提　言

私立大学向け

ネットワークセキュリティポリシー

2002 年版

社団法人 私立大学情報教育協会

はじめに

ネットワークの上に全ての情報が行き交う２１世紀社会の最大の脅威は、不正アクセス行為による情報の改ざんや破壊、知的所有権の侵害、情報操作等によって国民生活や社会の経済活動など、さまざまな分野に大きな影響を及ぼす、いわゆるサイバーテロ等の顔の見えない犯罪が横行することである。このような事態に対処するため、政府は２００５年を目標にｅ－Ｊａｐａｎ計画において高度通信情報ネットワークの安全性及び信頼性を確保するために、２００３年度までに情報セキュリティポリシーの評価・見直しの実施によるセキュリティ水準の確保を掲げ、関係省庁及び民間に対して不正アクセスやサイバーテロの予防・検知に関する技術等の実用化を計画している。このような中で、政府は「情報セキュリティに関するガイドライン」をまとめた。これを受けて文部科学省においても大学における不正侵入の実態を調査し、大学の情報セキュリティポリシーに関する研究会が「大学における情報セキュリティポリシーの考え方」をとりまとめた。

本協会においても、このような不正アクセス等の予防に対処するため、ネットワーク研究委員会不正侵入対策小委員会にて検討を行い、私立大学の特性を配慮した、ネットワークセキュリティポリシーのガイドラインをとりまとめ、大学あげて本問題に対処できるよう、大学の最高責任者を含めた組織的なセキュリティ対策の重要性を訴えるとともに、予防対策を具体化するために必要なあらゆる手段として、組織・制度、防御技術、利用者への情報倫理教育の徹底などについて体験を交えた解説書としてとりまとめることにした。

セキュリティポリシーの策定と運用は、大学のトップの十分な理解と指導のもとに全構成員の協力が得られなければ目的の達成は難しい。是非とも学長などのトップマネージメントの方がこの問題を意識され、体制、環境の整備について主導的に携わっていただきたいと思う。その対策を講じるための一助として本冊子が活用されることを願ってやまない。

平成１４年５月３１日

社団法人私立大学情報教育協会
ネットワーク研究委員会
担当理事　井　上　　靖

目　　次

Ⅳ．セキュリティポリシーを成功させるために

大学がセキュリティポリシーを策定する際の参考として、策定にあたっての留意点を失敗事例をもとに解説する。

Ⅴ．技術的な対応と教育

ネットワークへの不正侵入を防御するための技術的な対応策を紹介するとともに、技術では解決できない事項として、*ネットワークを利用する全ての構成員に必要な情報倫理教育*の概要を解説する。

※　ページ数の関係上、対策基準（遵守事項）の詳細、技術情報などは本協会会員専用のＷｅｂページから公開する。

http://www.shijokyo.or.jp/member/netsec/

用語の定義等について

用語の定義：

本冊子で使用する用語は「情報セキュリティに関するガイドライン（平成１２年７月、情報セキュリティ対策推進会議）」を参照しながら、一部に独自の用語を加えている。

・ネットワークセキュリティ（以下「セキュリティ」という）

ネットワーク及びネットワーク上にある情報資産の機密性、完全性及び可用性を維持すること。

・情報資産

情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）の総称。

・情報システム

同一組織内において、ハードウェア、ソフトウェア、ネットワーク、記録媒体で構成されるものであって、これら全体で業務処理を行うもの。

・ネットワークセキュリティポリシー（以下「セキュリティポリシー」という）

ネットワーク及びネットワーク上の情報資産について、何を、どのような脅威から、どのようにして守るのかについての基本的な考え方並びにセキュリティを確保するための体制、組織及び運用を含めた規定。基本方針、対策基準、実施手順からなる。

・基本方針

セキュリティ対策に対する根本的な考え方を表すもので、何を、どのような脅威から、なぜ保護しなければならないのかを明らかにし、大学のセキュリティに対する取組姿勢を示すもの。

・対策基準（遵守事項）

「基本方針」に定められたセキュリティを確保するために遵守すべき行為及び判断等の基準、つまり「基本方針」を実現するために何をやらなければいけないかを示すもの。

・実施手順（ガイドライン）

対策基準に定められた内容を、対象者ごとに、どのような手順に従って実行していくのかを示すもの。「情報セキュリティに関するガイドライン」では、実施手順等はポリシーに含めていないが、ここではセキュリティポリシーの一部であるという立場に立っている。

参考文献について：

参考文献は、文中等にて *1) *2) のように記号で表しており、対応する文献の一覧を巻末にまとめて掲載している。

Ⅰ　ネットワークセキュリティポリシーの考え方

１．必要性と対策

２１世紀社会において、高等教育は社会や世界の人々が共有すべき知的資源であり、大学は社会資産、世界資産の創造に貢献するという新たな役割に応える責務がある。ＩＴ（情報技術）の出現により、優れた教育コンテンツをリアルな形で教材として蓄積し、継承し、再利用することにより、新しい教育の創造が可能となってきている。グローバル時代においては、情報通信網の高度化・広域化を背景に、教育研究はあらゆる国、地域の高度な情報資産を享受することが可能となり、その上で、高いレベルの教育研究が進展することが必然的になる。大学の使命は、このような展開を考慮した上で、情報資産の利活用をはじめ、情報資産の創造がネットワーク上で安定して実現されるよう万全の対策を日常より講じておくことが求められる。

情報システムおよび情報資産の崩壊は、大学の機能停止に止まらず社会的信用の失墜にも繋がる。特に最近では、管理が不十分でたびたび外部のネットワークに被害を及ぼしている組織はブラックリストに登録され情報の配信を停止されるケースも見られる。また、大学は外部の攻撃による被害者となるだけではなく管理の甘さによる不正中継など故意でない加害者となる場合や興味、好奇心から外部を攻撃し加害者となる場合がある。このような事態を招かないためには全学的なコンセンサスのもとでセキュリティポリシーを策定、運用し社会的責任を果たすことが最重要課題である。

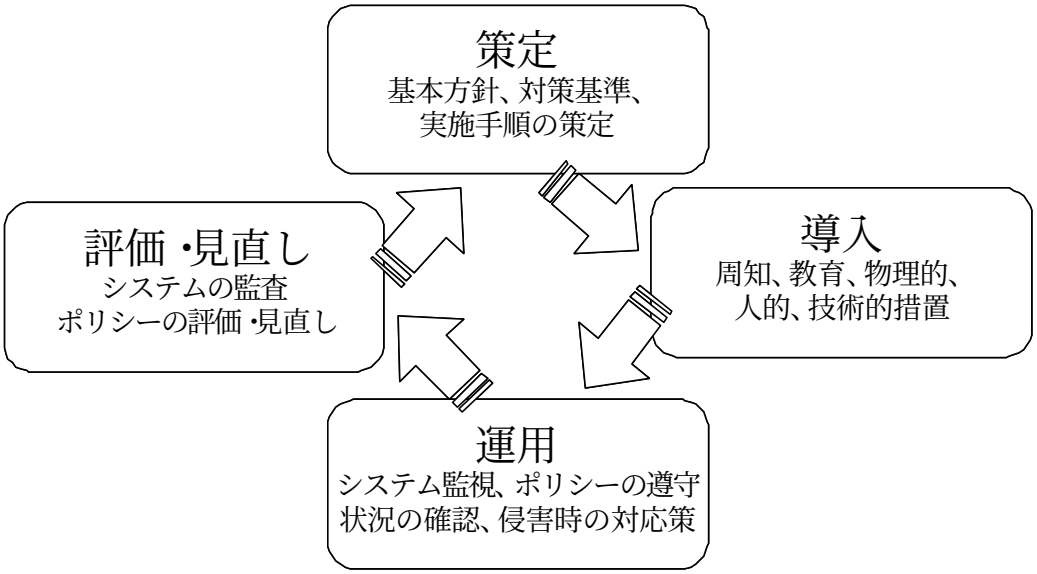
セキュリティポリシーは、大学の危機管理の一部と位置付けるべきであり、最高責任者（理事長、学長等）以下全員が以下の３つの基本方針に則り、全学的な課題として取り組まなければならない。

①　危機管理の一部と位置付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

セキュリティポリシーは、大学が所有するネットワーク及びネットワーク上の情報資産のセキュリティ対策について、大学が総合して体系的かつ具体的に取りまとめたものである。どのような情報資産をどのような脅威から、どのように守るかについての基本的な考え方並びにセキュリティを確保するための体制、組織及び運用を含めた規定で、セキュリティに関する基本方針や、対策基準及び実施手順からなる。

さらに、重要なことはポリシーを策定したのだけではセキュリティを確保することはで

きない。図１に示す策定～導入～運用～評価（Plan - Do - See）の実施サイクルが重要である。ここでは、基本方針、対策基準、実施手順をポリシーの基本的要件と定義し、以下に概説する。



【図１】 セキュリティポリシーの実施サイクル

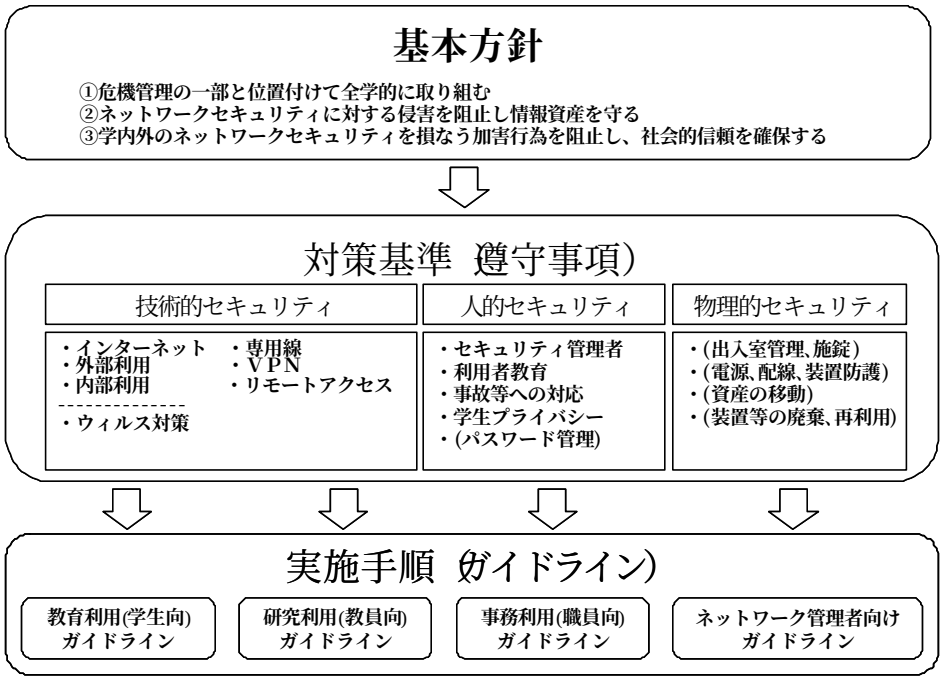
コラム「期末試験の内容がＬＡＮ経由で漏洩」

Ａ大学では、教員が期末試験の問題の作成を行っているパソコンで不用意に他のパソコンとの間でファイルを共有できる機能を設定してしまった。学生がこの共有フォルダ上の試験問題に難なくアクセスし、試験前に問題が学生間に流通するという事態となった。幸い、試験直前に事件が発覚したため、試験問題を再作成することで試験自体には影響は無かった。

しかし、同様の行為が考えられるため安心して学内ＬＡＮを利用できなくなっている。複数のパソコンの間でファイル移動等に便利な機能であるが、セキュリィを設定しなければ学内掲示板に問題を貼り付けるのと同じ行為である。この問題に対処するためには、学内のセキュリティポリシーとして、ネットワークで接続された相互のコンピュータで情報を検索できないようにしたり、検索できてもデータにアクセスできないような制限を強制的に行うなど、利用者の利便性よりも安全性を優先させる方針を取り決めるべきであろう。当該教員は入試問題に関しても同じコンピュータで作成していた。幸いにして、入試問題はフロッピーに保存していたために大事に至らなかったが、もし同じハードディスク上にあったなら、大きな社会問題を引き起こしていたかも知れない。

２．セキュリティポリシーの要件

セキュリティポリシーは、図２に示すように、次の３つの要素から構成されることが多い。



【図２】セキュリティポリシーの構成モデル

（１）基本方針

憲法に相当し、大学としてのネットワークセキュリティに関する考え方や方針を示したもので、基本ポリシーと呼ばれることもある。

上位の組織が、基本方針を持っている場合にはそれらを考慮しつつ基本方針を設定することが必要な場合もある。例えば、政府によって基本方針が決められている場合には各省庁は、それを尊重しながら、自分の省庁の基本方針を定めていく必要がある。また、同一組織であっても、上位のポリシーがある場合にはそれを尊重しつつセキュリティポリシーを策定していく必要がある。例えば、大学では危機管理ポリシーが制定されており、セキュリティポリシーがその下に位置付けられている場合には、その危機管理ポリシーを尊重しなければならない。

なお、基本方針は学内外に積極的に公開し、学内においてはポリシーの存在を知らせ、ポリシーのスムーズな運用を図り、学外に対しては信頼感を与えるべきである。

（２）対策基準（遵守事項）

基本方針を具体化し、システムの利用形態（例えば、Ｗｅｂページによる情報の外部公開、電子メールの利用）や脅威（例えばウイルスの侵入）など対策を考えやすいように分類した上で、それぞれについて遵守すべき規定を記述したもの。対策基準はスタンダードや対策標準と呼ばれることもある。

対策基準については、基本的に公開すべきでない。攻撃に有利な情報が外部にもれ出る可能性があるからである。内部に対しても全ての人に公開する必要はなく、必要最低限にすべきであろう。

（3）実施手順（ガイドライン）

対策基準を現場レベルで実施するために、配布すべき対象者（例えば学生、教員、事務職員、ネットワーク管理者など）ごとに内容を抜き出し、カスタマイズしたものである。実施手順はプロシージャやガイドラインと呼ばれることもある。この内容は、対策基準に書かれているレベルと基本的に同じである。

実施手順に関しては、積極的に公開すべきではないが、大学の場合は、学生などもおり、それを完全に秘密に保つことは困難であるためオープンになったとしても安全な実施手順書にしておく必要がある。

