名古屋大学情報セキュリティポリシー

平成 28 年 4 月 1 日

名古屋大学

- 目　　次 -

名古屋大学情報セキュリティポリシー

1. 基本方針

(1) 前文

名古屋大学は「自由闊達な学風の下、人間と社会と自然に関する研究と教育を通じて、人々の幸福に貢献すること」を大学の使命としている。研究・教育における情報の公開性・利便性は重要な社会的要請である一方で、不正アクセス、情報漏えい、サイバー犯罪などの問題も社会的に急増しており、安全性の確保が求められている。名古屋大学は、安全性に配慮しつつ、公開性・利便性を確保するという立場を選択する。また、多くの事項について事前に詳細で硬直化した制限を設けるよりは、各構成員が情報基盤の利用に関するあらゆる行動に責任をもち、情報利用技術の最新の成果を利用して柔軟な行動をとることを奨励する。公開性・利便性に伴う危険性を啓発し、利用者の情報セキュリティに関する自覚と技能の向上を目的とした教育・研修制度を導入する。

名古屋大学は、情報資産の重要度に応じた情報の機密性、完全性、可用性の確保、それらの適切な運用、保全及び検証の促進、ならびに、教育・研修制度に関する基本方針を定める。

(2) 条項

1. (基本姿勢)

名古屋大学は、社会を構成する一員として、安心・安全な情報環境を整え、これを維持し、学術の府としての社会的責任を果たす。

2. (未然防止)

名古屋大学は、情報セキュリティ障害を未然に防止し、教育研究及び付随業務の円滑な遂行が可能な情報基盤の確立を目指す。

3. (事後対策)

名古屋大学は、情報セキュリティ・インシデントが発生した場合には、その被害の最小化と迅速な復旧、再発防止に努める。

4. (運用及び保全のマネジメント)

名古屋大学は、情報セキュリティにおける役割と責任を明確にし、情報セキュリティマネジメントシステムによる、情報基盤の継続的な改善に努める。

5. (法令の遵守と社会倫理の尊重)

名古屋大学は、社会倫理の尊重、著作権保護、知的財産権保護、不正アクセス防止、個人情報の保護等の法令遵守を通して、安心と信頼に応える情報セキュリティ環境の構築を進める。

(3) 適用範囲

名古屋大学の学術活動及び事業活動に関わるすべての関係者とその情報資産に適用する。

2. 情報セキュリティ基準

情報セキュリティの基本方針にそって、情報資産を、故意及び偶発に関係なく、改竄、 破壊、漏洩等から保護し、事業の継続性を維持するために、以下の対策を策定する。

(1) 情報セキュリティ組織の設置

情報の自由な活用（受信・保存・加工・利用・発信など）の保障と情報の安全性の適切な管理とを最大限両立させる良好な環境の創出を目的として、セキュリティポリシーに基づいて具体的事項について企画・立案・実施・管理・継続的検討を行うための情報セキュリティ組織を名古屋大学に設ける。名古屋大学の情報セキュリティを全体として統合するため、情報セキュリティ戦略組織と全学情報セキュリティ組織を設ける一方、セキュリティポリシーを実施するため、関係部局その他を単位とする情報セキュリティ単位組織を設ける。また、情報セキュリティポリシーが遵守されているか否かを検証する情報セキュリティ監査組織を設置する。

a) 情報セキュリティ戦略組織

情報セキュリティ戦略組織は、全学情報セキュリティ組織と情報セキュリティ単位組織と協力して、以下の業務を担当する。なお、これらの組織の行う決定や基準・ガイドライン設定は、全学の構成員および大学外の関係者に大きな影響を及ぼす可能性があるので、十分な情報公開の体制をあわせて整備する。

1) 名古屋大学の情報セキュリティポリシーの立案・実施・継続的検討
2) 情報セキュリティ組織に関する基本的事項の決定
3) 情報セキュリティ組織間の調整
4) 明確なルール・ガイドラインの設定と、わかりやすいマニュアルの整備などによる情報関連施設利用者の権利義務の明確化
5) 情報関連施設の管理運営者の権限・裁量と責任の範囲の明確化
6) 発生した情報セキュリティ問題に関する個別の対応・処理
7) 情報セキュリティに関する情報の収集と提供
8) その他情報セキュリティに関わる事柄
9) 情報セキュリティ監査結果への対応

b) 全学情報セキュリティ組織

全学情報セキュリティ組織は以下の業務を担当する。

1) 全学的に検討を要する情報セキュリティ事項の特定と検討
2) 学内に設置される情報セキュリティ単位組織の編成方針の策定
3) 情報セキュリティ問題に対する全学的対応・処理プロセスの策定
4) 情報セキュリティ基準の全学的平準化
5) 情報セキュリティ単位組織による問題への対応・処理方法の調整と標準化
6) 情報セキュリティ問題に関わる対外的な対応
7) セキュリティポリシー実施のための支援・助言
8) セキュリティポリシーの具体化のための年次計画の策定と実施
9) 全学的なネットワーク管理者およびネットワーク機器・端末機器の機器設置責任者の選定
10) その他情報セキュリティに関わる事柄

