高等教育機関におけるネットワーク運用ガイドライン

（第一版・暫定版）

キャンパスネットワークの
運用ポリシーと実施要領策定に関する指針

平成 14 年 9 月 10 日

電子情報通信学会
ネットワーク運用ガイドライン検討WG

はじめに

本ガイドラインは、高等教育機関におけるネットワークの運用ポリシーを策定する際の指針を提示することにより、ネットワーク環境の構築・運用と、その発展に資することを目的とするものである。これにより、科学技術創造立国として高度な人材教育ならびに研究活動を行っている高等教育機関の適切で安全なネットワーク運用と利用を図るものである。

高等教育機関におけるネットワークは、教育・研究の基盤として不可欠であると同時に組織の経営基盤にもなっている。また、これからは社会人教育、産学官連携、地域連携など社会的貢献の活動基盤になることも期待されている。

高等教育機関におけるネットワークは、組織内で構築・運用されているものではあるが、広く世界中のネットワークとも接続されており、このことを十分考慮してネットワークの運用を行わなければならない。このためには、関係する法令や制度との整合性を十分考慮して、組織内でのネットワーク運用ポリシー（情報セキュリティポリシーを含む）を明確にして、そのポリシーに則した実施要領を策定し、全組織的にルール遵守に努めることが必須である。本ガイドラインは、これら運用ポリシーと実施要領策定のための指針として提供するものである。

本ガイドラインの構成は、次のようになっている。

- I　総則であり、キャンパスネットワークの運用組織の設置に始まる運用ポリシー策定のための考え方や考慮点を示す。
- II　ネットワークの運用・管理の面から実際に想定される留意点を示す。
- III　ネットワークの利用者に焦点を当て利用者の権利と責任の観点から留意点を示す。
- IV　ネットワークの運用やそれを利用する一人ひとりが適切に行動することが重要であり、そのための教育と倫理に関して示す。
- 付録　参考として、違反行為への対応、教育カリキュラムモデル、関連法規等を添付する。

最後に、高等教育機関において教育研究活動が円滑に行われるためには、ネットワークの利便性、信頼性、安全性の確保が不可欠であり、そのために必要にして十分な予算と要員の確保が極めて重要であることを加えておきたい。

I 総論

1. ネットワークの運用ポリシー

1.1 運用ポリシーと実施要領

ネットワークの運用に際して、「運用ポリシー」を策定することによってネットワーク運用の基本方針を明確にするとともに、その方針に基づいた具体的な行動手順を示すものとして「実施要領」を策定することにより、適切なネットワーク利用を図ることが重要である。また、この実施要領の実行をより確実にするためには、部門の実務に合わせてさらに具体的な行動を示した各種対応マニュアルを必要に応じて整備することも大切である。これらの関係を図 1 に示す。

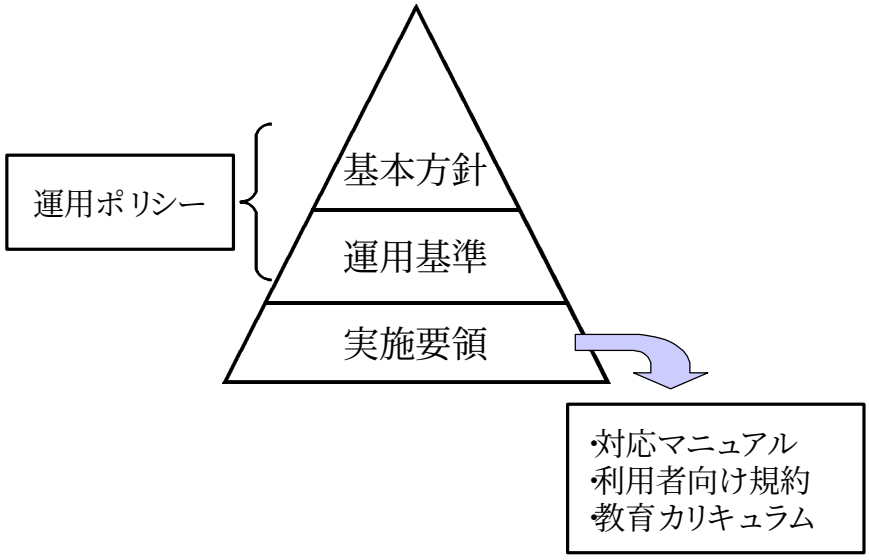

図1 運用ポリシーの位置付け

(1)ネットワーク運用ポリシー（以下「ポリシー」という）

ポリシーは、各高等教育機関が所有する情報資産のネットワークの運用・管理について、各高等教育機関が総合的、体系的かつ具体的にとりまとめたものである。どのような情報資産を、どのような目的に対して、どのようにして運営するのかについての基本的な考え方とそのネットワーク運用を実現するための体制、組織および運用を含めた規定である。ポリシーは、ネットワーク運用基本方針およびネットワーク運用基準からなる。

(2)ネットワーク運用基本方針（以下「基本方針」という）

基本方針は、各高等教育機関における、ネットワークの運用・管理に対する根本的な考え方を表すもので、各高等教育機関が、どのような情報資産を、どのような手法によって運営、保護、発展させなければならないのかを明らかにし、各高等教育機関のネットワーク運用に対する「取組姿勢」を示すものである。例えば、ネットワークの管理と表現の自由や通信の秘密は、衝突する場面があるが、どこでバランスさせるかといった方針を明確にする。

(3)ネットワーク運用基準（以下「運用基準」という）
運用基準は、基本方針に定められたネットワークの運用・管理を確保するために遵守すべき行為および判断等の基準、つまり基本方針を実現するためになすべきことを示すものである。例えば、ネットワーク利用者の守られるべき利益(権利)と制限(私的利用、商用利用等)をどこで線引きするかといった基準を明確にする。

(4)ネットワーク運用実施要領（以下「実施要領」という）
実施要領は、運用基準に定められた内容を具体的な情報システム又は業務において、どのような手順に従って実行していくのかを示すもので、各々のネットワークにおける実情に即して具体的な手順を明確にするものである。

1.2 ポリシーと実施要領の策定手続

ポリシーと実施要領を策定するためには、まず、ネットワークの運用と管理に責任を持つ組織・体制を確立しなければならない。この組織・体制の下で基本方針を策定し、運用によって守られるべき利益や制限を勘案して運用基準を策定する。このようにして作成されたポリシーを各教育機関内において正式に定める。各組織においては、そのポリシーに従い、運用基準に定められた事項を実施する手順を記述した実施要領を策定する。さらに、各部門の実務に即した具体的な行動を示す各種マニュアル等を整備する。このマニュアル類には、利用者向け規約や教育カリキュラムなどが含まれる。

2. 組織・体制の確立

2.1 基本となる体制

ポリシー策定には、組織の幹部の関与を明確にするとともに、その責任の所在を明確にするため、関係部局の長（総括責任者）、情報システムの管理者（技術責任者）およびネットワークの運用・管理に関する専門的知識を有する者などで構成する組織（本ガイドラインでは、以下「ネットワーク運用委員会」と呼ぶ。）を設ける必要がある。このため、ポリシーには、ネットワーク運用委員会の目的、権限、名称、業務、構成員等を定める。ポリシーでは組織内の種々の情報に係る問題を取り扱うことから、すべての部局等の関係者がこれにかかわることが考えられるが、図２の体制を基本構成として考える。

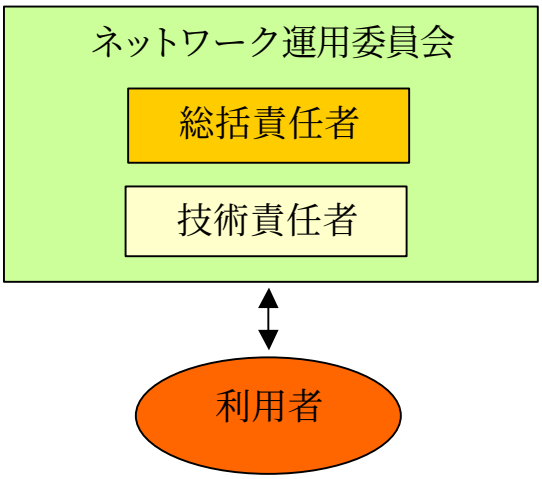

図 2 基本的な体制

この基本体制は、「総括責任者」、「技術責任者」および「利用者」の三者を基本とする。

(1) 総括責任者とは、当該ネットワークの基本構成、運用・管理に責任を持つ者で、ポリシーの決定やネットワーク上での各種問題に対する処置に責任を持つものとする。総括責任者は技術責任者と技術担当者等を招集して、ネットワーク運用委員会を開催する。

(2) 技術責任者は、当該ネットワークの設計や技術的問題（情報セキュリティ対策を含む）に対する処置に責任を持つものである。技術責任者は、複数の技術担当者を任命して実務を担当させる場合もある。

(3) 利用者とは、エンドユーザーとして当該ネットワークを利用する者を指し、総括責任者および技術責任者の指示に従わなくてはならない。

当該ネットワークがサブネットワーク、サブサブネットワークのように階層構造を構成する時は、それぞれのネットワークに総括責任者と技術責任者を置いて順次権限を委譲していくことが考えられる。ただし、管理の階層を深くしすぎると、末端ネットワークの責任の所在が不明確になる危険があることに注意を要する。

また、小さな組織では、総括責任者と技術責任者を兼務させることも考えられる。権限委譲を行う場合は、定常時、異常時など、それぞれの場合における対応を明確に規定しておくことが重要である。

2.2 全学ネットワークを総括する組織（全学ネットワーク運用委員会）

総合大学等では、部局(学部等)毎の独立性が高く、上記三者からなる単純な構造による運用が困難である場合も多い。また、大学では対外接続を担っている部局(情報基盤センター、情報処理センター等) が存在するのが一般的である。

このような場合、内外に対する緊急の措置を必要とするような日常のネットワーク運用に関しては、対外接続を担っている部局の総括責任者が、各部局の総括責任者と技術責任者を招集して、「全学ネットワーク運用委員会」を設けることが考えられる。図３で、事務部門は全組織に対する横断的な事務機能を果たすための事項に関する責任を持つ。

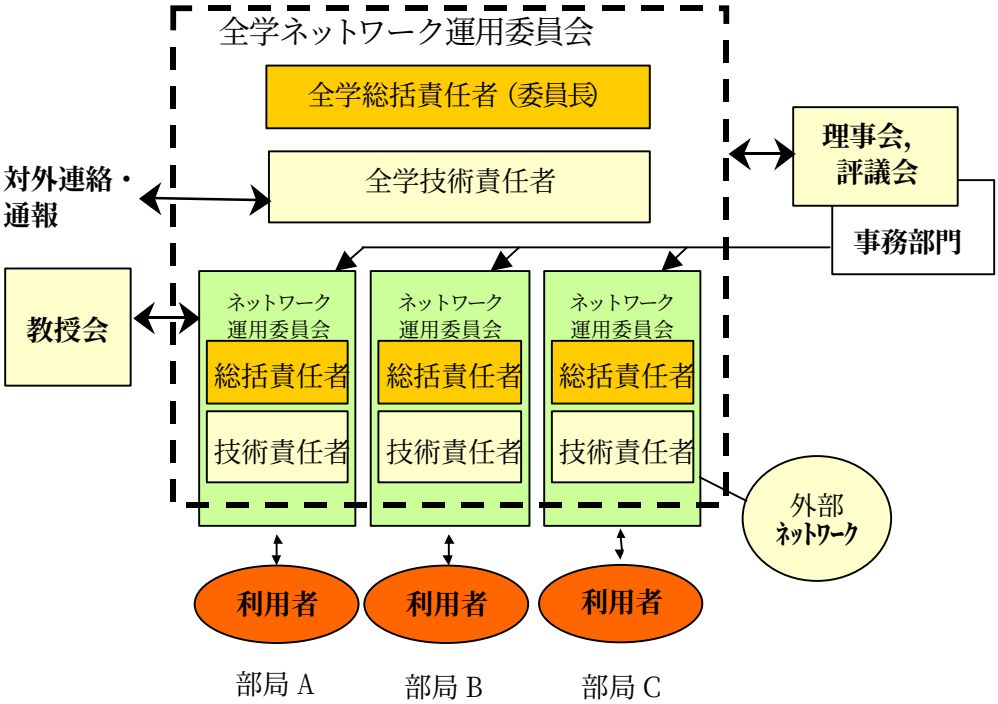

図３　ネットワーク運用管理体制

全学ネットワーク運用委員会では、全学的に定める必要のあるネットワーク運用のポリシー、情報セキュリティポリシー、対外的な対応方針等を検討するとともに規程類の審議を行う。したがって、本委員会の長（全学総括責任者）は、全学的に責任を持つ者として学長や副学長クラスの者が望ましい。本委員会の作業として、次のようなものが考えられる。

- ネットワークと教育研究活動との関係（利用ポリシー）、違反者への処罰ポリシー、情報セキュリティポリシーなどの制定を行う
- 処罰規程の策定方針（例えば、教授会で行うなど）の制定を行う
- 外部（例えば、外部からのクレームや損害賠償請求など）との折衝方針を検討する
- 内部の技術責任者、技術担当者への講習
- ネットワークの管理体制（通常は利用者の所属する組織）の単位と、実際のネットワークの運用単位を極力一致させる。複数学部で１つのサブネットワークを共有しているようなケースでは、共同して運用する体制をとる必要がある。

2.3 アウトソーシングの留意点

ネットワーク運用のアウトソーシングを行う場合は、学内者による責任体制とアウトソーシング事項（実務、権限）、連絡方法および責任事項を明確にしておく必要がある。また、アウトソーシングの契約方法（仕様を含む）を明確にしておく必要がある。

アウトソーシング事項の明確化については、まずネットワーク運用における業務を内容ごとに整理して、外部委託可能範囲を検討する必要がある。例えば、日常繰り返されるルーチン業務はアウトソーシングの対象としやすいが、利用規約違反者の処罰など、教授会や理事会の専管事項とされるものについてはアウトソーシングの対象とすることができない。アウトソーシングを行うことで外部業者に一定の権限および責任を委譲することになるが、全てを完全に委譲することはできないのである。

