国立大学法人
経営ハンドブック(2)

第５章　情報システム管理

独立行政法人　国立大学財務・経営センター

5. 1　国立大学法人における情報システムの特性

大学は「学術の中心として、広く知識を授けるとともに、深く専門の学芸を教授研究し、知的、道徳的及び応用能力を展開させることを目的とする」（学校教育法第 83 条）と定義される。また、国立大学法人については「大学の教育研究に対する国民の要請にこたえるとともに、我が国の高等教育及び学術研究の水準の向上と均衡ある発展を図るため、国立大学を設置」（国立大学法人法第 1 条）するとされている。これらを受けて大学の本質的機能は、下記に集約される。

・知を伝達する「教育」

・知を創造・発見する「研究」

・知を応用する「社会サービス」

これらの機能を果たすために必要な情報は何か、そのための情報システムはどのように構築・運用するかが課題となる。これらに加えて、国立大学法人には効率的な運営が求められるため、民間と同様に経営管理を行うための情報が必要である。したがって、人事管理や財務管理などのバックオフィス（事務局など）のオペレーション系やマネジメント系の経営管理情報システムも当然に必要となる。

また、国立大学法人の特徴の一つとして、各学部、図書館、研究所、管理棟、附属病院、附属学校などが一箇所の敷地内に設置されているというより複数の敷地に分散して設置されているケースが多い。さらに、国立大学法人の公的側面の特徴として、主に「知」を中心とした関連情報に関して民間企業より積極的な開示が求められる。具体的には、学生や教職員、他大学や関連研究機関の他、国民、企業、自治体、政府といった国立大学法人を取り巻く様々な利害関係者に対する種々の情報の発信や収集も、大学運営には欠かせない要素である。このような国立大学法人の広範な活動展開や情報の公開性に対応したネットワーク面の充実整備が図られることに加え、学内外の利害関係者に対し、その属性に応じてアクセス可能な情報資産を峻別するなど、セキュリティの構築も必要となる。

一方、国立大学法人は個々の基本理念や経営戦略に基づいて経営されることから、上記の本質的機能のどこに重点を置くかはそれぞれの国立大学法人によって異なる。したがって、どこまで、どのようにシステム化するか、情報システムに求める機能は何かなどの情報システム戦略についても各国立大学法人によって異なるものと考えられる。本章ではそのような点も考慮した上で、国立大学法人という共通性から、その有すべき情報システムに求められる機能に焦点を当てて記述する。

5. 2　国立大学法人の情報システムの概要

国立大学法人の情報システムとしては、教育、研究、社会サービスという本来の業務を支援する直接業務支援系システム、バックオフィスにおいて本来の業務を間接的に支援するオペレーション系システム、経営管理を高度化するマネジメント系システムが必要である。主な直接業務支援系システムとしては、教育、研究を直接支援する（1）教育・研究情報システム、及び社会サービスにおける代表的な病院サービスを支援する（2）病院情報システムが該当する。また、教育、研究あるいは社会サービスを実施する際に生じるバックオフィスの業務を支援するオペレーション系システムとしては、(3) 学務・学生情報システム、(4) 図書館情報システム、及び (5) 総務・広報情報システムが該当する。さらに、マネジメント系システムとしては、(6) 経営管理・目標管理情報システムが該当する。それらのシステム特性及び代表的な留意点を述べると以下のようになる。

（1）教育・研究情報システム

教育・研究情報システムとしては、各学部で管理されている教育用ナレッジシステム、遠隔地や通信教育用のe-learningデータベースなどの教育用情報システム及びシミュレーションツールなどの研究用各種処理システムや、研究用ナレッジシステムが該当する。これらは「知」の伝達・創造・発見を支援するシステムである。システム上の留意点としては、各学部の学生や教員が活用しやすいような「知」の伝達・発見の切り口である「類型化」、「体系化」の整備や検索の利便性が肝要となる。また、「知」の創造である「創出」に関しては、人事管理制度と直接・間接的に連動していることが重要であり、(6) の経営管理・目標管理情報システムに必要なデータ項目との整合性が必要となる。

(2) 病院情報システム

病院情報システムとしては、直接診療を支援するオーダーリングなどの診療支援システム及び輸血、麻酔、放射線などのコメディカルシステムが該当する。ここで、オーダーリングシステムとは、カルテや各種伝票に書かれた指示（オーダー）を、病院業務の省力化とサービス提供の短縮化を目的として電子的に行う「検査・処方等に係る情報伝達システム」のことをいう。また、コメディカルとは医師とともに力を合わせて医療を行う薬剤師、臨床検査技師、輸血検査技師、麻酔技師、放射線技師などの専門職が協同して医療を行うことを意味し、これをサポートするのがコメディカルシステムである。これらのシステムは診療行為や検査行為などの病院サービスを実施する上で必須であり、現場の利便性に基づいて構築されている。しかし、(1) と同様に病院管理会計システムなどのマネジメント系システムとの連動時には適切な収入・経費の直課データや配賦基準データが取得できない場合も多く、当該システムとのデータ連携の整合性に留意すべきである。

(3) 学務・学生情報システム

学務・学生情報システムとしては、学籍、シラバス、履修、成績などの学務情報を管理する学務情報システムと、休講や試験日程情報といった日常的な事務連絡にかかる情報、学内の年間行事に関する情報、学外研修、就職情報など様々な面から学生を支援する学生サポートシステムが該当する。これらのシステムは学生の利便性を考慮した設計及び構築となるのは当然であるが、これらと関連するバックオフィス全体の業務改善を同時に実施することが肝要である。

(4) 図書館情報システム

図書館情報システムとしては、図書検索や各種情報提供などを実施する利用者用システムと図書購入検収、蔵書管理及び利用統計などの業務用システムが該当する。利用者用システムに関しては、蔵書検索の容易性などの利用者の利便性を考慮する必要がある。一方、業務用システムは図書業務全般の業務改善とともに実施する必要があるだけでなく、利用統計などは (6) の経営管理システムとのデータ連携性も考慮しなければならない。

(5) 総務・広報・施設管理情報システム

総務・広報情報システムとしては、会計関連データを扱う総務情報システムと大学の広報全般を扱う学校情報システムが該当する。総務情報システムの留意点としてはリアルタイムの予算差引管理（国の予算を扱う特性)、固定資産の財源把握、取引における予算科目と勘定科目の把握、授業料債権の収益化（国立大学法人の会計特性）などがあり、どこまでシステムで取り扱うべきかを業務設計とともに検討する必要がある。学校情報システムについては、広報業務の改善とともに実施することが効果的である。また、人事システムについては、教職員の住所、通勤経路、家族といった人事情報の管理のみならず､将来的には人事評価に寄与するデータの管理ができることが望まれる。また人事システムは給与システムと扱うデータが重複することから、データの連携は必須である。

さらに、施設管理情報システムは単にコストデータだけでなく、当該施設で点検や評価すべき品質データや利用状況のデータが必要となる。

(6) 経営管理・目標管理情報システム

経営管理・目標管理情報システムとしては、経営業績評価、プロジェクト管理及び病院管理会計など、主に会計データなどの定量的情報を扱う経営管理システムと業務遂行状況などの定性的情報も扱う目標管理システムがある。これらのシステム設計は（1）～（5）の情報システムに依存する部分が大きく、それらのシステム構築以前に要件定義されていることが望ましい。

以上の各システムの留意点でも述べているが、マネジメント系システムの精緻化、システム相互間の整合化及びシステムライフサイクル全体のコスト低減化などのためには、マスタ管理の一元化やデータベース相互間のデータ項目の整合性などが必須である。したがって、マネジメント系システム以外のシステム導入時にはマネジメント系システムの要件を十分考慮するとともに、データ連携が必要な他システムとの整合性も視野に入れた設計をすることが必要である。

また、特にバックオフィスのオペレーション系システムについては、システム調達と同時に国立大学法人全体を考慮した重複する業務や帳票の削減などの業務改善を組織横断的に実施し、定型業務の効率化を図ることがシステム投資効果を高めることからも必須である。このことは、企画立案などの非定型業務時間を確保することとなり､バックオフィス業務の高度化も促進することとなる。現状、多くの大学では、あるシステムから出力したデータを別のシステムに連携する際にデータの変換作業を必要としている。例えば、従来から使用されているシステム（国立大学用新汎用システムや病院システム）などから財務会計システムへのデータ連携の際には、Access などの変換ツールによるか､あるいは出力帳票をベースとして新規に手入力されていることがある｡このような場合、

データ連携に関し、システム開発や保守業務などのシステムライフサイクルコスト全体が増加する。また、日常業務においてもデータ入力時とデータ収集時の両時点で金額などのチェックを実施しなければならず、法人全体として業務が増大する。これは連携開発コストの負担も含め、各担当部署が各システムの企画から保守までの管理を個別最適で実施していることが主要因である。したがって、国立大学法人全体の最適化を志向した情報システム面の戦略構築や管理を実施するトップマネジメント体制の構築を考慮すべきである。具体的には、システム全体を俯瞰し調整する最高情報担当責任者（CIO：Chief Information Officer）及びCIO直属の専門部署またはプロジェクト組織の設置などが必要と考えられる。

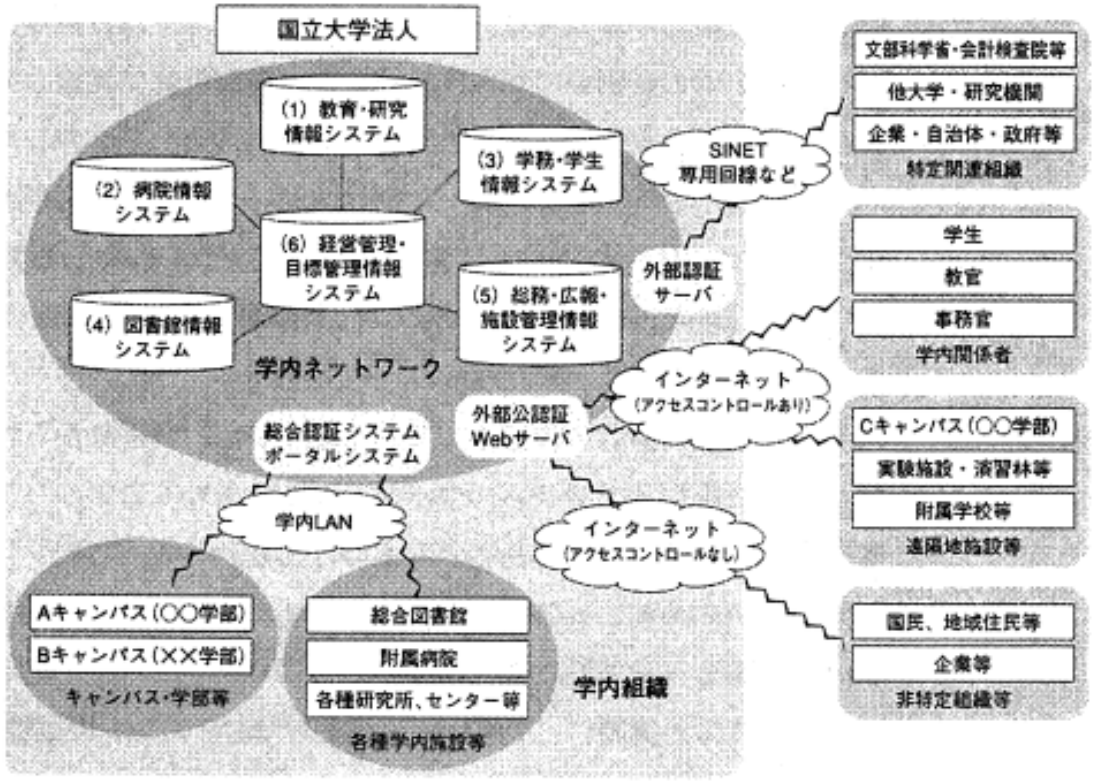
なお、今後の直近の展望として、平成19年には従来から使用されてきた国立大学新汎用事務システムのサポートが停止されることから、これに代わる各事務システムの調達が実施されるものと想定される。このシステム調達はバックオフィスの業務、システムの全体最適化を志向する良い機会である。この際に全体のあるべき業務フローを策定し、これをサポートするシステム全体像を明らかにすると同時に、管理体制の発展も検討することが重要である。

一方、ネットワーク面において、実際の物理的なサーバ設置場所はリスク分散の観点から複数箇所に及ぶことが想定される。この場合、データの収集及び配信に関し、学部や病院などの学内部局に対しては学内LAN、学内LANでカバーできない範囲の利害関係者、組織などに対してはインターネットなどの利用が想定される。この場合の留意点は、情報リソースの重要性レベルに応じて、許可される人物のみが当該情報への接触が可能であるなどのアクセスコントロールを始めとする種々のセキュリティが考慮されていなければならない。

具体的には、国立大学法人の特定の利害関係者のうち他大学、監督官庁及び共同研究を実施している企業や自治体などの特定関連組織に対しては、より機密性の高い情報連携を実施していることが多いものと想定される。したがって、学生や教員などの学内関係者のリモートアクセスに対しては、一定の機密性を確保の必要から、パスワード管理などによる一定レベルのアクセスコントロールを考慮したインターネット環境での情報集配信が有効である。また、国民や地域住民などの非特定組織に対しては、大学から社会一般に対する情報の発信を行うことを目的とするため、特にアクセスコントロールを行わないインターネット環境での情報集配信が効率的である。

以上を念頭に、図表１において国立大学法人における将来的なシステム概念図を一例として記載する。

図表１　国立大学法人システム概念図



※国立大学法人システム

(1) 教育・研究情報システム
- 教育用情報システム（教育用ナレッジ、e-learning用DB　等）
- 研究用情報システム（研究用各種処理、研究ナレッジ等）

