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（2023年度）

日本銀行金融機構局
金融庁総合政策局

2024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。2023年度が2回目。

- ✓ 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）

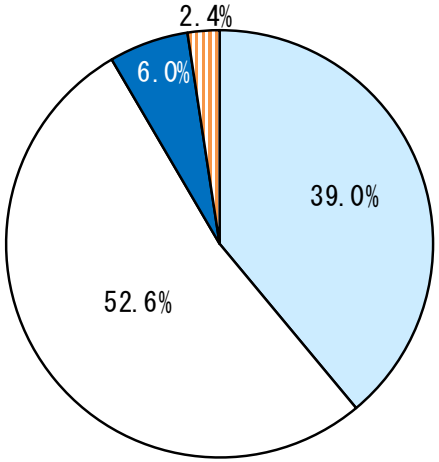
- ✓ 実施時期：自己評価期間は2023年7月～8月。11月に集計結果を還元。

集計結果の概要　1. 経営層の関与①

■ 経営方針・経営計画の策定、統括責任者の役割

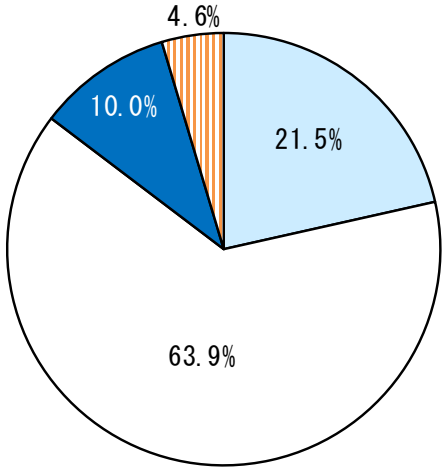
✓ 殆どの先が経営方針としてサイバーセキュリティの確保を掲げていたが、経営方針を定めていない先が8%程度みられた。また、経営計画については15%程度の先がこれを策定していなかった。

▽ サイバーセキュリティの経営方針（本文図表2）



- 経営トップ（頭取・社長・理事長等）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、ディスクロージャーやHP等で対外公表している
- 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（対外公表はしていない）
- 経営方針としてサイバーセキュリティの確保を掲げる予定がある
- 経営方針としてサイバーセキュリティの確保を掲げる予定はない

▽ サイバーセキュリティの経営計画（本文図表3）



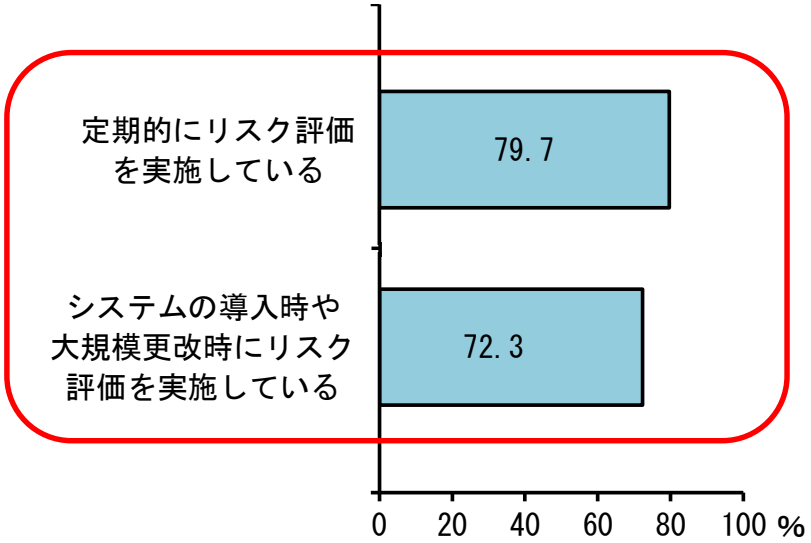
- サイバーセキュリティに関する複数年度の経営計画を策定している
- サイバーセキュリティに関する単年度の経営計画を策定している
- 今後、サイバーセキュリティに関する経営計画の策定を予定している
- サイバーセキュリティに関する経営計画策定する予定はない

集計結果の概要　1. 経営層の関与②

■ リスク管理と経営層の関与

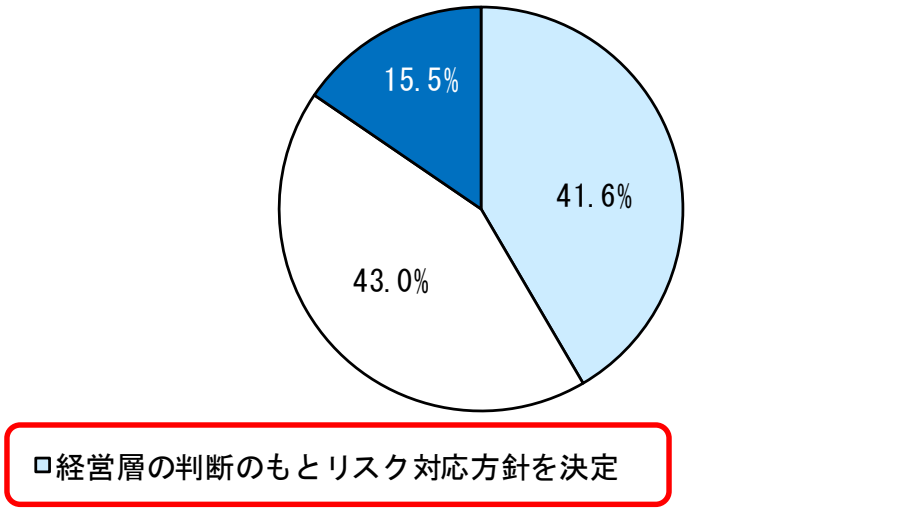
- ✓ サイバーセキュリティのリスクを導入時や定期的に評価する先が多い。
- ✓ 他方、経営層の判断のもとでリスク対応方針を決定している先は4割強にとどまった。