なお、アウトソーシングでは、トラブル発生時に臨機の対応ができないといった問題や、学内の個人情報や機密情報を完全には守り得ないといった問題も存在する。このような問題に対応するために、高等教育機関と委託業者との間にしっかりとしたパートナーシップを築き上げ、トラブルの発生に対応できる仕組みを整えることが必要となる。委託業者との間で信頼関係を醸成することが基本であるが、組織と目的にあった委託業者を選別することも重要となる。また、教育訓練を行うなど、高等教育機関自らが委託業者を育成する努力も必要である。

アウトソーシング契約においては、個人情報や機密情報の保護について、特に注意しなければならない。秘密保持契約の他に、システムの運用保守契約において、データの保管・管理・破棄の体制と基準を明確にするなど、契約に盛り込むべき内容を慎重に検討しておく必要がある。

また、委託業者のミスや、委託業者の責によらないトラブル等についても、事前の検討を要する。どの程度のミスやエラーならば許容できるか、ミスやエラーが発生したときにいかなる対応が可能であり、高等教育機関と委託業者の双方がそれぞれどの程度の責任を負担するのかを決めておく必要がある。例えば、情報セキュリティ管理業務を委託するなどの場合は、ミスやエラーが甚大な損害を招く可能性がある。損害発生の可能性を考え、あらかじめ保険に加入することも検討に値する。

3. ポリシーの策定

3.1 高等教育機関の使命とネットワークの特徴

ポリシーには、学内のネットワーク運用が高等教育機関にとって極めて重要なものであることが明示されるべきであり、また、ネットワーク運用は、それにふさわしい位置付けのなかに置かれなければならない。

高等教育機関においては、それぞれの学内組織の目的、組織体制や地理的条件、外部組織との関係や対外活動が多岐にわたる。そのため、ネットワーク運用も教育研究用、事務・経理用、特殊研究用、学生のサークル活動用などの用途、部局などの体制、キャンパスやビルなどの地理的状況などを考慮して情報の流通・制御・管理について明確に性格付けを行う必要がある。

3.2 ネットワーク運用の目標

(1) 教育目標の実現

高等教育機関におけるネットワーク運用は、法的な責任を明確にしておくことは当然のこととして、高度な人材教育機関としての教育的責任と社会的責任を果たす立場から十分考慮されたものでなければならない。

(2) 学問の自由･言論の自由市場

教育研究用のコンテンツについては､学問の自由および言論の自由が憲法上保証されており、それを最大限実現することが目標となる。

3.3 ネットワーク運用に際して配慮されるべき財産・権利等および法遵守

(1) ネットワーク運用における法遵守

社会的存在としての高等教育機関は、運用責任者としてネットワークサービスプロバイダおよびホスティングプロバイダ（特定電気通信役務提供者に相当）の立場にあり、法人としての社会的責任を負うことへの対応が予め盛り込まれている必要がある。また、後述するように情報セキュリティ管理などのための管理手法と個人の言論の自由･通信の秘密が衝突することがあり、その際は、法律および本ポリシーに定める原則･手順によって権利・利益間の調和が図られることになる。

ネットワークに関わる法律・制度について最新の情報を把握して、運用に活かせるようにしておく必要がある。現在までに制定されているインターネットに関わる法律には、民法や刑法などの基本法に加えて、不正アクセス禁止法、通信傍受法、サイバー犯罪条約、情報公開法、プロバイダ責任制限法、個人情報保護法案などがある（付録 C 参照）。

高等教育機関におけるネットワーク運用に関わる法的責任としては、後述するコンテンツに関連するもの以外に、利用者の通信の秘密に対する責任、利用者の個人情報管理に関する責任、情報セキュリティ管理に対する責任などがある。

(2) 通信の秘密・学問の自由・言論の自由

ネットワーク上を流通する情報・データに対する、機密性、公開性を利用目的に応じて明確にしておく必要がある。

メールは通信サービスであるため「信書、通信の秘密」原則から一般的には秘密の確保がなされなければならないが、情報セキュリティ上の問題が発生したときの解決手段などの条件によって秘密が侵される場合があれば、あらかじめ明確にしておく必要がある。

教育研究用のコンテンツについては、学問の自由および言論の自由が憲法上保証されていることが大原則となる。しかしながら、そのコンテンツにおいて、名誉棄損、信用毀損があれば、法的な責任が発生することとなる。また、著作権をはじめとして知的財産権を侵害する場合においても適切な手法によりそのコンテンツは､ネットワーク上から削除されるべきものとなる。そのために法的な枠組みおよびポリシーによって定められる個別の手続きが遵守されるようにしなければならない。

学生の行為に対する外部からのクレームへの対応は、ポリシーおよびそれによって展開される対処方針にしたがって処理されることになる。

3.4 情報セキュリティポリシーの確立

当該高等教育機関におけるネットワークのセキュリティが犯された場合やネットワーク上の情報の扱いに対する社会的責任を問われた場合の損害、信用失墜の経済的損失を推定評価し、情報セキュリティ対策にかける経費と人的パワーについて、全組織的な基本認識を作る必要がある。

ネットワークを構成するシステムや端末、およびネットワーク上を流通する情報の安全性と信頼性を確保するために、ネットワークの運用・管理および情報の管理において重視する事項を優先度とともに明確にした規程（情報セキュリティポリシー）をトップダウンで決定し、それに従って実行される明確な運用体制と管理体制を構築する必要がある。

安全性の確保と利便性の確保はトレードオフの関係にあるため、組織全体としてのポリシーに沿って、各部局における諸条件を考慮した細部の運用管理規程を階層的に作成する必要がある。さらに、内部規程の整備、運用管理体制に対して、専門機関による情報セキュリティ監査を受けるなどの方法で、定期的にチェックする体制が必要である。また、情報セキュリティ対策について十分な能力を有する人材を確保すること、またそれらの人材を組織内に有する場合は常に能力向上と最先端のセキュリティ情報を入手できるようにする施策が必要である。

4. 守られるべき財産や権利などについての考え方

4.1 ネットワークの資源

高等教育機関のネットワーク資源については、適正な使用によってこれが保護されなくてはならない。適正な利用のためには、許可された利用者のみがこれを利用でき、許可された利用形態のみが認められる。すなわち、許可された利用者が許可されない利用形態でネットワークを利用した時にはその利用は制限されるということである。例えば、商用目的でネットワークを使用したり、高等教育機関のネットワーク設備に対して過度の負荷、あるいは、他人がネットワーク設備を使用する際に不当な干渉を直接的、間接的に引き起こすことが当然予想される目的に使用したりしたときは、ネットワークの利用は制限されることになろう。

私的利用を認める場合であっても、私的利用の結果として生じたいかなる損失や損害についても高等教育機関は責任を負わないことも定めておくべきである。高等教育機関は、上記ネットワーク資源の妨害の恐れがなければ、法律に定める手続きによる場合を除き、私的利用を管理することはなく、対外的にも責任を負わないものとする考え方もある。一般に、高等教育機関は通信の内容に関しては関知できないし、関知する必要もない。高等教育機関は、利用者が受け取るかも知れない不快なメッセージから利用者を常に保護できるわけではない。

物理的資産としてのネットワークシステムやコンピュータシステムは、学校法人ないしは設立主体である国もしくは地方公共団体が所有または占有する財産である。これらの利用・管理・廃棄等については、別個の有体財産についての管理規則を適用することが妥当である場合が多いことに留意されるべきであろう。

4.2 情報セキュリティ

高等教育機関の管理するシステム内のデータの機密性、インテグリティ、可用性、およびそれらに対する信頼は保護されなければならない。高等教育機関は安全かつ信頼性の高いネットワークサービスを提供しようとしている。高等教育機関のネットワーク設備の運用者は、通信記録、データ、応用プログラムおよびシステムのセキュリティを提供する際には、運用者向けの規約に基づく権限の下で専門的な手法に従うことが期待されている。これらの事項を達成するために、次の項目に留意する必要がある。

(1) 情報セキュリティの保護

ネットワークの運用者は、他の条項によって別に認可されない限り、ネットワークサービスあるいは設備、あるいはこれらのサービスや設備により関連づけられるあらゆる記録やメッセ

ージを保護するために、高等教育機関の情報セキュリティ機構を破り、あるいは破ろうとしてはならない。

(2) 適切な情報セキュリティ機構の導入

高等教育機関のネットワークサービスの提供者は、例えばファイアウォール、認証技術、暗号化技術などを導入するものとする。ただし、他の規約等によって公開することが求められている情報は暗号化してはならない。

(3) 迅速な回復機構の実現

ネットワークに対する不正侵入や、攻撃によるサービスの中断を迅速に回復可能なように、適切な回復策を実現する必要がある。

(4) システムの監視

高等教育機関のネットワークサービスの提供者は、情報セキュリティを侵害した者を特定し、情報セキュリティ侵害からの迅速な回復を実現するために、費用対効果に優れた監視技術を実現・導入するものとする。そのような監視技術の利用は、他の条項、特にプライバシーの保護と矛盾するものであってはならない。

4.3 知的財産権など

高等教育機関のネットワーク上には種々の知的財産が存在する。例えば、画像データ、音楽データ、テキストファイル、コンピュータプログラム等は著作権法で保護され、コンピュータプログラムのロジックは特許で保護されるものもある。また、高等教育機関の名称やその他の名称には商標法で保護されているものもある。これら知的財産は、著作権法、特許法、商標法など知的財産法に基づいて保護されている。したがって、ネットワークに関連する知的財産権に関して、法律における定めに従わなければならない。すなわち、知的財産に関して自分のものと他人のもの、さらには高等教育機関のものを明確に認識して、他人のものを利用する時には許諾を得ることが原則である。中でも、著作権には著作者の人格を保護する著作者人格権があり、著作者に無断で著作物を改変することはできないので注意を要する。

自分で撮った写真であっても顔写真を Web 等に載せる時には、その被写体の肖像権に関する配慮が必要である。自分で撮った写真であれば、著作権の問題はないのであるが、その被写体となっている者に対して、使用目的等の許諾を得た上で利用しなければならない。また、芸能人などの顧客吸引力のある肖像であれば、パブリシティ権の許諾が必要となることにも留意が必要である。

知的財産権について、公正な利用(例えば、著作権法 30 条（私的使用のための複製）ないし 35 条（学校その他の教育機関における複製）に定める「著作権の制限」など)について、その範囲に関する疑念がある場合には、利用者は、ネットワーク運用委員会などに問い合わせることが望ましい。

各高等教育機関自体が有する知的財産権については、別途定める実施要領によって規定される。関係者は、この規約について熟知していなければならない。例えば、高等教育機関の名称や商標を利用するときには、ネットワーク運用委員会が定める実施要領に従って申請するといった方針を決めておくことが重要である。

4.4 個人情報の保護

高等教育機関のネットワークにおいて、個人情報は保護されなければならない。高等教育機関は、本ポリシーで規定される限定された条件を満たす場合以外には、個人の同意なしに、通信内容を定期的に検査したり、監視したり、公開したりしてはならない。

権限のない高等教育機関の職員や、ネットワークの管理者は、特定の個人情報を検索したり、利用したり、公開したりしてはならない。また、正当な職務中に偶然に知るかもしれない個人情報に関してもその秘密が保持されるように、職務規程その他を整備する必要がある。

コンピュータシステムにおいては、アクセスログ等、システムが自動的に収集する個人情報が存在する。どのような種類の情報が収集されており、それらがどのように利用される可能性があるかを事前に利用者に公開する必要がある。高等教育機関のネットワークサービスを外部業者に委託するような場合には、当該業者に対して、個人情報の保護に関して本ポリシーの内容を遵守するよう契約等に反映させるものとする。

(1) 保護されるべき個人情報の範囲

本ポリシーでは「個人情報」を「個人を特定することが可能な情報」として、例えば、個人情報保護法案等で規定されている定義に従う。具体的には、学籍情報（成績の情報を含む）、電子メールアドレス、その他、当該個人によって適切にアクセス保護が講じられているデータ、システムやアプリケーションが自動的に収集する個人を特定可能なデータ、および個人のアクセス履歴等に関するデータ（クッキー等）を指すものとする。

(2) 個人情報の利用

高等教育機関のネットワーク運用に関して、利用者の個人情報を利用する目的、およびその利用形態を特定して、利用者に明示しておくことが重要である。その上で、これらの目的の範囲内で個人情報を利用しなければならない。利用者に明示する利用目的として例えば、次のようなものが考えられる。

・教育・研究目的での利用
・高等教育機関のネットワークシステムの機能を保持するための検査・作業時に必要となる利用
（この場合にも個人情報の利用は最低限にとどめるとともに、作業者が知り得た情報の機密保持に関しても配慮が必要である。）
・システムを管理する者が、必要に応じて行う利用者情報のバックアップ
・本ポリシー、あるいは他の規程等によって、あらかじめ公開することが定められている情報

(3) 個人情報の目的外利用

上に示した個人情報の利用目的以外にも、法律に従って開示が求められたときや別に定める重要な理由が存在するとき、あるいは緊急を要する事態が発生したときなど、個人情報を利用し、または開示するケースがあることを利用者に明示しておくべきである。また、個人情報を目的外に利用する場合は、その手順を定めておくものとする。例えば、次の手順が考えられる。

- 緊急を要する事態を除き、事前に責任者が書面により認可する。
- 緊急を要する事態の場合には、事後に遅滞なく責任者に報告し、認可を受ける。
- 個人情報へアクセスした場合は、その理由と影響範囲を関係者に通知する。
- 個人情報へのアクセス行為が本ポリシーに違反していると考えられる場合、当該個人が調査を要求できるような機構を用意する。

5. ポリシーの実施

5.1 実施の責任者

ネットワーク運用ポリシーの発効とその実施に際して、発効の責任者、そのポリシーの作成権限・訂正権限を持つ者、およびそれらの手順が定められていなければならない。例えば、次の点をポリシーに明示しておくべきである。

(1) 発効
　本ポリシーは、○○大学の学長により発布される。全学ネットワーク運用委員会委員長は本ポリシーの維持に責任を持つものとする。
(2) 実施
　全学ネットワーク運用委員会委員長は、本ポリシーを実現する実施要領を策定し、これを維持する。これには、学生のアクセス情報、認可利用者、制限あるいは拒否されるアクセス、苦情処理、そのほかの事項、ポリシーと実施要領の作成等が含まれる。
(3) 情報資料
　大学は、ネットワークの利用者に、本ポリシーと実施要領を理解するための資料を提供する。

