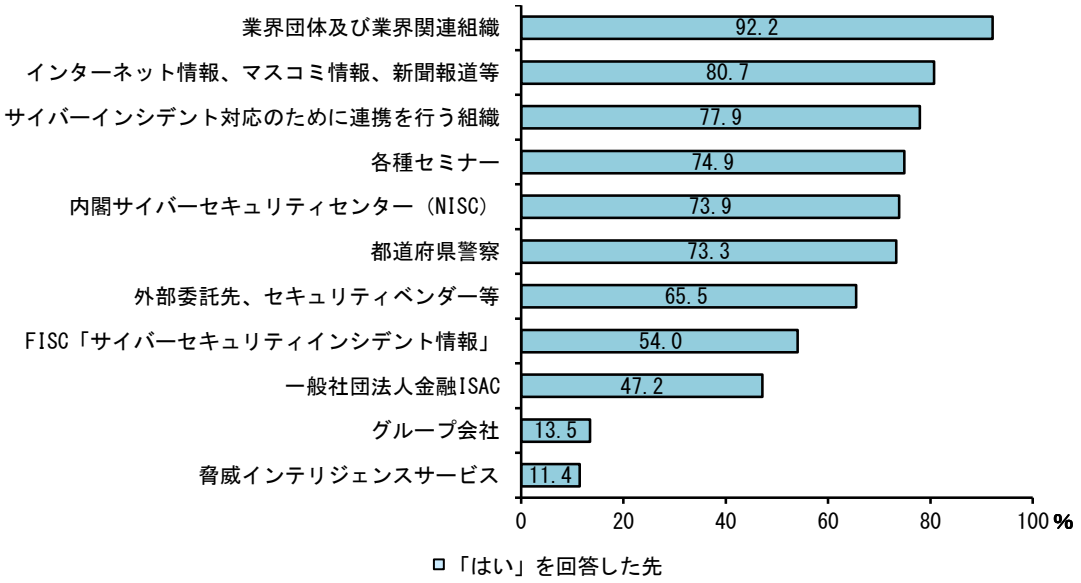
図表 B1-1 攻撃者の侵入経路



脆弱性を悪用した攻撃への対策としては、第一歩として、脆弱性に関する正確な情報を収集することが重要である。脆弱性を含めサイバーセキュリティに関する情報の収集状況をみると、多くの先では様々な情報収集源から情報を収集していることが確認できた（図表 B1-2）。このうち、業界団体および業界関連組織が最も高い割合となっていたが、この背景としては、協同組織金融機関では、共同利用しているシステム会社が活用されていると考えられるほか[15]、金融分野を含むわが国の重要インフラにおけるサイバーセキュリティの確保を支援する内閣サイバーセキュリティセンター（NISC）からの情報提供や、金融業界全体のサイバーセキュリティ関係の共助組織である一般社団法人金融 ISAC を通じた情報連携が有効に機能していると考えられる。外部環境の変化が進むなかで、こうした共助組織が業界全体のハブとなって、脆弱性をはじめとするリスク情報を円滑に連携することは重要であり、今後とも業界全体としての取り組み強化が期待される。

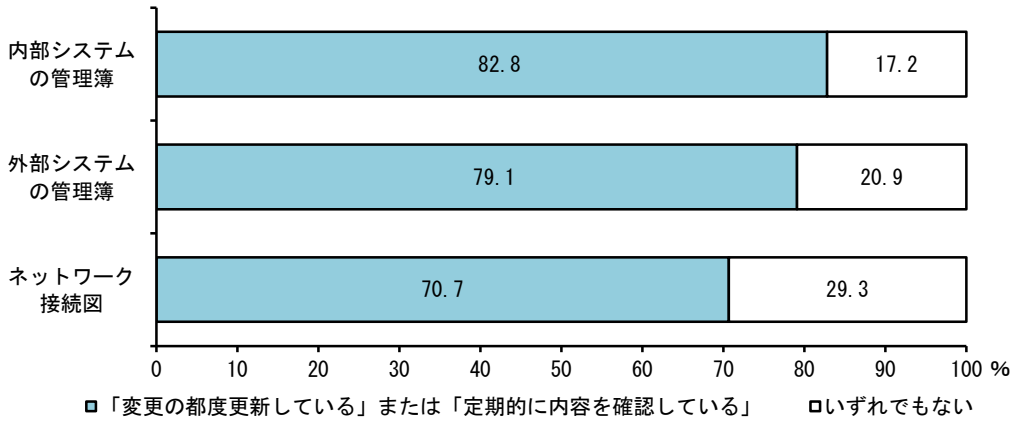
[15] 例えば、信用金庫については信金情報システムセンター（SSC）を、信用組合については信組情報サービス（SKC）を利用していることが考えられる。

図表 B1-2 サイバーセキュリティに関する情報収集源



脆弱性に関する情報を入手した際、当該情報が自組織にどの程度の影響を及ぼし得るかを迅速に確認し、必要に応じて対応を行うことが求められる。そのためには、インターネットに接続するシステムの特定をはじめ、OS やソフトウェアのバージョン等が当該脆弱性に該当しているか、パッチの提供等を受けられる保守サービスを締結しているか等を確認できるよう、システム資産の全体像や最新の状況が「見える化」されていることが重要である。システム資産の管理簿等の整備状況をみると、システム変更の都度更新している、または定期的に内容を確認している先が 7～8 割程度、そうした管理をしていない先はなお 2～3 割程度みられた（図表 B1-3）。システム資産や構成情報の適切な管理に取り組むことが重要である。