▽ 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。

▽ リスク評価を踏まえた対応方針の決定者（本文図表7）

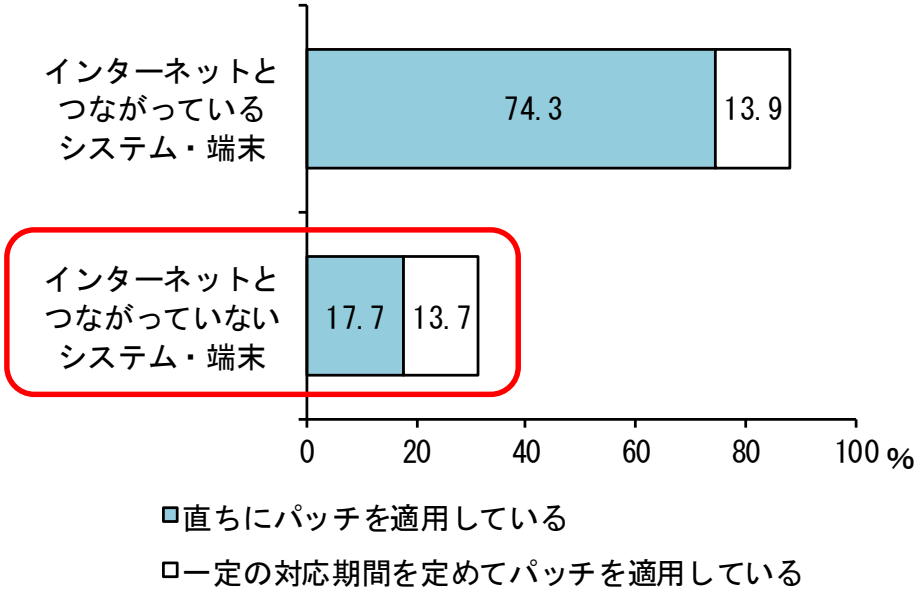


集計結果の概要　1. 経営層の関与③

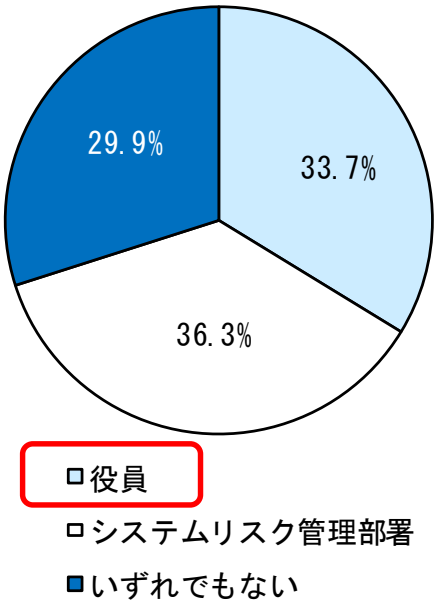
■ リスク管理と経営層の関与

- ✓ 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セキュリティパッチを適用している先が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。
- ✓ 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。

