【概要】
保険会社における
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）

金融庁
2024年4月

実施概要

✓ 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。
保険会社を対象に、自己評価を求め、その集計結果を還元。
保険会社の実施は2023年度が初回。

✓ 実施方法：金融庁が実施。

✓ 対　　象：保険会社71先
（生命保険協会加盟42先、日本損害保険協会加盟29先）

✓ 実施時期：自己評価期間は2023年7月～8月。10月に集計結果を還元。

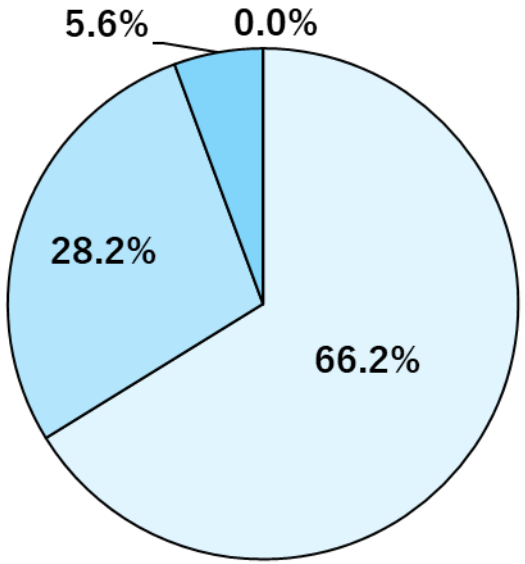
以下では、自己評価の結果から読み取れる保険会社での各種対策の状況を概観する。

（注）資料上のグラフの数値は小数点第2位以下を四捨五入しているため、割合の合計は必ずしも100にならない。

集計結果の概要　経営方針・経営計画の策定

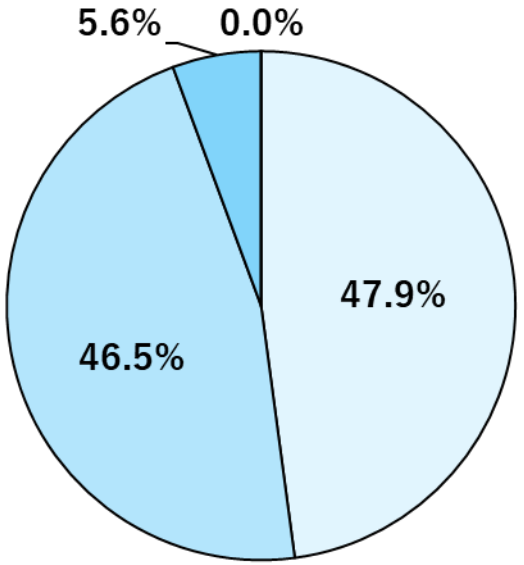
- ✓ 対顧客サービスの拡充や業務改革の推進といったデジタル化戦略を推進するにあたり、サイバーセキュリティ管理態勢の整備も同時に行う必要がある。経営トップの関与のもと、サイバーセキュリティを組み込んだ経営方針を定め、デジタル化戦略の前提であるサイバーセキュリティに対する経営資源の投入を含む具体的な計画を策定し、IT部門だけではなく、組織としてその計画を実行していくことが重要である。
- ✓ ほとんどの先が、経営方針としてサイバーセキュリティの確保を掲げ、経営計画を策定しているなか、これらを定めていない先が約6%見られた（図表1、2）　。

図表1 サイバーセキュリティの経営方針



- 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ており、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（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ている（対外公表はしていない）
- 今後、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

図表2 サイバーセキュリティの経営計画

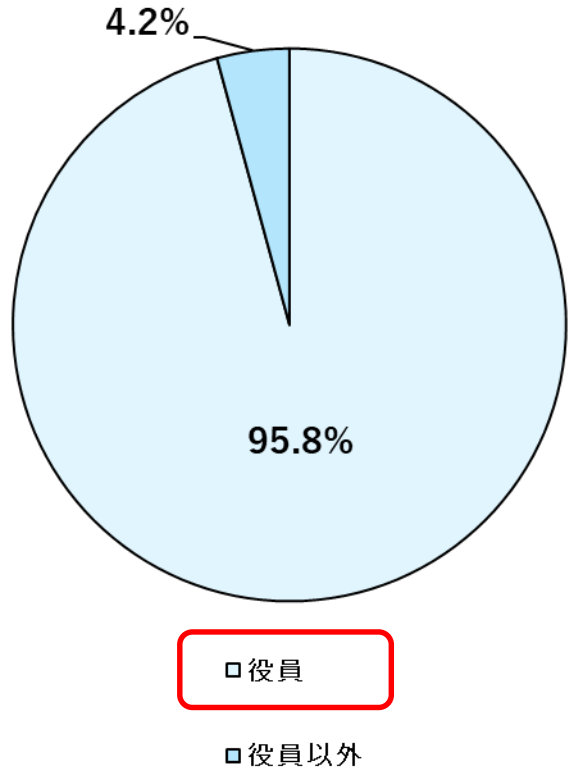


- サイバーセキュリティに関する（単年度に加えて）複数年度の経営計画を策定している
- サイバーセキュリティに関する単年度の経営計画を策定している
- 今後、サイバーセキュリティに関する経営計画の策定を予定している
- サイバーセキュリティに関する経営計画を策定する予定はない

