ネットワークの運用体制に関するガイドライン

平成10年3月現在
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

はじめに：

教育・研究へのインターネットの利用が普及するに伴い、利用のための運営体制等、情報環境の整備が急がれている。

ネットワークを介して居ながらにして情報交流できる高度情報社会では、「便利さ」という光の部分と「もろさ」、「危険」という影の部分が常に併存しており、光の部分が高まればそれだけ影の比重が高まるという特質を持っている。

それ故に、初めて経験するインターネットへの対応を大学はどのような点に留意して始めればよいのだろうか。ここでは、大学から見た運営体制・運用体制の側面から対応策の試案をとりまとめてみたが、経験が少ない中での一つの考え方であるので全ての問題に対処できるとは考えていない。しかしながら、少なくともここに示すような対応をとることが影の部分から大学を守ることになろう。

以下に、現時点で考えられる対応策を掲げる。

１．大学の責任を考慮した対応策

正課授業、サークル活動その他の目的で、学生や教職員が大学のネットワーク施設等を利用してインターネットをはじめとする各種ネットワーク・サービスに接続・使用した場合に、他者に損害を生じさせ法的責任が発生することがある。わざと損害を発生させた場合だけではなく、何らかの間違いによって損害が発生した場合も同様である。このような場合に、ネットワーク・サービスへの接続に使用された大学のネットワーク設備の設置管理者として、大学(法人)が何らかの社会的責任を負うこともあり得る。各大学は、このような事態への対応も予め検討しておくことが望ましい。

社会的責任の中には、法的責任とそれ以外の社会的責任とがある。

法的責任以外の社会的責任としては、マスコミや社会一般からの批判などがあり得る。また、当該大学に対する社会的評価の低下その他の事実上の不利益も無視することができない。何らかの問題によって当該大学に対する社会的評価が低下してしまった場合、長年にわたって築かれた大学の名声や評価が一気に崩壊することもあり得るし、在学生や現職の教職員だけではなく、社会に出て大いに活躍している卒業生やＯＢなどに対しても少なからぬ不利益や名誉の失墜という打撃を与えることにもなりかねない。一方、法的責任としては、損害賠償責任を含む民事責任と刑罰等の刑事責任のほか、さまざまな行政法上のペナルティがある。民事責任に関連して、大学施設・財産等に対する仮差押えや種々の仮処分の可能性を考慮しなければならないし、刑事責任に関連しては、大学施設の捜索・押収とか、学生や教職員等の逮捕の可能性も

考慮しなければならない。

これら法的責任を含む社会的責任の問題に対する対応は、もちろん事柄によって異なるべきものである。特に、現実に問題が発生し、そのために何らかの訴訟を提起されたような場合には、弁護士その他の専門家の支援を受けながら具体的に対応をしなければならないであろう。また、その他の社会的責任に関しては、各大学の広報担当者がどの時期に、どのようなやり方で、どのような内容の対処をするのかの判断が非常に重要な課題となる。したがって、それぞれの問題の特質をよく考えて、それに適した最も合理的で分かりやすい対応策をきめ細やかに講ずるべきであろうし、予め検討した対応策をマニュアル化しておくことが望ましい。

対　応

(1) ネットワークシステム利用上の情報倫理規程の策定

法的責任を含む社会的責任を問われるような事態が起こるとすれば、それは、情報倫理に反する出来事が存在する場合である。したがって、そのような事態の発生を予防するためには、情報倫理の徹底が不可欠である。情報倫理の確立・普及は、いわば、予防的な対応策となる。

そこで、各大学は、基準となる情報倫理規程やその他の関連規程を整備しておくとともに、情報倫理規程の立案、啓蒙活動、規程違反行為に対する対処等の業務を担当する学内組織を予め設けておくことが望ましい。そして、情報倫理規程の中には、違反行為に対する処分（即時に行う仮の措置、ネットワーク接続の停止・廃止を含む措置、学則に照らして行う最終処分等）の内容、即時に行う仮の措置や処分の手続き（不服申し立てを含む）なども規定しておくべきである。

