愛知大学

情報セキュリティ対策基準

制　定　日：平成 18 年 4 月 20 日
最終修正日：平成 21 年 2 月 18 日

目　次

1 目 的

この基準は、学校法人愛知大学（以下、「大学」という）の情報セキュリティポリシーに基づくとともに、大学の情報資産が、改竄や破壊から保護され、定められた方法で常に利用でき、情報のセキュリティを確保した状態で、情報の利用が行われることで、大学運営の安定、継続、繁栄に寄与することを目的とする。

2 基本的な考え方

情報のセキュリティを確保した状態で、大学の情報を利用するため、別途定める「情報セキュリティ管理マニュアル」に則ったリスクアセスメントの結果を踏まえて、適用すべき情報セキュリティのための管理策を策定する。

この基準では、当該のリスクアセスメントの結果に基づいて管理策を策定するにあたり、踏まえるべき基本的な規則を記載する。昨今の情報技術の進展の速さ及び情報管理に対する社会的な変化の急激さを考慮すると、一時点における情報セキュリティ確保のための画一的な規則を策定する作業は困難であり、かつ、有意性の薄い作業であるとも考えられ得る。そのため、「情報セキュリティ管理マニュアル」に則り、本基準も含めて管理策の見直しを適宜実施する。

3 適用範囲

本対策基準及び各対策ガイドラインは、本学の所有する全ての情報資産ならびに本学の情報資産を利用する全ての者に対して適用するものとする。ただし学生については、別に定める学生向け対策基準を適用するものとする。

4 定義

(1) 「完全性」とは、情報及び処理方法の正確さ及び完全である状態を安全防護することをいう。
(2) 「機密性」とは、情報にアクセスすることが許可された者だけがアクセスできることを確実にすることをいう。
(3) 「可用性」とは、許可された利用者が、必要なときに情報にアクセスできることを確実にすることをいう。
(4) 「情報セキュリティ」とは、情報資産の完全性、機密性及び可用性を維持することをいう。
(5) 「アクセスコントロール」とは、情報の内容に応じて、情報にアクセス可能な利用者を定めることをいう。
(6) 「オペレーティングシステム」とは、入出力機能やディスクやメモリの管理など、多くのアプリケーションソフトから共通して利用される基本的な機能を提供し、コンピュータシステム全体を管理するソフトウェアのことをいう。
(7) 「コンピュータウィルス」とは、第三者のプログラムやデータベースに対して意図的になんらかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能を一つ以上有するものをいう。
(8) 「コンプライアンス」とは、守られるべき倫理や行動規範なども含んだルールを遵守し、社会秩序を乱す行動や社会から非難される行動をしないことをいう。
(9) 「情報資産」とは、情報（個人情報を含む）及び情報を管理する仕組み（情報システムならびにシステム開発、運用及び保守のための資料等）の総称をいう。

5 情報セキュリティのための規則

情報セキュリティ責任者は、「情報セキュリティ管理マニュアル」に則ったリスクアセスメントの結果及び以下の規則に基づき、情報保護のための管理策を策定する。管理策は、リスクの受容レベルを特定した上で、個別案件のリスクの受容の決定、リスクの移転、リスクを受容できるまで低減等を行う。

(1) アクセスコントロールに関わる規則

ア 大学の組織外の者が利用する情報システムについては、大学の関係者のみで利用する情報システムに比べ、情報システムの無断使用や情報漏洩、改竄等が発生しやすいことが懸念されるため、アクセスコントロールを厳格に実施しなければならない。また、適切であれば利用者に対し契約上の利用制限を明記しなければならない。

イ 情報資産及び情報資産の設置場所には、その情報資産の盗難及び物理的な破壊等による被害を防止するために、物理的なアクセスコントロールを実施し、アクセスは必要最低限の要員に限定しなければならない。

ウ 情報へのアクセスコントロールについては、大学が正当と認める利用者が業務上の必要性に応じて確実に必要な情報へアクセスできるとともに、業務上の必要性がなく、情報を利用する権限のない者の情報へのアクセスを防止するため、業務上必要な情報へのアクセス者を明確に定め、その定めに沿って情報へのアクセスの権限を付与しなければならない。

