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）

調査報告書

2021年3月

みずほ情報総研株式会社

目 次

1. 調査実施の目的、実施内容等

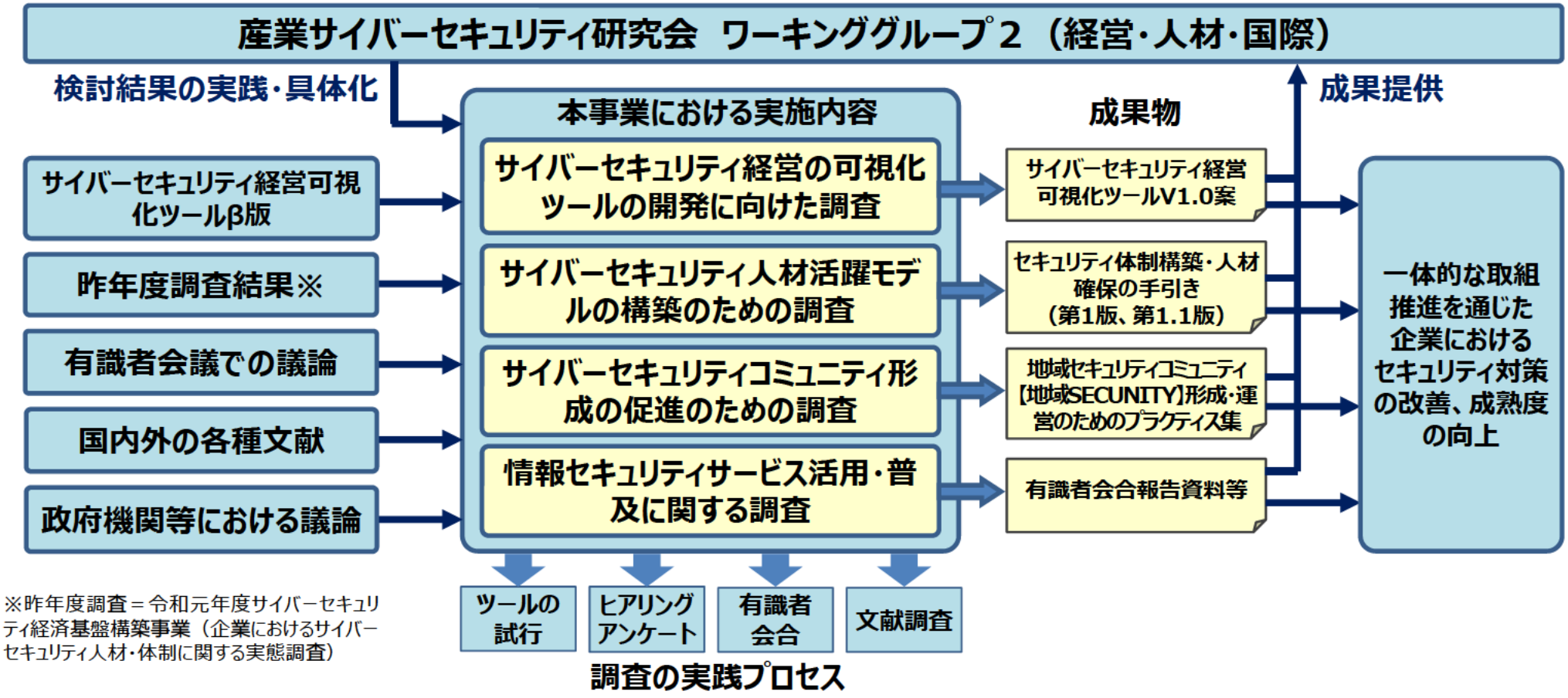
(1) 調査目的

- 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、セキュリティ人材にはこれを支えるセキュリティコミュニティが必要となる。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）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
  - サイバーセキュリティコミュニティ形成の促進のための調査
  - 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（みずほ情報総研株式会社及び一般社団法人日本情報システム・ユーザー協会）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４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における今後の取組に資するように努めた。



※昨年度調査＝令和元年度サイバーセキュリティ経済基盤構築事業（企業におけるサイバーセキュリティ人材・体制に関する実態調査）

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経営ガイドラインベースの可視化ツールβ版を用いた企業調査の企画・実施	● 製造業16社、非製造業12社による試行を実施し、使った感想、改善要望、利用シーン/想定利用者等についての意見をとりまとめた。
	他団体の可視化ツールの調査・動向把握	● 国内外の可視化に関するツール、方式、方法論の収集を行った。
	有識者会議の開催	● 企業のセキュリティ対策に知見を有する5名の有識者によるタスクフォースを設置し、9回にわたって議論を行った。
	可視化ツールVer1.0案の作成	● 調査結果をもとにβ版を改修してV1.0版とする方針を定めた。
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	企業調査	● 10社を対象に情報セキュリティ組織体制及びセキュリティ関連人材に関するヒアリング調査を実施し、結果をティップス集にとりまとめた。 ● IT/セキュリティベンダー6者にヒアリングを実施し、結果をとりまとめた。
	有識者ヒアリング	● 専門家・学識者計6名とICSCoE修了者2名にヒアリングを実施し、結果を「セキュリティ体制構築・人材確保の手引き」に反映した。
	有識者会議の開催	● 企業のセキュリティ対策に知見を有する5名の有識者によるタスクフォースを設置し、9回にわたって議論を行った。
	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。
	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。
	「セキュリティ体制構築・人材確保の手引き」の開発	● 有識者会議及びヒアリング調査結果をもとに、2020年9月に第1版、2021年3月に第1.1版のそれぞれコンテンツを作成した。
	政策的課題の洗い出し及び施策の検討	● 個々の企業では対応が難しく、国や公的機関が何らかの施策を講じるべき課題として、「共通言語」の普及等の事項を洗い出した。

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
3. サイバーセキュリティコミュニティ形成の促進のための調査	サイバーセキュリティコミュニティの調査	● 全国の9事例についてヒアリングによる事例調査を実施した。 ● 調査結果をもとに「地域セキュリティコミュニティ【地域SECUNITY】形成・運営のためのプラクティス集」を作成した。
	地域に駆けつけ可能な専門家や専門家派遣制度等の情報・問合せリストの作成	● 文献・ヒアリング調査等をもとに下表に示す駆けつけ可能な専門家や専門家派遣制度等の情報・問合せリストを作成した。
	有識者ヒアリング	● 地域のサイバーセキュリティの活動やコミュニティ形成に詳しい有識者11名にヒアリング調査を実施し、コミュニティの実態や支援の在り方について調査した。
	イベント情報や取組共有を目的とした国内政策調査	● 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普及啓発・人材育成ポータルサイト』等、関連する政策について調査した。 ● ユーザー企業でセキュリティ対策に従事するモニターを対象とするアンケート調査を実施し、コミュニティ活動への参加意向等について調査・分析した。
4. 情報セキュリティサービス活用・普及に関する調査	情報セキュリティサービス活用・普及に関する企業調査の実施	● ユーザー企業等11者、ベンダー企業等18者を対象にヒアリング調査を実施し、情報セキュリティサービス審査登録制度の認知度や利用状況、メリット、改善要望等について、セキュリティサービスの利用実態と合わせて調査した。 ● ユーザー企業でセキュリティ対策に従事するモニターを対象とするアンケート調査を実施し、情報セキュリティサービス審査登録制度の認知度や利用状況、サービスへの需要等について調査・分析した。
	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普及及び改善に関する議論を行った。
5. 報告書の作成	報告書の作成	● 1～4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の可視化ツールの開発に向けた調査

2.1 可視化ツールβ版を用いた企業調査

(1) 調査概要

- 調査対象企業の選定にあたっては、以下の条件を参考に実施した。
  - 上場企業（東京証券取引所第一部、第二部及びマザーズ上場企業）
  - 従業員数が300人以上
  - グループ企業を多数保有している／いない、海外拠点を保有している／いないといった企業の業態の違いを考慮し、できるだけ幅広い条件の企業を含める
- 本調査の実施に協力いただいたのは次表の28社である。

表2.1　調査協力企業

製造業	非製造業
16社	12社

2.1 可視化ツールβ版を用いた企業調査

(2) β版試行の回答結果（各指示ごとの平均値と成熟度）

- β版試行参加企業28社の評価結果を示す。
  - 各指標ごとの平均値が1点台をピンク、2点台を黄色とした
- 試行の結果：
  - 成熟度A：6社
  - 成熟度B：7社
  - 成熟度C：15社

となり、令和元年度調査結果より厳しめの評価結果であった。

表2.2　調査協力企業による自己評価結果

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
KK-1	機械器具製造	2.3	3.3	2.0	2.0	1.8	1.3	1.0	1.0	1.3	1.0	C
KD-1	建築・土木	5.0	3.3	3.8	4.7	3.7	3.3	2.8	3.0	2.3	4.0	B
KK-2	機械器具製造	4.3	5.0	4.0	3.0	3.5	3.3	4.0	4.5	1.7	3.5	B
KY-1	金融	5.0	5.0	4.5	4.3	4.3	4.0	5.0	4.0	4.0	4.5	A
KK-3	機械器具製造	4.7	1.7	2.3	3.3	3.9	3.8	2.6	2.5	1.3	3.5	B
KK-4	機械器具製造	2.3	2.7	1.3	1.3	2.7	1.8	1.6	1.5	2.0	1.0	C
KK-5	機械器具製造	4.0	2.7	2.3	2.3	2.7	1.8	1.8	1.0	2.0	2.0	C
SS-1	素材製造	2.0	1.7	2.3	2.0	3.6	2.3	1.4	1.0	1.7	1.5	C
KY-2	金融	5.0	5.0	5.0	4.0	5.0	5.0	5.0	5.0	5.0	4.0	A
KK-6	機械器具製造	4.3	3.7	2.5	3.3	2.5	1.8	3.2	1.0	1.7	3.0	B
SS-2	素材製造	3.3	2.3	1.5	2.3	2.7	2.0	2.0	2.0	2.3	2.5	C
SS-3	素材製造	4.0	3.0	2.0	2.0	2.9	2.3	2.4	1.0	1.7	2.5	C
SI-1	社会インフラ	1.7	2.7	1.3	2.7	2.8	2.5	2.4	4.0	1.7	2.5	C
SI-2	社会インフラ	4.7	4.7	4.8	3.3	4.5	4.0	3.2	3.0	3.0	3.0	A
SV-1	サービス	4.3	3.0	3.3	1.3	2.9	1.5	2.4	1.0	2.0	1.5	C
KD-2	建築・土木	3.0	2.0	1.8	1.3	2.9	1.8	2.2	1.0	1.3	2.0	C
KK-7	機械器具製造	3.0	2.3	2.3	3.0	3.6	4.3	2.2	1.5	1.7	1.0	C
KY-3	金融	4.3	2.3	2.8	4.0	4.6	2.0	3.8	1.0	1.7	4.0	B
SV-2	サービス	4.7	5.0	4.5	5.0	4.9	4.8	5.0	5.0	4.0	3.5	A
SI-3	社会インフラ	3.3	2.7	2.3	2.0	2.7	2.0	3.0	1.0	1.7	1.5	C
SS-4	素材製造	4.0	1.7	3.0	2.3	2.4	2.8	4.2	1.0	2.0	3.0	C
KK-8	機械器具製造	2.0	1.0	1.0	1.0	1.6	1.5	1.8	1.0	1.0	2.5	C
KK-9	機械器具製造	3.0	2.3	1.0	2.3	2.7	1.3	1.6	1.0	1.3	2.0	C
SS-5	素材製造	2.0	1.0	1.3	2.3	3.1	1.0	1.4	1.0	1.0	1.5	C
KK-10	機械器具製造	4.7	3.7	4.5	4.0	4.8	4.5	4.6	4.5	4.3	5.0	A
KD-3	建築・土木	3.0	3.0	2.8	2.7	3.4	3.0	2.2	2.0	2.0	3.0	B
SI-4	社会インフラ	5.0	3.7	4.3	3.3	4.4	3.5	3.4	3.0	3.0	3.0	B
KK-11	機械器具製造	5.0	4.7	4.3	3.3	4.8	4.5	4.6	3.0	4.0	4.0	A

2.1 可視化ツールβ版を用いた企業調査

(3) β版回答企業の成熟度別平均値

- 全体平均では指示1が3.7で最も高い。指示2～7および10は3前後で概ねセキュリティ対策が実施できているが、指示8、9は2.2と低く復旧体制の整備とサプライチェーン全体の対策が遅れている。
- 成熟度A企業の平均はすべて4以上でセキュリティ対策のPDCAが回っている。
- 成熟度B企業では指示1が4.4と突出して高く、リスクの認識や対応方針はできている。一方、指示9が2.0と最も低くサプライチェーン全体の対策が遅れている。
- 成熟度C企業では指示1が3.0でリスクの認識や対応方針はできているが、他は3以下であり全体的に対策の強化が必要である。

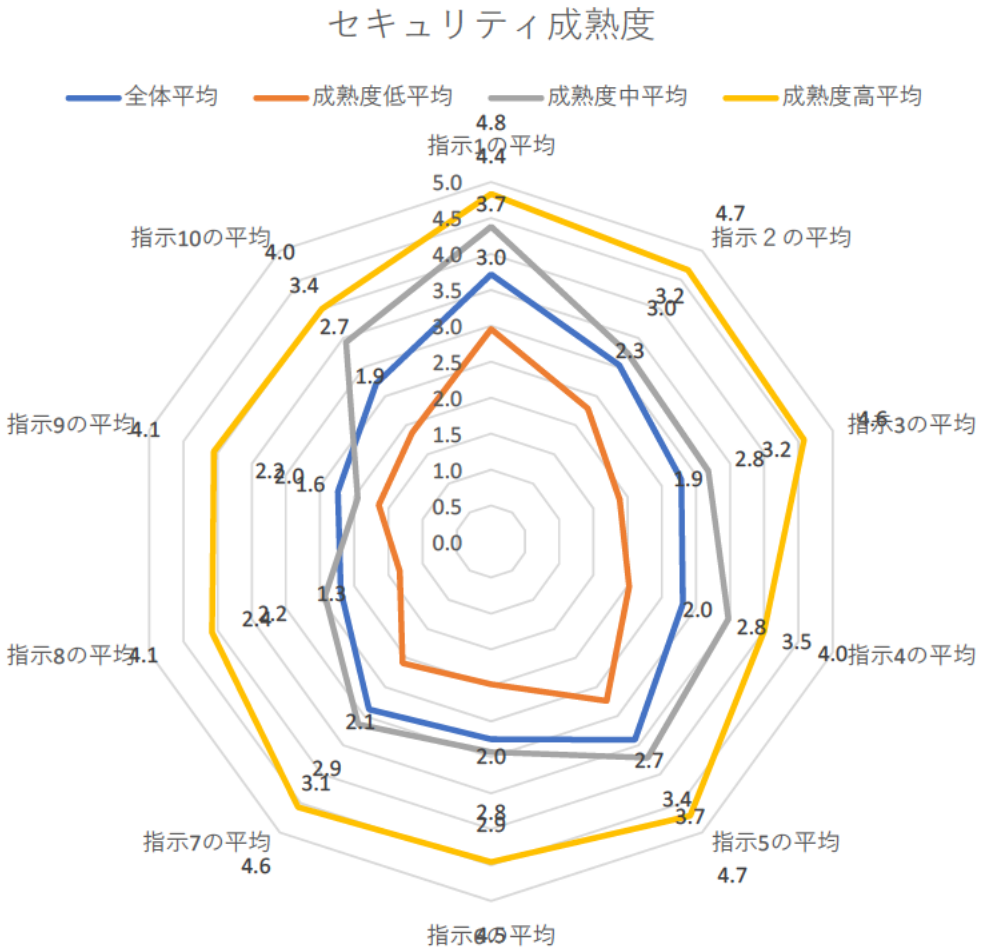


図2.1　成熟度別平均値のレーダーチャート

表2.3　調査協力企業による自己評価の成熟度カテゴリ毎の平均

	指示1	指示2	指示3	指示4	指示5	指示6	指示7	指示8	指示9	指示10
全体平均	3.7	3.0	2.8	2.8	3.4	2.8	2.9	2.2	2.2	2.7
成熟度C平均	3.0	2.3	1.9	2.0	2.7	2.0	2.1	1.3	1.6	1.9
成熟度B平均	4.4	3.2	3.2	3.5	3.7	2.9	3.1	2.4	2.0	3.4
成熟度A平均	4.8	4.7	4.6	4.0	4.7	4.5	4.6	4.1	4.1	4.0

2.1 可視化ツールβ版を用いた企業調査

(4) 可視化ツールβ版評価結果（カルテ）イメージ

■ 成熟度A企業の例

会社名	**KY-1**
業種グループ	**金融**
成熟度総合評価	**A**

指示ごとの平均値と成熟度平均値との差

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
5.0	5.0	4.5	4.3	4.3	4.0	5.0	4.0	4.0	4.5

全体平均	3.6	2.9	2.7	2.8	3.3	2.6	2.8	2.1	2.1	2.6
成熟度C平均	3.0	2.3	1.9	2.0	2.7	2.0	2.1	1.3	1.6	1.9
成熟度B平均	4.5	3.2	3.1	3.7	3.6	2.8	3.3	2.4	1.7	3.6
成熟度A平均	4.8	4.7	4.7	4.1	4.7	4.5	4.6	4.3	4.1	4.0

・指示１，２，７はレベル5に達している
・指示６，８，９はレベル4で改善の余地がある

更なる成熟度向上のヒント

ヒント１：
成熟度を更に向上するには指示6の改善が必要です。サイバーセキュリティのKPIを決め、経営会議に定期的に報告するとともに経営の主導で対策を実施しましょう。
実施にあたってはティップス6－Xを参照してください。

ヒント２：
指示８も改善が必要です。
インシデント被害による復旧計画を策定し、訓練を行いましょう。
実施にあたってはティップス8－Xを参照してください。

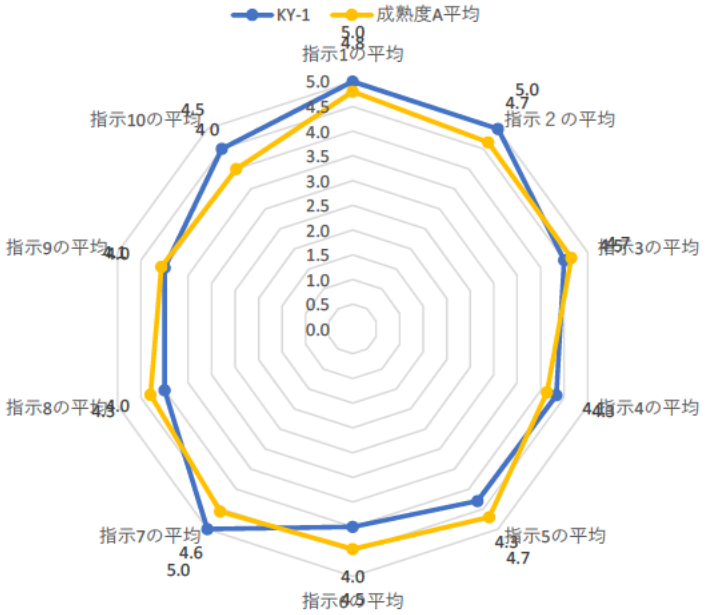


図2.2　評価結果（カルテ）イメージ（成熟度Aの企業例）

2.1 可視化ツールβ版を用いた企業調査

(4) 可視化ツールβ版評価結果（カルテ）イメージ

■ 成熟度B企業の例

会社名	**KK-2**
業種グループ	**機械器具製造**
成熟度総合評価	**B**

指示ごとの平均値と成熟度平均値との差

	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
	4.3	5.0	4.0	3.0	3.5	3.3	4.0	4.5	1.7	3.5
全体平均	3.6	2.9	2.7	2.8	3.3	2.6	2.8	2.1	2.1	2.6
成熟度C平均	3.0	2.3	1.9	2.0	2.7	2.0	2.1	1.3	1.6	1.9
成熟度B平均	4.5	3.2	3.1	3.7	3.6	2.8	3.3	2.4	1.7	3.6
成熟度A平均	4.8	4.7	4.7	4.1	4.7	4.5	4.6	4.3	4.1	4.0
成熟度Aとの差	0.5	-0.3	0.7	1.1	1.2	1.2	0.6	-0.2	2.4	0.5

・指示４、５、６が成熟度Aと１ポイント以上差がある
・指示９が成熟度Aと２ポイント以上差がある

成熟度Aになるためのヒント

ヒント１：
指示９の改善が急務です。
グループ企業に関するリスク分析を行い対策を実施し結果を確認しましょう。
実施にあたってはティップス９－Xを参照してください。

ヒント２：
指示４、５、６も改善が必要です。
サイバーセキュリティリスク対応計画を策定してください。
実施にあたってはティップス４－Xを参照してください。

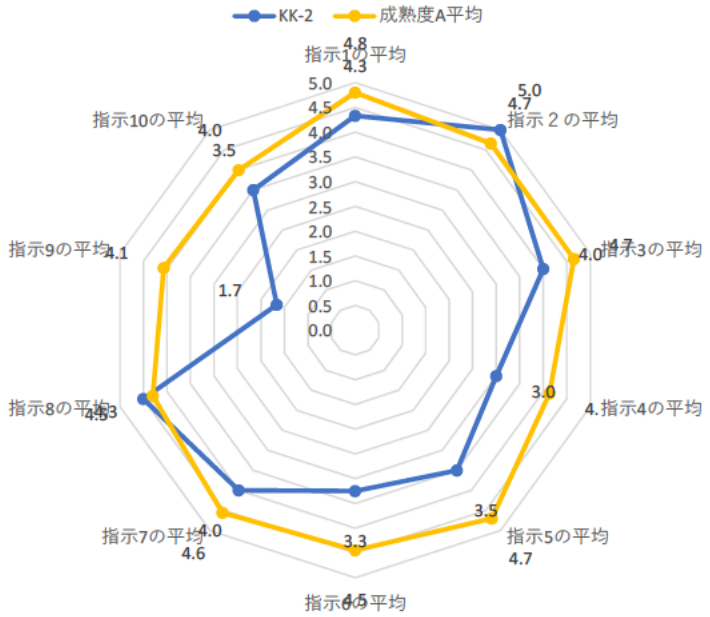


図2.3　評価結果（カルテ）イメージ（成熟度Bの企業例）

2.1 可視化ツールβ版を用いた企業調査

(4) 可視化ツールβ版評価結果（カルテ）イメージ

■ 成熟度C企業の例

会社名	SV-1
業種グループ	サービス
成熟度総合評価	C

指示ごとの平均値と成熟度平均値との差

	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
	4.3	3.0	3.3	1.3	2.9	1.5	2.4	1.0	2.0	1.5
全体平均	3.6	2.9	2.7	2.8	3.3	2.6	2.8	2.1	2.1	2.6
成熟度C平均	3.0	2.3	1.9	2.0	2.7	2.0	2.1	1.3	1.6	1.9
成熟度B平均	4.5	3.2	3.1	3.7	3.6	2.8	3.3	2.4	1.7	3.6
成熟度A平均	4.8	4.7	4.7	4.1	4.7	4.5	4.6	4.3	4.1	4.0
成熟度Bとの差	0.2	0.2	-0.2	2.3	0.7	1.3	0.9	1.4	-0.3	2.1

・指示6，８が成熟度Bと１ポイント以上差がある
・指示4，10が成熟度Bと２ポイント以上差がある

成熟度Bになるためのヒント

ヒント１：
指示4の改善が急務です。
守るべきIT資産に対するサイバー攻撃の脅威を認識しリスク対応計画を立案しましょう。
実施にあたってはティップス4－Xを参照してください。

ヒント２：
指示10も改善が必要です。
情報共有活動に参画しサイバーセキュリティの情報を入手し対策に活用しましょう。
実施にあたってはティップス10－Xを参照してください。

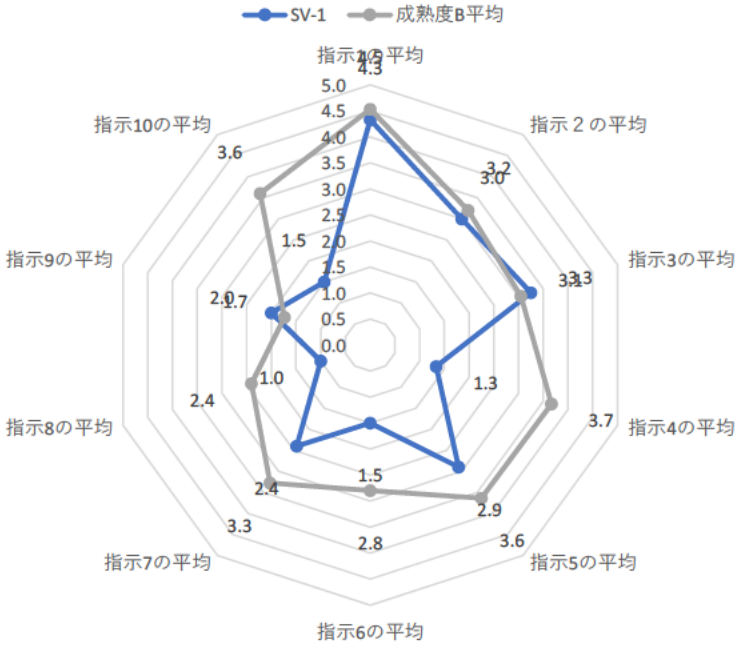


図2.4　評価結果（カルテ）イメージ（成熟度Cの企業例）

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

- 可視化ツールβ版について、次表の項目について実施したアンケート調査の結果を示す（回答総数26件）。

表2.4　アンケート設問一覧

Q1. 貴社名
Q2. 貴社の業種グループ
Q3. 回答者の属性
Q4. セキュリティ成熟度可視化ツールを試行した感想（使い勝手、設問内容、選択肢など）
Q5. セキュリティ成熟度可視化ツールの利用シーンとしてどのようなことが想定されるか
Q6. セキュリティ成熟度可視化ツールの想定利用者
Q7. セキュリティ成熟度可視化ツールは自己評価ツールだが、評価の甘辛を抑えるにはどのようか取組みが必要か
Q8. セキュリティ成熟度可視化ツールの総合的な評価
Q9. 修正すべき内容
Q10. サイバーセキュリティ経営ガイドラインの活用状況
Q11. サイバーセキュリティに関する検討において参考としている基準・ガイドライン等
Q12. 自社のセキュリティ対策状況や成熟度を評価するために用いている指標

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

■ 回答企業の業種グループ

- 製造業（素材製造＋機械器具製造）が約６割、非製造業が約４割
- 商社・流通は回答企業がなかった

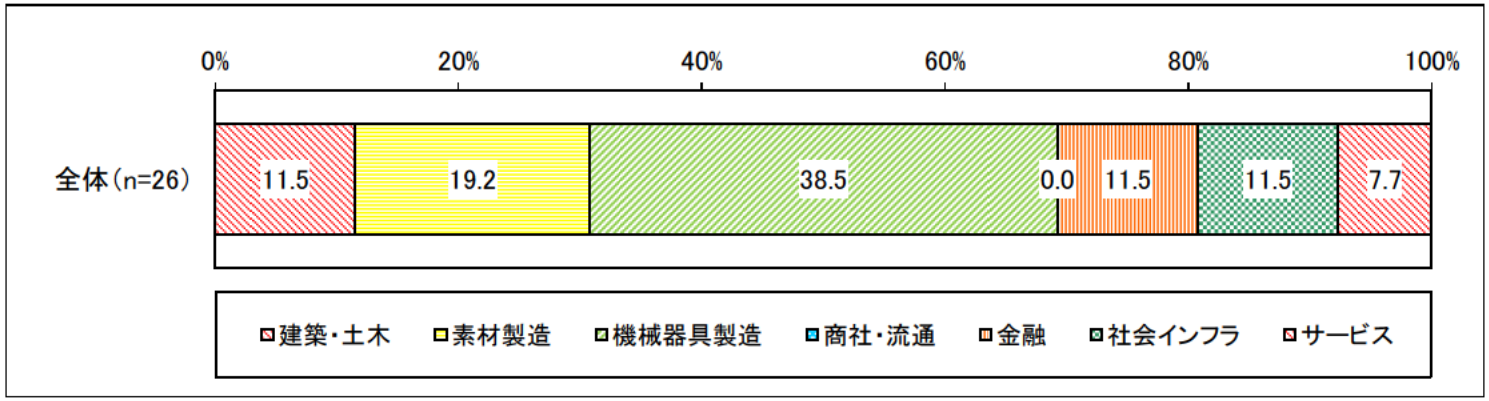


図2.5　回答企業の業種グループ

■ 回答企業の属性

- 情報セキュリティ統括責任者が約2割、統括担当者（専任）が約4割
- 兼務の情報セキュリティ担当者も約35%

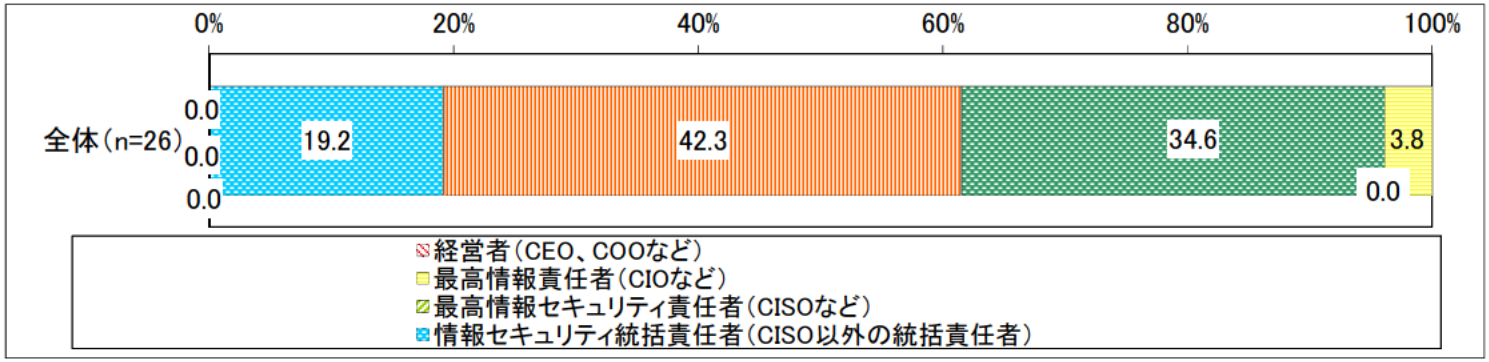


図2.6　回答企業の属性

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

■ 可視化ツールの総合評価

- 利用できる、一部修正すれば利用できるの合計が約8割
- 一方、利用しない、他のツールを使っているので必要ないが各1社

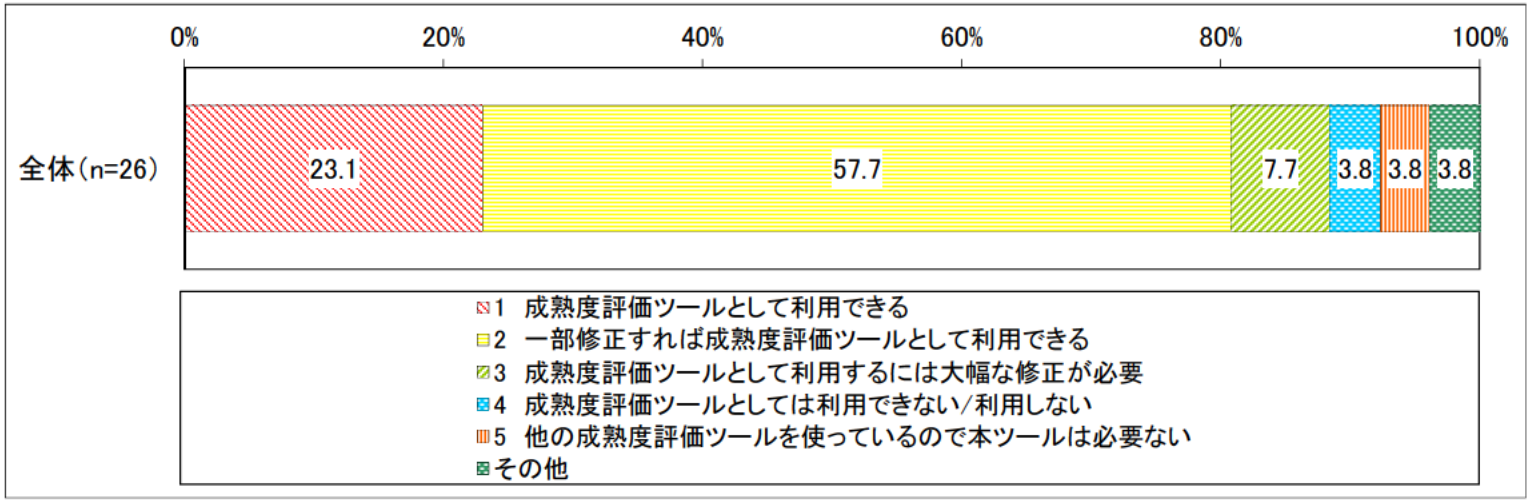


図2.7 可視化ツールの総合評価

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

■ 可視化ツールの利用シーン（複数回答）

- 3社に2社はセキュリティ対策の検討、ベンチマークに利用を想定
- 約半数の企業は成熟度評価結果を経営層に報告
- 関連会社の成熟度を評価しセキュリティガバナンスを行う企業も約3割

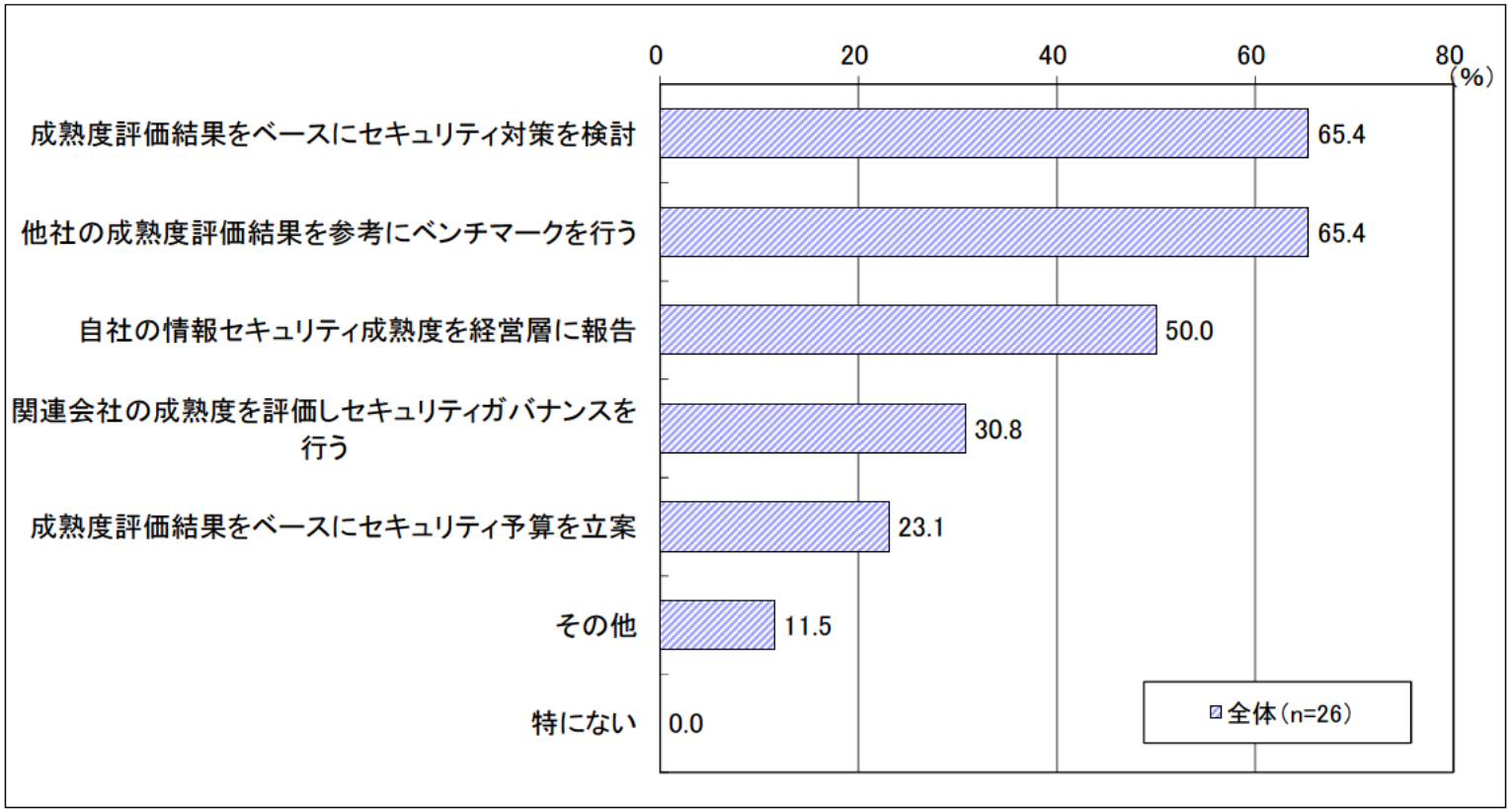


図2.8　可視化ツールの利用シーン

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

■ 製造・非製造別　可視化ツールの利用シーン（複数回答）

- 製造業・非製造業ともセキュリティ対策検討、ベンチマークが最も多い
- 次いで製造業では経営層に報告が多く60%、非製造業では関連会社のセキュリティガバナンスが多く45.5%