ところで、ネットワークシステム利用上の「情報倫理」という概念に関しては、いわゆるマナー（あるいは心得）等のネットワーク上の申し合わせに限定する見解と法的責任をも含むものとする見解など、さまざまな立場が存在する※1。また、適用対象者によって、一定の方向性や限定を伴ったものもある。たとえば、情報処理に携わる自然科学者・研究者等を主たる対象として想定された情報処理学会の情報倫理綱領※2などがその例である。

しかし、とりわけ学生にあっては、刑罰を含む社会的責任に無自覚な者がいないわけではなく、一般に社会の一員としての経験も乏しいわけであるから、大学における情報倫理基準としては、狭い意味での情報倫理のみではなく、法的責任に関連する一般的な倫理基準も含むものとして策定するのが妥当である。

そこで、情報倫理規程策定上の参考として、モデルを示すことにする。なお、このモデルは、想定されるすべての要素を勘案したものであるから、各大学において実際に情報倫理規程を策定する場合には、当該大学の組織、とりわけ、情報倫理規程を策定・実施する

※1 東北大学山根信二氏『コンピュータネットワーク時代に叫ばれる「倫理」についての情報源』
(http://www.vacia.is.tohoku.ac.jp/~s-yamane/articles/ethiclink.html)
『ネチケット・ホームページ』 (http://www.wind.co.jp/hirose/netiquette/index-j.html)

※2 『情報処理学会倫理綱領』 (http://ipsj.or.jp/sig/ipsjcode.html)

大学の組織上体とその手順、ネットワーク・システムの運用実績及び将来の見込み等に応じて、適宜取捨選択し、あるいは、一定の修正を加える必要がある。また、情報倫理規程の実施に際しては、さらに詳細な実施細則等を設けたり、各利用者のレベルや利用環境等に応じた説明書の配布や講習会の実施等を準備する必要があることにも留意すべきである。

●*ネットワークシステム利用上の情報倫理規程モデル*

大学は本規程の実施・運用に際して、教育研究機関としての使命、目的に沿って、教育・研究の自由を最大限に尊重し、通信の秘密を守り、個人情報及びプライバシーの権利を保護することを常に意識しなければならない。

§１　情報倫理規程の趣旨・目的等

本規程は、本学情報ネットワーク・システムの円滑な利用を促進し、本学の教育・研究の充実を図ることを目的として、ネットワーク・システム利用における情報倫理の基準を定め、利用者が良識的行動規範を持って臨めるようにするとともに、基準違反行為に対する措置並びに罰則及びその適用手続を明らかにすることを目的とするものである。

対象者は、本学の教員（非常勤教員、名誉教授等を含む。）、職員（臨時雇い、アルバイト等を含む。）及び学生（聴講生、交換留学生等を含む。）で本学情報ネットワーク・システムの利用が本学の敷地内でなされたと否とを問わず適用される。

なお、学外者（卒業生等を含む。）については、たとえば、本規程の遵守を旨とする同意を得るなどして、実施に疎漏がないようにしなければならない。

また、本学のネットワーク・システムの運用の全部または一部について外部のプロバイダを利用し、あるいは外部プロバイダに業務委託する場合には、プロバイダと利用者との間の利用契約約款の中に本規程の趣旨が含まれるようにするものとする。これら学外者に対する利用準則は、別に定める。

§２　用語の定義

本規程において使用する用語は、次の通り理解するものとする。

(1)　ここで言う「情報倫理」とは、本学情報ネットワーク・システム及びインターネットを含む情報ネットワーク・システム利用上の行為基準であって、その遵守が利用者の健全な社会規範意識によるもの並びに法令または本学学則によってその遵守が義務づけられているものを意味する。
(2)　「システム利用上の遵守事項」とは、別に定める本学システム運用基準に規定する順守事項の実施細則を意味する。
(3)　「ネチケット」とは、一般にネットワーク上で各個人が最低限守るべきルールとして理解されているものを意味する。
(4)　「法律上の義務」とは、日本国の法律、規則、政令または条例によって規定された義務並びに本規程の適用対象者に対して適用のある契約上の義務（約款による場合を含む。）及び慣習法上のすべての義務を意味する。
(5)　「罰則」は、本学学則に基づく除籍処分、停学処分、注意処分その他の処分、本学就業規則に基づく懲戒処分、本規程に定める措置を含む。
(6)　「措置」とは、措置及び仮の措置を意味する。
(7)　「違反行為」とは、情報倫理に反する行為を意味する。
(8)　「アクセス時間」とは、利用者が本学情報ネットワーク・システムを利用することのできる時間を意味する。
(9)　「ネットワーク・サービス」とは、プログラムの使用、データの入力、挿入、削除、出力その他の使用、電子メール・システムの使用、ハードディスクの使用、通信設備の使用、プ

