○学校法人大阪電気通信大学情報セキュリティ対策基本規則

令和6年5月21日

制定

前文

学校法人大阪電気通信大学（以下「本法人」という。）における学術研究活動、社会貢献活動、業務運営等を安定的かつ効率的に実施するためには、電子情報が持つ情報セキュリティ上の脆弱性を十分認識し、情報セキュリティを確保するとともに、それを実行するための情報システムの整備が不可欠である。本法人は、情報セキュリティの重要性と学術研究における自由の尊重を認識し、情報資産の円滑な運用と保護に取り組むため、情報セキュリティポリシー（以下「ポリシー」という。）を定める。

総則

（ポリシーの構成）

第1条　ポリシーは、次のとおり構成する。

（1）情報セキュリティ基本方針

本法人が情報セキュリティに取り組むうえでの基本となる方針を定め、ポリシーの対象者に対して、基本的な考え方、役割及び責任を明確にする。

（2）情報セキュリティ対策基準

情報セキュリティ基本方針のもと、組織的に情報セキュリティ対策を行うための具体的な施策と達成すべき基準を定める。

2　ポリシーの実施手順は、情報セキュリティ対策基準に基づき各組織等において定める。ただし、体制図及び緊急連絡網はこれに含めなければならない。

（適用対象範囲）

第2条　ポリシーの適用対象範囲は、次の各号に定めるとおりとする。

（1）適用対象資産

本法人が管理するすべての情報資産とする。

（2）適用対象者

本法人の情報資産を利用する全ての者で、役員、教員（非常勤教員を含む）、職員（嘱託職員、臨時職員、派遣職員等を含む）、共同研究者、学生（大学院生、学部生、研究生、科目等履修生等）、生徒、委託業者、来学者等とする。

（遵守義務）

第3条　本法人の情報資産を利用する全ての者は、情報セキュリティの重要性について、共通

の認識を持ち、業務の遂行にあたっては、ポリシー、ポリシーの実施手順及びその他関連法令等を遵守しなければならない。

Ⅰ　情報セキュリティ基本方針

（情報セキュリティ基本方針）

第4条　情報セキュリティ基本方針（以下「基本方針」という。）は、次のとおりとする。

（1）情報セキュリティに関する法令、国が定める指針、その他の規範を遵守する。

（2）情報セキュリティに関する責任を明確にし、対策を実施するための体制を整備する。

（3）情報セキュリティに関するリスクを識別し、組織的、物理的、人的、技術的に適切な対策を実施する。

（4）情報セキュリティに関する教育及び啓発を実施し、情報セキュリティリテラシーをもって業務を遂行できるようにする。

（5）情報セキュリティに関する問題が生じたときは、速やかに被害防止を図るとともに、原因究明及び再発防止に努める。

（6）情報セキュリティを脅かす者に対し適切な措置を講じる。

（7）情報セキュリティに関する管理体制及び取り組みについて点検を実施し、組織的に改善・見直しを行う。

Ⅱ　情報セキュリティ対策基準

第1章　総則

（趣旨）

第5条　ここに規定する情報セキュリティ対策基準（以下「対策基準」という。）は、基本方針に基づき、情報セキュリティ対策を講ずるにあたり遵守すべき行為及び判断等の基準を統一するため、必要となる基本的要件を定めるものである。

（用語の定義）

第6条　ポリシーで使用する用語の定義は、次のとおりとする。

（1）情報

本法人の教育・研究・管理運営に関わる者が作成し、又は収集及び取得した内容が記録された電磁的媒体、紙媒体及びそれに準ずる媒体をいう。

（2）情報資産

情報システムに記録された情報及び情報システムに関係がある書面に記載された情報であり、電磁的に記録された情報全てを含む。書面に記載された情報には、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面、情報シ

ステムから出力した情報を記載した書面）及び情報システムに関する設計書が含まれる。

（3） 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（ア） 機密性・・・情報資産にアクセスすることを許可された者だけが、情報資産にアクセスできることを確保すること。

（イ） 完全性・・・情報資産が破壊、改ざん又は消去されていない状態を確保すること。

（ウ） 可用性・・・情報資産にアクセスすることを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状態を確保すること。

（4） 情報システム

ハードウェア、ソフトウェア、ネットワーク、記録媒体で構成されるものであって情報処理を行う仕組みをいう。本法人の情報システムは、本法人により所有又は管理されているもの及び本法人との契約又は他の協定に従って提供されるものをいい、本法人の情報ネットワークに接続される機器を含む。