(2) 病院システム
- 診療支援システム（オーダリング、病床管理、病歴管理　等）
- 各診療システム（手術・麻酔、放射線、輸血、検査　等）

(3) 学務・学生情報システム
- 学務情報システム（学籍管理、シラバス・履修・成績管理　等）
- 学生サポートシステム（休講等各種学務情報、就職情報　等）

(4) 図書館情報システム
- 利用者用システム（図書検索、各種情報提供、電子図書館等）
- 業務用システム（蔵書管理、閲覧管理、発注受入、相互貸借、統計　等）

(5) 総務・広報・施設管理情報システム
- 総務情報システム（予算管理、財務会計、医事会計、人事・給与　等）
- 学校情報システム（入試、講座案内、大学情報案内　等）
- 施設管理情報システム（コスト、品質、利用状況　等）

(6) 経営管理・目標管理情報システム
- 経営管理システム（経営業績評価、プロジェクト管理、病院管理会計　等）
- 目標管理システム（中期目標管理、学部別目標管理、個人別目標管理　等）

5. 3　情報システム管理の基礎

（1）情報システム管理の目的及び必要性

現代社会の組織において、情報システムはますます多様化、複雑化し、それに伴い様々なリスクが顕在化してきている。また、情報システムに関わる利害関係者も組織内にとどまらず、社会へと拡大している。したがって、このような情報システムに関わるリスクを適切にコントロールすることが組織における重要な経営課題となっている。

情報システムの重要性の高まりを受けて、経済産業省は2004年10月8日に、情報化投資が適正かどうかを判断する手がかりとなる「システム管理基準」と新「システム監査基準」の二つの基準を発表した。この「システム管理基準」は、旧システム監査基準の実施基準（企画業務、開発業務、運用業務、保守業務及び共通業務に対する監査基準）に加え、情報戦略（全体最適化、組織体制、情報化投資、事業継続計画、コンプライアンスなど）に対する監査基準を統合したものである。つまり、「システム管理基準」は、情報システムを持つ組織がどのように行動すべきかをまとめたものであり、システム管理全般にわたるガイドライン的な位置付けのものと考えることができる。この「システム管理基準」を参考に、組織が情報システムに関わるリスクを適切に管理する目的を挙げると、以下の4点となる。

・情報システムが、組織の経営方針及び戦略目標の実現に貢献するため
・情報システムが、組織の目的を実現するように安全、有効かつ効率的に機能するため
・情報システムが、内部又は外部に報告する情報の信頼性を保つように機能するため
・情報システムが、関連法令、契約又は内部規定などに準拠するようにするため

これらの一般的な目的を考慮した上で、国立大学法人におけるシステム管理の必要性を考察する。

国立大学は今回の法人化により、予算、組織、人事など様々な面での規制が緩和され、大学の裁量が大幅に拡大された。この結果、大学経営について大きな裁量権限を与えられた学長などのトップマネジメントには、それに応じた実行責任を有することになる。さらには教育研究の世界に第三者評価が導入されることにより、確実に国民の付託に応えるべく国立大学法人の経営を行う必要がある。すなわち、拡大した経営面の権限を活用して学内の資源配分を戦略的に見直し、機動的に実行し得るよう、全学的な視点に立ったトップダウンによる意思決定の仕組みを確立する必要が生じてきている。したがって、トップマネジメントは、自ら設定した経営目標の達成を阻害するリスクについては、組織全体にわたるリスク管理状況を把握し、適切なリスク管理を行う必要がある。これは一般企業同様に、国立大学法人においてもコーポレートガバナンスの確立が一段と重要になっ

てきていることを意味している。その様々なリスクの中でも、効率的、効果的な大学経営のために導入した情報システムが当初の目的の達成を阻害するリスク（情報システムリスク）が、大学経営にとって致命的な損害を与える可能性があることを、トップマネジメントは十分認識しておかなければならない。例えば、情報システムリスクには次のようなものが挙げられる。

・巨額の情報システム投資をしたが、利用者にとって当初想定した効果が得られない。
・外部や内部から不正なアクセスを受け、学内の個人情報が改ざんされる、あるいはまた外部に漏洩する。
・システムダウンにより、業務活動が停滞する、あるいは活動できなくなる。

したがって、トップマネジメントは、経営目標達成のために情報システム戦略を策定・実践し、その結果についての責任を負うとともに、情報システムリスクを適切に管理するための方針や目標を設定し、情報システムのリスク管理体制を構築していかなければならない。このように、経営の観点から情報技術（IT）を適切に運営管理することを「IT ガバナンス」という。具体的には、組織のもつ経営戦略と情報化戦略、情報化戦略と全体の情報化計画、全体の情報化計画と個々の情報システム間の整合性がとれているか、情報システムの開発や運用が計画通りに行われているかを管理することをいう。

また、国からの財政投入に支えられる国立大学法人は大学経営や教育、研究などの結果についての説明責任も有することになる。すなわち、国立大学法人は業績や財務内容などに関し、正確な情報の開示を行う必要があるとともに、開示した情報について、客観的な資料に基づく説明責任を確保しなければならない。このような情報開示や説明責任の確保を実効性のあるものとしていくためには、トップマネジメントの方針や指示を受けて活動する組織や教職員の業務執行状況を的確に把握しなければならず、そのためにはいわゆる内部統制の充実を図ることが不可欠である。とりわけ業務のほとんどを情報システムに依存している現代の業務環境においては、情報システムに対するリスクを把握し、適切に管理することが必要となっている。

(2) 情報システム管理体制

情報システムリスクに対して、これまで主体的なリスク管理を担っていたのは情報システム部門であった。情報システム部門は、情報システムの企画・開発・保守・運用業務を通じて、利用者に情報システムを提供する立場にあったので、情報システムリスクのほとんどが情報システム部門に集中していたからである。ところが今日では、情報システムの持つ役割が拡大して、その所在も情報システム部門にとどまらず、組織全体に広がり、全体的な情報システムリスク管理体制の構築が求められるようになった。

また、技術的にも情報システムが、コンピューターセンターのメインフレームシステムで集中的に管理され、その開発や運用も情報システム部門、あるいはシステム運用部門を対象に設けられるものが大半であり、またそうすることが情報システムリスク管理の観点から効果的であった。現在は、小型・分散化、LAN/WAN やイントラネットの浸透、オープンネットワークとの接続、各個別システムの複雑化などシステムの利用形態が大きく変化している。このような状況においては、情報システム全体を見渡したうえで重要な情報システムリスクを漏れなく識別し、適切な管理を設ける必要がある。

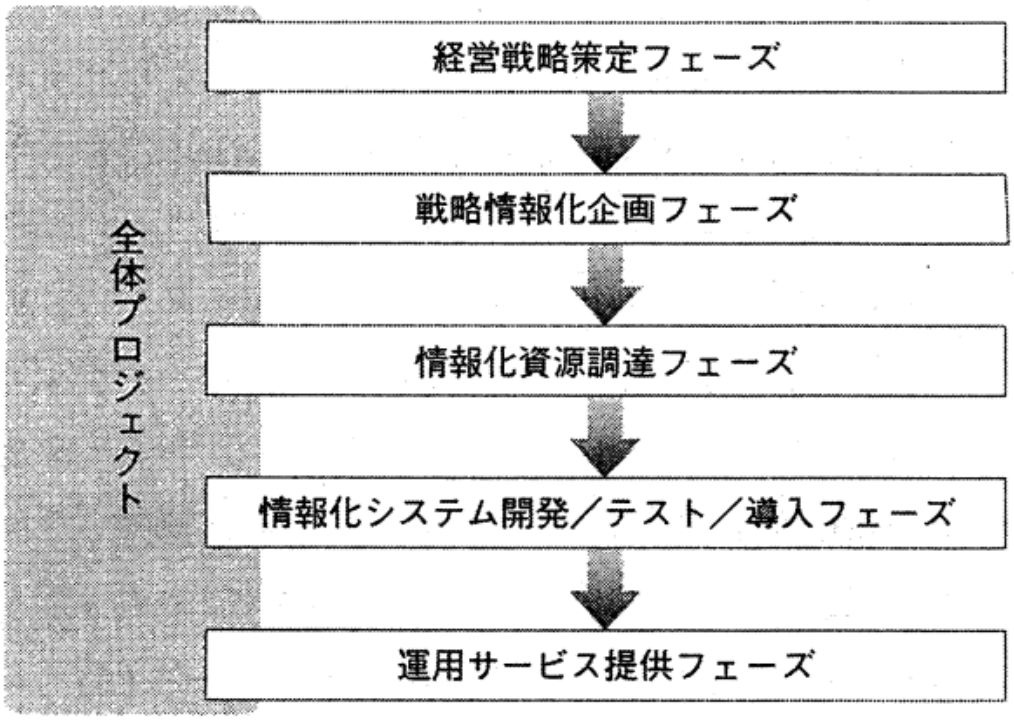
以上のような背景より、情報化戦略の策定のような経営に密着した業務では、トップマネジメントが直接関与することが重要となる。そのため、トップマネジメントに CIO を設置している組織も増加している。CIO の主たる任務としては、IT ガバナンスの確立がある。CIO に求められる機能は、経営戦略の一部としての情報化戦略を立案・実行すること、また逆に情報技術に基づいた形で自組織に適切な経営戦略を提案すること、部門間や外部との調整を行い業務組織や業務プロセスを改革して情報システムに適合させること、そして情報部門を含めて全社の IT 資産（人材、ハードウェア、ソフトウェアなど）の保持や調達を最適化することなどである。日本では米国流の執行役員は必ずしも一般的ではなく、CIO という肩書きは部門（ライン）の長である情報システム部長、あるいは情報システムの担当者というような意味で使われている場合もある。しかし、本来的にはトップマネジメントレベルの役職で「IT を活用して経営を変革するミッションを持つ」という役割を担っている。

(3) 各段階における情報システム管理の概要

情報システム管理を具体的に定義した場合、情報システム管理とは、そのライフサイクルの中で効果的な情報システム投資を行い、関連するリスクを低減するためのコントロールを、適切に整備・運用することを目的として実施するものである。なお、ライフサイクルとは、組織が経営戦略に整合した効果的な情報システム戦略を主体的に立案し、その戦略に基づいた情報システムの企画・設計・開発・運用・保守・廃棄までを指している。ここで、このライフサイクル全体をプロジェクトと捉えた場合、プロジェクト管理の手法を活用できる。通常、プロジェクト全体は小さな期間・規模でプロジェクトを区切った単位（フェーズ）の各段階の部分プロジェクトから構成される。プロジェクト管理は、①立上げのプロセスで始まり、必要に応じて②計画、③実行、④チェック、⑤アクションを繰り返し（PDCA サイクル）、⑥完了のプロセスで終了し、次期段階に移行するという原則がある。その理由は、プロジェクトは個別に実施されるため、絶えずリスクを伴っているものであるが、こうしたプロジェクトのリスクと効果を各段階で比較考慮し、プロジェクト全体を続行するか、中止するかの意思決定をトップマネジメントが確実に実施していくためである。

ここでは、情報システムライフサイクル全体を図表 2 で示すとともに、各段階について具体的に述べる。

図表 2　情報システムの構築プロジェクトのフェーズ



第一段階の「経営戦略策定フェーズ」は、情報システム戦略のベースとなる経営戦略を策定するフェーズであり、本来は情報システムのライフサイクルを直接構成するものではない。しかし、情報技術の発展は新しい業種・業態を生み出すとともに、情報システムが密接に業務の遂行に関わり、大きなインパクトを与えることには留意すべきである。つまり、常に最先端の経営を実施している国立大学法人は別であるが、経営戦略を検討する際は、同一経営モデルの情報システム活用動向を無視することはできないのである。例えば、コンピュータネットワークを通じた教育である「e ラーニング」という概念を大学の経営戦略に採用する場合などは、すでにこれを実施する他の組織体の動向に注視しなければならない。このことは、国公私を問わず、同一経営モデルの情報戦略が自大学の経営戦略に影響を与えるということを意味する。このフェーズの詳細は既述したが、成果物である経営戦略企画書は経営目標を達成するためのビジネスモデルや計画も含めて表現され、情報システム戦略のインプットとなる。

第二段階の「戦略情報化企画フェーズ」では「経営戦略を実現するには何が必要か」ということを情報化の視点から策定する。この戦略情報化企画フェーズでの成果物は戦略情報化企画書となる。以後のフェーズでの活動のベースとなる計画書として、情報システム化の背景、コンセプト、範囲、概要、情報システム概念図および導入にあたってのプロジェクト体制、マススケジュールと呼ばれる大日程、費用対効果などが盛り込まれる。

この段階の留意点は、情報システムが企業目的や戦略目標の実現に向けて適切に計画、組織化され管理される必要があるということである。その理由は、最新の経営戦略と整合性のとれた情報化戦略の策定、これを具体化した中長期、短期の計画立案、あるいは組織運営などが適切に行われないと、国立大学法人の情報システムおよびそれに関する活動全体が有効性や効率性を失うというリスクに直面するからである。したがって、このフェーズにおいては情報システムの計画と管理のプロセスの中に情報システムリスクを管理するための手続を確立し、遵守する必要がある。特に重要な「経営戦略と情報化戦略の整合性」及び「情報化戦略の全体最適」については、4. 情報システムの戦略・企画にて詳述する。

第三段階の「情報化資源調達フェーズ」では、戦略情報化企画フェーズで作成された戦略情報化企画書を基に、情報システムへの要求事項を文書化する。具体的には、情報システムに必要な機能・性能・操作性・信頼性などを明確にし、文書化する。

今日の情報システムでは、自組織のみで設計・開発・運用・保守を実行する場合は少なく、その一部あるいは全部を外部のベンダーといわれる専門機関に委託することが多い。この理由は、情報システムに関わるコストの削減、ユーザー企業内要員の削減、ベンダーの先端技術の活用及びコアビジネスへの資源集中などのためである。