リンタ等の出力を含め本学情報ネットワーク・システムに含まれる資源の全て、あるいは、利用者の段階に応じた一部の提供を意味する。

§３　システム利用上の遵守事項

(1)　利用者は、本学の建学精神に則り、品位を保ち、社会の一員としての自覚に基づいて、同システムを利用しなければならない。
(2)　本学情報ネットワーク・システム（以下「システム」と言う）を利用するためには、別に定めるシステム利用細則に基づき、利用資格の取得を申請し、所定の情報倫理講習を受講した上、利用資格及びアカウントを取得しなければならない。
(3)　システムの利用に際しては、同システム管理者の指示に従わなければならない。
(4)　システムの利用は、本学が定めるアクセス時間内に限られる。管理者は、停電、システムの保守・点検、システムの更新作業の実施、入試事務等に伴うシステムの閉鎖その他の合理的な理由があるときを除き、原則として、利用者が必要とするアクセス時間を付与し、通常のネットワーク・サービスを提供しなければならない。ただし、教育研究のために公衆回線を利用した学外からのアクセスについては原則として無制限とする。また、授業利用にあたっては、自学自習のための情報コンセントへの接続も含めて、施設利用規程の範囲内とする。
(5)　本学の情報機器又は個人が所有する情報機器をシステムに接続する場合は、大学側の指示を遵守しなければならない。
(6)　技術上のトラブル、利用上のトラブル、その他何らかのトラブルを発見した利用者は、そのトラブルの発生原因が利用者にあると否とを問わず、担当教員または同システム管理者に対し、直ちにその事実を申告しなければならない。
(7)　システム利用を終了するときは、当該利用者は、サーバ内のすべての個人ファイルの削除、メーリングからの退会を含め原状回復の義務を負う。

§４　ネチケット（最低限守るべきルール）

(1)　利用者は、利用資格を取得した後はすべての利用行為に関して全責任を負う。
(2)　虚偽または二重の利用資格を申請してはならない。
(3)　他の利用者と利用資格を共有してはならない。ただし、特に必要があってグループ ID の申請をしようとするときは、別に定めるところに従う。
(4)　事前の同意なしに、他の利用者が保有するファイルまたはデータを削除し、複製し、改変してはならない。
(5)　システムのリソース（計算時間、ハードディスク使用量、通信時間）を大量に消費し続けることにより、他の利用者の利用を妨害してはならない。
(6)　設備またはサービスを営利目的に使用してはならない。
(7)　コンピュータ・システムを毀損し、混乱させ、性能を変更し、故障の原因となるような行為をしてはならない。
(8)　第三者の著作物であるファイルやデータの引用・参照をするときは、著作権法の規定及び公正な慣行に従わなければならない。
(9)　発信された電子メールは、その発信者がすべての責任を負う。
(10)　電子メールを偽造し、または、その偽造を試みてはならない。
(11)　他の利用者の電子メールを許可なく読み、削除、複製、変造又は公開してはならない。
(12)　いやがらせや公序良俗に反する内容の電子メール、脅迫的な電子メール、不確かな情報を内容とする電子メールを発信してはならない。
(13)　求められていないメール、営利を目的とするメッセージ等、迷惑となる電子メールを発信してはならない。
(14)　Web ページ等を悪用して社会通念に反する情報を流してはならない。
(15)　機密を要するメッセージを送信するときは、デジタル署名その他公に承認された電子認証を用い、テキストを暗号化して送信するように努める。
(16)　リモートシステムへの権限外のアクセスを試みるために本学のシステムを利用してはならない。

