第５分科会Ｂグループ　報告
－「安心安全な情報システム環境の提供」－

１．テーマの検討

Ｂグループに所属したメンバーにおいては、本講習会に臨むにあたって、事前に検討を行った自大学の課題として、学内の情報セキュリティ対策の必要性（ルールの制定、教職員の意識改革等）を挙げていた。

各メンバーが、共通した課題として認識していた事から、まず情報セキュリティ対策をどのように進めていくべきか、という観点で、テーマの検討を行っていく事とした。

まず始めに、現状の把握のため、各校で起きている情報セキュリティ事故につながりかねない利用実態を確認する事から検討を開始した。ここでは、様々な利用実態が挙げられ、メンバーの認識として、このままでは問題になる、という事を再認識した。

そこで、情報システム部門としてどのような対応が可能か、討議を行っていく事とした。当初の議論の中では、主に利用者側の意識の問題を重要視し、どのように意識付けを行っていくかという点に注視して、検討を重ねていった。

その中で大きく課題として挙げられたのが、**情報システム部門の位置付け**になる。経営層として、情報セキュリティに対する認識を強く持ち、大学としての意向を学生・教員・職員に浸透させる事が必要であるのではないかとの議論となった。この点に着目し、初期のテーマとして、**「情報システム部門のあり方」**を設定する事とした。

２．目的（テーマ）の掘り下げ

情報セキュリティ対策が必要という認識の上で、なぜ対策が必要なのか、対策を行わなかった場合に、どのような事象が発生するか、具体的な内容について、討議を進めた。

その結果、情報事故が発生した場合、どのような問題が発生し、それがどのように大学に影響を与えるかを認識した。

表 1 問題とその影響

問題	想定される影響
情報の流出（紛失）	志願者・入学者の減少（大学としての収入減）
	マスコミ対策、謝罪対応等による費用の発生
	対応のための職員稼働の増加（肉体的負荷、精神的苦痛、人件費の増加）
	流出者当人の社会的地位の降下
情報の消失	事業継続の停止
	復元のための作業コストの発生
機能の停止	事業継続の停止
システムの乗っ取り（破壊）	事業継続の停止
	不適切な情報の発信

このように、情報事故が発生した場合、大学として「信頼」「お金」「時間」といった損失が発生する事が確認出来た。これらの損失は、大学運営において、非常に大きな痛手となり、運営継続にもかかわってくる事だと言える。

上記を踏まえた上で、情報システム部門に対しては、単なるシステムの運用・保守という立場だけではなく、**「信頼を確立し継続した大学運営の実現」**が求められているのではないかと確信するに至った。

それに伴い、本検討の目的（テーマ）も、単に情報システム部門の在り方を論ずるのではなく、**「安心安全な情報システム環境の提供」**を目的として、対策の検討を進めていく事に変更を行った。

３．対策の検討

対策を検討するにあたって、前項で記載した４つの問題が何故発生するのか、原因を追究する事とした。

その結果、原因として大きく「人的問題」「システム的問題」「災害対策」の３つに分類されるのではないかとの結論に達した。

表 2 問題の分類

分類	想定される原因
人的問題	ルールが明確化されていない（セキュリティポリシーがない）
	ルールが守られない
システム的問題	守るべき情報資産が整理できていない
	影響範囲が明確化されていない
	ソフトウェアのアップデート方針が確立されていない
災害対策	災害時の業務継続計画が制定されていない
	データの遠隔バックアップ等保全計画が存在しない

むろん、これらの原因に関しては、大学ごとに異なる状況であるため一概に同一視出来るものではないが、各校とも何かしらこのような課題を抱えているのではないかと考える。その上で、これらの課題に対して、具体的な対策の検討を行った。

対策の検討にあたっては、検討時のポイントとして、出来る限り、システム管理者目線ではなく、学生・教職員等のユーザ目線に立った形で、進める事とした。情報セキュリティ事故を起こすのが（ルールを守らないのが）守りたくないから守らないのではなく、使い勝手や実運用の点で、効果的だからという事も考えられるためである。

その結果、対策のアウトラインとして、以下の点を柱として、対策を進めていく必要があるとの結論に達した。

(1) ユーザのセキュリティ意識向上（情報事故に対する認識の強化）

・情報セキュリティ講習会、試験の実施（継続的な啓蒙活動）

(2) 情報資産の把握・整理

・保護すべき情報の整理、バックアップ体制の確保

(3) ユーザニーズの把握

・利用者目線で、使い勝手とセキュリティの両立を目指す

(4) セキュリティ対策の確実な実施

・教職共同で、トップダウン的に施策を実施できる体制の確保（情報セキュリティ委員会の設置等）

４．最後に

当初は、情報セキュリティ対策は大事だという（暗黙の）認識の元で、情報セキュリティ対策をどのように実現していくか、という点にとらわれ過ぎていた。しかし、そもそも何のために対策を行うのか、対策を行わない場合に大学に対してどのような影響があるのか、じっくりと考えることができた。

大学という組織は、非常に多くの関係者（学生・保護者・教員・職員・OB・関係企業等）が存在している。重大な情報セキュリティ事故を起こす事は、その関係者に対し多大な迷惑をかける事になり、大学運営にも多大な影響を及ぼす為、情報システム部門としてその存在意義は大きいと考える。

情報システム部門に所属する我々としては、その事を念頭に置いた上で、まずはできる部分から業務改善に継続的に取り組んでいく必要があると考える。大学ごとに、環境も、業務内容も異なる部分も多いが、今回の講習会を通じて、共通の認識を持つことができた。

以上