福山大学情報セキュリティポリシー

福山大学

平成２８年３月

目次

付録

附則

本ポリシーは，平成２８年3月９日より施行する.

１．情報セキュリティ基本方針

福山大学（以下,「本学」という.）は，教育，研究，社会連携・貢献及び管理運営等（以下「教育等」という.）の充実のために，数多くの情報資産を保有している．情報資産のき損,消失があれば,教育等の継続に大きな支障を招く可能性がある.さらには，本学は，高等教育機関であるから，学生の健全な育成等のため，数千名規模の学生の個人情報を取扱っている．その中には学生のプライバシに関するデータも含まれる．それらが漏えいした場合には，個人情報保護，プライバシ保護等の大きな問題を招く可能性がある．以上のことから，本学の情報資産を，データの消失やデータの漏えい等，種々の情報セキュリティ事故から守ることは，本学の事業の継続を守り，本学に在籍する教職員及び学生を守り，本学の社会的信用を守ることになる．すでに，本学では，情報セキュリティ対策として，技術的な対策と，人的・組織的な対策を種々講じてきた．今後も，本学においては，教育等の充実のために，情報通信技術の導入と情報資産の整備拡充を続けていくことが必要不可欠である．そのために，情報セキュリティに関する技術的な対策の包括的基準，人的・組織的な対策の包括的基準，情報資産の利活用にあたって本学の情報資産の利用者が行う標準的な行動を,情報セキュリティポリシーとして文書化し，運用していくことで，本学の情報セキュリティを適正に確保しながら，情報通信技術の導入と情報資産の整備拡充を推進する.

福山大学情報セキュリティポリシーとは,本学の情報セキュリティ基本方針および情報セキュリティ対策基準のことをいい,本学の情報セキュリティに対する基本的な考えを示すとともに，情報セキュリティに関する技術的な対策の基準，人的・組織的な対策の基準，本学の学生及び教職員等が行う標準的な行動を体系的，包括的にまとめたものである．本ポリシーは，本学が保有する情報資産の情報セキュリティの確保のために,本学の情報資産の利用者が,本学の情報資産を取扱うときの標準的な行動等に関する意思統一を行うとともに，学生の個人情報等の種々の情報を適正に取扱いながら，本学の教育等をさらに発展させ充実させるための指針となる役割を持っている.

情報セキュリティを将来にわたって適正に確保していくためには,本学における情報資産の整備拡充の進展，情報通信技術の発展，特に高等教育における情報通信技術の利活用等の状況変化にあわせ,情報セキュリティ対策を適宜更新していくことが必要になる.そのため,必要に応じて,本ポリシーの内容の充実などの改訂を行うことによって，将来にわたり，本学における情報セキュリティを適正に確保していくものとする．本学

では，利用者の自由闊達な意見表明を奨励し，本ポリシーの改善に努める．利用者は，本ポリシーが定める基本方針ならびに対策基準を理解し，支持の上，本学の情報資産を利用するだけでなく，本ポリシーが定める基本方針ならびに対策基準に不備を感じるときには，積極的に意見表明することが求められる．情報セキュリティに関して不測の事態があるときは，本ポリシーの定めが簡潔で実施に問題が無いか，十分に効率的であるか，実現困難な内容でないか，実際のリスクに応じた適正な規模の対策であるか，本学の教育等の推進を妨げてはいないかなどをあわせて確認する．

利用者は，本ポリシーの記述が，情報セキュリティの確保の妨げになると判断するときや，標準的な行動をそのまま実行しては業務や学修等の妨げになると判断するときや，標準的な行動をそのまま実行しては効率が良くないなどの問題があると判断するときは，各自，適切な行動により情報セキュリティの確保を行うものとする．同時に，積極的に意見表明を行ったり，情報セキュリティ管理者や，共同利用機器等のシステム管理者からの求めに応じて，どのような行動を実行したかの報告が行える準備をしたりすることで，情報セキュリティの向上に協力する．利用者は，本ポリシーを運用するにあたっては，本ポリシーの記述のみに固執したり，書面等での手続きの拡充のみに固執したりするような形式的なだけの運用を避ける．利用者は，本学における教育等の発展と充実，情報通信技術の発展等に伴って，本ポリシーの記述が必ずしも適切なものではなくなる可能性があり，絶えず見直しが必要であることを理解する．

情報セキュリティ管理者や，共同利用機器等のシステム管理者は，常に，最新の情報セキュリティ技術に関する調査を行いながら，本学の情報セキュリティ施策に対する一般利用者の不満や改善点の収集を行い，ときには，一般利用者に対して，本ポリシーの対策基準に記述された標準的な行動に替わる，適切な行動を具体的に提示することによって，本学の教育等をさらに発展させ充実させるものとする．さらに，学内の情報セキュリティ関連規程等について，今度も，適宜見直しを実施したり，適切な例外措置を設けたりなど，本学の教育等をさらに発展させ充実させるための適切な手段を講じるものとする．情報セキュリティ管理者や，共同利用機器等のシステム管理者が，情報セキュリティの確保や情報セキュリティ事故への対処等を目的として，種々の調査を行うときは，個々の利用者のプライバシを最大限に尊重しながら客観的な証拠等に基づく調査を実施する．このとき，調査における利用者のプライバシ保護について，調査対象者に分かりやすく書面等で説明したり，調査に関する異議申し立ての窓口を設けたりするなど

の配慮も行って，調査手続きが不備であるかのような誤解が生じることが無いように最大限の対策を講じる．情報セキュリティマネジメントの推進では，一般利用者の協力が欠かせない．情報セキュリティ管理者や，共同利用機器等のシステム管理者は，情報セキュリティの確保に伴う業務や学修上の余分な負担が，効果に見合うものであることを十分に確認しながら，一般利用者にそのことが十分に理解されるよう周知にも努めるものとする．

本ポリシーが定める対策基準等の実施を，外部業者等に全部または一部委託する場合には，本ポリシーについて十分な理解を得られるようにするとともに，情報セキュリティ事故時の連絡・即応体制について，検討せねばならないとする．

なお，情報資産の利活用にあたっては，サイバーセキュリティ，不正アクセス行為の禁止，著作権，肖像権，プライバシ保護，個人情報保護等，情報通信機器の利活用に関する関係法令を遵守することは当然のことである．また，学校法人福山大学（以下，「本法人」という）が定める「学校法人福山大学個人情報管理基本方針」，本学が定める「福山大学情報倫理規程」，利用者が属する部局等が独自に定める情報セキュリティ関連規則，共同利用機器等の利用規則，その他情報セキュリティ関連規則等を遵守することも当然のことである．また，本学の教職員や学生が，秘密保持契約のもと外部より情報資産の提供を受けている場合には，個々の秘密保持契約が定める事項を遵守することは当然のことである．これら関係法令等は，適宜，改訂され拡充されるものである．関係法令等の改訂や拡充に伴って，本ポリシー内での記述に，関係法令等との不一致が生じ，情報セキュリティ管理に関する混乱が生じることを避けるために，本ポリシーでは，関係法令等の遵守について，あえて明記は行わないものとする

本ポリシーは，本学の情報資産の利用者全てに公開する．外部業者に業務を委託するなど，公開しなければ，業務を遂行できない場合には，秘密保持契約を締結したうえで対象を限定して公開する場合がある．本学の情報セキュリティ対策等を広く説明するために，外部に本ポリシーを公開する場合には，公開することにより，本学の情報セキュリティが低下する恐れがある部分を除いて公開する場合がある．

