上智学院情報システムセキュリティ対策に関する細則

制定　2019年４月１日
改定　2019年10月1日

（趣旨）
第１条　この細則は、上智学院情報システムセキュリティ規程第11条に基づき、上智学院（中学・高等学校を除く。以下「本学院」という）において、本学院の教職員が情報システムを利用するにあたり情報システムセキュリティ対策を実施するために必要な事項を定め、もって本学院の情報システムにおける円滑で効果的な情報流通、及び優れた秩序と安全性のもと、情報システムの安定的かつ効率的な運用を図ることを目的とする。
（適用範囲）
第２条　この細則の適用対象者は、本学院の全教職員とする。
２　この細則は、本学院が所有・管理するすべての情報及び機器（一時的にネットワークに接続されたものを含む。以下同じ）又はネットワークに適用されるものとする。
３　前項の情報には、「重要情報」が含まれるものとし、その意義は次のとおりとする。
（１）本学院独自の情報であり、その漏えいにより、本学院の社会的信用を損なうとともに、業務や研究活動に支障を来たす情報で、次に掲げるものを含むがこれに限らない。
ア　経営等にかかる内部情報
イ　入学試験、定期試験等にかかる情報
ウ　出願又は公開前の本学院独自の研究に基づく発明、ノウハウその他の研究成果にかかる情報
エ　学会又は論文発表前の本学院独自の研究内容にかかる情報
（２）本学院独自でない情報又は個人情報で、その漏えいにより、法令違反又は第三者との契約違反が生じ、本学院の社会的信用を損なうとともに、第三者との信頼関係を毀損する情報で、次に掲げるものを含むがこれに限らない。
ア　教職員及び学生の個人情報並びにプライバシーにかかる情報
イ　契約に基づき、機密として開示された情報
ウ　共同研究、受託研究等において、機密として提供を受けた情報
エ　出願又は公開前の共同研究、受託研究に基づく発明、ノウハウその他の研究成果にかかる情報
オ　学会又は論文発表前の共同研究の内容にかかる情報
４　第1項の適用対象者が個人的に所有・管理する機器を利用した場合であっても、業務及び教育研究活動を目的として使用するとき、又は本学院が所有・管理するネットワークに接続して使用するときには、この細則が適用されるものとする。
（具体的な情報システムセキュリティ対策）
第３条　本学院の教職員は、前条の適用対象となる情報を利用又は機器を使用するにあたって、次の各号に掲げるセキュリティ対策を実施しなくてはならない。
（１）ソフトウェア（OS・Officeアプリケーション等）の脆弱性対策
Webブラウザや電子メールソフト、OS、Officeアプリケーション等のソフトウェアには、マルウェアへの感染、パソコンへ侵入を防止するため、脆弱性対策として次の措置を講じなくてはならない。
ア　OSや各種ソフトウェアのアップデートを定期的に実行すること。
イ　サポートが終了しているOS・ソフトウェアは、やむを得ない事情のない限り使用しないこと。
ウ　パソコン等に標準でファイアウォールの機能が実装されている場合には、適切な設定をすること。
（２）パソコン等におけるウイルスを含むマルウェア（以下「マルウェア」という。）対策
マルウェア感染による情報漏洩防止のため、パソコン等のマルウェア対策として次の措置を講じなくてはならない。
ア　マルウェア対策ソフトを導入すること。
イ　マルウェア対策ソフトの定義ファイル（パターンファイル）を常に最新に自動更新すること。
ウ　ウイルススキャンを定期的に実行すること。
エ　マルウェア感染による、学内外の被害事例を確認するよう努めること。
オ　記憶媒体の利用に際しては、フォルダ、ファイル等を開く前にマルウェアチェックを実行すること。
（３）無線LANのセキュリティ対策
通信内容が盗聴されないよう、無線LANを利用する際には、セキュリティ対策として、次の措置を講じなくてはならない。
ア　本学院内においては、やむを得ない事情のない限り、本学院の提供するWi-Fiを利用すること。

イ　パスワード等の入力を必要としないもの、又は共通のパスワードで利用できる無線LANは、やむを得ない事情のない限り、本学院の業務及び教育研究活動では利用しないこと。
ウ　利用者自身が購入した無線LANルータを設置する場合は、WPA2-AES等の強固な暗号化やMACアドレスによる接続制限等の設定を施すこと。
エ　無線LANルータを識別するための名前(SSID)において、使用名、組織名等が推測されやすい情報は使わないこと。
オ　その他、無線LANルータのセキュリティ機能を活用し、第三者に悪用されないため可能な限りの措置を施すこと。