(17)　本学のシステムを使用して不正な利用をしてはならない。
(18)　システムおよびユーザーのパスワードの解読を試みてはならない。
(19)　システム・ファイルを複製、削除、改変してはならない。
(20)　第三者のソフトウェアなど著作権の対象となっているものを、許可を得ずに複製してはならない。
(21)　ネットワーク・システム、プログラムまたはデータを破壊または改変してはならない。
(22)　正規の手続によらずにより高いレベルの利用資格を入手しようと試みてはならない。
(23)　コンピュータ・ウイルス等、システムの混乱の原因となる有害プログラムまたはデータを本学情報ネットワーク・システム内に持ち込んではならない。
(24)　機密であることが分かっているファイルにアクセスしてはならない。アクセス後に当該ファイルが機密であることが分かったときは、直ちにアクセスを中止しなければならない。

§５　法律上の義務

ネットワーク・システムの利用に関連する法令は次のとおりである。なお、これらに違反する行為は、いずれも犯罪行為であり、処罰される行為である。システムの利用者は、これらの義務を遵守すべきであるのはもちろんのこと、同システムの利用に際して、法令に触れる行為をしてはならない。

(1)　コンピュータで使用するファイルを不正に作成してはならない(刑法 161 条の 2)
(2)　コンピュータを破壊したり不正の指令を与えるなどしてコンピュータによる業務を妨害してはならない(刑法 234 条の 2)
(3)　コンピュータに不正の指令を与えるなどしてコンピュータを誤作動させ、不正の利益を得てはならない(刑法 246 条の 2)
(4)　コンピュータで使用するファイルを破壊してはならない(刑法 258 条、259 条)
(5)　他人の特許権を侵害してはならない(特許法 196 条)
(6)　特許がないのに特許とまぎらわしい表示をしてはならない(特許法 198 条)
(7)　他人の商標権を侵害してはならない(商標法 78 条)
(8)　登録商標でないのにこれと紛らわしい商標を使用してはならない(商標法 80 条)
(9)　他人の著作権、著作者人格権、出版権、著作隣接権を侵害してはならない(著作権法 119 条)
(10)　著作者でない者の実名または周知の変名を著作者であるとして表示して著作物を頒布してはならない(著作権法 121 条)
(11)　商業用レコードを複製し、その複製物を頒布してはならない(著作権法 121 条の 2)
(12)　他人の商品と誤認するような商品表示をしたり、国際機関の標章と誤認させるような標章を使用して不正競争をしてはならない(不正競争防止法 13 条)
(13)　郵政大臣の許可を得ないで第 1 種電気通信事業を営んではならない(電気通信事業法 100 条)
(14)　みだりに電気通信事業者の設備を操作してネットワーク・サービスの提供を妨害してはならない(電気通信事業法 102 条)
(15)　電気通信事業者が取扱中の通信の秘密を侵してはならない(電気通信事業法 104 条)
(16)　他人の名誉を毀損してはならない(刑法 230 条)
(17)　公然と他人を侮辱してはならない(刑法 231 条)
(18)　他人の生命、身体、自由、名誉または財産に対して危害を加える旨を告知して脅迫してはならない(刑法 222 条)
(19)　虚偽の風説を流布するなどして、他人の信用を毀損し、または、他人の業務を妨害してはならない(刑法 233 条)
(20)　他人の物を盗んではならない(刑法 235 条)
(21)　他人を欺いて物を交付させたり、財産上の利益を得たりしてはならない(刑法 246 条)
(22)　未成年者の知慮浅薄または他人の心神耗弱を利用して物を交付させたり、財産上の利益を得たりしてはならない(刑法 248 条)
(23)　他人を恐喝して物を交付させてはならない(刑法 249 条)
(24)　自分が占有する他人の物を横領してはならない(刑法 252 条)
(25)　賭博をしてはならない(刑法 185 条)
(26)　富くじを発売してはならない(刑法 187 条)

(27)　わいせつな文書、図画その他の物を頒布したり、公然と陳列してはならない(刑法 175 条)
(28)　営利の目的で、淫行の常習のない女子を勧誘して姦淫させてはならない(刑法 182 条)

§６　違反行為に対する措置

システムの管理者は、本規程の違反行為をした者（アカウントを盗まれた場合の盗まれた者を含む）に対し、利用資格の取消ないしその他の教育的措置をとることができる。ただし、利用資格の停止、利用資格の変更については、システムの管理者は、いつでも解除することができる。また、本規程の§７に定める教授会からの解除決定の通知を受けたときは直ちに解除しなければならない。なお、利用資格取消の措置を解除した時は、新規アカウントを付与するか、取り消したアカウントを復活して利用を再開することとする。

