Financial System Report – Annex

【概要】
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

概要

- ✓ 目　　的：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を認識することで、自律的なサイバーセキュリティ対策の強化に取り組むよう促す。

- ✓ 実施内容：サイバーセキュリティ管理態勢の自己評価ツール（点検票）を整備。地域金融機関を対象に、自己評価を求め、その集計結果を還元。2022年度が初回。

- ✓ 実施方法：日本銀行および金融庁が共同で実施。

- ✓ 対　　象：地域金融機関498先（地域銀行99先、信用金庫254先、信用組合145先）

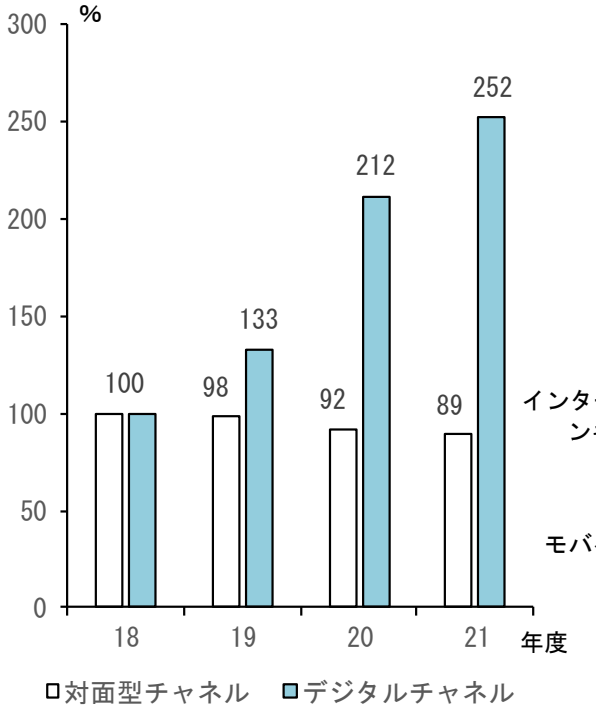
- ✓ 実施時期：自己評価期間は2022年7月～8月。11月に集計結果を還元。

わが国金融機関を取り巻く環境①

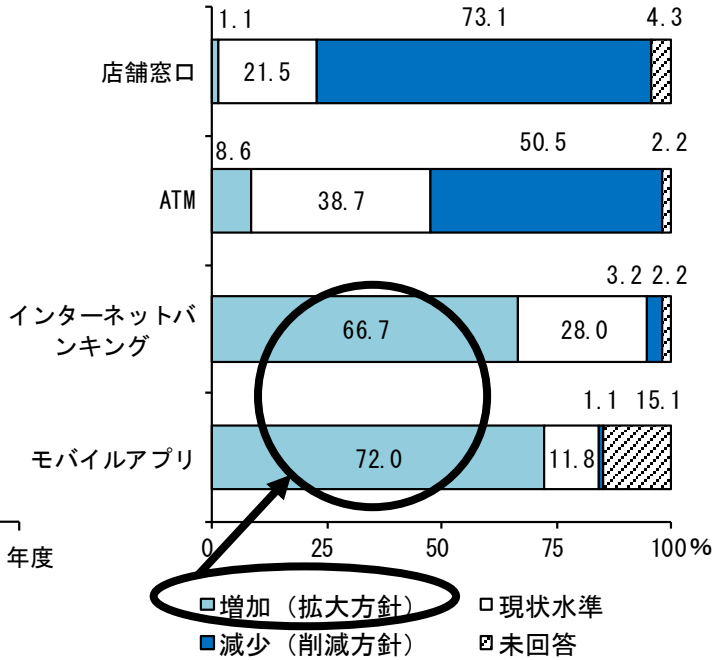
■ 対顧客チャネルにおけるデジタル化の進展（外部資料より）

✓ デジタルチャネルの事務量は、足もと、対面型チャネルの伸びを上回って増加。

