情報セキュリティ維持に関するガイドライン

１　趣旨

このガイドラインは、兵庫県立大学情報セキュリティポリシー（以下「ポリシー」という。）に基づき、兵庫県立大学（以下「本学」という。）の情報資産を脅威（機器障害、悪意ある行為など）から保護するための情報セキュリティ維持に関する必要な事項を定めたものである。

２　物理的セキュリティ

本学のネットワークに接続するすべてのクライアント機器、サーバ機器およびネットワーク機器に関する情報セキュリティの維持に必要な物理的対策について以下に示す。

（１）クライアント機器

ア　ネットワークへの接続

クライアント機器をネットワークへ接続する場合、以下のような物理的対策を講じなければならない。

(ア)有線を使用する場合には、悪意又は過失によるケーブル切断を防ぐための措置を施すことが望ましい。

(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ことが望ましい。

(ウ)クライアント機器接続用のネットワーク機器に、許可なく別の機器が接続されないよう対策を施さなければならない。

イ　クライアント機器の保全

クライアント機器は、許可なく学外に持ち出されないよう次のような対策を講じなければならない。

(ア)クライアント機器を室内に設置する場合には、その部屋を空けるときは施錠すること。

(イ)クライアント機器をオープンスペース等に設置する場合には、ワイヤ一等により固定すること。

ウ　クライアント機器及びリムーバブルメディア（以下「クライアント機器等」という。）の持ち出し

クライアント機器等を学外へ持ち出す際には、以下の事項を遵守しなければならない。

(ア) 大学構成員がクライアント機器等を学外へ持ち出す場合においては、部局情報セキュリティ責任者または地区システム管理責任者の承認を得るとともに、その事実について記録しなければならない。

(イ)大学構成員がクライアント機器等を学外に持ち出したときは、盗難、紛失、情報漏洩、コンピュータウイルス感染、不正アクセス等が発生しないよう十分に留意しなければならない。

(ウ)大学構成員以外の者がクライアント機器等を学外に持ち出すことは、原則として禁止する。

（２）サーバ機器

ア　管理区域の設置

サーバ機器は、以下の条件を満たす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。

(ア)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しなければならない。

(イ)重要なサーバ機器に対しては、第三者の認証と入退室の記録が残される隔離された区域を設定しなければならない。重要なサーバとは、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サーバを指す。

(ウ)重要度の軽微なサーバ機器については、施錠などによる入退室管理形態をとるものとする。

(エ)管理区域の物理的な場所は、許可された特定の者以外には公開してはならない。

イ　電源

電源を供給する際には、電圧の変動や突発的な停電、過電流に対応する装置を経由することが望ましい。

ウ　ネットワークへの接続

サーバ機器をネットワークへ接続する場合、以下のような情報セキュリティ対策を講じなければならない。

(ア)有線を使用する場合には、悪意又は過失によるケーブル切断を防ぐための措置を施すことが望ましい。

(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ことが望ましい。

エ　データのバックアップ

(ア)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しなければならない。

(イ)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されなければならない。

(ウ)データをバックアップした記憶媒体は、データの重要度に応じて、適正な環境のもとに保管されなければならない。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別個に保管することを検討しなければならない。

(エ)データをバックアップした記憶媒体は、データの重要度に応じた適正な入退室管理が行われている管理区域内に保管しなければならない。

オ　多重化

(ア)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、重要度に応じて多重化を検討しなければならない。

(イ)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いないことを確かめなければならない。

カ　サーバ機器の保全

サーバ機器のシステム管理者は、機器が管理区域から許可なく持ち出されないよう、ラックへの固定、設置場所の施錠などの対策を施さなければならない。

キ　災害への対策

(ア)重要なサーバ機器は、耐震を考慮した据付を行わなければならない。

(イ)管理区域には、火災の一次消火手段が提供されなければならない。

ク　保守

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なければならない。

（3）ネットワーク機器

ア　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しなければならない。

イ　設置場所の秘匿

基幹ネットワーク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、その設置場所を許可された特定の者以外に公開してはならない。

ウ　盗聴対策

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ことが望ましい。

エ　多重化

機器の障害によるネットワークの切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しなければならない。

オ　保守

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なければならない。

3　技術的セキュリティ

本学のネットワークおよび機器の設定、運用等に関する情報セキュリティの維持に必要な技術的対策について以下に示す。

（1）ネットワークの運用

ア　ネットワークの設計および改変

(ア)ネットワークの設計・構築にあたっては、学生情報等の事務系、教育研究系および図書情報系といった目的の異なるネットワークを論理的に混在させてはならない。

(イ)ネットワークの新設・構成変更にあたっては、情報システム部会の承認を得なければならない。

イ　セキュリティ機器およびその運用

(ア)全学情報セキュリティ管理者は、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しなければならない。