このような外部委託を実施する場合、上記の文書化とともに導入にあたっての条件となる事項(著作権や納期などの契約事項）も含めて文書化する。この文書を、提案依頼書（RFP：Request For Proposal）という。この RFP は、開発者に的確な提案を依頼するための文書であり、自大学にとり必要な IT システムとはどのようなものかについて開発者に理解してもらい、その上でさらなる提案を促すような内容となる。

外部委託を実施する場合の留意点は、委託先であるベンダーとの契約内容がどのようなものであれ、情報システムリスクの適切な管理に対する責任は委託元である国立大学法人にあるということである。しかしながら、ベンダーが別機関であるため国立大学法人が直接的にベンダーで行われる活動を管理することは困難である。したがって、国立大学法人はベンダーにおける開発や運用が適切に行われ、ベンダーとの間で十分なコミュニケーションがとられるように、契約や取決めなどを通じた効果的な管理を実施し、適切に実践する必要がある。

この段階での成果物は RFP や評価基準書のほかに、開発者を含めた関係者の役割、週単位ベースの中日程、各作業単位の予算や情報システムが目指す品質などの情報化実行計画書がある。情報化実行計画書により導入計画がさらに具体的になり、各関係者の役割がより明確になるのである。特に重要な「契約に盛り込むべき内容」については、5. 情報システムの設計・開発にて詳述する。

第四段階の「情報システム開発／テスト／導入フェーズ」では、中長期、短期の情報システム計画や利用部門からの開発要求に基づいて、新規情報システムや個別システムの開発、修正、追加などについての設計、開発、テスト、本番移行までを含むフェーズである。

この段階での留意点は、前段階までの要件定義などが設計やプログラミングに正確に伝達されることが非常に重要である。さらに、機能要件や品質要件を充足した効率的で信頼性、安全性の高いシステムを開発すること、また開発過程における生産性を高めながら重要情報や資源の安全を確保することが必要である。

また、各部局の情報システムの有効性や効率性への要請を優先し、ユーザーニーズを迅速かつ柔軟に情報システムに反映する部分最適と国立大学法人全体の安全性や効率性などの全体最適との間にトレードオフの関係が生じることにも留意すべきである。この区別が明確に行われないと、組織全体にわたる観点で重要な情報や業務の安全性がリスクに晒されたままになったり、逆に個別部局本来の有効性や効率性の発揮を妨げるような過度の管理が設けられたりするおそれがある。したがって、部分最適と全体最適の両面を勘案した独自のリスク評価に基づく管理が必要であると同時に、その業務やシステムの設計を国立大学法人全体として管理すべきか否かの判断が適切に行われるような方針や手続きなどが確立され、遵守される必要がある。

以上に加えて、これらの留意点も踏まえた前提である設計、コーディング、テストなどのシステム開発管理に必須とされる基礎的情報の伝達及び記録手段である文書化が肝要となる。その作成や変更を管理するための標準や手続きなどが確立され、適切に実践されている必要がある。

特に重要な「変更管理」及び「テスト」については、5. 情報システムの設計・開発にて詳述する。

第五段階の「運用サービス提供フェーズ」は、システムの本稼動からシステム廃棄までのフェーズである。このフェーズの主な作業は、システムライフサイクルの全体プロジェクトを前提とした場合、情報システムの効果をモニタリングし、さらに効果をあげる次の対策を検討するための情報を蓄積することである。すなわち、情報システムが経営戦略にどの程度の効果を発揮しているか、また情報システムのおかれている環境が導入当初とどのように変化しているかという観点で定性的なモニタリングを実施する。具体的には、定期的なモニタリングの評価結果、アクションプラン、次の期間の目標などを情報化・経営改革モニタリング報告書としてまとめ、トップマネジメントに報告し、承認を得る。このように、次の全体プロジェクトの経営戦略及び情報化企画材料としてトップマネジメントに報告することで、情報システムを活用した継続的・戦略的な経営をおこなうことができるのである。

このフェーズの留意点としては、当該フェーズの計画は戦略情報化企画フェーズから開始されているということである。具体的には、主要モニタリング項目である「定量的な業務改革目標（KPI）」、「必要な情報システム運用面での品質達成度」、「情報システムの運用成熟度」は戦略情報化企画フェーズにおいて予算内で設定し、情報化資源調達フェーズで RFP に反映させ前フェーズで具現化されるのである。この「品質達成度」は SLA（Service Level Agreement）と呼ばれ、対内的な合意と対外的合意がある。後者はシステム運用を外部委託する場合であり、契約が締結される。

また、このフェーズのみで実施されるわけではないが、重要な定常的活動として完成した情報システムをユーザーが安定して利用できるように運用する活動がある。この活動については、「SLA」とともに 6. 情報システムの運用・保守で詳述する。

なお、情報管理の観点から英国のイングランド高等教育財政カウンシルが作成しているチェックリスト（Information Systems and Technology Management : Value for Money Study Management Review Guide, HEFCE 98/43）を参考として章末に示しておく。このチェックリストでは、戦略枠組みは本章の第一段階、組織枠組みは第二段階、投資枠組みは第三・第四段階、運用枠組みは第五段階にそれぞれ対応している。

5. 4　情報システムの戦略・企画

（1）情報システムの戦略・企画の概要

3. 情報システム管理の基礎で述べたように、情報システムの戦略・企画のアウトップトは戦略情報化企画書である。その中には、「情報化戦略」と「情報化計画」から構成される。「情報化戦略」とは、経営的な観点から、自組織の情報化の重要指針である。「情報化計画」とは、経営戦略や情報化戦略を受けて、情報システムの品質、予算やスケジュールなどの目標を具体的に計画することである。その中には、戦略情報化企画書の意思決定に十分役立つように、情報システム面だけでなく、現状の組織や業務フローなどの姿（As Is Model）をもとに、経営戦略を実現するにあたって必要なあるべきそれらの姿（To Be Model）の概要も策定されることが多い。これは情報システム導入により、ヒト・モノ・カネ・情報の流れが変化するため、同時に業務改善などを実施する方が効果的、効率的なためである。また、この段階での To Be Model は概要版であるものの、トップマネジメントが投資効果の意思決定を判断できるものでなければならない。

（2）経営戦略と情報化戦略の整合性

情報システムが、組織体の経営方針及び戦略目標の実現に貢献するためには、当然経営戦略と情報化戦略が整合していなければならない。両戦略が整合しない場合、無駄な投資となるだけでなく、整合している場合に比べた損失は莫大なものとなる。したがって、経営戦略と整合しない情報システムが経営戦略を阻害する一因となることをトップマネジメントは認識しなければならない。

また、情報化戦略は「どのような目的で情報システム化するのか」「このシステムはどのような目的で必要なのか」といったことを情報システムに関わる関係者全員が明確に理解できる具体的な「情報化計画」まで整合していることが必須である。抽象的なレベルの整合性は似て非なるシステムを生み出す原因となるからである。このことにより、情報システムの導入を推進する学長などのトップマネジメントと、実際に情報システムを活用する教職員との意識統一が図られる。

（3）情報化戦略の全体最適

例えば、ある国立大学法人においてA学部とB学部があったと仮定した場合、各々の最適な行動が、A学部とB学部の組織全体の最適になるとは限らない。すなわち、A学部、B学部の部分最適化の積み重ねが全体最適に一致するのではなく、経営戦略の方向性と一致する全体最適化を追求することが重要となる。これは全ての組織活動においていえることであるが、情報システムにおいても全体の情報化計画のない個別システムの開発は部分最適の縦割りシステムになってしまうため、全体最適の実現が重要である。具体的に全体最適な情報化戦略の主なメリットとしては、以下のものが挙げられる。

第一に、「二重開発投資コストの防止」がある。すなわち、同様の機能を持つシステムが個々の学部や部門に導入される可能性を排除できる。また、例えば「プログラムの部品化による再利用」という方針をあらかじめ情報化戦略に掲げておけば、完全に同一機能の情報システムではなくても、類似システムのプログラム再利用ということも選択肢として考慮することが可能となる。

次に、「改修追加コストの削減」がある。2. 国立大学法人のシステム概要でも述べたように、マネジメント系システムの精緻化を図る際には直接業務支援系システムやオペレーション系システムの高度化が必須になる場合が多い。後者のシステムが前者のシステム要件を全く考慮せずに導入した場合、その改修コストは考慮した場合に比し、多額とならざるを得ない。また、オペレーション系システム相互間のデータ項目の不整合も同様のことが言える。したがって、情報化戦略を構築する場合には各システムの連携を十分考慮した全体最適な導入計画を構築することによって、改修追加コストの削減を図ることができるのである。

最後に、「運用コストの低減」がある。例えば、国立大学法人全体では同一属性であるマスタが各個別システムで別々に管理された場合、個別システム毎に同様のマスタファイルが存在することになる。このことは同様のマスタを別々に登録することとなり、データ管理を複雑にしてしまうだけでなく、その運用コストを増加させることにもなる。また、ある個別システムと他システムとの間でデータ連携が必要な場合に、一時的な外部支出の改修コストであるインターフェースコストの増大を理由に、二重入力を実施すればそれに伴う業務コストが増大する。したがって、マスタの主要項目の一元管理、改修コストと運用コストとの比較考慮などの全体最適を勘案した情報化戦略は、運用コストの低減につながるのである。

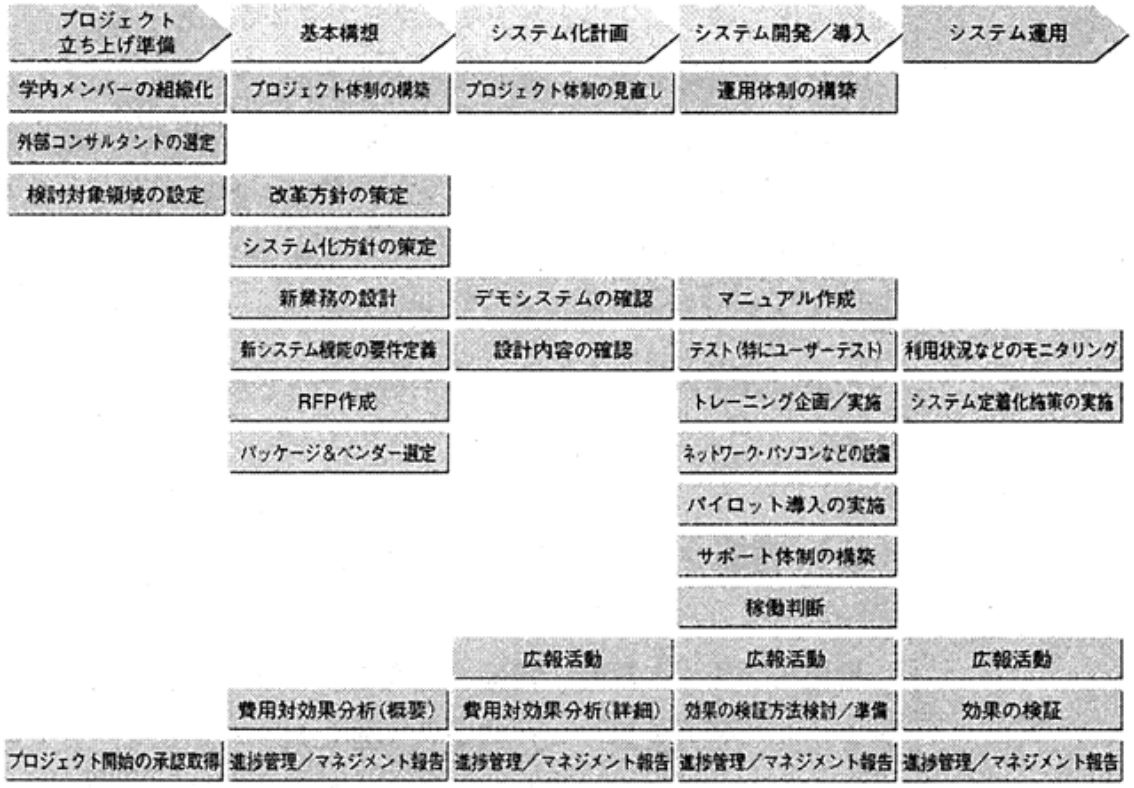
一方で、情報化戦略策定の全体最適には、情報システム全体を網羅的に検討できる人材（CIO 及び CIO 直属の専門部署など）が必要であるが、そのような人材を即座に獲得することは困難な側面がある。このような人材は労働市場全体においても不足しており、相応の報酬コストが発生する。その他に、たとえそのような人材を確保したとしても、各個別システム間の調整の必要が生じる。つまり、全体最適を優先する方針を打ち出した場合、予算の制約上ユーザーの利便性の機能が制約される可能性があり、調整コストが必要となる。したがって、一般にはそれらのコストよりも全体最適の効果が大きいことが、情報化戦略の全体最適を全面的に適用する条件となる。しかし、現状の多くの国立大学法人では、今まで各部局の部分最適を優先してきており、全体最適の効果は部分最適のメリットを上回り、情報化戦略に全体最適の考え方を導入する余地は大きいものと考えられる。

5. 5　情報システムの設計・開発

（1）情報システムの設計・開発の概要

先述のように、今日では、情報システムを自組織で開発するのではなく、ベンダーといわれる専門会社に設計･開発を依頼することが多い。実際のシステム導入に伴う作業の進め方や区切り方は、ベンダーやコンサルタント、システム規模などからも影響を受けるため、一律に考えることは困難であるが、発注元の国立大学法人の立場から、プロジェクト立上げの準備や導入後のシステム運用も考慮した場合、一般に図表 3 のように整理できる。

