総合情報センターの利用における遵守事項（第５版）

（第5版改訂　2020年4月1日）

この遵守事項は、東海大学総合情報センターが取扱うコンピューター等の情報資産を利用するにあたり、守っていただきたいことをまとめたものです。

「東海大学情報セキュリティポリシー」のもと、利用者が、本遵守事項や本学規程に違反していると総合情報センター所長または所属長が認めた場合は、利用を停止することがあります。

用語の説明

コンピューター等	：	総合情報センターが管理するコンピューター、周辺機器、ネットワーク、システム等
ログイン名	：	コンピューターを利用するためのIDであり、総合情報センターから割り当てられたもの ユーザー名ということもあります
コンピューター室	：	総合情報センターが管理するコンピューター等が整備されている教室・部屋・場所等

１．コンピューター等の利用における遵守事項

「利用の手引」等の定めに従うとともに、以下の事項を遵守してください。

（１）自分のログイン名、パスワードを他人に使用させないこと
（２）他人のログイン名、パスワードを使用しないこと
（３）他人のプライバシーを侵害しないこと、たとえば
　　・他人のファイルやフォルダーを許可なく参照しないこと
（４）知的財産権（著作権、特許権、商標権、肖像権等）に十分配慮すること
（５）公序良俗に反する行為をしないこと
（６）特定の個人や団体を誹謗中傷しないこと
（７）営利を目的とした行為をしないこと
（８）法律及び本学規程等に違反しないこと
（９）他人に迷惑もしくは損害を与えないこと
（10）個人情報等の重要な情報を保存する場合、保存場所やアクセス権を確認し、情報の漏洩がないよう心がけること

２．電子メールの利用における遵守事項

「１．コンピューター等の利用における遵守事項」の他に、以下の事項を遵守してください。

（１）許可されたログイン名で電子メールを送受信すること
（２）他人のプライバシーを侵害しないこと、たとえば
　　・受信した電子メール及び他人のメールアドレスを許可なく公開しないこと
　　・他人の電子メールを許可なく見ないこと
（３）情報の機密性に注意し、電子メールでの送受信が適当かどうか判断すること
（４）送信先メールアドレスの間違いや記載内容に十分注意して送信すること
（５）メールボックス容量を考慮し、不要な電子メールは削除する等、定期的に整理すること
（６）見知らぬ人から受信した電子メールの添付ファイルやURLを安易に開かないこと
（７）正規の電子メールを装って「偽のホームページ」へ誘導し、個人情報を入力させる「フィッシング（Phishing）」詐欺に注意すること

３．情報サービス（ホームページ・SNS等の閲覧・作成、データ入力）の利用における遵守事項

「１．コンピューター等の利用における遵守事項」の他に、以下の事項を遵守してください。
（１）情報サービスを利用して情報の書込み･発信を行う場合は、以下のことを守ること
・他人の個人情報を許可なく書込み･発信しないこと
・大学の品位を損なうような情報の書込み･発信はしないこと
・書込み･発信した内容については、個人が責任を持つこと
（２）知的財産権（著作権、特許権、商標権、肖像権等）を侵害しないこと

４．学内ネットワークの利用における遵守事項

「１．コンピューター等の利用における遵守事項」の他に、以下の事項を遵守してください。
（１）研究室等で使用するIPアドレスは、許可されたものを使用すること
（２）他人のプライバシーを侵害しないこと、たとえば
・ネットワーク上のデータを許可なく参照しないこと
（３）コンピューターウィルス等の感染や外部からの不正利用を防ぐために、セキュリティ対策ソフトの導入等、対策を施すこと
また、感染等が疑われる場合は、速やかにネットワークから切離し、駆除対策等を施すこと

