令和３年度サイバー･フィジカル･セキュリティ対策促進事業
（サイバーセキュリティ経営に関する調査）

調査報告書

2022年3月

みずほリサーチ＆テクノロジーズ株式会社

目 次

1. 調査実施の目的、実施内容等

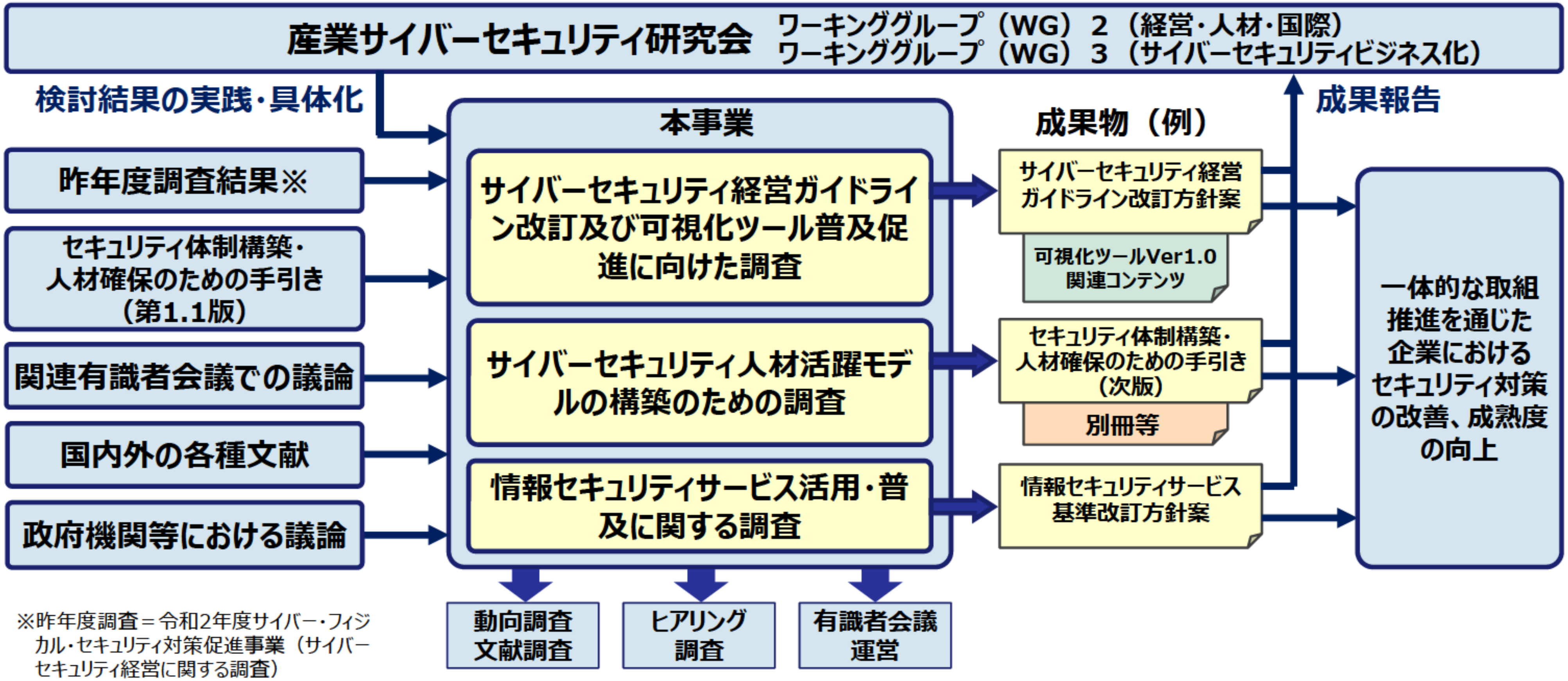
(1) 調査目的

- 経済産業省では、産業サイバーセキュリティ研究会 ワーキンググループ２（経営・人材・国際）（以下、「WG2」という。）において、段階的なサイバーセキュリティ経営の実現に向けた取組や、企業におけるセキュリティ人材の活躍モデルの提示、各地域でのセキュリティコミュニティ形成に向けた取組を進めている。
- これらの取組は相互に関連しており、セキュリティ経営の実現に向けてはセキュリティ人材の活躍が必要であり、また、セキュリティ人材不足に悩むユーザ企業においてはセキュリティ対策の一部をアウトソースする必要があり、情報セキュリティサービスの普及を促進し、ユーザ企業が情報セキュリティサービスを安心して活用することができる環境を醸成することが必要である。
- これらの取組を一体的に進めていくため、本事業（令和３年度サイバー・フィジカル・セキュリティ対策促進事業（サイバーセキュリティ経営に関する調査）では以下の事項についての調査を実施した。
  - サイバーセキュリティ経営の可視化ツールの開発に向けた調査
  - サイバーセキュリティ人材活躍モデルの構築のための調査
  - 情報セキュリティサービス活用・普及に関する調査

1. 調査実施の目的、実施内容等

(2) 調査の実施方針

- 前ページに示した調査目的を踏まえ、主にユーザ企業における適切なサイバーセキュリティ対策の実現を支援するため、受託者（みずほリサーチ＆テクノロジーズ株式会社）及び再委託先がこれまで関連事業の実践を通じて得た知見やネットワークを活用しつつ、本事業における３種類の調査を効率的かつ実効的に実施することで、最大限の事業成果を得て、WG2/3における今後の取組に資するように務めた。



※昨年度調査＝令和2年度サイバー・フィジカル・セキュリティ対策促進事業（サイバーセキュリティ経営に関する調査）

図1.1　調査の実施方針

1. 調査実施の目的、実施内容等

(3) 実施内容

- (1)(2)を踏まえ、本事業で実施した調査は次表の通りである。調査結果の詳細を本報告書第2章以降で示す。

表1.1　調査実施内容

調査項目（大項目）	調査項目（小項目）	実施内容
1. サイバーセキュリティ経営ガイドライン改訂及び可視化ツール普及促進に向けた調査	1.1 経営ガイドラインの改訂に向けた調査と改訂方針案の作成	● サイバー・フィジカル・セキュリティ対策フレームワーク（以下、「CPSF」という。）ほか、経済産業省との協議のもとに定めた調査対象について、最新の動向調査を実施した。 ● サイバーセキュリティ経営ガイドライン（以下、「経営ガイドライン」という。）Ver.2.0本文（英訳版を含む）について、改訂の必要性についての検討を行うとともに、改訂素案をとりまとめた。 ● 経営ガイドライン付録Aについてはサイバーセキュリティ経営可視化ツール（以下、「可視化ツール」という。）の質問項目に合わせた形での修正を実施した。
	1.2 企業調査	● ユーザ系企業10社、ベンダ系企業3社を対象に、経営ガイドラインへの意見や改訂版に盛り込むべき事項等について調査を実施した。
	1.3 機関投資家へのヒアリング調査	● サイバーセキュリティやリスクマネジメント、ESG等について企業を評価、投資判断当行ったことがあり、見解を持つ機関投資家又はその団体8者に対し、企業を評価する際に見る項目、サイバーセキュリティに関して見る内容、企業をサイバーセキュリティの観点で評価するときに参考にするガイドライン等及び課題等について調査を実施した。
	1.4 海外動向調査	● 海外企業8社及び対照群としてそれぞれの同業種の国内企業7社を対象に、企業が開示しているサイバーセキュリティに関する情報に関する取組事例と動向について整理した。
	1.5 有識者会議の開催	● 企業のサイバーセキュリティ対策に知見を有する6名の有識者によるタスクフォースを設置し、9回にわたる開催にあたっての事務局運営を担当した。

1. 調査実施の目的、実施内容等

(3) 実施内容（続き）

調査項目（大項目）	調査項目（小項目）	実施内容
2. サイバーセキュリティ人材活躍モデルの構築のための調査	2.1 企業調査	● ユーザ系企業10社、ベンダ系企業3社を対象に、サプライチェーンのセキュリティ対策に向けた体制構築、最新の動向を踏まえた体制構築の変化・社内でセキュリティ対策に取り組む人材のキャリア事例やその背景、OT/IoT分野のセキュリティ体制や人材の実態、「セキュリティ体制構築・人材確保のための手引き」（以下、「手引き」という。）第1.1版の活用方法や改善に関する意見等について調査を実施した。 ● うちユーザ系企業については可視化ツールを用いて企業のセキュリティ成熟度を評価した。
	2.2 有識者ヒアリング	● サイバーセキュリティの業界動向に詳しい有識者10名に対し、セキュリティ人材確保・体制構築に関して求められる政策等についてヒアリングを実施した。
	2.3 有識者会議の開催	● 企業のサイバーセキュリティ対策に知見を有する6名の有識者によるタスクフォースを設置し、9回にわたる開催にあたっての事務局運営を担当した。
	2.4 文献調査	● 国内外のサイバーセキュリティ人材育成に関する文献の調査を行った。
	2.5 政府機関等における議論の把握	● 産業サイバーセキュリティ研究会を中心に議論の把握を行った。
	2.6「セキュリティ体制構築・人材確保のための手引き（第1.1版）」の内容拡充・改善及び普及啓発	● 有識者会議における議論、及び企業調査、有識者ヒアリング調査結果をもとに、改訂版の公表に向けたコンテンツ案を作成した。
	2.7 政策的課題の洗い出し及び施策の検討	● 企業におけるDX推進等の動きの中で、ユーザ企業とベンダ企業の区分、プラス・セキュリティの重要度の高まりの結果、セキュリティ対策を担う人材のとらえ方を見直す必要がある点について検討を行った。

1. 調査実施の目的、実施内容等

(3) 実施内容（続き）

調査項目（大項目）	調査項目（小項目）	実施内容
3. 情報セキュリティサービス活用・普及に関する調査	3.1 有識者会議の開催	● 情報セキュリティサービスに関する有識者10名で構成される検討会を設置し、3回にわたって情報セキュリティサービス審査登録制度の活用・普及に関する議論を行うにあたっての事務局運営を担当した。 ● 本調査の期間中に実施した情報セキュリティサービス基準等の改訂に関する審議及びパブリックコメントに寄せられた意見に対する審議についての事務局運営を担当した。
	3.2 情報セキュリティサービス基準等の改訂支援	● 有識者会議における議論をもとに、情報セキュリティサービス基準及び情報セキュリティサービスに関する審査登録機関基準の改訂案、並びに情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示案をとりまとめた。
4. 報告書の作成	報告書の作成	● 1～3の調査結果をもとに、本報告書を作成した。

2. サイバーセキュリティ経営ガイドライン改訂及び可視化ツール普及促進に向けた調査

2.1 経営ガイドラインの改訂に向けた調査と改訂方針案の作成

(1) 動向調査

- 調査趣旨を踏まえ、経営ガイドラインVer.2.0公表以降に社会や技術で生じた変化を反映したフレームワークやガイドライン等の文書から、改訂作業において反映すべき同項の変化を明らかにした。

(2) サイバーセキュリティ経営ガイドラインの見直し方針の検討

- (1)の動向調査結果等を踏まえ、現行ガイドラインの構成毎に見直し方針を作成し、有識者会議における議論に用いた。

(3) サイバーセキュリティ経営ガイドラインの改訂素案の作成

- 有識者会議における審議をもとに、改訂素案を作成した。

2.2 企業調査

- 本事業における企業調査は、3.1における企業調査と併せて実施したため、本項にて両者の調査結果をまとめて示す。

2.2.1 ユーザ系企業調査

(1) 対象企業

- JUAS情報セキュリティWG参加企業を中心に、調査項目に照らして適切と考えられるユーザー企業10社とする。
- 可能な限りサイバーセキュリティの成熟度、業種・業態の違いが明らかになるよう抽出する。

(2) 調査項目

- 調査項目については以下の項目を基本とし、みずほリサーチ＆テクノロジーズ株式会社及び経済産業省サイバーセキュリティ課と協議の上で決定した。
  - サイバーセキュリティ経営ガイドラインVer.2.0に対する意見や改訂版に盛り込むべき事項
  - 経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」（令和2年12月18日）等に対する意見やこれらを踏まえた取組状況
  - サプライチェーン（取引先や海外拠点）のセキュリティ対策に向けた体制構築
  - 最新の動向を踏まえた体制構築の変化・社内のセキュリティ人材やプラス・セキュリティ人材のキャリアパス事例やその背景
  - OT/IoT分野のセキュリティに関する体制や人材の役割定義の実態・課題
  - 「サイバーセキュリティ体制構築・人材確保の手引き（第1.1版）」の活用方法や改善に向けた意見
- なお、サイバーセキュリティの成熟度、業種・業態により一部項目をヒアリング対象外としている場合がある。

2.2.1 ユーザ系企業調査

(3) 調査方法

- ヒアリングの事前調査として、調査項目に関連した各社のセキュリティ対策実施状況に関するアンケート調査、およびサーバーセキュリティ経営可視化ツールによる成熟度調査を実施した。
- ヒアリング調査はWeb形式の個別インタビュー形式、或いはクローズドのグループインタビュー形式を基本として実施した。但し、グループインタビュー形式であっても参加者は最大3社程度である。

(4) ヒアリング対象企業の選出

- JUAS情報セキュリティWG参加企業より、調査項目に照らして適切と考えられるユーザー企業10社を選出。

2.2.1 ユーザ系企業調査

(5) 調査項目

① 事前アンケート調査

- ヒアリングの事前調査として、調査項目に関連した各社の実施状況に関するアンケート調査を行った。
  - ①　サイバーセキュリティ経営ガイドラインVer.2.0の活用状況と改定の必要性
  - ②　経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」に対する取組状況
  - ③　グループ・グローバル関連会社およびサプライチェーン（取引先）のセキュリティ対策実施状況把握
  - ④　コロナ禍を経たセキュリティ体制や対策の変化
  - ⑤　社内のセキュリティ人材やプラス・セキュリティ人材の育成計画の有無、キャリアパスの有無
  - ⑥　「サイバーセキュリティ体制構築・人材確保の手引き（第1.1版）」の活用状況

② サイバーセキュリティ経営可視化ツールによる成熟度調査

- ヒアリング対象企業のサイバーセキュリティ成熟度を以下の手順で把握する。
  - ➢ 「サーバーセキュリティ経営可視化ツール」を用いて各社のサイバーセキュリティ実施状況を評価してもらう。
  - ➢ 上記結果をもとに各社のサイバーセキュリティ成熟度を評価する。成熟度はJUASが令和2年度に実施した「サイバーセキュリティ経営に関する調査」における次の成熟度評価基準をベースとする

＜成熟度評価基準＞

成熟度C（低）：指示の平均値3未満が6個以上
成熟度B（中）：指示の平均値3以上が過半数（5個以上）、または平均値3未満あっても平均値4以上が4個以上ある場合
成熟度A（高）：平均値3未満がなく、かつ平均値4以上が4個以上

2.2.1 ユーザ系企業調査

③ ヒアリング調査

- 調査は主に経済産業省、IPAにおけるサイバーセキュリティ関連施策への取組み状況と改善要望、および最新の状況を踏まえた各社におけるサイバーセキュリティへの取組状況をインタビュー形式で調査した。
  1. 経済産業省、IPAにおけるサイバーセキュリティ関連施策への取組状況と改善要望
     - i. サイバーセキュリティ経営ガイドラインV2.0に対する意見や改訂版に盛り込むべき事項
     - ii. 経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」に対する意見や取組状況
     - iii. 「サイバーセキュリティ体制構築・人材確保の手引き（第1.1版）」の活用方法や改善に向けた意見
  2. 最新の状況を踏まえた各社におけるサイバーセキュリティへの取組状況
     - i. セキュリティ体制や施策に変化があったかとその具体的内容
     - ii. セキュリティ人材やプラス・セキュリティ人材の育成方法とキャリアパス事例
     - iii. グループ・グローバル関連会社のセキュリティ対策実施状況把握方法と実行体制
     - iv. サプライチェーン（取引先）のセキュリティ対策実施状況把握方法と実行体制
     - v. ＯＴ/ＩｏＴ分野のセキュリティに関する体制や人材の役割定義の実態・課題

