群馬県公立大学法人情報セキュリティポリシー

平成30年４月１日制定
一部改正　令和２年３月24日
一部改正　令和２年４月１日

第１章　情報セキュリティ基本方針

１　趣旨

群馬県公立大学法人（以下「法人」という。）が保有、管理する情報資産は、女子大学及び県民健康科学大学の学生に関する個人情報及び教育活動並びに学術研究に係る情報等、法人の運営にとって重要な資産である。これらが外部へ漏えい又は消失等した場合、法人の事業の停滞及び社会的信頼失墜等といった極めて重大な事態を招くことになる。

このような事態を防止するため、法人の情報資産を利用する者は、不断の努力をもってその保全に努めなければならない。そこで、法人の情報資産に関する情報セキュリティ対策の統一的かつ基本的な方針及び基準として、群馬県公立大学法人情報セキュリティポリシー（以下「ポリシー」という。）を定めるものとする。

２　構成

ポリシーは、「情報セキュリティ基本方針」及び「情報セキュリティ対策基準」の二階層で構成する。

また、「情報セキュリティ対策基準」に基づき、ネットワーク及び情報システムごとに、具体的な情報セキュリティ対策の実施手順（以下「実施手順」という。）を策定するものとする。

３　定義

このポリシーで使用する用語の定義は、「情報通信技術の利用における安全性及び信頼性の確保に関する基本要綱（群馬県情報セキュリティポリシー）」（平成29年８月17日群馬県高度情報化推進本部）で使用する用語の例による。

４　適用範囲及び対象者

ポリシーの適用範囲は、所有又は契約に基づく提供等により、法人が管理しているすべての情報資産とする。また、法人のネットワークに一時的又は継続的に接続する上記以外の情報機器については、接続している間は適用範囲に含めるものとする。

ポリシーの適用対象者は、法人の役員、職員（非常勤職員及び派遣労働者を含む。）、学生、外部委託の受託者及び法人の情報資産を利用する来学者等（以下「利用者」という。）とする。

５　情報資産を取り扱う者の責務

利用者は、情報セキュリティの重要性を理解し、情報資産の取り扱いに当たってはポリシーを遵守しなければならない。

6　情報セキュリティ管理体制

法人の情報資産に関する情報セキュリティ対策は、情報セキュリティ対策を推進及び管理するための体制を確立して実施する。

7　情報資産の管理

法人の情報資産をその重要度に応じて分類し、その分類ごとに適切な管理を行う。

8　情報セキュリティへの脅威

情報セキュリティ対策を実施する上で特に認識すべき脅威は、以下のとおりである。

（1）部外者の侵入、不正アクセス、不正操作、コンピュータウイルス攻撃、サービス不能攻撃等外部の要因による情報資産の漏えい、破壊、盗聴、改ざん、消去、盗難等

（2）利用者による情報資産の無断持ち出し及び無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、利用者の操作ミス、故障等の内部の要因による情報資産の漏えい、破壊、消去等

（3）地震、落雷、火災等の災害又は事故によるサービス及び業務の停止等

9　情報セキュリティ対策

情報セキュリティへの脅威等から情報セキュリティを保護するために、以下の情報セキュリティ対策を講ずる。

（1）物理的セキュリティ

ネットワーク及び情報システムを設置する施設等への不正な立入りを防止するとともに、ネットワーク及び情報システムを災害等から保護するため、必要な物理的対策を講ずる。

（2）人的セキュリティ

情報セキュリティに関する利用者の遵守義務を定め、利用者に情報セキュリティ対策の内容を周知徹底するための教育、訓練を実施する等、必要な人的対策を講ずる。

（3）技術的セキュリティ

情報資産を不正なアクセス等から適切に保護するため、ネットワーク及び情報システムの管理、アクセス制御、コンピュータウイルス等の不正プログラム対策、不正アクセス対策等、必要な技術的対策を講ずる。

10　評価及び見直し

情報セキュリティ対策を定期的に評価し、必要に応じてポリシー及び実施手順の見直しを行う。

11　実施手順の非公開

実施手順は、公にすることにより法人の情報セキュリティ対策に支障を及ぼすおそれがあるため、非公開とする。

第２章　情報セキュリティ対策基準

１　情報セキュリティ管理体制

（１）体制及び組織

群馬県の情報セキュリティ管理については、以下の体制及び組織とする。

ア　統括情報セキュリティ責任者（CISO）
イ　情報セキュリティ責任者
ウ　情報セキュリティ監督者
エ　ネットワーク管理者
オ　情報システム管理者
カ　セキュリティ事案対応チーム（CSIRT）

