大学における
情報セキュリティポリシー
の考え方

平成１４年３月２９日

大学の情報セキュリティポリシーに関する研究会

目　　次

大学における情報セキュリティポリシーの考え方

大学の情報セキュリティポリシーに関する研究会

本ポリシーは、主として国立大学における情報セキュリティポリシーの考え方および一例を示したものである。各大学においてポリシーを策定する場合に、本ポリシーが参考となるとともに、今後、情報セキュリティを高めていく際の方向を示すことも狙いとしている。国立大学を前提としてはいるものの、公私立大学においても十分参考に値するものと考えている。

情報セキュリティポリシーを策定するにあたっては、まず各大学において、その必要性を十分に認識しなければならない。高度情報社会の一員である大学は、情報セキュリティの確保と不正なアクセスの抑止のレベルによって、プレゼンスが全く異なってくることを理解すべきである。高いレベルのセキュリティを確保するためには、自由なアクセスに制限が生じうることも十分に理解すべきである。従って、大学ごとに情報セキュリティポリシーを検討し、策定しなければならない。

情報セキュリティポリシーは、大学の構成員すべての努力によって遵守されなければならない。情報セキュリティポリシーによって、大学の本来の活動を妨げるような制約や制限を設けることは、避けなければならない。一方、安易なポリシーでは社会から切り離されるきらいのあることを忘れてはならない。従って、大学の実状にあったポリシーを早急に策定し、引き続いて、短期間でセキュリティのレベルを上げていくことがキーポイントとなる。

このポリシーにおいて、それぞれの用件がどの程度重要であるかを明確にするため、次のような用語を使用している。

しなければならない：　最低限実施すべきであることを示す。

すべきである：可能な限り早期に実施すべきであることを示す。

することが重要である：即座に実施しなくても優先的に実施すべきであることを示す。

することが望ましい：　実施または考慮することが望ましいことを示す。

一方、このポリシーでは、理解しやすいように具体的な実施手順などにも言及している点に留意されたい。

Ⅰ　情報セキュリティの基本方針

１．情報セキュリティの基本方針

高度情報社会において、大学が学術研究・教育活動を高めようとするためには、情報基盤の整備に加えて、大学の情報資産のセキュリティを確保することが不可欠である。情報セキュリティの大切さを大学の全構成員に十分意識させ、情報資産を確固として守るため、「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 日情報セキュリティ対策推進会議決定）」を踏まえ、各大学は情報セキュリティポリシーを速やかに定めなければならない。

情報セキュリティポリシーによって目指すものは次のとおりである。

(a) 各大学の情報セキュリティに対する侵害を阻止。
(b) 学内外の情報セキュリティを損ねる加害行為を抑止。
(c) 情報資産に関して、重要度による分類とそれに見合った管理。
(d) 情報セキュリティに関する情報の取得を支援。

一方、大学は、少数のシステム管理者が情報システムを提供し特定の利用者が使用する一般の省庁と異なる。次のような点を十分に斟酌しなければならない。

(a) 構成員として教職員だけでなく、学生や大学院生等が利用者として含まれること。
(b) 情報資源を管理している教職員が、システム管理者として責任を負うべきこと。研究室のパソコンなどは教員がシステム管理者となることが多い。
(c) 大学内で開催される学会などへの参加者が持ち込む情報機器（ノートパソコン）も対象となりうること。

このような状況のもとで、情報セキュリティを守るため、各大学において、次の事項を内容とする情報セキュリティポリシー（基本方針・対策基準）を早急に策定しなければならない。さらに、具体的な情報システムまたは業務において、どのような手順に従って実行するかを明確にすることが肝要である。

①　組織・体制

全学に対する最高情報セキュリティ責任者をおき、情報セキュリティ委員会（全学的な委員会）の委員長となり、大学における情報セキュリティ対策を推進する。その果たすべき役割、責任および権限を明確にしておかねばならない。

さらに、日常的な業務、例えば、学外からの種々様々な攻撃および学内からの加害行為に対する遮断等の措置を、どの組織で、どのような手順で、どのような体制で行うかを明確にしておかねばならない。

② 情報の分類と管理

大学で扱われるすべての電磁的に記録された情報について、情報の重要度による分類、情報の管理方法、管理責任を規定する。情報の種類として、大別すれば、各省庁におけるいわゆる事務情報に加えて、医療情報、研究情報、教育情報がある。

重要度の分類と、改ざんや破壊によるリスク分析を、全学レベルおよび部局レベルで検討する必要がある。

③ 物理的セキュリティ

情報システムの設置場所について、安全性を保ち、不正な立入りを阻止する対策を立てることのほかに、デスク上のパソコンまたは持ち運びを前提としたノートパソコン等の情報資産を保護するための対策にも十分配慮しなければならない。

④ 人的セキュリティ

全構成員に対して、情報セキュリティポリシーを周知徹底させるとともに、各人がどのような権限と責任を持っているかを明らかにし、情報セキュリティを確保するための啓発活動や教育を講じなければならない。

さらに、キャンパスネットワークのバックボーンの維持管理に関しては、24 時間 365 日運用を前提として、要員を確保すべきである。

⑤ 技術セキュリティ

学外または学内からの不正なアクセスによる情報資産の破壊を阻止するため、情報ネットワークのアクセス制御・管理に必要な対策を講じるべきである。情報の分類によって物理的または論理的に異なるネットワークの導入を考慮すべきである。

⑥ 評価・見直し

情報セキュリティポリシーは、秒進分歩の情報技術の発展、ならびに、策定したポリシーの遵守度により、定期的に見直して改定を行い、セキュリティレベルを絶えず上げるよう努力しなければならない。

