MUSASHI
UNIVERSITY

武蔵大学情報セキュリティポリシー

武蔵大学情報セキュリティ委員会

初版 (2004 年 6 月 17 日)rev0.3

目次

要旨

インターネットを中心とする情報システムは、目覚しい発展を遂げてきている。しかし、それに呼応して、コンピュータセキュリティインシデントが年々増加の一途をたどっているのもまた事実である。

本学においては、インシデントレスポンスの責務は情報システム担当部局が主として担ってきており、外部からの不正アクセス、サービス不能攻撃、コンピュータワームやコンピュータウィルスの侵入等に対するセキュリティ対策や情報セキュリティに関するユーザへの教育等の各種の対策を講じてきたところである。

しかし、コンピュータセキュリティインシデントは、年々巧妙になり、また複雑化しており、最近では、遂に本学が従来から講じてきた対策の範囲を超えるケースが散見されるようになってきた。本学における情報システム担当部局中心のセキュリティ対策は、もはや限界を迎えている。

完全なセキュリティというものはあり得ない。

情報システムは、いつかは脅威にさらされ、重要な情報資産が流出するという事態の発生を完全に防ぐことはできないものと考えるべきである。このためセキュリティインシデントに対する予防とインシデント発生時の的確な対策のための危機管理を本ポリシーではもっとも重視している。

以上のような本学をめぐる情報セキュリティの実態を踏まえ、本セキュリティポリシーにおいては、今後のコンピュータセキュリティインシデントの発生に対して、機動的かつ確実に対処することを目標として、以下の点に重点を置いたポリシー策定を行うこととする。

1. 大学として不可欠な社会的信頼の維持
2. コンピュータセキュリティインシデント発生時に迅速に対応できる体制の確立
3. 不測の事態によるコンピュータセキュリティインシデント発生後の対策方針
4. コンピュータセキュリティインシデントの予防のための技術的な指針
5. コンピュータセキュリティインシデント発生時の個人情報、プライバシーの保護

なお、本学の学生、教職員等の構成員が、本セキュリティポリシーを維持するために必要なガイドラインを別途策定するものとする。

変更履歴

2004 年 6 月 17 日　初版発行

rev. 0.1　図版をカラー化

「インシデントの大きさ」を「高い、低い」と言う表現から「大きい、小さい」という表現に変更

rev. 0.2　組織名変更：情報システムセンター　→　情報・メディア教育センター

用語の統一：マネジメント　→　マネージメント、コンピュータ　→　コンピューター

rev. 0.3　用語の統一：語尾の長音符号について”JIS Z8301:2005”に準ずる表現に変更

用語の定義

本セキュリティポリシーにおいて使用する用語中、社会通念上意味が十分確定されていない用語については以下の定義により使用するものとする。

情報資産　本学が所有権または利用権を持つ情報システム、システム開発、情報システムの運用保守、および情報システム上に保管される情報そのもの。

情報セキュリティポリシー　情報資産の運用管理に関する規程であり、本学の情報資産を利用する学生、教職員等は、それを遵守する義務を負っている。

コンピュータセキュリティインシデント　学内への不正アクセス、サービス不能攻撃、コンピュータワームやコンピュータウィルスの学内への蔓延等、人為的事象に起因して、本学の情報資産に脅威を与えるような事象、およびそれに至るための行為または事象のこと。意図的か偶発的かを問わず、また疑いがある場合を含む。本ポリシーでは単にインシデントと呼ぶことがある。

インシデントレスポンス　コンピュータセキュリティインシデントに対する事前の対策、インシデントの発見、復旧、事後対策などの一連の活動を指す。本セキュリティポリシーもインシデントレスポンスの一部となる。

不正アクセス　本学のコンピュータシステムに、本学の望まない方法でアクセスすること。

不正侵入　不正アクセスの結果、本学のコンピュータシステムへの侵入に成功すること。

サービス不能攻撃　DOS (Denial of Services) と呼ばれる。本学のコンピュータシステムに悪意を持って高負荷をかけ、コンピュータシステムの一部あるいは全部の運用を妨害すること。本セキュリティポリシーでは「分散型サービス不能攻撃」DDOS (Distributed Denial of Service) も含めている。

