資料５

平成30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体制の構築及び戦略マネジメント層の育成に関する実態調査）

産業サイバーセキュリティ研究会 WG2　ご説明資料

2019年3月

一般社団法人日本情報システム・ユーザー協会（JUAS）
みずほ情報総研株式会社

1．調査の目的と仮説

調査の目的

セキュリティ体制の実態や、戦略マネジメント層に相当する人材の位置づけ・役割・育成方法を明らかにする。また、経営者や自社のセキュリティポリシー及び体制などの企画を担当する者にとって、セキュリティ対応力を高める際に参考となるプラクティスの整理や必要な政策などの検討を行う。

セキュリティ成熟度と体制における仮説

＜従来の仮説＞

セキュリティ成熟度を高めるには専任のセキュリティ体制が望ましい。

＜事業環境の変化＞

事業の多角化、グローバル化の進展や、IoT・AIを活用したDXへの取り組みを進めるには、セキュリティ対応への一層のスピードアップが求められる。

＜本調査における仮説＞

事業形態ごとに望ましいセキュリティ体制が異なるのではないか？
すなわち、成熟化＝組織の特徴に応じた最適な体制（組織により異なる）の確立
（JUASにおけるこれまでのセキュリティ関連活動の経験を踏まえた設定）
→ 本調査における検証と分析：

- 上記の仮説は正しいか？
- 事業形態に合わせたセキュリティ体制にするためにはどのようにすべきか。そのときの課題は何か？

1．調査の目的と仮説

セキュリティ成熟度の評価

セキュリティ成熟度に影響を与える因子は
①経営者の認識・意識
②企業規模
③事業形態（BtoB/BtoBtoC/BtoC、単一/多角化など※）
④インシデントの発生有無
但し、②企業規模は大規模企業に絞っていること、④については調査が困難な（回答してもらえない）ことが予測されることから、今回は①③に絞って分析する。

＜成熟度の評価＞
成熟度は経営ガイドラインの指示10項目に対する達成度（CMMIの5段階）で評価する。
成熟度　“低”：達成度3未満（一部しか出来ていない）が多数（6割超）を占める
成熟度　“中”：達成度3以上（出来ている）が過半数、
　　または達成度3未満あっても、達成度4以上が4割以上ある場合
成熟度　“高”：達成度3未満がなく、かつ達成度4以上（展開されている）が4割以上

※事業部におけるセキュリティの課題としてOT/IoT/DXに関するセキュリティガバナンスなどが挙げられた場合にはそれも課題として付記する

1．調査の目的と仮説

調査実施概要

（1）企業調査

- 様々な規模・業種・成熟度の企業におけるセキュリティ体制の実態や人材の位置づけ・役割・育成方法等についてアンケートおよびヒアリングを実施。
- アンケート72回答(回答率47%)、ヒアリング31社＜建築・土木(2),素材製造(11),機械器具製造(10),商社・流通(1),金融(3),社会インフラ(1),サービス(3）＞

（2）文献調査

- サイバーセキュリティに関する既存の文献を調査・整理した。

（3）政府会議等における議論の把握

- 経済産業省、NISC等、関連する政府の会議等における有識者の議論を把握し、整合性を取るとともに、調査結果の分析や報告書の作成の参考とした。

（4）有識者ヒアリング

- 調査結果の分析・報告書の作成に当たり、サイバーセキュリティの業界動向に詳しい有識者10名に対しヒアリングを実施。

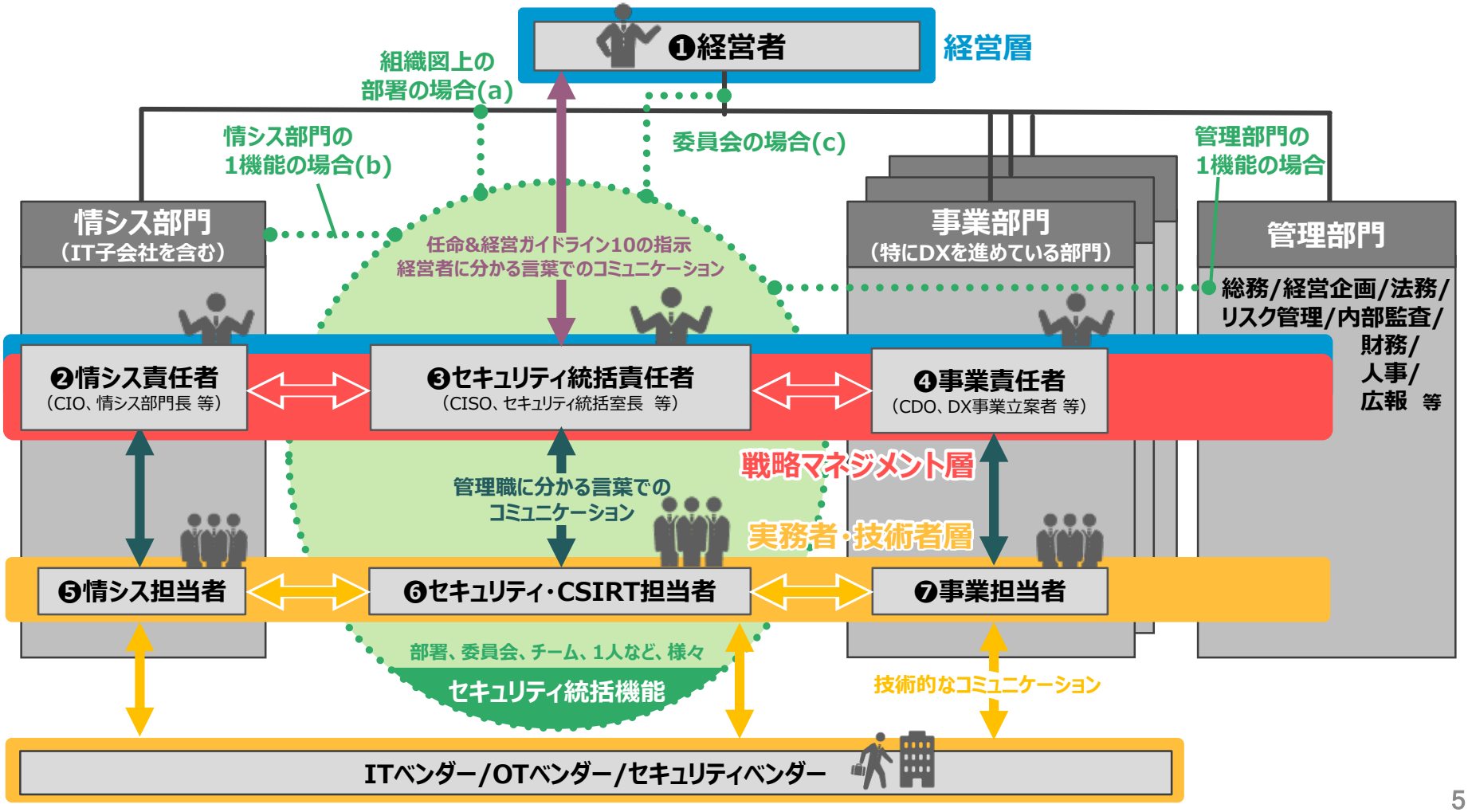
（5）調査結果の分析・報告書の作成

- プラクティスの取りまとめおよび、政策的課題の洗い出し・施策の検討を実施。

2．「セキュリティ統括機能」の定義（経産省資料より）

セキュリティ統括機能：部門横断的な立場でCISOの役割を担う経営幹部を補佐し、組織内のすべてのセキュリティ戦略に対応（産業横断サイバーセキュリティ人材育成研究会に定義による）

戦略マネジメント層：　経営・事業戦略に係るサイバーセキュリティリスクのマネジメントを中心になって支え、対策を立案し、実務者・技術者を指揮し、経営者に報告する（NISCの定義による）