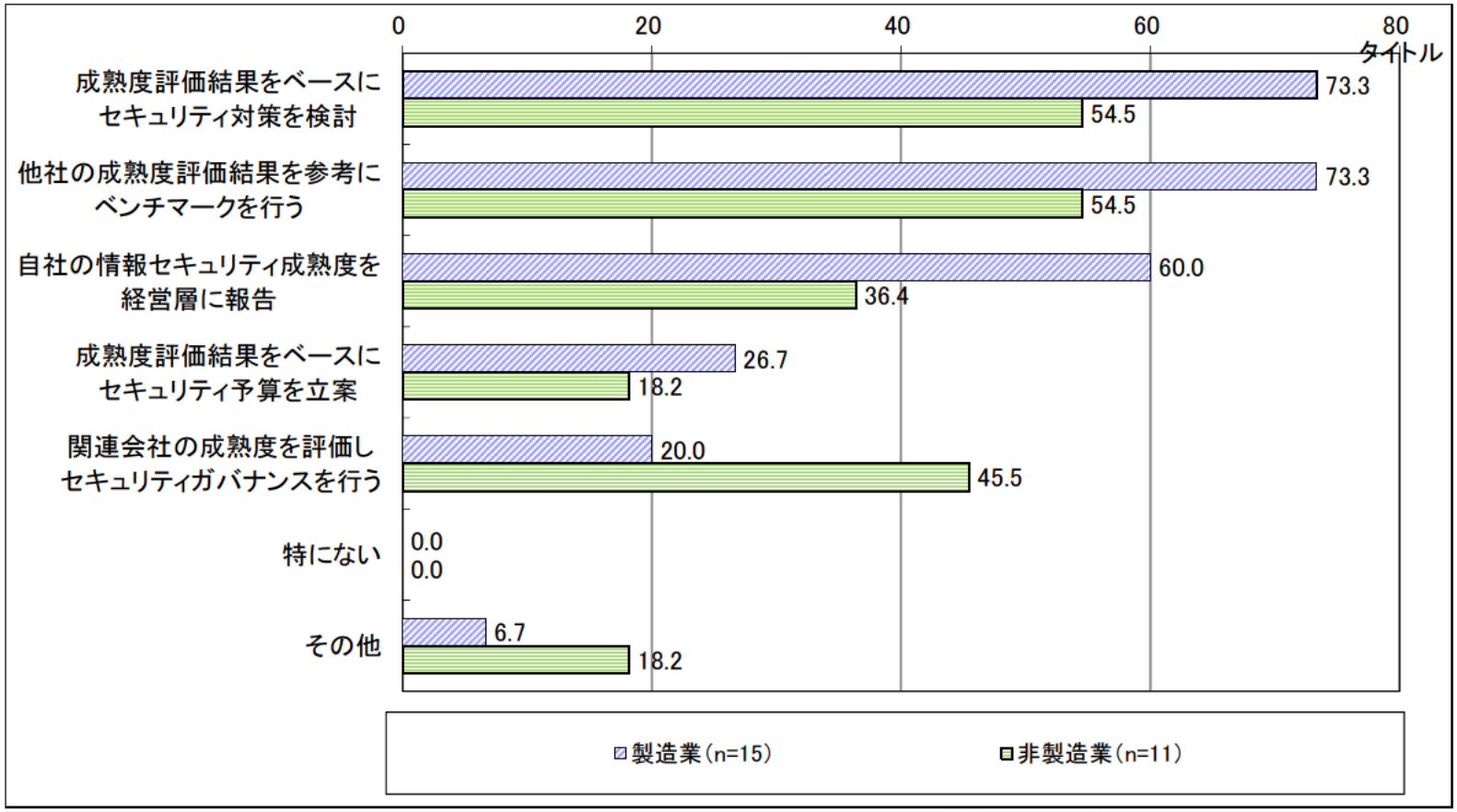


図2.9　可視化ツールの利用シーン（製造・非製造別）

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

■ 可視化ツールの想定利用者（複数回答）

- 想定利用者は4社に3社はセキュリティ統括の担当者
- CISO、セキュリティ統括責任者は約6割
- 経営者が利用すると想定しているのは7.7%（2社）に留まる

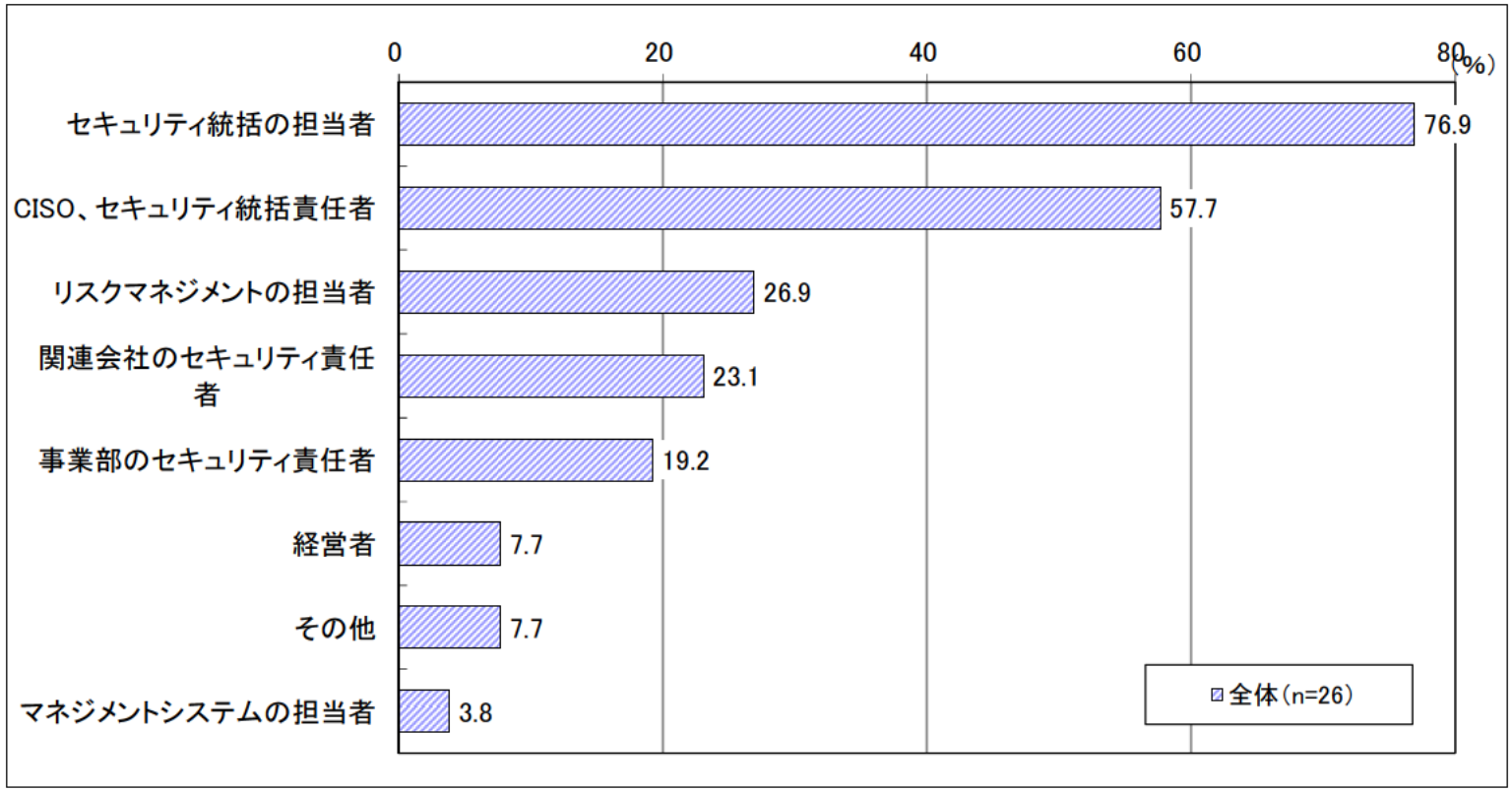


図2.10　可視化ツールの想定利用者

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

■ 製造・非製造別　可視化ツールの想定利用者（複数回答）

- 製造業・非製造業ともセキュリティ統括担当者、統括責任者が1位、2位
- 次いで製造業では関連会社のセキュリティ責任者で33.3%、非製造業ではリスクマネジメント担当者で36.4%

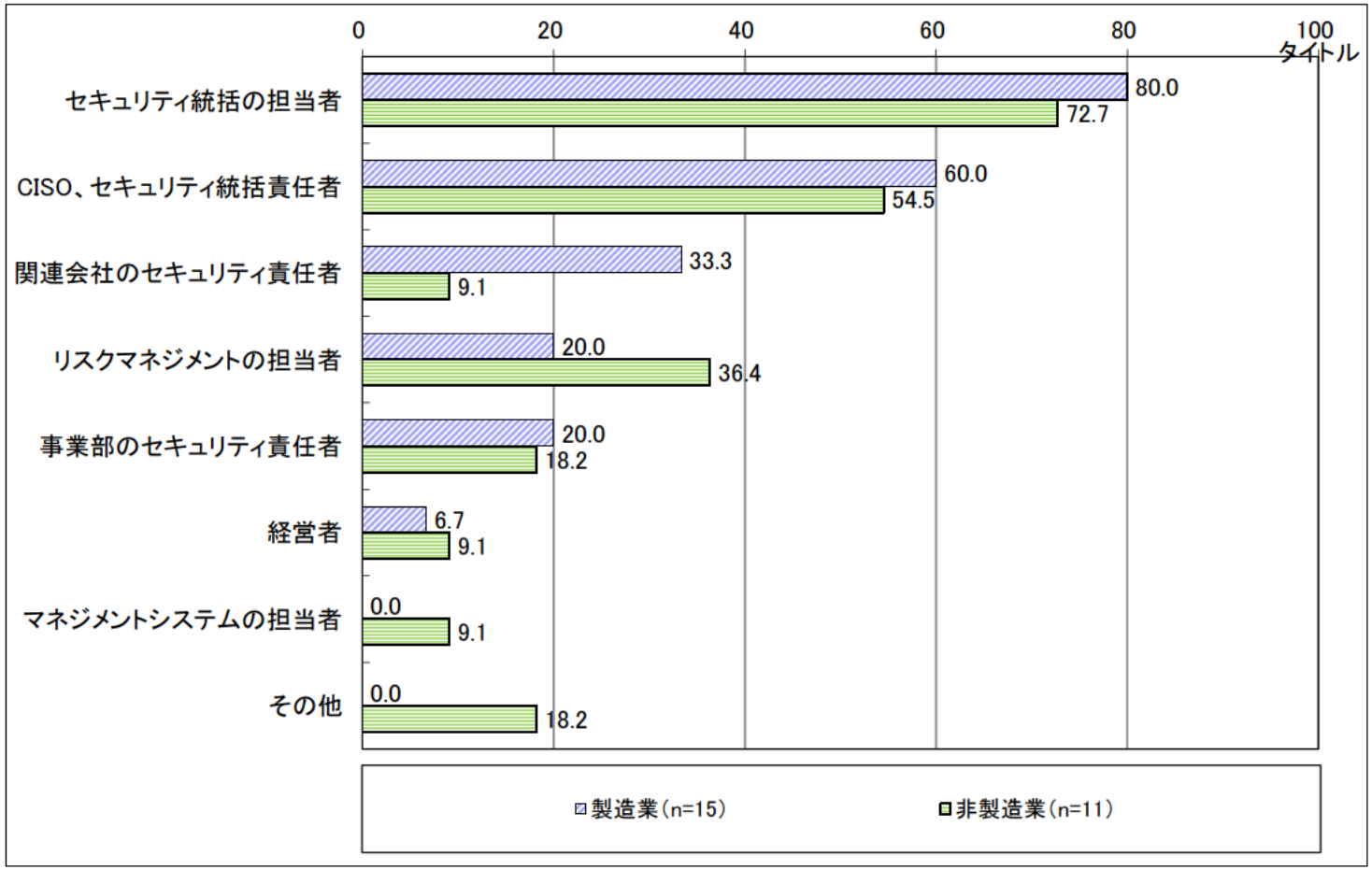


図2.11　可視化ツールの想定利用者（製造・非製造別）

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

■ 可視化ツールの甘辛を抑える取組み

- 基準となる回答を用意するが約35%で最も多く、備考（回答のヒント）の充実が望まれる
- 複数の評価者で評価するが約3割、監査部門が評価するが約2割で評価体制の工夫も必要。
- ツールとしてはWeb直接入力だけではなく調査票をダウンロードして使う選択肢も必要

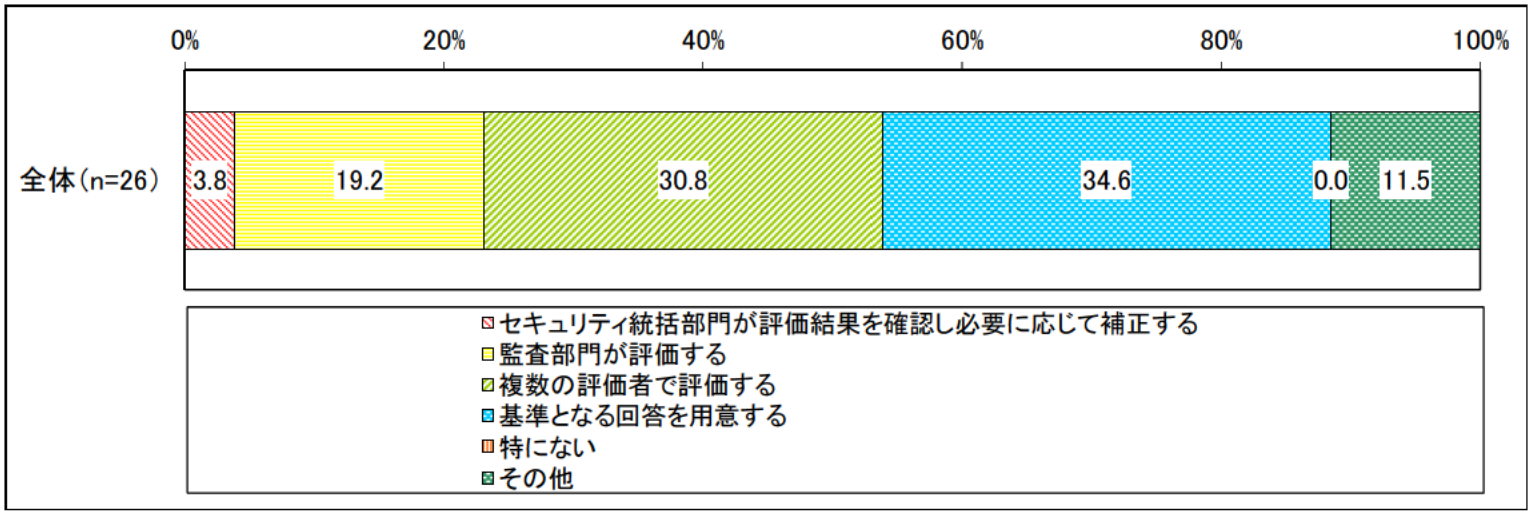


図2.12　可視化ツールの甘辛を抑える取組み

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

■ サイバーセキュリティ経営ガイドラインの活用状況

- CISO、セキュリティ統括責任者、またはセキュリティ統括部門の担当者が経営ガイドラインを参考にセキュリティ対策を実施がそれぞれ27%
- 一方、経営ガイドラインは知っているが活用していない企業も23%
- 経営ガイドラインを知らない企業はないが、経営者が経営ガイドラインを参考にセキュリティ対策を指示している企業は7.7%（2社）に留まる

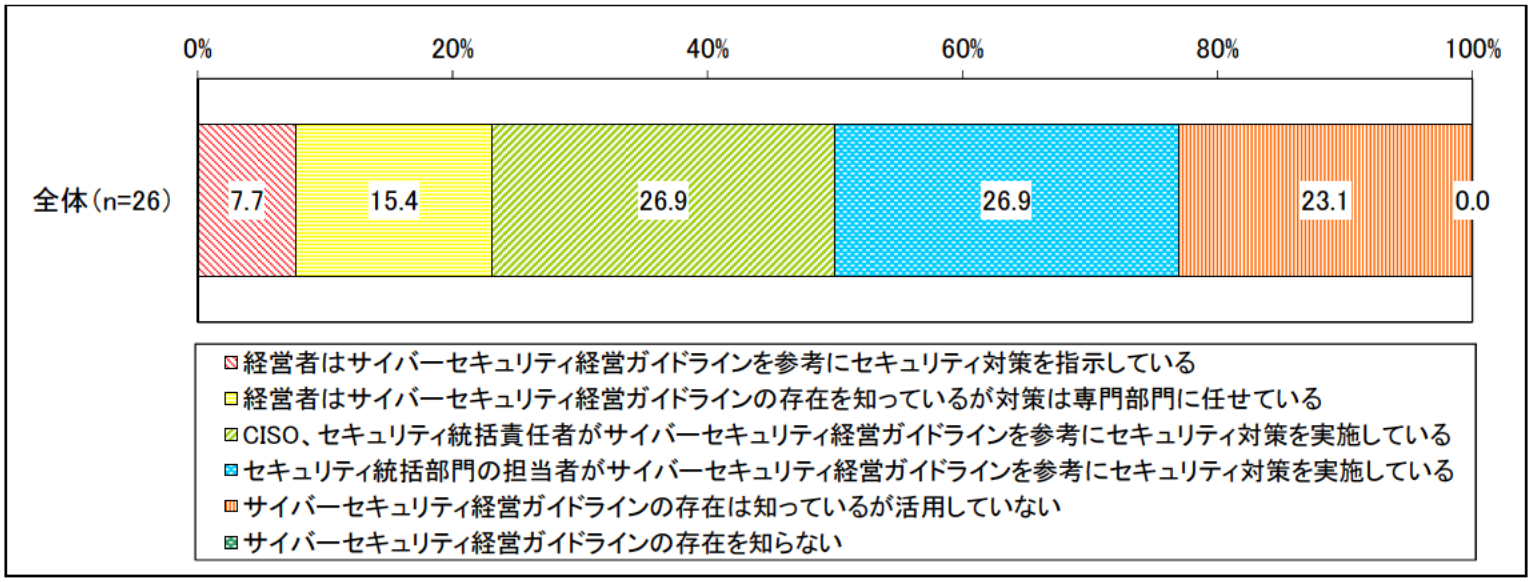


図2.13　サイバーセキュリティ経営ガイドラインの活用状況

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

■ 製造・非製造別　経営ガイドラインの活用状況

- 製造業では経営者は経営ガイドラインを知っているが対策は専門部門に任せるが26.7%
- 非製造業では経営ガイドラインの存在は知っているが活用していない企業が36.4%

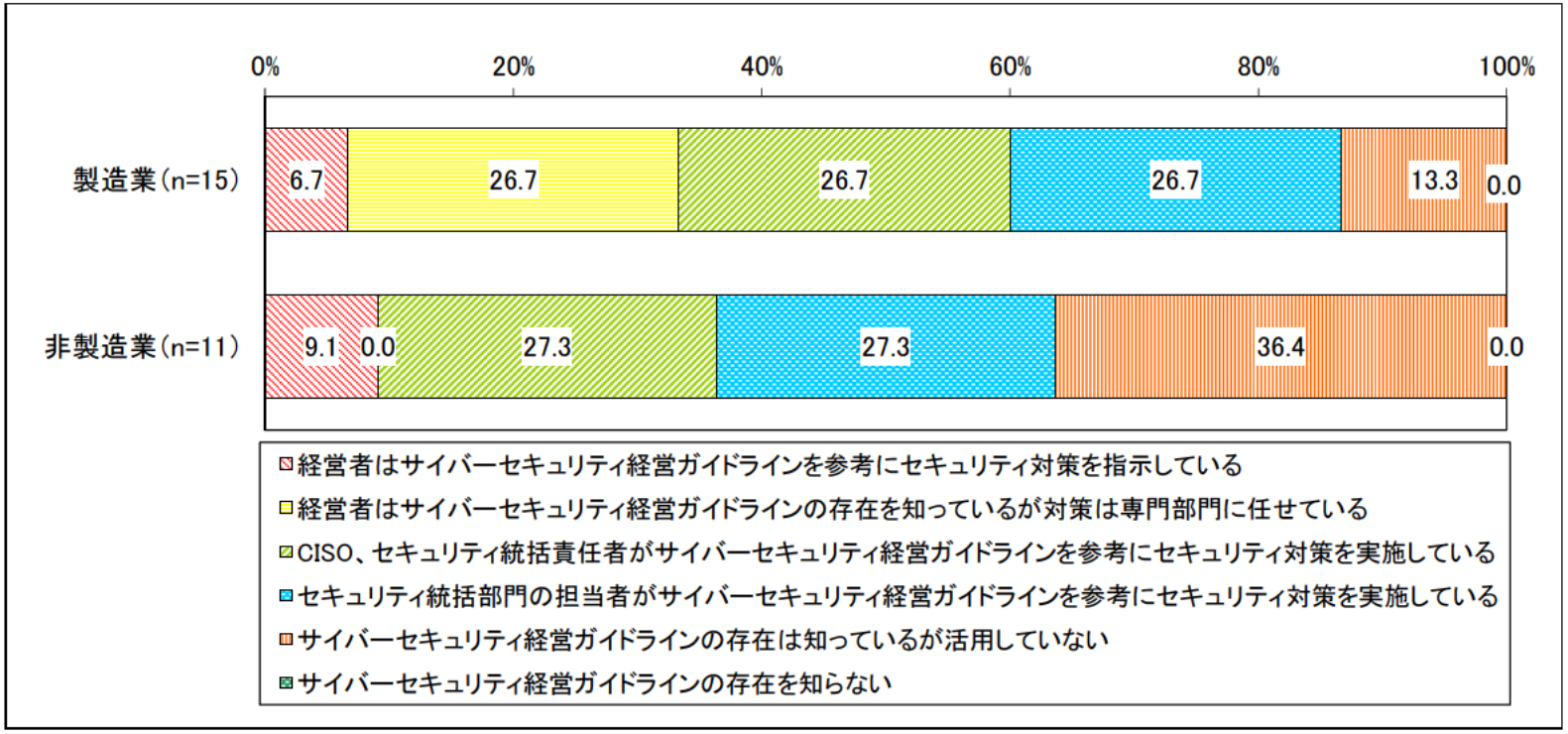


図2.14　サイバーセキュリティ経営ガイドラインの活用状況（製造・非製造別）

2.1 可視化ツールβ版を用いた企業調査

(5) β版試行アンケート分析

■ 参考にする基準・ガイドライン等（複数回答）

- 最も多いのがISO2700、次いで個人情報保護法のガイドラインで約7割
- NIST SP800シリーズも約6割の企業で参考にしている
- 自社で独自に検討は27%しかなく、ベンター・コンサルの情報を利用いている企業が65%あり外部依存している

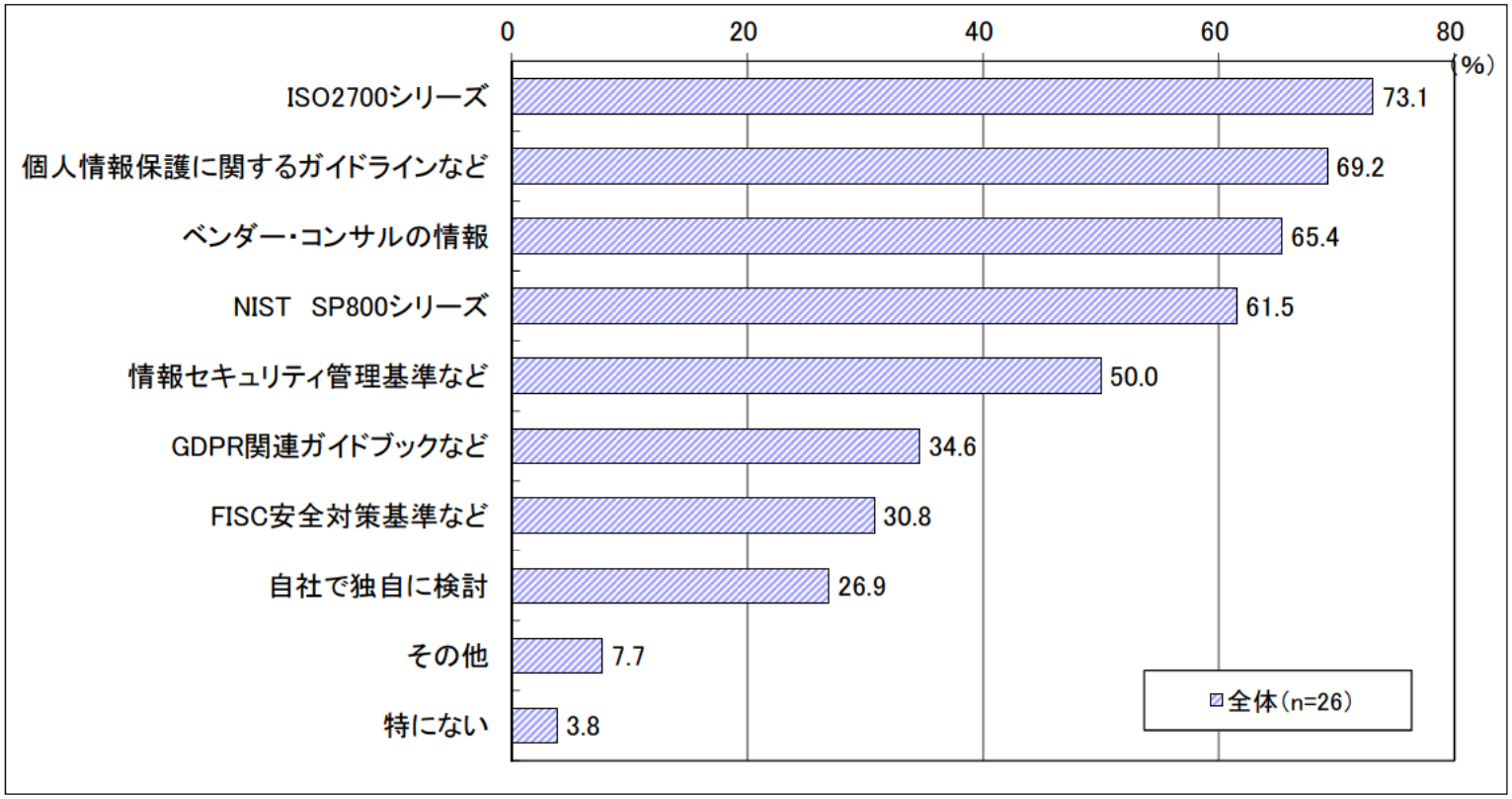


図2.15 サイバーセキュリティ経営ガイドラインの活用状況（製造・非製造別）

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

■ インタビュー実施企業

- 新型コロナ禍の影響もあり、インタビューはすべてリモート会議で実施した。
- インタビューはグループインタビューと単独形式を併用して実施した。

（インタビュー対象企業の構成数）

- グループインタビュー：11社
- 単独インタビュー：10社

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

■ インタビュー実施内容

- 可視化ツールβ版に関するインタビュー項目は次のとおりである。

(1) 可視化ツールβ版の試行結果について
（主な視点）
・試行した感想
・利用シーン（ユースケース）と想定利用者
・判断の甘辛の一貫性を担保できるか？
・カスタマイズは必要か？

(2) 自社の対策状況について
（主な視点）
・サイバーセキュリティ経営ガイドラインの活用状況
・準拠している基準、参照しているフレームワーク、利用しているツール等
・自社のセキュリティ対策状況を評価するために用いている指標

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

① 可視化ツールβ版の試行結果について

■ β版を試行した感想

- アンケート同様に評価ツールとしては概ね好評価がえられている
- 回答に迷う･ばらつきが出る、回答のレベル感が分からないなどの指摘が多い。
- 評価の対象、スコープに迷うとの意見もあった。

■可視化ツールの総合評価

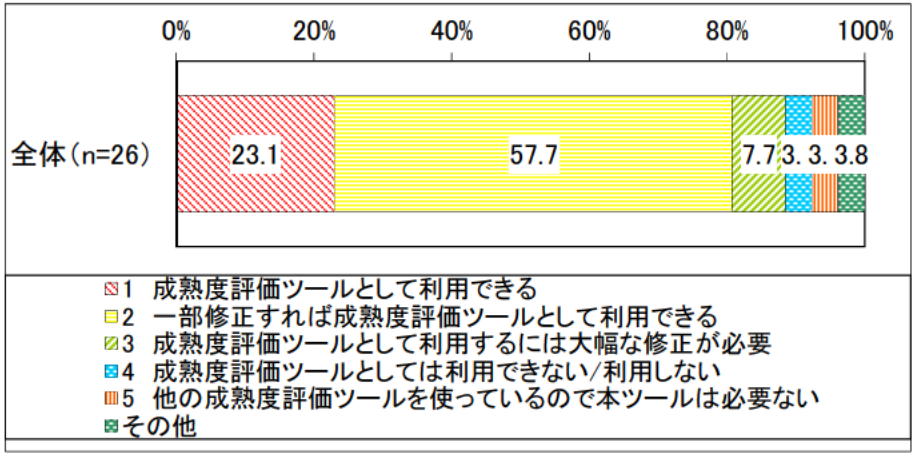


表2.5　試行した感想

分類	主なコメント	具体的な意見
試行した感想	評価ツールは有効である	●自己診断のツールとしては有効 ●成熟度評価ツールは有用である ●設問内容や選択肢は分かりやすい
	回答しづらい 回答に迷う/判断しづらい 回答にばらつきが出る	●回答者や業種・規模・扱っている商品・保有する情報によって温度差がでる ●経営者目線のところから実務者レベルのところまで多岐にわたるので、回答者によってばらつきが出そう。 ●選択に迷う。考え方の違いで判断がぶれる。同じ部門でも違う回答なる ●例えばツールを使っているかの設問でもツールの違いなどで回答が異なる ●マネジメント系の評価は定性的になるので評価にばらつきが出る ●スコープによっては部分的にできているときにどこまで評価してよいか判断に迷う ●項目間でバラツキがあるので、レベル感に違いがあるのではないか

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

① 可視化ツールβ版の試行結果について

表2.5 試行した感想（続き）

分類	主なコメント	具体的な意見
試行した感想	回答のレベル感がわからない	●「できている」はどこまででいいのか？8割なのか？6割なのか？で悩んだ。 ●部分的にできていることに対して、どのように回答していいかわからない。 ●回答しにくい設問があった。「定期的改善」というレベル感について、将来の見通しまで含めて回答していいのか悩む
	定性評価では実際的な取組み状況までは評価できない	●文章（定性的）での評価では、表面的な施策の有無は判別できるが、実際的な取組ができているかまでは落とし込めない。例えばツールが導入されているが実際有効に機能しているかどうかは分からない ●評価は守るべき情報資産の価値によって細かく実施しなければならない
	設問が多い	●β版は設問が多すぎる。選択肢の自由度が大きいので判断に迷う
	自己評価のバラツキは許容しても良い	●自己評価のばらつきは、ある程度許容する必要があるし、自己評価でいい。態勢や意識をなやみながら評価することそのものが大事である。セキュリティとは基本的にはツールがどうこうというのではなく、構えを整理してどうまわすかである。
	評価の対象、スコープに迷う	●β版は評価の際、グループ全体なのか、単体なのかのスコープに悩む。 ●関連会社を評価する場合は、評価する人がいてその人がヒアリングして評価しないと回答に差が出る ●サプライチェーンや子会社のガバナンスやチェックリストとして活用するには項目が多すぎるし、高度すぎる。
	ベンチマーク	●ベンチマークとして同業他社と比較ができると良い ●同業で自社の立ち位置がわかっているのであればこのツールは不要。

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

① 可視化ツールβ版の試行結果について

■ 改善要望

- 改善要望としては設問意図の明確化、備考欄の充実、評価結果に対して改善指針を提示してほしいとの意見が多い
- NISTとの関連付けやカスタマイズを望む声もある

表2.6 改善要望

分類	主なコメント	具体的な意見
改善要望	設問意図を明確化し、選択肢の具体例を示してほしい	●質問の意図を明確にすると答えやすい ●もう少し具体的に～ができているという設問があるとよい。中小向けのチェックリストのようなイメージ。 ●選択肢にはより具体的な内容を入れたほうが良いのではないか（別紙参照） ●選択肢が分かりづらい、成熟度のレベルと選択肢が合わない。（別紙参照） ●選択肢はより具体化したほうが良い。例えばある部分はできているが他の部分はできてない場合など評価者によって判断が異なるので具体例が欲しい
	備考欄の拡充	●備考欄が多くとられているので、それを拡充すれば温度差が埋めていける ●回答の際に何をもってそのレベル感と答えるのかが明確になるとよい。 ●項目毎に自社としてどこまで目指すのかをまず決める必要がある。その目指すべき姿の例が示されているとよい。 ●「できている」ことのエビデンスがあるとよい。備考にあるような例を拡充してほしい。 ●ブレを少なくするということでは備考欄は参考になったので更に充実してほしい