5.2 適用範囲

ポリシーの適用範囲を定めておく必要がある。例えば、次のようなものが考えられる。

- 高等教育機関によって所有、または管理されている全てのネットワーク
- 高等教育機関との契約、あるいは他の協定に従って、高等教育機関により提供される全てのネットワーク
- 高等教育機関のネットワークにおける全ての利用者と用途
- 高等教育機関により提供されたネットワークにおける教職員あるいは他の利用者が所有する全てのログ
- 通信内容と電気的な付属物、通信に付随する取引情報

本ポリシーは、原則としてシステムログのプリントアウト等の印刷物にも適用される。例えば、電子メールアドレスと学生の名前との一覧表は、今後、問題となる個人情報などに該当する場合もあると思われる。

5.3 例外規定

各高等教育機関においては、同窓会や生協等に対して、高等教育機関のネットワーク設備に対する利用を許容しているところも多いと思われる。そのような団体等は、高等教育機関から独立した存在ともいえるが、そのような団体に対しても原則としてポリシー等の適用範囲にあることを明らかにしておく必要がある。

6. ポリシーの評価および見直し

ポリシーは、策定、発効しただけでは絵に描いた餅と同じであり、適切に導入・運用されて初めて意味のあるものである。さらに、実際の運用上の問題点をポリシーに反映するために継続的に見直すことが重要である。この際、次の事項に留意しなければならないであろう。

- ポリシーは、日々の具体的な運用に密接に適合する、いわばカスタムメイドとして考えられるべきものであること。従って、当初から極めて高度なポリシーを策定することや、逆に一つの雛型を各高等教育機関の個性を考慮しないで適合させようとすると、運用が極めて困難となる可能性がある。
- まず、実態に即したポリシーを計画的に策定・運用し、その実施状況を踏まえて見直し、徐々に目標を達成するために、ネットワーク運用および管理に携わる者が、自ら運用ポリシーを立案・具体化・展開しようと試みることこそが重要である。
- 大規模災害等の緊急時、実施要領の手順にそぐわないことがある。このような時には、総括責任者の権限で処理し、事後で承認するなどの緊急手順も考慮すべきである。
- ポリシーと実施要領は、運用を通して遵守状況を確認するなど、図４に示すように評価・見直しを行い、それによってポリシーを改訂することを繰り返さなければならない。

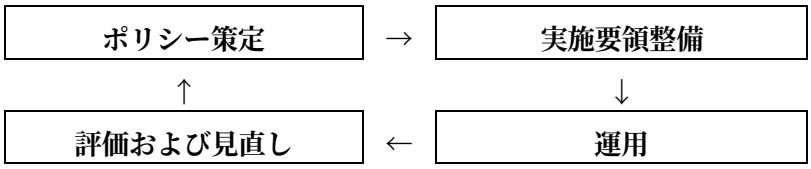

図 4　ポリシーの評価および見直し

7. 法的責任と学内処罰

(1) 法的責任

次にあげるような行為については関連する法律で禁止されており、刑事罰または、民事責任として損害賠償請求や差止め請求を受ける可能性がある。

- 不正アクセス
- データ妨害(データの毀損、消去、劣化、改変、抑制行為)
- システム妨害(データの入力、伝送、毀損、消去、改変等によるシステム機能への重大な妨害行為)
- 名誉毀損、侮辱
- 詐欺、窃盗
- 著作権、特許権、商標権等の知的財産権侵害
- わいせつ罪

(2) 高等教育機関による処罰

高等教育機関のポリシーは、不正な目的、あるいは高等教育機関の使命の実現にそぐわない目的による高等教育機関の財産の使用を禁止している。外的に加えられる法的処罰はもちろんであるが、ポリシーの違反者は、ポリシーと学則、就業規則等により、解雇あるいは退学を含む高等教育機関の懲罰を受ける可能性についても周知されるものとする。許可あるいは禁止されている利用に関する詳細は個別の実施要領によって詳述される。また、学生の違反に対しては教育的観点から総合的判断を要する場合があるため、教育組織として（例えば教授会における）一元的な判断基準に基づくものとする必要がある。

II　ネットワークの運用・管理に関するガイドライン

1. ネットワーク運用・管理の体制と役割

1.1 組織・体制

ネットワークを運用するにあたって、責任の所在と範囲を明確にするために、総括責任者と技術責任者とでネットワーク運用委員会を組織し、ポリシーおよび実施要領の策定を行う。技術責任者は、それらのポリシー・実施要領に従って実際のネットワークの運用・管理を行う。

技術責任者は、利用者教育や利用規約違反行為等の発見と対応の他に、情報セキュリティ対策やアカウント管理など技術的な問題に責任を持つ。なお、実際には技術責任者の担うべき役割は多岐にわたり、高度な専門知識や技術が必要となる場面も少なくないため、技術責任者の下に複数の技術担当者を置いて実務を担当させることが考えられる。

(1) 技術責任者

技術担当者を監督し、システムの運用状況や組織構成等について、総括責任者に適宜報告する。情報通信技術の高度化・複雑化とそれに伴う多種多様な問題発生の可能性に鑑みると、組織においては技術責任者に専任専従の人員を確保すること、およびそのために適切な予算を計上することが必須となる。円滑で安全なネットワーク運用には相当なコストがかかることを、組織として理解し対応することが肝要である。

また、ネットワーク運用が正常で安全に行われるのは当たり前という意識が働くと、技術責任者に対する評価が適切に行われないことも起こり得るため、技術責任者を適切に評価する仕組みが求められる。利用者との関係では、技術責任者に過度の責任が課せられることも多いので、技術責任者の地位の保証という点も考慮しなければならない。

(2) 技術担当者

技術責任者の監督の下、運用・管理の実質的作業に従事する。技術的な事柄に関しては、専門の外部業者に実際の作業をアウトソーシングすることも考えられる。その場合は契約によって責任範囲・守秘義務・損害賠償等を明確に定めておくことが必要である。また、学生がアルバイトやボランティアで技術担当者の職務を担当することは、業務範囲や責任範囲の規定において問題があるため、基本的に避けるべきと言える。

組織によっては、技術責任者と技術担当者を分離することが困難な場合（両者を一名の者が兼任するなど）もあろう。その場合でも、誰が誰に対してどのような責任を持ち、どのように運用・管理を行うのか。また、緊急時にどのような手続きで対応すべきかについて、事前にポリシー、実施要領および利用規約を詳細に定めておかなければならない。

また，ネットワーク管理者（総括責任者・技術責任者を含む）が賠償責任を負いかねない場合、それに対応する保険にも加入する必要性があろう。

1.2 技術責任者と技術担当者の役割と責任

技術責任者と技術担当者は運用・管理の実務を執り行うが、そこではポリシーを利用者に伝え、利用者からのフィードバックを総括責任者に返すパイプとしての役割が基本となる。このとき、技術責任者と技術担当者が総括責任者と利用者の中間に位置することから、両者の間で板挟みとなることのないよう十分な配慮が求められる。

なお、運用・管理における個別の事項別に、技術責任者と技術担当者の担う役割を示すと、概ね以下のようになる。それぞれについて具体的な問題は後述する。

・ アカウントの管理

技術責任者の責任において、利用資格の発行・削除・有効性の確認等を行う。技術担当者は、技術面において上記業務を補佐する。

・ 教育

利用者を対象とした情報リテラシー教育や情報倫理教育は、技術責任者がその役割を担うことが多い。技術責任者はネットワーク運用委員会の定める利用規約を利用者に周知徹底させ、技術担当者は上記業務を補佐する。

・ 技術的対応

技術責任者は、ネットワーク運用委員会の定めるポリシーや実施要領をもとに、具体的な技術的対応を検討し、指示する。技術担当者は、上記の技術的対応を実施する。

また、技術担当者はネットワークシステム（サーバと端末の両方を含む）の運用状況およびセキュリティ状態を把握し、技術責任者に定期的に報告する。技術責任者は、ポリシーや実施要領が適正に実施されるよう必要な措置を講じる。

・ 利用規約違反行為等の発見と対応

技術担当者は、規約違反行為に関する情報収集と技術責任者への報告を行う。報告を受けた技術責任者は、実施要領や対応マニュアルに従って措置し、その結果を総括責任者に報告する。ただし、コンテンツに関する規約違反行為については、総括責任者の判断のもとに対処するものとする。

情報セキュリティインシデントへの対応については、技術責任者は対応マニュアルに従った措置を指示し、技術担当者がこれを実施する。技術担当者が技術責任者の指示を得られない場合は、技術担当者が措置を行った後、技術責任者に報告することも考えられる。技術責任者は、措置の結果を総括責任者に報告すると共に、必要な範囲で処置の相手方（利用者であることもあり得る）にも報告を行う。情報セキュリティインシデント発生時の措置によっては、利用者や外部者の利益を損なう可能性もあるが、いかなる場合にいかなる措置がなされるか、いかなる場合を緊急と判定するかは、その判定方法も含めて、あらかじめ実施要領や対応マニュアルに定めておかなければならない。ここでは、技術責任者・技術担当者が、究極的な判断権限を有しないことに注意すべきである。

・ 連絡・通報窓口の設置

技術責任者の責任において、連絡・通報窓口を設置する。技術責任者・技術担当者間の連絡体制を明らかにしておく必要がある。

・ ネットワーク機器の物理的な管理

技術責任者の責任において、コンピュータ室やサーバ室の管理並びにネットワーク機器の物理的な管理を行う。

・ 資源管理

技術責任者の責任において、コンピュータの CPU 資源・ディスク資源・ネットワーク帯域資源などの管理を行う。技術担当者は、技術面において上記業務を補佐する。

・ ネットワーク情報の管理

技術責任者の責任において、ドメイン名や IP アドレスなどのネットワーク情報の割り当てならびに管理を行う。技術担当者は、技術面において上記業務を補佐する。ネットワーク情報の管理方法については、実施要領にあらかじめ明示しておくものとする。

・ 外部ネットワークとの接続の問題
　対外接続を担う部局においては、技術責任者は外部ネットワークとの接続に関わって生じる問題に対処する。技術担当者は、技術面において上記業務を補佐する。

技術責任者・技術担当者向けガイドラインを策定するにあたっては、それぞれの役割を明確にするとともに、それぞれが負うべき責任・義務についても併せて規定するようにする。その内容としては、概ね次のようなものが挙げられる。

・ 内部規約の遵守
・ 法令の遵守
・ 情報倫理の維持確保
・ 運用・管理上得られた個人情報の保護
・ ネットワーク構成等の物理的管理
・ 利用者教育に関わる責任
・ 技術担当者の監督責任（技術責任者）
・ 技術責任者に対する報告義務（技術担当者）
・ 守秘義務（技術担当者、アウトソーシングでは特に注意が必要）
・ 指示および契約の遵守（技術担当者、アウトソーシングでは特に注意が必要）

2. アカウントの管理

ネットワークおよびコンピュータ、システムの利用にあたっては、それぞれのサービスについて、利用しようとする者が利用資格および利用権限（以下「アカウント」という）を有していることが当然の前提となる。そのため、利用規約等において利用資格を明確に定めると共に、具体的な利用申請手続きについても明示しておくこととする。

> 利用資格の例：
> 　○○を利用できるのは、次のいずれかに該当する者とする。
> 　(1) 本学の構成員（学生および教職員）
> 　(2) その他総括責任者が認めた者
>
> 利用申請手続きの例：
> 　利用しようとする者は、別紙様式の申請書を総括責任者へ提出し、許可を得なければならない。

例えば大学で、学部や大学院への入学時に、新入生全員に大学の情報システムを利用するためのユーザ ID およびパスワードをいっせいに発行することも考えられる。このような場合に、正当な利用資格に基づくアカウントであることを啓発し、自覚させることが特に必要である。利用者が実際に利用を開始するより前に、利用者講習会や正課授業の中で適切な情報倫理教育を受講させ、利用規約のみならず、ネットワークの秩序を維持する上で必要なエチケットやルールを周知することが重要である。例えば、情報倫理教育を受け、一定の理解度に達して初めてアカウントが有効になるなどの手続きが考えられるが、実際は入学後すぐに電子メールによる連絡が必要となるなど、実際の運用とバランスを取りながら慎重に制度を組み立てていくことになるだろう。

なお、他人のアカウントを用いて情報システムを利用し、または利用させてはならない。一定の要件に該当した場合、不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）によって刑事罰の対象ともなる。

ネットワーク管理者（総括責任者、技術責任者、技術担当者を含む）は、システム上強力なアクセス権限を持っていたとしても、他人のアカウントに属する情報に必要以上にアクセスしてはならない。システム障害やシステム侵害に対する防御措置として、あるいはバックアップ等運用・管理上必要な限度においてアクセスせざるを得ない場合は、実施要領等において想定される事例を列挙し、利用者に事前に周知することが望ましい。

ネットワーク管理者は、アカウント発行後も、定期的にアカウントの有効性を確認し、利用されていないアカウントについて照会を求めたり、不審なアカウントや不審な利用形跡があれば、調査の上アカウントを削除したりシステムの再インストールを行ったりするなどの対応を取ることとなる。

アカウントの削除については、やはり利用規約等において廃止手続きを明示しておくべきであるが、アカウントが不要になったからといって、わざわざ申請して来ないといった問題もある。学生の卒業や教職員の異動に伴って削除することが多いので、ネットワーク管理者が、それらの情報を把握できるよう、教務課や人事課などの事務組織との連携が重要となる。アカウントの有効期限をあらかじめ定めておき、期限満了後更新手続きを経ない者に対して自動的にアカウントを削除するなどの対応をすることが望ましい。

アカウント管理を外部業者にアウトソーシングしている場合は、利用者名簿や電子メールアドレスなどの個人情報の取り扱いに関しては、特に注意が必要である。契約の変更により業者が変わることもあり得るので、そのような事態にも対応できなければならない。

3. 教育

ネットワークを安全かつ円滑に運用していくためには、ネットワークを利用するすべての者に対して、適切な教育が行われなければならない。運用・管理の場面では、ポリシーや実施要領、利用規約等をトップダウンで利用者に伝えることが重要であり、技術責任者・技術担当者が負うべき役割を、実施要領等であらかじめ明確にしておくことが必要である。

また、それと同時に、技術責任者・技術担当者に対しては、その職責に応じた教育が行われるべきであり、そのための体制づくりや教育プログラムの整備が必要となる。教育と倫理に関する諸問題については、「IV 教育・倫理に関する事項」を参照されたい。

