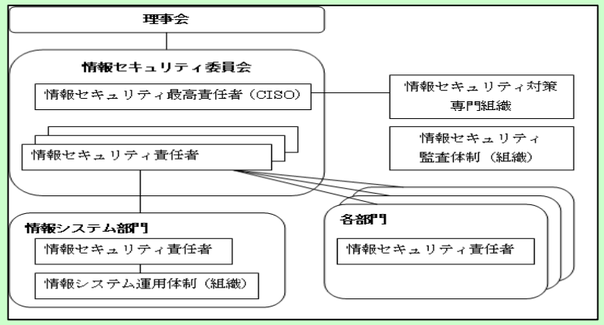
2. 組織的対応

チェックリスト項目	説明	対策例	関連資料
(1)意思決定	【狙い】 「意思決定」の狙いは、「誰が」、「何を」判断し、「行動」できるかを定めることです。そのためには、①全学横断的な意思決定組織であること、②各種情報の取り扱い者が明確であり、役割と責任範囲を規定できていること、③情報セキュリティに関するルールを策定し、承認、周知徹底できていること、が必要となります。たとえば、図1のような体制が構築できているかがポイントです。また、セキュリティインシデント発生時においては、管理運営を問われることが多くあります。そのためにも適切な体制整備が重要となります。	 図1．情報セキュリティの組織サンプルイメージ	
・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	情報セキュリティ対策には、費用も工数もかかり、多くのリソースを投入しなければなりません。また、対策が不十分であることが大学組織としての信頼を失うことに繋がります。情報セキュリティ対策を全学的に推進するには、経営判断を含む組織横断的な体制が必要です。よって、経営判断ができる理事会において、「情報セキュリティ最高責任者（以下CISO（Chief Information Security Officer）という」をおくことが求められます。	・理事会の責によりCISOを選出する。 ・各部門、各学部での情報セキュリティ責任者の決定 ・全学横断的な情報セキュリティ委員会の設置。 ・情報セキュリティ対策専門組織とCISOの連携構築	【参考情報】 ・ JISQ27002：2006 ・ 独立行政法人情報処理推進機構（IPA）「情報セキュリティ対策 実践情報」 http://www.ipa.go.jp/security/awareness/awareness.html 【参考情報（書籍）】 ・「ISO/IEC27001情報セキュリティマネジメントシステムISMS構築読本」志村満（著） ・「情報セキュリティ教本　改訂版　ー組織の情報セキュリティ対策実践の手引きー」独立行政法人情報処理推進機構（IPA）（著）
・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。	情報システム環境における脅威や脆弱性は日々急速に変化していることから専門的知識と経験が必要です。CISOが情報セキュリティに関しての課題解決のために、情報セキュリティ対策の専門組織と連携することが、より効果的な手立てと言えるでしょう。専門組織は、学外組織の活用も考えられます。		
・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。	大学は、企業と比べ情報を一元管理することが困難な組織です。よって、各学部での教育活動や各部門のサービスに即した対策を具体的に検討できる体制を整備し、組織単位で情報セキュリティ責任者を確定し、その役割を明確にしておくことが重要です。		
(2)運用体制	【狙い】 情報セキュリティ対策は、常に対策改善が求められることから、Plan（企画・計画）、Do（実行）、Check（点検・評価）、Act（改善処置）を行うPDCAサイクルでのプロセスアプローチが必要となります。情報セキュリティ対策は一度行ったら終わりというものではなく、情報環境の進展に伴い絶えず変化し、改善が求められるのです。以下に記述する監査体制と運用体制を組織として分けることが望ましいと考えられます。		
・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。	情報セキュリティは、常に対策改善が求められる仕事です。よって、組織整備において、PDCAサイクルでのプロセスアプローチが可能な体制を構築することが必要となります。運用体制では、Plan（企画・計画）、Do（実行）、を行い、Check（点検・評価）、Act（改善処置）は監査体制が担うことが望ましいです。また、セキュリティ対策は、全学横断的に対応する必要があるため、組織単位での体制確保が求められます。	・ 情報セキュリティ運用体制の整備 情報セキュリティのための全学組織 ・ 情報セキュリティに関する規格・法令・技術動向などの情報収集 ・ 学内外で発生しているセキュリティインシデントの把握 ・ 組織の情報セキュリティ対策状況を定期的に確認する仕組みと相談・支援体制の構築	
・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。	情報セキュリティの運用体制では、学内外での情報セキュリティインシデント、情報環境の変化を把握することで、迅速かつ適切なセキュリティ対策を講じることを可能とします。		
・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。	学内で使用しているシステムにおいて、ライセンス違反などを発生させないため、管理することが必要となります。		

