学校法人中内学園情報セキュリティ対策基本規程

（目　的）

第１条　本規程は、学校法人中内学園及び流通科学大学（以下「本学園」という。）における情報及び情報システムの情報セキュリティ対策について基本的な事項を定め、もって本学の保有する情報の保護と活用及び情報セキュリティ水準の適切な維持向上を図ることを目的とする。

（適用範囲）

第２条　本規程において適用対象とする者は、本学園の教職員(専任・非常勤問わず)、入学志願者、在学生、卒業生、保護者、アルバイト、委託業者、来学者など本学園情報システムを利用するすべての者とする。

２　本規程において適用対象とする情報は、本学園が所有するすべての情報資産（書類、電子情報等）　として、以下の情報とする。

（１）教職員等が職務上使用することを目的として本学園が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

（２）その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、教職員等が職務上取り扱う情報

（３）第１号及び第２号のほか、本学園が調達し、又は開発した情報システムの設計又は運用管理に関する情報

３　本規程において適用対象とする情報システム及び機器は、本規程の適用対象となる情報を取り扱う全ての情報システムとし、次の通りとする。

（１）本学園が所有または管理しているすべてのIT機器、ネットワーク及び、情報システム

（２）常時または一時的に、本学園が管理しているネットワークへ接続されたIT機器、ネットワーク及び、情報システム

（３）本学園が他者から提供されて利用する情報システム及び機器

（最高情報セキュリティ責任者）

第３条　本学園に最高情報セキュリティ責任者を置き、理事長がこれを任命する。

２　最高情報セキュリティ責任者は、本学園の情報セキュリティに関する総括的な権限（予算と人事の権限を含む）及び情報セキュリティ対策の実施状況を理事長に報告する責任を有する。

３　最高情報セキュリティ責任者を助けて本学における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の命を受けて本学の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者１人を必要に応じて置く。

４　最高情報セキュリティ責任者は、次に掲げる事務を統括すること。

（１）情報セキュリティ対策推進のための組織・体制の整備

（２）情報セキュリティ対策基準の決定、見直し

（３）対策推進計画の決定、見直し

（４）情報セキュリティインシデントに対処するために必要な指示その他の措置

（５）前各号に掲げるもののほか、情報セキュリティに関する重要事項

（情報セキュリティ委員会）

第４条　最高情報セキュリティ責任者は、情報セキュリティ対策を適正に行うため、対策基準等の審議を行う機能を持つ組織として、情報セキュリティ対策推進体制及びその他業務を実施する部局の代表者を構成員とする情報セキュリティ委員会（以下、委員会という。）を置く。

２　情報セキュリティ委員会の委員は、最高情報セキュリティ責任者が、以下を含む情報セキュリティ対策推進体制及びその他の業務を実施する部局の代表者から指名すること。

（１）最高情報セキュリティ責任者

（２）最高情報セキュリティ副責任者

（３）情報セキュリティ実施責任者

（４）情報セキュリティ監査責任者

（５）部局総括責任者

（６）部局技術責任者

（７）最高情報セキュリティ責任者が必要と認めた者 若干名

３　委員会の委員長は、最高情報セキュリティ責任者が指名し、委員長は、必要に応じ関係者を出席させ、意見を聴くことができる。
４　情報セキュリティ委員会は、次に掲げる事項を審議すること。
（１）情報セキュリティ対策基準
（２）対策推進計画
（３）情報セキュリティ対策に関する全学的な施策に関する事項
（４）新たなリスクに対応するための情報セキュリティの安全管理措置の評価、見直し及び改善に向けた取組み
（５）教職員等に対する教育・研修計画の企画・立案
（６）その他情報セキュリティ対策のために必要な事項
（７）前各号に掲げるもののほか、情報セキュリティに関し必要な事項
５　委員会に関する庶務は、情報システム室が行う。

（情報セキュリティ監査責任者）
第５条　最高情報セキュリティ責任者を含めては、その指示に基づき実施される情報セキュリティ対策を監査する事務を統括する者として、情報セキュリティ監査責任者１人を置き、理事長がこれを任命する。
２　情報セキュリティ監査責任者は、次の事務を統括すること。
（１）監査実施計画の策定
（２）監査実施体制の整備
（３）監査の実施指示及び監査結果の理事長への報告
（４）前各号に掲げるもののほか、情報セキュリティの監査に関する事項

（情報セキュリティ実施責任者）
第６条　最高情報セキュリティ責任者は、本学園における情報セキュリティ対策の実施に関し総括し、情報セキュリティ実施責任者を置き、これを任命する。
２　最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、部局総括責任者１人を置き、これを任命する。
３　情報セキュリティ実施責任者は、次の事務を統括すること。
（１）要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の