２．定義

（１）情報セキュリティ

ISO/IEC 17799 が定める通り，情報の機密性，情報の完全性及び情報の利用の可用性のことをいう．情報の機密性とは，情報にアクセスすることを許可された者だけが情報にアクセスできるようにすることである．情報の完全性とは，保有する情報が正確であり完全である状態を維持することである．情報の利用の可用性とは，情報にアクセスすることを許可された者が，必要なときに，いつでも情報にアクセスできる状態を維持することである．

（２）脅威

機密情報や個人情報の漏えい，Ｗｅｂページ等のデータの改ざん，データの消失，情報サービスの予期せぬ停止等の，情報セキュリティの確保ができなくなる事態が発生する要因のことである．脅威には，機器の不具合や故障，情報通信機器の置忘れ・紛失や盗難，電子メールでの誤送信，Ｗｅｂでの誤公開，Ｐ２Ｐ型ファイル共有ソフトウェア等の不適切な利用，外部からの不正アクセス，不正プログラム（コンピュータウイルスやトロイの木馬等），外部の掲示板への不適切な掲載等が該当する．

（３）脆弱性

情報通信機器に関する種々の不備により，脅威の可能性が増大している状態のことである．

（４）情報セキュリティ対策

脆弱性を可能な限り軽減することにより，情報セキュリティの確保を維持し続けることである．

（５）情報セキュリティポリシー（以下，「**本ポリシー**」という．）

情報セキュリティに関する本学の考え方である情報セキュリティ基本方針と，情報セキュリティ対策基準を文書でまとめたものである．

（６）情報セキュリティ基本方針（以下，「**基本方針**」という．）

本学において情報セキュリティの確保が必要である理由，情報セキュリティの目標，その目標を達成するために本学がとるべき行動の方針を定めたものである．基本方針は，「**1**．情報セキュリティ基本方針」に記述している．

（7）情報セキュリティ対策基準（以下，「**対策基準**」という．）

情報セキュリティ対策のため，本学の情報資産の利用者が情報資産を取扱うときの情報セキュリティに関する技術的な対策の基準と人的・組織的な対策の基準，本学の情報資産の利用者が行う標準的な行動等を体系的，包括的にまとめたものをいう．対策基準は，本ポリシーの３章以降に記述している．

（8）人的・組織的な対応

情報セキュリティ対策として，人的・組織的な対応を行うことをいう．次が事項が該当する．

- 退職時や卒業時に，適切にアカウントを削除すること．
- 情報セキュリティ事故のための体制，特に再発防止策の策定や，社会的信用の維持のための体制を整備すること．
- 機密情報や個人情報の学外持ち出しに関する体制を整備すること．
- 外部業者に情報資産に関する業務を委託するときに，適切に監督を行うための体制を整備すること．

（9）情報セキュリティマネジメント

本ポリシーの運用と改善に関わる全学的な取組みのことをいう．これら活動に関わる学内の人材の育成も含む．

（１０）個人情報

生存する個人に関する情報であって，次のいずれかに該当するものをいう．

- 当該情報に含まれる氏名，生年月日その他の記述等（文書，図画もしくは電磁的記録に記載され，もしくは記録され，または音声，動作その他の方法を用いて表された一切の事項（個人識別符号を除く）をいう．）により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより

特定の個人を識別できることとなるものを含む).

- 個人識別符号が含まれるもの.

本人特定が困難なように撮影されたか加工された顔貌や風貌，表情，姿勢，視線，本人特定が困難なように計測されたか加工された身体特徴量（体重や身長や視力等），本人特定が困難なように計測されたか加工された生体計測値（血圧，血糖，体温，睡眠状態，発汗等），服装，所持品，車両の車種などは，それらだけでは，特定の個人を識別できないので個人情報にはあたらない.

（１１）個人識別符号

個人識別符号とは,次のいずれかに該当する文字,番号,記号その他の符号のうち,別途本学が定めるものをいう.

- 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字，番号，記号その他の符号であって，当該特定の個人を識別することができるもの.
- 個人に提供される役務の利用に関し割り当てられ，または個人に発行されるカードその他の書類に記載され，もしくは電磁的方式により記録された文字，番号，記号その他の符号であって，その利用または発行を受ける者ごとに異なるものとなるように割り当てられ，又は記載され，もしくは記録されることにより，特定の利用者または発行を受ける者を識別することができるもの.

指紋，顔貌（目の部分を黒塗りして個人を特定できなくするなどの匿名加工を行っていない顔貌），運転免許証番号，旅券番号，マイナンバー，基礎年金番号，保険証番号，印鑑登録証明書の印影画像は個人識別符号である.

携帯電話番号，メールアドレス，クレジットカード番号，住所，車両のナンバープレート，車両個体番号，ネットワーク通信におけるＭＡＣアドレスやＩＰアドレス，第三者が提供する情報サービス等のＩＤで本人確認が徹底されていない符号は,それら単独では，特定の利用者または発行を受ける者を識別することができないので，原則個人識別符号にはあたらない.

（１２）要配慮個人情報

本人の人種，信条，社会的身分，病歴，犯罪の経歴，犯罪により害を被った事実そ

の他本人に対する不当な差別，偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして本学が定める記述が含まれる個人情報をいう．

（１３）個人情報データベース

個人情報を含む情報の集合物であって，特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したものをいう．

（１４）個人データ

個人情報データベースを構成する個人情報をいう．

（１５）保有個人データ

本学が，開示，内容の訂正，追加または削除，利用の停止，消去及び第三者への提供の停止を行うことができる権限を有する個人データをいう．

（１６）匿名加工情報

特定の個人を識別することができないように個人情報を加工したものをいう．

（１７）プライバシ

個人の行動や私的領分にあたるもので，私物，自宅，学内でも各個人に割り当てられた居室や机やロッカー等の中身，個々の利用者が作成し保有しているデータ，個々の利用者のあらゆる通信内容，学生が修学の種々の場面で残す種々の行動を記述したデータで私的なもの（成績，進路，資格，学歴，職歴，既往歴，健康状態，健康診断結果，生活習慣や嗜好，学費支払い状況を記述したデータなど），教職員の種々の行動を記述したデータで私的なもの（既往歴，健康状態，健康診断結果，生活習慣や嗜好を記述したデータなど）など，個人の秘密にあたるものをいう．要配慮個人情報はプライバシに含まれる．通信内容はプライバシであるから，ネットワーク通信におけるＭＡＣアドレスやＩＰアドレスも，プライバシに含まれる．但し，学生の氏名，教職員の氏名，教職員の電子メールアドレス，教職員の内線番号，教職員の所属，教職員の職位，教職員の研究業績情報は，学内で公知のものであり，プライバシには含まれないものとする．教職員の資格や学歴や職歴などで，学内で公知になっているもの

は，プライバシに含まれないものとする.

（１８）情報資産

本学の「福山大学情報倫理規程」の第２条第１項が定める「情報資産」のことであり，次に掲げるものをいう.

