情報通信委員会

3月3日(金)広島市において、約40名の出席(現地＋オンライン)のもと、2022年度情報通信委員会を開催しました。

当日は、NTTコミュニケーションズ株式会社のエバンジェリスト竹内文孝氏によるご講演の後、当委員会の2022年度事業報告案および2023年度事業計画案を審議し、原案どおり承認されました。ここでは、講演の概要を紹介します。

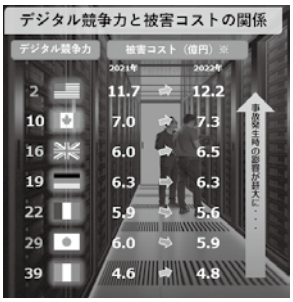
〔講演要旨〕

「これからの経営基盤を守るサイバーリスクマネジメント～新常態の企業文化を醸成し、競争力を最大化するために～」

NTTコミュニケーションズ株式会社
プラットフォームサービス本部マネージド＆セキュリティサービス部
セキュリティサービス部門 部門長
竹内　文孝 氏

■デジタル化とセキュリティ対策は両輪

SDGsやコロナ等への対応として、リモートワーク等のデジタル化が進んでいるが、デジタル競争力が高いほどセキュリティ事故の被害コストが大きく経営へのインパクトが大きいため、デジタル化とセキュリティは両輪で取組む必要がある。



※1ドル：130円、一つの情報漏洩事故が発生した場合の平均コスト

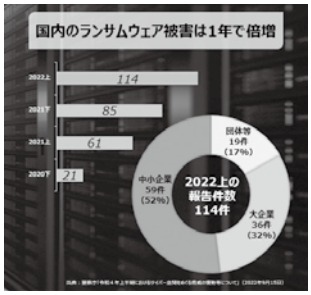
【セキュリティ事故が及ぼす経営インパクト】
(出典：情報通信委員会資料(一部加筆))

■セキュリティ事故はどこでも起こり、リモート接続環境の弱点が狙われる

以前は大企業が狙われる感覚だったが、ランサムウェア※の被害報告件数をみると中小企業が半数を占めている。

※ランサムウェアとは、暗号化することでファイルを利用不可能な状態にした上で、そのファイルを元に戻すことと引き換えに金銭(身代金)を要求するマルウェア

攻撃者は、リモート接続環境の弱点の一つであるシステム構成品の欠陥(脆弱性)を狙っている。脆弱性は、システムの機能向上等により発生し続け、ユーザにて予防できないため、修正プログラムを都度あてて、弱点をふさいでいくしかない。



【ランサムウェアの被害報告状況】
(出典：情報通信委員会資料)

脆弱性の放置により200日以上気付かずに攻撃され続け、被害が拡大した事例もあるため、脆弱性管理は重要である。

■セキュリティアウェアネスの底上げ

攻撃は巧妙化しており、100%の防御を狙うのではなく、インシデントは起こることを前提に被害の最小化を目的に対策することが大切である。その一つとして、攻撃メール訓練等により、企業文化を醸成するセキュリティアウェアネスの底上げ(セキュリティ意識の向上)が有効である。

【企業文化を醸成するセキュリティアウェアネスの底上げ】
(出典：情報通信委員会資料)

セキュリティ対策を、会社を強くする戦略的な投資に位置づけ、各リスクを可視化し、優先度をつけて取組んでいただきたい。

(担当：中本)