決定

（２）情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務の取りまとめ

（３）情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備

（４）例外措置の適用審査記録の台帳整備等

（５）情報セキュリティインシデントに対処するための緊急連絡窓口の整備等

（６）定められた区域ごとの責任者の設置

（７）職場情報セキュリティ責任者の設置

（８）部局技術責任者の設置

（９）情報セキュリティインシデントの原因調査、再発防止策等の実施

（１０）情報セキュリティに係る自己点検計画の策定及び実施手順の整備

（１１）前各号に掲げるもののほか、情報セキュリティ対策に係る事務

（職場情報セキュリティ責任者の設置）

第７条　職場情報セキュリティ責任者は、教室、研究室、部署等の管理組織単位における情報の取扱いその他の情報セキュリティ対策に関する事務を統括する。

（部局技術責任者）

第８条　情報セキュリティ実施責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、部局技術責任者を選任する。

２　部局技術責任者は、情報システムにおける情報セキュリティ対策に関する事務を担う。

３　部局技術責任者は、所管する情報システムの管理業務において必要な単位ごとに部局技術担当者を置くこと。

４　部局技術担当者は、所管する情報システムの運用・管理を行う。

（情報セキュリティアドバイザー）

第９条　最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する者を情報セキュリティアドバイザーとして置く。

２　情報セキュリティアドバイザーは、次の事務を実施する。

（１）情報セキュリティ対策の推進に係る最高情報セキュリティ責任者、情報セ

キュリティ実施責任者への助言

（２）情報セキュリティ関係規程の整備に係る助言

（３）対策推進計画の策定に係る助言

（４）教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援

（５）情報システムに係る技術的事項に係る助言

（６）情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言

（７）利用者に対する日常的な相談対応

（８）情報セキュリティインシデントへの対処の支援

（９）前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

（情報セキュリティ対策推進体制の整備）

第１０条　最高情報セキュリティ責任者は、本学園の情報セキュリティ対策推進体制を整備し、その役割を規定すること。

２　最高情報セキュリティ責任者は、情報セキュリティ対策推進体制の責任者を定めること。

３　最高情報セキュリティ責任者は、以下を含む情報セキュリティ対策推進体制の役割を規定すること。

（１）情報セキュリティ関係規程及び対策推進計画の策定に係る事務

（２）情報セキュリティ関係規程の運用に係る事務

（３）例外措置に係る事務

（４）情報セキュリティ対策の教育の実施に係る事務

（５）情報セキュリティ対策の自己点検に係る事務

（６）情報セキュリティ関係規程及び対策推進計画の見直しに係る事務

（７）マネジメントレビューに係る事務

（マネジメントレビュー）

第１１条　最高情報セキュリティ責任者は、情報セキュリティ対策の状況について、年１回理事長へ報告し、理事長からのフィードバックを時機を逸することなく確実に情報セキュリティ対策に組み込むこと。

２　マネジメントレビューのインプットには、以下を含めること。

（１）情報セキュリティ対策の実施状況（目的及び目標の達成状況並びに不適合及び是正処置の状況）
（２）内部監査（外部監査）の結果

（情報セキュリティインシデントに備えた体制）
第１２条　最高情報セキュリティ責任者は、インシデントの発生時に、迅速かつ円滑に対応するため、情報セキュリティ委員会の下に、情報セキュリティインシデント対応チーム（以下「CSIRT」という。）を置く。
２　最高情報セキュリティ責任者は、教職員等のうちからCSIRTに属する職員として専門的な知識又は適性を有すると認められる者を選任する。本学園における情報セキュリティインシデントに対処するための責任者として情報セキュリティ実施責任者（CSIRT責任者）を置く。また、CSIRT内の業務統括及び外部との連携等を行う教職員等を定める。
３　最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を定める。
４　最高情報セキュリティ責任者は、以下を含むCSIRTの役割を規定すること。
（１）本学園に関わる情報セキュリティインシデント発生時の対処の一元管理
・全学における情報セキュリティインシデント対処の管理
・情報セキュリティインシデントの可能性の報告受付
・本学園における情報セキュリティインシデントに関する情報の集約
・情報セキュリティインシデントの最高情報セキュリティ責任者等への報告
・情報セキュリティインシデントへの対処に関する指示系統の一本化
（２）情報セキュリティインシデントへの迅速かつ的確な対処
・情報セキュリティインシデントであるかの評価
・被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
・文部科学省への連絡
・外部専門機関等からの情報セキュリティインシデントに係る情報の収集
・他の機関等への情報セキュリティインシデントに係る情報の共有
・情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施