4. 技術的対応

分散ネットワークとして発達したインターネットは、オープンであるが故の利便性と、セキュリティ上の弱点を持つ。クラッカーと呼ばれる者たちがセキュリティの弱点を突いて、インターネットに接続されているコンピュータに不正侵入を試みたり、そこに蓄積されたデータを盗み出し、あるいは改ざんするといった事件が頻繁に起きている。ネットワークをめぐる問題は、単なる社会の縮図である場合とネットワークであるが故の問題とに分けることができるが、後者は技術的対応（とそれに関する教育）が有効であることが多い。技術的対応によって外形的に違法あるいは有害なアクセスを遮断し、組織外部からの攻撃だけでなく組織内部からの攻撃を未然に防ぐことが、利用者を守り安全なネットワーク運用を実現するために必要である。

情報セキュリティに関しては、定められた情報セキュリティポリシーを基にして、実際の対応について計画・構築・運用・分析のサイクルを繰り返し、日々新しく生じる問題や事情の変化に応じて情報セキュリティポリシーを修正するといった継続的な努力が重要となる。高い品質の情報セキュリティの実現は、このサイクルをうまく動作させることに外ならないが、以下のようなシステム上の対策と運用上の対策に大きく依存する。

4.1 ファイアウォールによる防御

技術的対策として一般にとられるのが、ファイアウォールの導入である。ファイアウォールは組織の内外を分断し、不要あるいは不正な情報をフィルタリングするといった考え方を指すものであり、機器や製品を単に設置するだけで防御できるものではない。

ファイアウォールの位置は、組織全体の情報セキュリティポリシー、ネットワーク・サーバ類の設置形態と部局組織の関係､用途などを考慮して緻密な計画に基づいて定める必要がある。

4.2 ネットワーク侵入検知システム（IDS）による監視

IDS はファイアウォールの一機能として実装されることが多い｡ネットワークを常時監視し、既知のセキュリティホールへの攻撃など適切でない特定の通信パターン見つけ、それを阻止する。システム方式、検知方式を知り、効果の限度について理解しておく必要がある。

4.3 サーバのセキュリティ強化

一定水準の情報セキュリティを確保してサーバを設定しようとする場合、情報処理振興事業協会のセキュリティ対策セルフチェックシート(1)が参考になる。さらに CERT/CC などが発行するセキュリティ情報に常に留意し、パッチ当てなど対策を迅速に行えるように体制を整える必要がある。

4.4 認証技術・暗号技術の導入

モバイル端末や DHCP 用コンセントなどに関しては、管理上、情報発信者たる個人が特定できるように、何らかの認証機構を取り入れておく必要がある。

認証や暗号の技術を導入する際は、まず鍵の管理のルールを定めることが必要である。次にそれらをどこに集めるかについて、および総括責任者による管理の可否について検討する。また、どの認証システムを利用するかに関しても併せて検討すべきである。

4.5 ログの管理

不正行為の解明は、ログの解析が鍵となることが多いが、個人情報を含むことやコンピュータ資源の観点から、ネットワーク管理者のみが参照できるようなアクセス権の設定、および保存期間と消去方法の規程を定めておくことが必要である。システムログを記録する際の留意点については後述する。

4.6 バックアップ

システム、個人領域を問わず、安全のために定期的な差分もしくはフルバックアップが必要である。規模や回数によっては省力化とともに、確実なバックアップを実施するためにテープロボットの利用なども検討することが望ましい。バックアップファイルの検証、バックアップ装置のクリーニング、バックアップメディアの寿命などにも留意することが必要である。

4.7 システム監査

定期的にシステムの監査を行うことによりシステムのセキュリティレベルを保つ。外部委託もしくは内部監査の方法が考えられるが、早急に監査方法の確立が必要である。

4.8 ネットワークおよびシステムの設計

ネットワークを設計し構築する際は、将来起こり得るネットワークおよびシステム障害に備えて、多重構成を考慮し、そのための予算を確保するべきである。電源、電源系（AC ライン

(1) セキュリティ対策セルフチェックシート
http://www.ipa.go.jp/security/ciadr/checksheet.html

そのもの)、機器、ネットワーク配線、対外接続組織（プロバイダなども含む）などの二重化などを考慮する。

また、利用者や下位ネットワークの希望および現実の将来構想（定員増、コンピュータ教室の設置予定など）と、ネットワークの状態推移とから、機器、対外接続速度、サーバなどの将来構想を立てる。特に、機器は耐用年数や予算周期から早めにリプレース計画を立てる必要がある。また、IPv6 への移行、VoIP の実装など、近い将来予測されることは事前の検討を要する。

4.9 ネットワークおよびシステムの保守・管理

保守・管理に関しては、次の点について対処しておくことが重要である[2]。

- 導入時に保守に関わる予算を確保する
- ネットワークメンテナンスに伴う運用停止などは、ユーザおよび下位接続ネットワークに早めに告知を出す。また、その際、ユーザ・下位ネットワークの授業・重要業務等を避けるように注意すべきである
- トラブル発生時の緊急連絡方法を確保しておく
- 最低一人の技術担当者はモバイル常時接続などで確実にシステムにログインできる環境を確保しておく

また、予想されるトラブルにはあらかじめできるだけの対処をしておく。無停電装置の設置や、ユーザ ID、初期パスワードには数字の 1 と英字の l など間違えやすい文字を含めないというような、機械的、運用的トラブルに対しての対処を事前に実行しておく。

5. 利用規約違反行為等の発見と対応

5.1 利用規約違反行為等の分類

利用規約違反行為の内容とその対処方針は、明確に規定されている必要がある。何が利用規約違反に該当するかを明確にし、利用者の予見性を高めることによりネットワークの適切な利用が促進されるからである。

利用規約違反行為を大別すると、次のようなものがある。

(1) ネットワークを利用した情報発信内容（以下「コンテンツ」という）が利用規約違反（著作権侵害等違法行為も含む）である行為
(2) 権限無くシステムにアクセスし、あるいはウイルスを意図的に頒布することにより、データを改ざんしたり消失させたりして、ネットワークやシステムの稼動を妨害する行為
(3) 利用行為の形態自体には問題はないが、ネットワークの帯域やディスクや CPU の資源を浪費するなど、システムや他の利用者の迷惑となる行為

その他、利用者による行為であって、外部ネットワークにおけるあるいは外部のシステムに対して行われる違法な行為や、利用者によらない行為であって、外部のネットワークから内部に向かって行われる違法な行為などがある。

利用規約違反や学外から学内への攻撃行為への対応については、あらかじめ実施要領や対応マニュアルに具体的な手順を明記しておかなければならない。付録 A に「利用規約違反行為への対応モデル」を示すが、各高等教育機関においては、それぞれの実情に即して対応手順を個別に定めることになるだろう。具体的な対応については、前述の通りコンテンツにかかわる問題とセキュリティにかかわる問題とで分けて考えることに注意が必要である。

---

[2] 次世代デジタル応用基盤技術開発事業「セキュリティ運用ガイドライン実地適用研究」平成 12 年 3 月情報処理振興事業協会
http://www.ipa.go.jp/security/fy11/report/contents/intrusion/security-guideline/guideline_report.pdf

なお、ネットワークをめぐる問題は多種多様であり、すべての対応を網羅的に定めることは難しいかもしれない。ポリシーの見直しが行われる際は、利用規約違反行為等への対応についても、実際の運用経験を反映させた見直しが行われるべきである。

5.2 コンテンツ問題とセキュリティ問題の切り分け

利用規約違反行為にあたる行為については、①電子掲示板での名誉毀損、他人の著作物の違法コピー、データやプログラムの不正公開、わいせつ画像の公開、ネットワークを利用したねずみ講など、通信の内容すなわちネットワーク上のコンテンツをめぐる問題と、②スパムメール、コンピュータウイルスの発信、不正アクセス、DoS 攻撃、P2P ソフトウェアの利用等のように、ネットワークやシステムの機能を妨害したりリソースを浪費したりといった技術的セキュリティに関する問題の二通りが存在する。

コンテンツに関わって生じる問題については、慎重な法的判断を要することが多く、また通信の秘密あるいはプライバシー保護の観点から、技術責任者と技術担当者が立ち入ることが適当でない場合が少なくないため、技術責任者がコンテンツ問題と信じた場合は、総括責任者に一次判断を求めるものとする。一方、情報セキュリティに関する問題については、利用規約違反の判断が比較的容易であること、被害の拡大防止のために緊急の技術的対応が必要となる場合も少なくないことなどから、技術責任者と技術担当者の一次判断が重要となる。

5.3 コンテンツ監視の原則禁止

コンテンツに基づく利用規約違反行為については、外部からのクレームによって技術責任者がその事実を認知しあるいは自ら発見してはじめて対応を開始することが原則である。利用者によって行われる情報発信行為の内容については、通信の秘密や表現の自由を守る観点から、利用者の承諾なく監視を行ってはならない。ネットワークを運用・管理する側に常時監視義務がないことは、判例法上も認められるところである。

総括責任者は、情報発信内容について利用者による承諾のない監視（システムによる記録を含む）が行われることのないよう、技術責任者や技術担当者を指導するものとする。

5.4 セキュリティ対応としてのシステムログの記録

学外から学内へのあるいは学内から学外へのネットワークやシステムのアクセスについては、システムログ等を設定した上でそれを記録し、一定期間保存することがある。システムログの取得・保存については、利用者のプライバシーとの関係がしばしば問題となる。しかし、システムログを全く記録しないことが最良の方法とは言えない。システムログを記録し解析することは、システムの安定稼動に不可欠であり、不正アクセス等によるネットワークやシステムおよびシステム内の情報への被害を未然に防ぐことにもつながるからである。また、問題が起こったときの原因究明にも役立ち、アクセスが正当であることあるいは不正であることの論拠となり、更には管理責任を果たしたことの証明にもなる。このようにシステムログの記録は、ネットワークを適正かつ円滑に運用するためには不可欠のものであると言ってよい。

ただし、利用者のプライバシーが損なわれることのないよう、以下の点に特に留意し、必要な事項は実施要領や利用規約等にあらかじめ明記し、利用者に周知しておくこととする。

(1) 記録の目的をあらかじめ明確にしておく。システムログの利用は、利用者の同意がある場合、法令に基づく場合を除いては、明確化された目的以外に行われるべきでない。
(2) 記録の範囲をあらかじめ明確にしておく。システムログの取得は、適法かつ公正な手段によって収集されなければならない。場合によっては、利用者にあらかじめ通知または同意を得てから収集を行うこと。
(3) 保存されるシステムログは、適切に保護され、粉失・無権限アクセス・破壊・改ざん・開示等の危険から守られなければならない。

(4) 利用者のメール等、通信の秘密に関する情報や、非公開とされる情報については、システムバックアップ等に不可欠である場合を除いては、本人の同意なしに記録を行わない。
(5) 取得したシステムログは、所定の保存期間を経過した後、完全かつ速やかに破棄されなければならない。
(6) ネットワーク管理者は、システムログの取り扱いによって業務上知り得た利用者の秘密を守らなければならない。システムログの取得・保存を含むシステム管理をアウトソーシングするなどして外部業者のアクセスが可能である場合は、外部業者との間で秘密保持契約を結ぶなど、秘密の保持に特に留意すること。

6.連絡・通報窓口の設置

問題発生時の対処を迅速・確実に行うためネットワーク運用と利用の問題についての学外・学内の連絡・通報窓口を設定しておくことが必要である。

連絡窓口は部署別あるいは機能別に複数設置してもよいが、問題の切り分けの実施が効率的にできるのであれば、一箇所に集中して設け、関連部門の技術責任者や担当者等、学内の担当者への連絡網を整備し情報を配布することでもよい。メーリングリストのアドレスあるいは自動転送をして関係者で同時に情報共有をすることなども考えられるが、一時対応する責任者を明確にしておく必要がある。

7. ネットワーク機器の物理的な管理

利用権限を持たない者には、コンピュータおよびネットワークを使用させない。コンピュータ室（端末室）やサーバ室を施錠して、ID 認証を行わないと入室できないような入退室管理の仕組みを作ることが考えられる。また、機器の盗難・毀損やネットワークケーブルの切断など、物理的な破壊行為によってネットワーク利用が妨げられることもあり得る。

現在、ネットワークは高等教育機関の研究教育に不可欠な存在となっており、機器の物理的な管理がおろそかであってはならない。

また、キャンパス内に情報コンセントや無線 LAN などのアクセスポイントを備える組織もあるが、それらを発信源として違法情報や有害情報が発信されることもあり得る。利用者認証が必要であることは前述の通りであるが、学外への通信を制限する、講義・演習など必要なとき以外は利用させないなどの対応も必要であろう。

学内の電話回線あるいは携帯電話を使って学外にダイアルアップで接続し、学内ネットワークと外部ネットワークを無断で接続するような利用も許されない。同様に、VPN を構築することも、許諾条件とすべきである。ただし、機器の物理的な管理にはどうしても限界があるため、実施要領や利用規約等に禁止事項を明記しておくことも必要となるだろう。

8. 資源管理

ここにいう資源とは、コンピュータの CPU 資源・ディスク資源・ネットワーク帯域資源などを指す。これらの資源は一般に有限であるため、利用者の利用に応じて資源を適切に分配することになる。

例えば、大規模計算を行うために利用者の少ない夜間に複数のコンピュータを並列計算に用いたり、ネットワークによる遠隔講義のために一定範囲のネットワーク帯域を割り当てたりすることなどが考えられる。また、ある特定の利用者が大量の資源を占用している場合やプログラムのエラーによりほとんどの資源が使い尽くされている場合も考えられるので、このような場合の対応についてもあらかじめ検討しておく必要がある。

9.ネットワーク情報の管理

ドメイン名や IP アドレスなどのネットワーク情報に関しては、ネットワークの運用の単位ごとに一元的に管理を行う必要がある。そのための窓口を設置し、申請や廃止の手続きを明らかにするとともに、ネットワーク情報の不正利用・無許可利用についての対応手順を定めなければならない。

10. 外部ネットワークとの接続の問題

自組織のネットワークと接続される上流ネットワークの利用規約（上位 AUP という）に抵触しないように、自組織のネットワーク構成や利用規約を設計し運用する必要がある。

