大学におけるネットワーク運用管理者のためのセキュリティ体制の構築

Revision 2 (2004/4/26) 佐藤慶浩

1 セキュリティプログラムの構築の仕方

情報セキュリティプログラムの構築の仕方は、民間企業等によって広く経験が蓄積され、共有されている。大学におけるプログラムを考える場合には、民間企業等のような教育機関以外の一般的組織でのプログラムを参考にすることができるが、それら一般とは異なる条件を加味しなければならない。ここでは、一般的な取り組みについては概説と重点項目の再確認にとどめて、大学における差異を少し強調して解説する。一般的な取り組みの詳細については、書籍等によって理解を深めることができる。

大学における情報セキュリティプログラム
＝ 大学以外の一般組織におけるプログラム ＋ 大学における特徴あるプログラム

図 1

1．1 情報セキュリティプログラムのライフサイクル

情報セキュリティプログラムのライフサイクルは、基本的に「計画」、「実施」、「確認」、「見直し」の繰り返しである。

情報セキュリティプログラムのライフサイクル

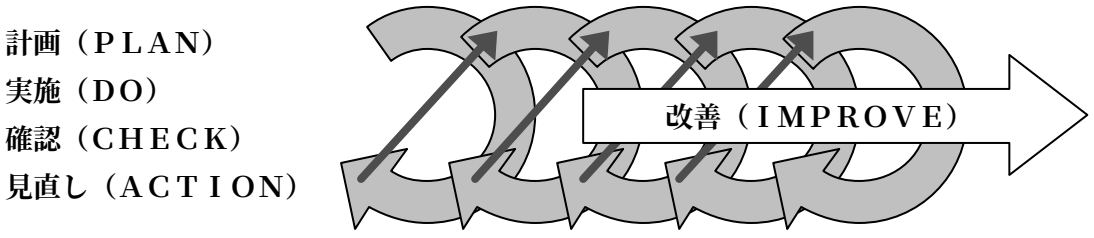

図 2

このうち最初の段階である「計画」について、「見直し」も意識しながら本稿では主として述べる。「実施」と「確認」の実現手段の技術的な選択肢は、一般組織のものと大学とで基本的に変わらない。むしろ、一般に供されているものを採用することは、安定性やコストの面で有益である。運用方法については、大学特有の配慮が必要であるため、適宜説明することにする。

本稿は、国立情報学研究所(http://www.nii.ac.jp/) からの委託報告書として執筆したものを、同研究所の許可を得て公開するものです。

１．２　情報セキュリティポリシー策定委員会

「計画」段階の主たる作業は、調査と審議であり、その成果物としての計画関連文書の作成である。以下では、まず、情報セキュリティに関する目的、原則、ポリシーの策定方法を順に説明していくが、これらの文書をまとめて、情報セキュリティポリシー関連文書群と呼ぶことにする。そして、実際に策定する担当者を、情報セキュリティポリシー策定委員会、あるいは、策定委員会と呼ぶことにする。
情報セキュリティポリシー関連文書群を策定して制定するまでには、主として４つの作業を経ることになる。作文し、審議・調整し、承認を得て、発布する。前２つが策定で、後ろ２つが制定に関することである。

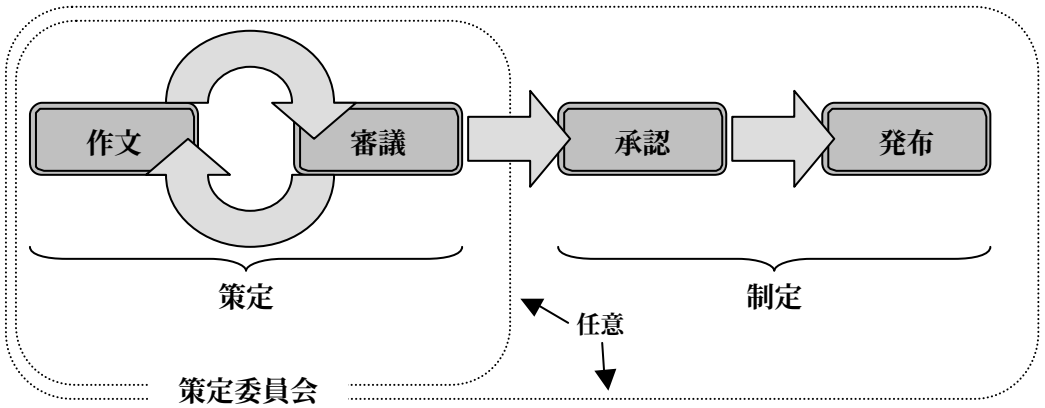

図 3

４つの作業のどの範囲を策定委員会に含めるかは、任意であるが、４種類の作業があることを意識して、委員の選任を行うとよい。
人選であるが、民間企業での策定、制定の経験則からすると、情報セキュリティの技術専門家は、情報セキュリティプログラムの計画段階では、相談役程度でよく、むしろ、組織内に何らかの決め事を作り上げていく経験を有する方々の協力の方が貴重である。
それらの方々に加えて、民間企業であれば、品質保証部門などの取り組みや課題解決の経験が活用できる。大学であれば、環境保護対策に取り組んだことがあれば、その方々の協力を得られれば心強い。
また、後述するが、学内の規則全般に通じた方の協力は必須である。その協力が得られない場合には、規則全般の読み合わせが必要となる。同様に大学組織の関連法令等に通じた方が少なくとも相談役として参加することがコンプライアンス（遵法）について審議する