④ スケジュール

- ①のアンケート調査：2021年10月後半に実施
- ②の成熟度調査及び③のヒアリング調査：2021年11月～12月に実施

2.2.1 ユーザ系企業調査

(6) 事前アンケート調査結果

- 回答企業の業種グループ
  - 製造業が6社、金融業が2社、通信業が1社、ガス供給業が1社

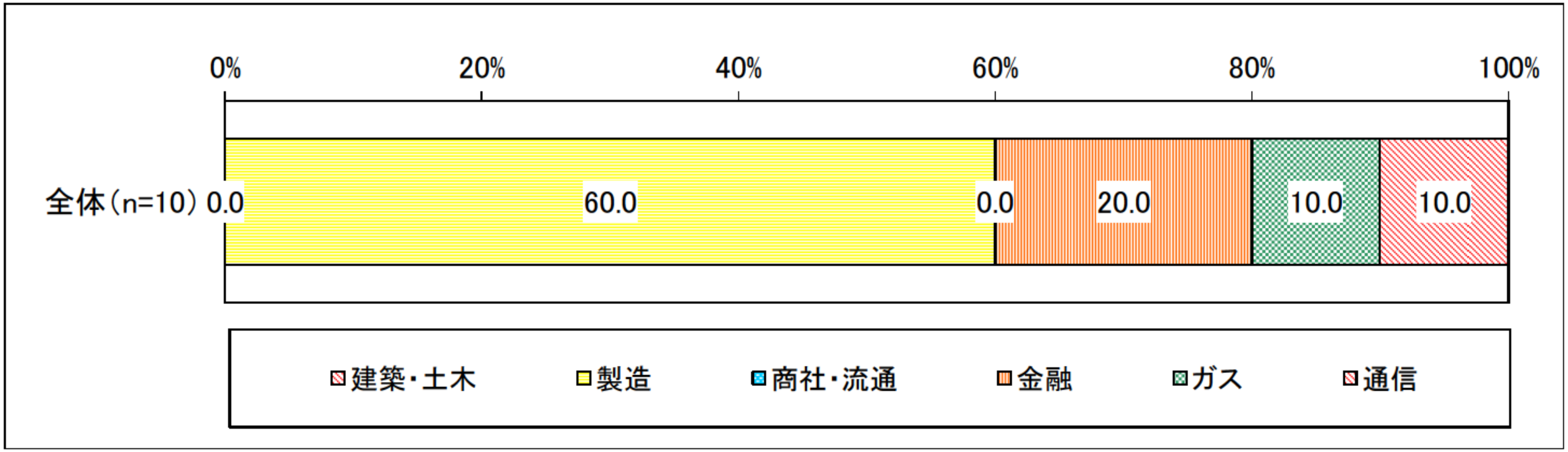


図2.1　回答企業の業種グループ

2.2.1 ユーザ系企業調査

(6) 事前アンケート調査結果

- 回答者の属性
  - 情報セキュリティ統括担当者（専任）が約4割
  - 情報セキュリティ担当者（兼任）が約4割

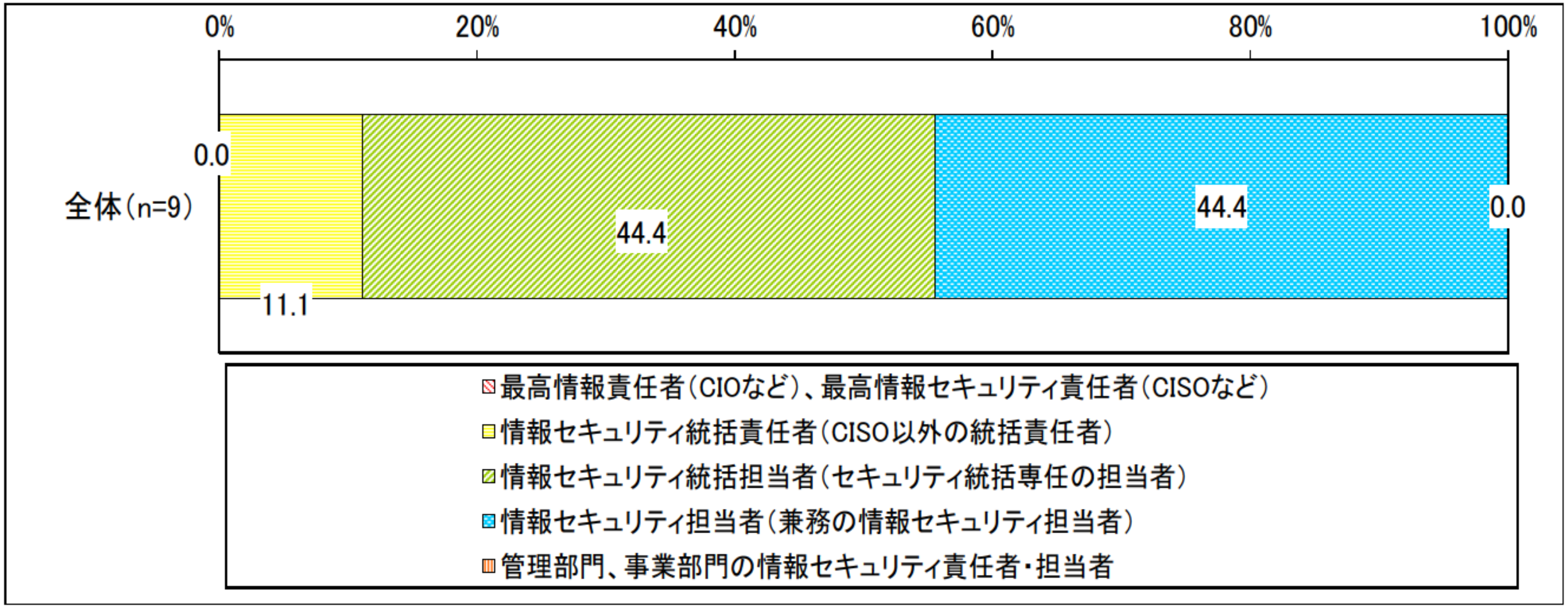


図2.2 回答者の属性

Q3-Q15の調査結果については2.2.1(8)ヒアリング調査結果に合わせて説明する。

2.2.1 ユーザ系企業調査

(7) サイバーセキュリティ経営可視化ツールによる成熟度調査結果

- 成熟度高が2社（いずれも金融業）、成熟度中が5社、成熟度低が2社（いずれも製造業）

表2.1　サイバーセキュリティ経営可視化ツールによる成熟度調査結果（対象企業9社）

会社記号	業種グループ	指示1の平均	指示2の平均	指示3の平均	指示4の平均	指示5の平均	指示6の平均	指示7の平均	指示8の平均	指示9の平均	指示10の平均	成熟度低	成熟度中	成熟度高
K-1	金融・保険業	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	0	0	1
I-1	通信業・放送業・ISP・	4.0	4.7	3.3	3.7	3.8	2.8	3.4	2.5	3.0	3.0	0	1	0
S-1	製造業	3.7	3.7	3.8	3.7	3.8	2.8	3.6	3.0	2.3	3.0	0	1	0
S-2	製造業	4.0	3.0	3.8	3.7	3.5	3.5	3.4	1.5	1.7	3.5	0	1	0
S-3	製造業	2.0	2.3	1.5	1.3	2.5	1.3	1.2	1.0	1.3	1.5	1	0	0
S-4	製造業	4.7	4.0	4.3	4.3	4.8	3.5	4.8	5.0	2.7	5.0	0	1	0
K-2	金融・保険業	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	4.3	5.0	0	0	1
C-1	電力・ガス・熱供給業・	3.7	3.3	2.3	3.7	4.1	3.5	3.0	3.0	2.3	3.0	0	1	0
S-5	製造業	2.7	3.0	2.5	2.0	3.3	1.0	1.8	1.0	1.7	1.5	1	0	0

2.2.1 ユーザ系企業調査

(8) ヒアリング調査調査

① サイバーセキュリティ経営ガイドラインVer.2.0の活用状況

- ルール、規定などをチェックし必要に応じて改訂している企業が1/3
- 一方、ガイドラインを活用していない企業も1/3

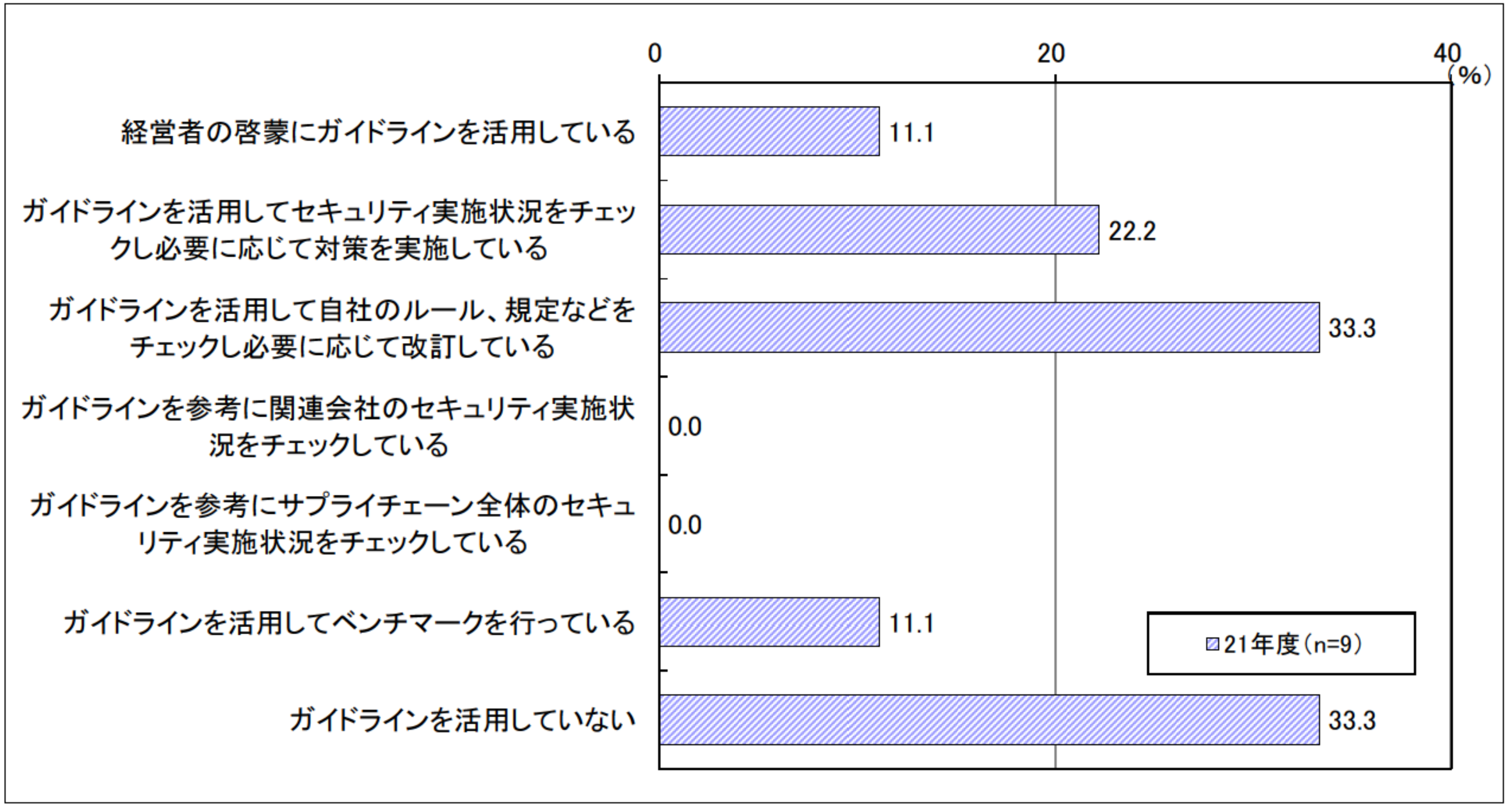


図2.3 事前アンケート調査結果（サイバーセキュリティ経営ガイドラインVer.2.0の活用状況）

2.2.1 ユーザ系企業調査

(8) ヒアリング調査調査

① サイバーセキュリティ経営ガイドラインVer.2.0の活用状況

＜活用方法＞

- ガイドラインの認知度は高く、施策や規定類の抜け漏れチェックやCISOの役割設定などに活用されている。
- セキュリティ統括部門の立ち上げや年間計画/5か年計画の作成時や経営会議での報告時にも活用されている。
- 成熟度低の企業では最近になってガイドラインを活用してセキュリティ対策をアセスしている。
- 経営層に説明する際に経産省のガイドラインで確認していることで納得が得られる（説得力がある）。
- 経営層に理解してもらうためにガイドラインを活用。

＜経営者の意識、認識＞

- 経営者にはリスクや経営への影響を認識してもらえば良く、技術的内容まで理解してもらう必要はない。
- セキュリティは専門性が高く、経営者がリーダーシップを発揮するのは難しいのではないか。
- 成熟度低の企業では経営者の意識を変えたい、セキュリティの重要性を認識してもらたいと考えているができていない。

＜経営への報告＞

- 経営者には定期的にリスク管理委員会からセキュリティの状況を報告。
- 経営者はセキュリティの重要性を認識しており、関係性も良いので予算や人の確保もできている。

2.2.1 ユーザ系企業調査

(8) ヒアリング調査調査

① サイバーセキュリティ経営ガイドラインVer.2.0の活用状況

＜活用していない理由＞

- ガイドラインはセキュリティ対策が進んでいる企業では有効ではない。
- セキュリティ施策は企業文化により異なるので、ベーシックな内容では活用しづらい。

＜可視化ツール＞

- 可視化ツールを使って実施状況を評価し経営会議に報告している。
- レーダーチャートで到達点を決め現状を評価することが有効。

＜他のガイドラインの参照先として活用＞

- 管轄省庁のガイドラインを参照しているが、このガイドランは経営ガイドラインを踏まえていると認識している。
- ベンダーの診断サービスで経営ガイドラインを参照した評価ができるようになっている。

2.2.1 ユーザ系企業調査

② サイバーセキュリティ経営ガイドラインVer.2.0の改訂について

- 特に改訂の必要はないが約45%
- ガイドラインを活用していない企業は分からないと回答（全体の1/3）

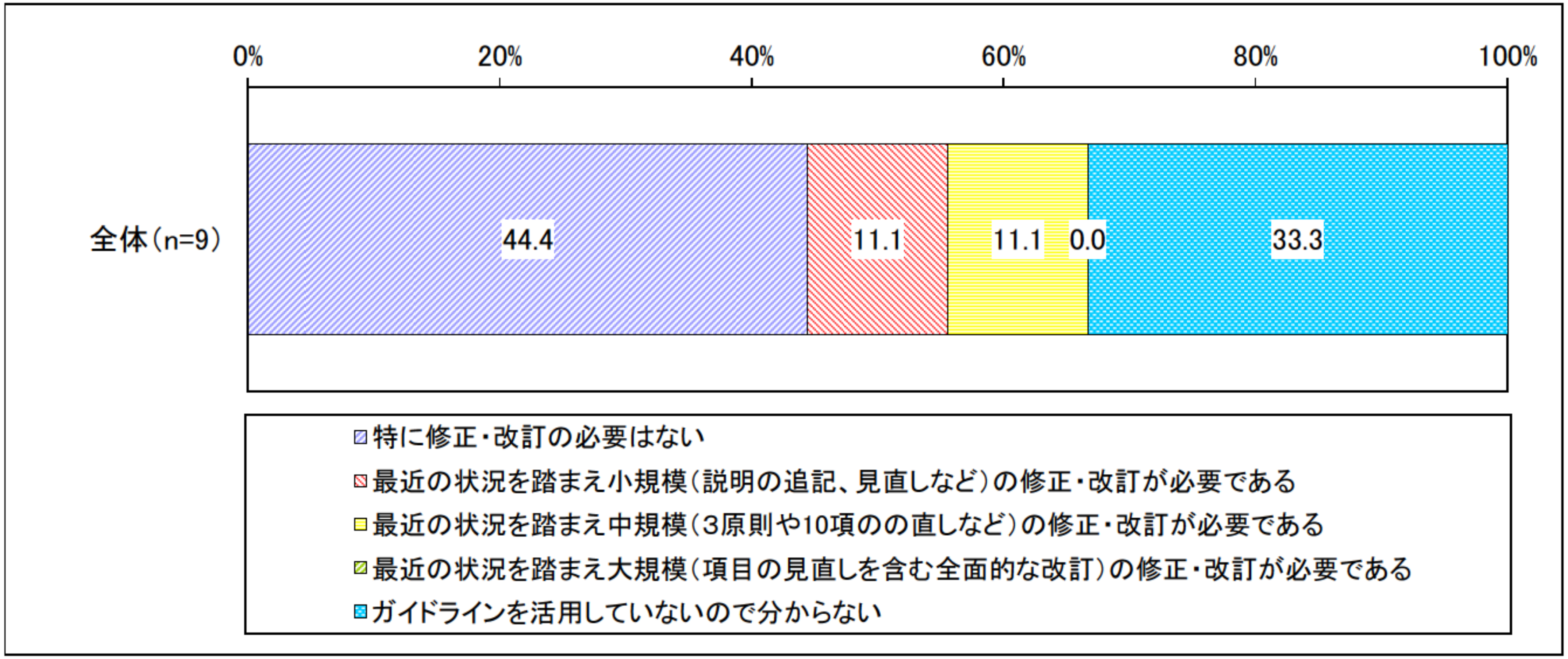


図2.4　事前アンケート調査結果（サイバーセキュリティ経営ガイドラインVer.2.0の改訂について）

2.2.1 ユーザ系企業調査

② サイバーセキュリティ経営ガイドラインVer.2.0の改訂について

＜改訂に対する意見＞

- 攻撃者から支払いを求められたときの対処方法をガイドしてほしい。
- リスクベースアプローチ、残存リスクに対する具体的アプローチ。
- CISOの役割とか必要となる能力について提言してほしい。
- 現実と対比して分かりにくい部分や、同様の記述があるので見直してほしい。
- 定量的に脅威を可視化して把握することを盛り込んでほしい。