アカウント取消中または停止中の電子メールの消滅、不到達、ファイル等の削除等が発生しても、本学は、その責任を一切負わない。

これらの措置に対する不服申立等を審理するため、本学システム運営委員会内に審査委員会を設置する。審査委員会の組織等については、別に定める。

(1)　利用資格の取消
(2)　利用資格の停止（１年を超えない期間内に限る）
(3)　利用資格の変更
(4)　違反行為に使用され、または、違反行為の結果として生じたファイル、データ、プログラム等の削除
(5)　違反行為に使用され、または、違反行為の結果として生じたファイル、データ、プログラム等への一般的もしくは個別的なアクセス制限
(6)　アカウントの停止・変更
(7)　その他の教育的措置

§７　違反行為に対する措置の適用手続

(1)　システムの管理者が措置を講じようとするときは、違反行為の疑いのある利用者から事前に事情を聴取しなければならない。ただし、緊急を要し、事前に聴取をすることができない場合には、この限りでない。
(2)　また、違反行為に対する措置を講じたときは、２４時間以内に、違反者が学生である場合には学務部に対し、それ以外の者である場合には総務部に対し、その措置を講じたこと及びその内容を通知しなければならない。
(3)　学務部がシステム管理者からの通知を受けたときは、その通知を受けた時から 24 時間以内に、当該学生所属の学部に対し、措置が講じられたこと及びその内容を通知しなければならない。
(4)　通知を受けた学部の教授会は、３０日以内に当該学生に対する本学学則に基づく処分の要否、または、既に講じられた措置の解除の要否を決定しなければならない。
(5)　教授会が措置の解除を決定したときは、システムの管理者に対し、その決定の時から 24 時間以内に措置解除決定及びその内容を通知しなければならない。

§８　相談窓口

相談窓口に関しては、別に定めることとする（巻末「仮想大学ネットワーク利用相談室」参照）

§９　その他の雑則

（省略）

(2) 情報倫理の周知徹底

現在のネットワーク環境の下では、無自覚または意図的なものとして、学生が著作権侵害行為、その他の不法行為、あるいは犯罪行為など第三者に対する加害行為をしたり、逆に、第三者の行為によって被害を受けることを完全に避けることは不可能というべきであろう。教員による直接の監督・指導が行き届かない利用形態においては、特にそうである。もし、学生が何らかの意味での加害者となる場合には、インターネット環境を設置している者としての大学が社会的責任を問われることもあり得る。

これらの加害行為または被害の防止のためには、講習会、正課教育、広報活動等を通じて、パスワード管理の重要性、インターネット環境の特質、情報倫理の基本的内容等を学生に十分に理解させ、これらを周知徹底することが重要である。また、その周知徹底をより確実なものにするための具体的方策として、情報倫理講習等の受講を利用資格としてのアカウントやパスワード付与のための要件としたり、情報倫理の基本的内容等を習得していない学生に対してはネットワーク利用を制限・禁止することなどが考えられる。

情報倫理の周知徹底のためには、学生や教職員に対する教育・研修だけでは十分とは言えない。大学は、教育・研究という立場から、各大学におけるネットワーク設置の趣旨に照らして最も適切な方法で、ネットワーク利用者すべてに対して、情報倫理に関する情報を提供し続けることが望ましい。また、ネットワーク利用の開始に際して、後に実例として掲げる「同意書」や「契約書」等によって各利用者へもルールの徹底を図り、あるいは、情報倫理違反事例とそれに対する対応に関する情報の提供をすることも重要である。

また、条文の形式による関連規程の整備と併せて、一般利用者にも理解しやすい形式で編集したガイドラインやパンフレット等を準備し、ネットワーク利用者や情報倫理講習等の受講者である学生に対しては全員配布するなどして、一般利用者レベルでの啓蒙活動にも力を入れる必要があろう。

さらに、大学は、ネットワークの管理者として、問題発見のための継続的な努力を尽すこと、そして責任ある対応をとることが望まれる。

(3) 違反行為の発見

正課授業で発生するトラブルの発見や予知の方法としては、教員が授業の範囲内で責任をもって対応することが望ましい。その他のトラブルの発生の可能性については、大学内でネットワークを実際に管理・運営するセクションが責任をもって対処すべきである。この責任ある対処の中には、違反行為に関する情報収集も含まれる。

