公立大学法人京都市立芸術大学情報セキュリティガイドライン

1　趣旨

公立大学法人京都市立芸術大学情報セキュリティガイドライン（以下「本ガイドライン」という。）は，公立大学法人京都市立芸術大学情報セキュリティポリシー（以下「ポリシー」という。）に基づいて公立大学法人京都市立芸術大学（以下「法人」という。）が保有する情報資産の適正かつ安全な管理のために，教職員・学生ならびに関係者が具体的に実施すべき事項をまとめたものである。

2　情報の分類と管理

サーバに保存された情報は，職務上定められた責任者が管理する。個人的に管理されたパソコンなどの内部に保存された情報に関しては，それを管理する者が管理しなければならない。また，どの範囲で情報共有するか，非公開情報の情報開示にはどのような加工をするかを明確にしておく必要がある。

⑴　情報の分類と管理

情報は，重要度に応じて適正に分類し，管理されなければならない。また，それぞれの情報について，公開・非公開や公開する範囲を定めなければならない。本ガイドラインでは，情報を以下のように分類する。

①　非公開情報

非公開情報は，重要度が高く，かつ漏洩した場合著しく法人の信用や利益を損なう情報をいい，以下のように管理する。

ア　業務上必要な者以外が閲覧，改変できないように制限をしなければならない。

イ　業務上必要として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。また，一時的であっても，教職員が日常的に使用するコンピュータに非公開情報を不特定の者が可読な状態で複製してはならない。

ウ　非公開情報を扱うネットワークは，学術研究・教育用の一般ネットワークと論理的に異なるべきである。できれば，物理的に異なる回線を利用することが望ましい。さらに，暗号化や，盗聴防止策を講じることが望ましい。

エ　一般ネットワークと非公開情報ネットワークの間でアクセスする必要がある場合は，非公開ネットワークからのみアクセス可能としなければならない。さらに，両ネットワークの接続点を必要最小限とすべきで，できれば必要なときのみ通信を可能とすることが望ましい。

オ　物理的な盗難等を防止するため，利用を許可された場所から外部に非公開情報を持ち出してはならない。同様に，盗聴防止のため，インターネット等の公衆回線を介して不特定の者が傍受可能な方式で非公開情報にアクセスすることも原則禁止する。

カ　外注などのため，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。

キ　必要に応じて，管理に関する実施手順を定めるものとする。

②　限定公開情報

限定公開情報は，限定された者だけに公開する情報をいい，以下のように管理する。

ア　許可された者以外が閲覧，改変できないように制限をしなければならない。

イ　許可された者以外の情報の扱いは，非公開情報と同じものとする。

ウ　必要に応じて，管理に関する実施手順を定めるものとする。

③　公開情報

公開情報は，不特定多数の者に公開してもよい情報いい，以下のように管理する。

ア　公開情報は任意の場所からアクセス可能な性質を持つため，情報の改ざんや偽情報の流布に対し，防止策を講じなければならない。

イ　必要に応じて，管理に関する実施手順を定めるものとする。

④　発信情報

発信情報は，大学側から外部の者に発信する情報をいい，以下のように管理する。

ア　発信情報は公開情報と同じく，防止策を講じるだけでなく，正規の発信情報であることを証明する必要がある。

イ　必要に応じて，管理に関する実施手順を定めるものとする。

⑤　受信情報

受信情報は，大学側で受信する外部の者からの情報をいい，以下のように管理する。

ア　必要に応じて，制限を加えるものとする。

イ　必要に応じて，管理に関する実施手順を定めるものとする。

⑵　情報の公開化

非公開情報を公開化する場合には，個人情報の漏洩，プライバシーや著作権の侵害に十分注意し，公開できる情報だけを抽出する，あるいは，統計処理などの加工を行う必要がある。

⑶　情報の限定公開

特定の利用者に特定の情報を開示する必要がある場合は，情報の登録および閲覧について許可された者が許可された操作だけを行えるように，認証およびアクセス制御機能を設けなければならない。さらに，異常な登録や閲覧が行われていないか，定期的に状況を確認しなければならない。

⑷　情報改ざんおよび偽情報流布の防止

法人が管理し掌握する非公開情報および公開情報の原本は，書き換え不能な記憶媒体に保存するなどにより原本性を保証しなければならない。また，それぞれの情報ご

とにシステム管理責任者を設けなければならない。保存については，その利用形態に合わせて定めなければならない。

公開情報は改ざんへの対策を講じるとともに改ざんを受けた場合の速やかな回復機構も備えなければならない。さらに，公開情報（Web での掲示情報やメールマガジンによる情報発信を含む）の複製・加筆による偽情報の作成および流布を防止するため，電子署名の導入など原本性の維持に努める必要がある。

⑸　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修理または破棄する場合は，第三者に利用されることのないよう適切な措置を施さなければならない。