＜改訂の必要ない＞

- 成熟度高の企業ではガイドラインはベーシックなものと認識しており、改訂の必要はないと考えている。
- ガイドラインは経営層向けであり、DX関連の動向で見直す必要はない。

2.2.1 ユーザ系企業調査

③「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」に対する取組状況

- 注意喚起を踏まえてセキュリティ対策状況をチェックし必要な対策を実施している企業が1/3、関連会社やサプライチェーンまで展開している企業もある。
- 特に対応していない企業が約45%

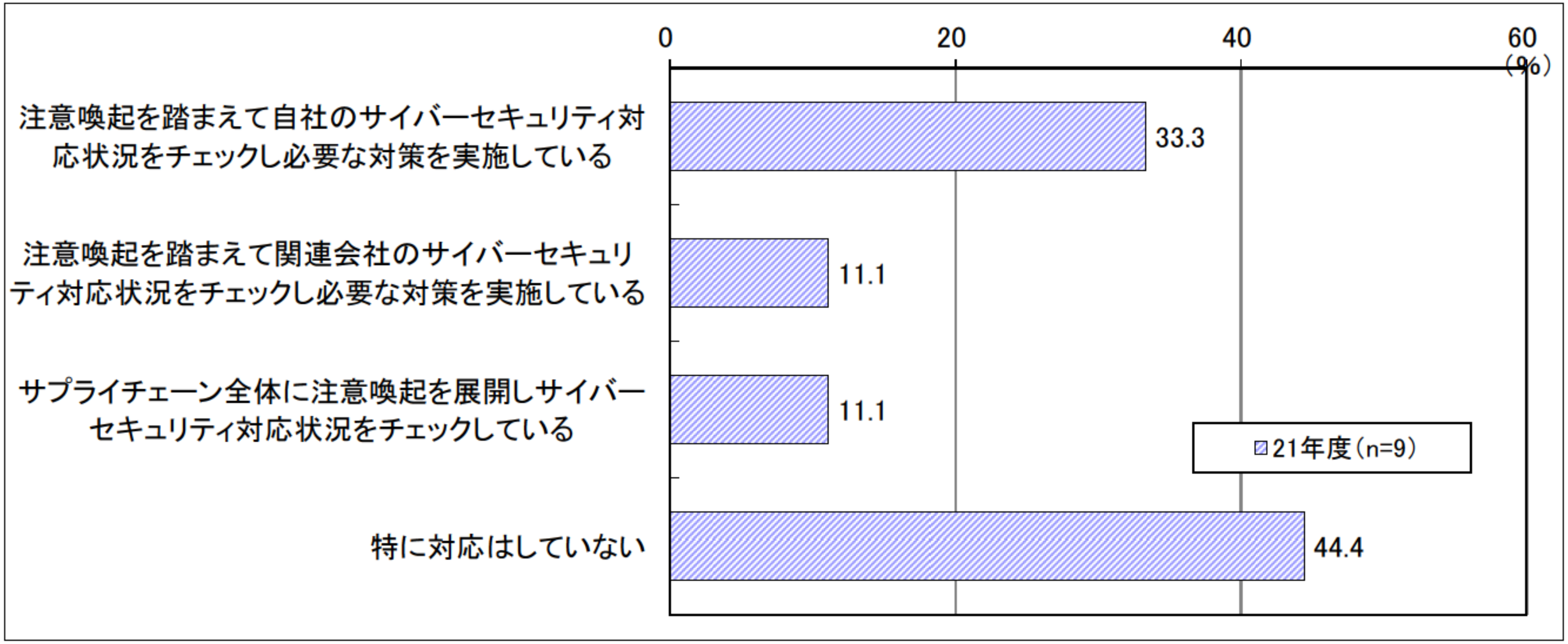


図2.5 事前アンケート調査結果（「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」に対する取組状況）

2.2.1 ユーザ系企業調査

③「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」に対する取組状況

＜注意喚起を利用している＞

- 注意喚起はタイムリーであり、分かり易くまとめられており使いやすい。
- 経営層には直接またはサイバーセキュリティ委員会から報告している。

＜注意喚起を利用していない＞

- 注意喚起はベーシックな内容なので参考にならないし、経営者にはこの手の情報は必要ないのではないか。
- CISOには定期的に報告しているので注意喚起を見ることはない。

＜注意喚起への意見＞

- 決算遅延、業務停止、取引停止など経営に影響があるものを中心に具体的に記載してもらうと経営者がイメージしやすく刺さる資料になる。
- 今回の注意喚起はスピード感が感じられない。

＜情報入手ルート＞

- インシデント情報の入手先は、IPA、JPCERT、NISC、ISAC、警察、Web、有識者、セミナー、ベンダーなど様々。
- セキュリティ関連情報は統括部門（HD、CSIRTなど）で収集し、連絡会で関連会社も含めて注意喚起している。

＜セキュリティ意識向上、グループ会社への展開＞

- 今回の注意喚起が出たからという事ではなく、いこいろな形で関連会社には注意喚起を行ったり、実施状況をチェックしたりしている。

2.2.1 ユーザ系企業調査

④「サイバーセキュリティ体制構築・人材確保の手引き（第1.1版）」の活用状況

- 手引きは知っているが活用していないが約45%、手引きを知らないが1/3。
- 手引きを参考にしているのは約2割に留まる。

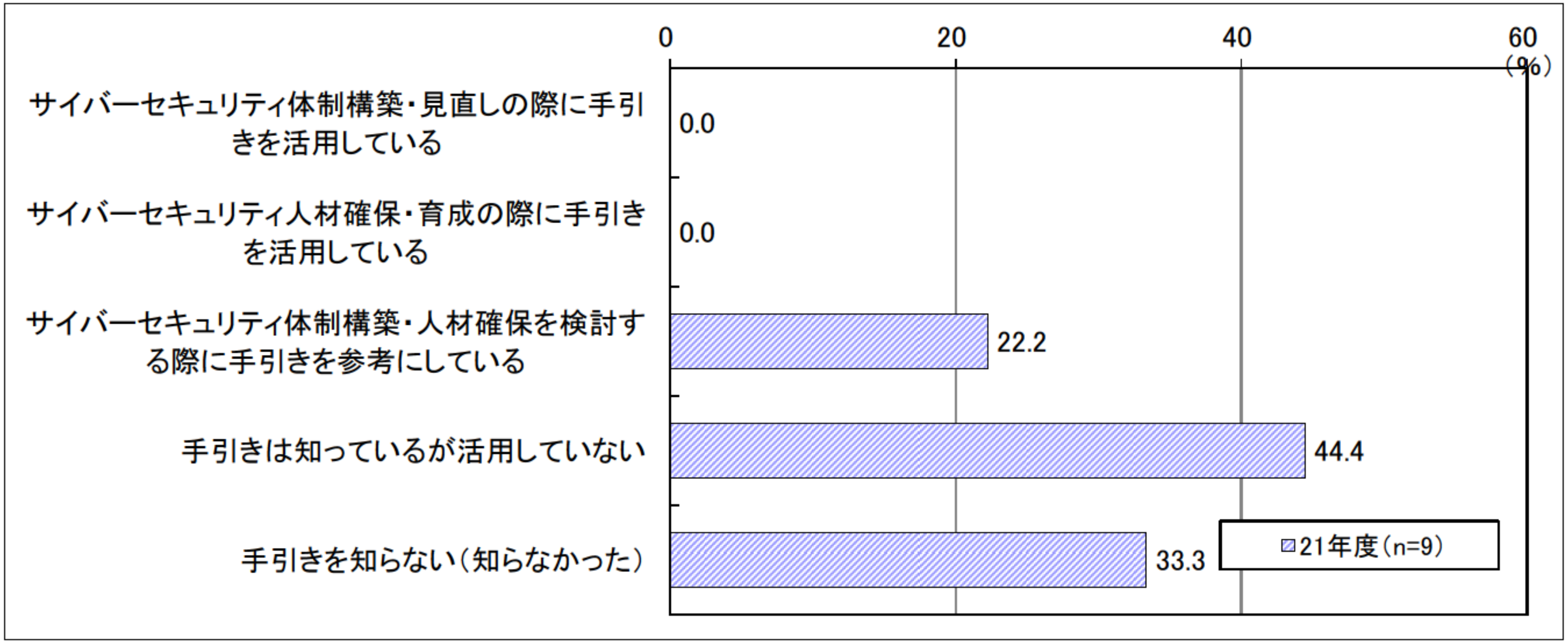


図2.6 事前アンケート調査結果（「サイバーセキュリティ体制構築・人材確保の手引き（第1.1版）」の活用状況）

2.2.1 ユーザ系企業調査

④「サイバーセキュリティ体制構築・人材確保の手引き（第1.1版）」の活用状況

＜活用した、今後活用したい＞

- 成熟度高の企業では人材のマッピングを検討する際に利用している。
- 成熟度低の企業では立ち上げた専門組織の人材の活用や育成に活用したい意向がある。

＜活用していない＞

- セキュリティ体制はできているので手引書は必要ない。体制は企業文化や組織体制にもかかわってくるので参考になりにくい。

2.2.1 ユーザ系企業調査

⑤「サイバーセキュリティ体制構築・人材確保の手引き（第1.1版）」の改善について

- 特に改善の必要はないが約2割、内容を充実してほしいも約2割。
- 手引きを活用していないので分からないが約55%。

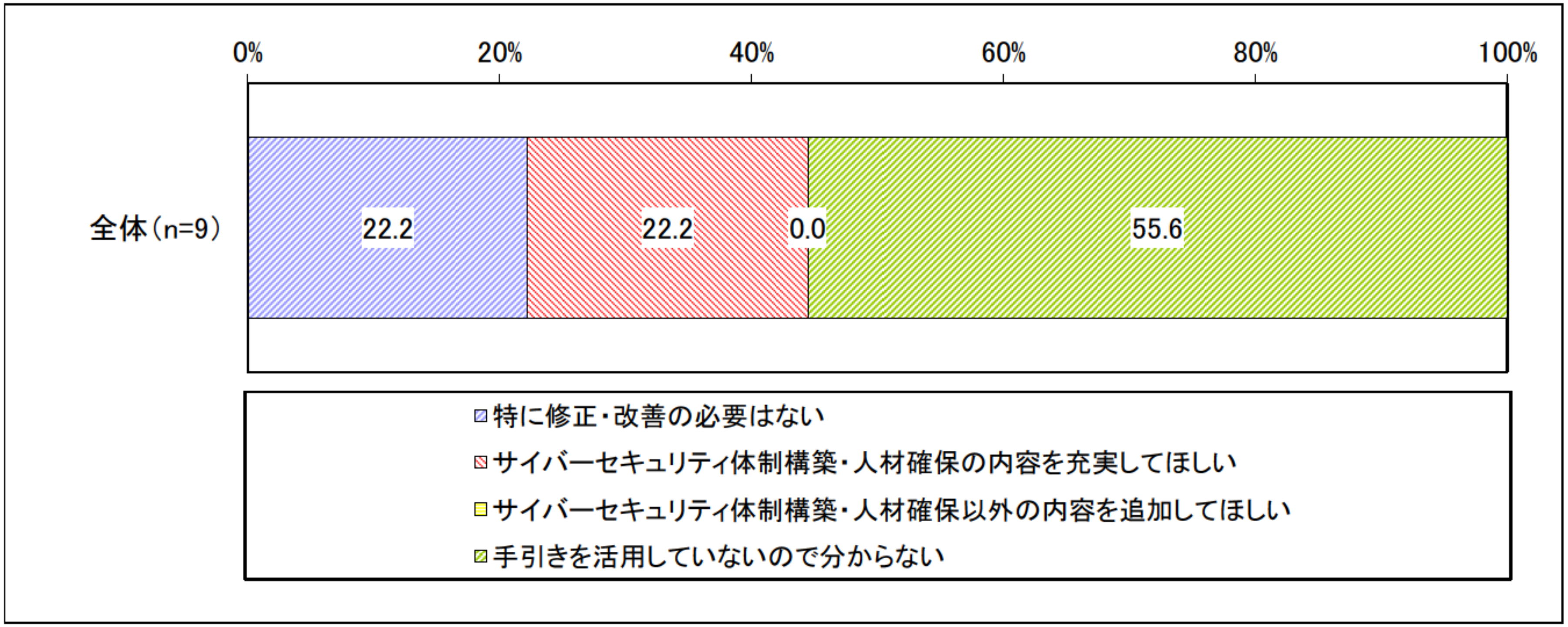


図2.7 事前アンケート調査結果（「サイバーセキュリティ体制構築・人材確保の手引き（第1.1版）」の改善について）

2.2.1 ユーザ系企業調査

⑤「サイバーセキュリティ体制構築・人材確保の手引き（第1.1版）」の改善について

＜事例の追加＞

- 海外の良い事例も盛り込んでほしい。
- セキュリティをどう位置付けるかの事例やガイドが欲しい。どこまでセキュリティを特別に扱うのか、人材をどう差別化するのかの事例が欲しい。

＜人材確保＞

- 会社規模ごとのベストプラクティスとして人数や社内外の区分があると良い。ベストプラクティス事例として具体的な数字があると参考になる。
- 人材がいない場合にどうするか、外部をどう活用するかは参考になる。
- 人材マッピングの表とか保有スキルは参考になるが、参考書が多いとどれを見ればよいのか悩ましくなる。
- 人材確保は困難なので、社内の人材をどう育成するか検討しなければならない。

＜人材育成＞

- セキュリティ人材は専門性が高いだけでなくビジネスや業務の理解が必要であり、人材育成のロードマップが重要。インフラから入ってもらうか、法務・リスク管理と人材交換するか、生産などから入ってもらうかなど人材の幅をどうするのかが課題である。
- ローテーションすることも必要だが、業務に波があり経験値を積ませるのが難しい。

2.2.1 ユーザ系企業調査

⑤「サイバーセキュリティ体制構築・人材確保の手引き（第1.1版）」の改善について

＜キャリアパス・処遇＞

- セキュリティ人材はゼネラリストベースの処遇からスペシャリストの処遇にしていく必要がある。そのためには求められるスキルが体系立てられ、経営者が見て納得できる標準的なものにしてほしい。
- キャリアパスの最終ゴールがセキュリティではない。会社全体としてのセキュリティレベルを上げるには、セキュリティ部門からローテーションで人材を輩出していく必要がある。

＜外部活用＞

- ベンダーは専門知識があっても社内情報は知らないので受け身型の仕事になりがちでなので、ベンダーや社外人材の活用方法を知りたい。
- インソースとアウトソースを組み合わせて最適な人材配置をすることが重要。

＜プラス・セキュリティ＞

- プラス・セキュリティの考えを整備して、サーバーセキュリティ基本方針にも盛り込まれたことは非常にありがたい。
- プラス・セキュリティは一人一人が自分事としてセキュリティ対策をしなければならないといった意識づけが必要であり、これに関するガイドラインがあったら活用したい。

＜サプライチェーン＞

- お客様からチェックシートがきて提出するようなケースも増えてきているので、国際基準を基にしている事を一言で言えることが重要である。
- サプライチェーンのチェックができていないので、管理方法の手引きがあると参考になる。