迷惑メール送信　本セキュリティポリシーでは、UBE(Unsolicited Bulk e-mail) または UCE(Unsolicited Commercial e-mail) もしくは、スパム (spam) メールと呼ばれる行為を指す。悪意を持って大量のメールを不特定多数のアカウントに送りつける行為。

コンピュータウィルス　電子メールまたは CD-ROM 等の磁気記録媒体等を通じて、コンピュータシステムに侵入し、時として、他のコンピュータシステムへの侵入を試みたり、情報の搾取や破壊活動を試みることもあるプログラム。

コンピュータワーム　インターネットや LAN 等のネットワークを利用してコンピュータシステムに侵入し、コンピュータやネットワーク上で自己増殖を繰り返しながら、時として情報の搾取や破壊活動を試みることもあるプログラム。

リスクマネージメント　インシデント等のリスク発生に対する備えを管理すること。

危機管理　インシデント等の実際のリスク発生後の対処を管理すること。

システムの利用　エンドユーザによる WEB ブラウザの利用、メールの送受信等のコンピュータシステムの利用を指す。

システムの運用　コンピュータシステムを管理する立場の責任者、技術者のサーバ等の運用管理業務を指す。

1　基本方針

1.1　セキュリティマネージメント

情報セキュリティの対策は、PDCA(Plan-Do-Check-Action) サイクルを中心にした適切な情報セキュリティマネージメントシステムを構築し、情報セキュリティに関する社会的な動向に柔軟に対応できる組織を構成することを目標にする。

このための情報セキュリティ対策の PDCA は以下のように構成するものとする。

PLAN　情報セキュリティポリシーの策定

DO　ポリシーに基づくセキュリティ対策の実施

CHECK　セキュリティ対策の監査

ACTION　監査結果に基づくポリシーの見直し

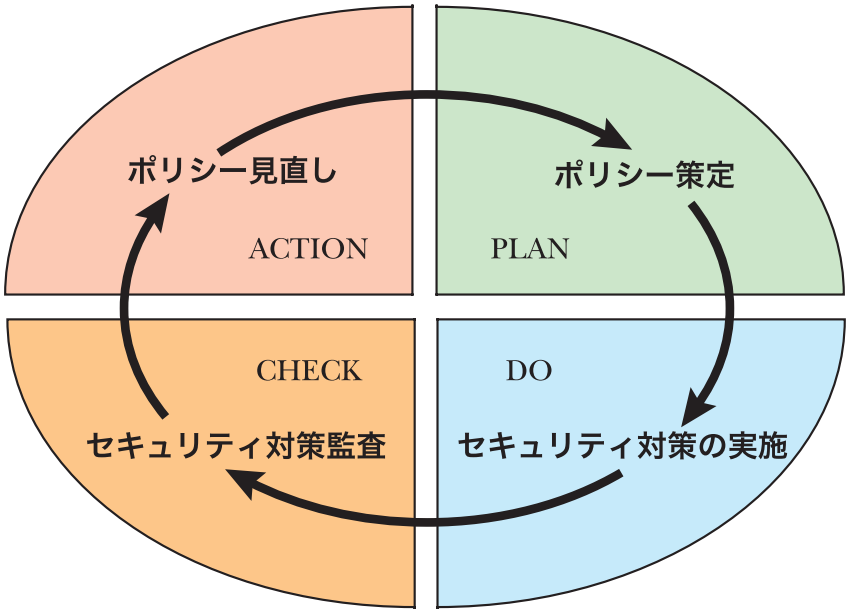

図 1　セキュリティマネージメントの PDCA

以上の PDCA サイクルに応じて以下の事項につきネットワークセキュリティポリシーを提言する。

1. セキュリティ維持のための体制
2. セキュリティのレベルに応じた取り組み
3. セキュリティ違反に対する措置
4. 監査
5. インシデントに関する情報公開

1.2　ポリシーの区分

大学の情報資産の管理は、教育研究を中心とするフロントエンドシステムと学生のライフサイクルを管理する事務を中心とするバックエンドシステムでは大きく異なり、両者に適用するポリシーには相違がある。

