情報セキュリティ管理要領

平成２０年４月１日
公立大学法人福井県立大学要領５号

目次

第１章　要領について

（概要）

第１条　本要領は、公立大学法人福井県立大学総合情報ネットワークシステム運用管理規程（平成１９年公立大学法人福井県立大学規程第９０号）第９条の規定に基づき、公立大学法人福井県立大学（以下「法人」という。）における情報ネットワーク上を流通する情報やコンピュータおよびネットワーク機器など（以下情報資産）を保護・管理する情報セキュリティ対策を実施するため定めるものとする。

本要領は、情報セキュリティ確保のため、遵守すべき事項を具体的かつ網羅的に記載したものである。

（対象範囲）

第２条　本要領の適用範囲（対象システム）は、本学の情報資産に関係する人的・物理的・環境的資源とする。

（対象者）

第３条　本要領の対象者は、管理の内容によって異なるため、各方針で対象者を明確に記載するものとする。

（用語）

第４条　各方針で用いられる用語について、以下のように定義する。

(1)「FPUnet」は、福井県立大学が運用管理する情報関連システムで、ネットワーク通信回線、サーバ類、ネットワーク機器、これらに接続して使用する情報システム、端末機、周辺装置および共通情報演習室、学部等情報演習室、ＬＬ教室等のメディア機器等を含む。

(2)「情報統括責任者（ＣＩＯ)」は、情報セキュリティ管理作業の責任を有し、管理を依頼された情報機器に対して、情報セキュリティ対策を実施する責任者である。

(3)「情報統括補佐（ＣＩＯ補佐)」はＣＩＯを補佐し、「情報ネットワーク管理室」の業務を掌理し、後述のネットワーク管理者、サーバ管理者への作業指示、進捗管理を行う。

(4)「FPUnet 運用管理連絡会議」は本学の情報セキュリティを維持・調整する組織であり、全学的な管理体制を整える。

(5)「情報ネットワーク管理室」は、情報セキュリティ対策を実施および推進する担当部署で、FPUnetのネットワークを管理するネットワーク管理者、共同利用の情報システムのサーバを管理するサーバ管理者を有する。

(6)「学部等情報担当者」は、各部局、事務局から選出され、部局、事務局内におけるセキュリティ推進および情報収集担当である。

（改訂）

第５条　本要領の変更は、情報統括責任者（ＣＩＯ）に申請し、「FPUnet 運用管理連絡会議」で協議し変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知する。また、定期的に内容を精査し、変更が必要であると認められた場合には速やかに変更し、その変更内容を学内に通知する。

第２章　一般利用者向けの方針

第１節　パソコン利用におけるセキュリティ方針

（パソコン利用におけるセキュリティ方針の趣旨）

第６条　本方針は、パソコン上の機密性・完全性を確保し、発生し得る障害を未然に防ぐことを目的とする。

（パソコン利用におけるセキュリティ方針の対象者）

第７条　本方針の対象者は、 パソコンを利用するすべての職員

（パソコン利用におけるセキュリティ方針の対象システム）

第８条　本方針の対象システムは、業務（学内事務システム等）に使用するパソコン

（遵守事項）

第９条　パソコンの使用に関し、次に掲げる事項を遵守しなければならない。

(1) 本学の学内事務において、職員が使用できるパソコンは、「第３章 第７節 ソフトウェア・ハードウェアの購入および導入方針」に則った製品とする。

(2) 学内で実施される情報セキュリティに関する講習会等を通じた情報セキュリティ情報の収集

第１０条　パソコンに導入するソフトウェアに関し、次に掲げる事項を遵守しなければならない。

(1) 原則として、本学で利用するパソコンは、「第３章 第７節 ソフトウェア・ハードウェアの購入および導入方針」で規定されたソフトウェアを導入することとする。業務上やむを得ず導入しなければならないソフトウェアは、情報ネットワーク管理室に申請し、許可を得なければならない。

(2) 導入したソフトウェアは、常に最新の状態で使用することとし、情報ネットワーク管理室が提供するソフトウェア情報をもとに修正プログラム等を導入しなければならない。

第１１条　パソコンの他者への利用の制限に関し、次に掲げる事項を遵守しなければならない。

(1) 不正な操作や盗み見を防止するため、離席時にはログオフするか、画面・キーボードのロック設定機能を使用しなければならない。

(2) 「第３章 第４節 ユーザ認証方針」に従い、パソコンに対するパスワード管理を厳重にしなければならない。

(3) ノート型パソコンは、基本認証以外にも BIOS での認証を行うことが望ましい。

第１２条　パソコンでの情報の取り扱いに関し、次に掲げる事項を遵守しなければならない。

(1) パソコンで機密情報を取り扱う場合、長期期間その情報を利用する場合には、機密情報を取り扱う許可を情報ネットワーク管理室に申請し、許可を得なければならない。許可を得た機密情報は、万一の漏洩に備え、暗号化等の対策を実施しなければならない。

(2) パソコンで一時的に機密情報を取り扱う場合、取り扱い後には、不必要となった情報を削除しなければならない。

(3) 使用後の帳票類や記録媒体はキャビネット等へ収納し、机上等に放置してはならない。

(4) 重要度の高い帳票類や記録媒体は施錠保管し、特に重要な場合は耐火金庫・耐熱金庫に保管しなければならない。

第１３条　ウイルス対策の実施に関し、次に掲げる事項を遵守しなければならない。

(1) 「第１章 第２節 ウイルス対策方針」に従いウイルス対策を実施しなければならない。

第１４条　パソコンの移設に関し、次に掲げる事項を遵守しなければならない。

(1) パソコンの移設が必要な場合には、情報ネットワーク管理室に申請し、許可を得なければならない。

第１５条　ノートパソコンの利用上の注意事項に関し、次に掲げる事項を遵守しなければならない。

(1) 学外にノート型パソコンを持ち出す場合、盗難・窃盗に注意し、情報の盗難を防止する対策を行わなければならない

第２節　ウイルス対策方針

（ウイルス対策方針の趣旨）

第１６条　本方針は、ウイルス・ワームによって引き起こされる情報漏えいやシステム破壊の被害を未然に防ぐことを目的とする。

（ウイルス対策方針の対象者）

第１７条　本方針の対象者は、 パソコンを利用するすべての職員・学生

（ウイルス対策方針の対象システム）

第１８条　本方針の対象システムは、 本学で使用するパソコンおよびサーバ

（遵守事項）

第１９条　ウイルス対策ソフトの導入に関し、次に掲げる事項を遵守しなければならない。

(1) パソコンおよびサーバにウイルス対策ソフトを導入する。

(2) ウイルス対策ソフトは、情報ネットワーク管理室が指定したソフトを導入することとする。

(3) 選択するウイルス対策ソフトの要件には、以下の機能が含まれていなければならない。

・定義ファイルの自動更新機能

・常時スキャン機能

第２０条　ウイルス対策ソフトの利用に関し、次に掲げる事項を遵守しなければならない。

(1) 利用者は、パソコンに導入されたウイルス対策ソフトを常駐設定にし、ファイルへのアクセスおよび電子メールの受信時には、常時スキャンできるように設定しなければならない。

(2) 利用者は、常時スキャンだけではなく定期的に、ファイル全体のスキャンを実施することとする。

(3) 利用者は、定義ファイルを毎日一度は更新するように設定しなければならない。

第２１条　パソコンおよびサーバソフトウェアのセキュリティ対策に関し、次に掲げる事項を遵守しなければならない。

(1) パソコンに導入されているソフトウェアを最新状態に維持しなければならない。

(2) サーバ管理者は、サーバに導入されているソフトウェアを最新状態に維持しなければならない。

第２２条　パソコンにおける電子メールを介してのウイルス被害の防止に関し、次に掲げる事項を遵守しなければならない。

(1) 電子メールの受信にあたっては、電子メール保護機能を有効にしなければならない。

(2) 送信元不明の電子メールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な添付ファイルに対してはこれに操作を加えてはならない。

(3) ファイルを添付してメールを送信する場合、当該ファイルのウイルス感染が無いことを必ず確認しなければならない。

第２３条　ウイルス・ワームに関する啓発教育の受講に関し、次に掲げる事項を遵守しなければならない。

(1) 本学でパソコンを利用する場合には、ウイルス・ワームに関する啓発教育を受講しなければならない。

第２４条　情報ネットワーク管理室におけるウイルス対策窓口の設置に関し、次に掲げる事項を遵守・実施しなければならない。

(1) 情報ネットワーク管理室は、学内のウイルス被害状況等を迅速に収集するために、ウイルス対策窓口を設置し周知徹底しなければならない。

(2) ウイルス対策窓口は、学内のウイルス被害状況を掌握し、問題発生時の初期対応を実施する。

第２５条　ウイルス対策ソフトがウイルスを検知した場合に、次に掲げる事項を遵守しなければならない。

(1) 対象者は、ウイルス対策ソフトの駆除機能を使用してウイルスを駆除しなければならない。

第２６条　ウイルスに感染した場合、次に掲げる事項を遵守しなければならない。

(1) 対象者は、以下の症状が発生した場合には、ウイルス対策窓口に報告し、対処しなければならない。

・パソコンの動作が重くなった。
・ウイルス付のメールが送られたとの連絡があった。
・突然、パソコン画面に不審な画像が表示された。
・ファイルを開こうとしたら、警告ポップアップが出た。