2.2.1 ユーザ系企業調査

⑥ 最近の状況（コロナ禍、DX進展など）によるセキュリティ体制の変化

- セキュリティ体制を強化した、もしくは検討中の企業が約8割。
- 一方で従来の体制で問題ないとしている企業も約2割。

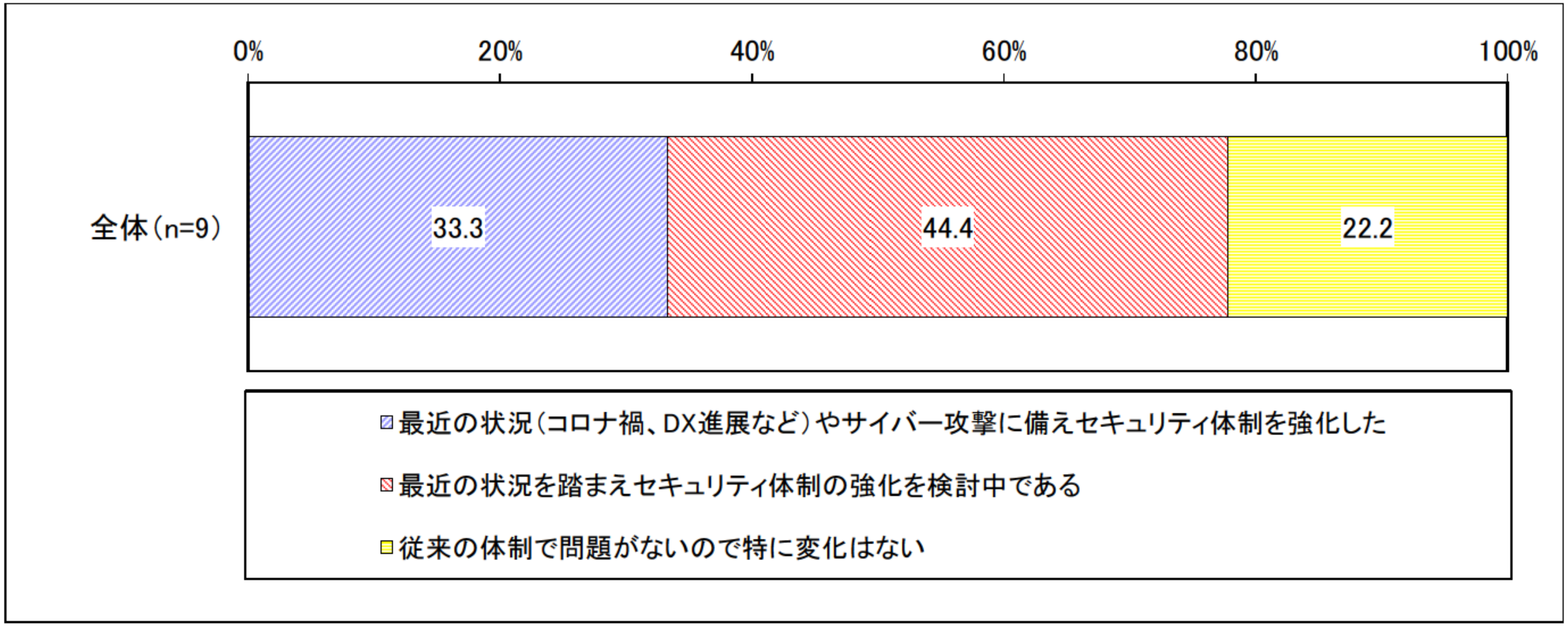


図2.8 事前アンケート調査結果（最近の状況（コロナ禍、DX進展など）によるセキュリティ体制の変化）

2.2.1 ユーザ系企業調査

⑥ 最近の状況（コロナ禍、DX進展など）によるセキュリティ体制の変化

＜セキュリティ体制＞

- コロナやDXということではなく、セキュリティの最新動向や技術動向チェックし体制に落とし込んでいる。
- デジタル化では事業部門の要求に対して、セキュリティを保護する適正な形で管理することが必要であり、そのために体制強化する必要がある。
- 成熟度低の企業では、最近になってセキュリティ専門組織や情報セキュリティ委員会を立ち上げ体制を強化している。

＜セキュリティガバナンスの強化＞

- セキュリティの実施状況調査をチェックシートによる自己評価に加えてインタビューによる第三者検証と、外部からの診断を定期的に実施している。
- 最近ではクラウドを活用して各部門が個別にシステム構築をしている。これらにセキュリティを横串で通して同一基準で開発してもらうためのガイドを設定して、遵守するように求めている。
- クラウドが増えて境界型が役に立たなくなった時にこのままではまずいという認識はIT部門にはある。しかし、リスクマネジメントとか経営層が認識しているかというとそうでもない。

＜サプライチェーン＞

- これまでは自社の資本が入っているところはガバナンスしてきていたが、サプライチェーン先もチェックすることにした。
- 最近の変化としては経営からの指示もあり、自社だけではなく関連会社や取引先を含めてサプライチェーンに積極的にアプローチしている。

2.2.1 ユーザ系企業調査

⑦ 最近の状況によるセキュリティ施策の変化

- 最近の状況に対応したセキュリティ施策を導入、もしくは検討中の企業が約9割。
- 一方で従来の施策で問題ないとしている企業も約1割。

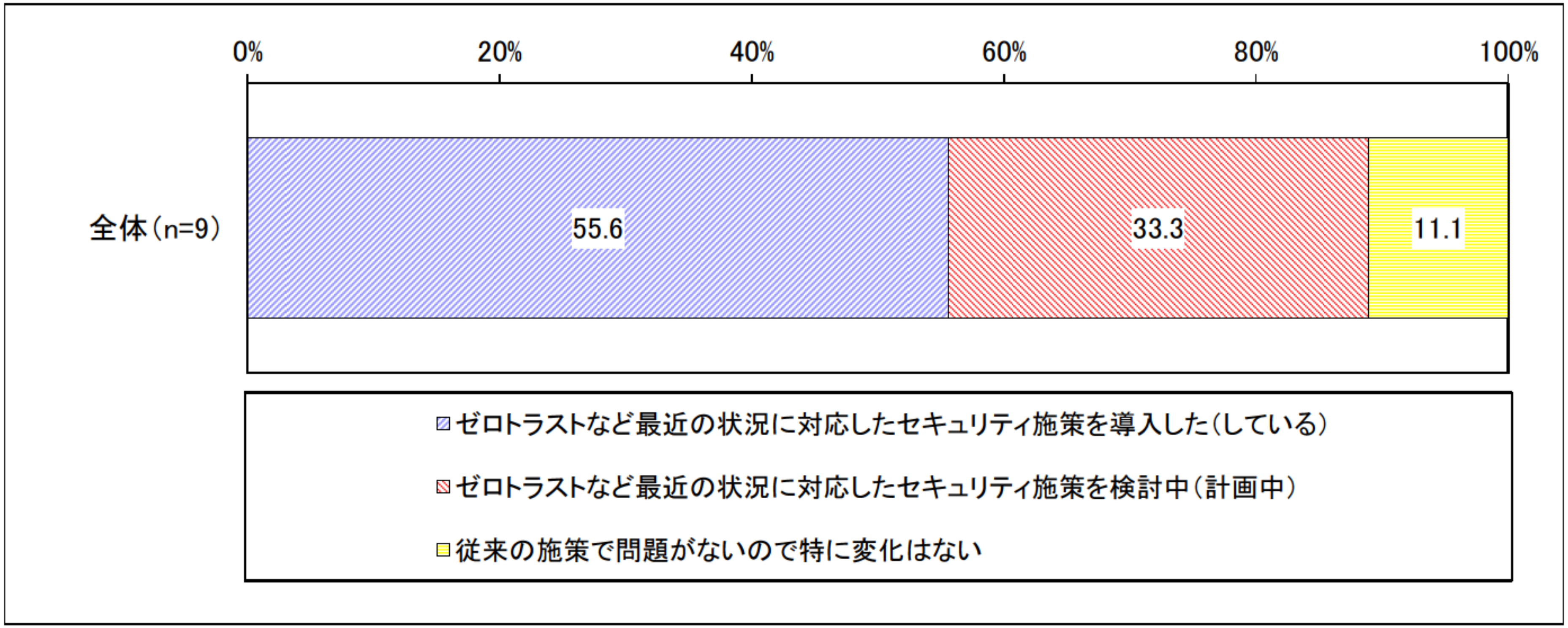


図2.9　事前アンケート調査結果（最近の状況によるセキュリティ施策の変化）

2.2.1 ユーザ系企業調査

⑦ 最近の状況によるセキュリティ施策の変化

＜リモートワーク、ネットワーク＞

- コロナによりリモートワーク中心となったので、リモートワーク前提で施策の見直しを行っている。
- リモート前提のセキュリティ施策としてグループ会社を含めてシェアードの全社共通セキュリティサービスを展開している。
- コロナやDXといったことではなく、セキュリティの最新動向や技術動向をチェックし体制に落とし込んでいる。
- デジタル化では事業部門の要求に対して、セキュリティを保護する適正な形で管理することが必要であり、そのために体制強化する必要がある。

＜ローカルブレイクアウト＞

- コロナの一年前からローカルブレイクアウトさせてインターネットをフル活用して安全にできる構成に変えてきている。
- ローカルブレイクアウトにはクラウドプロキシーサービスを導入して、それと連携する形である程度セキュアな環境で基幹システムにアクセスできる環境を担保している

2.2.1 ユーザ系企業調査

⑦ 最近の状況によるセキュリティ施策の変化

＜ゼロトラスト、EDR＞

- クラウドの利用拡大、DXの推進でインターネット接続が前提となる業務が今後拡大し、インターネットと社内ネットの分離は非効率になってきているので、ゼロトラストの考えを入れて仕組みを見直そうとしている。
- 全社共通サービスはゼロトラストを前提としている。EDRをベースにデバイス、端末を防衛する共通のサービスをグループ会社向けに展開している。
- ゼロトラストに向けてはクラウドGW、EDR、SGW、IDAS、デバイス制御などのツールを検討または導入中である。
- ゼロトラストに向けてはIDの使いまわしや共有を止め、特権IDシステムも入れようとしている。

＜ゼロトラストに向けた計画＞

- ゼロトラストの方針策定や要件定義などにコンサルに入ってもらっている。ゼロトラストに向けて1.5年くらいで変えていく計画である。
- ゼロトラストはVPNも含めてID基盤（IAM）を入れたうえでやっていく必要がある。全体ロードマップはそれも含めて5年後をめどに完成させたい。

＜暗号化、セキュリティチェック、資産管理、SOC、ID管理、他＞

- 最近のインシデントに対応した施策を様々入れている。例えば最新の暗号化ツールの展開、開発時のセキュリティゲートとかリリース時のセキュリティチェックの強化、構成情報を細かくするような資産管理など。
- GWをグローバルで共通に監視するSOCを導入中。
- 特権ID管理にIDオペレーションかサイバーアークの導入を検討中である。その他にはメール添付文書やデータストレージとしてクラウドストレージを導入している

2.2.1 ユーザ系企業調査

⑦ 最近の状況によるセキュリティ施策の変化

＜レガシー刷新＞

- 基幹システムやデータセンター、プライベートクラウドが残っておりセキュリティ的にも良くないので刷新する必要がある。

＜クラウド活用＞

- クラウドは利用ルールを決めており、セキュリティ統括でクラウドの審査を行っている。ID/PW+2要素認証や脆弱性診断をルールで決めている。
- システムはほぼクラウドに移行しており（90%以上）、クラウドベースのセキュリティアーキテクチャを構築している。

＜インシデント発生時の対応＞

- リモートワークになっているのでインシデント発生時の対応は工夫している。リモート会議で影響のあるシステムの洗い出しとか対策の検討を行っているが、進捗の管理はExcelのままである。
- 被害が大きい場合は幹部を含めた体制を立ち上げてリモートで連携しながら実施することになるので、大人数をリモートで連携させる必要があり訓練をやってブラッシュアップしている。

＜セキュリティ教育＞

- テレワークについてはガイドラインを作って安全に仕事ができるよう教育をしている
- セキュリティ専用の教育プログラムがなく、標的型メール訓練とかeラーニングを個別に実施しているので、他の教育プログラムに入れて全社的な仕組みとすることが効果的である。

2.2.1 ユーザ系企業調査

⑧ セキュリティ人材の確保・育成方法

- セキュリティ研修や資格委取得支援を行っている企業は2/3。
- 計画的に採用・育成、ローテーションを実施しているのは1/3。
- セキュリティ人材活躍に向けた人事施策を導入している企業は約1割。

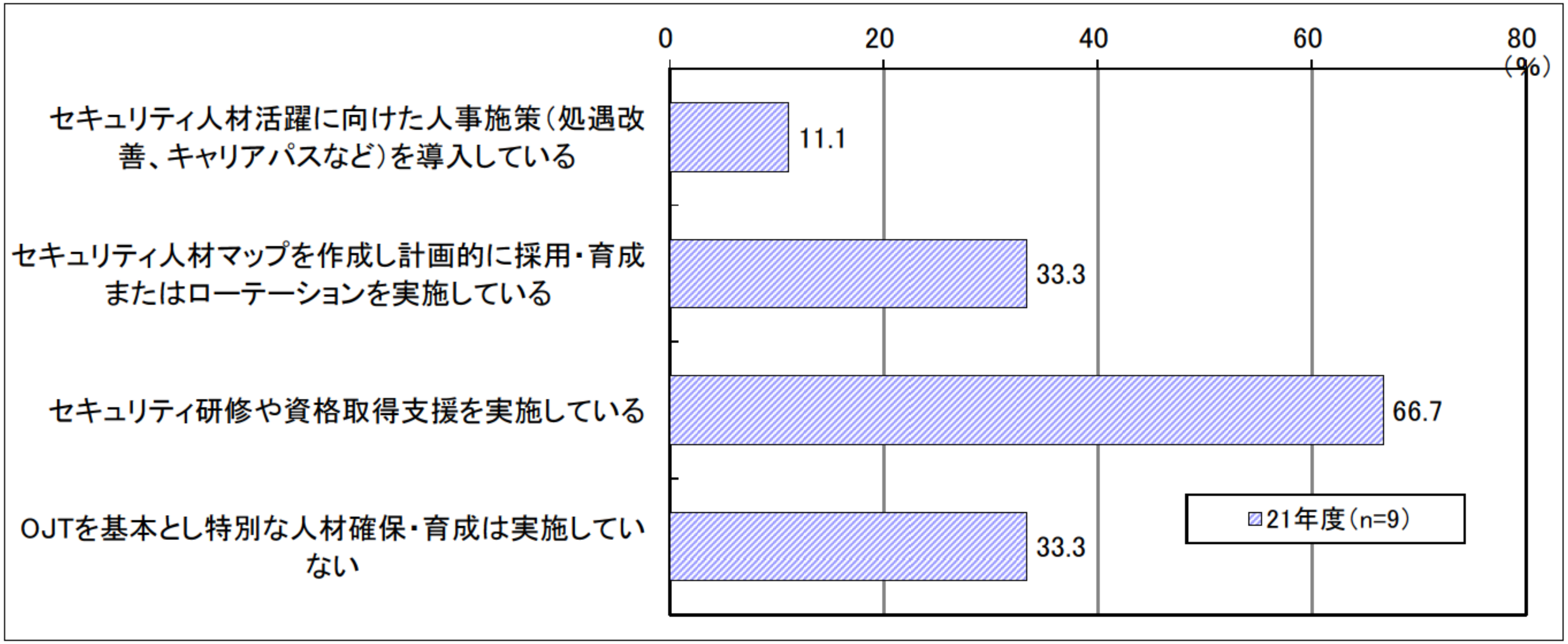


図2.10 事前アンケート調査結果（セキュリティ人材の確保・育成方法）

2.2.1 ユーザ系企業調査

⑧ セキュリティ人材の確保・育成方法

＜セキュリティ部門と関連部門の役割＞

- 社員は企画、チェック、診断結果の確認、インシデント対応を行い、セキュリティの監視、診断等は外部に委託している。
- セキュリティセンターが専門的にセキュリティを実施していて、他の部署でシステムを持っているところはセキュリティのルールをベースにやってもらっている。
- 各部門にはIT担当がおりセキュリティも担当しているが、セキュリティ施策の展開は任せずにセキュリティ統括が一括して実施している。