外部ネットワークとの接続は、原則として組織の長の権限と責任において行われるが、キャンパスネットワークにおいては、全学ネットワーク運用委員会が果たす役割が大きい。上流ネットワークとの整合性を維持し、円滑で安全なネットワーク接続を提供するとともに、学内でサブドメイン・サブサブドメインなどネットワークを細分化するときには、全学の利用規約と部局の利用規約に矛盾が生じないように指導する必要がある。

技術責任者・技術担当者に期待される役割としては、上位 AUP を利用者に周知させ遵守させること、上流ネットワークに迷惑をかける通信を行わせないようにすることなどがある。ネットワークの持つ互助的な特質を理解し、慎重に行動することが求められる。

III ネットワークの利用に関するガイドライン

1. ネットワークの利用

高等教育機関のネットワークは、利用者に対してネットワークサービスを提供するものであるが、そのサービスには技術的、法的な制約から限度がある。一方、利用者にとってもそのサービスを受けるにあたって守らなければならないルールがある。高等教育機関は、ネットワークの目的やサービスの範囲を明確にしてそれを利用者に告知し、その上で利用者が守るべきルールを明示しなければならない。

1.1 ネットワークの目的

高等教育機関においてネットワークサービスを提供する目的をポリシー上で明確にし、それを利用者に対して明示する。例えば、次のような例が考えられる。

「大学のネットワークは、大学あるいはその下部組織によって、大学の教育、研究および管理機能の基盤として提供されるものである。」

1.2 サービスの範囲

ポリシーに定めた目的に照らして、利用者に提供するサービスの範囲と高等教育機関の責任を明確にし、それを利用者に告知しておかなければならない。例えば、商用利用や私的な利用に関してどのような範囲で許可するのか、利用上のトラブルに関する責任などを明確にしておくことが望ましい。

1.2.1 商用利用の許諾範囲

ネットワークの商用利用をどの程度認めるのか明確にしなければならない。商用利用に関して次に例を紹介する。

「大学のネットワーク設備は、承認された場合を除き、商用利用に提供されるものではない。」

この例は、高等教育機関におけるネットワークの商用利用を一切禁止するものではない。高等教育機関においては、企業との共同研究や学生の起業のための利用が考えられる。このような利用をどのようにとらえるかは各高等教育機関の個性によるものと考えられる。ただし、日本においては、高等教育機関が利用しているネットワークによって制限を受ける場合もあるし、また、高等教育機関のスタンスや国公立大学特有の規制の可能性があることにも留意が必要であろう。

1.2.2 私的な利用の許諾範囲

ネットワークの私的な利用についてもそれを認めるのか否かを明確にする。もし、私的な使用を認めるのであれば、その通信内容について通信の秘密やプライバシーの権利を守らなければはならない。この場合であっても、データのバックアップやトラブル時の調査といったネットワーク運用上必要最小限のアクセスは、高等教育機関の権利として留保しておかなくてはならない。ここで、トラブルとは、技術的なドラブルだけではなく、法的なトラブル、セキュリティ上のトラブルが含まれる点も考慮しなくてはならない。

米国の大学には「大学は、電子メールの内容を統制することに興味はないが、電子メールのプライバシーや秘匿性は保証できない。」として、「基本的にはすべてのメッセージは公的なものとみなされ、大学は常に電子メールを監視しているわけではないが、大学のポリシー、法の侵害、安全性の侵害が行われていると考えられる時には大学は権利として通信内容をモニターする。それゆえ公的でないメッセージを含むような電子メールを送信しないことを大学は勧める。」というポリシーを掲げている例もある。

逆に、「大学は、法的な措置以外では利用者の同意無しでは定期的な調査、監視、電子メールの公開は行わない。」とし、「緊急の場合でも、事後の承認、大学のとった措置とその理由を個人に必ず通知する」としている大学もある。

この運用ポリシーは、ネットワークを運用する側の権利とそのネットワークを利用する側の権利をどのようにバランスさせるかという問題であり、慎重に検討するのが望ましい。

1.2.3 免責

ネットワークの運用時間や停止時期を事前に利用者に通知しておかなければならない。システムの保守や工事など、やむを得ないサービス停止による利用者の不利益について高等教育機関は責任を負わないこと、緊急を要する時には事前の通知なしに停止することなどを利用者に明示すべきである。さらに、ネットワークのサービスそのものを廃止する時の責任についても言及するのが望ましい。

また、利用者がネットワークを利用する行為は、自己責任を原則とする。すなわち、利用者がネットワークを利用したことにより被った損害、または、利用者が第三者に与えた損害については、高等教育機関は一切の責任を負わず、利用者本人の責任において解決する旨明示しておく必要がある。

1.3 利用資格

ネットワークの利用者は、利用資格を得た学生、教員、職員、および他の高等教育機関の提携者(高等教育機関と関係のあるプログラム、契約、ライセンスにおける提携を含む)を指し、ネットワークの経路選択プロトコルの結果として単に高等教育機関の設備を通過するだけにすぎない通信を行うような利用者は、本ポリシーの目的にいう利用者とは言わない。

このような利用資格を得るためには、単に学生や教員といった身分だけではなく、ネットワークを利用する能力を有しているかが大切である。従って、後に述べるようなネットワーク利用に関する教育を受講することによって資格を与えるという方法もある。

また、学生、教員、職員、訪問者など利用者の区分ごとに利用資格の付与条件、終了条件についても明確にすべきである。

1.4 個人情報の保護

高等教育機関のネットワークの中には、利用者のアカウント、氏名、電子メールアドレス等様々の個人情報が存在する。ネットワークを運用管理する者は、このような個人情報の利用目的を明確にし、その目的を利用者に明示しなければならない。その上で、これらの個人情報を利用するときには、利用者に明示した利用目的の範囲で利用することとする。また、利用者の個人情報について変更や疑義がある場合の連絡先も明示しておかなければならない。

例えば、次のような利用目的が考えられる。

「大学のネットワークを利用するためのアカウント、氏名、電子メールアドレス等の個人情報は、ネットワークの運用および管理のために利用することとし、他の目的で使用する時には当該利用者の事前の承諾を得る。」

ただし、次のような場合については、事前の承諾なしに利用することがあることを告知しておく必要がある。

- 法的義務の履行のために必要な場合
- 情報主体の生命、健康、財産等の重大な利益を保護するために必要な場合であって、本人の同意を得ることが困難な場合
- 法あるいは高等教育機関のポリシーに対する違反が行われていると信じられる具体的な理由がある場合
- その他法令で認められる場合(情報公開法の関係で開示が必要になることも考えられる)

1.5 制裁手続き

高等教育機関のポリシーや実施要領に違反した場合、適切な手続きのもとにネットワークの利用停止や学生規則、就業規則に定める処罰の対象になることを明示する。また、著作権侵害や不正アクセス禁止法違反など違法な行為に対しては、刑事罰や民事責任としての損害賠償、差止め請求の対象になることも告知すべきである。

また、学生の違反に対しては教育的観点から総合的判断を要する場合があるため、教育組織として（例えば教授会における）一元的な判断基準に基づくものとする必要がある。

2. ネットワーク利用の禁止事項および利用の制限

ネットワーク利用の禁止事項および利用の制限について、利用規約に明文化しておく必要がある。利用規約は利用者が常に参照可能な形で一元的に公開され、また状況に応じて修正可能なようにしておくべきである。

利用者はこれら最新のネットワーク利用の禁止事項・利用の制限を知っておく必要があるため、上記利用規約および告知を常に参照する義務を負うこととすべきである。

2.1 禁止事項

一般的な禁止事項として以下のような例が考えられる。

(1) 国内の法律に反する行為
(2) 利用者個人が利用しうる情報以外の情報を改ざんまたは消去する行為
(3) 有害なコンピュータプログラム等を送信または書き込む行為
(4) 他の利用者のユーザ ID およびパスワードを不正に使用する行為
(5) システムの不正な利用を助ける行為
(6) 自らのユーザ ID およびパスワードを、第三者に使用させる行為
(7) 知的財産権を侵害する行為
(8) 他者を誹謗中傷しまたは名誉もしくは信用を傷つけるような行為
(9) 他者の財産またはプライバシー等を侵害する行為
(10) 詐欺等の犯罪に結びつく行為
(11) 無限連鎖講を開設し、またはこれを勧誘する行為
(12) 他者に対し無断で広告、宣伝、勧誘等の電子メールを送信する行為
(13) 他者が嫌悪感を抱くメールを送信する行為
(14) わいせつ等不適当な内容の画像、文書等を送信する行為
(15) 他者の設備等または本サービス設備の利用または運営に支障を与える行為
(16) 故意に事実に反する情報、意味のない情報を送信する行為
(17) その他法令に違反しまたは公序良俗に反する行為
(18) その他本システムの運営を妨げるような行為
(19) その他各号に該当するおそれのある行為またはこれに類する行為

組織で特異的に定められるような禁止事項に関しては、きちんと明文化し利用規約に記す必要がある。上位 AUP に依存するような禁止事項に関しては、その内容を利用規約に明文化するか、上位 AUP へのポインタを用意するとともに、利用者が必ず上位 AUP を参照するように利用規約に定める必要がある。

2.2 利用者に責のないネットワーク利用の制限の告知

利用者に責のない、ネットワーク利用の制限がおきる可能性がある場合、その日時・理由などの情報が、明らかになり次第、すみやかに利用者に告知される必要がある。このためには周知された特定の場所にこれらの情報が一元的に開示されるようになっていることが必要であ

る。ネットワークの利用の制限があった場合、利用者がその情報を知らないと不利益を被るが、しかし利用者が能動的にこれらの情報を確認する義務をおう。

これら制限の例としては以下のようなものが考えられる。

・電気設備法定点検など停電に伴うネットワークの停止
・ネットワーク機器・設備工事に伴うネットワークの停止
・上流 ISP のネットワークの停止に伴うネットワーク停止
・国内外の電気通信事業者等が定める契約約款等によるネットワークの利用の制限
・入試などによる入構(校)制限にともなう学内端末への物理的アクセス制限

2.3 加害者・被害者にならないために

利用者は、犯罪、故意もしくは過失にかかわらず自分が加害者とならないように十分留意する必要がある。また利用者は、利用規約に禁止事項として記されるような事象を引き起こした場合、ネットワークの利用が制限されることを知っておく必要がある。たとえばウイルスに感染したパソコンが対処されるまで一時的にネットワークから切り離されたり、ネットワーク資源を占有するような共用計算機上のプログラムが停止させられたりすることである。場合によっては「1.5 制裁手続き」を経たネットワーク利用の制限もあり得ることを知っておく。

利用者は同様に被害者にもならないようにつとめなければならない。現在では ID・パスワードを書いた紙を置き忘れ、結果として第三者に使用されることになったり、メールソフトの適切な設定を怠るなどで、メール経由型のウイルスに感染し、結果、ウイルスをさらに送信して拡散させる立場に陥るなど、被害者であると同時に加害者となる場合がある。

これらに対処するためには利用者が教育をうけることが必要である。ネットワークセキュリティ、ネットワーク関連法規や情報倫理に関しての教育を通して、危険の可能性とそれに対する防御や対処を学び、適切な行動をとることができるようになる。これらは義務であると共に、自らを守ることができることを利用者は知る必要がある。

IV　教育・倫理に関する事項

1. 情報倫理教育の目的

ネットワークの円滑な運用のために作成されたポリシーや実施要領の内容を、関係者に周知徹底するという観点から、ネットワークの秩序を維持する重要な「情報モラル」を身につけることが、情報倫理教育の第一の目的となる。ここで「情報モラル」とは、情報社会で適正な活動を行うための基礎となる考え方と態度とを言う。すなわち、日常生活上のモラルに加えて、コンピュータやネットワークなどの情報技術の特性と、情報技術の利用によって文化的・社会的なコミュニケーションの範囲や深度などが変化する特性を踏まえて、適正な活動を行うための考え方と態度をさすものである。

高等教育機関における情報倫理教育は、その学問的性格に着眼するならば、情報モラルの育成という目的のみにとどまるものではない。ポリシーや利用規約において「遵守すべし」とされている倫理原則や倫理的態度そのものを多角的な視点から捉える学問的・批判的態度を養うことも、情報倫理教育の重要な目標である。従って、ネットワーク運用のためのポリシーや実施要領を作成する担当者は、ネットワークを活用する際に既存の価値として「遵守すべき善」とされている行為規範を身に付けさせることに偏ることのないように、配慮することが求められる。すなわち、学部カリキュラムにおける情報倫理教育との連続性、関連性を意識しつつ、ポリシーの策定・運用に取り組むことが望ましい。

2. 情報倫理教育の基本的な方向性

2.1 「情報モラルの育成」としての情報倫理教育

前述のように､ネットワークの円滑な運営と秩序を維持するという観点からするならば､「情報モラル」の育成ということが、情報倫理教育の当面の目標となる。ポリシーや利用規約は、既存のネットワークシステムの秩序を維持し、すべての利用者がネットワーク社会の中で「快適に」過ごすための最低限のルールや、エチケットを明記してあるものである。その意味においては、ネットワーク運用に関連する「倫理教育」は、いわゆるネチケットを代表とするような「情報モラル」を育成することが出発点になる。

「情報モラルの育成」といっても、それがポリシーや利用規約を遵守する倫理的態度を育成するという目的のみに集中してしまうと、利用規約の中で前提とされている倫理的価値を「身につけさせる」ことに目を奪われ、その価値観を学生に「押し付ける」だけになる危険性があることには注意すべきである｡こうした既存の価値観を押し付けるような｢刷り込み｣型では、情報モラルを育成するという目的は達成されないと思われる。特に、新入生ガイダンスのような大規模な講習会などでは、ポリシーや利用規約の内容を、時間的な制約などから、文書で配布するといった「一方的な申し伝え」に終わってしまうのが実情であるが、「情報モラル」を周知徹底するためには、「ID やパスワードの管理を徹底する」とだけ申し伝えるのではなく、なぜそれが重要なのか、事例(「なりすまし」による被害例など)をあげて、学生に討論させるなどして自分で考えさせるように指導することが望ましい。ただし、それを新入生ガイダンス等で行うことは時間的な制約から難しいので、学部教育の初期段階に情報処理関連の必修科目の中に事例教育を位置付けることによって、ガイダンス内容の周知徹底を具体化し、「情報モラル教育」の継続的実施を行うことが望ましい。