（5） 情報セキュリティ実施手順

情報セキュリティ対策を実施するため、対策基準に基づいて適宜策定される基準をいう。

（6） 情報機器

サーバ機器、クライアント機器等のコンピュータ本体及びディスプレイ、プリンタ等の周辺機器をいう。

（7） サーバ機器

複数のクライアント機器からアクセスされ、共同で利用される情報機器をいう。

（8） クライアント機器

サーバ機器の提供する機能やデータへアクセスすることで処理を進めていく情報機器をいう。

（9） 記録媒体

電磁的又は光学的に情報を記録した媒体又は情報をプリントアウトした紙媒体等をいう。

（10） 組織等

本法人が設置する学校で、大学においては、各学部、機構、大学院の各研究科、各研究所、各センター及び高等学校、事務組織においては、学校法人大阪電気通信大学事務組織規則（以下「事務組織規則」という。）に規定する事務組織をいう。

（11） 教職員等

本法人の役員、教員、職員、共同研究者等、必要な許可を得て本法人の情報資産を利用する者をいう。

（12） 学生等

本法人の設置する大学の学生（研究生、聴講生、科目履修生を含む。）及び高等学校の生徒、その他本法人保有の情報資産に対するアクセス権限を認められている者（委託業者、来学者）をいう。

（13） 情報セキュリティインシデント（以下「インシデント」という。）

不正アクセス、情報漏えい、データの改ざん、ウィルス感染等により、情報セキュリティに脅威が発生している又は発生するおそれがある事象をいう。

（14） CSIRT（シーサート）

本法人において発生したインシデントに備えた体制をいう。CSIRTはComputer Security Incident Response Teamの略。

第2章 情報セキュリティの管理体制

（組織・体制）

第7条 本法人における情報基盤を整備し、情報資産の有効活用・情報セキュリティ確保を実現するための組織・体制を次のとおり定める。

（1） 最高情報セキュリティ管理者

本法人に最高情報セキュリティ管理者を置き、理事長をもって充てる。最高情報セキュリティ管理者は、本法人の情報セキュリティに関する総轄的な意思決定をし、法人内及び法人外に対する責任を負う。

（2） 統括情報セキュリティ管理者

本法人に統括情報セキュリティ管理者を置き、法人においては法人事務局長、大学においては学長、高等学校においては校長をもって充てる。統括情報セキュリティ管理者は、本法人各組織等において情報セキュリティ対策の実施に関し次の業務を統括する。

ア ポリシーの周知徹底

イ インシデントの原因調査の指示と再発防止策の策定及び実施

ウ 情報セキュリティ対策の啓発、教育の指示

（3） 総括情報セキュリティ管理者

本法人に総括情報セキュリティ管理者を置き、法人事務局長をもって充てる。総括情報セキュリティ管理者は、法人全体の情報セキュリティに関する業務を総括する。

（4） 情報セキュリティ実施責任者

本法人に情報セキュリティ実施責任者を置き、メディアコミュニケーションセンター長をもって充てる。情報セキュリティ実施責任者は、本法人における情報セキュリティ対策の実施を総括する。

（5） CSIRT長

本法人のCSIRTに情報セキュリティインシデント対応チーム長（以下「CSIRT長」という。）を置き、情報セキュリティ実施責任者をもって充てる。

（6） 情報セキュリティ責任者

組織等に情報セキュリティの責任と権限を有する者として、次号に規定する情報セキュリティ管理者を統括し、統括情報セキュリティ責任者を補佐する者として、情報セキュリティ責任者を置き、大学においては、学部長、研究科長及び機構長、高等学校においては、教頭、事務組織においては、事務組織規則に規定する部長の職にある者をもって充てる。情報セキュリティ責任者は、当該組織等の部等における情報セキュリティ対策を実施するため、次の業務を統括する。

ア ポリシー等に基づく指示

イ インシデントの原因調査の取りまとめと再発防止策の検討及び実施

ウ 情報セキュリティ対策の啓発、教育の実施

（7） 情報セキュリティ管理者

組織等に、所管する個々の情報機器、ソフトウェア及び情報を管理・監督し、情報セキュリティを維持し、情報セキュリティ対策を実施する者として、情報セキュリティ管理者を置き、大学においては、各学部、機構、大学院各研究科、研究所及び各センターにおける各研究室の教員、高等学校においては、各高校教諭及び常勤講師、事務組織においては、事務組織規則に規定する課長又は室長をもって充てる。情報セキュリティ管理者は、所管する区域における情報セキュリティ対策を実施するため、次の業務を行う。