一．本学が所有又は管理する情報ネットワーク，コンピュータ，それらに接続された情報関連機器

二．本学の教職員，学生等が所有及び管理する情報ネットワーク，コンピュータ，それらに接続された情報関連機器で、第一号に接続されているもの

三．情報ネットワーク，コンピュータ，それらに接続された情報関連機器で，本学の個人情報を扱うもの

四．情報ネットワーク，コンピュータ，それらに接続された情報関連機器で，本学を呼称しての本学外への情報発信、本学を呼称しての本学外への情報サービスを提供するもの

五．第一号から第四号において用いられるソフトウェア

六．本学の教職員，学生等が業務上又は修学上取得及び作成した情報で，第一号から第四号に記録されたもの

七．本学の教職員，学生等が業務上又は修学上取得及び作成した情報で，第一号から第四号で利用できる電磁的記録媒体に記録されたもの

（１９）利用者

本学の「福山大学情報倫理規程」の第２条第２項が定める「利用者」のことであり，本学が所有又は管理する情報資産に対する利用資格を与えられている者をいう.

（２０）情報通信機器

特に断らない場合には，情報資産のうち情報ネットワーク，コンピュータ，それらに接続された情報関連機器をいう.

（２１）共同利用機器

情報通信機器のうち，ある程度長期間にわたって，複数人で共同利用する者をいう.

一時的にＵＳＢメモリやタブレットやパーソナルコンピュータなどを貸し借りするような場合は含まれない.

（２２）個人利用機器

情報通信機器のうち，もっぱら特定の個人で利用されるか，共同利用機器であっても特定の少人数グループでのみ利用されるものをいう．個人利用機器の利用者は，その当該個人利用機器のシステム管理者でもある.

（２３）インターネットサービス公開

次の各号のいずれかに該当するものをいう.

一．利用者が自らもしくは外部業者に委託して，インターネットを利用して，学内から，外部の不特定多数に情報を発信したり，情報サービスを提供するような情報システムを設置，運用，管理する場合.

二．利用者が自らもしくは外部業者に委託して，インターネットを利用して，本学のロゴを使用したり，本学の名称を大きく表示したり，本学の公式Ｗｅｂページとデザインを統一したりなどで本学を呼称して，外部の不特定多数に情報を発信したり，情報サービスを提供するような情報システムを設置，運用，管理する場合．但し，教職員や学生による本学の敷地外での私的な活動等を本ポリシーの範囲外とするため，次に該当する場合は，本学を呼称していることには該当しないものと定める.

- 情報発信を行う発信者の所属，情報サービスの提供者の所属，利用者による著作物の所属として本学の説明が行われている程度にとどまる場合.
- 本学に関する紹介が行われている程度にとどまる場合.
- 公知でない本学の個人情報が取扱われておらず，本学を呼称しているとまでは容易に認識できない場合.

情報を発信したり，情報サービスを提供したりする情報システムには，Ｗｅｂサーバ，メールサーバ，ＳＮＳサーバ，ファイルサーバ，ＤＮＳサーバ，認証サーバなどが該当する.

（２４）インターネットサービス利用

利用者が，本学の情報ネットワークとインターネットとを利用して，外部のサービスを受けることをいう．

（２５）アップデート

特に断らない場合には，ソフトウェアを最新の状態に更新する操作のことをいう．例えば，ウイルス対策ソフトウェアのパターンファイル等を最新のものに更新したり，オペレーティングシステムのセキュリティフィックス，バグフィックスを行って最新の状態に更新したりする操作である．

（２６）バージョンアップ

特に断らない場合には，ソフトウェアを新規のバージョンに置き換えることをいう．

（２７）不正プログラム

情報通信機器の利用者の意図に反し，情報通信機器を破壊したり，情報を漏えいさせたり，広告やＷｅｂページを勝手に表示したり，他の情報通信機器への攻撃のための踏み台として機能したりなど，何らかの被害を及ぼすように作成されたプログラムをいう．但し，学術研究や教育の目的のために，関係法令等を遵守しながら作成，使用され，使用の結果，被害が発生せず，意図に反して配布や複製されることがなく，使用後にすべての複製を含めて消去され，情報セキュリティの脅威にならない場合は，不正プログラムから除外する．

（２８）コンピュータウイルス

自己複製機能を持った不正プログラムをいう．ＨＴＭＬファイル，電子メールの添付ファイル，ＷｏｒｄやＥｘｃｅｌのマクロ等の中に潜んでいたり，独立のプログラムとして動作したりする場合がある．

（２９）トロイの木馬

自己複製機能のない不正プログラムをいう．自己複製を行わないので，コンピュータウイルスよりも発見が難しい．バックドア（外部からの指令により不正な操作を行える機能），パスワードやアクセス履歴等の秘密データや個人データの窃盗，特定の

Ｗｅｂサイトへの誘導，意図に反するプログラムのダウンロード，意図に反するプログラムのインストール，意図に反するプロキシサーバ，スパム配送，ドライブバイダウンロードなど，何らかの被害を及ぼす機能を持つ．

（３０）ルートキット

トロイの木馬等の不正プログラムの存在を隠し，ウイルス対策ソフトウェア等からの検知も逃れるようにするためのプログラムをいう．

（３１）ドライブバイダウンロード

Ｗｅｂサイトを閲覧した際に、ユーザの許可なしにプログラムをダウンロード及びインストールさせることをいう．ＷｅｂサイトのＷｅｂページが改ざんされ，ドライブバイダウンロードの機能を持つプログラム等が埋め込まれた場合には，当該Ｗｅｂサイトが，不正プログラムの拡散元として機能する可能性がある．

（３２）コンピュータウイルス等のスキャン

ウイルス対策ソフトウェア等を用いて，情報通信機器内のメモリやファイル等のスキャンを行って，コンピュータウイルス，トロイの木馬やルートキットなどの不正プログラムの検知や駆除を行うことをいう．

（３３）ファイル共有ソフトウェア

インターネットで，匿名で，不特定多数とファイルのやり取りができる機能を持ったソフトウェアのことをいう．匿名であっても，限られた人数や特定の組織内でのみファイルのやり取りを行うグループウェアやオンラインストレージは該当しない．

（３４）機密情報や個人情報の学外持ち出し

本学の情報資産における機密情報や個人情報を，電磁的記録媒体などの情報通信機器に格納して，学外に持ち出すことをいう．なお，本学の情報資産における機密情報や個人情報を，インターネットで不特定多数からアクセスできるような状態に置いて情報漏えいさせて情報セキュリティ事故が発生した場合や，電子メールで不特定多数に発信して情報を漏えいさせて情報セキュリティ事故が発生した場合などは，学外持

ち出しではなく，「情報漏えい」として取扱う．

（３５）福山大学情報倫理委員会

本学の「福山大学情報倫理規程」の第５条が定める福山大学情報倫理委員会のことをいう．

（３６）福山大学情報倫理委員会委員長

本学の「福山大学情報倫理委員会規則」の第４条が定める福山大学情報倫理委員会の委員長のことをいう．

（３７）福山大学部局等情報倫理委員会

本学の「福山大学情報倫理規程」の第８条が定める福山大学部局等情報倫理委員会のことをいう．

（３８）情報セキュリティ管理者

本学の「福山大学情報倫理規程」の第７条が定める情報セキュリティ管理者のことをいう．

（３９）福山大学ファイヤウオール運用基本方針

本学の情報ネットワークと，インターネットの接続点において，ＩＰアドレス，ポート番号，プロトコル種類ごとに通信の遮断を行うファイヤウオール機器の運用基本方針について，本学共同利用センターＩＣＴサービス部門が定めた文書をいう．

