企業におけるサイバーセキュリティ対策に関する考察 -セキュリティ人材育成-

Study on the Cybersecurity measures for private sector

梅木久志・法制倫理分科会・情報セキュリティ大学院大学

With the rapid expansion of cloud computing and IoT devices, the network environment of enterprises is changing. Cyber-attacks are becoming increasingly sophisticated and diversified, and not only the IT system department, which has been mainly engaged in corporate cyber security measures, all stakeholders need to tackle cyber security measures. In this study, the goal is to propose the best practice to serve as a reference for Cybersecurity measures in private sector with taking an on-site viewpoint.

背景・課題

■ 政府やシンクタンクなどの調査結果によると、日本ではサイバーセキュリティ人材が不足しており、人材育成が急務となっている

✓ 具体的にどのようなスキルや知見を有した人々が足りないのか明確化されていない

■ IoT技術の普及等により，サイバー空間と実空間の融合が加速、社内の様々なデバイスがネットワークに接続

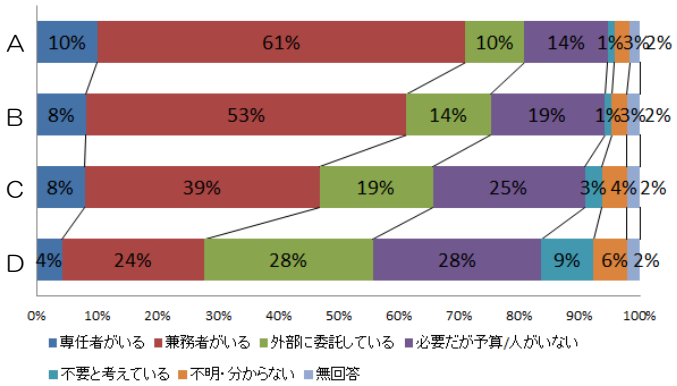
✓ これまで主にセキュリティ対策を行って来た情報システム部門だけでなく、現場でのセキュリティ対応も必要

情報セキュリティ調査

■ 情報セキュリティに関わる業務の担当者の有無に関する調査を実施

- 調査対象：日本国内のPマーク取得組織、ISMS認証取得組織、官公庁、教育機関から選んだ4,500組織（回答429件(9.5%)）
- 調査期間：2017年7月22日～10月31日
- 調査方法：調査票の郵送によるアンケート調査

《情報セキュリティ業務の担当者はいますか？》

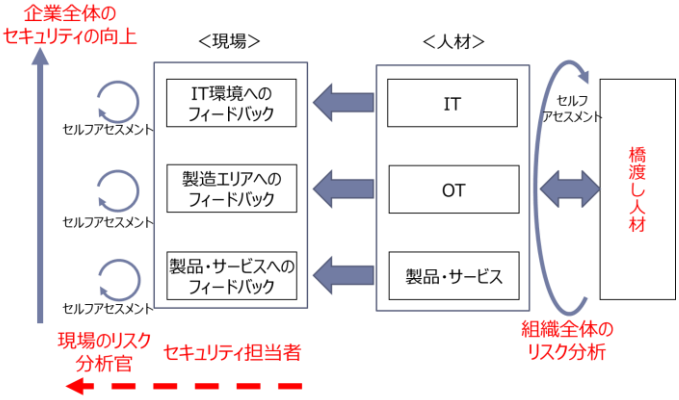


A：インシデント対応の全体を管理し、指揮命令ができる技術者
B：セキュリティ教育や啓発など、リテラシー向上を行うことができる技術者
C：セキュリティポリシーやセキュリティ設計などが正しく実装されているかを評価、確認できる技術者
D：ウイルスの解析やフォレンジック調査などができる技術者

人材育成の仕組み作りの提案

■ 部署毎のセキュリティ人材では全社の観点でリスク(マネジメント)を考えることができない

■ 部署毎のセキュリティ人材＋全社的な視野でリスクを考える人材育成の仕組みが必要



「情報セキュリティ調査」結果
- セキュリティ業務の担当者は兼務者が多い
- 必要性は認識していても予算／人の確保が困難

今後の研究活動

➢ 部署毎のセキュリティ人材＋全社的な視野でリスクを考える人材育成の仕組み作りの検討

➢ セキュリティキャリアパスの検討
(キャリアパスの形成により人材育成が推進？)