（「付録 B. 教育カリキュラム」を参照）

2.2 「情報倫理」としての教育

情報倫理教育には、もうひとつ大切な側面がある。それは、特定の前提された価値観を「教

える」のではなく、その価値観そのものを問い直し、道徳的推論に基づいた倫理的な価値判断ができるように、倫理的意思決定の能力を育成することを目的とする点である。

こうした倫理的意思決定の能力育成を目的とする倫理教育には、具体的なケースに基づいた事例教育を導入することが、より一層重要になってくる。こうした情報倫理教育は、学部教育の後半に位置付け、倫理教育の段階的・体系的位置付けを意識しつつ、ネットワーク運用のためのポリシーや利用規約の遵守教育としての「情報モラル教育」を実施することが重要である。

（「付録 B. 教育カリキュラム」を参照）

2.3 高等教育機関の教育理念や規模との関係

ネットワークの利用規約を制定する際には、個々の高等教育機関の教育理念や設置基準などに関する違いを考慮する必要がある。特に設置基準については、国公立か私立か、総合大学か単科大学か高等専門学校か、また、情報系学部(学科)か否かに依存するところがある。

例えば、国立の高等教育機関では基本的に国民の税金で賄われているため、国有財産の使用という面で拘束がある。一方、私立の場合は、経営母体(学校法人)と利用者の間の契約となるので、その内容が教育にも反映されるであろう。また、単科大学や専門大学の場合は利用規約が単一かもしれないが、総合大学の場合は、大学全体のポリシーと学部・学科別の利用規約が制定される場合もあり、その両方を教育で扱うことも必要になろう。情報系の学部・学科の場合は、特に「情報を扱う専門家としての情報倫理教育」も考えるべきである。

3. 総括責任者に対する教育

総括責任者は、当該ネットワークのポリシーの決定やネットワーク上での各種問題に対する処置に責任を持つ。従って、総括責任者は、高等教育機関もしくはそれを構成する学部等として高い倫理を尊重する環境と文化を有しているか、ネットワークのリスクをどのように把握しどのように管理しているか、またその管理体制は有効に機能しているかなどについて、しっかりした見識を持って答えられなければならない。

そのためには、総括責任者は、ネットワーク運用に関する基本的な事項や実際の事件について、少なくとも 1 年に 1 回、技術責任者から説明を受けるべきである。同時に、技術責任者は総括責任者へこれらの事項を説明する義務がある。総括責任者に対する教育としては、これ以外になく、あとは責任者自身がいかに高い見識を持つかである。昨今、企業においてはコンプライアンス経営が重要な課題になっている。私立の高等教育機関は言うまでもなく、独立学校法人化が予定されている国公立機関においてもコンプライアンス経営の観点は必須であり、ネットワーク運用管理についてもアカウンタビリティ(責任をもった説明ができること)がこれまで以上に求められる。総括責任者は、各高等教育機関もしくは各学部等の自己点検・自己評価に、研究教育業績だけでなくネットワーク管理業務に対する評価を含めるようにするなどして、制度面からも組織構成員の意識を高めるなどの方策を推進すべきである。

4. 技術責任者・技術担当者に対する教育

技術責任者・技術担当者は、当該ネットワークの設計や技術的問題（情報セキュリティ対策を含む）を取り扱うため、管理技術に関する教育のみならず、職業としての情報倫理教育を受ける必要がある。

人事面では、(1) 人事評価制度の中に資格認定制度や業績評価制度を確立すること、また、(2) 定期的な人事異動が行われる職場にあっては、数年単位で計画的に人材育成を図ること、(3) このための教育予算を確保することが重要である。

4.1 ネットワーク運用管理技術の教育

この教育は OJT を基本とするものの、組織内部での勉強会などの研修制度を設けるとともに、外部講習を受講できるようにしたり、同じ業務を担う組織の管理者・担当者との技術交流の機会を定期的に持つように配慮することが望ましい。そのためには、外部講習会への派遣費用などを予算に組み入れておくことも必須である。

OJT としては、所属部門のネットワーク管理だけでなく、所属機関のメディアセンター等の中心的なネットワーク管理部門において実務研修を行うなども効果的であろう。また、運用ネットワークとは別に実験用ネットワークを構築し、技術の切磋琢磨を図れるように設備面を充実することも有効である。当然ながら、これには経営資源の投入が必要である。

セキュリティインシデントに対する対応訓練も、防災訓練のように定期的に実施すべきである。

管理を外部発注（アウトソーシング）している場合は、業務委託先の業者が適切な管理をしているかどうかを監視できるためにも、技術教育は必要である。

4.2 職業倫理教育

専門職としての社会的責任を果たすためには、専門家としての情報倫理教育を受講することが望ましい。教育内容は、情報工学や情報科学を専門とする学生に対するものと同じでよいが、実際の経験に基づいた事例研究は、未経験の学生よりも内容の深さが期待できる。

教育体制としては、技術と法律と倫理の三つの柱を教えることができるような講師陣を揃えることが望ましい。例えば総合大学では、情報基盤センターや情報処理センター等が中心となって、情報系学部/学科や法学部・文学部と連携した教育体制をとることができる。

5. 利用者に対する情報倫理教育

ここではまず、学生に対する教育を中心に述べ、最後に教職員に対する利用者としての教育に触れる。

5.1 学生に対する情報倫理教育

5.1.1 新入生ガイダンス

新入生が新学期からすぐに教育用コンピュータやネットワークを利用できるようにしている大学は多い。家庭でもインターネットに常時接続できる環境が急速に普及し、初等中等教育でコンピュータを操作する機会も増えたので、パソコンをよく利用する新入生も増えているが、情報倫理に関する知識は乏しいのが実情である。実際に、大学においてもインターネットに関わるいろいろな事件が発生している。従って、コンピュータネットワークの利用規約やエチケットは、新入生に対する利用ガイダンスや、基本操作を含めた講習会の形で周知させることが望ましい。

ここでの新入生ガイダンスは、履修説明会などと併せて開催される 1 時間程度のものを想定している。学生数に比例してガイダンスの実施担当者の人数が必要になるため、担当者が必ずしも情報処理教育に携わっている人であるとは限らない。従って、担当者用の資料を整備し、実施担当者に対する説明会を開催することが必要である。内容としては、コンピュータネットワークの利用規約に関するものが中心であるが、余り多くの内容を含めることは避けて、利用目的やパスワードの扱いについて重点を置くべきである。

5.1.2 講習会

コンピュータネットワークの基礎的な利用方法について、講習会を実施する場合も考えられる。1〜3 日程度を想定しているが、この場合には、コンピュータネットワーク利用の技能だけでなく、利用規約やエチケット、マナーについても触れなければならない。この場合にも、初心者が対象であることを考えると、技術の本質、関連する法令、社会的な側面なども含めた教育は難しいと考えられる。これらについては、情報教育関連の授業の中で教えるべきである。

5.1.3 授業の中での教育

利用ガイダンスや講習会の中で扱えない部分については、授業の中で教育することになる。現在は、「情報処理入門」といった、どちらかと言えば狭い意味でのコンピュータリテラシーの教育がよく見受けられるが、高等教育におけるコンピュータ技能教育は今後減っていく傾向であり、むしろ情報倫理をまとまった形で含めることが望ましい。一般教養科目として「情報倫理」という授業科目を開講することも考えられる。この科目では、コンピュータネットワーク利用の技能に関わるエチケットやマナーにとどまらず、(1)技術に基づいて本質を理解すること、(2)関連する法令の主旨を理解し社会的な側面から考えられるようにすること、(3)自分で考え他人と議論することで、発達段階にふさわしい倫理的思考を身につけることが肝要である。

5.1.4 学部カリキュラムとの関係について

学部専門科目の中に職業倫理教育を含めるべきであるという要請が大きな流れになっている。特に工学系学部では、日本技術者教育認定制度(日本技術者教育認定機構:JABEE)を受けて、工学倫理に関する内容が授業の中に組み込まれることになってきた。今日，ほとんどの産業分野において「情報」の取り扱いは非常に重要な問題になっているので、すべての学部における職業倫理教育の一環として、情報倫理教育を含めるべきである。この教育内容は、事例研究を中心として、前節に述べた教育をさらに分野ごとの専門性と関連づけて扱うことになろう。

5.1.5 既存の一般情報処理教育カリキュラムとの関係

大学等での一般情報処理教育において、情報倫理に関する教育がすでに組み入れられている場合もある。実際、いわゆるコンピュータリテラシーと呼ばれる授業科目の中で、ワープロ、表計算、Web ブラウザー、電子メールなどの操作と関連して、情報倫理に関する内容が扱われることが増えている。今後、初等中等教育における情報教育が進展するに従って、大学等における一般情報処理教育も変容する必要がある。コンピュータリテラシーの操作に関する部分の比重を大幅に減らし、情報倫理に関する部分として、技術と法律と倫理の三つを柱とした教育内容を増やすことが望ましい。

5.1.6 初等中等教育との関係

高等学校では 2003 年度から教科「情報」が必修になり、情報 A、情報 B、情報 C のすべての科目で「情報社会に参画する態度」が扱われる。また、中学校においては、技術・家庭科の「情報とコンピュータ」の中で、情報モラルの重要性について考えさせることになっている。小学校では、特別に情報教育を行う教科・科目は存在しないが、「総合的な学習の時間」では情報機器を活用することが求められていることから、この時間に情報倫理に関連する内容に触れる場合が多い。また、総合的な学習の時間のテーマとして、情報倫理関連のテーマが選ばれる場合もある。

数年後には著作権などについて知識をもった学生が大学へ入学してくるようになるであろうが、さらに大学においても学生の発達段階に応じた教育、すなわち高等教育としてふさわしい内容の情報倫理教育が必要である。前節に述べたように、技術と法律と倫理の三つを柱としたカリキュラムを策定する必要がある。

5.2 教職員利用者に対する情報倫理教育

教職員に対する教育内容について、簡単に触れておきたい。ここでは利用者としての教職員を対象とし、総括管理者や技術管理者・技術担当者を除く。

教員に対する教育は簡単ではないが、ファカルティ・ディベロップメント制度が徐々に普及しつつあるので、その一環として「ネットワーク利用勉強会」として開催するなど、各組織で工夫する必要がある。基本的なネチケットについては、学生に対する教育内容と基本的に変わるものではない。さらに、所属組織のポリシーを理解し、その実施要領とそれを具体化した利用規約などを把握することが求められる。特に「なぜそのようにすべきか」をきちんと説明することが肝要であろう(例えば、なぜ機種依存文字を使うべきではないかなど)。

職員に対しては、たいてい研修制度があるのでそこに情報倫理教育を組み込むのがよい。基本的なネチケットから始めて、ポリシーや実施要領を理解することは、教員と同様に必要である。

技術の進歩に伴い法律も変わるので、教職員に対してそれらを随時通知するとともに、例えば 3 年に 1 度の勉強会もしくは研修講座の受講を義務づけるなど、制度化しておくことが望ましい。そこでは単に知識の更新だけでなく、管理の重要性、事故報告の重要性について、ケーススタディを中心とした内容を研修できるように、技術責任者レベルで策定すべきである。

付録 A. 利用規約違反行為への対応モデル

1. 利用規約違反行為等の対応判断の手順

利用規約違反や学外から学内への攻撃行為について、技術責任者が発見あるいは通報によって認知した場合の対応手順は、あらかじめ実施要領や対応マニュアルに規定しておかなければならない。以下に、具体的な対応についてのモデルを示す。

まず、技術担当者は、利用規約違反のおそれまたは外部からの学内ネットワークへの攻撃を発見し、または相談窓口等を通じて内部・外部からの通報を受けた場合、ただちに技術責任者に報告するものとする。

技術責任者は、利用規約違反行為等について、自ら認知するか技術担当者から報告を受けた場合、下記の手順により一次切り分け判断を行う。（図 A1 を併せて参照のこと。）

(1) 緊急性の判断（セキュリティインシデントの該当性の判断）を行い、技術的な緊急性を要すると判断される場合は、セキュリティインシデント対応のプロセスに移行する。
(2) コンテンツにかかわる問題は、通常、総括責任者に一次判断がゆだねられるが、爆破予告・自殺予告など、生命・身体への危険等の緊急性がある場合は、コンテンツに関する緊急対応のプロセスに移行する。
(3) 緊急性がない場合、学外からのクレームもしくは法律上の請求に基づく場合には、学外クレーム対応とする。
(4) 学内問題として処理可能である場合は、通常の利用規約違反対応とする。

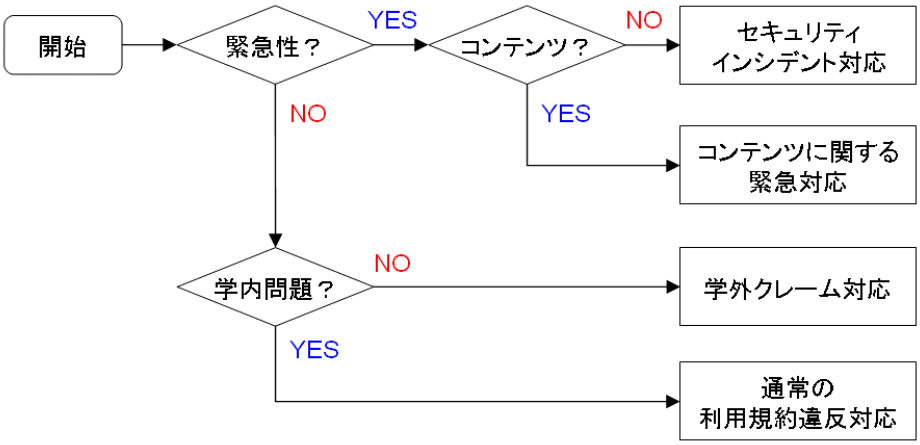

図 A1　一次切り分け判断のプロセス

技術責任者は、あらかじめ定められた手順に従って、緊急な技術的対応が必要なときは技術担当者に指示を与え、総括責任者に報告をし、指示をあおぐ。法的に慎重な判断を要する場合は、対応を実施する前に必ず総括責任者に報告し、指示を受けることとする。