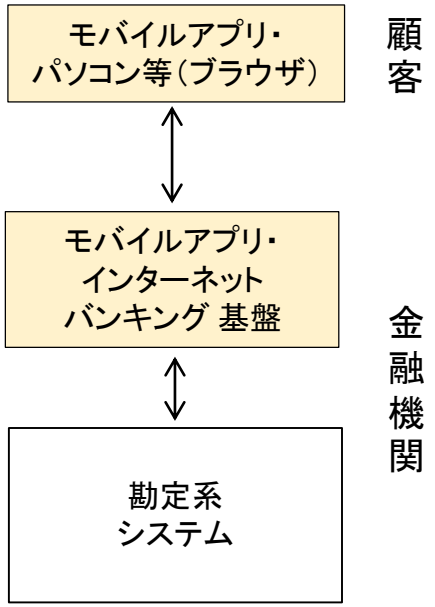
▽ 事務量の推移



▽ チャネル別事務量の見通し



（参考）デジタルチャネルのイメージ



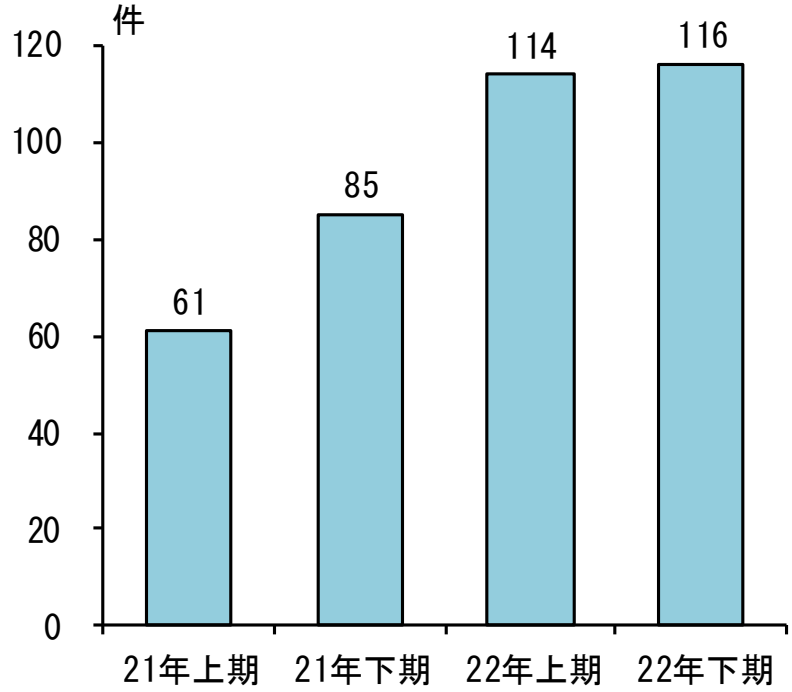
（資料）「事務量の推移」、「チャネル別事務量の見通し」は、日本銀行 金融システムレポート別冊「金融機関におけるモバイルアプリの提供状況と管理体制について —アンケート調査結果から—（2022年11月）」
https://www.boj.or.jp/research/brp/fsr/fsrb221115.htm

わが国金融機関を取り巻く環境②

■　金融機関を取り巻くサイバー脅威の動向（外部資料より）

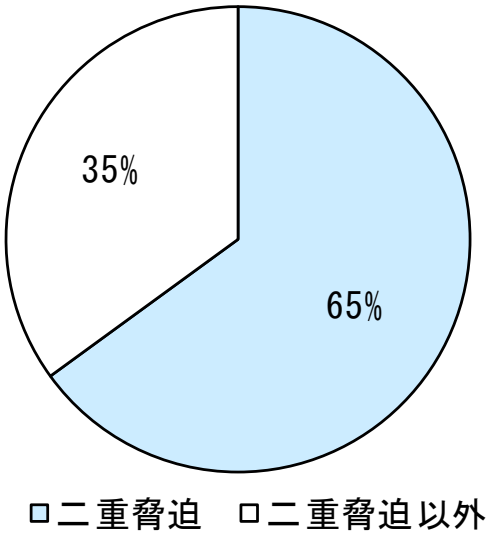
✓ ランサムウェアの被害件数は右肩上がり。その手口は巧妙化している。

▽　ランサムウェア被害件数



▽　ランサムウェア被害手口

（手口を確認できた被害：182件＜22年通期＞）



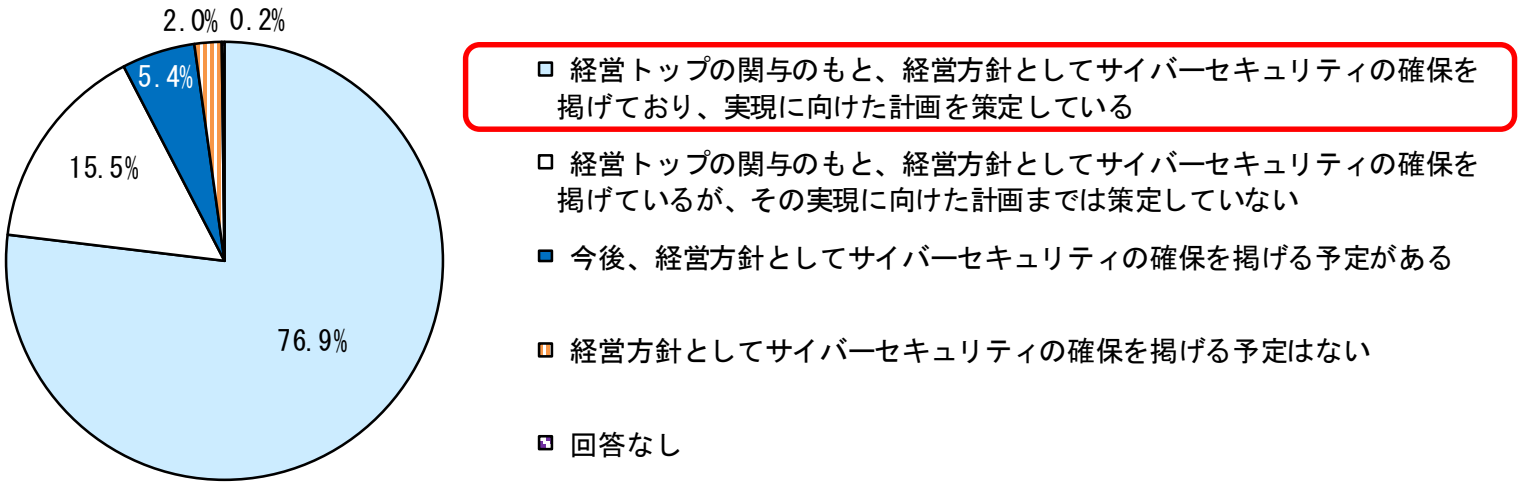
（資料）警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