チェックリスト項目	説明	対策例	関連資料
(3)監査体制	【狙い】 情報セキュリティ対策が当初目指していた通りの効果をあげているか、現実と乖離しているところはないかなどの実施状況を確認していくことが必要です。このため、運用体制と監査体制を分ける必要があります。		
・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。	導入した対策が計画通りに実行されているか、予定通りの効果があがっているかを検証することが求められます。よって、Check(点検・評価)、Act(改善処置)を担うための監査体制を整備するなど、意思決定機能を点検する仕組みが必要となります。	・ 監査体制の構築 (監査体制の構築が困難な場合は、情報セキュリティ対策の運用状況を定期的に確認する仕組みや相談・支援体制を構築)	
・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。	情報セキュリティ対策が適切になされているかを判断するためには、専門的知識や経験が必要であることから、専門家による評価が必要となります。ただし、必ずしも学内での組織整備が必要ではなく、学外リソースを有効活用することも可能です。		
・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。	PDCAサイクルを担保するために運用体制と監査体制を分けて設置することが望ましく、点検、評価、改善する体制の確保が必要となります。また、セキュリティ対策は、全学横断的に対応する必要があるため、組織単位での体制確保が求められます。そのために、情報セキュリティポリシー策定の際には、「いつ」、「誰が」、「どのように」対策への点検、評価、改善を行うかを記載しておきます。		
・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。	情報セキュリティ対策を実施した結果として、各種実績データがどのように推移しているかを正確に把握することが必要となります。実績データを基に現対策の品質を判断し、改善の具体的な指標を示すことが可能となります。		
(4)情報セキュリティポリシー	【狙い】 情報セキュリティポリシーは、全学の方針や行動指針をさします。情報セキュリティポリシーが策定できていないと、法人としての社会的責任を果たすことができません。その策定には大学としてのガバナンスの発揮が求められます。 また、情報セキュリティポリシー策定にあたり、以下の3点について押さえておきたい。 ①危機管理の一部と位置づけて全学的に取り組む ②セキュリティに対する侵害を阻止し、情報資産を守る。 ③学内外のセキュリティを損なう加害行為を阻止し、社会的信頼を確保する。 「提言 私立大学向けネットワークセキュリティポリシー（2003.1）」より抜粋 SaaS(Software as a Service)や、それを内包するクラウドコンピューティングなど学外のサービス提供を求める形態が今後増加していくことが予想されますが、この場合でも大学の策定した情報セキュリティポリシーを遵守する必要があります。		
・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とは、組織において実施する情報セキュリティ対策の方針や行動指針のことです。情報セキュリティポリシーの構成としては、「基本方針（ポリシー）」、「対策基準」、「実施手順」の3階層とするのが一般的です。 基本方針（ポリシー）は、「なぜ情報セキュリティ対策が必要か」という「Why」について規定します。  図2. 情報セキュリティポリシー構成イメージ	・ 情報セキュリティポリシーを策定体制の確立 ・ 情報セキュリティポリシーを策定する (基本方針には以下の項目を含む) ①基本理念及び目的、②情報セキュリティポリシーの役割と位置付け、③情報セキュリティポリシーの見直しと改訂、④法令等の遵守、⑤適用対象範囲、⑥情報セキュリティポリシーの全体構成、⑦評価、⑧罰則、⑨用語の定義、⑩付則。 (対策基準と実施手順については、それぞれの項目を参照)	【参考情報】 提言 私立大学向けネットワークセキュリティポリシー (2003.1) http://www.juce.jp/LINK/report/netsec2002.pdf 【参考情報(書籍)】 ・「ISO/IEC27001情報セキュリティマネジメントシステムISMS構築読本」志村満(著) ・「情報セキュリティ教本　改訂版　－組織の情報セキュリティ対策実践の手引き－」独立行政法人情報処理推進機構(IPA)(著) 【参考雛形】 ・JISQ27002：2006 ・「高等教育機関の情報セキュリティ対策のためのサンプル規程集」国立情報学研究所 http://www.ieice.org/jpn/ h191031.html
・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。	基本方針は、情報セキュリティ対策における憲法のようなものです。一度定めたら頻繁に改訂するものではないので、これらの項目は必ず含んでいる必要があります。		
・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。	情報セキュリティポリシーは、策定が目的ではなく、学内関係者が理解し、遵守することが求められます。		