５．コンピューター室の利用における遵守事項

「１．コンピューター等の利用における遵守事項」の他に、以下の事項を遵守してください。
（１）他人に迷惑をかけないこと
（２）コンピューター室内で飲食をしないこと
（３）コンピューター室内へ飲食物を持込む場合は、かばん等に入れること
（４）コンピューター室内で喫煙をしないこと
（５）コンピューター室内でゲームをしないこと
（６）ゴミ、不要用紙等は決められた場所に捨てること
（７）机、コンピューター、室内を汚さないこと
（８）授業利用の妨げにならないよう、授業の利用時間開始前までにコンピューター室から退出すること
（９）コンピューター室内の機器、装置、マニュアル類を壊したり、外部へ持出さないこと
(10) 総合情報センターが管理する機器以外のコンピューターや周辺機器を持ち込んで使用する場合には、許可を得ること
(11) 用紙の節約に努めること
(12) コンピューター室内では、スマートフォン、携帯電話の電源を切るかマナーモードにし、通話は室外で行うこと
(13) コンピューター室内の機器を使用中に破損、故障が生じた場合は、速やかに窓口・事務室まで申出ること
(14) コンピューター室内の機器を使用後は、適切な終了処理を行うこと
(15) モバイルバッテリー等、コンピューター室の利用目的に反する機器を充電しないこと

以上

東海大学情報セキュリティポリシー

（制定　2006 年 1 月 1 日）

Ⅰ　情報セキュリティの基本方針

1. 基本方針

高度情報化社会の中で東海大学の構成員が教育や研究、社会活動を安全に遂行していくためには、大学の情報資産の安全性を確保することが不可欠である。

本学の学生、教職員のすべてが、情報資産の価値を認識することが肝要であり、自身の情報を守るだけでなく、他者の資産も侵してはならないものとして行動すべきである。

本学は、構成員や学外社会に向けて、高度の安全性が確保された情報システム環境を提供する。本学の構成員はそれを正しく利用する。それにとどまらず、本学からの不正な情報提供や不正アクセスをなくして学外に対しても本学の情報システムの信頼性を高めていく。

本学の全構成員が、情報環境を個々の活動の中で正しく利用していけるよう、情報システムの運用、利用についての指針として、情報セキュリティポリシーを制定する。

情報セキュリティポリシーの目指すところは

(a)本学の情報セキュリティに対する侵害を阻止すること

(b)学内外の情報セキュリティを損ねる加害行為を抑止すること

(c)情報資産に関して、重要度に見合った管理を行うこと

(d)情報セキュリティに関する情報の取得を支援すること

である。

2. 用語の定義

東海大学情報セキュリティポリシー（以下、ポリシーと記す）で使用する用語の定義については、平成 12 年 7 月 18 日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とする。

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

3. 対象範囲

ポリシーの対象範囲は、本学のすべての情報資産に加えて、ポリシーの対象者が本学のネットワークに接続して使用するコンピュータを含むものとする。

ポリシーの対象者は、本学の全構成員（専任教職員、特任教職員、非常勤教職員、委託業者、大学院生、大学生、研究生、聴講生など）および本学の情報資産を学内で利用しようとする来学者とする。

4. 実施手順の作成

東海大学情報セキュリティポリシー実施手順（以下、実施手順と記す）を別途定めて情報セキュリティ対策推進の詳細を規定する。学部等および事務部門は部門ごとの情報セキュリティポリシー実施手順を定めてこれを補完する。

Ⅱ　対策基準

1. 組織・体制

本学に情報セキュリティ責任者を長とする情報セキュリティ委員会を設置する。情報セキュリティ委員会はポリシーを策定し、情報セキュリティ対策に関する重要事項を決定する。

学部等および事務部門ごとに情報システム管理責任者を置く。情報システム管理責任者はそれぞれの部門での情報セキュリティ対策実施手順を策定して実施する。

情報セキュリティ責任者は情報システム管理責任者連絡会議を開いて連絡調整、情報交換を行う。組織、体制等の詳細については実施手順に定める。

2. 情報の分類と管理

2.1 情報の管理

情報資産は、管理の権限を有する者によって管理される。管理の権限については実施手順に規定する。

本学の設置するすべてのパソコン、サーバおよび、ネットワーク設備にシステム管理者を定める。

情報をパソコンやサーバに保存する場合、情報の管理者は、バックアップ等の業務をシステム管理者に代行させることができる。システム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、自己の管理する情報へのアクセスのためであっても、システム管理者から許可を得ていない者に情報システムを使用させてはならない。