集計結果の概要　1. 経営層の関与①

■　経営方針の策定とその実現に向けた態勢

✓ 経営トップの関与のもと、サイバーセキュリティの確保に向けた計画を策定している先は8割弱。

▽　サイバーセキュリティの経営方針・計画（本文図表2）

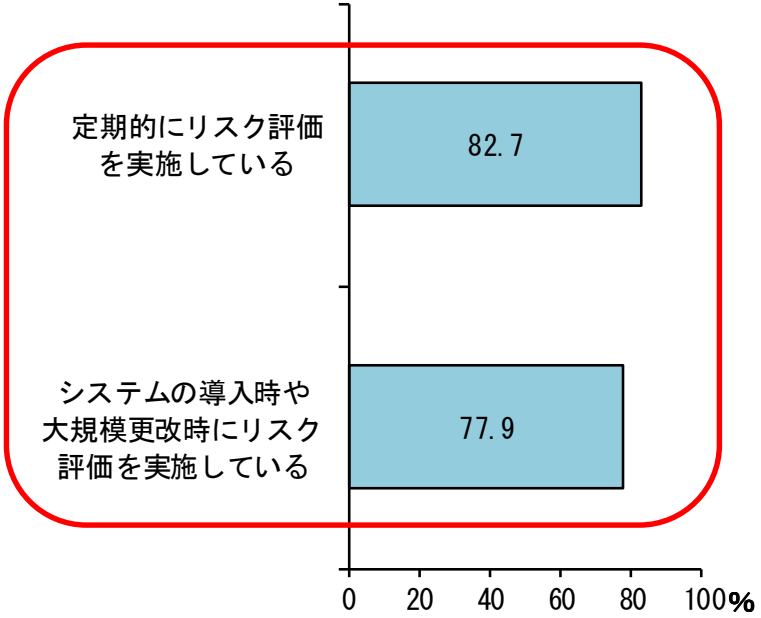


集計結果の概要　1. 経営層の関与②

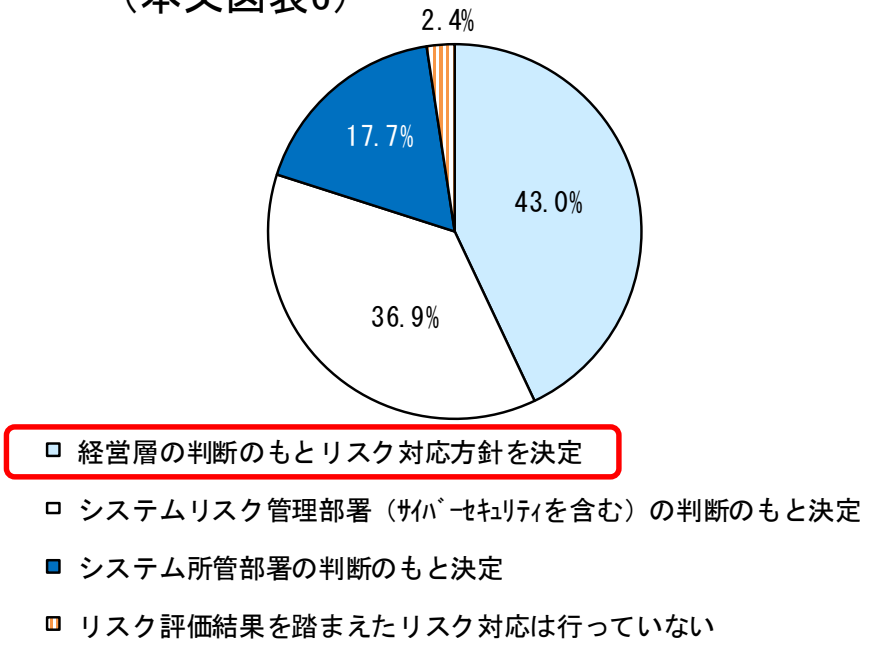
■ サイバーセキュリティに関するリスク評価の実施

- ✓ サイバーセキュリティのリスクを導入時や定期的に評価する先が多い。
- ✓ 経営層の判断のもとでリスク対応方針を決定している先は4割強。

▽ 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（本文図表5）



▽ リスク評価を踏まえた対応方針の決定者（本文図表6）



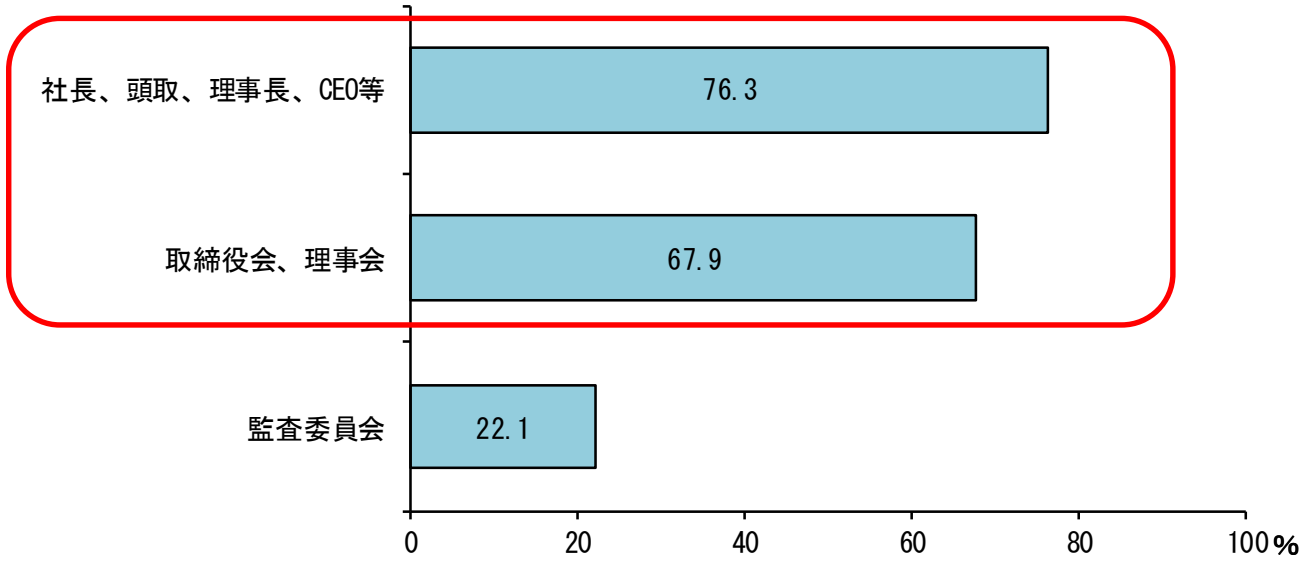
（注）今回のサイバーセキュリティセルフアセスメントでは、「重要なシステム」とは、「勘定系や顧客情報を扱うシステムなど自組織として業務運営上特に重要と認識しているシステム」と定義。