図表 3　発注元が主体的に実施すべき作業



第一段階の「基本構想」では、目的や範囲を特定し、情報システムの品質や業務フローなどの To Be Model をより詳細に分析し、情報システムに必要な機能・性能・操作性・信頼性などを明確にした RFP でパッケージやベンダーを選定する作業となる。また、RFP 作成と同時に、ベンダーからの提案の評価基準書も作成しておかなければならない。複数のベンダーからの提案を受け、各々の提案を評価基準に照らし合わせて評価し、候補を選ぶことになる。候補が複数となり、甲乙がつ

けがたい場合、さらに具体的な評価および条件交渉を行い、ベンダーを選定することとなる。

第二段階の「システム化計画」では、システム機能の設計を実施する。具体的には、ベンダーなどの要請に応えた細かな業務の説明や既存のシステムの説明、基本設計書や詳細設計書の承認などが必要である。

第三段階の「システム開発／導入」では、ベンダーによる開発・テストやユーザー教育・導入が実施される。重要な作業として、情報システムの業務への導入作業がある。具体的には、情報システムの運用体制や利用ルールの設定、利用者への教育などである。さらに、既存の業務データやマスタの移行作業も必要となることを考慮しなければならない。

第二段階と第三段階の重要な共通作業は、常に作業進捗をモニタリング（監視・点検）することである。具体的には、情報化実行計画書に基づいて展開されるスケジュールなどに基づいて、品質（Q）、コスト（C）、期間（T）が適正な範囲内で推移しているかをモニタリングすることとなる。

また、全段階を通じて留意するべき点として、常に国立大学法人が主導権を握らなければならないということである。この理由は、安易なベンダーへの依存に比べ、導入コストや運用コストの低減を図れるだけでなく、品質の向上や期間の遵守も達成できる可能性が高くなるからである。さらに、発注単位を分割することにより、中小のベンダーやベンチャー企業の活用も可能となるからである。国立大学法人が主導権を確立する体制については、次の（2）で詳述する。

（2）情報システムの設計・開発の管理体制（プロジェクト体制）

情報システムを設計・開発する場合、学内の情報システム部門と利用部門のメンバー（学内要員）に外部要員を加えたプロジェクトチームによるのが一般的である。ここでいう外部要員とは、設計・開発を専門に行うベンダーの人員やシステム導入を支援する専門のコンサルタントなどを意味する。学内要員と外部要員の任務や作業量の程度により、プロジェクトチームは多様な形態になることが想定される。相応の対価を支払うことを前提とすれば、学内要員を最小限に抑えて、外部要員に任せることも可能である。しかし、情報システム調達を本当に成功させるためには、外部要員に任せきりにすることは好ましくなく、むしろユーザーが積極的に関与することが必要である。この理由として、業務フローを把握しているユーザーの実務担当者がシステムの設計・開発に参加することで、使いやすいシステムを目指すことが可能となるからである。また、ユーザーがシステムの設計・開発に積極的に関与しなかった情報システムは、たとえユーザーニーズを満たしていても、ユーザー側の関心が薄く、実際にシステム導入の効果を創出することが難しいからである。現実問題として情報システム調達のために現業の要員を割きたくないという思いを管理者が抱くのは当然のことであるが、情報システム調達を成功に導くためには学内要員をプロジェクトチームに参加させるこ

とが必要不可欠なのである。

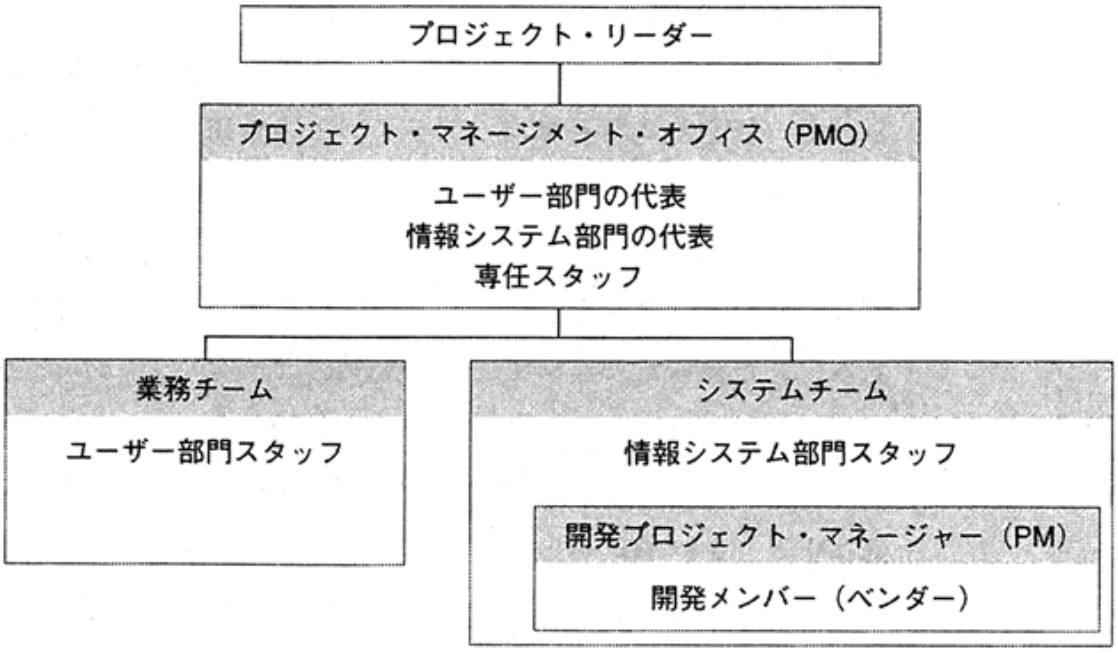
また、ベンダーを自組織のプロジェクト体制に組入れることも大切である。開発は「開発メンバー」の一員としてベンダーが行うのだからといって、自組織の情報システム部門にはベンダーとの窓口を用意するというだけでは不十分である。導入後の新システムを管理・運用していくのは情報システム部門であるので、肝心の当事者が新システムの中身を理解しておくことが必要となる。また、必要なシステムの機能が確定しないといった問題が発生した場合に、ユーザー部門とベンダーとの間に入って、コミュニケーションの円滑化を図り、プロジェクトを推進していくことができる唯一の立場が情報システム部門でもある。したがって、ベンダーを自大学のプロジェクトの中に組み込み、共同で作業をする必要があるのである。

さらに、「プロジェクトの組織化」や「進捗管理」のために優秀な管理職を参画させることが不可欠となる。実際にはしばしば、パソコンに精通している若手教職員を専任メンバーにしているケースが見受けられる。しかし、交渉面、権限面でも組織内で影響力を発揮しにくい若手教職員では適切にプロジェクトを運営することが困難である。したがって、プロジェクトは、あくまでも管理職として優秀な人材主導で進めるべきで、これを実務面でサポートするために、システムに詳しい若手を加えることが有効と考えられる。このようなプロジェクトを組織する管理職メンバーを、プロジェクト・マネジメント・オフィス（PMO）、またはプロジェクト事務局として組織する。PMO は昨今、IT プロジェクトを効率化し、チェック体制を厳格化するための組織として設置されるケースが増えている。ベンダーとのコミュニケーションを満足に行うためにも、この PMO にはユーザー部門と情報システム部門からそれぞれ参画する必要がある。なお、ユーザー部門と情報システム部門とともに、国立大学法人の経営的視点から、大規模なプロジェクトには経営企画部などの専任スタッフを参加させることも重要となる。

最後に、プロジェクト・リーダーとしては、システム規模にもよるが CIO が最適である。その理由として、CIO はトップマネジメントレベルの役職としてリーダーシップを発揮し、プロジェクトの円滑な遂行に大いに加担しなければならないからである。具体的には、ユーザー部門の個別最適と全体最適との調整、追加コストやスケジュールの遅延などの経営に影響を与える事項発生時のトップマネジメント層への報告などである。

以上を考慮した上で、プロジェクト体制の一例を示すと、図表４のようになる。

図表４　プロジェクト体制の例



(3) 契約に盛り込むべき内容

まず、取引形態としては「請負」、「委任」、「派遣」の三種類が想定されるが、その特徴は以下のとおりである。

①請負

・ベンダーが定められたシステムの開発を行い、そのシステムの納入まで請け負う形態

・できあがったシステムの欠陥不良などの責任はベンダーが負う

・納期遅れや、未完成となった場合の責任もベンダーが負う

・開発従事者の指揮命令権は、ベンダーにある

②委託

・ベンダーに、定められたシステム開発作業を委託する形態

・できあがったシステムに関する欠陥不良の責任は、通常は発注元が負う

・納期遅れや未完成となった場合の責任でベンダーは善良なる管理者としての注意義務を負うだけであり、ベンダーに求めることは困難

・開発従事者の指揮命令権は、ベンダーにある

③派遣

・ベンダーの要員を発注元に受け入れ開発業務を行ってもらう形態

・欠陥不良・納期遅れや未完成となった場合の責任を、ベンダーに求めることは困難

・開発従事者の指揮命令権は、発注元にある

以上のように、ベンダーの責任が一番重い取引形態は請負であり、外注の詳細な作業管理は通常困難であるため、多くの開発契約は請負契約が締結される。

次に、システム開発に関する契約は、「モノ」ではなく形のない機能を、ベンダーと共同で開発するため、発注元とベンダーとの間で、誤解、不満、トラブルが発生しやすい契約といえる。したがって、システム開発に関するトラブルを踏まえ、経済産業省の産業構造審議会情報産業部会は、「ソフトウェア開発に盛り込むべき主要事項」として、「推進体制の強化」、「仕様の確定」、「仕様の変更」、「検収」、「瑕疵担保責任」、「知的財産権」、「機密保持義務」を挙げている。さらに、社団法人情報サービス産業協会（JISA）もソフトウェア開発委託契約書のモデル契約を更改し、取引の適正化に努めている。これらを参考に、代表的な留意点を挙げる。

第一に、「推進体制」や「仕様の確定」においては、発注元である国立大学法人とベンダーとの間の話合いのルールをあらかじめ明示する必要がある。具体的には、国立大学法人とベンダーの各担当者がバラバラに連絡を取り合った場合、誤解が発生しやすいため、相手方からの要請や指示などを取り扱う窓口を一本化しておくことが重要となる。また、進捗状況の報告・確認を行い、発生した問題点を解決するための定期的な協議会を設定し、その際の議事録の作成・承認を徹底する必要がある。双方の役割分担を明確にするためにも「国立大学法人がベンダーに委託する業務の内容」と「国立大学法人がシステム開発において、どのような役割を負うのか」は明示しておくべきである。また、設計書の承認ルールも設定すべきである。

次に、検収終了後の「瑕疵担保責任」であるが、仕様書の完成度が低い場合、仕様の変更・追加との境界が曖昧となる。瑕疵担保責任のトラブルを減らすためには、詳細な機能仕様の確定が必要となる。なお、瑕疵担保責任の期間は民法の規定では、検収後１年間となっている。

さらに、「知的財産権」に関しては、開発費を負担している国立大学法人としては、業務上のノウハウやアイディアが含まれている情報システムのあらゆる権利を自大学に移転したいところである。一方ベンダーも、システム開発上の蓄積してきた技術・ノウハウなど、今後のシステム開発に汎用的に利用できるものが含まれているなどの理由で、権利の移転に反対する傾向がある。契約パターンの原則としては、開発の際に生じた知的財産権を発注元に移転する「譲渡」、両者が知的財産権の半分の持分を保持する「共有」、開発元が知的財産権を保持し、発注元に使用権を許諾する「利用許諾」がある。いずれにしてもシステムの開発目的・形態・コスト（著作権の発注元への移転は、通常他に利用できないため、コストが他のパターンに比べて高い）などの様々な要因を検討した上で、各関係者の利益が均衡するように協議していく必要がある。

最後に、「機密保持義務」に関しては、最近、特に開発元の個人情報の持ち出しなどが生じているため、単なる相手方の営業・技術上の機密だけでなく、それらをカバーするような文言が必須となる。なお、「仕様の変更」及び「検収」に関しては、「(4) 変更管理」及び「(5) テスト」で述べる。

(4) 変更管理

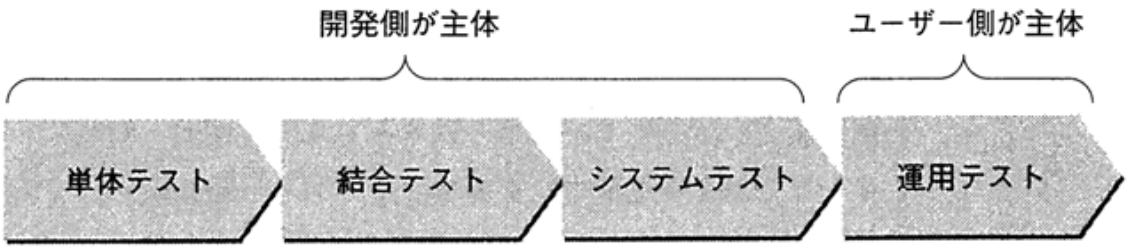
設計・開発のモニタリングは主に、「要件が設計・開発に正しく反映されているか」、「スケジュールは守られているか」、「追加費用が発生しないか」といった観点で行われ、適正な範囲を超えて問題が発生した場合は、関係者が協力して早期に解決を図らなければならない。

しかし、特に開発プロジェクトは不確実であるため、計画を変更する必要が生じる場合がある。その際、特に大規模プロジェクトの場合、対内的にはトップマネジメントの承認事項となる一方、対外的なベンダーとは契約事項の変更となる。「仕様の変更」は、費用やスケジュールに影響する重要な事項であるため、変更の手続きを明確にして、変更による混乱をあらかじめ防ぐ必要がある。具体的には、CIO などのプロジェクト・リーダーによるトップマネジメント層への報告・承認及び開発者との変更契約の締結である。後者の変更契約締結は開発契約締結時に、「変更の申し入れ方法」、「変更の受け入れ方法」、「変更仕様書（RFC：Request For Change）の作成」、「RFC の確定手続き」などを明確化して条文化する必要がある。

