大学の情報セキュリティ対策の自己点検・評価リストについて

「大学の情報セキュリティ対策の自己点検・評価リスト」は、大学が情報管理の責任を明確化し、取組み状況を体系的に把握した上で弱点の発見と改善を期すために当面、必用と思われる情報セキュリティの自己点検・評価のためのチェックリストとして作成したものです。　情報管理責任者の方が適切に取り組みめるように、項目ごとに「内容や重要性の説明」、「取組むべき対策例」、「参考情報」などを掲載しております。

本システムは私情協サーバーに置いてありますので、ＩＤ、パスワードで随時、項目ごとの点検・評価が可能です。

点検結果は、色で表示されますので、対策の状況が一眼視できます。なお、点検を客観的に数値で把握することができますように、4月以降にシステムを改良する予定にしております。

本チェックリストの点検を通じて大学の情報管理の政策・運用・技術の見直しが一層進められ、情報セキュリティに関する大学のガバナンスの確立につながることを期待しています。

チェックリストの各項目に対する点検・評価点は以下の通りです。

①	本チェックリストの方法で対応している。	5点
②	本チェックリスト以外の方法で対応している。	5点
③	一部（部門・項目）に対応している。	4点
④	対応していないが対応を具体的に計画している。	3点
⑤	対応していないが必要性を感じており、これからの課題と考えている。	1点
⑥	必要性を感じていない。	0点

大学の情報セキュリティ対策の自己点検・評価チェックリストの項目

１．情報資産の把握	点検・評価欄
(1)情報資産の目録作成	
・ 情報資産の作成者、入手先が明確になっているか。	
・ 情報資産の管理部署・管理責任者は明確になっているか。	
・ 情報資産の保存場所･保存形態が明確になっているか。	
・ 情報資産の主な利用目的が記載されているか。	
・ 情報資産の公開対象が明確になっているか。	
(2)情報資産の重要度	
・ 情報資産の内容について組織的な重み付けがなされているか。	
・ 情報資産の重要度の指標について適切な基準が設定されているか。	
(3) 情報資産の管理・運用	
・ 情報資産の種類に応じて、物理的、電磁的アクセス権の設定がなされているか。	
・ 適切な時期に情報資産の棚卸しが行われており、変更の履歴が保存されているか。	
・ 情報資産の重要度に合わせて作成、保管、修正、廃棄、公開の手順が定められているか。	
(4) リスク分析・対応	
・ 情報資産のリスク評価基準が明確になっているか。	
・ リスク別にどのような対策をとるべきかの指針が整理されているか。	

２．組織的対応	点検・評価欄
(1)意思決定	
・ 経営責任の一部として、情報セキュリティの最高責任者を決めているか。	
・ 情報セキュリティに関して専門に検討する組織が設定されているか。	
・ 組織単位で情報セキュリティの責任者を決定しているか。	
(2)運用体制	
・ 組織単位で情報セキュリティに取り組む体制(企画、実行、評価・改善)が確保できているか。	
・ 情報セキュリティに関する学内外の障害・事故状況を的確に把握し、改善につなげているか。	
・ ソフトウェアのライセンス管理体制が確立されており、知的財産権を侵害していないか。	
(3)監査体制	
・ 意思決定の機能(報告・連絡・相談)が正常に働いているかを点検する仕組みがあるか。	
・ 意思決定内容が適切になされているか、学内外の専門家による評価の仕組みがあるか。	
・ 組織単位での情報セキュリティの実施状況を点検・評価し、改善する体制が確保できているか。	
・ 点検・評価は、実績データに基づき継続的に実施され、その結果がフィードバックされ改善に活かされているか。	
(4)情報セキュリティポリシー	
・ 情報セキュリティポリシーが策定できているか。	
・ 情報セキュリティポリシーには、「目的」、「基本方針」、「適用者」、「利用者の義務・責任」を定めているか。	
・ 情報セキュリティポリシーが公開され、学内関係者に周知徹底されているか。	
(5)情報セキュリティポリシーの対策基準	
・ 組織的セキュリティ、人的セキュリティ、技術的セキュリティ、物理的セキュリティについての遵守事項、PDCAサイクルを意識した運用が明確化されているか。	
・ 対策基準が公開され、学内関係者に周知徹底されているか。	
学外関係者としての関連業者等に業務や情報システムの運用管理を委託する際、情報セキュリティポリシーに基づいた適切な契約がなされているか。	
(6)情報セキュリティポリシーの実施手順	
・ 対策基準で定められた内容が、各構成員の行動指針としてガイドライン化されているか。	
・ 組織単位で実施手順を点検・評価し、改善する仕組みができているか。	
・ 危機管理のための実施マニュアルを作成しているか。	