▽　深刻な脆弱性が判明した場合のパッチの適用方針（本文図表8）



▽　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（本文図表9）

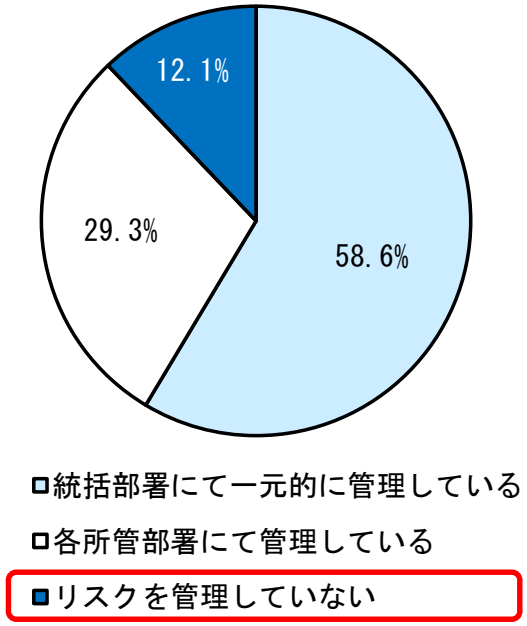


集計結果の概要　1. 経営層の関与④

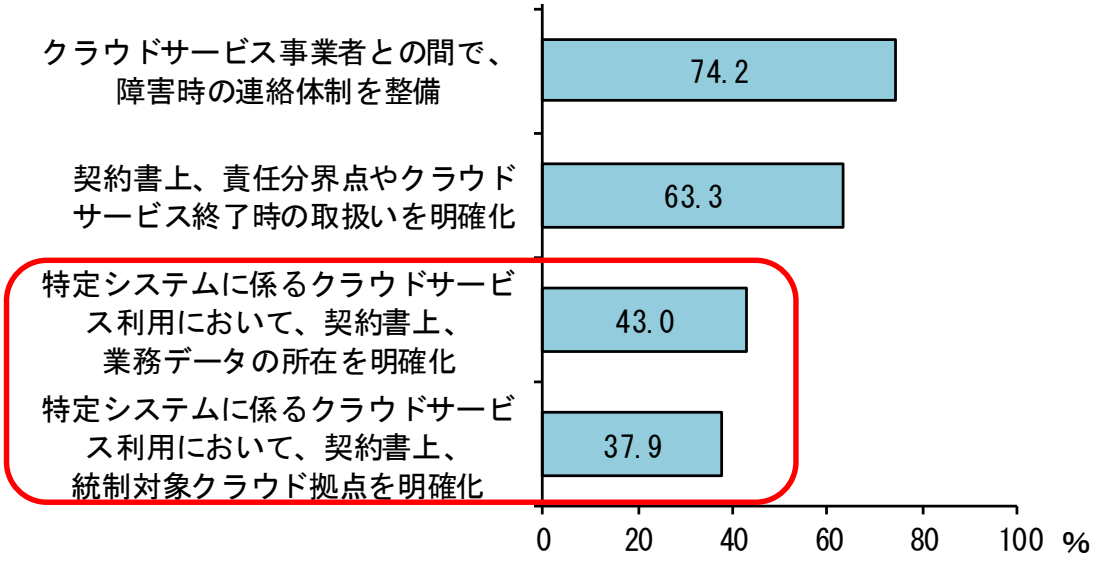
■ サードパーティリスクへの取り組み

- ✓ 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、統括部署にて一元管理している先は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。
- ✓ また、クラウド事業者との間で、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。

▽ 重要なサードパーティのリスク管理状況（本文図表10）



▽ クラウド事業者と契約等で定めている事項（本文図表11）



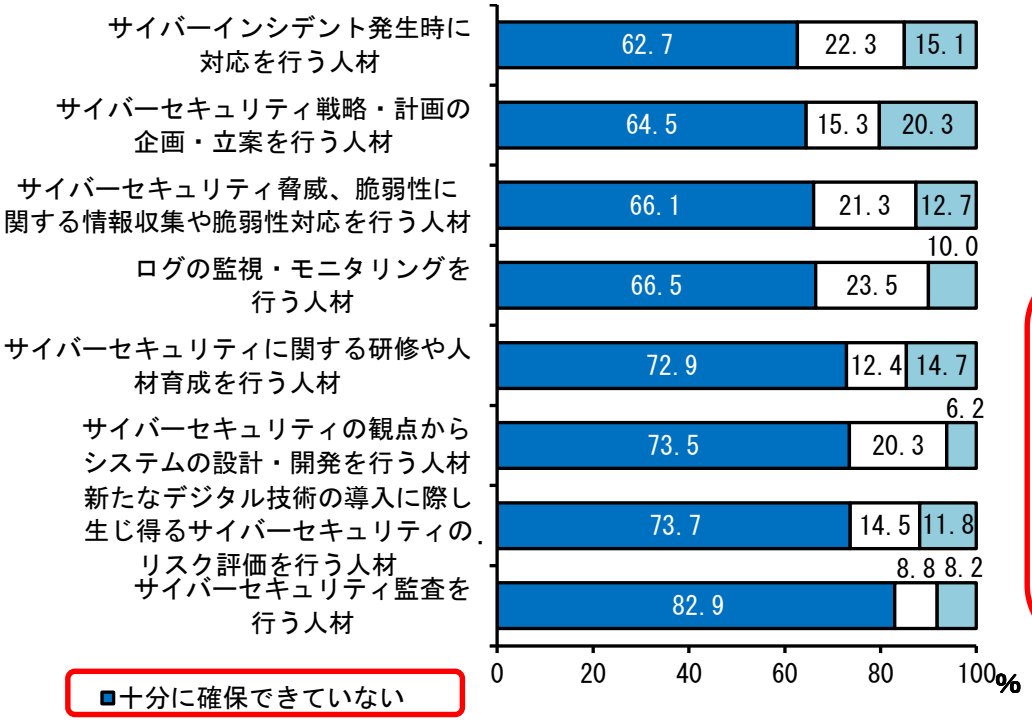
（注）今回のCSSAにおける「重要なサードパーティ」とは、「自組織として業務運営上重要と認識しているサードパーティ」と定義。