2.2 情報の分類

情報の管理者は、ポリシーの対象となるすべての情報について、公開・非公開を定めなければならない。

以下、閲覧できる者を限定した情報を非公開情報といい、情報の利用者すべてに閲覧を許す情報を公開情報という。

(a) 非公開情報

システム管理者から許可された者以外がコンピュータに非公開情報を保管してはならない。システム管理者は情報の機密性や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管理しなければならない。

非公開情報へのアクセスを許可する者の範囲は情報の管理者が定める。

(b) 公開情報

公開情報は情報の改ざんや偽情報の流布への対抗策と、個人情報の漏洩、プライバシーや著作権の侵害への防止策が講じられなければならない。

情報発信を行う場合は、正規の発信者であることを証明する必要が生ずることに留意しなければならない。

2.3 情報の作成、保守、システム開発

情報を作成する際は、著作権などの他者の知的財産権を侵していないことを確認しなければならない。

外部委託などのために、非公開情報を限定された第三者に開示する必要がある場合は、開示の都度、守秘義務契約を結ばなければならない。

2.4 情報機器および記憶媒体の処分

情報機器および記憶媒体を廃棄する場合は、その処分方法に注意しなければならない。

情報機器および記憶媒体を保守契約により交換する場合、またはレンタル機器の撤去を行う場合は、撤去後の記憶媒体の処理法についても十分配慮しなければならない。

3. 物理的セキュリティ

3.1 パソコン端末機器とネットワーク設備

システム管理者から許可を得ていないものが機器や設備を使えないような方策を整えなければならない。

パソコンや、ネットワークについては認証と使用の記録を残さなければならない。

端末機器とネットワーク設備には、災害、事故および情報機器の盗難への対策を講じておかなければならない。

3.2 サーバ機器

サーバ機器は、その重要度に応じたセキュリティ対策が施された管理場所に設置されなければならない。停止したときに大学内の業務遂行に重大な支障をきたす重要なサーバ機器に対しては、認証と入退室の記録を残さなければならない。

サーバ機器に記録される情報資源は、サーバ機器の重要度に応じて定期的にバックアップを行うこととする。

情報資源を保存するサーバ機器や、情報をバックアップしたメディアには、火災、地震等の災害や盗難等の犯罪から守るための対策を施さなければならない。

重要なサーバ機器については、故障や停電などの事故の際、迅速に保守、回復ができるような体制を整えておかなければならない。

4. 人的セキュリティ

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。

システム管理者は、責任を持って個々の情報システムの維持に努めなければならない。

4.1 教育・研修

本学の全構成員は、研修会や説明会または講義等を通じ、ポリシーおよび実施手順を理解し、情報セキュリティ上の問題が生じないように努めなければならない。

情報セキュリティ委員会は、システム管理者等が行う教職員向けのポリシーに関する研修の支援をしなければならない。また、教職員が行う学生向けのポリシーに関するオリエンテーションまたは講義に協力しなければならない。

情報セキュリティ委員会は、システム管理責任者がシステム管理者に行う研修プログラムの実施に必要な措置を施さなければならない。

4.2 パスワード管理

自己のパスワードは秘密としなければならない。また、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および変更に配慮しなければならない。

他の利用者のアカウントを使用してはならない。

4.3 利用範囲

情報機器やネットワーク設備は利用が許可される際に利用目的が限定されている。許された目的以外で機器や設備を使用してはならない。

アクセス権のない情報システムや情報に入り込もうとしてはならない。意図的でなく入り込んだときは、速やかに退出しなければならない。

4.4 システム管理

システム管理者は情報システムの利用資格者の規程を定めなければならない。

規程に基づく利用資格を有する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を速やかに除去しなければならない。