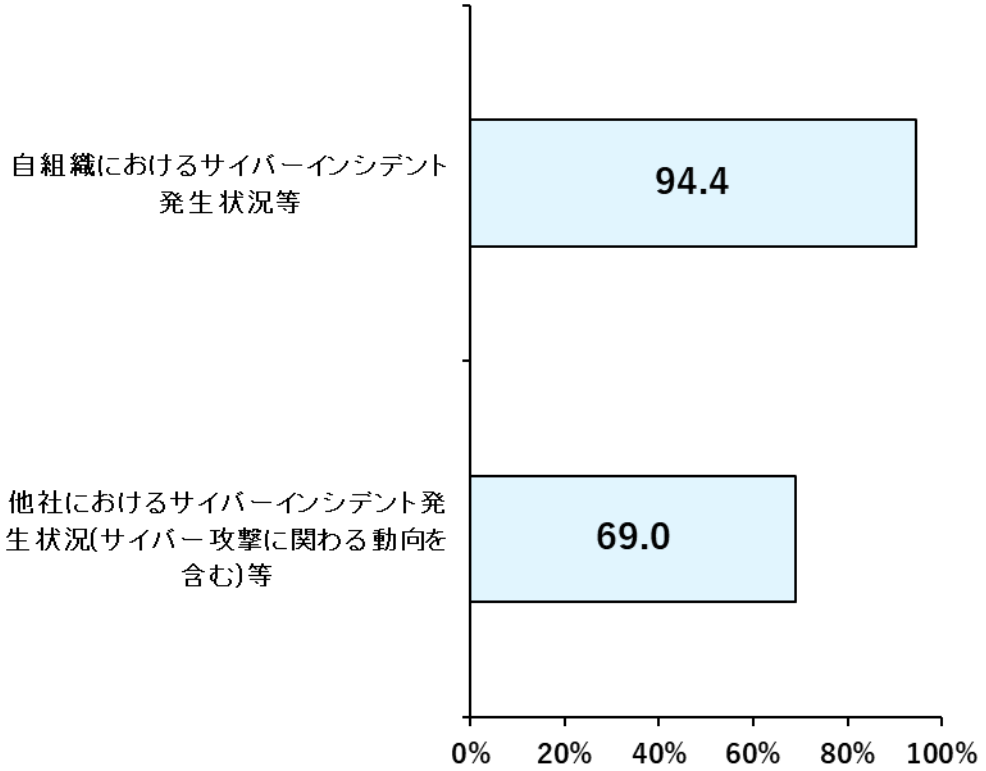
集計結果の概要　統括責任者への報告

- ✓ 経営層（役員（※））に対し、他社事例を含め、最近の脅威動向に関する情報を報告することは、自組織の対策状況の点検に繋げていく土壌を作るうえで重要である。
- ✓ ほとんどの先が、役員をサイバーセキュリティの統括責任者としており（図表3）、自組織のサイバーインシデントの発生状況をサイバーセキュリティ統括責任者に定期的に報告しているが、他社事例を定期的に報告している保険会社の割合は相対的に低くなっている（図表4）　。

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、統括責任者に定例報告している内容

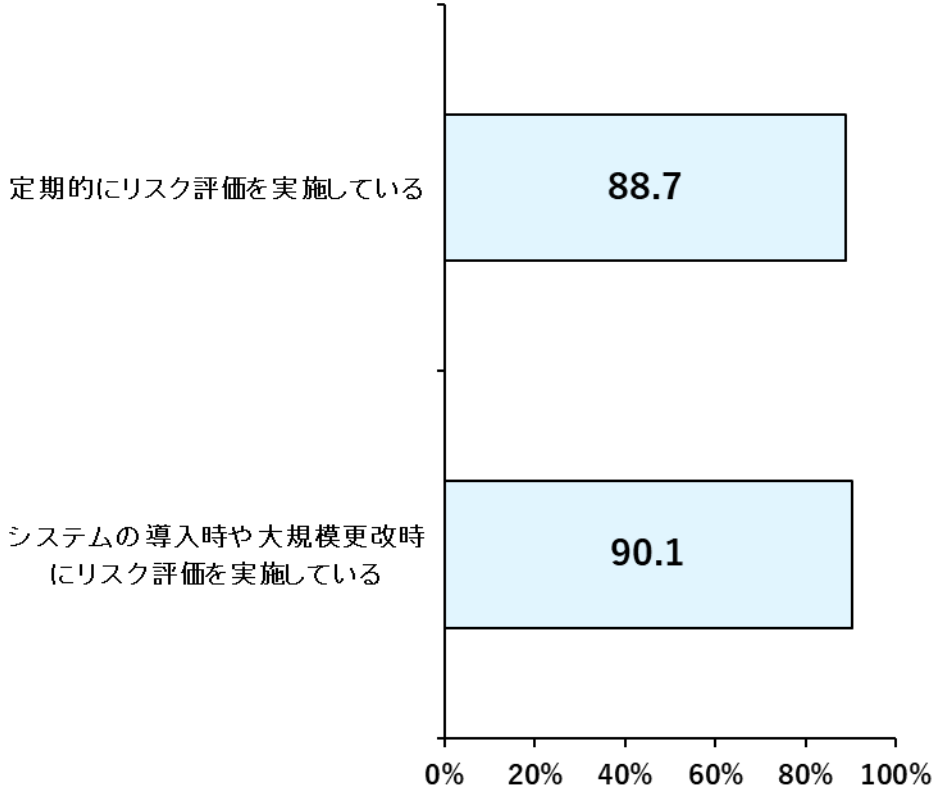


※役員には、執行役員などの従業員役職者を含みます。

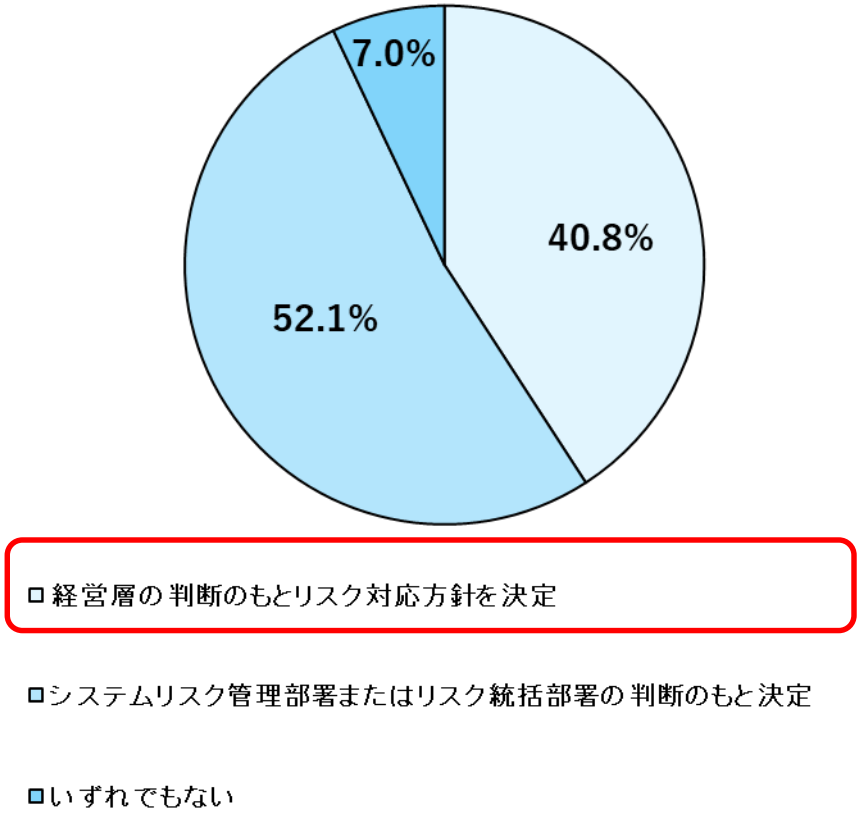
集計結果の概要　リスク管理と経営層の関与

- ✓ サイバー攻撃に適切に対応するため、サイバーリスクを評価し、その低減策を講じることが重要である。多くの保険会社において、重要なシステム（※）のサイバーリスクの評価が定期的及びシステム導入時・大規模更改時に行われている（図表5）。
- ✓ サイバーリスクを評価し、低減策を講じたうえでの残存するリスクへの対応（受容の可否含む）は、その重要度に応じ、経営層の判断のもと、決定すべきである。残存するリスクへの対応について、経営層の判断のもと、決定している先は４割程度にとどまった（図表6）。