(5) テスト

契約が締結され、基本設計書や詳細設計書などのシステム仕様書に基づいてベンダーが情報システム開発を実施するが、発注元は開発された情報システムがその仕様を満たしているのか、必要な品質を確保しているかなどを確認する必要がある。その確認が「検収」であり、検査仕様書が作成され、発注元である国立大学法人は質量ともに満足するまで自らテストを実施することが必要となる。ここでの留意点は、開発契約に検査仕様書やテストで使用する検査データの作成主体、システムの欠陥や仕様書との相違が発生した場合の対処方法などを明文化なければならないということである。具体的なシステム開発テストの流れは、ベンダーによって、ステップの分け方や名称、実施する内容が大きく異なるが、概ね図表 5 のようになり、複数回のテストを行う必要がある。

図表 5　システム開発テストの流れ



また、テストの主な目的には以下のようなものがある。

・要求仕様を満たしているか
・使い勝手がよいか
・レスポンスなどのパフォーマンスが出ているか
・安定しているか
・例外も含めてテストすべきすべてのケースを想定しているか
・全てのケースに対して正しい結果を事前に設定し、その結果と一致しているか

さらに留意点としては、ベンダーに任せきりにせず、各テストにユーザーがモニタリングや自ら実施して関わっていくことが開発プロジェクト成功の鍵を握るということである。また、運用テストは実際に使う立場になるエンドユーザーが主体的に行わなければならない。その理由は、開発プロジェクトチームだけでは想定できない様々なケースをテストする必要があるためである。

それに加えて、できるだけ早期にシステムのバグ（不具合）を発見することが、テストのポイントになる。その理由は、後期に行われるテストで問題が発覚した場合、当該不具合を直すために、最初の段階に遡ってテストをやり直すことが必要となり、コストと時間が膨大にかかってしまう可能性があるからである。したがって、テストはベンダーにはもちろん、国立大学法人にとっても大切なものである。このような留意点を踏まえて、禍根の残さない十分なテストを行う必要がある。

5. 6　情報システムの運用・保守

(1) 情報システムの運用・保守の必要性

情報システムの運用とは、情報システムに期待されている機能および性能が、一定レベル以上で維持されているように運用することである。一方、情報システムの保守とは、対象業務あるいは利用している情報技術に関する環境変化に対応して、情報システムを改変していく活動である。保守は業務環境や IT 環境の変化に対応して、情報システムの価値を維持・拡大し、システムライフサイクルを長くするために重要な活動である。それに対して、運用は導入された情報システムが経営戦略上の目標に対する効果を計画どおりに発揮するための活動であり、保守以上に重要となる。特に、国立大学法人のシステムは事務職員だけでなく、教員や学生など多くの利用者がいるので、ユーザーフレンドリーな運用が肝要となる。次に、特に重要な運用の代表的管理を中心に述べることとする。

(2) 情報システムの運用の具体的内容

①性能管理

大学経営において想定される業務最大量で運用可能なハードウェアの容量やソフトウェアの能力などを、将来想定も考慮して管理することである。この管理をしない場合、システムのレスポンスタイム遅延などによる業務効率の悪化だけでなく、システムダウンにもつながる可能性がある。

②継続的サービス管理

広域災害、その他の緊急事態に際しても、経営上重要な情報システムが、効果的な継続的計画でカバーされている必要があり、そのための管理が方針や手続きなどとして確立され、適切に実践する必要がある。

③教育・トレーニング

情報システムや業務の教育・トレーニングを計画的に実施して、オペレーションミスや不正操作によって重要な情報資産の安全が損なわれたり、業務が中断したりするなどのリスクが適切に管理されなければならない。

④ヘルプデスク

ユーザーの質問や問題に的確に回答する活動である。この活動において、ヘルプデスクは、問い合わせ電話などのモニタリング、それに対応する適切なスキルを維持することが必要であり、そのための方針や手続きが確立されていなければならない。

⑤設備管理

電源設備やバックアップシステムなどの各設備が、情報システムの発展に対応できる拡張性や施設設備の不備（セキュリティ）や不具合によるシステム障害の発生を抑える信頼性を確保する方針や手続きが確立されていなければならない。

⑥コスト管理

情報システムは開発時の初期コストだけでなく、維持コストが発生する。維持コストには、設備とシステムの維持に大きく分けられ、前者には、消耗品や電気代、水道光熱費などがあり、後者には保守料や人件費などがある。これらの維持コストを予算、実績、差異分析及び改善案、次期予算への反映という PDCA サイクルで実施し、システム関連コストを的確にコントロールしていくことが必要である。

⑦データ管理

データは組織の情報に関する要求の中核であるため、その発生から廃棄まで健全性、安全性及びその維持を考慮した方針や手続きが確立されていなければならない。具体的には、データの正確性、完全性及び正当性（承認）が確立されたデータの処理手続き、バックアップ方法、データ廃棄方法などがある。

代表的な上記の管理を含む全運用において、学内に要員や設備がない場合は、外部に運用を委託（アウトソーシング）することもできるが、その場合は委託先との間に SLA を結び、責任範囲を明確にしておかなければならない。SLA については、次に述べる。

(3) SLA（品質達成度）

SLA は前述のように、ユーザーである国立大学法人とベンダーがサービスレベルで合意した契約書である。なお、サービスレベルは曖昧性を排除するために、定量的に国立大学法人側が明示する必要がある。

SLA を明確化することにより、国立大学法人内においてはシステム部門がユーザー部門の満足度を把握することが可能となるだけでなく、合意した品質を備えた情報システムに関わる運用サービスを提供する責務が生じる。同様に、対外的な SLA の締結により、ベンダーは国立大学法人に対し同様の責務が生じるため、当初の投資効果の実現可能性が高まるのである。

日本では、SLA は最近の概念であり、国立大学法人でも採用している例は少ないと考えられるため、合意すべき主要な項目を以下に示す。

・サービス内容（サービス一覧など）
・サービス実施条件（サービス体制、対象範囲、時間など）
・サービスの責任範囲（免責事項など）
・評価基準とその基礎データ
・サービス実施状況の評価方法
・サービス料金基準
・ペナルティ条項
・サービス期間

5. 7　情報セキュリティ／監査

(1) 情報セキュリティの定義

一般的に、情報セキュリティとは、自組織、または自分以外に知られたくない情報について、知られる危険性から保護することとされている。また、BSI（British Standards Institution：英国規格協会）による情報セキュリティマネジメントに関する基準と仕様を規定した BS7799 をベースに策定された ISMS（Information Security Management System）認証基準（Ver.2.0）では、情報セキュリティを「情報の機密性、完全性及び可用性の維持」と定義している。具体的には、「機密性」とは、アクセスを許可された者だけが情報にアクセスできるようにすること、「完全性」とは、情報及び処理方法が、正確であること及び完全であることを保護すること、「可用性」とは、認可された

利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすることである。

簡潔に述べると、ある情報について、見たり、聞いたり、触れたりすることが許された特定の人のみであることが「機密性」である。また、当該情報が何者かによって改ざんされないようにすることが「完全性」である。さらに特定の人が、見たり、聞いたり、触れたりする必要がある時に、可能な状態を維持することが「可用性」である。

(2) 国立大学法人における情報セキュリティの必要性

情報セキュリティは、あらゆる地域、あらゆる組織において取組まなければならない課題であり、我が国における国立大学法人も当然に例外ではない。国立大学法人の特徴としては、国家財源が投入されているため、開示すべき情報資産（学術論文、研究資料、実験データ、文献など）が民間組織に比して多くなるものと考えられるが、保護すべき個人情報（学生の成績など）も当然存在することから、その切り分けなどが重要となる。すなわち、各国立大学法人は、現在有している情報資産の識別、管理者、保存期間、廃棄方法などを一元的に管理する必要がある。また、電子媒体だけでなく、紙媒体での情報資産についての取扱においても十分な留意が必要となる。一方で、インターネットの活用も先進的に取り組んできたため、外部からアクセス可能な膨大な情報資産が存在するが、他の組織同様、ネット攻撃などに十分耐えうるセキュリティ対策が必要となる。

さらに、「個人情報の保護に関する法律」、いわゆる個人情報保護法が施行される前までは、単に経営上・運営上のリスクだけを負えば済んでいたが、今後はリーガルリスクも認識する必要がある。個人情報が漏えいした一部の企業では、自主的に自社の顧客に少額の商品券などを配布しているが、顧客数の多さから、その金額は数億～数十億円にもなり、その後の対策費用もやはり同額以上に要しているのが現状である。従来であれば、「組織外」の第三者（委託先）、「組織内」の従業者の責任を追及すれば事足りていたものが、今後は「組織外」の第三者（委託先）及び「組織内」の従事者の監督義務が、個人情報取扱事業者や独立行政法人などにおいて負わされることになる。国立大学法人にも適用される「独立行政法人等の保有する個人情報の保護に関する法律」では、その施行が2005年4月1日からとなっている。

(3) 情報セキュリティ管理

①原則

1992 年に、OECD（経済協力開発機構）において、2 年間検討した情報システムのセキュリティのための国際的なガイドラインが採択された。この OECD セキュリティガイドラインは九つの原則から成っており、OECD は各国政府のみならず、民間団体もこの原則の確立を求めている。このガイドラインは 5 年後毎の見直しが決まっているが、2002 年に見直した後の九つの原則は図表 6 のとおりである。

図表 6

1	認識 （Awareness）	参加者は、情報システム及びネットワークのセキュリティの必要性並びにセキュリティを強化するために自分達にできることについて認識すべきである。
2	責任 （Responsibility）	すべての参加者は、情報システム及びネットワークのセキュリティに責任を負う。
3	対応 （Response）	参加者は、セキュリティの事件・事故に対する予防、検出及び対応のために、時宜を得たかつ協力的な方法で行動すべきである。
4	倫理 （Ethics）	参加者は、他者の正当な利益を尊重するべきである。
5	民主主義 （Democracy）	情報システム及びネットワークのセキュリティは、民主主義社会の本質的な価値に適合すべきである。
6	リスクアセスメント （Risk assessment）	参加者は、リスクアセスメントを行うべきである。
7	セキュリティの設計及び実施 （Security design and implementation）	参加者は、情報システム及びネットワークの本質的な要素としてセキュリティを組み込むべきである。
8	セキュリティマネジメント （Security management）	参加者は、セキュリティマネジメントへの包括的アプローチを採用するべきである。
9	再評価 （Reassessment）	参加者は、情報システム及びネットワークのセキュリティのレビュー及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである。

②PDCA モデルとその効果

情報セキュリティである「情報の機密性、完全性及び可用性の維持」を達成するために、「Plan－Do－Check－Act（計画－実施－点検－処置）」（PDCA）モデルに基づいた「情報セキュリティマネジメントシステム（ISMS）」の構築・運用が必要となる。ISMS 認証基準（Ver.2.0）では、「ISMS」

を「マネジメントシステム全体のなかで、事業リスクに対するアプローチに基づいて情報セキュリティの確立、導入、運用、監視、見直し、維持、改善をになう部分（参考　マネジメントシステムには、組織の構造、及び方針、計画作成活動、責任、実践、手順、プロセス及び経営資源が含まれる）」と定義している。この考え方は OECD セキュリティガイドラインの 6～9 と整合している。また、同認証基準では、「ISMS は情報資産を保護するため、十分でバランスのとれた適切な情報セキュリティ管理策を確保し、顧客及び他の利害関係者に対して信頼を与えるように設計されるものである。このように設計された ISMS は、競争力、キャッシュフロー、収益性、法令などの遵守及び組織イメージを維持し、改善することにつながる。」とその効果を説明している。

次に、セキュリティにおける PDCA モデルについて概観した場合、図表 7 のようになる。

図表 7

Plan一計画 （ISMSの確立）	組織の全般的な基本方針及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティ基本方針、目標、対象、プロセス及び手順を確立する。具体的には ① 情報資産の洗い出し ② 各情報資産が情報セキュリティ上、どのようなリクを抱えているかについて、リスクアセスメントを実施 ③ リスクアセスメントの結果から、必要な管理策を策定（予算とのバランスが重要） ④ 管理策を織り込んだセキュリティポリシーの策定
Do一実施 （ISMSの導入及び運用）	その情報セキュリティ基本方針、管理策、プロセス及び手順を導入し適用する。（セキュリティポリシーに沿った運用）
Check一点検 （ISMSの監視及び見直し）	情報セキュリティ基本方針、目標及び実際の経験に照らしてプロセスの実施状況を評価し、可能な場合これを測定し、その結果を見直すために経営陣に報告する。（セキュリティポリシーへの準拠性監査）
Act一処置 （ISMSの維持及び改善）	ISMSの継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。（各国立大学法人運営主体によるISMS全体の見直しの実施）

前表のようにあらゆる段階で基盤となるポイントとしてセキュリティポリシーがある。セキュリティポリシーとは「情報の機密性、完全性及び可用性の維持」を確保するための方針や基準を明文化したものである。通常、情報セキュリティ基本方針（ポリシー）、情報セキュリティ管理基準（スタンダード）及び情報セキュリティ実施手順（プロシージャ）の構成から成るが、前二者をセキュリティポリシーと呼ぶことが多い。また、情報セキュリティマネジメントにおいては、「リスクアセスメント」の成否が情報セキュリティのレベルを左右するということが特に重要である。つまり、民間のセキュリティポリシーサンプルを各国立大学法人に取り込んだだけでは、真の情報セキュリティとはならず、国立大学法人毎にリスクアセスメントを実施し、リスクアセスメントの結果を反映すると共に、運営方法、規模、予算などに見合ったセキュリティポリシーとしていかなければならない。したがって、各国立大学法人の IT 化の進捗状況により、当然にセキュリティポリシーは異なったものとなるのである。