集計結果の概要　1. 経営層の関与⑤

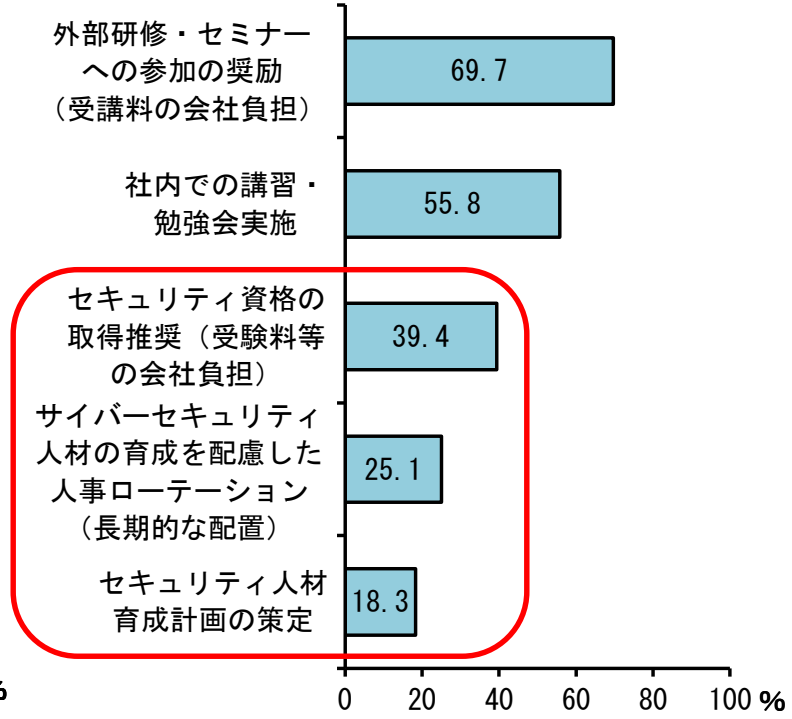
■ サイバーセキュリティ人材の確保

- ✓ サイバーセキュリティ人材は、いずれの機能でも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が確認された。
- ✓ 人材育成は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、中長期的な視点に立って取り組む先は限定的となっていた。

▽ 機能別にみたサイバーセキュリティ人材の確保状況（本文図表12）



▽　人材育成の取り組み（本文図表13）

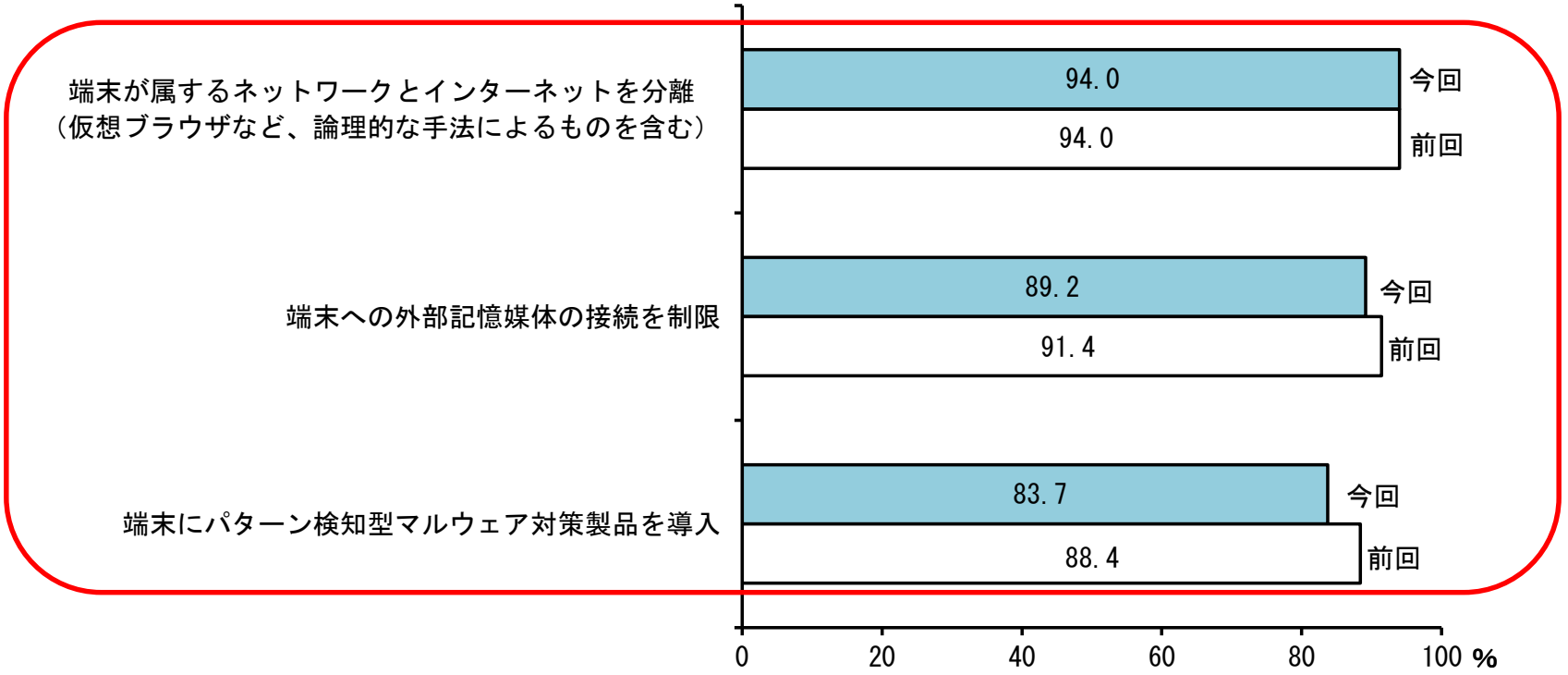


集計結果の概要　2. リスクへの対策①

■　OA端末における対策

- ✓ 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境界防御型の対策は8～9割の先が実施。
- ✓ デジタル化施策を一段と推進していく場合、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ことが必要。