c) 情報セキュリティ単位組織

情報セキュリティ単位組織は以下の業務を担当する。

1) 全学情報セキュリティ組織の定める組織編成方針に沿った情報セキュリティ単位組織の設立と運営

2) 情報セキュリティ単位組織におけるセキュリティポリシー具体化の年次計画の策定と実施

3) 情報セキュリティ単位組織における情報セキュリティの確保に関連する業務

4) 全学情報セキュリティ組織との共同業務

5) 情報セキュリティ単位組織のネットワーク管理者およびネットワーク機器・端末機器の機器設置責任者の選定

6) その他情報セキュリティに関わる事柄

d) 情報セキュリティ監査組織

情報セキュリティ監査組織は以下の業務を担当する。

1) 情報セキュリティ監査計画の策定

2) 情報セキュリティ監査計画に基づく監査の実施

(2) 電子化情報に対する保全・管理

情報をオンライン化し、ネットワークに接続された機器に保存する場合には、通常の印刷物とは別個の慎重な取り扱いが求められる。ネットワーク機器に保存された情報は、原則として名古屋大学行政文書管理規程に準拠して扱うべきであるが、情報保存の特殊性に応じた体制と規程・手引きを別途整備する。また、第三者が保有する電子化情報に対しても適切な取り扱いが必要となる。

a) 情報の管理

a-1) 情報の管理

公的情報をネットワーク機器上に保存しようとする者は、情報の重要性を考慮し、情報の正確性・改竄防止・アクセス権限・公開範囲・複製・更新・その他情報管理に関わる事項について基準・手続を定め、それよって情報を管理しなければならない。

a-2) 公的情報管理者の報告義務

公的情報の管理者は、情報セキュリティ組織の求めがあった場合、情報の管理状況を報告しなければならない。

a-3) 秘密情報等

公的情報の管理者により、秘密情報に指定された情報を個人の機器等に複製し、外部に持ち出す場合には、決められた手順によらなければならない。機器の認証情報その他の情報セキュリティに関わる情報は、情報セキュリティ組織の許可なしに公開してはならない。

b) 無権限アクセスの禁止

情報を利用しようとするものは、アクセス制御機構の有無にかかわらず、自己の権限外または権利侵害となるような情報へのアクセスを試みてはならない。

(3) 情報セキュリティ研修制度の高度化と啓発活動

名古屋大学の各組織は、情報セキュリティとして組織でどのような情報の扱いが求められているかを周知徹底すると共に、その管理体制の見直しを適宜行い、その結果を広報することで各人の情報セキュリティ意識の向上を図る体制を整備しなければならない。

(4) 情報セキュリティポリシーの実効性の確保

名古屋大学の各組織は情報セキュリティ監査組織による情報セキュリティ監査を受けるものとする。情報セキュリティ監査とは、被監査部門とは独立性を有した組織又は者が行う情報セキュリティに関する確認行為（独立的評価）を意味する。情報セキュリティ監査では、自己点検結果等をサンプリングし、その確認・評価を行い、その結果を各組織に報告することにより、名古屋大学内におけるセキュリティレベルの向上に資する。

(5) 情報セキュリティ技術基本方針の設定

本情報セキュリティポリシーで述べる情報セキュリティを実現するには、技術的な基本方針の設定が必要である。以下、名古屋大学が保有する情報機器に対する情報セキュリティ技術基本方針を設定するとともに、別途ガイドライン等を策定する。

a) 基本方針

a-1) 対外接続

名古屋大学のネットワークは、外部からの接続に関しては、申請に基づき必要に応じて開放することを原則とする。

a-2) ネットワーク管理者の権限

不正アクセスその他の理由によって緊急の対処を必要とする場合には、被害の拡大を防止するために、日常のネットワーク管理を行う者は、情報セキュリティ組織の議を経ずに、特定のサービスを停止する、または、特定の機器から外部へのアクセスを遮断することができる。

ネットワーク管理者は、ネットワーク機器の機器設置責任者がセキュリティポリシー、または、別途定める技術基準に違反していると認めた場合には、改善を求めることができる。

a-3) 機器設置責任者の義務

機器設置責任者が、情報セキュリティに関する義務を十分果たさなかった結果として、被害が学内外に発生した場合には、機器設置責任者だけでなく、大学全体が社会的に指弾される可能性がある。したがって、機器設置責任者は、情報セキュリティ確保のために最善の努力をしなければならない。

a-4) 情報セキュリティガイドライン

情報セキュリティ組織は、情報セキュリティガイドライン等を策定して公表するとともに、ネットワーク管理者、機器設置責任者、ネットワークの利用者に対して、情報セキュリティに関する研修を実施するものとする。

b) ネットワーク設計

b-1) 情報セキュリティ

新たなネットワークの設計・構築にあたっては、情報セキュリティを十分に考慮した設計にしなければならない。

b-2) 情報セキュリティ組織との協議

新たにネットワークを設計・構築して運用に供する場合には、事前に情報セキュリティ組織と協議して、その承認を得なければならない。既設のネットワークを延長したり、改変を計画する場合にも、情報セキュリティ組織との協議と承認が必要である。情報セキュリティ

