群馬パース大学情報セキュリティ運用規程

（目　的）

第１条　この規程は、群馬パース大学（以下、「本学」という。）の情報セキュリティポリシーに基づき、本学における情報システムのセキュリティの維持向上に関する事項を定めることにより、本学の有する情報資産を適正に保護活用し、情報システムの信頼性、安全性及び効率性の向上に資することを目的とする。

（禁止事項）

第２条　利用者は、次に掲げる事項を行ってはならない。また、他の者に行わせてもならない。

（１）情報資産の目的外利用

（２）守秘義務に違反する情報の開示

（３）ネットワークを介し行われる通信の傍受及び監視

（４）ネットワーク機器、サーバー装置及び端末の利用記録を採取する行為

（５）セキュリティ上の脆弱性を検知する行為

（６）法令又はこの規程に違反する情報の発信

（７）上記の行為を助長する行為

（学内ネットワークの設計・構築及び利用）

第３条　学内ネットワークは、セキュリティ要件に基づき設計され、情報セキュリティ技術責任者の承認を得たうえで構築、運用するものとする。

２　学内ネットワークを改版（増改築、廃止）する際は、設計書にて情報セキュリティ技術責任者の承認を得たうえで施工することとする。

３　利用者は許可された接続方法以外の方法で学内ネットワークに接続してはならない。

４　利用者は学内に個人的なネットワークを構築してはならない。ただし、「利用目的、必要性、利用機器、利用の範囲」を情報セキュリティ技術責任者（以下、「技術責任者」という。）に申し出て、承認を得た場合に限り、構築することができる。技術責任者は、申請内容を精査し、必要であれば、情報システム委員会に諮り、利用の可否を決定し、利用者へ通知するものとする。

５　学外から学内ネットワークへ侵入できない策を講ずることとする。ただし、リモートメンテナンス等で必要と認められた場合で、情報漏洩に関する制約事項が契約書又は覚書等により担保されていることを前提に許可するものとする。

６　学内ネットワークを介する通信は監視されていることを利用者に周知するものとする。また、通信状況を収集する仕組みを構築し、運用者を選任し、運用できるものとする。

（セキュリティホール・不正プログラム感染対策）

第４条　技術責任者は、以下の対策の策定、周知を行い。適用状況の確認を年１回以上実施し、セキュリティの維持に努めるものとする。

（１）情報機器に対して、セキュリティホール等の脆弱性対策として配布される更新プログラムが適用させていること。

（２）サーバーや通信機器に対して、配布された更新プログラムを確認し、遅滞なく適用すること。

（３）ウィルス対策ソフトを導入し、セキュリティレベルの維持向上を図ること。（当該装置で動作可能なウィルス対策ソフト等が存在しない場合を除く。）

（４）標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。

（５）内部に侵入した攻撃の早期検知、拡大困難施策、外部との不正通信検知等の対策（内部対策）を講ずること。

（メールサーバー）

第５条　技術責任者は、電子メールサーバーの管理や設定において、以下に掲げる項目を確認し、必要と認めた場合は措置を講ずることができるものとする。

（１）電子メールの不正な中継を行わない仕組み

（２）電子メールのなりすましを防止する仕組み

２　技術責任者は、詐欺メール・ウィルス付与メールの情報取得に留意し、本学のメール環境を利用する者に対し、注意喚起情報を発信できるものとする。

３　利用者は、詐欺メール・ウィルス付与メールには十分注意し、発信元の不明瞭なメール及び添付ファイルは極力開かない、リンク先へ遷移しない等の対処をすること。また、前項の注意喚起情報には注意を払い、疑わしいメールが来た際は、技術責任者に報告することとする。

４　外部業者のレンタルサーバーを利用する場合、技術責任者は、セキュリティ要件を満たしていることを確認し、契約の許可を与えることができるものとする。

（ウェブサーバー）

第６条　技術責任者は、ウェブサーバーの管理や設定において、以下に掲げる項目を確認し、必要と認めた場合は措置を講ずることができるものとする。

（１）通信データを暗号化して送受信する仕組み

（２）利用者の入力情報を管理部署へ伝達する仕組み

（３）コンテンツの改ざんを防止する仕組み

２　管理部署は、ウェブコンテンツを公開する際、公序良俗に反する記載がないこと、許諾の無い個人情報の記載がないこと等に十分に配慮することとする。

３　管理部署は、ウェブコンテンツとして公開した内容に改ざんがないかを監視し、改ざんを発見した場合は、速やかに改修すると共に、情報システム委員

会に報告することとする。

4　外部業者のレンタルサーバーを利用する場合、技術責任者は、セキュリティ要件を満たしていることを確認し、契約の許可を与えることができるものとする。

（学内サーバー）

第７条　技術責任者は、本学が所有する情報システム（サーバー）へのアクセスは必ず主体認証（ユーザ ID・パスワード等の識別コードによる認証）にて認証される仕組であること、また接続情報が各々の情報システム内に一定期間保存される仕組みが構築されていることを確認し、設置を許可するものとする。

