資料７－１

金融庁
Financial Services Agency

金融庁におけるサイバーセキュリティに関する取組状況

2023年6月

金融庁総合政策局リスク分析総括課
サイバーセキュリティ対策企画調整室

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（Ver. 3.0）

～サイバーセキュリティを確保し、安心・安全かつ利便性の高い金融サービスの実現へ～

サイバー空間の変化

- 国家の関与が疑われる**組織化・洗練化されたサイバー攻撃**や、国際的なハッカー集団等による**ランサムウェア攻撃の多発**
- デジタライゼーションの進展による**金融サービスの担い手の多様化**と、キャッシュレス決済などの**連携サービスの進展**
- クラウドサービスをはじめとした**外部委託の拡大、サプライチェーンの複雑化・グローバル化**等による**リスク管理の難度の高まり**

新たな取組方針（以下、5項目）

1. モニタリング・演習の高度化

金融機関の規模・特性やサイバーセキュリティリスクに応じて、検査・モニタリングを実施し、サイバーセキュリティ管理態勢を検証する。
共通の課題や好事例については業界団体を通じて傘下金融機関に還元し、金融業界全体のサイバーセキュリティの高度化を促す。特に

- ✓ 3メガバンクについては、**サイバー攻撃の脅威動向の変化への対応**や**海外大手金融機関における先進事例**を参考にしたサイバーセキュリティの高度化に着目しつつ、モニタリングを実施する
- ✓ 地域金融機関については、**サイバーセキュリティに関する自己評価ツールを整備**し、各金融機関の自己評価結果を収集、分析、還元し、**自律的なサイバーセキュリティの高度化を促す**
- ✓ サイバー演習については、引き続き、**サイバー攻撃の脅威動向**や**他国の演習**等を踏まえて高度化を図る

2. 新たなリスクへの備え

- ✓ **キャッシュレス決済サービス**の安全性を確保するため、リスクに見合った**堅牢な認証方式の導入等**を促す（**セキュリティバイデザインの実践**）
- ✓ クラウドサービスの安全な利用に向けて、**利用実態**や**安全対策**の把握を進めるとともに、**クラウドサービス事業者との対話**も実施

3. サイバーセキュリティ確保に向けた組織全体での取組み

- ✓ 経営層の積極的な関与の下、**組織全体でサイバーセキュリティの実効性**の向上を促す（セキュリティ人材の育成も含む）

4. 関係機関との連携強化

- ✓ サイバー攻撃等の情報収集・分析、金融犯罪の未然防止と被害拡大防止への対応を強化するため**関係機関（NISC、警察庁、公安調査庁、金融ISAC、海外当局等）との連携を強化**

