○学校法人金沢工業大学の情報セキュリティポリシー

（平成 17 年 4 月 1 日施行）

１．基本指針

学校法人金沢工業大学(以下「本法人」という。）では、設置する金沢工業大学並びに金沢工業高等専門学校の教育研究及び管理運営にかかる諸業務において、システム化、ネットワーク化による教育システムや修学支援システムなど、多岐にわたる情報システムを構築している。その結果、所有する教育、研究、管理運営業務などに利用される諸情報の安全性の確保が本法人の健全な経営を維持していくうえでの重要な課題になってきている。

また、学内外の研究者、教育者、その他関係者との学内ネットワークやインターネットを介した情報交換においても、ネットワークの国際的レベルの安全性や高い信頼性が求められるようになってきた。このため本法人では、情報資産を保護し、情報セキュリティの管理を的確に遂行するため、情報セキュリティポリシーを定めるものとする。

また、本セキュリティポリシーは、1980 年に採択されたＯＥＣＤプライバシー・ガイドライン８原則のうち、情報の正確性、完全性、最新性を求めた「データ内容の原則」、目的外の使用の制限を求めた「利用制限の原則」、そして、情報の紛失、破壊、修正、開示等の危険に対する安全保護措置を求めた「安全保護の原則」に照らして策定するものとする。

２．セキュリティポリシーの適用範囲と対象

本セキュリティポリシーの適用範囲は、本法人が有する教育研究及び学校運営に係わる情報資産（ハードウェア、ソフトウェア、データ、情報、ネットワーク及びこれらに関連する施設、設備、ドキュメント、保存媒体等）であり、適用対象者はこれらの情報資産を取り扱う次のものすべてとする。

（１）本学の理事
（２）本学の教職員
（３）本学の学部生、大学院生、高専生、研究生、聴講生
（４）本学の教職員と共同して教育研究を行う者
（５）情報セキュリティ責任者が適当と認めた者
（６）非常勤教職員
（７）（１）～（６）の他、派遣社員、委託先業務従事者など、雇用形態、職位、勤務場所を問わず、本学の情報システムを使用する者

３．セキュリティポリシーの管理体制

本セキュリティポリシーは、情報セキュリティ責任者（以下「ＣＩＳＯ：Chief Information Security Officer」という。）のもとで策定し運用するものとする。

また，本学の運営環境やシステム利用環境の変化、情報技術の進展などに伴い、必要に応じてＣ

ＩＳＯを長とする情報セキュリティ委員会（以下「セキュリティ委員会」という。）を設置する場合がある。

セキュリティ委員会が設置された場合の構成員は次のとおりとする。

（1）情報セキュリティ責任者（ＣＩＳＯ）

（2）個人情報管理責任者

（3）情報システム部門責任者

（4）情報システム部門技術者

（5）情報資産管理者の代表

4．セキュリティ管理責任

（1）情報資産管理者の責務

各部局が保有する情報資産の管理を行うため、各部局に情報資産管理者を置く。情報資産管理者は、その管理対象となる情報資産の保護に関し、本セキュリティポリシーの定めに則って管理がなされているかを継続的に監視し、違反行為を発見したときは、改善を施すと共にＣＩＳＯに報告する義務と責任を負う。

（2）情報資産利用者の責務

情報資産の利用者（以下「利用者」という。）は、当該所属部局及び利用する業務に係る情報資産の利用権限に応じて、本セキュリティポリシーを遵守する義務と責任を負う。

5．コンピュータネットワーク利用規範

本学では、正規の利用者に対して、ネットワークならびにサーバコンピュータへのアクセスを保証し安定した運用を行うために、利用者が遵守すべき行動の基準（規範）を次のように定めている。