1.2.1 教育研究システムのポリシーの基本

大学のフロントエンドシステムを担う教育研究システムにおいては、各学部等および、個人の研究活動および教育活動遂行の独自のポリシーを尊重しつつ、大学のインフラストラクチャーのセキュリティの維持管理に必要なポリシーを提供するものとする。

ここに含まれるシステムには、情報・メディア教育センターの所管するシステム、各学部のグループスタディルームなどのシステム、コール教室など各センターが所管するシステム、教員が個人で管理するシステムなどがある。

1.2.2 事務システムのポリシーの基本

大学のバックエンドシステムを主として担う事務システムにおいては、学生の個人情報管理等価値の高い情報資産の管理運用を担っている。したがって、教育研究システムに比較して、より高度なセキュリティポリシーを提供するものとする。

ここに含まれるシステムには、各部課室等の管理する財務システム、教務システム、入試システム、就職システム、事務用のグループウェアシステムなどがある。

なお、図書館関係のシステムについては、教育研究システムと事務システムの両方のポリシーの影響を受ける特別なシステムである。

1.3 体制

1.3.1 構成

本学の情報セキュリティ対策の活動の中心は情報セキュリティ委員会にある。情報セキュリティ委員会の役割は、本学における情報セキュリティの PDCA サイクルの維持を主導することにある。

情報セキュリティ対策においては、最終的な責任関係の明確化と、迅速な対策の実施の両立が不可欠である。このため、情報セキュリティ委員会は学長の主宰する情報システム会議の下に設置し、情報システム会議 CIO を委員長として、各学部、事務組織の代表を委員として構成する。

また、情報セキュリティの維持、迅速なインシデントレスポンスのためには、全学的な取り組み体制が必要である。このための本学の組織構成の全体は次の通りとなる。

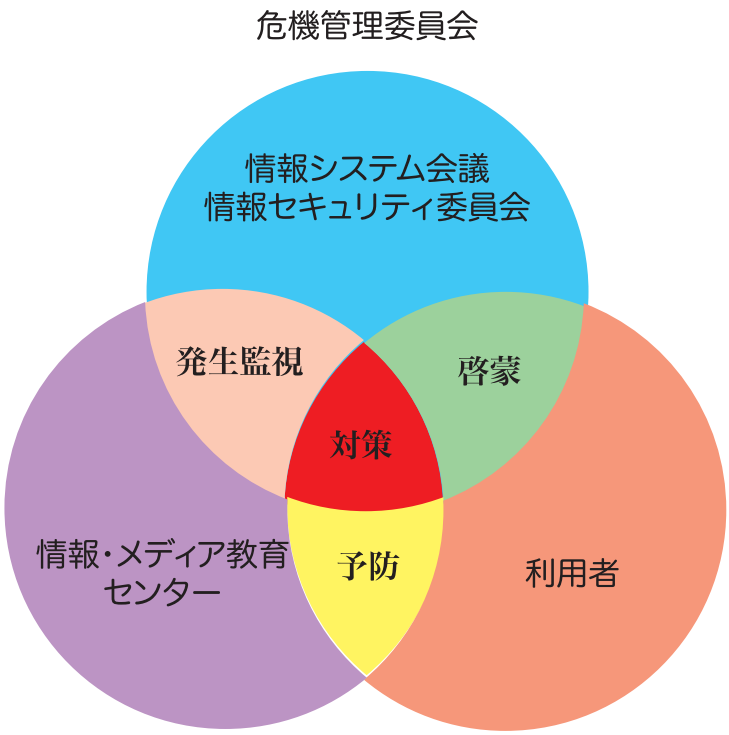

図 2　情報セキュリティ対策に対する役割

- 危機管理委員会
- 情報システム会議
- 情報セキュリティ委員会
- 情報・メディア教育センター
- 利用者

1.3.2 利用者の役割

利用者は、コンピュータセキュリティインシデントを水際で防ぐためのもっとも重要な役割を果たしている。その具体的な役割は以下のとおりである。

1. 情報セキュリティ委員会の定めるガイダンスに従った適切なセキュリティ対策を講ずること。
2. インシデント発生に際し、情報セキュリティ担当者または情報セキュリティ委員会への通報を行うこと。
3. その他本学におけるインシデントレスポンス活動への協力を行うこと。