エ 情報へのアクセス権限の付与を確実に行うため、情報の利用者の登録及び権限の付与をしなければならない。特にシステムを管理するための権限等、権限の及ぶ範囲の広い権限を保有する利用者については厳格な管理を実施しなければならない。

オ 情報へアクセスする権限のない者による成りすましによる情報の不正利用を防止するため、利用者が情報の利用権限を適切に管理しなければならない。

カ コンピュータネットワーク（以下、「ネットワーク」）を利用した論理的な不正アクセスを防止するため、ネットワーク利用者の特定によるアクセスコントロールを講じるとともに、利用場所や接続機器の特定によるアクセスコントロールを可能な限り実施しなければならない。

キ 情報システムの不正利用を防止するため、ネットワークのアクセスコントロール、オペレーティングシステムのアクセスコントロール、情報システムのアプリケーション毎のアクセスコントロールを可能な限り実施しなければならない。

ク 情報システムの不正利用を防止するため、情報システムは業務上必要な者のみが利用できるように利用者権限による論理的アクセスコントロールに加え、必要に応じて端末の設置場所に物理的なアクセスコントロールを実施しなければならない。

(2) 情報システムの開発に関わる規則

ア 新規に開発、あるいは変更を加える情報システムにおいて、必要な情報セキュリティを確保するため、業務要件定義の際、機能要件だけでなく、必要なセキュリティ要件を明確にし、その要件を確実にシステムに反映しなければならない。

イ 情報システムの開発にあたっては、情報システムで取り扱う情報の完全性を確保するため、データの入力、処理、出力時に完全性を可能な限り確認しなければならない。

ウ 暗号技術の不適切な又は正しくない使用を避けるために、暗号技術の利用に関わる規則を定め、規則に基づいて暗号技術の導入検討を実施しなければならない。

エ 作成される情報システムの信頼性及び安全性を確保するため、情報システムの開発環境におけるソフトウェア、プログラムソース、テストデータに対し改竄を防止しなければならない。

オ 新規に開発、あるいは変更を加えるアプリケーションの不備に起因して、本番システムに悪影響が発生することを防止するため、アプリケーションの開発及び変更に関わる規則及び手続を定めなければならない。

(3) 情報システムの運用に関わる規則

ア 情報処理設備の不備に起因する情報システムの停止を防止するため、情報処理設備には物理的なアクセスコントロールを講じるとともに、情報処理設備の設置にあたっては、当該設備を保護しなければならない。

イ 情報システムの信頼性及び安全性を確保するため、運用手順及び障害対応手順等の運用手続を標準化し、それに準拠した運用を実施しなければならない。また、開発者の誤謬、不正から本番稼動する情報システムで処理される情報を保護するため、本番稼動する情報システムと開発用の情報システムを可能な限り分離しなければならない。加えて、開発要員の運用業務兼務及び本番システムにある全ての情報資産へのアクセスを可能な限り防止しなければならない。

ウ 情報システムの信頼性及び安全性を確保するため、将来的に必要なキャパシティ及びパフォーマンスの計画を策定し、その状況を監視しなければならない。

エ 情報システムの信頼性及び安全性を確保するため、システムを本番システムへ移行する際の受け入れ基準を明確にしなければならない。また、受け入れ時には当該基準を満たしていることが確実に保証されなければならない。

オ コンピュータウィルスが情報システムで取り扱う情報の完全性を損なうことを防止するため、コンピュータウィルスに感染することを予防しなければならない。また、感染時の被害を最小化するための対応を実施しなければならない。

カ 情報システムの信頼性及び安全性を確保するため、情報のバックアップ手続及びオペレーション記録、障害記録等の取得、管理を実施しなければならない。

キ ネットワークの信頼性及び安全性を確保するため、ネットワーク機器の管理を実施しなければならない。また、公共のネットワークに接続する場合に通過するデータの機密性及び完全性を保護しなければならない。

(4) 情報の収集、利用、管理に関わる規則

ア 情報の利用権限の無い者への情報の開示、情報の利用権限の無い者による情報の変更、窃盗を防止するため、ハードディスクのデータ消去（無効化）、離席時にはパソコンのログオフやスクリーンセーバーを実施しなければならない。

