上智学院情報システムセキュリティ規程

制定 2018年11月1日
改定 2019年10月1日

第１章　総則

（趣旨）

第１条　この規程は、上智学院（中学・高等学校を除く。以下「本学院」という。）における情報システムセキュリティの運用及び管理について必要な事項を定め、もって本学院の情報の保護と活用及び適切なセキュリティ対策を図ることを目的とする。

２　この規程は、情報のセキュリティを確保した状態で本学院の情報資産を利用するために必要となるガイドライン等を策定するにあたり、踏まえるべき基本的な基準を定めるものとする。

（用語の定義）

第２条　この規程における用語の定義は、次の各号に定めるとおりとする。

（１）情報システム

同一組織内において、ハードウエア、ソフトウエア、ネットワーク、記録媒体で構成されるものであって、これら全体で業務処理を行うものをいう。

（２）情報

個人情報を含む、次の情報をいう。

ア　情報システム内部に記録された情報

イ　情報システム外部の電磁的記録媒体に記録された情報

ウ　情報システムに関係がある書面に記載された情報

（３）実施手順

この規程、又はこの規程に基づき定める細則若しくは内規により策定する手順、基準、計画、マニュアル、ガイドライン等をいう。

（４）利用者

本学院の情報システムを一定期間利用する許可を受けて利用する者をいう。

（５）臨時利用者

前号以外の者で、本学院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者をいう。

（６）情報セキュリティ

情報の完全性（情報及び処理方法の正確さ並びに完全である状態を安全防護すること）、機密性（情報にアクセスすることが許可されたものだけがアクセスできることを確実にすること）及び可用性（許可された利用者が、必要な時に情報にアクセスできることを確実にすること）に対する脅威から情報を保護することをいう。

（７）電磁的記録

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、コンピュータによる情報処理に供されるものをいう。

（８）インシデント

情報セキュリティに関し、意図的又は偶発的に生じる、関係法令又は本学院の諸規程に違反する事故又は事件をいう。

（９）明示等

情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように周知又は個別に通知することをいう。

（10）完全性

情報及び処理方法の正確性並びに完全性を安全防護することをいう。

（11）機密性

情報へのアクセスを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。

（12）可用性

許可された利用者が、必要な時に情報にアクセスできることを確実にすることをいう。

（13）アクセスコントロール

情報の完全性、機密性及び可用性を維持することをいう。

（14）オペレーティングシステム

入出力機能及びディスク並びにメモリの管理など、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。

（15）コンピュータウィルス

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。

（16）コンプライアンス

守られるべき倫理及び行動規範等を含め、関係法令又は本学院の諸規程が定めるルールを遵守し、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。

（適用範囲及び適用対象者）

第３条　この規程及び、この規程に基づき定める細則、内規又はこれに準ずる文書の適用範囲は、本学院が所有・管理するすべての情報並びに機器（一時的にネットワークに接続されたものを含む）又ネットワークとする。

２　適用対象者は、本学院の情報システムを利用する者及び運用業務に携わる者（以下「利用者等」という。）とする。

第２章　情報システムセキュリティ体制

（情報システムセキュリティ責任者）

第４条　本学院は、情報システムセキュリティの運用に責任を負う者として、情報システムセキュリティ責任者（以下「セキュリティ責任者」という。）を置く。

２　情報システムの運用及び管理にかかるセキュリティ責任者は、経営企画担当理事をもって充てる。

３　セキュリティ責任者は、この規程及び本学院の諸規程その他の定めに従い、情報システムセキュリティに係る事項の決定並びに情報システムセキュリティ上での各種問題に対する処置を行う。

４　セキュリティ責任者は、この規程及び本学院の諸規程その他の定めに従い、本学院の情報システムセキュリティの整備並びに運用を行う。

５　セキュリティ責任者は、全学の情報基盤として供される本学院の情報システムのうちセキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。この場合において、指定された情報システムを「高重要度情報システム」という。

６　セキュリティ責任者は、全学向け教育及び全学情報システムを担当する部局担当者向け教育を統括・実施する。この場合において、セキュリティ責任者は、当該教育の実施にかかる権限を局長等に委譲することができる。