第３節　電子メールサービス利用方針

（電子メールサービス利用方針の趣旨）

第２７条　本方針は、電子メールで受け渡される情報の完全性を確保し、電子メール利用にあたって発生し得る各種の問題を未然に防ぐことを目的とする。

（電子メールサービス利用方針の対象者）

第２８条　本方針の対象者は、 電子メールサービスを利用する職員・学生

（電子メールサービス利用方針の対象システム）

第２９条　本方針の対象システムは、 本学より発行された電子メールアドレスを用いてメールの送受信を行うパソコン等

（遵守事項）

第３０条　電子メールサービス利用端末機器のセキュリティに関し、次に掲げる事項を遵守しなければならない。

(1) 電子メールの送受信にあたっては、情報ネットワーク管理室が指定した電子メールソフトウェアを用いなければならない。また、情報ネットワーク管理室の指示に従い、当該ソフトウェアのバージョンアップを行わなければならない。

(2) 電子メールアドレスは初期パスワードとともに発行される。初期パスワードは直ちに変更しなければならない。また、パスワードは最低１年に１度、定期的に変更しなければならない。設定するパスワードは、「第３章 第４節 ユーザ認証方針」に則ったものとする。

第３１条　電子メールで送受信される情報の保護に関し、次に掲げる事項を遵守しなければならない。

(1) 本学の業務や、個人情報に関わる機密情報は、原則として電子メールを用いて送信してはならない。

(2) 業務上やむを得ず機密情報を送受信する場合は、情報ネットワーク管理室の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。

(3) 電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。

(4) 本学から複数のメールアドレスに対し、同報送信する場合は、送信先メールアドレスが受信者間で閲覧できないよう、設定しなければならない。

(5) 電子メールを学外のメールアドレスに自動転送する場合は、可能な限り内容を暗号化し、電子署名

などの処置を施さなければならない。

第３２条　電子メールサービスとネットワーク保護に関し、次に掲げる事項を遵守しなければならない。

(1) 研究・教育・学内事務等の目的以外に電子メールサービスを利用してはならない。

(2) スパムメールを受信した場合は、これを転送してはならない。

(3) 本学より発行されたメールアドレスを利用して、学外のメーリングリストに参加する場合は、当該メーリングリストの信頼性、および業務への必要性を充分考慮した上で参加しなければならない。また、参加意義の無くなった場合は、直ちに脱退しなくてはならない。

(4) 電子メールの送信にあたっては、送信するメールサイズを考慮しなければならない。送信可能なメールサイズは、情報ネットワーク管理室にて規定する。

(5) その他、無用な電子メールを送受信することにより、ネットワークに負荷をかけてはならない。

第３３条　電子メールを介してのウイルス被害の防止に関し、次に掲げる事項を遵守しなければならない。

(1) メールの受信にあたっては、「第２章 第２節 ウイルス対策方針」に基づき、電子メール保護機能を有効にしなければならない。

(2) 送信元不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な添付ファイルに対してはこれに操作を加えてはならない。

(3) ファイルを添付してメールを送信する場合、当該ファイルのウイルス感染が無いことを必ず確認しなければならない。

(4) 電子メールサービスを利用中に、ウイルスの発見や、ウイルスと思われる症状を発見した場合は、「第３章 第１０節 セキュリティインシデント報告、対応方針」に基づき対応しなければならない。

第３４条　電子メール通信状況の記録・保管許可に関し、次に掲げる事項を遵守しなければならない。

(1) 電子メールの発受信状況は、情報ネットワーク管理室により記録・保管されていることを承諾しなければならない。

第４節　Ｗｅｂサービス利用方針

（ＷＥＢサービス利用方針の趣旨）

第３５条　本方針は、Web ブラウザを使用し、学内および学外のサイトを利用するにあたって発生し得る各種の問題を未然に防ぐことを目的とする。

（ＷＥＢサービス利用方針の対象者）

第３６条　本方針の対象者は、Web ブラウザを利用する職員・学生

（ＷＥＢサービス利用方針の対象システム）

第３７条　本方針の対象システムは、Web ブラウザを使用し、学内外の Web サイトにアクセスするコンピュータ

（遵守事項）

第３８条　Web サービスの利用に関し、次に掲げる事項を遵守しなければならない。

(1) 利用者は、学内およびインターネット上の Web サーバへのアクセスは、業務（学生においては教育・研究）上必要な場合のみ利用できる

(2) 利用者は、信頼できない Web サーバにアクセスしてはならない。

(3) 発信(掲示板等への書き込み)に関しては、情報の正確性を確保し、必要最小限の範囲で発信するものとする。また、下記に該当する情報の発信は禁止する。

・著作権、商標、肖像権を侵害するおそれのあるもの
・プライバシーを侵害するおそれのあるもの、差別的なもの
・他者の社会的評価・名誉・信用を傷つけるおそれのあるもの
・本学の信用・品位を傷つけるおそれのあるもの、本学の機密情報
・不正アクセスを助長するおそれのあるもの
・その他公序良俗に反するおそれのあるもの

(4) 利用者は、学内外の Web サーバに対して、攻撃等不正なアクセスを行ってはならない。また、攻撃、不正なアクセスの手段として学内外のシステムを利用してはならない。

(5) 利用者は、学内外の Web サーバに対して、他人のユーザ ID やパスワードなどを利用してアクセスしてはならない。

第３９条　Ｗｅｂブラウザ利用端末機器のセキュリティに関し、次に掲げる事項を遵守しなければならない。

(1) 利用者は、Web 閲覧にあたって、情報ネットワーク管理室が指定した Web ブラウザソフトを用いなければならない。また、情報ネットワーク管理室の指示に従い、当該ソフトウェアのバージョンアップおよびセキュリティ修正プログラムの適用を行わなければならない。

(2) 上記ソフトウェアを使用するコンピュータは、「第３章 第７節 ソフトウェア・ハードウェアの購入および導入方針」に基づいて導入され、「第２章 第１節 パソコン利用におけるセキュリティ対策方針」に基づいたセキュリティ対策を施したものでなければならない。

(3) 利用者は、インターネット上のサイトにアクセスするときは、必ず情報ネットワーク管理室が指定する Proxy サーバを経由しなければならない。

第４０条　Ｗｅｂサーバへのアクセスに関し、次に掲げる事項を遵守しなければならない。

(1) 利用者は、インターネット上のサイトへのアクセスにおいて、やむを得ない場合を除き、Cookie の設定をオフにしなければならない。

(2) 利用者は、署名の無く、安全が確認されていない ActiveX や Java、JavaScript、VBScript などのコードは実行してはならない。

(3) 利用者は、情報統括責任者（ＣＩＯ）が禁止するソフトウェアもしくはファイルをインターネット上からダウンロードして、実行、閲覧してはならない。禁止されていないファイルやソフトウェアであっても、必ずダウンロードし、ウイルスチェックを実施してから表示、実行しなければならない。

(4) 利用者は、リンクをクリックするとき、リンク先を確認してからクリックしなければならない。この場合、リンク先が、信頼できない URL である場合は、クリックしてはならない。また、バナー広告についても同様で、業務上必要のないバナー広告はクリックしてはならない。

第４１条　アクセス制御されたＷｅｂサイトの閲覧に関し、次に掲げる事項を遵守しなければならない。

(1) 利用者は、自身の占有パソコン以外で、パスワードを Web ブラウザに記憶させるような行為を行ってはならない。

(2) 利用者は、離席する場合は必ず、Web ブラウザを終了させるか、OS のパスワード付スクリーンロックを実施しなければならない。

(3) 利用者がクライアント証明書を必要とする場合は、情報統括責任者（ＣＩＯ）の承認後取得申請できるものとする。これらの証明書は各自厳密に管理しなければならない。