さらに、セキュリティ監査についても、何らかの措置をとることが望ましい。

2．定義

このポリシーの用語の定義については、「情報セキュリティポリシーに関するガイドライン」に定める定義と同様とし、附録１に示す。

3．対象範囲

ポリシーの対象範囲は、当該大学の情報資産に加えて、当該大学以外のコンピュータ

で、当該大学のネットワークに一時的に接続されたコンピュータを含む。

ポリシーの対象者は、教職員、臨時職員、非常勤教職員、委託業者、大学院生、大学生、研究生、来学者などとする。

４．実施手順の作成

ポリシーの具体的な実施手順は、全学的に定めることが望ましいが、大学の規模・構成を鑑み、部局毎に定めてもよい。

Ⅱ　対策基準

１．組織・体制

1.1 管理・運用組織の構成

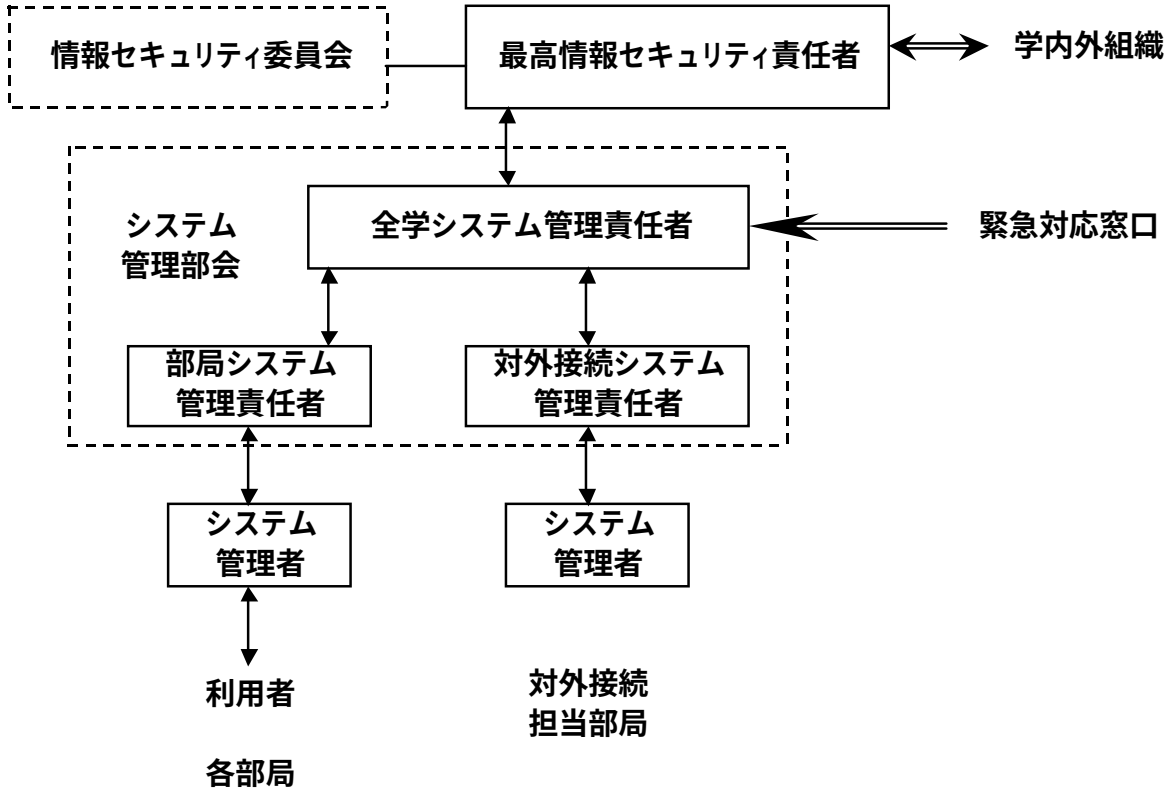


図　1　組織の構成図

1.1.1 最高情報セキュリティ責任者

- 全学の情報セキュリティに関する総括的な意思決定と、学内、他の組織および学外に対する責任を負う。副学長相当の役職と考えるのが適当である。役割等の詳細は、4.1.1 に述べる。

1.1.2 全学システム管理責任者

- 全学の情報システム管理の実施に関し、緊急時の連絡など、総括的な対応に当り、最高情報セキュリティ責任者を補佐する。役割の詳細は 4.1.2 に述べる。

1.1.3 部局システム管理責任者

- 部局内の情報システム管理の実施に関し、全学システム管理責任者との連絡などの

対応に当り、システム管理者を統括する。なお、部局のとらえ方について、建物等の管理運用の単位、もしくは、学部等の組織運営の単位、の二通り意味があり、両者が一致しない場合には、状況に合わせて適切な定義を選択する必要がある。

1.1.4 情報セキュリティ委員会

- 全学の情報セキュリティに関し、基本的なセキュリティポリシーの策定および重要事項の決定を行うとともに、対外的な対応等を行う。
  - ・セキュリティポリシーの策定と改訂。
  - ・セキュリティポリシーの遵守の励行および違反に対する措置。
  - ・教育研究活動におけるネットワークの利用ルールの制定。
  - ・学内の他の意思決定機構との調整。
  - ・外部との折衝。
- 情報セキュリティに関する啓発および教育について、部局システム管理責任者とシステム管理者に対するレベルの高い教育を行うとともに、一般の利用者に幅広く初心者教育を行う。
- 最高情報セキュリティ責任者が委員長となり、各部局の代表者（以後、部局情報セキュリティ委員という。）および全学システム管理責任者等で構成する。

1.1.5 システム管理部会

- 全学の情報システムのセキュリティ管理を実施するための連絡調整および部局システム管理責任者への技術的助言等の支援を行う。
  - ・24 時間 365 日、ネットワークの動作状況と不正アクセスの監視。
  - ・緊急事態に対応する CERT（緊急対応チーム）のような即応体制の確立。
  - ・情報セキュリティに関する情報の周知。
  - ・セキュリティ監査の実施。
- 情報セキュリティ委員会の下に置き、全学システム管理責任者が主査となり、部局システム管理責任者等で構成する。

1.1.6 注意事項

情報セキュリティ委員会およびシステム管理部会は、その責務を効率的に遂行するため、次の事項に注意することが適当である。

- 大規模な大学においては、部局に情報セキュリティに関する委員会を設けて、全学的な情報セキュリティ委員会を支援すれば、円滑に運用できると考えられる。部局情報セキュリティ委員がその委員会の長となるのが適当である。
- 部局情報セキュリティ委員が、当該部局と情報セキュリティ委員会との窓口的役

割を果たすことが望ましい。

- 組織の管理運用の単位(部局)と、サブネットワークの構成等、ネットワークの管理単位を一致させることが望ましい。複数学部で１つのサブネットワークを共有するのは避けたほうがよい。ただし、末端までのネットワークの責任の所在が分かりにくくなる等の弊害が考えられるので、ネットワークの管理階層を深くしすぎないよう、できるだけフラットにするよう注意しなければならない。
- 外部ネットワークとの接続は一つの部局に管理を集約することが望ましい。
- 対外接続について、それを担っている部局(情報基盤センター、情報処理センター等)はその部局自身に対する対応の他に、対外接続に対する体制も持つ必要がある。
- 事務情報（経理、人事など）と医療情報等については、別個にサブ体制を整えることもありうる。
- システム管理部会は、24 時間 365 日、緊急に対応する必要があり、情報セキュリティ委員会はそのための要員または費用を準備することが重要である。
- 学内の組織変更、ネットワーク構成の変更等に対応できるよう、変更方法のマニュアル化などを行うべきである。

1.2 不正アクセス等への対応

システム管理部会は、外部または内部からの不正アクセスを検出した場合、情報セキュリティ委員会が定めた緊急措置手順に従い、関連する通信の遮断または該当する情報機器の切り離しを実施する。ただし，あらかじめ手順に定められていない状況には、最高情報セキュリティ責任者が判断する。

情報セキュリティ委員会は，不正アクセスが継続する場合に、当該情報機器またはそれを接続するネットワークについて、定常的な利用の停止などの抑止措置をとることができる。

情報セキュリティ委員会は、不正アクセスを行う等セキュリティ規定に違反した大学構成員の身分に関する処分について、その権限を有する意思決定機構（教授会，評議会，理事会等）に対し、違反行為の報告および処分の勧告を行う。当該機構は、この報告および勧告に沿って処分を決定することが妥当である。

情報セキュリティ委員会による措置、報告および勧告に際し、当該構成員(必要であれば、外部組織を含む)に調査と判断の内容を開示する手続きを定めるとともに、内容に不服がある場合の異議申し立て方法が決められていることが必要である。

