私情協ニュース NO.5

大学情報セキュリティベンチマークリストの見直し

情報セキュリティ研究講習会運営委員会
情報セキュリティ対策問題研究小委員会

情報セキュリティに関する対応状況を確認するため、求められる対策等を想定して「大学情報セキュリティベンチマークリスト」の見直しを行いました。

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、組織や技術的な対応の関係性、個人情報の取り扱いなどの観点から自己点検・評価し、改善に向けた組織的な計画・行動が展開されることを期待します。

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　サイバー攻撃による情報資産、金融資産の窃取・漏洩・破壊など情報管理やシステム運用に関する脅威となる事象について、担当役員もしくはそれに準ずる法人・大学執行部メンバーが統括責任者としてリーダーシップを発揮し、危機意識の共有化に努めていますか。

※　危機意識の共有化とは、サイバー攻撃の脅威を理解していただくため、例えば、文書・Webサイト・会議等での注意喚起や研修会などへの対応があります。

① 経営執行部が中心となり、全学組織を対象に危機意識の共有化に努めている。
② 経営執行部の方針により、学部単位など部門の管理責任者を通じて危機意識の共有化に努めている。
③ 経営執行部の方針により、情報センター等部門を通じて危機意識の共有化に努めている。
④ 経営執行部による危機意識の共有化はしていないが、現在、検討している。
⑤ 経営執行部による危機意識の共有化はしていない。

問２　経営執行部の方針により、情報セキュリティポリシーを策定し学外に公開するとともに学内で周知徹底に努めていますか。

① 経営執行部の方針により、情報セキュリティポリシーを策定し、学外に公開し学内で周知徹底を行っている。
② 経営執行部の方針により、情報セキュリティポリシーを策定し、学内で周知徹底を行っているが、学外には公開していない。
③ 経営執行部の方針により、情報セキュリティポリシーの策定を行っているが、周知徹底はできていない。
④ 経営執行部ではなく情報センター等部門により、情報セキュリティポリシーを策定し、その周知徹底を行っている。
⑤ 経営執行部ではなく情報センター等部門により、情報セキュリティポリシーを策定しているが、周知徹底はできていない。
⑥ 情報セキュリティポリシーの策定とその周知徹底を検討している。
⑦ 情報セキュリティポリシーの策定はしていない。

問３　経営執行部の方針により、個人情報保護の基本方針(プライバシーポリシー)を策定し、学外に公開する共に、学内で周知徹底を努めていますか。

① 経営執行部の方針により、個人情報保護の基本方針を策定し、学外に公開し学内での策定とその周知徹底を行っている。
② 経営執行部の方針により、個人情報保護の基本方針を策定し、学内で周知徹底を行っているが、学外には公開していない。
③ 経営執行部の方針により、個人情報保護の基本方針の策定を行っているが、周知徹底はできていない。
④ 経営執行部ではなく情報センター等部門により、個人情報保護の基本方針を策定し、その周知徹底を行っている。
⑤ 経営執行部ではなく情報センター等部門により、個人情報保護の基本方針を策定しているが、周知徹底はできていない。
⑥ 個人情報保護の基本方針の策定とその周知徹底を検討している。
⑦ 個人情報保護の基本方針の策定はしていない。

問４　経営執行部により情報セキュリティを管理するための体制を構築していますか。

① 経営執行部が中心となり、全学組織を対象に管理体制を構築している。
② 経営執行部の方針により、学部単位など部門の管理責任者を通じて管理体制を構築している。
③ 経営執行部の方針により、情報センター等部門を通じて管理体制を構築している。
④ 経営執行部として管理体制を構築していないが、現在、検討している。
⑤ 経営執行部として管理体制を構築していない。

問５　今年度、貴大学のICT予算(人件費を除く)の中で、セキュリティ対策に充当している費用の割合を選択してください。

① １０％以上
② ７％～９％
③ ４％～６％
④ ３％以下
⑤ 予算化はしていない。

問６　上記セキュリティ対策費の中で、費用をかけている内容を選択してください。
(複数回答)

① ファイアウォール
② 侵入検知システム
③ VLANなどネットワーク関連
④ ウイルス対策ソフト・サービス
⑤ セキュリティ監視サービス
⑥ フィルタリングソフト(Web、メール)
⑦ 暗号化対策
⑧ USB、SDカード、DVDなどの書き込み制御ソフト
⑨ 不審なファイルを外部から保護された仮想環境で確認を行う攻撃対策ツール
⑩ バックアップ対策
⑪ その他(　　)