第４２条　Ｗｅｂサイトの閲覧状況の記録・保管許可に関し、次に掲げる事項を承諾しなければならな

い。

(1) Web サイトの閲覧状況は、情報ネットワーク管理室によって記録・保管されていることを承諾しなければならない。

(2) URL フィルタリングを導入する場合、情報統括責任者（ＣＩＯ）は、閲覧禁止サイトを決定できるものとする。

(3) 情報ネットワーク管理室は、危険な Web サイトや、不正アクセスを発見した場合は、情報統括責任者（ＣＩＯ）に報告を行わなければならない。

第５節　リモートアクセスサービス利用方針

（リモートアクセスサービス利用方針の趣旨）

第４３条　本方針は、ダイヤルアップ、VPN 等によりリモートアクセスサービス利用にあたり、本学の情報資産を外部から守ることを目的とする。

（リモートアクセスサービス利用方針の対象者）

第４４条　本方針の対象者は、リモートアクセスサービスを利用する職員、学生

（リモートアクセスサービス利用方針の対象機器・対象システム）

第４５条　本方針の対象システムは、リモートアクセスで利用する機器(パソコン、PDA、携帯電話など)およびリモートアクセスシステム

（遵守事項）

第４６条　リモートアクセス使用機器に関し、次に掲げる事項を遵守しなければならない。

(1) 利用者は、ダイヤルアップによる学内ネットワークへのアクセスにおいて、情報ネットワーク管理室が構築した機器を利用しなければならない。

(2) 利用者は、ダイヤルアップルータおよびサーバ・モデムなどによる学内ネットワークへの接続手段を、情報ネットワーク管理室の許可を得ることなく設置してはならない。

第４７条　リモートアクセス機器の管理に関し、次に掲げる事項を遵守しなければならない。

(1) リモートアクセスサービスは、許可された利用者のみ利用することができる。

(2) リモートアクセスで使用する機器の管理は、所有する利用者が行わなければならない。

第４８条　リモートアクセス利用環境に関し、次に掲げる事項を遵守しなければならない。

(1) リモートアクセスで利用できる機器は、「第２章 第１節 パソコン利用におけるセキュリティ方針」に従ったものなければならない。

(2) リモートアクセスの利用場所は、情報ネットワーク管理室の定める場所でなければならない。

(3) リモートアクセスによる接続形態、利用サービスは、情報ネットワーク管理室の定めるものでなければならない。

第４９条　リモートアクセス利用手順に関し、次に掲げる事項を遵守しなければならない。

(1) 利用者は、リモートアクセスを行う場合、利用者を識別する情報を入力しリモートアクセスサーバで認証されなければならない。

(2) 利用者は、リモートアクセスしている間に利用者がクライアントから離れる場合、接続を中止するか第三者の利用ができないようにしなければならない。

第５０条　リモートアクセス利用時の緊急対応に関し、次に掲げる事項を遵守しなければならない。

(1) 利用者は、リモートアクセス可能なパソコンおよび携帯電話を紛失した場合に、速やかに情報ネットワーク管理室に報告し具体的な指示を受け、対処しなければならない。

(2) 利用者は、リモートアクセスで使用するパソコンおよび携帯電話で使用するパスワードを忘れた場合に、情報ネットワーク管理室に連絡し、速やかに新たなパスワードへ変更しなければならない。

第６節　ネットワーク接続方針

（FPUnet に接続するサーバ・パソコン等の接続方針の趣旨）

第５１条　本方針は、FPUnet へのサーバ・パソコン等の接続において発生し得る各種の問題を未然に防ぎ、情報資産を保護することを目的とする。

（FPUnet に接続するサーバ・パソコン等の接続方針の準拠）

第５２条 本方針は「公立大学法人福井県立大学情報システム利用方針」を準用する。

第７節　ネットワーク利用方針

（ネットワーク利用方針の趣旨）

第５３条　本方針は、FPUnet 利用時の、機密保持および情報資産の保護、有効活用を目的とする。

（ネットワーク利用方針の対象者）

第５４条　本方針の対象者は、 FPUnet にコンピュータを接続し利用する職員・学生

（ネットワーク利用方針の対象システム）

第５５条　本方針の対象システムは、 FPUnet に接続し、通信を行うコンピュータおよびシステム

（遵守事項）

第５６条　FPUnet およびインターネットの利用に関し、次に掲げる事項を遵守しなければならない。

(1) FPUnet は、大学の情報資産であり、電子メールや Web サイトの利用などにおいて、教育・研究・学内事務目的以外の使用を禁止する。インターネットの利用についても同様である。

(2) 情報ネットワーク管理室の許可無く、FPUnet 上に、電子メールサーバや、Web サーバ、FTP サーバなどを構築してはならない。

(3) 他人の利用者 ID を用いて、FPUnet および、学外のネットワーク、インターネット上のサイトへアクセスしてはならない。

(4) ネットワーク利用者は、故意もしくは不注意を問わず、FPUnet および学外ネットワーク、インターネット上のサーバに対して、許可されたアクセス権限以上のアクセスを行ってはならない。

第５７条　FPUnet を利用した機密情報の送受信に関し、次に掲げる事項を遵守しなければならない。

(1) ネットワーク利用者は、学内事務に関わる情報や、学生や職員の個人情報などの機密性の高い情報が学外へ漏洩することを防ぐために、これらのファイルのアップロードや学外への送信を行ってはならない。

(2) 出所が不明なファイルや内容に確証の持てないファイルをダウンロードや実行してはならない。

(3) 業務上やむを得ず機密情報を学外へ送信もしくは学外から受信する場合は、情報ネットワーク管理室の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。

第５８条　インターネットで利用可能なサービスに関し、次に掲げる事項を遵守しなければならない。

(1) 原則として、利用者は、インターネットの利用において、電子メールおよび Web 閲覧以外を使用してはならない。情報ネットワーク管理室は、この２サービス以外利用できないようなアクセス制御を実施することができる。

(2) 業務上やむを得ず電子メールおよび Web 閲覧以外のサービスを利用したい場合は、情報統括責任者（ＣＩＯ）の承認を得ること。

(3) 暗号通信を用いたインターネットへのアクセスは、情報ネットワーク管理室の確認を得たサイトのみ許可するものとする。

(4) Web サービスの利用については、「第２章 第４節 Web サービス利用方針」を遵守すること。

第５９条 FPUnet で利用するサービスに関し、次に掲げる事項を遵守しなければならない。

(1) 電子メールの利用において、本学が管理する電子メールサーバを利用しなければならない。その他の電子メールの利用については、「第２章 第３節 電子メールサービス利用方針」を遵守しなければならない。

(2) インターネット上のサーバに Web ブラウザを用いてアクセスする場合は、必ず、本学が管理する Proxy サーバを経由しなければならない。

(3) 本学サーバゾーンにて管理される各種システムへのアクセスは、許可されたユーザ以外利用してはならない。

(4) 業務上やむを得ず、ネットワークを介して機密情報を扱う場合は、情報ネットワーク管理室の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。

(5) ネットワーク利用者は、FPUnet において、ネットワークモニターなどの、ネットワーク上を流れるパケットを盗聴できる機器およびソフトウェア使用してはならない。但し、情報統括責任者（ＣＩＯ）が承認した調査および監視目的のネットワーク IDS やネットワークモニターなどの利用はできることとする。

(6) ネットワーク利用者は、FPUnet サーバへのアクセス用の ID およびパスワード、証明書は適切に管理しなければならない。特にパスワードの選択および使用については、「第３章 第４節 ユーザ認証に関する方針」に基づいたものを利用しなければならない。

第６０条 FPUnet の接続時に関し、次に掲げる事項を遵守しなければならない。

(1) 自宅や、他組織のネットワークへ接続したパソコンは、ウイルス検査とセキュリティ検査を実施し、異常が発見されなかった後でなければ、学内ネットワークに接続してはならない。

(2) ネットワーク利用ユーザは、学内ネットワークに接続中のコンピュータを、情報ネットワーク管理室の許可の無い電話回線、携帯電話、PHS、無線 LAN、専用線などを利用して、学外のネットワークへ接続してはならない。

第６１条 ネットワーク利用状況の記録・保管許可に関し、次に掲げる事項を遵守しなければならない。

(1) ネットワークの利用状況は、情報ネットワーク管理室によって記録・保管されていることを承諾しなければならない。

第８節 外部公開サーバに関する方針

（外部公開サーバに関する方針の趣旨）

第６２条 本方針は、外部へ公開するサーバに関して、セキュリティレベルの維持と公開情報の適切性の確保を目的とする。

（外部公開サーバに関する方針の対象者）

第６３条 本方針の対象者は、 情報ネットワーク管理室以外の外部公開サーバ管理者

（外部公開サーバに関する方針の対象システム）

第６４条 本方針の対象システムは、 インターネットに接続し、不特定多数のインターネットユーザに IP アドレスおよび情報を公開する情報システム、情報機器を対象とする。(ウェブサーバ、メールサーバ、FTP サーバ、DNS サーバ、プロキシサーバ、データベースサーバ等)