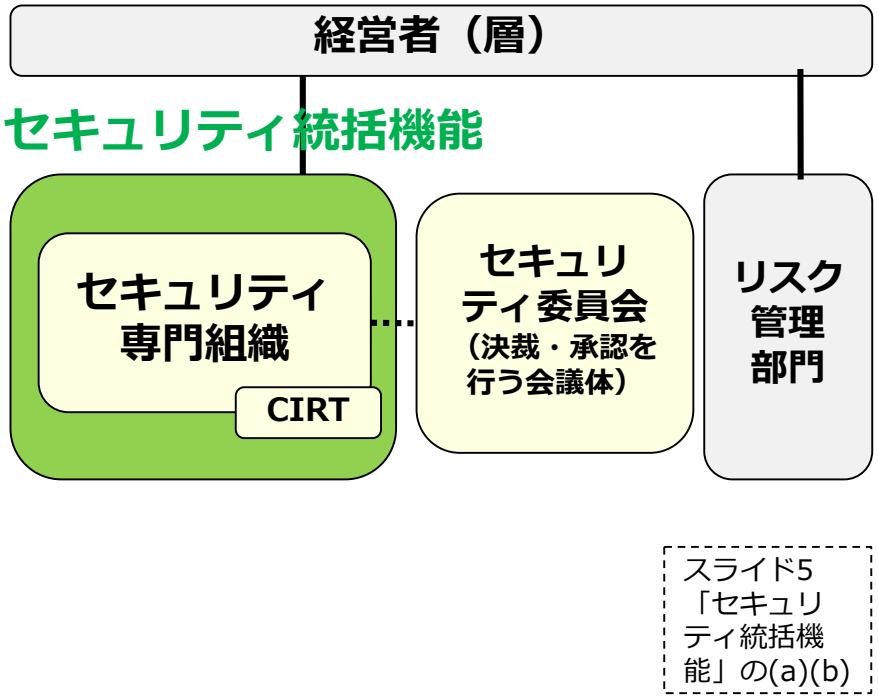


出典：経済産業省「産業サイバーセキュリティ研究会WG2」資料

3．セキュリティ体制の類型化

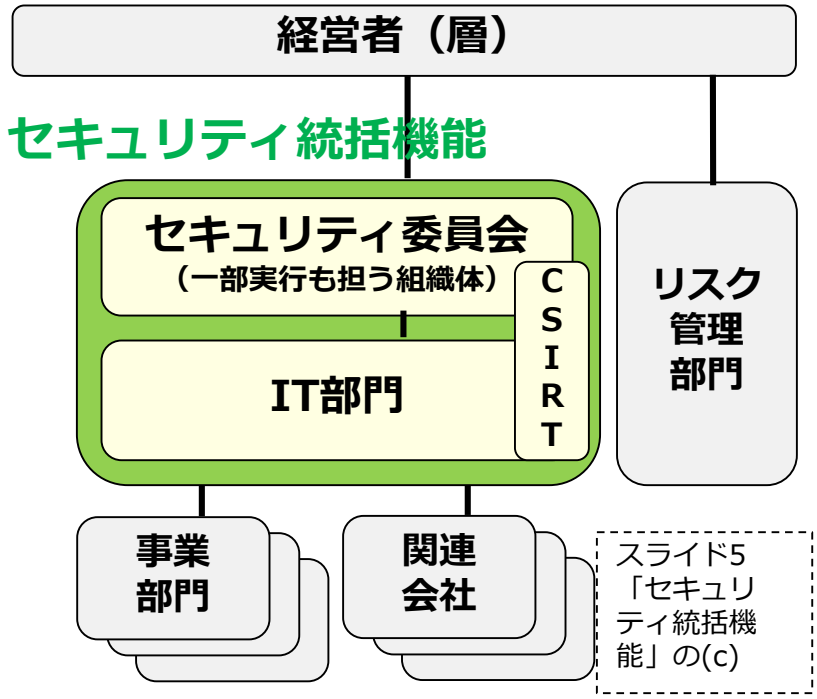
■形態から見たサイバーセキュリティ体制の類型

専門組織型



セキュリティ統括機能をセキュリティ専門組織が担う形態である。セキュリティ専門組織には、明示的に独立した部門のほか、IT部門の中にセキュリティチームを設置し専門組織として遂行するケースも多い。また、セキュリティに関する委員会が会議体として存在し、方針・規定類の決裁や承認、インシデントの報告共有、有事の危機管理委員会とし機能する。委員会は四半期に1回や年に1～2回程度または有事の際に開かれ、実行機能はセキュリティ専門組織が担う形式である。

委員会型



セキュリティ統括機能をセキュリティ委員会およびIT部門とで担う形態である。管理系や事業系の部門（関連会社が含まれる場合もある）とIT部門からなるセキュリティ委員会が一部実行も担う組織体として存在し、そのアンダーにIT部門が位置づいて、各事業部門や関連会社へのガバナンスを実施する形式である。

3．セキュリティ体制の類型化

■機能分担から見たサイバーセキュリティ体制の類型

集権型：全社で統一されたセキュリティ対策のルールに基づき、一元的に管理
連邦型：セキュリティ対策のうち、全社システムは一か所で統括、各事業部・関連会社固有のシステムは各々が担当
分権型：セキュリティ対策の企画機能をはじめとする、ほとんどの機能を各事業部・関連会社に分散（事例は少ない）

	集権型	タスク	連邦型
役割			
セキュリティ統括機能	(4)リスクアセスメント、セキュリティ対応策策定 (5)セキュリティ対策実施、展開 (9)インシデント発生時の危機管理（CSIRT/SOC活動）	(1)セキュリティ方針作成・体制構築 (2)セキュリティ戦略・計画の策定（予算、体制含む） (3)セキュリティ規定類作成 (7)セキュリティ教育、啓発、訓練 (8)インシデント対応計画策定・体制構築（CSIRT構築）	(9)インシデント発生時の危機管理（CSIRT/SOC活動）【全社共通の管理・対応機能】
リスク管理部門		(6)セキュリティ監査・点検	
事業部門（関連会社含む）（※）		(10)サプライチェーン管理	(4)リスクアセスメント、セキュリティ対応策策定 (5)セキュリティ対策実施、展開 (9)インシデント発生時の危機管理（CSIRT/SOC活動）【主にセキュリティ統括機能との連携窓口】

（※）個別システムのセキュリティは事業部が管理する。IT部門もセキュリティ統括機能としての位置づけではなく、インフラ系のシステムを全社に提供する一事業部としての位置づけではここに含まれる。

3．セキュリティ体制の類型化

■機能分担類型による特徴

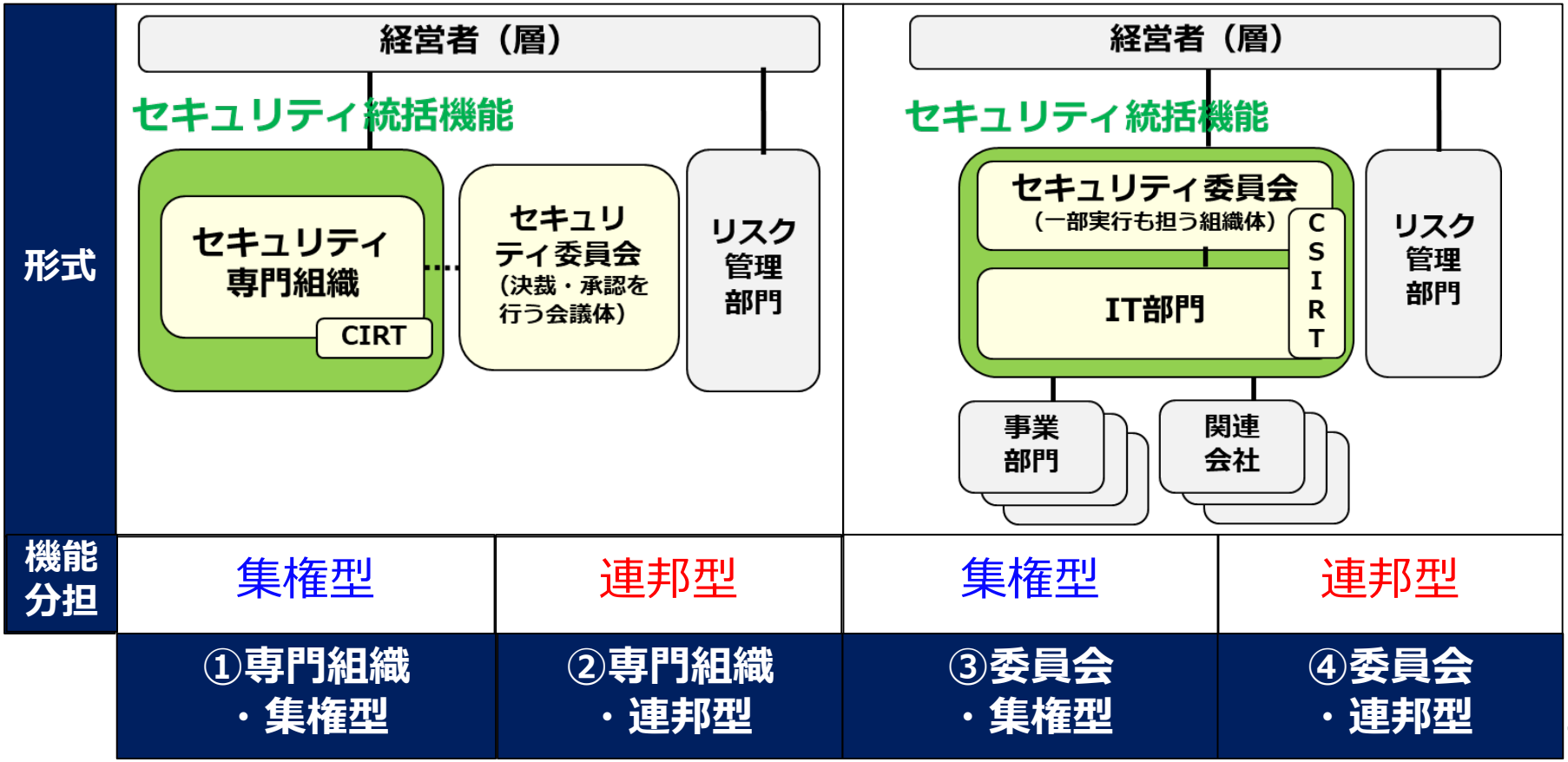
・各企業は次のような特徴を踏まえて、自らのセキュリティ組織体制を決定していると考えられる。

類型	利点（〇）、課題（×）
集権型	〇 専門人材のリソースが限られている場合に最大の効果を発揮 〇 セキュリティ対策組織の運営コストを最小化できる 〇 組織におけるセキュリティ対策のレベルを均質化しやすい × セキュリティ統括組織が事業部門の業務内容やリスクを把握するのに時間がかかる × 現場の事情を対策に反映しにくい × 事業内容に応じた柔軟な対応を行いにくい
連邦型 分権型	〇 事業実施における意思決定が早い 〇 現場の事情を対策に反映しやすい 〇 多角的な事業を行っている場合に、事業毎に柔軟な運用が可能 × 事業部門毎にセキュリティ対策の専門性を備えた人材を配置する必要がある × 集権型よりも運営コストがかかる × 特定の事業部門のセキュリティ対策レベルが低下しても気付きにくい