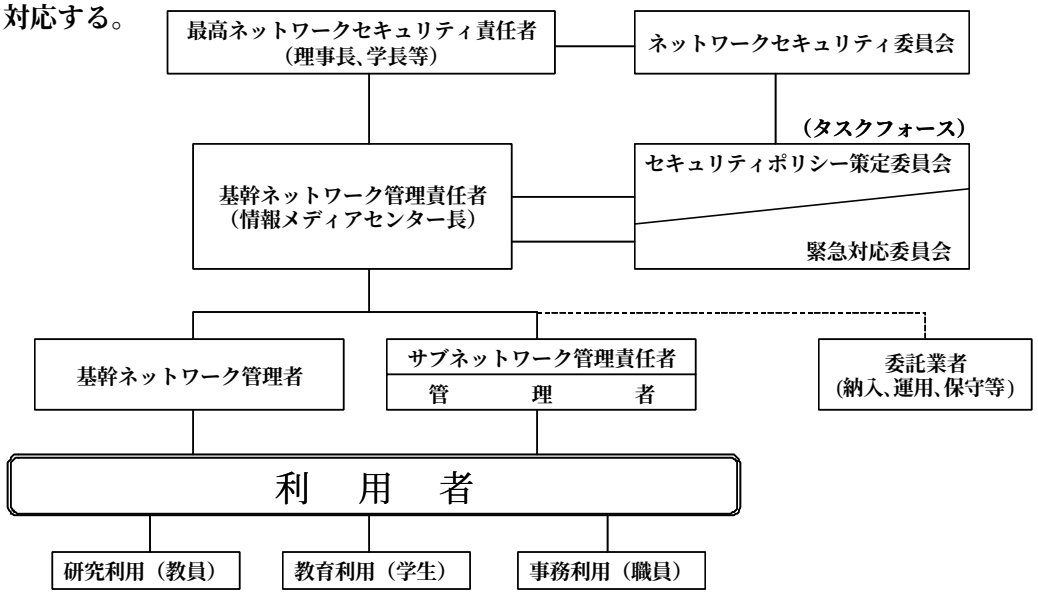
なお、基本方針と対策基準だけをセキュリティポリシーという場合もあるが、具体的な対策を各グループに対し明示的に示すために、ここでは、実施手順も含めてセキュリティポリシーということにする。

II　セキュリティポリシーの策定と運用

1．セキュリティポリシー策定の手順

（1）策定体制の確立

ポリシーを策定し、円滑な運用を行うためには、図3に示すような全学的な組織を構成して対応する。



【図3】セキュリティポリシー策定の組織・体制モデル

（２）基本方針の策定

①何を守りたいのか、②どのような脅威が存在するのか、③どのような行為から守りたいのか、などを明確化する。これは、大学の最高責任者がトップダウンに決定すべき項目である。基本方針をどこまで書くかについてはいろいろな考え方があり、（ａ）１ページぐらいの本当の宣言だけを書くものから、（ｂ）基本となる考えや関連する事項を、全てを十数ページに渡り書くものまである。最近は、（ｂ）の方が採用されることが多く、セキュリティに関する大学としての考え方、セキュリティポリシーの位置付け・役割、セキュリティポリシーを運用するための体制、遵守の義務と違反者への罰則、構成についての説明や用語の定義、などを記述することが多い。

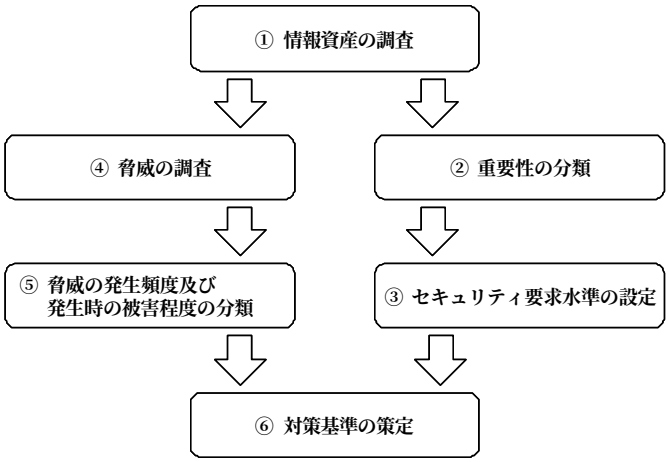
（ｂ）の一例の目次を表１に記述する。なお、要旨の例や全文は別項に記載する。この例においては、基本方針として被害者にならないだけでなく、意識的無意識的に加害者にならなくすることもあげている。

１．要旨・・・・・・・この要旨の部分が基本指針になる
２．適用範囲・・・・・基本的に部外接続に関するものを対象とする。学生に関する人的セキュリティも部外接続を中心にして扱う
３．適用者・・・・・・大学構成員：学生、教員、職員、情報メディアセンター職員
４．構成と位置付け・・本方針の構成と位置付け
５．公開対象者・・・・基本方針は学内外、方針は大学構成員、対策標準は委員会メンバーと情報メディアセンター職員、ガイドラインは該当者（例：学生、教員）
６．公開・・・・・・・学外への公開の手順
７．基本用語の定義・・「情報セキュリティに関するガイドライン(情報セキュリティ対策推進会議編)」等より
８．体制・・・・・・・ネットワークセキュリティ委員会、ネットワークセキュリティ責任者、システム管理者など
９．ネットワークセキュリティ委員会の体制図および構成メンバー
10．ネットワークセキュリティ委員会の役割と責務
11．セキュリティマネージメント
（委員会によるリスク分析、ポリシー策定、対策の実施、教育・啓蒙、監査・評価、文書の改廃など）
12．違反時の罰則
13．侵害時の対応
14．執行期日

【表１】基本方針の目次例

（３）リスク分析の実施

リスク分析とは、保護すべき情報資産を明らかにし、それに対するリスクを評価することで、図４のような手順で進められることが多い。 *7)



【図４】リスク分析の手順

分析には、大学が保有する情報資産を、例えば、卒業記録や学籍関連データ等の『改ざんされたら困る情報』、研究関連データや学籍関連データ等の『破壊されたら困る情報』、試験問題や成績情報等の『見られたら困る情報』など、重要性の種類により分類し、それぞれの情報について要求されるセキュリティ水準を決定する作業と、情報資産を取り巻く脅威を発生頻度と発生時の影響の大きさにより分類する作業があり、分析(1)作業の結果から、リスクの大きさがセキュリティ要求水準を下回るよう対策基準を策定する。ここでは、定性的解析法のひとつであるマトリックス表を用いた評価法により、大学への適用の一例を図５に示す。

影響度＼発生可能性		外部よりの攻撃		内部よりの攻撃	
		一般的知識利用	特殊な知識・ツール利用	一般的知識利用	特殊な知識・ツール利用
重要なデータが改ざんされる	卒業記録、学籍関連データなど	１－①端末への接近と不正使用 グループ１	２－①外部からの不正侵入とデータの改ざん	３－①買収などによるデータの改ざん グループ３	４－①職場の同僚に成りすましてのデータの改ざん
重要なデータが破壊される	**学籍関連データ 研究関連データなど**	１－②端末への接近と不正使用 １－③計算機の破壊 １－④ウイルスによるデータの破壊	２－②外部からの不正侵入とデータの破壊	３－②恨みなどによるデータの破壊	４－②職場の同僚に成りすましてのデータの破壊
重要なデータが見られる	試験情報 成績データなど	１－⑤入出力データの盗み見 グループ２	２－③通信路上でのデータの不正入手 ２－④ウイルスによるデータの送りだし ２－⑤ディスプレイの電磁波もれによる盗み見		４－③職場の同僚に成りすましてのデータの盗み見
その他	職場の混乱 信用の失墜		２－⑥関連ＷＥＢサイトの書き換え		

【図５】マトリックス表を用いたリスク評価の一例

(1) リスク分析の技法には「定性的分析法」、「定量的分析法」などがあるので巻末に記載の参考文献 1)、8)、9)を参照されたい。

ここでは、情報資産への脅威として、外部からの攻撃と内部からの攻撃に大別している。両者の発生する比率は半々程度と予想されており、内部からの攻撃の検討を忘れないことも大切である。リスクが最も大きいと考えられるのがグループ１であり、グループ２、グループ３がそれに続く。

対策には、（イ）技術的対策、（ロ）物理的対策、（ハ）人的対策などがある。

技術的対策としては、破壊活動にはアクセス制御技術やセキュリティ管理技術が、改ざんや盗み見の防止には暗号化やアクセス制御技術などが有効である。また、物理的セキュリティは、コンピュータのある部屋への入退出管理などを考えておけば良い。人的セキュリティとしては、各人の任務を明確にすると共に、取るべき行動について教育・訓練をすることが必要である。詳しくはセキュリティに関する文献を参照願いたい(2)。また、これらの対策が十分であるかどうかのチェックには、ＩＳＯ１７７９９などにリストアップされた項目を参照すれば良いだろう。ＩＳＯ１７７９９の解説書としては文献１１）などがある。

（４）対策基準（遵守事項）の策定

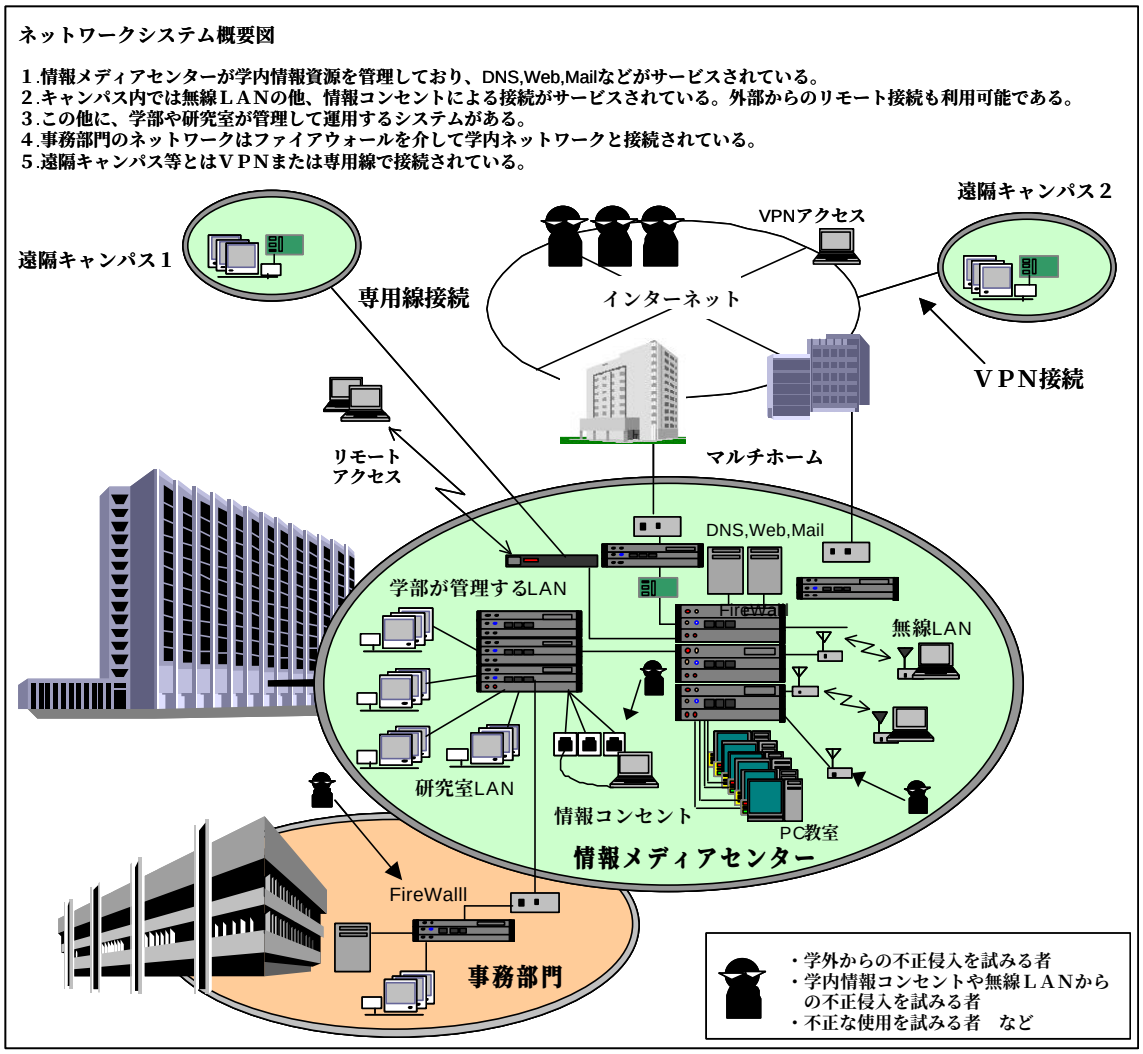
基本方針を具体化し、例えば、Ｗｅｂページによる情報の外部公開、電子メールの利用などシステムの利用形態、ウイルス混入などの脅威に分類した上で、それぞれの項目について、リスク分析結果などを基に遵守すべき事項を規定する。この場合、加害防止・被害防止の両面について対策の検討も実施しなければならない。

ネットワークシステムの機能別に作成した対策基準の目次の一例を表２に示すとともに、各項目別対策基準の一例を別項にて掲載する。雛形となれば幸いである。*6) *7) また、対象となるネットワークのイメージを図６に示す。

１．インターネット利用に関する対策基準
２．外部公開に関する対策基準
３．内部利用に関する対策基準
４．VPN および専用線接続に関する対策基準
５．リモートアクセスに関する対策基準
６．ウイルス対策に関する対策基準
７．学生のプライバシーに関する対策基準
８．人的セキュリティに関する対策基準
９．物理的セキュリティに関する対策基準

【表２】対策基準の構成例

(2) 例えば巻末に記載の参考文献 １０）など



【図６】ネットワークシステムのイメージ

（５）実施手順（ガイドライン）の策定

実施手順は対策基準を現場レベルで実施するために、配布すべき対象者（例えば学生、教員、事務職員、システム管理者など）ごとに内容を抜き出し、カスタマイズしたものである。実施手順はプロシージャやガイドラインと呼ばれることもある。