5. 経済安全保障上の対応

- ✓ 政府全体の取組みの中で、機器・システムの利用や業務委託等を通じたリスクについて適切に対応を行う

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

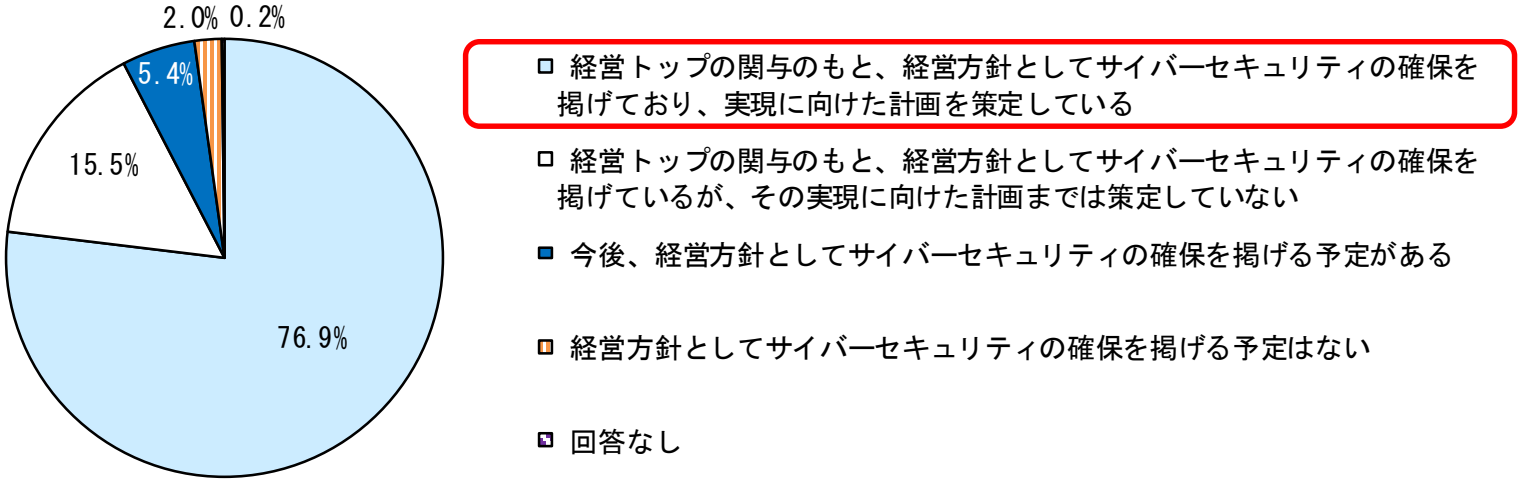
- ✓ 目　　的：　金融機関が他の金融機関対比での自組織の立ち位置や課題を認識することで、自律的なサイバーセキュリティ対策の強化に取り組むよう促す。
- ✓ 実施内容：　サイバーセキュリティ管理態勢の自己評価ツール（点検票）を整備。地域金融機関を対象に、自己評価を求め、その集計結果を還元。2022年度が初回。
- ✓ 実施方法：　日本銀行および金融庁が共同で実施。
- ✓ 対　　象：　地域金融機関498先（地域銀行99先、信用金庫254先、信用組合145先）
- ✓ 実施時期：　自己評価期間は2022年7月～8月。11月に集計結果を還元。