場面では必要である。

１．３　情報セキュリティプログラムの目的

委員会が発足して、最初にすべきことは意識合わせである。
どんな事柄であれ、やろうとしていることの目的を考えることは重要である。情報セキュリティプログラムを構築する目的は、情報の安全性を保つことによって、情報活用を円滑に進めることだと考えるべきである。別の言い方をすれば、情報のセキュリティを守ることは、目的ではなく情報活用の要件になる。
情報セキュリティ対策を進める場合には、セキュリティ対策を目的とした検討だけをすると、うまく運用できなくなることがある。特に情報システムが、情報を活用するために導入しているものであるのに対して、情報セキュリティ対策は、情報の使用を制限する側面がある。この相反する使命のバランスを見出すことが、情報セキュリティプログラムを成功させるために、もっとも重要なことである。セキュリティ対策の強度だけを高めようとすれば、現場にとって受け入れ難い目標設定となった場合に、定めた対策は単なる努力目標としてとらえられ、形骸無実化することになる。情報を活用するために必要なセキュリティ対策としてのバランスを常に取ることが成功の鍵である。バランスを取るために、現状の確認と見直しが必要になる。計画した目標に対する検査や監査だけに終始すれば、当初いくら吟味された目標であっても、環境の変化に追従できずにバランスを失うことになる。新しい技術の導入や組織の情報活用への依存度などの環境変化に対応して、適切に変化することがバランスとしての安定を保つことになる。変化しないことが安定だとまちがえてはならない。

図４に情報セキュリティプログラムの目的の例を示す。このような文章を作成して、プログラムの構築を検討する委員全員が十分に審議することによって、プログラムの目的についての認識を共有することは非常に重要である。情報セキュリティの目的は、一見、当然のことのように思われるが、実際に審議を尽くせば、意識の違いが出てくるはずである。目的段階でその違いをなくしておかないと、これ以後のプログラム全体の構築を揺るがしかねない。認識を共有するための審議において心がけるとよい事柄のひとつとして、「カタカナ言葉をなるべく使わないこと」を推奨する。カタカナ言葉は、仮性対話[1]を生じやすいからである。たとえば、本稿では「情報セキュリティプログラム」という語句を使用しているが、その語句の妥当性までも疑ってかかるのは、実は正しい姿勢である。

---

[1] 仮性対話：会話の内容が通じ合っていないのに、相づちなどだけが、あたかも、会話の内容が通じ合っているような状態。たとえば、ポリシーについての定義や位置付けなどを十分にしていない状況で、「ポリシーって重要だよね？」「うん。うん。」と会話する状態。

情報セキュリティプログラムの目的（例）

情報システムは、情報の隠蔽を目的としない。積極的な情報の開示／共有をするための基盤である。
情報セキュリティは、積極的情報利用を現実のものとするために、情報を適切に保護するための取り組みである。

「情報資産に対するアクセスへの必要性」と「これらの資産の機密性、保全性、可用性および適正な使用を守る」との効果的なバランスを取るために情報セキュリティプログラムを構築する。

図 4

１．４　情報セキュリティポリシー

情報活用と情報セキュリティのバランスの目標とその保ち方を定めて明文化したものが情報セキュリティポリシーであり、情報セキュリティプログラム構築の基礎となるべきものである。セキュリティ対策をどれだけやらなければならないかを定めるというよりは、どの程度やらなくてよいかが明確に判断できる内容となっていることが望ましい。ポリシーについては後述する。

１．５　情報セキュリティ原則

１．５．１　一般的な原則の例

また、基礎に相当するものとして、情報セキュリティ原則がある。情報セキュリティポリシーの策定に先駆けて、ポリシー策定そのものの規範とも言うべき情報セキュリティの原則について検討するとよい。情報セキュリティ原則は、組織の背景や目的に合わせて自由に発想すればよいが、ＯＥＣＤ（経済協力開発機構）の情報セキュリティ原則などをたたき台として参考にすることもできる。（図５）
９つの原則のうち、不要なものを削除したり、必要なものを追加したり、項目をまとめるなどして、これから検討する情報セキュリティポリシーをどういう原則で策定するのかを審議することは、前述した目的の審議と同じく意味のあるものである。
図５の９原則は、ＯＥＣＤ情報システム及びネットワークのセキュリティのためのガイド

ラインという全文[2]の一部を引用したものである。引用部分だけからは趣旨がわかりにくいかもしれないので、全文を参照していただくとよい。しかしここでは、わかりにくいということに、あえて着目していただきたい。解説的な「ガイドライン本文」と、図に引用した部分のような「まとめの一行文」との関係を確認した上で、この審議をしていただくと、情報セキュリティに関することについて、伝えたい内容を簡潔な文章にすることの難しさや、文章作成の際に心がけなければならないことを実感できると思う。そのように、原則の審議は、ポリシーを策定する前の肩ならしとして、情報セキュリティプログラム構築の初期の段階で策定委員会の委員によって審議していただきたい。わずか９つの項目を審議するだけで、そこから得られる教訓は多いはずである。