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

① 可視化ツールβ版の試行結果について

表2.6 改善要望（続き）

分類	主なコメント	具体的な意見
改善要望	評価結果に対する改善指針やプラクティスがあると良い	● 評価し、弱点を可視化できたら、それに対して次に打つとよい対策や、めざすべき段階・優先度が表示されるとよい。 ● これをすると評価が上がるといったプラクティスが出てくるといい。例えばメール訓練は実施していないがこれを実施すると評価があがるといった内容で、費用などもわかるといい
	評価の重み付けがあると良い	● 設問の重みづけがされることで、優先順位がわかるとよい
	設問とNISTとの関連付けがほしい	● 設問とNIST等の標準との参照ができるとよい。有償だがコンサル会社が提供しているサービスには似たようなものがある
	CISOがいるか、CSIRTがあるかを問うたほうが良い	● 評価の設問に入る前にセキュリティの専任者がいるか、シーサート、CISOがいるかをまず質問したほうが良い
	カスタマイズできると良い	● 改善点としてはツールを例えば松竹梅のように分けたら使いやすくなる。業種、業態に合わせてカスタマイズできるといい ● 個別のカスタマイズができたほうが良い。自分たちがカスタマイズできる余地があるといい

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

① 可視化ツールβ版の試行結果について

■ 利用シーン／想定利用者

- 経営の報告に使う、ベンチマークに使うが2大利用シーン
- IRやステークホルダーの評価、セキュリティ監査に使うとの意見もある

表2.7 利用シーン／想定利用者

分類	主なコメント	具体的な意見
利用シーン 想定利用者	経営への報告に使う	●経営ガイドラインは経営への報告に利用している（年２回）。その裏付けとしてβ版も活用できれば良い。グループ会社には別途もうすこしかみ砕いたものを整理したい。 ●経営ガイドラインを年1回で評価して、経営層へ報告し現状と重点施策を説明する。自社のセキュリティレベルを客観的に把握・俯瞰するためのツールとしてβ版を活用したい。セキュリティの全体像が把握できるツールとして公的なものなので良い ●経営層への教育や会話のツールとして役立てることを想定。本来は経営層自ら回答してほしいが、専門的な要素も含まれるので回答させるのは難しい。 ●サイバーセキュリティ経営ガイドラインは、経営向けの説明に有効。ただし、独自のチェックシートとの紐づけは悩ましい。 ●経営に対してのコミュニケーションツールとして使いたいが、経営ガイドライン10項目が経営に理解されていることが前提である。 ●利用シーンとしては会社の成熟度レベルを評価して、経営層に報告することがある。そのためには成熟度が低いところはどのような対策をしたらよいかがあればなお良い。 ●使い方としては担当者が自社のレベルを把握する、経営層に報告、グループ会社のガバナンス、サプライチェーンの点検など。ただし、サプライチェーンの点検に広く使うにはレベル感が多すぎる。

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

① 可視化ツールβ版の試行結果について

表2.7 利用シーン／想定利用者（続き）

分類	主なコメント	具体的な意見
利用シーン 想定利用者	ベンチマークに使う	● 自社ができていない点を説明するために経営層の一歩手前の層に使いたい。そのためには評価のベンチマークができるといい ● 「業界や企業全体などでの自社の立ち位置がわかる」というのは非常にありがたい。 ● β版は他者とのベンチマークとして活用できそう。そのためには入力の各社でセルフチェックが必要 ● ISAC内などの業界内でのベンチマークには有効 ● ツールとしては結果の他社比較や過去の自社との比較が簡単に閲覧できるとよい
	利用者はセキュリティ統括の責任者、または担当者	● このツールを使うのはセキュリティ統括の担当者 ● ツールの想定利用者は情報セキュリティをコーポレートの立場で推進している者 ● セキュリティ責任者が自分たちのセキュリティ対応状況を棚卸しする際に使う
	IRやステークホルダーの評価に使う	● IR評価としてもセキュリティの評価が重要であり、その評価に使える ● ステークホルダーの評価に使うことはできると思う。そもそも日本ではランキングのようなものを使っているのか。この辺から意識を変えていかないと難しい
	セキュリティ監査に使う	● セキュリティ監査に活用できる。IT部門ではなく、より経営スタッフや監査部門が勉強もかねて評価させてみたい ●監査に使うことも一つだが、海外拠点に適用するのは難しい。もっとシンプルに、平易な言葉で、YES・NOで答えらえるようなものでないと厳しい。

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

① 可視化ツールβ版の試行結果について

■ 他のツールの利用

- 現状は独自に評価、NIST CSFをベースとしたツール、ベンダー・コンサルのツール、業界団体や納入先のチェックリストを使っている等の回答あり。

表2.8 他のツールの利用

分類	主なコメント	具体的な意見
他のツールの利用	セキュリティの対策状況を独自に評価している	●独自にグループ会社の成熟度評価を行っており、社内規定に対する適合を3段階評価としている。評価にはIT部門が各グループを手伝っている。横並びで見て、強化施策を検討しており、実施予算はグループもちである ●独自にITカルテ（スプレッドシート形式）として関連会社やサプライチェーンに対してチェックをしている。 ●セキュリティチェックシートを独自にグループ会社にまで実施しはじめている。将来は監査につなげていきたい。 ●成熟度評価にはコントロールベースとリスクベースがあるが、金融ではリスクベースでリスクの高いところを評価している
	NIST CSFをベースとしたツールを使っている	●成熟度評価は２つ実施している。一つはセキュリティリスク管理態勢の評価で、調査会社やコンサルティングファームのフレームワークを使っている。もう一つはサイバーセキュリティの評価でNIST CSF、SP800-53をベースにしたCAP（サイバーアシュアランスプログラム）をグローバルで実施している（コンサルティングファームが実施）。セキュリティ対策の有効性と自動化のレベルで評価している。 ●NIST　CSFをベースとしたツールを使っている

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

① 可視化ツールβ版の試行結果について

表2.8 他のツールの利用（続き）

分類	主なコメント	具体的な意見
他のツールの利用	ベンダー、コンサルのツールを使っている	● 自己評価ツールはいくつか試したことがある。コンサルティングファームや調査会社にも似たようなものがある。 ● 米国ベンダーのツールを使っている。実際にやり取りしている情報を監視して評価される。例えば公開サイトに登録するとスコアがわかるので、サプライイヤーのセキュリティレベルを評価するのに使える。企業がやりとりしているデータをのぞける範囲でのぞいて評価している ● 成熟度を客観的に測るツールが出てきている。例えば使っているソフトウエアコンポーネントについて客観的に評価するツールなどある ● 成熟度評価にはSANS CSCをベースとした評価を実施
	業界団体や納入先のチェックリストを使っている	● 自工会では部品メーカー向けのチェックリストをリリース予定、これは情報セキュリティ経営ガイドラインに近いもの。β版はISMS系よりもサイバー系。自工会でやっているのはいわゆる情報セキュリティ系。 ● 得意先から依頼があって30項目弱のチェックをした。サイバーセキュリティガイドラインをベースにしたものだった。また、仕入れ先などの関係会社のものも別にある。こういうチェックは複数あるので、横並びで統一的なツールがあるとよいとは思う ● 関連会社の調査にはIPAの中小企業向けサイバーセキュリティチェックリストを使った

2.1 可視化ツールβ版を用いた企業調査

(6) β版試行インタビュー結果分析

① 可視化ツールβ版の試行結果について

■ 甘辛をなくすには

- 複数部門／人での評価や第三者的評価が有効だが、実施上の工夫も必要
- 回答例の充実が必要

■可視化ツールの甘辛を抑える取組み

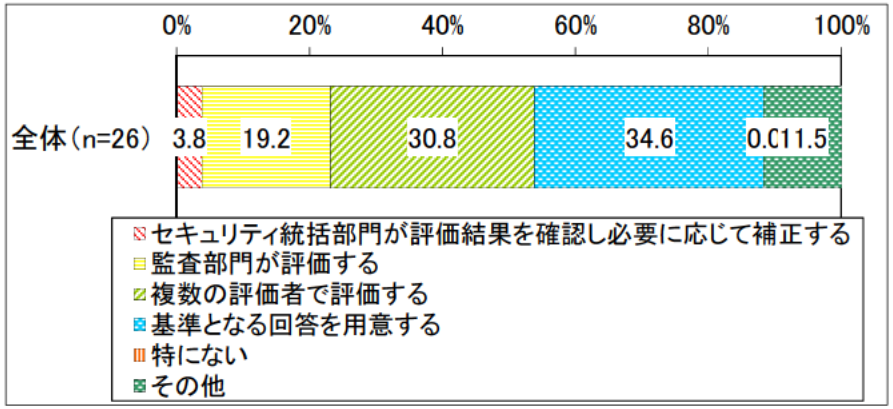


表2.9　甘辛をなくすには

分類	主なコメント	具体的な意見
甘辛をなくすには	複数部門／人での評価	● 甘辛を抑えるには、複数部門で評価する／監査部門で評価するとよい。客観的に評価できる基準があるとなおよいとは思う。 ● セルフチェックではなく統一的な担当者でグループを評価したほうがばらつきはないとは思うが、パワーがかかるので、現場につけてもらって、エビデンスをつけるとかヒアリングするとかでフォローする必要がある。 ● 複数人で評価したところ、ばらつきが出た。ばらつきについては話し合って合意形成。ガバナンスチームと対策実行チームとで議論した。特に「管理していますか？」設問について、ツールか人手かや、PDCAのレベル感が人によって違うので意見が分かれた。
	回答例の充実	● 甘辛をなくすには回答例をより充実するのも良いかもしれない
	第3者的な評価を行う	● 評価する人がいて、ヒアリングするほうが統一した回答を引き出せる

2.2 投資家等ステークホルダー調査

(1) 実施したヒアリング調査の概要

- 調査趣旨を踏まえ、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の観点から、企業におけるサイバーセキュリティ対策の評価及びそれに関わる業務を行っている下表の関係者にヒアリング対象を実施した。

表2.10 ステークホルダーを対象とするヒアリング調査の対象一覧

分類
投資会社・投資顧問会社
監査法人
コンサルティングファーム
証券会社
調査会社
損害保険会社
企業評価ツールベンダー
その他関係者

2.2 投資家等ステークホルダー調査

(2) ヒアリング調査結果

① 企業の評価に用いている情報

- サイバーセキュリティ経営の実現には、取締役会で自社のサイバーリスクへの対策状況が確認されていることが重要。そのため社外取締役がセキュリティを十分に理解しているかをヒアリングで尋ねている。（投資会社）
- M&Aのデューデリでは、サイバーセキュリティ対策状況の評価を松竹梅レベルで行う。経営ガイドラインが共通言語として利用できるのではないか。（コンサルティングファーム）
- サイバー保険加入時の告知様式は保険会社毎で異なり、統一されていない。（損害保険）
- 参考とする基準は、ISMS、所管官庁ガイドライン。（損害保険）
- 企業のサイバーを含む事業リスクを、業種その他の区分毎に50種類のリスクマップとして整理。（損害保険）
- 自社のサイバーセキュリティ対策状況を開示する企業は増えているが、内容はまだ一般的なものが多く、項目も企業間でバラバラ。共通の可視化ツールによる横並び比較ができると良い。（監査法人）
- 基準として業界横断でNISTサイバーセキュリティフレームワークが用いられており、金融系ではFFIEC CATがベンチマークとして利用されている。（監査法人）
- 関心の度合いと対象は業界毎に異なる。（監査法人）
- サイバーセキュリティは2016年に新興リスク、2019年に重要リスクと認識された新しいテーマであり、まだデータの蓄積がない。DXと同様今後重要性が高まると見込まれることから、現在は啓発をしていく段階と認識。（コンサルティングファーム）
- 外部監査をしっかりやっているということが重要なポイント。（調査会社）
- セキュリティ対策投資額の大小では評価しない。投資が大きければできているとは限らない。（調査会社）

2.2 投資家等ステークホルダー調査

(2) ヒアリング調査結果

② 企業のサイバーセキュリティ対策に関して知りたい情報

- 損保会社は代理店等での保険引受時のオペレーションをできるだけ簡略化したいと考えており、国内で標準的な基準ができ、その準拠状況で評価項目を減らせれば有益。（損害保険）
- 経営会議の議題とすることを求めるより、KPI指標としてオーソライズするほうが効くのではないか。（損害保険）
- DB化してベンチマークにすれば、個別詳細の課題は扱えなくても、大きな方向性を示せる。（監査法人）
- 重要インフラ系は業界特有の可視化・比較ツールがあるべき。各業界内の情報共有促進にもつながる。（監査法人）
- 国内企業は一般にグループ管理が弱い。委託先にNISTフレームワークの要求は困難な場合も多く、共通言語としての本ツールの活用に期待。（監査法人）
- 現状ではサイバーセキュリティをリスクと認識して取り組んでいる企業は上場企業で100社もないと思う。①社内でガイドラインを策定しているか、②それを公表しているか、③可視化ツールで回答しているかの３段階の〇×で評価することで、一定の規模での評価が可能となるのではないか。（コンサルティングファーム）
- リスクが大きいかどうかではなく、事業上避けられないリスクをどうマネージしているかを示すことで、機会としてのプラス側面示す方向を目指すべき。（コンサルティングファーム）
- かつて企業評価は財務指標一辺倒であったが、非財務情報としてESG、気候変動なども取り上げられてきた。ESGの定量評価もCO2やゴミの排出量など無理矢理の感もあったが、現在は一般化している。サイバーセキュリティも将来的には定量化される方向と考えている。（コンサルティングファーム）
- セキュリティ情報は開示しすぎると攻撃対象となるので難しい問題。企業とのブリーフィングの中でのやりとりであれば扱われる可能性はある。（調査会社）
- アナリストにとっては比較と予測に利用できる情報が重要。（投資顧問会社）

2.2 投資家等ステークホルダー調査

(2) ヒアリング調査結果

③ サイバーセキュリティ対策が投資判断に及ぼす影響

- 米国企業のサイバーに関する情報開示も一般的な内容が多く投資家から不満の声が上がっている。（コンサルティングファーム）
- 投資家との対話で最悪なのは、「わかりません」ということ。わかっているが言えないは 2 番目に悪い。言えないことがあるのはやむを得ないが、何らかの形で説明できるようにする必要がある。（投資顧問会社）

2.2 投資家等ステークホルダー調査

(2) ヒアリング調査結果

④ 自己評価の有効性

- 自己評価であっても、評価結果の透明性・客観性・継続性が担保されれば活用可能。（投資会社）
- 汎用の可視化ツールの評価結果を保険の引き受けにそのまま活用するのは困難。ただし、自己評価結果は参考情報として有用。（損害保険）
- 自己評価の信頼性は評価者のスキルに依存。誰が何をもとに評価したか等の付加情報が欲しい。（監査法人）
- コーポレートガバナンスコードも自己評価である。10年前は見栄えのよいことばかりを書いて参考にならなかったが、現在はすべての上場企業が開示しており、内容も正直に記載し、望ましくない結果の場合はその理由を示すようになった。かつて海外から日本のコーポレートガバナンスはひどいと言われていたが、現在は先進国並みと評価されている。ESGもそうだが、サイバーセキュリティについても今後同様の方向に進むのではないか。サイバーセキュリティの第三者評価には難しさがあると思う。（コンサルティングファーム）
- 自己評価はあくまで内部目的で活用すべきであって、投資家としては判断材料には使いにくい。（調査会社）
- 米国NISTのサイバーセキュリティフレームワークは自己宣言型であったが、監査を行ったところ宣言の内容と異なる実態が明らかとなり、認証制度に変わっていくこととなった。サプライチェーンも同様であり、自己評価でなく外部に証明していくことが重要になってくることから、認証制度が重要になる。（コンサルティングファーム）
- 自己評価が有効かどうかは内部統制が機能しているかどうかに関わる。事業部門が自己点検で検査し、それを内部監査部門で監査して、監査役が内部監査部門を監査する。内部統制ではこれが有効に機能していることが求められ、最終的には取締役会の実効性が問われる。（投資顧問会社）

2.2 投資家等ステークホルダー調査

(2) ヒアリング調査結果

⑤ 業種や事業内容への特化（テーラーメイド化）の必要性

- B2Cサービス企業は企業毎にリスクと対策状況の格差が大きい。本業がサイバーと無関係と認識。（投資会社）
- サプライチェーンは大手でも十分な対策ができていない場合が多く、自分達のガバナンスが届かないところでどこまでカバーできるかが経営課題となっている。（コンサルティングファーム）
- 過去にサイバーセキュリティ経営ガイドラインを用いて企業を評価した際、業種毎に評価項目の重きを変えた。具体的にはDXの影響や事業リスクなどが対象。（コンサルティングファーム）
- 自社の企業価値創造にプラスになる、リスクを減らすなどにつながっていることが重要。セキュリティの観点では、コアの部分がうまく結びつき、うまく流れていることが重要。そこが確認できれば、テーラーメイドであるかどうかは問題ではない。（投資顧問会社）
- スタートアップ企業はマネジメント、イノベーション、リスクマネジメントの 3 点で評価する。大企業と同じレベルで実施する必要は無い。（投資顧問会社）

2.2 投資家等ステークホルダー調査

(2) ヒアリング調査結果

⑥ 可視化ツールβ版についての意見

- サイバーセキュリティ分野の情報開示については海外でも模索中である。日本が先んじて取り組むのは非常に良いことであり、可視化ツールを英語化して紹介してはどうか。サイバーセキュリティの成熟度について適切に説明ができ、それが海外でも通用するものであれば、理解は早いと思う。（コンサルティングファーム）
- 業種別、企業規模別のベンチマークがあると良い。このとき、点数の定義がぶれない必要がある。（コンサルティングファーム）
- グローバルスタンダードと整合していることが重要。（コンサルティングファーム）

⑦ その他の意見

- 国内企業は、米国と比較してペネトレ等の実践が少なく、防御する側の視点が弱い印象。（投資会社）
- 「投資家はサイバーセキュリティ対策状況も見る」というメッセージを出すことが重要。（コンサルティングファーム）
- 小規模事業者向けサイバー保険の告知書は、大手・中堅とは別に用意している。可視化ツールも小規模向けを別に用意してはどうか。（損害保険）
- DXの認証制度の普及に合わせて、そのセキュリティ対策として本ツールが活用できるとよい。（監査法人）

2.3 他団体の可視化ツールの調査・動向把握

- 情報/サイバーセキュリティ対策状況に関する可視化を行うためのツール、方式、方法論として公表されているものを調査した結果を次表に示す。なお、内容は2020年4月時点のものである。

表2.11 他団体の可視化ツールの例

No	分類(ツール、方式、方法論)	名称	提供機関	可視化内容	ターゲット	構成	設問数・内容	回答方式	URL
1	ツール（民間）	セキュリティ対策状況可視化サービス	NRIセキュアテクノロジーズ	組織・拠点ごとのセキュリティレベルの横断的な評価	汎用	第三者によるヒアリング	Governance, Risk, Compliance, Physical, Technicalの3つの観点で可視化する。	独自モデル	https://www.nri-secure.co.jp/service/consulting/security_visualization
2	ツール（民間）	グローバルセキュリティアセスメント	NRIセキュアテクノロジーズ	海外拠点ののセキュリティレベルの横断的な評価	汎用（海外拠点を有する企業）	第三者によるヒアリング＋実機診断（現地）	Governance, Risk, Compliance, Physical, Technicalの3つの観点で可視化する。	独自モデル	https://www.nri-secure.co.jp/service/consulting/global_assessment
3	方式	CMMC（CyberSecurity Maturity Model Certification）	DoD（米国国防総省）	FCI（Federal Contract Information）とCUI（Controlled Unclassified Information）の保護の能力を測定することを通じ、防衛産業基盤企業のサプライチェーン全体のセキュリティを強化	防衛産業基盤企業	認証プロセス	ドキュメント、ポリシーおよび実際の技術的管理の実装を評価する。 17個のドメインと43個の機能が対象。	5段階の成熟度モデル	https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf
4	方法論	情報セキュリティ対策状況の評価手法の提案	三菱電機株式会社 武曽 徹、飯田 茂	情報セキュリティ対策をどのように実施しているかという要素を含めた対策実施強度の評価を行う	―	自己診断	評価項目は、組織のセキュリティポリシー等から洗い出しを行う。	指標として運用レベルの充足率を導入する。 充足率を脅威と対策箇所毎に集計して、提示する。	https://ci.nii.ac.jp/naid/110008003507/
5	方法論	グループ企業におけるセキュリティアーキテクチャ実装状況に関する可視化手法の提案	情報セキュリティ大学院大学 佐藤 雄二、大久保 隆夫	現在のセキュリティ対策状況に関して、共通認識を持つための、セキュリティアーキテクチャ実装状況に関する可視化手法	民間企業（グループ企業を有する企業）	―	対象利用者の知識レベルを考慮して、可視化する方法を検討。	―	https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=146841&item_no=1&page_id=13&block_id=8
6	ツール（民間）	SIM3（Security Incident Management Maturity Model）	Open CSIRT Foundation	セキュリティインシデントのマネジメントの成熟度を評価	CSIRTを有する組織	オンラインによるチェックシートの自己診断	Organization、Human、Tools、Processの4つのカテゴリに分類される44個のパラメータに対して評価。	4段階の成熟度モデル	https://opencsirt.org/csirt-maturity/sim3-and-references/ http://sim3-check.opencsirt.org/#/
7	ツール（民間）	BSIMM（Building Security In Maturity Model）	BSIMM	ソフトウェア開発プロセスにおけるセキュリティ構築の成熟度モデルを基に評価し、改善する	民間企業	チェックシートの自己診断	ソフトウェア開発の上流工程から運用保守までをカバーし、各工程のセキュリティに対する取り組みを評価。4つのドメインとして、「ガバナンス」と「インテリジェンス」、「ソフトウェアセキュリティ開発ライフサイクル」と「デプロイメント」で構成される。	12のクライテリアが用意され、自社の行動を110個の質問に回答することでスコアリング	https://www.bsimm.com/ja-jp.html

2.3 他団体の可視化ツールの調査・動向把握

表2.11 他団体の可視化ツールの例（続き）

No	分類(ツール、方式、方法論)	識別	出典	No	ターゲット	構成	設問数・内容	回答方式（成熟度モデル）	URL
8	ツール（公的機関）	ES-C2M2 (Electricity Subsector Cybersecurity Capability Maturity Model)	DOE（米国エネルギー省）	電力業界向けのセキュリティ能力成熟度モデル	電力および公益事業会社	チェックシートの自己診断	事業者のサイバーセキュリティへの対応状況を10のドメインに分類している。（危機管理、資産・変更・構成の管理、アイデンティティおよびアクセス管理、脅威と脆弱性の管理、状況認識、情報共有とコミュニケーション、イベントおよびインシデント対応、運用の継続性、サプライチェーンと外部依存関係の管理、従業員管理とサイバーセキュリティプログラム管理） それぞれのドメイン内に37の「目標」、目標ごとに312の「プラクティス」を整備している。	4段階の成熟度モデル	https://www.energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf
9	ツール（公的機関）	C2M2（Cybersecurity Capability Maturity Model）	DOE（米国エネルギー省）	ES-C2M2の電力の特有の部分を除いたサイバーセキュリティ能力成熟度モデル	電力および公益事業会社を対象として開発されているが、どの組織でも利用可能	同上	同上	同上	https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0 https://apps.dtic.mil/dtic/tr/fulltext/u2/1026943.pdf ツールは、C2M2@doe.govにメールで要求する
10	方式	Cyber Essentials	NCSC（英国National Cyber Security Centre）	審査合格マークの掲載を通じて、ステークホルダーへのサイバー対策への取り組みのアピールと、政府入札要件による英国のレベル底上げを図る	大企業から中小企業まで。 公的機関も対象。	自己診断 （なお、Plusメニューではオンサイトでの脆弱性診断が追加）	認証機関から提供されるアンケートへの回答。アンケートの対象は、ファイアウォール、安全な構成、ユーザーアクセス制御、マルウェア保護、パッチ管理。	基準達成を示す証明書が交付される。	https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
11	ツール（民間）	ISF Maturity Model Accelerator Tool	ISF (Information Security Forum)	21の情報セキュリティ分野で成熟度を測定	—	—	—	—	https://www.securityforum.org/tool/the-isf-maturity-model-accelerator-tool/
12	ツール（公的機関）	SECURITY ACTION	IPA	中小企業が自己宣言する形での取り組みアピール	中小企業	自己診断	情報セキュリティ5か条、もしくは情報セキュリティ基本方針の策定実施状況を回答	2段階で結果を表示。	https://www.ipa.go.jp/security/security-action/mark/index.html
13	ツール（公的機関）	FFIEC Cybersecurity Assessment Tool	FFIEC（米国連邦金融機関検査協議会）	金融機関の自組織のリスクの識別とサイバーセキュリティの成熟度の評価	金融機関	チェックシートの自己診断	ビジネスリスク状況に関する5つのカテゴリ、サイバーセキュリティ成熟度に関する5つの領域を回答する。	5段階	https://www.fsscc.org/files/galleries/Copy_of_FSSCC_ACAT_v2.xlsx
14	ツール（民間）	CMMI Institute Cybermaturity Platform	CMMI Institute（ISACA Enterprisesの関連会社）	組織全体の人々、プロセス、テクノロジーの現在のサイバー成熟度を測定	—	オンラインによるチェックシートの自己診断	3000以上の設問に回答する。	5段階	https://cmmiinstitute.com/news/press-releases/april-2018/cmmi-cybermaturity-platform-builds-board-and-c-sui
15	ツール（公的機関）	情報セキュリティ対策ベンチマーク	IPA	組織の情報セキュリティへの取組状況の把握	民間企業および政府機関、地方自治体、公益法人	オンラインによるチェックシートの自己診断	27項目の設問に回答。	組織の情報セキュリティへの取組状況（自組織がどのグループに属するか、同じグループ内における自社と他社との比較による、セキュリティ対策の取り組み状況）	https://www.ipa.go.jp/security/benchmark/index.html

2.3 他団体の可視化ツールの調査・動向把握

表2.11 他団体の可視化ツールの例（続き）

No	分類(ツール、方式、方法論)	識別	出典	No	ターゲット	構成	設問数・内容	回答方式（成熟度モデル）	URL
16	ツール（民間）	ISOMM（ISOG-J SOC/CSIRT Maturity Model）	ISOG-J	セキュリティインシデントのマネジメントの機能別成熟度を評価	CSIRT、SOC等を有する組織	チェックシート	セキュリティ対応組織が持つべき9つの機能と54の役割について確認するもの。6段階で評価する。	5段階	https://isog-j.org/output/2017/Textbook_soc-csirt_v2.2_maturity-checklist.xlsx
17	方式	ISO/IEC 21827	ISO	CMMをセキュリティに適用したものであり、組織のセキュリティに関するシステムの開発・運用プロセスの運用能力を評価。前進はSSE-CMM（Systems Security Engineering-Capability Maturity Model）であり、2002年にISO化された。	—	第三者評価もしくは自己診断	22のプロセスエリアについて評価を行う。	5段階	https://www.iso.org/obp/ui/#iso:std:iso-iec:21827:ed-2:v1:en http://www.sse-cmm.org/index.html
18	ツール（民間）	サイバーセキュリティ強化点検サービス	NTTデータ	システムや組織におけるセキュリティ対策状況を短期間で網羅的に可視化	—	既存情報およびヒアリング	—	強化すべき対策とその優先度を提示する。	https://www.nttdata.com/jp/ja/lineup/cybersecurity/
19	ツール（民間）	BitSight Security Ratings	米BitSight Technologies	インターネットアクセス可能なシステムのセキュリティ対策状況の把握	—	オンラインによる自動収集	—	インターネット上から対象システムを日々検査し企業のサイバーセキュリティ対策状況をレーティングするSaaS型のサービス	https://www.ctc-g.co.jp/news/press/20191010a.html
20	ツール（民間）	サイバーセキュリティ評価チェックシート	ゾーホージャパン株式会社	サイバーセキュリティ経営ガイドラインにより自社を評価する際に活用できるツール	—	チェックシート	—	サイバーセキュリティ経営ガイドラインの重要10項目それぞれに対して、何点だったのか自動計算で結果が表示される。	https://www.manageengine.jp/solutions/csm_guideline/lp/
21	ツール（民間）	SAMM（Software Assurance Maturity Model）	OWASP	ソフトウェア開発および運用体制における、リスクの可視化とセキュリティ活動の効果の評価	組織規模は問わない、ソフトウェア開発に関わる組織	自己診断	ソフトウェア開発を4つのビジネス機能として定義し、それらに対して12のセキュリティ対策を対応付けている。これらについて、評価を行う。	3段階	https://owasp.org/www-project-samm/
22	ツール（公的機関）	CRR（Cyber Resilience Review）	US-CERT	運用面のレジリエンスとサイバーセキュリティの対策状況の評価	—	オンラインによるチェックシートの自己診断	リスク管理、インシデント管理、サービス継続性などを含む10領域を評価。	—	https://www.us-cert.gov/resources/assessments
23	ツール（公的機関）	Baldrige Cybersecurity Excellence Builder	NIST	民間セクターの組織がサイバーセキュリティのリスクマネジメントの実効性をより良く理解することを支援	民間組織	チェックシートの自己診断	リーダーシップ、戦略等の6つのプロセスと運用結果の7つの領域を評価。	—	https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative
24	ツール（公的機関）	CSET（Cyber Security Evaluation Tool ）	DHSおよびINL	ユーザーのサイバーシステムおよびネットワークのセキュリティ態勢を評価し、対策の推奨事項を検討	制御システム	自己診断（デスクトップソフトウェア）	NISTやDoDなどの標準を選択して、質問に回答。	—	https://cset.inl.gov/SitePages/Home.aspx

2.4 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、次表のメンバーで構成される「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。
  - β版テストの企画内容、実施状況、結果報告
  - 各種調査結果を基にした可視化ツールのあるべき姿（可視化ツール Ver1.0 の企画）
  - 可視化ツールの普及促進に必要となる政策　等

表2.12 「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」構成員

分類	対象者名（敬称略）	所　属
委員	荒川　大	株式会社ENNA 代表取締役 一般社団法人サイバーリスク情報センター 事務局長
	武智　洋	日本電気株式会社 サイバーセキュリティ戦略本部 主席技術主幹 一般社団法人サイバーリスク情報センター 代表理事
	平山　敏弘	学校法人電子学園　情報経営イノベーション専門職大学 教授 特定非営利活動法人日本ネットワークセキュリティ協会　教育部会長
	宮下　清	一般社団法人日本情報システム・ユーザー協会　参与
	持田　啓司	株式会社ラック　理事 情報セキュリティ教育事業者連絡会（ISEPA）代表
オブザーバ	経済産業省 商務情報政策局 サイバーセキュリティ課／情報技術利用促進課／地域情報化人材育成推進室 独立行政法人情報処理推進機構 セキュリティセンター／社会基盤センター	

2.4 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2.13 「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	おもな議題（文字が灰色の内容は本報告書第３章に関するもの）
第1回	2020年4月27日	●『サイバーセキュリティ経営可視化ツールβ版』の改良について（目的、使い方、修正方針等） ● 手引き書の検討課題について（リスクマネジメント、外部委託、スキル・能力の考え方等）
第2回	2020年5月19日	● 手引き書の検討課題について（構成案、業種別体制図等）
第3回	2020年6月17日	●『サイバーセキュリティ経営可視化ツールβ版』の改良について（改良方針、調査項目案等） ● 手引き書案の見直し方法について ● ユーザー企業調査の実施方法について
第4回	2020年7月14日	●『セキュリティ体制構築・人材確保の手引き（第１版）』の内容案の検討
第5回	2020年8月4日	●『セキュリティ体制構築・人材確保の手引き（第１版）』のレビュー
第6回	2020年12月16日	● 手引き書に追加すべき内容の検討 ●『サイバーセキュリティ経営可視化ツールβ版』を試行した企業を対象とする調査結果について
第7回	2021年1月26日	● 手引き書の改定の方向性の検討 ●『サイバーセキュリティ経営可視化ツールver.1.0』に向けた進捗報告
第8回	2021年2月16日	●『セキュリティ体制構築・人材確保の手引き（第１.1版）』の内容案の検討 ● 企業ヒアリング調査結果報告
第9回	2021年3月2日	●『セキュリティ体制構築・人材確保の手引き（第１.1版）』のレビュー

2.5 可視化ツール Ver.1.0案の作成

- 調査の結果、ユーザー企業、ステークホルダーともβ版に対して「抜本的な改修が必要」という意見はなかったことから、得られた改善要望をもとに下表の要領にてβ版を改修し、V1.0としてリリース、ユーザ企業に展開することとなった。
- 同時並行で投資家等ステークホルダーにも共通言語としての活用を促していくことが予定されている。

表2.14 可視化ツール Ver.1.0案の作成方針

ユーザ企業	• 経営層とのコミュニケーション（定期報告等）に使える／使いたい • セキュリティに関する全体的な態勢・構えを見たい **⇒β版の質問構成で対応可能** • 業種・業界内比較（ベンチマーク）をしたい **⇒DB化することでベンチマーク機能を実現する** • 海外拠点等のチェックにも使いたい **⇒NIST Cybersecurity Framework (CSF) 等のグローバル標準と紐づける** • 推奨対策（で、どうすればいい？）を示してほしい **⇒プラクティス集と紐づける** • 投資家等ステークホルダーとのコミュニケーションに使いたい • その他（質問文・選択肢に関する指摘等） **⇒「備考」を「回答のヒント」に改称、ユーザがより客観的に回答できるよう記述を増強する**
投資家等 ステークホルダー	• 機関投資家からは、可視化ツールが共通言語として投資家と企業の間のリスクに関する コミュニケーション・議論に使えるとの可能性が示された • β版に対する細かな改修要望もユーザ企業と共通（ベンチマーク等） • ただし、多くの投資家はDXについて企業と話し始めた段階であり、サイバーセキュリティはその一歩先 **⇒ユーザ企業向けに可視化ツールV1.0を開発し、ユーザ企業での普及を進めながら、投資家にも同じものを将来的に利用することを促していく**

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

(1) ユーザー企業ヒアリング調査

■ インタビュー実施方法

- 新型コロナ禍の影響もあり、インタビューはすべてリモート会議で実施した。
- 企業の選定にあたっては、可能な範囲で多様な業種・業態の意見を反映できるように選択した。

■ インタビュー参加企業総数：10社

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ インタビュー内容

1) 情報セキュリティ組織体制について

① 情報セキュリティ組織体制の構築状況

（主な視点）

- 既存のリスクマネジメント体制との対応
- アウトソーシングしているセキュリティ関連業務とその理由、社内体制との切り分け状況、委託先の選定基準など
- OTの管理体制や商品開発体制（PSIRT等）との関連
- グループ会社の管理・ガバナンスとの関係

② 現体制となった背景・経緯

（主な視点）

- おもな影響要因（グループ企業や海外拠点の影響、DX推進体制、OTやIoTとの関係、取引先との関係、等）
- 体制の構築、役割やタスクの割当に際して参考にした情報、利用しているフレームワーク、ガイドライン

③ インシデント発生時の緊急対応／復旧体制の整備状況

（主な視点）

- 緊急連絡先・伝達ルート
- 初動対応マニュアルの整備・運用
- CSIRT有無、経営者への報告ルート
- 公表内容やタイミング
- 訓練・演習
- 業務の復旧計画の策定・見直し

④ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策状況の把握

（主な視点）

- 委託先の評価・管理のPDCA

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ インタビュー内容（続き）

2) ユーザー企業におけるセキュリティ関連人材

① セキュリティ人材（セキュリティ業務に専任で従事している人材：不在の場合は略）

（主な視点）

- セキュリティ統括機能を担う人材の確保に向けた考え方や取組
- 実務者・技術者層のセキュリティ担当者の確保に向けた考え方や取組
- セキュリティ人材の活躍（キャリアパス、処遇ほか）

