情報セキュリティベンチマーク評価のガイドライン

情報セキュリティ対策問題研究小委員会

１．ベンチマーク評価の視点

ベンチマーク評価は、昨年度作成した「大学セキュリティ運用ベンチマークテスト」の点検項目について評価の重み付けをする観点から大学として情報セキュリティ対策を振り返る上で基本となる４つの視点で再構成した。内容としては、アウトカム評価に不可欠な要素を設定し、点検項目及び対策内容について見直しを行い、昨年度の５１項目から２３項目に選別して情報セキュリティの対応状況を一覧できるようにした。とりわけ、大学執行部として情報セキュリティに関与することを重要視し、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マッチングすることにした。

２．ベンチマークによる対応状況の確認

情報セキュリティに関する対応状況を確認するため、別紙の「ベンチマークリストの評価配点表」にもとづき、「経営執行部の情報セキュリティに対する取組み」に３０点、「重要な情報資産の把握と管理対策」に２０点、「組織的・人的な対応」に２０点、「技術的・物理的対策」に３０点を配点し、４つの視点に重み付けを行った。特に、「経営執行部の取組み」に３０点の重み付けを行うことで、大学が組織をあげて対応することの重要性を強調した。

以上の視点によるベンチマークは、経営執行部の取組み状況をもとに、一貫した情報セキュリティ対策が展開されているか否かを振り返ることにより、情報資産の把握と組織や技術的な対応の関係性について自己点検・評価し、不足している取組みについて改善に向け組織的に計画・行動できるようにした。

３．情報セキュリティの改善に向けた対策

ベンチマークリストによる評価結果にもとづき、各大学が今後改善に向けて取組むべき対応及び個別の対策について、どのように改善行動を進めていくべきか、参考となる取組みについていくつかのパターンを例示的に掲げる。

（１）４つの視点で重視すべき改善対策

① 「危機意識の共有化対策」としては、情報セキュリティの脅威となる事象がもたらす被害の重大性について全学的に理解を普及し、大学構成員一人ひとりが危機回避のために気づきができるよう周知徹底を図る意思決定を行う必要があります。

具体的な対策としては、脅威となる事象の被害事例を説明し、自大学で起きた場合のリスクを想定して大学構成員一人ひとりが心得るべき気づきを促します。

※ 学内外の情報セキュリティ研修会参加の義務化（例えば２年に１回）
※ FD・SD、教授会、職員会議などでの定期的な情報提供
※ Web サイトや学内文書による定期的な情報提供
※ 学生に対する注意喚起（学部・学科の履修説明会など）

② 「構成員に学内ルールの周知徹底と遵守の対策」としては、IPA（情報処理推進機構）の情報セキュリティに関する脅威や対策などの映像コンテンツを学内 LAN で強制的に視聴させるなどのほか、心掛けが必要な最小限度の学内ルールの遵守状況についてアンケートで確認する必要があります。

③　「情報セキュリティに関する意思決定や脅威となる事象に対応する組織」としては、統括責任者の役割と権限を明確にした上で、専門の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規定化します。その上で、インシデントに緊急対応する権限や防御の仕方及び外部機関や業者と情報の交換・共有をする組織を設置する必要があります。

④　「重要な情報資産の把握対策」としては、職員は、組織的に重要な情報資産に対するアクセス制御及びリスク評価を義務付ける必要があります。教員は、情報資産を研究室単位で管理するために、情報資産の一元管理、アクセス制御、ネットワーク制御の実施を行うか、あるいは学内クラウドのように全学一元管理システムの利用などが必要となります。

⑤　「教職員への危機意識の対策」としては、パソコン画面に「メール開封時の注意喚起」を掲示し、注意履行の確認を行わせる仕組みを設ける必要があります。また、「不審メール見極めの対策」としては、ウイルス拡散、機密情報の外部漏えい、システム破壊など被害の重大性について認識できるよう、学科単位、部署単位の関係代表者を対象にワークショップなどの見極め対策を行う必要があります。

⑥　「不用意な情報漏えい対策」としては、大学構成員が USB などで重要な情報資産の持ち出しをできないように規定し、システム上で禁止する対策を講じておく必要があります。

（2）自己点検・評価結果を受けた段階的な改善行動

①　「ベンチマーク評価の中で検討中または対応していない場合」については、危機意識が不足していると思われることから、情報セキュリティの脅威について関心が高まることを優先し、情報センター等部門または委員会などで私情協や報道関係の資料を学内に発信する取組みを早急に始めることが必要です。

　なお、「情報セキュリティポリシーなど学内ルールを策定していない場合」については、私情協の Web サイトに掲載されている他大学の規定を参考にセンター等部門または委員会組織で早急に策定する必要があります。

②　「経営執行部が関与していないが情報センター等部門で対応している場合」については、まず執行部に対して、脅威となる事象による被害の想定や情報セキュリティに関する映像コンテンツを用いて、大学として対応すべき対策の重要性について説明します。その上で、大学として取組んでいる状況のベンチマーク評価結果を踏まえて、問題点を抽出し、不足している対策について認識を共有します。

③　「経営執行部が関与している場合」については、ベンチマーク評価結果にもとづき、不足している対策について他大学及び他機関での対応状況を踏まえて、改善計画を提案し、予算化を含めて実現に向けた行動の準備をする必要があります。

　なお、最適な改善計画を整備するために、他大学及び他機関との情報共有の仕組みを構築する必要があります。