（４０）遵守事項

情報セキュリティを確保するために本ポリシーが定める遵守事項をいう．

（４１）例外措置

本ポリシーが定める遵守事項に対する例外措置のことをいう．本ポリシーが定める遵守事項の実施により，教育等の推進に支障を来す場合には，利用者は例外措置を申請できるものとする．例外措置の許可権限者は，別途，定める．緊急を要する申請の

ために，別途，代理許可権限者を定める．許可権限者および代理許可権限者が不在の場合を想定して，別途，事後の許可に関する規程を定める．

（４２）標準的な行動

情報セキュリティを確保するために，一般利用者やシステム管理者だけでなく，本学の情報セキュリティマネジメントを推進する者が行うと想定される標準的な行動をいう．本ポリシーの対策基準に記述された種々の行動は，遵守事項であると特に断りのない限り，標準的な行動を記述したものである．本ポリシーでは，標準的な行動を体系的，包括的にまとめることにより，本学の情報資産を取扱うときの意思統一を行い，情報セキュリティを確保しながら，本学の教育等のさらなる発展に活用する．

３．組織体制

本学の情報セキュリティを確保する体制は次の通りである．

（１）福山大学情報倫理委員会委員長

福山大学情報倫理委員会委員長は，福山大学情報倫理委員会を主宰する．

（２）福山大学情報倫理委員会

福山大学情報倫理委員会は，次の事項を行う．

- 情報セキュリティ等に関する審議を行う．
- 情報セキュリティ事故が発生したときは，調査と審査を行い，処置を決定する．また，必要に応じて，部局等情報倫理委員会を指揮し，適切な指示を行う．

（３）部局等情報倫理委員会

部局等情報倫理委員会は，当該部局における次の事項を行う．

- 情報セキュリティ等に関する審議を行う．
- 情報セキュリティ事故が発生したときは，調査と審査を行い，処置を決定する．必要に応じて，緊急措置を執ることができる．また，福山大学情報倫理委員会からの指示があるときは指示に従う．

（４）情報セキュリティ管理者

情報セキュリティ管理者は，次の事項を行う．

一．情報セキュリティ管理者は，普段は次の業務を行う．

- 本学における情報セキュリティ対策を推進する．
- 本ポリシー等が定める本学の情報セキュリティ施策に対する利用者の不満や改善点の収集を行い，必要に応じて，福山大学情報倫理委員会，部局等情報倫理委員会，共同利用センター，その他関係する委員会等に提起する．

二．情報セキュリティ管理者は，情報セキュリティ事故の報告を受けたときは，次の業務を行う．

- 被害の拡大等を防ぐために，報告者に適切な助言や指示及び，適切な措置を執るなどの対応を行い，必要に応じ，システム管理者の協力を求める．
- 報告のあった事項について，情報セキュリティ事故の事実確認を行うとともに，可能な限り，情報通信機器内のログファイル等，調査に必要となるデータの保全作業を行う．このとき，想定される被害の重大性についての格付けを行う．
- 情報セキュリティ事故であると確認され，格付けの結果，情報セキュリティ事故の解決のために，部局等レベル，全学レベルでの調査や審査や措置が必要と判断する場合には，福山大学情報倫理委員会，部局等情報倫理委員会に調査や審査や措置を求める．
- 緊急を要する場合などに，迅速に対処できるようにするために，情報セキュリティ管理者は，独自の判断で種々の処置を行い，情報セキュリティ事故の全部または一部の解決が行えるものとする．全ての利用者は，その処置を支持し，協力する．また，情報セキュリティ事故に対して情報セキュリティ管理者が実施した処置については，福山大学情報倫理委員会あるいは部局等情報倫理委員会に事後報告し，情報セキュリティの向上に役立てる．
- 情報セキュリティ事故であると確認されたときは，その事実を文書等で記録し，将来の調査等に備える．情報セキュリティ事故の再発防止策を検討し，必要に応じて，福山大学情報倫理委員会，部局等情報倫理委員会，共同利用センター，その他関係する委員会等に提起する．

三．情報セキュリティ管理者は，福山大学情報倫理委員会，部局等情報倫理委員会からの，情報セキュリティ事故審査結果の報告に基づき，次の業務を行う．

- 適切かつ実現可能な再発防止策を立案し，必要に応じて，福山大学情報倫理委員会，部局等情報倫理委員会，共同利用センター，その他関係する委員会等に提言する．

（5）**システム管理者**

システム管理者は，情報セキュリティが確保できるように，適切にシステムを管理する．情報セキュリティ事故が発生したときは，所定の情報セキュリティ管理者に報

告するとともに，調査や措置に協力する．

（６）**利用者**

一般利用者は，情報セキュリティが確保できるように，適切にシステムを利用する．情報セキュリティ事故が発生したときは，所定の情報セキュリティ管理者に報告するとともに，調査や措置に協力する．

（７）**共同利用センター**

共同利用センターは次の業務を行う．

- 共同利用機器のうち，共同利用センターが管理する者についてのシステム管理
- 各種情報サービスの企画，立案，提供
- 福山大学ファイヤウオール運用基本方針の策定と運用と改善
- 福山大学情報セキュリティパンフレットの発行
- 情報セキュリティに関する相談窓口
- 情報セキュリティ事故が発生したときの相談窓口
- 情報セキュリティ事故が発生したときの情報セキュリティ事故の再発防止策と，本学の社会的信用の維持に関する提言
- 本学専任教職員によるインターネットサービス利用，インターネットサービス公開に関する相談窓口
- 本ポリシー等が定める本学の情報セキュリティ施策に対する利用者の不満や改善点の収集を行い，必要に応じて，共同利用センター運営委員会，福山大学情報倫理委員会，福山大学部局等情報倫理委員会等に提言等を行う．

共同利用センターが発行する福山大学情報セキュリティパンフレットには，利用者に対する以下の注意事項を記載し，利用者のセキュリティ意識を向上させて，情報セキュリティを確保する．情報セキュリティパンフレットは，日本語版，英語版，中国語版の３つを作成し，外国人教職員や留学生にも役立てる．情報セキュリティパンフレットは，本学Ｗｅｂページで公開する．

- ソフトウェアのアップデートが情報セキュリティの確保に有効である．
- パスワードを安全に利用することが重要である．共同利用機器の利用のために

各自に発行された ID やパスワードを，家族や友人を含む他者に利用させてはならない.

- ウイルス対策ソフトウェアの利用に効果がある.
- 個人情報を扱う場合などは，不注意による情報漏えいに注意する.
- データのバックアップは各自で行う.