② プラス・セキュリティ人材（セキュリティ業務に兼務で従事している人材）

（主な視点）

- 管理部門でセキュリティ関連業務を担う人材の確保に向けた考え方や取組
- 情報システム部門でセキュリティ関連業務を担う人材の確保に向けた考え方や取組
- 工場現場でセキュリティ関連業務を担う人材の確保に向けた考え方や取組
- プラス・セキュリティ人材の活躍（キャリアパス、処遇ほか）

③ セキュリティに関する教育・研修の実施状況

（主な視点）

- スキル向上に向けた育成の方針・考え方
- 活用している外部教育サービスや教材/セキュリティスキルのアセスメント状況

3.1 企業調査

(1) ユーザー企業ヒアリング調査

① 情報セキュリティ組織体制について

■ 情報セキュリティ体制の構築状況

- 情報セキュリティ体制は各社各様であり正解はないが一般的に以下の進化をたどるケースが多い

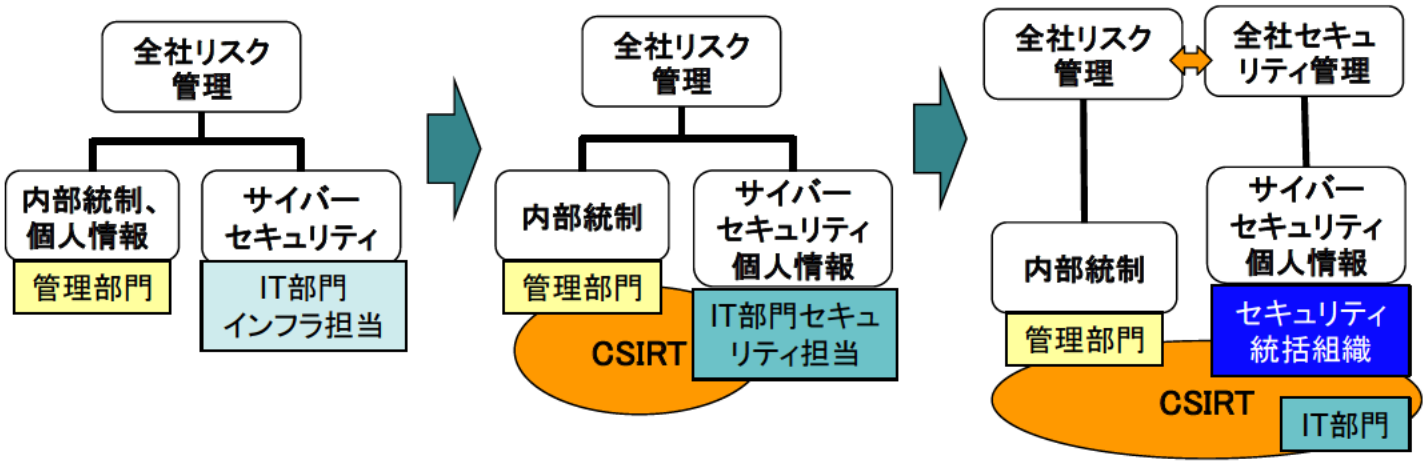


図3.1 情報セキュリティ体制の進化例

表3.1 情報セキュリティ体制に関するコメント

分類	主なコメント	具体的な意見
情報セキュリティ体制の構築状況	情報セキュリティ部会、委員会	●情報セキュリティ部会があるがルールやポリシーの変更時に開催し承認してもらうのが役割 ●セキュリティ定例会(2回/月)があったが、議題が少なくなり都度開催となった ●セキュリティ個別の体制はない。危機管理委員会の中で他のリスクと同様にセキュリティを扱っている ●ビジネスそのものがデジタルにシフトしてきているので、セキュリティについては情報セキュリティ統括組織がガバナンスしている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ 情報セキュリティ体制の構築状況（続き）

表3.2 情報セキュリティ担当組織／CSIRT構築状況

分類	主なコメント	具体的な意見
情報セキュリティ体制の構築状況	情報セキュリティ担当組織	●セキュリティ対策は実質的にはIT部門が実施している ●全社規定は総務部門が作る。その下にセキュリティポリシーがあり、規定がある。これらは情報システム部門が担当 ●IT部門の中にセキュリティ担当がいる　インフラと兼務　実質1名 ●事業会社のセキュリティ統括機能の長であるが、ホールディングのセキュリティ統括組織も兼務している ●セキュリティ統括組織は専任で、ITとは別組織。社内ITインフラのセキュリティはセキュリティが方針を出してITが対策を実施している。関連各社も同様に対策は各社が実施している。SIRT、SOCはセキュリティ統括組織。脆弱性診断も統括組織であり、第三者的機能としてセキュリティ統括が行っている ●憲法みたいなルールはセキュリティ統括が実施するが、ハウツー部分は関連会社の任せている ●セキュリティの専任者はいない。全員が兼務でインフラ担当が行っている ●規定・ポリシーはIT部門が法務部と協業で作成しているが、規定の主管は総務部となっている ●個人情報は通常ネットから切り離して別枠で管理している
	CSIRT構築状況	●CSIRTは構築済みでメンバーは事業部門、総務部門、ＩＴ部門、情報子会社等の実務リーダー8名で全員兼務 ●CSIRTが活動するのは重大インシデント発生時のみ ●CSIRTの役割などはコンサル会社と一緒に作った。シーサート協議会にも参画している ●CSIRTは世の中の動向に合わせて作った⇒CSIRT協議会には入っている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ 情報セキュリティ体制の構築状況（続き）

- 既存のリスクマネジメント体制との関係として、サイバーセキュリティへの認識が高まり、全社リスク管理委員会とは別枠で議論されるようになってきているとの傾向が注目される。なお、両者は相互連携することが前提である。

表3.3 既存のリスクマネジメント体制との関係に関するコメント

分類	主なコメント	具体的な意見
情報セキュリティ体制の構築状況	既存のリスクマネジメント体制との関係	● 全社リスク管理委員会があるがBCPが中心で、ITセキュリティはあまり議論されない。情報セキュリティ部会とはリンクしていない ● パンデミックやBCPなどの全社リスクはコーポレートガバナンス委員会で管理しているが、サイバー含む情報セキュリティはIT本部。相互連携している。 ● 全社リスクはコーポレートガバナンス委員会で管理しているが、サイバーセキュリティは別枠で管理している ● HDにITガバナンス部を新設した、ガバナンス担当、セキュリティ担当（2名）、部長含め4名で構成され、グループ会社のガバナンス（共通ツールを使うなど）を行っている。海外については十分にできておらず課題である ● リスクマネジメントはERMとして別組織になっており、セキュリティとは対になる関係。ERMとは連携している ● 全般的なリスクと情報セキュリティリスクは別になっていて、情報セキュリティと個人情報はセキュリティ専門部署が担当しているIT部門とは別組織となっている。IT部門はセキュリティ対策の実施を担当しており実質的なCSIRTである ● 全社的なリスクは委員会（リスク管理委員会）が担当しており、情報セキュリティもその一つではあるが情報セキュリティは別組織にしており連携する形になっている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ 情報セキュリティ体制の構築状況（続き）

- 24時間365日の運用が必要なSOCや専門技術が必要な業務が外部委託するという傾向が示される一方、外部委託のルールは基本的なもので、選定基準は設けていないとの意見もみられる。

表3.4 アウトソーシングしているセキュリティ関連業務とその理由、社内体制との切り分け状況、委託先の選定基準に関するコメント

分類	主なコメント	具体的な意見
情報セキュリティ体制の構築状況	アウトソーシングしているセキュリティ関連業務とその理由、社内体制との切り分け状況、委託先の選定基準など	● 外部委託のルールはないが、運用（オペレーション）は基本的に外部、企画や管理は社内。セキュリティ専門知識が必要な業務は外部委託。SOCも外部 ● 外部委託の基本的な方針はあるが選定基準は特になく都度判断している。例えばSOCなど24/365はアウトソース。アウトソース判断の起案はIT本部（セキュリティ統括）が行っている ● 外部委託の明確な方針はないが、コスト的に見て都度判断している。脆弱性診断はベンダーに委託している。SOCまでは委託していない　インシデント発生の対応も内部で実施 ● セキュリティ監視は24/365であるので外部委託している。インシデント対応は内部であるがフォレンジックは一部外部。脆弱性診断も専門性が高い部分は外部に委託している。SOCの管理部分は社内 ● ISMS取得のための足りない知識など外から借りる ● 第三社評価はITベンダー・コンサルにそれぞれ偏りがあるので、少しずつ変えながらやっている。 ● CSIRT構築時にコンサルに入ってもらった。 ● クラウドについてもチェックリストはあるが、十分ではない ● 検知ソフトとの連動、脆弱性診断、FW監視、SOCなどは外部委託 ● セキュリティ対策は基本的に自社が行うのが基本方針。但し、フォレンジックなど専門技術が必要なものは外部委託

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ 情報セキュリティ体制の構築状況（続き）

- IoT、工場系システムは生産本部が統制しITが支援しているケースが多い
- 商品開発のセキュリティは品質管理の中でチェックしている

表3.5 OTの管理体制や商品開発体制（PSIRT等）に関するコメント

分類	主なコメント	具体的な意見
情報セキュリティ体制の構築状況	OTの管理体制や商品開発体制（PSIRT等）との関連	● IoT、工場系システムは情報系からノウハウを展開し、生産本部などが統制をとっている。ITが作ったセキュリティガイドを生産本部に渡して対応してもらっている ● 開発は品質に重点を置いているので、セキュリティも品質でチェックしている ● IoTセキュリティガイドラインを作ろうとしている。協力会社は現場ではカメラを使えないようにしている ● 情報セキュリティ責任者会議のもとに、製品セキュリティとエンタープライズ系のセキュリティについて、それぞれの主体領域に応じて部会に分けて活動。上位の責任者会議には部会のメンバーが重複してでてくるので自然な形で情報連携できるようになっている ● 商品開発にセキュリティがわかる人がいないので、開発案件にITガバナンス部が参加している ● 工場などのシステム・セキュリティなどは全社統一ルールになっている。工場の総務部門が窓口 ● 生産では機密情報を扱っていないのでセキュリティ管理していない ● ECサイトの基盤はITが提供しており、脆弱性診断などはIT部門が実施 ● 商品開発は品証が管轄しているが、ITに関わるところはIT部門が実施 ● 工場系については社内ネットの関係もありITが指示したりチェックしたりしている ● MSIRT、PSIRTなどはなくCSIRTが全体をカバーしている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ 情報セキュリティ体制の構築状況（続き）

- グループ会社のセキュリティガバナンスが重要な課題となってきている
- グループ会社にはセキュリティ担当がいないケースが多く、IT部門が支援している
- グループ会社は点検シートで定期的にチェックし、改善するまでフォローしている

表3.6 グループ会社の管理・ガバナンスとの関係に関するコメント

分類	主なコメント	具体的な意見
情報セキュリティ体制の構築状況	グループ会社の管理・ガバナンスとの関係	● 関連会社へのガバナンスは、日本・APAC・チャイナには日本の施策等を展開している。欧州は情報共有 ● 海外とは定期的に情報交換しているが、規定は個別に作っている ● 今後は代理店のセキュリティガバナンスが優先的な課題。部品メーカーについては、専売的につきあっている小規模なメーカーには責任者をたててもらったりしている。去年くらいからは、新聞事案などもふえたこともあり興味をもってもらってきている。お助け隊の無料サービスも活用している。 ● グループ会社にはIT担当はいるがセキュリティ担当はいないので、セキュリティに関してはITガバナンス部が担当している ● 各統括組織は個別に点検シートを使って評価しているが、半期に一度実査をしている。期待値とギャップがある場合は改善されるまでフォローしている。 ● 物流倉庫のセキュリティなどは個別に実施してもらっている。情報セキュリティはセキュリティ統括だがそれ以外のセキュリティは個別に実施している ● サプライチェーンは半期に一度点検してもらっている。 ● 海外関連会社の評価用にチェックシートは作っている。各社にセキュリティのヒアリング（経理・総務などに、駐在員がいればアサイン）している ● セキュリティのガバナンスをきつめに（中央集権的）に行っている。例えばPCの管理者権限はすべて取り上げITガバナンス部で管理している ● インターネットのサービスに対するガバナンスは情報セキュリティ本部とITがガイドラインを出したりツールを提供している ● 各事業会社、事業部門には責任者と担当（IT系の担当）を置くことになっている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ 現体制となった背景・経緯

- 事業拡大に伴い集中型から連邦型に転換。各統括本部にセキュリティ責任者を置いて階層的な管理としている
- グループ会社の業種・業態により体制を変えることも検討されている

表3.7 現体制となった背景・経緯に関するコメント

分類	主なコメント	具体的な意見
現体制となった背景・経緯	おもな影響要因（グループ企業や海外拠点の影響、DX推進体制、OTやIoTとの関係、取引先との関係、等?）	● グローバルでは日本の傘下にAPAC、中国があり、日本がガバナンスしている欧・米にはそれぞれCIOがおり、それぞれで対策を実施している ● 海外の契約がのびているが、海外にはセキュリティ担当がいないのでITガバナンス部が見ることになっているがリソースの問題もあり十分に対応できていない ● 事業の拡大に伴って今の形になった。集中型は難しくなってきたので連邦型にした。各統括本部にセキュリティ責任者を置いて階層的な管理をしている。また、業種業態によって体制を変えることも検討している。例えば金融は多と異なるのでそれに合わせた合理的な体制にする。但しホールディングはきちんと管理する。 ● セキュリティ統括組織は10年くらい前に作った。各統括本部にもセキュリティ責任者も置いてもらった。 ● セキュリティ事故が大きな転機となって、ISMS認証取得をした。意識レベルも上がった。 ● セキュリティ関連は必ずCISOに相談することになっており、意識レベルはかなり高いといえる。CISOの権限も強いので商品開発でリスクがある場合は改善がされない場合はストップできる。CEOもセキュリティ意識が高い ● 2000年初頭にワームなどのインシデントが多発したのをきっかけにセキュリティ委員会と事務局ができた ● 2006年に大規模な個人情報漏洩事故が発生し、この時にセキュリティ統括組織を作って強化した

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ インシデント発生時の緊急対応／復旧体制の整備状況

- インシデントの大きさによって伝達ルートが異なる。インシデント発生時にランクを判断し、重大インシデントは危機管理委員会に直接報告
- インシデント管理システムでインシデントの発生から終息まで管理

表3.8 インシデント発生時の緊急対応／復旧体制の整備状況に関するコメント

分類	主なコメント	具体的な意見
インシデント発生時の緊急対応／復旧体制の整備状況	緊急連絡先・伝達ルート	● 緊急連絡は整備している。CSIRTはないが、インシデントの大きさによって適切なメンバーを招集している。この時のリーダーはIT部長が行っている ● 在宅勤務体制の場合はキーマンにダイレクトに話をするほうが早い ● インシデントの伝達ルートはあるが、インシデントの大きさによってルートが異なる。インシデント発生時にリストによりランクを判断し、インシデント大は直接危機管理委員会に報告する ● BCPマニュアルにセキュリティインシデントの対応方法が決まっている ● インシデントが発生したら専用のメーリングリストに速報する。各部署にキーパーソンがいて初動をサポートしている。またこのMLにはセキュリティ統括も入っていて状況を確認している。SOCが検知した場合はセキュリティ統括に連絡は入る ● インシデント管理システム（ワークフロー）でインシデントの状況（発生から終息まで）が見えるようになっている ● レベル判定は当事者とセキュリティセンターで行っている ● インシデントには6つある。パンデミック、システム障害、自然災害、セキュリティなどでそれぞれに管理部門が決まっている ● 伝達ルート：従来は組織の上長経由で、工場などは上長決裁後にエスカレーションされたりするので時間がかかった。今年1月にCSIRTができてからは直接上げるようになった。

3.1 企業調査

(1) ユーザー企業ヒアリング調査

表3.8 インシデント発生時の緊急対応／復旧体制の整備状況に関するコメント（続き）

分類	主なコメント	具体的な意見
インシデント発生時の緊急対応／復旧体制の整備状況	緊急連絡先・伝達ルート	● 経営へのインシデント報告。PC紛失などはITのほうに上がってくるが、本当にビジネスインパクトの大きいインシデントはコーポレートガバナンスのほうに上がってきてしまうことが多い。 ● グローバルSOCがある。グローバルで共通の監視方法が決まっており、検知できるインシデントは自動で監視している ● 情報漏洩にあたるかどうかわからないケースもある。例えば個人情報が入っているファイルがあり、外から見える状態になっていたとしてもそれだけではインシデントにはならない ● インシデントになる前段階で検出することを検討している ● ツールで検知した結果が正しいかどうかを判断することも難しい ● 伝達ルートはあるが、セキュリティで何かあったら担当に直接言えとなっている ● CSIRTを何時招集するかは明確に決まっていないが、自分に報告があった時に判断している ● インシデントは伝達のワークフローがありそこに流している ● インシデントはワークフローに乗ればすべてCIOまであがる ● SOCからの監視報告はワークフローではなくIT部長経由でCIOに直接報告している ● ワークフローで管理しているのは報告のみで、対策などは別管理 ● 情報セキュリティ体制がありセキュリティ窓口もあるのでそこから情報が上がってくる。すべて情報セキュリティ本部に報告することになっている ● インシデントは各組織の窓口で報告するかどうかを判断している。外部に影響しているかが判断に基準 ● 関連会社からは各社の経営統括部を経由してインシデントが上がってくる

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ インシデント発生時の緊急対応／復旧体制の整備状況（続き）

- 初動マニュアルは整備しており、訓練もしているがインシデントには様々なケースがあり、マニュアル化しきれない
- 初動マニュアル、復旧マニュアルを廃止した。マニュアルだけに頼っていると機能しないし、慣れると見なくなる（形骸化する）。プリンシパルベースにしてインシデントの一報は入れるが、対応はそれぞれの専門家、担当者が適切な対応をすることにした

表3.9 初動対応マニュアルの整備・運用に関するコメント

分類	主なコメント	具体的な意見
インシデント発生時の緊急対応／復旧体制の整備状況	初動対応マニュアルの整備・運用	● 各部署にキーパーソンがいて初動をサポートしている。またこのMLにはセキュリティ統括も入っていて状況を確認している。SOCが検知した場合はセキュリティ統括に連絡は入る ● 危機管理室が経営直下にあり、ここが初動を行う。以前は会議体だった。 ● 初動マニュアル、復旧マニュアルがありそれぞれ訓練していたが、今年1月に廃止になった。マニュアルに頼っても機能しないし、慣れてくると見ない。現在はプリンシパルベースとしており、インシデントが発生したら危機管理室に必ず一報を入れることだけが決まっている。それぞれの専門者、部門がインシデントに対して適切な対応をとることが求められる ● 初動対応マニュアル：インシデントが発生したときは速やかに通報することが基本。インシデントはCSIRTからコーポレートガバナンスに報告して、そこからトップに挙げている。訓練も実施している。 ● ファイル1つが漏れたとしても、様々なケースがありルールやガイドでは決めきれない。難しい案件はマネージャが判断するしかない⇒マニュアル化しきれない ● 初動対応マニュアルは作った。インシデントが発生したらCSIRTで取りまとめて、リスクレベルを判定し部長、常務に報告し対策本部の設置有無を決めることになっている。

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ インシデント発生時の緊急対応／復旧体制の整備状況（続き）

- サイバーセキュリティやコーポレートガバナンス担当でインパクトを評価し、その結果をもとに広報部門で公表を判断

表3.10 インシデントの報告･公表等に関するコメント

分類	主なコメント	具体的な意見
インシデント発生時の緊急対応／復旧体制の整備状況	CSIRT有無、経営者への報告ルート	● CSIRTを何時招集するかは明確に決まっていないが、自分に報告があった時に判断している
	公表内容やタイミング	● 公表は広報部門が判断。サイバーセキュリティとコーポレートガバナンスの担当がインパクトを評価し、広報部門に提出する
	業務の復旧計画の策定・見直し	● 重要システムにつては復旧計画を作っているが、訓練は実施していない

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ インシデント発生時の緊急対応／復旧体制の整備状況（続き）

- 訓練は形ではなく実働に沿った形で定期的に行う（表面的な訓練では意味がない）
- サーバーセキュリティはグローバルでの訓練も有効
- 在宅勤務になりTeamsなどのツールを使った訓練も試行しているが、フローが細切れになり全体像が見えにくいなどの課題もある

表3.11 訓練・演習に関するコメント

分類	主なコメント	具体的な意見
インシデント発生時の緊急対応／復旧体制の整備状況	訓練・演習	● 重大障害時のシステム切り替え訓練は実施しているが、セキュリティインシデント発生時の訓練は実施していない ● 初動訓練は毎月のセキュリティ会議で毎回実施している（20分程度）。形ではなく実働に沿った訓練を行っている ● 経営や広報も巻き込んだ訓練を計画していたが新型コロナの影響で延期となった ● サイバーセキュリティはグローバルの訓練をしている ● 訓練は定期的にやっている。在宅勤務時の訓練は想定フロー作って Teamsを使ってのオンライン会議で実施している。フローを細切れにしてやってみたので、全体像がみえにくかった。シナリオはCISRTにかかわる人用のみ。全社員には、怪しいことが起こったらとにかくサイバーセキュリティ窓口に連絡してくれといっている ● 訓練は基本的に行っていない。表面的な訓練では意味がない。問題解決の風土があるのでマニュアルや訓練をしなくても最適な対応ができる ● 訓練シナリオ（事故時の報道対応）は作ったが、新型コロナで未実施のままである。メールの訓練は継続してやっている ● インシデント訓練はしている。メール訓練、インシデントが発生したときの連絡訓練などを実施している ● ハードニングという訓練をしている。各部門から5名くらいを集めて、役割を決めて実際のインシデントが発生してことを想定した訓練を行っている。訓練の結果は点数をつけて評価している。インシデントの対処を現場を交えて実施している。頻度は年に1回で一大イベントとして実施している。 ● メール訓練、e-learningは実施している ● インシデント発生時の訓練は全体では実施していないが、各組織（ITも含めて）では実施している

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策状況の把握

- クラウドサービスを使うときはセキュリティ要件を確認する
- 委託先のセキュリティ評価をしていない場合でも契約を締結すること

表3.12 委託先の評価・管理のPDCAに関するコメント

分類	主なコメント	具体的な意見
ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策状況の把握	委託先の評価・管理のPDCA	● クラウドサービスを使うときはかなり厳格に評価している ● クラウド選定の際はセキュリティ要件を確認している　ルールが古いので見直しは必要 ● 委託先は契約書で縛る程度で個別には評価・管理していない ● 委託先には常駐型と非常駐型があるが、大手のベンダーが入っているので導入時には評価したがそのあとは分からない ● グループ会社とのネットワークは2種類あり、本社と直接つながるAネットには関連会社はつながせていない。本社とつなぐ必要があるときは本社から専用端末を送っている。50%以上の子会社はAネットにつないでいるが、本社と同等のセキュリティ対策とチェックを行っている ● 通常の委託先はセキュリティの評価はしていない（秘密保持契約は締結） ● クラウドサービスを使うときはチェックリストで委託際評価を実施している ● 常駐している委託先は社員と同じ扱いで管理している ● 外部委託先は別ルートで管理している ● クラウド利用はチェックシートをつけて申請してもらっている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

② ユーザー企業におけるセキュリティ関連人材

■ セキュリティ人材（セキュリティ業務に専任で従事している人材）

- ホールディングス、事業会社にセキュリティ統括組織を配置
- 事業部門や関連会社にはセキュリティ統括責任者をアサインしているが、育成のためセキュリティ統括組織に兼務してもらうこともある
- ホールディングス、事業会社、事業部門でローテーションを行い人材を確保

表3.13 セキュリティ統括機能を担う人材の確保に向けた考え方や取組に関するコメント

分類	主なコメント	具体的な意見
セキュリティ人材（セキュリティ業務に専任で従事している人材）	セキュリティ統括機能を担う人材の確保に向けた考え方や取組	● 専任は統括に60名。部門からの兼務が30～35名で半分くらいはセキュリティの仕事をしている（本籍は各部門：プラスセキュリティ人材２） ● 責任者にはISMSをベースとした研修を受けてもらっている ● 責任者がセキュリティ統括組織に来ることもある ● ビジネスがデジタルによってきているのでその意味でもセキュリティ担当は不足している ● 人材開発のチームと協業してICT統括としてどう人材配置するかをガバナンスしている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ セキュリティ人材（セキュリティ業務に専任で従事している人材）（続き）

- セキュリティ人材の採用は中途採用が中心で、人事部が介在せず直接採用
- セキュリティ人材の採用には責任者自らが参画、実務者の声を載せるなどの工夫が必要
- セキュリティ統括担当には全社のシステム理解やインフラの経験が必要で容易には育成できない
- 事業部でセキュリティを担当する人材を一旦セキュリティに配転し育成することも検討し、最終的にどのような人材をどこに配置するかを検討する

表3.14 実務者･技術者層のセキュリティ担当者の確保に向けた考え方や取組みに関するコメント

分類	主なコメント	具体的な意見
セキュリティ人材（セキュリティ業務に専任で従事している人材）	実務者・技術者層のセキュリティ担当者の確保に向けた考え方や取組	● 確保は中途採用と派遣を行っているが、最近ようやく派遣を採用した ● 採用は中途が99%。セキュリティのようなスペシャリストは人事部が介在せず部門で直接採用している。 ● キャリア採用も行っており、自身が採用活動（説明会、インターンシップ）を行っている。しかし、地元での採用は難しい。また特別な処遇を行っていないのでなかなか集まらない ● セキュリティ担当は技術的専門集団と、ガバナンス（設計管理系の2名）系とがいる。キャリア採用もしている。 ● セキュリティの人材はまだ不足している。ここ2年くらいで拡充してきているが、100名くらいにしたい。セキュリティオペレーションを担う技術者と監視する人（テレワークで需要増）、関連部門・会社を実査する担当 ● 人材確保はローテーションと中途採用。採用ページに実務者の声を載せている。カジュアル面談も行っている。社内紹介として中途採用で入った人に紹介してもらっている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

表3.14 実務者･技術者層のセキュリティ担当者の確保に向けた考え方や取組みに関するコメント（続き）

分類	主なコメント	具体的な意見
セキュリティ人材（セキュリティ業務に専任で従事している人材）	実務者・技術者層のセキュリティ担当者の確保に向けた考え方や取組	● セキュリティ統括担当には全社のシステムの理解、インフラや開発の経験が必要で、容易には育たないし確保できない ● 過去にセキュリティ技術を担当した人を中心にチームを作って育成している ● ガバナンス系のセキュリティ人材は、経験年数の豊富なシニアを活用していようとしている。 ● コネクテッドインダストリー系の人材もセキュリティに配転してコネクテッドセキュリティを育てようともしている。最終的にこういう人材がどこにいたらいいのかも含めて検討中。 ● 不足するスキルはセキュリティベンダーからアドバイスを得る ● ゼロトラストなどインフラに関しても考慮しなければいけないのでセキュリティ担当の不足感が強くなっている ● インシデントがなるべく起こらないようにするには社員のリテラシー向上が必要でe-learningなどを実施しているが、それでもサイバー攻撃は起きるので検知をしたりビジネスをデザインするには外部から人材を持ってくるしかない

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ セキュリティ人材（セキュリティ業務に専任で従事している人材）（続き）

- セキュリティ専門人材の育成にはIPAのICSCoEを活用し中核人材とする
- セキュリティ人材を3段階に分類して育成。1段目はIT関係者レベル、2段目は情報システム管理者レベル、3段目はエキスパートレベル
- インフラ担当をセキュリティ部門で育成し戻すなどのローテーションも検討
- セキュリティ担当向けの特別な人事制度はほとんど持っていない
- 高度な専門技術者は人材価値を設定しセキュリティ部門で報酬を決めている
- 資格取得の費用を負担しているところが多く、一部では資格維持費用も会社負担としている

表3.15 セキュリティ人材の活躍（キャリアパス、処遇ほか）に関するコメント

分類	主なコメント	具体的な意見
セキュリティ人材（セキュリティ業務に専任で従事している人材）	セキュリティ人材の活躍（キャリアパス、処遇ほか）	● セキュリティ専門人材の育成はICSCoEを活用している。これまで3名（製造と設計から各1名参加）が参加している。これらの人材を今後の中核人材にしていきたい。できるだけ早く課長に上げたりはしているが、特別な処遇はない。しかし残念ながら1名は転職してしまったので、ここが課題である。 ● 最近セキュリティ人材を3段階に分類して育成をしている。1段目はIT関係者レベルでセキュリティの教育やテストを行っている。２段目は情報システム管理者レベルで一段と高い教育をしている。3段目はエキスパートで公的資格（CISSPなど）を取ってもらっている。取得・維持費用は会社持ちだが人事評価まではつながっていない。しかし、処遇はあまり変わらない　給与への直接的反映もない ● インフラを2年経験した人材をセキュリティで預かり育成後に戻すことを検討

3.1 企業調査

(1) ユーザー企業ヒアリング調査

表3.15 セキュリティ人材の活躍（キャリアパス、処遇ほか）に関するコメント（続き）

分類	主なコメント	具体的な意見
セキュリティ人材（セキュリティ業務に専任で従事している人材）	セキュリティ人材の活躍（キャリアパス、処遇ほか）	● 人事制度は最近変えた。セキュリティ人材は1年契約の成果報酬型で専門力の高い人材は高報酬 ● 専門職制度はなく、管理職でも専門的知識が求められる ● 今後は橋渡し人材が重要である ● 人事制度は全社共通だが、報酬はセキュリティ部門で決められる。自部門で人材価値を設定して報酬を決められる。 ● 資格の費用は試験から登録・維持まで補助している。チャレンジそのものにサポートしている。対象資格は7つ位、CISSP、セキスペ、CISM、CHなど。しかし、これが報酬には反映されない ● キャリアパス支援として資格取得の支援とか大規模プロジェクトのPMに対する手当などはやっている。 ● プロフェッショナルに対する手当などがないと人が集まらない

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ プラス・セキュリティ人材（セキュリティ業務に兼務で従事している人材）

- 情報システム部門のインフラ担当がセキュリティを包含して取り組んでいる
- 事業部のセキュリティ責任者・担当者をローテーションして確保することも

表3.16 情報システム部門でセキュリティ関連業務を担う人材の確保に向けた考え方や取組に関するコメント

分類	主なコメント	具体的な意見
プラス・セキュリティ人材（セキュリティ業務に兼務で従事している人材）	情報システム部門でセキュリティ関連業務を担う人材の確保に向けた考え方や取組	● インフラ全体の中にセキュリティを包含して取り組んでいる ● ITの仕事の一環としてインフラ全体の中にセキュリティを包含して取り組んでいる ● 兼務のセキュリティ担当は10名ほどいるが、自分がセキュリティ担当と分かっていない人もいる。例えばSIEMの導入担当はITインフラの仕事として実施しているかもしれない ● ITインフラで対策実施項目を決めて、その中でセキュリティも担当しているかたち ● 事業部のセキュリティ責任者がセキュリティ統括組織に来ることもある ● セキュリティ担当は3名いるが全員IT部門インフラ担当が兼任している

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ プラス・セキュリティ人材（セキュリティ業務に兼務で従事している人材）

- 事業部のセキュリティ人材育成に力を入れるところが増えている
- 事業部のセキュリティ担当はシステムアドミニストレータ（SA）が必須
- セキュリティ統括に入ってもらうなどローテーションも有効

表3.17 事業部でセキュリティ関連業務を担う人材の確保に向けた考え方や取組に関するコメント

分類	主なコメント	具体的な意見
プラス・セキュリティ人材（セキュリティ業務に兼務で従事している人材）	事業部でセキュリティ関連業務を担う人材の確保に向けた考え方や取組	● 事業部のセキュリティ担当はシステム連絡窓口、情報システム部門とのつなぎ ● 事業部門には情報セキュリティ責任者と担当者をアサインしてもらっているが、担当者に特別な教育は行っていない ● 事業部の人材育成を重点的にやろうとしている ● 事業部の人材育成に事例を使った研修を考えている ● 事業部門のセキュリティ担当はシステムセキュリティアドミニストレータ（SA）を必須でアサインすることになっている。SAの育成は専門の教育クラスを設けている ● セキュリティ統括のチームに入ってもらい育成している ● 人材育成のカリキュラムは作っていないが、ローテーションは計画している ● 各事業所ごとにシステムとセキュリティの担当者が決まっている。こういった人材にもセキュリティ教育を使っている ● 製品開発者のセキュリティ教育は別枠で行っている。研究所では勉強会を行っており、事務局機能はセキュリティ統括部門が担当している ● 事業部のセキュリティ担当はISMSの担当者がやっている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ プラス・セキュリティ人材（セキュリティ業務に兼務で従事している人材）

- ICSCoEなどのセキュリティ専門教育を受けた人材は直接現場に戻す前にセキュリティ統括で育成（熟成）してから戻すなどの工夫が示されている。

表3.18 管理部門・工場現場でセキュリティ関連業務を担う人材の確保に向けた考え方や取組に関するコメント

分類	主なコメント	具体的な意見
プラス・セキュリティ人材（セキュリティ業務に兼務で従事している人材）	管理部門でセキュリティ関連業務を担う人材の確保に向けた考え方や取組	● 特別な部門、機密情報を多く扱う部門（人事、戦略など）はITも含めて部門で人材を抱えているが、フォレンジックのような専門性の高い案件はセキュリティ統括と連携している
	工場現場でセキュリティ関連業務を担う人材の確保に向けた考え方や取組	● 生産部門からICSCoEに出した人材も本当に生産部門にもどしていいのか。セキュリティの重要性をかたろうとするとブレーキをかけることにもなる。生産部門にもどしても浮いてしまうのではないか。ある程度そろってから現場へ戻そうとしている。 ● セキュリティ業務に兼務で従事している人材向けの教育カリキュラムはないが、工場保全の人などと現場とのローテーションによって学んでもらおうとしている。 ● 生産設備自体がIT化する流れの中、ITセキュリティがセットになっているので生産の人にもわかってもらわないといけない。IT系の人間が工場に出向いたりもしている。 ● IoTのセキュリティガイドライン作りなど派遣の人にやってもらっている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ プラス・セキュリティ人材（セキュリティ業務に兼務で従事している人材）

- 各事業部のセキュリティ責任者／担当者を定期的に入れ替えることによりセキュリティ人材を育成
- 各事業部のセキュリティ責任者／担当者を関連会社のCISOにしたり、統括組織に移動するなどのローテーションを実施

表3.19 プラス・セキュリティ人材の活躍（キャリアパス、処遇ほか）に関するコメント

分類	主なコメント	具体的な意見
プラス・セキュリティ人材（セキュリティ業務に兼務で従事している人材）	プラス・セキュリティ人材の活躍（キャリアパス、処遇ほか）	● 各統括部にはセキュリティ責任者のほかにセキュリティ担当者（責任者の予備軍）が数名いる。責任者は年に20%くらい入れ替わるが、それによって育成ができている。また元責任者は関連会社のCISOになったりしている。また責任者が専任の担当になることもある

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ セキュリティに関する教育・研修の実施状況

- 一般社員向けのセキュリティ教育はeラーニングで実施。コンテンツは自社で作成または外部購入
- セキュリティ意識向上にはWebサイトを立ち上げ事例やアドバイスを載せる
- テレワーク向けにオンライン会議システムを活用した教育も有効
- 新人教育はセキュリティ枠を設けて実施、この時に自社事例を入れる
- セキュリティ統括組織の育成は資格取得支援。資格取得後はそれに見合った仕事のアサインが重要
- 事業部のセキュリティ責任者にはISMSをベースとした教育を実施