集計結果の概要　1. 経営層の関与③

■　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は、大半の先で経営層に報告されている。

▽　サイバーセキュリティに関する監査結果の報告先（本文図表7）

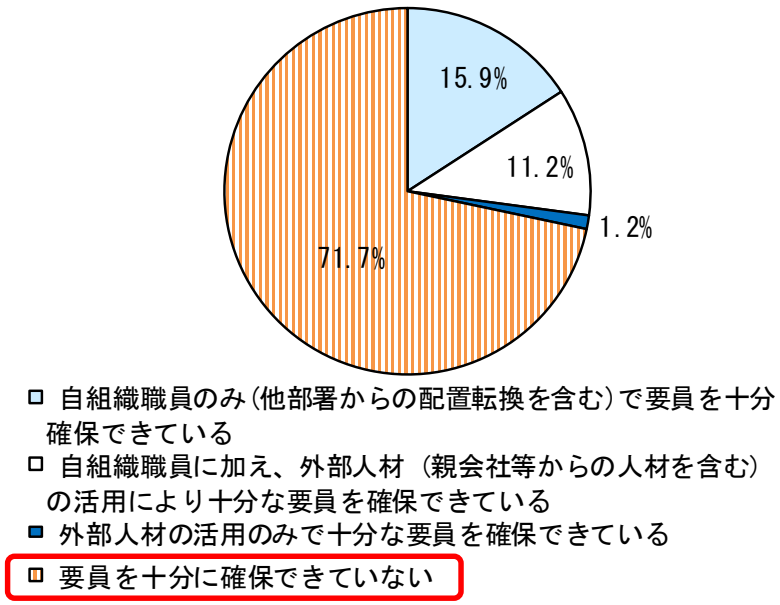


集計結果の概要　1. 経営層の関与④

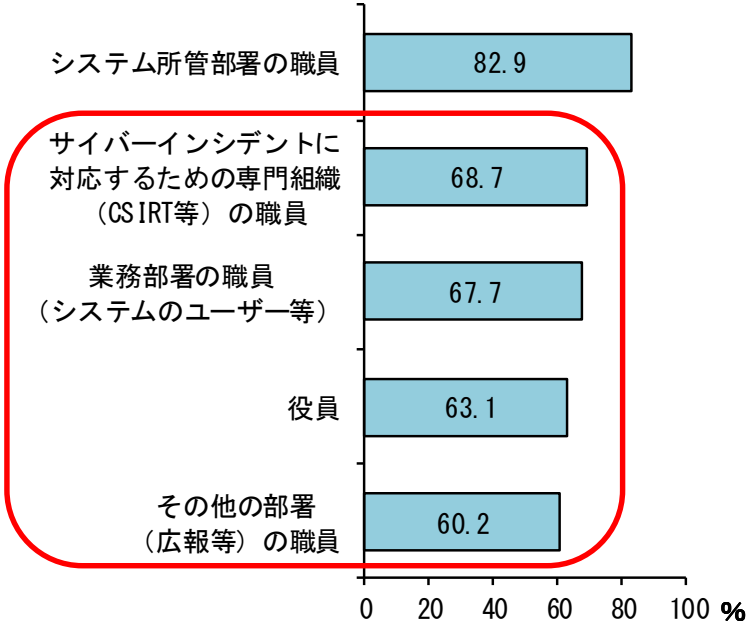
■ サイバーセキュリティ人材の確保の態勢

- ✓ 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を評価できる人材は、7割強の先が十分に確保できていない。
- ✓ サイバーセキュリティ人材の育成・強化策である e-learningの対象者は、システム所管部署の職員が相対的に高く、役員やその他の職員は6～7割。

