3.1. セキュリティマネージメントのための組織

大学における教育、研究、医療、そして組織運営の全てにわたって情報技術が不可欠な要素となっています。情報ネットワーク、情報システム、そしてその上に保有されている様々な情報は、まさしく大学の基盤を構成しています。こうした情報とシステムの有効活用は、組織の活性度や効率性を左右します。

一方で、コンピュータウィルスや情報システムへの様々な不正侵入によるセキュリティ脅威も日増しに大きく、社会問題にもなっています。コンピュータウィルスというと、コンピュータを管理する個人の問題のように矮小化されがちですが、そこで失われる、あるいは漏えいする情報が、個人情報漏えいなどとなり、組織に大きなダメージを与える場合もあります。

大学の情報システム、情報資源を守り、情報化による恩恵をうけるためには、組織的な対応が不可欠です。情報セキュリティの基本を定めるセキュリティポリシーの策定、そのポリシーに基づいた安全な情報システムの構築、そしてそのポリシーの遵守状況の確認のためにも、日常的な情報セキュリティマネージメント体制が必要です。情報漏えいや不正侵入などの事故に際しても、迅速かつ的確に対応するための非常時用体制を日頃から整えておく必要があります。

セキュリティポリシーは、主に日常的なセキュリティ維持・向上のための基本方針を定めるものです。セキュリティに関する責任者などの人的体制、セキュリティに関する教育体制、ポリシーの遵守状況の監査、情報の重要度を定めそれぞれの扱いを定めるための基本、情報システムの構築・運用の基本となる認証、権限管理、アクセス制限などを定めます。政府統一基準、高等教育機関向け規定集などのセキュリティポリシーの雛形が利用できます。また、雛形があれば、コンサルティングなどの手助けを受けることも可能となります。

セキュリティポリシー及びそれに基づく規程類を一度に完全にすることはできません。実施できないものを定めることで、かえってポリシー違反を誘発することもあります。策定、実施、そして見直しのサイクルを繰り返すことで、セキュリティ維持のレベルを上げることを考えるべきです。

情報漏えいや不正侵入などの事故は、無いにこしたことはありませんが、起きたときのための準備は必要です。発見者の通報義務、連絡網、緊急待避対策、対応体制を整備しておく必要があります。対外的な対応体制も必要です。文部科学省、IPA、警察などへの報告手順、必要に応じた記者会見、捜査への協力の基準なども定めておくべきです。また、緊急避難のためにネットワークを切断したりシステムを停止する必要があります。その時の責任体制を明確にする必要があります。特に、現場の技術担当者に過剰な責任を負わせない必要があります。IPA や JPCERT に対応マニュアルがあります。

情報セキュリティは技術だけでは守れません。情報システムの利用者の一人一人が注意しなくてはなりません。そのため、情報セキュリティに関する教育が重要となります。利用者への教育だけでなく、システム管理者そしてシステム発注者への教育が必要です。IPA からの資料が利用できます。

近年、ノートブック型パーソナルコンピュータが普及しています。また、様々なタイプの外部記憶装置も活用されています。このようなものを活用して、場所を問わずに活動するユビキタス環境は確かに便利です。しかし、同時に情報セキュリティにとって大きなリスクでもあります。セキュリティ対策としては、こうしたユビキタス環境との調整行う必要があります。この問題は、働き方の問題にも踏み込む難しい問題です。

情報セキュリティ対策を考えると行うべき業務が限りなく膨らみそうです。何のための情報システムかを見失うかもしれません。そこで情報システムに対する考え方の転換が必要に思われます。私たちが必要なのは情報システムのサービス・機能であって、システムそのものでは無いはずです。箱物としてのコンピュータの数を減らす、シンクライアントなど機能を絞った端末を活用する、情報を整理して共通化する、サービスを外注するなど、積極的な方向転換が必要な時期に来ています。