しかし、現実には、ネットワーク上の出来事の全てを組織的に調査・点検することなど不可能である。仮にそれが可能であったとしても、そのようにすることが、ネットワーク上の個人情報やプライバシーの保護と抵触する危険性があり、また、教育環境という観点からも、大学の教員と学生との間の信頼関係を危うくすることにもなりかねず、妥当でない。

そこで、考えられる方法としては、後に掲げる学生や学外者を含む利用者からクレームを受け付けるための窓口をネットワーク上に設けたり、情報倫理やネットワーク上のトラブルに関する電子掲示板サービス、ネットワーク・ニューズやメーリング・リストを設置し、これらによる情報交換を継続的に行うことなどが考えられる。他方、大学の Web ページ上で、ネットワークの利用者に対する各種苦情処理サービスを提供し、または、そのようなサービスを提供している公的団体等(コンピュータ・ウイルス発見の場合のＩＰＡ※3を含む)のサイトへの分かりやすいリンク集を準備しておくことも重要と思われる。

(4) 違反行為に対する対処

違反行為に対する対処には、ネットワークの管理者としての対処と、学則違反行為ないし法律に反する行為としてとらえ大学（法人）の処分としてする対処とがある。具体的には、即時的な対処としては、当該記事やＷｅｂページ（データ）の削除、アクセスの禁止、当該利用者の利用登録・資格の停止・取消等が考えられ、また、最終的な学則上の処分としては、事案の内容・程度に応じて、放校処分、停学処分、注意処分、その他の教育的措置等があり得る。

即時的な対処としてのネットワークの利用停止・取消等の措置は、ネットワーク管理者として、ネットワークの運営・維持上の必要上からなされるものであり、緊急の対応が求められることから、ネットワーク管理者の責任と権限の範囲内でなされるものであるが、この措置をもって学生等の身分に関する最終的な処分とすることはできない。これに対し、学則上の処分は、学則に定める規定に基づく罰則の適用ないし人事上の処分であり、一般に、教授会（学生の場合）や人事担当部署（職員等の場合）の所定の手続を経ることが必要である。

このように、ネットワーク管理者としての即時的な対処と最終的な学則上の処分とは相互に性質を異にするものである。したがって、各大学の実状に応じて、ネットワークの利用に関する措置と学則上の処分との関係を明確に意識した上で、緊急の措置を実行可能とするための各種関連規程の整備、組織の確立がなされるべきである。また、ネットワーク管理者による措置は、緊急の対応を要するものが多いと予想されるとはいえ、ネットワークの利用者に対して重大な影響ないし不利益を与え得るものであることは否定できない。たとえば、ネットワークの利用を前提とした必修科目の授業を受講している学生について、システム利用停止ないしアカウント取消の緊急措置がとられると、実質的には停学処分と同等以上の罰則を適用したのと同じ効果が生じることもあり得る。現実に、某大学において、不正使用を行った学生を一定期間利用停止にしたことに対し、講義担当教員から「課題利用ができないから利用停止を解除せよ」との要求がなされた事例がある。したがって、当該緊急の措置をする手続や不服申立等に関する規程も予め検討し、準備しておく必要があろうし、さらに、学則に基づく最終的な処分との整合性を保つために、各大学の組織及び実状に応じて、教授会等への連絡・通知の方法、緊急措置の解除方法などについても周

※3 『Information-technology Promotion Agency 情報処理振興事業協会』 (http://www.ipa.go.jp/index.html)

到な検討が必要となろう。

他方、最終処分としての学則上の処分は、各大学によってその内容及び手続とも異なると思われるが、実際の例としては、期末試験における不正行為に対するものと同程度の厳しい処分を行った大学の事例もある。情報倫理の授業に関しては、当該担当教員が学生の行動に対する第一次的な教育・指導責任を有することを考えると、情報教育担当教員を含む教職員に対する情報倫理教育の実施・徹底の重要性を更に深く認識すべきである。

なお、アメリカ合衆国の例を見ると、カリフォルニア州の刑法は、大学の学生に関しては、コンピュータ犯罪者に対する刑事処分（拘禁刑及び罰金）や矯正措置（一定年限のコンピュータ使用禁止措置等）に準じた措置を各大学の学則の中で定めることを求めており、参考となろう※4。