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

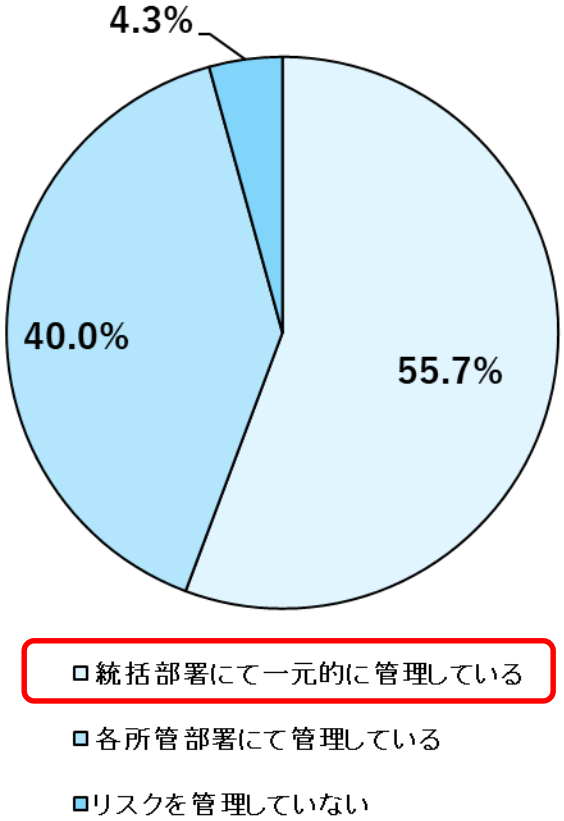


※今回のCSSAにおける「重要なシステム」とは、「勘定系や顧客情報を扱うシステムなど自組織として業務運営上特に重要と認識しているシステム」と定義。

集計結果の概要　サードパーティリスクへの取組

- ✓ 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しており、これを適切に管理することが重要である。特に、重要なサードパーティ（※）については、責任の所在や管理内容の目線が曖昧になることを防ぐため、組織横断的・一元的に管理する態勢を構築することが重要である。
- ✓ 重要なサードパーティが存在する先の中で、重要なサードパーティを一元的に管理している先は5割程度にとどまっており、リスクを管理していない先も一定数みられた（図表7）　。

図表7　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

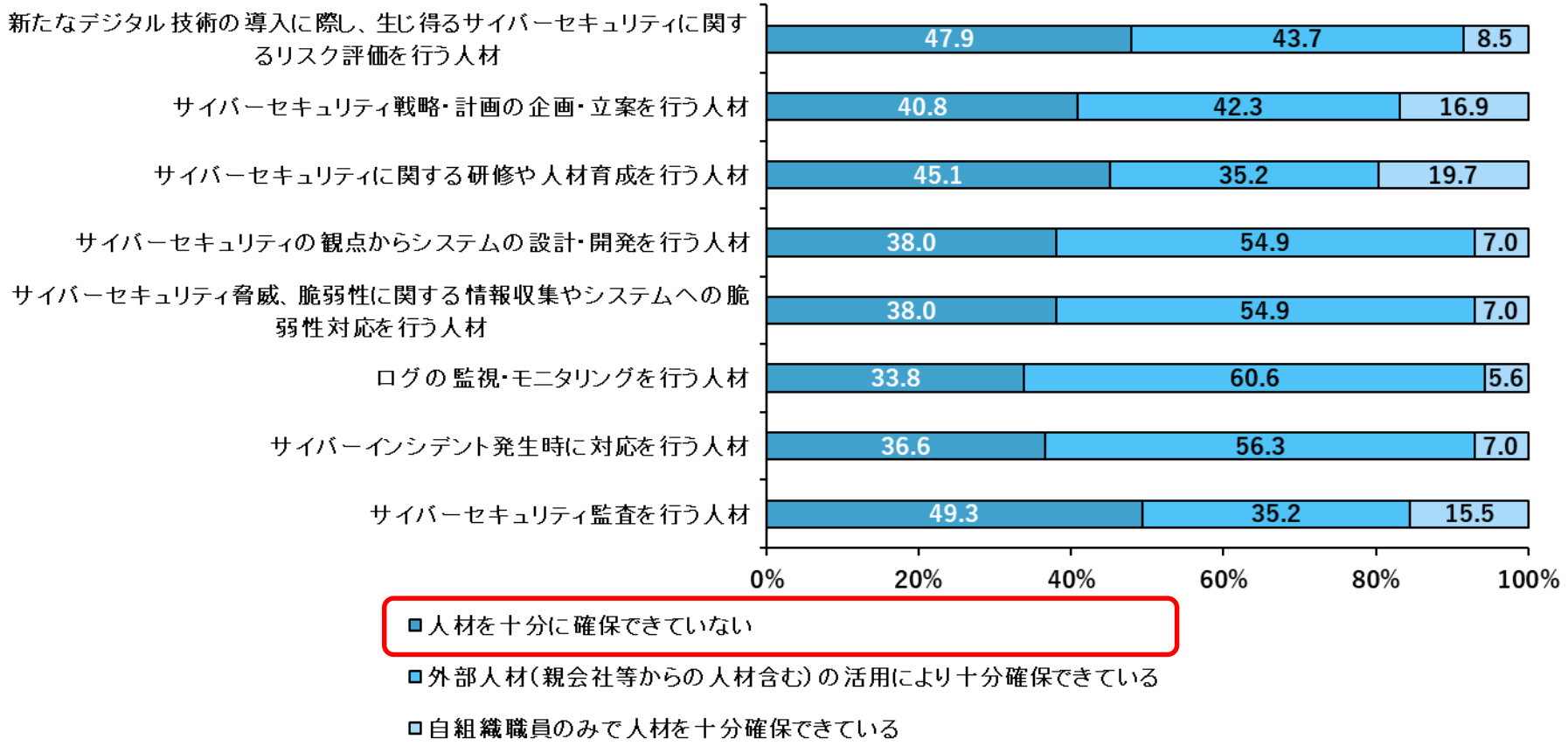


※今回のCSSAにおける「重要なサードパーティ」とは、「自組織として業務運営上重要と認識しているサードパーティ」と定義。
なお、「サードパーティ」とは、「自組織がサービスを提供するために、業務上の関係や契約等を有する他の組織」と定義
（例：システム子会社、ベンダー等の外部委託先、クラウド等のサービス提供事業者、資金移動業者等の業務提携先など）。