この内容は、対策基準に書かれているレベルと基本的に同じである。しかし、場合によっては、対策基準に比べより具体化した部分があったり、逆に、いくつかの事項をまとめて簡潔に表現したりすることがあってもよい。たとえば、対策基準では「管理者に届けなければならない」と書いていても実施手順では、具体的にどのようなフォーマットでどのようなルートで届け出るかを書くことがあるだろう。また、対策基準では、パスワードの管理は利用形態においていろいろなところで書かれているが、実施手順ではそれらをまと

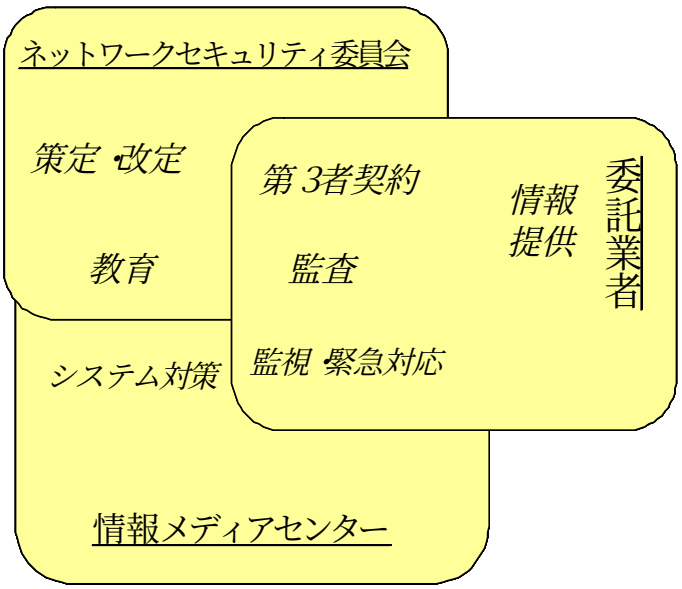
めて一箇所で書いてもよい。いずれにしても対象者が行動しやすくすることが大切である。

２．運用のための組織・体制、利用者教育

セキュリティポリシーはきちんと運用できることが必要であり、運用できないポリシーを作っても意味がない。また、運用するための組織体制を作ることが必要である。また、情報システムを利用する全ての者にポリシーを遵守させるための利用者教育は欠かせない要素であり、運用組織は必要に応じてこれらの教育体制の一翼を担う必要がある。さらに、単にポリシー遵守のための教育を施すだけでなく、必要に応じて情報倫理に関する教育を施し、全体のモラルの向上にも努めるべきである。本冊子では、そのために情報倫理に関する問題について「Ⅴ．技術的な対応と教育」において触れている。

セキュリティポリシーの運用体制として、図７のような３者の連携が必要である。

しかしながら、全学組織のネットワークセキュリティ委員会が実運用の面まで手を出すことは実質的に不可能である。そこで、セキュリティ委員会の下に、実働部隊としてのタスクフォースを設置する。タスクフォースの構成は種々考えられるが、ポリシー策定・改定、監査・緊急対応、教育などが考えられる。タスクフォースはネットワークセキュリティ委員会の下に置かれるが、実際には先に示した３者が協力して実働できる体制を整えることが必要である。



【図７】セキュリティポリシー運用体制の一例

図に示すとおり、３者はそれぞれが協力し合うとともに、役割を分担し円滑なセキュリティポリシーの運用にあたるべきである。ここでは、それぞれの役割分担と協力関係を次のように考え、それぞれの役割に対して表３のようなタスクフォースを設けることを想定している。

①ネットワークセキュリティ委員会：ポリシーの策定・改定
②情報メディアセンター：情報システムに対するセキュリティ対策
③協力関係：
　ア　委員会＋センター：セキュリティ教育
　イ　委員会＋委託業者：第３者契約（委託業者を含めた取引業者との間のセキュリティポリシー遵守に関する取り決めを協議し、実行することを指す）
　ウ　委託業者＋センター：インシデントの監視・緊急対応
　エ　３者：セキュリティポリシーの監査

【表３】セキュリティポリシー運用のタスクフォースの一例

ただし、以上は、あくまでも一つの例であり、これらのタスクフォースを全て立ち上げなければならないわけではなく、大学の実情に応じて種々の組合せを選択すればよい。例えば、業者に運用等を委託していない場合には情報メディアセンターが担当することになろう。なお、これらのタスクフォースはあくまでも委員会の下部組織と位置付けており、全学的に承認された問題解決の権限が与えられていなければならない。

コラム「学生の教育もれ」
あるとき、プログラムを書くのが得意で SMTP を理解しているある社会人大学院生がこともあろうに、大学内に持ちこんだ自分のコンピュータから一人あたり数通、合計 2 万通を超える電子メールを、ある大企業の顧客の携帯電話あてに発したことが一利用者からのクレームから発覚した。
幸いその企業にとってはこの程度のことは日常茶飯事でクレームは来なかったが、この学生は、別の業者から口約束で受けた仕事として、実在するメールアドレスを抽出する目的で実施したそうで、明らかに故意である。結果としてしかるべき処分を受けた。
大学では、全学生にコンピュータとネットワーク利用アカウントを発行していて、発行時の講習の中で、利用規則の教育を実施しているつもりだった。ところが、実は他大学から来た大学院生、編入、転入、短期留学の学生には十分な講習が実施されていないことが判明した。つまり、全構成員にセキュリティ教育を施すというポリシがなかったから起きた問題である。

Ⅲ　セキュリティポリシーモデル

本冊子が取り扱うセキュリティポリシーは、基本方針、対策基準、実施手順（ガイドライン）の３つの部分からなる。ここでは、これら３つの部分について具体的な例を示す。しかしながら、これらはあくまで例であり、各大学の実情に合わせたセキュリティポリシーを作成する必要がある。

基本方針は必須であり、これがないと以下の対策基準、実施手順を作成する場合の根拠が失われる。

対策基準は、ネットワークを利用する教職員あるいは管理者が守らなければならないこ

と（遵守事項）を、インターネット利用、情報の外部公開など分野別に列挙したものである。したがって、各大学のシステム構成やサービス内容により異なるものとなる。また、対策基準の中に多くの重複部分を含むように見えるが、それぞれのシステムやサービスの対策基準のみを読むことで完結するように配慮したためである。遵守事項を列挙してあることが大事であり、記述の重複があってもかまわないというのが本冊子の立場である。

実施手順（ガイドライン）は、教員、職員、学生、管理者など、対象者単位に遵守事項を整理したものであり、膨大な対策基準を全て読まなくても、自分が守るべき事項が何であるかが解るように配慮した。したがって、一般的な利用者や管理者はガイドラインを読み、そこに記述されていることを守ることで、セキュリティポリシーを遵守することができる。

しかしながら、特殊な場合、例えば外部の機関との共同研究などで新しい専用線を設置し、その上でＶＰＮを使って相手の機関と直接通信を行う必要が生じた場合などは、それぞれの対策基準の内容にしたがってセキュリティ対策をとらなければならない。

１．大学の基本方針モデル

基本方針はセキュリティポリシーの基本理念を示したものであり、表１に示した基本ポリシー構成の『要旨』がこれにあたる。表４に要旨の一例を示した。

インターネットの普及は目覚しく、電子商取引や電子政府など、従来はできなかった種々の活動が容易に行えるようになってきた。本大学では、インターネットを積極的に利用する環境の提供と、教育を行ってきた。

一方、不正アクセスやコンピュータウイルスの被害が増加するとともに、知識の不足により、学外の利用者に対し加害者になる状況も生じはじめ、本学においてもセキュリティ対策が不可欠となってきている。このような背景の下、セキュリティ対策を定める基本となるセキュリティポリシーの作成が必要となった。

セキュリティの脅威から守るべきもののうち、本学において、特に優先するのは以下の通りである。

（１）学内に設置された重要な情報を、不正な攻撃による改ざん、破壊、漏洩などから防御する。

（２）意識的無意識的に学外の利用者に対し加害者になることを防止する。

本学は、これらのことを可能とするため、セキュリティポリシーを策定する。本学の学生、教員、職員などの構成員は、セキュリティの重要性を認識し、本セキュリティポリシーを遵守しなければならない。

【表４】セキュリティ基本ポリシー要旨の一例

基本方針の策定は、セキュリティ委員会で十分に議論し、大学の管理者側が納得したものでなくてはならない。特にセキュリティ委員会の長が学長のような意思決定をできる役

職者以外の場合は、より上位の役職者が納得したものでなければならない。

また、基本方針はセキュリティポリシーの中で唯一一般公開される可能性があるため、平易な誤解を生じない文章となっていなければならない。

２．必要な対策基準（遵守事項）モデル

対策基準は各大学の情報ネットワークシステムおよびサービスについて網羅的に作成されなければならない。例えば、研究室ごとのリモートアクセスに対する基準がないと、そこがバックドア（裏口）としてのセキュリティホールとなり大学全体のシステムを脅かす可能性がある。

対策基準作成の基本的な考え方は網羅性であり、全てのシステムおよびサービスについての基準が列挙されていることが必要である。本冊子では、以下の９項目について対策基準を設けることにしたが、各大学の実情に相応しい対策基準を作成することが大切である。

	対策基準	内　容
①	インターネット利用に関する対策基準	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
②	外部公開に関する対策基準	学外に情報を公開するためのサーバ設置に関する基準
③	内部利用に関する対策基準	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
④	ＶＰＮおよび専用線接続に関する対策基準	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、
⑤	リモートアクセスに関する対策基準	学外からのリモートアクセスについての基準
⑥	ウイルス対策に関する対策基準	コンピュータウイルスに関する対策基準
⑦	学生のプライバシーに関する対策基準	学生のプライバシー保護に関する対策基準
⑧	人的セキュリティ対策に関する対策基準	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
⑨	物理的セキュリティ対策に関する対策基準	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

【表５】対策基準（遵守事項）の例

※　「ウイルス対策に関する対策基準」は、今日、コンピュータウイルスが蔓延しているため、ウイルス対策を強化・徹底する目的で独立させた。

※　「学生のプライバシーに関する対策基準」は、個人情報の流出が多くの社会的な問題を生むことを配慮して独立させたもので「人的セキュリティ対策に関する対策基準」に含めることもできる。

①から⑨の全ては、本協会のＷｅｂページにて公開することにしている。各大学にて必要な対策基準を作成する際の参考になれば幸いである。

コラム「管理者不在のサーバ」

研究室に設置されているＵＮＩＸマシンが外部から不正侵入され、学内ＬＡＮのパケットが盗聴された。このＵＮＩＸマシンは、設置当初は管理する院生がいて、設置申請等もきちんと行われていたが、数年前から明確な管理者がいない状態で、主に学部の４年生が卒論の片手間に利用者管理を行っていた。このため、ＯＳも、アプリケーションもバージョンも古いままで運用されていた。アプリケーションのよく知られたセキュリティホールを攻撃され、いとも簡単に侵入を許していた。侵入に気がついたあとも、責任の所在が明確でなかったため、数日間放置され被害を拡大してしまった。専門スタッフがいるセンター部門と異なり、研究室に設置されるシステムの管理者はさまざまである。助手が管理する場合から、この例のように学部生が片手間に管理しているものまである。管理責任者・運用管理者を明確にし、管理手順を明確に規定しておかなければ大学全体が危険にさらされることになる。また、事件が発生した場合の対応手順を明確にしておくことも重要である。

３．実施手順（ガイドライン）モデル

①　学生（教育利用）向けガイドライン（案）

＜位置付け＞

本ガイドラインは、学生が大学においてコンピュータやネットワークを利用するにあたって遵守すべき事項をまとめたものである。

＜一般利用＞

１．　インターネットの利用において、やり取りする情報の内容については、本学は基本的には関知せず、利用者が良識を持って判断しなければならない。

２．　コンピュータやネットワークの利用のために発行されたＩＤとパスワードは本人のみが利用できる。そのため、他の利用者ＩＤを用いて身分を隠してはならない。また、他人に自分のＩＤを貸与してはならない。

３．　掲示板やニューズグループなど公的な場所で学内から意見を表明するときは、関与者の人権やプライバシーを尊重すると共に、知的所有権（著作権、商標権、特許権など）に配慮しなければならない。

４．　コンピュータやネットワークを本来の目的以外に使ってはならず、特に商業目的に使ってはならない。

＜電子メール利用時＞

１．　第３者のプライバシーや知的所有権には十分尊重しなければならない。

２．　機密情報を学外に流してはならない。

３．　不必要な相手にまで送付したり、不必要なファイルを添付するなどにより、計算機やネットワークに不要な負担をかけてはならない。 特に、チェーンメールに協力

することが無いよう注意しなければならない。

4．　通信相手を罵倒したり、誹謗中傷してはならない。

5．　ネズミ講やマルチ商法などに荷担してはならない。

6．　学内の電子メールを学外のメールサーバへ転送することは基本的に妨げないが、転送先の設定などに十分注意しなければならない。

7．　添付ファイルにウイルスが内在する可能性を考慮しなければならない。

8．　安全を確保するためには暗号メールを必要に応じて使用することが望ましい。

＜Ｗｅｂアクセス＞

1．　Ｗｅｂ運用者からプライバシーを守りたい場合には Cookiee を OFF に指定おかなければならない。

2．　署名のない ActiveX や Java,JavaScript,などのコードを実行する場合はウイルス対策などに十分注意しなければならない。

3．　不適切なサイトにアクセスしてはならない。また、信頼できないサイトへアクセスする場合は、取引時のトラブルなどに十分注意しなければならない。

＜ファイル転送＞

1．　出所が不明なファイルや内容に確証がもてないファイルをダウンロードしてはならない。

2．　大きなサイズのファイルをダウンロードするときは、他の利用者への影響を考慮しなければならない。

＜公開情報に関する遵守事項＞

1．　Ｗｅｂサーバの管理者は設置目的以外の利用をしてはならない。例えば学術目的に設置したサーバを、業務目的に利用してはならない。

2．　公開サーバで公序良俗に反する情報を発信してはならない。

3．　Ｗｅｂサーバなどにより情報を公開する場合は、関与者の人権やプライバシーなどに十分配慮しなければならない。

4．　Ｗｅｂに掲載する事項に関しては他人の知的所有権（著作権、商標権、特許権など）に十分配慮しなければならない。

5．　個人ごとのＷｅｂページの開設が認められている場合は、その内容に関しては個人が責任を負うものとするが、上記の各項目に記した条項は個人のページにもあてはまる。

＜ウイルス対策＞

1．　万一のウイルス被害に備えるためデータのバックアップを行わなければならない。

2．　ウイルスの兆候を見逃さず、ウイルス感染の可能性が考えられる場合ウイルス検査を行わなければならない。

３．　メールの添付ファイルはウイルス検査後開く。
４．　ウイルス感染の可能性のあるファイルを扱う時は、マクロ機能の自動実行は行わない。
５．　外部から持ち込まれたＦＤ及ダウンロードしたファイルはウイルス検査後使用する。
６．　コンピュータの共同利用時の管理を徹底する。
７．　メールの本文で済むものを添付ファイルにしない。
８．　ウイルス発見時・感染時には所属組織のセキュリティ担当者に報告しなければならない。