また、セキュリティポリシーを策定するためには、さまざまな管理を考慮する必要があるが、特に重要な概念である「情報リソース管理」について、次に述べる。

③情報リソース管理

2004 年に発生した様々な情報漏えいなどのセキュリティ事故の大半は不正な持ち出しになどよる人的要因によるものであることが明らかになっている。このことからも判明するように、情報セキュリティの場合、ネットワークやコンピュータに対する技術的な対策と、人の管理という二つの側面から考えなければならない。

前者に関しては、「組織の情報セキュリティ管理基準（スタンダード）及び情報セキュリティ実施手順（プロシージャ）と、現在の業務目的との合致」が重要となる。当然ながら、セキュリティポリシーが策定されていなければならない。次にこれをサポートする「IT 障害対策グループ」を発足させる。

これらが整備された段階で、「認証」、「権限付与」、「アカウント管理」、「物理的アクセスコントロール」、「論理的アクセスコントロール」といったセキュリティの実装がなされる。

これらの中でも情報リソース管理として「物理的アクセスコントロール」、「論理的アクセスコントロール」は、実装の中で主要な部分である。「物理的アクセスコントロール」としては、鍵、IC カード、警報器、警備員、防犯カメラなどが挙げられるが、その配置は、情報資産の重要性に対応したものとしなければならない。「論理的アクセスコントロール」は、ファイアウォール、ルータ、スイッチ、VPN などのシステムとネットワークのコントロールがなされる。従って、実装が先ではなく、情報資産の洗い出し、リスクアセスメント、管理策策定、セキュリティポリシー策定とのとの整合性が図られなければ、設計とは言えないのである。

一方、PDCA モデルを採用した ISMS などでは、情報セキュリティを単に技術的な課題だけではなく、人的側面の管理をも含めたマネジメントシステムとして捉えることにより、情報セキュリティの機密性、完全性及び可用性の維持を図っている。これはセキュリティ事故の大半が高度なセキュリティ知識を有していなくても、放置された電子・紙媒体の持ち出しや、ゴミ箱あさりなどのような、ソーシャルエンジニアリングにより試されていることからも裏づけされるものである。このため、情報セキュリティにおいては、情報資産に関わる人の教育が重要視されるのである。

一方、法的側面でもセキュリティにおける情報リソースの重要性が認識され、「個人情報の保護に関する法律」、「独立行政法人等の保有する個人情報の保護に関する法律」では、個人情報の取扱について利用目的の通知及びそれによる制限、適正な取得や第三者提供の制限、開示・訂正・利用停止とともに、直接関連するものとして「安全管理措置」が要求されている。但し、これらの法律の具体的な「安全管理措置」については明らかではないため、経済産業省の「個人情報保護に関する法律についての経済産業分野を対象とするガイドライン」を参考として、図表８に記載する。

図表 8

i	組織的安全管理措置	安全管理について従業者（法第21条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下規程などという）を整備運用し、その実施状況を確認すること。
ii	人的安全管理措置	従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や、教育・訓練などの措置。
iii	物理的安全管理措置	入退館（室）の管理、個人データの盗難の防止対策、機器・装置などの物理的な保護などの措置。
iv	技術的安全管理措置	個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視など、個人データに対する技術的な安全管理措置。具体的には、アクセスにおける識別など。

このガイドラインにおいても人的側面と技術的側面の両面をカバーしていることに注意すべきであり、情報セキュリティ面の PDCA サイクルの整備・確立が国立大学法人においても早急に必要となっている。また、経済産業省の外郭団体である JIPDEC（日本情報処理開発協会）が認定機関となっている、組織の情報セキュリティ運用を評価する国内認証制度の ISMS 適合性評価制度を利用することも効果的・効率的な PDCA サイクルの整備・確立に当たって考慮すべきである。この情報セキュリティ面の PDCA サイクルを整備・確立する国立大学法人内の体制については、次の④で記述する。

④管理組織体制

情報セキュリティの運用管理は日常的かつ定常的な作業であるため、プロジェクト型ではなく、委員会型が一般的である。しかし、セキュリティポリシーの改訂や対策の改善が頻繁な段階の場合、常設の情報セキュリティ管理部署や担当者を設置する必要がある。

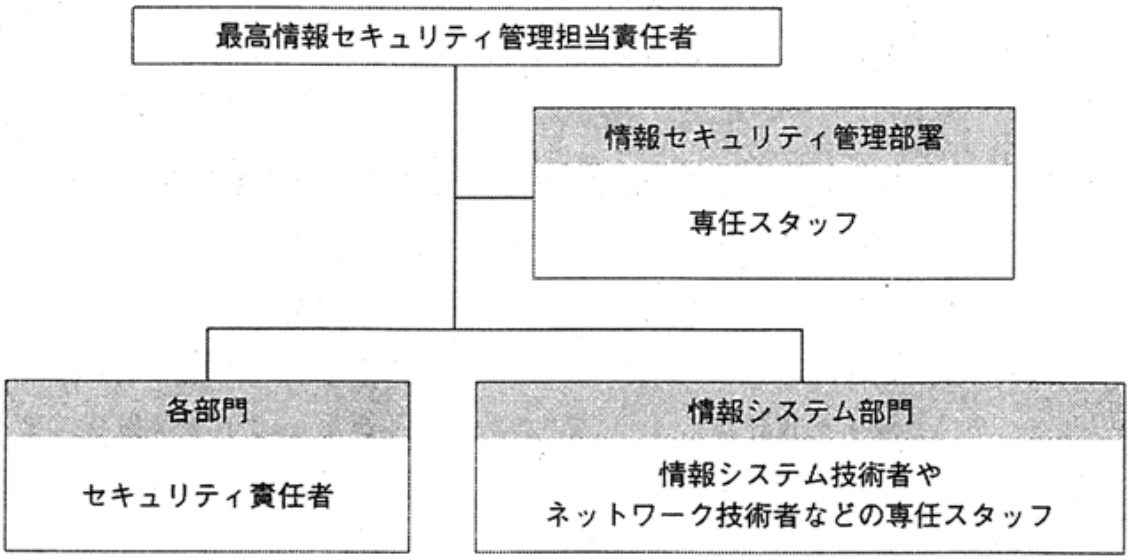
情報セキュリティ管理委員会は、情報セキュリティの運用管理を実行する組織であり、情報セキュリティポリシーを実装した情報セキュリティマネジメントシステムのリスク管理の維持が主な役割である。構成メンバーは最高情報セキュリティ管理担当責任者（CISO：Chief Information Security Officer）を中心として、各部門情報セキュリティ責任者や情報システム技術者やネットワーク技術者などから構成される。

次に、情報セキュリティ管理部署は、一般的に情報セキュリティポリシー運用計画の策定や改訂、リスク分析、セキュリティ対策の実装作業などの進捗管理などが役割となる。運用時には情報セキュリティに関するヘルプデスクの役割も担う。

最後に、各部門情報セキュリティ責任者は、所属部門のセキュリティ監視やセキュリティポリシーの遵守状況の把握を行い、定期的に委員会に報告する役割を担う。

以上を考慮した上で、情報セキュリティ管理の組織体制の一例を示すと、図表 9 のようになる。

図表 9　情報セキュリティ管理体制の例



（4）システム面の監査

①システム監査の目的及び必要性

3. システム管理の基礎で述べたように、国立大学法人は客観的な資料に基づいての説明責任を確保しなければならない。このような情報開示や説明責任の確保を実効性のあるものとしていくためには、トップマネジメントの方針や指示を受けて活動する組織や役職員の業務執行状況を的確に把握しなければならず、そのためにはいわゆる内部統制の充実を図ることが不可欠である。組織体の内部統制が適切に機能することを確保するために、その現状を把握し、問題点の抽出、改善提案を行う内部監査が必要である。しかも業務のほとんどを情報システムに依存している現代の業務環境においては、情報システムや情報システムを利用する業務プロセスに対して、内部監査としてのシステム監査を実施して、情報システムに対するリスク管理の状況を評価することが強く求められる。

また、IT の進歩に伴い、情報システムに係るリスクも多様化しており、その領域も拡大している。さらに、万一リスクが現実のものとなった場合の影響の重大さも増し続けてきている。大学運営においても全く同様であり、情報システムがその組織目的や戦略に則して適切な情報、コミュニケーション手段、あるいは処理機能などを提供し続けられるように、情報システムリスクを的確に把握しこれに対処することができるリスク管理体制の充実を図ることが必要である。内部監査としてのシステム監査は、情報システムリスクの管理体制が適切であるか、また効果的であるかどうかという評価を通じて、リスク管理体制やトップマネジメントの意思決定を側面から支援するものである。

②システム監査の定義及び新システム監査基準の意義

システム監査の対象は情報システムであり、システム監査では国立大学法人が保有する情報システムに内在する情報システムリスクとその管理の状況を評価する。その情報システムリスクの現実化を予防し、検知し、正常な状態に回復する責任は、トップマネジメントあるいは当該情報システムの計画と管理に関する責任と権限を委譲された部門、すなわち情報システム部門や情報システム利用部門などの被監査部門にある。これらの部門では、経営目標や戦略に従って情報システムリスクを識別し、評価し、これを適切かつ効果的に管理する責任を負っている。システム監査人は、これらの責任が果たされていることを独立した立場から評価する。

具体的には、システム監査とは、情報システムの機能特性を有効性、効率性、信頼性、遵守性、及び安全性という 5 つに分解して、それぞれの特性を阻害する可能性のある情報システムリスクに対して、被監査部門のリスク管理の状態を、監査対象から組織的に独立したシステム監査人が把握、評価し、その結果をトップマネジメントに報告するものである。ここで、（ｉ）「有効性」とは、情報システムが経営目標や戦略の策定および実現に対して効果的な情報や業務処理機能を提供していることである。これには、目的適合性、適時性、有用性、利便性などが含まれる。（ii）「効率性」とは、情報システムによる情報や機能の提供が、より生産性や経済性の高い方法で行われていることである。これには、資源の効率的活用だけでなく、将来的な拡張性や、他システムとの連携の柔軟性なども含まれる。（iii）「信頼性」とは、情報システムが提供する情報や機能が、信頼できるものであることである。これには、情報システムに期待される情報や機能を情報システムが確実に提供していることが含まれ、結果やプロセスの正確性なども含まれる。（iv）の「遵守性」とは、情報システムや情報処理プロセスが、法令、規制、あるいは当該国立大学法人の方針および手続きなどを遵守していることである。また、情報処理プロセスにこれらの規制情報が組み込まれていることである。（ｖ）「安全性」とは、情報システムが災害、障害、犯罪、不正行為、その他の不測の脅威から保護されていることである。情報セキュリティの国際規格（ISO/IEC　17799：2000）や国内規格（JISX　5080：2002）では、安全性をさらに機密性、完全性、可用性の視点に分解して評価している。

さらに、2004 年 10 月に経済産業省から、これまでのシステム監査基準を改訂した「システム監査基準」及び「システム管理基準」が公表された。今回の改訂は、情報システムが経営戦略を実現するために不可欠のものとなっていることや、インターネットの急速な発展による内外のサービスツールとしての重要性によるリスクの拡大・変容を反映している。特に、システム監査に期待されている点の中で、（ⅰ）システム監査人の質の向上、（ⅱ）IT ガバナンス、あるいはコーポレートガバナンスの有効性の評価、（ⅲ）内部統制あるいは内部監査としてのシステム監査の不可欠性、（ⅳ）の情報システムの有効性、効率性、リスク管理（セキュリティ管理など）、コンプライアンスの重視、が強調されている。

具体的には、効果的な監査のための判断尺度となる「システム管理基準」と監査主体の行為規範を定めた「システム監査基準」の二部構成となった。このように二部構成にしたのは、情報システム監査人が、社会に対して監査結果に関する説明責任（結果責任と過程を含めた説明）が求められる必要性が高まったことに関係している。この二部構成により、システム監査の実施形態も、旧制度ではあくまで「助言型」一本であったのに比べ、今後は「保証型」、「助言型」の二本立ての監査が想定され、下記の「情報セキュリティ監査」との整合性が図られている。「保証型」は対外的には取引先などの利害関係者への説明に利用し、対内的には内部統制の整備と運用を経営者に保証する目的で実施される。一方の「助言型」は管理基準とのギャップについての指摘が中心であり、組織内部の対策面の強化に適用する目的で実施される。

③情報セキュリティ監査

国立大学法人においても、情報システムに関わりを持つ人員がすべての教職員へ、あるいはオープンネットワークなどを通じて学外の不特定多数者にまで拡大したことに伴い、重要な情報に対する不正アクセス、漏洩、改ざんなどのリスクも拡大している。したがって、重要な情報資産を識別、管理するために、適切な組織体制のもとでセキュリティ基本方針やスタンダード・ルールなどが設定され、あるいは関連システムに組み込まれて、適切に実践されているかを評価する必要がある。また、それと同時にネットワークを構成する資源およびネットワーク上の情報資産の管理プロセスについても、その安全性や信頼性、効率性などに対する管理の中に、適切な手続きは確立され、遵守されているかなどを評価する必要がある。

このような情報セキュリティ面の規範に関しては、別途「情報セキュリティ監査制度」がある。「情報セキュリティ監査制度」は 2003 年 4 月から運用開始された、経済産業省が制定した制度であり、「助言型」と「保証型」がある。