（遵守事項）

第６５条　外部サーバ公開に関し、次に挙げる事項を遵守しなければならない。

(1) 外部公開サーバの管理者は、外部公開サーバの設置の際、以下の項目を情報ネットワーク管理室に申請し許可を受けなければならない。

・システム設置の趣旨と扱う情報の内容
・システム構成
・システムの設置場所の住所と組織名称
・セキュリティ責任者名
・運用開始希望日

(2) 外部公開サーバの管理者（以下、サーバ管理者）は、外部公開サーバの設置の目的と当該サーバにて公開される情報を明確にしなければならない。また公開される情報に「個人情報、プライバシー情報」などを含む場合は、「第３章 第５節 個人情報保護方針」を遵守しなければならない。

(3) サーバ管理者は、外部公開サーバから容易に学内ネットワークへアクセスできないように設計しなければならない。

(4) サーバ管理者は、必要最低限のアクセスのみ許可するようアクセス制御を実施し、OS のアクセス制御とアプリケーションとサービス、格納データへのアクセス制御を厳密に設定しなければならない。

(5) サーバ管理者は、常に最新のセキュリティ情報を入手し、OS およびインストールされた、アプリケーション・サービスについて、随時、必要な最新のアプリケーションのバージョン、セキュリティ修正プログラムを適用しなければならない。

(6) 各サーバにて、業務上必要な情報を公開する場合には、情報自体のアクセス権限を明確にし、IP アドレスや、ID、パスワードなどを利用したアクセス制御を必ず行わなければならない。このときファイルやアプリケーションをアップロードする場合には、必ずウイルスチェックを実施しなければならない。

第９節　WWW ホームページ作成に関する方針

（WWW ホームページ作成に関する方針の趣旨）

第６６条　本方針は、本学に設置されているコンピュータを利用して、WWW ホームページを作成し運用する場合の公開情報の適切性の確保を目的とする。

（WWW ホームページ作成に関する方針の対象者）

第６７条　本方針の対象者は、WWW ホームページを作成し運用する職員および学生

（責任主体の明示）

第６８条　WWWホームページを作成し運用する個人および組織は、その情報内容について責任を持つとともに、当該ホームページに責任主体としての氏名または組織名を明示しなければならない。

（遵守事項）

第６９条　WWWホームページには、次の各号に該当する情報内容を掲載してはならない。

(1) 著作権等を侵害するもの
(2) 営利を目的とするもの
(3) 個人および団体等を誹謗中傷するもの
(4) 公序良俗に反するもの

(5) その他大学の品位にふさわしくないもの

（総合調整等）

第７０条　WWWホームページの作成と運用に関する総合調整、標準化および運用の適正化等については、情報統括責任者（CIO）およびFPUnet運用管理連絡会議が当たる。

２　情報統括責任者（CIO）は、ホームページが第４の各号のいずれかに違反すると判断したときは、当該責任主体に通告するとともに、掲載の中止、その他必要な是正措置を求めることができる。

（非公開の措置）

第７１条　WWWホームページのうち、学外に公開することが適当でないと判断される情報内容については、当該責任主体において必要な措置を講じなければならない。

（記載が望ましい項目）

第７２条　WWWホームページには、以下の項目を表示することが望ましい。

(1) 責任主体の電子メールアドレス

(2) ホームページ作成日

(3) 最終更新日

(4) 著作権、転載、複写および再配布等の権利関係に関する表示

(5) 福井県立大学トップページへのリンク表示

(6) 学外からのリンクの可否に関する表示

（コンテンツの容量）

第７３条　各ホームページのトップページは、背景の画像情報等も含めて容量を２０ＫＢ程度までとすることが望ましい。ただし、送信～受信間のネットワーク回線速度が十分な場合は、この限りではない。

（権利保護）

第７４条　次の各号に該当するときは、当該権利保有者の権利を侵害することのないよう、適切な措置をとること。

(1) 書籍、雑誌等の出版物に掲載されている図画、写真等の複製および文章を全文書き写す等、正当な範囲を超えて引用する場合

(2) 他のホームページ、CD、LD、DVDなどのデジタル画像、音声、動画を複製して掲載する場合

(3) レコード、ビデオなどのアナログ画像、音声、動画をデジタル化して掲載する場合

(4) 電子通信、CD-ROM等で頒布された、著作性を有するデータベース等を再頒布する場合

(5) 複製が制限されているプログラム等を頒布する場合

(6) 特許庁に登録されている等、権利保護の対象となっている意匠、商標等を使用する場合

(7) 個人の肖像等を掲載する場合

第３章　管理者向けの方針

第１節　ネットワーク構築方針

（ネットワーク構築方針の趣旨）

第７５条　本方針は、本学のネットワーク構築をする際に必要なセキュリティに関して記載するもので、インターネット接続環境、学内 LAN 環境、WAN 環境においてネットワーク機器および各種サーバの構築の条件、および運用・管理の実施方法の遵守事項を規定する。

（ネットワーク構築方針の対象者）

第７６条　本方針の対象者は、情報ネットワーク管理室のネットワーク管理者（以下、ネットワーク管理者）

（ネットワーク構築方針の対象システム）

第７７条　本方針の対象システムは、 インターネット接続、学内 LAN、キャンパス間ネットワークで使用するネットワーク機器および各種サーバ

（遵守事項）

第７８条　ネットワーク構築全般に関し、次に掲げる事項を遵守・実施しなければならない。

(1) ネットワーク環境は、以下の 3 つの環境に分けて構築しなければならない。
- インターネットに接続するネットワーク環境(グローバルアドレスを利用したネットワークとし、グローバルゾーンと DMZ の 2 区域)
- 学内に設置する LAN を利用した学内 LAN 環境（プライベートアドレスを利用したネットワークとし、サーバゾーンと各教室・研究室、情報演習室、事務室ゾーンの 4 区域）
- 専用線を利用したキャンパス間ネットワーク環境

(2) ネットワーク構築のための機器は、以下に示す機器とする。
- 通信制御装置(ルータ、ハブ、スイッチ(レイヤ 3、レイヤ 2)、負荷分散装置、VPN 装置等
- ファイアウォール
- インターネットサーバ(DNS サーバ、WWW サーバ、メールサーバ、Proxy サーバ、ウイルス対策サーバ、FTP サーバ等)
- イントラネットサーバ(WWW サーバ、LDAP サーバ、ファイルサーバ、プリンタサーバ、ウイルス対策サーバ、業務サーバ)
- 認証サーバ、不正アクセス監視サーバ、稼動監視サーバ、時刻同期サーバ

(3) インターネット接続環境に接続する機器は、ルータ、スイッチングハブ、サーバとする。

(4) インターネット接続環境には、不正アクセス防止機能を設置し、通信監視を行って、不正アクセスを検出した場合には速やかに情報ネットワーク管理室に報告しなければならない

(5) 主要な機器は、ログ採取とネットワーク監視を実施すること。

(6) パスワードの設定が可能な機器には、「第 3 章 第 4 節 ユーザ認証方針」に準拠すること。

(7) アクセス制御の設定が可能な機器には、特定の機器からのみ接続可能な設定をすること

(8) 各機器は、設置場所・接続機器状況・管理者を明確にすること。

(9) 主要なサーバ(インターネットサーバ・イントラネットサーバ)は、情報ネットワーク管理室管理のコンピュータ室（以下、サーバルーム）に構築するサーバ専用セグメントに接続すること。

第７９条　インターネット接続環境に関し、次に掲げる事項を遵守・実施しなければならない。

(1) ネットワーク構成に関して以下の事項を装備しなくてはならない。

・ルータによるインターネットプロバイダ接続とし、プロバイダ側のネットワークはグローバルアドレスを利用しなければならない。

・プロバイダと本学の境界にファイアウォールを設置し、不正アクセスの対策をしなければならない。

・ファイアウォールには、DMZ を用意し公開用サーバを設置できるようにしなければならない。

・ファイアウォールでは、特別な場合を除きグローバルアドレスとプライベートアドレスの変換を行うこと。

・外部への Web アクセスおよびファイル転送は、Proxy サーバを経由すること。

・外部とのメールの送受信は、ウイルス対策サーバを経由しウイルスチェックをすると共に不正中継対策を実施すること。

・インターネットサーバは、情報ネットワーク管理室が指示する OS および修正プログラムの適用をし、常に最新のセキュリティ対策を実施しなければならない。

(2) インターネット接続において次のサービスを提供しなければならない。

・WWW サービス

・電子メールサービス

・ドメインネームサービス

・ファイル転送サービス

・時刻同期サービス　等

第８０条　学内ＬＡＮ環境に関し、次に掲げる事項を遵守・実施しなければならない。

(1) ネットワーク構成に関して以下の事項を装備しなくてはならない。

・スイッチングハブ(レイヤ 3、レイヤ 2)とハブを使用したネットワークとする。

・ネットワーク制御を行う機器は、サーバルーム、各棟 EPS 等に設置すること。

・ネットワークセグメント間は、アクセス制限を実施し不正アクセスを防止しなければならない。

・ネットワーク機器に対しては、通信状態・稼動状況の監視を実施すること。

・使用するアドレスは、プライベートアドレスを利用すること。

(2) 学内 LAN 環境において次のサービスを提供しなければならない。

・WWW サービス

・イントラネット(学内事務システム等)