表3.20 スキル向上に向けた育成の方針・考え方に関するコメント

分類	主なコメント	具体的な意見
セキュリティに関する教育・研修の実施状況	スキル向上に向けた育成の方針・考え方	● セキュリティ教育はeラーニングで実施している。eラーニング教材は総務部が作っているが、コンテンツの情報をITが提供している。 ● セキュリティ統括組織としても教材を作るうえで勉強している ● その他には新人向け教育、中途採用向け教育を行っている ● セキュリティ教育はeラーニングで行っている。コンテンツは外部から購入している ● リテラシー向上はe-learningをしている。e-learning教材は内製 ● セキュリティの日常的コミュニケーションのためにWebサイトを立ち上げた。ここには様々な事例やＦＡＱ的なアドバイス集などを載せている ● Teamsを使ったセキュリティ管理者向けの研修なども検討中 ● テレワークのセキュリティは時間がなく対応しきれていない。今後、ガイドラインをつくって教育していく ● 社内ポータルでセキュリティ関連の情報を継続的に発信している

3.1 企業調査

(1) ユーザー企業ヒアリング調査

表3.20 スキル向上に向けた育成の方針･考え方に関するコメント（続き）

分類	主なコメント	具体的な意見
セキュリティに関する教育・研修の実施状況	スキル向上に向けた育成の方針・考え方	● 新人向け教育、中途採用向け教育を行っている ● 新人教育はセキュリティ枠を設けて行っている。このとき自社事例を入れている ● セキュリティ統括組織内の育成は資格取得支援、仕事のアサインを行っている。個人の特性に合わせた仕事のアサインを行っている。 ● セキュリティ担当者に必要な経験は何か起きた際の対応力 ● サイバーセキュリティの運用監視などの専門教育はグローバルエクスチェンジプログラムに送って教育している。グローバルで同じスキームを使っている ● 責任者にはISMSをベースとした研修を受けてもらっている ● 人材は育成がベースで、セキュリティベンダーと一緒にやっているのでそこでOJTで育成している

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ セキュリティに関する教育・研修の実施状況

- 活用している資格はISACA、CISSP、セキスペなどがあるが、取得費用が高く維持費用も高い
- 開発者にはセキュリティデベロップメントライフサイクルに関する研修を受けてもらう
- セキュリティコーディングを必ず受講させている
- セキュリティ専門人材の育成はICSCoEを活用

表3.21 活用している外部教育サービスや教材に関するコメント

分類	主なコメント	具体的な意見
セキュリティに関する教育・研修の実施状況	活用している外部教育サービスや教材	● 資格としてはISACA、CISSP、セキスペなどがあり、人材ごとに設定して取得させるようにしている（マストに近い）。取得費用が高く維持費用も高いのが悩み ● 開発者向けにはセキュアSDL（セキュリティデベロップメントライフサイクル）を使っている。コンテンツは内製している ● セキュリティ専門人材の育成はICSCoEを活用している。これまで3名（製造と設計から各1名参加）が参加している。しかし残念ながら1名は転職してしまったので、ここが課題である ● エンジニアにはセキュリティコーディングを必ず受講してもらっている

3.1 企業調査

(1) ユーザー企業ヒアリング調査

■ セキュリティに関する教育・研修の実施状況

- セキュリティスキルマップまではまだできていないが、人材開発カルテがあってコンピテンシーを棚卸ししている
- 仕事のアサインはマネージャが能力を見極めて実施

表3.22 セキュリティスキルのアセスメント状況に関するコメント

分類	主なコメント	具体的な意見
セキュリティに関する教育・研修の実施状況	セキュリティスキルのアセスメント状況	● セキュリティについてはスキルマップまでは整理できていない ● これを身につけろというのではなく、自分でも率先して勉強できるようにしている。そのため費用も出している ● 人材開発カルテがあってコンピテンシーを棚卸しして評価している仕組みはある ● 仕事のアサインはマネージャが能力を見極めて実施している

3.1 企業調査

(1) ユーザー企業ヒアリング調査

③ ティップス集について

- ユーザー企業におけるセキュリティ人材・組織体制について10社にヒアリングを実施した。その結果からセキュリティ対策を検討する際の参考となる取り組みのヒントをまとめたのがティップス集（右図）である。サイバーセキュリティ成熟度評価を実施した結果、自社において改善すべき対策を検討する上で活用していただくことを想定している。
- ティップスは「サイバーセキュリティ経営ガイドライン Ver2.0ー付録A サイバーセキュリティ経営チェックシート」の項目ごとに整理した。
- なお、本ティップス集には令和元年度にまとめたティップス集も組み入れて再構成している。
- 次ページにティップス集のタイトル一覧を示す。

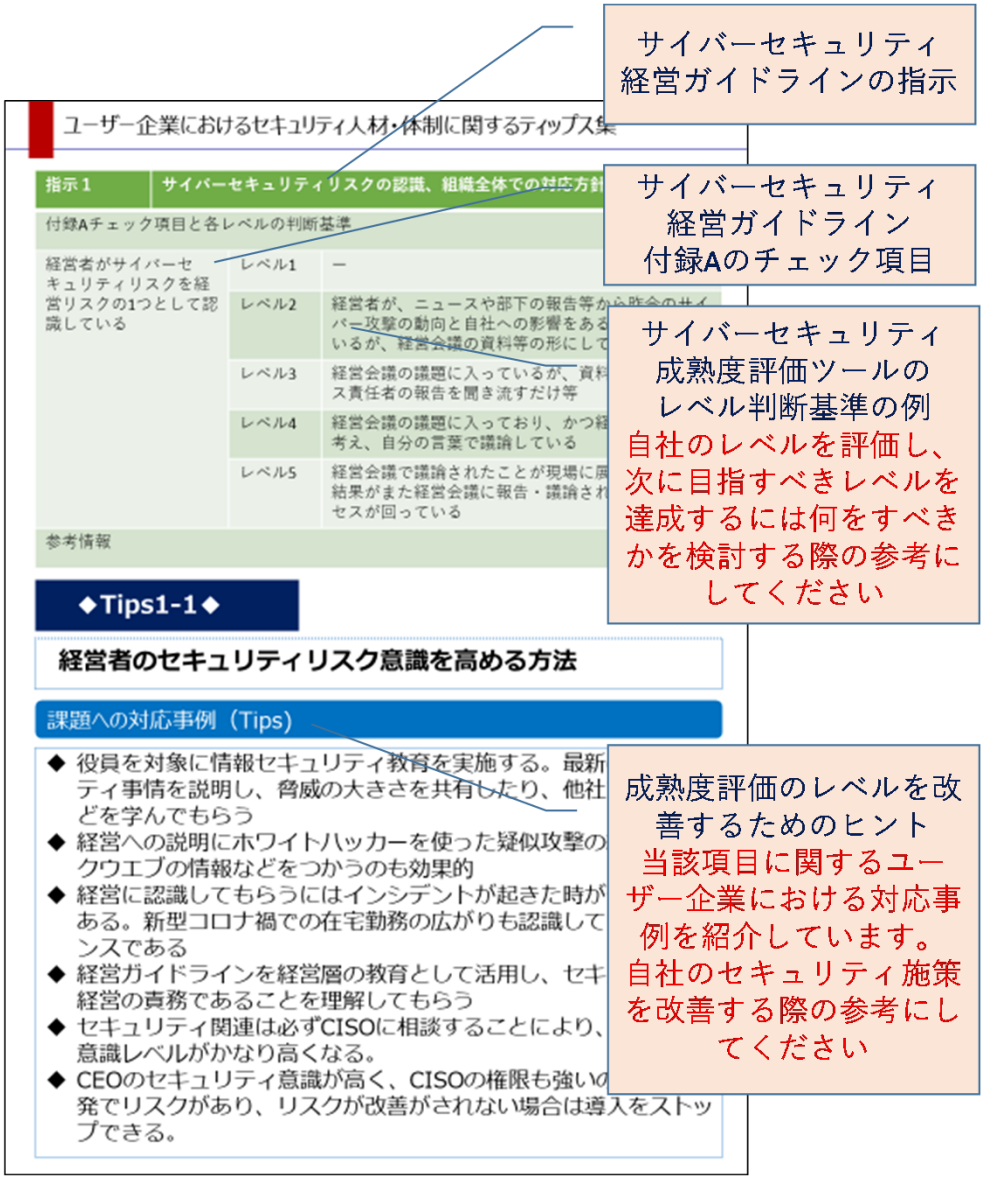


図3.2 ティップスイメージ

3.1 企業調査

(1) ユーザー企業ヒアリング調査

表3.23 ティップス集のタイトル一覧

指示NO	指示内容	#	付録A項目	Tips番号	Tipsタイトル
指示１	サイバーセキュリティリスクの認識、組織全体での対応方針の策定	1-1	経営者がサイバーセキュリティリスクを経営リスクの1つとして認識している	1-1	経営者のセキュリティリスク意識を高める方法
		1-2	経営者が、組織全体としてのサイバーセキュリティリスクを考慮した基本方針を策定し、宣言している	1-2	セキュリティガバナンスの強化
		1-3	法令・契約やガイドライン等の要求事項を把握し、対応している	1-3	各国法令の理解と対応
指示2	サイバーセキュリティリスク管理体制の構築	2-1	組織の基本方針に基づき、CISO等からなるサイバーセキュリティリスク管理体制を構築している	2-1	セキュリティ管理体制の構築 2-1-A:スピードアップ、クイックレスポンスに対応した体制構築 2-1-B:グループ・グローバルのセキュリティ管理体制（集権型） 2-1-C:グループ・グローバルのセキュリティ管理体制（連邦型） 2-1-D:OTやIoTを含めたセキュリティ体制の構築
		2-2	セキュリティリスク管理体制において、各関係者の役割と責任を明確にしている	2-2	セキュリティ部門と管理部門、事業部門の役割と責任
		2-3	組織内のリスク管理体制（リスク委員会等）とサイバーセキュリティリスク管理体制（セキュリティ委員会等）の関係を明確にしている	2-3	企業リスク管理とサイバーセキュリティリスク管理体制の明確化
指示3	サイバーセキュリティ対策のための資源（予算、人材等）確保	3-1	経営会議等の議論により、サイバーセキュリティ対策とそれを実施できる資源（予算、人材等）を明確にしている	3-1	セキュリティ対策に必要なスキル・能力 3-1-A:セキュリティ管理者に必要なスキル・能力 3-1-B:セキュリティ担当者に必要なスキル・能力（マネジメント） 3-1-C:セキュリティ担当者に必要なスキル・能力（技術） 3-1-D:事業部のセキュリティ担当者に必要なスキル・能力 3-1-E:プラスセキュリティに必要なスキル・能力
		3-2	自組織で対応する部分と外部に委託する部分を適切に切り分けている	3-2	外部委託の活用基準
		3-3	自組織に求められる体制を明らかにし、計画的にサイバーセキュリティ人材を確保、育成するとともに、適正な処遇を検討している	3-3	セキュリティ人材の確保と育成の方法 3-3-A:セキュリティ人材の育成（OJT編） 3-3-B:セキュリティ人材の育成（外部研修編） 3-3-C:事業部のセキュリティ人材育成 3-3-D:商品開発担当者などのセキュリティ人材育成 3-3-E:生産部門、工場などのセキュリティ人材育成 3-3-F:セキュリティ人材の評価とキャリアパス 3-3-G:セキュリティ人材不足の対応方法
		3-4	外部に委託する部分について、自社の課題、予算、場所等を考慮して適切な外部リソースを選定し、活用している	3-4	外部リソースの選択と活用方法

3.1 企業調査

(1) ユーザー企業ヒアリング調査

表3.23 ティップス集のタイトル一覧（続き）

指示NO	指示内容	#	付録A項目	Tips番号	Tipsタイトル
指示4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	4-1	守るべきIT資産（情報資産やシステム）を特定し、当該資産の場所やビジネス上の価値等に基づいて優先順位付けを行っている	4-1	リスクアセスメントの実施（何を守るべきか、敵は誰か）
		4-2	特定した守るべきIT資産に対するサイバー攻撃の脅威、脆弱性を、脅威情報のデータベース等を用いて認識し、これらによるサイバーセキュリティリスクが自社の事業にいかなる影響があるかを把握している	4-2	脅威情報の入手と自社への影響の把握
		4-3	サイバーセキュリティリスクの影響の度合いに従ってリスク対応計画を策定している	4-3	リスク対応計画（ロードマップ）の作成
指示5	サイバーセキュリティリスクに対応するための仕組みの構築	5-1	情報システムのIT資産管理・構成管理・パッチ管理を行っている	5-1	IT資産管理・構成管理の方法
		5-2	組織内でシャドーITを利用させない対策を行っている	5-2	シャドーITへの対策
		5-3	システム設計時にリスク分析を行い、必要なセキュリティ機能を具体化し、開発時に実装している	5-3	セキュリティ・バイ・デザイン、セキュアコーディングの実施
		5-4	重要業務を行う端末・サーバ等には複数の技術的防御策を実施している	5-4	端末・サーバなどのセキュリティ対策の実施
		5-5	重要業務を行うネットワークには複数の技術的防御策を実施している	5-5	ネットワークのセキュリティ対策の実施
		5-6	システム等に対する定期的な脆弱性診断や、継続的なパッチ適用、その他の緩和策等の脆弱性対策の計画を立て、実行している	5-6	脆弱性診断と対策立案の定期的実施
		5-7	端末やネットワークからのログを収集・分析している。	5-7	ログの収集と分析方法
		5-8	サイバー攻撃を検知した際に不正通信を遮断する等のインシデント対応の仕組みを導入している	5-8	サイバー攻撃の検知と対応方法の明確化
		5-9	インシデントの管理の仕組みを導入している	5-9	インシデント管理の仕組み導入
		5-10	従業員に対して、サイバーセキュリティの教育・演習を実施している	5-10	サイバーセキュリティ教育と演習の実施

※　グレーアウトしたティップスは今後作成予定

3.1 企業調査

(1) ユーザー企業ヒアリング調査

表3.23 ティップス集のタイトル一覧（続き）

指示NO	指示内容	#	付録A項目	Tips番号	Tipsタイトル
指示6	サイバーセキュリティ対策における PDCAサイクルの実施	6-1	サイバーセキュリティ運用管理に関するKPIを定めている	6-1	セキュリティKPIの設定と報告
		6-2	経営者が定期的に、サイバーセキュリティ運用に関する報告を受け、認識対策を指示している	6-2	経営会議等でのセキュリティ状況の報告と対策の審議
		6-3	サイバーセキュリティにかかる内部監査、外部監査を踏まえ、サイバーセキュリティ対策を適時見直している	6-3	セキュリティ監査の実施
		6-4	サイバーセキュリティリスクや取組状況をステークホルダーに情報公開している	6-4	セキュリティレポートの作成と公開
指示7	インシデント発生時の緊急対応体制の整備	7-1	インシデント対応計画を策定している	7-1	インシデント対応計画の作成と連絡網の整備
		7-2	インシデント対応の専門チーム（CSIRT等）を設置している	7-2	CSIRTの構築方法
		7-3	組織外に報告・公表すべき内容やタイミングを定めている	7-3	インシデント発生状況の報告と発表
		7-4	インシデント発生時の緊急対応の演習を定期的に行っている	7-4	インシデント対応訓練の実施
		7-5	インシデント発生時のログ分析・調査を速やかに行い、影響範囲を特定できるよう実施計画を策定している	7-5	インシデントのログ分析・調査と初動対応
指示8	インシデントによる被害に備えた復旧体制の整備	8-1	被害が発生した際に備えた業務の復旧計画を策定している	8-1	復旧計画の策定
		8-2	定期的に復旧対応演習を行っている	8-2	復旧訓練の実施
指示9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	9-1	グループ企業に関するリスク分析を行い、対策をグループ内の規程等で明確にし、対策状況の報告を受け、適時見直している	9-1	グループ会社のリスク分析・評価と対策の実施
		9-2	委託先等の取引先に関するリスク分析を行い、対策を契約書等で明確にし、対策状況の報告を受け、適時見直している	9-2	取引先、委託先の評価と契約の締結
		9-3	サプライチェーン全体を俯瞰した関連組織全体で、リスク分析を行い対策状況の検討を行っている	9-3	サプライチェーン全体のリスク分析と対策の実施
指示10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	10-1	関係団体が提供する注意喚起情報の入手や、業界のセキュリティコミュニティ等への参加を通して情報共有を行い、自社の対策に活かしている	10-1	サイバーセキュリティ関係団体への参画と情報共有
		10-2	マルウェア感染、不正アクセス等のインシデントがあった際に、関係団体やコミュニティに情報提供や相談を実施している	10-2	サイバーセキュリティ関係団体へのインシデント情報の提供

※　グレーアウトしたティップスは今後作成予定

3.1 企業調査

(2) IT／セキュリティベンダー企業ヒアリング調査

- ユーザー企業でサイバーセキュリティ対策に従事する人材に求められる知識・スキル等に知見を有するIT/セキュリティベンダーとして、人材育成や人材派遣、資格制度運用等の事業を行っている企業を対象とするヒアリング調査を実施した。
  - 新型コロナ禍の影響もあり、インタビューはすべてリモート会議で実施した。
  - 企業の選定にあたっては、調査趣旨を踏まえた多様性を有するように配慮した。
- インタビュー参加企業・団体：6社

3.1 企業調査

(2) IT／セキュリティベンダー企業ヒアリング調査

- 前ページに示したIT/セキュリティベンダーへのヒアリング結果を示す。

① 企業でサイバーセキュリティ対策に従事する人材市場の実態

- 人材派遣市場では、テストと運用・保守の単価は他よりも低い。ゆえに、ITSS+の運用・保守の区分に単価の高い「マルウェア解析」があるのに違和感がある。研究開発に置くほうが実態に即している印象。
- 業務ごとに金額は異なる。マニュアルに沿ってオペレーションする場合は単価は低い。運用設計等、上流にいくほど高くなる。
- CSIRTの中での業務の細分化は行っていない。
- 経験年数による切り分けとして、体感レベルとしては、3年目で中堅、5年目以上でベテランである。
- 年収800～1000万円クラスの人材が転職市場に現れることはほとんどなく、たまに出てもすぐ決まってしまう。運用監視などのオペレーションレベル業務にはそこまでの年収が示されることはなく、市場にいないということもない。
- 求人側がセキュリティ担当者の募集時に細かい分野指定を行うことはほとんどない。なぜなら市場にセキュリティの専門性を有する人材が潤沢におらず、細かく条件を示したところで採用に苦労することを理解しているため。細かく経験を把握したい場合は、業務を通じた苦労話を聞く。
- 応募側では業務経験を書く際に「OTの脆弱性診断実績あり」や診断ツール名など細かく書いてアピールする。SOC/CSIRTの業務経験であればNCAの人材区分相当で実績を示したり、運用経験のある製品名を示したりする。
- セキュリティエンジニアは「守り」の印象がある。攻めていきたい・市場価値の高いエンジニアになりたい人の興味の対象になっていない。単価が上がれば変わるかもしれない。
- プラス・セキュリティは区別されておらず、ある程度充足している印象。ただしネットワークセキュリティやクラウドセキュリティを扱う人材は足りていない。これは既存のプラットフォームにセキュリティが加味されるところである。ネットワークやセキュリティという名前によって単価が大きく変わることはない。

3.1 企業調査

(2) IT／セキュリティベンダー企業ヒアリング調査

② サイバーセキュリティに関するスキルについて

- コミュニケーション力、プレゼンテーション力等、技術以外のスキルの要否がセキュリティ業務の種類毎に異なるのは事実であるが、案件紹介に際してそれでふるいにかけることはしていない。これは、未経験でもチャレンジしてみたい、あるいはコミュニケーション力はあっても別の仕事をしてみたいといった本人の意向を重視するため。むしろ、フォーマル／カジュアルといった企業カルチャーとの相性を意識している。
- 「プラス・セキュリティ」の職種で現状ではセキュリティスキルがあることは加点要素になっていない。一方で、データサイエンスなどのスキルがあるとプラスに評価される。
- 初心者レベルのセキュリティスキル評価は、ITSSレベル１や２の条件に準じて行っている。

③ 人材育成とキャリアについて

- アプリやサービスの欠陥が社会問題になる一方、その開発で「シフトレフト」「DevSecOps」等のセキュリティをどう取り込めばよいのかを学べる適切な場がない。
- ネットワークのアプライアンスの保守から設計のようにキャリアアップするモデルはある。
- 中小企業が気軽に学んだり相談できるコミュニティの普及が重要。
- セキュリティエンジニアを増やすための助成金や国主催のイベントや研修会があると、各企業も投資しやすいのではないか。

3.2 有識者ヒアリング調査

(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として下表の方々に対し、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　等
- さらに、セキュリティ統括等、ユーザー企業に所属する立場でセキュリティに関する専門的な知識・スキルを活用する人材のキャリアや育成についての経験・知見を把握する観点から、産業サイバーセキュリティセンター（ICSCoE）修了者２名の協力を得て、ICSCoEへの参加前後での業務内容の実態や効果等についても調査し、3.5における手引き書の作成時に反映した。

表3.26　サイバーセキュリティ人材活躍モデルの構築に関する有識者ヒアリング調査対象者

専門家・学識者	6名
ICSCoE修了生	2名

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。

① 企業によるサイバーセキュリティ対策の実態

- 起業家向けのセキュリティ講座を実施しているが、VPNが伝わらない。「VPNはどこに行ったら買えるのか？」という質問が出るほどである。
- 「なんとなく怖い」「気になるけれどどうしたらよいかわからない」というレベルが多く、対策まで踏み込もうとしない。
- 地方企業の人材育成にオンラインセミナーの活用は有用。ハードニングもオンラインで実施しているので、思いのほか学べる内容は多い。
- 地方企業向けの人材育成は、地方公共団体の産業振興系部署の主導でセミナーを開催するなどして、意識付けを図っていくのがよい。地方公共団体による事業実施や支援に期待している企業が多いので、関心を集めることは難しくない。

② サイバーセキュリティに関するスキルについて

- セキュリティ統括機能に関して、文系マネジメント層に理系技術者の思考パターンを理解してもらうのは良い考えかもしれない。セキュリティやITは文系からは依然として技術者目線で動いているように見える。
- プラス・セキュリティに関して、法務系の業務は論理的であり、ITやセキュリティとの相性がよいかもしれない。ITの知識がある人が法務を学ぶのは有益そうである。一方、法務をずっとやってきた人が、セキュリティを学ぶ場合、楽ではなさそうでありモチベーションを維持することに工夫が必要。

3.2 有識者ヒアリング調査

(2) ヒアリング結果

② 企業おける今後のサイバーセキュリティ対策の考え方

- 将来のビジネス展開との関連性を検討する必要がある。コンプライアンスとの関連性、経営者自身のリスク管理の考え方を考慮する必要がある。そこで、セキュリティがグローバルに注目されていると話している。セキュリティは技術だけではなくて、ビジネスや経営であるということを主張してほしい。
- セキュリティ対策の現場が担う責任と権限は一体。日本は明文化しなくてもうまくいっていた。今後は、少なくともどこの部門が責任を取るのかというルールを事前に固めておく必要がある。万が一、リスクベースで不測の自体が起こった場合に、ビジネスを縮退・停止する権限を委譲する仕組みを経営者のサポートの元で策定する必要がある。経団連も出し始めたので、強めに言ってもいい時期かもしれない。海外のステークホルダーに説明責任を果たすために必要である。
- 戦略的ローテーションは難しいと思う。現在、全社人事的な観点ではジョブ型が流行している。その中でセキュリティを一つのジョブとして定義・配置できるのかが課題。NISCでも職務明細書をはっきりさせていくことは必要と発言している。セキュリティはIT部門だけでなくコーポレート全体で考える必要があり、その点を明記する必要があるのではないか。
- 日本の経済界として発展していくマクロの話と、そこで活躍するセキュリティ人材は、将来どのようなキャリアを磨くのかという展望的な話があると、経営者や人事部門が食いつきやすい文書になるのではないか。
- 中小企業相手でやるには、個人を中小企業が雇うのではなく、商工会議所などが間に入って人材をプールし、派遣等の形態とするのが現実的と思う。

3.3 有識者会議の開催

(1) 有識者の選定

- 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、次表のメンバーで構成される「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2.4に示す有識者会議と一体化して運営した。
  - ユーザ企業におけるセキュリティ人材・体制の整備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
  - 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の活用促進策
  - セキュリティ人材のニーズとシーズのマッチングのために必要となるその他の政策　等

表3.25 「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」構成員（再掲）

分類	対象者名（敬称略）	所　属
委員	荒川　大	株式会社ENNA 代表取締役 一般社団法人サイバーリスク情報センター 事務局長
	武智　洋	日本電気株式会社 サイバーセキュリティ戦略本部 主席技術主幹 一般社団法人サイバーリスク情報センター 代表理事
	平山　敏弘	学校法人電子学園　情報経営イノベーション専門職大学 教授 特定非営利活動法人日本ネットワークセキュリティ協会　教育部会長
	宮下　清	一般社団法人日本情報システム・ユーザー協会　参与
	持田　啓司	株式会社ラック　理事 情報セキュリティ教育事業者連絡会（ISEPA）代表
オブザーバ	経済産業省 商務情報政策局 サイバーセキュリティ課／情報技術利用促進課／地域情報化人材育成推進室 独立行政法人情報処理推進機構 セキュリティセンター／社会基盤センター	

3.3 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3.26 「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	おもな議題（文字が灰色の内容は本報告書第２章に関するもの）
第1回	2020年4月27日	●『サイバーセキュリティ経営可視化ツールβ版』の改良について（目的、使い方、修正方針等） ● 手引き書の検討課題について（リスクマネジメント、外部委託、スキル・能力の考え方等）
第2回	2020年5月19日	● 手引き書の検討課題について（構成案、業種別体制図等）
第3回	2020年6月17日	●『サイバーセキュリティ経営可視化ツールβ版』の改良について（改良方針、調査項目案等） ● 手引き書案の見直し方法について ● ユーザー企業調査の実施方法について
第4回	2020年7月14日	●『セキュリティ体制構築・人材確保の手引き（第１版）』の内容案の検討
第5回	2020年8月4日	●『セキュリティ体制構築・人材確保の手引き（第１版）』のレビュー
第6回	2020年12月16日	● 手引き書に追加すべき内容の検討 ●『サイバーセキュリティ経営可視化ツールβ版』を試行した企業を対象とする調査結果について
第7回	2021年1月26日	● 手引き書の改定の方向性の検討 ●『サイバーセキュリティ経営可視化ツールver.1.0』に向けた進捗報告
第8回	2021年2月16日	●『セキュリティ体制構築・人材確保の手引き（第１.1版）』の内容案の検討 ● 企業ヒアリング調査結果報告
第9回	2021年3月2日	●『セキュリティ体制構築・人材確保の手引き（第１.1版）』のレビュー

3.3 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3.27 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
National Cyber Security Strategy 2016-2021	英国Cabinet Office	2016年
SFIA（Skills Framework for the Information Age）Version 7	英国SFIA Foundation	2017年

表3.28 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
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）

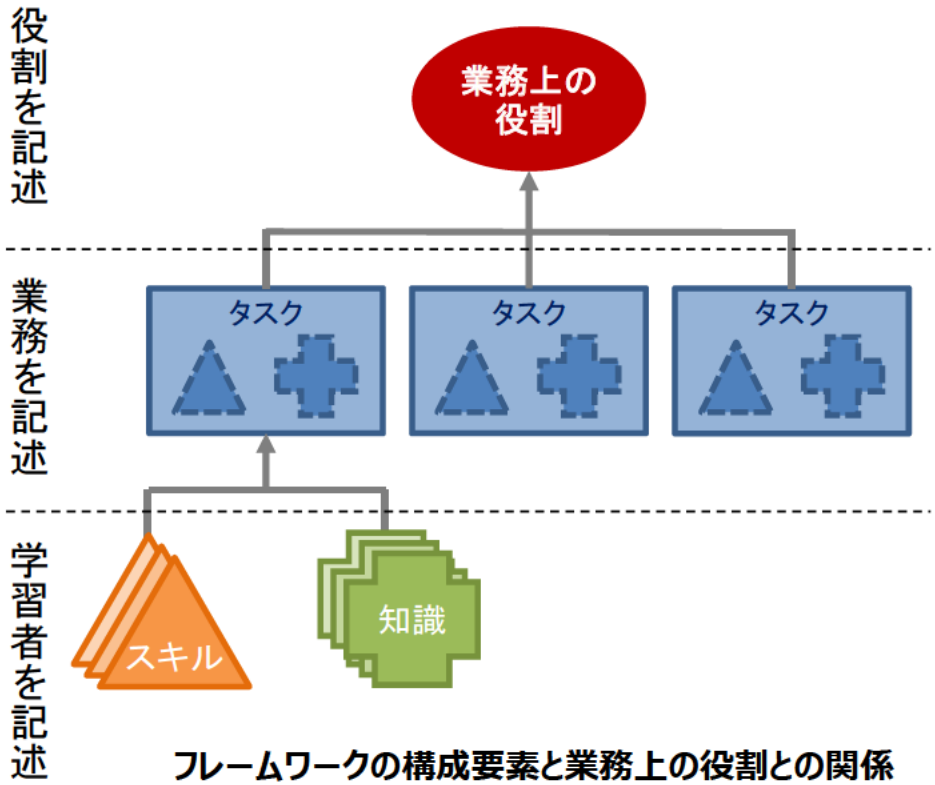
表3.29 民間団体が公表しているサイバーセキュリティ人材の育成・活用に関する文書

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.1.5）	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	2017年3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

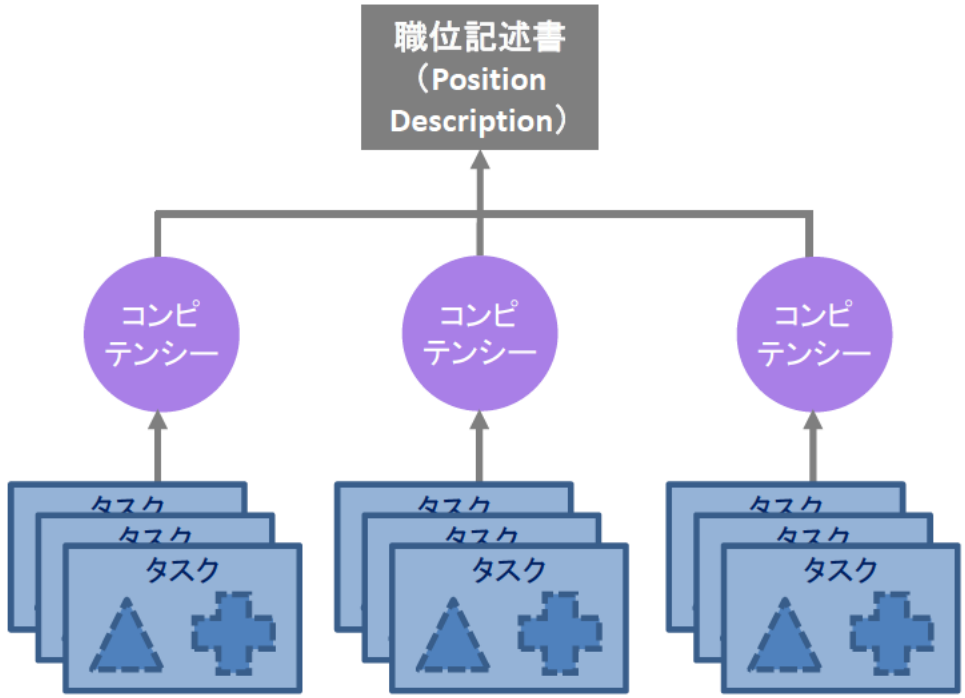
3.3 文献調査

(2) 調査結果

- 文献調査結果の例として、2020年11月に公表された米国NIST 800-181r1（NICE人材フレーワーク）における改定の概要を示す。
  - ➢ これまでは、米国政府機関に実在するサイバーセキュリティ対策関連の役割ごとに、必要となるタスクとKSA（知識、スキル、能力）の組合せで表現。
  - ➢ 現行版では、機関毎に適切なコンピテンシーをタスクの組合せで表現し、業務に関する職位記述書（Position Description）をコンピテンシーの組合せで表現。



フレームワークの構成要素と業務上の役割との関係
（これまでと大きな変更無し）



職位記述書を通じた学習者評価のためのコンピテンシーの利用
（新たに規定されたもの）

図3.3 NIST SP800-181r1における変更

3.4 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」
    - 第5回 産業サイバーセキュリティ研究会（2020年6月30日開催）
    - 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4回会合（2020年8月6日開催）
    - WG2 第6回会合（2020年8月25日開催）、第7回会合（2021年2月18日開催）
    - WG1 第5回会合（2020年9月11日開催）
    - WG1 電力サブワーキンググループ 第9回会合（2020年9月29日開催）、第10回会合（2020年12月17日開催）、第11回会合（2021年2月15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4回会合（2021年1月13日開催）
    - WG1 宇宙産業サブワーキンググループ 第1回会合（2021年1月14日開催）、第2回会合（2021年3月3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3回会合（2021年3月5日開催）
    - WG3 第6回会合（2021年3月10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13回会合（2020年7月31日開催）、第14回会合（2021年1月21日開催）

3.5 「セキュリティ体制構築・人材確保の手引き」の開発

- 調査結果をもとに、企業において経営者の指示のもと、実際に自社のセキュリティ体制の構築や、人材の確保・育成に取り組む方を対象に、サイバーセキュリティ経営ガイドライン経営ガイドライン付録F「セキュリティ体制構築・人材確保の手引き」として2020年9月に第1版、2021年3月に第1.1版の原稿をそれぞれ作成した。その内容を図3.4～図3.5に示す。