「助言型」とは、まだ情報セキュリティの管理体制が十分に整備されていない場合に、情報セキュリティ管理基準に準拠してセキュリティ監査を実施し、発見された問題点の指摘、あるいは改善提案のための報告書を提出するものである。具体的には、ISMS 適合性評価制度の認証取得を目指す場合、認証取得の段階に至らない組織が対象となる。情報セキュリティの欠陥を早期に発見し、情報セキュリティマネジメントシステム構築に役立たり、構築後の情報セキュリティ対策の継続的な向上を図る意味で、第三者の専門家が実施する情報セキュリティ監査は非常に有効である。

「保証型」では、情報セキュリティ管理基準に準拠してセキュリティ監査を実施することになる。ISMS 適合性評価制度の認証取得レベルにある組織を対象に、セキュリティ管理体制が十分に整備されていると認められる場合には、その旨の意見表明をした報告書を提出する。この保証型の報告書は、第三者に開示することができる。「保証型」の第三者の専門家によるサービスの代表例として、システムの信頼性又は電子商取引の安全性などに関する内部統制について保証を与える Trust サービスがある。その中には、「Sys Trust」と「Web Trust」がある。「Sys Trust」とは、Trust サービスの原則と規準に基づき検証されているシステムについて、組織の経営者が有効な内部統制を維持していることに関して、高水準の保証を与える目的で実施される検証業務である。また、「Web Trust」とは、Trust サービスの原則と規準に基づき検証されている電子商取引システムについて、組織の経営者が有効な内部統制を維持していること、及び該当する場合には、当該組織が定められた電子商取引のビジネスの方針に準拠していることに関して、高水準の保証を与える目的で実施される検証業務である。

④システム監査体制

システム監査を初めて導入しようとする場合、トップマネジメント、監査部門、及び被監査部門が、システム監査の目的や前項で述べたそれぞれの責任を十分に理解して、相互の協力のもとにシステム監査実施体制を構築することが重要である。特に、システム監査が、公正で偏りのない情報をトップマネジメントに提供するという内部監査としての役割を果たすためには、システム監査人が被監査部門から組織的に独立していることが必要である。このためには、システム監査人を監査部や検査部などの内部監査部門に所属させる体制にすることが必要である。

監査部門においては、自らの組織のシステム監査に関する活動指針を基本方針として策定し、自らの組織内および監査部門内の諸手続きと整合をとりながら、システム監査業務に関する諸手続き、様式などを制定する。

比較的小規模な組織、あるいはシステム監査部門の経験の浅い組織においては、システム監査に必要なスキルをもつ要員の確保が困難な場合も考えられる。このような場合は、システム監査の実施手段の一つとして外部の専門家を活用することも有効である。これらの場合、外部機関への委託は内部監査部門を所管する役員または監査部門を窓口として行う必要がある。そして、システム監査実施の目的や前提となるリスク認識などについて、委託する国立大学法人の主体性とこれに基づく外部機関との間の十分なコミュニケーションが求められる。

⑤システム監査の具体的アプローチ

システム監査の役割は重要なものであるが、その一方でシステム監査人のスキルや人数をはじめとして、これに向けることのできる監査資源は有限である。効果的なシステム監査を効率的に実施するためには、より大きな情報システムリスクが存在すると考えられる領域に対して監査資源を集中的に投入するリスクアプローチの考え方が利用される。リスクアプローチでは、情報システム全領域を適切な監査対象に分割してそれぞれの現存するリスクを識別、評価し、これに基づいて監査計画の策定や個々の監査活動の準備などを行う。システム監査の対象領域は被監査部門で行う情報システムリスク管理の対象領域と一致するので、監査実施においては被監査部門が行うリスク管理プロセスで用いた資料や作成された成果物を利用することができれば、効率的である。

システム監査の対象領域は、それぞれの対象領域における情報システムとこれに関わる活動の全体となる。具体的な対象領域としては、（ⅰ）情報システムの計画と管理、（ⅱ）情報システムリスク管理、（ⅲ）情報セキュリティ、（ⅳ）システム開発、（ⅴ）システム保守・運用、（ⅵ）システム利用、（ⅶ）入出力などの処理、（ⅷ）エンドユーザコンピューティング（以下、EUC）、（ⅸ）ネットワーク、（ⅹ）システム資産・資源管理、（ⅹⅰ）外部委託、（ⅹⅱ）コンティンジェンシープラン、（ⅹⅲ）ドキュメンテーション、（ⅹⅳ）個別アプリケーションシステムなどがある。

システム監査計画を策定する際には、情報資産や情報システムの把握後、組織全体にわたる情報システムのリスク評価、分析などを行って、監査対象とその情報システムリスクの重大性や特性などを明確にし、内外の要請などを総合的に勘案して、監査対象の優先順位付けと適切な監査方法、監査実施サイクルを決定する。なお、必要なシステム監査を効率的かつバランス良く実施するためには、監査方針や監査対象の優先順位付けなどを勘案した、中長期（数カ年程度）の監査の大綱となる中長期計画を策定することが望ましい。これにより、中長期における監査に必要な資源（人、物、金、時間など）の見積りが可能となるだけでなく、監査実施に関わる要員の採用や教育計画、あるいは IT に関する知識の習得計画など総合的な監査計画や方針の策定が容易になる。なお、システム監査計画策定サイクル（1 年間、半年など）ごとに、この中長期計画を詳細化、具体化したものが、短期計画となる。

短期実施計画に基づいて、個々の監査対象ごとにシステム監査の実施計画を作成し、当該監査の全プロセスの概要を明確にした後、監査部門長から被監査部門長に対して監査実施の通知を文書で行い、双方の協力体制や問題点に取り組む体制を整える。実施計画に基づく当該システム監査の実施に先立ち、監査対象に関して被監査部門からの資料収集などによる事前調査を行い、その概要を把握して監査手続を具体化させる。

その後、監査手続に従って、監査対象の管理を事実に基づいて検証し、その確証的な監査証拠を入手することにより問題点を摘出する。監査手続の実施に際しては、根拠となる事実を確かめ、これを監査調書として記録しておくことが重要である。またシステム監査人は、監査手続実施によって把握した事実から重大な問題点を発見した場合には、必要に応じて監査手続の再検討や要員などの監査資源を集中させるなど、その問題点に重点的に監査を実施する機動的な対応が求められることもある。

監査手続を通じて得られた事実や監査調書を分析し、当該事実は問題点として重要であるか（指摘事項に値するか）、またそれは改善を要する事項か（改善案を提示する）を検討する。このプロセスが監査意見形成の基礎となる。

監査の結果、明らかになった問題点（指摘事項）、改善提案、あるいは優れている点などをもとに監査報告書を作成する。正しい評価を行うためには、把握している事実が信頼できるものであることが前提となる。したがって、この段階で事実確認が不十分であったり、自信のない判断根拠があったりしてはならない。また、監査で把握した事実によっては、緊急な報告を要することもあり、その場合は適時に口頭で報告を行い、後日正式な監査報告書を作成する。監査報告書案に基づき、指摘事項、改善案の妥当性、評価の公平性、前回評価との継続性などについて監査部門内で意見を交換する。その際に、類似した監査対象の監査結果との比較などを行いながら最終的に評価の妥当性を確認する。その後、監査報告書について監査部門長の承認を得て、トップマネジメントに対す

る報告は、個別の報告会を設け、短期計画ごと（監査事業年度ごと）に行うなど、各国立大学法人の事情や手続きに応じて直接かつ定例的に行う。ただし、経営に重大な影響を与えるなど緊急を要する場合は速やかに行うことが望ましい。最後に、トップマネジメントに対して速やかに監査報告書を提出し、必要に応じて監査結果の報告を行う。被監査部門や関連部門に対しでは監査報告書の写しを回付することが望ましい。

監査報告後は、監査部門が提示した改善提案が確実に実行されていること、または他の方法などにより指摘事項の改善が行われていることを把握し、改善結果の妥当性を確認するためのフォローアップを行う。改善状況確認の結果、重大な指摘事項に対する改善状況に問題があると判断した場合や、改善結果を実際に監査で確認する必要があると判断した場合は、フォローアップ監査を実施する。フォローアップ監査結果についても、監査報告書にて報告する。

⑥小規模な大学組織におけるシステム監査の取組み

ここまでは規模の大小には関係なく、どのようなプロセス及び内容でシステム監査を実施するかを記述しているが、体系的なシステム監査を全面的に展開できる大学は現実的に少ないであろう。特に、規模の比較的小さい大学やシステム監査要員やシステム監査に充てる予算も少ない大学では、そのための予算や要員の確保作業から始める必要のある場合もあろう。ここでは、現時点でヒトもカネもなく自力でシステム監査を実施せざるを得ない場合のシステム監査への取組みについて述べたい。それにはリエンジニアリングでいうところの「現状（AS－IS）分析」「あるべき姿（TO－BE）分析」「ギャップ（GAP）分析」のプロセスが参考になる。これはシステム監査だけではなく、いろいろな業務にも適用されるので、システム監査要員が十分いない組織でもシステム監査業務に応用できるものと考えられる。

その第一段階は、組織の業務プロセスの中でどんな情報資産がどのように使われているのかについて棚卸しを実施することである。情報システムの棚卸しの次に、情報システムを利用する業務プロセス内に潜在するリスクを洗い出し、何らかの形でリスクの影響度を評価し、優先順位付けを行う。このためにも、情報システムと業務プロセスとの関係、特にレビュー、承認、監督、記録、連絡など内部統制手続がフロー上に表現されている業務フローがあれば便利である。ここまでが現状分析である。現状が把握できなければ、効果的、効率的な対策が検討できないので、このプロセスが最も重要である。

第二段階は、優先順位の高いリスクに対して自組織にとって間尺にあったリスク対策の「あるべき姿」を検討、決定することである。リスク対策には、上記のような内部統制手続きが確立していることが最低限必要である。内部統制の欠落、あるいは重複がないように、また重要な内部統制には相互牽制が効くような仕組みにしておく必要がある。またリスク対策には、当然ながらモノ、ヒト、カネといった資源が必要になるので、それらの制約条件をよく検討しておかなければならない。

第三段階は、現状とあるべき姿とのギャップを、誰がいつまでにどのように埋めるのかについてのアクションプランを立案実行する段階であり、その進行状況をフォローし、必要であればプランの改善も行う段階である。

システム監査を外部委託するとシステム監査の専門家が上記のようなプロセスを効率的に行い、問題点や課題の洗い出し、さらには改善提案も盛り込んだ監査報告書を作成してくれるが、自力でシステム監査を実施する場合には、上記のようなプロセスや既述した内容の作業を学習しながら進めていく必要がある。

参考文献

『よくわかる会計情報システム』　中央青山監査法人編　税務経理協会

『社内情報システム導入ガイド』　手塚聡、佐藤文弘著　日本経済新聞社

『成功するシステム導入の進め方』小野修一著　日本実業出版社

『ネットワークセキュリティー学術情報の発信と保護』　学術情報センター編丸善

『IT ガバナンス』　甲賀憲二、外村俊之、林口英治著　NTT 出版

『金融庁検査マニュアル（システムリスクチェックリスト項目）』　金融庁

『システム監査基準』『システム管理基準』『情報セキュリティ管理基準』経済産業省

『システム監査指針』『フレームワーク』　金融情報システムセンター

1. 戦略フレームワーク評価のチェックリスト

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
1a. 大学は以下の事柄に関する戦略を有しているかどうか。 ・情報 ・情報システム ・情報技術 1b. これらの事項に関する戦略を持っているのなら、それらが文書化され大学によって公式に受け入れられているか？ もしそうであるならば、だれが最終的にレビューし、誰が許可したのか？ 1c. 情報システム・情報技術戦略に関する文書は明確に、大学全体の戦略目標とのつながりを示しているか？ 1d. もしそうであるならば、それらの文書において戦略的目標はどのようにして達成すべきとなっているか（たとえば工程表の確立やタスクの認識など）？		・情報戦鴫が、大学における教育、学習、研究および経営管理情報の提供に必要な情報ニーズをきちんと反映しているかどうかについてレビューする。 ・大学の戦略計画が、情報システム・情報技術に関する戦略文書において、適切な形で反映されているかどうか、レビューする。 ・情報システム・情報技術戦略（もしくはそれにあたるもの）について、それが大学における情報ニーズを満たすのに必要な全てのシステムを認識していること、およびそれらのシステムを大学においてどのように発展させ、またサポートされるべきか、ということについてきちんとカバーしていることをレビューする（戦略はサービス提供の組織の枠組、メンテナンスに必要な資金及び物理的資源について考慮しなければならない）。	
1e. 情報システム・情報技術に関する戦略文書は、全ての資源（資金、スタッフ、設備その他の物理的資源）が効果的に提供されるよう計画される必要があることを認識しているか？またこれらの要求は大学の短期的・長期的な財務見通しを反映しているか？		・情報システム・情報技術に関わる、原価計算モデル／組織メカニズムをレビューするとともに、それらが戦略を実行するに当たって必要な財務的、人的および物理的な資源を適切に考慮しているかについてもレビューする。	

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
1f. 情報システム・情報技術に関して費用が十分手当てされているか（所有権に関わるトータルコストを考慮しているかどうかも含む-3.2 節参照）？ 1g. 情報システム・情報技術戦略が、大学における情報システム・情報技術に関する戦略目標を策定し、監視し、評価し、改訂するというスタッフの役割と責任を正式に特定化しているか？ またこれらの責任は所定の時間の枠内に特定されているか？ 1h. 上級経営者の中に、特に情報システム・情報技術戦略の導入に対する責任を持つ者がいるかどうか。 もしいるならば、その人物はかかる目的に用いられる情報技術に関する知識を有しているか？		・いつ情報システム・情報技術戦略が評価され、改訂されたかをはっきりさせるとともに、それらが所定の時間の枠内に収まるようにする。 ・上級経営者が戦略的見地から、情報システム・情報技術をどのように管理するか？ ・過去 12 ヶ月間において、学長が学内の情報システム・情報技術の発展において、どのように関わってきたかをはっきりさせる。	
1i. 学長は情報システム・情報技術に関する戦略の展開をどのようにコントロールするか？			