・ファイル共有サービス

・プリンタ共有サービス

・電子メールサービス　等

第８１条　キャンパス間ＷＡＮ環境に関し、次に掲げる事項を遵守・実施しなければならない。

(1) ネットワーク構成に関して以下の事項を装備しなくてはならない。

・ルータによる専用線接続とし、接続先は学内拠点(各キャンパス、各研究センター)とする。

・ネットワークセグメント間は、アクセス制限を実施し不正アクセスを防止しなければならない。

・ネットワーク機器に対しては、通信状態・稼動状況の監視を実施すること。

・使用するアドレスは、プライベートアドレスを利用すること。

(2) キャンパス間ＷＡＮ環境において次のサービスを提供しなければならない。

・WWW サービス

・イントラネット(学内各業務システム)
・ファイル共有サービス
・電子メールサービス

第８２条　リモートアクセス環境に関し、次に掲げる事項を遵守・実施しなければならない。

(1) 接続構成に関する事項。
・リモートアクセス時に利用者認証を行い、通信履歴の記録を行わなければならない。
・接続形態として、コールバックと VPN(暗号化)に対応していなければならない。
・一定時間無通信の場合は、接続を遮断する機能を実施すること

(2) 提供サービスは少なくとも次の事項を実施しなければならない。
・学内向け WWW サービス
・ファイル転送サービス
・電子メールサービス

第２節　サーバ管理方針

（サーバ管理方針の趣旨）

第８３条　本方針は各サーバ OS を含めたソフトウェア、ハードウェア、および運用管理を規定し、サーバに格納されている情報の保護を目的とする。

（サーバ管理方針の対象者）

第８４条　本方針の対象者は、 情報ネットワーク管理室のサーバ管理者（以下、サーバ管理者）

（サーバ管理方針の対象システム）

第８５条　本方針の対象システムは、 全学共同利用のサーバシステム

（遵守事項）

第８６条　サーバの導入に関し、次に掲げる事項を遵守しなければならない。

(1) サーバ管理者はシステムの設置場所を情報ネットワーク管理室管理のコンピュータ室（以下、サーバルーム）または、それに準ずる安全な場所に設置しなければならない。

(2) サーバ管理者は情報システムの正しく安全な運用を確実にするために、管理体制および運用責任者を明確にしなければならない。人的不注意および故意の誤用のリスクを低減するために、サーバ管理者およびオペレータを複数名置くことが望ましい。

(3) サーバ管理者はサーバの設置申請時に運用手順・障害対応手順書を作成しなければならない。

(4) 本方針が適用される以前のサーバについては、速やかに本方針に適合するようにしなければならない。

第８７条　サーバの環境設定に関し、次に掲げる事項を遵守しなければならない。

(1) サーバ管理者はサーバで使用する OS および、ソフトウェア(ウイルス対策ソフト、脆弱性検査ソフトを含む)はメーカ等によるサポートが可能なものを使用しなければならない。

(2) サーバ管理者はサーバで使用されるソフトウェアは常に最新の OS、最新のアプリケーション、最新のセキュリティ修正プログラムの適用、不要なサービスの削除を行わなければならない。

(3) サーバ管理者は OS のアクセス制御、ファイルのアクセス制御、アプリケーション、サービスのアクセス制御に関して、厳密にアクセス権を設定しなければならない。

(4) サーバ管理者はユーザ、WEB アクセスなどに使用する匿名ユーザアカウントを含む全てのアカウントのアクセス権限に対して、必要最低限のアクセス権限のみ許可しなければならない。

(5) サーバ管理者は、CGI、API などのアプリケーション開発を行うまたは委託する場合、仕様書の段階から、入力データの正当性チェック、内部データの処理プロセス、出力データの妥当性など、セキュリティ対策を十分に検討しなければなければならない。

(6) サーバ管理者は、サーバの趣旨、用途に応じた必要最低限のアプリケーション・サービス以外インストールしてはならない。

(7) サーバには、推測困難なパスワードを設定しなければならない。特にサーバ管理者もしくはサーバ管理者に類する権限を持つアカウントのパスワードは、厳重に管理されなければならない。

第８８条　サーバの運用に関し、次に掲げる事項を遵守しなければならない。

(1) サーバ管理者はサーバで使用されるソフトウェアは常に最新の OS、最新のアプリケーション、最新のセキュリティ修正プログラムの適用、不要なサービスの削除を常に行わなければならない。

(2) サーバ管理者は常にウイルス定義ファイル、ウイルス対策システムが最新のものとなるよう情報を収集し、更新があった場合は直ちに反映を行い、サーバのウイルスチェックを行わなければならない。

(3) サーバ管理者はサーバのパスワードを定期的に変更しなければならない。

(4) サーバ管理者はサーバのログの定期的に取得・解析・保存を行わなければならない。

(5) サーバ管理者は定期的に以下の検査を行わなければならない。

・脆弱性検査ソフトによる最新の脆弱性情報を含む検査

・不要なアクセス権、アカウントが存在しない事

・不要なサービスが存在しない事

(6) 検査によりセキュリティの不備が発見された場合は直ちに不備を是正しなければならない。

(7) セキュリティ侵害が発生した場合、セキュリティ侵害時の対応手順に則って対応しなければならない。 また、サーバ管理者は、セキュリティ侵害の状況を情報統括管理者（CIO）に報告しなければならない。さらに必要な情報を、学内へ通報しなければならない。

(8) 想定外のセキュリティ侵害が発生し、セキュリティ障害時の対応手順のみでは状況の改善が見込めない場合、手順書外の行為を行うことができる。但し、作業実施記録は詳細に記録し、CIO に報告しなければならない。さらに必要な情報を、学内へ通報しなければならない。

第８９条　サーバルームの物理的セキュリティに関し、次に掲げる事項を遵守しなければならない。

(1) サーバルームは、危険物保管場所、火気施設、水道設備等、災害のリスクの大きい場所からは遠ざけて設置しなければならない。

(2) サーバルームの出入は原則 1 箇所に限定し、施錠設備を設けなければならない。

(3) サーバルームには設置する機器・設備の重要度に応じて、防犯カメラ、侵入報知機等の防犯設備設置および、非常電話、非常ベル等の非常用連絡設備を設置することが望ましい。

第９０条　サーバルームの運用に関し、次に掲げる事項を遵守しなければならない。

(1) サーバルームは職員不在時には施錠しなければならない。

(2) サーバルームへの入室は、認証装置(入館カード、パスワード入力、生体認証)等によって特定の登録メンバに制限し、入退室履歴は記録しなければならない。

(3) サーバルームへの未登録者の入室および作業実施については管理責任者の許可と登録メンバの同伴がなければならない。

(4) 入室不要となったメンバは速やかに削除し、入室のための認証を無効にしなければならない。

(5) サーバルームで長時間作業を行う場合は単独ではなく、複数名で行うようにしなければならない。

(6) サーバルームで許可なく撮影・録音を行ってはならない。
(7) サーバルームに不必要のないものを置いてはならない。
(8) サーバルーム内の機器・設備の有無、配置、利用状況等は定期的に点検しなければならない。

第９１条　修正プログラム適用のルールに関し、次に掲げる事項を遵守しなければならない。

(1) サーバ管理者は、「第３章 第９節 セキュリティ情報収集および配信方針」基づいて情報ネットワーク管理室より配信された修正プログラム適用の指示に対して、自分が管理または使用している全ての機器に対して速やかに適用作業・検討をしなければならない。
(2) 適用作業によるサービスの停止など他システムへの影響が大きく、速やかに適用出来ない場合、サーバ管理者は適用計画を作成し、それに基づいて作業しなければならない。
(3) 修正プログラム等を適用する場合、サーバ管理者は修正プログラム概要とその理由を記録・保管しなければならない。