▽ 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（本文図表8）



▽ e-learning（ビデオ、書面等含む）による啓発の対象者（本文図表9）

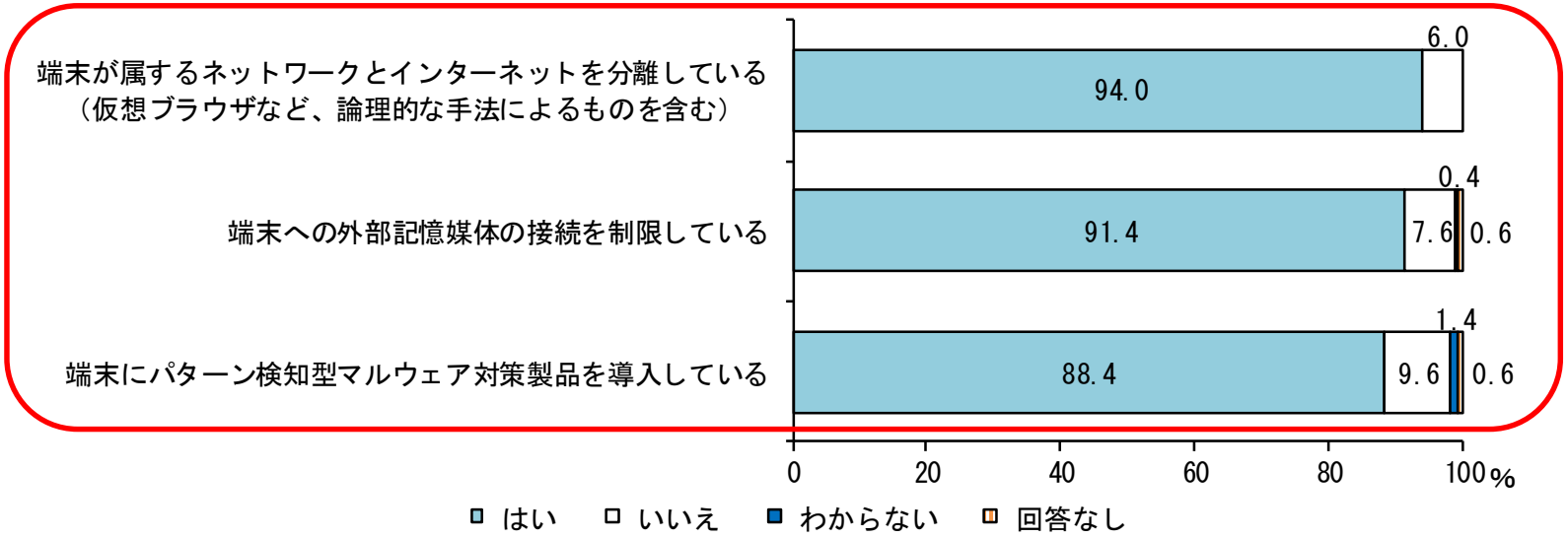


集計結果の概要　2. リスクへの構え①

■　サイバー攻撃への技術的対策

✓ OA端末のサイバー攻撃対策として、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が進んでいる。

▽　OA端末のサイバー攻撃対策（本文図表10）



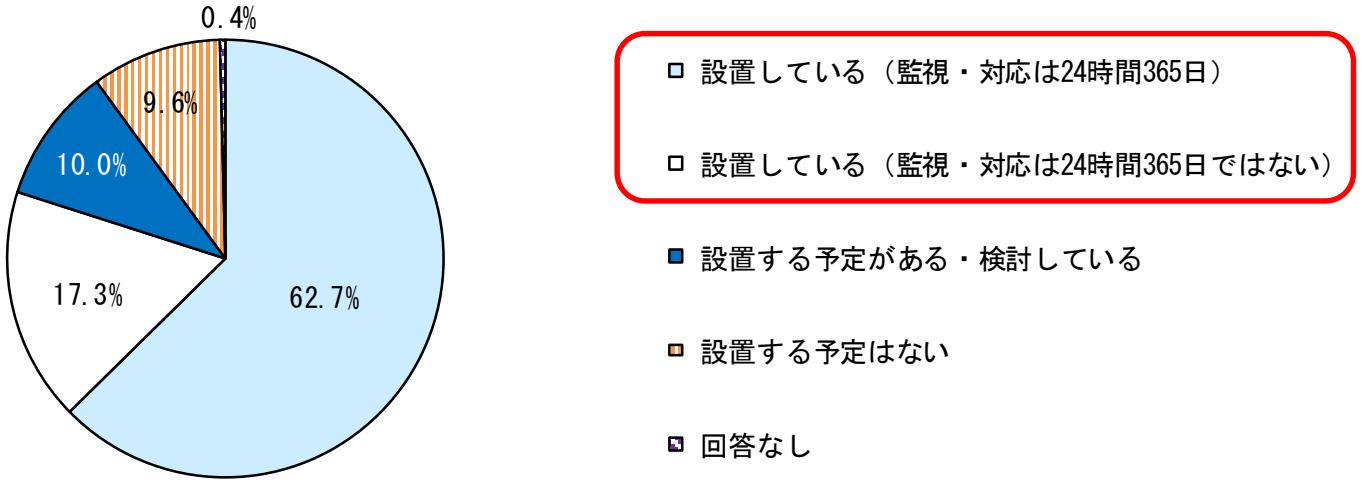