2. 組織フレームワーク評価のチェックリスト

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
2a. 情報システム・情報技術戦略の導入を主導し、監視する責任を持つ、効果的な戦略グループが存在するか？ もし存在するならば、そのグループの責任者には上級の経営者、ないし委員会等があてられているか？ その委員会等は、学内における教育、学習、研究及び経営管理の情報について何らかの関心を持っているか？ その委員会等は上級経営者ないしは全学の計画委員会へ報告を行っているか？		・情報システム・情報技術戦略グループの権限とメンバー構成を評価することで、グループの独立性を確保し、大学の戦略的ミッションに関連する部分における、グループの権限・任務の広がりと適切性を明らかにさせる。 ・情報システム・情報技術戦略グループの会議議事録をレビューすることにより、会議の開催頻度を定め、情報システム・情報技術に関する戦略および毎年の運用計画が効果的にモニタリングされるようにする。	
2b. 情報システム・情報技術部門戦略導入を支援する部門の役割および責任が、公式に定められているかどうか？ もし定められているなら、その文書は最新のものであり、現実の組織構造を反映しているかどうか？		・情報システム・情報技術部門の権限をレビューし、情報システム・情報技術戦略の要求を反映しているか、情報システム・情報技術サービスは適切に優先順位付けされているかをレビューする。	

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
2c. 大学には、情報システム・情報技術部門の運営をモニターし、レビューするための明確な報告システムが作られているか？ もし作られているのであれば、上級経営者のうち一名は当該部門による達成度およびその責任の遂行を監督しなければならない。情報システム・情報技術戦略グループ（ないし相当する部門）は情報システム・情報技術部門の活動をモニタリングする責任を持っているか？		・(2a. の行動への示唆を参照)	
2d. 中央集権的に管理するシステムと、分権的に管理するシステムの両者について、そのコストとベネフィットを比較したか？		・大学で行われているコスト／ベネフィット分析をレビューし、情報システム・情報技術が提供する VFM（支出に見合う価値）に関連して、現状の組織構造が有効か再考すべきかを決定する。	
2e. 情報システム・情報技術管理者が適切な情報技術スタッフを雇用するのに必要な知識と能力を持ち合わせているか？ 情報システム・情報技術戦略の効果的な導入を担保するのに必要な情報スキルが定められ、それに対する公式かつ日常的な援助がなされているか？		・情報システム・情報技術管理者がスタッフ採用に関する研修を受けるべきか否かを決定する。	
2f. 業務内容と、求める人材についての詳細が、すべての情報システム・情報技術のポストについて準備されているか？		・情報システム・情報技術へのサポートとサービス提供に関する、スタッフの業務内容と役割、責任をレビューすることで、適切な職務が確立されスタッフが適切な能力を身に着けられるようにする。	

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
2g. すべての情報システム・情報技術スタッフは、自己の責務を果たすのに必要な資格を持ち、研修を受けているか？		・情報技術スタッフの研修プログラムをレビューし、スタッフが最新技術を身につけ、各自の責任を効果的に果たすことが出来るようにする。	
2h. 核となる情報技術者の流出のリスクを認識しているか、またそれを管理しているか？		・核となる情報技術者を認識し、どういった処置が大学を守るのに用いられてきたかをはっきりとさせる。	
2i. 大学は情報技術研修の公式施策を確立しているか？ 2j. 全学におけるスタッフと学生に対する基本的な情報スキルの研修提供について、役割と責任が明確に定まっているかどうか？		・情報システム・情報技術戦略（またはそれにあたるもの）をレビューすることで、学生、教職員の異なる研修ニーズについて把握し、予算を配分し、レベルに応じた情報技術のスキルの目標を特定すること。	
2k. 全学の戦略計画および情報システム・情報技術戦略にいて、セキュリティ関係が正式に評価検討されたか？		・大学のセキュリティ政策をレビューし、情報システム・情報技術関連の事項を網羅するようにする。	
2l. 全学レベルで、情報システム・情報技術につき障害からの復旧施策と方法を発展させ、テストするための役割と責任がはっきりしているか？ はっきりしているならば責任はどのようにして遂行されるのか 潜在的な情報システム・情報技術上の障害の評価検討は正式になされているか？		・情報システム・情報技術の障害回復プランを 12 ヶ月に 1 度はテストされているようにするとともに、テストにおいて認識された弱点については修正しておく。	

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
2m. 情報技術セキュリティに関しては、以下の局面に対する役割と責任が明確に定められているか？ ・物理的セキュリティ ・ソフトウェアとデータへのアクセス・コントロール ・データの統一性 ・関連する法令にしたがっているか？		・情報技術セキュリティのこれらの局面に関する職務内容をレビューすることで、責任が公式に委任されていることを確実なものとする。	
2n. 情報システム・情報技術に関するセキュリティ上の事件が定期的に報告されているかどうか（年次報告への準備も含む）？ もし行われているなら、誰によってなされているか？		・どのようなものであれ、過去１年以内におきたセキュリティ上の事件を明らかにし、それが所定の方法によって確実に報告されるようにする。	
2o. 大学は情報関連機器について本部で集中して所有管理するのか、それとも分散して所有管理するのかについて、そのコストとベネフィットを考慮したかどうか？		・情報関連機器について本部で集中して所有管理するのか、それとも分散して所有管理するのかについてのコストとベネフィットをレビューし、直接費と間接費の両方、および財務的、非財務的なベネフィットの両方が確実に考慮されるようにする。	
2p. 全学のハードウェアとソフトウェアの需要を調整するため、情報関係資産すべての目録はあるか？		・情報関連資産をランダムにチェックすることで、資産目録の正確性を確保する。	

3. 投資マネジメント評価チェックリスト

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
3a. 大学は部局での使用分も含め、情報システム・情報技術に関する支出の全てを把握できるか？		・財務・電算システムをレビューし、情報システム・情報技術関連支出を確実に認識し計算できるようにする。	
3b. 所有にともなうコスト総額が、大学における現行の情報システム・情報技術配置において定量化されているか？ 情報システム・情報技術のイニシアチブにおいて所有にともなうコスト総額が定量化され、他の選択肢と対比されているか？		・所有に関わるコストの総額について 3.2.2 に挙げた例示と見積もりを用いて再計算し、自大学で計算したものと比較し、それらが確実に現実性を持つようにする。	
3c. 情報システム・情報技術投資への年度予算措置は全学的なものか？そうであるならば、予算は情報システム・情報技術戦略グループによって公式に認められたものか？		・情報システム・情報技術への支出に関連する全学的な予算コントロールの仕組みをレビューし、予算が効果的に計画・管理されるようにする。	
3d. 実績と予算が比較され、情報システム・情報技術戦略グループに対して、年間を通じて定期的に報告されているか？		・情報システム・情報技術戦略グループの議事録をレビューし、過去一年間の情報システム・情報技術関連支出が定期的に報告されるようにする。	
3e. 情報システム・情報技術支出は本部予算、部局予算全てにおいて認識できるものか？		・全学にわたる予算例をレビューし、情報システム・情報技術関連支出を確実に認識できるようにする。	

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
3f. 予算と実績は比較され、上級管理者に対して、年間を通じて定期的に報告されているか？		・情報システム・情報技術予算をレビューし、それらが現実性と十分な意味を持ち、年間を通じて実績をモニタリングするのに用いられるようにする。	
3g. 情報システム・情報技術関連プロジェクトへの投資はどのようにして正当化されたか、またこの方法は、全学の部局において標準的な方法として適用されているか？ 3h. 公式の投資評価技術が情報システム・情報技術関連プロジェクトに適用されているか、もし適用されているならば、それは幾ら以上の投資判断に用いられているか？		・大学による情報システム・情報技術投資への全般的アプローチをレビューし、それが効果的にコントロールされ、モニタリングされるようにする。 ・直近の主要な情報システム・情報技術関連プロジェクトをサンプルとして選び、それに対して用いられた方法の是非を検討する。	
3i. 情報システム・情報関連プロジェクトの評価、選択および優先順位付けに如何なる基準を用いるか？ これには幅広い選択肢の評価も含まれているか、またこれらの基準は同様に各学部における情報技術への支出にも適用されるのか？ 3j. 重要なプロジェクトは全て開始前にコストとベネフィットが認識されているか、されているなら当該分析は独立した担当者（財務担当など）によりレビューされるか？ 3k. コンピュータ関連プロジェクトの財務評価は、適切に訓練されたスタッフによってなされているか？		・情報システム・情報技術導入に用いられた投資基準をレビューし、選択されたプロジェクトが資金的に可能であり、大学にとって確実に受け入れられるようにする。 ・直近の主要な情報システム・情報技術関連プロジェクトについて、大学の管理手続きがそのようなプロジェクトに適切であるようにする（たとえば決定は選択肢の評価後に行う、プロジェクト原価計算を独立して行う、投資評価技術を展開する、正式な許可をプロジェクトのスタート前に入手するなど）	

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
3l. 情報機器の配置と更新への適切な財務計画があるか？		・更新政策が理にかなっているかをレビューする。	
3m. 大学の財務規定に、コンピュータ機器について、幾ら以上の価格のものを資産計上するか、何年間で減価償却するかといったことが明文化されているか？ 財務規定において、抱き合わせ購入について資産計上すべきか否かが明文化されているか？		・情報機器購入のサンプルを選び、大学のコンピュータ化政策に従って、適切に計算されるようにする。	
3n. 情報機器の購入において大学が VFM な購入が出来るようにするためには、どのような手続きと統制が必要か？ 3o. 主要な情報関連機器の購入において、正式な入札手続きが適用されているか？		・主要な情報関連機器の購入手続きをレビューし、大学がグッドプラクティスのためのガイダンスから効用を得られるようにする（各学部の機器購入も含む）。	
3p. 情報システム・情報技術関連部門は、すべての主要な情報関連の発注契約を廃棄しなければならないか（サポート、ネットワークの能力、互換性および所有に関わるコストに関して適切に考慮出来るように）？		・（3n 以下の示唆を参照）	

4. 運用管理レビューのためのチェックリスト

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
4a. 年間運用計画は中央における情報システム・情報技術の運用をカバーしているか？もしカバーしているならば、その運用計画は情報システム・情報技術戦略の目的に従っているか？　年間運用計画は人的資源をどのように拡大するかということや、異なるサービスに配分される予算について、どのように認識しているか？		・情報システム・情報技術戦略に関連する運用計画を考慮し、部局における計画が、戦略において示された大学の戦略計画に従っているかどうかを明らかにする。 ・年間運用計画と四半期／年間報告をレビューし、計画通りにサービスが提供され、行動がなされるようにする。	
4b. 運用計画の進行状況と達成度を確実に、適切にモニタリングし、報告ができるようにするために、公式の手続きが出来ているか？		・運用計画をレビューし、計画の導入と目的の達成がモニタリングされ、（情報システム・情報技術戦略グループ等に）報告されるようにする。	
4c. 正式なサービスを定義した明細書（サービスレベル合意書も含む）が情報システム・情報技術サービス向けに準備されているか？		・サービスを定義した明細書（あるいはサービスレベル合意書）をレビューし、それがユーザーへのサービスの正確さとサポートの範囲の詳細を示し、パフォーマンス基準のような、サービスの質と効果を測定するメカニズムを提供出来るようにする。	
4d. 情報システム・情報技術の運用とサービスの質に関するユーザーの満足度は定期的にモニターされているか？		・情報システム・情報技術サービスの質に関するユーザーのフィードバックを得、回答する手続をレビューし、前年度それらの手続に従った処理が行われていたかをはっきりさせる。	

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
4e. 全ての潜在的な新規プロジェクトに、必要な公式の評価手続きが行われるか		・最近のプロジェクトを選択し、鍵となる段階において適切なプロジェクト管理技術が適用されるようにする。	
4f. 以下の鍵となる段階において、情報システム・情報技術関連プロジェクトに対する適切なプロジェクト管理が行われているか？ ・計画 ・モニタリング ・報告 ・評価		・（行動への示唆 4e 以上を参照）	
4g. ウェブサイトの使用に関するモニタリングやトラフィックに対する課金がいつ行われ、これらのサービスに対するコストを最小化するかの確定するに対して適切な管理が行われているかどうか？		・課金が多くなっている場合、コントロールが効果的かをはっきりさせる。	
4h. 障害復旧プランはあるか？ もしあるならば、それは重要な業務システム全てをカバーし、少なくとも年一回十分にテストされているか 7		・障害復旧プランをレビューし、重要な業務システム全ての継続的な使用の確保に適当かを明らかにする。またのその計画は完全にテストされ、明らかな問題は確実に修正されるようにする。	

考慮すべき事項	コメント／ノート	行動への示唆	詳細なコメント／参考資料等
4i. 該当する情報関連法規に確実に従うための、適切な手続きが存在するかどうか？ 4j. 全てのユーザーは大学のネットワークへのアクセス、セキュリティおよびコンピュータ機器に関する定められた取り扱い方法について周知されているか？		・大学の持つ手続きと管理方法を明確にし、該当する法規の遵守、コンピュータ運用に関する健康および安全の確保、それらのアレンジが適切かどうかを確実に明らかにする。 ・学生やスタッフへのハンドブックやニュースレターをレビューし、情報関連機器の使用に対する適切なガイダンスの存在と、該当する規定やセキュリティ、適切な使用に関するユーザーの責任をはっきりとさせる。	
4k. 情報システム・情報技術に責任を持つ上級経営者は、管理情報や業績指標を定期的に提供されているか？		・どのような情報が提供されるか、ガイダンスへの参照と報告書の中で用いられるベンチマークが適切かを確実にする。	