できあがった情報セキュリティ原則は、情報セキュリティポリシーの策定審議の過程で使うものであるが、そのまま最終文書に残しておいてもよいし、あえて公開する必要のない原則については、策定委員会限りとして非公開にしてもよい。いずれにしても、その後のポリシー見直しの際に、どのような背景でポリシーを策定したかを再確認するのに役立てることができる。もちろん、見直しの際には、情報セキュリティ原則そのものが見直されることがあってもよい。

[2] ＯＥＣＤセキュリティガイドライン邦訳（経済産業省 商務情報政策局 情報セキュリティ政策室　http://www.meti.go.jp/policy/netsecurity/oecd2002.htm）

情報セキュリティ原則の例

ＯＥＣＤセキュリティガイドライン 2002 年版邦訳より

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装（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．セキュリティマネージメント（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。

図 5

１．５．２　大学における一般との相違点の洗い出し

これらの原則を検討する一部として考察すべきが、大学の相違点であろう。
巷にある情報セキュリティの事例の多くが民間企業での蓄積であることを冒頭で述べたが、そこでの暗黙の原則と比べて、大学において異なる点を明らかにしておくことが重要である。

政府や企業の組織の場合には、情報や情報システムを利用・運用する者は、基本的にそれらの組織に何らかの雇用あるいは従事契約関係を結んで従属している者である。大学においては、教職員がそれに相当する。したがって、教職員に係わる情報セキュリティ対策は、大学以外の対策を参考にすることができる。しかし、大学においては、情報セキュリティプログラムの要員として学生が含まれる。学生のような存在は、大学以外の組織では前提としていない。
図６　に学生の存在における相違点を列記する。

学生の存在における相違点（無雇用者参加の原則）

大学とは雇用や従事契約を締結していない学生が；
・大学施設内への立入許可を受けている
・大学設備を使用して学内情報にアクセスする
・大学設備を使用して学外インターネットを利用する
・大学設備に情報を蓄積することがある
・大学設備から情報を発信することがある
・情報システムの運用に従事することがある
・情報システムの管理者権限を有することがある
・情報セキュリティプログラムの役割の一部を担うことがある

図 6

民間企業等では、情報セキュリティプログラムに限らず、何らかの具体的被害が発生した場合に、加害者の特定やその証拠を得ることが組織自身によってできない場合には、捜査機関への協力を要請することが考えられる。また、逆に自組織の参加者によるものと思われる行為によって、他者に被害を与えてしまっている場合に、捜査機関からの証拠提出などの協力要請には、その内容が業務に支障を与えたりしない限り応じることになる。
大学においては、学生が当事者となっている場合について、捜査機関へ協力要請を依頼すること、捜査機関からの証拠提出などの協力要請に応じることについては、単純ではなく、慎重な判断を要することになる。場合によっては、それらを積極的に行うことはできず、加害者の特定や、その証拠の保全を困難にする場合がある。
このため、民間企業等では、捜査機関との連携関係も選択肢に入れて、情報セキュリティプログラムの構築をするが、大学においては、必ずしもそうとは言えない。

学生に対する捜査機関との関係における相違点（調査権謙抑の原則）

民間企業に比べて；
・捜査機関に対する、捜査要請を容易にできない
・捜査機関からの捜査協力要請（証拠提出等）に対して、容易に対応できない

図 7

民間企業等では、情報セキュリティプログラムに罰則を設けて、違反時に処罰などを検討し事後責任を明確にすることを前提にしている。しかし、学生が万が一、情報セキュリティプログラムへの違反を起こした際の相違点を図８に示す。
これらは大学における現実として、可罰が限定的にしか行使できない原則と言うことができる。

学生の違反時における相違点（可罰謙抑の原則）

退学勧告にまで達しない学生の違反に対しては；
・就学に支障を与えるような情報システム使用制限をできない（ＩＤの一時使用禁止等）

図 8

政府や企業の組織においては、業務に必要な最低限のアクセスを許可することによって、業務に不必要なアクセスを技術的に防止するという対策を講じるのが前提である。しかし、工学部などインターネット利用なども含めて広範な技術研究の対象としている場合には、そのアクセスに制限を与えることが困難となることも考えられる。

研究目的における相違点（アクセス自由の原則）

研究・教育の目的であれば；
・情報やネットワークへのアクセスを制限することはできない

図 9

ここで紹介したような大学特有の原則を確認することは重要である。民間企業等ではこれらの原則を前提としていないため、民間企業等で成功を収めている情報セキュリティ対策をそのまま活用するだけではなく、教育機関では何らかの独自の工夫を加えなければ、情報セキュリティプログラムがうまく構築できないことになる。
これらの相違点も加えて、みずからの大学の情報セキュリティ原則をまず検討して整理することで、環境に則した情報セキュリティポリシーを策定することができる。逆に、これらの特異な原則を考慮せずに、一般的な成功事例などだけを流用したのでは、大学において、そのポリシーは現場で受け入れられず、実効性のないものとなることが予想される。