イ 装置および電子記録媒体に記録されている情報の漏洩、改竄、破壊を防止するため、電子記録媒体の利用、保管、破棄、持ち出しについて管理を実施しなければならない。

ウ 情報システムの不正利用を早期に発見し、不正利用に起因する悪影響を最小化するため、情報システムの利用状況を正しく記録し、監視を実施しなければならない。また、記録された利用状況は、定期的に確認しなければならない。

エ 情報システムの保守やシステム監査等、通常業務とは別の目的で情報システムを利用する場合においても、情報システムの信頼性及び安全性を確保しなければならない。

(5) 情報資産の学外への持ち出し、学内への持ち込みに関わる規則

ア 大学外への重要な情報資産の持ち出しは、持ち出し手続及び大学外へ持ち出した情報資産が適切に取り扱われなければならない。

イ 情報の利用権限の無い者への情報の開示、情報の利用権限の無い者による情報の変更、窃盗を防止するため、情報資産の持ち出し状況について把握し、管理しなければならない。

ウ 情報資産の紛失、改竄、誤用を防止するため、大学以外の組織との情報（ソフトウェア、電子記録媒体、電子メール、電子商取引、情報公開等）のやり取りを管理しなければならない。

エ 情報の利用権限の無い者への情報の開示、情報の利用権限の無い者による情報の変更、窃盗を防止するため、モバイルコンピューティング又は在宅勤務等大学の物理的セキュリティが有効でない場所からアクセスする場合に必要な対策を明確にし、利用者は当該の対策を講じなけ

ればならない。

オ　情報の利用権限の無い者への情報の開示、情報の利用権限の無い者による情報の変更、窃盗を防止するため、私有するコンピュータ機器及び可搬媒体の持ち込みについて把握し、管理しなければならない。

カ　ネットワーク上の不正アクセス、ネットワーク障害を防止するため、私有するコンピュータをネットワーク機器に接続することを把握し、管理しなければならない。

キ　不正なソフトウェアの利用、コンピュータの誤作動を防止するため、私有するソフトウェアを大学内のコンピュータへ利用、インストールすることを把握し、管理しなければならない。

(6) 派遣要員、委託先の情報取り扱いに関わる規則

ア　外部委託先の情報セキュリティが確保されないことに起因して、預託した情報が委託先から漏洩すること、及び、預託した情報が委託先で無断使用されること等を防止するため、大学の情報の預託が発生する業務委託については必要な対策を契約書に明記し、業務委託先での情報の取り扱い状況を監視しなければならない。

(7) コンプライアンスに関わる規則

ア　大学の関係者が情報保護に関する法的要求事項及び学内規程等に確実に準拠しなければならない。

(8) 啓発、教育に関わる規則

ア　大学の関係者の情報保護への認識不足から情報が漏洩、改竄、破壊されることを防止するため、大学の関係者へ情報保護に関わる教育、訓練を実施しなければならない。

(9) 情報セキュリティ確保のための自主点検に関わる規則

ア　情報資産に対する情報保護対策が実施され有効に機能していることを確認するために、情報資産を所管する責を負う者は、定期的に自主的な点検を実施しなければならない。

(10) 例外に関わる規則

ア　大学で定める情報保護対策の実施が、費用対効果の分析や技術的な難易度により、困難であるような例外的な事項が発生する場合、関係する情報資産を所管する責を負う者が、情報セキュリティ委員会へ報告しなければならない。情報セキュリティ委員会は情報保護対策から逸脱する当該の例外事項を取りまとめ、情報セキュリティ責任者に報告しなければならない。

イ　「情報セキュリティポリシー」に記載の例外的な事項が発生する場合、当該の例外事項の取り扱いは、「情報セキュリティポリシー」の定める規則に拠る。

(11) 危機管理に関わる規則

ア　情報セキュリティ危機管理体制

　情報セキュリティに関わるリスクは可能な限り、軽減、回避を行なうこととするが、万一リスクが発現してしまった場合、情報セキュリティ責任者は情報セキュリティ危機管理体制を構築しなければならない。