第２部　重要な情報資産の把握と管理対策について

問１　情報の重要度を評価し、情報資産(金融資産情報を含む)のリスク評価と対策を実施し、情報資産管理台帳を整備していますか。

※　情報資産とは、大学で重要と重み付けをした情報及び情報を含むシステムです。例えば、重要な情報資産として、学生の個人情報・入試情報・学籍番号・履修成績情報、教職員の個人情報・マイナンバー・健康管理情報、教員の研究情報、業務システムデータ、部門外秘情報、卒業生名簿、保護者情報などがあります。

① 情報資産のリスク評価と対策を実施しており、情報資産管理台帳を毎年見直している。
② 情報資産のリスク評価と対策を実施しているが、情報資産管理台帳の定期的な見直しは行っていない。
③ 検討している。
④ 実施していない。

問２　重要な情報資産に対するアクセス制御を行っていますか。

① 重要な情報資産に対するアクセス制御を行っている。
② 検討している。
③ 実施していない。

問３　個人データや機密情報など重要な情報資産の管理について、入手から保管、消去・破棄に関わる責任者・取扱者、取扱手順、処理の履歴・点検などが定められていますか。

① 責任者・取扱者、取扱手順、処理の履歴・点検を定め、定期的に確認をしている。
② 責任者・取扱者、取扱手順、処理の履歴・点検を定めているが、定期的な確認はしていない。
③ 検討している。
④ 定めていない。

第３部　組織的・人的な対応について

問１　情報セキュリティに関する意思決定組織、脅威となる事象に対応するインシデント対応組織が設置されていますか。

※　インシデント対応組織とは、事件・事故に対する緊急対応及び防御方法の検討を専門に行う組織で、外部の機関や業者と情報を交換・共有する役割も含まれます。

① 経営執行部として統括責任者(CISO)を置き、情報セキュリティに関する専門の検討組織(情報セキュリティ委員会)を設置し、実施組織としてCSIRTを設置している。
② 統括責任者を置き、情報セキュリティに関する専門の検討組織を設置しているが、CSIRTは設置していない。
③ 統括責任者は置いていないが、情報セキュリティに関する専門の検討組織を設置し、実施組織としてCSIRTを設置している。
④ 情報センター等部門を中心に対応している。
⑤ 情報センター等部門ではなく、情報セキュリティなどの検討委員会で対応している。
⑥ 組織の設置を検討している。
⑦ 組織の設置はしていないが、外部業者に委託している。

⑧ 組織の設置は考えていない。

問２　教職員(非常勤・派遣を含む)の採用・退職に際して、守秘義務を書面で明確にしていますか。また、情報セキュリティポリシーに違反した場合の罰則が規定されていますか。
① 守秘義務の内容を書面で明確にしている。また、違反した場合の罰則を規定している。
② 守秘義務の内容を書面で明確にしているが、罰則規定は設けていない。
③ 守秘義務を書面で明確にしていないが、就業中の罰則で規定している。
④ 書面での明確化と罰則規定のいずれも対応していない。
⑤ その他(　　)

問３　脅威となる事象の学内連絡体制及び処理の責任体制は確立されていますか。また、対応手順は整備されていますか。
① 脅威となる事象の学内連絡体制及び処理の責任体制を確立し、対応手順も整備している。
② 学内の連絡体制と責任体制を確立しているが、対応手順は整備していない。
③ 学内の連絡体制を確立しているが、責任体制の確立と対応手順の整備はできていない。
④ 学内の連絡体制及び責任体制の確立と対応手順の整備はできていない。

問４　情報セキュリティに関する業務委託を外部組織と契約する際に、情報漏洩や情報消失・破壊など障害対応について責任の所在を明確にし、外部組織による定期的な点検・大学による点検の監視など障害を予防するための取り決めをしていますか。
① 障害対応の取扱いについて契約書の中で、外部組織及び大学による定期的な点検・監視について取り決めをしている。
② 障害対応の取扱いについて契約書の中で、外部組織による定期的な点検に留めている。
③ 障害対応の取扱いについて契約書で取り決めていない。

問５　経営執行部または部門単位で実施している危機意識の共有化、学内ルールの周知徹底・遵守の確認、攻撃に対する防御対策の内容について選択してください。
(複数回答可)
（１）危機意識の共有化
※　危機意識の共有化とは、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。
① 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）
② FD・SD、教授会、職員会議などでの定期的な情報提供
③ Webサイトや学内文書による定期的な情報提供
④ その他(　　)

（２）学内ルールの周知徹底と遵守の確認
① 情報センター等部門によるルールの周知とアンケートでの点検・確認
② 教授会、職員会議などでのルールの周知と遵守の確認
③ Webサイトでのルールの紹介と遵守の呼びかけ
④ 説明会でのルールの紹介と遵守の呼びかけ
⑤ その他(　　)