情報セキュリティを論じる多くの資料においては、これらの原則についてあえて触れられることが少ない。あえて触れなくても、民間企業等では、ＯＥＣＤのセキュリティ原則のようなものだけで十分なことが多いからだと考えられる。
大学における情報セキュリティプログラムの構築にあたっては、これらを再確認することが求められており、大学の特殊性を認識しておかないと、「一般にはうまくいくはずのことが、自分達の大学ではうまくいかない」という問題が起き、その解決策はおろか原因すらわからないということになってしまうかもしれない。その結果、「自分達の大学では情報セキュリティの意識が希薄で、なじまない」という誤った結論になることもある。情報セキュリティプログラムがうまく機能しない状況は、環境側の問題ではなく、情報セキュリティプログラムを環境に即すための検討が不十分なだけであることが多い。
実際には、大学以外の組織でも、情報セキュリティプログラムの計画段階において、一般的な環境との違いが見落とされることがないとは言い切れない。しかし、それを見直して、改善し、環境に馴染ませていくようにするものである。（図２参照）しかし、ここで述べたような大学特有の原則は、情報セキュリティプログラムに与える影響が非常に大きいため、計画段階で十分に検討しておく必要がある。

１．６　人為的な不正アクセス対策の構成モデル

１．６．１　一般的なモデル

情報セキュリティプログラムには、人為的な被害への対策と、人為的ではない被害への対策が含まれる。先述した情報セキュリティ原則に関する大学の相違点の考察から、大学の特殊性は学生の存在に起因することであり、人為的ではない問題は、概ね、大学以外の組織における対策をそのまま参考にすることができることがわかる。したがってここでは、人為的な被害への対策について考察する。人為的な被害への対策を簡潔に表現すれば、組

織の情報および情報資産に対する不正アクセスや不正使用を防ぐ取り組みである。ここでの注意点は、異なる側面を持った問題が複合していることである。複合問題に取り組むには、問題群を個々の問題に分解して、それぞれの問題に適した解決策を検討することが重要である。
人為的な不正アクセスの被害は図１０に示すように分類することができる。

人為的な不正アクセス被害の分類

無許可のアクセス(unauthorized access)
許可されたアクセスの誤使用(misuse of authorized access)
許可されたアクセスの濫用(abuse of authorized access)

図 10

ここでは；
業務を遂行したり就学したりするのにあたって、その目的のために、情報および情報資産に対してアクセスする権限を、管理者から予め許可された者のことを、以下単に「許可を受けた者」と言うことにする。逆に、管理者から予め許可を得ていない者のことを、単に「許可を受けていない者」と言うことにする。

無許可のアクセスによる被害とは；
許可を受けていない者が、情報や情報資産を使用することによって生じさせる被害を言う。

許可されたアクセスの誤使用による被害とは；
許可を受けた者が、許可の目的以外のことであるという認識なく、許可されたアクセス権を使って、情報や情報資産を使用することによって生じさせる被害を言う。

許可されたアクセスの濫用による被害とは；
許可を受けた者が、許可の目的以外のことと知りつつ、許可されたアクセス権を使って、情報や情報資産を使用することによって生じさせる被害を言う。

これら３つの被害を防ぐための対策は、本質的に異なる種類のものである。

「無許可のアクセス」を防止するためには、アクセス制御装置など技術的な対策を検討することができる。導入した対策の強度が十分か、不足はないかを検査することも技術的に

解決できることが多い。技術的ではない対策としては、ソーシャル・エンジニアリングなどの手法で、許可を受けていない者が、許可を受けた者のアクセス権を不正に取得されないように、情報セキュリティの啓発や教育、訓練を行うことも必要である。

「許可されたアクセスの誤使用」を予防するには、情報セキュリティに関する啓発や教育、訓練などが有効である。そこに悪意は存在しないので、正しい行いに関する知識について、不足していれば補い、誤っていれば是正するという教育で、問題を予防することが期待できる。

「許可されたアクセスの濫用」を防止することは技術的には困難である。これは、明確な悪意の持ち主による被害である。しかもその者は業務遂行のために有しているアクセスの権限内で不正を行う。業務を遂行するために与えているアクセス権であるから、その業務を遂行させるためには、アクセス権を不許可にすることはできない。
この問題に対して技術的にできるのは、アクセス権の精細度を高めて、業務目的ぎりぎりのアクセス権に絞りこむことによって業務以外のアクセスを防止することが考えられる。しかし、それでも、アクセス権の範囲内に対しては、アクセスを禁止できないのであるから抜本的な解決策を見出すのは困難である。
この問題に対する、政府や企業の組織での対策の基本は、事後に罰則を科すことを示すことで、濫用を抑止するという対策である。そのためには、事後に本人が特定できるような仕組みを構築しておくことで、抑止効果を高める必要がある。
それに加えて、問題を事後に察知することができるように、兆候把握のための技術措置を施すことが考えられる。たとえば、日常と異なるような頻度や量、時間帯などのアクセスがないかを監視するといったことである。

以上のような３つの要素に分けて、それぞれの対策を検討することによって、複合的な問題である不正アクセス対策の検討を深めることができよう。

「許可されたアクセスの誤使用」の対策の前提は、正しい理解を得てもらうことによって、不正なことをしないことを期待するのであるから、性善説であると言える。そして、「無許可のアクセス」の対策は、善意の参加者による構築、運用が不可欠である。かれら善意の参加者に、悪意ある者からの不正アクセスを防いでもらうことになるので、これも性善説を前提とすることになる。「許可されたアクセスの濫用」が唯一、参加者の悪意という性悪説を前提にするものである。これらのことから、情報セキュリティプログラムの大きな割合を占めるのは、性善説である。不用意に性悪説の前提を掲げることは、善意の参加者のプログラムへの参加意欲を阻害することにもなりかねない。「性善説を前提にした上で、性悪説も想定する」ことが重要である。そのことが認識できれば、性善説に基づく対策を基