（4）ファイル共有の安全に関する対策

業務又は教育研究活動上の必要性から、ファイルを共有する必要がある場合は、次の措置を講じなくてはならない。

ア　ファイルサーバ等を利用する場合は、アクセス権を適正に設定して使用すること。
イ　クラウドサービスを利用する必要がある場合は、本学院が提供するOffice365のOneDriveを使用するよう努めること。
ウ　やむをえず外部サービスを使用する場合は、セキュリティ対策に信頼性のある（契約約款等が存在する等）サービスを利用すること。

（5）パスワード管理

パスワードの作成及び管理にあたっては、次の措置を講じなくてはならない。

ア　名前、生年月日等、第三者が容易に類推できる個人情報を用いないこと。
イ　英数字を含む8文字以上とし、大文字・小文字・数字・記号を組み合わせるよう努めること。
ウ　パスワードは、第三者が簡単に見られるような場所にメモ等を置かないこと。
エ　いかなる理由があっても第三者に開示しないこと。
オ　複数のサービスで同じパスワードを使い回さないこと。
カ　必要に応じて、多段階認証（ID・パスワードの他にセキュリティコードを入力）等の仕組みを利用すること。

（6）共有機器を使用する場合の重要情報へのアクセス管理

共有機器を使用する場合には、第三者がネットワークを介して接続された共有機器に保存した情報を閲覧等したり、共有機器が不正利用されたりしないよう、次の措置を講じなくてはならない。

ア　アクセス権限を必要最少人数に限定すること。
イ　同じID・パスワード等を共有しないこと。
ウ　初期パスワード及び初期設定のまま使用しないこと。

（7）標的型攻撃メールへの対策

標的型攻撃メール（攻撃対象の組織から重要な情報を盗む等を目的として、業務に関係する電子メールだと信じこませてしまうように巧妙に作り込まれたマルウェア付きの電子メール）からの被害を防止するため、次の対応を心がけなければならない。

ア　電子メールに添付されたファイルを不用意に開封しないこと。
イ　電子メール中に記載されたURLを不用意にクリックしないこと。

（8）電子メールの誤送信対策

電子メールの誤送信を防止するため、次の措置を講じなくてはならない。

ア　送信する前に宛先を慎重に確認（複数回確認する等）すること。
イ　「To」、「Cc」又は「Bcc」の使い分けが適切か慎重に確認（複数回確認する等）すること。
ウ　複数の宛先に電子メールを頻繁に一斉送信する場合には、本学院が用意するML（メーリングリスト）を使用すること、及び、メーリングリストを使用しない場合は、宛先（「To」）を自分のアドレスにし、送り先のアドレスは「Bcc」に記載して送ること。また、送信前に必要に応じて複数人で設定が正しいか確認すること。
エ　必要に応じて、電子メールソフト（Outlook等）の機能でメール送信前に確認を促す「確認ダイアログ」を利用すること。

（9）電子メールからの情報漏洩対策

電子メールの誤送信等による情報の漏洩を防止するため、重要な情報については、次の措置を講じなくてはならない。

ア　ソフィアメールのアカウントを持つ者は、OneDriveの機能を使用し、公開範囲を厳密に設定した上で、リンクのみを先方に送信する等の手法を用いること。
イ　やむを得ない事情のない限り、添付ファイルは使用せず、セキュリティ対策に信頼性のあるファイル転送・共有サービスを利用すること。
ウ　ファイルを電子メールに添付する場合は、パスワードを使用してファイルを暗号化してから送信すること。

エ　暗号化に使用したパスワードは、ファイルを添付した電子メールに記載せず、電話等の別の手段を用いるか、又は別メールに記載して伝えること。

(10) インターネット（SNS等）でのトラブル回避対策

SNS等の利用により、トラブルが発生しないよう、次の措置を講じなくてはならない。本号の定めは、この細則の適用対象となる情報を利用又は機器を使用していない場合にも、準用する。

ア　SNS等の利用規約を遵守する等、常識的かつ適切なマナーを守ること。

イ　誹謗中傷その他第三者の権利を侵害するもの、違法な情報、公共の安全や秩序に対する危険を生じさせるおそれのある情報、有害な情報等、不適切な内容を書き込まないこと。

ウ　不用意に自身の個人情報を書き込まないこと。

エ　本学院の名誉を損なうような書き込みをしないこと。

オ　アカウント情報(IDやパスワード等)の適切な管理を行うこと。

(11) 重要情報のバックアップ対策

パソコン及び記憶媒体等の故障、誤操作、マルウェア感染等による情報（データ）の消失を防止するため、利用者は重要情報をファイルサーバ、外付けハードディスク、クラウドサービス等に定期的にバックアップを実行すること。

