産業技術委員会

２月17日（月）広島市において、87名出席のもと、産業技術委員会を開催した。

当日は、議事に先立ち国立大学法人大阪大学猪俣教授から講演をいただいた後、産業技術委員会の2019年度実施結果、2020年度中期事業計画（アクションプラン）・事業計画（案）について報告・審議を行い、原案どおり承認された。

〔講演要旨〕

「企業における情報セキュリティへの対応」

国立大学法人　大阪大学
教授　　猪俣　敦夫 氏

■記憶から忘れ去られる漏洩事件といつまで経っても消えない漏洩事件

企業による情報漏洩事件は多数発生しているが、人の記憶から忘れ去られるものと、いつまで経っても記憶から消えないものがある。その違いは、私が作った造語で「情報のTime to Live」すなわち“情報の生存時間”が関係している。例えば、50歳の人の個人情報は30年程度の生存時間だが、子供の場合は生存時間が長く、人の記憶に残るものと考える。この生存時間は情報価値（お金）にも関係しており、生存時間が長い情報ほど価値は高い。

漏洩した個人情報は、“ダークウェブ”といわれる、通常ではアクセスできないネット上で売買されている。

■情報セキュリティの３大要素CIA

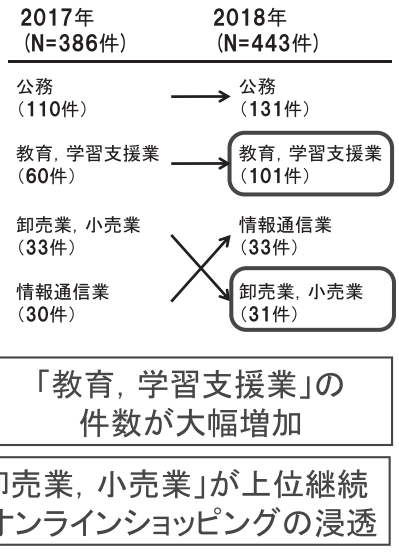
セキュリティ試験で必ず出題される「セキュリティ３大要素CIA」がある。C(Confidentiality)は、機密性を意味しており、「情報が漏れないこと」。I（Integrity）は、完全性を意味しており、「情報が保存された時点のまま、その状態で維持されること」。A（Availability）は、可用性を意味しており、「情報へのアクセスを認められている人（もの）が情報を利用したい時に利用できること」である。

またCIAには、「否認防止」という非常に重要な考え方がある。否認防止とは、「インターネットなどで利用者が事後になってその利用事実を否定することができないように証拠を残すこと」で、暗号技術により実現されている。

■2018年のインシデント事例

毎年、特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）が、１年間に発生したインシデント事例を公表している。業種別の発生割合では、情報資産価値

【業種別漏洩件数】

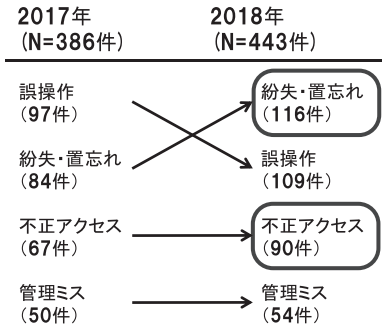


©JNSA　2018年情報セキュリティインシデントに関する調査報告書（報告）より

が高い（＝個人情報）「公務」「教育、学習支援業」「情報通信業」「卸売業、小売業」の順になっている。

原因別では、「紛失・置忘れ」「誤操作」「不正アクセス」の順となっている。ここでいう「不正アクセス」は、企業が施している堅牢なセキュリティを突破したものではなく、容易に想像できるパスワードの設定や、パスワードをかけていないことに起因するものである。

【原因別漏洩件数】



「紛失・置忘れ」「不正アクセス」の件数が増加

「紛失・置忘れ」「誤操作」「不正アクセス」3大原因（約70%）

©JNSA　2018年情報セキュリティインシデントに関する調査報告書（報告）より

■「リスク」と「安全」

リスクの定義は、「段階（レベル）で示されるものであり『安全』な状態との間の『中間的な領域』を含めて表現」という非常に曖昧なもの。つまり、リスクとは概念的なものであるため、「特定せよ」という話もあるが、無理なこと。リスク低減はシステムだけでは不可能で、人の判断も必要となることから、人の教育が不可欠となる。

次に安全とは、「許容できないリスクの無いこと」である。法律上の問題を例にあげると、外資系企業が提供するクラウドサービスは安価で非常に便利だが、問題が発生した場合、日本の法律に準拠していないため、対応してもらえないことがある。このため、安全を担保するには、たとえ安価で運用実績があったとしても、企業の機微な情報を外資系企業クラウドに預けるには十分な検討が必要である。

■「リスクアセスメント」と「リスク対応」

リスクアセスメントとは、「守るべき情報資産に対するリスク発生確率や発生した時の影響度を測る指標」のことである。

このため、適切なセキュリティ対策を施すには、事前に情報の価値を把握しておく必要があり、情報の棚卸しが必要となる。

また、リスク対応では、PMBOK（Project Management Body of Knowledge）というプロジェクトマネジメントの手法がある。PMBOKで重要なことは、「回避」「移転」「低減」「受容」の４つである。

■産業システムへのIoT技術の展開

現在、第４次産業革命と位置づけられ様々なプロジェクトが進行している中、外部ネットワークと産業機器の接続が増加している。これはサイバー攻撃を行いやすい環境を自ら作り出していると言える。情報システムの更新周期は３～５年程度だが、安定性や確実性を求められる制御システムは更新周期が10～20年と非常に長いことから、特に工場を持つ産業はシステムの安定稼働のため、セキュリティ意識を持つことが重要である。

■まとめ

最後に、情報セキュリティでは、脅威ばかりフォーカスすると肝心の事業を見失うことがある。これを回避するには、日頃から経営層のリーダーシップの下、情報資産の棚卸しを行い適切な情報セキュリティ対策を実施することが重要となる。情報セキュリティが生み出す最大価値は「０」、すなわち、何もなくて安心であることが最大の価値である。

（担当：菅原）