＜報告義務＞

１．　コンピュータを利用中に不正アクセスの痕跡（知らないファイルがあるとか起動したつもりがないプロセスが動いている）などを発見した場合は、速やかに報告しなければならない。
２．　ネットワークを利用中に障害を検知した場合は、速やかに報告しなければならない。

＜罰則＞

このガイドラインに違反する場合は、情報メディアセンターが管理するコンピュータやネットワークの利用を禁止する場合がある。さらに悪質な場合には学則にのっとり処罰する場合がある。

②　教員（研究利用）向けガイドライン（案）

＜位置付け＞

本ガイドラインは、教員が研究室で各種のコンピュータ及びネットワーク機器を設置してネットワークに接続し、運用するにあたって遵守すべき事項をまとめたものである。一般的な利用は、「①教育利用（学生向け）ガイドライン」を参照のこと。

＜接続時＞

研究室等でサブネットワーク（以下、「サブネット」とする）を設置して大学のネットワークに接続する場合には、情報メディアセンターに対し、以下を届け出なければならない。また、各種のサーバを設置する場合も同様であるが、この場合「ネットワーク管理者」などの「ネットワーク」の部分を「サーバ」と読み替えるものとする。

１．　ネットワーク管理責任者（以下責任者）とネットワーク管理者（以下管理者）等の氏名と運用体制。なお、責任者と管理者は同一であってもよい。ここで、責任者は、研究などの目的のために自己が管理する情報システムのセキュリティ確保の責任者であり、管理者に対し管理責任を持つ。管理者は、責任者により与えられた作業の管理責任を有する。
２．　システムの構成に関連し、情報メディアセンターが指定する項目（サブネットに関してはサブネットアドレス、接続機器構成及びそのアドレスなど、サーバに関し

てはシステム構成図、ＩＰアドレス、ＭＡＣアドレスなど)。

3．　セキュリティ対策のために実施ならびに実施予定している事項。

＜サブネット管理＞

1．　責任者はサブネットに対する機器の新しいコンピュータやネットワーク機器の接続を承認し、接続された機器に関する情報を速やかに情報メディアセンターに届けなければならない。

2．　責任者はサブネット内に設置された機器の管理責任を負うとともに、管理者と協力して、サブネットの維持・管理に勤めなければならない。

3．　サブネット内で異常を検知した場合は、速やかに上位の管理者に届け出なければならない。

＜利用者管理＞

1．責任者は、管理対象範囲の利用者に、アカウントおよびアクセス権の登録、変更を迅速に行う。

2．責任者は、利用者情報は常に最新の状態を維持し、卒業生などが不必要に利用者として登録され続けてはならない。

＜ログ管理＞

1．　責任者は、障害や不正が生じた場合に、その原因を究明し、違反者を特定するためにログの取得、管理を行う。

2．　責任者は、取得されたログは定期的にバックアップ媒体に記録しなければならない。

3．　責任者は、ログおよびバックアップ媒体は、改ざんや破壊、権限のない参照から保護しなければならない。

4．　ログの管理によって得られた個人情報については守秘義務を負うものとする。

＜セキュリティ監視＞

1．　責任者は不正侵入の有無に関する監視は積極的に行わなければならない。

2．　利用者や責任者が障害を検知したときは、速やかに情報メディアセンターに報告しなければならない。

＜外部公開時のアクセス管理＞

1．　サーバの内容を外部に公開する場合はOS、アプリケーションサービスのアクセス制御に関し、設計書を作成し、厳密にアクセス権を設定することが望ましい。

2．　サーバの内容を外部に公開する場合はデータのアクセス制御に関し、設計書を作成し、厳密にアクセス権を設定することが望ましい。

3．　責任者は、外部公開サーバの趣旨、用途に応じた必要最小限のアプリケーションサービス以外インストールしてはならない。

＜安全な設定＞

１．　最新のＯＳ、最新のアプリケーションを用い、最新のセキュリティパッチの適用しなければならない。

２．　不要なプログラムやサービスはサーバから削除しておかなければならない。

＜公開情報に関する遵守事項＞

１．　Ｗｅｂサーバの管理者は設置目的以外の利用をしてはならない。特に、学術目的に設置したサーバを、業務目的に利用してはならない。

２．　外部公開サーバで公序良俗に反する情報を発信してはならない。

３．　Ｗｅｂサーバなどにより情報を公開する場合は、関与者の人権やプライバシーなどに十分配慮しなければならない。

＜リモートアクセス>

１．　学外から学内のサーバに直接アクセスするリモートアクセスは、申請に基づき情報メディアセンターが認可した場合に限る。

２．　リモートアクセスを認める場合でも、利用できるサービスは、電子メール、ＨＴＴＰを利用したサービスに限定することが望ましい。使用するＰＣやアクセスする場所を限定することが望ましい。

３．　リモートアクセスサーバは専用のサーバあるいはネットワーク機器でなければならない。

４．　発信者識別、ワンタイムパスワードなどの利用者認証機能、コールバック機能、VPN（暗号化）機能、接続記録蓄積機能を持つことが望ましい。

＜罰則＞

このガイドラインに違反する場合は、情報メディアセンターが管理するコンピュータやネットワークの利用を禁止する場合がある。

③　職員（事務利用）向けガイドライン（案）

＜位置付け＞

本ガイドラインは、大学の事務職員が大学においてコンピュータやネットワークを利用するにあたって遵守すべき事項、特に業務で利用する際の注意事項をまとめたものである。一般的事項については「①教育利用（学生向け）ガイドライン」を参照のこと。

＜一般利用＞

１．　ＩＤ､パスワードは同一業務を担当する者であっても原則として他人と共用せず、操作とその結果については誰が行ったものか責任が明らかになるようにする。

２．　大学で業務のために設置されたコンピュータが不足するなどの理由で私物のコンピュータを持ち込み、磁気媒体で情報を交換する、またはネットワークに接続する

場合は、管理者に許可を申請し、大学設置機器と同じセキュリティ基準を満たすことの確認を受けなければならない。また、機密情報を自宅に持ち帰ってはならない。

3．　席を離れるときは、他者に勝手にコンピュータを利用されないようにしなければならない。

4．　業務データベースの操作など、機密かつ重要な情報をリモート入力または更新するときは、定められた暗号通信手順に従う。また誤操作を避けるため、体調が悪いときの利用は避ける。

5．　学外から学内のコンピュータやネットワークを利用するときは、盗聴を防ぐため機密事項の送受信は避ける。どうしても必要であれば暗号を用いる。

6．　人事異動、休退職のさいは、すみやかにシステム管理者に報告する。また、異動後、旧部署の情報やシステムの認証システムの設定変更が遅れていても、不正にアクセスしてはならない。

＜電子メール利用時＞

1．　業務で取り扱う情報の機密性に注意し、電子メールで送って良い情報とそうでないものを区別する。また、宛先のアドレスを十分確認する。

2．大学で標準的に使うワードプロセッサなどのデータ以外は添付ファイルとして送らない。

3．業務上の機密情報を受け取る可能性があるメールアドレスへのメッセージは自宅や携帯電話への転送してはならない。

4．　電子メールのメッセージを送った後は消去することはできず、証拠として残ることを意識し、内容を十分検討してから送らなければならない。

＜データ転送、Ｗｅｂアクセス＞

1．　業務に無関係な情報を入手して通信回線を混雑させてはならない。

2．　業務上用いるコンピュータの損傷、機密情報の流出を避けるため、信用性が低いと思われるＷｅｂページを閲覧したり、そのようなページからファイルを入手しないこと。

＜情報の取り扱いに関する遵守事項＞

1．　業務上作成する一般公開 Web ページに間違って学内限定の情報を提供しないように注意する。

2．　学内で公開された情報であっても、みだりに学外に持ち出さない。

3．　職務規程に従い業務上知り得た情報を他に漏らさない。

4．　重要な情報は必ず CD-R/RW やテープにバックアップし、媒体は鍵がかかる場所に保管する。

5．　担当者が急病や事故にあったさいに、この担当者が管理する重要な情報を他の担当者が利用できるようにする方法をあらかじめ打ち合せておく。

＜ウイルス対策＞

１．　業務用コンピュータがウイルスに感染したおそれがあるときは、すぐにネットワークケーブルを抜いて停止して、セキュリティ担当者に報告する。

＜機器納入時の注意＞

１．　業者が機器を納入するさいは、機密情報を取り扱う部屋への入室は認めず、入口で受け取ること。どうしても入室が必要な場合は、機密情報を格納し、本学職員が立ち会わなければならない。

２．　納入された機器の使用を開始する前に、本学で定める「納入機器に対するセキュリティ仕様」を満足することを管理部署（部門）のセキュリティ担当者に確認してもらわなければならない。もし仕様を満たしていない場合は、改善を要求する。

３．　ネットワーク機器は使用を開始する前にＩＰアドレスなどのパラメータを確認し、他に障害を与えないようにする。

４．　新たに納入した機器の管理者を定め、セキュリティ管理者に届ける。

＜罰則＞

このガイドラインに違反する場合は、部局のセキュリティ管理者が一時的にコンピュータやネットワークの利用を禁止することがある。悪質な違反の場合は職務規程に則り処罰することがある。

④　ネットワーク管理者向けガイドライン（案）

＜位置付け＞

本ガイドラインは基幹ネットワークと主要な業務用サーバの運用管理業務を担当する者がネットワークとサーバの安定した運用を維持するために遵守すべき事項をまとめたものである。

＜管理者の役割と権限＞

１．　定められた管理方針に従い、セキュリティネットワークの回線、機器、サーバなどが安定に稼働するように各種資源を運用する。そのための監視、設定修正、構成変更、利用者登録などの操作を日常業務としておこなう。

２．　障害やセキュリティ事件発生時の機器の停止、利用者に対する利用停止などの仮処分を含む緊急対応を実施し、その事実をすみやかにセキュリティ管理者に報告し、以後の対処の指示をあおぐ。

３．　機器の管理、特権ユーザの認証のためのパスワードを知るので、全てのファイルやシステムの資源にアクセス可能であるが、必要のない情報にアクセスしてはならない。

４．　主たる管理者が対応できないときに緊急対応する副管理者を定めておかなければ

ならない。

5．　与えられた権限を逸脱することがないように心掛け、セキュリティ管理者が担当部局の管理者の心身の健康状態を含めチェックすることも必要である。

＜特権ユーザとしての操作＞

1．　複数管理者による特権ユーザとしての操作の記録を残すため、また、誤操作を避けるために、特権ユーザとしての作業は最小限にとどめる。

2．　ＵＮＩＸシステムなどのようにＳＵ（Switch User）などの切り替えコマンドの実行で一般利用者から特権ユーザとして移行できる場合は、必ず一般利用者でログイン後に特権ユーザに移行しなければならない。

3．　特権ユーザとしての操作を実施する場合は、問題が起きたときに復旧が容易になるように、更新前のデータの日時を変えずに保存し、操作の記録をとらなければならない。

＜安定稼働のための作業＞

1．　停電、定期点検やシステム更新作業、構成変更作業などのために停止が必要な場合は、利用者が困らない日時を設定し、事前に全利用者に通知する。予告は重要なシステムの長時間の停止は１ヵ月前、短時間の場合は１週間前までに行うものとする。

2．特定の利用者がシステムの資源を独占的に利用していると思われるときは、利用者に連絡し、その実態に応じて、実行中のプロセスの停止を依頼する。他の利用者に迷惑がかかっていることが明白で、連絡が取れない場合は管理者の権限で停止し、その事実を当該利用者に報告する。

3．学外との通信、学内におけるトラフィックを監視し、通信障害があれば、解決のための対策を施す。

＜セキュリティ管理＞

1．　利用アカウントの作成と抹消には、学籍、人事データを用い、特に卒業や人事異動後速やかに定められた規則に従って処理しなければならない。

2．　サーバの利用記録、HIDS で収集した情報を監視し、異常があれば、必要と思われる調査、対処を施す。

3．　FWGW や NIDS から発せられる不正と思われる通信に対する警告を読み、必要と思われる調査、対処を施す。各利用者が管理するコンピュータに関する問題は利用者を補助し改善を要請する。ウイルス感染、踏台などにより短時間で他に迷惑が広がるものは、当該コンピュータの通信を遮断するなどの緊急対処を施す。

4．　利用者の使用するコンピュータの OS を把握し、関係するウイルスなどのセキュリティ関連情報を提供する。

５．　関係者に予告の上、定期的に自己セキュリティチェックを実施しなければならない。(セキュリティスキャナの実行、簡単に推測できるパスワードの検出など)加えてセキュリティ委員会と相談の上、外部監査を実施することが望ましい。

６．　リスク再分析のために、発生した重要な問題をまとめセキュリティ管理者に報告する。

７．　各ホストの root あての電子メールは実際の管理者に転送するように設定する。電子メールを中継するホストでは、postmaster についても、必ず実際の管理者に転送する。

＜緊急対応と対外連絡＞

１．　postmaster, webmaster, abuse などのメールアドレスに送り付けられた苦情などには慎重に対応する。重大または感情的な苦情については、メッセージの受領と調査中という報告のみを即答し、事実関係の調査を始めるとともに、ネットワークセキュリティ委員会や緊急対応委員会に報告し、状況を逐一報告して対応方針の決定を求める。

２．　本学に非があると事実が確認された場合は、緊急対処可能な場合は対処を施すが、謝罪の返信は慌てず、危機管理または広報部門に確認依頼する。

３．　障害やセキュリティ事件に学外組織も関係するときは、セキュリティ管理者と相談し、可能であれば関係組織の管理者と連絡を取り、問題の分析に協力を要請する。その際、調査に不要な情報は開示してはならない。問題が犯罪性をもつ深刻な場合は、危機管理部門の指示を仰ぎ、JPCERT、IPA 等への報告を検討する。本学が加害者側となる場合は弁護士等と相談、被害者となる場合は警察にも必要に応じて相談する。