1.3.3 情報・メディア教育センターの役割

情報・メディア教育センターの、情報セキュリティ対策に対する具体的な役割は以下の通りである。

1. インシデントに対する継続的な監視を行うこと。
2. インシデント発生時のインシデントレスポンス活動。
3. インシデント発生から終息までの間の技術的な対策活動。

1.3.4 情報セキュリティ委員会の役割

情報セキュリティ委員会の情報セキュリティ対策に対する具体的な役割は以下の通りである。

1. 情報セキュリティポリシーの策定と維持。
2. 学生、教職員向けのセキュリティポリシーの普及教育。
3. 本学の情報セキュリティ対策に関するホワイトペーパーの公表。
4. 情報セキュリティ監査の実施計画の策定。
5. 情報セキュリティ監査に基づく情報セキュリティ対策の見直し。
6. 情報システム会議 CIO の下でのコンピュータセキュリティインシデント発生から終息までの全活動の指揮監督（ただし、危機管理委員会に関する事項を除く）。
7. インシデントに対する学内の関係者の懲戒等の処分を情報システム会議に対し提案すること。

1.3.5 情報システム会議の役割

情報セキュリティ会議の情報セキュリティ対策に対する具体的な役割は以下の通りである。

1. インシデントレスポンスに対する全責任。
2. 情報セキュリティ委員会が提案する学内関係者の懲戒等の処分を関係部局へ要求すること。

1.3.6　危機管理委員会の役割

危機管理委員会の役割の規定は、本ポリシーの範囲外であるが、以下の場合には、情報システム会議が、その開催を求め、適切な対応を要求するものとする。

1. 法的措置を講ずることが必要となったとき。
2. 広報対策等対外的な対応が必要となったとき。
3. インシデントの状況が深刻であり、危機管理が必要であると情報システム会議が判断したとき。

1.4　情報セキュリティ対策

1.4.1　適用範囲

コンピュータセキュリティインシデントの発生は、通常予測し得ないほど突然であり、また、その態様も様々である。これに対するインシデントレスポンスもその態様に応じ適切な規模で行われなくてはならない。

このため、コンピュータセキュリティインシデントをその態様に応じて 5 段階のセキュリティレベルに分け、各レベルにおいて各組織の果たすべき役割を明確にしておくこととする。

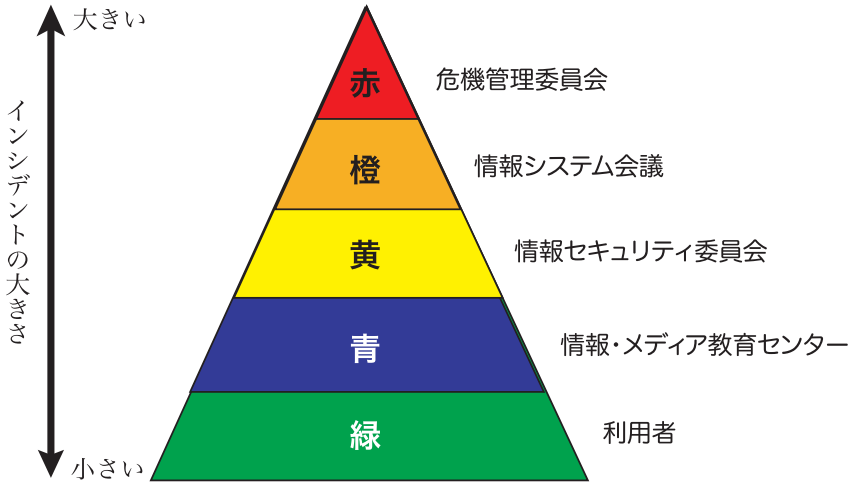

図 3　インシデントの区分

インシデントの状態の認知を容易にするために、本学では、以下のようにセキュリティレベルの状態を色によって表すものとする。

赤:深刻　危機管理委員会による管理が必要とされる状態
橙:重大　インシデントによる深刻な被害の発生した状態
黄:高い　インシデントにより実際の被害が確認された状態
青:注意　インシデントの発生が確認された状態
緑:低い　インシデント発生が確認されていない状態