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）

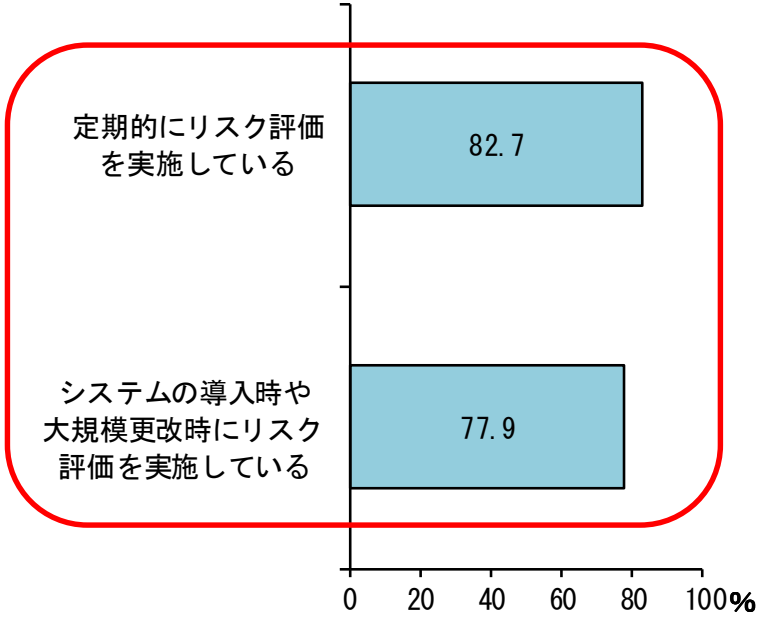


集計結果の概要　1. 経営層の関与②

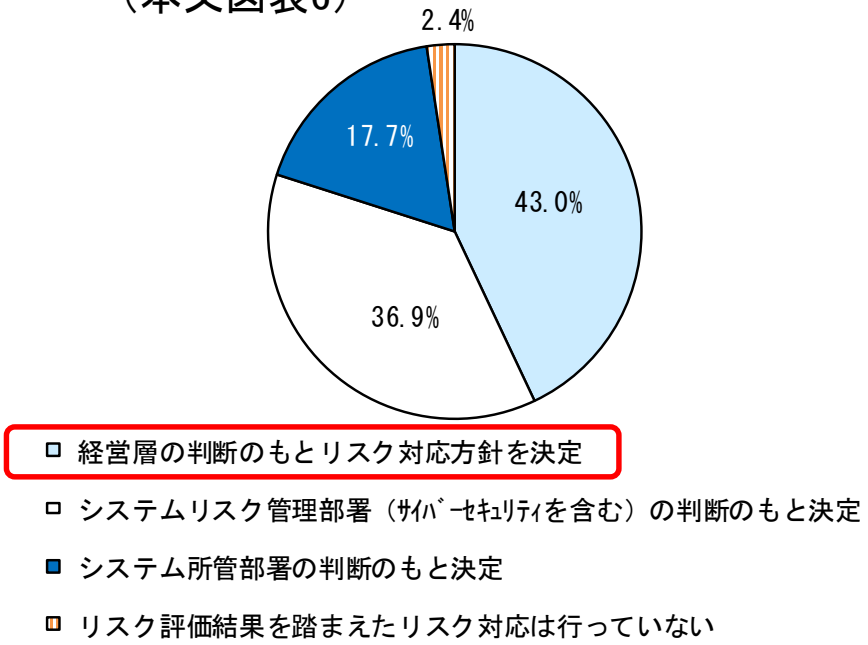
■　サイバーセキュリティに関するリスク評価の実施

- ✓ 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）



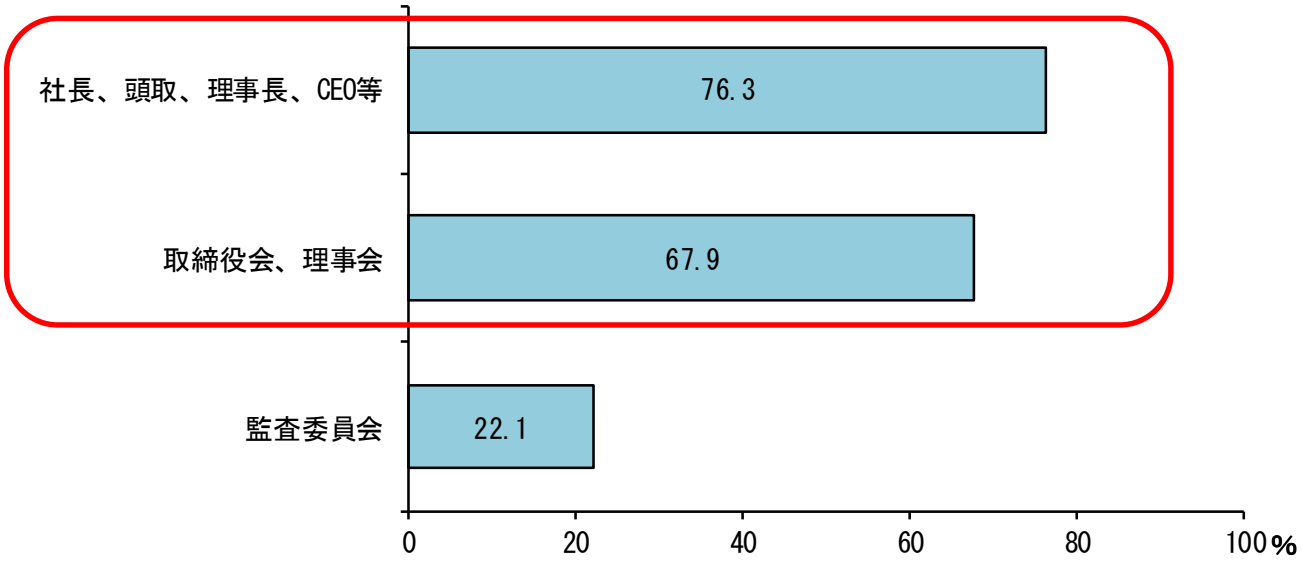
（注）今回のサイバーセキュリティセルフアセスメントでは、「重要なシステム」とは、「勘定系や顧客情報を扱うシステムなど自組織として業務運営上特に重要と認識しているシステム」と定義。