７　セキュリティ責任者は、本学院の情報システムに関する連絡及び通報において本学院の情報セキュリティを代表する。

８　セキュリティ責任者に事故があるときは、セキュリティ責任者があらかじめ指名する者が、その職務を代行する。

９　セキュリティ責任者は、情報システムセキュリティに関する専門的な知識及び経験を有した専門家をアドバイザーとして置くことができる。

（情報セキュリティ統括者）

第５条　本学院に、情報セキュリティ統括者（以下「統括者」という。）を置く。

２　統括者は、学術研究担当副学長をもって充てる。

３　統括者は、セキュリティ責任者を補佐し、その責任と権限の範囲において情報システムセキュリティ対策に関して適切な措置を講じるものとする。

（情報システム運用管理者）

第５条の２　本学院は、情報システムの運用管理に責任を負う者として、情報システム運用管理者（以下「システム運用管理者」という。）を置く。

２　システム運用管理者は、当該システムを運用する部署の所属長、又は研究室の場合は担当教員をもって充てる。

３　システム運用管理者は、本学院の諸規程その他の定めに従い、当該情報システムの整備及び運用の管理を行う。

４　システム運用管理者は、当該情報システムを優れた秩序と安全性をもって安定的かつ効率的に運用するために必要な管理及び処置を行わなければならない。

５　前項の管理及び処置を実施するにあたっては、第11条第2項第6号に定める基本基準を踏まえなければならない。

（情報システム委員会及び情報システムセキュリティワーキンググループ）
第６条　本学院の情報システムにかかるセキュリティの適正な管理、運用のため、情報システム委員会（以下「委員会」という。）を設ける。
２　委員会の運営等に必要な事項は別に定める。
３　委員会は、必要に応じて情報システムセキュリティに関する個別事項を検討する情報システムセキュリティワーキンググループ（以下「ワーキンググループ」という。）を置くことができる。
４　ワーキンググループは、情報システムの運用及び管理に関して、次の各号に掲げる委員会委員長からの諮問事項について検討し、情報システム委員会に答申する。
（１）規程及び全学向け教育の実施ガイドラインの改廃
（２）情報システムセキュリティの運用・利用及び教育に係る規程及び手順の制定並びに改廃
（３）情報システムセキュリティの運用・利用に関する教育の年度講習計画の制定及び改廃、並びにその計画の実施状況の把握
（４）情報システムセキュリティ運用リスク管理の検討及び実施
（５）情報システムセキュリティ監査対策の検討及び実施
（６）情報システムセキュリティ非常時行動計画の策定及び実施
（７）インシデントの再発防止策の検討及び実施
（８）その他委員会委員長からの諮問事項
（情報システムセキュリティ監査責任者）
第７条　本学院に情報システムセキュリティ監査責任者（以下「監査責任者」という。）を置く。
２　監査責任者は、監査室長をもって充てる。
３　監査責任者は、セキュリティ責任者の指示に基づき、監査に関する事務を統括する。
４　監査責任者は、監査を実施するため、情報システムセキュリティ対策を実行する各責任者と兼務することはできない。
（情報システムセキュリティ監査）
第８条　監査責任者は、情報システムセキュリティ対策がこの規程及び本学院の諸規程に基づく手順に従って実施されていることを監査する。
２　監査の実施等に必要な事項は、別に定める。
（所管部署）
第９条　情報システムセキュリティにかかる事務は、学術情報局情報システム室が所管とする。
２　所管部署は、セキュリティ責任者の指示により、次に定める事務を行う。
（１）情報システムセキュリティに関する事務全般
（２）本学院の情報システムセキュリティの運用及び利用における実施状況の取りまとめ
（３）講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ
（４）その他、本学院の情報システムシステムセキュリティに関する連絡及び通報
（役割の分離）
第10条　情報システムセキュリティ対策の運用において、次の役割を同じ者が兼務しないものとする。
（１）承認、又は許可事案の申請者とその承認、又は許可を行う者（以下「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　前項の定めにかかわらず、教職員等は、承認権限者等が有する職務上の権限等から、当該承認権限者等が承認又は許可（以下「承認等」という。）の可否の判断を行うことが不適切と認められる場合には、当該承認権限者等の上司に承認等の申請をする。この場合において、当該承認権限者等の上司の承認等を得たときは、当該承認権限者等の承認等を得ることを要しない。
３　承認権限者等の上司は、前項の場合において承認等を与えたときは、承認権限者等に係る遵守事項に準じて、措置を講ずる。

第３章　情報システムセキュリティ運用基準

（情報システムセキュリティ運用基準）
第11条　本学院は、本学院の情報システムにおいて円滑で効果的な情報流通を図るとともに、情報システムを優れた秩序と安全性をもって安定的かつ効率的に運用するために必要な規程又はこれに準ずる文書を策定しなければならない。
２　前項の規程又はこれに準ずる文書を策定するにあたっては、次の基本基準を踏まえなければならない。
（１）情報機器等の学外又は情報システムの運用部署以外の他部署等（学部学科、研究科等の教育研

究部門を含む。以下「他部署等」という。）への持出、学内持込に関する基準

ア　本学院外又は他部署等へ重要な情報を可搬可能な媒体に入れ持ち出す場合は、持出手続を取った上で本学院外又は他部署等へ持出した情報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、窃取を防止するため、情報の持出状況について可能な限り把握し、管理しなければならない。

ウ　情報の流出を防止するため、本学院以外の組織との情報のやり取りを可能な限り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、窃取を防止するため、モバイルコンピューティング又は在宅勤務等本学院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、窃取を防止するため、私有するコンピュータ機器及び可搬媒体の持込について可能な限り把握し、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の学内ネットワークへの接続状況を可能な限り把握し、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本学院内のコンピュータへ利用、インストールすることを可能な限り把握し、管理しなければならない。

（２）情報の収集、利用、管理に関する基準

ア　収集した情報の流出、誤用を防ぐため、情報の収集を行う際は、情報の利用目的を明確にした上で、収集について管理しなければならない。

イ　可搬可能な装置及び電子記録媒体に記録されている情報の漏洩、改ざん、破壊を防止するため、可搬可能な装置及び電子記録媒体に記録された情報の利用、保管、破棄について管理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。