４．　問題の連絡と緊急対応は発生から２４時間以内が望ましく、管理者、危機管理部門は休日であっても緊急連絡が可能な体制を整えておくべきである。また、webmaster には雑多な連絡が入ることが多く、webmaster を読む担当者に危機管理部門の担当者も加えておくべきである。

＜ログ管理＞

１．　ＵＮＩＸの syslog ファイルなどのアクセス記録は管理者のみが使用するホストに転送する設定としておくことが望ましい。共用ホスト置く場合は、管理者以外は読めないようにする。

２．　login の記録など、重要な記録は１ヵ月以上保存する。書替え不能なメディア等に保存することが望ましいが、やむを得ず書替え可能な磁気媒体等に保存する場合には必ず媒体を施錠できる場所に保管しなければならない。

３．　記録は、障害の分析、利用統計、不正または不適切な利用の追跡などシステム管理の目的以外には使用してはならない。

４．　不正アクセスの捜査のために警察から任意で情報提供を求められた場合は、危機

管理部門に指示をあおぎ最低限必要な情報のみを提供する。捜査令状を提示された場合は、弁護士の立ち会いを求める。

＜機密管理、個人情報保護＞

1．　管理特権で読めるファイルであっても、業務上アクセスする権限がないものは読んではならない。

2．　webmaster に寄せられる連絡の中には取り扱いに注意を要する情報を含むことがある。管理者はそれを適切な担当者に転送し、以後の連絡は担当者に任せるとともに、転送したメッセージの内容をみだりに他の教職員に漏らしてはならない。

3．　管理の必要からウイルス入りのメッセージの確認など、やむを得ず利用者宛のメールメッセージを検査するさいも、できるだけプログラムで一部分だけを抽出し、目視は避ける。

4．　その他アクセス記録も、全体件数の統計分析などの管理上の利用にとどめ、誰から誰にメッセージが何通送られたかなど、個人情報の分析は行わない。

＜その他＞

1．　コンピュータ犯罪、不正アクセス、電気通信事業法などの法令を読み、理解しておく必要がある。

2．　精神的不調などがあり業務に支障をきたすおそれがあると感じる、あるいは他者から指摘された場合は、上司に報告し、休養をとらなければならない。

＜罰則＞

業務上の権限を超える情報や資源にアクセスできる管理特権を持つので、罰則は重くならざるを得ない。重大な失敗に対しては叱責や他部署への配置転換などの処分を受けることがある。故意の不正行為は、職務規程に則った処罰の対象となる。また、退職後の不正侵入などの違法行為は刑事ならびに民事訴訟の対象となり得る。

コラム「安易に作れるメーリングリスト」

X大学では、ある学会の事務局を引き受けている関係で、学内利用者向けに運用してきたメーリングリストサーバで、その事務局の各種メーリングリストも引き受けることにしていた。あるとき、そのメーリングリストの参加者の一人が、コンピュータウイルスに感染したため、このメーリングリストを介在して、多くの人にコンピュータウイルスが流布される事態となってしまった。

この大学には、メールアドレスの学内向けの利用規程はあるが、メーリングリストに関する規程が未整備なため、メールサーバの管理組織による発見と対処に時間を要してしまった。

このような対応する規程の整備も進めるとともに、これまでは学内の全端末に、ウイルス駆除のソフトウェアを導入して対応してきた対策方針も、メールサーバ上でのウイルス駆除の対策も検討することも必要である。

Ⅳ．セキュリティポリシーを成功させるために

１．導入に際しての留意点

セキュリティポリシーを策定した後、ポリシーの運用開始までに、セキュリティポリシーを関係者に周知徹底し、確実に実施するための措置を行う必要がある。

このためには、ネットワークセキュリティ委員会は、ポリシーを関係者に周知するための、ポリシーの配布や説明会を行う。 ポリシーの配布（特に実施手順）の配布は、Ｗｅｂページなどに掲載するだけでなく、１、２枚の印刷物を配布することが必要である。また、グループごとに説明会を行い、セキュリティポリシーに対する意識を向上させることが望ましい。学内など人の入れ替わりが多い大学においては、新入学生に対してはできるだけ早く説明会を実施する必要がある。

２．運用に際しての留意点

次に実際の運用にあたっては次のような対応が必要となる*7) 。ポリシーを確実に運用していくために組織・体制の確立、監視、侵害時の対応等の措置を適切に行う必要がある。

（１）運用管理

ネットワークセキュリティ委員会の下で、情報メディアセンターは、ポリシーに従って、物理的セキュリティ対策、人的セキュリティ対策、技術的セキュリティ対策等が適切に遵守されているか確認する必要がある。セキュリティ上の重大な問題が生じる可能性がある悪質なポリシー違反が発見された場合には、ポリシーに記述された罰則規程に従って処理しなければならない。

（２）日常の訓練と緊急時の対応

① 訓練の実施等

緊急時対応計画の円滑な実施のため、定期的に訓練を実施することが望ましい。訓練の結果を踏まえ、緊急時対応計画の評価・見直しを適切に実施することも大切である。

② 緊急時の連絡と対処

緊急の連絡と対処は、あらかじめ定められた連絡ルート、対処マニュアル等に従って迅速に行う。その際、連絡手段はセキュリティ上安全かつ確実なものを用いる。

③再発防止の計画

再発防止計画については、当該侵害に関するリスク分析の結果を踏まえ、ポリシー、各種措置、緊急時対応計画、実施手順の評価・見直しに係る検討結果を具体的に示す。

また、定期的に評価・見なおしを行いポリシーの改善を図る必要がある。

３．作成と運用の失敗事例

（１）ポリシー策定のパターン

セキュリティポリシーの策定には次の３つのパターンがあるといわれている*1) 。

① 雛形活用型

あらかじめ用意したセキュリティ要件リストから取捨選択してポリシーを策定する方法。本冊子は、基本的にこの方式に基づくものである。短期間に低予算で実現できる反面、組織の事情に応じたポリシーを作成するのが難しいなどの問題点もある。

② ゼロベース型

策定グループのメンバーが関係者などにインタビューを行い、リスク分析を行い、ポリシーを設定していく方式。組織文化になじみ、わかりやすい言葉で記述できる反面、策定者に過度の負担がかかり、完成が遅れる可能性がある。また、ポリシーの妥当性を客観的に評価できないと言う問題がある。

③ コンサルティング型

外部コンサルタントを利用してポリシーを作成する方式。セキュリティポリシー策定委員会のメンバーの負担が軽い反面、ポリシーを正しく理解している人間が学内におらず、実際の運用が難しいなどの問題が生じうる。

いずれも長所欠点があり、各大学の特徴を考慮して決定するべきであるが、多くの大学では、何らかの雛型をベースにリスク分析を実施したり、学外のコンサルタントに一部コンサルティングを依頼することが多いのではないかと考える。いずれにしても、大学内においてセキュリティポリシーを作れる実力のある人間を育てる努力が必要である。

（２）作成と運用の失敗事例

セキュリティポリシーに関連してうまく行かないケースは次のようなものがあるといわれている*2) 。

① ポリシー作成の失敗

ア．いつまでたっても完成しない

リスク分析を厳密にやりすぎたり、対策を広げすぎたりして、時間がかかりすぎ、完成したときには現状に合わなくなっている場合がある。例えば、着手から半年以

内に第１版を完成することを目標にするなど、最初から完全を狙わず、徐々に洗練していくことが大切である。

イ．出来上がったポリシーが使い物にならない

サンプルを丸写しにしたり、企業等に一切の作成を委託してしまうと、実情を無視したものが出来上がることは言うまでもない。とにかく自分達で汗を流すことが必要である。

ウ．全学的に認めてもらえない

例えば、大学トップのお墨付きが無いため全学的に活動が認められない。そのため、関連部署の協力が得られず活動が中断したり、特定部署内のローカルルールになってしまうことがある。大学のトップマネージメントに携わる管理者の認知と協力を経て横断的な検討体制を作ることが不可欠である。

エ．ポリシーを作っただけで終わってしまった

ポリシー作成に必要な予算しか考えなかったため、ポリシーが完成しても実施のための経費が工面できなることがある。運用に必要な予算や人員確保の対策を含めて検討することが不可欠である。

② ポリシー運用の失敗

ア．構成員がポリシーの存在を知らない

ポリシーを作成しても対象者に周知しなければ実効はない。例えば、冊子を作成して全員に配布する等の対策が必要である。その際、読んでもらうための工夫も大切で、要約版も用意したり、電子メール等で質問に答えるなどの仕組みを用意することも大切である。

イ．構成員がポリシーを守らない

ネットワークの利用者からは、セキュリティポリシーによって利用内容が限定され利便性が損なわれるとの反発を招く場合がある。ポリシーを周知する際には、守ることにより生じるメリットと守らない場合の罰則を明示しておく必要がある。

コラム「ウイルス感染でネットワーク管理責任者はてんてこまい」

A大学のＬＡＮは情報コンセントの数が 6 千ポートを超え、かなりの規模になってきた。幸い、ＵＮＩＸホストを自己管理しようという教員や学生は情報系に限られ、深刻な不正アクセスの問題は起きていない。しかし、構成員が自宅で使用している Windows 系の PC のウイルス感染が結構あるようで、ＮＩＤＳでもよく検出される。大学のダイヤルアップ接続記録で利用者をつきとめて注意を促しているが、次から次へと発生するので、追い付かない。そこでウイルス対策ソフトウェアの一括購入を検討することとなった。他大学でも、同様の事態があるらしく、webmaster 宛にウイルス入りのメッセージが毎日数十件は届いている。情報系以外の利用者はＷｅｂと電子メールだけが使えればよいと割り切ってしまえば、ウイルスチェッカーつきのプロキシと電子メール中継サーバの導入で一気に解決出来そうだが、利用者を保護することが良いのか管理責任者は迷っている。

Ⅴ．技術的対応と教育

セキュリティポリシーにしたがった運用管理を実施するためには、技術的な対応と全ての利用者に対する教育が必要である。本章では、これらについて特に注意を求める点をセキュリティポリシーと絡めて重点的に解説する。

１．私立大学向け不正侵入検知・監視システムのあり方

いわゆるファイアウォール専用機をインターネットとの接続箇所に配置するか、ルータで通信制限を実施することは大学でも一般的になっていて、それらである程度の対策は可能である。

しかし、それだけでは不十分で、

① ファイアウォールやルータでの通信制限を間違って通過してしまう不正な通信

② 制限の対象としていない公開WWWサーバなどに対する不正なアクセス

③ 制限の対象としていない通信であっても、異常に短時間にアクセスが集中するもの(DoS 攻撃)

④ 大学のポリシーとして、通信制限を実施しない場合はすべての通信

に対して不正なアクセスの試みを検知する必要がある。その意味で、本稿では、特にまだ広く用いられていない、ＩＤＳ（侵入検知システム）を紹介する。ＩＤＳはまだ商品としては高価で、簡単に運用できるものではない。ここでは検出の原理、何が検知できるか、導入モデル、そして不正アクセス等の攻撃に対する防御だけでなく、ネットワークの可用性を保証するための、異常検出の機能も盛り込んだ「ネットワークセキュリティ検知・トラフィック監視システム」を紹介する。このシステムは近い将来に実現され、会員大学で導入されることを期待したものである。

すぐに高価なＩＤＳ機器を導入することが困難な場合は、まずは、実務管理者が無償で利用できるソフトウェアの試用を通じて、ＩＤＳの機能を理解することが有益である。

（１）不正侵入検知システム（ＩＤＳ）の概要

ＩＤＳ[1]とは、「侵入検知システム」という言葉通り、侵入を検知するシステムである。例えば、赤外線や他のセンサを用いた建物の侵入警報システムのネットワーク版と考えればよい。現在使用されているＩＤＳは大別すると、ＮＩＤＳ[2]とＨＩＤＳ[3]の２種類であ

(1) IDS: Intrusion Detection System
(2) NIDS: Network Intrusion Detection System

る。２種類のＩＤＳの主な機能をファイアウォール（FWGW：ファイアウォール・ゲートウェイ）、アンチウイルスゲートウェイの機能と比較すると表６のようになり、FWGWとＩＤＳは互いに機能を補うものであることがわかる。片方だけとするか、両方用いるかは、各大学のセキュリティポリシー次第である。

機 能	FWGW	ＮＩＤＳ	ＨＩＤＳ	ｱﾝﾁｳｲﾙｽ GW
アクセス制限	◎	×	×	×
不正アクセス・攻撃検出	○	◎	◎	×
不正アクセス・攻撃自動遮断	◎	△	×	×
ウイルス検出	○	○	×	◎
ＬＡＮ内トラフィック異常検出	×	△	×	×
通信処理速度低下の少なさ	△	◎	○	△

【表６】ＩＤＳ機能比較表

① ＮＩＤＳ

ＮＩＤＳはインターネット接続場所の他にＬＡＮで特に通信を監視したい場所に、センサ機器を配置し、センサ機器単独、またはセンサからの情報を一箇所に集め、異常があればコンソール画面や電子メール等管理者に警告するものである。

例えれば、警備員を複数箇所に配置し、その前を通過する怪しい人やその行動を警備本部に連絡する役割を果たす。

例えば以下のような警告がセンサ機器から管理者に送られる。同種の警告が１００回以上来る日もある。

《CISCO IDS からの警告例》
2002/03/19 12:16:05（発生日時）
SigID:5126　　（この IDS 商品で定義する分類番号）
SubSigID:0　　（小分類番号、この場合はないので 0）
EventMesg:WWW IIS .ida Indexing Service Overflow : .ida?<200+ chars> 4E4E4E4E
4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E4E
（中略）
3825753030303025753030 3D612020485454502F312E300DZZ
（攻撃してきたホストから送られたデータを 16 進数で表示。例えば 4E は'N'）
Protocol:TCP/IP（プロトコル種類、UDP でも TCP/IP と表示される）
SrcIPAddr:38.213.aa.bb　（攻撃したホスト）
DstIPAddr:133.29.xxx.yyy（攻撃を受けた学内ホストの１つ）
SrcPort:3051（攻撃してきたホスト側のポート、特に意味はない）
DstPort:80　（攻撃を受けた学内ホストのポート(HTTP)）