集計結果の概要　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に係るリスク評価、セキュリティインシデントへの対応、サイバーセキュリティ監査の適切な実施のためには、該当業務に知見を持つセキュリティ人材の確保が必要となる。
- ✓ 図表8に示されるように、あらゆる領域・機能に渡って、人材を十分に確保できていないと認識している先が一定割合存在している。

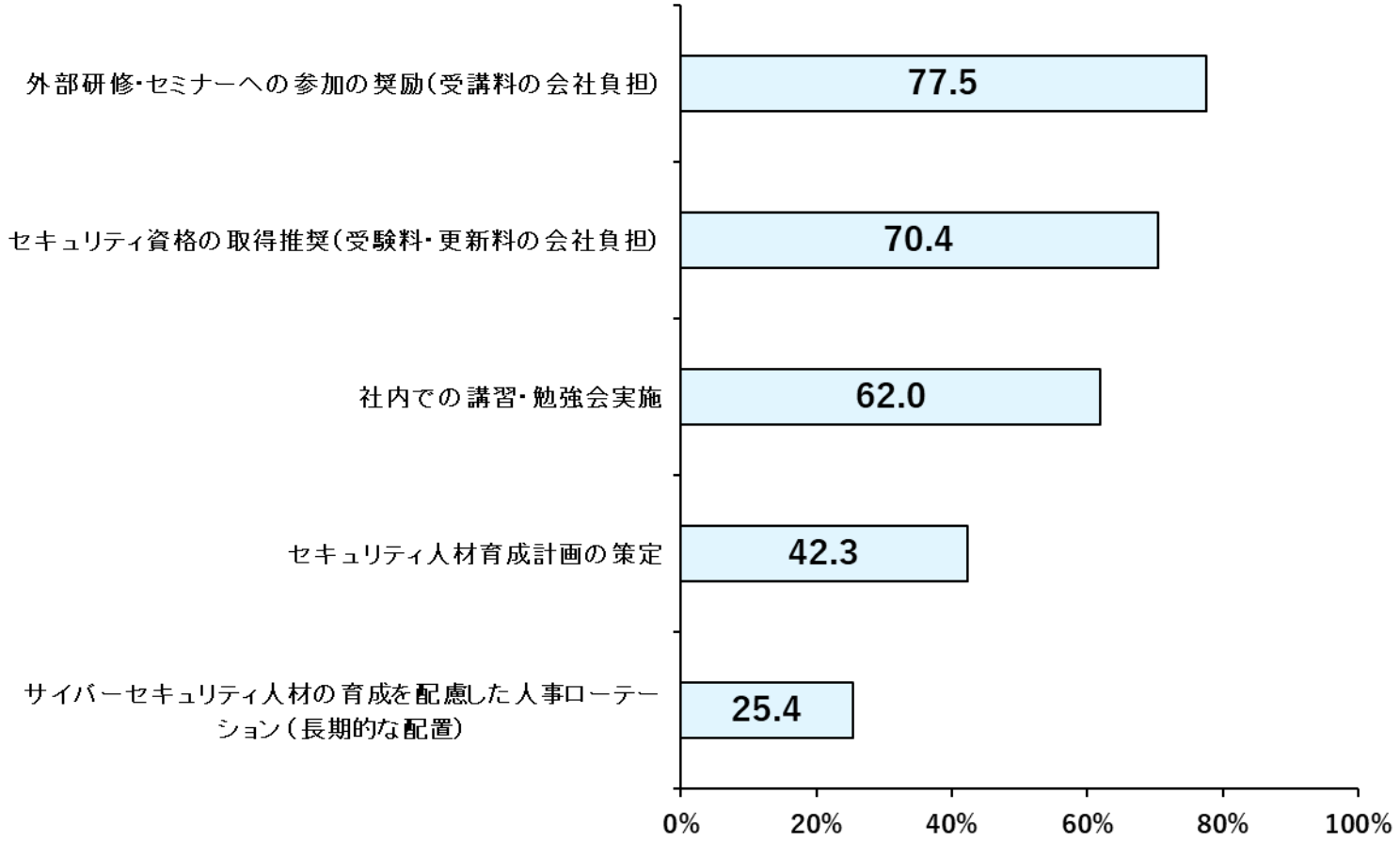
図表8　機能別にみたサイバーセキュリティ人材の確保状況



集計結果の概要　サイバーセキュリティ人材の育成

- ✓ サイバーセキュリティ人材の不足が続くことが見込まれるため、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・育成に取り組むことが重要である。
- ✓ 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セキュリティ資格の取得推奨、社内での講習・勉強会の実施といった短期的な取組が中心となっており、人材育成計画の策定などの中長期的な取組は限定的となっている。