状態が「緑」の場合と「青」の場合はリスクマネージメントが中心となり、状態が「黄」以上は何らかの危機管理が必要となる。

現在がどの状態にあるかは、「緑」と「青」にあっては、情報・メディア教育センターが決定し、「黄」は、情報セキュリティ委員会が決定する。また、「橙」と「赤」については、情報システム会議の決定が必要である。

現在のセキュリティレベルについては、情報・メディア教育センターにて、学内に向けて状態を色で提示す

ることとする。また、情報の速報性を重視するために、「緑」「青」「黄」については、情報・メディア教育センターの判断において提示し、事後の承諾を得ることができる。

1.4.2 状態:緑 予防と監視

- 学内においてインシデントの発生が確認されていない状態。
- 情報・メディア教育センターにおいて、常時インシデントに対する警戒を行う。
- ユーザは、学生、教職員、システム管理者それぞれの各ガイドラインに従った利用と運用を行う。
- 教育研究システム、事務システムともインシデント発生を検知した場合には情報・メディア教育センターが窓口となる。

1.4.3 状態:青 インシデントの発生

- 学内においてインシデントの発生が確認されている状態。
- 情報・メディア教育センターは被害の発生の防止に関する適切な対処を実施。
- 情報セキュリティ委員会は被害防止に向けて啓蒙活動を開始する。
- ユーザは、被害に遭ったと思われる場合には情報・メディア教育センターに速やかに情報を提供し対策を仰ぐ。

1.4.4 状態:黄 インシデント対策

- 学内においてインシデントによる被害が確認されている状態。
- このレベルでは、基幹ではない一部のネットワークを切り離す必要がある。
- 対策は情報セキュリティ委員会が実施し情報・メディア教育センターはその指揮下に入る。
- 情報セキュリティ委員会は学長へ進捗状況について随時報告を行う。
- 教育研究システムにおいては、システムの一部停止に伴う迂回措置などにつき、情報セキュリティ委員会の要請に従う。
- 事務システムにおいては、情報セキュリティ委員会の指示に従い、迂回措置、利用制限等の措置を行う。

1.4.5 状態:橙 重度対策

- 学内においてインシデントによる被害が深刻化している状態。
- この状態では、基幹ネットワークの停止が必要となる場合がある。
- この状態では、緊急の財務的な措置が必要となる場合がある。
- この状態を決定するためには、情報システム会議の開催が必要である。
- 情報セキュリティ委員会委員長は情報システム会議議長へ進捗状況について随時報告を行う。
- 情報・メディア教育センターは、情報セキュリティ委員会の指示に従い、基幹情報システムの停止等の対策を実施する。
- 財務的な手当が必要な場合は、情報セキュリティ委員会と関係機関で協議を行う。
- 教育研究システムにおいては、システムの管理部局となる学部、センター等の単位毎に情報セキュリティ委員会の要請する利用制限を実施する。
- 事務システムにおいては、情報セキュリティ委員会の指示に従い、個人情報等のセキュリティレベルの

高いシステムを中心として、運用停止、教育研究システムとの分離等の制限措置を実施する。

1.4.6 状態:赤 危機管理

- 法的措置を必要とするインシデントの発生。
- 対外的な対策を必要とするインシデントの発生。
- この状態を決定するためには、情報システム会議の開催が必要である。
- インシデントの状況が深刻であり、危機管理が必要であると情報システム会議が判断したとき。
- 活動は全て危機管理委員会に移行する。

1.4.7 緊急措置

どの状態にあっても、情報・メディア教育センターが、技術的に緊急措置をとらなければならないと判断した場合には、情報・メディア教育センターは、関係機関の事前の承諾なしに緊急の措置を実施し、事後の承諾を得ることができる。