（注）今回のサイバーセキュリティセルフアセスメントでは、「OA端末」とは、「職員が文書作成等で標準的に用いる端末」と定義。

集計結果の概要　2. リスクへの構え②

■　サイバーインシデントの監視・分析態勢

✓ セキュリティ関連の監視・分析等を行う組織（SOC）は、約8割が設置している。

▽　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（本文図表11）



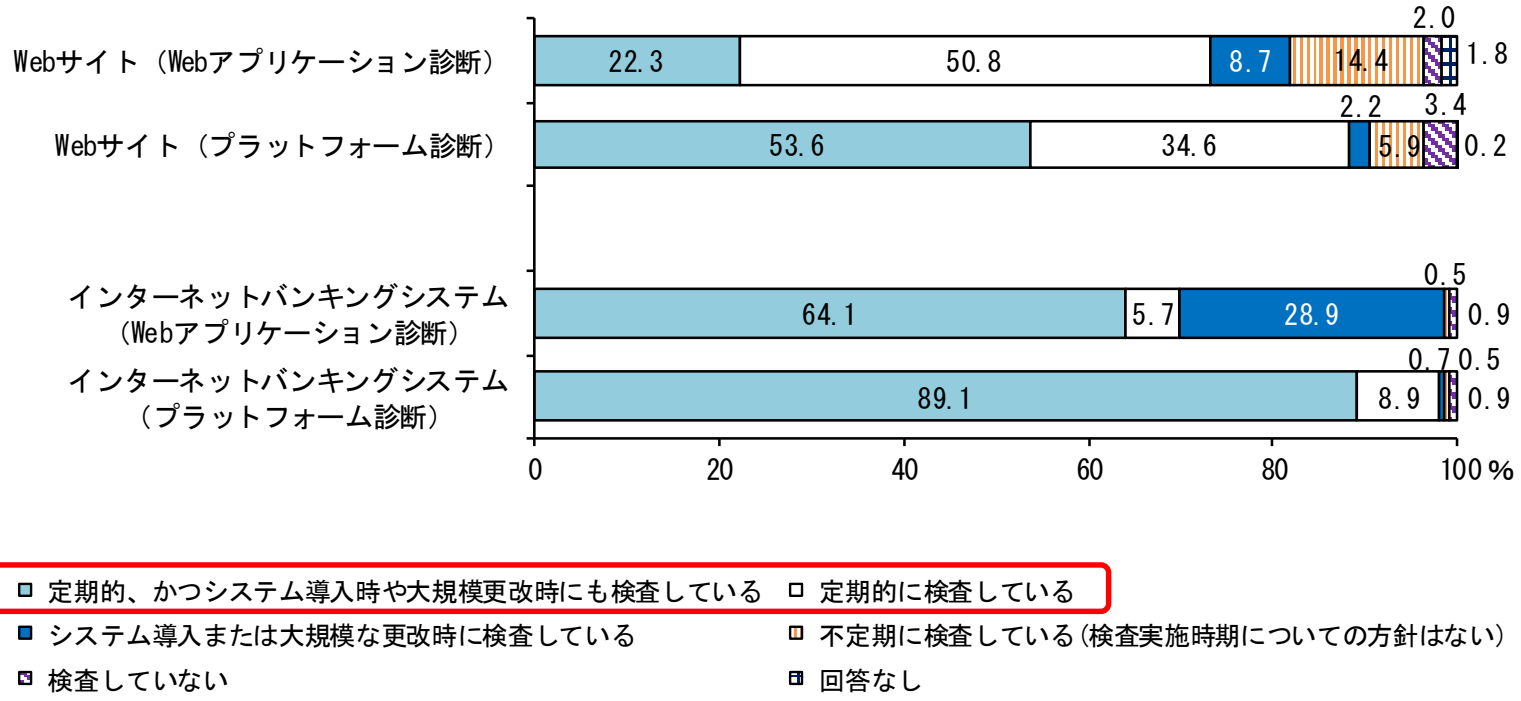
（注）SOCとは、Security Operation Centerの略。ネットワークやサーバ、ファイアウォール等の機器への攻撃状況など、セキュリティ関連の監視・分析等を行う組織。