３．人的対応	点検・評価欄
(1)構成員の把握	
・ 大学の情報資産に接する教員、職員、学生、関連業者等、構成員の範囲を明確にしているか。	
(2)職務責任	
・ 構成員に対して、セキュリティに対する問題意識を職務責任の中で明確にしているか。	
(3)機密保持	
・ 構成員である間および構成員でなくなった後の機密保持の取り扱いを適切に定めているか。	
(4)情報の利用	
・ 各構成員が利用できる情報の所在と利用できる対象者が明確になっているか。	
・ 身分変更があった場合のアクセス権の設定・制限・緩和・削除が適切に行われているか。	
(5)罰則規定	
・ 構成員が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るか。	
(6)情報資産の引継ぎ	
・ 人事異動、休職、退職等に対応した情報資産の引継ぎが適切(明文化、報告等)になされているか。	
(7)情報セキュリティ教育	
・ 情報セキュリティポリシーに従った教育がすべての構成員（学長などの役職者を含む）に適切に実施されているか。	
・ 情報セキュリティ教育は定期的に実施され、参加を促す工夫がなされているか。	
・ 過去の事故事例を共有し、情報セキュリティ教育などに活用しているか	
(8)事故対応と報告義務	
・ 事故の連絡体制、事故処理の責任体制が確立されているか。	
・ 重大な事故が発生した場合、警察や報道関係への対応体制及びマニュアルが整備されているか。	
・ 事故対応に対するトレーニングを定期的に実施しているか。	
・ 情報資産の管理者及び利用者が情報セキュリティに関する問題点を発見した場合、疑わしい状況を察知した場合の緊急連絡先が周知されているか。	

４．技術的・物理的対応	点検・評価欄
(1)ネットワーク	
・ 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の状況を定期的に点検しているか。	
・ 検知対象の情報を日々更新し、ログの保存・解析を行っているか。	
・ 組織が管理するネットワークを把握し、トラフィック監視を行っているか。	
・ 業務・研究・教育など用途ごとにネットワークを分離しているか。	
・ セキュリティ対策のなされていない無線LANのアクセスポイントはないか。	
・ ユーザ認証なしでだれでも利用できる情報コンセント等はないか。	
・ ルータやスイッチなどのアクセスコントロールや時刻同期を行っているか。	
(2)サーバ	
・ OSやサーバのソフトウェアは信頼できるバージョンを使用し、必要に応じてアップデートを行っているか。	
・ サーバの稼動状況や利用者ごとのアクセス状況を把握し、正確な時刻設定のもと、ログの保存と解析を行っているか。	
・ 不要なサービスやポート、アカウント等が稼動していないか。	
・ 定期的な監査を行い、セキュリティの基準を満たしていないサーバがないかチェックしているか。	
・ セキュリティホールとなるようなソフトウェアへの対策を行っているか。	
・ 障害発生時の復旧に備えて、バックアップをとっているか。	
・ 施錠された安全な場所に設置し、入退室者の記録をとっているか。	
・ 廃棄する際に、情報資産が流出しないよう、手順や履歴の管理を行っているか。	
・ パスワードを定期的に変更し、容易に推測できないものとなっているか。	
・ 不正侵入対策として、学外から管理者権限でサーバにログインできないようになっているか。	
・ Webサーバ上のコンテンツに対するアクセス権などを適切に設定しているか。	
・ Webアプリケーションに対する脆弱性対策(XSS,SQLインジェクション等)を行っているか。	
・ 重要な情報を取り扱う場合は暗号化を行っているか。	
・ 公開している情報が本当に正しいものなのか定期的にチェックしているか。	
・ 迷惑メール対策（ウィルス対策、spam対策、オープンリレー対策等）をしているか。	
・ ネームサーバのデータベースが適切に管理されているか。	
・ ファイルサーバへのアクセス権を適切に設定しているか。	
(3)クライアント	
・ 悪意のあるソフトウェア対策を行っているか。	
・ OSやソフトウェアは信頼できるバージョンを使用し、必要に応じてアップデートを行っているか。	
・ 不要なサービスやポート、アカウント等が稼動していないか。	
・ 正確な時刻設定のもと、利用者のログの保存と解析を行っているか。	
・ 障害発生時の復旧に備えて、バックアップをとっているか。	
・ 部外者が容易に立ち入らないような監視体制と盗難防止策を講じているか。	
・ 廃棄あるいは返却する際に、情報資産が流出しないよう、手順や履歴の管理を行っているか。	
(4)情報媒体の管理	
・ 情報媒体(USBメモリやハードディスクドライブ、ノートパソコン等)の持ち出しや持ち込みについて基準を設けているか。	
・ 情報媒体はパスワード設定や暗号化等の紛失・盗難対策を講じているか。	
(5)　情報施設・設備の管理	
・ 地震や火災等、施設に対する安全管理対策はできているか。	
・ 電源や空調の安定運用、盗難防止等、設備や機器等に対する安全対策はできているか。	