（３）啓発、教育に関する基準

ア　本学院の関係者の情報保護への認識不足から情報が漏洩、改ざん、破壊されることを防止するため、本学院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。

イ　本学院内外での本学院関係者によるインターネット使用での情報流出による本学院のブランド及びイメージの低下を防ぐため、個人並びに本学院でのインターネット使用に関わる本学院関係者への教育を実施し、インターネットリテラシーの向上を図らなければならない。

ウ　学内システムの利用の習熟を図り、誤操作、機器の取り扱いの不備でシステムに重大な損害を与えることを防ぐため、学内システム利用に関する教育を実施しなければならない。

（４）コンプライアンスに関する基準

ア　本学院の関係者は、情報保護に関する法令及び本学院の諸規程に確実に準拠しなければならない。

（５）学内システムに関する基準

ア　新規に開発又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、必要なセキュリティ要件を明確にし、その要件を確実に情報システムに反映しなければならない。

イ　情報システムの信頼性及び完全性、可用性を確保するため、運用手順及び障害対応手順等の運用手続きに関する実施手順書を作成し、それに準拠した運用を実施しなければならない。

ウ　コンピュータウィルス及び悪意ある第三者の攻撃により情報システムで取扱う情報の完全性並びに及びシステムの可用性を損なうことを防止するため、コンピュータウィルスへの感染や、悪意ある第三者の攻撃を予防しなければならない。また、コンピュータウィルスに感染した場合又は悪意ある第三者からの攻撃を受けた場合、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。

エ　学外からネットワーク経由で学内システムに接続する場合、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。

（６）アクセスコントロールに関する基準

ア　情報及び情報の設置場所には、その情報の盗難並びに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。

イ　情報へのアクセスコントロールについては、本学院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た上で、情報へのアクセスの権限を付与しなければならない。

ウ　情報へのアクセス権限の付与を確実に行うため、管理者の登録及び管理者への権限の付与を行わなくてはならない。システムを管理するための権限等、広範囲に及ぶ権限を保有する管理者については、厳格な管理を実施しなければならない。

エ　情報へアクセスする権限のない者による成りすましでの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。

オ　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実施しなければならない。

カ　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ごと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。

（７）情報セキュリティ確保のための自主点検に関する基準

ア　情報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、情報を所管する責を負うものは、定期的に自主点検を実施しなければならない。

（８）危機管理に関する基準

ア　情報セキュリティ危機管理体制

①　情報セキュリティに関わるリスクは可能な限り、軽減、回避を行うとともに、万が一リスクが発現してしまった場合、上智学院危機管理規程に基づき緊急対策本部を設置する。

ア　情報セキュリティ危機管理計画（以下「危機管理計画」という。）

②　セキュリティ責任者は情報の重要度から、セキュリティ事故対策における優先順位及び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。

③　セキュリティ責任者はセキュリティ事故対策における優先順位及び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。

④　セキュリティ責任者は対策及び復旧優先順位に沿って、セキュリティ事故における対応計画並びに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。

ア　危機管理計画の教育、訓練

⑤　セキュリティ責任者は、危機管理計画を効率的かつ有効に機能させるため、定期的に当該計画に基づく訓練を実施しなければならない。

ア　危機管理計画の定期的な見直し

⑥　セキュリティ責任者は、危機管理計画を有効に機能させるため、定期的に見直さなければならない。

（９）例外に関する基準

ア　本学院が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、関係する情報を所管する責を負う者が、情報システム委員会へ報告しなければならない。

イ　この章に記載のない例外的な事項が発生する場合、当該例外事項の取り扱いは、情報システム委員会において協議の上、この規程、本学院の諸規程又は関係法令に拠るものとする。

３　情報システム委員会は、個人情報保護法、不正アクセス防止法その他の関連法令に則ったリスクアセスメントの結果及び前項の基準に基づき、情報保護のため、リスクの大きさや特徴に対して、リスクの許容、リスクの低減、リスクの移転、リスクの回避等の管理方法及び対策を検討する。

第４章　情報の取扱い

（情報の取扱いに関するマニュアル）

第12条　本学院において、情報システムで取扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、並びに書面については機密性の観点から、当該情報の取扱制限の指定、又明示等の各種遵守事項を整備し、情報セキュリティ事故発生を未然に防ぐ防止対策として、保有する情

報の取扱いに関するマニュアルを別に定める。

第５章　情報漏洩時の対応

（情報漏洩時対応マニュアル）

第13条　本学院は、事故が発生した場合の被害を最小限とするため、危機対応として別に情報漏洩時対応マニュアルを定める。

第６章　雑則

（見直し）

第14条　情報システム室は、所管する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。

２　本学院の情報システムセキュリティを運用・管理する者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行う。

（規程の改廃）

第15条　この規程の改廃は、本学院の定める手続きにより行う。

附 則

この規程は、2018年11 月1日から施行する。

この規程は、2019年（令和元年）10月1日から改正、施行する。