鹿児島大学情報セキュリティポリシー
対策基準

(公開文書)

国立大学法人鹿児島大学

情報ネットワーク委員会

平成１６年9月２１日

目次

1. 考え方

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、本学は情報セキュリティポリシーを周知徹底しなければならない。ここでは、その考え方について示す。

1.1 情報セキュリティを脅かす要素

情報セキュリティを脅かす要素として以下のような脅威(リスク)がある。

- 不正アクセス
- ウィルス感染
- 情報改竄
- 情報漏えい
- 情報紛失
- 著作権侵害
- サービス妨害
- 利用妨害
- 自然災害
- システム障害
- その他

以上のようなリスクが存在することにより、本学の学生教職員や部局等が被害を被ったり、学外の人や組織に被害をあたえたりする恐れがある。被害を及ぼす出来事ができるだけ発生しないような対策と、それらが発生した場合に被害が最小限になるよう発生時の対策をあらかじめ定める必要がある。本対策基準はこれらの対策を定めるための基準となるものである。

1.2 対策の対象

対策の対象範囲は、部局等によって別に定める。例として、学生教職員、知的所有権、公開情報、情報システムや情報ネットワーク、管理運営に必要な情報などがある。

1.3 対策の内容

対策の内容を以下に分類する。

- 「組織・体制」

本学のキャンパス情報ネットワーク全体やそれに接続される情報機器は膨大な量になるため、これを１人の管理者や１つの組織で管理できるものではない。また、本学を構成する組織内の個別管理ポリシーをできる限り尊重する必要もある。従って、管理責任者や管理者を学内の組織別に配置し、これらをメンバーに持つ管理委員会を組織ごとに階層的に構成し、各管理責任者の責任範囲を明確化し、全体として少ない負荷で、効率的に管理運営を行う必要がある。

- 「情報の分類と管理」

本学の機密情報（知的所有権情報など）や個人情報などが分類管理されていない場合、これらが外部に漏洩して本学組織、教職員、学生に重大な危害や損失を及ぼしたり、本学に対して損害賠償が請求されたりする可能性がある。公開情報であっても、それが不正に改竄されることにより大きな被害が発生する。情報が紛失した場合にも、業務が行えなくなるなどの被害が発生する可能性がある。すでに存在する情報や新しく発生する情報を分類し、管理が必要な情報については、その情報の性質に応じてその情報の流通範囲を定め、管理体制を確立する必要がある。

- 「物理的セキュリティ」

情報は物理的な機器の上で利用されることが多い。また、情報を格納している情報メディアも物理的な存在である。従って、天災や人災から情報を守るためには、情報機器や情報メディアの物理的セキュリティポリシーを定める必要が生じる。これには、情報機器やメディアの管理場所や管理方法に関するとりきめ、鍵やパスワードなどの管理方法などが含まれる。

- 「人的セキュリティ」

情報を扱うのは人であり、人的セキュリティポリシーがなければ情報を管理することは不可能である。本学各組織の情報システムや情報ネットワークの管理者と利用者の役割を明らかにし、管理者の管理規定、利用者の利用規定、それぞれの罰則などを定める必要がある。

- 「技術的セキュリティ」

情報セキュリティを確保するためには、その情報が流れる機器や情報ネットワークの技術的なセキュリティ強化も必要である。これには、ファイヤーウォール、侵入監視システム、ウィルス対策ソフトウェアなどに関する取り決めや、情報ネットワーク構築の指針などが含まれる。不正侵入や不正アクセスなどが発生した場合の技術的な対処方法の指針も必要である。また、各組織において、これを行うための人材の確保と予算の確保などを行う必要がある。

- 「評価・見直し」

普遍かつ完全なポリシーを作成することは不可能であり、全学および各組織において、ポリシーを運用して明らかになる不具合を継続的に修正していく必要がある。

1.4 対象範囲

対策基準の対象範囲を、全学的な対策を対象とするものと各部局等において個別に定めるものに分ける。

1.4.1　全学的な対策基準の必要項目

以下を全学的な対策基準の必要項目とする。これらは公開するものとする。

- 「考え方」
- 「組織・体制」の全学的な部分
- 「評価・見直し」の全学的な部分

なお、「鹿児島大学キャンパス情報ネットワークの運用管理に関する申し合わせ」で定められている範囲に関しては、この申し合わせに従う。

1.4.2　各部局等で個別に定める対策基準の必要項目

以下を各部局等で定める対策基準の必要項目とする。これらを公開するか否かは各部局等で判断する。

- 「組織・体制」の各部局固有の部分
- 「情報の分類と管理」
- 「物理的セキュリティ」
- 「人的セキュリティ」
- 「技術的セキュリティ」
- 「評価・見直し」の各部局固有の部分