集計結果の概要　2. リスクへの構え③

■　システム資産の管理、脆弱性への対応

✓ システムへの脆弱性診断は、多くの先が相応の頻度で実施している。

▽　脆弱性診断等の実施状況（本文図表14）



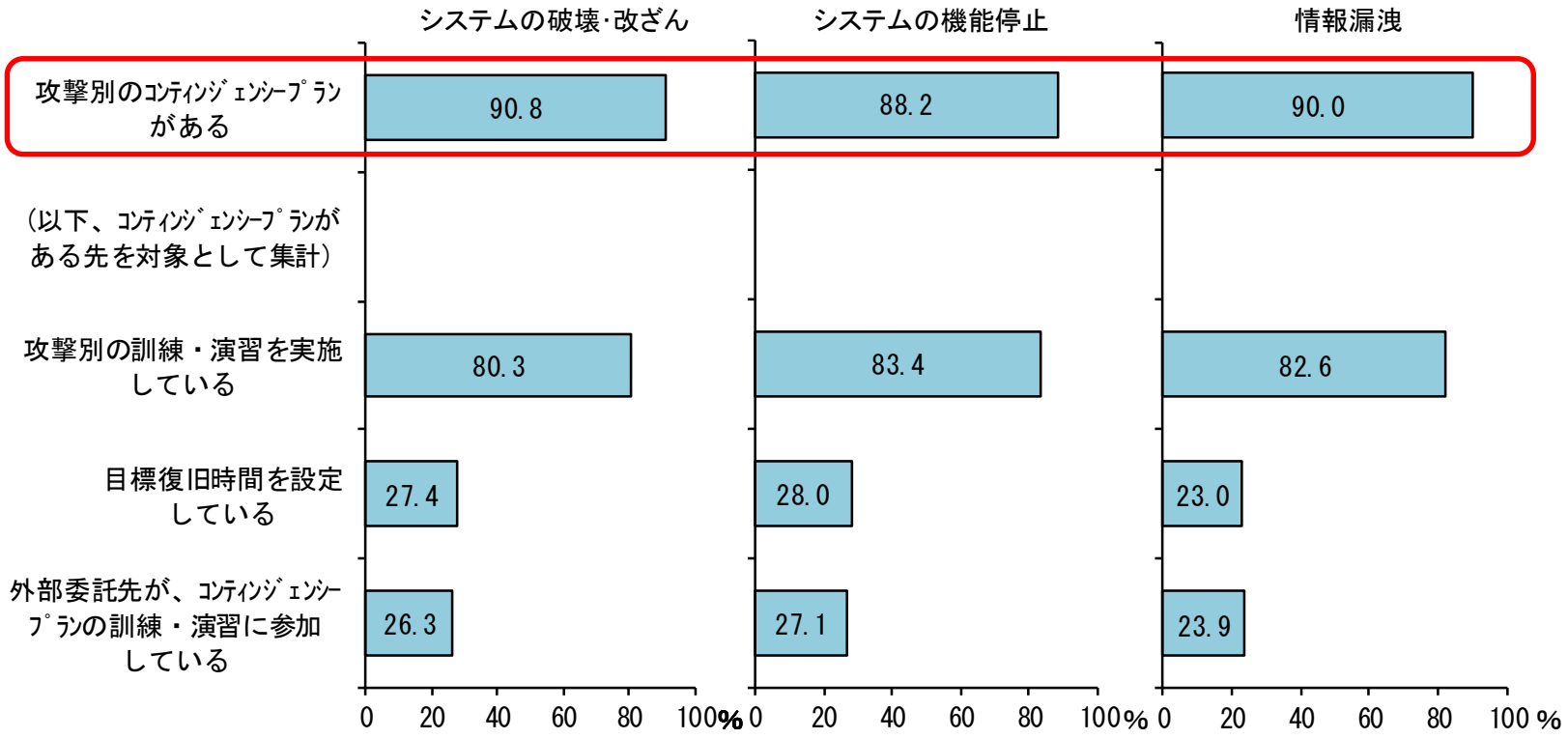
（注）診断等の実施には、外部にシステム運用を委託している場合の同先での診断等の実施状況を確認している場合も含む。