５　最高情報セキュリティ責任者は、実務担当者を含めた実効性のあるCSIRT体制を構築すること。

６　最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築しておくこと。

７　最高情報セキュリティ責任者は、全学における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者部局及びその他関連部局の役割分担を規定すること。

（全学BCPとの整合）

第１３条　最高情報セキュリティ責任者は、情報セキュリティ関連規程の整備又は見直しを指示するに際し、当該規程が満たすべき要件として本学園の事業継続計画（全学BCP）との整合性の確保を含めること。

（兼務を禁止する役割）

第１４条　教職員等は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。

（１）承認又は許可（以下本条において「承認等」という。）の申請者と当該承認を行う者（以下、本条において「承認権限者等」という。）

（２）監査を受ける者とその監査を実施する者

２　教職員等は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ること。

（対策基準の策定）

第１５条　最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、対策基準を定めること。また、対策基準は、本学園の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めること。

（本規程の周知）

第１６条　本学園は対象者に対して、ホームページ等を通じて、本規程を周知する。

（規程の見直し）

第１７条　最高情報セキュリティ責任者は本規程の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行う。

附 則

この規程は、令和６年５月25日から施行する。

＜用語集＞

	用語	説明
か	外部サービス	学外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において本学園の情報が取り扱われる場合に限る。
	外部サービス管理者	外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう。
	外部サービス提供者	外部サービスを提供する事業者をいう。外部サービスを利用して本学園に向けて独自のサービスを提供する事業者は含まれない。
	外部サービス利用者	外部サービスを利用する本学園の利用者等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。
	学生等	本学園通則に定める学部学生、大学院学生、研究生、研究員、研修員並びに研究者等、その他、情報セキュリティ実施責任者が認めた者をいう。
き	機器等	情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。
	教職員等	本学園を設置する法人の役員及び、本学園に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他、情報セキュリティ実施責任者が認めた者をいう。教職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。
	業務委託（外部委託）	本学園の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。ただし、当該業務において本学園の情報を取り扱わせる場合に限る。
	記録媒体	情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書

		面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USBメモリ、SDメモリカード、外付けハードディスクドライブ、DVD-R等の外部電磁的記録媒体がある。
さ	サーバ装置	情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学園が調達又は開発するものをいう。
	CSIRT（シーサート）	本学園において発生した情報セキュリティインシデントに対処するため、本学園に設置された体制をいう。Computer Security Incident Response Teamの略。
し	実施手順	対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。
	情報	本規程第２条第２項に定めるものをいう。
	情報システム	ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、本学園が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。
	情報セキュリティインシデント	JIS Q 27000:2019における『情報セキュリティインシデント』を示し、「望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確立及び情報セキュリティを脅かす確率が高いもの。」をいう。
	情報セキュリティ関連規程	対策基準及び実施手順を総称したものをいう。

	情報セキュリティ事象	重大事故に至る可能性がある事態が発生し、なおかつ実際には事故につながらなかった潜在的事例のことをさします。例えば、情報漏洩、紛失、誤送信、誤送付、不正侵入、システム（サービス）の停止、システム（サービス）障害、詐欺等悪意あるメールの受信、悪意あるWebサイトへのアクセス、SPAMメール、ウイルス感染、DoS攻撃などを指します。
	情報セキュリティ対策推進体制	本学園の情報セキュリティ対策の推進に係る事務を遂行するため、学内に設置された体制をいう。
た	対策基準	本学園における情報及び情報システムの情報セキュリティを確保するための対策の基準として定める「情報セキュリティ対策基準」をいう。
	端末	情報システムの構成要素である機器のうち、利用者等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学園が調達又は開発するものをいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、本学園が調達又は開発するもの以外を指す「本学園支給以外の端末」がある。また、本学園が調達又は開発した端末と本学園支給以外の端末の双方を合わせて「端末（支給外端末を含む）」という。
つ	通信回線	複数の情報システム又は機器等（本学園が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学園の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、本学園が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。
	通信回線装置	通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。

ほ	ポリシー	本学園が定める「情報セキュリティ対策基本方針」及び本規程をいう。
も	モバイル端末	端末のうち、必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。
よ	要管理対策区域	本学園の管理下にある区域（学外組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。
り	利用者	教職員等及び学生等で、本学園の情報システムを利用する許可を受けて利用するものをいう。
	臨時利用者	教職員等及び学生等以外の者で、本学園の情報システムを臨時に利用する許可を受けて利用するものをいう。