

関連動向

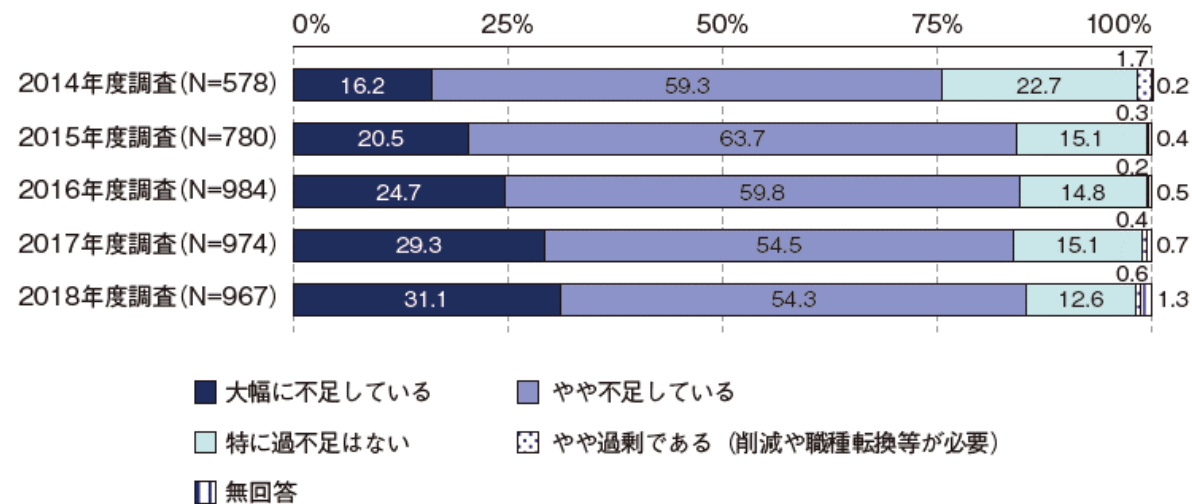
令和2年7月

内閣サイバーセキュリティセンター（NISC）
基本戦略第1グループ

ユーザ企業におけるIT人材、セキュリティ人材の不足

- ユーザ企業のIT人材の“量”に対する過不足感の割合は、「大幅に不足している」についての上昇幅は小さくなっているものの、年々高くなる傾向が続いている状況（2018年で31.1%）。

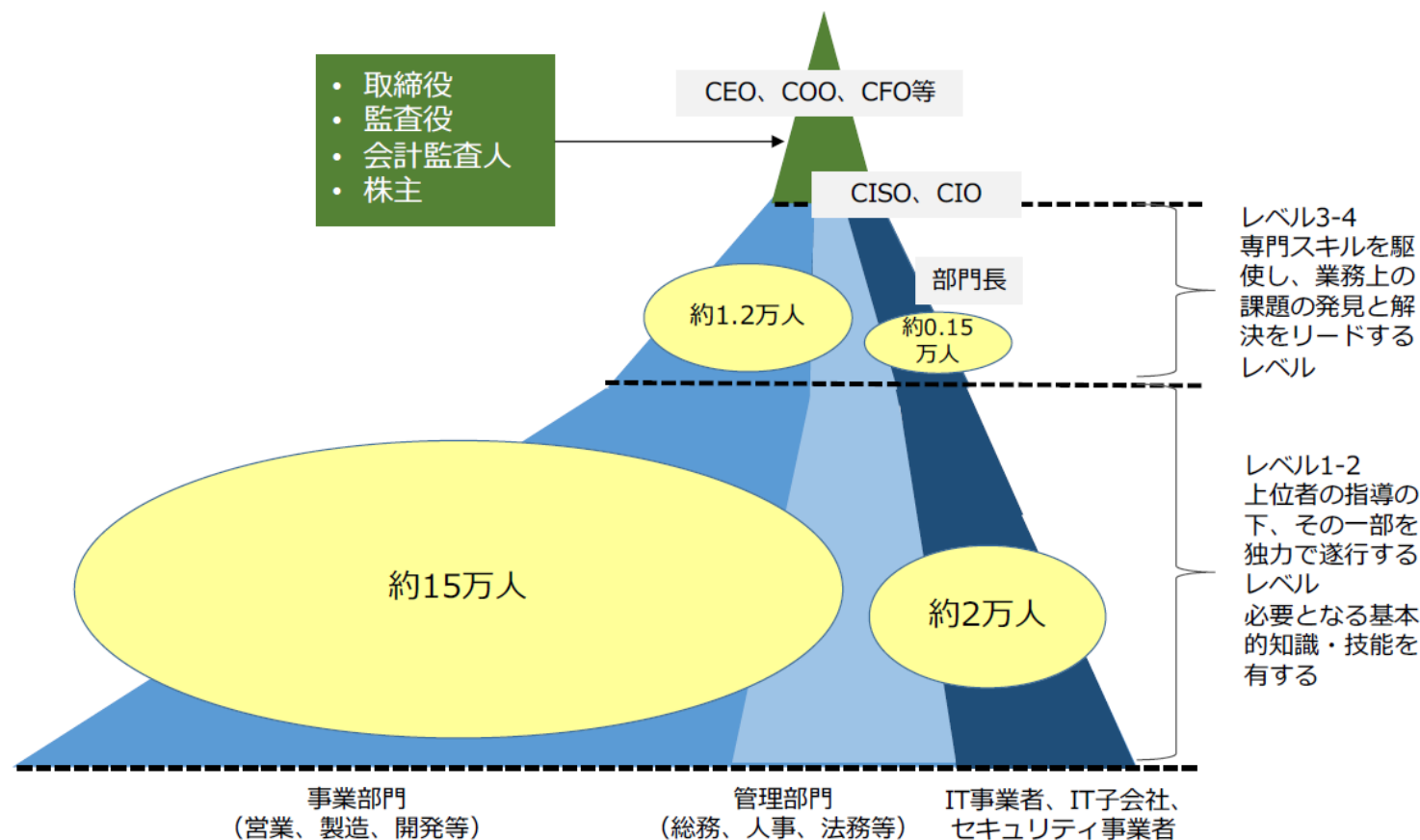
図表3-2-14 ユーザー企業のIT人材の“量”に対する過不足感【過去5年間の変化】