ア ポリシー等の実施

イ インシデントの原因調査と再発防止策の立案及び実施

ウ その他所管する区域における情報セキュリティ対策への対応

（情報セキュリティ委員会）

第8条 本法人における情報セキュリティに関する事項を決定するため、情報セキュリティ委員会（以下「委員会」という。）を置く。

2 委員会は、次の者をもって構成する。

（1） 理事長
（2） 学長
（3） 校長
（4） 法人事務局長
（5） 副学長(情報担当)
（6） 大学事務局長
（7） 教頭(情報担当)又は事務長
（8） メディアコミュニケーションセンター長
（9） 総務部長
（10） 学事部長
（11） 最高情報セキュリティ管理者が指名する者　若干名

3　委員会に委員長を置き、前項第1号の者をもって充てる。

4　委員長に事故があるときは、委員長が第2項の者のなかから予め指名した者が、その職務を代行する。

5　委員会は、委員の過半数の出席をもって成立する。

6　委員会において決するべき事項が生じた場合は、出席者の過半数をもって決する。ただし、可否同数のときは、委員長の決するところによる。

（委員会の職務等）

第9条　委員会は、次の事項を審議する。
（1） 情報セキュリティ対策を推進するための企画及び立案に関すること。
（2） 情報セキュリティにかかわる事件・事故の調査・分析及び再発防止策の立案に関すること。
（3） 情報セキュリティに係る教育及び研修に関すること。
（4） 情報セキュリティ監査に関すること。
（5） ポリシー、関連規則等の制定及び改廃に関すること。
（6） その他情報セキュリティに係る重要事項に関すること。

2　委員会は、組織等と連携・協力し、組織等が所管する情報資産のセキュリティの管理状況の把握に努めなければならない。

（CSIRT）

第10条　本法人の信用にかかわる重大なインシデント発生時に迅速かつ円滑な対応を図り、被害を最小限とする対策を行い、情報資産の安全を確保することを目的として、総括情報セ

キュリティ管理者の下にCSIRTを置く。

2 CSIRTは、次の者をもって構成する。

（1） 情報セキュリティ実施責任者

（2） メディアコミュニケーションセンター副センター長

（3） メディアコミュニケーションセンター事務室長

（4） 総括情報セキュリティ管理者が指名する者 若干名

3 インシデント発生時には、前項に掲げる者のほか、次の者を加える。

（1） 法人・大学部門でのインシデント対応

（ア） 法人事務局長

（イ） 大学事務局長

（ウ） 総務部長

（エ） 学事部長

（オ） 広報部長

（カ） メディアコミュニケーションセンター職員

（2） 高等学校部門のインシデント対応

（ア） 事務長

（イ） 総務部長

（ウ） 広報部長

（エ） メディアコミュニケーションセンター職員

4 CSIRT長は、第3章に規定する措置を講じるために必要な指揮及び、監督を行う。

5 CSIRT長は、重大なインシデント発生時において、必要に応じて、統括情報セキュリティ管理者又は総括情報セキュリティ管理者の了承の上、最高情報セキュリティ管理者に委員会開催を要請することができる。

6 CSIRT長に事故あるとき又は不在のときは、総括情報セキュリティ管理者が予め定めた者がその職務を代行する。

7 CSIRTの職務は、次のとおりとする。

（1） インシデントに関する通報及び問い合わせ受付

（2） インシデントの障害切り分け

（3） インシデントの原因究明に係る調査及び証拠保全に係る指示

（4） インシデントにおける被害拡大防止及び復旧に係る支援

（5） インシデントに関する学外関係機関への連絡及び情報共有

（6） その他インシデントに関して必要な措置

（通報等受付窓口）

第11条 インシデントに関する通報及び問い合わせは、CSIRTに行うものとし、当該窓口はメディアコミュニケーションセンター事務室をとする。

2 窓口における職務は次のとおりとする。

（1） インシデントに係る報告の受付を行い記録すること

（2） 必要に応じて、通報に関係する者との的確な連絡を行うこと

（3） その他、通報の対応に関する必要事項を実施すること

（インシデントの発生に備えた体制）

第12条 情報セキュリティ責任者は、インシデントの発生に備え、CSIRTと連携し、報告、連絡、情報集約及び被害拡大防止のための緊急対応に必要な体制を整えなければならない。