技術責任者から報告を受けた総括責任者は、利用規約違反対応について、技術責任者・技術担当者を指揮監督する。セキュリティインシデント対応については、ポリシーに基づいてネットワーク運用委員会に指示や承認を求める。また、法的判断を要する問題のうち、通報者への内容確認や定型回答文書の発信等、技術責任者や外部対応窓口に対して一定の一時的対応を実施する。

2. セキュリティインシデント発生時の対応

セキュリティインシデントに対して、技術的対応とともに重要となるのが、インシデント発生前の準備である。組織においていかに技術的対応を強固にしても、組織をインターネットに接続する限り常に情報セキュリティ上の脅威は存在しているのであって、潜在的かつ必然的にインシデントに対応しなければならない状況にあることをまず理解しなければならない。

JPCERT/CC によるセキュリティインシデントの対応手順の例は以下の通りである[1]。

- 手順の確認
- 作業記録の作成
- 責任者、担当者への連絡
- 事実の確認
- スナップショットの保存
- ネットワーク接続やシステムの遮断もしくは停止
- 影響範囲の特定
- 渉外、関係サイトへの連絡
- 要因の特定
- システムの復旧
- 再発防止策の実施
- 監視体制の強化
- 作業結果の報告
- 作業の評価、ポリシー・運用体制・運用手順の見直し

2.1 発生から緊急措置決定まで

- 通報・発見等でセキュリティインシデントの可能性を認知した技術担当者は、事実を確認するとともに技術責任者に報告し、被害拡大防止のための緊急措置の必要性について判断を求めるものとする。
- 後日の調査に備え、インシデント発生時の状況、例えばログイン状況、ネットワーク接続や手順の稼働状況に関する記録を作成し、バックアップデータの作成、ハードディスクのイメージの保存等を行う。
- 継続している攻撃であって攻撃元サイトへの対処依頼が必要な場合、総括責任者の承認を得て技術責任者から相手方サイトへの対処依頼を行う。

2.2 被害拡大防止の緊急措置の実施

- 技術責任者は、個別システムの停止やネットワークからの遮断等の緊急措置の必要性を判断し、実施を技術担当者に指示する。
- 利用者での対処が必要な場合には、対処依頼をする。

2.3 緊急連絡および報告

- 技術責任者は、緊急の被害拡大防止措置の実施についてネットワーク運用委員会に報告する。
- 緊急措置の実施により影響を受ける利用者へ連絡する。
- 攻撃元サイトや関係するサイトへの連絡、外部広報、および JPCERT/CC への連絡などを行う。

---

[1] JPCERT/CC 技術メモ　- コンピュータセキュリティインシデントへの対応
2001-12-27　(Ver.03)　http://www.jpcert.or.jp/ed/2001/ed010004.txtを参照のこと。

2.4 事後の対応

- 技術担当者は、セキュリティインシデントの被害や緊急措置の影響を特定し、システムやネットワークの復旧計画を立案する。
- 技術責任者は、復旧計画を検討し、復旧実施の可否を判断する。
- 技術担当者は、セキュリティインシデント発生の要因を特定し、再発防止策を立案する。
- 技術責任者は、利用者への注意喚起等を含めた再発防止策を検討し、実施する。
- 技術担当者と技術責任者は、インシデント対応作業の結果をまとめ、ネットワーク運用委員会に報告するとともに、必要により運用体制や運用手順、情報セキュリティポリシーの改善提案を行う。

3. コンテンツに関する緊急対応

- 技術担当者は、生命・身体への危険の可能性を示唆するコンテンツ（爆破予告、自殺予告等）を発見したり通報により認知した場合、技術責任者の指示によりコンテンツの情報発信元を探知し、その結果を技術責任者に報告するものとする。
- 技術責任者は、総括責任者にコンテンツの情報発信元の探知結果を報告し、学内緊急連絡についての指示を求める。
- 総括責任者は、技術責任者に、学内緊急連絡についての指示をする。
- 広報、警察への連絡等の学内ポリシーに従う。

4. 外部からのクレーム（対応要求）時の対応

学内の利用者による情報発信行為について、外部から発信中止を求める要求、損害賠償の請求、さらには発信者情報の開示の請求等があることが考えられる。

以下にこのような場合に対する具体的な手続きの手順をまとめるが、請求の有効性や指摘されたコンテンツや行為の違法性判断については、必ず法律の専門家に相談するものとする。

4.1 利用者のコンテンツの違法性を主張した送信中止・削除の要求

プロバイダ責任制限法第 3 条では、いかなる場合に違法な情報を削除すべきなのかについては規定がない。しかし、一方、外部からの明確な要求があったにも関わらず、送信中止や削除等をしないと不法行為法に基づく不作為の不法行為として損害賠償責任を負う場合がある。

従って、高等教育機関が、その教育的見地から学生や教職員等の利用者の行為を高等教育機関の行為と同視しうる行為であるとして積極的に責任を負う方針である場合はともかく、通常は、損害賠償責任を回避する標準的対処を定めて実施する必要がある。手続の詳細はプロバイダ業界等のガイドラインが参考となる[(2)]。

(1) （通常手続き）コンテンツを発信した利用者への通知と削除
   - 技術担当者は、事実関係を調査し、発信元利用者を特定する。
   - 送信中止・削除請求があった場合であり、かつ指摘されたコンテンツの違法性の判断が困難な場合、プロバイダ責任制限法第 3 条第 2 項第 2 号に基づき利用者に請求があった旨通知し、通知後 7 日以内に利用者から反論がない場合は、送信中止あるいは削除を実施するものとする。
   - 有効と思われる反論があった場合は、その旨、削除請求者に伝えるとともに、当事者間での紛争解決を依頼する。

(2) （緊急手続き）利用者への通知前に一旦保留する。
   - 技術担当者は、事実関係を調査し、発信元利用者を特定する。

[(2)] 例えば,「プロバイダ責任法に関するガイドラインの公表について」（2002.05.24），社団法人テレコムサービス協会，http://www.telesa.or.jp/。

- 送信中止や削除請求があった場合であり、指摘されたコンテンツの違法性が疑いもなく明らかと思える場合、一旦利用者のコンテンツの送信を保留し、その旨利用者に伝えるものとする。有効な反論があれば送信を復活するものとする。
- この手続が適用されることもあることは利用規約に明示するものとし、本手続きの対象は、著名な音楽 CD の丸写しや個人の住所や電話の暴露等、権利侵害の疑いが濃厚である場合、緊急な救済の必要性がある場合のみとする。

4.2 利用者の発信したコンテンツの刑事的違法性の指摘および送信中止・削除の要求

刑事法上違法な可能性の高いコンテンツについては、違法性判断が困難であるので、基本的には、利用者の反論を待ってから送信防止措置を講ずることとする。すなわち、違法性の指摘があった旨、コンテンツを発信した利用者に通知して、自主的な対応を求め、一定の手続きを経た上で削除を実施する。

- 技術担当者は、事実関係を調査し、発信元利用者を特定する。
- 利用者に違法性の指摘があった旨通知し、一定期間（例えば 7 日）を経過しても利用者から反論がない場合は、送信中止あるいは削除を実施するものとする。

4.3 利用者の行為（コンテンツ発信以外）の違法性を主張した送信中止・アカウント削除等の要求

プロバイダ責任制限法第 3 条は、不特定の者により受信される通信（いわゆる公然性を有する通信）を対象としており、インターネット接続サービスやメールサービスのような 1 対 1 通信には適用されない。従って、脅迫メール、特定のメールボックスをターゲットにしたメール爆弾や、特定サーバへのクラッキング等、システムの機能障害を引き起こす動作やコンテンツが問題となる場合であっても特定の者相手の通信には適用がない。

しかし、プロバイダ責任制限法の適用範囲には入らないとはいえ学内利用規程としては、これらの行為についても手続きを明確にして利用規約違反とし、外部からの送信停止要求についても対応できるようにすることは民事法上問題がない。これは学問の自由や表現の自由との関係においても問題が少ないと考えられる。

(1) （通常の対応）コンテンツ外違法通信を発信した利用者への通知と利用資格停止
- 技術担当者は、事実関係を調査し、発信元利用者を特定する。
- 事実確認を行い、特定できた利用者に対し、コンテンツ外違法通信の発信を中止するよう通知する。これには再度行った場合には関連する利用資格（学外発信資格等）を停止する旨警告することを含む。
- 利用者からの反証があった場合には、再度確認する。
- 同様の手順を経て再発が確認できた場合には、高等教育機関による処罰の手順に移行する。

(2) （セキュリティインシデント対応）利用者の利用資格の一時停止
- 技術担当者は、事実を調査し、発信元利用者を特定する。
- 技術担当者は、利用者の行為が学内・学外のセキュリティインシデントの原因であると判断するに足る相当の理由がある場合には、技術責任者に報告し、その判断を求めるものとする。
- 技術担当者からの報告を受け、技術責任者は、必要な場合、利用者の関連する利用資格を一時停止するとともに、総括責任者およびネットワーク運用委員会に報告する。
- 請求者が連絡を要求しているときには一時停止した旨連絡する。

- 利用資格を一時停止した旨利用者に通知するとともに、再度行った場合には関連する利用資格を停止する旨警告する。
- 利用者から有効な反証があれれば、関連する利用資格の一時停止を解除する。
- 念書をとるなどの対応の後、利用資格の復活手続きを行う。
- 同様の手順を経て再発が確認できた場合には、高等教育機関による処罰の手順に移行する。

4.4 損害賠償請求等

利用者の情報発信や学外でのネットワークを利用した行為について損害賠償請求があった場合には、法律の専門家と共に対応する必要がある。

なお、プロバイダ責任制限法第 3 条第 1 項に定める要件に該当し、損害賠償責任の免責の範囲外である場合であっても、最終的にネットワークの管理者として損害賠償責任を負うとは限らないことに注意を要する。（都立大学事件[3]やニフティ事件[4]を参照すること。）具体的な削除請求が同時になされた場合には、上記 4.1 または 4.2 の手続きに従っていることが作為義務違反とされない有効な方策となる。

4.5 発信者情報開示請求

(1) プロバイダ責任制限法第 4 条に基づく場合

利用者の情報発信や学外でのネットワークを利用した行為について発信者情報の開示請求があった場合であって、Web ページ等 1 対多の通信によるものの場合、プロバイダ責任制限法の規定に基づき専門家と共に対処する必要がある。（通信事業者団体がガイドラインを公表していれば参考とする。）プロバイダ責任制限法第 4 条に基づく手順としては、概ね下記の通りとなる。

a) 発信者情報の保有の有無、技術的に特定できるかどうかの判断
　＊ 開示できる発信者情報がなければその旨を請求者に通知する。
b) 発信者情報開示請求の根拠の確認と違法性の判断
　＊ 必ず法律の専門家に相談する。
c) 開示について発信者の意見を聞く。
　＊ 発信者が開示に同意すれば開示してよい。
d) 発信者情報開示をする法律要件を確実には満たしていないと判断すれば開示を拒否する旨通知する。不開示の判断に故意または重過失がなければ責任を問われないので、少しでも法律要件を満たさない事実があれば、不開示判断をすべきである。
e) 発信者情報開示の要件に該当することが確実である場合には開示できる。しかし、開示判断を誤った場合には電気通信事業法上の通信の秘密侵害罪やプライバシー侵害による損害賠償責任から免責されないので、慎重な判断を要する。発信者が開示に同意しない場合、特に慎重な判断を要する。

(2) 他の発信者情報開示請求（民事および任意の照会）

利用者の情報発信や学外でのネットワークを利用した行為について発信者情報の開示請求があった場合であって、メール等 1 対 1 の通信によるものの場合、下記の手順をとるものとする。警察官、検察官、検察事務官、国税職員、麻薬取締官、弁護士会、裁判所等の

---

[3] 東京地裁平成 11 年 9 月 24 日判決（判時 1707 号 139 頁）。
[4] 東京地裁平成 9 年 5 月 26 日判決（判時 1610 号 22 頁、判タ 947 号 125 頁）、東京高裁平成 13 年 9 月 5 日判決（判時 1786 号 80 頁）。

法律上照会権限を有する者から照会を受けた場合であっても、原則として発信者情報を開示してはならないので同様の手順となる。

a) 電子メールアドレス等、発信者情報の一部について事前に開示の許諾を得ている発信者情報が請求されている場合については開示してもよい。また、開示と同時に当事者間紛争解決を依頼する。
b) 許諾を得ていない発信者情報の開示について発信者の意見を聞く。
    ＊ 発信者が開示に同意すれば開示してよい。
    ＊ 発信者が開示に同意しない場合は、開示を拒絶する。その場合は、通信の秘密およびプライバシーの保護を理由とする。
c) 発信者情報の保有の有無、技術的に特定できるか否かの判断
    ＊ 開示できる発信者情報がなければその旨を請求者に通知する。

(3) 強制捜査による発信者情報開示

技術担当者は、発信者情報を含む情報の強制捜査の事前打診があった場合には、発信者情報その他の強制捜査対象の情報を印刷あるいは記憶媒体に出力できるよう準備をしておくものとする。

総括責任者もしくは対外折衝事務担当者は、技術担当者の協力を得て、ネットワークの稼動への影響が最小限になるような方法で強制捜査に協力するものとする。捜査当局から強制捜査の令状の呈示を受けた場合、令状の記載事項等を確認の上、立会いを求められたときは立会い、押収物があるときは押収目録の交付を受けるものとする。

5. 通常の利用規約違反行為の対応

(1) 発見または通報等による認知と事実確認（情報発信者の特定を含む）

技術担当者は発見あるいは通報により利用規約違反の疑いを得たときは、事実関係を調査し、発信元利用者を特定した上で技術責任者に報告する。

(2) 利用規約違反の該当性判断

技術担当者の報告を受けた技術責任者は、通常の利用規約違反の対応手順にのせることが可能と考える場合は、その旨総括責任者に報告し、確認を得るものとする。

技術責任者は、技術的事項に関する利用規約違反に該当するか否かを判断し、該当する場合には情報発信の一時停止等の措置の必要性を総括責任者に報告するものとする。

総括責任者は、技術的事項以外の利用規約違反に該当するか否かを判断し、該当する場合には情報発信の一時停止等の措置の必要性およびアカウントの一時停止等、個別の情報発信の一時停止以上の措置の必要性を判断する。判断にあたっては、必要に応じてネットワーク運用委員会の判断を求めるものとする。