▽　OA端末のサイバー攻撃対策（本文図表15）



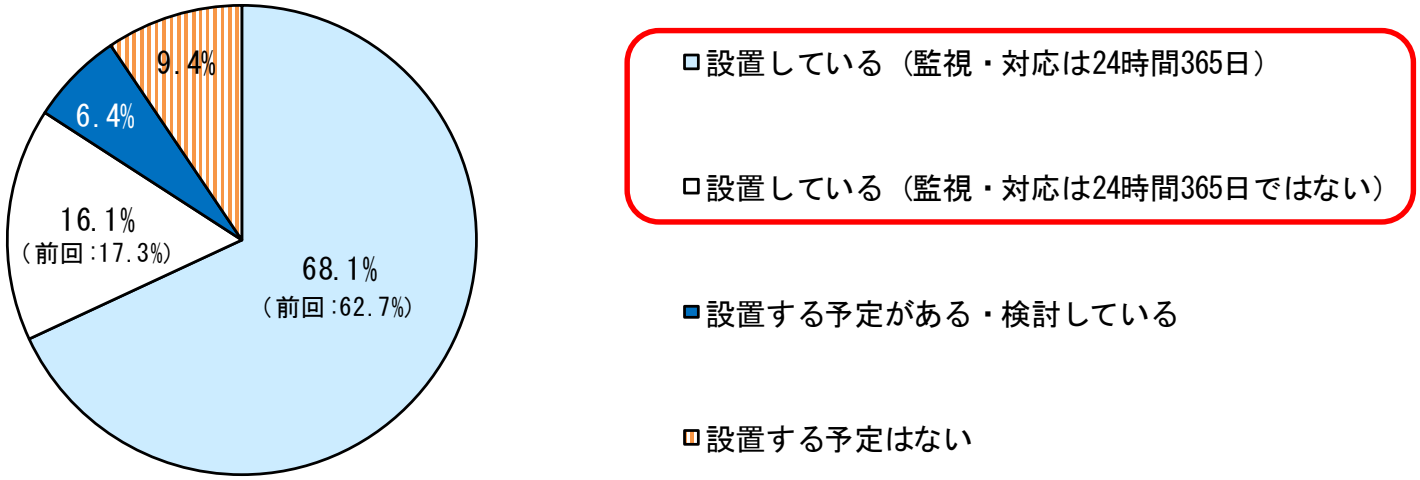
（注）今回のサイバーセキュリティセルフアセスメントでは、「OA端末」とは、「職員が文書作成等で標準的に用いる端末」と定義。

集計結果の概要　2. リスクへの対策②

■　サイバーインシデントの監視・分析等の態勢

✓ セキュリティ関連の監視・分析等を行う組織（SOC）等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。

▽　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16）



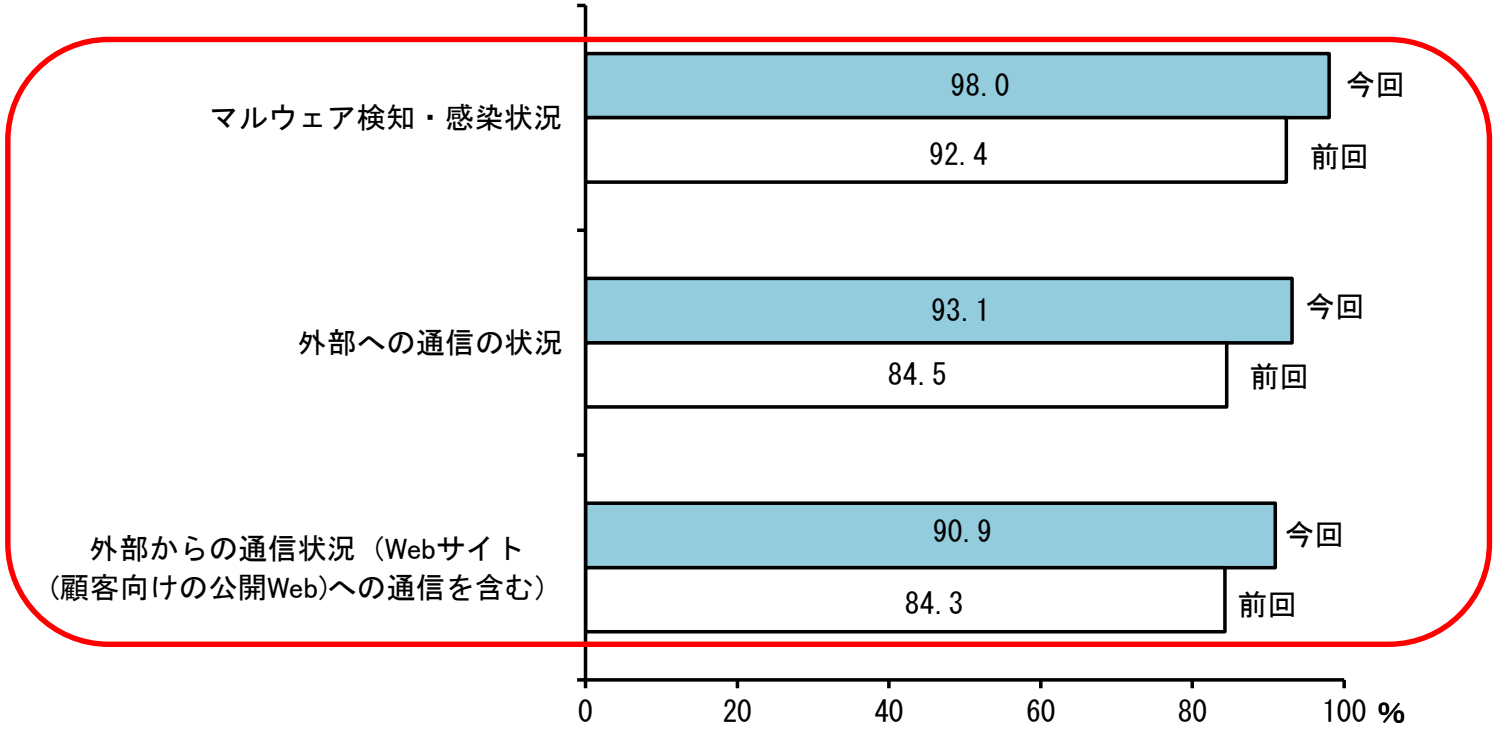
（注）SOCとは、Security Operation Centerの略。ネットワークやサーバ、ファイアウォール等の機器への攻撃状況など、セキュリティ関連の監視・分析等を行う組織。