また、利用者には、ネットワークを使用する際のすべての行為に対して責任を負うとともに、情報セキュリティ関連法規や規則の遵守を義務づけている。

（1）虚偽に利用者ＩＤを申請したり、不正に他人の利用者ＩＤを使用してはならない。

（2）自分の利用者ＩＤを他人に使用させてはならない。

（3）システム資源を大量に消費することにより他の利用者の正常な使用を妨害したり、コンピュータシステムの正常な運用を妨げるような行為により、他の利用者に迷惑又は損害を与えてはならない。（求められていないゴミメールやチェーンレターの送信を禁止する。また、故意にコンピュータシステムを混乱させる行為や有害なプログラムの持ち込みを禁止する。）

（4）営利、非営利を問わず、商用を目的とした利用をしてはならない。

（5）他人のプライバシーを侵害したり、他人を誹謗中傷してはならない。

（6）嫌がらせや、公序良俗に反する行為、その他脅迫的行為をしてはならない。

（7）著作権の対象になっているものに対して、著作権者の許可や正規のライセンスなしにこれを侵害してはならない。

さらに、学内ネットワークや情報システムの安全性を確保するため次の遵守事項を定めている。

（1）学内ネットワークは、教育研究及び設置する学校の運営業務以外の目的に使用してはならない。

（2）学内ネットワークに、コンピュータやネットワーク機器を接続しようとする者は、必要なネットワーク接続手続きを行なわなければならない。

（3）学内ネットワークに、コンピュータを接続しようとする者は、ウィルスの感染を防止する対策を講じなければならない。

（4）ウィルスに感染した場合、あるいは感染の疑いがある場合は、直ちにネットワークから切り離し感染の拡大を防止しなければならない。

一方､学内ネットワークや情報システムの安全性を確保するため､次の措置を講じるものとする。

（1）悪意ある者からの学内ネットワークに対する攻撃やウィルスの侵入を防御するため、ネットワークの出入口で､FireWall によるパケットフィルタリングやメールサーバによるウィルス検知を行う。

（2）個人情報などの重要な情報へのアクセスにあたっては、情報の登録時や参照時の認証やアクセス制御ならびに暗号化などの対策を施し、安全性と信頼性を確立するものとする。

6．一般的な遵守事項

本法人の情報資産を保護するために、適用対象者は次に掲げる事項を遵守しなければならない。

（1）学外への持ち出しの制限

情報の漏えい、改ざんを防止する観点から、情報資産が記憶されたコンピュータ機器や記憶媒体を学外へ持ち出してはならない。

（2）情報資産の複製の制限

情報の正確性、完全性、最新性を求めた「データ内容の原則」から、情報システム部門が管理する情報資産が収納されたサーバシステムからのデータの複製をしてはならない。なお、業務運営上の必然性により、やむを得ず複製が必要な場合は、ＣＩＳＯの事前承認を必要とする。

（3）守秘義務

公共の利益を優先する必要があると判断される場合、及び業務遂行上必要と認められる場合を除き、業務遂行に際して知り得た情報及び技術を、第三者に開示、提供、漏えいしてはならない。また、個人のプライバシーに関する情報を取り扱う場合は、その保護に留意すると共に、事故が発生しないように対策を講じなければならない。

（4）知的財産権の保護

本法人が保有する知的財産権を保護し、また、第三者が保有する知的財産権を侵害してはならない。

（5）事故、障害の報告義務

事故及び障害を発見したとき、或いは発生が予測されるときは、各部局の情報資産管理者等に速やかに報告し、その損害を最小限に抑制する行動をとらなければならない。

（6）外部委託時のセキュリティ管理

情報資産に関わる業務を外部に委託する場合は、外部委託業者と交わす契約書に、問題が発生した場合に責任の所在が明確になる項目や、本法人の情報セキュリティポリシーが遵守されなかった

場合の対応に係わる項目などを明記するなど、情報資産の外部への漏えいを防止するための措置を講じなければならない。

（7）情報セキュリティ関連法規や規則の遵守義務

個人情報の保護に関する法律をはじめ、不正アクセス行為の禁止等に関する法律、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（通称　プロバイダ責任法）、電子署名認証法、電子帳簿保存法、著作権法および刑法ならびに今後制定される情報セキュリティ関連法規等を遵守しなければならない。