1.5 実施手順の作成

対策基準を元に、各部局等で具体的な実施手順を作成しなければならない。実施手順には、情報や情報機器の利用マニュアル、利用規定、罰則などが含まれる。また、既存の規定や規則などが含まれる場合もある。

なお、実施手順作成において、管理者以外の一般利用者が必要となる利用方法、利用規定、罰則などは公開すべきであり、管理者が必要となる管理運営マニュアルや管理規定などについては、これが悪意のある利用者や外部の人が知ることにより重大な被害が発生する可能性があるため、管理者および管理責任者以外には原則として非公開とすべきである。行政管理文書に相当するものは、その規定に従わなければならない。

実施手順は、利用者や管理者が、目的に即して、無理なく、現実的に実施可能なものにしなければならない。例えば、多くの末端利用者が使用する機器の認証を複雑であまり厳しくすると、利用者がいなくなったり、利用者がこの利用規定を守ろうとしなったりする可能性が高くなる。

2. 組織・体制(全学的な部分)

2.1 管理・運用組織の構成

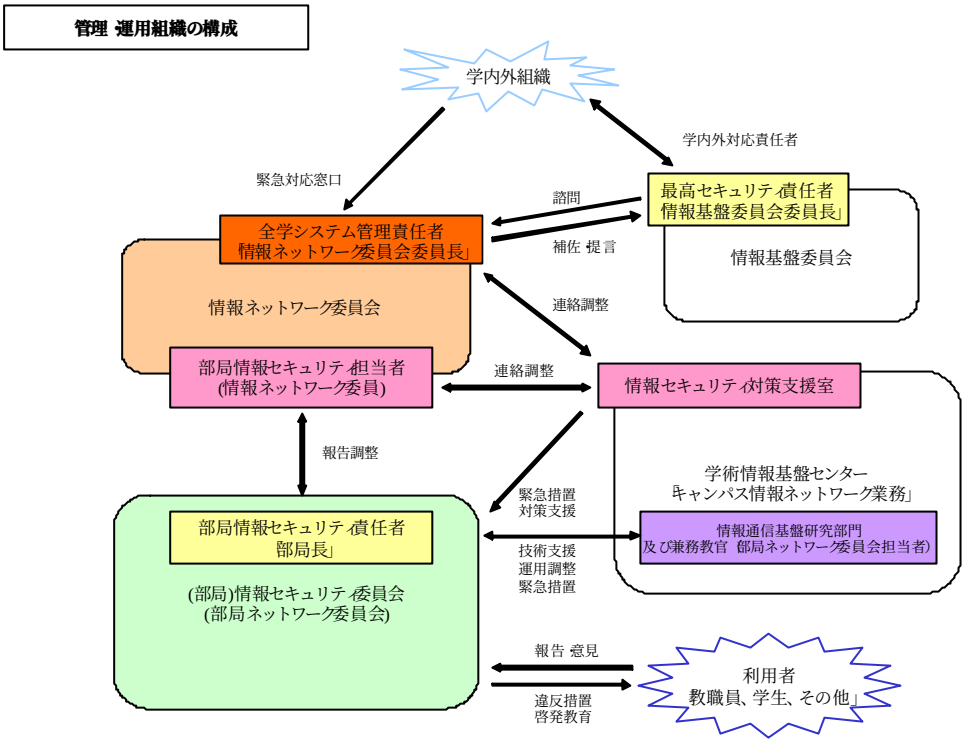

図 1: 組織の構成図

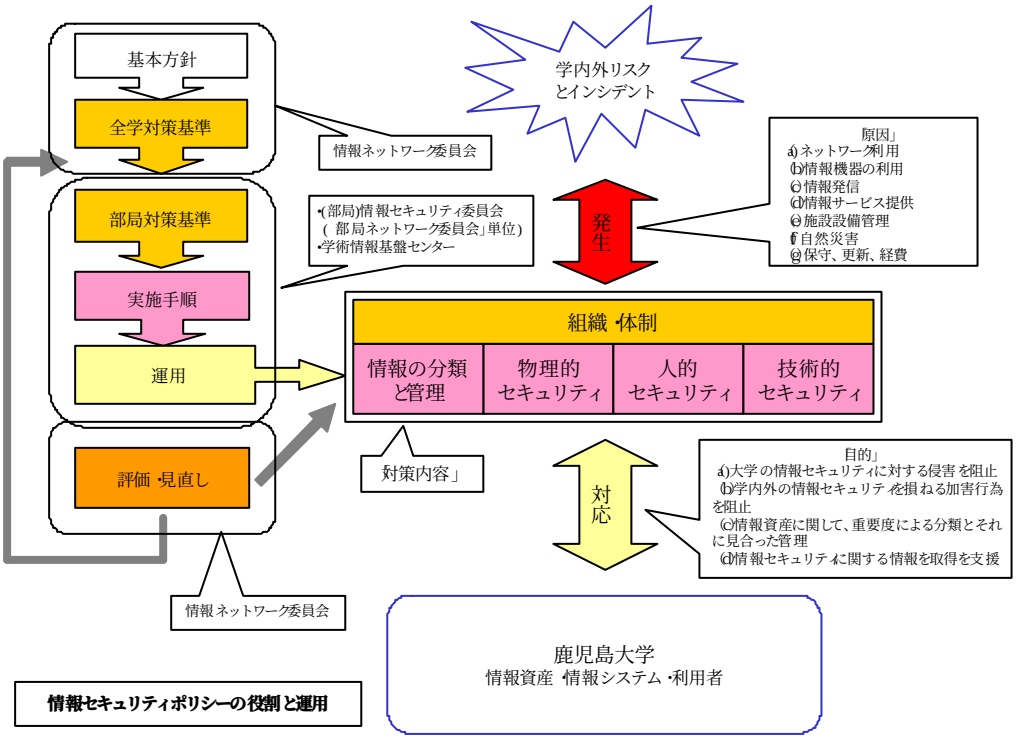

図 2 役割と運用

2.1.1　情報基盤委員会委員長

全学の最高情報セキュリティ責任者であり、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。

2.1.2　情報基盤委員会

全学の情報セキュリティに関し、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遵守の励行および違反に対する措置。
・学内の他の意思決定機構との調整。
・外部との折衝。
・情報ネットワーク委員会に対する、セキュリティポリシー策定、改定、実施、教育の依頼とこれらの管理。

2.1.3　情報ネットワーク委員会委員長

