※　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

た。学内ネットワークの遮断など緊急対応の決定や防御方法を専門的に検討する組織及び、攻撃情報及び被害回復情報を交換・共有する組織の設置を点検しました。また、防御対策では、メール及び、パスワードの見直しの注意喚起、VLANなどによるアクセス制限、データ暗号化などの対応を点検しました。

第４部の「技術的・物理的な対応」では、リスクを分散するネットワークの分離と不正通信などを可視化する侵入検知システムを重視しました。特に、通信の監視では外部委託だけではなく、学内で定期的に点検する必要があります。さらに、重要な情報資産の持ち出しについてノートPCやUSBメモリなどの取り扱いを点検しました。

２．ベンチマーク評価の重み付け

情報セキュリティに関する対応状況を確認するため、以下の「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いました。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ました。

３．ベンチマーク評価結果に基づく改善への取り組み

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ます。

（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。

ベンチマークリストの評価配点表

第1部　経営執行部の情報セキュリティに対する取組み			
問1　危機意識の共有化		10	30
問2　学内ルールの徹底		8	
問3　防御体制の構築		7	
問4　予算		5	
問5　予算の内容		－	
第2部　重要な情報資産の把握と管理対策について			
問1　目録作成		10	20
問2　アクセス権とリスク評価		5	
問3　個人データ管理		5	
第3部　組織的・人的な対応について			
問1　意思決定組織		5	20
問2　罰則規定		1	
問3　責任体制		1	
問4　外部契約		2	
問5　実施内容	(1) 危機意識の共有化	3	
	(2) ルールの徹底	3	
	(3) 防御対策	5	
第4部　技術的・物理的対策について			
問1　ログ管理		3	30
問2　侵入検知の導入		5	
問3　持ち出し制限		3	
問4　ID管理と認証		3	
問5　アクセス制限		4	
問6　ネットワーク分離		6	
問7　ぜい弱性対策		3	
問8　バックアップ		3	

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ますことから、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。