経営執行部の情報セキュリティに対する取組み

サイバー攻撃などによる情報セキュリティの問題は社会・経済全体にも波及する可能性があることから、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。

1．サイバー攻撃による情報資産・金融資産の脅威に対する危機意識の共有化を推進

※　理事会でサイバー攻撃への防御を全学的課題として意思決定しておく。

※　担当役員もしくはそれに準ずる大学執行部の関係者を配置し、サイバー攻撃による脅威の認識を徹底。

※　構成員一人ひとりが防御意識の持続化を図れるように、振り返りをさせる仕組みが必要。

※　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。

2. 学内ルールの構築と周知徹底

※　情報セキュリティポリシーに関する取り扱い基準の構築、構成員全員にサイバー攻撃に対する最小限度の行動基準を作成し、理解を徹底。

※　構成員一人ひとりが情報資産の所在を明確化し、情報資産別に被害の重大性を想定して防御の仕方を共有しておく。

　また、請負業者についても情報セキュリティの問題意識を職務責任として契約などで明確化しておく。

※　攻撃を受けたときの緊急対応として、被害の拡大を防ぐために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。

3. 防御体制の構築と点検評価の徹底

※　統括責任者の役割と権限を明確化する。

※　防御に関する取り組み対策のとりまとめや点検・評価のガイドラインを検討する「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」の充実が不可欠。

※「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る。

※　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の働きかけ、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。

4. 教職員に対する教育や模擬訓練の実施と徹底

※　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。

※　サイバー攻撃の事例を通じて脅威に関する認識を徹底し、脅威に遭遇した時の緊急対応について模擬訓練などにより修得。

※最小限度心がけておくべき対応として、

①　不審メール見極めの模擬訓練の体験

②　ウイルス拡散、機密情報の外部への漏えい、システム破壊などの被害の知識共有化、被害防止意識の向上

③　被害の拡散を防ぐため相談・連絡手順の修得