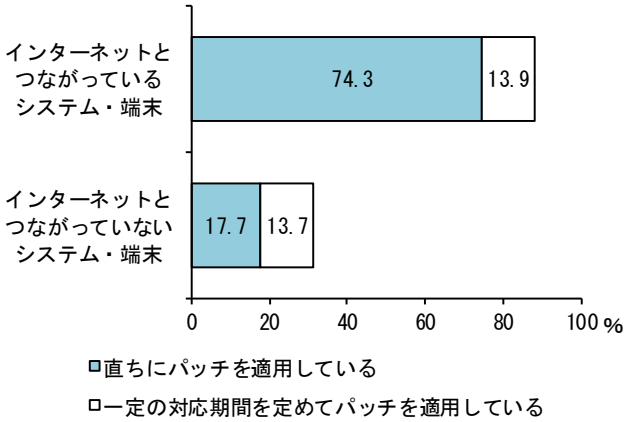
図表 B1-3 システムの管理簿等の整備状況



（注）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」、「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。

深刻な脆弱性が見つかった場合、速やかにセキュリティパッチ（脆弱性修正プログラム）を適用することが大原則である。本文（Ⅱ章 1 節の「リスク管理と経営層の関与」）で述べたとおり、現状、インターネットに接続しているシステムを優先的に対応する取扱いとなっている（図表 B1-4 <本文図表 8 を再掲>）。

図表 B1-4 深刻な脆弱性が判明した場合のパッチの適用方針

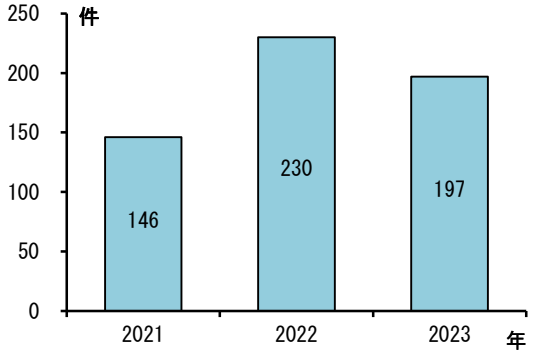


もっとも、最近のサイバーインシデントでは、例えば、VPN 機器等の脆弱性を起因とし、自組織とインターネットで接続しない閉域網を経由したランサムウェア攻撃の被害を受けた事例がみられており、「インターネットに接続していない内部システムの対応は劣後させても差し支えない」という、いわば「閉域網への過信」は禁物である。深刻な脆弱性が判明した場合、内部システムであっても速やかにセキュリティパッチを適用し、自組織が利用するシステム環境全体として、脆弱性というセキュリティホールを塞いでおく取り組みを強化することが重要である（この取り組みは、サイバー空間の衛生管理を意味することから、「サイバーハイジーン」と呼ばれることもある）。

BOX2　ランサムウェア攻撃の動向

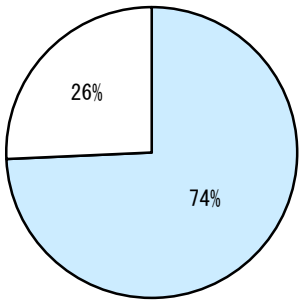
警察庁が発表[16]しているランサムウェア攻撃による被害報告件数をみると、ここ数年高水準となっている（図表 B2-1）。ランサムウェア攻撃は、システムのデータを暗号化し暗号解除の対価として金銭や暗号資産を要求するものであるが、最近の手口をみると、データの暗号化と窃取を同時に行い、「ファイルを復旧するための暗号鍵を渡さない」、かつ、「窃取した情報を漏えいする」と脅迫する「二重の脅迫」が過半となっている（図表 B2-2）。

図表 B2-1 企業等におけるランサムウェア被害



（資料）警察庁

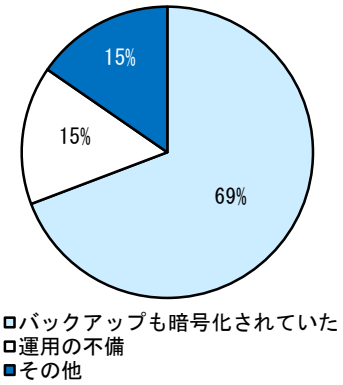
図表 B2-2 脅迫の手口



（注）2023 年の計数のうち、手口が確認できた 175 件の内訳
（資料）警察庁

また、あらかじめバックアップデータを取得していたものの、システムを復旧できなかった理由をみると、「バックアップも暗号化されていた」が 7 割弱となっている（図表 B2-3）。ランサムウェア攻撃では、バックアップデータも攻撃対象となっていることを認識し、バックアップデータが破壊・改ざん（暗号化）されないための対策を行うことが重要である。

図表 B2-3　被害企業等がバックアップから復元できなかった理由



（注）2023 年の計数のうち、バックアップから復元できなかった理由が判明した 104 件の内訳
（資料）警察庁

[16] 警察庁「令和５年におけるサイバー空間をめぐる脅威の情勢等について」（2024 年 3 月）を参照。

III. おわりに

本レポートでは、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、①経営層の関与、②リスクへの対策、③有事への備えの切り口から整理を行った。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、技術・組織両面での対策の導入による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着実に進めているが、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については、なお課題を抱えていることが確認できた。

もとより、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、サイバー攻撃の起点となり得るインターネットとの接続点（いわゆる「アタック・サーフェス」）が異なることから、サイバーセキュリティ確保のために求められる取り組みも一律ではない。ただ全体としてみれば、地域金融機関を含めわが国金融機関がデジタル技術の活用を指向しているなかで、サイバー攻撃の脅威が一層高まっている現状に鑑みると、ゼロトラストの考え方を踏まえ、今後と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。地域金融機関による自己評価に基づいて自組織の課題を認識し、自律的なサイバーセキュリティ対策の取り組み強化を促す本施策については、2024 年度以降も継続的に実施していくことを予定している。

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。