(3) 情報発信の一時停止措置

技術担当者は、総括責任者または技術責任者の指示を受けて、利用規約違反に関係する情報発信の一時停止措置等を実施する。

(4) 情報発信者に対する通知・注意・警告・当事者間紛争解決要請

技術責任者または総括責任者は、事案に応じて下記内容を発信者に通知するものとする。

・ 利用規約違反の疑いがあること

- **一時停止措置等の利用を制約する措置を講じた場合はそのこと、およびその理由・根拠**
- **利用行為の是正の要請**
- **利用行為が是正されなかった場合の効果（情報の削除やアカウントの停止、学内処分等）**
- **反論を受け付ける期間とその効果**
- **利用者当事者間の紛争解決の要請**

(5) **個別の情報発信または情報発信資格（利用資格）の停止と復活**

総括責任者または技術責任者は、(4)後の利用者の対応により、必要に応じネットワーク運用委員会の承認を得て、下記を実施するものとする。

- **有効な反論があった場合または利用行為が是正された場合の情報発信やアカウントの復活**
- **利用行為が是正されなかった場合の情報の削除やアカウントの停止、学内処分の開始手続き**
- **利用者当事者間の紛争解決着手の有無の確認**

(6) **学内処分との関係**

総括責任者は、学内処分に関し、アカウント停止処分やその他の利用制約処分の必要性の有無について意見を述べることができる。

付録B．教育カリキュラム

「情報倫理」のシラバス例

●概要

情報技術の進展が社会に及ぼす影響について技術の面から概観する。同時に、情報を利用する立場、および情報を発信する立場に立ったとき、いかに行動するべきかを倫理学の観点から検討し、法律との関連について学ぶことを目的とする。

●授業計画

ここでは、数個の領域について概ね 90 分×2 回程度でカバーする例を示す。それぞれの領域について、技術と社会(法律・倫理)の両面から理解することを目指している。

第 1〜2 回 情報システム、インターネットと WWW のしくみ

情報システムが社会に不可欠になっており、その基盤としてインターネットがある。インターネットショッピングなどを情報システムの例としてとりあげ、インターネットの基礎的技術を理解する。

- ネットワーク技術
- WWW のしくみ
- パスワードや暗号化通信によるセキュリティ保持(詳細はあとの講義で)
- ディジタル情報の特徴：情報の受け手だけでなく、簡単に発信者になれること(被害者だけでなく、加害者になる可能性)

第 3〜4 回 情報倫理

情報倫理はどうして「倫理」なのか、情報化社会における原則、情報倫理に必要な知識、ネットワーク利用時の判断のあり方

- 自分にとって、また周囲の人々にとってのリスクの評価
- ネットワーク上のルールを守ることの意味
- 社会の規範（法律や慣習）を守り、社会秩序形成に寄与することと、個人の自主性を発揮することとの関連（場合によってはディレンマ）
- 他人との関係の中で、自分の倫理的態度を見直すことの必要性、倫理は覚えることではなく、道徳的なきまりを守ることであるが、きまりははっきりしていないこと。自分がどんなディレンマに直面しているかを自分で知覚することが重要である。

第 5〜6 回 表現の自由とプライバシー保護

インターネットの媒体の性質を考える。例えば、ビラ(ちらし)と何が違うか。多くの人が同時にアクセスできることから、インターネット上での名誉毀損は、被害が広い範囲に及ぶ。文字情報だけで直ぐに相手に伝わることから、フレーミングも起きる。エチケット違反、マナー違反だけでなく法律問題(刑事、民事)になる可能性がある。

- 個人情報とは何か
- 名誉毀損とは
- 情報公開制度の意味、情報公開法の目的
- 情報公開とプライバシー

・プライバシーと個人情報保護

・憲法 21 条「表現の自由」

第 7 回 知的財産権

知的財産権の概要、特に著作権について理解し、Napster, Gnutella, WinMX などについて、利用者、著作者、プロバイダ等の面から考える。

・工業所有権法(産業発展):「特許法」(発明)、「商標法」(商標)など

・著作権法(文化発展)　:「著作権法」(著作物)

・特に、著作権に関して、複製権、公衆送信権、送信可能化権...

第 8〜9 回 インターネットと刑法

事件の解説から、法律面、特に刑法との関連について理解する。わいせつ情報とは何か、大学内だけで見える Web ページなら許されるか、管理者の立場であればどう考えるかなど。後半では、情報フィルタリングのしくみを理解する。

・ファイルマスクソフトウェアとわいせつ画像

・社内メールの検閲。封書の場合の親書開封罪との対応

・不正アクセス禁止法とは。パスワードを教えただけでも罪になる等。

・有害情報とは何か、情報フィルタリング技術と「言論の自由」

第 10 回 暗号、電子透かし、認証のしくみ

情報管理の重要性と、それを保護する暗号などのしくみを理解する。

・パスワードの暗号化、暗号化された通信路(SSL など)

・著作権を保護する技術としての電子透かし

・Web サイトの認証のしくみ(認証技術とベリサイン社など)

・電子投票のしくみ

第 11〜12 回 情報危機管理

情報危機管理がなぜ必要か、自分の身を守るだけでなく、システム運用について理解し、組織の一員としてなすべきことを考える。

・コンピュータウイルスのしくみ

・危険なクッキー

・不正アクセスとセキュリティ保護技術、ファイアウォール技術

・情報セキュリティポリシー/運用ポリシーと利用者の価値観

・利用規約と管理組織

第 13〜14 回 プレゼンテーション、ディスカッション

情報倫理に関するテーマを選択し、問題点を調査して、班単位でコンピュータを用いたプレゼンテーションを行う。質疑応答や、他の班のプレゼンテーションに対する評価を含む。ケーススタディのテーマの例としては、次のようなものが挙げられる。

・ディジタルデバイド

・Hate Speech Site

・テレビ番組を録画したテープの取り扱い

・当たり屋情報

・シグネチャと匿名性の問題

・Nifty の掲示板事件

・コンピュータウイルス

・迷惑メールなど

これらから一つないし二つを選択し、 (1)問題の概要を調べ、(2)問題の本質をつかみ、(3)逆の立場で考えるなど多面的に捉え直して、(4)発表する。

●前提条件

この授業科目を受講するために前提として必要な知識や技能は次の通りである。

・メールや Web サービスの基本的仕組みの理解

・メール、Web、ワープロなどの基礎的な利用技能

必須では無いが、前提として習得してあることが望ましい知識や技能は次の通りである。

・HTML を用いた Web ページの作成

・プレゼンテーションソフトウェアの利用方法

●教科書・参考書

・辰己丈夫著「情報化社会と情報倫理」共立出版、ISBN4-320-02964-X

・情報教育学研究会編「インターネットの光と影」北大路書房、ISBN4-7628-2191-8

・松井ほか編「インターネットと法」(第 2 版) 有斐閣、ISBN4-641-12891-X

・サラ=バーズ著、日本情報倫理協会訳「IT 社会の法と倫理」ピアソンエデュケーション、ISBN4-89471-554-6

・ジョセフ=キッザ著、大野・永安監訳「IT 社会の情報倫理」日本経済評論社、ISBN4-8188-1362-1

など

●成績評価

授業中のディスカッションにおける貢献度、プレゼンテーションの評価点、数回のレポートで総合的に評価する。

●「情報」の教職課程との関係

この授業科目を、教職課程の「情報社会と情報倫理」に充てることも考えられる。ただし、職業倫理(professional ethics)の一部を含むが、「情報と職業」で教える内容とは少しずれがあることに留意する必要がある。

付録C．インターネットに関連する法律・制度

1. 不正アクセス禁止法

「不正アクセス行為の禁止等に関する法律(2000 年 2 月 13 日施行)」は、他人のネットワークに許諾無くアクセスすることを禁止した法律であり、次の行為は犯罪となる。

(1)電気通信回線に接続されアクセス制限されているコンピュータに他人の ID とパスワード を無断使用して侵入、または、セキュリティホールを突いて侵入する行為(1 年以下の懲役または 50 万円以下の罰金)

(2)他人の ID やパスワードを無断で販売・配布する行為(30 万円以下の罰金)

さらにネットワーク管理者においては、適切な防御策を講じるよう努める義務が課せられている。ただし、罰則がないので、「努力義務」である。

従って、高等教育機関ネットワークの利用者は学内設備を利用して、外部のネットワークに無断で侵入したり、侵入するための ID・パスワード等を配布したりする行為を行ってはならない。

2. 通信傍受法

「犯罪捜査のための通信傍受に関する法律(平成 13 年 1 月 16 日施行)」は、組織的な殺人、薬物および銃器の不正取引に係わる重大犯罪の捜査において、通信傍受が事件解決のための有力な手段であり、国際的な捜査共助においても必要なことから作られた法律である。犯罪関連通信を傍受する時には、裁判官の発する傍受令状により行われ、一般市民の通信の秘密を不当に侵害することのないよう配慮されている。

通信事業者等(高等教育機関も含む)においては、傍受実施に際して傍受のための機器の接続などに協力する義務が課せられている。また、検察官、司法警察員は傍受に際して通信事業者等の立会いが義務づけられており、立会人は、傍受を記録した媒体の封印作業を求められるので、あらかじめ立会人又はその代理を決めておくことも大切である。

3. サイバー犯罪条約

日本政府は、平成 13 年 11 月 23 日に欧州評議会の「サイバー犯罪条約」に署名した。この条約は、インターネットを悪用した国際的な犯罪に対して各国一致して対応するために定められた。この条約では、次の行為を犯罪として取り締まることができよう各国に法整備を求めている。

a. 違法なアクセス

b. 違法な傍受

c. データ妨害（データの毀損・消去・劣化・改変・抑制行為）

d. システム妨害（データの入力・伝送・毀損・消去・劣化・改変・抑制等によるシステム機能への重大な妨害行為）

e. 機器の濫用（a.から d.までの行為を行うための機器、プログラムの製造、販売調達、輸入、配布、意図をもった保有）

f. 児童ポルノ

g. 著作権侵害

h. その他

また、これらの犯罪を捜査するためのコンピュータ・データの「応急保全命令」、「提出命令」、「押収」、「傍受」等についても法整備を求めている。日本では本条約の批准に向けて法整備を行うことになるが、日本の法律が改正された時には、その法律に従う必要がある。

4. 情報公開法

「行政機関の保有する情報の公開に関する法律(平成 13 年 4 月 1 日施行)」は、国の行政機関(国立大学を含む)が保有する行政文書の原則公開および交換のための手続きを定めたものである。地方自治体によっては、同等の条例を持っている自治体もあり、その場合には公立大学も同様の配慮が必要となる。

この法律の行政文書には、電磁的記録も含まれるため、ネットワーク運用のためのログやプログラムも公開文書の対象となる。したがって、ネットワーク運用においては、公開請求されることを前提に文書を保管しておくことが重要である。

ただし、次のものは不開示が原則になっているので、注意を要する。

a. 個人に関する情報で特定の個人を識別できるもの。ただし、公務員の職に関する情報は除く
b. 法人等に関する情報で、公にすると、法人等の正当な利益を害する恐れがあるもの
c. 公にすると、国の安全が害されるおそれ、他国との信頼関係が損なわれる恐れがあるもの
d. 公にすると、犯罪の予防、捜査等の公共の安全と秩序の維持に支障を及ぼす恐れがあるもの
e. その他

5. プロバイダ責任制限法

「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法(2003 年 5 月 27 日施行)」は、プロバイダの損害賠償責任を制限し、プロバイダに対する発信者情報の開示請求権を創設した法律である。ここにいうプロバイダには、商用プロバイダのみではなく、Web ページのホスティングサービスをする者や掲示板を管理している者全てが含まれる。したがって、高等教育機関のネットワーク管理者も本法律の対象となる。

従来、プロバイダが運用するネットワークで、他人を誹謗中傷する発言や他人の著作権を侵害するコンテンツが掲載された場合、被害者側から当該コンテンツを削除するよう要求され、それを放置するとプロバイダにも何らかの不法行為責任が生じる可能性があった。逆に、その申し出に従って当該コンテンツを削除すると、情報発信者側から表現の自由やサービス提供義務違反を理由にクレームを受ける可能性がある。この双方からの要求の板挟みを解消するのがこの法律の目的である。

この法律では、プロバイダが被害者から削除請求を受けた時にはその旨情報発信者に通知し、7 日を経過しても侵害情報を削除することに同意しない旨の返事が無かった時は、当該コンテンツを削除しても賠償責任は負わないとしている (これをノーティス&テイクダウンという) 。

また、被害者から情報発信者の情報(氏名、住所、その他情報発信者を特定する情報)を開示する請求を受けた時は、情報発信者に対して開示の可否について意見を聞く義務がある。発信者の意見等から判断して法律の要件を充たしているとは確信できない場合、誤って、情報発信者の情報開示を拒否した場合でも、賠償責任を負うことはない。

従って、高等教育機関ネットワークの運用者は、被害者からの削除請求や情報発信者の

情報開示請求に関して、まず当該情報の発信者に連絡することが重要である。ただし、このノーティス＆テイクダウンはプロバイダに対する法律上の義務ではない。

6. 個人情報保護法

「個人情報の保護に関する法律(2002 年 8 月末時点では未可決)」は、個人を特定できる情報(氏名、住所、電子メールアドレス等)の収集、利用開示に関する法律である。この法律は「基本原則」と「個人情報取扱事業者の義務」に大きく分かれており、国立大学の場合は、事業者の義務は課せられないと思われる。基本原則には、個人情報はその利用目的を明確にし、その目的の範囲内で取り扱うとなっている。また、個人情報は適法かつ適正に取得し、その管理は漏洩・滅失・棄損のないよう安全管理のために必要な措置を講ずるよう求めている。

さらに、収集した情報は利用目的の達成に必要な範囲で正確かつ最新の内容に保ち、その取り扱いに関して本人が適切に関与できるよう配慮するよう求められる。

従って、高等教育機関のネットワーク利用者の個人情報に関してもその利用目的を明確にして、その目的の範囲内での利用と安全管理を心掛けなくてはならない。

高等教育機関におけるネットワーク運用ガイドライン（第一版・暫定版）
- キャンパスネットワークの運用ポリシーと実施要領策定に関する指針 -

平成 14 年 9 月 10 日

電子情報通信学会 ネットワーク運用ガイドライン検討WG
（ご意見・連絡先： netguide@ieice.org）