第９２条　サーバのバックアップに関し、次に掲げる事項を遵守しなければならない。

(1) 業務上重要なサーバ(WWW サーバ、Mail サーバ、学内事務システムなど)については、そのデータおよび稼動履歴等を定期的にバックアップしなければならない。
(2) 修正プログラムの適用など、サーバのシステムに対して何らかの変更を行う場合、変更後の不具合が発生する可能性がある。その為、サーバに対して変更を行う前にサーバのシステムバックアップを取らなければならない。
(3) 修正プログラムの適用など、サーバのシステムに対して何らかの変更を行った場合は、安定動作確認後にサーバのシステムバックアップを取らなければならない。
(4) バックアップ作業は業務に影響が及ばないように作業時間は十分に配慮しなければならない。
(5) バックアップ媒体はテープ形態が望ましい。
(6) 過去数回分のバックアップデータを保持することが望ましい。
(7) バックアップに使用する媒体は、鍵付きの保管場所に置くなど、厳重に管理しなければならない。
(8) バックアップに使用した媒体の破棄は、復元不可能な状態で、確実に行わなければならない。

第９３条　システムの監視に関し、次に掲げる事項を遵守しなければならない。

(1) サーバ管理者は、システム障害等の兆候をいち早く見つけるために、サーバおよびネットワークの監視を行わなければならない。

第３節　アカウント管理方針

（アカウント管理方針の趣旨）

第９４条　情報システムを利用する場合に使用するユーザＩＤ・パスワード等（以下、アカウント）は必要なユーザにのみ発行され、必要最小限の権限が与えるなど、セキュリティを保つ為に、本方針を遵守しなければならない。

（アカウント管理方針の対象者）

第９５条　本方針の対象者は、(1) 情報ネットワーク管理室のアカウントの管理者（以下、アカウント管理者)、(2) アカウントを受けている学生・職員

（アカウント管理方針の対象システム）

第９６条　本方針の対象システムは、 アカウントを使用している情報システム

（遵守事項）

第９７条　新規アカウントの発行に関し、次に掲げる事項を遵守しなければならない。

(1) 新規のアカウントが必要になった場合には、アカウント管理者に申請する。
(2) 申請を受けたアカウント管理者は、必要最小限のアクセス権限と、「第３章 第４節 ユーザ認証方針」に従ったパスワードを設定しなければならない。

第９８条 アカウントの変更に関し、次に掲げる事項を遵守しなければならない。
(1) アカウントに与えられている権限を変更する場合には、新規アカウントの発行と同様にアカウント管理者に申請する。
(2) 特に、権限の縮小が行われた場合には、業務上の不都合とは関係なく、セキュリティ上の理由から、速やかにアクセス権限の変更を行わなければならない。

第９９条 不要となったアカウントの削除に関し、次に掲げる事項を遵守しなければならない。
(1) 学籍異動、人事異動などで不要となったアカウントは、速やかに削除・停止しなければならない。
(2) 学籍担当は、退学や休学などでアカウントが不要になった場合には、速やかにアカウント管理者に通知し、アカウントを削除・停止しなければならない。
(3) 人事担当は、退職や休職などでアカウントが不要になった場合には、速やかにアカウント管理者に通知し、アカウントを削除・停止しなければならない。

第４節 ユーザ認証方針

（ユーザ認証方針の趣旨）

第１００条 本方針は、情報を守る為に使用されるユーザ認証に関して、セキュリティを確保しつつ利便性を実現する運用を目的とする。

（ユーザ認証方針の対象者）

第１０１条 本方針の対象者は、情報ネットワーク管理室のサーバ管理者（以下、サーバ管理者）情報ネットワーク管理室のネットワーク管理者（以下、ネットワーク管理者）

（ユーザ認証方針の対象システム）

第１０２条 本方針の対象システムは、 以下のいずれかに該当する機器、システムおよびアプリケーション
(1) 汎用的に使われている OS などでネットワーク機能を持つ機器
(2) ハードディスクなどの記憶媒体を持つ機器
(3) ルータ
(4) ユーザが用いるメールソフトウェア
(5) 学内情報システム

（遵守事項）

第１０３条 ユーザ認証を用いたセキュリティ確保に関し、次に掲げる事項を遵守しなければならない。
(1) 情報セキュリティの確保が必要な機器、システムおよびアプリケーションは、すべてユーザ認証を行なわなければならない。

第１０４条 対象システムにおける認証システムの選定に関し、次に掲げる事項を遵守しなければならない。
(1) サーバ・ネットワーク管理者は、対象システムの重要性と、セキュリティ確保のコストを考慮してパスワード、生体認証等のユーザ認証システムを構築しなければならない。

第１０５条 パスワードに関し、次に掲げる事項を遵守しなければならない。
(1) 8 文字以上で 3 種類以上の文字種を 1 種類以上含む構成が望ましい。

(2) 英単語や本人の属性など、推測されやすいパスワードを使用してはならない。
(3) 設定されたパスワードは最長でも１年に一度、更新することが望ましい。
(4) パスワードは原則として該当システムの管理者が生成して管理を行うものとする。
(5) パスワードを口外するとか、ヒントとなるような物品を身の回りに置いておいてはならない。

第１０６条　パスワードの初期設定に関し、次に掲げる事項を遵守しなければならない。
(1) 利用者が最初に使用する初期設定のパスワードは、サーバ管理者が発行し、口頭もしくは書面で該当者に通知する。
(2) 初期設定のパスワードは、規則性のある予測できるものに設定してはならない。
(3) 利用者はパスワードが発行後、速やかに自らログインしパスワードを変更しなければならない。

第１０７条　パスワードを忘れた場合の処置に関し、次に掲げる事項を遵守しなければならない。
(1) 利用者がパスワードを忘れた場合は、既存のパスワードを廃棄し、新規パスワードを発行しなければなければならない。
(2) サーバ管理者は、申請者の本人確認を何らかの方法で確認しなければならない。

第１０８条　生体認証に関し、次に掲げる事項を遵守しなければならない。
(1) 生体認証の方式は、最新技術動向やコストなどを勘案して、選択しなければならない。
(2) 生体認証を使用する場合は、生体認証のデータそのものが重要な個人情報であるので、厳重に管理しなければならない。
(3) サーバルームなどの高いセキュリティを要求される入退室管理には、高レベルのセキュリティを実現する認証システムを用いなければならない。

第５節　個人情報保護方針

（個人情報保護方針の趣旨）

第１０９条　本方針は、情報システムが取り扱う個人情報の収集・維持・破棄における注意事項をまとめ、発生しうる問題を未然に防ぐことを目的とする。

（個人情報保護方針の対象者）

第１１０条　本方針の対象者は、個人情報が含まれる情報システムを利用するすべての職員

（個人情報保護方針の対象システム）

第１１１条　本方針の対象システムは、 個人情報を取り扱うすべてのシステム

（遵守事項）

第１１２条　個人情報を取り扱う部門の特定に関し、次に掲げる事項を遵守しなければならない。
(1) 情報統括責任者（ＣＩＯ）は、本学で個人情報を取扱う部門を特定し、その部門長に対して、遵守事項を徹底しなければならない。
(2) 特定されていない部門においては、個人情報を取扱ってはならない。

第１１３条　個人情報管理責任者の設置に関し、次に掲げる事項を実施しなければならない。
(1) 個人情報の収集・維持・破棄を行う部門の部門長は、個人情報管理責任者を設置し、部門の責任者を明確にしなければならない。

第１１４条　個人情報保護方針の公開に関し、次に掲げる事項を遵守しなければならない。
(1) 個人情報管理責任者は、個人情報を広く一般から収集する場合、本学の Web サイト等に本学の個人情報保護方針を公開しなければならない。
(2) 個人情報保護方針には、遵守事項の内容および本学への連絡先を明確にしなければならない。

第１１５条　個人情報の収集に関し、次に掲げる事項を遵守しなければならない。

(1) 個人情報の収集時には、対象者に対して利用目的を明示し、本人から同意を得なければならない。なお、収集以外の形で得た個人情報を利用する場合は改めて本人から同意を得なければならない。