４．情報資産に含まれる機密情報や個人情報等の取扱いに関する対策基準

本学の情報資産は，機密情報や個人情報等を含むため，慎重な取扱いを必要とする．その利活用にあたっては，サイバーセキュリティ，不正アクセス行為の禁止，著作権，肖像権，プライバシ保護，個人情報保護等の関係法令を遵守することは当然のことである．また，本法人が定める「学校法人福山大学個人情報管理基本方針」，本学が定める「福山大学情報倫理規程」，利用者が属する部局等が独自に定める情報セキュリティ関連規則，共同利用機器等の利用規則，その他情報セキュリティ関連規則等を遵守することも当然のことである．本学での教育等の推進，とりわけ学生の健全な育成には，個人情報等の適切な利用が必要不可欠であるという認識のもとに，関連法令等ならびに本法人や本学が定める規程等で義務と定められている事項とは別に，厳格な対策基準を定めることにより，本学の情報資産における機密情報や個人情報等の安全の確保と適切な利用を推進するものとする．

種々の情報の中で，とりわけ慎重な取扱いを必要とする情報には，「**表１．本ポリシーにおける情報の種類**」に示す通り，個人情報，要配慮個人情報，個人属性情報，プライバシに関する情報，機密情報がある．これら情報を取扱う者は，これら情報の種類を正しく理解することが求められる．本節においては，次の（１）と（２）の２区分により，対策基準を定める．

（１）**機密情報や個人情報（要配慮個人情報を含む）**

機密情報や個人情報の取扱いには慎重を要するため，遵守事項を「**４．１　機密情報や個人情報を取扱う情報通信機器の利用者の遵守事項**」に定め，同時に，個人情報の取扱いに関する対策基準を「**４．２　個人情報の取扱いに関する対策基準**」に定めることにより，機密情報や個人情報の安全の確保と適切な利用を推進するものとする．さらに，機密情報や個人情報の学外持ち出しにおいては，とりわけ慎重な扱いを必要とするため「**４．３　本学の情報資産における機密情報や個人情報の学外持ち出しに関する対策基準**」において，追加事項を定めるものとする．

情報セキュリティすなわち情報の機密性，情報の完全性及び情報の利用の可用性を確保するために，やむを得ず，システム管理者等が個人情報を収集し，利用する場合がある．このとき，情報漏えいなどで一般利用者に被害を与えたり，目的外利用を

表１．本ポリシーにおける情報の種類

情報の種類	性質	例
個人情報	特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別できることとなるものを含む）や，個人識別符号.	指紋，顔貌，遺伝子配列，氏名，生年月日，運転免許証番号，旅券番号，マイナンバー，基礎年金番号，保険証番号，印鑑登録証明書の印影画像.
要配慮個人情報	本人に対する不当な差別，偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして本学が定める記述が含まれる個人情報.	本人の人種，信条，社会的身分，病歴，犯罪の経歴，犯罪により害を被った事実などのうち，本学が定めるもの.
個人属性情報	個人に関する情報や，個人間の関係に関する情報で，個人情報以外のもの.	● 指紋，顔貌でも，本人特定が困難なように撮影されたか加工されたもの. ● 風貌，表情，姿勢，身体特徴量（体重や身長や視力等），生体計測値（血圧，血糖，体温，睡眠状態，発汗，視線等），服装，所持品，車両の車種など，それらだけでは，本人特定が困難であったり，困難になるように加工されたもの. ● 携帯電話番号，メールアドレス，クレジットカード番号，住所，車両のナンバープレート，車両個体番号，ネットワーク通信におけるＭＡＣアドレスやＩＰアドレス，第三者が提供する情報サービス等のＩＤで本人確認が徹底されていない符号など，それらだけでは，本人特定が困難である符号.
プライバシに関する情報	個人の行動や私的領分にあたるもので，個人の秘密にあたるもの. 要配慮個人情報はプライバシに含まれる. ※　但し，学生の氏名，教職員の氏名，教職員の電子メールアドレス，教職員の内線番号，教職員の所属，教職員の職位，教職員の研究業績情報は，学内で公知のものであり，プライバシには含まれないものとする. 教職員の資格や学歴や職歴などで，学内で公知になっているものは，プライバシに含まれないものとする.	● 私物，自宅，学内でも私的領分にあたるもの ● 信書 ● 情報ネットワークでのあらゆる通信内容（ＭＡＣアドレス，ＩＰアドレスを含む） ● 個々の利用者が作成し保有しているデータで，当該利用者の私的領分にあたるもの ● 学生や教職員の行動にあたるもの．登校，出勤，授業中，勤務中，休養中など学内でのあらゆる行動が該当する ● 学生が修学の種々の場面で残す種々の行動を記述したデータで私的なもの（成績，進路，資格，学歴，職歴，既往歴，健康状態，健康診断結果，生活習慣や嗜好，学費支払い状況を記述したデータなど） ● 教職員の種々の行動を記述したデータで私的なもの（既往歴，健康状態，健康診断結果，生活習慣や嗜好を記述したデータなど）
機密情報	本法人もしくは本学が機密であると文書で明示した情報	財務や入試情報などのうち，本法人や本学が文書で機密であると指定したり，文書で機密であると明示したもの.

行いプライバシを侵害したり（例えば，本人の了解等の適切な手続きを経ることなく，学術雑誌等でプライバシを侵害する情報が公開されるなど）などの事態が発生すると，学内の情報セキュリティマネジメントそのものへの信頼が損なわれる可能性があり，情報セキュリティマネジメントが失敗する可能性がある．そこで，情報セキュリティすなわち情報の機密性，情報の完全性及び情報の利用の可用性の確保のために個人情報を取扱う場合について，「**４．４**　情報セキュリティマネジメント目的での個人情報の取扱いに関する特別の対策基準」に，追加事項を定めることにより，個人情報の安全の確保と適切な利用を推進するものとする．

学術研究目的で個人情報を収集し，利用する場合，「**４．１**　機密情報や個人情報を取扱う情報通信機器の利用者の遵守事項」で定める遵守事項により，学術研究の推進に支障を来す可能性がある．そうした場合のために，「**４．１**　機密情報や個人情報を取扱う情報通信機器の利用者の遵守事項」に替わる特別の対策基準として，「**４．５**　学術研究目的での個人情報の取扱いに関する特別の対策基準」を定めることにより，学術研究における個人情報の安全の確保と適切な利用を推進するものとする．

（２）個人属性情報やプライバシに関する情報

個人属性情報やプライバシに関する情報を収集し，利用するときも，関連法令等ならびに本法人や本学が定める規程等を遵守することは当然のことである．また，個人情報の機密性を確保することにより，結果として，プライバシ保護ができる．しかしながら，個人情報に該当しない情報にもプライバシに関する情報があり，プライバシ保護のためには，慎重な取扱いを必要とする．

個人属性情報やプライバシに関する情報の取扱いについては，適切な対策基準を定める必要がある．個人属性情報やプライバシに関する情報を取扱う場合で，ＩＰアドレス，ＭＡＣアドレス，座席番号など，個人情報でない符号や番号を単独で収集し，特定個人を推定したり特定するための情報として利用する場合がある．このような場合，個人情報と同様の対策基準で取扱うのが自然であり，運用に混乱がなく，的確な対策基準となる．一方で，教育や，情報セキュリティの確保や，学術研究目的などで，アンケート，生体情報収集，行動情報収集を実施するなど，個人属性情報やプライバシに関する情報を収集し，しかも，単独の個人識別符号等よりも多種，多様で，ち密であり，個人の私的領域に踏み込んだ情報を収集する場合がある．こうした場合，個

人情報には該当しなかったり，あるいは個人情報を匿名加工した上で利用するような場合であっても，慎重な取り扱いが必要になる．そのため，厳格な対策基準を必要とする．そのための対策基準を「**４．６　個人属性情報およびプライバシに関する情報の取扱いに関する対策基準**」に記述している．