２．情報の分類と管理

サーバに保存された情報は、職務上定められたシステム管理者が管理しなければならないが、個人的に管理されたパソコン内の情報に関しては、そのパソコンのシステム管理者と利用者が管理しなければならない。どの範囲で情報共有するか、非公開情報の情報開示にはどのような加工をするか明確にしておく必要がある。

2.1 アクセス制限

情報の内容に応じて、情報にアクセス可能な利用者を定めなければならない。非公開と公開という 2 種類の区別のほかに、経理系事務限定、研究室内限定のように公開の範囲を限定する必要のある情報がある。

利用者は、アクセス権のない情報システムや情報に入り込もうとしてはならない。意図的でなく入り込んだときは、速やかに出てくるよう周知徹底するべきである。

アクセスの制限方法としては、ID とパスワード、IC カード、入退室管理、VLAN による接続制限などが考えられる。

2.2 情報の分類

それぞれの情報について、公開・非公開を定めること。

2.2.1　非公開情報

- 許可された者以外がコンピュータに非公開情報を保管してはならない。また、一時的であっても、教職員が日常的に使用するコンピュータに非公開情報を不特定の者が可読な状態で複製してはならない。
- 非公開情報を扱うネットワークは、学術研究・教育用の一般ネットワークと論理的に異なるべきである。できれば、物理的に異なる回線を利用することが望ましい。さらに、暗号化や、盗聴防止策を講じることが望ましい。
- 一般ネットワークと非公開情報ネットワークの間でアクセスする必要がある場合は、非公開ネットワークからのみアクセス可能としなければならない。さらに、両ネットワークの接続点を必要最小限とすべきで、できれば必要なときのみ通信を可能とすることが望ましい。
- 物理的な盗難等を防止するため、利用を許可された場所から外部に非公開情報を持ち出してはならない。同様に、盗聴防止のため、インターネット等の公衆回線を介して不特定の者が傍受可能な方式で非公開情報にアクセスすることも原則禁止する。
- 外注などのため、非公開情報を限定された第三者に開示する必要がある場合は、開示の都度、守秘義務契約を結ばなければならない。
- 非公開情報の一部を公開することは技術的に不可能である。

2.2.2　公開情報

- 公開情報は任意の場所からアクセス可能な性質を持つため、情報の改ざんや偽情報

の流布に対し、2.3 に掲げる防止策を講じなければならない。

2.2.3　発信情報(プッシュ型メール等)

- 大学側から不特定多数の者に発信する情報を言う。発信情報は公開情報と同じく 2.3 に掲げる防止策を講じるだけでなく、正規の発信者であることを証明する必要がある。

2.3　情報の公開化

非公開情報を公開化する場合には、個人情報の漏洩、プライバシーや著作権の侵害に十分注意し、公開できる情報だけを抽出する、あるいは、統計処理などの加工を行う必要がある。

2.4　情報の限定公開

情報の中には、特定の利用者に特定の情報を開示する必要が生じる。例えば、成績情報に対する担当教員または学生のアクセスがこれに該当する。情報の登録および閲覧は、許可された者が許可された操作だけを行えるように、認証およびアクセス制御機能を設けなければならない。さらに、異常な登録や閲覧が行われていないか、定期的に状況を確認しなければならない。

2.5　情報改ざんおよび偽情報流布の防止

非公開情報および公開情報の原本は、CD-ROM/CD-R 等の書き換え不能な記憶媒体に保存するなどにより原本性を保証しなければならない。また、それぞれの情報ごとにシステム管理者を設けなければならない。

一方、公開情報は改ざんへの対策を講じなければならないが、常に進化する不正アクセス技術の脅威に対し、改ざんを受けた場合の速やかな回復機構も備えなければならない。さらに、公開情報(Web での掲示情報やメールマガジンによる情報発信を含む)の複製・加筆による偽情報の作成および流布を防止するため、原本性の維持に努める必要がある。このため電子署名の導入を検討することが望ましい。

2.6　情報機器および記憶媒体の処分

公開・非公開を問わず、情報機器および記憶媒体を破棄する場合は、その処分方法に注意しなければならない。特に、ハードディスクおよびフロッピーディスク等の記憶媒体は、通常の消去操作では管理情報のみが消去されるだけでデータそのものは消去されないため、また、数回の上書き消去では残留磁気情報の読み出しによって、情報を復元できる点に十分配慮しなければならない。

さらに、情報機器の記憶媒体を保守契約により交換する場合、またはレンタル機器の撤去を行う場合は、撤去後の記憶媒体の処理法についても十分配慮しなければならない。

３．物理的セキュリティ

3.1 クライアント機器

3.1.1　クライアント機器の定義

・クライアント機器とは、主としてパーソナルな利用で用いられ、他の情報機器へアクセスすることで処理を進めていくものを指す。後で示すサーバ機器に対するものである。

・システム管理部会は対象となるクライアント機器を把握しなければならない。

3.1.2　クライアント機器の使用

・大学内にクライアント機器を設置する場合（据付および一時的設置のいずれにおいても）、利用者がクライアント機器を使用する前に物理的認証または電子的認証、あるいは、両方を経るべきである。

・電子的認証を用いる場合、ディスクブートによる電子的認証すり抜けに対する対策を施さなければならない。

3.1.3　据付型クライアント機器の盗難対策

・据付型クライアント機器が犯罪者によって学外に持ち出されないよう何らかの対策を施さなければならない。

3.1.4　ネットワークへの接続

・有線（ネットワークケーブル）を使用する場合には、過失によるケーブル切断を防ぐための措置を施すべきである。

・有線、無線どちらの場合においても、ネットワークの盗聴に対する対策を施すべきである。

・クライアント機器接続用のネットワークケーブルに違うコンピュータが接続されないよう、物理アドレスと IP アドレスの対比表を定期的に検査すべきである。

3.1.5　貸出型クライアント機器の備品管理

・大学構成員がクライアント機器を学外へ持ち出す場合においては、貸し出しの事実について記録しなければならない。

・クライアント機器経由による秘密または非公開情報の漏洩が発生しないよう留意すること。

・学外持ち出しを想定した専用のクライアント機器を準備するのも一法である。

・非大学構成員がクライアント機器を学外に持ち出すことは、原則として禁止すべきである。

3.1.6　保守

・保守においては、パスワードやシステム設定情報などの非公開情報の開示について守秘義務契約を結ぶべきである。

3.2 サーバ機器

3.2.1　サーバ機器の定義

・サーバ機器とは、複数のクライアント機器からアクセスされ、共同で利用される情報機器をいう。その停止は多くの利用者に影響を与えるため、セキュリティを守ることが肝要である。

3.2.2　管理区域の設置

・サーバ機器は設定された管理区域に設置されなければならない。コンソールも同様である。

・管理区域内はサーバ機器の動作補償範囲内の温度、湿度を 24 時間保つべきである。

・管理区域の物理的隔離の度合いは守るべきサーバの重要性に応じて段階的に設定されるべきである。重要なサーバとは、停止したときに大学内の業務遂行に重大な支障をきたすサーバを指す。重要なサーバ機器に対しては物理的に区切られており、第三者の認証と入退室の記録が残される区域を設定すべきである。一方で重要度の軽微なサーバ機器については、鍵などによる認証による入退室管理形態であっても良い。