3．セキュリティ体制の類型化

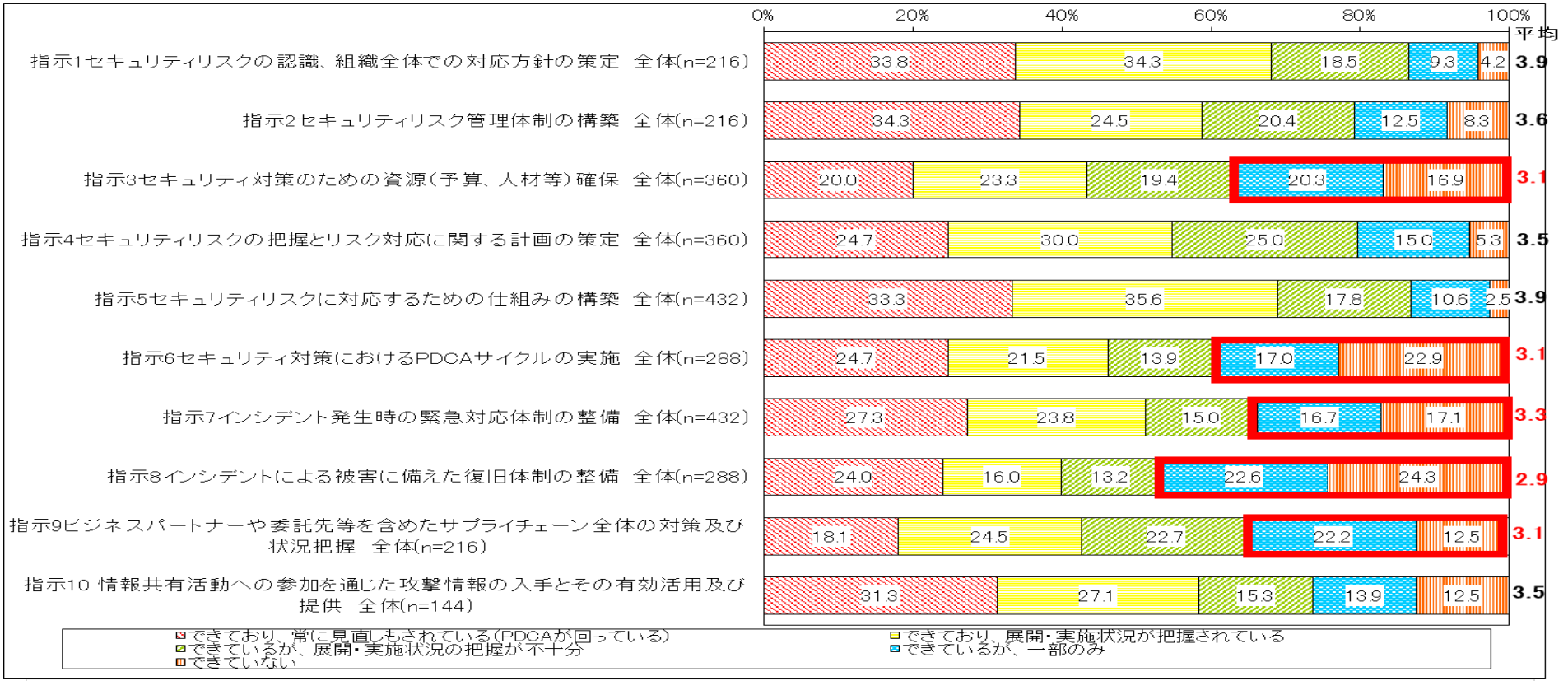
■セキュリティ組織における４つの体制パターン

- 形態（専門組織型／委員会型）および機能分担（集権型／連邦型）から4つの体制パターンに類型化できると考える。
- 今後セキュリティ体制を強化、再編成する場合には、これらのパターンを参考に、**自社のビジネス形態や経営者の方針等の環境に応じて自社に最適な体制をユーザー企業が主体的に検討・選択していくことが重要である。**



4．セキュリティ成熟度の分析結果

■サイバーセキュリティ経営ガイドラインチェックシート項目毎の達成状況



- ✓ **全体的には「できており、常に見直しもされている」「できており、展開・実施状況が把握されている」とも２～３割で、約半数の企業では経営ガイドラインを実施できている。**
- ✓ **「指示１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」や「指示5セキュリティリスクに対応するための仕組みの構築」が比較的達成度が高い。**
- ✓ **「指示3セキュリティ対策のための資源（予算、人材等）確保」、「指示6セキュリティ対策におけるPDCAサイクルの実施」、「指示7インシデント発生時の緊急対応体制の整備」、「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」および「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」が達成度が低い傾向。**

4．セキュリティ成熟度の分析結果

■チェックシート項目毎の達成状況の比較（5段階の平均値と分散）

✓チェックリストの41項目の達成状況を、全体と成熟度別に平均値及び分散で数値化した（達成度最高=5, 最低＝1）。
✓教育関連で従業員向けセキュリティ教育（指示5-6）が平均値最高、セキュリティ人材のキャリア設計（指示3-4）が最低と二分する結果に。
✓分散が大きいのは、訓練・演習関連（指示8-4）の項目であり、達成可否で企業間に差が生じている。

全体平均値のベスト・ワースト3				全体	成熟度別平均値			コメント
					高	中	低	
ベスト3	指示5-6	従業員に対して、サイバーセキュリティに関する教育（防御の基本となる対策実施（ソフトウェアの更新の徹底、マルウェア対策ソフトの導入等）の周知、標的型攻撃メール訓練など）を実施している。	平均	4.29	4.71	4.50	3.47	平均値が高く、分散が小さい。すなわち、回答した企業において最も達成できている項目である。
			分散	0.68	0.30	0.44	0.57	
	指示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	平均	3.99	4.71	4.13	2.95	成熟度中の企業で平均値が高めかつ分散が最小であり、成熟度高中の企業では経営層の認識は達成できているものと推察される。
			分散	0.90	0.30	0.36	0.79	
	指示7-1	組織の内外における緊急連絡先・伝達ルートを整備している（緊急連絡先には、システム運用、Webサイト保守・運用、契約しているセキュリティベンダの連絡先含む）	平均	3.94	4.71	4.19	2.68	成熟度中の企業でも比較的達成されている項目。
			分散	1.22	0.20	0.53	1.16	
ワースト3	指示6-2	サイバーセキュリティにかかる外部監査を実施している	平均	2.57	3.67	2.31	1.79	ISMSやPマークの審査も外部監査の一種とみなせば、実態はもう少し高い数値と考えられる。
			分散	2.11	1.75	1.96	0.69	
	指示6-4	サイバーセキュリティリスクや取組状況を外部に公開している	平均	2.25	3.43	2.03	1.32	平均値が人材キャリアパスの設計に次いで低く、中⇔低間のギャップが低めであることから、成熟度中以下の企業ではほとんど達成できてない。
			分散	2.24	1.86	2.03	0.53	
	指示3-4	組織内のサイバーセキュリティ人材のキャリアパスの設計を検討、及び適正な処遇をしている	平均	2.07	3.10	1.91	1.21	全体で最も達成できていない項目。ただし、成熟度高で分散が全項目中最大となっており、一部企業では取り組まれていることがわかる。
			分散	1.65	1.90	1.15	0.27	

全体平均値のベスト・ワースト3				全体	成熟度別平均値			コメント
					高	中	低	
	指示8-4	定期的に復旧対応訓練や演習を行っている	平均	2.61	4.43	2.22	1.26	全項目中で最も分散値の高い項目。成熟度高の企業でのみ高く、中低で低いことから、復旧対応訓練の実施は成熟度高のバロメータと言えそうである。
			分散	2.57	0.63	1.73	0.40	