(3) HDIS: Host Intrusion Detection System

http://(略)/expsig_5126.html（ソフトウェア付属の解説Webページ）

《解説》

マイクロソフトIISの拡張機能のIndex Service（索引サービス）を200文字以上のデータとともに利用しようとしたら、この警告が発せられる。実際にホスト133.29.xxx.yyyがWebサービスを提供しているか、IISを動かしているか、Index Service を動かしているか、はわからない。したがって、この攻撃が成功して被害を受けたかどうかはわからない。

検出は、センサでその場所を通過するすべてのＩＰパケット(通信データ)を傍受し、そのＩＰパケットのヘッダ情報、ＴＣＰまたはＵＤＰヘッダ、データ内容、同種の通信の単位時間あたり件数を分析することで可能となる。

多くの市販製品で見られる検出方法は、

1) 正常な通信ではあり得ないパラメータの組合せの通信
2) データが特定の文字列パターンと一致
3) 短時間における特定のアクセスの集中

を発見することである。示した例は、2)である。その他に、通信をタイプ別に分類し急激な増加や減少により異常を発見する統計的手法もあるが、製品としてはまだ少ない。

② ＨＩＤＳ

ＮＩＤＳは門番的役割を果たすが、ＨＩＤＳは各ホスト(インターネットやＬＡＮに接続されたコンピュータ)の見張り番の役割を果たす。各ホストのＨＩＤＳは、警備本部にあたるコンピュータにすべての記録を送るか、異常のみを検出して送る。警備本部にあたるコンピュータでは、異常を発見し管理者に警告する。大学には教室、研究室も含め多数のホストが設置されているため、管理面を考慮すると主要サーバホストにのみ使用するのが現実的である。例えば、あるホストにloginしようとして4回失敗した記録がそのホストで観察された場合に、それを警備本部に通知するようなソフトウェアを導入する。

《4回loginに失敗した記録》

```
Apr 16 14:03:08 kgoto login[31912]: FAILED LOGIN 1 FROM kgoto4 FOR goto,
     User not known to the underlying authentication module
Apr 16 14:03:12 kgoto login[31912]: FAILED LOGIN 2 FROM kgoto4 FOR goto,
     User not known to the underlying authentication module
Apr 16 14:03:15 kgoto login[31912]: FAILED LOGIN 3 FROM kgoto4 FOR goto,
     User not known to the underlying authentication module
Apr 16 14:03:21 kgoto login[31912]: FAILED LOGIN SESSION FROM kgoto4 FOR goto,
     User not known to the underlying authentication module
```

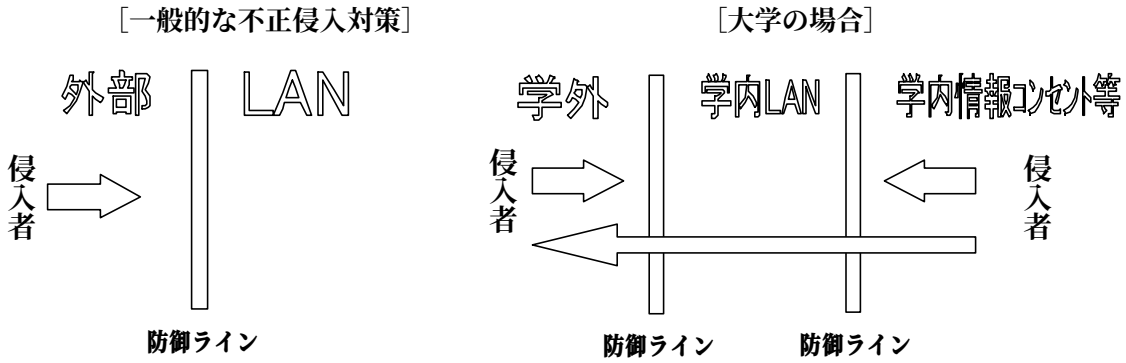
このような記録は一般にUnixのsyslog機能で各ホストに出力される。多くのルータにもsyslog出力機能がある。syslog出力をsyslog蓄積用サーバに転送し、サーバに分

析するソフトウェアを導入すればＨＩＤＳが構成できる。syslog の転送だけであれば、syslog 分析サーバ以外の各ホストには特別なソフトウェアは必要ない。Windows NT などの記録も同様に分析サーバに集めればよい。

不正なアクセスの他に、ファイルの変更/かいざんを検出することも有効である。一日一回程度、監視対象とするシステムのファイルやディレクトリのチェックサム(ハッシュ関数を用いたダイジェスト)を計算し、前回の値と比較するプログラムを実行する。

（２）大学のネットワーク規模・種別による検知システムの設置モデル

企業等の不正侵入対策は、外部からの不正侵入を検出するため、外部との接続点を集中的に監視する方法をとることが一般的である。しかし、大学の場合は学外からの不正侵入に限らず、教室等自由に出入りできる場所に設置された情報コンセント等から学内ＬＡＮに侵入する場合や、学内ＬＡＮを経由して学外のネットワークに侵入する場合があり、これら内部の不正使用を監視するため、学内ＬＡＮに多くの監視点を設ける必要がある。

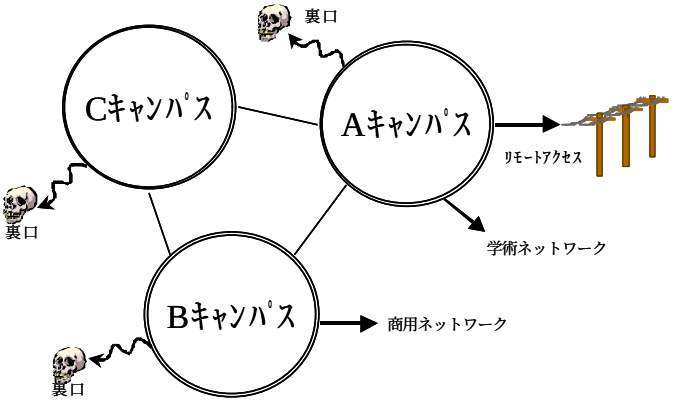


【図８】大学における不正侵入対策の特徴

また、大学によってネットワークの規模・構成、ネットワークの活用状況、運用管理の技術力に差異があることが考えられるが、ネットワークを介した大学間の情報共有や知的資産の共同利用が進展するためには、全ての私立大学・短期大学で一定水準のセキュリティを実現する必要がある。ここでは、私立大学におけるネットワーク構成と特徴を次のように分類し、ＩＤＳの設置場所と監視の方法について例示する。

A．分散キャンパス大規模ネットワーク ――――――――――――――――――――――――

《状況》

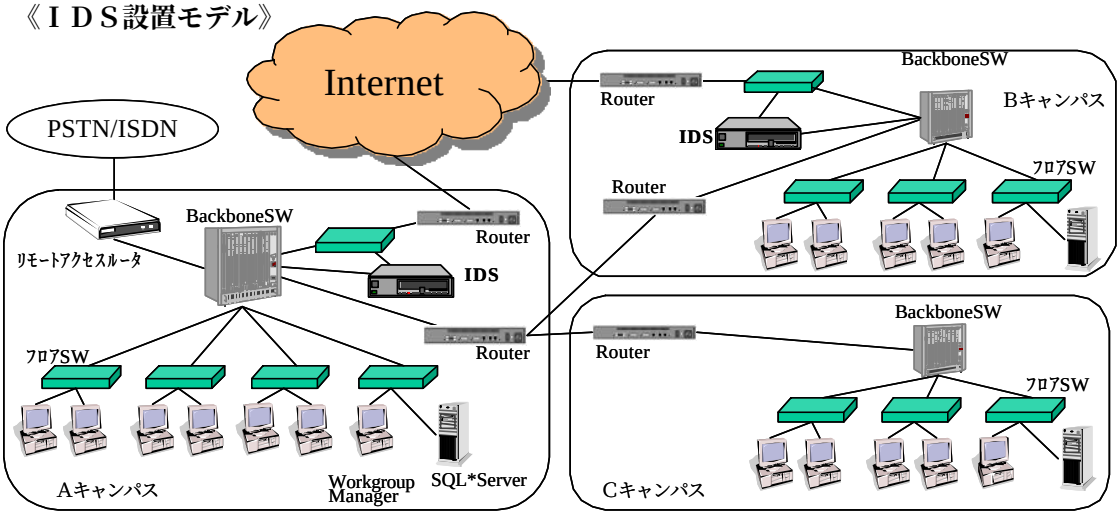


入学定員が３,０００人を越えるような大規模大学では、多くの場合、人文、社会、理工、医歯薬などの複数学部が複数キャンパスに分散している。マルチホーム接続により多くの利用者に対応している。問題点としては、利用者が多く、利用形態、利用内容も様々であるため、統一的なセキュリティポリシーの策定や情報センター等による一元管理が難しいこと、また、特に理工系の研究室等では全学的なＬＡＮ整備以前からネットワーク利用を開始しており、いわゆる裏口の存在が危惧されることなどである。

《特徴》

① 規模：複数分散キャンパス（学部数：８学部、学生数：15,000 人、教職員数：3,000 名）
② キャンパス間の接続：　キャンパス間接続あり
③ 学外接続先：　マルチホーム（学術ネットワーク＋商用ネットワーク）
④ アドレス体系：　グローバルアドレス
⑤ サブネットの有無：　サブネット有り
⑥ ルーティングポリシー：　基幹：RIP、支線：Static
⑦ トポロジー：　リング＋スター
⑧ ファイアウォール：　なし、フィルタリングのみ（メインの外部接続点のみ）
⑨ リモートアクセスの可否：　可（情報センター等で集中管理）
⑩ 裏口：　あり（すべてのキャンパスに可能性あり）

《ＩＤＳ設置モデル》

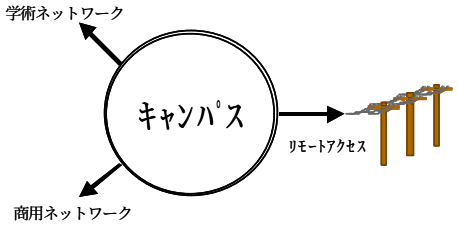


【図９】分散キャンパス大規模ネットワークにおけるＩＤＳ設置モデル

図９のように、インターネットに接続する各キャンパスの出入口にＩＤＳを設置して外部からの不正侵入を集中的に検出する。しかし、いわゆる裏口を通じた外部接続には対応できない。したがって、裏口を禁止するか、裏口に対しても小規模なＩＤＳを導入するなどの処置が必要である。

B．中小規模ネットワーク ――――――――――――――――――――――――――――――――

《状況》

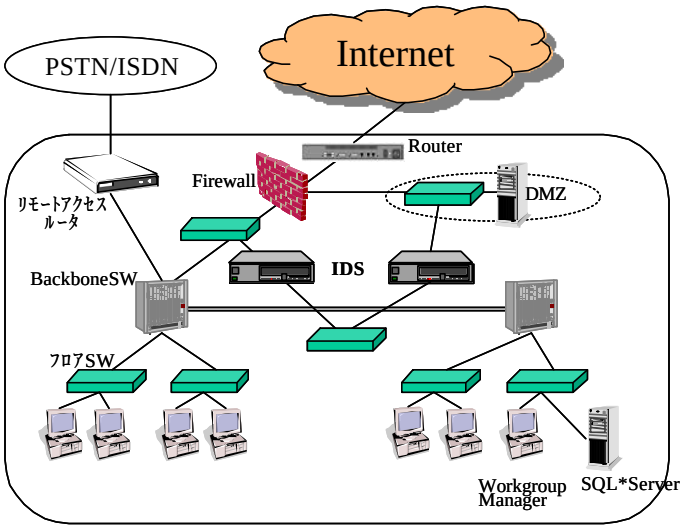


入学定員が２,０００人程度で人文科学系複数学部の大学。近年、学内のネットワーク需要が急増しており、マルチホーム接続を実施した他、学生の自学自習用として学外からのリモートアクセスも準備した。サブネットワークはなく、各種サーバの設定・運用状況は情報センターが一括管理しており、ファイアウォール、DMZにより不正侵入を防御している。現状では、技術的に高度な利用は行われていないが、学内の多地点に情報コンセントが設置されオープン利用に供されているため、不正使用を招く恐れがある。

《特徴》

① 規模：　単一キャンパス（学部数：4学部、学生数：8,000 人、教職員数：500 名）
② 学外接続先：　マルチホーム（学術ネットワーク＋商用ネットワーク）
③ アドレス体系：　グローバルアドレス＋プライベート
④ サブネットの有無：　サブネットなし
⑤ ルーティングポリシー：　なし
⑥ トポロジー：　リング＋スター
⑦ ファイアウォール：　あり（AltervistaFW）、DMZ 設置
⑧ リモートアクセスの可否：　可（情報センター等で集中管理）
⑨ 裏口：　なし

《ＩＤＳ設置モデル》



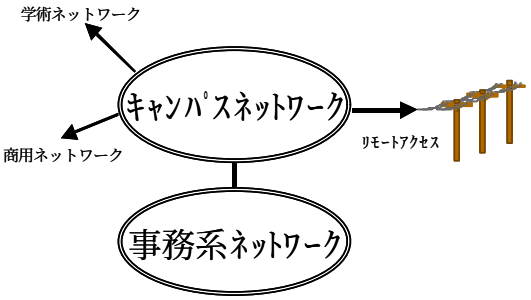
先ずインターネットに接続する出入口に設置されたファイアウォールの外側にＩＤＳを設置して様々な不正侵入の予兆を捕らえるとともに、ファイアウォールを通過した不正侵入に対応するため、ファイアウォールの内側にも設置して監視体制を強化する。

【図１０】単一キャンパス中小規模ネットワークにおけるＩＤＳ設置モデル

C．事務系ネットワーク――――――――――――――――――――――――――――――――

《状況》

教育用の学内ＬＡＮとは別に事務用のＬＡＮを整備した。学生個人情報や経営に関する情報を取り扱うため、情報の漏洩、破壊、改ざんの被害が生じないよう強固な防御対策を講じる必要がある。

