特集　情報セキュリティ

経営執行部（役員）の情報セキュリティに対する取り組みについて

サイバー攻撃などによる情報セキュリティの問題は、一大学の問題に留まることなく社会・経済全体にも波及する可能性があることから、大学・法人の全構成員が意識を共有し、組織的に取組むことができるよう経営執行に携わる役員のリーダーシップが極めて重要となっています。そこで、情報セキュリティに対する取組みについて、大学法人全体としての問題意識の共有化、学内ルールの確立、教職員に対する教育・訓練、運営体制などのマネジメントを遂行するための役割・責任の範囲・内容に関して経営執行部として以下の視点で振り返る必要があります。

1．サイバー攻撃による情報資産・金融資産の脅威やインシデントに対する危機意識の共有化を推進

※　危機意識の共有化を推進していくには、法人組織（理事会）でサイバー攻撃の防御を全学的な課題として捉え意思決定しておくことが望まれる。

※　全学的に展開していくためには、担当役員もしくはそれに準ずる法人・大学執行部の関係者を配置し、法人及び大学の構成員全員にサイバー攻撃による脅威の認識を徹底する必要がある。

※　脅威を周知徹底していくには、構成員一人ひとりがサイバー攻撃や情報セキュリティの確保に向けて意識の持続化を図るとともに、振り返りをさせる仕組みが必要となる。

※　構成員一人ひとりによる自己点検・評価の結果を踏まえて、全学的な取り組みについて見直し・改善する仕組みが必要となる。

2．学内ルール（情報セキュリティポリシー、情報資産の把握など）の構築と周知徹底

※　法人・大学の危機管理の一部として情報セキュリティポリシーに関する取り扱いの判断基準を構築するとともに、構成員全員にサイバー攻撃から法人・大学の情報資産・金融資産を守るために最小限度の行動基準に関するガイドラインを作成し、理解の徹底を図る必要がある。

※　そのためには、法人・大学の構成員一人ひとりが利用または作成する情報資産の所在を明確にし、被害の重大性を想定して情報資産別に防御の仕方を共有しておく必要がある。また、請負業者についても情報セキュリティに対する問題意識を職務責任として契約などで明確にしておく必要がある。

※　なお、攻撃を受けたときの緊急対応としては、被害の拡大を防ぐために別途ネットワークの切断などの初動対応について予め定めておく必要がある。

3．情報セキュリティ委員会、情報センター等部門による防御体制の構築と点検評価の徹底

※　防御体制の組織としては、担当役員もしくはそれに準ずる法人・大学執行部による統括責任者の配置、防御に関する全学的な取り組み対策のとりまとめや点検・評価のガイドラインなどを検討する情報セキュリティ委員会の設置、防御の実施と点検・評価の徹底を働きかける情報センター等部門の充実が求められる。

※　防御体制を実質的に機能させていくためには、統括責任者の役割と権限を明確にした上で、情報セキュリティ委員会が危機管理マネジメントの内部統制組織として機能できるよう位置づけを確保する。また、委員会の下でガイドラインに沿って構成員一人ひとりに防御行動を働きかけるとともに緊急対応としてのインシデントに対応する情報センター等部門の役割と権限を強化しておく必要がある。

４．教職員に対する教育や模擬訓練の実施とその徹底

※　大学構成員一人ひとりに防御意識を持たせて対応できるようにするには、担当役員もしくはそれに準ずる法人・大学執行部の関係者による全学的な呼びかけによる危機管理研修が不可欠である。

※　研修は、サイバー攻撃の事例を通じて脅威に関する認識を持たせるとともに、脅威に遭遇したときの緊急対応について関連知識の活用を模擬訓練などにより修得させる。

※　その際、最小限度心がけておくべき対応として、不審メール見極めの模擬訓練を体験させることを通じて、ウイルス拡散、機密情報の外部への漏えい、システムの破壊など想定される被害について知識の共有を図るとともに被害を防止する意識の向上を図る。また、被害の拡散を防ぐための対応として速やかに相談・連絡する手順を修得させる。

情報セキュリティのベンチマーク評価と改善取り組みのガイドライン

１．ベンチマーク評価の導入

サイバー攻撃の被害に合わないようにすることは難しいですが、被害の拡大を防ぐための対策を法人及び大学全体で整備していく必要があります。とりわけ、大学には教員、職員、学生、企業などの関係者が多数関っており、情報の取り扱いや管理運用、緊急対応を一元的に管理することが難しい状況にあります。

そのため、まず法人・大学を構成する教職員が情報セキュリティの現状を把握し、攻撃による被害を想定した危機意識の共有が必要となりますが、その一つの手段として、情報セキュリティへの対応状況を自己点検・評価するベンチマークがあります。

ベンチマークでは、経営執行部との関りの中で、情報セキュリティ対策が一貫して展開されているか否か振り返ることにより、不足している取組みを抽出し、改善に向けて組織的に計画・行動できることを目指しています。評価の重み付けするために、点検項目を４つの視点で構成しました。内容は、全学的に攻撃の脅威を認識できるように危機意識の共有を最重視しました。その上で、情報資産の把握、組織的な対応、技術・物理的対応との関係性を照合することにしました。

第１部の「経営執行部の情報セキュリティに対する取組み」では、全学的に攻撃の脅威を認識する危機意識の共有化を最重視しました。その上で学内ルールの徹底、防御体制の構築、それを実現するための予算化の点検としました。

第２部の「重要な情報資産の把握と管理対策」では、金融資産情報を含む重要な情報資産の目録作成を最重視しました。重要な情報資産とは、例えば、入試情報、学生の学籍・成績等の個人情報、マイナンバーを含む教職員の個人情報、研究情報、IR情報、業務システム、卒業生・保護者情報、部門外秘情報などです。その上で、重要な情報資産に対するアクセス制御・リスク評価の実施と重要な情報資産の入手から破棄に関るデータ管理の点検としました。

第３部の「組織的・人的な対応」では、脅威となる事象に対応した組織の設置を重視しまし