4．セキュリティ成熟度の分析結果

■成熟度高⇔中⇔低の差を表象する典型的な項目

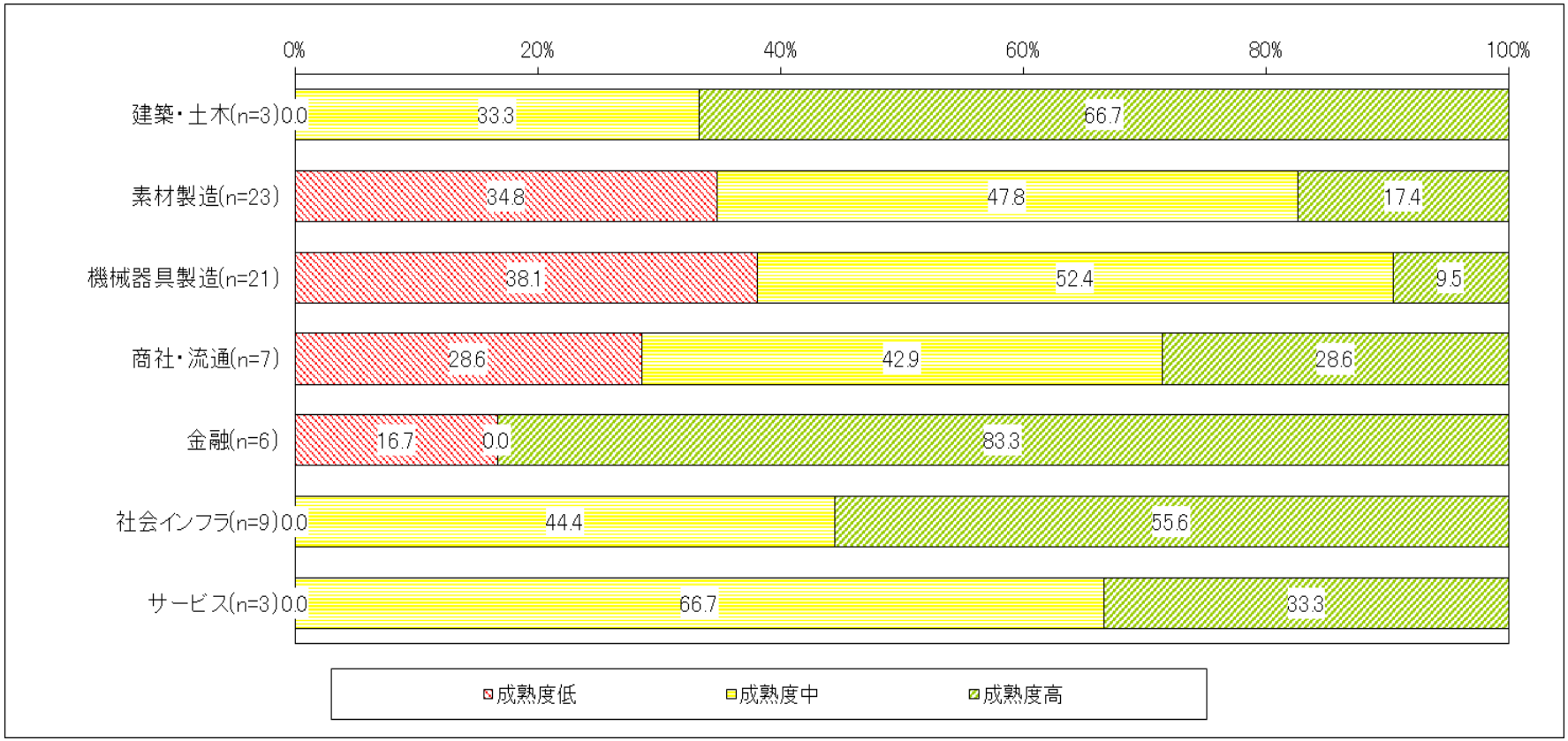
- ✓回答企業の成熟度別に高・中・低の３グループに分類したとき、チェックリスト項目毎の回答結果においてグループ間の平均値のギャップが大きな項目を抽出した結果を下表に示す。
- ✓**成熟度「中」と「低」のギャップ**が大きな項目の傾向から、両者の差は**セキュリティ対策のための体制や仕組みの整備が済んでいるかどうか**にあることがわかる。
- ✓同様に、**「高」と「中」のギャップ**が大きな項目の傾向から、両者の差は**セキュリティ対策の仕組みの実効的な運用ができているかどうか**にあることが読み取れる。

	高グループ平均		中グループ平均	中低間ギャップ	低グループ平均
指示7-3 CSIRTの設置	4.71		3.44	1.86	1.58
指示6-3 PDCA体制の整備・維持	4.71		3.78	1.62	2.16
指示1-3法律等の要求事項の把握	4.76		3.94	1.62	2.32

	高グループ平均	高中間ギャップ	中グループ平均		低グループ平均
指示8-1 復旧計画の策定	4.33	1.74	2.59		1.47
指示8-2 復旧計画の見直し	4.43	1.90	2.53		1.42
指示8-4 復旧対応訓練の実施	4.43	2.21	2.22		1.26

4．セキュリティ成熟度の分析結果

＜「セキュリティ成熟度」と「業種」との関係＞

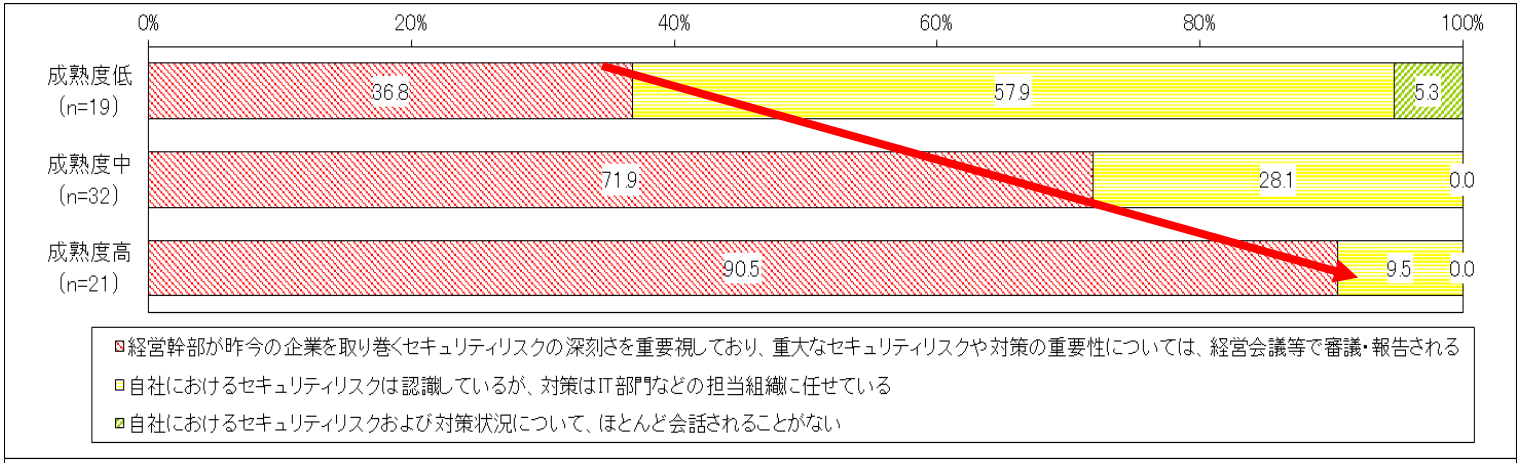


✓ 「金融」「建築・土木」「社会インフラ」は成熟度が高い傾向にあり、「素材製造」「機械器具製造」「商社・流通」は成熟度中～低が多い傾向にある。

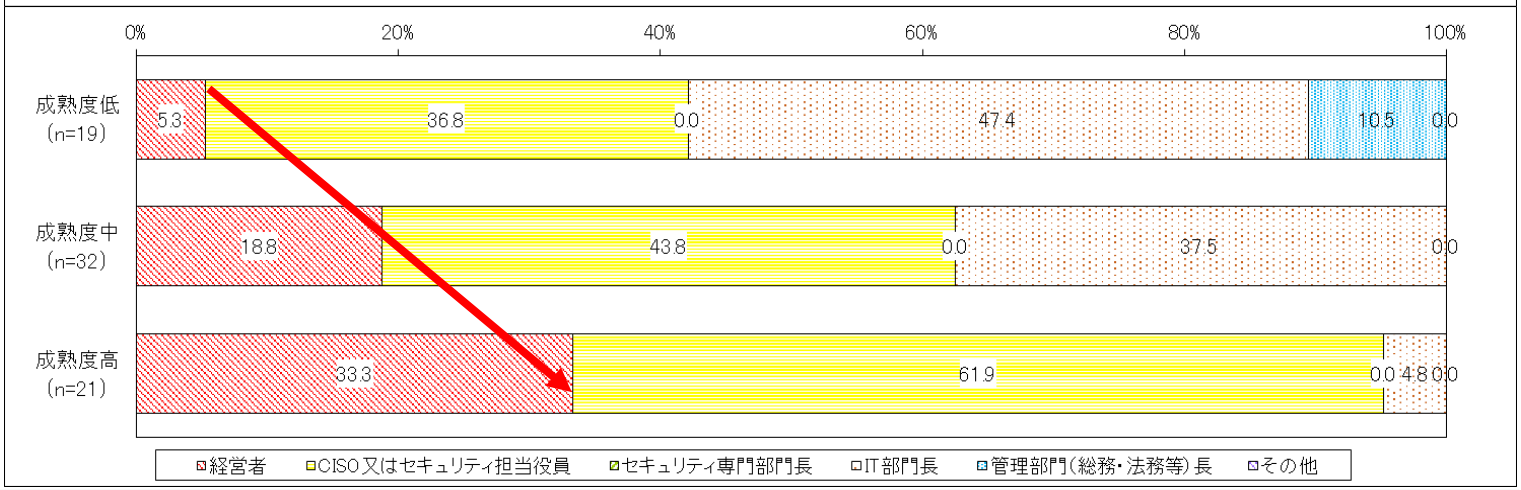
4．セキュリティ成熟度の分析結果

＜「セキュリティ成熟度」と「経営の関与」との関係＞

「セキュリティ成熟度」と「経営の関与」との関係



「セキュリティ成熟度」と「意志決定の最上位者」との関係

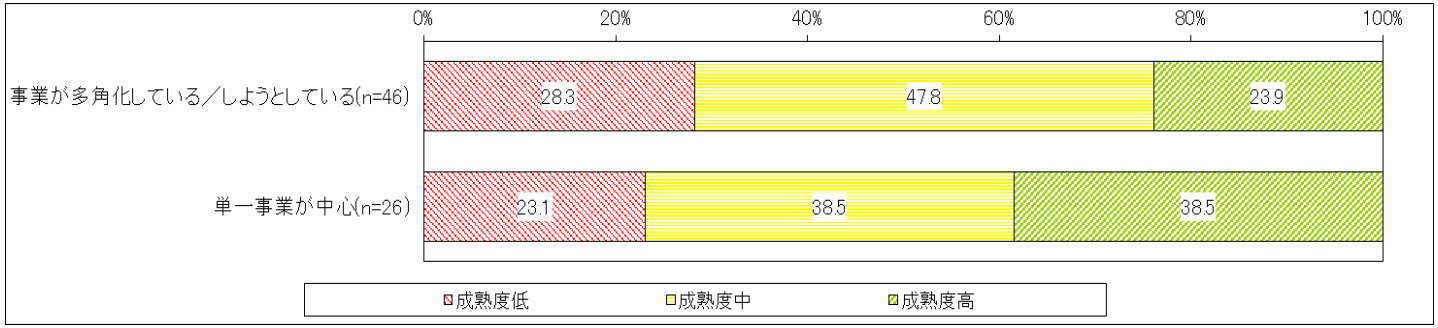


- ✓ **成熟度が高いほど、経営の関与度が高い。また、意思決定者も経営に近くなる傾向にある。経営が、経営リスクの一環としてセキュリティを認識するだけでなく、セキュリティの最上位者として位置づくことで、トップダウンでの推進が可能となり、成熟度を高めることにつながっていると推察される。**