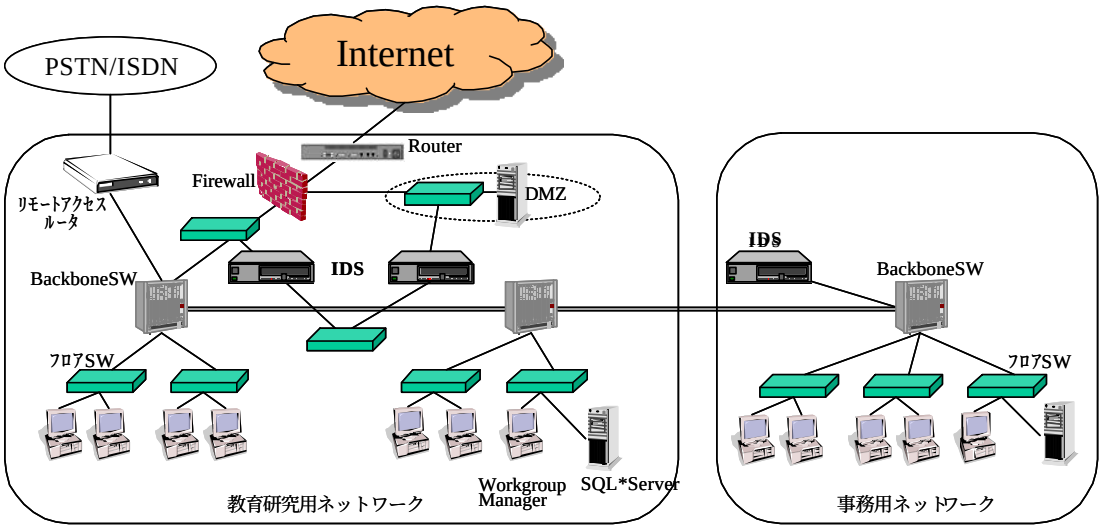


《特徴》

① 規模：　完全隔離型の１セグメントネットワーク、利用者は事務職員 300 名のみ
② 学外接続先：　外部接続はキャンパスネットに接続
③ アドレス体系：　プライベートアドレス
④ サブネットの有無：　サブネット無し
⑤ ルーティングポリシー：　なし
⑥ トポロジー：　スター
⑦ ファイアウォール：　ファイアウォール＋アプリケーションゲートウェイ
（強固な Firewall の設置が前提）
⑧ リモートアクセスの可否：　不可
⑨ 裏口：　なし

《ＩＤＳ設置モデル》

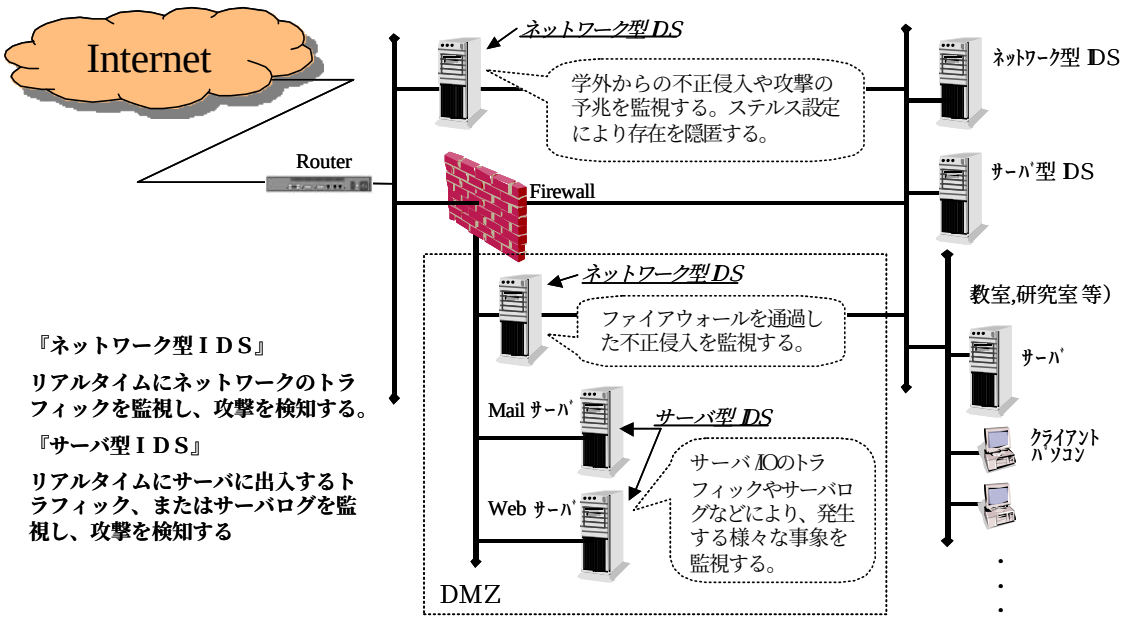
インターネット接続の出入口のファイアウォールの前後にＩＤＳを設置してファイアウォールを通過した不正侵入を検出するとともに、さらに、教育研究用ネットワークと事務系ネットワークの接続点にもＩＤＳを設置し、事務系ネットワークへの不正侵入を検出できるようにする。



【図１１】事務系ネットワークにおけるＩＤＳ設置モデル

なお、ネットワーク上のサーバ機内部に侵入してデータの破壊や改ざん、サーバの占拠、さらには学内のサーバを経由して他大学や企業等のネットワークを攻撃する場合がある。このため、不正侵入の検出・監視は、学内ＬＡＮの基幹線及び支線を流れる不正侵入を捕らえるだけではなく、ＬＡＮ上のサーバ機に ＨＩＤＳプログラムを設定してサーバ内部の不正使用を検出する必要がある。

以上のＩＤＳ設置モデルを整理すると以下のような構成となる。



【図１２】ＩＤＳの種類と設置場所一覧

図１２のようにセンサは一般に二つ以上のネットワークインタフェースを持ち、監視用インタフェースは性能を上げるためと、ＩＤＳ設置を敵から隠すために、ＩＰアドレスをつけずに受信専用とする。これをステルス設定と呼ぶことがある。このインタフェースはすべてのパケット（フレーム）を受信できる共有ハブか他のポートへのフレームもすべて出力できるスイッチに接続する。他の機器とはＩＰアドレスをつけた他のインタフェースで通信する。ただし、実験的な運用においては、インタフェースは一つでもかまわない。また、現状では 1Gbps ＬＡＮで使用できるＩＤＳは少なく、高価なので、100Mbps 以下のＬＡＮ部分での設置から始めるのが現実的である。

（３）異常検出時の対処（アラームの分析と対処例 ）

警告に基づいて管理者がとるべき対処の手順と内容は、大学のセキュリティポリシーに

基いて決定される。逆に言えば、セキュリティポリシーがなければ、明確な対応手順が決まらず、例えば、管理者が業務に忙殺されているときには警告が放置されてしまうことになりかねない。

以下に、ＩＤＳから警告が発せられた場合の対処について例示する。(警告例は２７ページを参照)

《ＩＤＳからの警告に基く対処例》

1．分析 ・・・・・・・(技術的内容なので、セキュリティポリシーへの依存度は低い)
①攻撃の方向
②被害を実際に受けている可能性（対象となるホスト、特定のソフトウェアによるサービスが実在するか)
③同種の攻撃の頻度
＜手順＞
①ＩＰアドレスから学内から学外、学外から学内か判断する。
※学内から学内は、ＩＤＳが学内ネットワーク内になければ検出されない。
②-A 学内への攻撃の場合
※攻撃を受けたホストでの WWW サービスの有無を調べる
Unix で、telnet 133.29.xxx.yyy 80
・接続できなかったらサービスはないので、実際に攻撃は受けていない。
・接続できた場合は、応答から Apache、IIS、あるいは他のサーバかわかる。
・IIS でなければ問題はない。
IIS の場合は実際に攻撃された可能性が高い。
②-B 学外への攻撃の場合
・攻撃した学内ホストがウイルス等に感染しているか侵入を受けている
・このホストの利用者(学生等)がいたずらした可能性が高い
＜調査結果＞
当該ホストは IIS で WWW サービスが稼働している。Index 機能が稼働しているかは不明。攻撃は外部からなされた。

2．対処 ・・・・・・・(セキュリティポリシーにより対処法は異なる)
ポリシーA
『侵入された可能性があるとき、重要でないサービスは停止。重要なサービスは代替機で継続。』
対処: 当該ホストが大学の業務サービス用であれば、至急サーバソフトウェアのバージョン、機能を確認する。疑わしい場合は、至急ネットワークから切り離し、別のサーバで機能を代替する。準備ができるまで、あるいは管理担当者から連絡がない場合は、サービス停止もやむを得ない。当該ホストが研究室や個人管理であれば、通信をそのホスト付近のルータで一時遮断するかホストを上級管理者が停止する。その事実を管理者に通知し、機能確認報告後、通信再開。
ポリシーB
『各ホストの管理者が当該ホストの管理責任を持つ。』
対処: 警告内容を伝え、機能確認を求める。返事がなく、他へ怪しい通信が発せられたときは、通信をそのホスト付近のルータで一時遮断。

（4）私立大学に相応しい不正侵入検出・監視システムの姿

先に述べたように、私立大学のＬＡＮにおける不正侵入対策は外部からの侵入を防御するとともに、内部における不正使用にも対応する必要があり、多くの構成員が様々な目的でネットワークを利用している状況では、ＩＤＳを一点に設置しただけでは十分な防御ができない。学内の多地点にＩＤＳを設置し、管理者の技術水準に関わらず一定の監視能力

を発揮するためには、次のような特徴を備えた検出・監視システムが必要となる。

● 特徴 ――

① *学内多地点への展開が可能であること*

学外からの不正侵入および内部からの不正使用を監視するため、対外接続点、基幹ＬＡＮ、支線ＬＡＮ、研究室等、学内ネットワーク上の多地点に設置し、運用できるようにする。

② 機動性に優れていること

監視の必要性が生じた地点で直ちに運用するため、自由に設置場所を移動できるようにする。そのため、本体はノートパソコン等による運用を可能とする。

③ インストールおよび設定が簡単であること

本システムを多くの私立大学に普及するため、インストールおよび機能設定は大学の技術水準に関わらず平易な手順で実施できるようにする。

④ 常に最新の情報に基く検出・監視が可能であること

既知の攻撃手法および対応策に関するパターンファイルを備え、常に最新の情報に基づく検出と対応策の提示を行えるようにする。

⑤ 導入・運用が安価であること

１大学が多数のシステムを導入できるよう、１システムの価格を低価格にする。そのため、高価な SNMP(Simple Network Management Protocol)マネージャ、データベースの使用を前提としない。

⑥ ネットワークの規模、管理者の技術水準に応じた柔軟な設定、運用が可能であること

検知する不正侵入等の種類・内容、管理者に通知する内容は、大学のネットワークの規模や管理者の技術水準に応じて柔軟に設定できるようにする。

⑦ 本体のセキュリティ機能が強力であること

システム自体への攻撃に十分耐えるよう対策が施されるとともに、本体のプログラムは最新のセキュリティ技術が施されるよう更新できるようにする。

⑧ 目的以外の使用を認めないこと

本システムを用いた不正侵入・不正使用が行われないよう、システムの設定、データの取得・閲覧などは強固な認証技術により管理者以外は使用できないようにする。

また、システムの機能、動作環境、運用方法については、管理者が必要とする情報を直ちに取得できるよう、設置後に平易な設定で稼動できるよう工夫が必要であり、従来のＩＤＳ製品に見られるような過剰な検出や難解な警告表示がなく、必要十分な情報を抽出できるようにするなど、強力な機能と柔軟な運用を可能にすることが必要である。特に市販製品にみられない機能は☆マークで示す。

●求められる機能 ――――――――――――――――――――――――――――――――

① 不正侵入および通信異常の検出

外部から学内ＬＡＮへのログインの成功／失敗や、学内外からの管理者権限によるログインなど、ネットワークにアクセスする者を監視する他、学外からのポートスキャンの実行など、不正侵入の手掛かりを探る行為、サーバ機におけるシステムファイル改ざんなどの不正使用、また、不正侵入、不正使用により生ずる通信異常を検出する。

② 利用状況の把握 ☆

Ｗｅｂページの利用、電子メールの利用など、学内から学外、学外から学内、学内相互の通信トラフィックを監視・記録するとともに、例えば急激なトラフィックの増加など、日常の利用状況と著しく異なる状況を検出する。

③ 管理者への通知、統計情報の提示 ☆

《不正侵入および通信異常検出時の通知》

a. 管理者への通知方法は、監視画面などへの警告表示、管理者アドレスへの電子メール送信、管理者の携帯電話への電子音声による呼び出し等の方法から管理者が選択できるようにする。
b. 通知内容は、管理者が、自身の技術水準等に応じて必要な情報を取得できるよう、通知する内容、詳細の度合いなどを任意に設定できるようにする。
c. 不正侵入および通信異常の状況を通知するとともに、考えられる対応策を提示する。通知内容と同様に提示する内容は階層化できることとする。

《統計情報の提供》

全ての監視データを記録可能とし、管理者に必要な統計情報を提示する。項目の種類、内容は、日報・月報などの報告単位に管理者が任意に設定できるようにする。

●柔軟な運用方法への対応 ――――――――――――――――――――――――――――――――

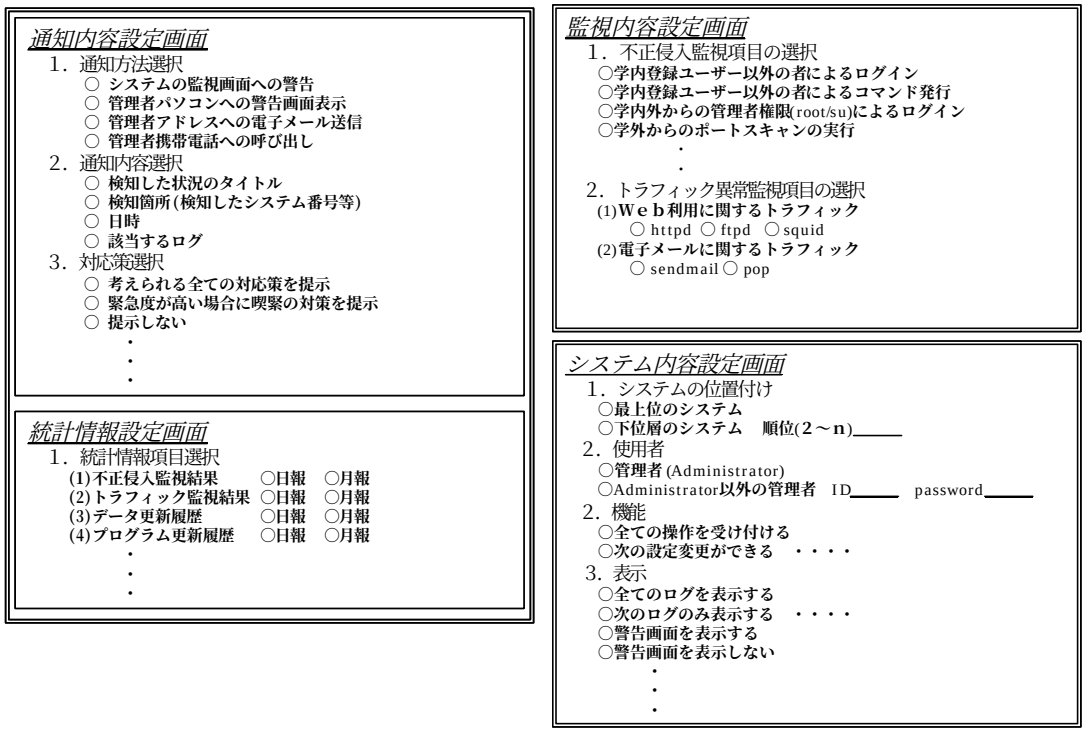
① 定常的な設置 ☆

初期導入の際、インストールから稼動まで、１週間程度で完了するようにする。設定作業は、経験の浅い職員でも対応できるようＷｅｂページによる平易な設定画面を用い、管理者が取得したい情報を、例えば対話形式等により順序立てて設定できるようにする。

