豊田工業大学 情報セキュリティポリシー

Ⅰ　情報セキュリティの基本方針

大学における研究や教育などのあらゆる活動を安全に運営するために、大学の情報資産を正しく扱うことの重要性は明白である。これまで考えられないような速度で、大量の情報が行き交う社会では、情報の発信が容易になる反面、一度流出した情報を止めることは困難である。情報の不正使用、不正流出あるいはネットワークへの不正侵入等を許せば取り返しのつかない事態となることも考えられる。本学の情報資産を守り、研究や教育に用いて使いやすい情報システムを運用するために、情報セキュリティポリシーを制定する。

１．目的

本学の情報セキュリティポリシー(以下ポリシーと記す。)の目指すところは次のとおりである。

(a) 本学の情報セキュリティに対する侵害の阻止
(b) 本学内外の情報セキュリティを損ねる加害行為の抑止
(c) 本学の情報資産に関して、重要度による分類と管理
(d) 利用者が必要とする情報セキュリティに関する情報取得の支援

２．対象の範囲

本学のポリシーの対象範囲は、電磁的に記録される情報、並びにこれらの情報に接するすべての利用者とする。

一時的あるいは永続的に、本学のネットワークに接続する全てのコンピュータとその利用者を含む。

３．用語の定義

本学ネットワークの利用者とは、本学の教職員、非常勤教職員、臨時職員、委託業者、大学生、大学院生、研究員等のほか、本学で開催されるあらゆる会議等に参加して本学のネットワークを利用するすべての者である。

本学のポリシーで使用する用語の定義は、平成 12 年 7 月 18 日の政府の情報セキュリティ対策推進会議による「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である。

http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html

４．実施手順の作成

本学のポリシー実施手順は、規定、規約等として付録１に示す。

Ⅱ　対策基準

１．組織・体制

１．１ 管理･運用体制

管理・運用の体制は付録２に示すとおりである。

１．２ 管理責任者等の役割

(1) 統括管理責任者

本学の情報を統括管理する。情報の管理責任者、システムの管理責任者を統括し本情報セキュリティポリシーが正しく実施されていることを管理統括する責任がある。

(2) 情報の管理責任者および管理者

サーバやクライアント等のコンピュータに記憶される重要な情報資産には情報の管理責任者および管理者を定めなければならない。

情報の管理責任者は管理者を取りまとめる責任がある。

情報の管理責任者および管理者は重要な情報資産の内容、アクセス許可者等を定め、情報資産の散逸、破壊等が起こらないよう管理する義務がある。

なお、重要な情報資産の指定は管理責任者の責任の下で決定されるものとする。

(3) システムの管理責任者および管理者

サーバやクライアント等のコンピュータおよびネットワーク機器にはシステムの管理責任者および管理者を定めなければならない。

システムの管理責任者は管理者を取りまとめる責任がある。

システムの管理責任者および管理者は、ネットワークに接続されたコンピュータのシステム運用を行い、情報システムの保護に努めなければならない。

なお、情報の管理責任者および管理者とシステムの管理責任者および管理者は兼ねることができる。

２．不正アクセス等への対応

２．１ 不正アクセスの対応

総合情報センターは外部または内部からの不正アクセス等の侵害行為を監視し、防止する努力を怠ってはならない。また、不正アクセスを検出した場合は当該情報機器を切り離す等、付録１に示す緊急措置手順に従って安全を確保するとともに、速やかに総合情報センター協議会に報告しなければならない。

２．２ 加害行為の抑止

総合情報センターは、本学の構成員に対し、不正アクセス等の加害行為をしないよ

うに指導する義務を有する。加害行為が認められた場合は総合情報センター協議会に報告し、構成員の身分に係わる処分については、その権限を有する機関に委ねるものとする。

３．情報の分類と管理

３．１ 情報の分類

情報の管理責任者は、管理の対象となる重要な情報資産について、公開・非公開を定めなければならない。非公開情報とは閲覧が制限された情報で、公開情報とは全ての利用者が閲覧することのできる情報である。

３．１．１　非公開情報

情報の管理責任者によって許可された者以外は､非公開情報を保管してはならない。システム管理者は重要度に応じた適切なセキュリティ対策を施して情報を保護しなければならない。

３．１．２　公開情報

公開情報は情報の改竄や偽情報の流布に対する防止策を施さなくてはならない。公開情報の中に、個人情報、プライバシーおよび著作権等の知的財産権の侵害に当たる情報を含ませてはならない。

不特定多数のものに情報の発信を行う場合は、法律(「特定電子メールの送信の適正化等に関する法律」など)に定められた基準を満たす必要があることに留意しなければならない。

３．２　情報の管理

本学の情報資産は職務上定められた権限を有する情報の管理者が管理しなければならない。

情報の管理者は、コンピュータに保存した情報のバックアップ等の業務をシステムの管理者に代行させることができる。

システムの管理者は管理する上で必要な範囲を超えて情報にアクセスしてはならない。

情報の管理者はシステムの管理責任者の許可を得ていない者に情報機器の運用をさせてはならない。

３．３　情報機器および記録媒体の処分

情報機器および記録媒体を廃棄するときは、処分方法に注意しなければならない。

レンタル機器の撤去に際しても同様な注意をしなければならない。

４．物理的セキュリティ

４．１　クライアント機器

主として利用者のパソコンとして用いられるクライアント機器は、システム管理

者の許可を得て用いなければならない。

４．２　ネットワーク機器

災害、事故等の非常時の対策を、付録 1 に示す緊急措置手順に定めておかなくてはならない。

４．３　サーバ機器

複数のクライアント機器からアクセスされ、共同で利用されるサーバ機器のうち、特に重要とシステム管理責任者が認めた場合は、管理された区域に設置し、入退室の記録を残されなければならない。