礎として、その上に性悪説に基づく対策を構築することで、情報セキュリティプログラムを構成することができる。
逆に、性悪説だけを前提にしたプログラムは、絶望的で悲観的なものになるであろう。
性善説に基づくとすれば、情報セキュリティの啓発や教育、訓練の重要性や、そこでの訴求内容を環境とプログラムに則して決めることができる。

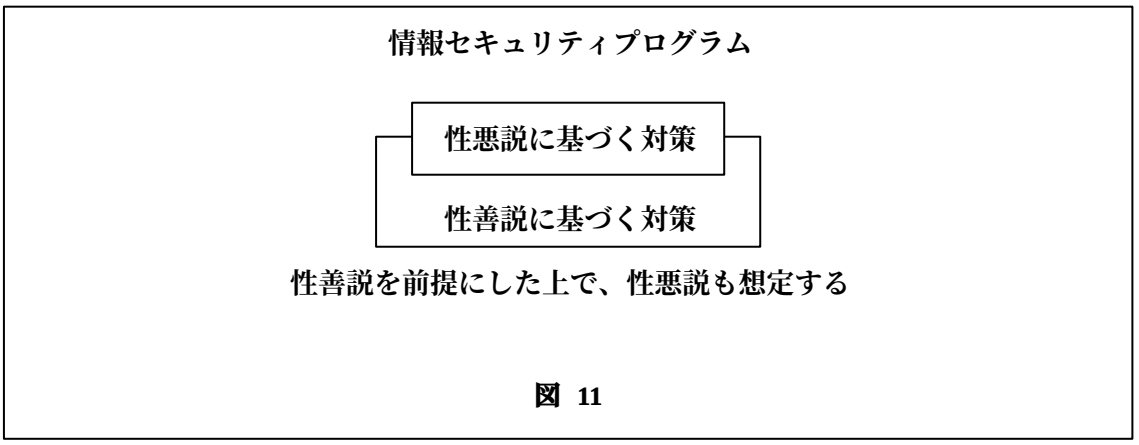

図 11

１．６．２　大学における不正アクセス対策の相違点

「無許可のアクセス」を防止するには、アクセス自由の原則により、大学以外の組織であれば技術対策で十分な課題に対して大学では対策を講じられない場合があるため、故意・過失の両方において一般に比べて脆弱となりやすい。

「許可されたアクセスの濫用」を予防するための抑止策が、大学においては、「調査権謙抑の原則」と「可罰謙抑の原則」により、対策困難となることも予測できる。すなわち、大学では、調査権謙抑の原則により、不正アクセス者の特定が困難となったり、可罰謙抑の原則により、事後の罰則を予め示すことによる抑止効果を期待することが困難になったりするため、確信的な悪意のある者に対しては一般に比べて脆弱となりやすいであろう。
この「許可されたアクセスの濫用」対策において、取りうる選択肢に、大学特有の原則が与える影響は、飛行機の両翼をもがれるに等しいくらいに大きなものと考えられる。

逆に、「許可されたアクセスの誤使用」を予防するための教育については、教育機関である大学においては、理解を深めさせるための手法や経験は、一般の組織よりも豊富であると考えられるので、それらを有効に活用するとよい。

これまでの考察からわかることは、大学においては、不正となることを予めできないよう

にする対策を講じることが困難であることと、それを罰則によって抑止することも困難であることである。このような環境では、「やればできるがやらない」という意識をいかに多くの者に広め、それぞれの意識をいかに高めるかについて、一般の組織での対策に追加して検討する必要のあることがわかる。

１．７　情報セキュリティポリシーによる目標設定

情報セキュリティポリシー策定時の目標設定

目標設定の最低レベルと仮の上限レベル
リスク管理としての目標設定
目標レベルの低下要因

図 12

１．７．１　目標設定の最低レベルと仮の上限レベル

情報セキュリティプログラムの目標達成のために組織の活動をすべて充当することは当然できない。したがって、ある程度の活動に留めて目標設定をすることになる。組織活動のすべてを１００％として、まったく情報セキュリティ対策を行わない状態を０％とすれば、情報セキュリティポリシーとして、０％から１００％の範囲の中で目標設定をすることになる。

目標設定の最低レベルとしては、法令等の準拠がある。このレベルを下回ることは、組織活動が違法であることを意味するからである。このため、大学に関係のある法令等を調査して、最低レベルを知ることが必要である。

たとえば、ソフトウエアの使用許諾ライセンスの遵守に違反しないようにすることは、最低レベルに関係することである。

次に、目標設定の当面の上限レベルとしては、ポリシー制定より以前にある組織内の規則等の限界がある。そのレベルまでのことであれば、そもそも規則で決められていることであるから、それを遵守することは当然のことだからである。しかし、先の最低レベルがそれを下回ることが許されないのに対して、この上限レベルについては、必要であれば、上回ることができる。その場合には、既存の規則との整合や、場合によっては、規則の改定を視野に入れればよい。そのため、最高レベルではなく、仮の上限レベルと表現した。