(2) 対象者に示した利用目的に関する情報以外を収集してはならない。

(3) 収集した情報を対象者に提示した利用目的以外の利用をしてはならない。

第１１６条　個人情報の維持に関し、次に掲げる事項を遵守しなければならない。

(1) 個人情報に対する登録・参照・変更・削除の実施可能な者を限定し、個人情報へのアクセス制限を実施しなければならない。

(2) 個人情報を利用する場合、正確な情報を利用するため、データ保護策を実施しなければならない。

(3) 本人から当該個人情報に関する開示・訂正・削除の要求があった場合、これに対応しなければならない。

第１１７条　個人情報の破棄に関し、個人情報管理責任者は、以下の事項を遵守しなければならない。

(1) 個人情報を破棄する場合、第三者の目にさらされないように注意して破棄しなければならない。

(2) 電子媒体等の破棄は、電子的に復元できない状態にしなければならない。

第１１８条　対象者からクレーム処理に関し、個人情報管理責任者は、以下の事項を遵守しなければならない。

(1) 本学の業務において対象者からクレームを受けた場合には、速やかに対応しなければならない。

(2) 個人情報が漏えいしてしまったなど必要がある場合、ＣＩＯに連絡し、本学の見解を迅速に明確にしなければならない。

第６節　情報システム・ネットワーク監視方針

（情報システム・ネットワーク監視方針の趣旨）

第１１９条　本方針は、本学情報システムの監視について規定し、システム障害、不正アクセスの兆候等を検知し、それらの原因究明を円滑に行うことを目的とする。

（情報システム・ネットワーク監視方針の対象者）

第１２０条　本方針の対象者は、情報ネットワーク管理室のサーバ管理者（以下、サーバ管理者）情報ネットワーク管理室のネットワーク管理者（以下、ネットワーク管理者）

（情報システム・ネットワーク監視方針の対象システム）

第１２１条　本方針の対象システムは、 情報ネットワーク管理室が管理するサーバ、およびネットワーク機器

（遵守事項）

第１２２条　対象システムのログ等による監視に関し、次に掲げる事項を遵守しなければならない。

(1) サーバ・ネットワーク管理者は、将来起こりうる調査やアクセス制御の監視に役立てるため、対象システムに関してアクセス時刻、発信元・発信先アドレスとポート番号、アクセス成功・失敗、認証成功・失敗等のログを取得し、一定期間、保管すること。

(2) サーバ・ネットワーク管理者は、許可された処理だけが実行されていることを確認するために、ログを定期的に解析すること。解析の結果、以下のような事象が確認された場合、情報統括責任者（ＣＩＯ）に報告すること。

・連続したアクセスの失敗

・連続した認証の失敗

・大量のデータの送受信
・権限外の処理の試み
・ユーザアカウントに関する不正な変更(追加、削除、グループ変更等)
・アクセス権の不正な変更

(3) サーバ・ネットワーク管理者は、ログ解析により、不正アクセスの疑いがある場合には、「第３章 第１０節 セキュリティインシデント報告、対応方針」に基づいて、原因究明、再発防止計画の作成等、適切な対応を実施しなければならない。

(4) サーバ・ネットワーク管理者は、ログの時間情報を適切に保ち、ログの証拠としての有効性を高めるため、NTP サーバ等を用いてシステム間の時刻同期をとらなければならない。

(5) サーバ・ネットワーク管理者は、ログのバックアップを、一定期間、適切に保管しなければならない。

第１２３条 侵入検知システムによる監視に関し、次に掲げる事項を遵守しなければならない。

(1) 本学のグローバルゾーンおよび DMZ のネットワークにおいては、ネットワーク監視型侵入検知システムを導入し、不正アクセスの発生状況を常時監視すること。

(2) 本学のグローバルゾーンおよび DMZ 上に設置されている DNS サーバ,WWW サーバ、Mail サーバ等においては、ホスト監視型侵入検知システムを導入し、不正アクセスの発生状況を常時監視すること。

(3) サーバ・ネットワーク管理者は監視によって、不正アクセスの兆候が検知された場合には、「第３章 第１０節 セキュリティインシデント報告・対応方針」に基づいて、速やかに対応しなければならない。

(4) サーバ・ネットワーク管理者は、保管している侵入検知システムのログを定期的に分析し、結果を情報統括責任者（ＣＩＯ）に報告しなければならない。

(5) サーバ・ネットワーク管理者は、学内－学外間、および学内間に対する全ての通信に対し、次の事項に関してはリアルタイムで監視することが望ましい。

・ 許可されていない通信先への接続、接続先 URL
・ 本学 Web サーバに対する通信状態
・ 量的に異常な電子メールの送受信状態
・ ダウンロード・アップロードするファイルの転送状態
・ ウイルス侵入

第１２４条 対象システムのログの取り扱いに関し、次に掲げる事項を遵守しなければならない。

(1) サーバ・ネットワーク管理者は、ログ解析の際に、個人情報・プライバシー情報の部分については、解析の過程でやむをえない場合を除いて参照してはならない。

(2) サーバ・ネットワーク管理者は、ログの保管について、情報漏洩を防ぐため厳重に行わなければならない。

第７節 ソフトウェア・ハードウェアの購入および導入方針

（ソフトウェア・ハードウェアの購入および導入方針の趣旨）

第１２５条 本方針は、業務使用を目的としたソフトウェア・ハードウェアの必要仕様を定めて運用管理することにより、全学的に統一されたセキュリティ対策の実現を容易にし、管理の効率化を図り、導入時の設定ミス等を防止することを目的とする。

（ソフトウェア・ハードウェアの購入および導入方針の対象者）

第１２６条　本方針の対象者は、業務使用を目的としたソフトウェア・ハードウェアの購入・導入を行うすべての学生・職員を対象とする。

（ソフトウェア・ハードウェアの購入および導入方針の対象システム）

第１２７条　本方針の対象システムは、業務使用を目的として導入するソフトウェア・ハードウェア(パソコン、ネットワーク機器、OS、アプリケーションソフトウェア等)

（遵守事項）

第１２８条　機能・製品一覧の作成に関し、次に掲げる事項を遵守しなければならない。

(1) 情報ネットワーク管理室のネットワーク管理者（以下、ネットワーク管理者）は、利用サービスごとに以下の内容の一覧を作成し、通知しなければならない。

・パソコンの最低限の性能、必須のソフトウェア（ＯＳ、ウイルス対策ソフトウェア等）

・不具合が生じるネットワーク機器（ルータ、スイッチングハブ等）

(2) ネットワーク管理者は、機能・製品一覧を定期的に見直さなければならない。

(3) ネットワーク管理者は、セキュリティ上の問題やその他のトラブルを防止するために、製品の適切な設定を検証して、設定マニュアル等を作成しなければならない。

第１２９条　指定外製品の購入・導入に関し、次に掲げる事項を遵守しなければならない。

(1) 指定外製品を購入・導入する場合は、情報ネットワーク管理者に、指定外製品を使用する理由、製品名、製品の種類、連絡者等の事項を通知しなければならない。

(2) 指定外製品の通知を受けた情報ネットワーク管理者は、機器の安全性を判断しなければならない。

(3) ネットワーク管理者は、既存の情報システムにセキュリティ上やその他のトラブルが発生した場合、指定外製品の購入・導入を行う者に対し、当該製品の設定変更や学内ネットワークからの切り離し、当該製品の使用停止等を指示することができる。

第８節　外部委託契約に関する方針

（外部委託契約に関する方針の趣旨）

第１３０条　本方針は、情報システムの開発・運用業務を外部の業者に委託し、実施する場合の契約における問題および委託作業時の問題を未然に防ぐことを目的とする。

（外部委託契約に関する方針の対象者）

第１３１条　本方針の対象者は、委託契約を行う職員

（外部委託契約に関する方針の対象システム）

第１３２条　本方針の対象システムは、委託業務に附するシステム

（遵守事項）

第１３３条　委託契約に関し、次に掲げる事項を遵守しなければならない。

(1) 委託契約を行う職員は、委託業務の仕様の他、以下の契約事項を盛り込まなければならない。

・機密保持に関する事項

・情報管理に関する事項

・品質管理に関する事項

・その他、必要性のある事項

第１３４条　情報管理に関し、次に掲げる事項を遵守しなければならない。

(1) 委託業者の情報管理責任者を明確にしなければならない。

(2) 委託業者の情報管理体制を明確にしなければならない。
(3) 委託業者と各種情報の授受状況を明確にしなければならない。
(4) 委託業者の情報を閲覧・利用できる者を特定し、明示しなければならない。

第１３５条　品質管理に関し、次に掲げる事項を遵守しなければならない。
(1) 委託業者の作業スケジュールを事前に確認し、進捗状況を把握しなければならない。
(2) 委託業者の品質管理のために実施する事項を明確にしなければならない。