4．セキュリティ成熟度の分析結果

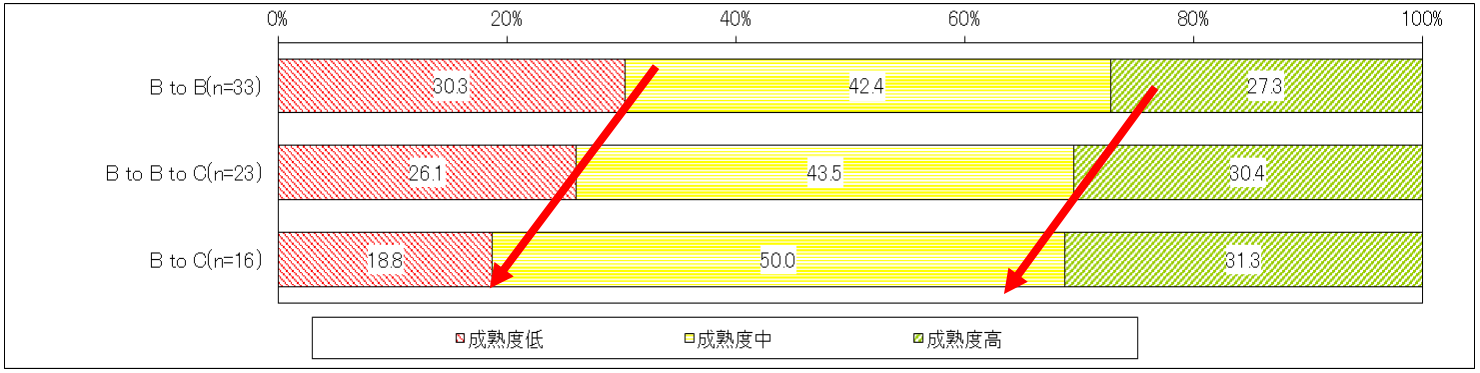
＜「セキュリティ成熟度」と「事業形態」との関係＞

「セキュリティ成熟度」と「事業形態事業形態（多角化／単一）」との関係



✓ 「単一事業が中心」の方が「事業が多角化している／しようとしている」企業群より成熟度が高い傾向。多角化により事業が複雑化しやすいことに比べると、単一事業のほうが比較的ガバナンスが展開しやすいことが影響していると推察される。

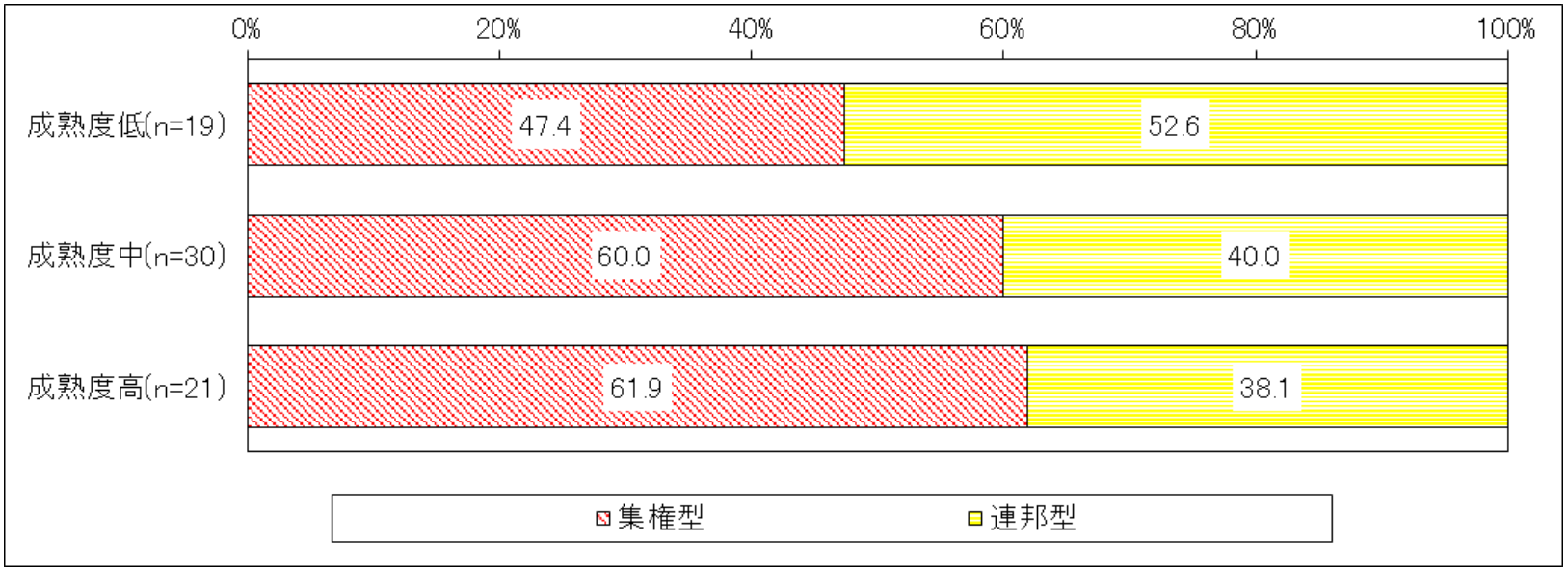
「セキュリティ成熟度」と「事業形態（BtoB/BtoBtoC/BtoC）」との関係



✓ BtoB、BtoBtoC、BtoCの順で成熟度が高くなる傾向にある。コンシューマーが近くなるにつれて、一般消費者への影響やレピュテーションリスクなどが意識され、セキュリティガバナンスを高めていこうとする意識が強く働いていくのではないかと推察される。

4．セキュリティ成熟度の分析結果

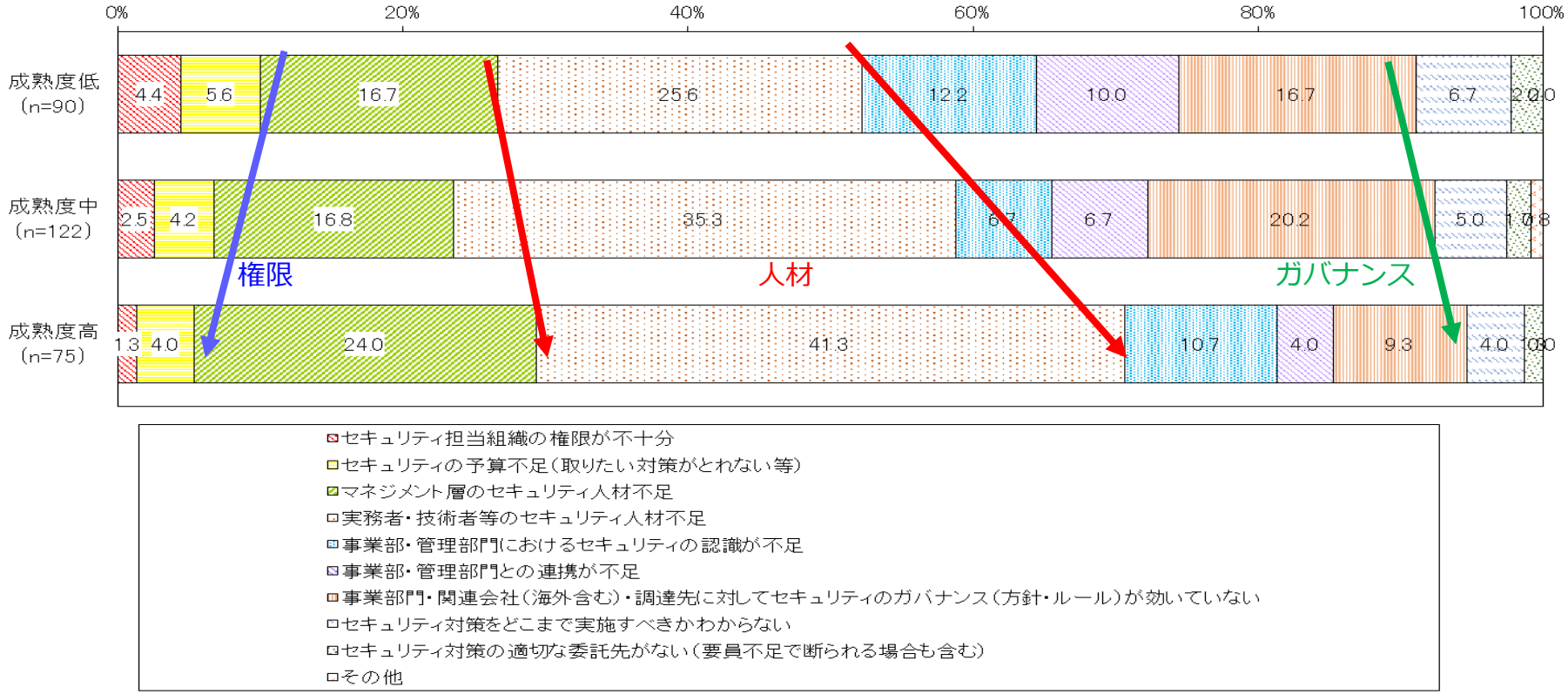
＜「セキュリティ成熟度」と「セキュリティ体制（機能分担）」との関係＞



- ✓ 「成熟度低」では「連邦型」が「集権型」よりもわずかに多いが、「成熟度中～高」では「集権型」のほうが20%多い回答となっている。一方、「集権型」と「連邦型」の比率は、「成熟度中」と「成熟度高」の間ではほぼ同じである。
- ✓ ビジネスに求めるスピード感やリスクのとらえ方は企業によって異なり、最適な体制の在り方は各社各様なため、自社ビジネスに合わせて「集権型」「連邦型」を採用していると考えられるが、ガバナンスの展開のしやすさという点では「集権型」のほうが展開しやすい傾向が見て取れる。
- ✓ 成熟度低から中・高へのステップアップには、集権型でガバナンスを強化することが有効と推察される。