・管理区域の物理的な場所は、当該サーバ機器のシステム管理者以外には公開すべきではない。

3.2.3　電源

・電源を供給する際には、電圧の流動や突発的な停電、過電流に対応する装置を経由することが望ましい。

3.2.4　ネットワークへの接続

・有線（ネットワークケーブル）を使用する場合には、過失によるケーブル切断を防ぐための措置を施すべきである。

・有線、無線どちらの場合においても、ネットワークの盗聴に対する対策を施すべきである。

3.2.5　データのバックアップ

・サーバ機器に記録されるデータは、定期的にバックアップすべきである。

・バックアップスケジュールは、サーバ機器の重要度に応じて決定されるべきである。

・データをバックアップしたメディアは、温度と湿度が適切な場所に保管されるべきである。重要なデータについては、バックアップを複数本作成し、物理的に離れた場所に個々に保管することを検討すべきである。

・データをバックアップしたメディアは、認証による入退室管理が行われている管理区域内に保管するべきである。

3.2.6　多重化

・ダウンタイムを短くすることを求められるサーバ機器については、多重化を検討すべきである。多重化した場合には、順番に運用機を切り替えるか、一定時間ごとにチェックするなどして、スタンバイ機が故障してないことを確かめる必要がある。

3.2.7　サーバ機器盗難への対策

・サーバ機器が管理区域から持ち出されないよう何らかの対策を施さなければならない。

3.2.8　災害への対策

・重要なサーバ機器は、耐震を考慮した据付を行うべきである。

・管理区域には、火災の一次消火手段が提供されるべきである。

3.2.9　保守

・保守においては、保守部品をできるだけ確保し、迅速に保守を行える体制を整えるべきである。

・保守においては、パスワードやシステム設定情報などの非公開情報の開示についての守秘義務契約を結ぶべきである。

3.3　ネットワーク機器

3.3.1　コンソールポートの隔離

・ルータ、インテリジェントスイッチは、コンソールポート、管理ポートが許可された特定のシステム管理者以外は使用できないように施錠などによって物理的に隔離された区域に設置しなければならない。

3.3.2　設置場所の秘匿

・バックボーンを構成する機器をはじめ、重要と思われるネットワーク機器については、その設置場所を限られたシステム管理者以外に公開すべきではない。

3.3.3　ネットワーク接続ポート

・原則として、物理的認証または電子的認証、あるいは、両方を経た後でなければ、ネットワーク接続ポートにコンピュータを接続してはならない。
・学会等のために期限を設定して来学者に接続ポートを開放する場合には、そのネットワークセグメントから学内へのアクセスは制限することが望ましい。

3.3.4　ネットワークケーブル

・バックボーンを構成するネットワークケーブルは、故意または過失によるケーブル切断を防ぐためにシールド等の措置を施さなければならない。他に重要と思われるネットワークケーブルについても同様にケーブル切断のための措置を講ずるべきである。
・有線、無線どちらの場合においても、ネットワークの盗聴に対する対策を施すべきである。

3.3.5　多重化

・機器の障害によるネットワーク断が重大な影響を及ぼすようなネットワーク機器については、多重化による信頼性の向上を検討すべきである。

3.3.6　保守

・保守においては、保守部品をできるだけ確保し、迅速に保守を行える体制を整えるべきである。
・保守においては、パスワードやネットワーク構成などの非公開情報の開示についての守秘義務契約を結ぶべきである。

４．人的セキュリティ

4.1. 役割・責任および免責事項

4.1.1 最高情報セキュリティ責任者

・最高情報セキュリティ責任者は、情報セキュリティ委員会で策定されたポリシーに基づき、学内のすべての情報セキュリティに関する総括的な権限と責任を有する。
・最高情報セキュリティ責任者は、情報セキュリティ委員会を構成する部局情報セキュリティ委員を通じて、すべての部局にポリシーの遵守を励行させる。
・最高情報セキュリティ責任者は、情報システムの円滑な運用に必要な措置を全学システム管理責任者に指示し、全学システム管理責任者が行った緊急避難措置に対処する。
・全学システム管理責任者による定常的なセキュリティ対策の措置、ならびに、セキュリティ管理の状況に関する報告に対処する。
・最高情報セキュリティ責任者は、学内の最高意思決定組織（理事会、評議会、教授会等）への情報セキュリティに関する重要事項の報告または勧告を行う。
・最高情報セキュリティ責任者は、情報セキュリティに関する学外からの苦情への対応（損害賠償請求など法的対応部署との連携を含む）、ならびに、学外から受けた被害への対応（被害回復請求など）にあたる。

4.1.2　全学システム管理責任者

・全学システム管理責任者は、全学の情報システムが円滑に運用されるように、情報セキュリティの保持と強化のための技術的な調査検討を行うとともに、緊急時の総括的な連絡窓口として機能する。これらの技術的対応の実施において、時間や曜日と無関係に即時対応できる体制が必要である。
・全学システム管理責任者は、情報セキュリティを守るために必要と判断したときは、緊急避難措置をとることができる。ただし、その措置によって影響を及ぼすと判断できる情報資源のシステム管理者に、その旨を速やかに通知しなければならない。システム管理者から対応策の実施が完了した旨の届が提出されたときは、速やかに対応策を検討し、十分であると判断した場合は、緊急避難措置を直ちに解除する。部局システム管理責任者およびシステム管理者から緊急避難措置の依頼があった場合も必要性を判断し同様に扱うものとする。
・全学システム管理責任者は、全学の情報セキュリティの管理および監査の実施に関し、最高情報セキュリティ責任者を補佐し、情報セキュリティの保持と強化のために必要な技術的措置を提案する。
・全学システム管理責任者は、システム管理部会において情報セキュリティの保持と強化のために必要な技術的措置を部局システム管理責任者に指示し、情報を提供す

るとともに、実施に関する協議を行う。

4.1.3　部局システム管理責任者

・部局システム管理責任者は、当該部局の情報システムが円滑に運用されるように、情報セキュリティの保持と強化のための技術的な調査検討と対策の実施にあたる。
・部局システム管理責任者は、システム管理者に対し情報システムの円滑な運用のために必要な技術的措置を提案する。
・部局システム管理責任者は、当該部局内において情報セキュリティを守るために必要と判断したときは、緊急避難措置をとることができる。緊急避難措置をとった場合には、全学システム管理責任者と部局情報セキュリティ委員にその事実を速やかに報告しなければならない。

4.1.4　システム管理者

・システム管理者は、個々の情報システムを維持・管理する者で、運用に則したパラメータの設定やセキュリティパッチの実施などセキュリティを維持するための責任を持つ。大学においては、パソコンのような場合、使用する教員がシステム管理者となることが多い。使用者が学生でもシステム管理者は教員である。
しかし､教員の監督下において大学院生などにシステム管理業務を補助させる場合、大学院生によるシステム管理業務の責任と権限の範囲を明確に定め、これを厳守させなければならない｡ただし､最終的な責任は教員にあることを忘れてはならない。