集計結果の概要　2. リスクへの対策③

■ サイバーインシデントの監視・分析等の態勢

- ✓ 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・分析は、殆どの先が実施。
- ✓ デジタル化施策を一段と推進していく場合、自組織内部への侵入や内部犯行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。

▽　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（本文図表17）

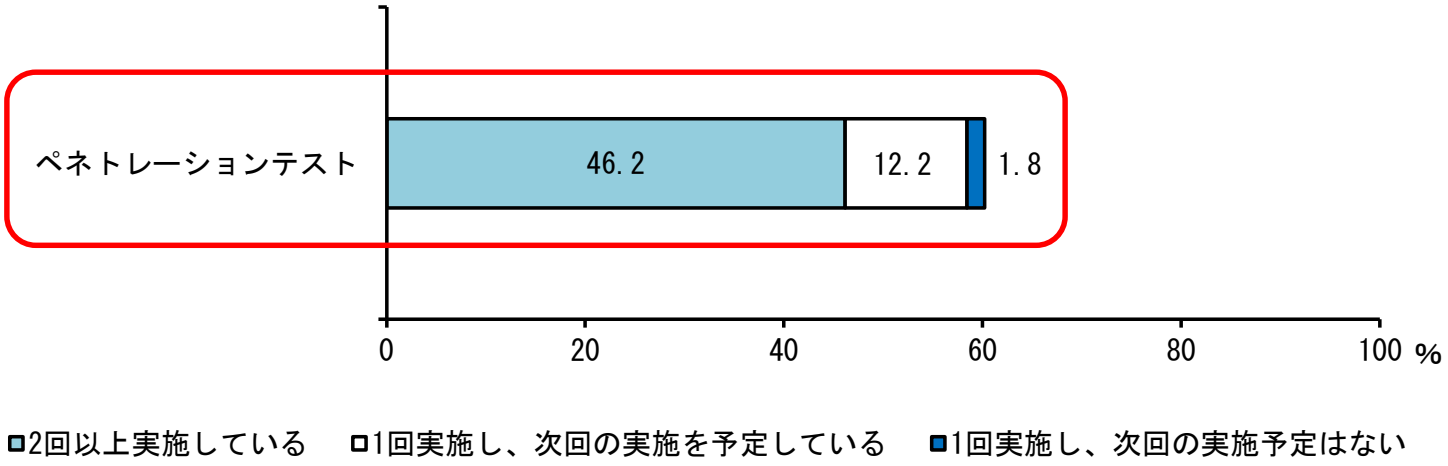


集計結果の概要　2. リスクへの対策④

■　検知・監視態勢の実効性の確認

- ✓ 検知・監視体制について第三者的な目線からの確認状況をみると、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。
- ✓ 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に取り組むことが期待される。