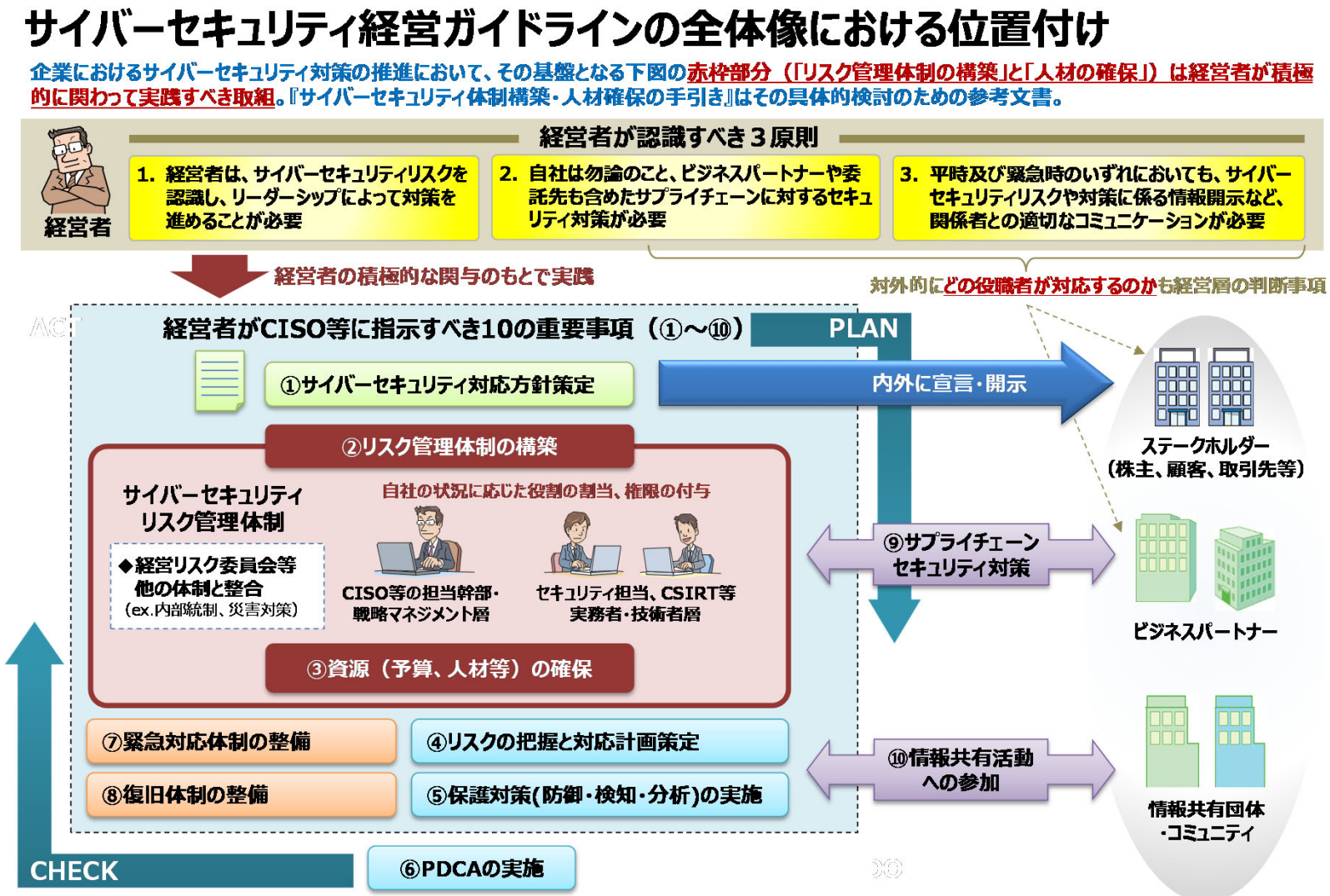


図3.4 「セキュリティ体制構築・人材確保の手引き」の位置付け

3.5 「セキュリティ体制構築・人材確保の手引き」の開発

- 「セキュリティ体制構築・人材確保の手引き」における説明内容のポイントは次の通りである。
  - サイバーセキュリティに関する役割の実践にあたっては、責任に見合った権限の付与が重要。
  - 特に「プラス・セキュリティ」業務においては組織内のセキュリティ対策における役割の自覚の観点からも重要。

指示２ **サイバーセキュリティリスク管理体制の構築**	**2.1** **経営者のリーダーシップの下でのセキュリティ体制の検討**	①デジタル技術の活用の進展に伴い、従来とは異なる全社的なセキュリティ体制が必要となってきている。 ②全社的なセキュリティ体制の確立は経営者の責務であり、経営者がリーダーシップをとる必要がある。
	2.2 **セキュリティ統括機能の検討**	①全社的なセキュリティ体制の確立のためには、CISO等の経営層を補佐する「セキュリティ統括機能」（次ページ参照）の設置が有効。 ②セキュリティ統括機能には大きく4つの類型があり、自社の状況に合わせて検討する必要がある。
	2.3 **セキュリティ関連タスクを担う部門・関係会社の特定・責任明確化**	①セキュリティ統括機能と連携しつつセキュリティ関連タスクを担う部門・関係会社を特定する際には、ITSS＋（セキュリティ領域）を参考にすることで、外部委託先も含めた見える化が可能。 ②外部委託先の選定に当たっては、情報セキュリティサービス基準適合サービスリスト等が活用可能。
指示３ **サイバーセキュリティ対策のための資源確保**	**3.1** **「セキュリティ人材」の確保**	①まずはサイバーセキュリティに関する専門性を備えたセキュリティ統括人材の確保を目指す。 ②担当する人材の育成を通じて質的充足を図る。
	3.2 **「プラス・セキュリティ」の取組推進**	①「セキュリティ人材」のみならず、デジタル部門、事業部門、管理部門等においてそれぞれの業務に従事する人材が、セキュリティを意識し、業務遂行に伴う適切なセキュリティ対策の実施やセキュリティ人材との円滑なコミュニケーションに必要な能力を育成する「プラス・セキュリティ」の取組も重要。 ②ITSS+（セキュリティ領域）等を活用し、関連部門でセキュリティ関連タスクを担う人材の特定・育成・配置等を検討。
	3.3 **教育プログラム・試験・資格等の活用と人材育成計画の検討**	①各分野に求められる知識・スキルを踏まえ、教育プログラムや試験・資格の活用を検討。 ②自社に必要な人材の配置計画をもとに、キャリアデザインを含めた育成計画を検討。

図3.5 「セキュリティ体制構築・人材確保の手引き」において示している検討のポイント

3.5 「セキュリティ体制構築・人材確保の手引き」の開発

- 「セキュリティ体制構築・人材確保の手引き」において扱っている概念として、下図に主要なものを示す。

セキュリティ統括機能

- セキュリティ対策及びインシデント対応において、CISOや経営層を補佐してセキュリティ対策を組織横断的に統括することにより、企業におけるリスクマネジメント活動の一部を担う
- 「機能」であって「組織」として設置しなくてもよい（状況に応じて、最適な形態は異なる）
  - 独立した組織として設置
  - 管理部門の１機能として割当
  - 情シス部門の１機能として割当
  - 組織横断的な委員会形態で運用

ITSS+（セキュリティ領域）

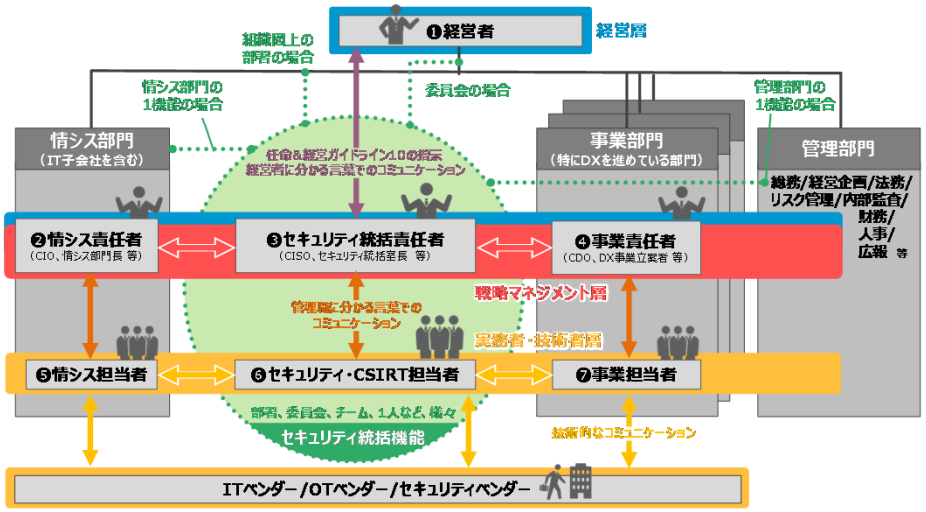
- 企業のセキュリティ対策に必要となる関連業務のまとまりを17分野に整理したもの
- セキュリティの専門性の高い分野だけでなく、経営層や法務部門、事業ドメインまで、サイバーセキュリティ対策に関わる幅広い領域を網羅
- DXの取り組みを通じたクラウド化、アジャイル開発、開発・セキュリティ対策・運用の一体化（DevSecOps）等の動きの中、ITSS＋で定める各分野の境界は曖昧化の傾向

プラス・セキュリティ

- セキュリティ対策を本務としないが、業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策の実践が求められる業務が「プラス・セキュリティ」の対象
- 「プラス・セキュリティ」人材が業務担当者と別に存在するわけではなく、これまでの業務担当者がサイバーセキュリティの知識・スキルを習得し、実践することを通じて対策を担う
- DXの取り組み有無に関わりなく、ITを活用するすべての企業において必要

セキュリティ統括機能のイメージ

企業の組織構造や事業内容に応じて下図の緑色部分の実現方法の検討が必要



ITSS＋（セキュリティ領域）（赤枠が「プラス・セキュリティ」の分野）

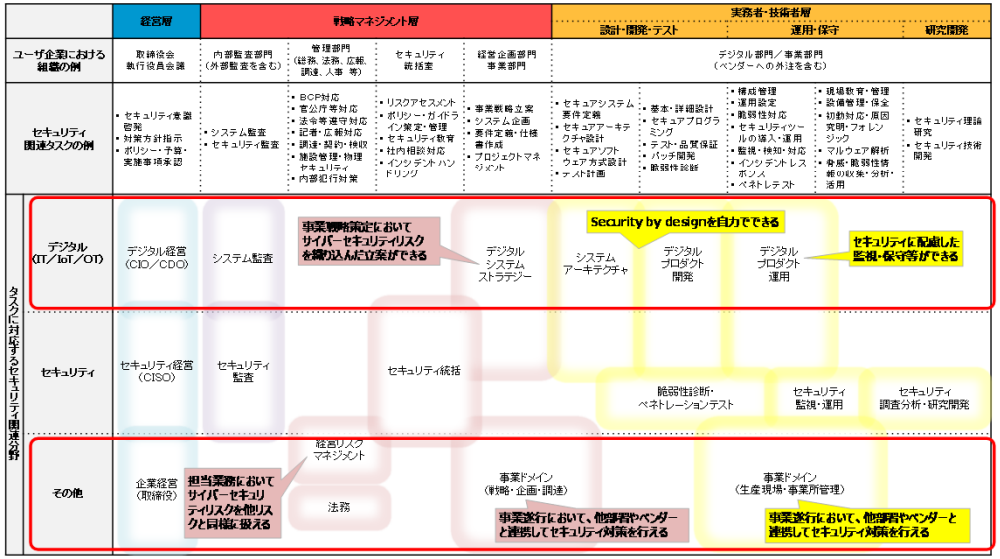


図3.6 「セキュリティ体制構築・人材確保の手引き」で扱っている主要概念

3.6 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

- 「共通言語」の必要性
  - 管理部門と事業部門、本社と工場、文系事務職と理系技術職、発注元と下請先、国内拠点と海外拠点などのように、リスクマネジメントの観点からは同程度の統制が機能してしかるべき条件において、サイバーセキュリティ対策の位置付けや扱いが異なることで適切に機能していないことが今後の脅威になる可能性がある。

② 課題解決の方向性

- 「共通言語」を用いることによる適切なデジタルガバナンスの実現
  - 3.5に示した「セキュリティ体制構築・人材確保の手引き」にて紹介しているITSS＋は、経営層から実務者層まで、セキュリティ専門業務から、プラス・セキュリティに相当する業務まで、企業においてサイバーセキュリティ対策を行う際に必要となる役割を横断的に扱えるようにすることを目的として作成されている。よって、企業が今後のDX推進にあわせて取り組んでいく必要があるデジタルガバナンスの一環としてのサイバーセキュリティ対策において、関係者間の共通言語として活用することで、役割の調整、人材の交流、連携による育成等を容易に行うことに役立つものと期待される。そこで、国や公的機関が今後ITSS＋のユースケースを示すことは、企業間での共通言語の利用を通じたリスクネジメントの実現の観点からも有効であり、現状における課題解決にも資するものと考えられる。

4. サイバーセキュリティコミュニティ形成の促進のための調査

4.1 サイバーセキュリティコミュニティの調査

(1) 文献調査

- インターネット等で公表されている情報をもとに、国内で現在活動しているサイバーセキュリティコミュニティ（勉強会、情報共有活動等）について調査し、ヒアリング調査対象選定の参考とした。

(2) ヒアリング調査

- 本事業において、８コミュニティを対象にコミュニティ形成・運営に関するプラクティスの把握を目的とするヒアリング調査を実施した。このうち、(3)に示す通プラクティス集に反映したもの以外の意見の要旨を以下に示す。

① 地域の企業の現状、コミュニティ活動を行っていく上での課題

- 企業の相談窓口としての役割を担っているが、機微な内容はコミュニティ経由での流出を恐れて相談しない傾向。公的機関ではないのでやむを得ないところ。
- コロナ禍で地理的制約が無くなった反面、コネクション形成の機会が失われてしまっている。オンラインで同様の効果をどうすれば得られるかは皆困っているところと思う。

② 公的機関による支援として期待するもの

- 公的機関を通じた告知や開催案内の配布により、集客を支援していただけるとありがたい。
- こちらから探しに行くのは大変なので、中小企業向けの資料や後援会情報などをコミュニティに流してもらえるとよい。
- 中小企業がサイバーセキュリティ対策費用を導入する際のインセンティブとなるような制度を拡充してほしい（SECURITY ACTIONよりも強い、契約・入札要件になるようなもの）。
- ユニークなベンダー資格が色々出てきているので、その取得補助を出すとエンジニアが興味を持ちそうである。
- 経済産業省系公的機関と中小企業との、サイバーセキュリティ対策目的でのいっそうの連携強化を期待したい。

4.1 サイバーセキュリティコミュニティの調査

(3) プラクティス集の作成

- 事例調査の結果及び経済産業省にて昨年度に３件のコミュニティを対象に実施された調査結果等をもとに、地域のセキュリティの関係者（公的機関、教育機関、地元企業、地元ベンダー等）が集まりセキュリティについての相談や意見交換を行うためのセキュリティコミュニティ（地域SECUNITY）形成の支援を目的として、各コミュニティが実践している次のような工夫をプラクティスとして紹介する資料として、『地域セキュリティコミュニティ【地域ＳＥＣＵＮＩＴＹ】形成・運営のためのプラクティス集第１版』を作成し、2021年2月に経済産業省より公表された。
  公表URL： https://www.meti.go.jp/press/2020/02/20210217001/20210217001.html

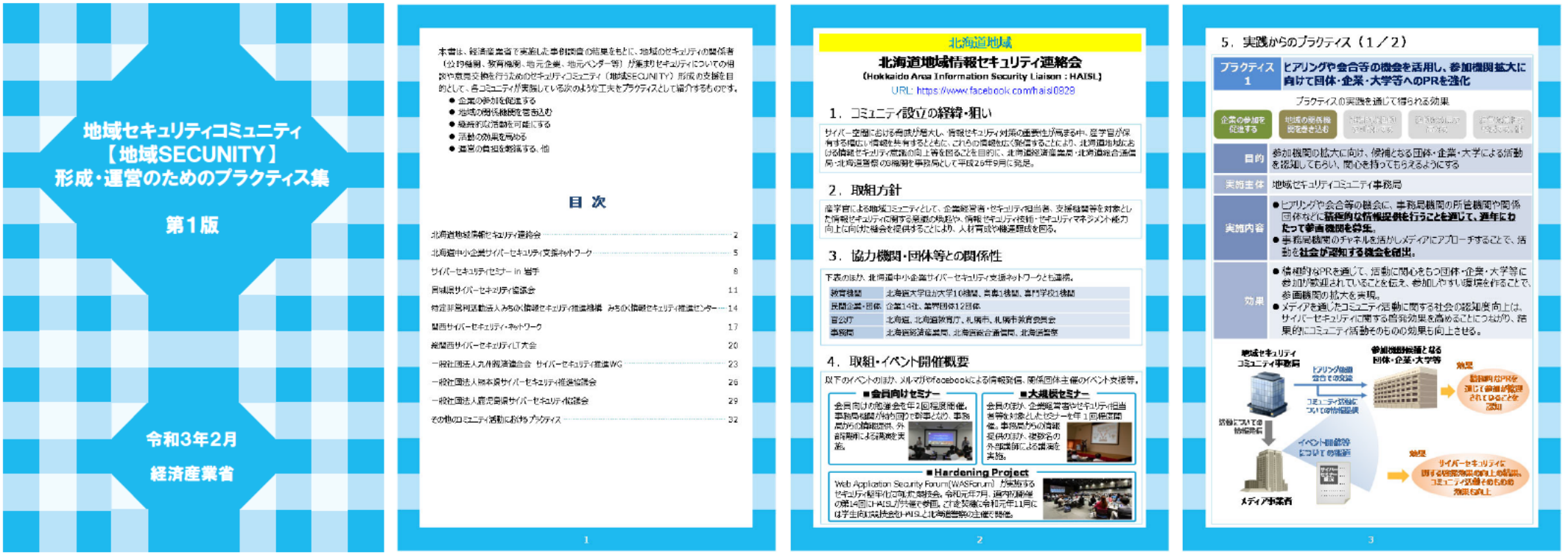


図4.1 『地域セキュリティコミュニティ【地域ＳＥＣＵＮＩＴＹ】形成・運営のためのプラクティス集第１版』の紙面例

4.2 各地域に駆けつけ可能な専門家や専門家派遣制度等の情報・問合せリストの作成

- 前ページに示したプラクティス集と合わせ、文献・ヒアリング調査等をもとに下表に示す駆けつけ可能な専門家や専門家派遣制度等の情報・問合せリストが作成され、2021年2月に公表された。

表4.1 各地域に駆けつけ可能な専門家や専門家派遣制度等の情報・問合せリスト

組織名	制度名	概要	担当	連絡先	URL
IPA	中小企業向け啓発セミナーへの講師派遣	中小企業へのセキュリティ対策普及を目的に、公的機関等の外部が主催するセミナーに対して、講師を派遣する。	IPAセキュリティセンター 企画部 中小企業支援グループ	Tel: 03-5978-7508 Fax: 03-5978-7546 E-mail : isec-pr-nw@ipa.go.jp	–
	地域の講習会	中小企業の情報セキュリティ対策向上のため、セキュリティプレゼンターを講師とした、情報セキュリティに関する講習会の開催を支援しています。	IPAセキュリティセンター 企画部　中小企業支援グループ IPA 地域の講習会事務局	Tel: 03-5978-7508 Fax: 03-5978-7546 E-mail : isec-semi@ipa.go.jp	https://www.ipa.go.jp/security/k_eihatsu/sme/local.html
	SECURITY ACTIONの普及啓発（講師派遣）	各地域で開催される情報セキュリティに関するセミナー等に対して、SECUNITY ACTIONの普及啓発を目的とした講師派遣を実施。	IPAセキュリティセンター 企画部 中小企業支援グループ	Tel: 03-5978-7508 Fax: 03-5978-7546 E-mail : isec-pr-nw@ipa.go.jp	–
	中小企業支援機関向け講師派遣	中小企業支援者の情報セキュリティ対策に関する指導スキルの向上を目的に、支援機関*が主催する内部研修等に、講師を派遣する。 *支援機関＝商工会議所連合会、商工会連合会、中小企業団体中央会、税理士会、よろず支援拠点、社会保険労務士会、中小企業診断(士)協	IPAセキュリティセンター 企画部 中小企業支援グループ	Tel: 03-5978-7508 Fax: 03-5978-7546 E-mail : isec-pr-nw@ipa.go.jp	https://www.ipa.go.jp/security/k_eihatsu/sme/shien.html
	セキュリティプレゼンター制度	セキュリティプレゼンター制度とは、IPAのセキュリティ対策資料等を活用して、中小企業等に対 して情報セキュリティの普及啓発を行う人材を「セ キュリティプレゼンター」として登録する制度で す。	IPAセキュリティセンター 企画部 中小企業支援グループ セキュリティプレゼンター担当	Tel: 03-5978-7508 Fax: 03-5978-7546 E-mail : isec-secushien-p@ipa.go.jp	https://www.ipa.go.jp/security/keihatsu/sme/presenter.html
JPCERT/CC	講師派遣	各地域で開催される情報セキュリティに関するセミナー等に対して、JPCERT/CCの職員を講師として派遣。	JPCERT/CC広報	E-mail: pr@jpcert.or.jp	https://www.jpcert.or.jp/kouen/2018.html
Grafsec（一般財団法人草の根サイバーセキュリティ運動全国連絡会）	シンポジウム、研修会等への講師派遣	地域支援活動の一環として、シンポジウム・研修会等への講師派遣、講演等を実施。	Grafsec事務局	E-mail: office@grafsec.or.jp	https://www.grafsec.or.jp/
JNSA（特定非営利活動法人日本ネットワークセキュリティ協会）	JNSA全国横断セミナー	サイバーセキュリティを事業運営に活用・定着させる上で参考となる国の政策や、最新脅威とその対策、マネジメントの解説、JNSAが提供している対策に活かせるツール等について紹介。	JNSA事務局	Tel: 03-3519-6440 E-mail: sec@jnsa.org	https://www.jnsa.org/seminar/2019/cross2019/

4.3 有識者ヒアリング調査

(1) ヒアリング対象者の選定

- 地域のサイバーセキュリティの活動やコミュニティ形成に詳しい有識者11名を対象に、次の項目についてのヒアリング調査を実施した。その意見要旨を以下に示す。
  - サイバーセキュリティコミュニティの調査方法、プラクティス集のまとめ方
  - サイバーセキュリティコミュニティが直面している課題、今後の支援の在り方

① 企業による地域セキュリティコミュニティの活用の実態

- 都内企業と比較すると、地域では「セキュリティは面倒」という認識のところが多い。
- 情報処理安全確保支援士の大半は企業に所属しており、この人達のうちコミュニティに関わる人は少ない。一方で、個人事業を営んでいる場合は積極的に関わる可能性がある。
- ITコーディネーターの会がうまく機能している。資格維持のためには講師経験が必要のため、彼らから動いてくれる。ただし謝金は少なくても必要。
- 資格制度のCPE（継続教育ポイント）の提供は企業からの参加者のモチベーション（インセンティブ）になっている。
- 勉強会に中小企業から参加する人には、一人情シスの担当者と、県警に誘われてくる人の 2 種類があり、これらが混じると満足度が高まらない。基本的には技術者向けと経営者向けを分けてイベントを行うのがよいが、たまに混ぜることにも意味がある。
- 温泉シンポジウムの参加者は専門性の高い人材が多く、地元人材とはギャップがある。それでも、人脈形成の場として活用している地元企業もある。セミナー講師候補とのチャネル構築にも有用。
- 継続的な活動には、地域に密着して活動している人とセキュリティの専門家とが連携することが必要。
- コロナ禍でリモート開催主体となったが、これまで対面の演習で行っていたものをどうするかは悩ましい。

4.3 有識者ヒアリング調査

(2) ヒアリング結果

② 地域セキュリティコミュニティに関する課題

- サイバーセキュリティ対策に関して、大学や県警に無料で相談できることが企業に知られていない。
- アフターファイブに社外で勉強することが、企業内で評価されないことがまだ多いようである。
- 企業のサポートを行う能力を養う必要がある。技術者がいきなりサポートを行えると思ってはいけない。
- 大学にセキュリティの専門家がいても、企業のセキュリティ対策を支援できる人とは限らない。高専でもサイバーセキュリティの専門家といえるのは片手で収まる程度の人数しかいない。
- 勉強会クラスのコミュニティが大学や商工会議所に協力を依頼しても、現実には動いてもらえない。
- 専門家が地元でお金を稼ぐことが難しい。士業しかできない業務を設定するなどが必要かもしれない。

4.3 有識者ヒアリング調査

(2) ヒアリング結果

③ 地域セキュリティコミュニティの支援方策

- オンラインでつながりができてくると、地域のつながりが薄れてくる。一方で地域で協力すべきこともあるので、地域コミュニティ形成の支援は有用である。
- 商工会議所・商工会に予算をつけ、そこで音頭をとってもらうのがよい。これらの経由でなければ中小企業にリーチできない。
- 中小機構の活用も考えられる。現状でも中小機構はコンサルタントの紹介をしている。
- 地域の情報産業協会の役割を明確化して参加を促す必要があるのではないか。
- 自治体が主導すべき。産業振興系部局が主導すると地元企業が集まる。担当者はセキュリティに詳しくなくても、重要性を理解していればよい。そのような人が異動等でいなくなると廃れる傾向。
- プログラムに経済的な援助を国が行うだけでなく、地域のCSIRTの表彰やプラクティスとしての共有はよい刺激になる
- 支援士会が、企業をサポートする人材の信頼性を保証するのがよいかもしれない。
- 認知されるまで時間がかかるので、回を重ねる必要がある。
- セキュリティに関心のある人がキーパーソンにいないと続かない。
- NPOとして活動するには、他では働かずに事務局を回せる人を確保できる予算（自主事業で確保等）が必要。公的な支援頼りでは持続的に活動するのは難しい。
- 大学で地域活動に貢献している人に対するインセンティブが必要。若い先生が研究活動を犠牲にするのは不幸であり、依頼側に理解が必要。
- DXのついでにセキュリティをやってもらうのがよい。

4.4 イベント情報や取組共有を目的とした国内政策調査

(1) 事例調査

- ユーザーにとっての利便性向上の在り方を検討することを目的として、国内のイベント情報や取組共有を目的とした国内政策に関する調査を実施した。次図に内閣サイバーセキュリティセンターで実施されている取り組み例を示す。

図4.2 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普及啓発・人材育成ポータルサイト』におけるイベント紹介事例

https://security-portal.nisc.go.jp/curriculum/dif_pickup05.html

4.4 イベント情報や取組共有を目的とした国内政策調査

(2) アンケート調査

- サイバーセキュリティコミュニティ形成を促進するツールの検討にあたり、主たるコミュニティ参加者として想定される企業のセキュリティ担当者を対象としたコミュニティへの関心や参加意向についてのアンケート調査を実施した。その実施要領は次表のとおりである。

表4.2 アンケート調査実施概要

対象	全国のユーザー企業でサイバーセキュリティ対策関連業務に従事するアンケート回答モニター 411名 （企業に勤務するモニター50,000名を対象とするスクリーニング調査をもとに抽出）
実施時期	2020年11月26日～27日
質問事項	●勤務先企業におけるIT利活用とセキュリティサービス利用状況 ●情報セキュリティサービス審査登録制度の認知と活用状況 ●登録サービスの利用経験 ●情報セキュリティサービス利用の課題と要望

4.4 イベント情報や取組共有を目的とした国内政策調査

(2) アンケート調査

① サイバーセキュリティコミュニティ活動への参加経験

- サイバーセキュリティ分野の学習や情報共有の手段として実施している取組（n=411、複数回答）

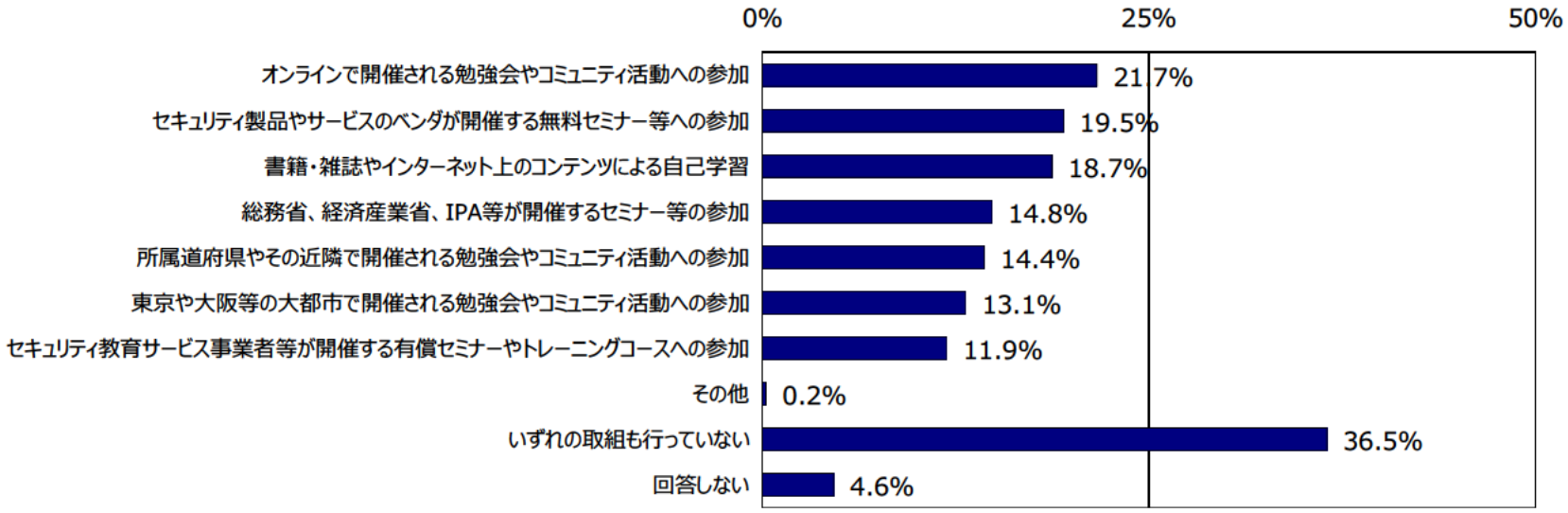


図4.3 サイバーセキュリティ分野の学習や情報共有の手段として実施している取組

- 参加したことがあるコミュニティ活動の内容（n=59、自由回答）
  - 企業が主催する講習会
  - 業界団体の勉強会に参加
  - 県や市で開催されている研修会
  - 商工会議所等が主催の勉強会に参加
  - 総務省 所管分野での団体に参加し、勉強会などのセミナーを開催
  - ベンダーのセミナー等に参加している
  - 同業他社と共同の勉強会