（３）攻撃に対する防御対策
① 公的機関を装った偽装メールの注意喚起
② メール添付ファイル開封の注意喚起
③ メールにリンクされたURL接続の注意喚起
④ USBメモリなど外部持ち込みの注意喚起
⑤ 脅威となる事象について被害状況の報告と対策の説明
⑥ IDの管理やパスワードの定期的な見直しの注意喚起
⑦ 不正アクセスの監視と異常事態の発見
⑧ ファイアウォールや迷惑メールの設定
⑨ VLANなどネットワークのアクセス制限の設定
⑩ 無線LANの暗号化及び認証方式の導入
⑪ データ暗号化の導入
⑫ クラウドに対する利活用の注意喚起
⑬ その他(　　)

第４部　技術的・物理的対策について

問１　ファイアウォールを導入しポリシーに基づきログ管理や通信を定期的に点検していますか。
① システムログを取得・解析し、通信を定期的に点検している。
② システムログの取得のみで解析していない。
③ システムログの取得はしていない。

問２　侵入検知システムなどを導入し、不正通信や不正プログラム(ウイルス、スパイウェア、外部から不正な接続など)を監視する対策を行っていますか。
① 侵入検知システムなどを導入し、定期的に通信の監視を行っている。
② 侵入検知システムなどを導入し、通信の監視を行っている。
③ 侵入検知システムなどの導入を検討している。
④ 侵入検知システムなどは導入していない。

問３　重要な情報資産についてUSBメモリ・ノートPCなどの持ち出し・持ち込みの禁止と制限を行っていますか。(複数回答)
① USBメモリの使用を禁止している。
② ノートPCの持ち出し・持ち込みを禁止している。
③ ノートPCの持ち出しは原則禁止しているが、暗号化で保護する場合のみ許可している。
④ 外部クラウドサービス利用の制限を行っている。
⑤ 持ち出し・持ち込みの制限を検討している。
⑥ 持ち出し・持ち込みの制限はしていない。

問４　認証情報安全性の確保を行っていますか。(複数回答)
① 多要素認証・２段階認証を導入している。
② 誕生日など推測しやすいパスワードを設定しないよう登録画面で注意喚起している。
③ パスワードの使いまわしをしないよう注意喚起している。
④ その他(　　)

問５　情報システムやコンテンツへのアクセス制限を行っていますか。
① 全学的にアクセス制限を行っている。
② 一部の部門（職員組織、学部、学科など）でアクセス制限を行っている。
③ アクセス制限を検討している。
④ アクセス制限は行っていない。

問６　リスクを軽減するため、ネットワークの分離を行っていますか。
① 全学的にVLAN(仮想的なネットワーク)などでネットワークを分離している。
② 事務部門など一部のネットワークをVLANなどで分離している。
③ VLANなどでネットワークの分離を検討している。
④ その他のネットワーク分離対策(　　)
⑤ ネットワークの分離はしていない。

問７　外部に公開しているWebサーバに関係して、利用者から取得した個人情報の取扱いについて明記していますか。
① 利用者から取得した個人情報の取扱いについて明記している。
② 検討している。
③ 特に明記していない。

問８　外部に公開しているサーバのぜい弱性対策を行っていますか。
※　ぜい弱性対策とは、ソフトウェアのセキュリティ不備を狙った悪意のある攻撃への対策をいいます。
① ぜい弱性に対して最新の修正プログラムを用いて対応している。
② 最新の修正プログラムを適用するまでの間、当面の対応としてぜい弱性を狙った攻撃を回避するソフトウェアもしくはハードウェアを導入して対応している。
③ ぜい弱性対策を検討している。
④ ぜい弱性対策はしていない。

問９　重要な情報資産をバックアップしていますか。また、システム障害等を想定し、必要最低限の業務ができる備えをしていますか。(複数回答)
① 遠隔地域の大学と業務提携によりバックアップデータを保管している。
② 遠隔地のデータセンターなどにバックアップデータを保管している。
③ 他のキャンパスにバックアップデータを保管している。
④ バックアップは毎日行っている。
⑤ バックアップは一定の期間で行っている。
⑥ 学内でシステムの二重化を行っている。
⑦ 部門単位でシステムの二重化を行っている。
⑧ バックアップの一つの方法として紙媒体で保管している。
⑨ その他のバックアップ方法(　　)
⑩ バックアップへの備えについて検討している。

問10　コンピュータフォレンジックに関係した対策が自組織で実行できますか。(複数回答)
※　コンピュータフォレンジックとは、セキュリティインシデントに関する機器等の情報を収集し、解析することです。
① ハードウェアの調査をすることができる。
② ソフトウェアの調査をすることができる。
③ フォレンジックを実施する組織がある。
④ フォレンジックに関係した法的・制度的な仕組みを理解している組織がある。
⑤ リスクの評価を適切に定義し、適切なフォレンジックを実行できる。
⑥ 専門の調査会社に依頼する体制がある。