上記の重要なサーバ機器は事故や故障の際、迅速に回復できるような体制を構築しておかなければならない。

重要なサーバ機器の情報は、定期的にバックアップを行うものとする。

重要なサーバ機器のアクセス等に関して、クライアント機器の認証と使用の記録を残さなくてはならない。

５．人的セキュリティ

本学の構成員等のポリシーの対象者は、ポリシーを遵守しなければならない。

５．１　教育・研修

総合情報センター等が行う定期的な講義や研修を通して、本学の全構成員がポリシーあるいは実施手順を理解し、情報セキュリティ上の問題が発生しないよう努めなければならない。

５．２　パスワード管理

本学のネットワークへの接続を許可された者(利用者)は、各自のパスワードの重要性を理解し、十分なセキュリティを保てるパスワードにしなければならない。いかなる場合でも他人に漏らしてはならない。

５．３　システム管理

規定に基づく利用者以外に、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速やかに除去しなければならない。

ログ情報および通信の保全のために情報を入手する場合は、規定に定められているような要件と手続きを遵守しなければならない。

システム管理者はいかなる場合も、利用者のパスワードの聞き取りを行ってはならない。

６．技術的セキュリティ

総合情報センターは情報を保護するため対策を講じ、利用者が安心して便利に使える環境の整備構築に努力しなければならない。

６．１　セキュリティ情報の入手と警告発信

総合情報センターは、ウィルス情報等インターネットで起きている状況を把握し、利用者に注意を呼びかけるものとする。

７．評価・点検

総合情報センターおよび総務部はポリシーに関する点検と評価のため、定期的に以下のような検討を行う。

(1) ポリシー運用実態の把握
(2) 利用者の意見の把握
(3) 情報セキュリティ診断
(4) 情報セキュリティ監査

上記の評価・点検を受け自己点検・評価委員会および総合情報センター協議会はポリシーの実効性を評価し、よりセキュリティレベルの高い、遵守可能なポリシーに変更しなければならない。

付則

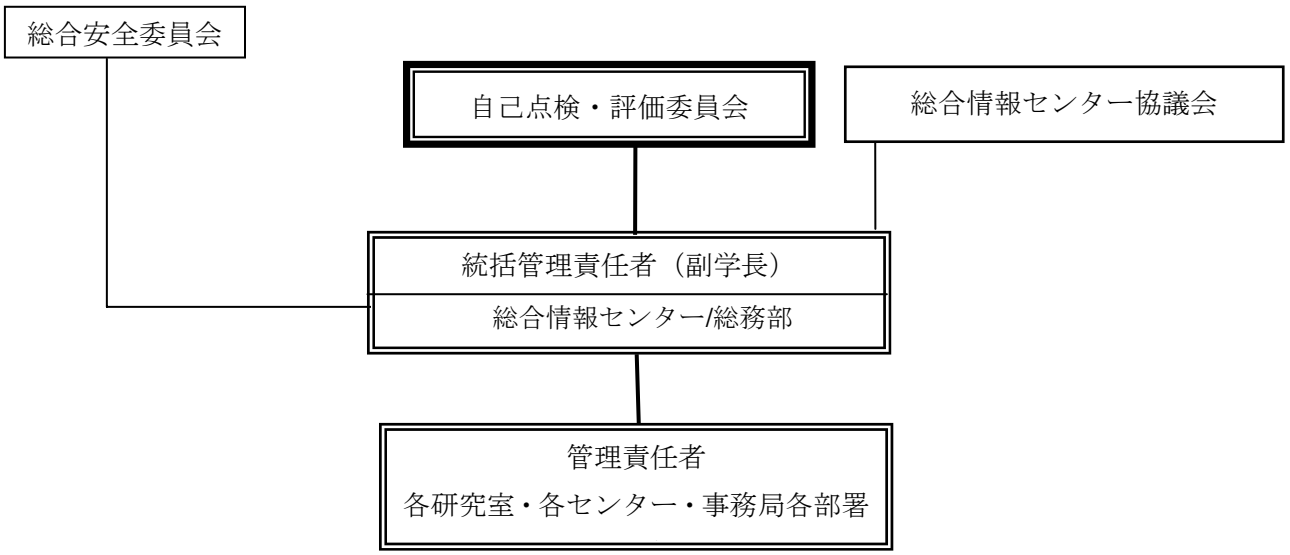
１．このポリシーは平成 19 年 4 月 1 日より施行する。

制定　平成 19 年 3 月 22 日

付録１　情報セキュリティポリシー実施手順

総合情報センター規定
情報処理関連施設利用規定
豊田工業大学総合ネットワーク利用心得
豊田工業大学総合ネットワーク利用者細則
豊田工業大学総合ネットワーク運用管理細則
豊田工業大学総合ネットワーク緊急措置手順

付録２　情報セキュリティポリシー管理・運用体制



管理・運用体制図

・総合情報センターと総務部は協力して、統括管理責任者をサポートしなければならない。
・統括管理責任者は総合情報センターと総務部と共に、自己点検・評価委員会にて本ポリシーの適用状況を審議し、高い実効性を保つよう努力しなければならない。
・統括管理責任者は自己点検・評価委員会にて決定された事項を、スムーズに実行できるよう各管理責任者に指示命令を下すことができる。
・総合情報センター協議会にて本ポリシーに係わる技術的な課題等を審議し、必要であれば自己点検・評価委員会に報告しなければならない。総合情報センター等は課題解決のために努力しなければならない。
・総合安全委員会には、本ポリシーに関する重要事項を報告し、指摘があれば、総合情報センター等はその課題の解決に努力しなければならない。