システム管理者は、いかなる場合にも利用者からのパスワードの聞き取りを行ってはならない。

ログ情報および通信内容の解析等にあたっては、利用者のプライバシーに配慮し、閲覧解析を認める場合の要件と手続きを定めなければならない。

4.5 外部委託

本学の業務を請け負う事業者（委託業者）はポリシーの対象者に含まれる。

情報システムの開発および保守ならびにシステム管理業務を委託業者に発注する場合は、契約書面にポリシーおよび実施手順の遵守を明記しなければならない。

5. 技術的セキュリティ

情報機器を不正なアクセス等から保護するため、情報機器へのアクセス制御、ネットワーク管理についての対策を講ずることとする。

この対策によって課される制限が教育研究上の利便性を過剰に損なうことは避けられなければならない。

5.1 ネットワーク設備およびパソコン、サーバの運用基準

パソコンなどの情報機器をネットワークに接続するときは、システム管理者を決めて、情報システム管理責任者の承認を得なければならない。

システム管理者は、許可を得ていない者が機器や設備を使えないような方策を整えなければならない。

学内のネットワークに接続されている情報機器を使うときは、認証によって利用許可が確認されなければならない。

システム管理者は、管理する情報機器のアクセス記録を、盗難、改ざんや消去等を防止する処置を施して一定期間保存しなければならない。また、定期的にそれらを分析、監視しなければならない。システム管理者の管理する情報機器が不正使用されて学内外に被害を及ぼしているときは、情報セキュリティ委員会や情報システム管理責任者が、対策に必要なアクセス記録の提出を求めることがある。システム管理者はこれに協力しなければならない。

5.2 コンピュータウィルス、スパイウェア対策

システム管理者は、不正アクセス、コンピュータウィルスやスパイウェア等情報システムの運用を妨害し、情報を漏洩しようとする攻撃行為から情報資産を守るために必要な対策を講じなければならない。

5.3 非公開情報流出への対策

情報の管理者の許可を得た場合を除いて、非公開情報の学外への持ち出し、あるいは、非公開情報への学外からのアクセスをしてはならない。

許可を得て非公開情報を学外に持ち出し、あるいは学外からアクセスするときは、情報を暗号化するなど盗難、紛失や盗聴による情報流出を防ぐための対策を講じなければならない。

6. 事故・犯罪と発生時の対処

6.1 事故、故障

ポリシーの対象者は、情報セキュリティに関する事故、システム上の障害を発見した場合には、システム管理責任者またはシステム管理者に直ちに報告しなければならない。

システム管理責任者およびシステム管理者は、報告のあった事故等について必要な措置を直ちに講じなければならない。

システム管理責任者は、発生した事故等に関する記録を一定期間保存し、情報セキュリティ委員会に報告するとともに、重大な事故に対しては、迅速な再発防止のための対策を講じなければならない。

6.2 不正使用

情報セキュリティ委員会は、情報機器の不正使用の範囲とそれに対処するための措置手順を定める。

システム管理責任者は、学内、学外からの報告や依頼を受けて、情報機器の不正使用の調査を早急に行う。不正使用が確認されたときは、手順に従って、関連する通信の遮断または該当する情報機器の切り離しを実施する。

あらかじめ定めのない行為によって情報セキュリティが阻害されたときは、情報セキュリティ責任者の判断で緊急に対処する。

本学の構成員が不正使用を行ったときは、学則、勤務規則、その他の諸規則に従って処分を受けることがある。

情報セキュリティ委員会は、発生した不正行為の内容と対処を、セキュリティを損なわない範囲で公表する。

7. 点検・評価

情報セキュリティ委員会は、ポリシーに関する点検と評価のために以下のような情報を収集して定期的に検討する。

(a) 本学の構成員からのポリシー遵守に関する意見と実施運用上の要望、クレーム

(b) 事故、故障、不正行為の事例、対策の成功事例、システム管理者からの意見や要望

(c) ポリシーの実施状況についての点検・監査結果

(d) 情報システムの機密性、完全性および可用性ならびに犯罪予防の観点からの情報セキュリティ診断結果

情報セキュリティ委員会は、これらの情報をもとに、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、かつ、遵守可能なポリシーに更新しなければならない。

情報セキュリティ責任者は学長に点検・評価の結果を報告し、本学の全構成員に提示して啓発する。

参考資料

1. 情報セキュリティ対策推進会議
「情報セキュリティポリシーに関するガイドライン」（平成 12 年 7 月 18 日）
http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html