4.1.5　利用者（教職員および学生）

・すべての教職員および学生は、情報セキュリティ委員会が策定したポリシーを遵守しなければならない。学生も情報システム利用者の一員として、情報セキュリティを維持する義務を有する。
・ポリシーおよび実施手順を遵守して、利用しなければならない。さらに、システム管理者からセキュリティ維持管理のために協力を依頼された場合には従わねばならない。

4.2　教育研究上の利便性の配慮

・情報セキュリティ対策について教育研究上の利便性を著しく損なう点、遵守することが現実的に困難な点については、最高情報セキュリティ責任者またはシステム管理者に対して、ポリシーおよび実施手順の改善を求めることができる。
・教職員および学生は、システム管理者の許可を得ずに情報端末等を執務室、研究室および教室外に持ち出してはならない。ただし、モバイル端末は、教育研究上の利便性を考慮し、その利用者の管理責任において、これを持ち出せるよう配慮することが望

ましい。
・教職員および学生以外の者（来学者）に学内の情報システム（公共情報端末や情報コンセントを含む）を一時的に使用させる場合においては、その利用者が守るべきポリシーを定め、これを厳守させるよう適切な措置を施さなければならない。

4.3　教育・研修

・情報セキュリティ委員会は、部局システム管理責任者向けの研修を開催しなければならない。
・情報セキュリティ委員会は、部局システム管理責任者がシステム管理者に行う研修プログラムの実施に必要な措置を施さなければならない。
・情報セキュリティ委員会は、システム管理者等が行う教職員向けのポリシーに関する研修の支援をしなければならない。また、教員が行う学生向けのポリシーに関するオリエンテーションまたは講義に協力しなければならない。
・すべての教職員および学生は、研修会や説明会または講義等を通じ、ポリシーおよび実施手順を理解し、情報セキュリティ上の問題が生じないように努めなければならない。

4.4　事故・障害の報告

・教職員および学生は、情報セキュリティに関する事故、情報システムの不審な動作、公開情報の改ざん、システム上の障害および誤動作を発見した場合には、部局システム管理責任者またはシステム管理者に直ちに報告しなければならない。
・部局システム管理責任者およびシステム管理者は、報告のあった事故等についてすべて全学システム管理責任者と部局情報セキュリティ委員に通知するとともに、必要な措置を直ちに講じなければならない。必要ならば、全学システム管理責任者に措置に関して指示または支援を要請すること。
・全学システム管理責任者は、発生したすべての情報セキュリティ上の事故等に関する記録を一定期間保存し、情報セキュリティ委員会に報告するとともに、重大な事故に対しては、迅速な再発防止のための対策を講じなければならない。
・一般利用者に対する情報セキュリティ上の事故・障害の通知は、問題の程度に応じた適切な表現に配慮し、速やかに行わなければなければならない。
・学内からの不正アクセスによって学外に被害を及ぼし、その事実関係の説明を被害者または第三者から求められた場合の対応手順を、規定として定めなければならない。
・事故等について、情報処理振興事業協会（IPA）の届出様式により、電子メールまたは FAX で速やかに大臣官房政策課情報化推進室に報告するとともに、IPA セキュリティセンター不正アクセス対策室に届けることと定められている。さらに、必要に応じて警察のネットワーク犯罪担当部署に相談などを行うこと。

4.5　パスワード管理・ログ管理

4.5.1　一般利用者向け

・自己のパスワードは秘密としなければならない。また、十分なセキュリティを維持できるよう、自己のパスワードの設定および変更に配慮しなければならない。
・他の利用者のアカウントを使用してはならない。
・いかなる場合も他の利用者のパスワードを聞き出してはならない。
・部局システム管理責任者またはシステム管理者が、不適切なパスワードの変更を求めた場合、利用者はその指示に従わなければならない。
・システムの管理権限を有する者や他の利用者になりすました第三者からのパスワードの聞き取りには、如何なる場合も応じてはならない。

4.5.2　システム管理者向け

・情報システムの利用資格者の規定を定めなければならない。
・規定に基づく利用資格を有する者以外に情報端末のアカウントを発行してはならない。また、利用資格を失った利用者のアカウントは、直ちに削除されなければならない。
・利用者のアカウントを管理権限のない第三者に漏洩してはならない。また、いかなる場合にも利用者からパスワードを聞き取りしてはならない。
・ログ情報および通信内容の解析等にあたっては、利用者のプライバシーに配慮し、閲覧解析を認める場合の要件と手続きを定めなければならない。

4.6　非常勤教職員および臨時職員ならびに外部委託

4.6.1　教務および事務系業務

・非常勤教職員および臨時職員（外部委託事業者を含む）には、雇用契約の際に、守るべきポリシーの内容を理解させ、実施および遵守させなければならない。

4.6.2　情報システムの開発および保守ならびに管理業務

・情報システムの開発および保守ならびにシステム管理業務を外部委託事業者に発注する場合は、外部委託事業者から下請けとして受託する業者を含めて、ポリシーのうち外部委託事業者が守るべき内容の遵守を明記した契約を行わなければならない。
・外部委託事業者との契約書には、責任所在の境界、ならびに、ポリシーが遵守されなかった場合の規定を定めなければならない。

５．技術的セキュリティ

5.1　基本方針

5.1.1 対外接続の方針と例外規程

内部ネットワークと外部ネットワークを接続する場合の接続セキュリティレベルは組織によって異なる。もっとも極端な例は、すべて開放とすべて閉鎖である。組織として、その両極端の間でどのようなレベルの接続セキュリティレベル方針を採用するかは、組織のネットワーク設計や運用と密接に関係する問題であり、簡単には決められない。ネットワーク社会の一員としては、外部に脅威を与えないために、適切な対外接続方針の確立とそれに基づいたネットワーク運用が要求されている。

すべて開放に近い方針を採用する場合には、セキュリティの確保は、ネットワークに接続される端末管理者のスキルや管理様態に大きく依存する。従って、情報セキュリティ委員会は、ネットワークに接続する機器の満たすべき技術的基準、機器管理者の義務と責任範囲を明示し、端末管理者のスキルや管理様態が平準化されるようにすべきである。

すべて閉鎖に近い方針を採用する場合には、情報セキュリティ委員会は外部に開放するサービスやネットワーク機器の満たすべき技術基準や認定基準を定め、構成員に明示しなければならない。すべて閉鎖方針のネットワークであっても、WEB のスクリプトウィルスの例で明らかなように、すべての脅威からネットワークやネットワーク端末を防護できるわけではないので、この点を十分に理解しておかなければならない。

どのような外部接続方針を採用するにしろ、対外接続方針の策定とネットワーク設計は不可分である。そして、常に、外部からの脅威だけでなく内部からの脅威にも対処でき､かつ外部に害を与えないネットワーク設計と運用が必要である｡技術的には、不適切な通信を検知したり、遮断する機能の採用が最低限必要である。