② 緊急時の設置 ☆

本システムをネットワーク上で障害等が発生している地点に単独で設置し、直ちに運用できるようにする。設定作業は、定常的な設置に比べ簡易に行うことができるよう、必要最低限度の項目設定で完了するようにする。

なお、MS-Windows、UNIX、Linux など、パソコンやワークステーションで一般的に用いられているオペレーティングシステム（ＯＳ）上で動作することとし、対応する通信方式（プロトコル）は、学内外のネットワークで広く使用されているＴＣＰ／ＩＰとする。また、機動性に優れたシステムとするため、ＣＰＵの能力、メモリ、ディスク容量は、ノートパソコンでの運用を可能とすることが求められる。



【図１３】設定画面のイメージ

なお、参考情報として、本協会会員専用のＷｅｂページから、本協会賛助会員の関連サービス、ＰＤＳ(Public Domain Software：製作者が著作権を放棄したソフトウェア)や無償のＩＤＳの利用方法などを紹介することにしているので参照されたい。

コラム「ファイアウォールを過信したばかりにメール不正中継」

Ｂ大学の事務系ネットワークは学内ＬＡＮとファイアウォールによって遮断されている。このファイアウォールの内側にあるメールサーバがスパムの不正中継に利用され数日間に数万通のメールを国内外に中継送信していた。ファイアウォールがあるから安心ということで、メールサーバのメンテナンスや利用状況の監査は十分に行われていなかった。ファイアウォール自体は警告メッセージを出力していたが、管理者はこれにも気がつかず、トラフィックの異常に気がついた教育系ネットワークの管理部門からの指摘で事件が発覚した。
一般的にファイアウォールを設置していても、外部からのメールはファイアウォールによって SMTP サーバへ中継される。このため外部と通信を行うサーバの設置に際しては、ファイアウォールの有無に関係なく慎重に行われる必要がある。特にシステムの監視の方法とログの監査を行う手順を明確にしておかなければ、ファイアウォールの性能を引き出せないばかりか、この事例のようにファイアウォールを過信して被害が拡大することになる。最近では、ファイアウォール自体を攻撃する手口も巧妙になってきているので、前段にパケットフィルタを行うチョークルータを置く対応も必要である。

２．ネットワークセキュリティと情報倫理教育

（１）情報倫理教育の必要性

情報倫理は、「情報社会において、われわれが社会生活を営む上で、他人の権利との衝突

を避けるべく、各個人が最低限守るべきルール」である。情報倫理とセキュリティとは、交わりの関係にある。例えば著作権侵害・違法コピー・掲示板やＷｅｂページ上での誹謗や中傷等々は、セキュリティからはみ出している。また、セキュリティに関わる極めて技術的な項目等は、情報倫理からはみ出している。しかし、両者は極めて広範囲に重なり合っており、相補う関係にある。何故なら、各大学がセキュリティポリシーを定め、かつ、防御環境を整備したとしても、そのようなインターネット環境を運用し利用するのが人間である以上、セキュリティをかいくぐり、かつ、情報倫理に反する運用や利用が生じてしまうからである。

情報倫理教育とセキュリティ対策はいずれも、高度情報化社会があわせ持つ影の部分への対処方法である。セキュリティ対策の主たる関心は、高度な技術を有する者による意図的な侵害行為からインターネット環境を防衛することであり、JPSERT 情報の常時点検と対応等「人」の導入という側面もあるものの、ＬＡＮの構成の見直し・ファイアウォールの設置等々「物」の導入という側面が強い。これに対して情報倫理教育の主たる関心は、アンチウィルスソフトの導入を推奨するなどの側面もあるものの、インターネット利用者の被害防止と、意図的でない加害の防止であり、そのための知識と判断力を身に付けさせ、日常的に実行させることである。

情報倫理は、これまで経験したことのない新しい情報化社会の社会通念をひとりひとりの価値観に基づいて創造していくものであることから、家庭で親から子に教えられるものではない。初等・中等教育では、インターネットの使い方やその便利さないし光の部分を教えるものの、影の部分までは教えていない。平成１５年度からの学習指導要領の改正によっても情報倫理は、「情報Ｃ」の一部にのみ採り入れられているにすぎない。平成１１年に制定され平成１２年に施行された「不正アクセス行為等の禁止に関する法律」の有する社会教育効果は、未知数である。

したがって大学は、インターネット環境の運用や利用をしている教職員、学生・院生に対して、情報倫理の教育を積極的に実施せざるを得ないのが現状なのである。なお、教育すべき情報倫理の内容のうち、セキュリティ方策と重なり合う部分にのみ、ここでは論及することとする。

（２）誰を対象にどのような内容を教えるべきか

①　学生に対して

インターネットを使っている学生や大学院生は、情報発信・情報収集の便利さや、ハードウェアやソフトウェアの先端性にのみ、目を奪われていることが少なくない。しか

し大学としては、被害者とならぬよう彼らを護らなければならない。意図的でない加害行為を彼らが行ってしまうことを、防がなければならない。意図的な加害行為を彼らが行うことを、防がなければならない。そのためには、次に述べるような基礎中の基礎を教える講習などの受講を義務付けるべきである。

インターネットを利用すると自動的に記録が残り、その利用者を割り出し可能である。この意味でインターネット上は、決して匿名社会ではない。それ故、インターネットを悪用しようとする者は、他人のＩＤとパスワードを用いてその他人になりすますものである。

インターネットでは利用者の確認をＩＤとパスワードにより行っているので、たとえなりすましであっても正規の利用者と扱ってしまうことになる。パスワードを決して他人に教えてはならないし、知られてはならない、推測され易いパスワードを付けてはならない。パスワードを頻繁に変更しなければならない等々の理由はこれである。

パスワードを推測するまでもなく簡単に他人になりすましうるのが、実習室などで、インターネットとの接続を正確に切断せぬままに離席したか、または、接続したままで一時離席したパソコンを使うことである。

なりすまされた者は、自分を不正アクセスされた被害者であるとのみ考えがちである。しかし、自分のＩＤを用いた不正アクセスに加担してしまったのは事実であるから、登録停止・登録取消し等々システム管理上の処分を受けることとなる。

インターネット利用に関わる処分としてはその他に、停学・退学など学則上の処分はもちろん、損害賠償など民事制裁、刑罰を科される刑事制裁などもある。なお、システム管理上の処分と学則上の処分については、その要件・効果や処分決定手続を、各大学は予め規定しておかなければならない。

セキュリティとの関連で、被害防止に関わり学生・院生に教えるべき基礎知識の中に、Ｗｅｂページに顔写真や電話番号を載せることはホテルの廊下ないし街中でそれを掲示することと同じであることや、電子メールがどこのサーバを順次経由して相手に届くかはそのときどきにより異なり、しかも、それぞれのサーバにおいてメールの内容を読めることも、含めるべきであろう。なお、後者については、セキュリティ対策の観点から、鍵技術が開発され既に利用されている。

② 一般教職員に対して

基本的には、学生・院生について述べた内容と同一であるので、相違点についてのみ記すこととする。

職員に対しては、職務命令により情報倫理講習会の受講を義務付けることができる。学生・院生や教職員のプライバシーに関する事項や大学業務の根幹に関わる事項をも扱う立場であるから、単独作業の禁止・担当者の異動に伴うパスワードの変更等々、講習には細部に渡る事項も含まれるべきこととなる。

教員に業務命令は馴染まないものの、情報倫理を身に付けていてもらわなければならない。ＩＤの期限やその更新をｅ－ラーニングによる講習と組み合わせるなど、工夫が必要であろう。これにより、教員が自分のＩＤとパスワードを学生・院生に使わせてしまうという事態を、無くすべきである。なお、学生・院生に対する停学・退学は、教職員に対しては休職・免職と対応する。

インターネットに関する知識が豊富であると自認している教員の中には、独自のサーバを立ち上げたがる者もいる。しかし、サーバの維持・管理には、システム管理者と同等の時間と労力を要するにもかかわらず、維持・管理を学生・院生任せにしたり、維持・管理をしていなかったりする者が少なくない。すなわち、光の部分に関する知識の豊富さと情報倫理が身に付いているかとの相関は決して大ではない。その結果、当該サーバが攻撃されたり異常発信をしたりして、全学のシステムダウンを引き起こすこともある。したがって、システム管理者は、許した場合の常時バックアップ体制を採れるのでない限り、教員からの要求であっても、独自サーバの立ち上げを安易に許すべきではない。

③　システム管理者に対して

システム管理者の権限は、当該システムについてオールマイティである。したがって、学生・院生に対する講習会の内容や一般教職員に対する講習会の内容は、システム管理者にとり常識でなければならない。システム管理者は、インターネットを用いた全てのメール内容や業務内容の点検が常時可能な地位にある。それにもかかわらず、それらの内容を点検・監視すべきではない。もしも点検・監視が行われていることを前提としなければならないとするならば、インターネット上の自由な情報通信は行われ得ないであろう。したがって、システム管理者には、強靱な精神力を要する「見えるけれども見ない」という、学生・院生や一般教職員に対するよりも高度な、情報倫理が要求されているのである。

インターネットを用いた犯罪などに当該システムが関与してしまっていたとき、犯罪捜査の目的で、任意捜査である過去ログの提出依頼や、強制捜査である令状に基づく機器の捜索差押がありうる。システム維持のためにその場で抵抗をしてしておかなければならないものの、抵抗自体は結局は無駄となることが多いから、事後救済を求めるしか

ない。とは言え、システムの運用指針として、積極的な協力まではしないことが、適切な運用をしている事案についてまで将来起きるかも知れない介入を防止するために、必要不可欠である。

④　大学経営者に対して

大学の理事会にとり、セキュリティ・ポリシーと情報倫理教育のあり方は、大学の経営基盤を揺るがしかねない重要な問題である。しかし、インターネットの普及があまりにも急速であったが故に、特に理事会はインターネット経験に乏しい理事で構成されていることが少なくない。

しかし、大学経営者、理事の理解を得ることは極めて重要であり、継続的な努力が必要である。理解を得なければならない内容も技術的なものよりも情報倫理教育の必要性・重要性であると考えるのが良いであろう。

参考文献：

1）高橋洋介「情報セキュリティポリシーの考え方とセキュリティ評価」信学会・情処学会平成１３年度専門講習会資料
2）勝村幸博「事例で知る・セキュリティポリシー失敗の仕方」日経オープンシステム、２００１年３月号
3）足利俊樹「セキュリティ・ポリシー実践ガイド　第１回概要と策定手順」日経オープンシステム 2001 年 1 月号
4）上原孝之「セキュリティ・ポリシー実践ガイド　第２回ポリシーの記述例」日経オープンシステム 2001 年２月号
5）田中健介「セキュリティ・ポリシー実践ガイド　第３回ポリシーの運用」日経オープンシステム 2001 年３月号
6）平成１２年度 JNSA 技術部会セキュリティポリシーWG「セキュリティポリシーサンプルドキュメント」http://www.jnsa.or.jp/
7）情報セキュリティ対策推進会議「情報セキュリティポリシーに関するガイドライン」平成 12 年 7 月 18 日 http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html
8）上原孝之「ネットワーク危機管理入門」翔泳社、２０００年
9）永井康彦「情報セキュリティ事典　18.3 節リスク分析」共立出版、2002 年（出版予定）
10）佐々木良一他「インターネット時代の情報セキュリティ　暗号と電子透かし」共立出版、2000 年
11）田渕治樹「国際セキュリティ標準　ＩＳＯ／ＩＥＣ１７７９９入門」オーム社、2000 年

社団法人私立大学情報教育協会
ネットワーク研究委員会不正侵入対策小委員会

担当理事	井上　　靖	東海大学総合センター所長
委 員 長	奥山　　徹	朝日大学経営学部教授
委　　員	大塚　秀治	麗澤大学国際経済学部助教授
	藤原　一博	上智大学電子計算機センター係長
	佐々木良一	東京電機大学工学部情報メディア学科教授
	鶴貝　達政	明治学院大学情報センター長補佐
	後藤　邦夫	南山大学数理情報学部教授、経営学部教授
	伊藤　剛和	園田学園女子大学情報教育センター助教授・主幹
	斎木　秀朗	神戸学院大学情報処理センター事務長
	窪田　　誠	前学習院大学計算機センター講師（平成１４年３月退任）

協力委員会：

社団法人私立大学情報教育協会 情報倫理教育振興研究委員会
「Ｖ－２．ネットワークセキュリティと情報倫理教育」のとりまとめ

賛助会員：

「Ｖ－１．私立大学向け不正侵入検知・監視システムのあり方」への情報提供及び相談助言

株式会社シーエーシー
日本電子計算株式会社
株式会社ネットマークス
三菱電機株式会社

社団法人私立大学情報教育協会
TEL:03-3261-2798
E-mail:info@shijokyo.or.jp
http://www.shijokyo.or.jp