4．セキュリティ成熟度の分析結果

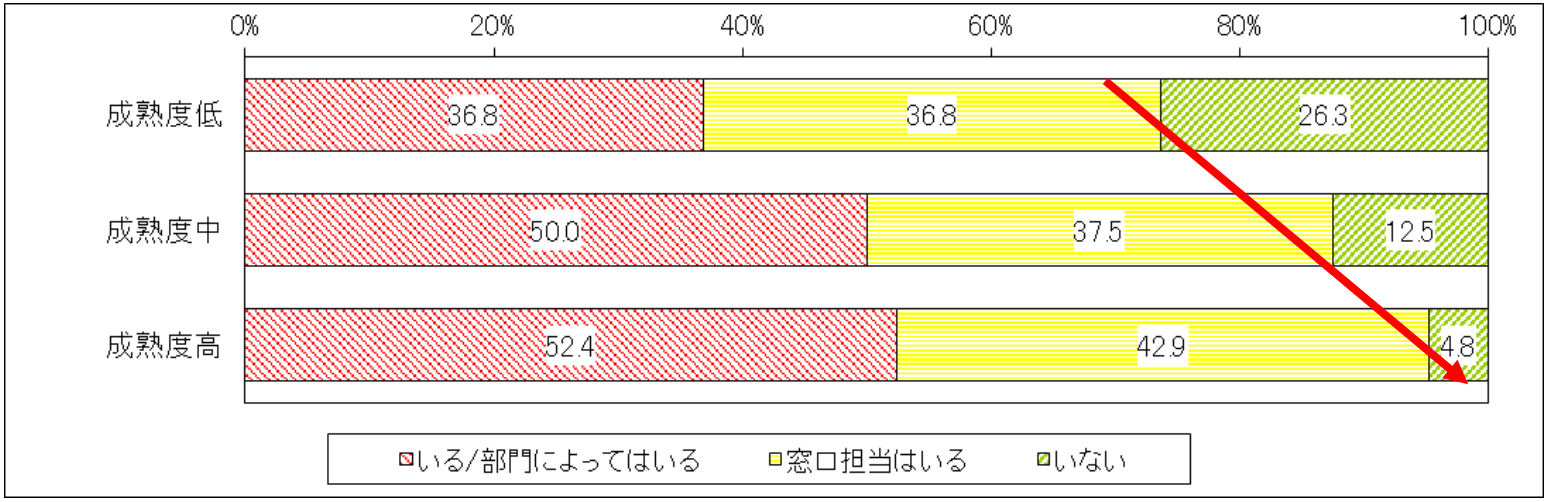
＜「セキュリティ成熟度」と「セキュリティガバナンスにおける課題」との関係＞



- ✓ **成熟度が上がるにつれ、セキュリティ担当組織の権限に対する課題感も減り、十分な権限が確保される傾向にある。また、事業部門・関連会社（海外含む）・調達先に対するセキュリティのガバナンスに対する課題感も減少する。**
- ✓ **セキュリティ担当組織の権限が確保され、組織的なガバナンスが充足してくると、次のステップとして、それを支える人材の確保・育成に目が向くようになり、課題として顕在化してくることがうかがえる。**

４．セキュリティ成熟度の分析結果

＜「セキュリティ成熟度」と「事業部門におけるセキュリティ担当」の関係＞



- ✓　成熟度が上がるにつれて、「事業部門におけるセキュリティ担当」が何らかの形でいる傾向にある。
- ✓　「いない」に着目すると、「成熟度低」と「成熟度中」とでは13.8ポイント減、「成熟度低」と「成熟度高」とでは21.5ポイント減となっている。
- ✓　「事業部門におけるセキュリティ担当」の設置は、「成熟度低」から「成熟度中または高」へステップアップしていく上での重要なファクターと考えられる。

4．セキュリティ成熟度の分析結果

■セキュリティ成熟度の分析における主な知見

課題の傾向

- ✓セキュリティリスクの認識および組織全体での対応方針の策定（指示1）や「セキュリティリスク対応のための仕組み構築（指示5）の達成度は比較的高い傾向にある。一方、**セキュリティ人材の育成**（指示3）やセキュリティ対策における**PDCAサイクルの実施**（指示6）、**インシデント発生時の緊急対応や復旧における訓練・演習の定期的な実施**（指示7、指示8）については、これからの課題と感じている傾向。
- ✓**成熟度が上がるにつれ組織的なガバナンスが充足してくると、人材の確保・育成に目が向く**ようになり、課題として顕在化する傾向にある。

成熟度の向上に資するポイント

- ✓**経営が、経営リスクの一環としてセキュリティを認識し意思決定の最上位者として位置づくこと**
- ✓**セキュリティ統括機能の設置**

成熟度「低」「中」「高」ごとに有効と思われる施策

- ✓「成熟度中」から「成熟度高」へはあまり大幅なギャップではないが「成熟度低」から「成熟度中」へのステップアップには大きなギャップがある。
- ✓**「成熟度低」から「成熟度中」以上へのステップアップに有効な施策**
  - ✓**CSIRT等セキュリティ統括機能にあたる体制や仕組みの整備**が有効。機能分担においては「成熟度中」以上ではガバナンスの展開のしやすさから**「集権型」が多い傾向**もみられた。
  - ✓**事業部門におけるセキュリティ担当の設置**も有効。
- ✓**「成熟度中」から「成熟度高」へのステップアップに有効な施策**
  - ✓**復旧計画の策定・見直し・訓練といったPDCAの観点を踏まえたより実効的な運用施策**が必要となる。

5.サイバーセキュリティ組織・体制・人材におけるポイント（31項目）

サイバーセキュリティ組織・体制とガバナンス

＜体制構築・ガバナンス＞

Point1：「何を何のために守るのか、守るために何をすべきか、有事の際一番大事なことは何か」という意識を全員が持つことがガバナンス強化につながる

Point2：事業リスクの視点でセキュリティを考えることが実効力ある仕組み作りに繋がる

Point3：「スムーズに情報が伝わること」が体制整備において大切な設計思想である

Point4：サービス部門ではなくガバナンス部門として位置づける

＜IT/IoT/OTセキュリティ組織の在り方＞

Point5：IT/IoT/OTセキュリティの要素技術は同じでも組織としての在り方は試行錯誤の段階。事業の性質、求めるスピードなどによってIT部内のセキュリティ組織に一元化するケースと分離独立するケースとに分かれている