＜セキュリティ人材の採用＞

- キャリア採用は人事で採用枠を作ってもらい、セキュリティ部門で直接採用している。
- セキュリティ専門人材を採用しておりCDP（キャリアデザイン）を作成して育成している。セキュリティ専門人材の採用枠があり、人事部門と一緒に採用活動を行っている。

＜セキュリティ人材の育成＞

- 人材育成は資格の報奨金制度、IT部門の新人研修、OJTが基本。
- 人材育成の面ではシステム開発におけるセキュリティメンバー、セキュアコーディングのメンバー、リスク管理チームに人材を配置している。
- 外部講習はベーシックな内容が多くあまり役に立たないが、SOCのメンバーにはフォレンジックの訓練を年一回、自社で実施する計画がある。
- 個人が成長できるような職場環境を作るとか、話しやすくするなどの心理的安全性を高めた組織にすることにより成果につながる。

2.2.1 ユーザ系企業調査

⑧ セキュリティ人材の確保・育成方法

＜セキュリティ人材の育成＞

- IT部門が最低限知らなければならない基礎的なことは部門全員にセキュリティ教育を行っている
- セキュリティ統括部門では外部の資格取得を進めている。例えば、CISSPやセキスペを取得してもらっている。
- CSIRTメンバーは外部の研修会には積極的に参加しているが、あくまでセキュリティに配属された人が参加しているところに留まっている。
- 共通の人材育成プランはあるが、セキュリティに特化した育成プランやキャリアパスはない。

＜ローテーション＞

- 他社や他部門とのローテーションは実施できていない。IT部門内でローテーションしている。
- 通常の人事ローテーションとして新人を中心に管理部門や開発部門との間でローテーションはしている。
- セキュリティは幅が広いのでガバナンス的なことや技術的なことなど複数のことができるように人材ローテーションを2年おきにやっている。
- 関連会社にもIT部門があるのでセキュリティに限らずIT人材の流動性を高めるうえでローテーションが必要であると認識している。

＜人材マップ＞

- 成熟度高の企業では人材マップを作っており、人材の育成や即戦力の配置などを行っている。
- 人材育成のフレームワーク（ITSS）を使ってマッピングしたことはある。デジタルもそうだが求められる人材像が変わってきているので制度とかスキル評価に結び付けて見直す必要がある。

2.2.1 ユーザ系企業調査

⑧ セキュリティ人材の確保・育成方法

＜処遇、キャリアパス＞

- ほとんどの企業でセキュリティ人材に特別な処遇やキャリアパスはない。
- 高度専門職という制度があり多少処遇が良くなることはある。セキュリティ人材だけを特別に処遇するのには違和感がある。いかに事業に貢献しているか、自分の成長が実感できるかが大事で、そこをやらずにキャリアパスとかインセンティブといってもついてこない。
- セキュリティは技術だけを習得しているスペシャリストではダメで、事業や業務も理解する必要がある。
- セキュリティにはスペシャリストもゼネラリストも必要だが、ゼネラリストが処遇される傾向がある。スペシャリストをどう処遇するかが課題。スペシャリストの処遇改善が必要だがそもそも人材の定義ができていない。

2.2.1 ユーザ系企業調査

⑨ プラス・セキュリティ人材の育成方法

- 管理部門、事業部門と連携し勉強会や研修会を実施している企業が約45%。
- OJTを基本とし特別な人材育成をしていない企業も約45%。
- プラス・セキュリティ人材の研修、資格取得支援を行っているのは約1割。

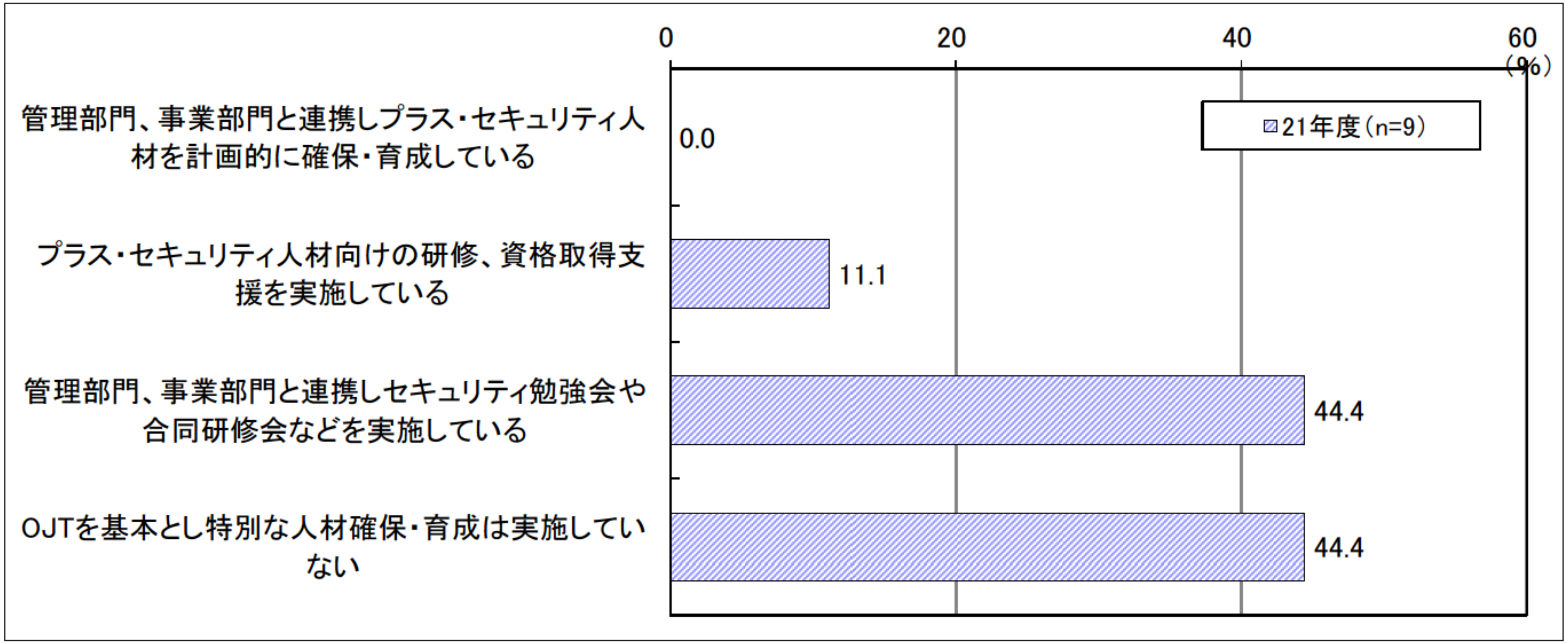


図2.11 事前アンケート調査結果（プラス・セキュリティ人材の育成方法）

2.2.1 ユーザ系企業調査

⑨ プラス・セキュリティ人材の育成方法

＜プラス・セキュリティ人材の教育、育成＞

- プラス・セキュリティとして人材確保や特別な教育を実施していない企業が大半であり、教育は個人任せになっている。
- 啓蒙活動はやっていてセキュリティの基本的なところをセキュリティ勉強会のような形でウェブ年6回の研修を行っている。
- プラス・セキュリティ人材には開発時のセキュリティチェックをしたり、第三者検証のインタビューに答えたりしてもらっている。このなかでチェックするための研修とか講習、システム開発管理者にはセキュリティチェックができるような教育をセキュリティ統括部門が実施している。
- クラウドのチェックリストを展開する際に、その説明会をグループ会社も含めて経営層やリスク管理部門、企画部門に何度も実施したが、これがセキュリティの勉強会になっている。
- 関連会社には情報管理責任者と情報管理担当者を任命し教育・研修を行っている。研修は自前プラス大阪府警の講演を入れているが、受ける人のレベル感が違うので難易度の設定に迷っている。

＜意識向上、必要性＞

- プラス・セキュリティ人材を一律に配置して育成するのは無理がある。
- セキュリティセンターが実施内容などを決め、現場部門で展開してもらう形にしているのでプラス・セキュリティ人材は特に必要性を感じない。
- プラス・セキュリティの考え方は理想的だが実際的にはなかなか回らない。開発部門だからこそ見えるセキュリティ施策もあるので、セキュリティに対する意識を変える必要がある。
- 各部門の意識改革が必要であるが、どこまでセキュリティを特別に意識する必要があるのか課題である。

2.2.1 ユーザ系企業調査

⑨ プラス・セキュリティ人材の育成方法

＜全社員向けセキュリティ教育＞

- 新人にはITパスポートは取得してもらっている。
- 全社員向けにはeラーニングとかサイバーセキュリティの全社員向け研修を行っている。攻撃型メール訓練も今後定期的にやることを計画している。
- 新人、中途採用、管理職昇級時にセキュリティ研修は行っているが、今後内容を充実させたい。

2.2.1 ユーザ系企業調査

⑩ グループ・グローバル関連会社のガバナンス方法

- 約８割の企業は連邦型のガバナンス。
- 集権型、分権型ガバナンスはそれぞれ約１割。

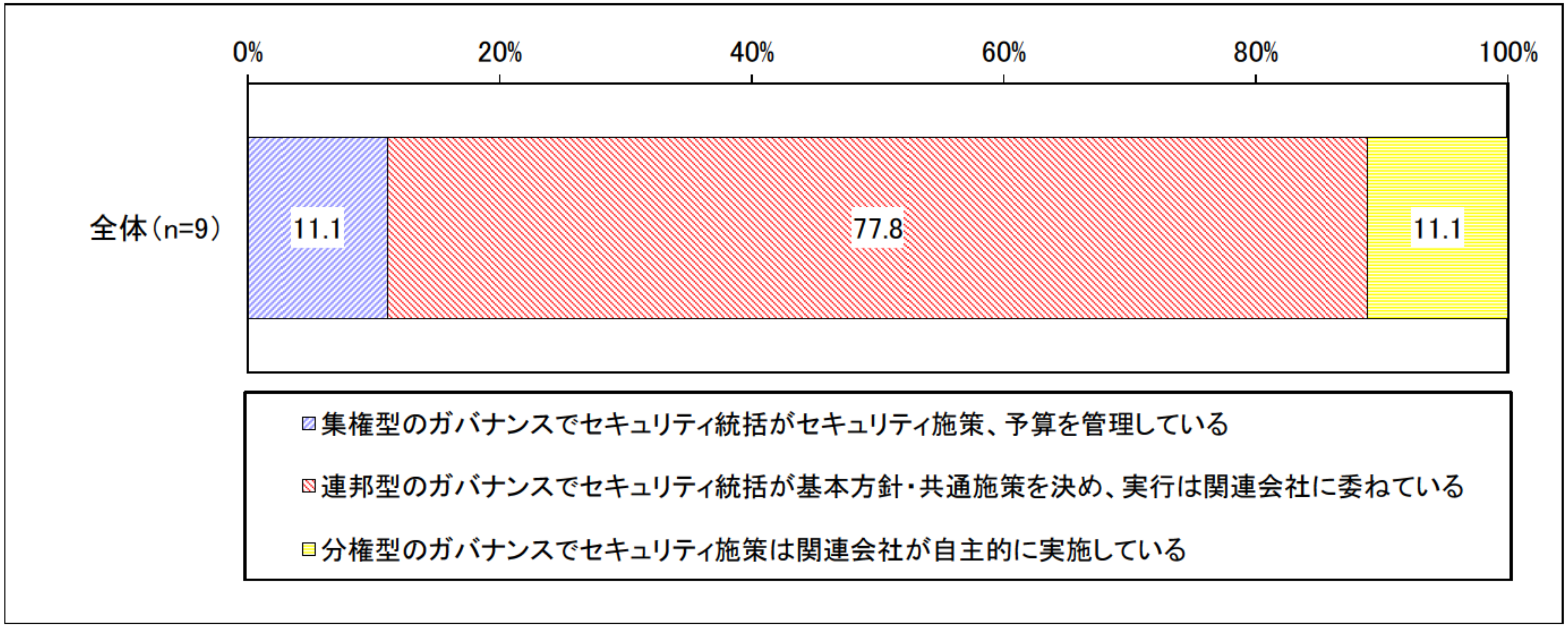


図2.12 事前アンケート調査結果（グループ・グローバル関連会社のガバナンス方法）

2.2.1 ユーザ系企業調査

⑩ グループ･グローバル関連会社のガバナンス方法

＜ガバナンス形態、役割分担＞

- 連邦型のガバナンスで、会社ごとにシステムや予算も別であるが、各社にCISOがいる体制。
- 100%子会社は集権型だが、それ以外の関連会社は連邦型で、各社でセキュリティ対策を実施してもらい結果を報告してもらっている。
- 買収した企業はイントラにつないでいない。既存環境を維持したい場合はSP800-171をベースにした規定を遵守してもらっている。それができない場合は、セキュリティセンターがひな形を用意して要求事項を守れるように自分たちで細則を作って実施してもらっている。

＜セキュリティ施策、IT環境＞

- 既存事業を行っている関連会社は、セキュリティ施策（PC、EDR、ウイルス検知など）、ネットワーク、PC等のIT環境を標準化している。
- ADはグローバルのADチームがあって、各国のHQによるツリーの上のところをグローバルで管理し、各国・地域のツリーの下のところに関しては各地域のHQで管理する形にしている。
- インシデントが発生した時は、ネットワークを遮断したり、どう復旧させるかはグローバルで取り仕切っている。但し、ネットワークはSOCが24365で監視しており、異常を検知した場合は即時性のためインフラ部門が判断して対処している。

2.2.1 ユーザ系企業調査

⑩ グループ・グローバル関連会社のガバナンス方法

＜予算、費用回収＞

- セキュリティ予算はグローバルでIT予算の枠内で管理している。
- IT統括部で集中的に管理しているPCとかネットットは一旦統括部でキャッシュアウトするが、内部で利用料として回収している。

＜規定・ルール＞

- 規定・ルールの基本的な部分はグローバル共通であるが、法令等により異なる部分は各リージョンに任せている。
- 関連会社も意識して規定・ガイドラインを作成している。

2.2.1 ユーザ系企業調査

⑪ グループ・グローバル関連会社のセキュリティ実施状況の把握方法

- チェックシートによりセキュリティ実施状況を把握している、検討している企業がそれぞれ1/3。
- 個別にセキュリティ実施状況を聞いている企業が1/3。

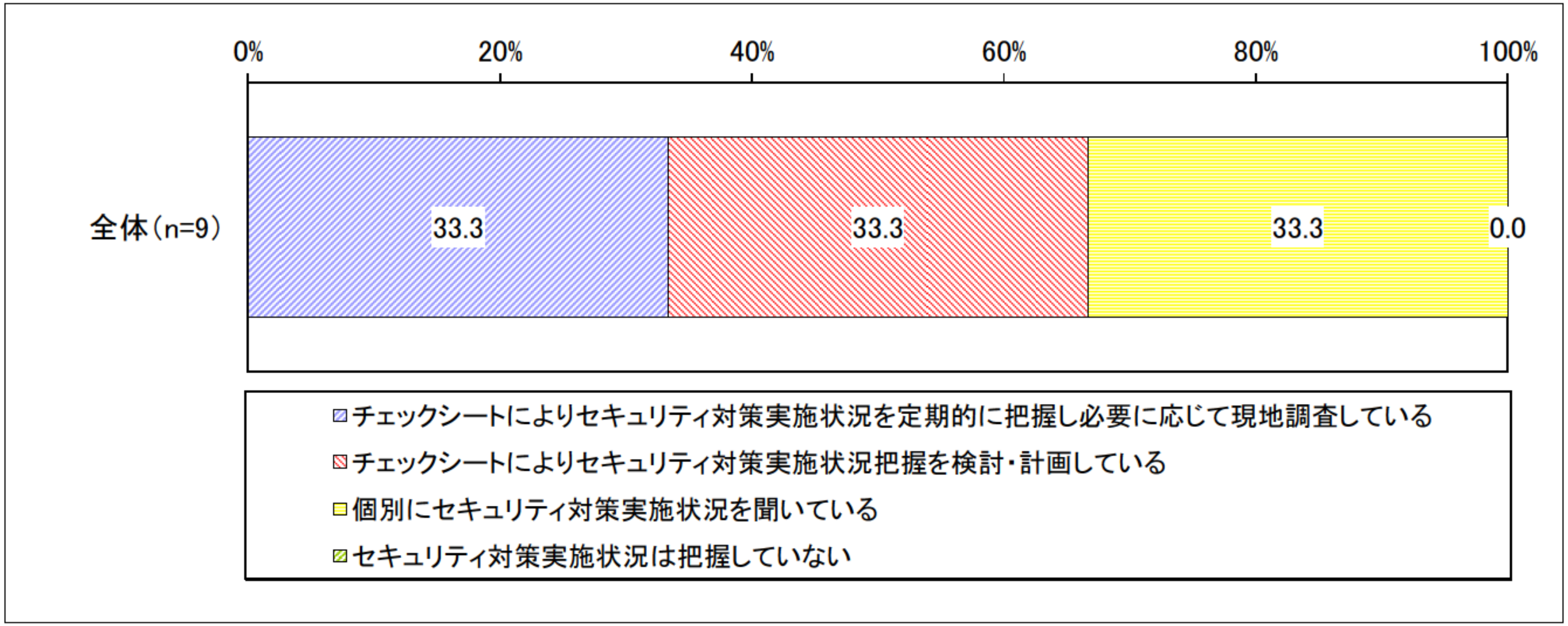


図2.13 事前アンケート調査結果（グループ・グローバル関連会社のセキュリティ実施状況の把握方法）

2.2.1 ユーザ系企業調査

⑪ グループ・グローバル関連会社のセキュリティ実施状況の把握方法

＜チェックリスト、定期的＞

- 成熟度高の企業では、FISCの安全対策基準や、海外はNIST SP800、EUのENISAなどをベースにチェックシートを作っている。それ以外にはMITRE ATT＆CKをベースにしたランサム攻撃に対する体制をみるチェックリストも作っている。
- 成熟度中の企業では国内関連会社はチェックシートによるチェックを毎年実施しているが、海外は実施していない。
- チェックシートは自己評価であり、インタビューなどで実施状況を確認することもあるが現地調査は実施できておらず、現場確認や実効性確認は課題である。
- 各部門、関連会社の対策状況を確認するためシステムの棚卸しを行っている。保有するシステムのセキュリティリスクに応じて３×３のラインマトリックスで分類して評価している。

