1．情報資産の把握リスト

チェックリスト項目	説明	対策例	関連資料
(1)情報資産の目録作成	【狙い】 情報資産目録は、情報セキュリティにおいて守るべき対策を明らかにするために、最も重要なものです。実際の情報セキュリティ対策は、この目録をもとに、それぞれの資産ごとに作成されます。したがって、最初に情報資産目録作成がなされているかをチェックします。情報資産は、以下要求事項が網羅されている必要があります。		
・情報資産の作成者、入手先が明確になっているか。	情報資産がどのように作成されるか、あるいは、どのような入手経路によって入手されたかを明確にしておく必要があります。特にデータ形式の情報資産に関しては、そのデータの内容や変更について資産管理者が十分に理解していない場合が多く、内容の変更や追加に関しての問い合わせ先としての情報としても、作成者や入手先の情報は重要です。	・情報資産目録を作成します。 ・情報資産ごとに、以下の項目を明確にします。 （作成者、入手先、管理部署、管理責任者、保存場所、保存形態、利用目的、公開対象）	（１）CECの学校情報セキュリティライブラリ： http://www.cec.or.jp/seculib/index.html （２）ISMS/ISO27001認証取得支援のためのページ http://www.pangkal.com/isms/isms2.html （３）JIPDECによるISMS適合性評価制度に関するページ： http://www.isms.jipdec.jp/std/index.html （４）プライバシーマーク取得支援・ISMS取得支援のためのページ： http://www.neouniverse.biz/isms_step_mokuteki-hani.html CECの情報資産目録（リスト）の具体例へのリンク： http://www.cec.or.jp/seculib/18y/k21infolist.xls （情報資産目録のEXCELで作成された情報資産目録（リスト）の具体例です。この例は、小中高等学校を例として記述されているが、大学にも項目を変更して適用可能です。この表は、情報資産の目録作成の全体の部分で示した（１）のリンクからダウンロード可能です。なお、私立大学情報教育協会では、私立大学向けの情報資産目録の具体例を準備中です。サンプルが作成でき次第、順次リンクを張る予定です。） １．羽生田 和正，池田 秀司，荒川 誠実，『ISMS構築・認証取得ハンドブック―ISO/IEC 27001対応 情報セキュリティマネジメントシステムの事例集 (情報セキュリティライブラリ)』，日科技連出版，2008. ２．静岡大学ISMS研究会 著，八巻 直一 監修，『実践ISMS講座 情報セキュリティマネジメントと経営戦略』，静岡学術出版，2007. ３．白潟 敏朗，安達 祐哉，『図解 ISO27001早わかり (2時間でわかる)』，中経出版，2006. ４．日本規格協会 編集，『対訳 ISO/IEC27001:2005(JIS Q 27001:2006)情報セキュリティマネジメントシステム ポケット版 (Management System ISO SERIES)』，日本規格協会，2006.
・情報資産の管理部署・管理責任者は明確になっているか。	管理責任者は情報資産の利用や運用に関して責任を持つと同時に、資産の分類や目録作成、重要度の決定などに関して責任を持たなければなりません。また、利用目的や資産公開に関する判断など重要な決定に責任を持たなければなりません。そのため、管理責任者の決定は最も重要な事項です。		
・情報資産の保存場所・保存形態が明確になっているか。	資産がどこにどのような形態で保存されているかが明確にされていると同時に、資産の保存場所からの持ち出しや複製の作成は、規定により管理されていなければなりません。この項目は、それを明確にするためのものであり、特に別媒体への複製の作成に関しては、十分な注意が必要です。		
・情報資産の主な利用目的が記載されているか。	利用目的は資産目録の中で重要な位置を占めています。その資産がどのような経緯で作成されたかは、一般的には資産の作成者や入手先と同時に明示されているはずであり、ここでは、さらに、その資産の利用目的を明らかにすることが求められています。利用目的が示されていなければ、目的外利用に関する判断は曖昧なものとなります。特に、個人情報のような法令で規定されているものに関しては、十分注意が必要です。		
・情報資産の公開対象が明確になっているか。	資産の公開範囲を明確にすることは重要です。特に限定的な公開以上の取扱いが規定に定められている場合、それが厳格に守られているかを常に監査する必要があります。公開対象を明示して、それが守られていることを担保することは、情報漏えい防止の第一歩です。		
(2) 情報資産の重要度	【狙い】 資産の重要度は、資産を守るためのリスク対応に大きな影響を及ぼす指標であり、重要度が明示されていなければ、資産に対するリスクマネージメントを十分に行うことはできません。一般に、資産評価表によりその基準が明示されると同時に、資産目録に重要度が記述されていなければなりません。ここでは、資産評価の指標が明確になっているかいるかをチェックします。		