さらに，情報機器の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定めなければならない。業者に委託する場合は，守秘義務とともに処理方法も契約に入れなければならない。

3　物理的セキュリティ

⑴　クライアント機器

①　クライアント機器の定義

クライアント機器とは，主として個人的な利用で用いられ，他の情報機器へアクセスすることで処理を進めていくものを指す。後で示すサーバ機器に対するものであり，情報セキュリティ管理者は対象となるクライアント機器を把握しなければならない。

②　クライアント機器の使用

クライアント機器の使用に当たっては，以下の点を考慮しなければならない。

ア　クライアント機器を設置する場合（据付および一時的設置のいずれにおいても），利用者がクライアント機器を使用する前に物理的認証または電子的認証，あるいは，両方を経るべきである。

イ　電子的認証を用いる場合，ディスクブート等による電子的認証すり抜けに対する対策を施さなければならない。

③　据付型クライアント機器の盗難対策

据付型クライアント機器が犯罪者によって外部に持ち出されないよう，何らかの対策を施さなければならない。

④　ネットワークへの接続

ア　有線（ネットワークケーブル）を使用する場合には，過失によるケーブル切断を防ぐための措置を施すべきである。

イ　有線，無線どちらの場合においても，ネットワークの盗聴に対する対策を施すべきである。

ウ　クライアント機器接続用のネットワークケーブルに違うコンピュータが接続さ

れないよう，物理アドレスと IP アドレスの対比表を定期的に検査すべきである。

⑤　可搬型クライアント機器の備品管理

クライアント機器経由による秘密または非公開情報の漏洩が発生しないよう留意しなければならない。

ア　非公開情報の入ったクライアント機器を外部に持ち出すことは，原則として禁止とする。大学構成員が持ち出す必要がある場合には，情報セキュリティ管理者の許可を得るとともに貸し出しの事実について記録しなければならない。非大学構成員が持ち出す必要がある場合には，情報セキュリティ管理者の許可を得るとともに，貸し出しの事実を記録し，守秘義務などの契約を結ぶものとする。

イ　クライアント機器の盗難または紛失防止のため，保管場所の施錠など必要な措置を講じなければならない。

⑥　持込型クライアント機器

有線，無線を問わず許可された機器以外が接続された場合には，情報セキュリティの低下を起こさないようその使用に制限を加える。

⑦　保守

保守においては，パスワードやシステム設定情報などの非公開情報の開示について守秘義務契約を結ぶものとする。

⑵　サーバ機器

①　サーバ機器の定義

サーバ機器とは，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。その停止は多くの利用者に影響を与えるため，セキュリティを守ることが肝要である。

②　管理区域の設置

機器の設置に当たっては，以下の点を考慮しなければならない。

ア　サーバ機器は設定された管理区域に設置されなければならない。コンソールも同様である。

イ　管理区域内はサーバ機器の動作補償範囲内の温度，湿度を 24 時間保つべきである。

ウ　管理区域の物理的隔離の度合いは守るべきサーバの重要性に応じて段階的に設定されるべきである。重要なサーバとは，停止したときに法人内の業務遂行に重大な支障をきたすサーバを指す。重要なサーバ機器に対しては物理的に区切られており，第三者の認証と入退室の記録が残される区域を設定すべきである。一方で重要度の軽微なサーバ機器については，鍵などによる認証による入退室管理形態であっても良い。

③　電源

電源を供給する際には，電圧の流動や突発的な停電，過電流に対応する装置を経

由することが望ましい。

④　ネットワークへの接続

ア　有線（ネットワークケーブル）を使用する場合には，過失によるケーブル切断を防ぐための措置を施すべきである。

イ　有線，無線どちらの場合においても，ネットワークの盗聴に対する対策を施すべきである。

⑤　データのバックアップ

サーバ機器に記録されるデータは，定期的にバックアップをとるものとする。

ア　バックアップスケジュールは，サーバ機器の重要度に応じて決定する。

イ　データをバックアップしたメディアは，温度と湿度が適切な場所に保管すべきである。また重要なデータについては，バックアップを複数本作成し，物理的に離れた場所に個々に保管することが望ましい。

ウ　データをバックアップしたメディアは，認証による入退室管理が行われている管理区域内に保管するべきである。

⑥　多重化

ダウンタイムを短くすることを求められるサーバ機器については，多重化を検討すべきである。多重化した場合には，順番に運用機を切り替えるか，一定時間ごとにチェックするなどして，スタンバイ機が故障してないことを確かめる必要がある。