<table>
<tr><th>チェックリスト項目</th><th>説明</th><th>対策例</th><th>関連資料</th></tr>
<tr><td>(5)情報セキュリティポリシーの対策基準</td><td colspan="2">【狙い】
対策基準は、基本方針を受けて具体的なルールを定めるものであり、情報セキュリティポリシーの中心部分となり、「何を情報セキュリティ対策として実施すべきか」という「What」について規定します。</td><td></td></tr>
<tr><td>・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。</td><td>対策基準の策定には、大学の方針、情報システム環境、システムの脆弱性の把握など高いスキルが必要であり、一から作るのは相当な作業となります。よって、雛形を参考とし大学の要件として再整理することが適切です。ただし、雛形をコピーし、組織名だけを変更するといった作成手順では、対策を内実化し大学全体に浸透させていくことはできないため、組織の特性を考慮し作成していくことが重要です。</td><td rowspan="2">・下記の項目を参考に実施対策基準を策定する

提言 私立大学向けネットワークセキュリティポリシーをもとに構成

<table><tr><th></th><th>対策基準</th><th>内　容</th></tr><tr><td>①</td><td>インターネット利用に関する対策基準</td><td>インターネットへ接続し、何かサービスを受けようとする全ての人が守るべき基準</td></tr><tr><td>②</td><td>外部公開に関する対策基準</td><td>学外に情報を公開するためのサーバ設置に関する基準</td></tr><tr><td>③</td><td>内部利用に関する対策基準</td><td>学内でネットワークにコンピュータを接続する際の基準</td></tr><tr><td>④</td><td>ＶＰＮおよび専用線接続に関する対策基準</td><td>主に専用線やブロードバンドアクセスライン等の双方向通信可能な回線を用いて外部と接続する際の基準、</td></tr><tr><td>⑤</td><td>リモートアクセスに関する対策基準</td><td>学外からのリモートアクセスについての基準</td></tr><tr><td>⑥</td><td>ウイルス対策に関する対策基準</td><td>コンピュータウイルスに関する対策基準</td></tr><tr><td>⑦</td><td>学生のプライバシーに関する対策基準</td><td>学生のプライバシー保護に関する対策基準</td></tr><tr><td>⑧</td><td>人的セキュリティ対策に関する対策基準</td><td>人が引き起こす可能性のある種々のセキュリティ上の問題に関する対策基準</td></tr><tr><td>⑨</td><td>物理的セキュリティ対策に関する対策基準</td><td>盗難や破壊を含めた物理的なセキュリティ問題への対策基準</td></tr></table>【表５】対策基準（遵守事項）の例

（上記に組織的セキュリティ対策も含める。）</td><td rowspan="2"></td></tr>
<tr><td>・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。</td><td>対策基準は、策定が目的ではなく、学内関係者が理解し、遵守することが求められます。また、業務委託を行う場合であっても、大学の情報資産を取り扱う以上、大学で定めた情報セキュリティポリシーを遵守させる必要があります。</td></tr>
<tr><td>(6)情報セキュリティポリシーの実施手順</td><td colspan="2">【狙い】
実施手順は、「情報セキュリティ対策をどのように実施するか」という「How」について規定します。具体的には、対策基準で定められた内容を、構成員の行動指針としてガイドライン化します。</td><td></td></tr>
<tr><td>・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。</td><td>対策基準で定められた内容を、マニュアルやガイドラインなどに具体化することで、システム運用や作業手順に間違いが起こらない手立てとして整備します。</td><td rowspan="3">・以下の項目を含んだ実施手順を策定する
提言 私立大学向けネットワークセキュリティポリシーを参考に構成

①学生（教育利用）向けガイドライン（案）
「位置付け、一般利用、電子メール利用時、Webアクセス、ファイル転送、公開情報に関する遵守事項、ウイルス対策、報告義務、罰則」
②教員（研究利用）向けガイドライン（案）
「位置付け、接続時、サブネット管理、利用管理、ログ管理、セキュリティ監視、外部公開時のアクセス管理、安全な設定、公開情報に関する遵守事項、リモートアクセス、罰則」
③職員（事務利用）向けガイドライン（案）
「位置付け、一般利用、電子メール利用時、データ転送Webアクセス、情報の取り扱いに関する遵守事項、ウイルス対策、機器購入時の注意、罰則」
④ネットワーク管理者向けガイドライン（案）
「位置付け、管理者の役割と権限、特権ユーザとしての操作、安定稼働のための作業、セキュリティ管理、緊急対応と対外連絡、ログ管理、機密管理、個人情報保護、その他、罰則」
「提言 私立大学向けネットワークセキュリティポリシー（2003.1）」より抜粋</td><td rowspan="3"></td></tr>
<tr><td>・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。</td><td>セキュリティ対策は、全学横断的に対応する必要があるため、組織単位での点検、評価、改善が求められます。</td></tr>
<tr><td>・危機管理のための実施マニュアルを作成しているか。</td><td>通常運用時のマニュアルだけでなく、障害発生時などの危機管理のための実施マニュアルが必要となります。</td></tr>
</table>