組織の承認なく、外部から名古屋大学キャンパス情報ネットワーク内に直接アクセスするためのネットワーク設備を設置することは許されない。

c) ネットワーク設備

ネットワーク設備とは、ルータやハブ装置およびネームサービスを行う機器をいう。これらの機器の設置および管理の詳細は、別に定めるガイドラインによるが、ネットワーク設備設置および維持に関しては少なくとも以下のような基準を満たさなければならない。

c-1) ソフトウエアの最新性

ネットワーク機器のソフトウエアは、最新の状態に保つ最大の努力をしなければならない。

c-2) ネットワーク管理者以外の者のアクセス防止

ソフトウエアにより機能の設定が可能なネットワーク機器にあっては、ネットワーク管理者以外の者が機器にアクセスできないような対策をとらなければならない。

c-3) 安全な設置場所の選定

新規のネットワーク設備の設置にあたっては、物理的な破壊行為等から機器を保護するために、安全な設置場所を選択しなければならない。

c-4) セキュリティ管理を回避する機器の設置禁止

本学構成員の管理下にない装置を無認証で名古屋大学キャンパス情報ネットワークに接続可能とする情報コンセントおよび無線 LAN 装置等のアクセス機器は設置してはならない。

c-5) 機器設置責任者の報告義務

機器設置責任者は、名古屋大学キャンパス情報ネットワークに接続する機器について所定の機器登録データベースに登録しなければならない。また、情報セキュリティ組織の求め があった場合、ネットワーク機器の稼動状況を報告しなければならない。

d) 端末機器

端末機器とは、ネットワーク機器以外のパーソナルコンピュータ、ワークステーション等をいう。端末機器の設置および管理の詳細は、別に定める「セキュリティ技術ガイドライン」によるが、少なくとも以下のような基準を満たさなければならない。

d-1) 特殊機器の接続

計測器、医療機器等の特殊な機器をネットワークに接続して利用しようとする場合には、情報セキュリティ組織と事前に協議しなければならない。

d-2) セキュリティ対策の不十分な機器の接続禁止

セキュリティ技術ガイドラインに合致したセキュリティ対策の施されていない機器をネットワークに接続してはならない。

d-3) 無資格利用の禁止

端末機器は、その機器設置責任者の許可した者だけが利用できる状態でなければならない。

d-4) 機器設置責任者の報告義務

機器設置責任者は、端末機器の利用状況を把握可能にし、情報セキュリティ組織の求めがあった場合、機器の利用状況を報告しなければならない。また、所定の機器登録データベースに登録しなければならない。

d-5) 情報セキュリティ組織の指示権限

情報セキュリティ組織がセキュリティ確保上必要と認めた場合、情報セキュリティ組織は、機器設置責任者に対して、一定の具体的対策をとるよう求めることができる。

e) 情報セキュリティ機器

情報セキュリティ組織は、名古屋大学キャンパス情報ネットワークのセキュリティを最大限確保するために、ファイアウォール装置、侵入検知装置等のセキュリティ機器を設置・維持・管理しなければならない。情報セキュリティ機器の設置および運用は、少なくとも以下のような基準を満たさなければならない。

e-1) 情報セキュリティ機器の最新性

セキュリティ組織は、セキュリティ機器を可能なかぎり最新のものに保つよう努めなければならない。

e-2) 問題への迅速な対応

情報セキュリティ機器等で、セキュリティ上重要と考えられる事象が発見された場合、情報セキュリティ組織は、遅滞なく必要な対策をとらなければならない。

e-3) ネットワーク通信の監視

情報セキュリティを確保するためには、セキュリティ機器によるネットワーク通信の監視が不可欠であり、全学構成員には、セキュリティ機器によるネットワーク通信の監視が行われることを通知し、その了承を求めなければならない。

e-4) 情報公開

情報セキュリティ組織は、情報セキュリティ機器の運用状況をセキュリティ維持と矛盾しない範囲でできるだけ詳細に全学構成員に公表しなければならない。

(5) 運用・保全

名古屋大学は情報セキュリティに関する相談窓口、ならびに、情報セキュリティインシデント発生あるいはその恐れがあるときの連絡体制を整えなければならない。

(6) 情報セキュリティインシデントへの対応

名古屋大学は情報セキュリティインシデント発生における迅速な対応を可能とするために、対応手順を別途定めなければならない。

3. 実施手順

名古屋大学は、情報セキュリティ基本方針、ならびに、情報セキュリティ対策基準を具体化するために別途情報セキュリティガイドラインを設定し、名古屋大学全構成員へ周知するとともに、名古屋大学の情報環境戦略を示す情報環境マスタープランと連動することで名古屋大学情報セキュリティポリシー、名古屋大学情報セキュリティガイドラインが遵守されるように最大限の努力を図る。