第3章 情報セキュリティインシデントへの対応

（情報資産利用者の通報・報告）

第13条 情報資産を利用する者は、インシデント、障害及び公開情報の改ざん等を発見した場合には、直ちにCSIRTに通報しなければならない。

2 CSIRTは、前項の通報を受けた場合、情報セキュリティ責任者又は情報セキュリティ管理者に報告しなければならない。

（外部からの通報・連絡）

第14条 外部からインシデント、障害及び公開情報の改ざん等の発見又はそのおそれがある旨の連絡があった場合、その受信者は、第11条に定める通報等受付窓口に直ちに通報しなければならない。

（インシデントの対処）

第15条 情報セキュリティ責任者又は情報セキュリティ管理者は、発生したインシデント、障害及び公開情報の改ざん等について、CSIRTと協議のうえ、直ちに必要な措置を講じなければならない。

（インシデントに対する措置）

第16条 CSIRT長が、緊急にインシデントへの対応が必要と判断した場合、当該システム等に対して、次の各号に定める措置を講じることが出来る。

（1） システムの停止

（2） ネットワークからの切り離し

（3） アカウントの停止

（4） その他のインシデント対応に有効となる措置

（インシデント発生時の報告）

第17条 CSIRT長は、インシデント及び公開情報の改ざん等が発生した場合は、統括情報セキュリティ管理者に報告しなければならない。

（重大なインシデント発生時の報告）

第18条 CSIRT長は、重大なインシデント及び公開情報の改ざん等が発生した場合、総括情報セキュリティ管理者、統括情報セキュリティ管理者及び最高情報セキュリティ管理者に報告しなければならない。

2 最高情報セキュリティ管理者は、重大な事故について審議する必要がある場合は、委員会に報告しなければならない。

（記録の保存）

第19条 情報セキュリティ責任者及び情報セキュリティ管理者は、発生した全てのインシデント及び公開情報の改ざん等に関する記録を一定期間保存しなければならない。

（再発防止策の報告）

第20条 情報セキュリティ責任者及び情報セキュリティ管理者は、発生したインシデント及び公開情報の改ざん等に関する再発防止策をCSIRT長と協議のうえ、統括情報セキュリティ管理者に報告しなければならない。

2 統括情報セキュリティ管理者は、再発防止策を委員会に報告しなければならない。

（復旧にあたっての事前承認）

第21条 情報セキュリティ責任者及び情報セキュリティ管理者は、発生したインシデント及び公開情報の改ざん等からの復旧にあたっては、CSIRT長と協議のうえ、総括情報セキュリティ管理者又は統括情報セキュリティ管理者の承認を得なければならない。

第4章 情報資産の分類

（情報資産の分類）

第22条 情報資産を利用する者が、情報資産を取り扱う際の分類は次のとおりとし、その重要度に応じた情報セキュリティ対策を講じなければならない。

（1） 特別限定的に扱うべき情報資産（他者との共有を行わない文書）

（2） 関係部門又は関係グループ等に限定する情報資産

（3） 法人内及び特定の関係者に利用を限定する情報資産

（4） 広く公開して活用する情報資産

2 前項第1号及び第2号に規定する情報資産を、非公開情報資産とする。

3　前項第3号で規定する情報資産を、限定公開情報資産とする。

4　前項第4号に規定する情報資産を、公開情報資産とする。

（非公開情報資産の取り扱い）

第23条　教職員等は、非公開情報資産を、次のとおり取り扱わなければならない。

（1）　個人情報、教育・研究、事務等における非公開情報資産を不当に利用してはならない。

（2）　非公開情報資産を不特定の者が可読な状態にしてはならない。

（3）　情報の盗難・漏えい等を防止するため、暗号化、盗聴防止策及び盗難防止策を講じなければならない。

（限定公開情報資産の取り扱い）

第24条　教職員等は、限定公開情報資産を、次のとおり取り扱わなければならない。

（1）　特定の利用者に特定の情報を公開する場合、その情報の登録・閲覧は、許可された者が許可された操作だけを行えるよう、認証及びアクセス制御等を実施しなければならない。