・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。	重みは、資産の重要度を示す唯一の指標であり、それが明示されていなければ、十分なリスクマネージメントに結びつけることができなくなります。	・情報資産評価表を作成します。 ・情報資産の重み付けの基準を明確にします。 ・資産目録に記載された情報資産に重み付けします。 ・重み付けの評価が変更になった場合は、その都度、新しい重み付けにより評価しなおします。	（１）JIPDECによるISMS適合性評価制度に関するページ： http://www.isms.jipdec.jp/std/index.html （２）社会保険庁の年金データベースに関する情報資産評価表の具体例： http://www.sia.go.jp/saitekika/1.3.1.2.pdf （３） 私立大学向けの情報資産目録の具体例を準備中です。
・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。	重み付けに対する基準が文書により明示されていることが重要です。一般に重要度はランク指標という数字などで示される場合が多いですが、資産評価表などによりその指標の基準が明示されていることが必要です。		
(3) 情報資産の管理・運用	【狙い】 情報資産目録を作成し、資産の重要度を把握した後、その資産の管理・運用が適正かどうか定期的にチェックする必要があります。ここでは、それらに対するチェック項目を示します。		
・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。	資産のアクセス権の設定は、情報資産の重みにより評価されると同時に、それにアクセスする必要があるかないかという職責に応じて評価されるべきです。この場合、資産の重みと職責とのマトリクス(アクセス制御方針表など)を必ず作成し、アクセス権付与の基準を明文化します。なお、職責に関しては、大学の実情に合わせて考えるべきであり、通常の企業等での職責とは必然的に異なります。	・アクセス制御方針表を作成し実施します。 ・物理的アクセス権はシステムを含む建物や部屋への入退室制限、システムのハードウェア的ロック機能を含みます。 ・電磁的アクセス権はシステムの利用権限のことです。	（１）「セキュリティ監査 入門7回目」、「情報資産の分類」 http://itpro.nikkeibp.co.jp/free/NGT/govtech/20050601/161939/ （２）「IT基盤を刷新するレガシーマイグレーション入門5回目」、「システム資産の棚卸」 http://www.thinkit.co.jp/free/article/0605/11/5/ （３）JIPDECのISMS適合性評価基準。 http://www.dipdec.jp/doc/JIP-ISMS100-20.pdf http://www.dipdec.jp/doc/JIP-ISMS100-21.pdf
・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。	情報資産に関する評価は、時間とともに変化するので、定期的に情報資産の重要度の再評価を行う必要があります。	・定期的に、情報資産を以下の手順に従って再評価します。 ① 資産目録の見直しと資産の追加・削除 ② 重要度に関する再評価 ③ アクセス権の再評価 ④ 変更履歴の保存	
・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。	情報資産の重要度に応じたセキュリティレベルを確保するためには、情報資産の作成・保管・修正・廃棄・公開の手続きを資産ごとに明確化する必要があります。	・現状行っている手順を明文化します。 ・保管・修正・廃棄・公開の手順書を作成します。	

チェックリスト項目	説明	対策例	関連資料
(4) リスク分析・対応	【狙い】 情報資産の評価をより適正に行うためには、情報資産が持っている価値の他に個々の情報資産の持つ脆弱性を分析し、対策を講じる必要があります。脆弱性がもたらす脅威の規模に応じた対策を検討する指標として脅威(リスク)の分析を行い、適切なリスク管理をしておく必要があります。		