出典：独立行政法人情報処理推進機構「IT人材白書2019」（2019年5月24日）より

セキュリティ人材の不足

- 国内のセキュリティ人材の不足は、いわゆるユーザ企業（事業部門及び管理部門）において顕著。

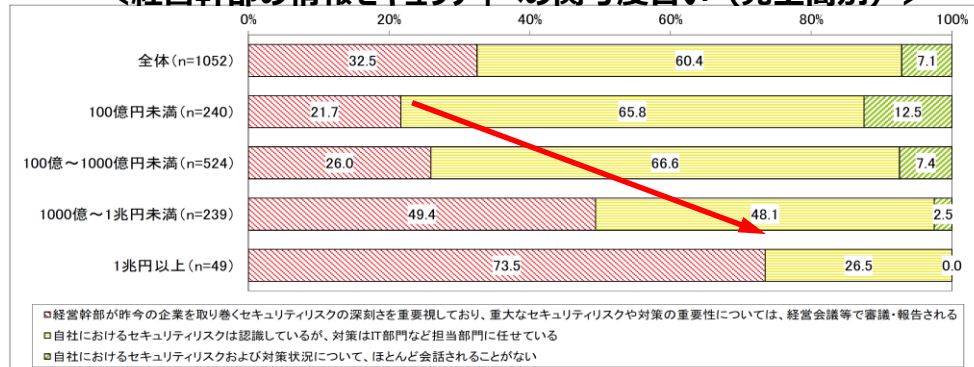


図表 5 セキュリティ人材不足数の各部門とスキルレベルとのマッピング

大企業の状況

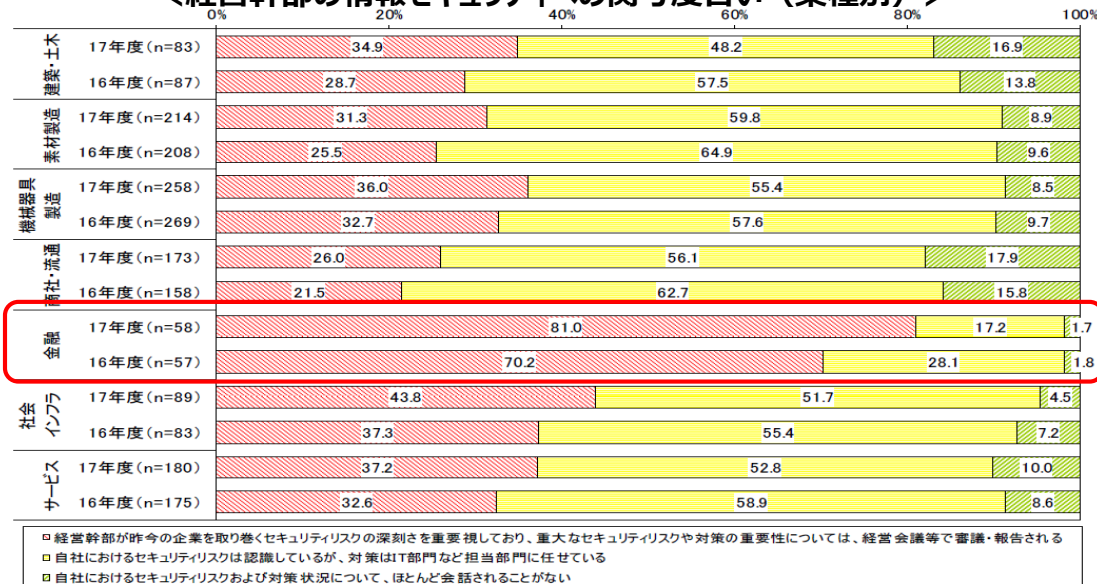
- 売上規模別でみると、売上の高い企業ほど、経営幹部のセキュリティへの関与の度合いが高い。また、業種別では、金融業が最も関与の度合いが高く、約 8 割の企業でセキュリティ対策の重要性が経営会議等で審議・報告されている。
- 経団連が、2018年 3 月に「経団連サイバーセキュリティ宣言」を公表しているほか、経営層を対象としたトップセミナーを開催するなど、サイバーセキュリティ対策の推進に向けた積極的な取組が進められている。

＜経営幹部の情報セキュリティへの関与度合い（売上高別）＞



(出典) 企業IT動向調査報告書 2016 (一般社団法人 日本情報システム・ユーザー協会)

＜経営幹部の情報セキュリティへの関与度合い（業種別）＞



(出典) 企業IT動向調査報告書 2018 (一般社団法人 日本情報システム・ユーザー協会)

＜経団連サイバーセキュリティ経営宣言＞

(2018年3月、日本経済団体連合会)



2018年3月

一般社団法人 日本経済団体連合会

最新テクノロジーとデータを活用して社会全体の生産性向上と課題解決を図る「Society 5.0」に向け、あらゆる場面でITとの融合が進む一方、サイバー空間の秩序や安全に脅威を与える、著しい悪意を持った行為も多発している。いまやすべての企業にとって価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題となっている。

重要インフラの多くを担い、さまざまな製品やサービスを提供する経済界は、主体的に対策を講じる必要性を強く自覚する。