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）

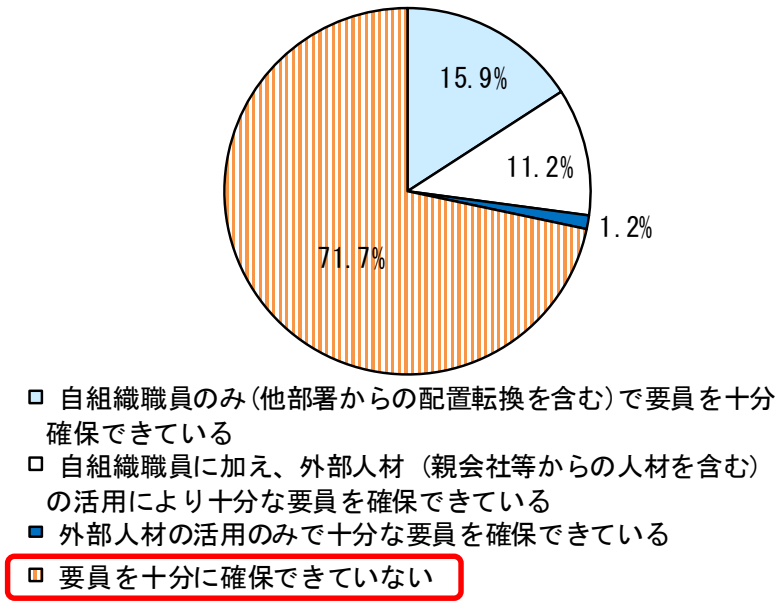


集計結果の概要　1. 経営層の関与④

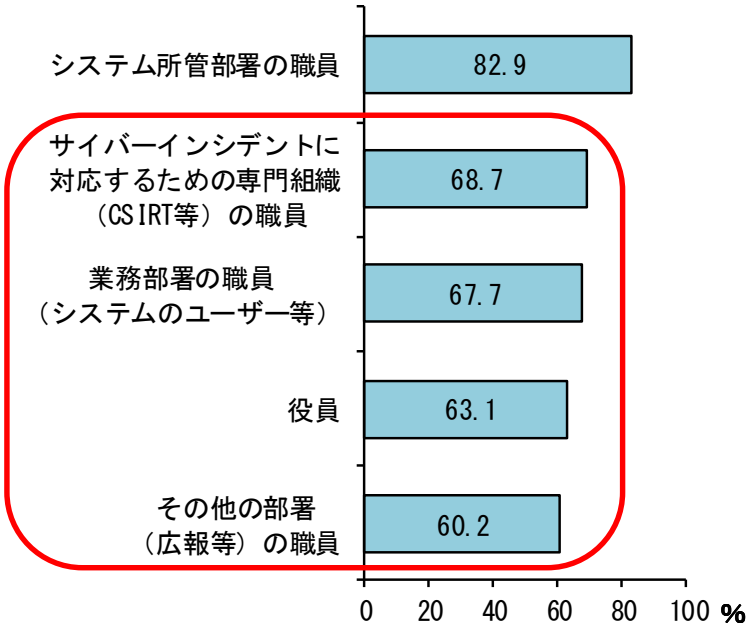
■ サイバーセキュリティ人材の確保の態勢

- ✓ 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）