ただし、情報システムに関する技術的な問題の範囲を超えてはならない。

関係機関が、情報・メディア教育センターの措置を適切ではなかったと認める場合には、本ポリシーに定める罰則等の適用を情報・メディア教育センターの関係者に対して適用する。ここにおいて関係機関とは、状態が「黄」の場合においては情報セキュリティ委員会、状態が「橙」の場合においては情報システム会議、状態が「赤」の場合においては危機管理委員会を指すものとする。

1.5 罰則等の適用

本ポリシーにおいては、懲戒等の身分上の処分についての適用に関する具体的な措置は提起しない。

ただし、情報セキュリティ委員会が、懲戒等の身分上の処分が必要と判断した場合には、情報システム会議に提案し、情報システム会議は、関係機関に対し、必要な措置を行なうように要請することができるものとする。

また経済的損失に対しては損害賠償請求を行うことができるものとする。

1.6 活動の検証

本ネットワークポリシーの実施が適正に実施されているかを検証するために、定期的な活動報告およびセキュリティ監査を実施する。

1.6.1 内部の活動

1. ホワイトペーパーの作成
   情報セキュリティ委員会はその活動情況について、少くとも年に一度公表を行うこととする。
2. 内部監査
   情報セキュリティに関する内部監査は、専務理事をリーダとして必要に応じて実施するものとし、少くとも年に一度の定期的な監査を実施することとする。
3. 内部監査結果の報告

内部監査結果は、情報システム会議に報告され、その結果は公表するものとする。ただし、情報システム会議 CIO がその公表を適切ではないと判断した場合はこの限りではない。

1.6.2 外部監査

第三者機関による情報セキュリティの外部監査は、少くとも年に一度実施することとし、そのために必要な予算措置を情報セキュリティ委員会において行なうものとする。

外部監査の検査項目は、次の通りとする。

1. 見逃されたインシデントはないのか
2. インシデントに対する対応は適切だったか
3. セキュリティ対策は適切だったか

より具体的な監査の依頼項目は、毎年度情報セキュリティ委員会において決定する。

外部監査結果は、セキュリティインシデントの発生素因となるセキュリティホール等の事象が含まれている場合には、その対策が講じられた後に公表するものとする。ただし、この場合にも、少なくとも外部監査終了後 3 ヶ月以内には公表するものとする。

1.6.3 監査による是正措置

情報セキュリティ委員会は監査により勧告された是正措置について、対策を講ずるか、対策を講ずることができない場合にはその理由を情報システム会議に対して明らかにする必要がある。

是正措置については公表するものとする。

1.7 インシデントに関する情報の公開

本学におけるインシデント並びにインシデントレスポンスに関する情報は、プライバシー保護とセキュリティ維持に配慮の上、すべて公開することとする。情報の積極的な公開は、結果的に本学の社会的信用の維持に貢献するからである。

情報公開の基準は以下の通りとする。

- 個人情報を特定されないように配慮しなければならない。
- 外部の組織を特定されないように配慮しなければならない。
- 学内において対策されていないセキュリティホールは公開してはならない。
- 以上の情報以外はすべて公開されるべきである。

2 対策基準

2.1 教育研究システムの対策基準

教育研究システムは、各学部、研究室で異なったポリシーにより運用されており、本セキュリティポリシーの基準の採用については、各学部、研究室等において適切な判断をする必要がある。

また、セキュリティインシデントが発生した場合に際し、各個人、組織の責任が明確にされていなければな

らない。

2.1.1 インターネット利用の基準

インターネット利用においては、少なくとも「ネチケットガイドライン」（FYI28、RFC1855）に準拠した利用方法を推奨すると同時に、個々のユーザが利用するコンピュータにおいては「ユーザのセキュリティハンドブック」（FYI34、RFC2504）に準拠した利用方法を推奨するほか、本学独自のポリシーに基づく利用方法を推奨する。

2.1.2 インターネットへの情報公開の基準

Web、FTP、SNS 等による外部への情報公開にあたっては以下の点に留意する。

- 学術研究利用を主たる目的とすること
- 個人のプライバシー保護
- 著作権の保護
- 公序良俗の維持
- その他法令に反しないこと

このうち学術研究利用に伴い発生する収益活動等については、その活動の態様に応じた判断が必要である。

また宗教活動、政治活動に対しても適切な判断を求めるものとする。現時点においては、本学全体の利用基準を定める「武蔵大学ネットワーク利用規程」において、特段の定めを行っていないが、各サーバの利用に当たっては一定の制限を設けた運用を行っている。