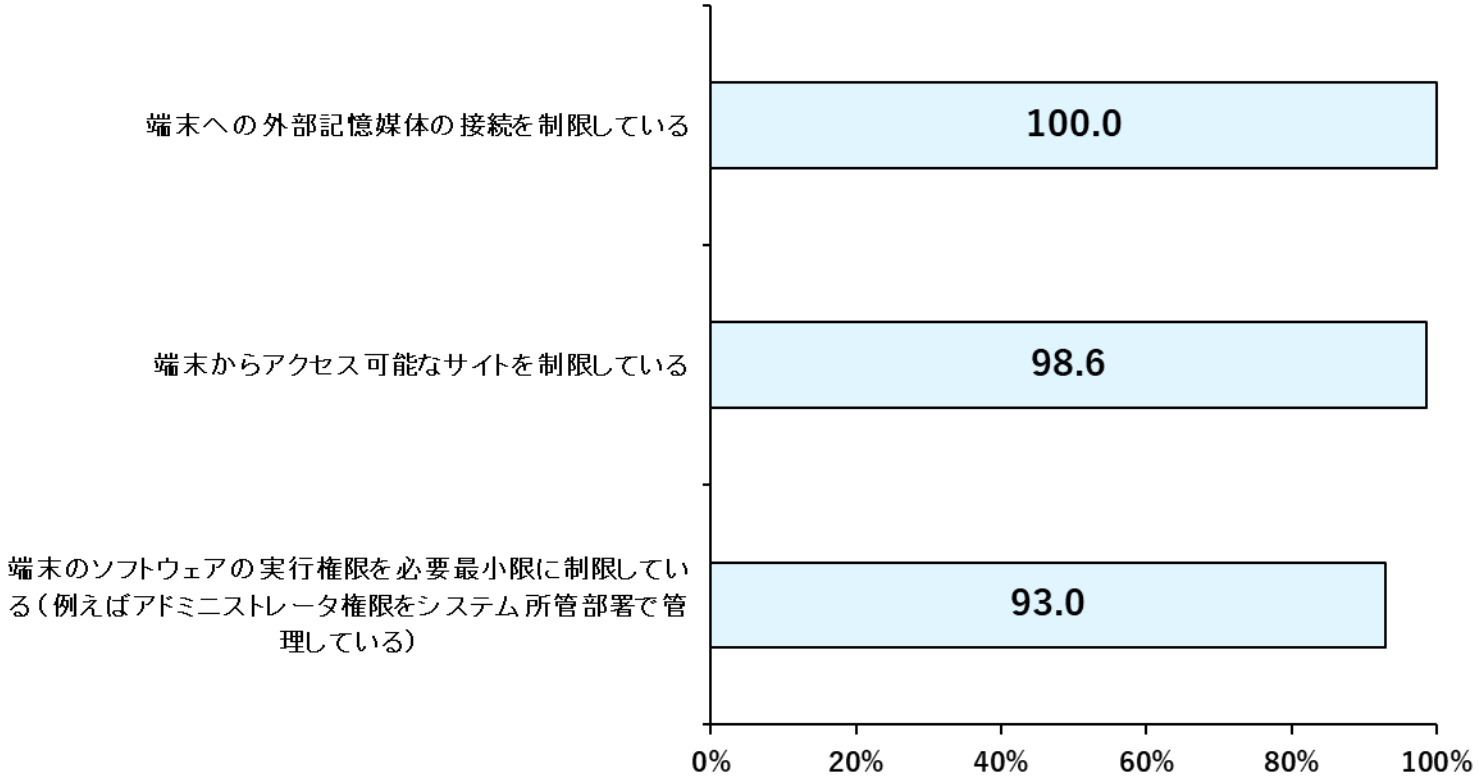
図表9　人材育成の取組



集計結果の概要　OA端末における対策

- ✓ OA端末（※）が、未知のマルウェアに感染したり、脆弱性を突かれて攻撃者に侵入されたりする可能性は完全に排除できないという前提のもと、対策を講じる必要がある。
- ✓ OA端末のサイバー攻撃対策に関して、外部記憶媒体の接続制限、アクセス可能なサイトの制限、ソフトウェアの実行権限の制限といった対策が9割以上の先で実施されている。