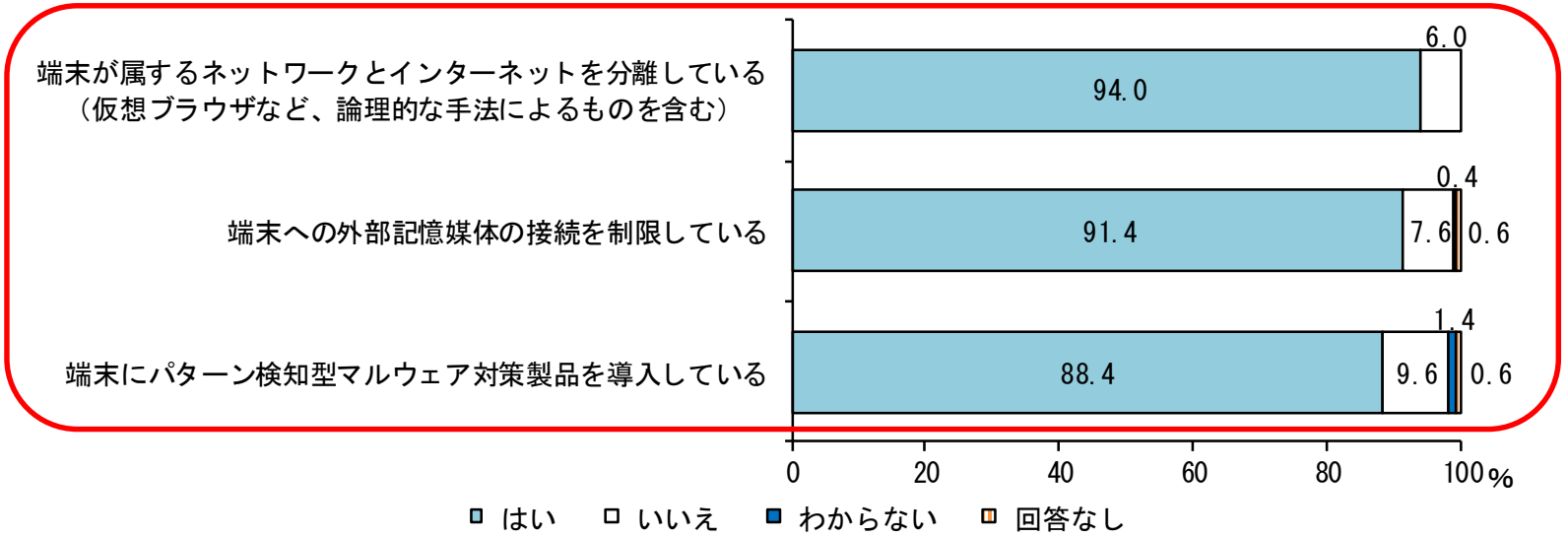


集計結果の概要　2. リスクへの構え①

■　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）



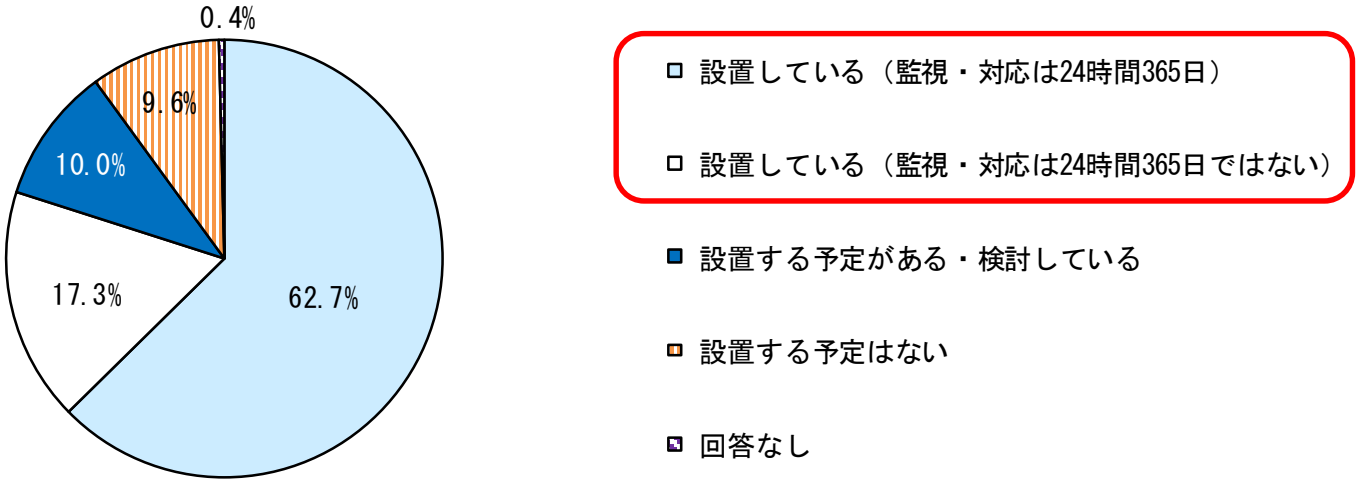
（注）今回のサイバーセキュリティセルフアセスメントでは、「OA端末」とは、「職員が文書作成等で標準的に用いる端末」と定義。