2. 大学の情報セキュリティポリシーに関する研究会
「大学における情報セキュリティポリシーの考え方」（平成 14 年 3 月 29 日）
http://www.kudpc.kyoto-u.ac.jp/Security/tosin2001.html

○東海大学個人情報保護に関する規程

（制定　2004年４月１日）

改訂　2005年４月１日　　2015年４月１日

第１章　総則

（目的）

第１条　この規程は，個人情報保護の重要性にかんがみ，東海大学（以下，「本学」という。）が保有する個人情報の取扱いに関して必要な事項を定めることにより，本学における個人の権利利益及びプライバシーの侵害の防止を図り，もって基本的人権の擁護に資することを目的とする。

（定義）

第２条　この規程において「個人情報」とは，現在及び過去における本学の学生及びその保証人並びに教職員及び校友，並びに本学への入学を志願する者その他これに準ずる者に関する情報であって，本学が執行する業務に関して職務上取得したもののうち，特定の個人が識別され，又は識別され得るものをいう。

２　この規程において「本人」とは，前項の個人情報によって識別され，又は識別され得る特定の個人をいう。

３　この規程において「記録文書」とは，個人情報を記録する目的で本学が作成し又は収集した文書，図面，写真，フィルム，磁気テープ，磁気ディスク，光ディスクその他の媒体をいう。

４　この規程において「個人情報管理者」とは，この規程の定めるところに従い，記録文書について個人情報の管理に当たる者をいう。

（責務）

第３条　本学は，個人情報の取扱いに際して，本人の権利利益及びプライバシーの保護に努め，これをみだりに侵害することがないよう必要な措置を講じなければならない。

２　本学の教職員は，職務上知り得た個人情報をみだりに第三者に知らせ，又は不当な目的に使用してはならない。その職を退いた後も同様とする。

（個人情報管理者）

第４条　研究科長，研究科委員長，学部長，付属研究機関及び付属施設の長並びに部長相当職位にある者は，その部署が所管する記録文書について個人情報管理者となる。

２　記録文書を所管すべき部署が明らかでないときは，学長が個人情報管理者を指名する。

３　個人情報管理者は，個人情報管理者補佐（以下，「補佐」という。）を置くことができる。補佐は，個人情報管理者の指揮監督の下に，その職務を代行する。

第２章　個人情報の収集，利用及び提供

（収集の制限）

第５条　個人情報の収集は，本学の業務に必要な範囲内において利用目的（以下，「収集目的」という。）を明確に定め，その達成に相当な限度において行わなければならない。

２　前項に関わらず，当該個人情報が思想，信条又は信仰に関わり，収集することが本人の基本的人権を侵害する恐れがある場合には，これを収集してはならない。

３　個人情報は，本人から，適正かつ公正な方法によって収集しなければならない。

４　前項に関わらず,次の各号に該当するときは,本人以外から収集することを妨げない。
（１）　法令に基づくとき。
（２）　本人の事前の同意があるとき。
（３）　当該情報が本人の同意の下に公開され，又は報道等により適正な方法及び態様で公にされているものであるとき。
（４）　本人又は第三者の生命，身体若しくは財産その他の権利を保護するために必要であり，かつ本人から当該情報を収集することができないか，又は本人から事前の同意を求めることが困難な状況にあるか，若しくは適切ではないとき。
（５）　本人が現時において本学に在籍する学生又はこれに準ずる身分にある者であって，本人の教育若しくは研究指導上，必要であり，かつ本人から当該情報を収集することができないか，又は本人から事前の同意を求めることが困難な状況にあるか，若しくは適切ではないとき。