5.2　ネットワーク運営方針

5.2.1 ネットワーク設計、機器導入および設定

(1)ネットワーク設計および改変

・大学での新たなネットワークの設計・構築にあたっては、事務、教務、医療、教育、研究といった目的の異なるネットワークトラフィックを物理的または論理的に混在させないことが重要である。

・情報セキュリティ委員会の許可を得ないネットワークの改変を禁じる。

(2)ネットワーク機器

・ルータやソフトウェア設定可能なハブ等の機器のシステム管理者は、機器障害や権限のないアクセスによって機器の構成や制御機能が損なわれないように管理し

なければならない。また、これらの機能を常に最新のものとするように努めなければならない。

(3)セキュリティ機器およびその運用

情報セキュリティ委員会は、ファイアウォールおよび侵入検知システムその他の必要と思われるセキュリティ機器を導入・運用し、外部からの脅威や内部から外部への攻撃に対処できるようにすべきである。さらに、これらの機器をネットワーク性能の向上や、新たな脅威の出現に対応可能なように、最新のものにすることが重要である。

大学のネットワークを利用しようとするものは、情報セキュリティ委員会が設置したネットワーク侵入検知システムその他によるトラフィックの検査を受け入れなければならない。拒否をする場合には、自前で別のネットワークを構築するよう指導することが妥当である。

5.2.2 ネットワークサービス選択

情報セキュリティ委員会は、構成員に対して、利用可能なネットワークサービスと利用形態を決定し、構成員に公表する。また、外部に対して、大学内ネットワーク上のどのような資源をだれに提供するかを決定する権限を持つ。

構成員は、情報セキュリティ委員会のこの決定に対して、異議を申し立てることができる。

5.2.3　ネットワークの無許可利用およびネットワークバックドアの排除

・ネットワークに接続する装置は、不特定多数の手に触れさせてはならない。

・ネットワークのセキュリティ機能の管理を回避する目的でのバックドア（PPP サーバ、コンピュータに接続する公衆回線、VPN 装置およびソフトウェア等）の設置を原則禁止する。

・情報セキュリティ委員会の許可を受けて、独自のハードウエア回線等を設置した場合には、情報セキュリティ委員会の求めに応じて、運用状況を報告しなければならない。

5.2.4 ネットワークの日常運用

ネットワークのバックボーンを担当するシステム管理者は、ファイアウォールや侵入検知システムのログを一定期間保存しなければならない。サーバ機器のシステム管理者は、情報システムへのアクセス記録を取得し一定期間保存しなければならない。定期的にそれらのログを分析し、侵入の試みがなされていないかなどをチェックすることが必要である。

システム管理部会が、ネットワークの監査を行う必要があるが、専門家に依頼して

外部からネットワークのセキュリティ監査を行うことも重要である。

5.3　端末機器等に関する基準

5.3.1 基本方針

ネットワークに接続を許される機器の満たすべき最低限のセキュリティ対策基準を示す技術ガイドラインを、セキュリティポリシーに従って策定すべきである。ガイドラインの基準に満たない機器をネットワークに接続してはならない。

システム管理者は、ガイドラインにかかわらず、常に最新のセキュリティ情報に注意を払い、端末機器を安全に運用できるように努力しなければならない。

システム管理者は、情報セキュリティ委員会の要請に応じて、ログ等の運用に関する情報を情報セキュリティ委員会に対して開示しなければならない。

5.3.2 端末機器設置運用基準

接続する機器は、利用者を何らかの方法で認証（部屋の入退室管理といった物理的な方法でも可）できなければならない。

機器を設置しようとするものは、設定作業（セキュリティ対策を含む）の完了していない装置をネットワークに接続してはならない。

機器の管理者は、設置機器の利用者を特定可能でなければならない。

６．評価・見直し

6.1 ポリシーの運用実態

最高情報セキュリティ責任者は、ポリシーの運用実態等を把握するため、情報セキュリティ委員会およびシステム管理部会に対し、次のような措置を求めなければならない。

6.1.1 ポリシー運用実態等の把握

全学システム管理責任者は、システム管理部会を定期的に開催し、収集した情報を分析・整理した上で、情報セキュリティ委員会に報告しなければならない。情報セキュリティ委員会は、この報告、ならびに、部局情報セキュリティ委員を通じて得られた全学におけるポリシーの運用実態に基づいて、定期的および必要に応じて随時検討し、ポリシーの不完全さを認識しなければならない。

6.1.2 利用者の意見

部局情報セキュリティ委員は、部局教職員および学生からポリシー遵守に関する意見を収集し、情報セキュリティ委員会に報告しなければならない。システム管理者経由で日々得られる意見も含めて収集すること。

6.1.3 情報セキュリティ診断

全学システム管理責任者は、情報システムの機密性、完全性および可用性ならびに犯罪予防の観点から情報システムに対する情報セキュリティ診断を実施すべきである。その結果をシステム管理部会において情報セキュリティ診断として取りまとめ、情報セキュリティ委員会に報告しなければならない。

診断過程で重大なセキュリティの脆弱性が発見された際は、緊急避難措置をとるとともに、部局システム管理責任者と部局情報セキュリティ委員にその事実を速やかに連絡しなければならない。

6.1.4 情報セキュリティ監査

全学システム管理責任者は、定期監査および抜き打ち監査を実施し、各部局が法令ならびにポリシーおよびこれに関連する規定・基準等を遵守しているか運用実態を把握すべきである。その結果をシステム管理部会において情報セキュリティ監査結果として取りまとめ、情報セキュリティ委員会に報告しなければならない。

診断および監査の実施において、実際に擬似アタック等を行う場合には、アタックを行うIPアドレスを学内に知らせるとともに、ホスト名をそれと判る名称にしておくことが、無用なトラブルを回避するために有効である。

6.1.5 セキュリティ対策費

情報セキュリティ委員会は、情報セキュリティ対策に要した直接的経費を把握しなければならない。システム管理部会が不正アクセス等の検出のために購入した装置（ハードウェア、ソフトウェア、ソフトウェアのバージョンアップを含む）、システム管理者が購入したウイルス対策ソフトウェア、外注したセキュリティ診断および監査などに要した費用が含まれる。

情報セキュリティを維持し続けるためには、経費を正しく見積もり、予算措置をとることが不可欠である。予算がないために重大な情報セキュリティの脆弱性を放置する事は許されない。

6.2 セキュリティレベル向上策

最高情報セキュリティ責任者は、ポリシーに添った対策がどの程度実施されているかを評価するとともに、セキュリティレベルの向上に必要な措置を講じるため、情報セキュリティ委員会を年1回以上召集しなければならない。

6.2.1 ポリシーの更新

情報セキュリティ委員会は、6.1の結果に基づき、ポリシーの実効性を少なくとも年１回評価し、必要な部分を見直して内容の変更および実施時期の決定を行い、よりセキュリティレベルの高い、かつ、遵守可能なポリシーに更新しなければならない。ポリシーを更新しないでいると、陳腐で役に立たないものになることは、容易に予測できる。