全学システム管理責任者であり、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、情報基盤委員会委員長を補佐する。

2.1.4　情報ネットワーク委員会

セキュリティポリシーの策定、改定、実施および部局等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等システム管理責任者への技術的助言等の支援を行う。

情報基盤委員会の下に置き、部局システム管理者等で構成する。

(部局)情報セキュリティ委員会に対する情報セキュリティに関する啓発および教育を行う。

2.1.5　情報ネットワーク委員会委員

部局内の情報システム管理の実施に関し、情報ネットワーク委員会委員長との連絡などの対応に当り、部局システム管理者を統括する。

2.1.6　部局長

「鹿児島大学情報セキュリティポリシー」に定められているとおり、部局長は、部局等の情報セキュリティ責任者を兼ねる。

2.1.7　(部局)情報セキュリティ委員会

情報ネットワークの運用形態に応じた部局等を単位として、部局等の情報セキュリティポリシーの策定、実施及び情報セキュリティに関する事項の審議を行う(部局)情報セキュリティ委員会等を置く。情報ネットワーク委員会委員はその部門の委員を兼ねる。一般の利用者に幅広く初心者教育を行う。

2.1.8　情報セキュリティ対策支援室

情報セキュリティ対策支援室を学術情報基盤センター内に置き､全学のセキュリティ強化に関する以下の業務を、情報ネットワーク委員会と協力して行う。

- 情報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
- 他

2.1.9 学術情報基盤センター

学術情報基盤センターは､「鹿児島大学キャンパス情報ネットワークの運用管理に関する申し合わせ」第７項に従い、各部局等の依頼に基づいて、この申し合わせに記載された範囲のキャンパス情報ネットワークの論理構成の変更や通信の遮断ポリシー設定を行う。この項に述べられているように、緊急避難的な対策も行う。