(イ)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よう努めなければならない。

(ウ)本学のネットワークを利用しようとする者は、全学情報セキュリティ管理者が設置した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。

ウ　ネットワークサービスの選択

情報システム部会は、利用者に対して、利用可能なネットワークサービスと利用形態を決定し、利用者に公表しなければならない。

（2）機器の運用

ア　アクセス制御

クライアント機器、サーバ機器およびネットワーク機器のシステム管理者は、それぞれの機器に対して以下のようなアクセス制御を行なわなければならない。

(ア)ネットワークへの機器の接続にあたっては、認証機能を持つものを利用することが望ましい。

(イ)認証機能を持つ機器については、利用者ごとにユーザIDを発行し、利用に際して認証を行なうこと。また、同じユーザIDを複数の利用者で共有しないこと。

(ウ)利用者の権限に応じアクセスできるデータや操作を限定すること。メール、Web等のみの利用者であれば､機器の構成や設定情報を取得･変更できないようにすることが望ましい。

(エ)特にサーバ機器において、利用者に提供するサービスを必要なもののみに限定し、利用者に通知すること。また、不要なサービスは起動しないこと。

(オ)無線LANのアクセスポイントを設置する場合は、想定した利用者のみにアクセスが限定できるようWPA等によるアクセス制御を行なうこと。また、適宜、物理アドレス（MACアドレス）による接続制限を実施することが望ましい。

イ　システムの更新

クライアント機器、サーバ機器およびネットワーク機器のシステム管理者は、適宜、システムを更新し、最新のものにするよう努めなければならない。

(ア)機器に情報セキュリティ上の脆弱性が発見された場合には、直ちにハードウェア・ソフトウェアの更新または設定変更などの対策を行なうこと。

(イ)その他、機器の機能・性能向上、障害対応等のためのハードウェア・ソフトウェアの更新または設定変更は、必要に応じて実施すること。

ウ　コンピュータウイルス対策

クライアント機器、サーバ機器のシステム管理者は、それぞれの機器について以下のようなコンピュータウイルス対策を行なわなければならない。

(ア)原則としてすべてのクライアント機器には、コンピュータウイルス対策ソフトを導入しなければならない。

(イ)サーバ機器については、その用途を考慮しコンピュータウイルス対策ソフトを導入するのが望ましい。

(ウ)コンピュータウイルス対策ソフトを導入した機器は、システムを起動している限

りにおいて毎日１回以上はウイルス検出パターンの更新を行なうことが望ましい。また、週１回以上はシステムの全ファイルに対してウイルススキヤンを行なうことが望ましい。

エ　機器の新規接続

クライアント機器、サーバ機器およびネットワーク機器を新たにネットワークに接続する際には、アクセス制御の設定がなされ、システムが最新の状態に更新され、ウイルス対策が施された状態であることが確認されなければならない。

オ　履歴情報の取得

サーバ機器およびネットワーク機器のシステム管理者は、それぞれの機器について、以下の履歴情報（ログ）を取得すること。また、取得した履歴情報は、１年以上保存しなければならない。

(ア)システムへの認証を伴うログイン記録

(イ)公開しているサービスを利用したクライアントのIPアドレス等

(ウ)その他システムの運用に関する記録

カ　履歴情報等の解析

システム管理者は、履歴情報および通信内容の解析等にあたって、以下の事項を遵守しなければならない。

(ア)日常的なシステム監視業務において履歴情報を利用する場合は、個別のアクセス・通信等の記録を閲覧する必要がないよう自動的に統計処理を行なうことが望ましい。

(イ)システムが正常に運用されていることを確認する場合、または不正アクセスや情報漏洩など正規外の利用が行なわれた恐れがある場合に限り、利用者のアクセスや通信を記録した履歴情報（日時、アドレス等）を閲覧することができる。

(ウ)前号の記録だけでは、不正アクセスや情報漏洩等の実態を解析できない場合に限り、利用者の通信内容等を閲覧することができる。この場合、閲覧した日時、ファイル名等を記録しておくこと。

４　人的セキュリティ

本学の情報セキュリティの維持に必要な人的な対策について以下に示す。

（１）システム管理者の遵守事項

各機器のシステム管理者は、以下の事項を遵守しなければならない。

ア　本ガイドライン２および３に示した手順に従い、適正にシステムを管理運用しなければならない。

イ　システム管理者の監督下において教職員または大学院生等にシステム管理業務を委譲する、または補助させる場合、これらの者によるシステム管理業務の責任と権限の範囲を明確に定め、これを厳守させなければならない。

ウ　情報システムの利用資格を明確に定めなければならない。

エ　利用資格を有する者以外に情報端末のユーザIDを発行してはならない。また、利用資格を失った利用者のユーザIDは、直ちに削除されなければならない。

オ　利用者のユーザID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。

カ　履歴情報および通信内容の解析等にあたっては、３．（２）.カに掲げる要件と手順に従うとともに、利用者のプライバシーに配慮し、職務上知り得た秘密を漏らしてはならない。