6.2.2 情報セキュリティ計画および予算案の作成

情報セキュリティ委員会は、評価・見直しの結果を踏まえ、次年度の情報セキュリティ計画および予算案の作成を行わなければならない。

6.2.3 報告義務

最高情報セキュリティ責任者は、学内の最高意志決定組織（理事会、評議会、教授会等）に評価・見直しの結果を報告しなければならない。さらに、ポリシーの遵守を啓発するためにも、その要約を全学の構成員に提示しなければならない。

図1　大学における情報セキュリティポリシーの概要

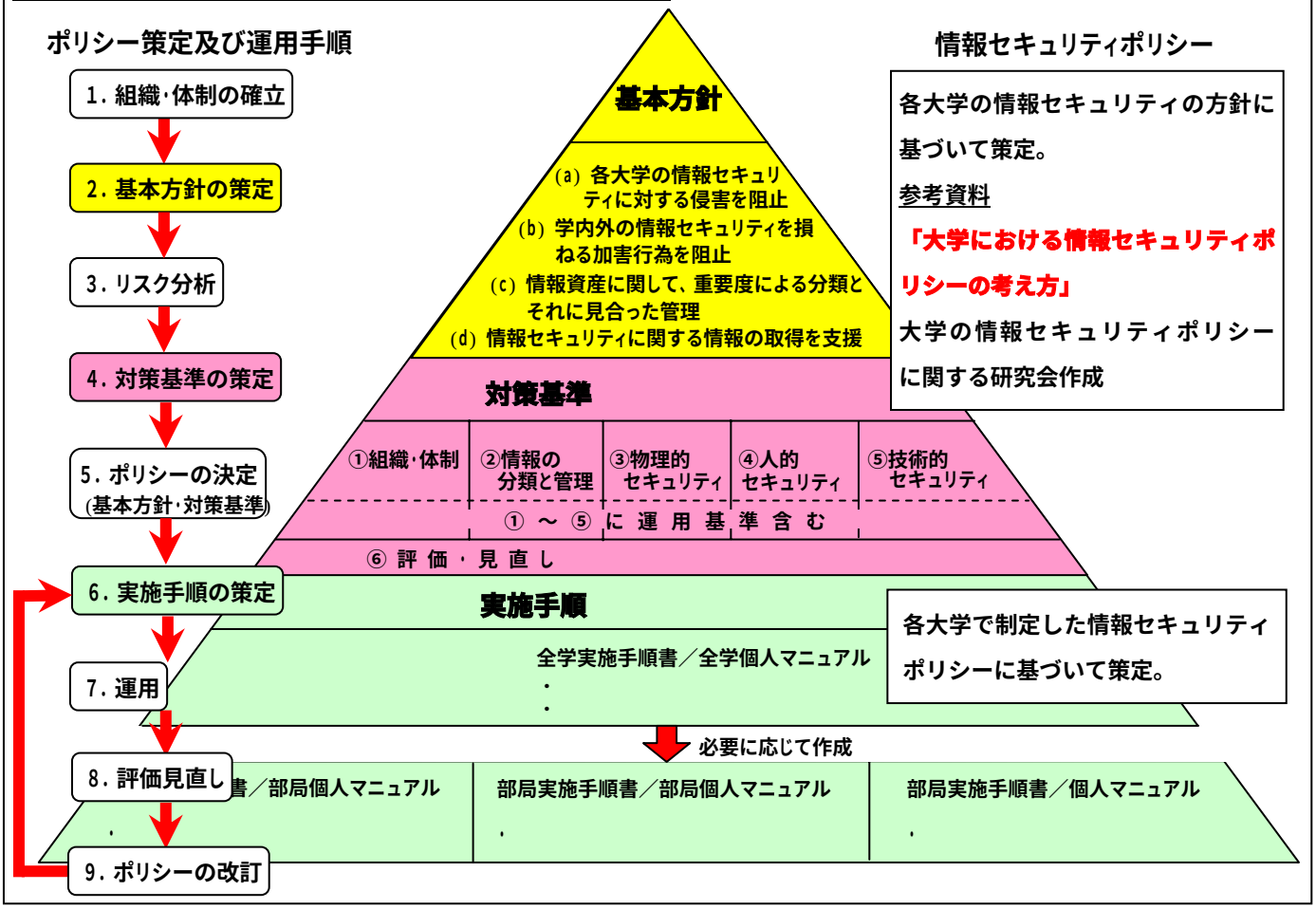
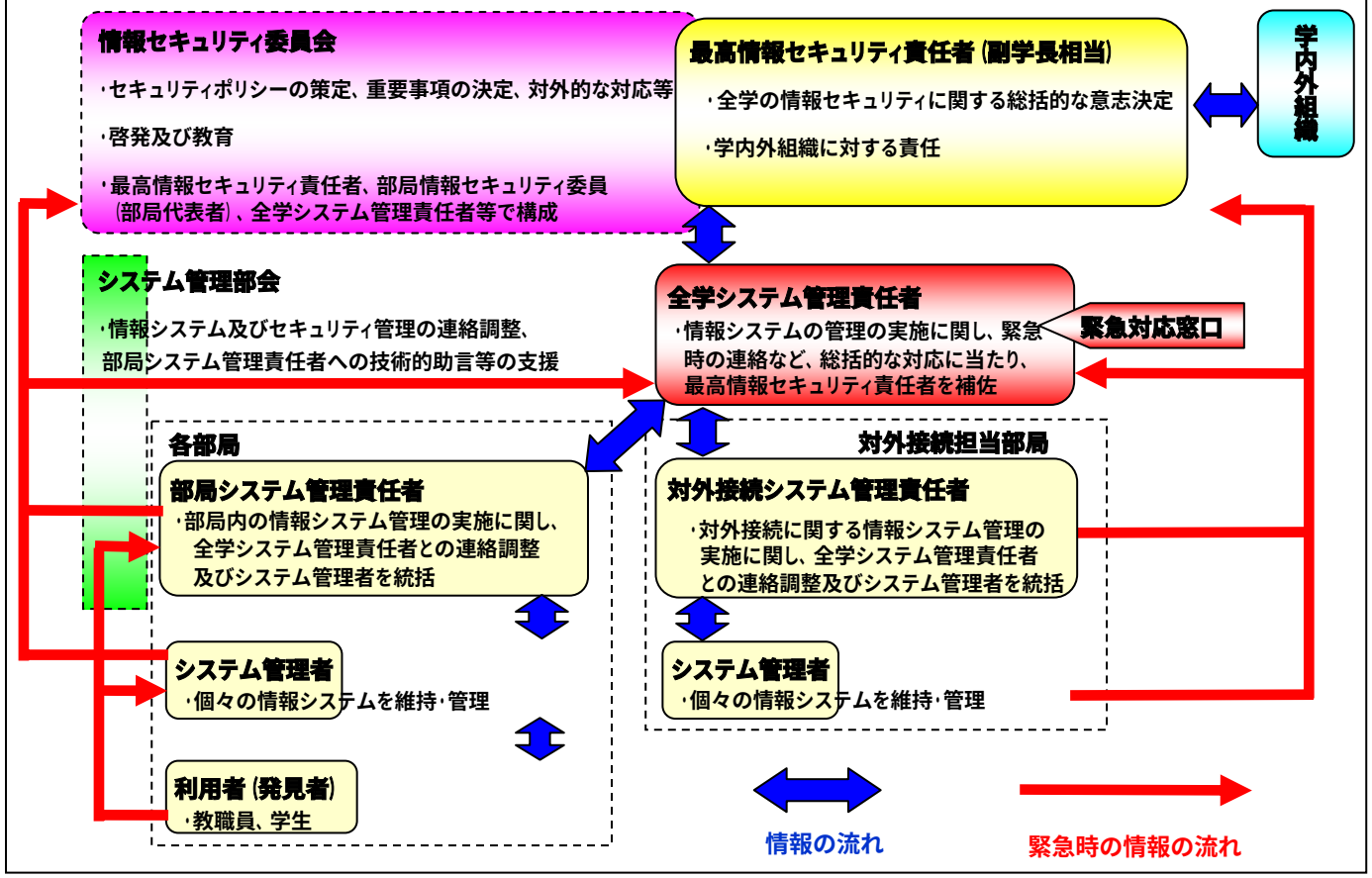


