最新セキュリティマネジメント（第5回）

# サイバーセキュリティ対策のための資源確保

2021.10.19

経済産業省が策定した「セキュリティ経営ガイドライン」で、経営者が社内に指示すべきポイントとして示された「重要10項目」。今回は3番目の項目となる「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」について解説する。

## 管理体制構築の進め方

経済産業省と独立行政法人情報処理推進機構（IPA）が共同で策定した「サイバーセキュリティ経営ガイドライン Ver2.0」では、企業のIT活用を推進する上で経営者が認識すべきサイバーセキュリティに関する原則や、経営者がリーダーシップをもって取り組むべき項目がまとめられている。

本ガイドラインで示された方針を踏まえ、経営者はセキュリティ対策に関連する業務を担当する人材を選出するとともに、対策に必要な予算を確保していくことになる。そこで今回は、サイバーセキュリティ対策のための資源確保について解説する。

## すべての部署が「当事者」に

近年、大きなビジネス上の課題となっている「人材不足」。業種や職種を問わず、さまざまな企業で必要な人材が十分確保できない状況が発生している。中でも専門的な知識、経験が求められるセキュリティ分野では、採用から育成に至るすべてのシーンで不足が深刻化しているのが現状となっている。

企業でセキュリティ対策の中心となるのは、全体的な取り組みを管理する「セキュリティ統括」分野や、関連するタスクを担う「セキュリティ監視・運用」分野だ。一方、情報処理推進機構が実施した調査によると、日本のユーザー企業で専任のCISO（最高情報セキュリティ責任者）を置いているのは全体の7.5%、インシデントへの対応を行うCSIRT（Computer Security Incident Response
Team）に1名以上の専任メンバーを配置している企業は31.1%で、多くの場合は他業務と兼務する形になっている。

また、JUAS（日本情報システム・ユーザー協会）の調査では、マネジメントレベル、および実務レベルのセキュリティ人材不足が大きな課題になっていることも示されている。このため、まずは担当者がセキュリティ業務に専念できる環境をつくるとともに、対策実施に求められる専門的なスキルの習得や向上などを進める必要がある。

## 「セキュリティ統括機能」の役割… 続きを読む