表２．本章の構成

	記述個所	特記事項
機密情報や個人情報（要配慮個人情報を含む）	４．１節，４．２節，４．３節，４．４節，４．５節	● ４．３節は，機密情報や個人情報の学外持ち出しにおける追加事項． ● ４．４節は，情報セキュリティの確保のために個人情報を扱うときの追加事項 ● ４．５節は，学術研究目的での個人情報の取扱いに関する特別の対策基準
個人属性情報やプライバシに関する情報	４．６節	なし

本章では，以上で記述した通り，機密情報や個人情報（要配慮個人情報を含む）の場合と，個人属性情報やプライバシに関する情報の場合との２つに分けて，対策基準を記述している．さらに，機密情報や個人情報（要配慮個人情報を含む）については，利用目的や状況に応じて追加事項や特別の対策基準を記述している．そのことを「**表２．本章の構成**」にまとめている．

４．１　機密情報や個人情報を取扱う情報通信機器の利用者の遵守事項

利用者が，情報通信機器を利用するとき，利用上の不注意等により，意図しないうちに，機密情報や個人情報の漏えい，紛失，改ざん，不正アクセスの助長など，情報の不適切な取扱いを行ってしまう可能性がある．この可能性を軽減するために，機密情報や個人情報を取扱うような情報通信機器の利用については，以下の各号を遵守事項として定め，利用者に周知し，別途，利用者への周知等の手続きを定めて，その徹底をはかることにより，情報の不適切な取扱いを防ぎながら，本学の情報資産の利活用を発展させるものとする．利用者への周知については，今後，「**付録８．情報通信関連サービス取扱い誓約書について**」に示すような文書等を利用して，効果的に周知を行うことを検討

する．学術研究目的で個人情報を取扱う場合の例外については「**４．５　学術研究目的での個人情報の取扱いに関する特別の対策基準**」で定めている．下記の遵守事項に関する例外措置の手続きは，教育等の必要に応じて，別途定める．

一．利用者は，情報漏えいやコンピュータウイルス等の脅威を軽減するために，学内で，Ｐ２Ｐ型ファイル共有ソフトウェアを使用しないものとする．

二．利用者は，学内の情報サービスの利用や，インターネットサービス利用では，適切にパスワードを使用するものとする．そのとき，パスワード管理ソフトウェアを利用したり，推測されやすいパスワードを避けたり，短いパスワードを避けるなど，安全にパスワードを使用することを心掛ける．

三．利用者は，情報セキュリティの確保のために，ファームウェア，オペレーティングシステム，アプリケーションソフトウェア（オフィスソフトウェア，ウイルス対策ソフトウェア，Ｗｅｂブラウザ，ＰＤＦビューワ，Ｆｌａｓｈプレーヤ等）のソフトウェアを最新の状態に保つアップデートが有効であること理解する．システム管理者は，そのための適切なアップデート計画を立て，可能な限り技術的な対策を講じる．

四．利用者は，通信の自由の重要性と，それに伴うプライバシの保護，表現の自由，思想の自由の重要性を理解する．本学の情報ネットワークにおける情報通信の秘密を確保するために，利用者は，本学の情報ネットワークのパケットの傍受は行わないものとする．また，利用者は，情報ネットワークのパケットの傍受のための傍受装置や傍受ソフトウェアを利用しないものとする．但し，教育や情報セキュリティの確保の目的で，情報ネットワークのパケットを傍受し，匿名化して利用する場合の例外については「**４．６　個人属性情報およびプライバシに関する情報の取扱いに関する対策基準**」で定めている．

五．本学の専任教職員が，インターネットサービス公開を行うときは，当該インターネットサービス公開を行うシステムのシステム管理や情報セキュリティの確保に従事する者は，インターネットサービス公開が教育等の充実に有効であるとともに，情報セキュリティ上の脆弱性に対する種々の対策が重要であることを理解する．インターネットサービス公開を企画し推進する者は，種々の事前対策が情報セキュリティの確保に有効であることを理解し，情報セキュリティについて，当該インターネットサービス公開を行うシステムのシステム管理や情報セキュリティの確保に

従事する者との情報交換や情報共有に協力する.

４．２　個人情報の取扱いに関する対策基準

個人情報保護に関する法令において，下に例示する条件等によって，個人情報取扱事業者の義務等の適用除外とされていたとしても，個人情報等の取扱いに慎重を要することは言うまでもない.

- 大学または大学に属する者が，目的の全部または一部として学術研究の用に供する目的で個人情報を用いる場合で，個人情報取扱事業者の義務等の適用除外として定められている場合
- 取扱う個人データの件数等により，個人情報取扱事業者の義務等の適用除外として定められている場合

そこで，本学の情報資産における個人情報の安全を確保し，個人情報を保護するために，次の（１），（２），（３）を対策基準として定め，利用者に周知し，理解を求めることとする.

（１）本学の情報資産における個人情報の取扱いに関する対策基準

学術研究目的の使用である場合も含めて，本学の情報資産における個人情報の取扱いについて，以下の対策基準を定め，利用者に周知し，理解を求めることとする.

一．個人情報を取扱うにあたっては，その利用目的をできるだけ特定する.

二．全ての個人情報の利用目的を，できるだけ本人の知り得る状態に置くか，できるだけ本人の求めに応じて遅滞なく回答する.

三．利用目的の達成に必要な範囲内において，個人情報を正確かつ最新の情報に保つとともに，利用する必要がなくなったときは，当該個人情報を遅滞なく消去する.

四．匿名加工されていない個人情報は，次のいずれかに該当する場合を除き，第三者に提供しない．但し，学生の個人情報を取扱う場合には，当該学生の保証人，保護者，代理人については第三者から除外する.

- 本人またはその代理人の同意が得られる場合
- 法令に基づく開示要請があった場合
- 不正アクセス，脅迫等の違法行為があった場合
- 個人情報の取扱いの全部または一部を外部業者等に委託する場合

- その他，本学が定める特別な理由に該当する場合

五．個人情報の取扱いの全部または一部を外部業者等に委託する場合は，利用目的の達成に必要な範囲内に限定する．また，その取扱いを委託された個人情報の安全管理が図られるよう，委託を受けた者に対する必要かつ適切な監督を行う．

六．Ｗｅｂサイト等で個人情報を取得し，利用する場合には，データの規模やデータの利用期間を勘案しながら，可能な限り，次の事項を行う．

- 「**付録６**．個人情報等の収集を行うサイト等での個人情報保護方針のひな形」を活用しながら，独自の個人情報保護方針を定め，個人情報を取扱う者に適切な指導を実施する．
- 個人情報保護方針をできるだけ個人情報の該当者本人の知り得る状態に置くことにより，関係者の理解を得る．

七．文書等で個人情報を取得し，利用する場合には，データの規模やデータの利用期間を勘案しながら，可能な限り，次の事項を行う．

- 「**付録７**．個人情報保護規範のひな形」を活用しながら，独自の個人情報保護規範を定め，個人情報を取扱う者に適切な指導を実施する．
- 個人情報保護規範をできるだけ個人情報の該当者本人の知り得る状態に置くことにより，関係者の理解を得る．

八．情報セキュリティ事故の調査において，調査結果として得られる個人情報の取扱いに関する対策基準は，事前に本学が定める明示された規定等が無い限り，「**４．２**　個人情報の取扱いに関する対策基準」に従うものとする．

（２）学生についての保有個人データの取扱いについて

本学が保有する学生についての保有個人データを取り扱う者は，それが，学生の個人情報の集合体であり，一層厳重に情報セキュリティを確保する必要があるということを十分に理解する．本学が保有する学生についての保有個人データの取扱いについては，上記（１）の対策基準に加えて，以下の各号を対策基準として定め，利用者に周知し，理解を求めることとする．

一．本学が保有する学生についての保有個人データを取り扱う者は，学生本人もしくはその保護者，保証人，代理人等の申し出により，内容の確認，内容の訂正が遅滞なく行えるように，技術的，人的・組織的な整備を行うか，それに協力する．

二. 本学が保有する学生についての保有個人データを取り扱う者は，個人情報の利用目的が適切に特定された上で個人情報が利用されるように，可能な限り適切な対策を講じるか，それに協力する.