＜グローバル・関係会社におけるセキュリティガバナンス＞

Point6：国内のガバナンスに比べ、グローバル・関連会社（特にM&A企業）のガバナンスの体制整備はこれから。コミュニケーションを重ねた体制づくりが必要である

Point7：クラウド活用やアセスメントツールによる標準化でガバナンス体制の省力化を図る

＜サプライチェーンにおけるセキュリティガバナンス＞

Point8：委託先を含めたセキュリティレベルアップには認証やチェックリストなどの活用が有効である

5.サイバーセキュリティ組織・体制・人材におけるポイント（31項目）

事業部門における体制およびサイバーセキュリティ組織・体制との関係

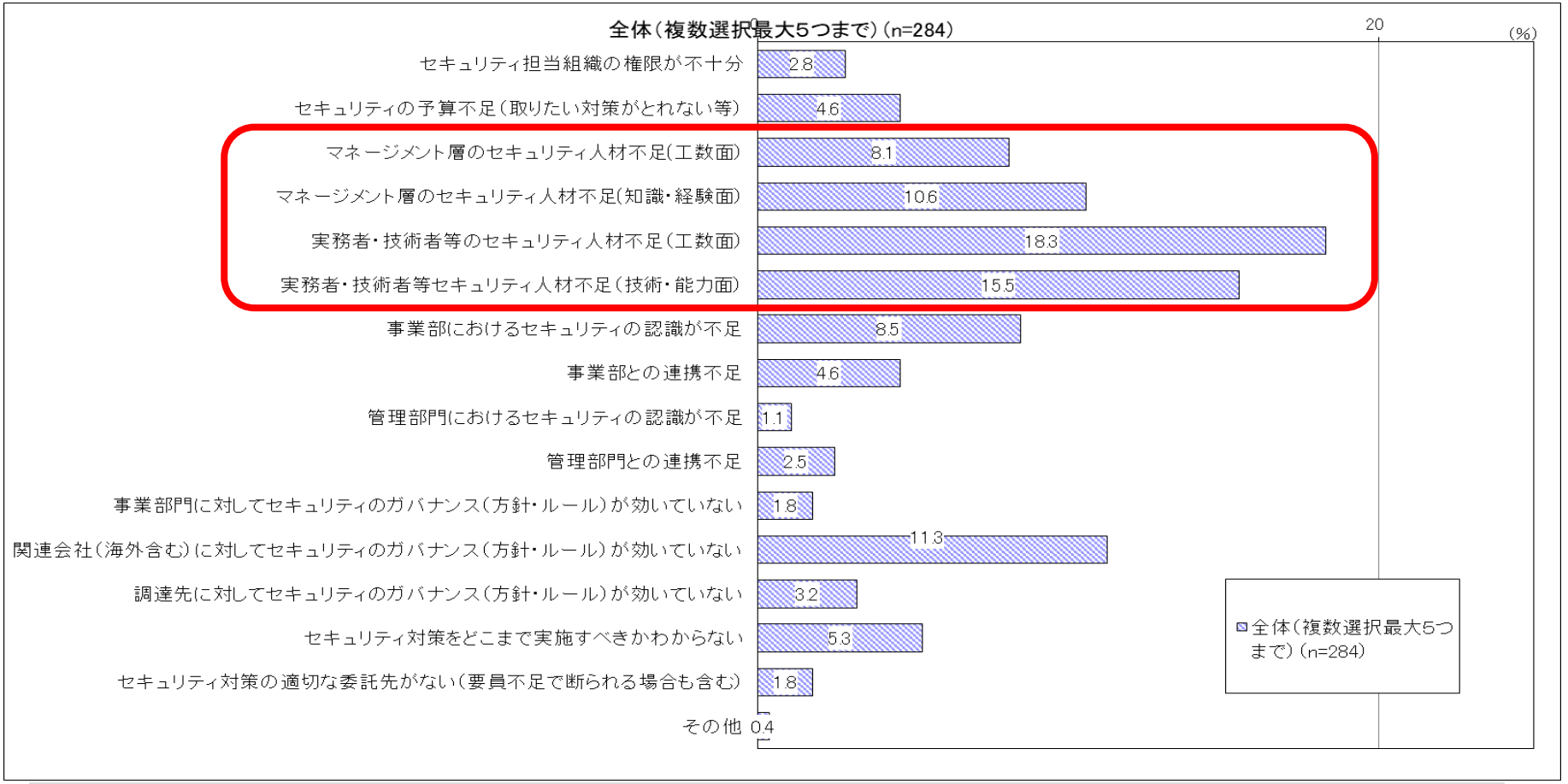
Point9　：事業部門におけるセキュリティ担当者の主な役割は「ハブ機能」にとどまっている。
　　事業内容や環境にあわせた役割の明確化が重要である
Point10：事業のオーナーとして主体的なセキュリティ意識をより向上させることが
　　事業部門には期待されている
Point11：セキュリティ組織が事業部門の良き「パートナー」として事業を支えることが
　　期待されている

セキュリティ業務のソーシング

Point12：セキュリティの技術的な専門性や、第三者としての監査・点検の視点は
　　外部ベンダーの活用が有効である
Point13：ユーザー企業が自らやるべきことは何かを主体的に切り分けることが重要である

5.サイバーセキュリティ組織・体制・人材におけるポイント（31項目）

<サイバーセキュリティの組織体制における課題>



- ✓ 「マネジメント層のセキュリティ人材不足」「実務者・技術者等のセキュリティ人材不足」との回答が多く、セキュリティ人材の不足が多くの企業での課題。
- ✓ 実務者・技術者等においては知識・経験面よりは工数面の不足感が高く、いわゆる人手が足りない状況にあるのがうかがえるのに対し、マネジメント層においては工数面に比べて知識・経験面での不足感が高い傾向にあった。

5.サイバーセキュリティ組織・体制・人材におけるポイント（31項目）

セキュリティマネジメント層 (※) のスキル・育成・採用・配置

※「セキュリティマネジメント層」とはスライド5の「戦略マネジメント層」のうち「セキュリティ統括責任者」「情シス責任者」を指すこととする。

＜モチベーション＞

Point14：セキュリティマネジメントのやりがいは、限られたリソースの中で自らセキュリティ施策を考え、経営とコミュニケーションしながら実現していく達成感

Point15：この会社を守りたいという強い意志とセキュリティへの「やる気」

＜求められるスキル・知識＞

Point16：自社のビジネスの視点から、俯瞰的にリスク管理や判断ができるプロジェクトマネジメント力

Point17：理想だけでなく現実解を考えられるバランス力

Point18：社内外の様々な人と連携しながら経営や事業部門の行動を促すコミュニケーション力

Point19：システム・情報の流れなど自社の仕組みを熟知する

Point20：求められるセキュリティ知識は高い専門性よりも幅広さ

Point21：資格は押さえるべきポイントの把握や知識の棚卸として有効だが、最も期待されているのは知識やスキルを「使いこなす力」

＜育成＞

Point22：ローテーションによって幅広い経験から自社の仕組みを体得する

Point23：インフラシステムの経験は自社の仕組みを体得することにつながる

Point24：自分の事業として痛みを感じながら経験を積むことが人を育てる

Point25：インシデント対応や報告などの「訓練」はスキルアップに有効

Point26：セキュリティに関するコミュニティに積極的に参加することで、「やるべきこと」が磨かれる

5.サイバーセキュリティ組織・体制・人材におけるポイント（31項目）

セキュリティマネジメント層のスキル・育成・採用・配置

＜採用・確保＞

Point27：ユーザー企業にフィットした即戦力人材の確保は困難。採用後長い目で自社なりの育成を模索することも必要である

Point28：経験豊富なシニア人材の活躍が人材確保の切り札になる

＜配置＞

Point29：マネジメントと専門技術とがわかるスーパーマンがいなくてもよい。組織機能としてこれらの役割をはたせる配置になっていることが大切である

事業部のセキュリティ担当者の育成・スキル

＜事業部におけるIT系のセキュリティ担当＞

Point30：大切なのは事業インパクトにてらした「セキュリティ感度」を持つこと

＜事業部におけるIoT/OT系のセキュリティ担当＞

Point31：事業部におけるIoT/OT系のセキュリティ担当に求められるスキルはIT系の担当者と同様だが、製品実務や技術への理解も求められる

6．政策的課題の洗い出し及び施策の検討

本調査によって明らかになった課題

- ✓ あるべきセキュリティ組織体制の姿に正解はなく、おかれているビジネス環境や重視するリスク、事業の成り立ち等をふまえて、自社に最適なあり方を模索し、様々なステークホルダーとの連携・調整を積み重ねて実現していかねばならない。
- ✓ 今後成熟度を高めていくにあたっては、成熟度ごとに効果的な施策が異なるため、自社の成熟度を見える化し、成熟度に合わせた効果的な施策を講じていくことも課題となる。
- ✓ いずれにおいても、経営の理解なくして推進は困難。経営の理解を促す、あるいは経営を説得できる人材がますます重要となる。この役割を担うセキュリティマネジメント人材をいかに確保し、育成するかが今後の最大の課題。

今後に向けた施策の提言

- ✓ 本調査によってセキュリティ体制の類型概念や、成熟度ごとの傾向、セキュリティマネジメント人材に求められるスキルや知識についての概念は整理できた。そこで今後はさらに次のような支援が望まれると考える。

  - **成熟度に応じて参考となるような、セキュリティ体制における施策（事例）の整理**
  - **セキュリティマネジメント人材の育成・確保における具体的な事例の整理**
  - **産業横断でのセキュリティマネジメント人材によるコミュニティ活動の支援**