図表10　導入しているOA端末のサイバー攻撃対策

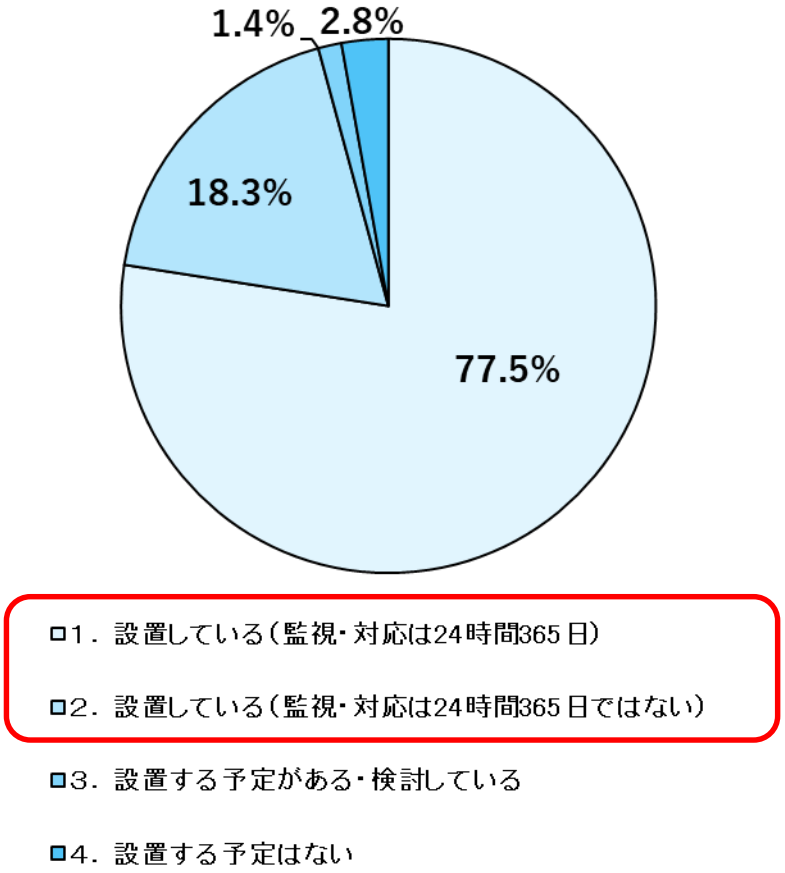


※今回のCSSAにおける「OA端末」とは、「職員が文書作成等で標準的に用いる端末」と定義。

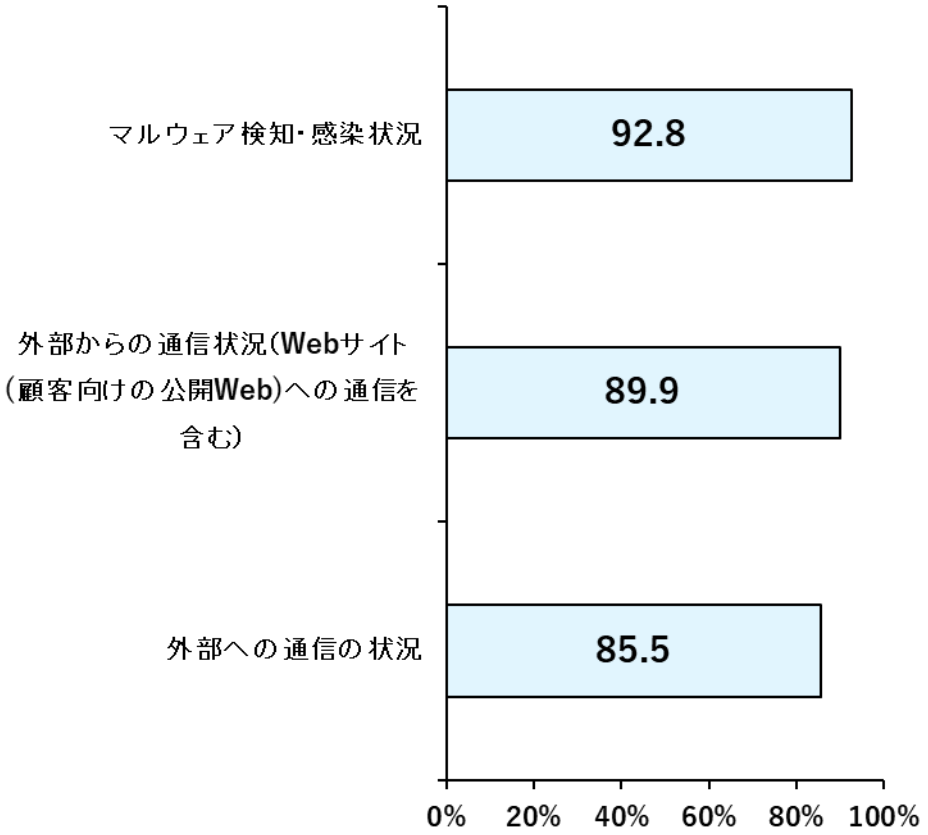
集計結果の概要　サイバーインシデントの監視・分析等の態勢

✓ セキュリティ関連の監視・分析等を行う組織（SOC*等）を設置しているのは9割強（図表11）。また、9割程度の先がマルウェア検知・感染状況や外部との通信状況をモニタリング対象としている（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。

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



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

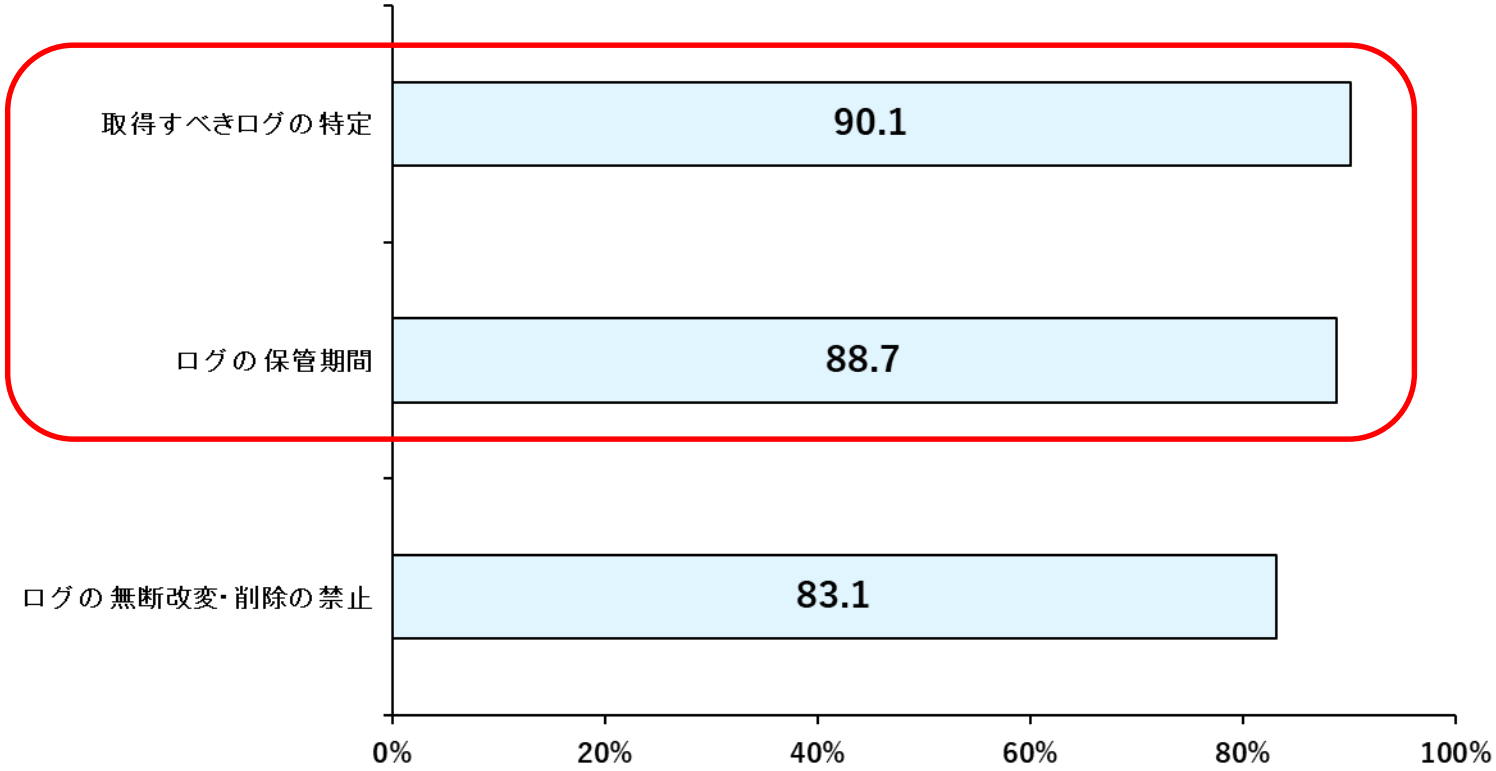


*Security Operation Centerの略。ネットワークやサーバ、ファイアウォール等の機器への攻撃状況など、セキュリティ関連の監視・分析等を行う組織。

集計結果の概要　システムのログについての規定

- ✓ システムのログは、インシデントの検知やインシデントの影響範囲の調査および復旧対応の検討にあたって必要不可欠であるため、ログの正確性や網羅性を担保することが重要である。
- ✓ 多くの保険会社において、取得すべきログの特定、ログの保管期間についてルール・手順を定めていることがうかがえる。