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）



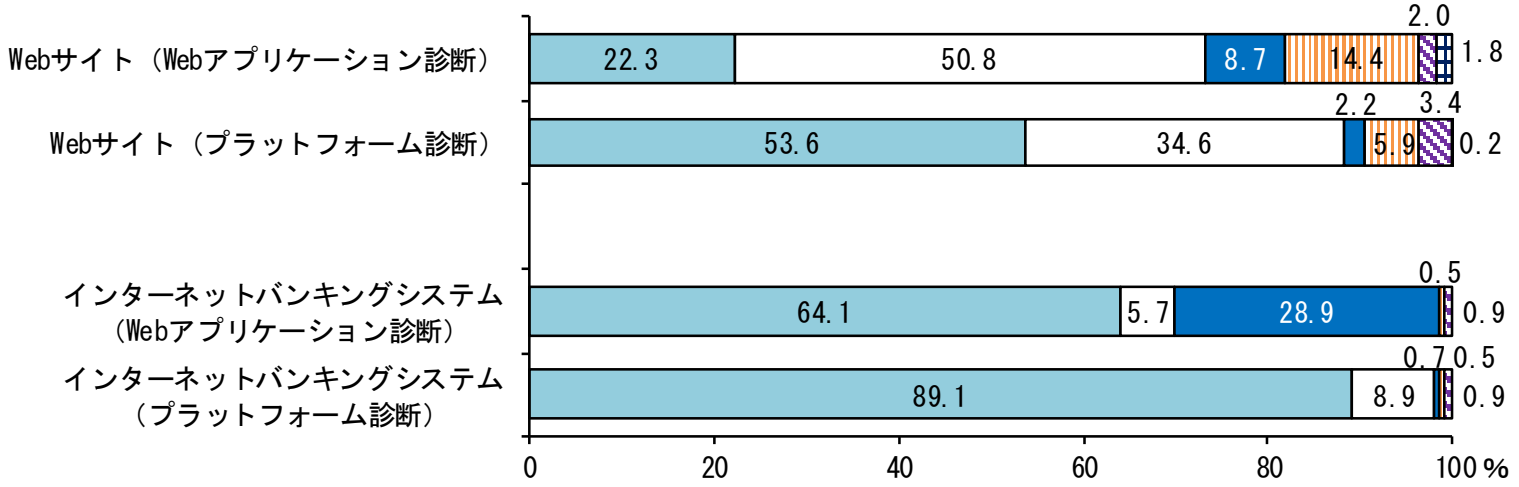
（注）SOCとは、Security Operation Centerの略。ネットワークやサーバ、ファイアウォール等の機器への攻撃状況など、セキュリティ関連の監視・分析等を行う組織。