＜個別チェック、特定分野のチェック＞

- 成熟度低の企業では、必要に応じて個別に、もしくは多要素認証を導入する場合など特定機能についてはチェックしている。
- クラウドはセキュリティ部門でチェックシートを作ってリスク評価している。

2.2.1 ユーザ系企業調査

⑫ サプライチェーン（取引先）のセキュリティ対策実施状況把握方法

- チェックシートによりセキュリティ対策状況を聞いている、もしくは計画しているは合計で1/3。
- 個別にセキュリティ対策状況を聞いている企業が1/3。
- 一方、セキュリティ対策状況を把握していない企業も1/3。

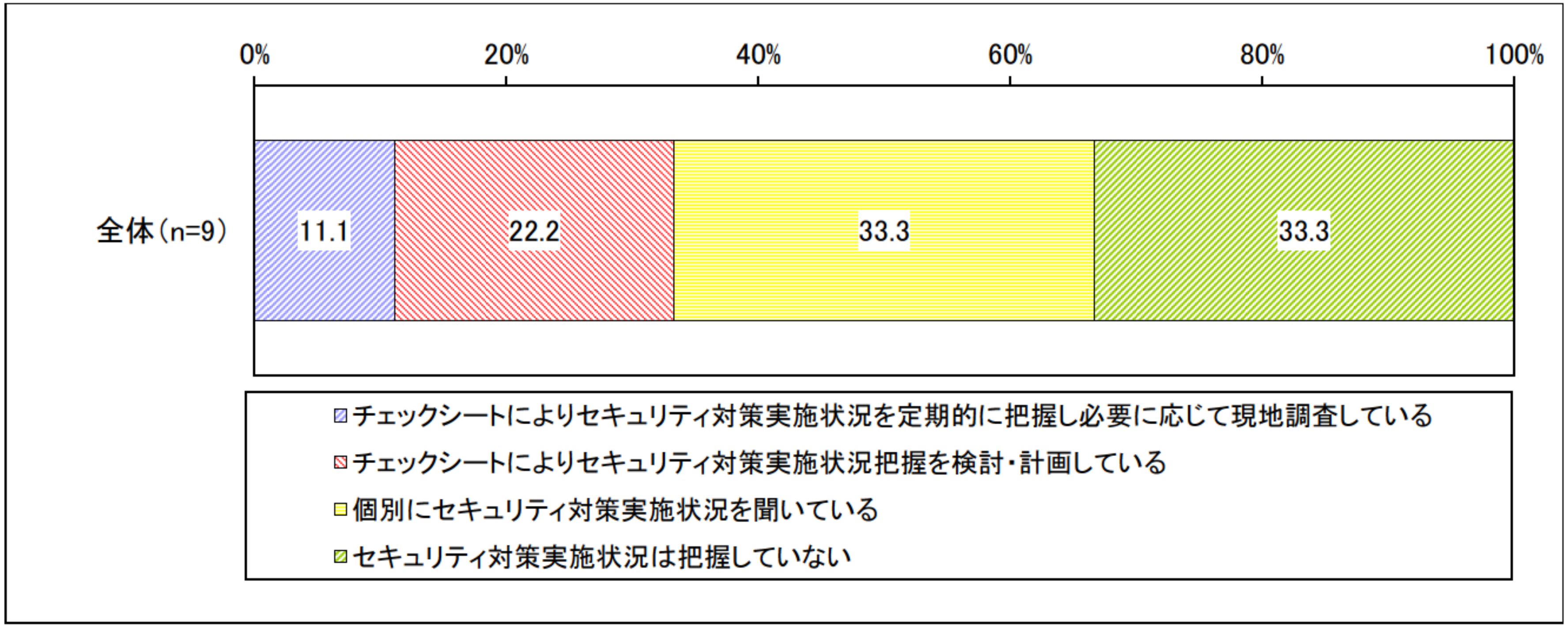


図2.14 事前アンケート調査結果（サプライチェーン（取引先）のセキュリティ対策実施状況把握方法）

2.2.1 ユーザ系企業調査

⑫ サプライチェーン（取引先）のセキュリティ対策実施状況把握方法

＜IT環境、責任分界点＞

- 取引先とのシステム接続仕様を決めており、その仕様の中でセキュリティ対策をしてもらうことが前提となっている。この中にインシデント発生時の責任分解点も含まれている
- システム開発会社とは専用の開発環境にしかつながらないような施策で、取り扱う情報も最小限にとどめて、かつモニタリングを掛けて後から追跡できるようにしている。
- 販売会社は契約ベースのガバナンスとなっている。シンクライアントを使ってもらい、ログを監視するなどガバナンスを強めている。

＜契約、規定・ルール＞

- システム開発の委託先とはセキュリティ基本契約を締結しており、定期的にセキュリティチェックしている。
- 取引先とは契約書にセキュリティ関連項目（NDAの保持、適切なセキュリティ対策の実施）が含まれている。個人情報を扱っているところは漏洩時の責任の明確化なども含まれている。
- 情報システムや情報資産を扱う取引先との契約書にはセキュリティ監査やチェック後の指示に従うような条項も含まれている。
- サプライチェーンのリスクが騒がれているので、機器とかソフトウエアを調達するときにセキュリティ条項を追加している。

2.2.1 ユーザ系企業調査

⑫ サプライチェーン（取引先）のセキュリティ対策実施状況把握方法

＜ネットワーク接続形態＞

- サプライチェーンを把握するのは事業規模的に無理なので社内ネットワークに繋がせないようにしている。
- 通信販売店とのネットはつながっている。個人情報を扱うオペレーションセンターとは別ネットにして分離しているが、ＦＷを介して繋がっている。
- 販売会社がシステムを使う場合は専用線とシンクライアントを使ってもらっている。そこから各店舗で持っているPCに情報を取り出せるようにしている。
- 開発会社とネット接続する場合は、決まった方法でしか接続させないようにしている。

＜インシデント発生時の対応＞

- ランサムウエアに感染した場合などはネットを遮断して状況を調査して、場合によっては広報と相談して社外公表することもある。
- サイバーセキュリティのインシデントが発生した場合に責任を取らせることはない。USBの紛失や個人情報の漏洩などは責任を追求することもある。

＜チェックリスト＞

- 成熟度高の会社ではサプライチェーンのセキュリティ対策実施状況をチェックリストでチェックしている。
- 事務やオペレーションの委託先のセキュリティ状況をどう把握するかは課題である。弁護士事務所、コールセンター、保険金査定会社などのセキュリティがどうなっているかは最近注目されている。

2.2.1 ユーザ系企業調査

⑫ サプライチェーン（取引先）のセキュリティ対策実施状況把握方法

＜個別チェック＞

- 成熟度中の企業では、セキュリティ認証状況の確認やセキュリティ責任者の設置などを書面で聞いている企業がある。
- IT部門では何を預けているかは分からないので、事業部門の判断としてやってもらっている。

＜特定分野のチェック＞

- クラウドベンダーや個人情報を扱っている取引先はセキュリティチェックを行っている。
- システム開発（ウエブサイト構築など）するときなどはウエブサイトの作り方に準拠した作り方になっているかなどをチェックすることはある。

＜顧客からのセキュリティチェック＞

- 取引先としてチェックされることが多い。チェックシートはお客様各社個別で別々に対応しなければならず、提出には社内稟議を通す必要があり大きな負荷となっている。確認する側も大変なので、社会全般的なルール・指針を作ってもらうと助かる。

2.2.1 ユーザ系企業調査

⑬ OT/IoT分野のセキュリティに関する体制や人材の役割定義

- OT/IoT分野もセキュリティ統括が担当しているのは約1割のみ。
- OT/IoT分野の制御部分は事業部門が担当し管理部分をセキュリティ統括が担当している企業が1/3。
- 最近の状況を考慮し役割分担と連携方法を検討している企業が1/3。

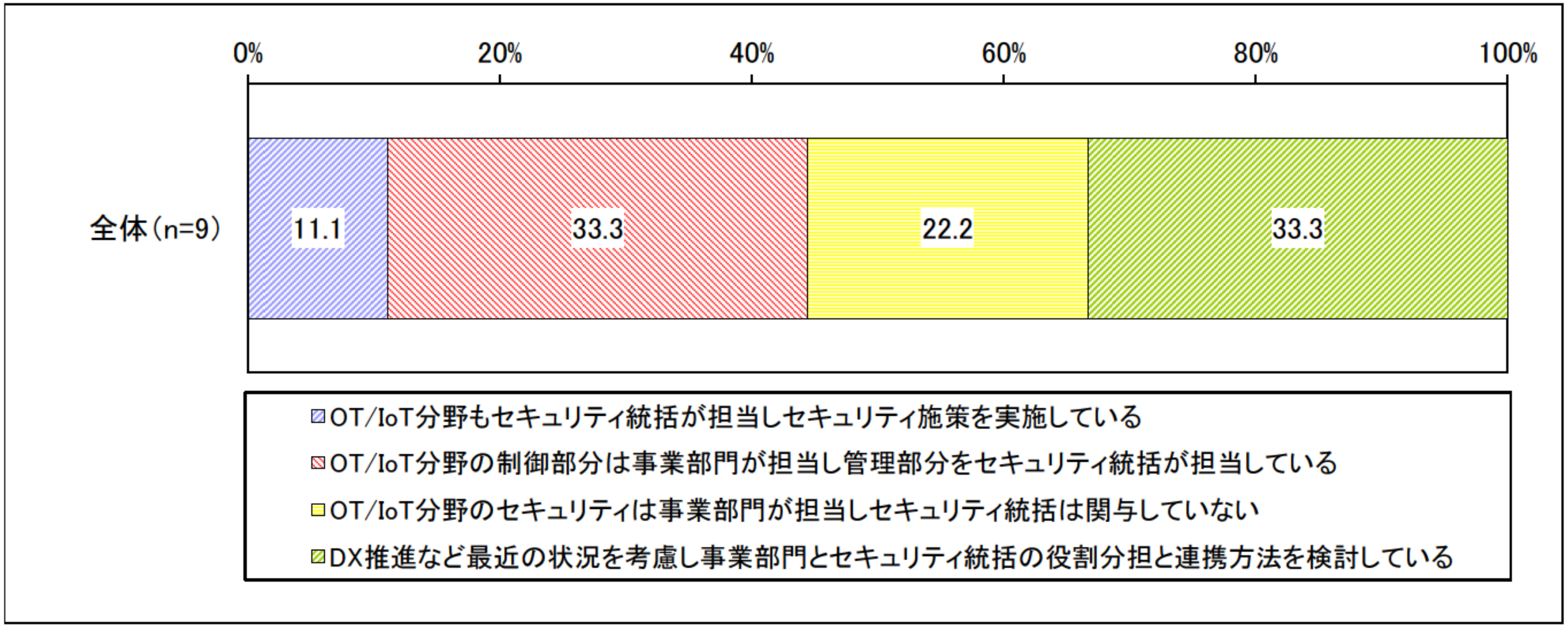


図2.15 事前アンケート調査結果（OT/IoT分野のセキュリティに関する体制や人材の役割定義）

⑬ OT/IoT分野のセキュリティに関する体制や人材の役割定義

＜OT/IoTの担当部門と役割分担＞

- 工場部門の独自ネットについてはセキュリティ統括は関与していないが、ITで管理しているネットにつなぐ場合は関与する。
- 工場のセキュリティについてはセキュリティ方針を経営の決定事項として展開している。工場の責任者会議、現場の担当者向け説明会でネットワークを接続する場合はセキュリティ統括が介入することを周知徹底している。
- 数年前に工場でラインが止まったこともあり、3年前から技術はセキュリティ統括、実施の責任は工場部門ということで二人三脚でセキュリティ強化を実施している。
- 工場部門のセキュリティは工場部門担当だが、技術的進歩が速くアドバイスを求められており、今後は積極的に関与していくことを検討している。
- OTとしては電気通信設備がある。電気通信設備の統括組織（ネットワーク事業推進本部）があり、その中にセキュリティ専門部隊が管理している。
- 新しい工場はネットワークアーキテクチャから、古い工場は機器の更新のタイミングに合わせて、アーキテクチャーとネットワークはIT部門が担当することになっておりセキュリティもチェックする。

⑬ OT/IoT分野のセキュリティに関する体制や人材の役割定義

＜OT/IoTの担当部門と役割分担＞

- 工場部門の独自ネットについてはセキュリティ統括は関与していないが、ITで管理しているネットにつなぐ場合は関与する。
- 工場のセキュリティについてはセキュリティ方針を経営の決定事項として展開している。工場の責任者会議、現場の担当者向け説明会でネットワークを接続する場合はセキュリティ統括が介入することを周知徹底している。
- 数年前に工場でラインが止まったこともあり、3年前から技術はセキュリティ統括、実施の責任は工場部門ということで二人三脚でセキュリティ強化を実施している。
- 工場部門のセキュリティは工場部門担当だが、技術的進歩が速くアドバイスを求められており、今後は積極的に関与していくことを検討している。
- OTとしては電気通信設備がある。電気通信設備の統括組織（ネットワーク事業推進本部）があり、その中にセキュリティ専門部隊が管理している。
- 新しい工場はネットワークアーキテクチャから、古い工場は機器の更新のタイミングに合わせて、アーキテクチャーとネットワークはIT部門が担当することになっておりセキュリティもチェックする。

2.2.2 ベンダー系企業調査

(1) ヒアリング対象事業者とヒアリング項目

- 本事業におけるベンダー系企業調査は、ユーザ系企業調査を補う観点から、以下の３社を対象に実施した。
- それぞれのヒアリング項目を併せて示す。

表2.2 ベンダー系企業ヒアリング調査の対象企業一覧

企業の分類	ヒアリング項目
教育サービスベンダー	● 国内企業における試験・資格制度の活用状況について
制御系セキュリティサービス	● 制御系のセキュリティ対策を担う体制について ● 制御系のセキュリティ対策を担う人材について
技術系人材サービス	●「サイバーセキュリティ体制構築・人材確保の手引き」改訂案について

2.3 機関投資家へのヒアリング調査

(1) 実施したヒアリング調査の概要

- 調査趣旨を踏まえ、機関投資家の視点をもち、企業におけるIT/デジタルガバナンスやリスクマネジメントに関する評価及びそれに関わる業務を行っている関係者（8社、10名）にヒアリング対象を実施した。