(12) 重要機器の管理

重要情報がパソコン（タブレット等を含む）に記録されている場合には、当該パソコンの盗難、及び記録されている情報の漏洩を防止するため、次の措置を講じなくてはならない。

ア　業務又は教育研究活動の終了後は、パソコン等を施錠された環境で保管すること。

イ　可能であれば、パソコンや記憶媒体は暗号化を施して使用すること。

(13) 重要情報の物理的管理

パソコン（タブレット等を含む）の画面に表示される情報を第三者が閲覧できないようにする等、重要情報の物理的管理のため、次の措置を講じなくてはならない。

ア　パソコン（タブレット等）、記憶媒体（USB等）及び重要情報の記載がある書類等を自席、教室等に放置しないこと。

イ　離席時にはパソコン等に画面ロック等をかけること。

ウ　重要情報が記載されたドキュメントは、施錠できるキャビネットに保管する等、第三者の目に触れないよう管理すること。

(14) 重要情報の持ち出し管理

情報漏洩を防止するため、重要情報の持ち出し管理として、次の事項を遵守しなければならない。

ア　重要情報の持ち出しは原則禁止とする。

イ　パソコン（タブレット　等）、記憶媒体（USB等）及び重要情報の記載がある書類等からは絶対に目を離さず、網棚等に置かない等、紛失したり、盗難にあったりしないように取り扱いに注意すること。

ウ　重要情報を持ち出すにあたっては、読み込みにパスワードの入力を必要とする暗号化対応のUSBメモリ等を使用すること。

エ　重要情報は第三者の立ち入りが制限された場所で取り扱い、公共の場等、不特定多数の第三者の目に触れる場所で取り扱わないこと。

オ　離席時には部屋の施錠、パソコンのロック等の対策を実施し、第三者による重要情報のアクセスを防止すること。

カ　必要に応じて、本学院が承認するクラウドサービスの利用により物理的な持ち出しを回避すること。この場合において、ソフィアメールのアカウントを持つ者には、Office365で提供されているOneDriveを推奨する。

キ　パソコンやUSBメモリ等に、過去に持ち出した重要情報が入っていないか定期的に確認し、不要となった情報は廃棄又は消去すること。

(15) 不要になったパソコン等の廃棄に関する手続き

研究等で使用するサーバ等を廃棄する場合には、盗難や情報の盗み取り、直接サーバを操作されるリスクを防止するため、次のいずれかの措置を講じなくてはならない。

ア　データ消去用のソフトウェアを利用し、又はデータ消去の専門業者に依頼し、データを消去すること。

イ　パソコン等に搭載されているハードディスク等を取り外し、物理的に破壊すること。

ウ　個人データが記録された媒体(CD－ROMや書類等)を廃棄するときは、シュレッダー等で物理的に破壊すること。

(16) ソフトウェア等の適正な管理

ソフトウェア等の著作物保護のため、次の処置を講じなくてはならない。

ア　ソフトウェアライセンスの内容（使用権等）を確認した上で利用すること。

イ　ソフトウェアを著作権者の許可なく複製等しないこと。
ウ　ソフトウェアをダウンロードをするにあたっては、正規サイトから購入等するものとし、正規品かどうか疑わしいソフトウェアのダウンロードは回避すること。
エ　契約したソフトウェアの約款のとおりに適切に使用すること。

(17) サーバ室の管理

教育研究活動のためにサーバ等を設置する場合には、盗難や情報の盗み取り、直接サーバを操作されるリスクに対応するため、サーバ室の管理として次の措置を講じなくてはならない。

ア　サーバ等を設置する部屋は施錠管理を行うこと。
イ　サーバ等を設置する部屋の入退室を入退室管理票等で管理すること。

(18) 情報セキュリティ教育の受講

被害を未然に防ぐための対策を講じるため、講習会等、定期的に本学が実施する情報セキュリティ教育を受講しなくてはならない。

（所管部署）

第４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する。

（見直し）

第５条　情報システム室は、情報セキュリティ対策の内容を適時検討し、必要があると認めた場合には、総務グループのほか、関係部局と協議の上その見直しを行う。

（改廃）

第６条　この細則の改廃は、本学院の定める手続きにより行う。

附　則

この細則は2019年（平成31年）４月１日から施行する。
この細則は2019年（令和元年）10月1日から改正、施行する。