２．大学におけるセキュリティー管理体制の考え方

インターネットは誰もが参加できるオープンポリシーのネットワークであるため、匿名や偽名による利用、ウィルスの侵入、不適切な情報の受発信、情報の流出や破壊・改ざん等の防止が技術的に困難である。

対　応

(1) セキュリティー技術による対応

ファイアウォール・暗号技術等を導入し、外部からの不正なネットワーク侵入を防ぐとともに、CERT や JP-CERT※5 その他の公的機関から提供される情報（ip-connection@jepg-ip.ad.jp）の内容を理解し、対応できる担当者を置くことが必要である。

ただし、技術による対応には、その技術自体の限界およびその技術の運用上の限界があり、不正侵入、不正利用を完全に防ぐことはできないので、問題発生時における迅速な組織的対応が不可欠である。

●*主な技術的対応*

以下の対策のうち必要なものを組合せ、各大学でのセキュリティー上の要求に応じた運用を行う。

① UNIX,WindowsNT 等ネットワークサービスを行うホスト単位でのセキュリティー管理の強化
安全な OS 設定、OS 修正、接続サービスの制限と記録、パスワード推測プログラムの実

※4 『カリフォルニア州（ＵＳＡ）の「1989 年コンピュータ犯罪法」（仮訳）』
(http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/act-1989-California.htm)

※5 CERT (Computer Emergency Response Team)　JP-CERT(コンピュータ緊急対応センター)

行等による推測されにくい利用者パスワード設定の徹底、WWWサーバで実行されるプログラムの登録制限

② 標準的なルータでのパケットフィルタリング機能の設定
主に対外接続点で実施。不要なサービスを閉じて、必要なものだけ通過を許可する。

③ ファイアウォール製品、ネットワーク管理製品の導入
IP パケットに含まれる制御情報によってネットワークの通過を制限する方式（パケットフィルタリング）、IP アドレスやポート番号を静的/動的に変換する機能（アドレス変換）、アプリケーション毎のきめ細かな設定や利用者個人の識別が可能な機器やソフトウェア（アプリケーションゲートウェイ）の導入、接続監視・報告、メッセージ内容の監視

④ 暗号技術、認証技術の導入
メッセージやファイルの暗号化、電子署名、高度な利用者認証方式の採用、使い捨てパスワード、送信データが自動的に暗号化されて相手に届く方式（暗号化トンネリング）の採用

⑤ パソコンのウイルス除去ソフトウェアの導入、（教室パソコンを標準設定に戻す管理ソフトウェアの導入）

⑥ 重要データの保存(バックアップ)データ破壊、改ざんの予防措置

情報、それを流すネットワーク、そしてネットワークに接続されたホストのセキュリティーについて、それぞれ 3 段階程度のレベルに分類し、各部分で必要とされるセキュリティーレベルに見あった対処を行えばよい。

プライバシー尊重の意味からも、技術的対策では基本的にはネットワークを流れるデータやメッセージの意味までは解釈しないので、利用者自身による知的財産権を侵害するデータの流通、機密データの漏洩などの問題には対処できない。

また、しばしば膨大となる接続監視記録を人間が読んで異常を発見し、対処する必要がある。いずれにしても、セキュリティーと利便性の両立が難しく、両立のためにはシステム設計者の労力と費用が莫大なものとなる。

ファイアウォールについて

セキュリティーを重視すると、企業ＬＡＮのインターネット接続に見られるように、製品を利用して、ほとんどすべてのサービスを閉じ、安全と思われるものだけを通す設定をすることになる。一応の管理は楽であるが、利用者が自由に外部と通信できないため、要望に応じる度に設定変更が必要になる。

ファイアウォール外に対外サービスを行うWWWやメールサーバを配置する場合が多いが、それらのホストでは上述ホスト単位でのセキュリティーの強化を実施する必要が生じる。また、学内での問題に関しては、対外接続用に設置されたファイアウォール単独では全く効果がないことを忘れてはならない。

一方、大学で多かった利便性重視の開放的な環境では、不正侵入の防止のために直接外部と通信をするすべてのホストでホスト単位でのセキュリティーの強化、対外接続ルータ

でパケットフィルタリング機能の設定を実施する必要がある。高度なセキュリティーが必要ないホストでも、他サイトへの不正侵入に利用されるおそれがあるため、対策は必要である。