（２）役割・責任

ア　統括情報セキュリティ責任者

(ｱ) 統括情報セキュリティ責任者（以下「統括責任者」という。）は、理事長をもって充てる。

(ｲ) 統括責任者は、法人が所有する情報資産の情報セキュリティ対策に関する統括的な権限と責任を有する。

(ｳ) 統括責任者は、法人の情報セキュリティ対策に関する統括的な意見の集約、指導、助言及び指示を行う。

(ｴ) 統括責任者は、法人の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、必要かつ十分な措置を行う権限及び責任を有する。

イ　情報セキュリティ責任者

(ｱ) 情報セキュリティ責任者（以下「責任者」）は、法人事務局においては事務局長、大学においては学長をもって充てる。

(ｲ) 責任者は、所掌に属する組織で取り扱う情報資産の情報セキュリティ対策に関する権限と責任を有する。

(ｳ) 責任者は、所掌に属する組織において情報セキュリティ対策に関する意見の集約、指導及び助言を行う権限を有する。

(ｴ) 責任者は、役員及び職員（以下「役職員」という。）に対する教育及び研修を行う。

ウ　情報セキュリティ監督者

(ｱ) 情報セキュリティ監督者（以下「監督者」という。）は、法人事務局及び大学の事務局においては次長、大学の学部、研究科、外国語教育研究所、群馬学センター、地域連携センター、地域日本語教育センター、キャリア支援センター、附属図書館においてはこれらの組織の長をもって充てる。

(ｲ) 監督者は、組織内の情報資産の情報セキュリティ対策について責任者を補佐す

るとともに、組織内の職員に対して情報セキュリティ対策に関する指導及び助言を行う権限を有する。

(ｳ) 監督者は、組織内の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、責任者の指示に従い、責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

(ｴ) 責任者は、利用者がポリシー及び関係するネットワーク及び情報システムの実施手順を、必要な範囲で参照できるよう配慮しなければならない。

エ　ネットワーク管理者

(ｱ) ネットワーク管理者は、法人が所有する又は契約等によって法人に提供されているネットワークを管理する組織の責任者とする。

(ｲ) ネットワーク管理者は、当該ネットワークの情報セキュリティ対策について、運用管理を担当する職員を指揮監督する。

(ｳ) ネットワーク管理者は、当該ネットワークを利用する者に情報セキュリティ対策を遵守するよう周知、指導等必要な措置を取らなければならない。

オ　情報システム管理者

(ｱ) 情報システム管理者は、法人が所有する又は契約等によって法人にサービスが提供されているシステムを管理する組織の責任者とする。

(ｲ) 情報システム管理者は、当該システムの情報セキュリティ対策について、運用管理を担当する職員を指揮監督する。

(ｳ) 情報システム管理者は、当該システムを利用する者に情報セキュリティ対策を遵守するよう周知、指導等必要な措置を取らなければならない。

カ　セキュリティ事案対応チーム

(ｱ) セキュリティ事案対応チームは、統括情報セキュリティ責任者の下に整備する。

(ｲ) セキュリティ事案対応チームは、情報セキュリティインシデント（6（1）に定める「情報セキュリティインシデント」をいう。）の発生が予見される場合及び発生時に迅速かつ円滑な対応を図り、その拡大及び再発を防止するための業務を行う。

(ｳ) セキュリティ事案対応チームの運用に関して必要な事項は、別に定める。

2　情報資産の管理

（1）情報資産の管理

ア　情報資産の作成

利用者は、教育研究又は法人業務（以下「教育研究等」という。）上必要のない情報を作成してはならない。

イ　情報資産の利用

情報資産を利用する者は、当該情報資産を利用目的以外の目的に利用してはならない。

ウ　情報資産の廃棄

情報資産を廃棄する場合、日時、担当者及び処理内容を記録しなければならない。

（2）保護が必要な情報資産の管理

情報資産のうち保護が必要なものについて、機密性、完全性及び可用性の観点から次のとおり分類し、当該分類に応じた管理を行うものとする。

分類	分類基準	分類に応じた管理の例
要機密情報資産	秘密文書に相当する機密性を要する情報資産、又は秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	・必要以上の複製及び配布禁止 ・保管場所の制限、保管場所への必要以上の記録媒体等の持ち込み禁止 ・記録媒体等への書き込み禁止 ・暗号化、パスワード設定を施しての保管 ・情報資産の送信、運搬、提供時における暗号化・パスワード設定 ・復元不可能な処理を施しての廃棄 ・外部で情報処理を行う際の安全管理措置の規定 ・耐火、耐震等の対策を講じた施錠可能な場所での保管
要保全情報資産	改ざん、誤びゅう又は破損により、取引相手及び学生等の権利が侵害される、又は業務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定・耐火、耐震等の対策を講じた施錠可能な場所での保管
要安定情報資産	滅失、紛失又は当該情報資産が利用不可能であることにより、利用者の権利が侵害される、又は法人の業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・耐火、耐震等の対策を講じた施錠可能な場所での保管