7．情報セキュリティに係わる禁止行為

次に掲げる情報セキュリティを脅かす行為は、いかなる場合も行ってはならない。また、利用者は、悪意を持ってこれらの行為を行う者が存在することを認識し、被害に遭わないように各々が予防措置を講ずるなど、十分な注意を払うことが求められる。

（1）不正アクセス

他人の利用者ＩＤとパスワードを用いて、正当な所有者の許可なくネットワーク・サーバや情報システムに不正にアクセスし、情報の盗聴、窃盗、漏えい、改ざん、破壊、消失等を行う。

（2）不正浸入

セキュリティ・ホール（システムの欠陥）やサーバの不適切な設定を突いて、管理者権限を奪いシステムに不正にアクセスし、Ｗｅｂページの書き換えや情報の漏えい、改ざん、破壊等を行う。

（3）不正攻撃

悪意を持った者によるポート攻撃などにより、ネットワークや情報システムへの運用妨害を行い、異常停止に至らしめる。

（4）スパム・メールの送信

受信を希望していない者に不要なメールを大量に送りつけ、混乱を引き起こす。

（5）メール爆弾の送信

大量のメールや大容量の添付ファイルを一度に特定のメール・サーバや個人に対して送信し、混乱を引き起こしたり運用妨害を行う。

（6）なりすまし

他人の利用者ＩＤとパスワードを用いて、正当な所有者に成り代わってネットワーク・サーバや情報システムからのサービスを受けたり、情報の窃盗、漏えい、改ざんを行う。

（7）盗聴

ネットワーク上を流れるパスワード情報やメールの内容などを盗聴し、情報の窃盗、漏えいを行う。

（8）盗難

盗難や置き忘れられたコンピュータや記憶媒体から、情報の窃盗・漏えいを行う。

（9）ＤｏＳ（サービス不能）攻撃（ＤｏＳ:Denial of Service ）

意図的に大量のパケットを送り付けて、特定のサービスやコンピュータおよびネットワークを一

時的あるいは継続的に使用不能にさせる。

(10) コンピュータ・ウィルスの配信

不正プログラムを広く配信することにより、データの破壊、消失やコンピュータを機能不全に陥れる行為で、拡散により多くのコンピュータに被害を及ぼす。

(11) その他

倫理観、道徳観の欠如による機密情報の漏えいや窃盗、迷惑メールの発信や掲示板へのいたずら書き、著作権違反や肖像権の侵害、人権侵害やプライバシー侵害などの行為

８．事故発生時の報告義務

本セキュリティポリシーに基づく適切な情報セキュリティ管理を行っていても、不測の事故や障害などの発生に加え、様々な攻撃にさらされることが予想される。このような不測事態発生時には、ＣＩＳＯに対して速やかに報告するものとする。

９．遵守義務と罰則

本セキュリティポリシーは、適用範囲で規定したすべての者にその遵守を義務づける。また、本セキュリティポリシーの違反者には罰則を科すことがある。

さらに、セキュリティポリシー適用対象者が、本法人の情報セキュリティシステムに重大な影響を与える行為、個人のプライバシー侵害に該当する行為、資産損失を招くような悪質な行為等を行ったと認められる場合には、就業規則や学則等に則った処分を科すことがある。

また、不測事態の発生により社会的信用の失墜が避けられない場合は、ＣＩＳＯの判断により、その改善措置がとられるまでの間、例外措置を設定することを妨げない。

10．他の規則等との関係

学術情報ネットワークに係る部分は、国立情報学研究所の「ＳＩＮＥＴ（Science Information NETwork）の利用に関する規則」が優先的に適用されるものとする。

11．セキュリティポリシーの開示

本学の情報資産を使用するすべての者に対して本セキュリティポリシーを周知するため、ホームページを通じて開示するものとする。

12．適用時期

このセキュリティポリシーは、平成17年３月22日に制定し、平成17年４月１日施行する。