▽　ペネトレーションテストの実施状況（本文図表19）



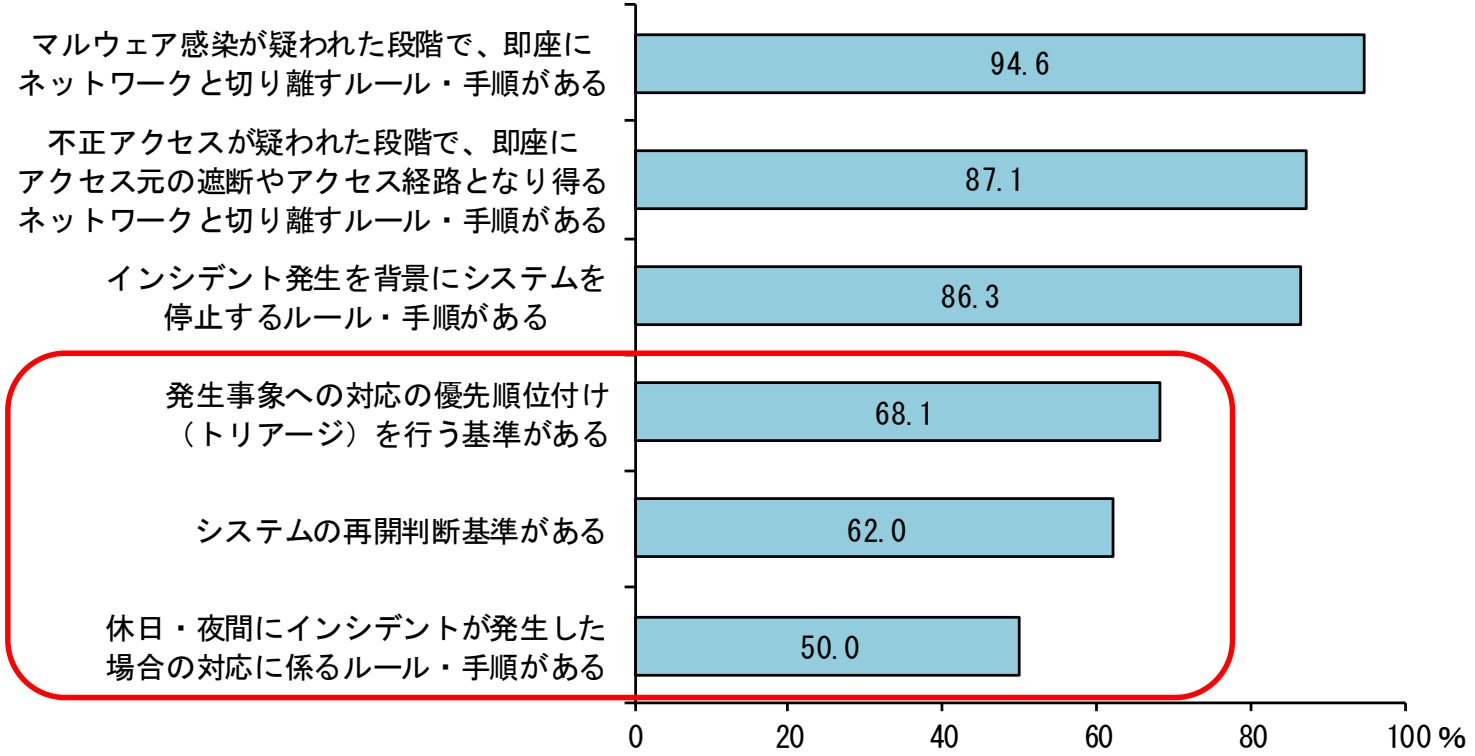
（注）今回のCSSAにおける「ペネトレーションテスト」とは、擬似的なマルウェアを利用したり、脆弱性・設定不備等を悪用したりするなど擬似的な攻撃を仕掛けることで、侵入・改ざんの可否や検知の可否、対応の迅速性・適切性を検証するテスト」と定義。

集計結果の概要　3. 有事への備え①

■　被害拡大防止のための対応手順の整備

✓ 初動に関するルール・手順は大半の先が整備していたが、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・休日の対応手順を整備している先は5～7割となった。