⑦　サーバ機器盗難への対策

サーバ機器が管理区域から持ち出されないよう何らかの対策を施さなければならない。

⑧　災害への対策

災害への対策がとられなければならない。

ア　重要なサーバ機器は，耐震を考慮した据付を行う。

イ　管理区域には，火災の一次消火手段が提供されるべきである。

⑨　保守

ア　保守においては保守部品をできるだけ確保し，迅速に保守を行える体制を整えるべきである。

イ　保守においては，パスワードやシステム設定情報などの非公開情報の開示についての守秘義務契約を結ばなければならない。

⑶　ネットワーク機器

①　コンソールポートの隔離

ルータ，インテリジェントスイッチは，コンソールポート，管理ポートが許可された特定のシステム管理担当者以外は使用できないように施錠などによって物理的に隔離された区域に設置すべきである。

②　設置場所の秘匿

バックボーンを構成する機器をはじめ，重要と思われるネットワーク機器については，その設置場所を限られたシステム管理者以外に公開すべきではない。

③　ネットワーク接続ポート

ア　有線，無線にかかわらず，不特定の者が接続する可能性がある場所の接続ポートを開放する場合には，そのネットワークセグメントから法人内へのアクセスを制限する。

イ　原則として，物理的認証または電子的認証，あるいは，両方を経た後でなければ，ネットワーク接続ポートにコンピュータを接続してはならない。

ウ　学会等のために期限を設定して来訪者に接続ポートを開放する場合には，そのネットワークセグメントから法人内へのアクセスは制限する。

④　ネットワークケーブル

ア　バックボーンを構成するネットワークケーブルは，故意または過失によるケーブル切断を防ぐためにシールド等の措置を施さなければならない。他に重要と思われるネットワークケーブルについても同様にケーブル切断のための措置を講ずるべきである。

イ　有線，無線どちらの場合においても，ネットワークの盗聴に対する対策を施すべきである。

⑤　多重化

機器の障害によるネットワーク断が重大な影響を及ぼすようなネットワーク機器については，多重化による信頼性の向上を検討する。

⑥　保守

ア　保守においては保守部品をできるだけ確保し，迅速に保守を行える体制を整えるべきである。

イ　保守においてはパスワードやネットワーク構成などの非公開情報の開示についての守秘義務契約を結ぶべきである。

4　人的セキュリティ

⑴　役割・責任および免責事項

①　利用者

ア　すべての利用者は，ポリシーを遵守しなければならない。学生も情報システム利用者の一員として，情報セキュリティを維持する義務を有する。

イ　ポリシーおよび本ガイドライン等を遵守して，利用しなければならない。

ウ　情報システム管理者からセキュリティ維持管理のために協力を依頼された場合には従わねばならない。

⑵　教育研究上の利便性の配慮

①　情報セキュリティ対策について教育研究上の利便性を著しく損なう点，遵守する

ことが現実的に困難な点については，情報セキュリティ管理者に対して，ポリシーおよびガイドライン等の改善を求めることができる。

② 教職員および学生は，情報システム管理者の許可を得ずに情報端末等を執務室，研究室および教室外に持ち出してはならない。ただし，モバイル端末は，教育研究上の利便性を考慮し，その利用者の管理責任において，これを持ち出せるよう配慮できる。

③ 教職員および学生以外の者（来訪者）に法人の情報システム（公共情報端末や情報コンセントを含む）を一時的に使用させる場合においては，その利用者が守るべきポリシーを定め，これを厳守させるよう適切な措置を施さなければならない。

⑶ 事故・障害の報告

① 教職員および学生は，情報セキュリティに関する事故，情報システムの不審な動作，公開情報の改ざん，システム上の障害および誤動作を発見した場合には，情報セキュリティ管理者に直ちに報告しなければならない。

② 情報セキュリティ管理者は，発生したすべての情報セキュリティ上の事故等に関する記録を一定期間保存し，情報セキュリティ責任者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。

③ 一般利用者に対する情報セキュリティ上の事故・障害の通知は，問題の程度に応じた適切な表現に配慮し，速やかに行わなければなければならない。

④ 法人内からの不正アクセスによって外部に被害を及ぼし，その事実関係の説明を被害者または第三者から求められた場合の対応手順を，必要に応じ定めるものとする。

⑤ コンピュータウイルスの感染および不正アクセスが発見された場合について，被害の拡大と再発防止の目的のため，独立行政法人情報処理推進機構（IPA）セキュリティセンターに速やかに届け出ることが定められている。さらに，必要に応じて警察のネットワーク犯罪担当部署に相談などを行うこと。