たとえば、企業であれば、昼休みに私的なインターネット・サーフィンをすることは、就業規則における、会社資産の業務外使用を禁ずる規程に抵触するかもしれない。そのよう

な規程がある企業であれば、上限レベルの範囲内であり、私的なインターネット・サーフィンを情報セキュリティポリシーで禁止することについて、組織内で改めて同意を得る必要はないことになる。もしも、規程がなければ、上限レベルの範囲内かは明確ではないことになるので、組織内での同意を得る調整をし、場合によっては、既存の規則の改定もしなければならないことになる。上限レベルを意識することで、既存の規則の改定の必要性を知ることができる。
これらの民間企業での目標設定については、教職員に対しては、同様に適用することができるであろう。
大学における相違としては、大学が独立行政法人となる場合には、以下のような法令等[3]についても考慮する必要がある。

「独立行政法人情報公開法」
「独立行政法人情報公開法施行令」
「独立行政法人情報公開法施行令情報提供の対象となる法人の範囲省令」
「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」

どのような法令等が最低レベルを決定し、どのような既存の組織内規則が上限レベルを決定するのかを調べて理解しておくことは大切である。

１．７．２　リスク管理としての目標設定

最低レベルを上回り、上限レベルを目安に、ポリシーによる目標設定をすることになるが、情報セキュリティ対策の充実のためには、より高いレベルにしたくなるかもしれない。しかし、レベルを高くすることは、組織の活動を圧迫することになるので、必要以上に高めることは組織にとって必ずしも有益ではない。そこで、どのレベルを適正とすればよいかを決定するには、リスクの許容限界を検討することが良策である。言い換えれば、情報セキュリティ対策をどれだけやるかを考えるのではなく、どれだけやらなくてもよいかを考えるのである。
リスク管理としては、そのリスクを受け入れるのか、受け入れないのかを検討するが、リスクを受け入れない場合に、リスクを軽減するか回避することになる。情報セキュリティにおいては、リスクの軽減策が、すなわちポリシーで定める目標となる。
目標レベルを下げることで生じるリスクが受け入れられるのか、受け入れられないかを検討することが、ポリシーを環境に則したものとするのに重要である。
また、この検討は、ポリシーによる目標設定の理由を組織内に示して同意を得るのに不可欠である。この検討がされていないと、参加者からの「なぜ？」の問いに対して、環境に則した明確な回答を示すことができず、情報セキュリティプログラムが定着しないことに

[3] http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi

なるかもしれない。一見、当たり前のことである情報セキュリティの維持が、なぜ必要なのかを改めて本質的に考えることは大切である。

１．７．３　目標レベルの低下要因

組織活動の資源は、人、物、金、情報と言われて久しい。近年の組織には、資源の有効活用が産・官・学の区別なく、求められている。そのための方策として、情報システムの積極的な活用が求められる。その場合に、情報システムの活用は、情報セキュリティとのバランスを変化させる。積極的な活用は、多くの場合、ポリシーに対しては、レベルの低下を強いることが予想される。
たとえば、民間企業における過去の変化として、正社員以外に社内システムを使用させるようにしたこと、社内のネットワークをインターネットに接続したこと、ホストコンピュータ経由であった業務支援をＰＣなどで社内外と直接できるようにしたことなどがあげられる。これらは、すべて、業務の効率化のために採られた改善策であるが、情報セキュリティポリシーのレベルとして検証してみれば、これらの変化の前と後では、レベルが相対的に下がったことになる。このように、情報システムの活用促進は、レベルを低下させる要因になることがあるという認識をしておくことは大切である。

１．８　情報セキュリティポリシーの策定

ポリシーの策定では、ポリシーで記述する項目を決めなければならない。これには、JIS X 5080（ISO/IEC 17799）に記された項目群をたたき台として参考にすることができる。これらの項目群のうち、大学に必要なものを採用し項目ごとの目標設定を行う。また、項目として不足しているものがあれば、適宜追加する。JIS X 5080 本文の「コントロール」と呼ばれる管理策は、後述するポリシーとスタンダードが混在している。したがって、JIS X 5080からは項目を参考にして、それらについて策定委員会で審議して作文するのがよい。

１．８．１　情報の格付け

JIX X 5080 のうち、必須であるが、日本でおろそかになりやすいのが、情報の格付け（classification[4]）である。情報の格付けとは、情報に対して、「極秘」や「秘」などの種別を定義して、情報をそれらの種別に基づいて格付けし、それに従って取り扱うというものである。情報セキュリティが、情報の機密性(confidentiality)、完全性(integrity)、可用性(availability)の３つの観点で論じられるため、欧米では、それら３種の格付けを

[4] 「classification」は「情報種別」と訳されることが多いが、ここでは「情報格付け」としている。

行う。機密性に関しては、「TOP SECRET」「SECRET」「UNCLASSIFIED」などである。「UNCLASSIFIED」は、「機密ではない」ということだが、日本では「無指定＝非機密」という暗黙にすることが多い。これをあえて種別として設けると、本当に機密ではないのか、情報の格付けを忘れてしまったのかを区別するのに役立つ。完全性については、「CRITICAL」か「NON-CRITICAL」という種別を、可用性については、「VITAL」と「NON-VITAL」という種別などを用いることがある。「CRITICAL」や「VITAL」などの表記内容は様々であるが、完全性と可用性の観点での種別を設けることは重要である。日本では、機密性についてだけが論じられることが少なくない。ひどい場合には、機密性の観点だけで、「重要性」という表記を用いている場合もある。その情報の重要性は、機密性、完全性、可用性の３つの独立した観点によって決まるものであり、１次元的な重要度というものを決められないのが一般的であろう。たとえば従業員の実家の住所が人事記録にあるとすれば、実家の住所に機密性はあるが、完全性や可用性は低い。インターネットに公開しているホームページには完全性を求められるが、機密性はない。多くの情報に可用性は共通に求められるが、給与情報などは、給与支給日以外には、あまり高く求められない。など、機密性、完全性、可用性は独立した要件として扱うのがよい。このため、欧米では、「TOP SECRET」で「CRITICAL」などのように、３つの要件を適宜組み合わせて格付けを行っている。