図表13　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

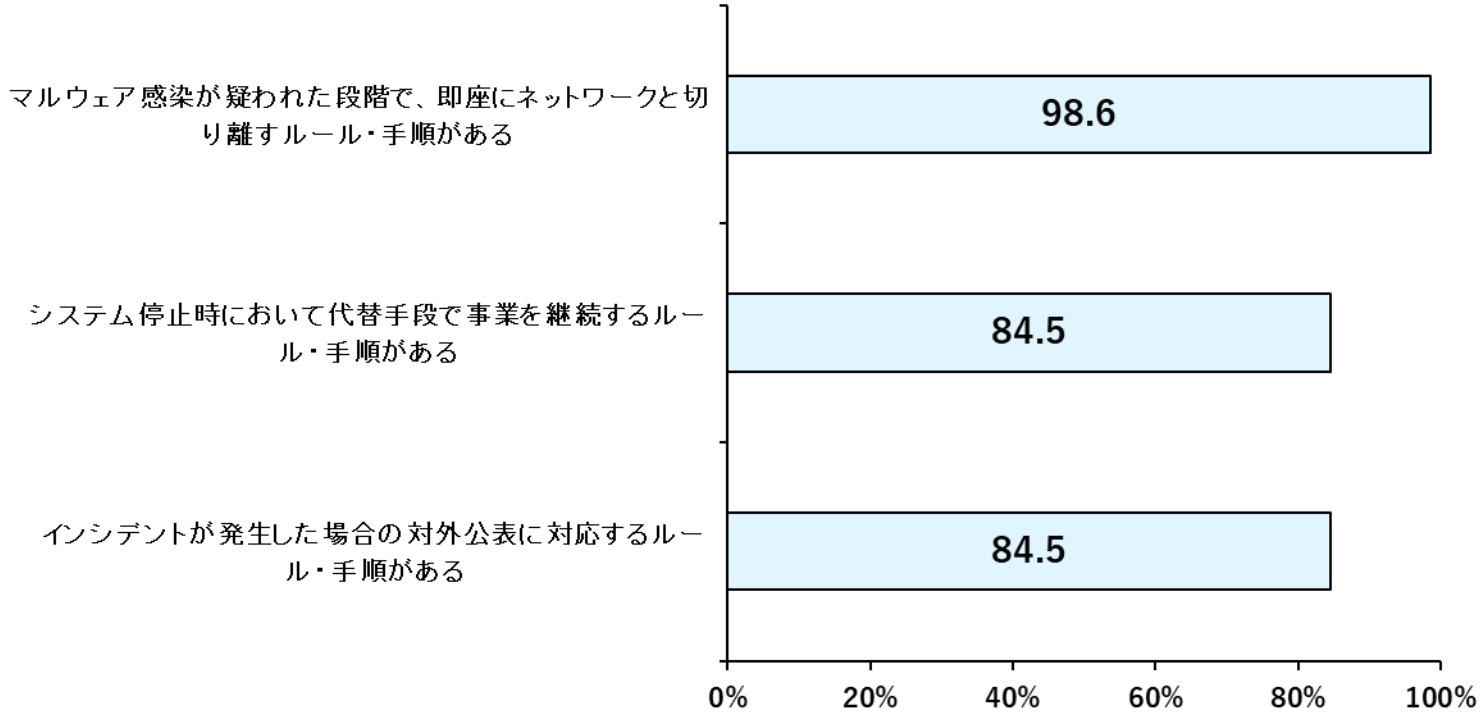


※「ルール・手順を定めており、対策の実施状況をモニタリングしている」、「ルール・手順を定めている」と回答した先を集計

集計結果の概要　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、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り、そのための態勢構築が必要である。
- ✓ 多くの保険会社が、マルウェア感染が疑われた段階で即座にネットワークと切り離したり、代替手段で業務を継続したり、インシデントが発生した場合に対外公表したりすることに関するルール・手順を定めている。