4.4 イベント情報や取組共有を目的とした国内政策調査

(2) アンケート調査

① サイバーセキュリティコミュニティ活動への参加経験

● 勉強会やコミュニティ活動に参加したことで得られた効果（n＝154、複数回答）

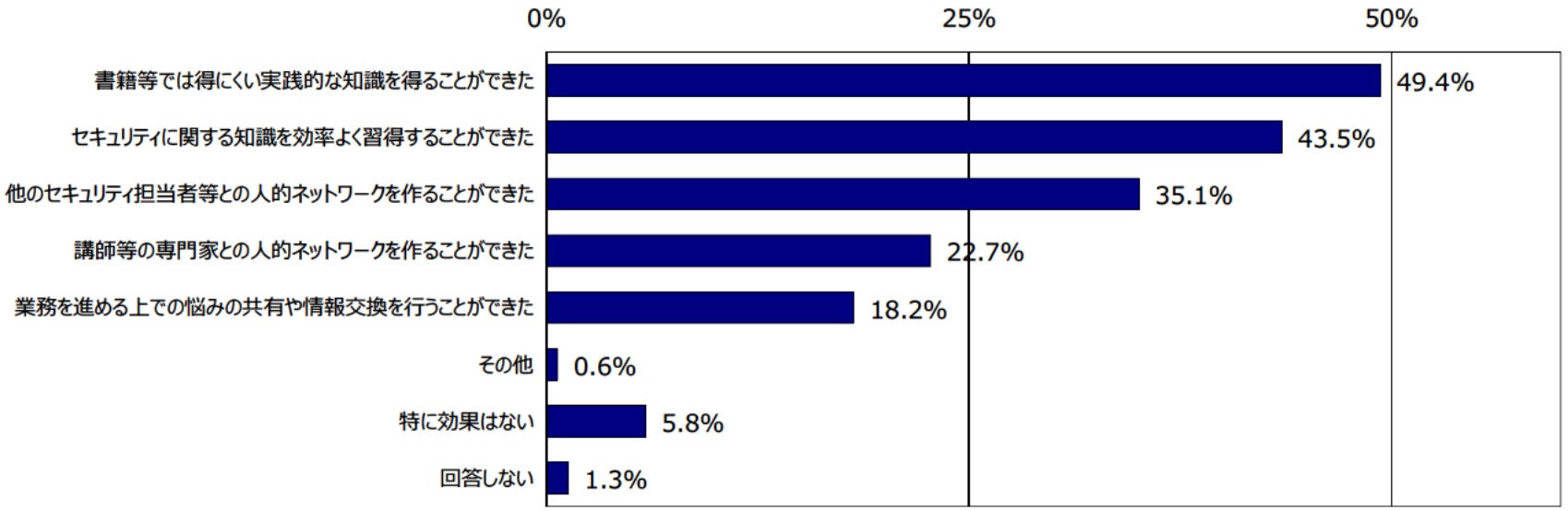


図4.4 勉強会やコミュニティ活動に参加したことで得られた効果

4.4 イベント情報や取組共有を目的とした国内政策調査

(2) アンケート調査

② サイバーセキュリティコミュニティ活動への参加意向

● サイバーセキュリティ分野の勉強会やコミュニティ活動に参加したことがない回答者の参加意向（n=257）

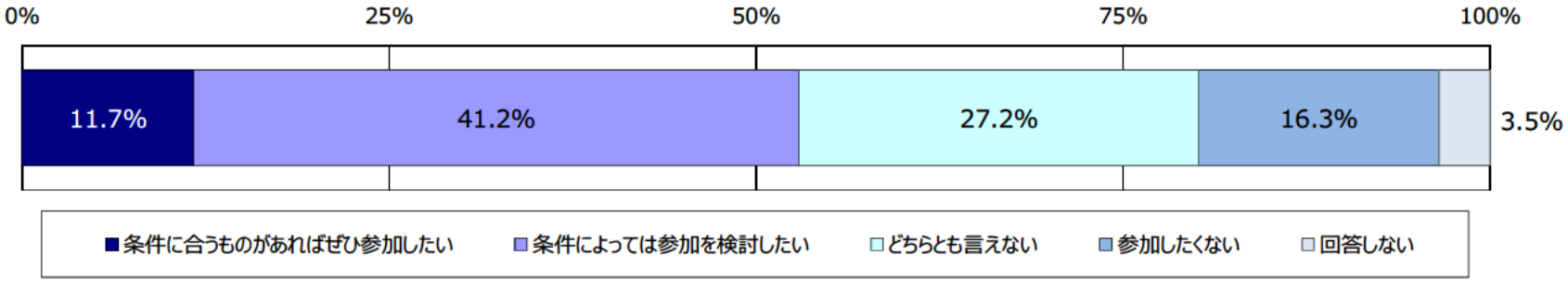


図4.5 サイバーセキュリティ分野の勉強会やコミュニティ活動に参加したことがない回答者の参加意向

● これまで勉強会やコミュニティ活動に参加しなかった理由（n=136、複数回答）

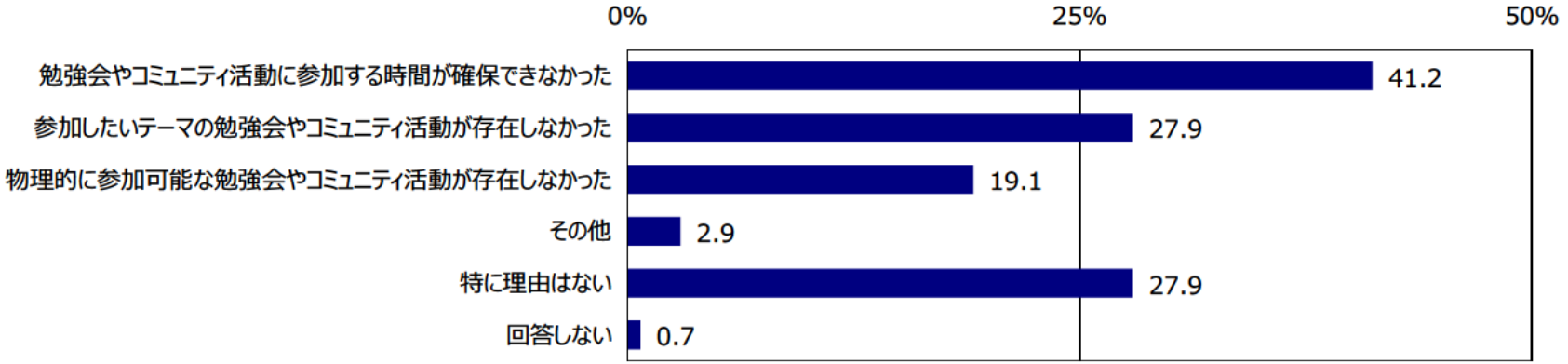


図4.6 勉強会やコミュニティ活動に参加しなかった理由

4.4 イベント情報や取組共有を目的とした国内政策調査

(2) アンケート調査

③ サイバーセキュリティコミュニティ活動の普及方策

● 今後、セキュリティ分野の勉強会やコミュニティ活動をさらに活性化させる上で必要と考えるもの（n=287、3つまで）

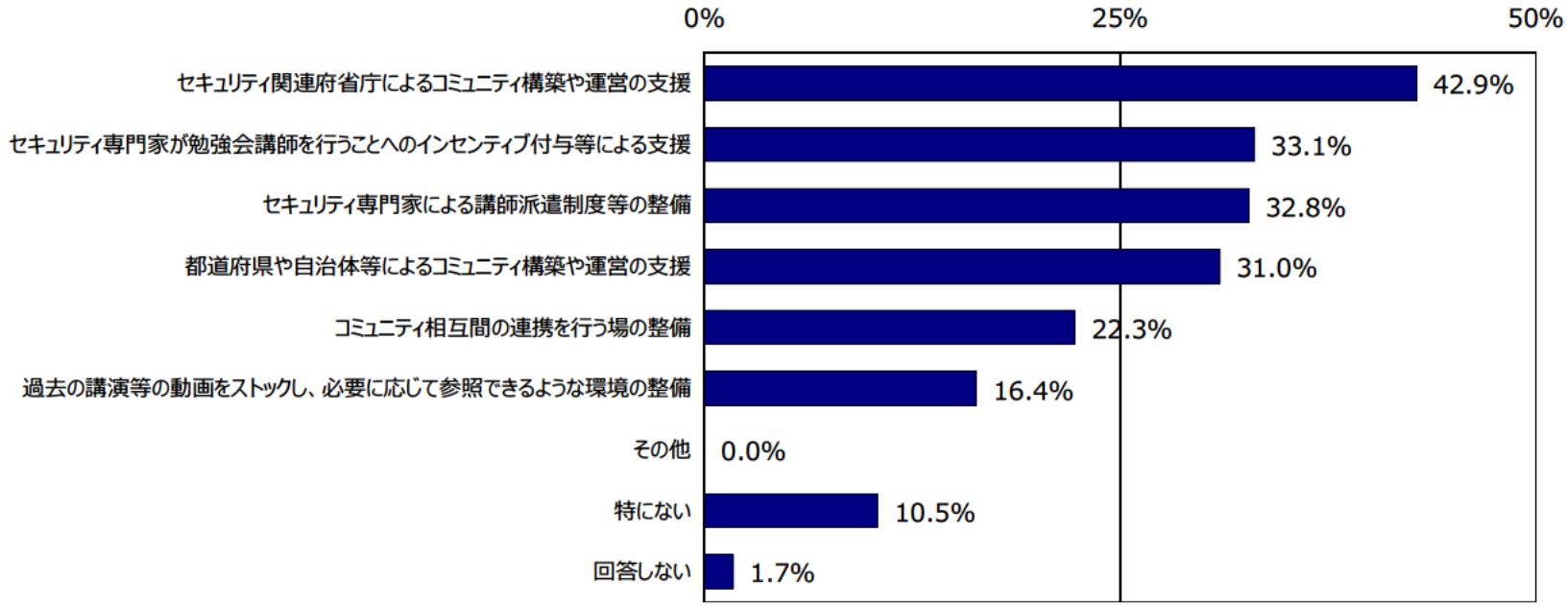


図4.7 今後、セキュリティ分野の勉強会やコミュニティ活動をさらに活性化させる上で必要と考えるもの

4.4 イベント情報や取組共有を目的とした国内政策調査

(2) アンケート調査

③ サイバーセキュリティコミュニティ活動の普及方策

● 今後、国内企業等におけるセキュリティ対策に関する普及啓発を進めるために、公的機関が実施すべきと考える取組
（n=411、3つまで）

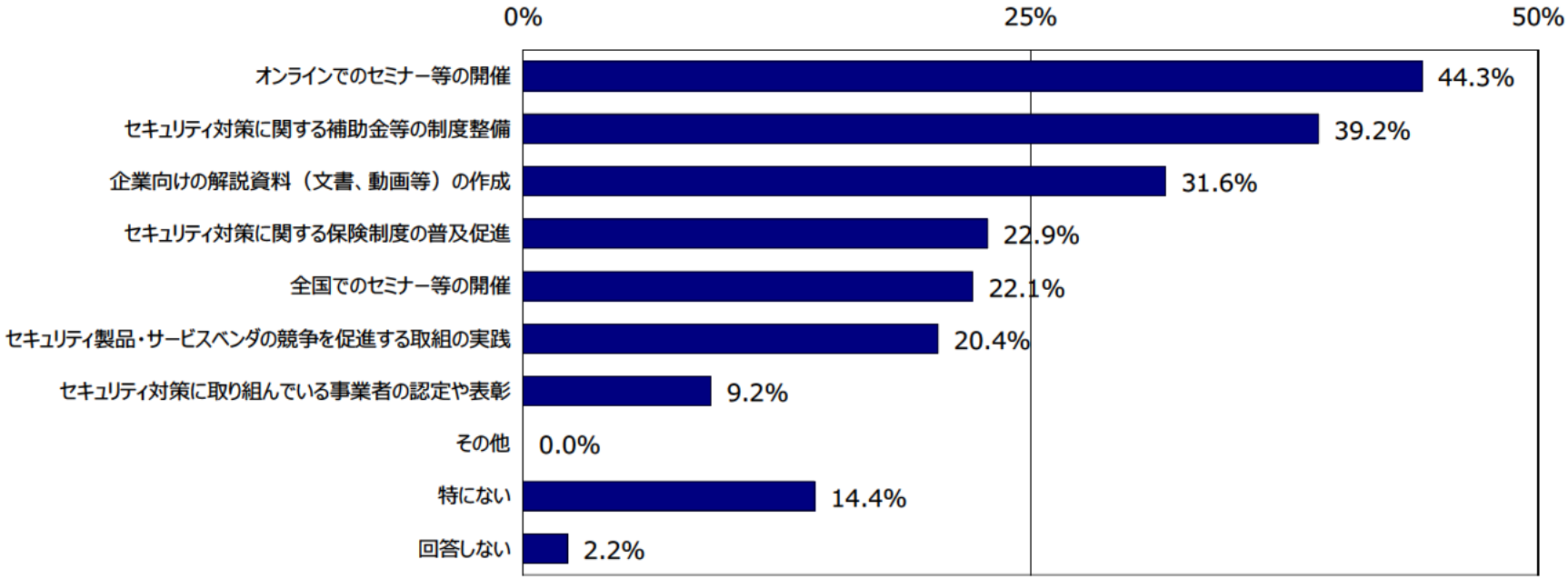


図4.8 今後、国内企業等におけるセキュリティ対策に関する普及啓発を進めるために、公的機関が実施すべきと考える取組

4.4 イベント情報や取組共有を目的とした国内政策調査

(3) ユーザにとって使いやすいツールとするための検討

- (1)(2)で行った調査結果をもとに、企業においてサイバーセキュリティ対策に従事する人材や組織が、サイバーセキュリティコミュニティの主催するイベントや取組に関する情報の提供・共有のためのツールについて、どのような方法を用いることで使いやすくなるのかについて、以下のような検討を実施した。
  - 企業において解決したい課題を切り口とした整理
  - 企業にとっての参加・相談のしやすさ（敷居の低さ）
  - 公的機関のウェブサイト等で紹介することによる、信頼感の醸成・提供

5. 情報セキュリティサービス活動・普及に関する調査

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(1) 対象企業の選定

- 調査趣旨を踏まえ、次表に示すユーザー企業等11件及びベンダー企業等18件の計29件についてヒアリング調査を実施した。
- なお、ユーザー企業ヒアリング調査を補足する意図から実施したアンケート調査について、その内容を(3)に示す。

(2) ヒアリング調査結果

① 本制度の認知度、登録検討状況

- アンケートでは大企業中心に一定の認知度があったが、ヒアリング対象としたユーザー企業では地域企業を中心に、今回のヒアリングで初めて知ったとの回答が多い。
- ベンダーの登録意向はそれぞれの事業方針に依存する。

表5.1 ヒアリング調査結果（本制度の認知度、登録検討状況）

ユーザー	● リストをこれまでも参照していた。（東名阪公的機関） ● 制度が開始したときに参照したことはあるが、調達手段としては利用していない。（東名阪企業） ● これまで調達の必要がなく認知していなかったが、今後は使おうと考えている。（東名阪自治体） ● 経済産業省が情報セキュリティサービスのリストを提供していることは今回初めて知った。情報セキュリティ監査企業台帳については、前任者が利用していた可能性はあるが把握していない。（非東名阪企業） ● 制度について知らなかった。（非東名阪企業）
ベンダー	● 監査企業台帳の廃止に備えて登録した。公的機関の入札要件となることが見込まれたため、社内で審査登録費用が問題になることはなかった。（非東名阪・登録ベンダー） ● 制度のことは認知しているが、自社として対応できるか疑問があり、登録していない。顧客から依頼があっても対応できないのであれば責任も発生する為、登録に躊躇する。（非東名阪・非登録ベンダー） ● 自社の技術者が限られており、余裕がない。セキュリティ人材の育成は自社のデータセンターの維持管理のために育成する方針であって、外販サービスを目的とした育成を想定していない。（非東名阪・非登録ベンダー）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

② 本制度の利用／登録に関するメリット

- 情報セキュリティ監査企業台帳の代替目的以外は、組織事情に応じて様々に示されている。

表5.2 ヒアリング調査結果（本制度の利用／登録に関するメリット）

ユーザー	● お墨付きの裏付け程度に活用している。（東名阪企業） ● 制度のコンセプトはよい。ただし、登録サービス数が増えてくると、どのように選定すればよいのかわからなくなる。（東名阪企業） ● ベンダーへの苦情申し立て制度があるのはよい。直接言いにくい場合も多い。（東名阪自治体） ● 情報セキュリティ監査台帳の代替として、リスト掲載を入札参加資格としている。情報セキュリティ監査と併せて脆弱性診断も行うため、両者とも要件は同じである。（非東名阪自治体） ● リストがあるだけでも効果はあると思う。（非東名阪自治体） ● これまではリストにある事業者名から検索していたので、概要とリンクが利用できるようになったのはありがたい。ただし実際の調達においては、自組織での実績の比重が大きくなる。（東名阪公的機関）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

② 本制度の利用／登録に関するメリット

- リストに掲載されることが認知度向上につながったとの回答が示される一方、効果を実感できないとする事業者も多い。

表5.3 ヒアリング調査結果（本制度の利用／登録に関するメリット）

ベンダー	● 顧客から登録の有無を尋ねる問合せはあるようである。（東名阪・登録ベンダー） ● 大手の取引先からリストに掲載されているかどうかの照会があり、大手企業には本制度が認知されているようである。（東名阪・登録ベンダー） ● 知名度の低い企業には、声掛けのチャンスになっているのではないか。（東名阪・登録ベンダー） ● 登録があることで、営業活動を行う際に顧客と話をしやすいと感じる。思いのほか制度が認知されている印象を受ける。（非東名阪・登録ベンダー） ● 登録をきっかけに「サイバーセキュリティお助け隊」の協力依頼が来た。（非東名阪・登録ベンダー） ● 登録の効果はないが、同業他社が登録している中で、自社がないのは体面としてよくない。（東名阪・登録ベンダー） ● 「リストに登録されているから、当社にした」という声を聞いたことがないため、効果の実感が得られていない。（非東名阪・登録ベンダー） ● 脆弱性診断サービスも、公的機関等の調達要件に取り入れられていくとよい。一方で、本制度以外の要件が厳しく、参加しにくい調達もある。（非東名阪・登録ベンダー） ● 費用対効果の観点からは、登録費用は高く感じられる。（東名阪・登録ベンダー）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

③ 本制度に関する改善要望

- 検索機能の充実と、サービスの技術・品質指標のさらなる可視化の要望がある。

表5.4 ヒアリング調査結果（本制度に関する改善要望）

ユーザー	● 情報が汎用的過ぎる印象。もう少し実装レベルに近い情報が欲しい。例えば、「SOCサービス」や「標的型メール訓練」といった粒度で探せないと一次情報源としては使えない。（東名阪企業） ● 事業者のウェブサイトへのリンクは有用であるが、事業者のトップページへのリングではわかりにくい。（東名阪企業） ● 近年の実績（民間〇件、公的機関〇件）といった主観が含まれない情報を掲載してもらえるとよい。（東名阪公的機関） ● サービスの登録申請時に情報を提供しているのであれば、在籍しているエンジニアの資格等の保有数を開示してもらえると良い。ただし人材の流動性があって正確性の維持が容易ではないのは理解している。（東名阪公的機関） ● IPAからISMAPのリストも公表されたが、調達にあたって参照すべきリソースが分散されていると使いにくい。集約等の工夫をしていただきたい。（東名阪自治体）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

③ 本制度に関する改善要望

- サービスのレベル分け、及び品質の低い事業者を載せない工夫に関する要望が多い。

表5.5 ヒアリング調査結果（本制度に関する改善要望）

ベンダー	● 脆弱性診断の項目として、「デバイス」を対象とする区分があるとよい。これまでは「プラットフォーム」の一部として実施していた。ただし、顧客からの引き合いの際は、「IoT」というキーワードで来ることが多く、顧客から見て分かりやすいジャンルで区分できるとよい。（東名阪・登録ベンダー） ● 苦情申し立ての制度は形としてはよい。（東名阪・登録ベンダー） ● このまま登録事業者が増えていくと、サービスレベルの低い事業者も登録される可能性が高い。今でも「あれ？」と感じるような事業者も掲載されている。ただし、どうすれば改善できるかの答えは持ち合わせていない。（東名阪・登録ベンダー） ● 質の高い登録ベンダーを「お奨めサービス」として、目利きのできる人が紹介する仕組みを設けてはどうか。そうしないと登録メリットが見えてこない。もっとも、監視サービスは実態が表に出てこないので難しいかもしれない。（東名阪・登録ベンダー） ● 資格要件として、セミナーを受講すればよい、というのは緩い印象。（東名阪・登録ベンダー） ● 資格要件として、講師経験も加えて欲しい。（非東名阪・登録ベンダー） ● 審査・登録に要する費用感は妥当である。（非東名阪・登録ベンダー） ● ベンダーの技術レベルの可視化（ランク付け）があるとよい（非東名阪・登録ベンダー） ● 脆弱性診断とペネトレ、機器の監視とグローバル環境の監視など、レベル感の異なるサービスを区別できるとよい。（東名阪・登録ベンダー） ● 登録の効果測定として、リストの公表サイトへのアクセス数が知りたい。（東名阪・登録ベンダー） ● リストの内容の更新頻度を高めることができないか。リストと実態との乖離は利用者に不利益をもたらす。（東名阪・登録ベンダー） ● 英国のActive Cyber Defenceプログラムは規模感も似ており、参考にしてはどうか。（東名阪・登録ベンダー）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

③ 本制度に関する改善要望

- 制度運用について、具体的な改善要望が示されている。

表5.6 ヒアリング調査結果（本制度に関する改善要望：審査登録機関による運用について）

ベンダー	● 技術要件における資格保有・コミュニティ活動・研修等の実績がAND条件と誤解している事業者がいる。もっとわかりやすく伝える工夫が必要ではないか。（東名阪・非登録ベンダー） ● 品質管理要件を充足するための「教育又は研修」の証跡として、OJTについても「研修メニューや目次等の提出」を要求される。OJTにメニューや目次はないのが普通であり、代替としてどのような証跡を出せばよいのかを明確化してほしい。（東名阪・非登録ベンダー） ● 登録時の「アンケート」はWebフォームの形態のため申請のタイミングでしか入力できないが、内容に即答できないものが（＝組織としての判断が必要なもの）多い。また、監査サービス前提の内容になっており、他サービスで回答しにくいものがある。「審査の流れ」の説明ページにおいて、アンケート項目について予め参照できるようにしてほしい。（東名阪・非登録ベンダー） ● 登録システムで用いるメールアドレスは、メーリングリスト（同報）アドレスは不可、個人アドレス限定となっているが、担当者の異動・退職等による連絡不能のリスクがあり、個人アドレス以外での登録も許容してほしい。（東名阪・非登録ベンダー）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

④ セキュリティサービスの調達・利用に関する実態

- サービス品質の対象は提案力、実績、費用対効果等様々である。
- ベンダーへの問合せを避け、他の情報源を活用している実態が示されている

表5.7 ヒアリング調査結果（セキュリティサービスの調達・利用に関する実態）

ユーザー	**＜セキュリティサービスを外部委託する際にサービス品質として考慮する事項＞** ● セキュリティサービスのみ特別扱いすることはない。ただし、初めて委託する事業者の場合はSLA等の要求事項を満足してもらうことに関する合意を交わすようにしている。（東名阪企業） ● ベンダーの提案力を重視している。（東名阪企業） ● サービスの費用対効果を考慮している。（非東名阪企業） ● 実績も参考にしている。（非東名阪企業） **＜自治体情報セキュリティクラウドについて＞** ● 都道府県が契約しているクラウドサービスにセキュリティ監視・運用や脆弱性診断サービスに相当する機能が包含されているため、個別のセキュリティ調達を行っていない。（東名阪自治体、非東名阪自治体） **＜セキュリティサービスの調達の際に参考にしている情報＞** ● IPAやJPCERT/CCの情報は参考にしている。ベンダーへの問合せは自社推しが激しいので避けている。（東名阪企業） ● JUASの事例調査を現場の生の声として活用している。（東名阪企業） ● ベンダーに過去の実績を尋ねて参考にしている。（東名阪企業） ● 中小企業向けのガイドブック等はわかりやすい。（東名阪企業） ● 金融ISAC、および地元の金融機関や企業と毎月１回開催しているセキュリティ情報の共有会。こうした場で他社がどのようなサービスや製品を使っているかについての情報を得ている。（非東名阪企業） ● たまに開催されるイベントに参加し、「こんなセキュリティサービスを提供している事業者がある」といった情報を入手している。（非東名阪企業）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

⑤ 情報セキュリティサービス提供の実態

- 情報セキュリティサービスへの需要は高まる傾向にあることが認められる。

表5.8 ヒアリング調査結果（情報セキュリティサービス提供の実態）

ベンダー	＜サービスへの需要動向について＞ ● 引き合いは増えている。ネットワークに接続される機器が増えたことで、ハードウェアデバイスを対象とするセキュリティ診断の需要が増えている。（東名阪・登録ベンダー） ● 監督官庁からの指導がある業界はサービスを委託するニーズが明確であるが、それ以外の業界ではニーズがなく、費用をかけられないという顧客が多い。（非東名阪・登録ベンダー） ● 脆弱性診断サービスの場合、しっかり診断して欲しい場合と、形だけやって欲しい場合の両極端の印象。結局は予算に依存するので、ゲートウェイ部分のみ細かく診断し、それ以外は簡単に行うようなことはある。（非東名阪・登録ベンダー） ● Emotetが流行っていることもあり、中小企業のニーズが少しずつ高まってきている。（非東名阪・登録ベンダー） ● セキュリティ意識の高低は業種よりも個々の企業毎の差である。デジタル化を進めている会社だからといって、準大手以下はセキュリティ意識が高い訳ではない。（非東名阪・登録ベンダー） ● 低価格の脆弱性診断を提供していると、中小企業の中にも理解のある企業があることがわかる。デジタルフォレンジックについては、大手以外の理解が追いついていない。（非東名阪・登録ベンダー）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

⑤ 情報セキュリティサービス提供の実態

- セキュリティサービスを他サービスとのセットで提供する形態が増える傾向にある。

表5.9 ヒアリング調査結果（情報セキュリティサービス提供の実態：特徴のあるサービス）

ベンダー	**＜制御系/OTを対象とするサービスの動向＞** ● IoT特化型としてデバイスセキュリティ診断サービスを提供している。ただし、IoTシステム全体として、プラットフォームやスマートフォンとセットで診断することもある。（東名阪・登録ベンダー） ● 制御系の顧客は以前から事業系インフラの関連でつながりがあったところであり、本制度を意識していない。（非東名阪・登録ベンダー） **＜セキュリティサービスを包含したクラウドサービスの提供＞** ● 自治体セキュリティクラウドに限らず、クラウドサービスにセキュリティサービスが付随した契約は増えている。ただしそうすればセキュリティサービスの契約が不要になるかといえばそうではない。また、セキュリティサービスの委託をすれば責任をベンダーが取ってもらえると考えるユーザーもいて困る。（東名阪・登録ベンダー）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

⑥ サービス利用で困った経験

- ユーザーにおける課題は偏らず、事情に応じて様々な問題が指摘されている。

表5.10 ヒアリング調査結果（サービス利用で困った経験）

ユーザー	● ツールによる診断がどこまでカバーしているかがわからない。（東名阪企業） ● 無償の診断サービスの提案を受けたが、診断結果の解決策がベンダー製品の導入であった。（東名阪企業） ● 自社の予算やリソースを超えた提案をもらっても対応できない。（東名阪企業） ● 県外事業者に委託すると日程調整で苦労する。（非東名阪自治体） ● 今のところ特にない。ただし、ペネトレーションテストとしてどのようなことを行うのかについては、費用が高いこともあって事前に十分な相談が必要になると思う。（非東名阪企業） ● 脆弱性診断の費用感がわかりにくい。画面数といわれてもどのようにカウントすれば良いのかわからない。（非東名阪自治体）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

⑦ サービス提供で苦労した経験

- ベンダーにとっては、ユーザーにおける認識の低さが最大の課題となっている。

表5.11 ヒアリング調査結果（サービス提供で苦労した経験）

ベンダー	● API監視サービス等、ユニークなサービスを提供しているが、ユーザー企業にその価値が伝わらない。（東名阪・登録ベンダー） ● 中小企業の場合、担当者がやろうと思っても稟議を上げると却下されるケースがあるようである。経営層の意識を変える必要がある。（非東名阪・登録ベンダー） ● 地元ユーザー企業が支出可能な予算の規模感が「桁違い」である（数万円なら、というレベル）。（非東名阪、非登録ベンダー） ● ユーザー企業のサービスに関する理解度が低い。ファイアウォールを入れれば完璧というレベルであり、顧客が実施すべき事項を理解してもらうことが課題である。（非東名阪、非登録ベンダー） ● セキュリティの専門人材が限られるため、自社の体力的な面もあって事業拡大に踏み出すことが難しい。（非東名阪・非登録ベンダー）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

⑧ 普及に向けた啓発活動への期待

- ユーザーの意見は立場に応じて様々なものが挙げられている。

表5.12 ヒアリング調査結果（普及に向けた啓発活動への期待：ユーザー）

ユーザー	● 最後はユーザーの認識が重要なので、ユーザー教育の重要性に関するアナウンスをお願いしたい。（東名阪企業） ● クラウドのチェック項目を策定し、クラウド事業者がその状況を公開すれば、ベンダー・ユーザーとも効率化がなされるのではないか。（東名阪企業） ● 大規模組織で脆弱性診断を行おうとすると、対象となる情報システムの管理体制も異なるので、調整に大きな負担がかかる。診断結果の展開もこちらで行うと負担が大きい。本制度の問題ではないが、ベンダーで複数窓口に対応できるような体制を提供してもらえるとありがたい。（東名阪自治体）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(2) ヒアリング調査結果

⑧ 普及に向けた啓発活動への期待

- ベンダーからはさらなる認知度向上とマッチングの場の提供に関する期待が示されている。

表5.13 ヒアリング調査結果（普及に向けた啓発活動への期待：ベンダー）

ベンダー	● プロモーションをさらに推進すべき。営業活動を後押ししてほしいというのが、ベンダー共通の思いではないか。マーケティングの観点からできることを見ていく必要がある。（東名阪・非登録ベンダー） ● 多くのセキュリティベンダーは地域SIerとの繋がりがない。普及に向けた取組として、マッチングの機会を提供してはどうか。地域のSIerを100～200社集めて商談会のようなものを設定し、そこでセキュリティベンダーが実際にこんなサービスをこの価格で提供できるというプレゼンを行う。気になったところは名刺交換をする、といった機会ができると有意義と思う。（東名阪・非登録ベンダー） ● ユーザー企業において、セキュリティ診断や監視は継続的に実施しないと意味が無い、また自社の責任で実施すべきことがあるという認識が不足している。認識のギャップを埋めることに時間を要しており、そうしたリテラシーの向上が必要である。（非東名阪・非登録ベンダー） ● 「こうした対策をしていないと、こんなリスクがある」というわかりやすい説明が必要。ガイドラインで強制したところで、あまり変わらないかもしれない。（非東名阪・非登録ベンダー） ● どのような取組をしていて、それが全体像の中でどの部分に居続けられるのかをわかりやすく説明して欲しい。（非東名阪・非登録ベンダー） ● 補助金が利用できるというよりも、税金が下がる、各社のセキュリティ投資状況が公表されるなど、実際にセキュリティ対策を実施せざるを得なくなるような制度になるとよい。（非東名阪・登録ベンダー） ● 医療系機関を対象とするセキュリティサービス利用のプロモーションを、厚労省の協力を得て実施すべきではないか。（非東名阪・登録ベンダー）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

- 情報セキュリティサービス審査登録制度の改善を効果的に実現するためには、情報セキュリティサービスを利用する企業における認知や活用に関する実態を可能な限り正確に把握することが重要と考えられることから、より多くのサンプルを調査可能なアンケート調査を併用して実施した。アンケート調査の実施概要は次表の通りである。なお、アンケート対象者は表4.2に示すアンケート調査の回答者と同一である。

表5.14 アンケート調査実施概要

対象	全国のユーザー企業でサイバーセキュリティ対策関連業務に従事するアンケート回答モニター 411名 （企業に勤務するモニター50,000名を対象とするスクリーニング調査をもとに抽出）
実施時期	2020年11月26日～27日
質問事項	●勤務先企業におけるIT利活用とセキュリティサービス利用状況 ●情報セキュリティサービス審査登録制度の認知と活用状況 ●登録サービスの利用経験 ●情報セキュリティサービス利用の課題と要望

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

① 情報セキュリティサービスの利用状況

● 情報セキュリティ監査サービス

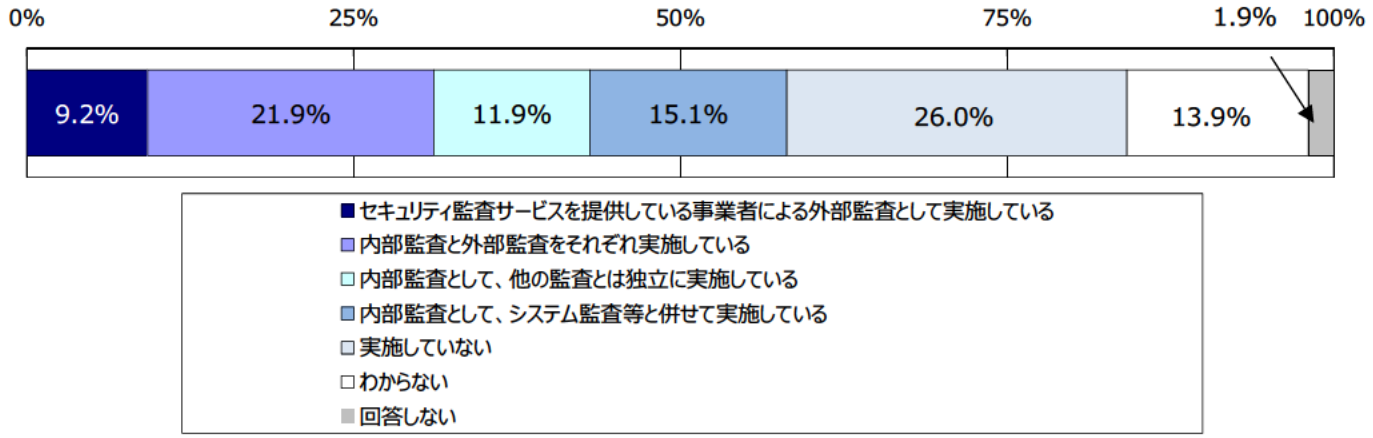


図5.1 情報セキュリティ監査サービスの利用状況

● 脆弱性診断、デジタルフォレンジック、セキュリティ監視・運用サービス

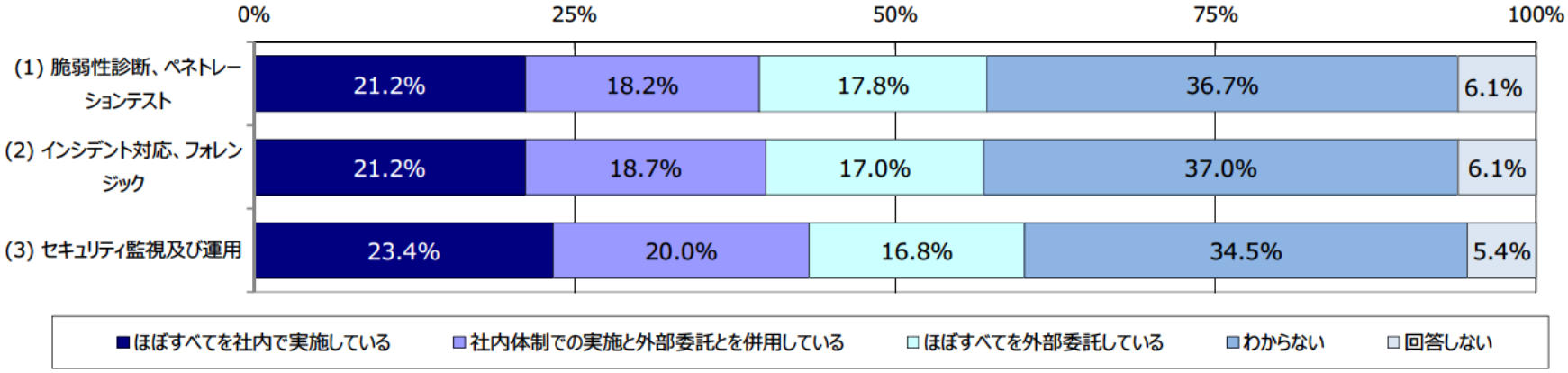


図5.2 脆弱性診断、デジタルフォレンジック、セキュリティ監視・運用サービスの利用状況

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

② 情報セキュリティサービス審査登録制度の認知状況

● 全体（n=411）

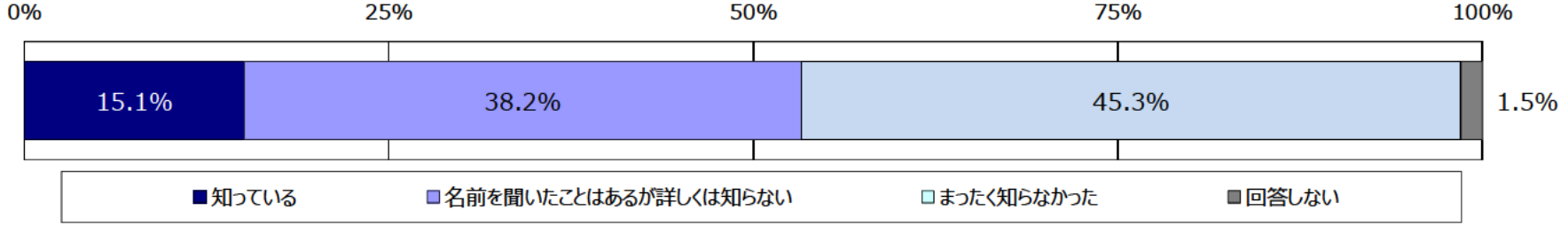


図5.3 情報セキュリティサービス審査登録制度の認知度（全体）

● 企業規模別クロス集計結果

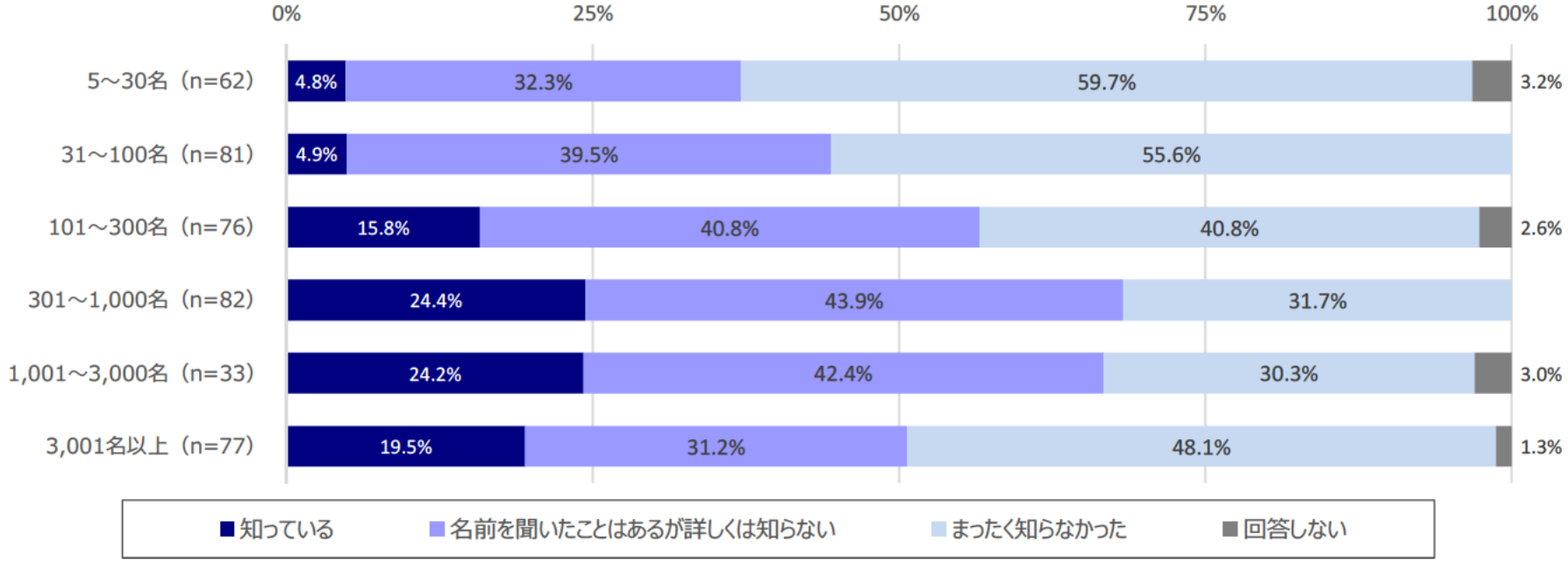


図5.4 情報セキュリティサービス審査登録制度の認知度（企業規模別クロス集計）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