2.1.10 注意事項

情報基盤委員会、情報ネットワーク委員会、学術情報基盤センターは、その責務を効率的に遂行するため、次の事項に注意する。

- 情報ネットワーク委員会委員が担当する部門ごとに､(部局)情報セキュリティ委員会を組織する。情報ネットワーク委員会委員はその部門の委員を兼ねる。
- 管理されていない情報機器や情報ネットワークがあってはならない。キャンパス情報ネットワークとは接続されていない部局独自のネットワークも担当部局等でセキュリティポリシーを定め、管理しなければならない。同じ組織内の情報ネットワークや機器について、様々な運用ポリシーが適用され、その部局等内を複数の情報ネットワーク管理者と責任者が担当する場合も考えられるが、その場合、関係者間の連絡を密に行い、円滑な運用管理が行われるよう注意しなければならない。また個々の情報ネットワークや機器の管理責任者は一人になるよう調整しなければならない。
- 末端までの情報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、情報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。
- 学術情報基盤センターはそれ自身の対応の他に、本学と学外との接続に対する体制も持つ。
- 情報基盤委員会、情報ネットワーク委員会及び学術情報基盤センターは、24 時間 365 日、緊急に対応できる体制を整備するべく努力する。
- 学内の組織変更、情報ネットワーク構成の変更時に、情報ネットワークや情報機器の管理責任者や管理者がいなくなる等の不備がないよう、マニュアル化などを行う。
- 部局等をまたいだ情報システム管理組織がある場合は、関係部局等で協議し、その組織の管理責任体制を確立しなければならない。

2.2 不正アクセス等への対応

学術情報基盤センターは、外部または内部からの不正アクセスを検出した場合、情報基盤委員会が定めた緊急措置手順「鹿児島大学キャンパス情報ネットワークの運用管理に関する申し合わせ」第７項に従い、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,「申し

合わせ」やセキュリティポリシーなどの手順に定められていない状況では、情報基盤委員会委員長が最終判断する。情報基盤委員会は、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違反行為の報告を、その処分に関する権限を有する意思決定組織（教授会等）に対して行う。

3. 評価・見直し(全学的な部分)

3.1 ポリシーの運用実態

情報基盤委員会委員長は、ポリシーの運用実態等を把握するため、情報ネットワーク委員会に対し、次のような措置を求めなければならない。

3.1.1 ポリシー運用実態等の把握

情報ネットワーク委員会委員長は、情報ネットワーク委員会を定期的に開催し、収集した情報を分析・整理した上で、情報基盤委員会に報告しなければならない。

情報基盤委員会は、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。

3.1.2 利用者の意見

情報ネットワーク委員は、(部局)情報セキュリティ委員を通じて、部局等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、情報ネットワーク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。

3.1.3 情報セキュリティ診断と監査

学術情報基盤センターは「鹿児島大学キャンパス情報ネットワークの運用管理に関する申し合わせ」第８項に定めているように、運用の管理範囲で鹿児島大学キャンパス情報ネットワークの機器等のログを記録・解析することができる。この中で学術情報基盤センターは情報セキュリティ診断と監査を実施すべきである。

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､「鹿児島大学キャンパス情報ネットワークの運用管理に関する申し合わせ」第７項に記載された緊急避難措置とその後の処置をとらなければならない。

監査の過程で法令ならびにポリシーおよびこれに関連する規定･基準等が遵守されていない場合、当該部局へ連絡しなければならない。

3.1.4 セキュリティ対策費

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。

情報基盤委員会は、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。これには、学術情報基盤センター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)、ウィ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。

3.2　セキュリティレベル向上策

情報ネットワーク委員長は、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、情報ネットワーク委員会を年 1 回以上召集しなければならない。この中で、セキュリティの現状、ポリシーの見直し、セキュリティ強化のための計画や予算案などについて情報基盤委員会に提案し、(部局)情報セキュリティ委員会と関連部局へ次期セキュリティポリシーの実施を指示しなければならない。

情報基盤委員会委員長は、学内の最高意志決定組織（大学運営会議、役員会等）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。