（2）　情報の盗難・漏えい等を防止するため、暗号化、盗聴防止策及び盗難防止策を講じることに努めなければならない。

（3）　異常な登録、閲覧及び操作が行われていないか、定期的に調査・確認を行わなければならない。

（公開情報資産の取り扱い）

第25条　教職員等は、公開情報資産を、次のとおり取り扱わなければならない。

（1）　公開情報資産は、改ざん、破壊されないよう、適切に管理されなければならない。

（2）　情報を公開する場合には、個人情報の漏えい、プライバシーや著作権の侵害に十分に注意し、公開できる情報だけの抽出を行い、公開してよい形に加工しなければならない。

（情報資産の管理）

第26条　情報資産を作成した組織等の教職員等は、情報資産を第22条に定める分類により管理しなければならない。

2　本法人が所有するサーバ機器に保存されず、個々のクライアント機器に保存された情報資産は、原則として、当該クライアント機器を日常的に利用する者が管理しなければならない。

第5章　物理的セキュリティ

（管理区域の設置）

第27条　情報セキュリティ実施責任者は、サーバ機器等の重要な情報システム又は情報資産を、管理する情報の重要度に従い、それぞれ設定された管理区域内に設置し、正当なアクセ

ス権のない者が使用できないよう、必要に応じて入退室の認証・記録や警備システムの設置等、物理的なセキュリティ確保に努めなければならない。

（情報機器及び記録媒体の盗難対策）

第28条　情報セキュリティ管理者は、情報機器及び記録媒体の盗難予防に努めなければならない。

（情報機器及び記録媒体の紛失及び置き忘れの予防）

第29条　情報セキュリティ管理者は、情報機器及び記録媒体の紛失又は置き忘れの予防に努めなければならない。

（情報機器及び記録媒体の法人外への持ち出し）

第30条　教職員等及び学生等は、個人情報及び本法人の重要なデータが入った情報機器及び記録媒体を法人外へ持ち出してはならない。ただし、やむを得ず情報機器及び記録媒体を法人外へ持ち出す場合は、情報セキュリティ管理者の許可を受けて情報の漏えいが発生しないよう、情報セキュリティ対策を講じなければならない。

（情報機器及び記録媒体の法人内への持ち込み）

第31条　情報セキュリティ管理者は、情報機器及び記録媒体を法人内へ持ち込むことを認めた場合、ウイルスチェックを行う等の情報セキュリティ対策を講じなければならない。

（情報のバックアップ）

第32条　情報セキュリティ管理者は、サーバ機器等に記録するデータは、必要に応じて定期的にバックアップしなければならない。

（情報機器及び記録媒体の処分）

第33条　情報セキュリティ管理者は、情報機器及び記録媒体を破棄する場合は、残存情報が第三者に読み取られることのないようにしなければならない。

第6章　人的セキュリティ

（教育及び研修）

第34条　最高情報セキュリティ管理者は、情報セキュリティに関する啓発や教育を実施するため、必要な措置を講じるように努めるものとする。

2　教職員等及び学生等は、研修等を通じて、ポリシー等を理解し、情報セキュリティ上の問題が発生しないように努めなければならない。

（委託契約）

第35条　教職員等が情報システムの開発及び保守並びにシステム管理業務を委託業者に発注する場合は、外部委託業者から再委託を受ける業者を含め、ポリシーを遵守することを明記

した契約を締結するものとする。

第7章　技術的セキュリティ

（不正アクセス等への対応）

第36条　情報セキュリティ実施責任者は、不正アクセスの防止及び検出するための適切な手段を講じなければならない。

2　情報セキュリティ管理者は、不正アクセスが検出された場合は、第3章の規定に基づき、本法人内で連携を行い、関連する通信の遮断又は該当する情報機器の切り離しを実施する。

（アクセス制限）

第37条　情報セキュリティ管理者は、情報資産の内容に応じて、アクセス可能な利用者を定め、不正なアクセスを阻止するために必要なアクセス制限を行わなければならない。

2　情報資産を利用する者は、アクセス権限のない情報資産へのアクセス、許可されていない情報資産を利用してはならない。

（ネットワークの運用管理）

第38条　本法人の基幹ネットワークの管理は、情報セキュリティ実施責任者が行い、サブネットワークの管理は、情報セキュリティ実施責任者により、その設置が許可された者がこれを行う。

2　情報セキュリティ実施責任者は、基幹ネットワーク及び重要なサブネットワークについて、ファイアウォール等のセキュリティ対策機器を導入し、本法人外部からの不正アクセス等に対する防御や内部から外部への攻撃に対処しなければならない。