１．８．２　主語の記述

ポリシーを作文するにあたっては、文章としての主語を明確に記述することが重要である。たとえば、「重要なシステムについては、安全対策措置を講じなければならない」という文章は一見正しいが、主語である「誰が」が記載されていないため、このポリシーを読んだすべての参加者が「誰かがやっているのだろう」と解釈して、結果的に誰もやろうとしない場合もある。目標達成に向けての施策の主語が情報セキュリティ関連文書に記載しない文章は好ましくない。ただし、「誰が」については、スタンダードで必ず記述するなどの策定手法をとることなどで、明確になることが担保されていれば、必ずしもポリシー本文に書かれなくてもよい。この場合、主語は「人」でなければならない。先の例であれば、「重要なシステムについては、安全対策措置が講じられていなければならない」という文章は、日本語の文法上は「安全対策措置」が主語であるが、それでは当然意味がない。受動態の文章になる場合には注意するとよい。基本的には、能動態の文章で作文するのがよい。

１．８．３　役割の定義

主語としての「人」については、個人名を書くのはあり得ないが、役職名や部署名を本文に直接書かない方がよい。情報セキュリティプログラムとしての役割を定義して、「情報セキュリティ管理者が」とか、「情報セキュリティ担当者が」などとした方がよい。それらの

役割をポリシーなどの冒頭で、「情報セキュリティ管理者は、職場の長が務める」「情報セキュリティ情報収集担当者は、情報システム部内に置く」などのようにして、一括して役職名や部署名に紐付けするとよい。このようにしないと、情報セキュリティ関連文書の本文のあちこちで、無造作に登場人物が増えてしまい、それらの関係がわかりにくくなるからである。たとえば、「情報セキュリティ策定委員会」は、役割名称のひとつである。

１．８．４　用語の定義

JIS X 5080 など情報セキュリティに関連する文書を参考にして、ポリシーを作文すると、いつしか専門用語が増えていくものである。学内で理解を得られないと思われる用語については、適宜解説や定義をするように心がけるとよい。
その場合に、解説や定義が必ずしも世の中の標準などに厳密に合致していなくてもよいかもしれない。情報セキュリティの専門家から異論が出るかも知れないが、情報セキュリティプログラムを学内で定着させることが、最重要であるので、そのためであれば、若干の厳密さを欠いてもよいと割り切った方が検討を進めやすい。そのような場合には、別途、ただし書きのようなものをまとめておけばよい。「本学で○○○と表記したものは、一般では○○○と表記されている」などである。後に、外部からの認定を受けるなどの場合には、認定機関に対して、そのただし書きを示して、認定作業を実施してもらう方が、ポリシーを難解にして、学内にその解説書を用意するよりも現実に則している。専門家から理解が得られても、学内の理解が得られないような文章を作文するのは、本末転倒だと考えるべきである。

１．８．５　目標と努力目標

ポリシーでは目標設定をするが、やはり、現実的には達成が困難と思われることもあろう。その場合には、記述表現を努力目標にすることがあってもよい。たとえば、「～しなければならない」に対して、「～することが望ましい」などの表現である。努力目標だけにすると結果的になにも担保されないこともあるので、努力目標は、必ず目標設定に付加的に用いるとよい。すなわち、「～しなければならない。また、それに加えて～することが望ましい」というようにである。このようにすれば、最低限前者が目標設定され、それに加えて後者が努力目標として設定されることになる。しかし、これを乱用してはならない。たとえば、先の例に加えて、「原則として～しなければならい」や「～すべきである」などの多種多様な表現を使い始めると、目標と努力目標の区別がつかなくなる。このような表現の多様化は、策定委員会活動の後半に発生しやすい。それは、審議に疲れてきて、審議の結論をあいまいなまま終わらせようとする場合などに発生しやすくなる。
したがって、策定作業の最初の時点で、「語尾表現の統一」について決定しておくとよい。

ポリシー文章の語尾（述語）は、「～しなければならない」「～することが望ましい」「～してはならない」「～しないように努める」などの具体的な表現を定めて、それぞれの表現の意味するところの意識合わせをしてから、それら以外の文章を書かないようにするのである。策定作業の途中で、追加や変更を適宜するのはよい。定型の語尾に統一し、意識合わせをして語尾を決定すればよい。これをせずに、「原則として～しなければならい」などを無作為に採用すると、策定作業に疲れてきたために、実は仮性対話が発生している可能性が高い。

主語が役割で統一され、学内で用いられる用語を使って、述語である語尾が一定の表現に統一されたポリシー文章は、とても整然としたものになり、読者に対する理解を得やすいものになる。
以上のようなグランドルールを決めて、ポリシーの作文を進めていくとよいであろう。