2.1.3 学外から学内へのネットワークへのアクセスの基準

学外と学内の間のネットワーク接続については、以下のように定める。

- 情報・メディア教育センターの所管するネットワークにあっては、情報・メディア教育センターの定める基準により運営を行う。
- 上記の基準については、情報セキュリティ委員会の承認を得たものとする。
- 情報・メディア教育センターの所管外のネットワークにあっては、情報・メディア教育センターの所管するネットワークを経由しない外部接続に関して、以下の基準を満たしている必要がある。
  - 接続の安全性が技術的に確認されていること。
  - 基幹ネットワークへのセキュリティ上の影響が最小限であること。
- 上記の基準を満たしていることについては、情報セキュリティ委員会の認証を必要とする。

2.1.4 システム管理の基準

ネットワークが接続されているどのコンピュータにおいても、運用責任者とシステム管理者が明確でなければならない。

2.2 事務システムの対策基準

事務システムは、大学における価値の高い情報資産を管理している。このためシステム全体がセキュリティポリシーの対象となる。情報セキュリティの PDCA サイクル全般にわたって適切な基準を定めておく必要がある。

2.2.1 情報セキュリティ担当窓口の設置

事務システム全般のセキュリティ維持のために総務部長のもとに情報セキュリティ担当を設置し、事務システムのセキュリティ担当窓口を開設するものとする。

2.2.2 インターネット利用の基準

事務システムからのインターネットの利用は、与えられた業務目的に従って適切な方法で利用されなければならない。インターネットを利用するための Web ブラウザ、電子メールソフト、SNS ツール等についての明確な基準が定められていなければならない。

2.2.3 インターネットへの情報公開の基準

インターネットへの情報公開に当たっては、公開の妥当性を判断する窓口を設置し、その窓口を経由しない公開を行うべきではない。窓口は案件ごとに別に設置されていても良いが、情報セキュリティの担当者を設置しなければならない。

2.2.4 学外から学内へのネットワークへのアクセスの基準

学外から学内へのネットワークへの接続は、情報セキュリティ担当窓口による承認を必要とする。

2.2.5 システム管理の基準

一貫した情報セキュリティポリシーを維持するためには、システム全体をシステム管理を専任で行う組織においてシステムを運用することが望ましいが、そのような運用に馴染まないシステムの運用に当たっては、当該システムの組織の長が運用責任者となり、セキュリティとシステム運用に経験のある担当者を技術担当者として設置する必要がある。これはコンピューター台といった小さなシステムにおいても適用される。

2.3 プライバシー保護の基準

プライバシー保護は、個人情報保護法に依拠しながら、以下のケースについて個別に定める必要がある。

- 日常業務において学生、教職員その他の個人情報を取り扱う場合。
- 通常のシステムの運用管理、インシデントの監視等情報システムの運用保守を実施する場合。
- インシデント発生時の対策。
- インシデント発生に関する被害者、加害者、第三者を含む関係者。
- 情報公開時。

プライバシー保護は、情報資産の保全の重要な位置を占めており、資産保全の中でも優先すべき項目のひとつである。

2.4 罰則等の適用基準

本ポリシーに基づき罰則を適用する場合の基準と手続は以下のとおりとする。

- 学生に対する処分については、関係する学部および学生部に対して、処分に必要な情報提供を行うとともに、 その処分の程度についての意見を付すものとする。
- 教員に対する処分については、原則として情報システム会議議長が関係学部の長と協議を行ない、適切な措置を要請するものとする。
- 職員に対する処分については、原則として情報システム会議 CIO が総務部長と協議を行ない、適切な措置を要請するものとする。
- 教職員に対する処分について、深刻な事例が発生した場合には、情報システム会議 CIO は、以上に関わらず懲戒委員会の開催等を要求することができるものとする。
- 経済的損失が発生した場合には、身分上の措置のほか、損害賠償を要求する。損害賠償は情報システム会議 CIO がその被害額を算出し、学園長から関係者に対して請求を行う手続を踏むものとする。