3　情報セキュリティ実施責任者は、ファイアウォール等のログを一定期間保存しなければならない。

4　情報セキュリティ実施責任者は、新たな技術による本法人内ネットワークへの攻撃に対処できるよう、必要に応じて、セキュリティ対策機器及びセキュリティ対策機器上のソフトウェア（ファームウェアを含む）を更新しなければならない。

（ネットワークバックドアの排除）

第39条　本法人のネットワークのセキュリティ機能を回避する目的でバックドア（コンピュータに接続する外部ネットワーク、VPN装置、ソフトウェア等）を設置することは、原則として禁止する。

（ネットワーク接続機器）

第40条　本法人のネットワークに接続する情報機器は、ウィルス対策ソフトを導入する等のセキュリティ対策を講じたものでなければならない。

2　情報セキュリティ実施責任者は、本法人のネットワークに接続する情報機器の利用者を把握しておかなければならない。

（利用記録の保存）

第41条　個人情報等の非公開情報資産を管理するサーバ及び必要とされるサーバについては、システムログやアクセス記録等の運用に関する記録を一定期間保存しなければならない。

2　最高情報セキュリティ管理者又は委員会から運用に関する記録の提供を求められた場合は、速やかに開示しなければならない。

（アカウント及びパスワードの整備）

第42条　本法人の情報資産を利用する者は、自己のアカウントのパスワードを秘密としなければならない。又、十分なセキュリティを維持できるよう、自己のパスワードの設定及び変更に配慮しなければならない。

（非公開情報資産流出への対策）

第43条　本法人の情報資産を利用する教職員等は、情報セキュリティ管理者が許可した場合を除き、非公開情報資産の本法人外への持ち出し及び非公開情報資産への本法人外からのアクセスをしてはならない。

2　情報セキュリティ管理者の許可を得た上で、非公開情報資産を本法人外への持ち出し又は本法人外からアクセスする場合は、情報資産を暗号化する等盗難、紛失、盗聴等による情報資産流出を防ぐための対策を講じなければならない。

第8章　評価・見直し

（情報資産の点検）

第44条　情報セキュリティ実施責任者は、情報資産に係る物理的・技術的・人的セキュリティ対策について、定期的な点検を実施し、その結果を最高情報セキュリティ管理者に報告しなければならない。

（情報セキュリティ対策の更新）

第45条　最高情報セキュリティ管理者は、前条の報告により、改善が必要と認められる場合、情報セキュリティ実施責任者に対して、情報セキュリティ対策の更新等、必要な措置を講じるよう命じなければならない。

（点検・評価）

第46条　情報セキュリティ管理者は、所管する情報資産に対し、適切な情報セキュリティ対策が取られているか、適宜、点検・評価を実施しなければならない。

（監査）

第47条　最高情報セキュリティ管理者は、組織等において情報セキュリティが適正であるか、必要に応じ監査を実施しなければならない。

2　最高情報セキュリティ管理者は、前項に定める監査を実施するため、監査人を指名する。

（専門家等による監査）

第48条　監査人は、監査に必要と判断する場合は、最高情報セキュリティ管理者の承認を得て、外部の情報セキュリティの専門家又は有識者を監査人に加えることができる。

（勧告・報告に対する最高情報セキュリティ管理者の措置）

第49条　最高情報セキュリティ管理者は、監査人からの勧告に基づき情報セキュリティに関する措置等が必要と判断した場合、情報セキュリティ管理者に対し、速やかに必要な情報セキュリティ対策を講ずるよう指示するものとする。

（ポリシーの評価）

第50条　委員会は、ポリシーの実効性について、定期的に評価を行い、改善が必要と認められる場合には、セキュリティレベルの高い、かつ遵守可能なポリシーに更新しなければならない。

（違反者への措置）

第51条　最高情報セキュリティ管理者は、教職員等及び学生等がこのポリシーに違反した場合、関係法令及び法人内諸規程に基づく処置を講じることができる。

（事務所管）

第52条　この規則に関する事務は、法人事務局総務部総務課及びメディアコミュニケーションセンター事務室で行う。

（改廃）

第53条　この規則の改廃は、情報セキュリティ委員会での審議を経て、当該委員会委員長が理事長に上程し、常任理事会での審議を経て理事長が決裁する。

附　則

1　この規則は、2024年5月21日から施行する。

2　大阪電気通信大学における情報の安全性確保に関する基本指針（平成21年2月24日制定）は、廃止する。

3　大阪電気通信大学高等学校における情報の安全性確保に関する基本指針（2021年6月1日施行）は、廃止する。