（利用及び提供の制限）

第６条　個人情報は，利用目的の達成に必要な範囲を超えて利用を行ってはならない。また，本学以外の者に対してこれを提供してはならない。
２　前項に関わらず，次の各号に該当するときは，収集目的以外の利用に供し，又は本学以外の者に対して提供することを妨げない。
（１）　法令に基づくとき。
（２）　本人の事前の同意があるとき。
（３）　本人又は第三者の生命，身体若しくは財産その他の権利を保護するために必要であり，かつ本人から事前の同意を求めることが困難な状況にあるか，若しくは適切ではないとき。
３　前項の他，本人が現時において本学に在籍する学生又はこれに準ずる身分にある者であって，本人の教育若しくは研究指導上，必要である場合には，個人情報管理者は，その個人情報を保証人，法定代理人，本人が他の機関等から本学に派遣された者である場合においてその機関等若しくはそれに準ずる者に対して提供する。
４　前第２項・第３項に定めるところにより，本学以外の者に対して個人情報を提供する場合においては，第１条の目的に反することがないよう，予めその者に対して個人情報の保護のために適正な取扱いを求め，その他必要な措置を講じなければならない。

第３章　個人情報の管理等

（個人情報の適正管理）

第７条　個人情報管理者は，個人情報の正確性を保持するよう努めなければならない。
２　個人情報管理者は，個人情報の漏洩，改ざん又は消失を防止するため，記録文書の安全管理に努め，かつそのために必要な措置を講じなければならない。

（業務の学外委託に伴う取扱い）

第８条　個人情報管理者は,個人情報の取扱いを含む業務を学外の者に委託する場合には,受託者において遵守すべき事項を契約において定めるとともに，個人情報の保護のために必要な措置を講じなければならない。
２　前項は，個人情報の取扱いを含む業務を行わせるため，学外から人員を受け入れる場合について準用する。

第４章　個人情報の開示，訂正，利用停止等の請求

（自己情報の開示請求）

第９条　本人は，本学が記録文書において保有する自己に関する個人情報の開示を請求することができる。

２　前項の請求は，別に定める方法で書面をもって行う。

３　前項の書面には次の事項を記載しなければならない。

（１）　氏名，身分，所属及びその他請求者を特定する事項

（２）　開示を求める個人情報を含む記録文書の名称等の記録文書を特定する事項及び開示を求める個人情報

（３）　開示を求める理由

（４）　その他個人情報保護委員会が定める事項

（開示の方法）

第１０条　個人情報の開示は，記録文書の写しを交付して行う。記録文書が磁気テープ，磁気ディスク，光ディスクその他の電子媒体による場合には，プリンター等によって出力した写しを交付する。

２　前項の方法による交付が困難なものについては，別の適切な方法により行うものとする。

（開示又は不開示の決定）

第１１条　第９条第１項に関わらず，個人情報管理者は，開示請求のあった個人情報が次の各号のいずれかに該当する場合には，当該個人情報の全部又は一部を開示しないことができる。

（１）　開示請求の対象となる個人情報を含む記録文書に，請求者に対して開示することができない第三者の個人情報が含まれているとき。

（２）　本人の選考，評価，判定等に関する個人情報で，それを開示することにより，当該選考，評価，判定等に重大な支障を生ずる恐れがあるとき。その他，本学の業務の適正な執行に重大な支障を生ずる恐れがあるとき。

（３）　開示請求のあった個人情報が，記録文書に含まれていないとき。

２　第９条第１項の請求を受けたときは，遅滞なく，開示するか否かの決定をしなければならない。不開示の決定をするときは，請求者に対し文書をもって決定を通知し，その理由を示さなければならない。

（個人情報の訂正又は削除請求）

第１２条　本人は，本学が記録文書において保有する自己に関する個人情報に誤りがあるとき，又は，個人情報が記録文書に記録されることがこの規程その他の個人情報保護に関する定めに反するときは，その訂正又は削除を請求することができる。

２　前項の請求については，第９条第２項及び第３項，並びに前条第２項を準用する。

３　第１項の請求に応じる場合には，訂正又は削除を行った記録文書の写しを交付しなければならない。この場合においては第 10 条を準用する。ただし，削除が当該記録文書に含まれる本人に係る個人情報の全部に及び，記録文書に記録が存在しなくなった場合はこの限りでない。

