3. 人的対応

チェックリスト項目	説明	対策例	関連資料
(1)構成員の把握	【狙い】 大学の情報資産に接する可能性のある人の範囲を洗い出し，情報セキュリティの人の管理範囲を明確にすることを狙いとします。		【参考情報】 ・情報セキュリティマネジメントシステム適合性評価制度　-ISMS認証基準（Ver.2.0）-　（附属書「詳細管理策」） http://www.isms.jipdec.jp/doc/JIP-ISMS100-20.pdf ・IPA対策のしおりシリーズ（5）　情報漏洩対策のしおり、情報処理推進機構セキュリティセンター http://www.ipa.go.jp/security/antivirus/documents/5_roei_v3_2.pdf ・2006年情報セキュリティインシデントに関する調査報告書、NPO日本ネットワークセキュリティ協会 http://www.jnsa.org/result/2006/pol/insident/070720/2006incidentsurvey-02-080526rev_.pdf ・中小企業の情報セキュリティ対策ガイドライン、情報処理推進機構セキュリティセンター http://www.ipa.go.jp/security/fy20/reports/sme-guide/index.html ・小規模企業のための情報セキュリティ対策、情報処理推進機構セキュリティセンター http://www.ipa.go.jp/security/fy18/reports/contents/soho/soho.pdf ・情報セキュリティガバナンス導入ガイド、経済産業省 http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf ・アウトソーシングに関する情報セキュリティ対策ガイダンス、経済産業省 http://www.meti.go.jp/policy/netsecurity/downloadfiles/outsourcing_guidelines.pdf ・情報セキュリティ報告書モデル、経済産業省 http://www.meti.go.jp/policy/netsecurity/downloadfiles/070824securityreportmodel.pdf
・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。	「大学の情報資産に接する」という意味は、現に接している場合に限定するものではなく接する可能性がある場合も含めます。 構成員には、大学に在学する学生・専任教職員の他，交換留学生・非常勤・臨時の教職員・在外研究などの研究者・嘱託，アルバイト等も含まれます。また、大学との間に雇用関係が無くても、大学の情報資産に接する可能性があれば業者や派遣業務員なども含みます。	・情報資産に接する構成員の所属、身分、職責等の把握（留学生・非常勤・臨時教職員・在外研究者・嘱託，アルバイト等） ・教員・職員・学生等の構成員のデータベース化	
(2)職務責任	【狙い】 情報セキュリティに関する個人レベルでの取り組みは重要です。ここでは，大学組織における職務責任として明確に位置づけられているかの確認を狙いとしています。		
・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。	大学の運営体制と各構成員の業務内容に応じて、情報セキュリティに関する役割と責任を定める。たとえば，職務分掌規程や業務契約書などにより文書化されているかどうかをチェックします。 学生等については，学則に情報セキュリティに関する責任と義務について盛り込むことが望ましいが，少なくとも学生に配布する手引きなどに，明記しているかどうかをチェックします。	・情報セキュリティポリシーの全構成員への周知徹底 ・雇用条件や人事規定に情報セキュリティに関する責任を明記 ・学生に対しても情報システム利用規定などで情報セキュリティに関する責任を明記	
(3)機密保持	【狙い】 構成員に対する機密保持が適切に管理されているかどうかチェックすることを狙いとしています。		
・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。	採用時，人事異動時，休職時，退職後における遵守事項に機密保持に関する内容が含まれているかどうかをチェックします。採用時における情報セキュリティに関する審査要件が明確に定められているかどうか，業務契約書において機密保持契約を行っているかどうかのチェックを含みます。	・構成員に対して、情報セキュリティに関して就業上の遵守事項を明示 ・採用時に、守秘義務契約や誓約書などを交わす ・必要に応じて、情報セキュリティや機密保持契約を結ぶ	
(4)情報の利用	【狙い】 構成員ごとに，利用可能な情報資産の範囲とその所在が明らかにされ，文書化されているかどうかをチェックすることを狙いとしています。		
・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。	構成員が身分や職責に応じて利用することができる情報資産の目録が整備されているかチェックします。	・構成員の身分や職責に応じたアクセス権の管理を適切に行う	
・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。	人事異動，休職，退職のような身分・職責の変更があった場合，情報資産に対するアクセス権の変更が適切に行われているかどうか，をチェックします。		
(5)罰則規定	【狙い】 情報セキュリティ管理の実効性を担保するために，構成員に対する罰則が明示されているかどうかをチェックすることが狙いです。		
・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。	構成員による大学のセキュリティ基本方針および規則への違反は、正式な懲戒手続きによって処理される必要があります。	・構成員に関する就業規則の中に情報セキュリティに関する項目を含める	
(6)情報資産の引継ぎ	【狙い】 身分の変更等に対応した情報資産の引き継ぎが適切に行われているかどうかをチェックすることが狙いです。		
・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になされているか。	人事異動，休職，退職のような身分変更があった場合，適切な方法で情報資産の引き継ぎがなされているかどうかをチェックします。	・身分変更があった場合には、情報資産の引き継ぎを文書化する ・情報資産の引き継ぎをチェックできる仕組みを構築する	
(7)情報セキュリティ教育	【狙い】 構成員に対して情報セキュリティ教育が適切に行われているかどうかをチェックすることが狙いです。		
・情報セキュリティポリシーに沿った教育がすべての構成員に適切に実施されているか。	構成員の責任と義務に対応した教育プログラムが開発され，実施されているかどうかをチェックします。	・情報セキュリティに関する教育プログラムの開発・実施を担当する部署の明確化 ・情報セキュリティ教育の十分な回数の確保 ・LMSなどを利用したe-ラーニングを実施する	
・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。	構成員の特性を考慮し，受講回数や実施人数を管理・評価する体制が確立されているかどうかをチェックします。		
・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。	情報セキュリティの教育プログラムに，学内外の事故事例を反映してるかどうかチェックします。		
(8)事故対応と報告義務	【狙い】 ここでは，迅速な事故対応及びそれらからの教訓をフィードバックする体制が確立されているかどうかをチェックすることが狙いです。		
・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。	情報セキュリティに関する事故の連絡体制や責任体制が文書化されているかどうかをチェックします。	・情報資産の管理責任者を明確にする ・IRT（Incident Response Team：コンピュータセキュリティインシデントに対応する組織）を組織し、対応方法を定める	
・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。	警察や報道関係に対応する担当者，担当部局，あるいは緊急の際のチームメンバーなどが事前に明確にされているかどうかをチェックします。		
・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。	事故に適切に対応するためには、過去の事例を活かしたトレーニングが実施されていることが必要となります。		
・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。	構成員の報告義務，報告先及び報告を受けた場合の対処方法が確立されているかどうかをチェックします。		