第９節　セキュリティ情報収集および配信方針

（セキュリティ情報収集および配信方針の趣旨）

第１３６条　本方針は、学内で使用されている情報機器・ソフトウェアのセキュリティ情報を収集し、セキュリティレベルを維持する事を目的とする。

（セキュリティ情報収集および配信方針の対象者）

第１３７条　本方針の対象者は、情報ネットワーク管理室のネットワーク管理者（以下、ネットワーク管理者）

（セキュリティ情報収集および配信方針の対象システム）

第１３８条　本方針の対象システムは、 本学に導入されているすべてのソフトウェアおよびハードウェア

（遵守事項）

第１３９条　セキュリティ情報の収集に関し、次に掲げる事項を実施しなければならない。
(1) ネットワーク管理者は、学内に導入されているハードウェアおよびソフトウェアのセキュリティ情報について、定期的に情報を収集しなければならない。
(2) セキュリティ情報は各ベンダーの Web サイトやサポートページなどから収集する。
(3) ネットワーク管理者はセキュリティ関連のメーリングリスト、セキュリティセミナーなどに参加し情報を収集する。
(4) 収集した情報は、重要性、影響範囲などから、
- 危険度－高:サーバの管理権限の剥奪などにより、業務が停止してしまう、 または相手先などに影響を与える可能性があり、即座に対応 が必要な情報
- 危険度－中:業務が停止するあるいは相手先などに影響は与えないため、 即座に対応する必要はないが、定期メンテナンス時などに対処する必要がある情報
- 危険度－低:特殊な環境・設定でのみ発生し、学内のシステムには関係がないため、特に対処しなくともよい情報

に区別し、対処しなければならない。

第１４０条　セキュリティ情報の配信に関し、次に掲げる事項を遵守・実施しなければならない。
(1) ネットワーク管理者は、収集した情報を危険度に応じて関係者に連絡しなければならない。
- 危険度－高:発見次第即座に関係者全員に電子メール、電話等で連絡する。
- 危険度－中:週１回程度の定例報告（メール等）にて関係者全員に連絡する。
- 危険度－小:年数回程度の定期報告を行う。

(2) ネットワーク管理者より通知を受けた者は速やかにその指示に従わなければならない。修正プログラムを適用が必要な場合は「第３章 第２節 サーバ管理方針」、ウイルス定義ファイルを更新する場合には「第２章 第２節 ウイルス対策方針」に基づいて行わなければならない。

(3) ネットワーク管理者は、以下の情報を周知しなければならない。

・ サーバ設置時の OS の適用修正プログラム一覧
・ サーバ設置時に必要となるサービスなどをまとめたセキュリティ設定チェックリスト
・ アプリケーションの適用修正プログラム一覧
・ アプリケーションの実装変更

第１０節　セキュリティインシデント報告・対応方針

（セキュリティインシデント報告・対応方針の趣旨）

第１４１条　本方針は、業務システム・サーバにおいて次の各号に示すセキュリティインシデント（情報セキュリティに関する人為的事象）が発生した場合に迅速に対応し、円滑に業務継続がなされることを目的とする。

(1) 不正アクセスによる情報漏洩、職員による情報漏洩、ウイルス感染、 なりすまし、使用不能攻撃、ハードウェア紛失

(2) 電源異常、機器の熱暴走・破損等のシステム・ネットワークの故障

（セキュリティインシデント報告・対応方針の対象者）

第１４２条　本方針の対象者は、各業務システムの管理者

（セキュリティインシデント報告・対応方針の対象システム）

第１４３条　本方針の対象システムは、本学の業務システム

（遵守事項）

第１４４条　平時の準備に関し、次に掲げる事項を実施しなければならない。

(1) 業務上、利用するすべてのコンピュータについて、「第２章 第２節 ウイルス対策方針」に基づき、適切にウイルス検査を実行しなければならない。

(2) ノートパソコン・機密資料等の情報資産を紛失しないように十分、注意しなければならない。

(3) 「第３章 第９節 セキュリティ情報収集および配信方針」に基づいて、日常的にセキュリティ情報を収集し、適切な対策を実施しなければならない。

(4) 将来起こりうる調査やアクセス制御の監視に役立てるために「第３章 第６節 情報システム・ネットワーク監視方針」に基づいて、適切にログを取得しなければならない。

(5) 将来起こりうるシステムの復旧作業に役立てるために「第３章 第２節 サーバ管理方針」に基づいて、適切にバックアップを取得しなければならない。

(6) 不正アクセスを検知するため、「第３章 第６節 情報システム・ネットワーク監視方針」に基づき、侵入検知システム(IDS)を使用し、システムおよびネットワークの監視を行わなければならない。

(7) 重要なシステムに対して UPS を使用し、停電時には自動でシャットダウンを行うように設定しなければならない。

第１４５条　セキュリティインシデント発生時に関し、次に掲げる事項を遵守・実施しなければならない。

(1) 本学ではセキュリティインシデントを被害の深刻度に応じて、以下のようにレベル分けする。職員はレベルに応じた報告先に対し、速やかに報告し、指示を仰がなければならない。

・レベル 1(深刻度:低) 問題の発生原因・被害の範囲とも当学内に限定される場合
<報告先>情報ネットワーク管理室のネットワーク管理者（以下、ネットワーク管理者）
・レベル 2(深刻度:中) 学外の第三者からのセキュリティ侵害により、本学が被害者となる場合

<報告先> ネットワーク管理者、警察機関（任意)、
コンピュータ緊急対応センター(JSERT)（任意)、 情報処理振興事業協会(IPA)（任意）
・レベル 3(深刻度:高) 学外に対して、本学が加害者となる場合
<報告先> 情報統括責任者（CIO)、ネットワーク管理者、広報担当、該当する相手先

(2) ネットワーク管理者は、ウイルス感染や不正アクセスを確認次第、対象システムをネットワークから切り離し、ウイルス拡散対策を実施すること。

(3) ネットワーク管理者は、ログ・IDS の監視レポート・関係者へのヒアリング等に基づいて、速やかに被害状況を把握し、対策にあたらなければならない。

(4) ネットワーク管理者は、被害状況を把握するにあたり、「セキュリティインシデントの種類」、「被害を受けた日時」、「原因と対処方法」、「被害の拡大範囲」 を確認しなければならない。

(5) ネットワーク管理者は、侵害原因が解消された後、速やかにバックアップテープを用いてシステムを正常な状態に復旧しなければならない。

(6) ウイルス感染などが原因で OS,アプリケーションの入れ替えが必要になった場合は、適切なメディアを使用して速やかに再インストールを実施すること。

第１４６条 再発防止計画に関し、次に掲げる事項を実施しなければならない。

(1) セキュリティインシデントへの対応が完了した後、情報統括責任者（CIO）およびネットワーク管理者は、調査した被害状況をもとに再発防止計画を作成しなければならない。再発防止計画作成時には、技術的側面と組織的(制度的)側面の両方に留意すること。

(2) 再発防止計画は、すべての職員に周知され、適切に実施されなければならない。

(3) ネットワーク管理者は、セキュリティインシデントの発生から再発防止計画作成までの一連の記録を保管・管理しなければならない。

第１４７条 対応訓練に関し、次に掲げる事項を実施しなければならない。

(1) 本方針の内容の実効性を担保するため、ネットワーク管理者は、定期的にセキュリティインシデント対応訓練を計画し、すべての職員を対象とした訓練を実施しなければならない。

(2) 訓練の結果は、情報ネットワーク管理室において、レビュー、改善策の検討を実施し、改善策とともにすべての職員に周知されなければならない。

第１１節 セキュリティ教育に関する方針

（セキュリティ教育に関する方針の趣旨）

第１４８条 本方針では、セキュリティ教育、訓練に関わる事項を規定し、安全なネットワークの運用を図ることを目的とする。

（セキュリティ教育に関する方針の対象者）

第１４９条 本方針の対象者は、FPUnet を利用する学生・職員

（セキュリティ教育に関する方針の対象システム）

第１５０条 本方針の対象システムは、 本方針はセキュリティ教育に関するものであり、情報システムや情報機器を対象としない。

（遵守事項）

第１５１条 セキュリティ教育に関し、情報ネットワーク管理室は、学部等情報担当者と協力して、コンピュータを利用する学生・職員に対し、以下の説明会等を実施しなければならない。

(1) 情報ネットワーク管理室は、年 1 回程度、セキュリティに関する説明会等を実施しなければならな

い。

(2) 情報ネットワーク管理室は、新任職員に対して、着任時にセキュリティに関する説明会等を実施しなければならない。

(3) 説明には以下の内容が含まれていなければならない

・組織や個人の情報セキュリティの重要性
・セキュリティ対策
・データ所有者の責任
・モラル教育
・禁止行為に関しての教育 等

第１５２条　セキュリティ担当者向けの研修に関し、次に掲げる事項を実施しなければならない。

(1) 情報ネットワーク管理室、学部等情報担当者等は、定期的に、以下の事項についての、セキュリティ担当者向けの研修を受講しなければならない。

・セキュリティに関するリスク分析
・セキュリティ対策について
・トラブル発生時の対処・復旧について

附　則

この要領は、平成２０年４月１日から施行する。

（参考文献）

本要領を策定するにあたり以下の文献を参考にしている。

「情報セキュリティポリシーサンプル(0.91 版)」NPO 日本ネットワークセキュリティ協会(JNSA)