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）



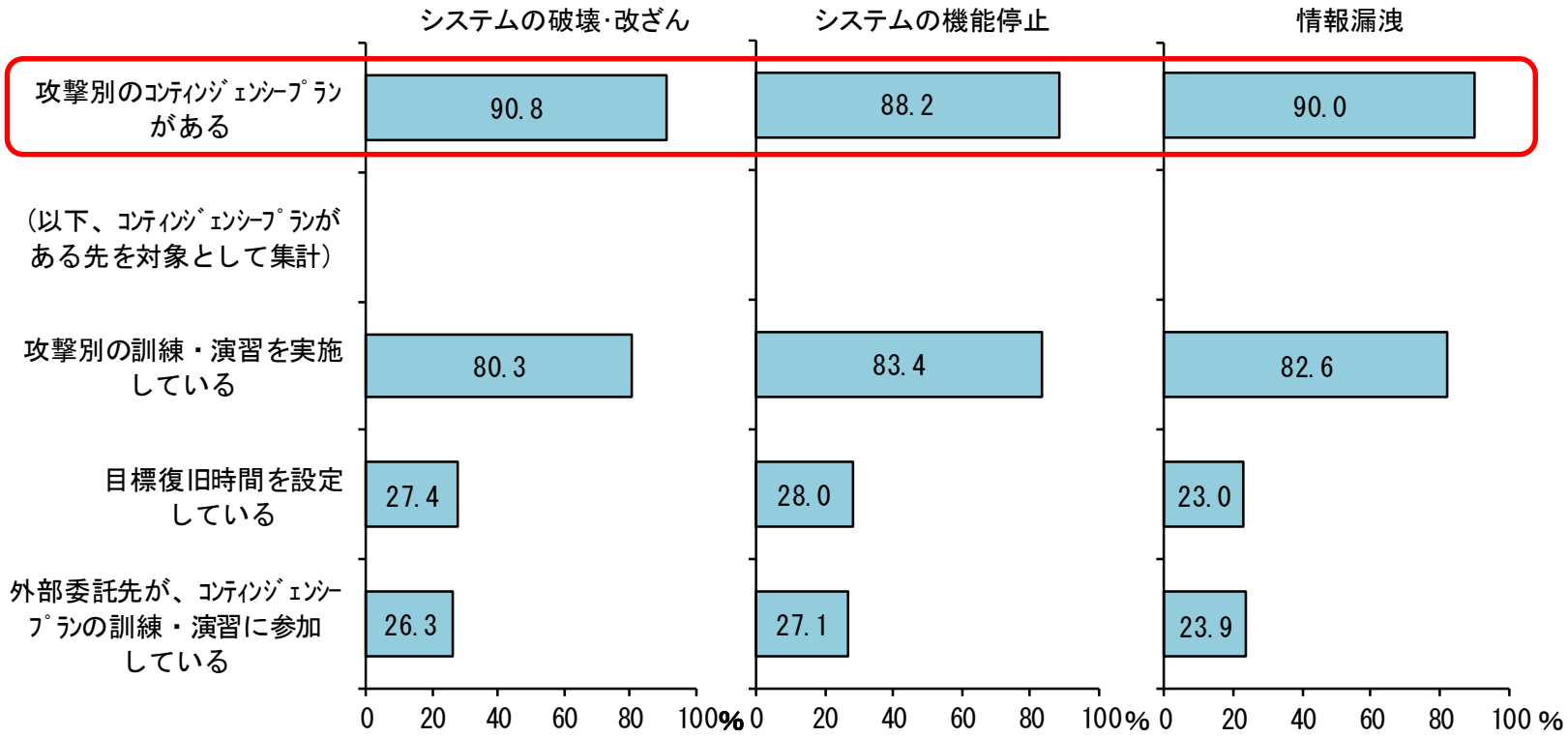
（注）診断等の実施には、外部にシステム運用を委託している場合の同先での診断等の実施状況を確認している場合も含む。