2　識別コードは、技術責任者により一括で管理発行され、利用者に周知することとする。ただし、内部秘匿が必要な場合は、担当部署にて主体認証の発行を許可するものとする。

3　利用者は、情報システム内に保存されている情報を収集し、外部媒体に格納してはならない。やむを得ない事情により学外に持ち出す際は、上長の許可を得ることとする。また、「情報の運搬及び送信」に記載の事項に留意することとする。

4　外部業者のレンタルサーバーを利用する場合、技術責任者は、セキュリティ要件を満たしていることを確認し、契約の許可を与えることができるものとする。

（識別コード及び主体認証情報の取扱い）

第８条　利用者は、自己に付与された識別コードを適切に管理し、情報システムを利用することとする。識別コードの再発行や再確認は、原則不可とする。ただし、技術責任者に申し出て許可された場合は、情報を開示できるものとする。

2　利用者は、他者に付与された識別コードを用いて情報システムを利用してはならない。

3　利用者は、管理者権限を持つ識別コードを付与された場合、管理者としての業務遂行時に限定して、当該識別コードを利用できるものとする。

（クラウド環境の利用）

第９条 利用者は、クラウド環境の利用に際し、以下の事項を遵守することとする。

（１）情報システム委員会に申し出て、承認されたクラウド環境を利用すること。ただし、承認システムが構築されるまでは、各部署・各学科の長の許可のもとで使用すること。

（２）主体認証機能や暗号化機能を備えるセキュアなクラウド環境を利用する場合、これに備わる機能を必ず有効にすること。

（３）要機密情報は、必要がなくなった時点で速やかに削除すること。

（外部記憶媒体の利用）

第 10 条 利用者は、外部記憶媒体の利用に際し、以下の事項を遵守することとする。

（１）情報システム委員会に申し出て、承認された外部記憶媒体を使用すること。ただし、承認システムが構築されるまでは、各部署・各学科の長の許可のもとで使用すること。

（２）外部記憶媒体を使用する際には、事前にウィルス対策ソフトによる検疫及び駆除を行うこと。

（３）主体認証機能や暗号化機能を備えるセキュアな外部記憶媒体を利用する場合、その機能を必ず有効にすること。

（４）要機密情報は、必要がなくなった時点で速やかに削除すること。

２　外部記憶媒体の紛失確認のため、年１回以上は存在確認を実施することとする。ただし、チェックシステムが構築されるまでは、各部署・各学科の管理のもとで存在確認を実施すること。

（情報の運搬及び送信）

第 11 条　利用者は､要保護情報を安全区域外に持ち出し､他の場所に運搬する場合は、安全確保、紛失等には十分に留意して運搬方法を決定し、適切な措置を講ずること。

２　利用者は、要保護情報を安全区域外に通信回線を使用して送信する場合には、安全確保、盗聴等には十分に留意して送信方法を決定し、適切な措置を講ずること。

（ネットワーク環境・クラウド環境の監視）

第 12 条　利用者は、ネットワークを通じて行われる通信を傍受してはならない。ただし、情報システム委員会で選任された者に関しては、ネットワークを介して行われる全ての通信の監視を行わせることができる。

２　前項にて選任された者は、監視によって知り得たいかなる情報も他者に伝達してはならない。ただし、本学又は学外に対する重大なセキュリティ侵害を防止するために必要と認められる場合、監視した内容を情報セキュリティ委員会及び特に定める者に伝達することができる。

（外部記憶媒体利用状況の監視）

第 13 条　利用者は、外部記憶媒体の利用状況を監視してはならない。ただし、情報システム委員会で選任された者に関しては、外部記憶媒体の利用状況の監視を行わせることができる。

２　前項にて選任された者は、監視によって知り得たいかなる情報も他者に伝達してはならない。ただし、本学又は学外に対する重大なセキュリティ侵害を防止するために必要と認められる場合、監視した内容を情報セキュリティ委員会及び特に定める者に伝達することができる。

（ソーシャル・ネットワーキング・サービスによる情報発信時の対策）

第 14 条 公式な情報発信のためにソーシャル・ネットワーキング・サービス（以下、「SNS」という。）を利用する場合、運用する SNS 毎に運用責任者を定め、情報セキュリティ委員会に届出、承認を得るものとする。ただし、承認システムが構築されるまでは、各部署・各学科の長の許可のもとで運用すること。