2.3 機関投資家へのヒアリング調査

(2) ヒアリング調査結果

① 企業を評価する際に見る項目（機関投資家等）

- リスクとして調査対象とするのは５年程度の時間軸でみる長期のものであり、移行リスク（気候変動の影響等）とオペレーショナルリスク（サプライチェーンの健全性等）に分けて扱う。それぞれの重みは業種によって異なるので、業種毎の担当を置いて取材する。
- 企業の評価の際に確認する内容は、企業の業種や成長ステージによって異なるが、いずれも事業におけるリスクを把握するところから始まる。
- 企業が指標として用いている値の経年変化はかなり参考になる。ただし指標として妥当かどうかは確認が必要。デジタル人材の充足目標に対する進捗率を出している企業があり、参考にしている。
- 投資家による単独での企業との対話には限界があり、集団で分担して企業を調べるようにしている。これにより、質問対象を絞る代わりに深い内容について尋ねることができる。こうした動きを踏まえ、経営層は投資家からの質問に対して、リスクがどの程度見込まれ、どう対策をしているか答えられるようにしておくべき。
- CEOがシステムに明るく、自分の言葉でDXの方向性や、活用するプラットフォームの考え方、外部連携を自分の言葉で語れると安心感がある。誰か担当者に尋ねた上で回答していると不安になる。
- 経営陣が適切な課題認識をもっているかどうかは重視している。課題について論理的に説明できることを期待している。
- 「気候関連財務情報開示タスクフォース（TCFD）」が「ガバナンス」、「戦略」、「リスク管理」、「指標と目標」の４つの柱に関して開示のプロトタイプを示している。投資家はこうした動きになじみはじめており、他のリスクに関しても開示のプロトタイプとして、わかりやすい開示を求める動きが出てくる可能性がある。
- 法律で開示が求められている情報の内容は各社とも似通っており、あまり読むことはない。自社にとって致命的なリスクをメリハリをもって示すことが重要。

2.3 機関投資家へのヒアリング調査

(2) ヒアリング調査結果

② サイバーセキュリティに関して見る内容（機関投資家等）

- 企業がサイバーセキュリティを評価するのは、企業におけるリスクとして重要性（マテリアリティ）が高い場合。そうでない場合、事業上のすべてのリスクをチェックすることは一般的ではなく、対話のテーマにならない。
- サイバーセキュリティを含むITリスクの重要度が高いのはゲーム業界や金融業界。
- セキュリティ体制は機能していることが重要。現場と経営陣が円滑につながっているかを確認したい。
- 経営層がリスクをどの程度把握しているかを確認するため、開示内容は一通り参照する。サイバーセキュリティのリスクが高ければ、それをピックアップして確認する。
- ある企業で情報漏えいが生じたから、同じ業種のリスクが高いとは考えない。事故の当事者企業には個別に対策状況等を確認することはある。扱う情報が多い業種・業態のリスクは高いとは考えている。データの流出が企業の存続に関わるようなケースでは詳細に確認する。
- 開示される情報のエビデンスは重視していない。エビデンスがあってもリスクはゼロにならない。ただしプライバシーマークやISO認証などは若干の安心材料。それよりも、体制や想定リスクに関する質問に対し、クリアな情報が提示されることが重要。ある保健医療関係の組織の場合、機微データを扱える人数、場所の制限、監視状況などの具体的な説明があったので、信憑性があると判断した。
- 事故発生の可能性はゼロにならないので、リカバリーの体制が取られているのかを含めた開示を期待する。
- 「デジタルガバナンスコード」に準拠しているといった説明を受けるが、準拠していれば情報漏えいが生じないわけではないことは理解している。
- サイバーセキュリティの世界は、人権デューデリジェンスに近い捕捉の難しさがあると感じている。PDCAを通じたレベルアップを前提に、基準や取組事項をまとめた行動計画を普及させるべきではないか。

2.3 機関投資家へのヒアリング調査

(2) ヒアリング調査結果

③ サイバーセキュリティに関して見る内容（M&Aにおけるデューデリジェンス）

- サイバーセキュリティ対策状況を評価する際に、かけている費用よりは、構築している体制や管理状況を主に評価する。費用だけでの判断は難しく、多額の費用を投じていることもない。買収先の社内環境をそのまま繋げて問題ないかどうかの視点で見る。
- M&AにおけるIT関連のデューデリジェンスはほとんどの企業を対象に実施している。サイバーセキュリティを対象とすることはまだ少ないが、以前に比べると増えている。
- M&Aにおいて、買収対象企業のIT管理体制、委託関係、運用・監査等の規定整備状況等を確認する。この中にサイバーセキュリティ対策状況も含まれる。場合により、サイバーセキュリティを重点的に確認してほしいと依頼されることもある。
- M&Aにおけるデューデリジェンスのプロセスにおいて、サイバーセキュリティを早期の段階から細かく調査することはない。買収が決まったところで改めてアセスメントするのが普通である。
- セキュリティ対策に問題があったことで買収が不成立になった事例は国内では聞いたことがない。ただし海外では個人情報の管理に問題があると指摘され、損害賠償に至ったケースはある。今後は国内でも損害賠償の事例が生じる可能性はある。
- 企業に対して情報提供を求める際、拒絶されることはないが、結果的に出てこないことはある。その結果、リスクとして検討すべきことが残留することになり、その旨を依頼元に報告する。

2.3 機関投資家へのヒアリング調査

(2) ヒアリング調査結果

④ 企業をサイバーセキュリティの観点で評価する際に参考にしているガイドライン等

- ISO26000（組織の社会的責任）をもとに対応状況を把握している。
- 企業のサイバーセキュリティ対策の評価には、経営ガイドラインを利用している。網羅的にまとまっていることを評価している。経済産業省が作成したという点でも通りが良い。可視化ツールについては認知はしていたが使ったことはなかった。
- BtoCの小売業などの場合は個人情報管理について気にすることが多い。この場合は個人情報保護委員会のガイドラインなどをベースに確認する。
- 経済産業省における取組を認識していなかった。DXを進めていく上での落とし穴などは経済産業省などで手引きとして示してもらえるとよいと思う。
- ステークホルダー保護の観点から、公的機関が最低限やるべきレベルを示してもらえるとよい。

⑤ 企業をサイバーセキュリティの観点で評価する際の課題

- サイバーセキュリティに関する認識と取組は日本全体で遅れていると認識しており、それは機関投資家においても同様である。その結果、資金の集まり方も鈍いのではないか。
- サイバーセキュリティ対策に携わる人材が圧倒的に不足しており、人材の認知と支援プログラムを整備すべきではないか。

2.3 機関投資家へのヒアリング調査

(2) ヒアリング調査結果

⑥ 経済産業省による機関投資家への普及啓発の方法について

- 証券会社が開催するセミナーには多くの投資関係者が参加する。そこでサイバーセキュリティ経営や可視化について紹介すれば認知度が高まるのではないか。
- 機関投資家は証券会社のウェビナーを見るので、そこで経済産業省が取組を紹介してはどうか。
- 投資家の横の繋がりは弱い。個人単位で業界コミュニティ（投資家フォーラム、投信協会等）に参加する人はいる。

2.4 海外動向調査

(1) 実施した動向調査の概要

- 10社以上の海外企業を対象に、サイバーセキュリティに関する情報開示の取組事例とその関連動向について、公表されている情報をもとに以下の項目について分析を行った。
  - 各社が情報を開示している場・ツール（有価証券報告書等）、開示している情報の内容（表現等も含む）
  - 各社が情報開示の根拠にしている法令、基準等
  - 情報開示に関する過去数年間の動向の変化
- 海外企業との比較のための対照群として、調査対象とした海外企業の同業に相当する国内企業7社について、比較のために同様の調査を実施した。
- 調査実施時期は2021年11月下旬であり、その後に開示された情報は対象に含まれない。

2.4 海外動向調査

(2) 調査結果から判読される事項

- 一般に海外企業のほうが国内企業より開示が積極的な傾向がみられるが、一部国内企業は海外の同業企業と同程度の開示を行っている。
- 国内企業はセキュリティ体制の説明までにとどまる場合が多く、海外企業は対策まで踏み込んだ内容が多い。
- 世界的に著名な企業であっても、投資家向けにサイバーセキュリティ関連情報をほとんど開示していない企業もある。
- 国内外を問わず、「Sustainability」の一環としてサイバーセキュリティリスクとその軽減策について開示している企業が多い。
- 海外企業のうち、英国企業はすべての企業がリスクに関するMitigationの取組を具体的に示している。
- 開示が一部の企業に限られている理由として、次の仮説が想定される。2.3に示した機関投資家ヒアリング調査はこれらの仮説を検証する観点も含めて実施している。
  - 開示が義務づけられていない限り、自らの手の内を明かすことになるセキュリティ対策の開示を避けたいと考える企業が多い。
  - 投資家におけるサイバーセキュリティに関するリスクの優先順位が他のリスクに比べて低いため、投資対象企業に開示を要求することがあまり行われていない。
  - 定性的かつ自己表明にならざるを得ないため、投資家へのメッセージとしての実効性が不十分と考えられている。
  - 広報やIR担当者において、事業リスクに関する説明責任としてのサイバーセキュリティ対策の開示についての認識が不十分。
  - 広報やIR担当者において、Sustainabilityにおけるサイバーセキュリティリスクの優先順位が低く評価されている。

2.5 有識者会議の開催

(1) 有識者会議の設置

- 以下を含む事項について議論を行うための有識者会議として、6名で構成される「セキュリティ経営・人材確保の在り方検討タスクフォース」を設置した。なお、本タスクフォースは本報告書3.3に示す有識者会議と一体化して運営した。
  - 経営ガイドラインの前回改訂以降の各種動向を踏まえた改訂の在り方
  - 「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」を踏まえた取組状況ほか、企業調査結果の分析
  - 機関投資家ヒアリング調査の実施方法、及びヒアリング調査結果を踏まえた可視化ツールの普及促進方法
  - 海外における企業によるサイバーセキュリティ、リスクマネジメント及びESGに関する情報開示内容、根拠法令・基準、過去数年間の変化等を踏まえた対応の在り方　等

2.5 有識者会議の開催

(2) 有識者会議の開催状況

- 前ページの構成メンバーにより、以下の９回にわたり議論を実施した（いずれもオンラインによる開催）。

表2.3 「セキュリティ経営・人材確保の在り方検討タスクフォース」開催状況

会議	開催日	サイバーセキュリティ経営ガイドライン見直し関連 （本項に関するテーマ）	セキュリティ人材活躍モデルの構築及び普及啓発関連 （3.3に関するテーマ）
第1回	2021年9月10日	● 今年度の調査計画について ● 今年度審議すべき論点の抽出	● 今年度審議すべき論点の抽出 ● 手引き書英訳版で用いる訳語について
第2回	2021年10月12日	● 経営ガイドラインのスコープについて	
第3回	2021年12月3日	● 経営ガイドラインの改訂方針案について ● 海外動向調査結果の報告【済】 ● 機関投資家調査の実施方法について	● 企業調査結果中間報告
第4回	2021年12月27日	● 経営ガイドラインの位置付けについて	● プラス・セキュリティの概念整理 ● 手引書拡充に向けた方針案の検討
第5回	2022年1月25日	● 経営ガイドラインに関するまとめ	● 手引書拡充案の検討 ● 手引き既存コンテンツの見直し
第6回	2022年2月8日	● 機関投資家ヒアリングで得られた意見について ● 経営ガイドラインの改訂について	－
第7回	2022年3月7日	－	● 有識者ヒアリングで得られた意見について ● 手引き見直し方針について
第8回	2022年3月15日	● 経営ガイドラインの改訂についてのまとめ	● OT環境に関するヒアリングで得られた意見について ● 手引き第2版案について
第9回	2022年3月23日 （持ち回り開催）	－	● 手引き第2版案レビュー

3. サイバーセキュリティ人材活躍モデルの構築のための調査

3.1 企業調査

- 本項に相当する企業調査の内容は、2.2で実施した企業調査に含まれているため、当該項参照。

3.2 有識者ヒアリング

(1) ヒアリング対象者

- サイバーセキュリティの業界動向に詳しい有識者10名に対し、以下の事項について尋ねた。
  - ユーザ企業におけるセキュリティ人材確保・体制構築に関して求められる政策
  - セキュリティ専門人材の役割・スキル定義・キャリアパスの見える化のための政策
  - 情報処理安全確保支援士や情報セキュリティマネジメント試験等の資格・研修の活用促進策
  - 各国におけるセキュリティ人材育成の取組　等

3.2 有識者ヒアリング調査

(2) ヒアリング結果

- 前ページに示した有識者による意見を示す。なお、「セキュリティ体制構築・人材確保の手引き」改訂案へのコメントについては3.6にて反映した。

① セキュリティ統括機能について

- 「セキュリティ業務を一極集中させる」という誤解を与えないように留意すべき。セキュリティ対策が現場と離れてしまうと、「仕事の邪魔をする」と現場からの反発が強くなって協力してくれない。
- セキュリティ部門はあってもよいが、現場部門と兼務にするなどして孤立させない工夫が必要。現場の企画会議に参加して「一緒に汗をかきます」という態度をとるなど、現場を支えていくという姿勢がよい。自分の言うことを聞けといってよいのは社長のみである。
- 事業部門でセキュリティの素養がありそうな人材に、事業ラインに沿った業務の組込を推進してもらうと受け入れやすいのではないか。
- 委員会方式の場合は孤立は無いが、誰も責任をとらなくなるので社長のガバナンスが重要になる。日常から「セキュリティを考えるのは社長の仕事」と言っておくなど。
- セキュリティ統括機能では技術よりもマネジメントスキルが重要。現場と仲良くしておき、どうにもならなくなったときに技術系人材に相談すればよい。
- 組織上は現場部署の上の位置付けとして置くのでは無く、並ぶ形のサポート組織としておくのがよい。

3.2 有識者ヒアリング調査

(2) ヒアリング結果

② ユーザ企業が賢く調達し、ベンダーと会話できるようになるためのスキルについて

- 大企業でも、「明らかに担当者がベンダーのカモにされたのでは」という事例をみかける。
- 複数のベンダーと付き合ったり、業界団体で他社の話を聞く、複数の情報源を持つことも有益。
- 専門用語を理解することがベースになる。ただし、中途半端な知識はかえって有害な場合もある。
- セキュリティマネジメント試験に合格した上で、毎年知識を更新出来るようにするとよい。
- セキュリティ製品・サービスは性能や効能の表示が共通化できていない。ベンダーからの歩み寄りが必要。

③ ユーザ企業が賢く調達し、ベンダーと会話できるようになるためのスキルについて

- 国内企業はセキュリティ体制構築の前にリスク分析ができていない。経営者が自社のリスクを頭に入れておらず、ヒト・モノ・カネに終始している。顧客情報の何を守り、誰に迷惑をかけないかを明らかにした上で対策を考える必要がある。
- 全方位対応しようとしてもできないので、業界毎の目標・価値観をもとにベースラインを定めるのが良い。そのときのベンダーの役割は、環境変化でリスクが大きくなったことを伝えること。
- サイバーリスクに関する関係者とのリスクコミュニケーションができるようになるとよい。

3.2 有識者ヒアリング調査

(2) ヒアリング結果

④ OT環境のリスク（ベンダー企業ヒアリング結果を含む）

- OT環境でもクラウドを利用するようになっているが、IT系で把握していない状態でクラウドにデータがアップロードされるなど、無法地帯として運用されてしまうことが起きている。
- 地方の工場のネットワーク設備の面倒を大手SIerはみないので、通信キャリアが対応しているケースが多い。その結果、工場の外部接続用ルータとして家庭用と同じ製品が使われていることがある。
- 海外制御機器ベンダーの最近の製品は、自社のVPNルータ経由で海外のクラウドサーバに接続し、そこからソフトウェアをダウンロードし、状況を確認することもできる。ベンダーは事業者に対して「専用線と同じ」という説明をしているようである。
- SOCのSPLUNKからみると、CASBで繋がれた先の制御機器も通常のサーバと同じに見えてしまい、ITとOTの識別ができない。
- 工場の非常事態で全面停止となると、アクセスログも記録できなくなる。それを防いでもらうことはできないので、電源が止まっても記録をどう保持するかを考えながらシステムを作る必要がある。

⑤ OT環境におけるxSIRTの扱い

- 事業内容や工場毎にOT環境のリスクが異なると、共通のOT-SIRTを作ってもうまく機能しない可能性がある。一方で個別にSIRTを設置すると必要なスキルを有する人材が足りない問題が生じる。IT部門で対応する場合もあるが、共通解はない。
- 出荷する製品については品質管理部門にすべての権限があり、PSIRTは助言の立場。