⑷ パスワード管理・ログ管理

① 一般利用者

ア 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。

イ 他の利用者のアカウントを使用してはならない。

ウ いかなる場合も他の利用者のパスワードを聞き出してはならない。

エ 情報システム管理者が，パスワードが不適切のため変更を求めた場合，利用者はその指示に従わなければならない。

オ システムの管理権限を有する者や他の利用者になりすました第三者からのパスワードの聞き取りには，如何なる場合も応じてはならない。

② 情報システム管理者

ア　情報システムの利用資格者の規定を定めなければならない。

イ　規定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は，直ちに除されなければならない。

ウ　利用者のアカウントを管理権限のない第三者に漏洩してはならない。また，いかなる場合にも利用者からパスワードを聞き取りしてはならない。

エ　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。

⑸　教職員・学生以外の利用者

①　教務および事務系業務

非常勤教員および臨時職員（外部委託事業者を含む）には，雇用契約の際に，守るべきポリシーの内容を理解させ，実施および遵守させなければならない。

②　情報システムの開発および保守ならびに管理業務

ア　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外部委託事業者に発注する場合は，外部委託事業者から下請けとして受託する業者を含めて，ポリシーのうち外部委託事業者が守るべき内容の遵守を明記した契約を行わなければならない。

イ　外部委託事業者との契約書には，責任所在の境界，ならびに，ポリシーが遵守されなかった場合の規定を定めなければならない。

5　技術的セキュリティ

⑴　基本方針

外部からの脅威だけでなく内部からの脅威にも対処でき，かつ外部に害を与えないネットワーク設計と運用が必要である。技術的には，不適切な通信を検知し，遮断する機能の採用が最低限必要である。

⑵　ネットワーク運営方針

①　ネットワーク設計，機器導入および設定

ア　ネットワーク設計および改変

・　新たなネットワークの設計・構築にあたっては，事務，教務，教育，研究といった目的の異なるネットワークトラフィックを物理的または論理的に混在させないことが重要である。

・　情報セキュリティ管理者の許可を得ないネットワークの改変を禁じる。

イ　ネットワーク機器

・　ルータやソフトウェア設定可能なハブ等の機器を管理する情報システム管理者は，機器障害や権限のないアクセスによって機器の構成や制御機能が損なわれないように管理しなければならない。また，これらの機能を常に最新のもの

とするように努めなければならない。

ウ　セキュリティ機器およびその運用

・　情報システム管理者は，ファイアウォールおよび侵入検知システムその他の必要と思われるセキュリティ機器を導入・運用し，外部からの脅威や内部から外部への攻撃に対処できるようにすべきである。さらに，これらの機器をネットワーク性能の向上や，新たな脅威の出現に対応可能なように，最新のものにすることが重要である。

・　法人のネットワークを利用しようとするものは，ネットワーク侵入検知システムその他によるトラフィックの検査を受け入れなければならない。

② ネットワークサービス選択

ア　情報セキュリティ管理者は，構成員に対して，利用可能なネットワークサービスと利用形態を決定し，構成員に公表する。また，外部に対して，法人のネットワーク上のどのような資源をだれに提供するかを決定する権限を持つ。

イ　構成員は，情報セキュリティ管理者のこの決定に対して，異議を申し立てることができる。

③ ネットワークの無許可利用およびネットワークバックドアの排除

ア　ネットワークに接続する装置は，不特定多数の手に触れさせてはならない。

イ　ネットワークのセキュリティ機能の管理を回避する目的でのバックドア（PPP サーバ，コンピュータに接続する公衆回線，VPN 装置およびソフトウェア等）の設置を原則禁止する。

ウ　情報セキュリティ管理者の許可を受けて，独自のハードウエア回線等を設置した場合には，情報セキュリティ管理者の求めに応じて，運用状況を報告しなければならない。

④ ネットワークの日常運用

ネットワークのバックボーンを担当する情報システム管理者は，ファイアウォールや侵入検知システムなどセキュリティ上必要と思われるシステムのログを一定期間保存しなければならない。また，サーバ機器の情報システム管理者は，情報システムへのアクセス記録を取得し一定期間保存しなければならない。定期的にそれらのログを分析し，侵入の試みや不審な法人内外へのアクセスなどがなされていないかなどをチェックすることが必要である。

⑶ 端末機器等に関する基準

① 基本方針

ネットワークに接続を許される機器について，本ポリシーに従って基準に満たないネットワークに接続してはならない。

情報セキュリティ管理者は，ガイドラインにかかわらず，常に最新のセキュリティ情報に注意を払い，端末機器を安全に運用できるように努力しなければならない。

情報システム管理者は，情報セキュリティ管理者の要請に応じて，ログ等の運用に関する情報を情報セキュリティ管理者に対して開示しなければならない。

② 端末機器設置運用基準

接続する機器は，利用者を何らかの方法で認証（部屋の入退室管理といった物理的な方法でも可）できなければならない。

一時的であるなしにかかわらず，機器を設置しようとするものは，設定作業（セキュリティ対策を含む）の完了していない装置をネットワークに接続してはならない。

機器の管理者は，設置機器の利用者を特定可能でなければならない。

附　則

本ガイドラインは平成２９年４月１日から施行する。