経済界は、全員参加でサイバーセキュリティ対策を推進し、安心・安全なサイバー空間の構築に貢献する。サイバー攻撃が激化する 2020 年の東京オリンピック・パラリンピック競技大会までを重点取り組み期間として、以下の事項の実践に努めることを宣言する。

1 経営課題としての認識

- 経営者自らが最新情勢への理解を深めることを怠らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組む。
- 経営者自らが現実を直視してリスクと向き合い、経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組む。

2 経営方針の策定と意思表明

- 特定・防衛だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けたBCP(事業継続計画)の策定を行う。
- 経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に自主的に記載するなど開示に努める。

3 社内外体制の構築・対策の実施

- 予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じる。
- 経営・企画管理・技術者・従業員各層における人材育成と必要な教育を行う。
- 取引先や委託先、海外も含めたサプライチェーン対策に努める。

4 対策を講じた製品・システムやサービスの社会への普及

- 製品・システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努める。

5 安心・安全なエコシステムの構築への貢献

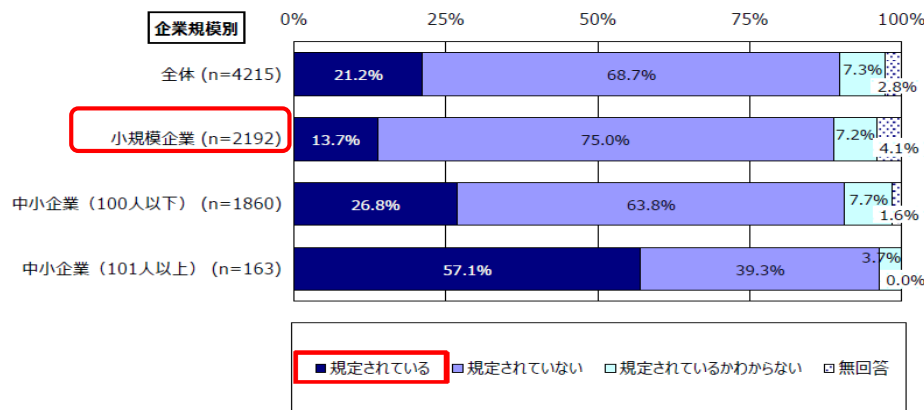
- 関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図る。
- 各種情報を踏まえた対策に関して注意喚起することによって、社会全体のサイバーセキュリティ強化に寄与する。