2.5 セキュリティポリシーの改定

毎年度の情報・メディア教育センターホワイトペーパーおよび外部監査の結果に基づき、情報セキュリティ委員会が改定する。

3 実施手順

ネットワークポリシーの具体的な手順については、別途ガイドラインを作成することとする。ここでは各ガイドライン作成に必要な要件について定める。

なお、個人情報保護に関するガイドラインは、「個人情報の保護に関する法律」（平成 15 年 5 月 30 日法律第 57 号）の趣旨に従い、別途定めることとする。

3.1 学生向け実施手順

学生へのセキュリティポリシー対策は、従来のセキュリティガイダンス、誓約書の提出、およびセキュリティテストの枠組で実施する。

3.2 教育研究システムに関わる教職員向け実施手順

主として教育研究システムを利用する教職員に対しては、以下の手順を実施するものとする。

- セキュリティガイドラインの配布
- セキュリティに関する誓約書の提出

3.2.1 セキュリティガイドラインの配布

教育研究システムに関するガイドラインは、以下の内容を含むものとする。

- セキュリティに関する基本的な知識
- 個人で行えるセキュリティ対策
- セキュリティに関するサポート体制
- 罰則

3.2.2 誓約書の提出

誓約書はセキュリティガイドラインに付属し、その趣旨を理解した旨の誓約を行うものであり、学長宛に提出するものとする。

3.2.3 サポート体制

教育研究システムに関する情報セキュリティのサポートは情報・メディア教育センターユーザサポート室において実施する。

サービス内容については別途定める。

3.3 事務システムにかかわる教職員向け実施手順

事務システムに関わる教職員に関しては、以下の手順を実施するものとする。

- セキュリティガイダンスの実施
- セキュリティガイドラインの配布
- セキュリティに関する誓約書の提出

3.3.1 セキュリティガイダンスおよび誓約書の提出

事務システムを利用するユーザの全て、すなわち、専任、非常勤教職員および派遣委託業務等の外部者を含めて全員がガイダンスを受講し、セキュリティに関する誓約書を提出しなければならない。

誓約書は、総務部長宛に提出するものとする。

3.3.2 サポート体制

事務システムに関する情報セキュリティのサポートは総務部長が実施者となり、別に定める基準に従ったサービスを提供するものとする。

3.4 システム管理者向け実施手順

情報資産にかかわる運用保守を行うシステム管理者に対しては以下の対策を講ずるものとする。

3.4.1 情報・メディア教育センターおよび情報システム部

情報・メディア教育センターおよび情報システム部に所属し、情報・メディア教育センター長からネットワーク利用規程に基づきシステム管理者として指名された管理者については、一般の利用者に関する実施手順に加え以下の対策を実施する。

- 高度なセキュリティ対策に関する研修の実施
- システム管理者向けセキュリティガイドラインの配布
- システム管理者としてのセキュリティに関する誓約書の提出

3.4.2 教育研究システムにかかわるシステム管理者

教育研究システムにかかわる管理者とは、各学部、大学院等に設置されているホストの管理者、「武蔵大学ネットワーク利用規程」に基づき研究室等において個人で運用するサーバの管理者を指すものとする。

これらの管理者に対しては以下の手順を実施するものとする。

- システム管理者向けセキュリティガイドラインの配布
- システム管理者としてのセキュリティに関する誓約書の提出

ここで定めるシステム管理者は、情報セキュリティ委員会の勧告するセキュリティ対策を適切に講じ、セキュリティの現状を情報セキュリティ委員会の求めに応じ随時の提出する義務を負うものとする。

3.4.3 事務システムにかかわるシステム管理者

事務システムにかかわるシステム管理者とは、各事務室等において独自に運営されている、図書システム、財務システム、教務システム、就職システム等の管理者を指すものとする。

これらの管理者に対しては以下の手順を実施するものとする。

- システム管理者向けセキュリティガイドラインの配布
- システム管理者向けセキュリティに関する誓約書の提出

ここで定めるシステム管理者は、情報セキュリティ委員会の支援を受けて適切なセキュリティ管理を行う義務を負う。