（3）要配慮個人情報の取得における本人の同意について

要配慮個人情報については，不当な差別，偏見，その他の不利益な取扱いを防ぐために，慎重な扱いを要する．とりわけ，要配慮個人情報を取得する際に，それが学生の健全な育成等に必要であったとしても，本人の理解を得られ，同意が得られていることが，適切な教育等の実施のために重要である．要配慮個人情報の取得における本人の同意について，以下の各号を対策基準として定め，利用者に周知し，理解を求めることとする.

一. 本人が情報の提供を拒むことにより，本人に何らかの不利益が生じる可能性がある場合には，可能な限り，次の事項を実施し，本人の理解が得られるようにする.

- 提供が必要である合理的な理由を明示する.
- 提供を拒否した場合の想定される不利益について明示する.
- 異議申し立てや相談ができる第三者を明示する.

二. 次に掲げる場合を除くほか，あらかじめ本人の同意を得ないで，要配慮個人情報を取得しない.

- 人の生命，身体もしくは財産の保護のために必要がある場合であって，本人の同意を得ることが困難な場合.
- 本学の教職員が，国の機関もしくは地方公共団体の委託を受け，法令の定める事務を遂行することに対して協力する必要がある場合であって，本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき.
- その他，本学が定める場合.

４．３　本学の情報資産における機密情報や個人情報の学外持ち出しに関する対策基準

本学の情報資産における機密情報や個人情報を，電磁的記録媒体などの情報通信機器に格納して学外に持ち出す場合，持ち出された情報通信機器の紛失・置忘れや盗難や自然災害等による情報セキュリティ事故の可能性がある．過去，国内外で，情報通信機器

の紛失・置忘れや盗難による情報セキュリティ事故の事例が多数報告されてきたことから，紛失・置忘れや盗難や自然災害の場面を想定した対策基準を定めておくことが重要である．情報セキュリティ事故発生時の被害の拡大を防ぎ，適切に対処するために，本学の情報資産における機密情報や個人情報を，電磁的記録媒体などの情報通信機器に格納して学外に持ち出す場合については，以下の各号を対策基準として定め，利用者に周知し，理解を求めることとする．

一．機密情報や個人情報を学外に持ち出す者は，可能な限り，鍵のかかる容器等で厳重に管理するか，パスワードでデータを暗号化するなど，安全を保つ．このとき，持ち出した情報通信機器に，パスワードを書いた紙を張り付けるようなことは避ける．

二．持ち出す情報の種類や件数を最小限に留める．

三．機密情報や個人情報を学外に持ち出さずに済ませるための方策があり，それが十分に実現可能で，業務を複雑化しない場合には，利用者は積極的に意見を表明する．当該機密情報や個人情報などの情報資産の管理に従事する者は，単純に機密情報や個人情報の学外持ち出しを規制することは，情報の利用の可用性を損なう可能性があり，情報セキュリティを損なう可能性があることを十分に考慮するとともに，常に，利用者からの意見を聴取し，技術的対策，人的・組織的対策に関与することで，必要な情報の利用の可用性を確保しながら，情報セキュリティ対策を推進する．

四．機密情報や個人情報などの情報資産の管理に従事する者は，紛失・置忘れや盗難や自然災害等の不測の事態による情報セキュリティ事故が発生したとき，緊急性を要しない調査や無用な叱責等で当事者を委縮，混乱させて，対処への集中を妨げるようなことは慎む．特に，盗難や自然災害などの危険な事故が発生したときは，当事者が，人体や財産に関する安全の確保あるいは避難，関係各所への事故の届け出，捜査機関や救命救急機関への通報等，被害の拡大の防止に集中できるように適切な助言や援助を与える．さらには，学生に帯同して学外出張しているような場合には，学生の身体や財産の安全の確保ができるように十分に配慮する．

五．機密情報や個人情報を学外に持ち出す者は，万一の情報セキュリティ事故での被害拡大防止が容易にできるようにするために，下記の情報の全てまたは一部を明らかにしておく．

- 氏名

- 情報通信機器名
- 学外持ち出し期間
- 利用場所（国名，住所など）
- 機密情報，個人情報の有無およびその概要（対象者の範囲や内容など）
- 情報通信機器のログインパスワードやＢＩＯＳパスワード等の有無
- 電磁的記録媒体のパスワードの有無
- 個人情報，機密情報の暗号化
- ＬＡＮ内の不特定多数がアクセス可能な共有ディレクトリ／共有フォルダの有無
- 電子メールソフトウェアによる電子メールボックス内の機密情報や個人情報の有無
- Ｗｅｂブラウザに記録させているインターネットサービス用パスワード等の有無．特に，学内の情報サービスサイトや，インターネット決済サイト等に注意する．

六．可能な限り，情報セキュリティ事故発生時に現場等で責任をもって調査等に協力できる能力を持った者１名以上を定めておく．

七．紛失・置忘れや盗難などにより，機密情報や個人情報に関する情報セキュリティ事故が発生したときは，事実を隠蔽したり，誤った情報を公表することは，被害の拡大を招く可能性もあり，被害者への適切な補償に支障が出る可能性もあり，本学の社会的信用を損なう可能性もあるので絶対に避ける．Ｗｅｂページやメディア発表などでの事実の公表は，全学出動で行う．公表の内容により被害のさらなる拡大を招かないように注意しながら，正確な事実を速やかに公表する．同時に，個人情報が漏えいした場合には，適切な手順で，対象者に報告し，個人情報の漏えいに伴う被害の拡大を防ぐ．

４．４　情報セキュリティマネジメント目的での個人情報の取扱いに関する特別の対策基準

情報セキュリティすなわち情報の機密性，情報の完全性及び情報の利用の可用性を確保するために，システム管理者等が個人情報を収集し，利用する場合がある．このとき，「**４．２**　個人情報の取扱いに関する対策基準」の対策基準に加えて，以下の各号を対

策基準として定め，利用者に周知し，理解を求めることにより，学内の情報セキュリティマネジメントそのものへの信頼を維持する．

一．学生や部外者が往来しえる通路や，利用することがありえる教室，居室，実験室等に，情報セキュリティの確保を目的として防犯カメラを設置するときは，次の通りに取扱う．