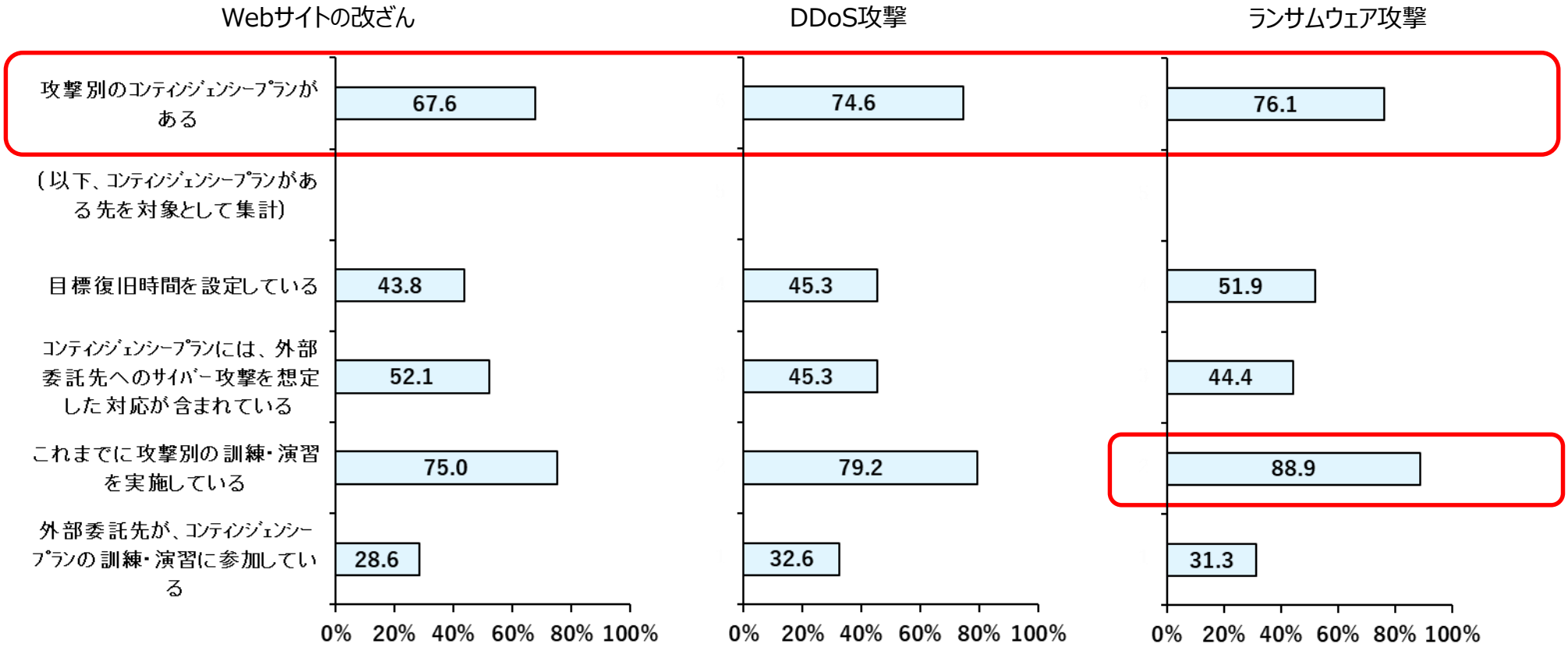
図表14　被害拡大防止のためのルール・手順の整備状況



集計結果の概要　コンティンジェンシープランの策定、訓練・演習の実施

- ✓ サイバー攻撃を受けた際、適切に対応・復旧ができるように、サイバー攻撃の種類別にコンティンジェンシープランを設定することが望ましい。図表15に示すように、それぞれのサイバー攻撃の類型に関するコンティンジェンシープランを整備していない保険会社が一定数存在する。
- ✓ 訓練や演習により、コンティンジェンシープランの有効性を確認することが重要である。ランサムウェア攻撃に関しては、コンティンジェンシープランを策定している保険会社の9割近くが、訓練や演習を実施している。
- ✓ 外部委託先が攻撃を受け自組織に影響が及ぶ可能性を想定することや、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を設定するなど、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。

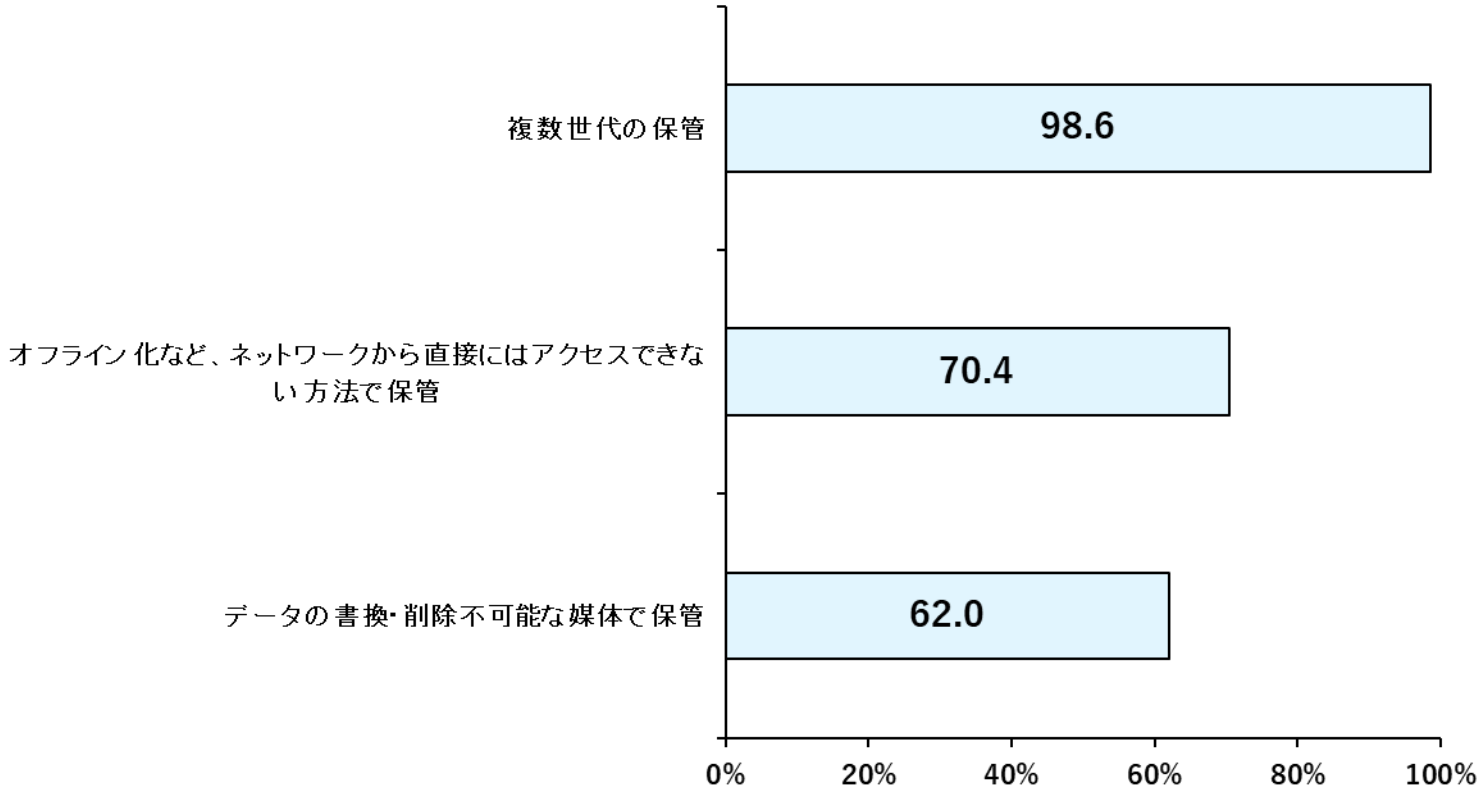
図表15　サイバー攻撃（被害）に対応するコンティンジェンシープランおよび取組内容



集計結果の概要　バックアップデータの保護

- ✓ データが破壊された場合に、バックアップデータを用いてシステムを復旧し、早期に業務を再開できるように対策を講じておくことが重要である。
- ✓ データ保管の対策状況に関して、多くの保険会社が複数世代の保管を実施している。また、ネットワークから直接にはアクセスできない方法で保管を実施している先や、データの書換・削除不可能な媒体で保管している先も一定数存在した。

図表16　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



※「ルール・手順を定めており、対策の実施状況をモニタリングしている」、「ルール・手順を定めている」と回答した先を集計

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み、サイバー空間での活動が増大するなかで、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。

- ✓ 多くの保険会社では、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組を進めているが、重要なサードパーティのリスク管理や人材確保・育成、コンティンジェンシープランの整備で改善の余地があることが読み取れる。

- ✓ こうした状況を踏まえ、本取組は、環境変化を踏まえ、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。

- ✓ 金融庁としては、保険会社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組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、そうした取組を後押ししていく方針である。