集計結果の概要　3. 有事への備え①

■ コンティンジェンシープランの策定、訓練・演習の実施

✓ 大半の先がサイバー攻撃（被害）別のコンティンジェンシープランを整備している。

▽ 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（本文図表16）

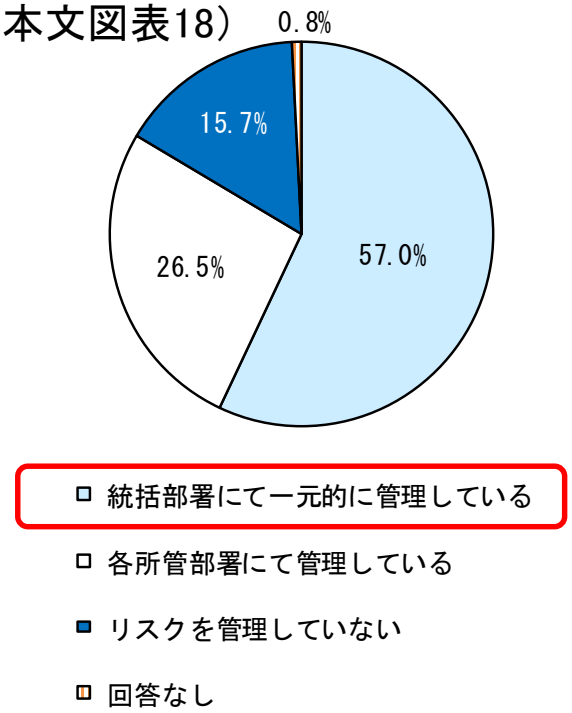


集計結果の概要　3. 有事への備え②

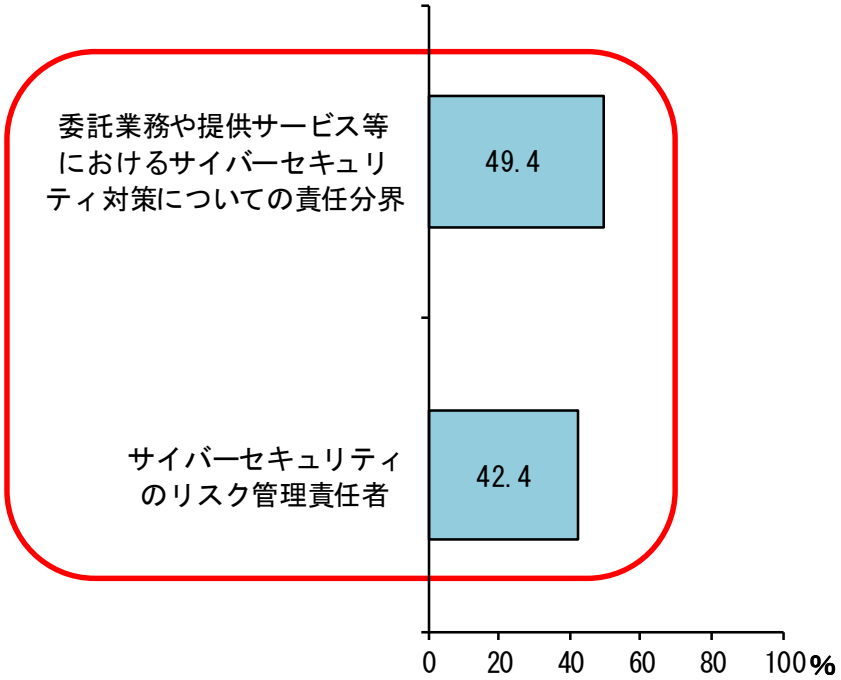
■ サードパーティリスクへの取り組み

- ✓ 重要なサードパーティに関するサイバーセキュリティのリスクは、半数以上が統括部署にて一元管理している。
- ✓ セキュリティの責任分界や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。

▽ 重要なサードパーティのリスク管理状況（本文図表18）



▽ 外部委託先との契約等で定めている事項（本文図表19）



（注）今回のサイバーセキュリティセルフアセスメントでは、「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。
また、「サードパーティー」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。

まとめ

- ✓ 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。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。
- ✓ 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、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、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、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。