（２）不正アクセス・事故等への対応

ア　不正アクセス・事故等の発見

(ア)利用者は、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、不正アクセス（侵入、情報漏洩、改ざん、踏み台等）、システム上の障害および誤動作を発見した場合には、地区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。

(イ)地区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全学情報セキュリティ管理者に通知するとともに、必要な措置を直ちに講じなければならない。必要があると判断した場合、全学情報セキュリティ管理者に措置に関して指示または支援を要請しなければならない。

イ　不正アクセス・事故等の緊急措置

(ア)発生した事故等が、第三者による不正アクセスによるものである場合、全学情報セキュリティ管理者および地区システム管理責任者は、当該機器を直ちにネットワークから分離するとともに、アクセス記録の保全、適正なデータや設定の回復、原因の分析等必要な措置を行ない、また再発防止のための対策を講じなければならない。

(イ)発生した事故等が、コンピュータウイルスの感染による二次的な感染源あるいは第三者への自動攻撃等である場合、全学情報セキュリティ管理者および地区システム管理責任者は、当該機器を直ちにネットワークから分離するとともに、アクセス記録の保全、コンピュータウイルスの駆除、セキュリティホールの除去等必要な措置を行ない、また再発防止のための対策を講じなければならない。

(ウ)発生した事故等が、全学に被害が拡大する恐れのある場合には、直ちに最高情報セキュリティ責任者の判断のもと、地区全体のネットワークの接続遮断をしなければならない。

(エ)学内からの不正アクセス等によって学内外に被害を及ぼし、社会的に重大な信用問題等が発生した場合は、直ちに最高情報セキュリティ責任者の判断のもと、関連する通信を遮断し、または該当する機器を切り離すとともに、被害者や関係者への事実関係の説明、再発防止のための対策、その他必要な措置を実施しなければならない。

(オ)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らない。

(カ)全学情報セキュリティ管理者は、発生した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、情報システム部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。

(キ)地区システム管理責任者およびシステム管理者は、システムの障害、不正アクセ

ス、その他法令上、倫理上の問題等が発生した場合には、全学情報システム管理者の指示に従い、調査および事態収拾に協力しなければならない。

(ク)その他、本実施手順で定められていない状況に対しては、最高情報セキュリティ責任者が判断する。

ウ　緊急の措置からの回復

機器の切り離しからの回復は、地区情報システム部会の判断に、地区全体のネットワークの接続遮断からの回復は、全学情報システム部会の判断による。

（3）教職員・学生以外の利用

ア　学生情報等事務系業務

非常勤教職員および臨時職員（外部委託事業者を含む）には、雇用契約の際に、ポリシーの内容を理解させ、実施および遵守させるための手順を定めなければならない。

イ　情報システムの開発・保守運用

(ア)情報システムの開発・保守運用を民間事業者等に委託する場合は、このポリシーを踏まえ、当該外部委託事業者が遵守すべき事項を明記した契約を締結しなければならない。

(イ)個人情報取扱事務その他の個人情報を取り扱う事務を外部委託事業者に委託する場合は、当該外部委託事業者との契約書に、個人情報取扱特記事項（「個人情報を取り扱う事務の委託に伴う措置について（平成9年11月21日付文第294号知事公室長通知）」）を規定しなければならない。

(ウ)外部委託事業者との契約には、契約が遵守されなかった場合の損害賠償等の規定を定めなければならない。

ウ　学外利用者の機器持ち込み

教職員または学生以外の者が、クライアント機器を持ち込み、本学のネットワークに接続して利用する場合は、以下のようにしなければならない。

(ア)接続先ネットワークの地区システム管理責任者の承認を得るとともに、本学の教職員をシステム管理者として運用しなければならない。

(イ)利用者にポリシーの内容を理解させ、実施および遵守させるための適切な措置を施さなければならない。

エ　来学者等の一時利用

学会等のために期限を設定して来学者等に情報ネットワークを一時的に利用させる場合、以下のようにしなければならない。

(ア)本学教職員であるシステム管理者を定め、地区情報システム部会へ申請をした上、来学者等に開放する期間および場所を明確にすること。

(イ)利用者にポリシーの必要な事項を理解させ、遵守させるための適切な措置を施さなければならない。

(ウ)無線LANによるアクセスポイントを提供する場合は、想定した利用者のみにアクセスが限定できるよう、WPA等によるアクセス制御を行なうこと。また、適宜、物理アドレス（MACアドレス）による接続制限を実施することが望ましい。

(エ)プライベートネットワークを特設するなどして、そのネットワークセグメントか

ら学内へのアクセスは制限することが望ましい。

(オ)接続機器の物理アドレスを記録することが望ましい。

附　則

このガイドラインは平成１８年１１月２２目から施行する。