図2　組織・体制（緊急時対応体制）



付録１　用語の定義

・情報システム等

ネットワーク機器（ルータ、ファイアウォール、ハブ、ケーブルなど）、サーバ、パソコン、基本ソフトウェア、応用ソフトウェア、システム設定情報（パスワードファイル等）、記録媒体（MO,FD）、システム構成図、持ち込まれたノートパソコンなどの総称。

情報システムに記録される情報とは、アクセス記録(ログ)、文書及び図面等の電磁的記録を指す。

・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）の総称である。電磁的に記録された情報すべてを含む。

・情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することである。

機密性とは、情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性とは、情報及び処理方法の正確さ及び完全である状態を安全防護すること。

可用性とは、許可された利用者が、必要なときに情報にアクセスできることを確実にすること。

・情報セキュリティポリシー

当該大学の情報セキュリティ対策について、当該大学が総合的・体系的かつ具体的にまとめるもので、根本的な考えを示す情報セキュリティ基本方針と、情報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の基準を示す情報セキュリティ対策基準からなる。

・情報セキュリティ実施手順等

情報セキュリティ対策基準に定められた内容を具体的に情報システムにおいて、どのような手順に従って実行していくのかを示すもの。

付録２　情報セキュリティ関係法令

１．主な情報セキュリティ関係法令

・不正アクセス行為の禁止等に関する法律
・行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律
・行政機関の保有する情報の公開に関する法律
・電子署名及び認証業務に関する法律
・著作権法
・不正競争防止法
・犯罪捜査のための通信傍受に関する法律
・刑法
　第７条の２（定義）
　第１５７条第１項（公正証書原本不実記載等）
　第１５８条第１項（偽造公文書行使等）
　第１６１条の２（電磁的記録不正作出及び供用）
　第２３４条の２（電子計算機損壊等業務妨害）
　第２４６条の２（電子計算機使用詐欺）
　第２５８条（公用文書等毀棄）
　第２５９条（私用文書等毀棄）

※電子政府の総合窓口の法令データ提供システムを参照すること。
（http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi）

２．施行が予定されている法律

・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律

※総務省のホームページを参照すること。
（http://www.soumu.go.jp/joho_tsusin/top/denki_h.html）

３．成立が予想される法律案

・個人情報の保護に関する法律案

※情報通信技術（ＩＴ）戦略本部のホームページを参照すること。
（http://www.kantei.go.jp/jp/it/index.html）

付録３　ウィルス情報ＵＲＬ集

１．情報処理振興事業協会（ＩＰＡ）セキュリティセンター
　　http://www.ipa.go.jp/security/
２．コンピュータ緊急対応センター（ＪＰＣＥＲＴ／ＣＣ）
　　http://www.jpcert.or.jp/
３．警察庁ハイテク犯罪対策
　　http://www.npa.go.jp/hightech/
４．ＪＣＳＡ（日本コンピュータセキュリティ協会）
　　http://www.jcsa.or.jp/
５．財団法人日本情報処理開発協会
　　http://www.jipdec.jp/
６．通信総合研究所非常時通信グループ　不正アクセス関連情報
　　http://www2.crl.go.jp/jt/a114/incident_top.html
７．ＣＥＲＴ
　　http://www.cert.org/
８．トレンドマイクロ株式会社
　　http://www.trendmicro.co.jp/
９．株式会社シマンテック
　　http://www.symantec.co.jp/
10．マイクロソフト株式会社
　　http://www.microsoft.com/japan/security/
　　http://www.microsoft.com/japan/technet/security/
11．日本ネットワークアソシエイツ株式会社
　　http://www.nai.com/japan/
12．株式会社山田洋行
　　http://www.fs-support.yamada.co.jp/
13．ＺＤＮＥＴ
　　http://www.zdnet.co.jp/
14．日経ＩＴ　ＰＲＯ
　　http://itpro.nikkeibp.co.jp/
15．日経ＩＴニュース
　　http://it.nikkei.co.jp/it/
16．JWNTUG OPEN FORUM
　　http://forum.jwntug.or.jp/

17. Winセキュリティ虎の穴
    http://winsec.toranoana.ne.jp/
18. セキュリティホールmemo
    http://www.st.ryukoku.ac.jp/~kjm/security/memo/
19. ワクチンバンク
    http://www.vaccinebank.or.jp/
20. CSE のセキュリティソリューション
    http://www.cseltd.co.jp/security/
21. 日本の Linux 情報
    http://www.linux.or.jp/
22. Security Focus
    http://securityfocus.com/
23. Computer Incident Advisory Capability (CIAC)
    http://www.ciac.org/ciac/

代表的と思われる URL を列挙したもので、すべてを網羅したものではない。

大学の情報セキュリティポリシーに関する研究会*の構成

（主　　査）

・金澤　　正憲（京都大学大型計算機センター教授）

（委　　員）

・高井　　昌彰（北海道大学大型計算機センター助教授）
・南　　弘征（北海道大学情報メディア教育研究総合センター助教授）
・曽根　　秀昭（東北大学情報シナジーセンター教授）
・水木　　敬明（東北大学情報シナジーセンター助教授）
・玉造　　潤史（東京大学情報基盤センター助手）
・加藤　　朗（東京大学情報基盤センター助手）
・長谷川　明生（名古屋大学大型計算機センター助教授）
・山口　由紀子（名古屋大学大型計算機センター助手）
・高倉　　弘喜（京都大学大型計算機センター助教授）
・岡部　　寿男（京都大学大学院情報学研究科助教授）
・野川　　裕記（大阪大学サイバーメディアセンター講師）
・秋山　　豊和（大阪大学サイバーメディアセンター助手）
・岡村　　耕二（九州大学情報基盤センター助教授）
・池田　　大輔（九州大学情報基盤センター講師）
・淺野　正一郎（国立情報学研究所情報基盤研究系研究主幹）
・藤野　　貴之（国立情報学研究所情報基盤研究系助手）

（オブザーバ）

文部科学省

（事　務　局）

国立情報学研究所

* 全国共同利用大型計算機センター長会議の下, 大学の情報セキュリティポリシーの在り方について実践的な研究を行う会議