3　物理的セキュリティ

（1）サーバ等機器の管理

ア　機器の取付け

ネットワーク管理者及び情報システム管理者は、サーバ等機器の取付けを行う場合、地震、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除する対策を講じた場所に設置し、ラックへ固定等必要な措置を講じなければならない。

イ　サーバの冗長化

停止等した場合に教育研究等の遂行に重大な影響を及ぼすサーバは、冗長化しなければならない。

ウ　機器の電源

ネットワーク管理者及び情報システム管理者は、サーバ等機器の電源について、停電等による電源供給の停止、落雷等による過電流に対応するための措置を講じなければならない。

エ　設置場所の秘匿

ネットワーク及び情報システムの機器については、当該ネットワーク等の担当者以外にその設置場所を公開してはならない。

（2）情報システム室の管理

ネットワーク及び情報システムの基幹サーバ等機器を設置し、当該サーバ等機器の管理及び運用を行うための部屋（以下「情報システム室」という。）は常時施錠することとし、入室は、原則として、当該情報システム室を管理する職員、室内にサーバ等機器を設置している情報システム等の担当者のみとしなければならない。

（3）通信ケーブル等の配線

通信ケーブル及び電源ケーブルは、損傷等を防止するための措置を講じなければならない。

（4）コンピュータ等の管理・保全措置

責任者及び情報システム管理者は、法人のコンピュータ、通信回線装置、記録媒体等情報を保存又は送受信できる機器（以下「コンピュータ等」という。）について、盗難及びデータ漏えい防止のため必要な措置を講じなければならない。

（5）機器の廃棄等

責任者、ネットワーク管理者及び情報システム管理者は、機器の廃棄又はリース返却等を行う場合、機器に記録したすべての情報を復元不可能に消去又は記録媒体を物理的に破壊した上で行わなければならない。

4　人的セキュリティ

（1）役職員の遵守義務

ア　ポリシー等の遵守義務

役職員は、ポリシー及び実施手順を遵守しなければならない。

イ　教育研究等以外の目的での使用の禁止

役職員は、教育研究等以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

ウ　退職時等の遵守事項

役職員は、異動、退職等により教育研究等から離れる場合には、利用していた情報資産を返却しなければならない。また、その後も教育研究等の遂行上に知り得た情報を漏らしてはならない。

（2）機器の使用に関する措置

ア　コンピュータ及び記録媒体の管理

役職員は、使用するコンピュータ及び記録媒体について、第三者に不正に使用又は閲覧されないよう適切に管理しなければならない。

イ　機器構成の変更等の禁止

役職員は、責任者及び情報システム管理者の許可を得た場合を除き、コンピュータの機器構成、ソフトウェアに関するセキュリティ機能の設定及びネットワーク接続の変更並びに標準以外のアプリケーションソフトのインストール等を行ってはならない。

（3）コンピュータ等の持ち出し及び私物の使用制限

利用者は、原則として、責任者の許可を得た場合を除き、法人のコンピュータ等を法人の敷地の外に持ち出し、又は私物のコンピュータ等を教育研究等に使用してはならない。

（4）ＩＤ・パスワード等の利用、管理

利用者は、ＩＤ及びパスワード、ＩＣカード等利用者認証に用いるものを適正に利用及び管理しなければならない。

（5）非常勤職員等への対応

責任者は、利用者のうち非常勤職員（派遣労働者を含む。）、学生及び来学者（以下「非常勤職員等」という。）に対し、情報資産の利用開始時に、ポリシー等のうち非常勤職員等が守るべき内容を理解させ、遵守させなければならない。

（6）外部委託

役職員は、ネットワーク及び情報システムの開発、保守等を外部委託する場合は、本ポリシーに基づく外部委託事業者が守るべき内容の遵守及び委託業務上知り得た情報資産に関する守秘義務を契約に明記しなければならない。