１．９　ポリシーから手順書へ

情報セキュリティ関連文書には、目的、原則、ポリシーの他には、スタンダードとプロシージャが続く。
ポリシーとスタンダードの定義は、実はあいまいであり、自組織の運用に見合った定義をする方がよい。ただし、少なくともスタンダードについては、実施状況を計測できる(measurable)ようなものになっているのがよい。その観点からすると、ポリシーは定量的な計測が不可能な、精神論的な表現や、抽象的な表現をしてもよいと割り切って、ポリシーとスタンダードを定義するのもよいだろう。いずれにせよ、世の中で言われている定義に必ずしも合致させる必要はない。運用しやすいように定義することの方が重要である。
プロシージャ、すなわち、手順書については注意が必要である。ポリシー項目とスタンダード項目は、概ね一致させることになるであろう。なぜなら、ポリシーで述べたことをより具体的にしたものを、スタンダードとするからである。それと同様にして、スタンダードの項目をそのまま手順書にするのは、情報セキュリティ責任者や担当者など、情報セキュリティ維持を役割として直接担ったものにしか有効ではない。情報セキュリティプログラムの参加者の大部分を占める利用者に対して、情報セキュリティの手順書を提供することは避けたほうがよい。かれらは、情報セキュリティのために、システムを利用しているのではないからである。かれらへの手順は、システムとしての利用手順書の中に、システムを利用する手順の一部として浸透させるのが現実的である。

１．１０　対策の段階的モデル

対策には段階として大まかに、保護(protect)、検出(detect)、対応(respond)があるとさ

れる。これら段階全般をポリシーで目標設定し、スタンダードにて段階ごとの目標を具体化するものとなるが、保護や検出が技術的な対策が主であり、大学以外の事例と相違が少ないのに対して、対応の段階は、人的な対策が重要となり、大学に限らず、自組織の環境に深く依存した内容になるので、十分な検討が必要である。
この段階の対策については、最近では、インシデント・レスポンスやインシデント・マネージメントとして、注目されている。
また、JIS X 5080 の基である ISO/IEC 17799 においても、現行では「対応段階」については多くが書かれていないが、次期改訂では、ひとつの独立した章（17799 では domain と言う）として記載され、さらにその詳細が別の TR(Technical Report) として準備が進められている。事故の発生を前提とするのは無責任であるが、発生を想定した対応体制、管理体制については、今や必須の項目と考えてよいだろう。
これらの段階には含まれない「抑止」が、民間企業では大きな役目を果たしていることを紹介し、大学ではそこに課題があることを先述した。これについても大学においては、十分に検討する必要がある。

１．１１　教育

ポリシーを啓発、教育する場合には、図１３のようなことを予め示すことが必要であろう。
情報セキュリティプログラムだけで、情報セキュリティを完遂させるのは不可能である。関係するその他の施策と連携することで、目標を達成することができる。それにも関わらず、情報セキュリティプログラムには、それだけですべてを解決することが期待されているような風潮がある。これ以前に、組織が取り組んできた様々な施策と同様に、組織全体としての施策の一部として機能することで、プログラムが達成できるものであって、情報セキュリティプログラムだけが、特殊なものではないということは、改めて示した方がよいであろう。

ポリシー本文の読み方

ポリシーでは、
　しなければならないこと
　してはならないこと　等が主として記述されている。
しかし、だからといって、
　記述されていないことを、しなくてもよい
　記述されていないことを、してもよい
という訳ではない。

図 13

１．１２　検査と監査

ポリシー、スタンダードや手順書を策定し、対策を施し、教育を行うという一連の活動により、情報セキュリティプログラムが始動すれば、その状況が目標に達しているかを、検査や監査することで、見直すことができる。
情報セキュリティプログラムは、全員参加型のものという意識が必要である。検査や監査についても、多くの参加者に受け身になられない方がよい。そのためのひとつの方策としては、自主検査などを取り入れ、各自が最初に自分の状況を検査するということで、検査に参加させるとよい。このことはまた、内部監査の実施において、各自の自主検査の結果を確認するということにも役立てることができる。多くの参加者で構成される組織の場合、内部監査を監査チームの限られた人数で実施するには、対象の一部を抜き打ちにして行うしかない。それでも、全体に占める割合を大きくすることは困難であろう。それであれば、性善説を基礎にしていることを再認識して、参加者本人に、内部監査の一部としての検査を協力してもらうというのは、ひとつのやり方である。
また、内部監査においては、参加者との間に、敵対関係の構図を作ってはならない。むしろ、日々の情報セキュリティプログラムでの相談役あるいは、サポート役としての関係を構築することが大切である。
内部監査において、違反が見つかった場合には、それをいきなり責めるのではなく、まずは違反に至った理由を確認することが重要である。すなわち、性善説を一貫させるということである。違反を戒めるだけでは、見直して改善することはできない。性善説に基づけば、違反には、悪意以外の「理由」が存在するはずであり、その「理由」の「原因となっている問題」を解決することが、「見直し」になるからである。そのようにできれば、「違反時に責めたてるのではなく、違反せざるを得なかった現場の問題を解決してくれた」という関係が構築でき、サポート役として認識されることになり、結果的に、悪意ある人達に対する性悪説対策への協力を得ることにつながることを期待できる。

検査と監査

自主検査(self assessment)
内部監査(internal audit)
外部監査(external audit)

図 14