3.2 有識者ヒアリング調査

(2) ヒアリング結果

⑥ OT環境におけるセキュリティ体制

- これまでOTベンダーがセキュリティベンダーとの連携に積極的でなく、セキュリティベンダーはIT部門のみにコンタクトする傾向があり、結果的にIT部門がOT環境のセキュリティまで考えたり、OTベンダーがセキュリティを調べたりといった対応を通じて対策が実施されていた。
- 工場に導入するPC等の場合、制御機器の周辺機器としてOTベンダーが調達してソフトウェアを導入することもあり、ITベンダーの存在が事業者側からは直接見えないこともある。
- OT環境は自社固有であることが一般的なので、その管理体制は徹底的に自社で考えなければならない。これを一人で背負うのは荷が重く、相談できる環境が求められている。
- セキュリティ以前にITは手段に過ぎないので、そこを心掛けないとベンダーは顧客との対話ができない。

3.3 有識者会議の開催

(2) 有識者会議の開催状況

- 以下の議論を実施した（いずれもオンラインによる開催）。

表3.1 「セキュリティ経営・人材確保の在り方検討タスクフォース」開催状況

会議	開催日	サイバーセキュリティ経営ガイドライン見直し関連（2.5に関するテーマ）	セキュリティ人材活躍モデルの構築及び普及啓発関連（本項に関するテーマ）
第1回	2021年9月10日	● 今年度の調査計画について ● 今年度審議すべき論点の抽出	● 今年度審議すべき論点の抽出 ● 手引き書英訳版で用いる訳語について
第2回	2021年10月12日	● 経営ガイドラインのスコープについて	
第3回	2021年12月3日	● 経営ガイドラインの改訂方針案について ● 海外動向調査結果の報告【済】 ● 機関投資家調査の実施方法について	● 企業調査結果中間報告
第4回	2021年12月27日	● 経営ガイドラインの位置付けについて	● プラス・セキュリティの概念整理 ● 手引書拡充に向けた方針案の検討
第5回	2022年1月25日	● 経営ガイドラインに関するまとめ	● 手引書拡充案の検討 ● 手引き既存コンテンツの見直し
第6回	2022年2月8日	● 機関投資家ヒアリングで得られた意見について ● 経営ガイドラインの改訂について	–
第7回	2022年3月7日	–	● 有識者ヒアリングで得られた意見について ● 手引き見直し方針について
第8回	2022年3月15日	● 経営ガイドラインの改訂についてのまとめ	● OT環境に関するヒアリングで得られた意見について ● 手引き第2版案について
第9回	2022年3月23日（持ち回り開催）	–	● 手引き第2版案レビュー

3.4 文献調査

(1) 対象文献

- 本調査における文献調査において対象とした文献は次表の通りである。

表3.2 米国、EU、英国等におけるサイバーセキュリティ人材の育成・活用に関する文書

文献名	発行機関	発行時期
Initial National Cybersecurity Skills Strategy	英国デジタル・文化・メディア・スポーツ省（DCMS）	2018年12月
Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce	米国商務省・国土安全保障省	2018年5月
Special Publication 800-181r1 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework	米国国立標準技術研究所（NIST）	2020年11月（改定）
The Direction on Security of Network and Information Systems	EU	2016年
European e-Competence Framework 3.0	EU	2014年
Government Cyber Security Strategy: 2022 to 2030	英国Cabinet Office	2022年1月
SFIA（Skills Framework for the Information Age）8	英国SFIA Foundation	2021年9月

表3.3 日本の政府機関や独立行政法人が公表しているサイバーセキュリティ人材の育成・活用に関する文書

文献名	発行機関	発行時期
産業サイバーセキュリティ強化へ向けたアクションプラン	経済産業省	2018年5月30日
DXレポート2.1	経済産業省	2021年8月31日
サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書	内閣サイバーセキュリティセンターNISC）	2018年5月31日
「平成29年度企業において育成すべき人材の知識・スキル及びカリキュラムに関する調査」調査研究報告書	内閣サイバーセキュリティセンター（NISC）委託調査	2018年3月
ITSS+セキュリティ領域	独立行政法人情報処理推進機構（IPA）	2018年4月7日
iコンピテンシ ディクショナリ2018	独立行政法人情報処理推進機構（IPA）	2018年8月17日
情報セキュリティスキル強化についての取り組み	独立行政法人情報処理推進機構（IPA）	2018年4月7日
サイバーセキュリティ経営ガイドライン Ver 2.0実践のためのプラクティス集	独立行政法人情報処理推進機構（IPA）	2019年3月25日

3.3 文献調査

(1) 対象文献（続き）

表3.4 民間団体が公表しているサイバーセキュリティ人材の育成・活用に関する文書

文献名	発行機関	発行時期
キャリアパスグランドデザインの考察_ver1.0	NPO日本ネットワークセキュリティ協会（JNSA） 情報セキュリティ教育事業者連絡会	2019年10月
セキュリティ業務を担う人材のスキル可視化施策の考察～プラス・セキュリティ人材の可視化に向けて～ <1.0 版>	NPO日本ネットワークセキュリティ協会（JNSA） 情報セキュリティ教育事業者連絡会	2019年10月
セキュリティ業務を担う人材の現状調査報告書（2018年下期調査）	NPO日本ネットワークセキュリティ協会（JNSA） 情報セキュリティ教育事業者連絡会	2019年6月
セキュリティ知識分野（SecBoK）人材スキルマップ2019年版	NPO日本ネットワークセキュリティ協会（JNSA）	2019年3月
セキュリティ業務を担う人材のスキル可視化ガイドライン ～プラス・セキュリティ人材の可視化に向けて～ <β版>	NPO日本ネットワークセキュリティ協会（JNSA） 情報セキュリティ教育事業者連絡会	2019年1月
OT セキュリティ人材スキル定義リファレンス	一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会	2019年7月
産業横断サイバーセキュリティ人材育成検討会 第二期最終報告書	一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会	2018年11月
産業横断サイバーセキュリティ人材育成検討会 第一期最終報告書	一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会	2016年9月
CSIRT人材の定義と確保（Ver.2.1）	日本コンピュータセキュリティインシデント対応チーム協議会	2021年8月
統合セキュリティ人材モデル	日本電気・日立製作所・富士通	2018年10月
サイバーリスクハンドブック ～取締役向けハンドブック 日本版～	一般社団法人日本経済団体連合会	2019年10月
セキュリティ業務を担う人材のスキル可視化における概念検証報告書～トライアル結果の考察～	NPO日本ネットワークセキュリティ協会（JNSA） 情報セキュリティ教育事業者連絡会	2019年11月

3.3 文献調査

(2) 調査結果

- 文献調査結果の例として、2021年8月に公表された経済産業省のDXレポート2.1における企業類型を示す。
  - ユーザ企業とベンダー企業の分類から下図のような類型への変化が見込まれる中で、セキュリティ対策を担う人材の役割も変わっていくと考えられる。

① 企業の変革を共に推進するパートナー	**<u>例）コンサルティング事業者A</u>** • 経営トップから一気通貫で企業の変革を推進 • 組織の意識改革、再編、運用・保守を統合的にサポート • 顧客とのDX専門会社を設立
② DXに必要な技術を提供するパートナー	**<u>例）SI事業者B</u>** • 内製化志向の企業へアジャイルケイパビリティ習得を支援 • アジャイル開発支援/コーチング/組織変革をメニュー提供
③ 共通プラットフォームの提供主体	**<u>例）プラットフォーム事業者C</u>** • 非競争領域などの協調領域に対して、業界毎や課題毎に共通のプラット フォームを構築し、他社にサービスとして提供
④ 新ビジネス・サービスの提供主体	**<u>例）大手小売り事業者D</u>** • サービス開発はすべて内製であり、EC事業やコンテンツ事業などテクノロジー起点で業態を継続変革 • 自社のDXのために開発したデジタルソリューションを他社へ提供

図3.1 DXレポート2.1における企業類型と企業例

https://www.meti.go.jp/press/2021/08/20210831005/20210831005.html

3.5 政府会議等における議論の把握

- 本調査の実施にあたり、下記に示す政府会議等の公表情報（配付資料、議事録、報告書等）をもとに、有識者による議論を把握し、本事業の調査内容において整合を諮るとともに、調査結果の分析や報告書の作成に反映した。
  - 経済産業省「産業サイバーセキュリティ研究会」
    - WG1『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース 第5回会合（2021年11月29日開催）、第6回会合（2022年3月9日開催）
    - WG1『第3層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース 第5回会合（2021年12月13日開催）
    - WG1 サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース 第5回会合（2021年10月29日開催）、第6回会合（2022年3月3日開催）
    - WG1 電力サブワーキンググループ 第12回会合（2021年12月24日開催）、第13回会合（2022年2月21日開催）
    - WG1 宇宙産業サブワーキンググループ 第3回会合（2021年11月4日開催）、第4回会合（2022年2月7日開催）
    - WG1 工場サブワーキンググループ 第1回会合（2022年1月6日開催）
    - WG2 第8回会合（2022年3月23日開催）
  - 内閣サイバーセキュリティセンター「サイバーセキュリティ戦略本部」
    - 普及啓発・人材育成専門調査会 第16回会合（2021年12月9日開催）

3.6 「セキュリティ体制構築・人材確保の手引き（第1.1版）」の内容拡充・改善及び普及啓発

(1) 構成見直し方針

- 企業調査、有識者ヒアリング調査、及び有識者会議における審議の結果を踏まえ、以下の目的で手引きを利用するにはボリュームが大きすぎ、どのようにすべきかのポイントを掴みにくいことから、対象読者を想定したスリム化が必要との方針で合意された。
  - ①　これまであまり取り組めていない組織の担当者にポイントを伝える。
  - ②　すでに取り組んでいる企業にも、点検のために目を通してもらう。
- 上記のスリム化のための解決策として、次の案が示された。
  - ➢ “報告書”ではなく“手引き”とするため、全体的にポイントを絞り込む。
  - ➢ 「本来このように利用してほしい」、「このような活用の仕方がある」ということを整理して、どう利用したらよいのかの、“手引きの手引き”を作ることを検討する。
    - 現行の手引きでは単に整理（網羅）したのみの部分が多いので、例えば「セキュリティ統括機能は4パターンあり、300人くらいの組織なら一般的にはA、さらにレベルを上げたい場合はB、大企業はC、その理由はこの通りで、もしそうなっていなかったらこのように移行すべき」のように、読み手がどこを読めばよいかがわかるようにする。

3.6 「セキュリティ体制構築・人材確保の手引き（第1.1版）」の内容拡充・改善及び普及啓発

(2) 構成見直しの具体的なアクション

- (1)の方針をもとに、次のような取組を通じて第２版を作ることとなった。

① 原則的なもの

- 経営ガイドラインで扱うべき内容（経営者のリーダーシップが重要等）は手引きから除く。
  報告書テイストの部分は削除する（これまでのトレンドのグラフなど）。
- 例示は単に示すのではなく、「このような条件のときは、これ」という対応関係を付けて整理する。
- 文字の量を減らす、似たような図は１枚に集約する、等でページ数を削減する。

② 各論について

- 「経営層のリーダーシップ」の代わりに、「サイバーセキュリティに関して「やるべきこと」の明確化」として予め機能やタスクを明らかにしておくべきことを説明する。そこでITSS＋の説明をしてタスクを例示する。
- 「セキュリティ統括機能」の説明で、セキュリティ対策のすべてを取り仕切るものではなく、現場が負うべき責任を支援するくらいの位置付けであることを追記する。
- 「プラス・セキュリティ」にマネジメント的な要素も含まれることを説明する。
- 業種別の体制例は巻末付録とする。
- コラムは類似した内容のものを集約して掲載。

3.7 政策的課題の洗い出し及び施策の検討

- 個々の企業だけでは対応が難しく、国や公的機関が何らかの施策を講じるべきセキュリティ体制・人材の確保に関する課題として、本調査を通じて明らかになった事項とその解決のための施策の方向性を示す。

① セキュリティ体制・人材の確保に関する課題

- ユーザ企業とベンダー企業の区分の変化
  - 3.3(2)に例示したように、DXの進展の中で、「ユーザ企業であればこのような役割定義が必要」といったモデル化が難しくなっており、手引き読者において自社におけるセキュリティ体制をどのように考えるべきかがわかりにくくなっている。
- 「プラス・セキュリティ」の対象の拡大
  - これまで、アプリケーションの設計開発の過程でSecurity By Designを実践したり、DXの企画担当者が事業戦略の中でサイバーセキュリティを考慮したりするなど、プラス・セキュリティが必要となる業務は限られるイメージがあったものが、DXに限らないデジタル活用の普及の中で、より多くの業務や役割においてサイバーセキュリティを意識することが求められるようになっており、手引き1.1版での説明が実態にそぐわなくなりつつある。

② 課題解決の方向性

- ユーザ企業やIT関連業務に絞らない説明への移行
  - 3.6で行う手引き見直しの中では、想定読者をユーザ企業に限定するのではなく、複数のユースケースに応じた使い方（手引きの手引き）を示すことで①に示した課題に対処している。
  - 「プラス・セキュリティ」の考え方が広まる中で、あえて「セキュリティ人材」とカテゴライズすべき役割はセキュリティサービスを提供する事業者の担当者などに限られてくるとも見込まれ、読者にとって違和感のない表現について今後検討を重ねていくことが求められる。

4. 情報セキュリティサービス活用・普及に関する調査

4.1 有識者会議の開催

(1) 有識者の選定

- 調査趣旨を踏まえ、以下の目的を中心とする検討を行うため、有識者10名で構成される「情報セキュリティサービス普及促進に関する検討会」を設置した。
  - ➢ 情報セキュリティサービス基準（附則を含む）において見直しが必要な事項
  - ➢ 情報セキュリティサービス審査登録制度の普及促進における課題と取組の検討（地域ITベンダーの取込み、ユーザ企業の本制度の利用状況や期待を活用したベンダーへの登録働きかけ等）

(2) 有識者会議の開催状況

- (1)に示したメンバーにて、以下の計3回の検討を実施した。

表4.1 「情報セキュリティサービス普及促進に関する検討会」2021年度開催状況

会議	開催日	おもな議題
第1回	2021年9月28日	● 情報セキュリティサービス基準見直し案について ● 地域ITベンダーの登録方法について ● 情報セキュリティサービス審査登録制度の普及法策案について
第2回	2021年12月2日	● パブリックコメント案について ● 地域ITベンダーの登録方法について
第3回	2022年1月26日	● パブリックコメント対応方針案について ● 情報セキュリティサービス審査登録制度の普及啓発方法について

4.2 有識者会議の開催

(3) 有識者会議におけるおもな合意事項

- 「情報セキュリティサービス普及促進に関する検討会」において以下の各項の審議を実施した。
  - 情報セキュリティサービス基準の見直しについて
  - パブリックコメント対応について
  - 情報セキュリティサービス審査登録制度の普及啓発方法について

5. まとめ

- 本調査では、本報告書2.～4.までの各項において示した調査項目に基づき、企業におけるサイバーセキュリティ経営の実現を支援する取組に関する調査を実施した。
  - 企業経営層とその指示を受ける担当者を対象とするサイバーセキュリティ経営ガイドラインの改訂方針の検討及び可視化ツールの普及促進
  - 企業、ベンダー及び有識者を対象とする調査に基づく「サイバーセキュリティ体制の構築・人材確保の手引き」の改訂
  - 情報セキュリティサービス基準の改訂及びこれを用いて運用される情報セキュリティサービス審査登録制度の普及促進策の検討
- これらの取組は、国内企業や社会におけるデジタル活用の進展がもたらすサイバーセキュリティリスクの変化に対応するために適時に実施すべきものであり、本調査の実施期間中でも必要な見直しを実践することでニーズに対応している。一方で、経営ガイドラインの改訂については、改訂による影響も見据えて改訂内容を吟味する必要があることから、本調査においては改訂素案の作成にとどめ、具体的な改訂案の作成は次年度に実施することを想定している。3.7に示したように、企業におけるデジタル活用の形態が多様化する中で、いわゆるユーザ企業における体制も標準的なものとして表現することが難しくなっており、啓発の対象となる企業の関係者にとって理解しやすいものとしていくために、継続的な改善に取り組むことが求められる。