イ　情報セキュリティ危機管理計画

(ア)情報セキュリティ責任者は情報セキュリティ委員会で取り纏めた情報資産の重要度から、情報システムを復旧させる優先順位を決定しなければならない。

(イ)情報セキュリティ委員会は情報セキュリティ責任者が定める手続に沿って情報システムの復旧優先順位を策定しなければならない。

(ウ)情報セキュリティ委員会は復旧優先順位に沿ってシステムを復旧させるための計画を策定しなければならない。

ウ 情報セキュリティ危機管理計画の教育、訓練

情報セキュリティ責任者は、情報セキュリティ危機管理計画を効率的かつ有効に機能させるため、情報セキュリティ危機管理計画について定期的に訓練を実施しなければならない。

エ 情報セキュリティ危機管理計画の定期的な見直し

情報セキュリティ責任者は、情報セキュリティ危機管理計画を実態に沿って有効に機能させるため、情報セキュリティ危機管理計画を定期的に見直さなければならない。

(12) 処罰

ア この基準又はこの基準に則って策定された情報セキュリティ確保のための管理策に違反する不正な行為者を発見した場合、当該の行為者は就業規則並びに学則に基づき処罰される。

附則(リスクアセスメントの限定実施による適用範囲の制限)

当面の間、本対策基準及び各対策ガイドラインの適用範囲は、以下の部門に対して適用するものとする。

(1) 教学系課室の職員(豊橋教務課、名古屋教務課、車道教学課、豊橋学生課、名古屋学生課、短期大学部事務課)
(2) 法人系課室の職員(人事課、財務課、名古屋総務課、車道総務課)
(3) 情報企画課の職員

ただし、上記以外の課室事務職員、学生、教育職員等については、平成 18 年度以降のリクスアセスメント実施後に適用範囲を拡大するものとする。

附則(適用範囲の拡大に伴う改正)

当面の間、本対策基準及び各対策ガイドラインの適用範囲は、以下の部門に対して適用するものとする。

(1) 教育職員
(2) 教学系課室の職員(豊橋教務課、名古屋教務課、車道教学課、豊橋学生課、名古屋学生課、豊橋キャリア支援課、名古屋キャリア支援課、車道キャリア支援課、豊橋研究支援課、名古屋研究支援課、国際交流センター事務課、名古屋国際交流センター事務課、豊橋図書館事務課、名古屋図書館事務課、車道図書館事務室、短期大学部事務課)
(3) 法人系課室の職員(入試課、広報課、人事課、財務課、豊橋総務課、名古屋総務課、車道総務課、校友課)
(4) 情報企画課の職員

ただし、上記以外の課室事務職員等については、平成 19 年度以降のリクスアセスメント実施後に適用範囲を拡大するものとする。

附則(事務組織体系の変更及び適用範囲の拡大に伴う改正)

当面の間、本対策基準及び各対策ガイドラインの適用範囲は、以下の部門に対して適用するものとする。

(1) 教育職員
(2) 教学系課室の職員(豊橋教学課、豊橋キャリア支援課、豊橋研究支援課、国際交流センター事務課、豊橋図書館事務課、短期大学部事務課、名古屋教学課、名古屋キャリア支援課、名古屋研究支援課、名古屋国際交流センター事務課、名古屋図書館事務課、車道教学課、車道キャリア支援課、車道図書館事務室)
(3) 法人系課室の職員(企画・広報課、入試課、校友課、総務課、人事課、財務課、名古屋総務課、車道総務課、企画・広報課車道広報室)
(4) 情報システム課、豊橋情報メディアセンター事務室、名古屋情報メディアセンター事務室の職員
(5) 研究所・研究室等の職員(豊橋一般教育研究室、豊橋語学教育研究室、豊橋体育研究室、三遠南信地域連携センター事務室、中部地方産業研究所事務室、綜合郷土研究所

事務室、東亜同文書院大学記念センター、大学史事務室、経済学会事務室、文学会事務室、国際コミュニケーション学会事務室、名古屋一般教育研究室、名古屋語学教育研究室、名古屋体育研究室、国際問題研究所事務室、経営総合科学研究所事務室、国際中国学研究センター事務室、中日大辞典編纂所事務室、法学会・経営学会事務室、現代中国学会事務室）