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）

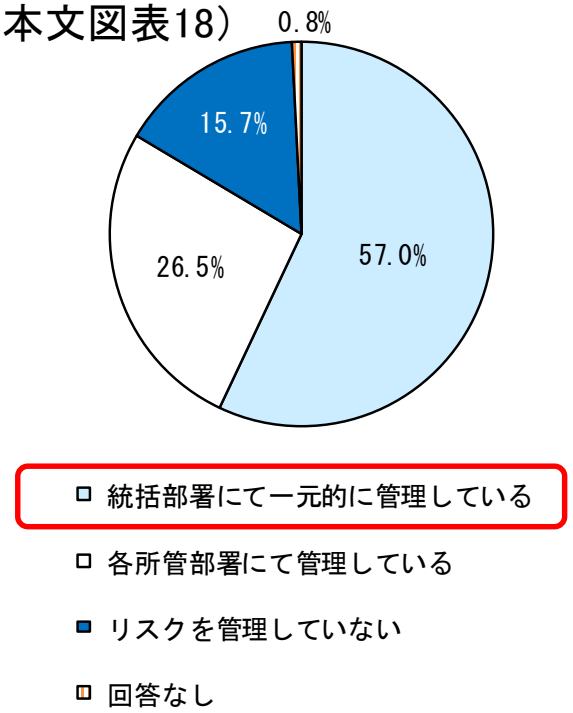


集計結果の概要　3. 有事への備え②

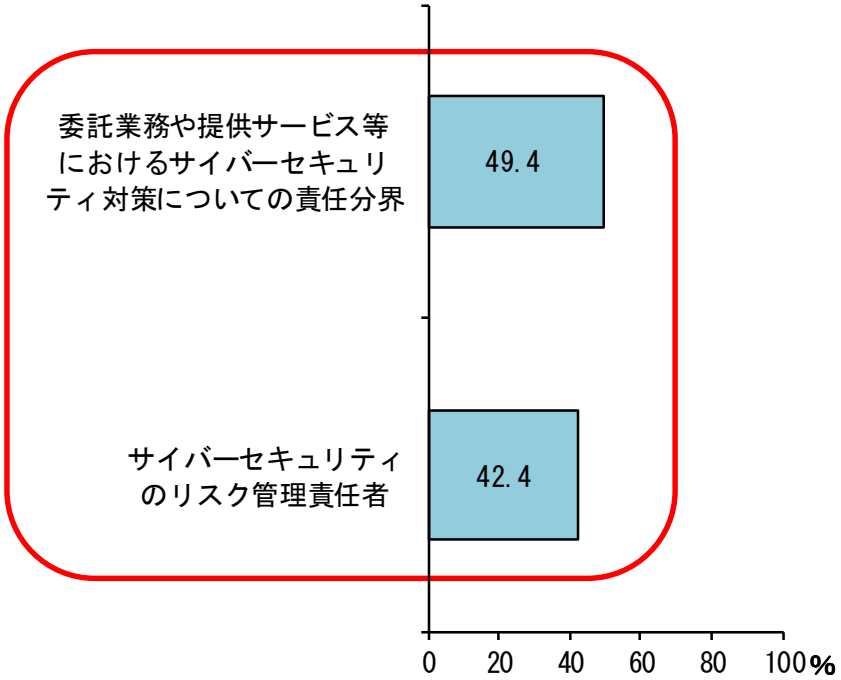
■ サードパーティリスクへの取り組み

- ✓ 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。