DECLARATION OF CYBER SECURITY MANAGEMENT

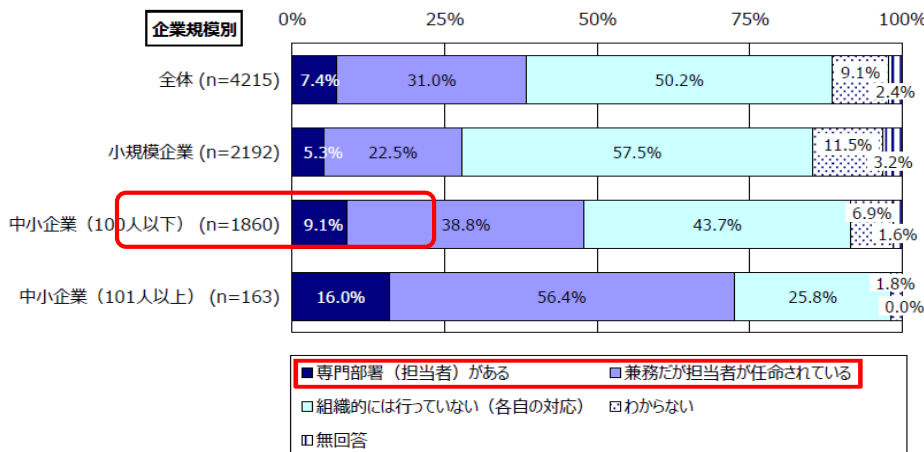
中小企業の状況

- 中小企業では、特に規模の小さい企業ほど、情報漏えい等への対応方法が規定されていない状況。また、サイバーセキュリティに関する専門部署や担当者が置かれていない場合も多い。
- 社内でのサイバーセキュリティ教育についても、「特に実施していない」との企業が全体の約 6 割を占める。

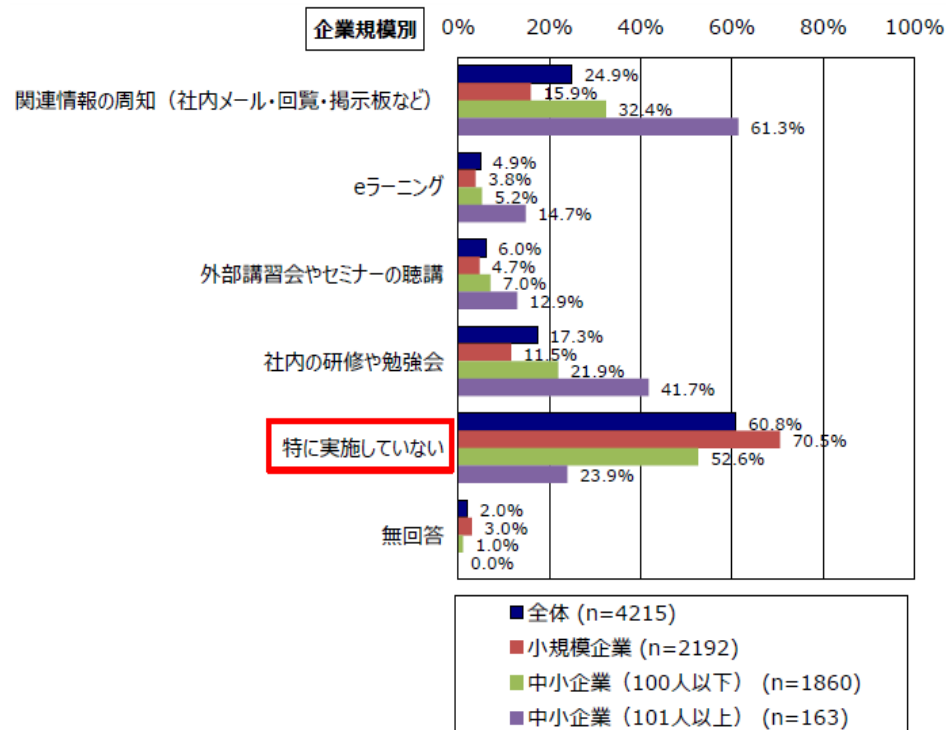
＜情報漏えい等への対応方法に関する規定の有無＞



＜情報セキュリティ対策に係る専門部署または担当者の有無＞



＜社内での情報セキュリティ教育の状況＞



（出典）IPA 2016年度中小企業における情報セキュリティ対策に関する実態調査報告書（2017年3月30日）より