さらに、構成員だけでなく外部からの侵入者がノートパソコンを持ち込むことがありうる。出入りが自由な教室やロビーなど、誰もがネットワークに物理的に接続できる場所では、利用者自身や物理的侵入者による不正利用への対処として、物理的なネットワーク接続制限、あるいはサービスを安全なものに限定する必要がある。

ＬＡＮや広域インターネット上のデータは通常暗号化されていないため、10Base-T 等の放送型ＬＡＮやルータに高度な技術をもつ者が侵入すれば、そこを通るパスワードや機密データを不正入手できる。そのため、不正侵入を試みる者の増加に伴い、特に学外からの学内ホストの利用に際しての認証方式の検討が必要である。また、重要な電子メールでの連絡には、発信者アドレス（From:）の偽造が可能であるということから、電子署名が必要となりつつある。商用 ISP を利用したキャンパス間の接続(Virtual Private Network)においては、業務データの暗号化が必要である。

(参考となる答申、指針 等)

http://www.npa.go.jp/soumu2/kokuji.htm
(警察庁 情報システム安全対策指針, 1997.9)
http://www.ipa.go.jp/SECURITY/antivirus/kijun429.txt
(at IPA, 通産省 1995, 7)
http://www.ipa.go.jp/SECURITY/ciadr/crack-gl.txt
コンピュータ不正アクセス対策基準(at IPA, 通商産業省告示第３６２号)
http://www.ipa.go.jp/SECURITY/ssh/ssh-ipa.html
サイトセキュリティーハンドブック(IETF)の日本語訳
http://www.saaj.or.jp/KIJUN2.HTM
(情報システム安全対策基準 at saaj, 通産省告示第５１８号)
http://www.mpt.go.jp/policyreports/japanese/group/internet/net-index.html
(郵政省、情報通信ネットワークの安全・信頼性に関する研究会報告書)

(2) セキュリティー管理組織のあり方

迅速な組織的対応のために、問題発生の予防・記録・被害拡大の抑制のための手順を確立する。そのためには、学内にネットワーク運用委員会等の企画・管理・運用体制を整備し、その組織において責任の所在と緊急対応手順を確立することが必要である。

●*組織モデル*

ネットワークセキュリティーに関する責任の所在を明らかにし、障害発生時の対応を機動的に行うとともに、セキュリティー対策の方針・内容を各部局に周知するため、全学一致のセキュリティー管理組織を設置する必要がある。しかしながら、実際にはネットワーク管理の専任者を置くことは難しく、担当者の過重負担が大きな問題となる。円滑なセキュリティー管理のためには、組織を設置するとともに、セキュリティー業務の重要性に関

する学内の共通理解を得ることが重要である。

①統括責任者

ネットワーク運用委員会等、全学のセキュリティー向上に関する意思決定機関を主宰し、緊急対応手順を統括する者を設置する。

②教育研究システム担当責任者
③事務システム担当者責任者

教育研究部門、事務部門それぞれに、部門の業務内容を把握している担当責任者を置き、部局内のセキュリティー向上策を検討するとともに、障害発生時の関係者への連絡と迅速な対応を指揮する。

④各部局の実務担当者

各部局それぞれに担当者を置き、部局内部のセキュリティー状態を把握するため、部局のシステムを監査し、ユーザー管理、外注管理を行う。

⑤技術担当者（技術委員会）

UNIX 及びルータ等担当、端末系(Windows,Macintosh 等)担当、委託業者への連絡担当等をとりきめ、大学の規模によって専門の委員会を構成する。セキュリティーソフトウェアのインストール、バージョンアップ、障害発生時の緊急対応等、現場の処置を行う。

ネットワークセキュリティーの弱点を発見・解消し、全学的な対応策を共通認識によって実施するためには、技術部門と上層機関の意志疎通が重要である。

●*効率的な組織運用*

ネットワーク管理組織業務を効率的に運用するためには、緊急時の電話連絡網、メーリングリストを定めておくとともに、不正侵入・ウィルス混入時の対処マニュアルを整備し、また、全学のネットワークユーザーに対する情報提供を遅滞なく行うことも必要である。