2　運用責任者は、情報発信が本学のものであると認識できるようにするため、以下の各号の対策を行うものとする。

（１）アカウント名やアカウント設定の自由記述欄等を利用し、本学が運用していることを明示すること。

（２）アカウント設定の自由記述欄等において、本学ウェブサイトの URL を記載すること。

（３）本学のウェブサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを記載すること。

（４）SNS 提供事業者が、「公式アカウント」と呼ばれるアカウントの認証を行っている場合には、可能な限りこれを取得すること。

（５）URL 短縮サービスは、その使用が避けられない場合を除き、使用しないこと。（利用者が認識不能な文字列は避ける。）

3　運用責任者は、アカウント乗っ取りやパスワードの搾取を防止するため、以下の各号の対策を行うものとする。

（１）パスワードは、十分な長さ(8 文字以上)と複雑さを持たせ、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。

（２）パスワードは端末に記憶させず、ログインの度に入力すること。

（３）二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。

（４）ログイン端末には、最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。

4　運用責任者は、アカウント乗っ取りを確認した場合には、被害を最小限とするため、ログインパスワードの変更やアカウントの停止を速やかに実施すると共に、情報セキュリティ委員会へ速やかに報告するものとする。

5　情報セキュリティ責任者は、なりすましを確認した場合の対処として、本学ウェブサイトに、なりすましアカウントが存在することや当該アカウントを運用していないこと等の周知施策を指示すると共に、公的メディア等を通じて注意喚起を行うものとする。

（情報漏洩、紛失、規程違反の報告と対応）

第 15 条 利用者は、情報漏洩、紛失、情報セキュリティ関連規程違反を知った場合は、所属部所の責任者にその旨を報告するものとする。

2　所属部所の責任者は、前項の報告を受けた場合又は自らがそれを知った場合

には、情報セキュリティ委員会にその旨を報告するものとする。

3　情報セキュリティ責任者は、前項の報告を受けた場合又は自らがそれを知った場合には、インシデント対応チームを速やかに設置し、調査を行い、事実を確認するものとする。

事実確認に当たっては、可能な限り当該行為を行った者の意見を聴取することとする。

4　情報セキュリティ責任者は、調査によって違反行為が判明した際には、次に掲げる措置を講ずることができる。

（１）当該行為者に対する当該行為の中止命令

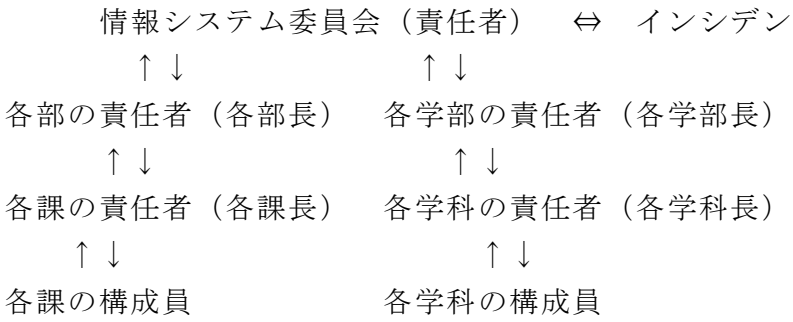
（２）当該行為に係る情報発信の遮断命令

（３）当該行為者のアカウント停止命令又は削除命令

（４）その他法令に基づく措置

5　情報セキュリティ責任者は、前項の措置を講じた場合は、遅滞なく当該行為者の所属部の責任者にその旨を報告するものとする。

図.インシデント報告経路と組織の関係



（改　廃）

第 17 条 この規程の改廃は、大学協議会の議を経て、学長がこれを行う。

（用語の定義）

（１）要機密情報

個人情報を含む記述を電磁的記録として格納した（ファイルを含む）情報のことをいう。

（２）安全区域

サーバー装置及び端末、ネットワーク機器を設置した事務室、研究室、講義室又はサーバールーム（学外のサーバールーム及びデータセンターを含む）等の内部であって、利用者以外の者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。

（３）利用者

教職員で許可を受けて本学情報システムを利用する者をいう。

臨時利用者を含む。

（10）主体認証

次号の識別コードを提示した主体が、その識別コードを付与された主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムアクセスを許可する。

（11）識別コード

主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。本学では、ユーザ ID とパスワードを組み合わせたものを指す。

（12）アカウント

主体認証を行う必要があると認めた情報システムにおいて、主体に付与された正当な権限をいう。

附則　　この規程は、2019 年 4 月 1 日から施行する。