▽　被害拡大防止のためのルール・手順の整備状況（本文図表20）

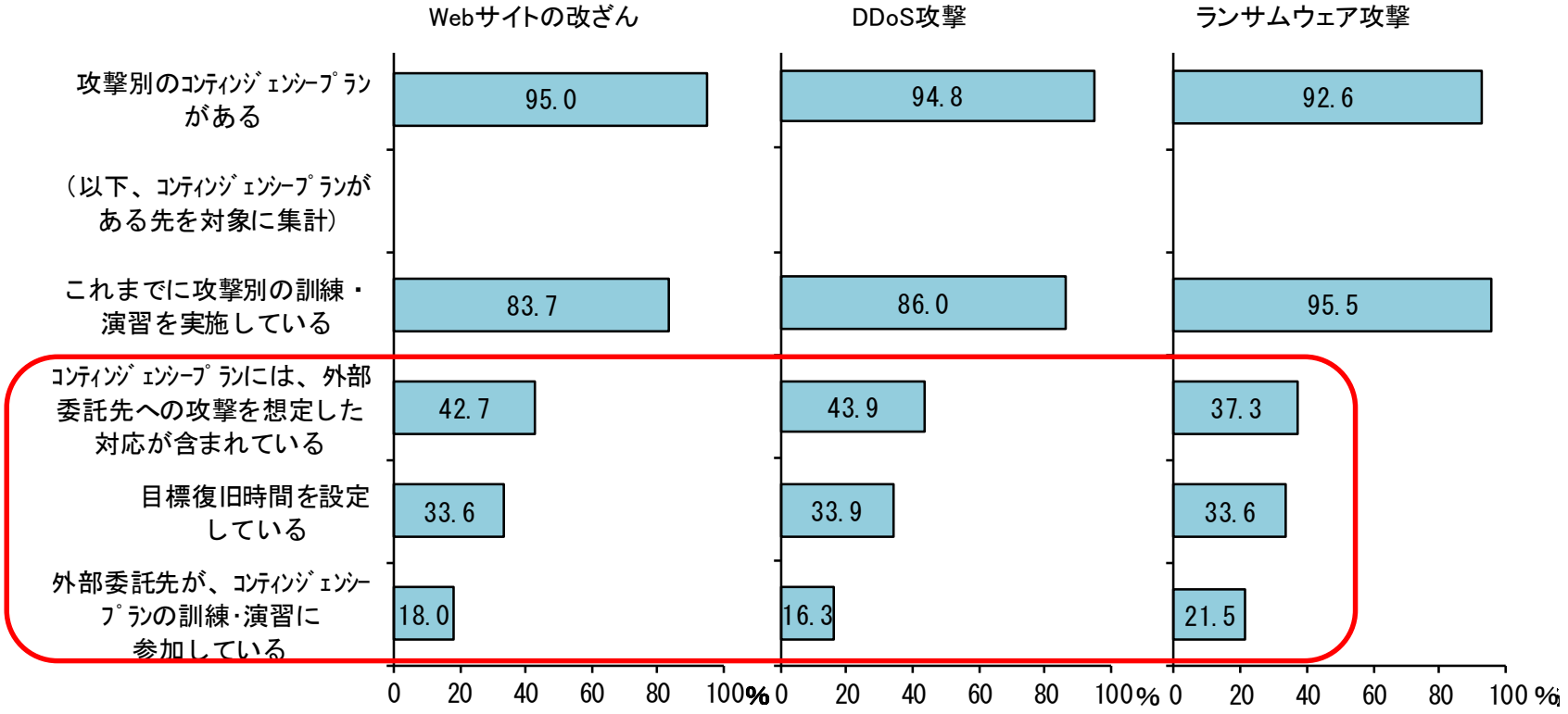


集計結果の概要　3. 有事への備え②

■ コンティンジェンシープランの策定、訓練・演習の実施

- ✓ サイバー攻撃別のコンティンジェンシー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た。
- ✓ もっとも、外部委託先への攻撃を含めたプランの整備、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。

▽　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（本文図表21）

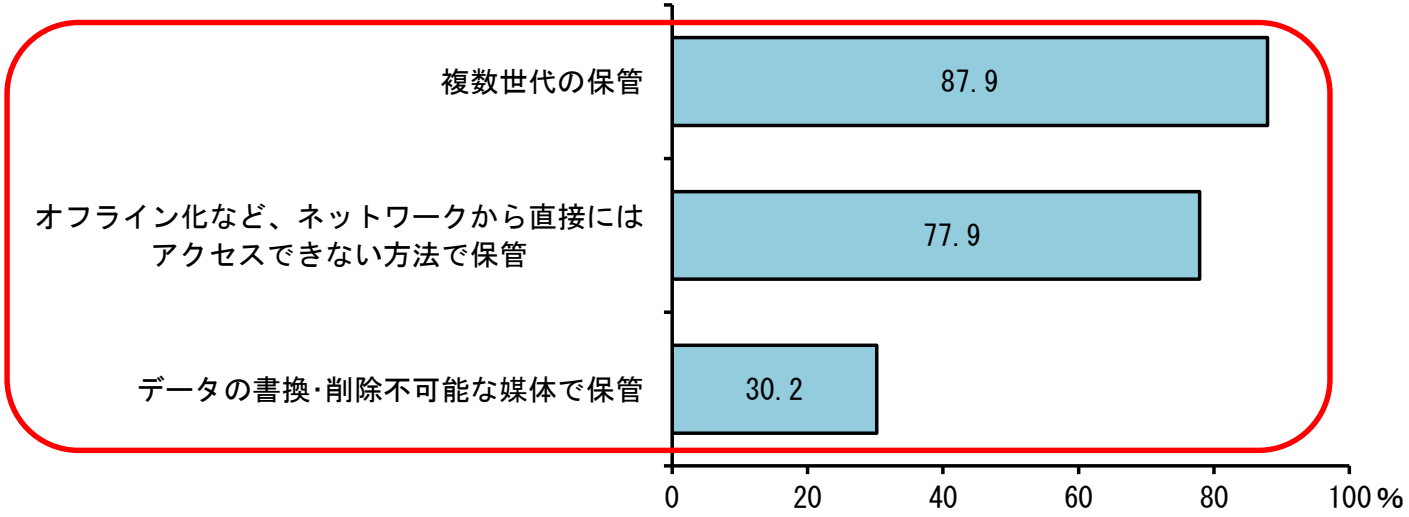


集計結果の概要　3. 有事への備え③

■ 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

- ✓ 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、バックアップデータの保護対策を講じている先が大半。
- ✓ 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、破壊・改ざんの対策を行うことが重要。

▽ 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（本文図表22）



■「ルール・手順を定め実施状況をモニタリングしている」または「ルール・手順を定めている」と回答した先

まとめ

- ✓ 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は重要な課題となっている。
- ✓ 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、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。
- ✓ 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、2024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。