② 情報セキュリティサービス審査登録制度の認知状況

● 業種別クロス集計結果

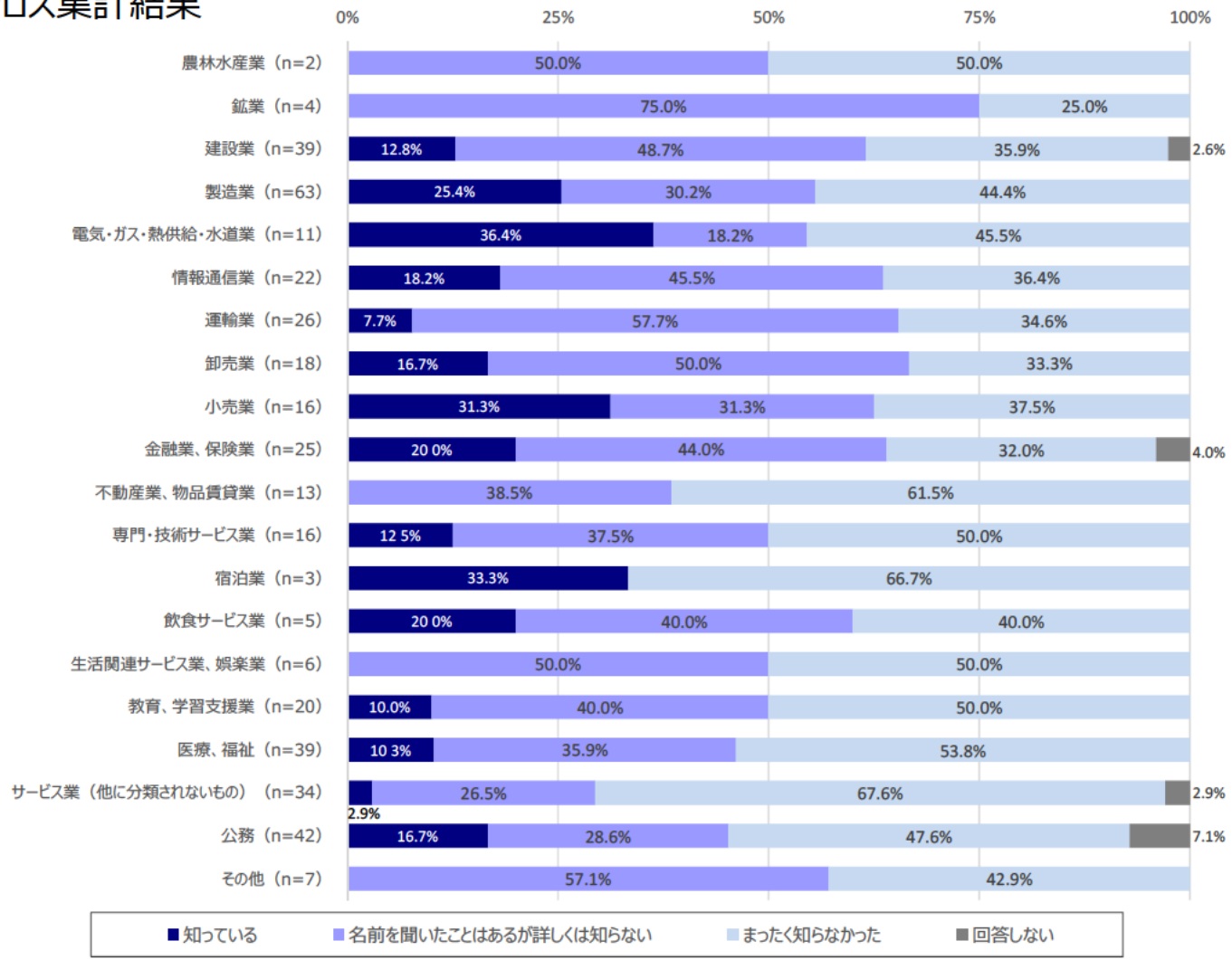


図5.5 情報セキュリティサービス審査登録制度の認知度（業種別クロス集計）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

③ 情報セキュリティサービス審査登録制度の利用状況

- 全体（n=62、回答者は②で制度を「知っている」と回答した者）

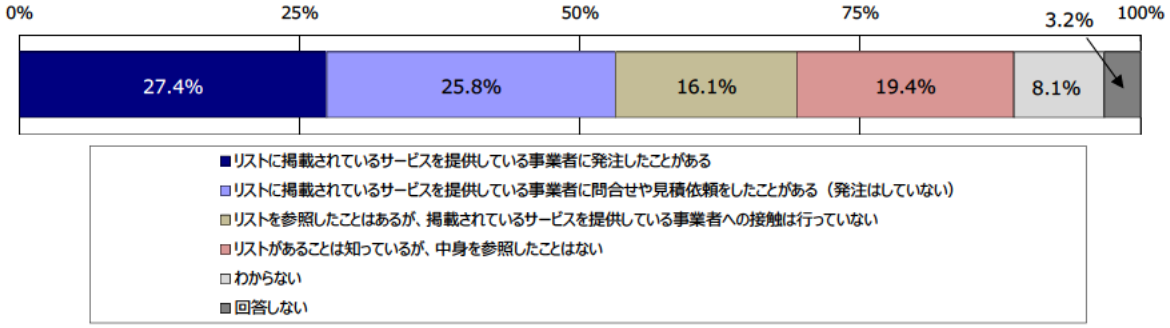


図5.6 情報セキュリティサービス審査登録制度の利用状況（全体）

- 企業規模別クロス集計結果

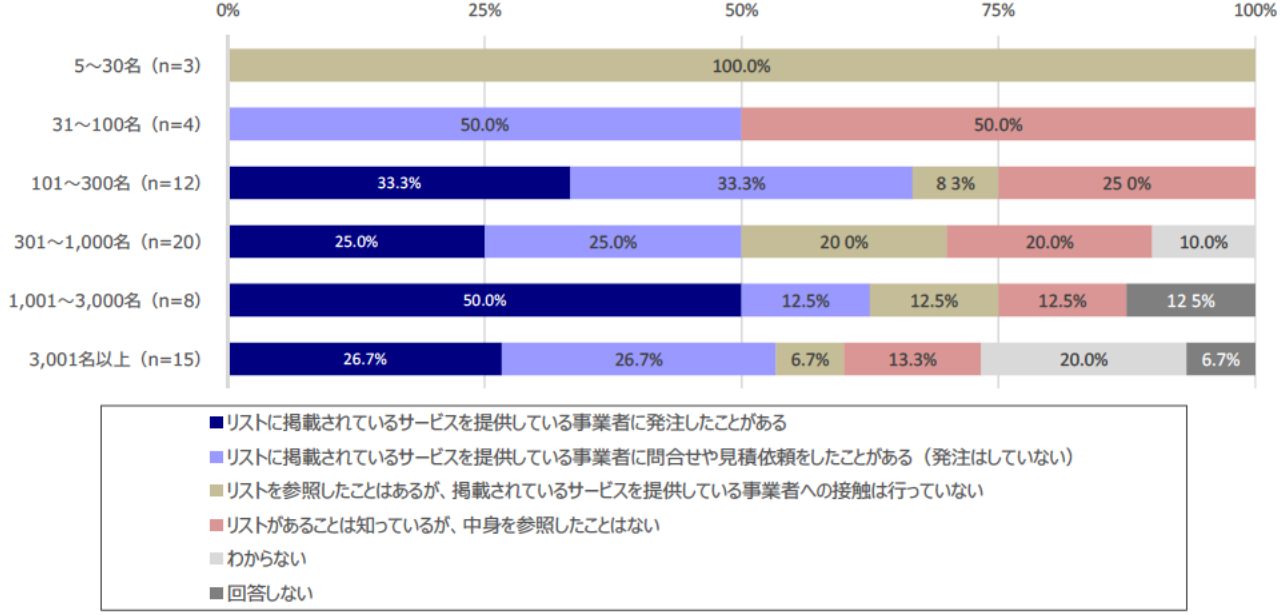


図5.7 情報セキュリティサービス審査登録制度の利用状況（企業規模別クロス集計）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

② 情報セキュリティサービス審査登録制度の利用状況

● 業種別クロス集計結果（回答者が存在しない業種は非表示）

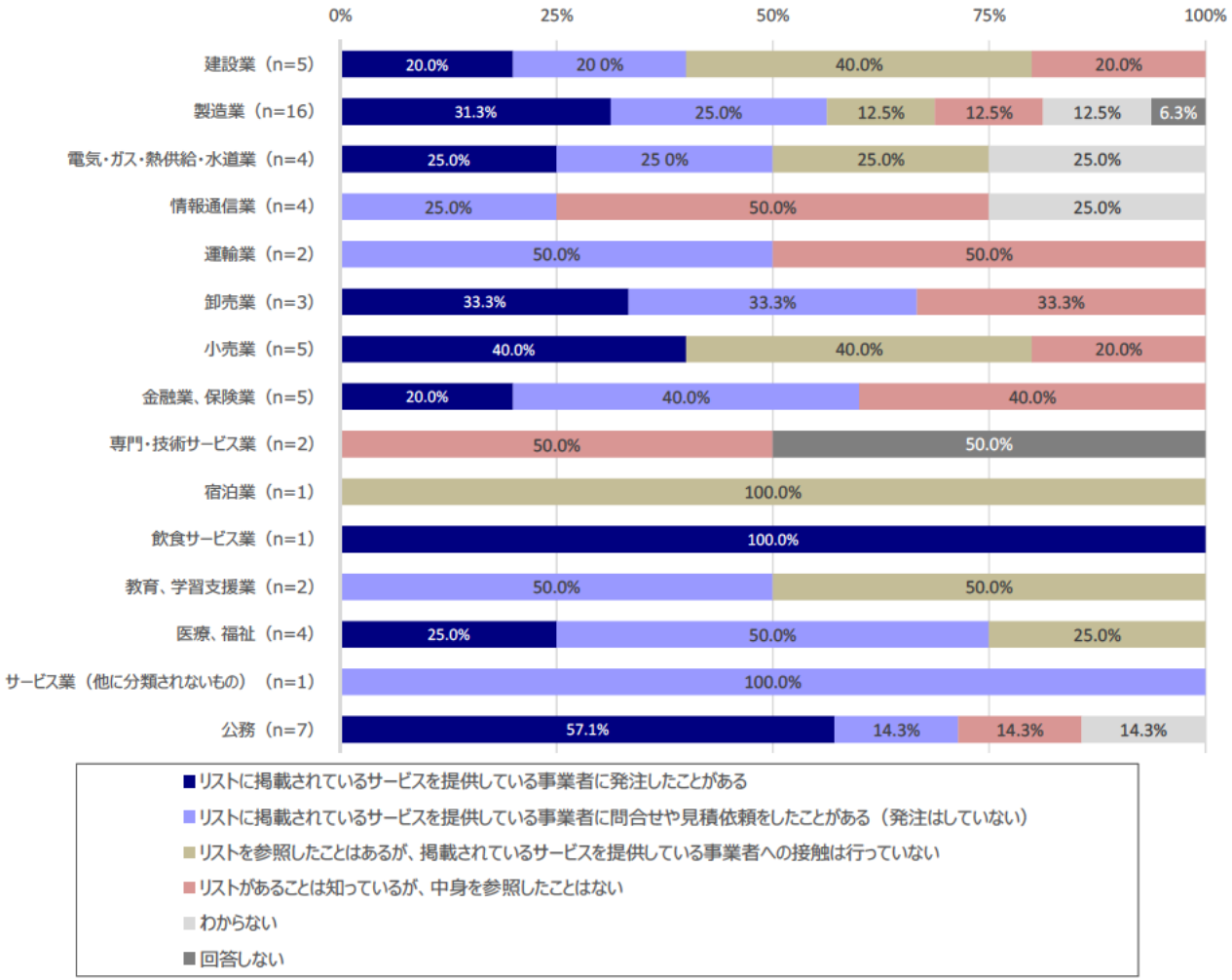


図5.8 情報セキュリティサービス審査登録制度の利用状況（業種別クロス集計）

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

④ 情報セキュリティサービス基準適合サービスリストの利用理由と登録サービスの利用結果

● 情報セキュリティサービス基準適合サービスリストの利用理由（n＝17、複数回答）

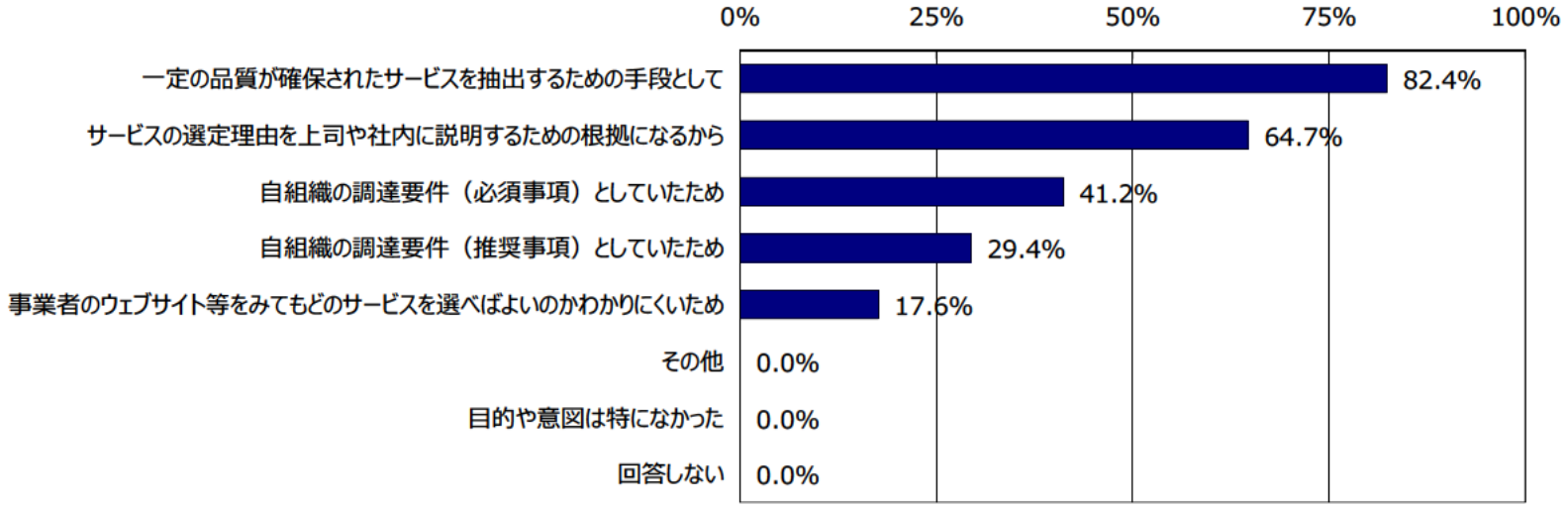


図5.9 情報セキュリティサービス基準適合サービスリストの利用の理由

● 登録サービスを利用した結果（n＝17、サービス品質についての評価）

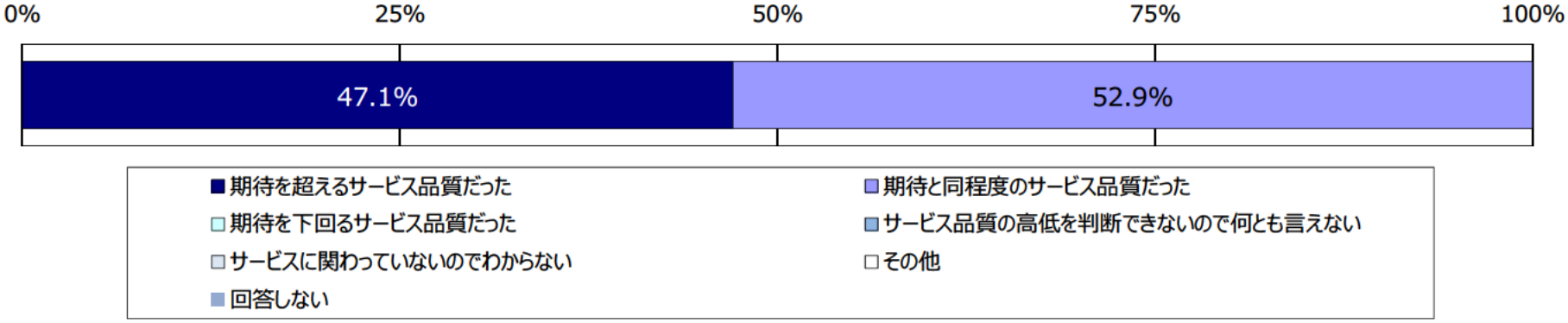


図5.10 登録サービスを利用した結果

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

⑤ 情報セキュリティサービス基準適合サービスリスト登録サービスを利用しなかった理由

● 事業者にコンタクトしたが、発注に至らなかった理由（n＝16、複数回答）

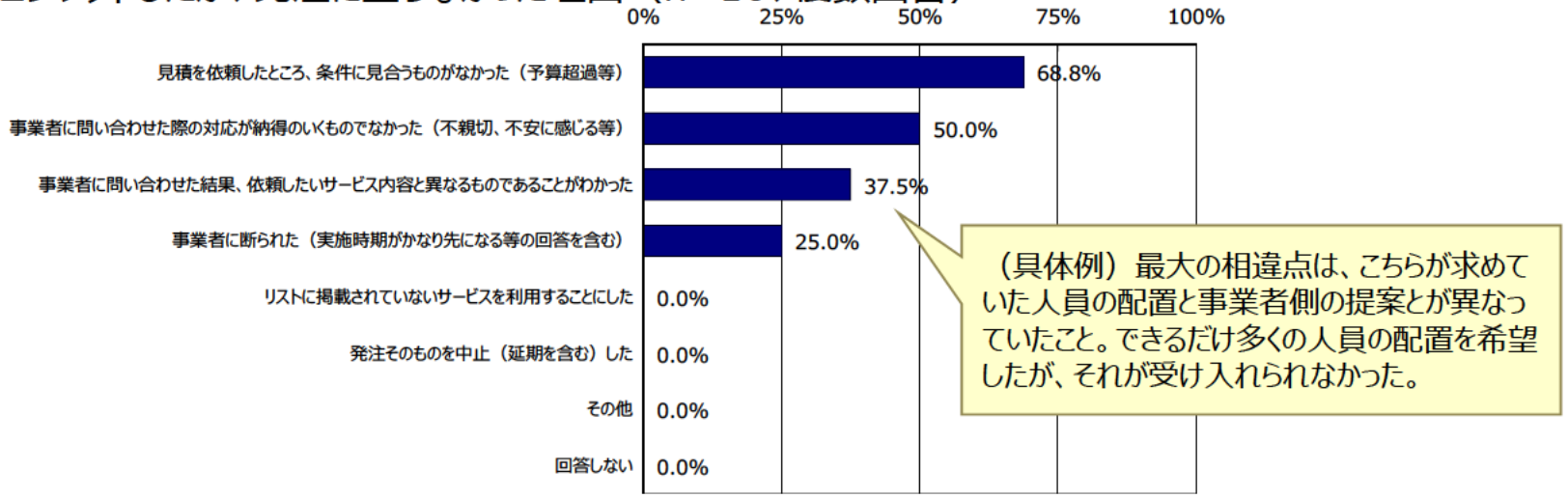


図5.11 事業者にコンタクトしたが、発注に至らなかった理由

● リストを参照したが、事業者にコンタクトしなかった理由（n＝10、複数回答）

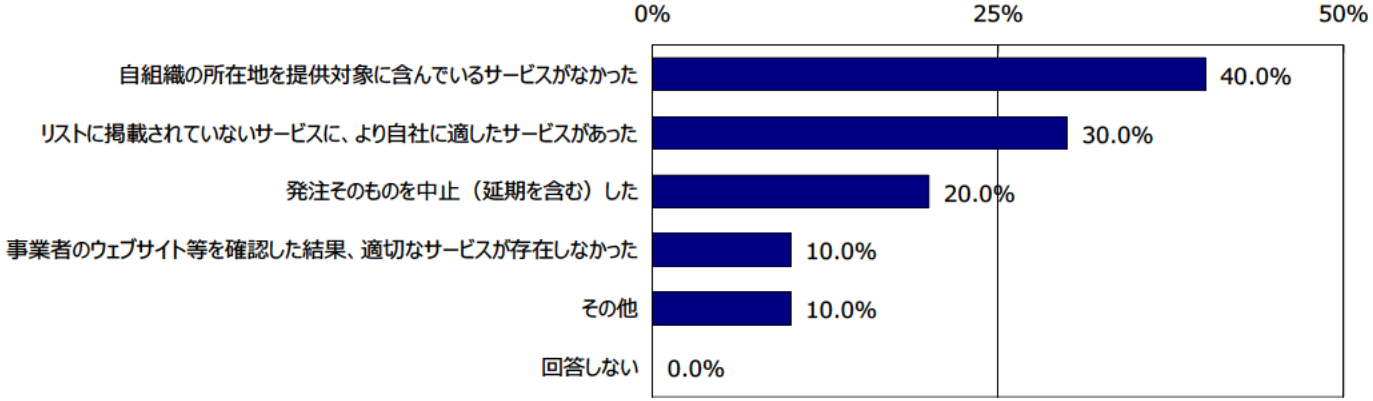


図5.12 リストを参照したが、事業者にコンタクトしなかった理由

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

⑥ 情報セキュリティサービスの需要動向

● 現在懸念していること（n=411、複数回答）

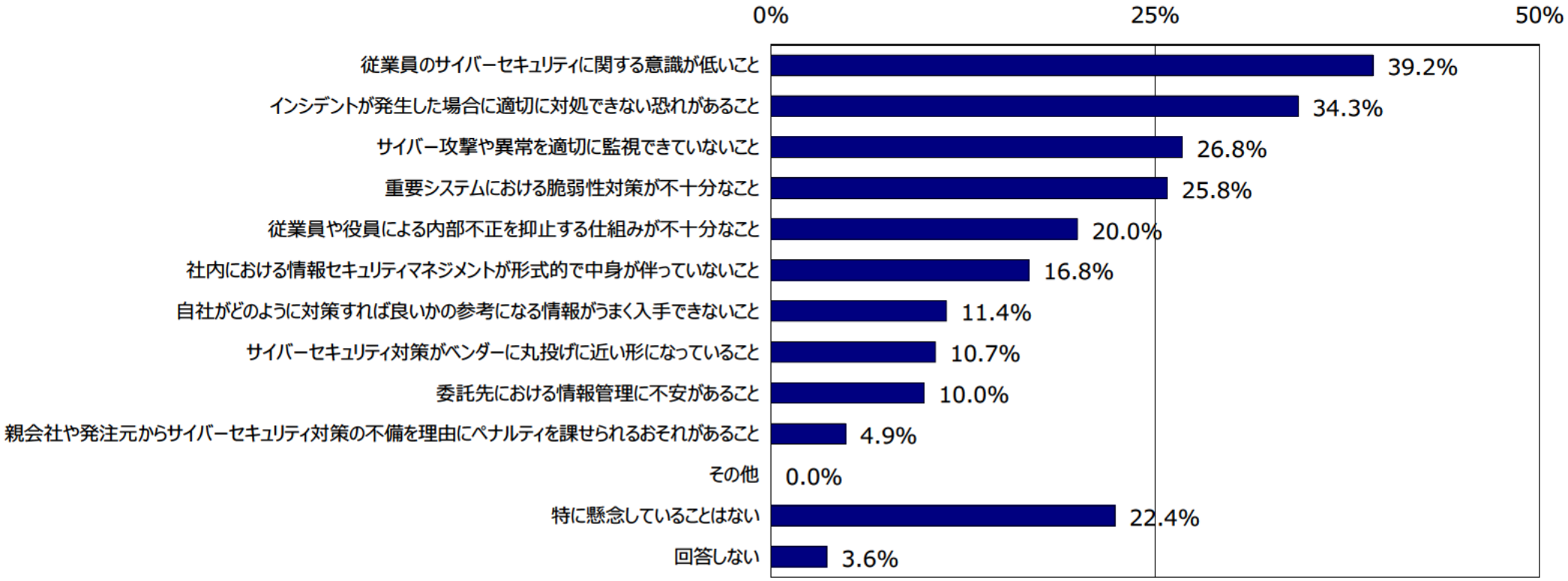


図5.13 情報セキュリティサービスの需要動向

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

⑥ 情報セキュリティサービスの需要動向

● 今後強化したい対策（n=411、複数回答）

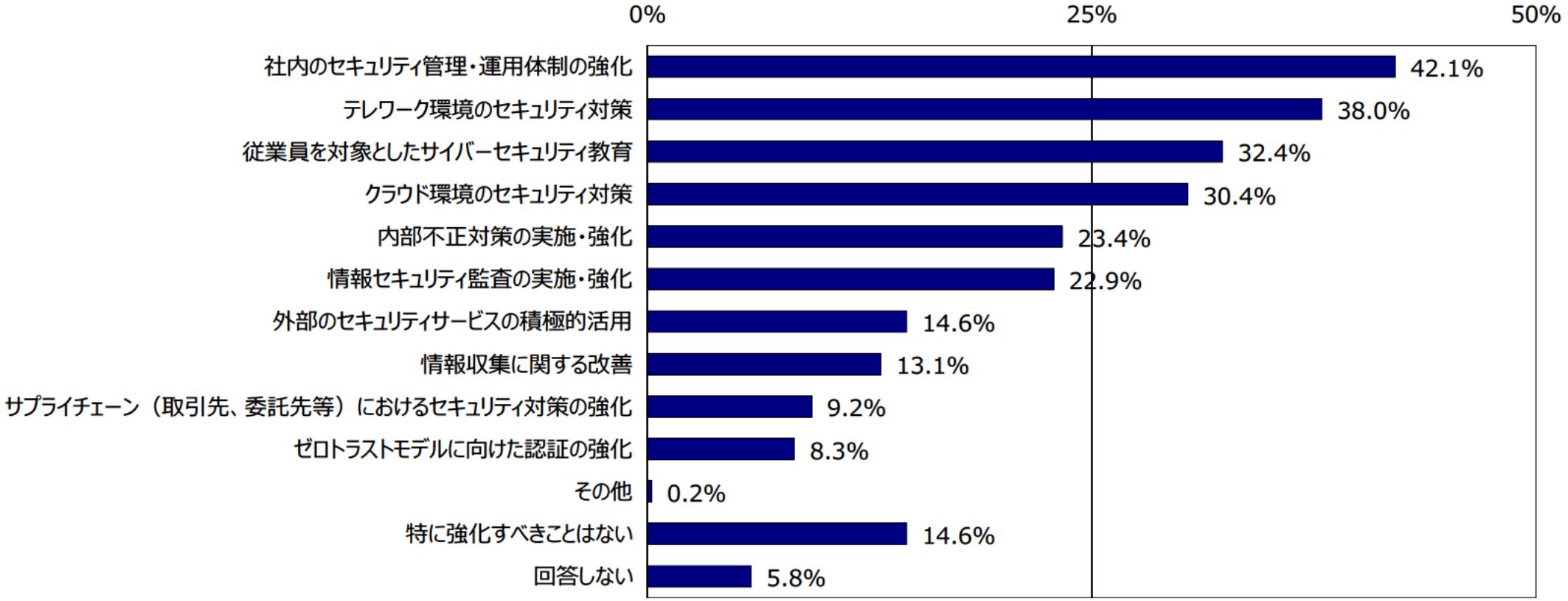


図5.14 今後強化したい対策

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

⑦ 制度への改善要望

● 自社でリストを活用しようとするときの課題（n=62、複数回答）

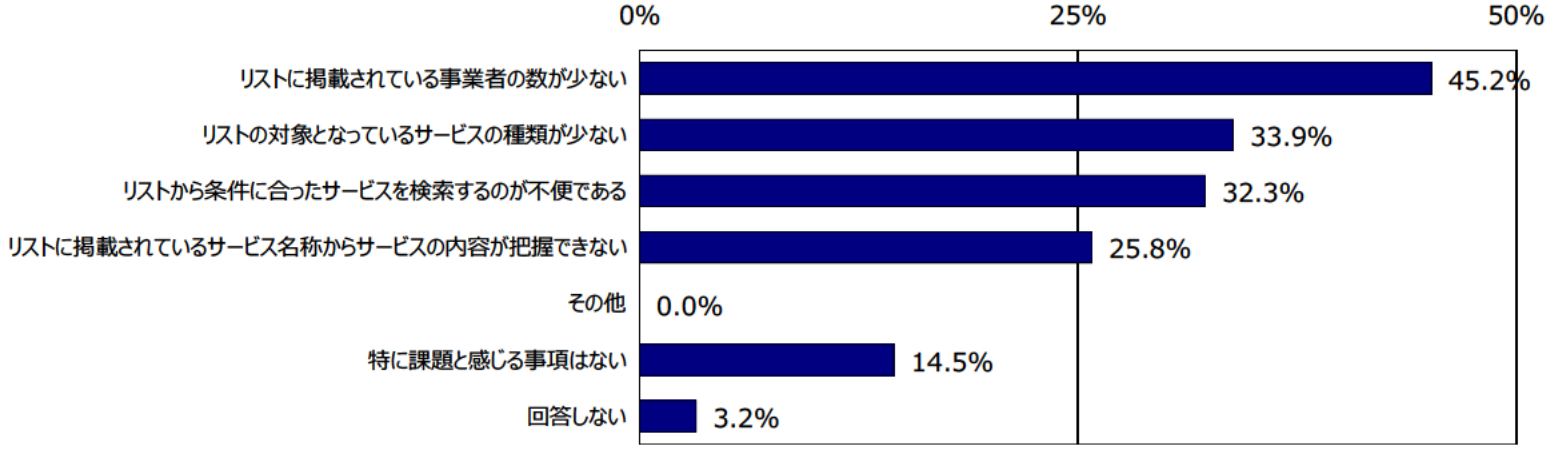


図5.15 自社でリストを活用しようとするときの課題

● 今後期待したい要望（n=62、複数回答）

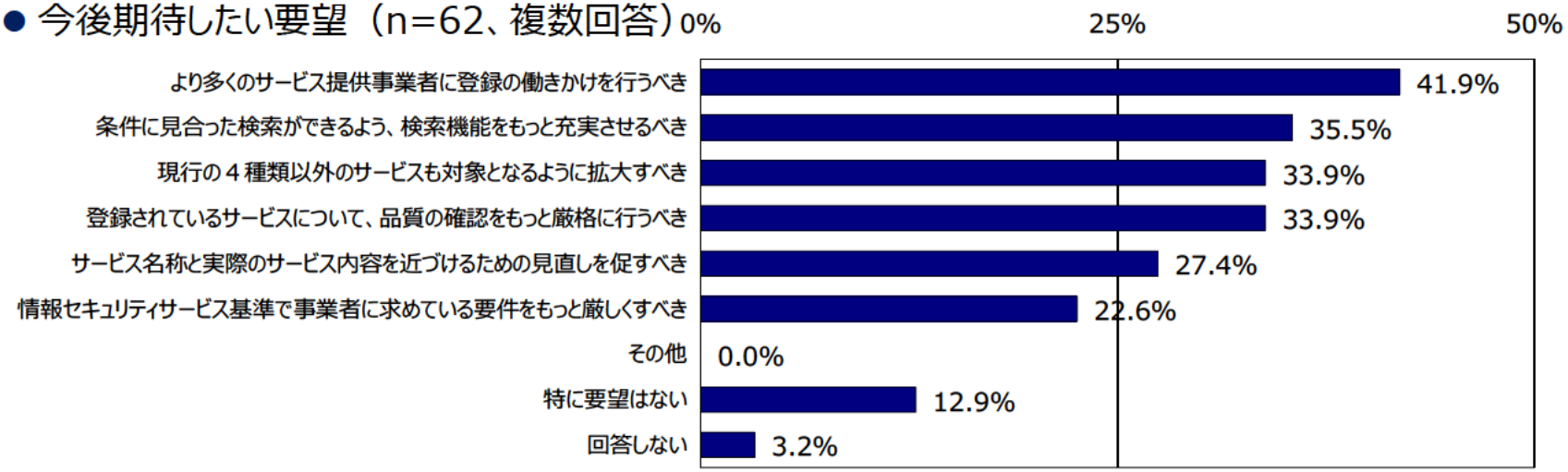


図5.16 今後期待したい要望

5.1 情報セキュリティサービス活用・普及に関する企業調査の実施

(3) ユーザー企業アンケート調査の実施

⑧ アンケート結果の総括

- アンケート調査の結果、次の傾向が確認された。
  - 回答企業のうち、30～35%の企業がセキュリティサービスの外部委託を実施。
  - 本制度は回答企業の半数で認知されており、他調査と比較して改善傾向。従業員数300～3,000名程度の企業では7割程度の認知度。
  - 制度を認知している回答者のうち、登録されているサービスを利用したことがある企業は27%程度。ただし中堅～大企業に限られる。
  - 登録サービスの利用企業において、サービス品質に関して「期待以下」と回答している企業は皆無であり、「最低限の品質を担保」という制度の目的は達成されている。
  - リストを参照したものの、サービスを利用しなかった理由としては、条件の不適合を挙げる回答者が多い。
  - 企業におけるセキュリティ管理・運用体制の強化を行いたいとの意見が強く示されており、ニーズは存在する。
  - 制度への要望のうち最多は「掲載事業者を増やす」ことである。

5.2 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。
  - 企業調査を踏まえた、情報セキュリティサービス基準の改定
  - 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の検討

(2) 有識者会議の開催状況

- 以下の計3回の検討を実施した。

表5.15 「情報セキュリティサービス普及促進に関する検討会」2020年度開催状況

会議	開催日	おもな議題
第1回	2020年8月5日	● 情報セキュリティサービス基準の改定に関する論点について ● 情報セキュリティサービス審査登録制度の普及方策に関する論点について ● ヒアリング及びアンケート調査で明らかにすべき事項について
第2回	2020年12月15日	● ヒアリング及びアンケート調査の結果報告 ● 情報セキュリティサービス基準適合サービスリストの改良方法について ● 情報セキュリティサービス基準の見直し方針について
第3回	2021年3月19日	● 情報セキュリティサービス基準適合サービスリストの改良に関する報告 ● ヒアリング及びアンケート調査結果の追加報告 ● 情報セキュリティサービス基準の見直し方針について

6. まとめ

- 本調査では、本報告書2.～5.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。
  - 企業及びステークホルダーを対象とする調査基づく「サイバーセキュリティ経営の可視化ツールVer.1.0」の開発
  - 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」の作成
  - 全国のサイバーセキュリティコミュニティ及び有識者を対象とする調査に基づく「地域セキュリティコミュニティ【地域SECUNITY】形成・運営のためのプラクティス集」の作成
  - ユーザー企業及びベンダー企業を対象とする調査に基づく情報セキュリティサービス審査登録制度の改善ならびに普及促進策の検討
- これらの取組は相互に連携することにより、その効果をさらに高めることが期待される。たとえば、「サイバーセキュリティ体制の構築・人材確保の手引き」を参照して自組織に不足している人材の育成にあたってはセキュリティコミュニティ活動への参加が有効であることを認識し、「地域セキュリティコミュニティ【地域SECUNITY】形成・運営のためのプラクティス集」を参照して地元の地域コミュニティの形成または発展に取り組むことなどが想定される。こうした活用は企業が自ら行う場合のほか、情報処理安全確保支援士など、企業のサイバーセキュリティ対策を推進する役割を担う人材がこれらの成果を用いて指導を行うことも想定される。
- 今後は、この成果を企業において実際に活用した成果をもとに、成果物のいっそうの充実に向けた改善に取り組むとともに、経済産業省及びIPAにて推進されている「サイバーセキュリティお助け隊」や「サイバーセキュリティサプライチェーンコンソーシアム」等の制度等も考慮しつつ、国内企業において対策が遅れている領域（金融や重要インフラ以外の業種や、中堅・中小企業等）における対策の加速化の方策について検討及び実践していくことが求められる。