「情報化された組織のセキュリティマネジメントWG」

活動報告

只木　進一
佐賀大学総合情報基盤センター

大学・研究機関の教育、研究、診療、組織業務のいずれもが、情報基盤への依存度を増している。それは同時に、セキュリティの脅威も増していることを意味している。「情報化された組織のセキュリティマネジメントWG」は、「教育研究機関におけるICT部門の事業継続計画」、「情報漏えい対策」、「セキュリティ向上を主眼とするDNS設定」をテーマとして活動を行い、報告書をまとめた。

業務のICT化が進んだ結果、情報基盤が失われた際の業務への影響は非常に大きい。そのため、情報基盤を担当する部署だけでも、先行して事業継続計画を持つことが必要と考えられる。事業継続計画を策定するための準備についてまとめを行った。また、事業継続計画の策定過程は、情報部門の業務の棚卸ともなる。その結果、日常的な保守業務に役立つ成果物が得られる。

また、本WG活動中の2011年3月に東日本大震災が発生した。この時、及びその後の計画停電実施期間中に、東北地方及び関東地方の大学等の情報部門にどのような被害があったかをアンケートとして調査させて頂くことができた。その結果についても報告書にまとめ、今後の対策の参考とさせていただくこととした。

大学・研究機関では、電子化された様々な機密情報が扱われている。一方、そのような情報に接する人数が多いため、情報漏えいのリスクが大きくなっている。そこで、情報を持ち出させない対策、誤って持ち出した場合の対策、条件を定めて持ち出すための対策について、検討を行った。利用できるデバイスや外部サービスが急速に変化しているため、継続的な検討が必要な課題である。

ホストの名前とIPアドレスを結びつけるDNSは、ネットワークサービスの基本である。クライアントは、DNSから得られた情報に従ってサービスに接続する。近年、DNS情報に偽情報を混入させることで、フィッシングサイトへ誘導したり、DoS攻撃を行ったりする事例が報告されている。そうような不正書き換えを受けないためのDNSの配置、設定について調査した。また、状況を把握するためのログ管理手法について整理した。