参考：チェックシート項目毎の達成状況の比較（5段階の平均値と分散）一覧

			全平均	成熟度別平均値			ギャップ（平均値同士の差）			全分散	成熟度別分散			コメント
				高（N=21）	中（N=32）	低（N=19）	高⇔低	高⇔中	中⇔低		高（N=22）	中（N=32）	低（N=19）	
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	3.99	4.71	4.13	2.95	1.77	0.59	1.18	0.90	0.30	0.36	0.79	成熟度中の企業で平均値が高めかつ分散が最小であり、成熟度高中の企業では経営層の認識は達成できているものと推察される。
	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対応方針（セキュリティポリシー）を策定し、宣言している	3.79	4.76	3.91	2.53	2.24	0.86	1.38	1.44	0.18	0.83	1.20	
	1−3	法律や業界のガイドライン等の要求事項を把握している	3.75	4.76	3.94	2.32	2.45	0.82	1.62	1.35	0.18	0.62	0.64	
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	組織の対応方針（セキュリティポリシー）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	3.72	4.76	3.88	2.32	2.45	0.89	1.56	1.73	0.18	0.92	1.58	成熟度低の企業における分散が全項目中最大であり、低の企業群の中で体制の有無で2分されていることがわかる。
	2−2	サイバー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	3.67	4.81	3.75	2.26	2.55	1.06	1.49	1.56	0.15	1.00	0.61	成熟度高の企業ではほぼ完璧に達成されている模様。
	2−3	組織内のリスク管理体制とサイバーセキュリティリスク管理体制の関係を明確に規定している	3.53	4.81	3.53	2.11	2.70	1.28	1.43	1.69	0.15	1.00	0.73	成熟度高の企業ではほぼ完璧に達成されている模様。
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	必要なサイバーセキュリティ対策を明確にし、経営会議などで対策の内容に見合った適切な費用かどうかを評価し、必要な予算を確保している	3.61	4.57	3.69	2.42	2.15	0.88	1.27	1.43	0.34	0.96	0.98	
	3−2	サイバーセキュリティ対策を実施できる人材を確保し、各担当者が自身の役割を理解している（組織の内外問わず）	3.18	4.10	3.31	1.95	2.15	0.78	1.37	1.54	0.56	1.09	0.89	
	3−3	組織内でサイバーセキュリティ人材を育成している	2.69	3.52	2.69	1.79	1.73	0.84	0.90	1.35	1.49	0.84	0.48	成熟度高の企業でも意外に平均値が低い。
	3−4	組織内のサイバーセキュリティ人材のキャリアパスの設計を検討、及び適正な処遇をしている	2.07	3.10	1.91	1.21	1.88	1.19	0.70	1.65	1.90	1.15	0.27	全体で最も達成できていない項目。ただし、成熟度高で分散が全項目中最大となっており、一部企業では取り組まれていることがわかる。
	3−5	セキュリティ担当者以外も含めた従業員向けセキュリティ研修等を継続的に実施している	3.90	4.57	4.19	2.68	1.89	0.38	1.50	1.42	0.53	1.03	0.95	成熟度中の企業でも比較的達成されている項目。5−6のセキュリティ教育への回答との差が大きいが、原因不明。研修という用語にトレーニングのニュアンスを感じるためか。
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	守るべき情報を特定し、当該情報の保管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	3.60	4.62	3.72	2.26	2.36	0.90	1.46	1.55	0.33	1.08	0.72	
	4−2	特定した守るべき情報に対するサイバー攻撃の脅威、脆弱性を識別し、経営戦略を踏まえたサイバーセキュリティリスクとして把握している	3.65	4.52	3.78	2.47	2.05	0.74	1.31	1.17	0.44	0.61	0.67	
	4−3	サイバーセキュリティリスクが事業にいかなる影響があるかを推定している	3.69	4.48	3.72	2.79	1.69	0.76	0.93	1.05	0.54	0.70	0.69	
	4−4	サイバーセキュリティリスクの影響の度合いに従って、リスク低減、リスク回避、リスク移転のためのリスク対応計画を策定している	3.51	4.48	3.53	2.42	2.06	0.94	1.11	1.17	0.34	0.56	0.88	
	4−5	サイバーセキュリティリスクの影響の度合いに従って対策を取らないと判断したものを残留リスクとして識別している	3.24	4.57	3.13	1.95	2.62	1.45	1.18	1.74	0.53	0.98	0.68	
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	重要業務を行う端末、ネットワーク、システム、またはサービスにおいて、ネットワークセグメントの分離、アクセス制御、暗号化等の多層防御を実施している	3.78	4.67	3.69	2.95	1.72	0.98	0.74	1.34	0.22	1.09	1.42	
	5−2	システム等に対して脆弱性診断を実施し、検出された脆弱性に対処している	3.90	4.57	3.94	3.11	1.47	0.63	0.83	1.14	0.53	0.87	1.15	成熟度低の平均も相対的に高く、教育に次いで取り組まれている比率が高い。
	5−3	検知すべきイベント（意図していないアクセスや通信）を特定し、当該イベントを迅速に検知するためのシステム・手順・体制（ログ収集や分析のための手順書策定）を構築している	3.78	4.67	3.78	2.79	1.88	0.89	0.99	1.23	0.22	0.73	1.32	
	5−4	意図していないアクセスや通信を検知した場合の対応計画（検知したイベントによる影響、対応者などの責任分担等）を策定している	3.65	4.62	3.75	2.42	2.20	0.87	1.33	1.23	0.33	0.56	0.77	
	5−5	サイバー攻撃の動向等を踏まえて、サイバーセキュリティリスクへの対応内容（検知すべきイベント、技術的対策の強化等）を適宜見直している	3.79	4.52	3.97	2.68	1.84	0.56	1.28	1.03	0.44	0.47	0.74	成熟度中の企業で平均値が高めかつ分散も小さく、成熟度高中の企業ではリスクの継続的見直しへの取組がなされていることがわかる。
	5−6	従業員に対して、サイバーセキュリティに関する教育（防御の基本となる対策実施（ソフトウェアの更新の徹底、マルウェア対策ソフトの導入等）の周知、標的型攻撃メール訓練など）を実施している。	4.29	4.71	4.50	3.47	1.24	0.21	1.03	0.68	0.30	0.44	0.57	平均値が高く、分散が小さい。すなわち、回答した企業において最も達成できている項目である。
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	経営者が定期的に、サイバーセキュリティ対策状況の報告を受け、把握している	3.88	4.67	4.09	2.63	2.04	0.57	1.46	1.25	0.22	0.77	0.86	
	6−2	サイバーセキュリティにかかる外部監査を実施している	2.57	3.67	2.31	1.79	1.88	1.35	0.52	2.11	1.75	1.96	0.69	ISMSやPマークの審査も外部監査の一種とみなせば、実態はもう少し高い数値と考えられる。
	6−3	サイバーセキュリティリスクや脅威を適時見直し、環境変化に応じた取組体制（PDCA）を整備・維持している	3.63	4.71	3.78	2.16	2.56	0.93	1.62	1.65	0.20	0.98	0.87	
	6−4	サイバーセキュリティリスクや取組状況を外部に公開している	2.25	3.43	2.03	1.32	2.11	1.40	0.72	2.24	1.86	2.03	0.53	平均値が人材キャリアパスの設計に次いで低く、中⇔低間のギャップが低めであることから、成熟度中以下の企業ではほとんど達成できてない。
指示７ インシデント発生時の緊急対応体制の整備	7−1	組織の内外における緊急連絡先・伝達ルートを整備している（緊急連絡先には、システム運用、Webサイト保守・運用、契約しているセキュリティベンダの連絡先含む）	3.94	4.71	4.19	2.68	2.03	0.53	1.50	1.22	0.20	0.53	1.16	成熟度中の企業でも比較的達成されている項目。
	7−2	サイバー攻撃の初動対応マニュアルを整備している	3.28	4.57	3.28	1.84	2.73	1.29	1.44	1.87	0.34	1.39	0.45	
	7−3	インシデント対応の専門チーム（CSIRT等）を設置している	3.32	4.71	3.44	1.58	3.14	1.28	1.86	2.50	0.30	1.87	0.77	成熟度中の企業と低の企業を隔てるのは、CSIRTの有無と言えそうである。
	7−4	経営者が責任を持って組織の内外へ説明ができるように、経営者への報告ルート、公表すべき内容やタイミング等を定めている	3.14	4.38	3.13	1.79	2.59	1.26	1.34	1.95	0.71	1.48	0.59	
	7−5	インシデント対応の課題も踏まえて、初動対応マニュアルを見直している	3.17	4.67	3.00	1.79	2.88	1.67	1.21	2.08	0.22	1.38	0.90	成熟度高の企業における平均値の高さは、形だけのマニュアルとしない意識の高さを示すものに思える。
	7−6	インシデント収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行っている	2.81	4.19	2.69	1.47	2.72	1.50	1.21	2.32	1.11	1.78	0.67	成熟度低の企業における実施率が低い点で特徴的。
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	被害が発生した場合に備えた業務の復旧計画を策定している	2.81	4.33	2.59	1.47	2.86	1.74	1.12	2.16	0.98	1.24	0.57	成熟度高の企業の平均が、8−4の復旧対応訓練の値より低いのは不自然。計画はないが訓練はするのか？
	8−2	復旧作業の課題を踏まえて、復旧計画を見直している	2.79	4.43	2.53	1.42	3.01	1.90	1.11	2.22	0.72	1.25	0.56	
	8−3	組織の内外における緊急連絡先・伝達ルートを整備している	3.50	4.57	3.66	2.05	2.52	0.92	1.60	1.83	0.34	1.10	1.31	
	8−4	定期的に復旧対応訓練や演習を行っている	2.61	4.43	2.22	1.26	3.17	2.21	0.96	2.57	0.63	1.73	0.40	全項目中で最も分散値の高い項目。成熟度高の企業でのみ高く、中低で低いことから、復旧対応訓練の実施は成熟度高のパロメータと言えそうである。
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	システム管理などについて、自組織のスキルや各種機能の重要性等を考慮して、自組織で対応できる部分と外部に委託する部分を適切に切り分けている	3.40	4.52	3.53	1.95	2.58	0.99	1.58	1.55	0.34	0.69	0.79	
	9−2	委託先が実施すべきサイバーセキュリティ対策について、契約書等により明確にしている	3.14	4.33	3.00	2.05	2.28	1.33	0.95	1.68	0.89	1.06	0.79	
	9−3	系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先などのセキュリティ対策状況（監査を含む）の報告を受け、把握している	2.86	4.14	2.72	1.68	2.46	1.42	1.03	1.65	0.60	0.95	0.74	
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	各種団体が提供するサイバーセキュリティに関する注意喚起情報やコミュニティへの参加等を通じて情報共有（情報提供と入手）を行い、自社の対策に活かしている	3.85	4.62	3.97	2.79	1.83	0.65	1.18	1.13	0.43	0.66	0.90	
	10−2	マルウェア情報、不正アクセス情報、インシデントがあった場合に、IPAへの届出や一般社団法人JPCERTコーディネーションセンターへの情報提供、その他民間企業等が推進している情報共有の仕組みへの情報提供を実施している	3.17	4.62	3.06	1.74	2.88	1.56	1.33	2.44	0.43	2.00	1.04	分散値が高めの項目。IPAやJPCERTと定期的な連絡関係を持つ企業とそうでない企業での差が顕在化している。