5　技術的セキュリティ

（1）外部ネットワークとの接続制限等

外部へのネットワーク接続は、必要最小限に限定するとともに、ネットワーク管理者は、外部ネットワークとの接続点において、ファイアウォール等の情報セキュリティ機器を導入し、外部からの脅威に対する措置を講じなければならない。

（2）無線ＬＡＮの対策

ネットワーク管理者は、教育研究等に無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。また、法人の敷地内に公衆通信回線（フリーWi-Fi）を設置する場合、教育研究等に利用するネットワークから分離させなければならない。

（3）ネットワーク及び情報システムの管理

ア　アクセス記録の取得等

ネットワーク管理者及び情報システム管理者は、アクセス記録その他情報セキュリティの確保に必要な記録を取得し、一定期間保存するとともに、アクセス記録等が窃取、改ざん、誤消去等されないように必要な措置を講じなければならない。

イ　ソフトウェアの修正及び更新

ネットワーク及び情報システムのソフトウェアに情報セキュリティに重大な影響を及ぼすセキュリティホールが発見された場合は、ネットワーク管理者及び情報システム管理者は、修正プログラムを速やかに適用しなければならない。

ウ　電子メールのセキュリティ管理

電子メールに係る情報システム管理者は、電子メールの中継処理その他の不正な電子メールの送受信が行われないよう、電子メールサーバの設定を行わなければならない。

（4）バックアップデータの作成

ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムで取り扱う情報について、故障その他からの復旧用としてバックアップデータを作成し、一定期間保存しなければならない。

（5）アクセス制御等

ア　アクセス制御

ネットワーク管理者及び情報システム管理者は、所管するネットワーク又は情報システムに権限のない職員等がアクセスできないよう制限しなければならない。

イ　外部からのアクセス等

外部から内部のネットワーク及び情報システムへのアクセスは、原則として外部アクセス用のサーバに対してのみとしなければならない。

ウ　外部公開用サーバの制御

ホームページ等外部公開用のサーバは、原則として、システム管理者の許可を受けた者以外の者が変更又は削除できないような権限制御等の措置を施さなければならない。

（6）不正プログラム対策

ネットワーク管理者及び情報システム管理者は、コンピュータウィルス等の不正プログラムから情報資産を守るために必要な対策を講じなければならない。

（7）不正アクセス対策

ネットワーク管理者及び情報システム管理者は、不正アクセスを防止及び早期検知するため必要な措置を講じなければならない。

（8）セキュリティ情報の収集

ネットワーク管理者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。

6　運用

（1）情報セキュリティインシデント発生時の対応

ア　利用者は、情報セキュリティに関する障害並びに事故及びネットワーク及び情報システム上の欠陥並びに誤動作（以下「情報セキュリティインシデント」という。）を認知した場合、速やかにセキュリティ事案対応チーム又は監督者に報告しなければならない。

イ　セキュリティ事案対応チームは、当該情報セキュリティインシデントの発生について法人内の関係者に報告又は外部の関係機関等に連絡しなければならない。

ウ　ネットワーク管理者及び情報システム管理者は、情報セキュリティインシデントの発生によりやむを得ない場合は、ネットワークの切断及びシステム停止等の措置を講じる。

エ　責任者、ネットワーク管理者及び情報システム管理者は、セキュリティ事案対応チームとともに情報セキュリティインシデントの内容及び発生原因を分析し、セキュリティ侵害防止の暫定措置を講じた上で、所管するネットワーク及び情報システムを復旧する。

オ　責任者、ネットワーク管理者及び情報システム管理者は、物理的、人的及び技術的セキュリティの改善に係る再発防止策を検討し、最高責任者の指示を受けて必要な措置を講じなければならない。

（２）懲戒処分等

ポリシー及び実施手順に違反した利用者は、その重大性、発生した事案の状況等に応じて、群馬県公立大学法人職員懲戒規程（群馬県公立大学法人規程第14号）又は各大学の学則等による懲戒処分の対象とすることがある。

７　情報セキュリティ対策の評価及び見直し

ポリシーを遵守した情報セキュリティ対策の実施状況や新たな脅威を想定した情報セキュリティ対策の有効性等についての検証結果を踏まえ、情報セキュリティ対策を定期的に評価し、必要に応じてポリシー及び実施手順の見直しを行う。

附　則

このポリシーは、平成30年４月１日から施行する。

附　則

このポリシーは、令和２年３月24日から施行する。

附　則

このポリシーは、令和２年４月１日から施行する。