・情報資産のリスク評価基準が明確になっているか。	「リスク評価」とは、「リスクの重大さを決定するために、算定されたリスクを与えられたリスク基準と比較するプロセスのことです。ここでリスクを評価するための基準を「リスク評価基準」と呼びます。 リスク評価基準は「リスク対応評価表」として作成されます。これは、守るべき情報資産の重要度とその脆弱性の検討から情報資産ごとのリスクに対する大学への影響度を評価します。そして、考えられるリスクへの対応の必要性を整理します。	・情報資産ごとにリスク対応評価表を作成します。そして、評価基準が変更された場合、リスク対応評価表のほうも必ず更新します。 ・リスク対応評価表は次のような方法で作成します。 ① 大学の情報資産のリストとその脆弱性を結びつけた脆弱性の評価リストを作成します。 ② 脆弱性の評価リストには脆弱性とともに、それに対するリスクを列挙します。 ③次に、脆弱性の大きさ、リスクの重大性(大学の情報資産に与える影響度)、リスクの起きる頻度の積として、リスクの重要性を評価します。 ④ リスク評価基準は、③で算出された値をもとに、リスクが決定されます。例えば、脆弱性の大きさ、リスクの重要度、頻度をそれぞれ3段階で評価すると、27が最も重大なリスクであり、1が最も軽微なリスクとなります。リスク評価基準は、算出された値に対する評価尺度(重大～警備まで)として与えられます。 ⑤ リスク対応評価表は、列挙されたリスクとそれに対する評価値の組み合わせで作成されます。	リスクの分析・評価・対応は情報資産を守るために重要な項目であり、情報資産を把握した次のステップとして必ず実施しなければならないものであり、ここで得られたリスク評価をセキュリティ対策に結びつけることが重要です。 （１）何回か引用しているJIPDECのISMS適合評価の次のドキュメントに詳しく記載されています。 http://www.dipdec.jp/doc/JIP-ISMS100-20.pdf http://www.dipdec.jp/doc/JIP-ISMS100-21.pdf （２）ThinkITの連載、「即活用！企業システムにおけるプロジェクト管理」の8回目、「リスク管理」の中には、何故リスク管理が成功しないのかを含めた解説があります。 http://www.thinkit.co.jp/free/project/1/8/1.html CECのリスク対応評価表（脅威の評価表）の具体例を示す。この例も、小中高等学校を対象としているが、大学への適用が可能です。なお、私立大学向けのサンプルは現在作成中です。 http://www.cec.or.jp/seculib/18y/k31threatRating.xls
・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。	情報資産に対してリスク対応が必要かどうかは、資産の重要度と潜在リスクの大きさによ決まります。重要な情報資産に対して大きなリスクが存在する場合は、リスクに対応すべきであり、存在しなければリスクに対応する必要はありません。リスク対応が必要な情報資産のリストはセキュリティリスクリストとして整理されます。整理されたリストから、情報資産ごとのリスク対応検討シートを作成します。このシートで検討したリスク対応が正しく行われたかどうかを検証することで、セキュリティ監査を行うことができるようになり、情報セキュリティのPDCAサイクルが正しく機能するようになります。		（１）CECのセキュリティリスクリストのフォーマットなどを例です。大学向けにアレンジする必要がありますが、基本的な形式はそのまま利用できます。 http://www.cec.or.jp/seculib/17y/h27arisklist.doc http://www.cec.or.jp/seculib/17y/h27brisklist-sample.doc http://www.cec.or.jp/seculib/17y/h28(D)risklist.xls （２）CECのリスク対応策検討シートのフォーマットの例です。セキュリティリスクリストと同様に、アレンジする必要がありますが、基本的な形式はそのまま利用できます。 http://www.cec.or.jp/seculib/17y/h31aactionlist.doc http://www.cec.or.jp/seculib/17y/h31bactionlist-sample.doc http://www.cec.or.jp/seculib/17y/h32(E)actionlist.xls （現在、私立大学向けのサンプルを作成中です。サンプルが出来次第、掲載する予定です。） 以下、リスク分析に関する関連書籍を示します。 １．デビッド ヴォース 著，長谷川 専，堤 盛人 訳，『入門リスク分析―基礎から実践』，勁草書房，2003. ２．Michel Crouhy，Dan Galai，Robert Mark 著，三浦 良造，小野 覚，多良 康彦，鉄田 義人，茶野 努，富安 弘毅，廣中 純，佐藤 克宏 翻訳，『リスクマネジメントの本質』，共立出版，2008. ３．畠中 伸敏，折原 秀博，伊藤 重隆，相沢 健実，羽生田 和正 著，『情報セキュリティのためのリスク分析・評価―官公庁・金融機関・一般企業におけるリスク分析・評価の実践（情報セキュリティライブラリ)』，日科技連，2008. ４．日本セキュリティ監査協会 編集，大木 栄二郎，『情報セキュリティ監査公式ガイドブック（情報セキュリティライブラリ)』，日科技連，2007.