（個人情報の利用，提供又は公開の停止請求）

第１３条　本学が記録文書において保有する個人情報が不適正な目的に利用され，又は第三者に提供される場合，若しくは不適正に公開される場合，本人は，その利用，提供若しくは公開の停止を請求することができる。
２　前項の請求については，前条第１項及び第２項を準用する。
（不服の申立）
第１４条　第11条における不開示の決定に対しては,請求者は不服の申立をすることができる。正当な理由なく相当の期間内に決定が行われない場合も同様とする。
２　前項の申立は，個人情報保護申立審査会委員長に対して，書面をもって行う。
３　前項の書面には次の事項を記載しなければならない。
（１）　氏名，身分，所属及びその他申立人を特定する事項
（２）　不服申立に係る記録文書の名称等の記録文書を特定する事項及び開示を求める個人情報
（３）　開示を求める理由
（４）　その他，個人情報保護申立審査会が定める事項
４　第２項の書面には,第11条第２項における不開示の決定理由通知書の写しを添付しなければならない。ただし，正当な理由なく相当の期間内に決定が行われないことをもって不服申立の理由とする場合には，この限りでない。
５　本条の規程は，第12条による訂正等の請求の場合及び第13条による利用等の停止請求の場合に準用する。
（決定通知）
第１５条　不服申立について学長が決定を行ったときは，その結果を申立人に通知する。
第５章　個人情報保護委員会
（設置）
第１６条　学長の下に個人情報保護委員会（以下「委員会」という。）を置く。
（審議事項）
第１７条　委員会は，次の各事項について審議し，学長に提言する。
（１）　個人情報保護に関わる施策に関する事項
（２）　個人情報管理者から個人情報の収集，利用，提供，開示及び訂正等について付議された事項
（３）　その他本学における個人情報保護を推進するために委員会が必要と認めた事項
（委員会の構成等）
第１８条　委員会は，次の各号に掲げる委員をもって構成する。
（１）　大学運営本部長，事務部長，教学部長及び情報処理運営委員会副委員長
（２）　第４条第１項に定める者を除く専任教職員から学長が指名する３名以上の者
（３）　必要に応じ，学外の有識者から，学長が指名する者
２　前項第２号及び第３号の委員の任期は，２年以内の期間をもって学長が定める。ただし，再任を妨げない。
（委員長及び副委員長）
第１９条　委員会に委員長及び副委員長各１名を置く。
２　委員長は，前条第１項第２号に定める委員のうちから学長が指名する。

３　副委員長は，委員のうちから委員長が指名する。
４　副委員長は，委員長を補佐し，委員長が職務を行うことができない場合に，その職務を代行する。
（委員会の運営）
第２０条　委員長は，委員会を招集し，議事を統括する。
２　委員会は，委員長を含む委員の３分の２以上の出席をもって開催する。
３　委員会の議事は，委員長を除く出席委員の過半数によって決し，可否同数のときは，委員長が決する。
４　委員会は，必要があると認めるときは委員以外の者を出席させ，その意見を求めることができる。
第２１条　委員会の事務は，大学運営本部高等教育室が行う。

第６章　個人情報保護申立審査会

（設置）
第２２条　学長の下に個人情報保護申立審査会（以下，「申立審査会」という。）を置く。
（審議事項）
第２３条申立審査会は，第 14 条第１項及び第５項に定める不服の申立を審査し，学長に提言する。
（申立審査会の構成等）
第２４条　申立審査会は，第 18 条第１項第２号に定める者のうちから学長が指名する３名以上の者をもって構成する。
２　申立審査会に委員長１名を置く。委員長は，委員の互選による。
３　申立審査会は，委員長が招集し，委員長を含む委員の過半数かつ３名以上の出席をもって開催する。
４　第 20 条第３項は，申立審査会に準用する。
５　申立審査会は，申立人，不服申立にかかる決定を行った個人情報管理者，その他本学の教職員を出席させ，意見を求めることができる。申立人が申し出るときは，意見を述べる機会を与えなければならない。
（申立審査会の事務）
第２５条　申立審査会の事務は，大学運営本部高等教育室が行う。

付　則

この規程は，2004 年４月１日から施行する。

付　則（2015 年４月１日）

この規程は，2015 年４月１日から施行する。