- 真にやむを得ない場合を除き，防犯カメラの利用目的を，学生や教職員の安全の確保，情報資産を含む本学の財産に関する安全の確保，違法行為があったときの調査などの防犯目的に限定する．それら以外の目的に利用するときは，利用目的を，撮影対象者全員の知り得る状態に置き，撮影についての撮影対象者全員からの合意を得ることとし，合意が得られないときは，その者の画像データを確実に消去するか，本人が特定できないように匿名加工するなどの措置を講ずる．
- 防犯カメラを設置し，運用する者は，防犯カメラを設置していることを広く周知し，また，防犯カメラを設置していることを容易に知りえる状態に置くことで，防犯効果を向上させるものとする．
- 防犯カメラから収集される画像データを管理する者は，防犯カメラの画像が個人情報であることを正しく理解し，慎重に取扱う．

二．情報システムのＩＤの発行のために学生番号や教職員番号を取扱うときは，次の通りに取扱う．

- 情報システムのＩＤの発行や運用を行うシステム管理者は，学生番号や教職員番号が漏えいしないための，技術的対策を講じる．
- 情報システムのＩＤの発行や運用を行うシステム管理者は，学生番号や教職員番号を，目的外に利用するときは，該当者全員の合意を得る．

三．限られた教職員のみが立ち入ることができる区域内への立ち入り時に，利用者に教職員カード等の提示等を求め，情報システムでその照合を行うなどで，教職員番号の収集や利用を行う場合は，次の通りに取扱う．

- 当該情報システムのシステム管理者は，教職員番号が漏えいしないための，技術的対策を講じる．
- 当該情報システムのシステム管理者は，教職員番号を，目的外に利用するときは，該当者全員の合意を得る．

四．その他，情報セキュリティの確保を目的として，個人情報の収集や利用を行う場合には，次の通りに取扱う．

- 情報セキュリティマネジメントへの信頼を維持するために，個人情報の収集を秘密に行わない．
- 情報セキュリティマネジメントへの信頼を維持するために，可能な限り，個人情報の利用目的を特定し，個人情報の収集における本人からの合意を取得する．
- 情報が漏えいしないための，技術的対策を講じる．
- 本人からの合意を得たときに本人に提示した目的以外に利用するときは，該当者全員の合意を得る．

４．５　学術研究目的での個人情報の取扱いに関する特別の対策基準

学術研究を目的とする場合は，個人情報保護に関する法令において，個人情報取扱事業者の義務等の適用除外が定められているという現状がある．大学における学術研究推進への社会からの大きな期待，個人情報の取扱いに関する信頼があることを適切に理解し，本学の専任教職員が，その学術研究の推進のため，学術研究を目的として個人情報を取扱う場合については，以下の対策基準を定め，利用者に周知し，理解を求めることにより，学術研究の推進と情報セキュリティの確保を行うものとする．

一．個人情報を取扱う場合には，関連法令等ならびに本法人や本学が定める規程等を正しく理解して，個人情報を取扱うことは当然のことである．学術研究を実施する者は，その責任において，個人情報を取扱う者全員に適切な指導を実施する．

二．学術研究目的で使用する個人情報の取扱いで，「**４．１**　機密情報や個人情報の保護のための利用者の遵守事項」をそのまま実施しては学術研究の推進に支障がある場合には，学術研究を実施する者は，個人情報管理基準を独自に定め，明示するとともに，それを，当該個人情報を取扱う者全員が理解し，遵守するように必要かつ適切な指導を行う．この個人情報管理基準では，個人情報の利用目的の特定，個人情報の厳格な管理手順，個人情報取得における本人からの同意取得手順と異議申し立て手順，本人の同意の強制を防ぐための対策，個人情報の第三者への提供の禁止，本人からの個人情報の照会等に対する対応を明示するものとする．

三．学術研究目的の場合でも「**４．２**　個人情報の取扱いに関する対策基準」および「**４．３**　本学の情報資産における機密情報や個人情報の学外持ち出しに関する対策基準」が定める対策基準を用いる．

四．学術研究への信頼を維持するために，個人情報の収集を秘密に行わない．

五．学術研究への信頼を維持するために，個人情報の収集における本人からの合意の取得では，次の項目のいずれかを実施する．

- 収集対象者と対面できる場合には，利用目的，収集対象者，収集される情報の種類，利用期間，保存期間，情報漏えい等の脅威について，収集対象者全員に，文書等で分かりやすく説明し，収集対象者全員の合意を得る．公共空間で収集するからといって，個人情報の取得における全員の合意が不必要というわけではない．
- Ｗｅｂサーバなど，サイトを用いて，個人情報を取集する場合は，利用目的，収集対象者，収集される情報の種類，利用期間，保存期間，情報漏えい等の脅威について，「**付録６**．個人情報等の収集や利用を行うサイト等での個人情報保護方針のひな形」を用いるなどで，個人情報保護方針を文書で定め，対象者が容易に知り得る状態に置く．

六．個人情報の収集における本人からの合意の取得において，正課の単位取得や報酬について説明を行う場合には，説明内容を文書で記述し，誤解が生じないようにする．説明に用いた文書は，学術研究を実施する者の責任において保存し，可能な限り，第三者からの開示請求に応じる．

七．個人情報の収集における本人からの合意の取得では，可能な限り，第三者の相談窓口，異議申し立て先を設ける．

八．遺伝子情報や要配慮個人情報を取扱う場合には，当該部局等の部局等情報倫理委員会での審査を行う．その審査手続きは，必要に応じて，当該部局等の部局等情報倫理委員会で別途定める．

九．隔離された情報ネットワーク内で収集を実施するなどの技術的な対策を実施することで，同意を得ていない者の個人情報を収集したり，同意を得ていない種類の個人情報を収集したりすることが無いようにする．

十．同意を得ていない者の個人情報を収集したり，同意を得ていない種類の個人情報を収集した場合には，直ちにその部分を破棄する．

十一．学術研究の実施を起因として．本学の情報資産のき損や消失を招くようなことを避けるための，技術的，人的・組織的な対策を講じる．情報資産のき損や消失の恐れが事前に見込まれる場合には，それを可能な限り軽減するための技術的，人的・組織的な対策を学術研究を実施する者の責任と負担で実施するとともに，当該部局等の部局等情報倫理委員会に事前の届け出を行う．その手続きは，必要に応じて，当該部局等の部局等情報倫理委員会で別途定める．

十二．学術研究を実施する者は，本学の情報資産のき損や消失を可能な限り防ぐ責任，万一の情報セキュリティ事故発生時の再発防止策の策定と実施，学術研究を実施する者自身の信頼の保持の重要性を，十分に理解する．

４．６　個人属性情報およびプライバシに関する情報の取扱いに関する対策基準

利用者は，大学における通信の自由，表現の自由，思想の自由，プライバシの尊重の重要性を常に十分に理解し行動する．本学における教育等の実施において，教職員や学生のプライバシを侵害しているかのごとき誤解を生むことは，外部からの本学における教育等への支持と協力を損なう可能性があるだけでなく，本学の社会的信用を損なう可能性もある．

近年，ネットワーク接続された監視カメラ，情報通信機器の操作を遠隔から簡単に監視できる技術，ＧＰＳや無線技術等を用いた位置計測・測位技術，通信パケットの収集技術，情報通信機器内のデータを，本人の許可なしに遠隔から簡単に収集できる技術等の進展により，容易にプライバシに関する情報が収集できる状況にある．こうした技術の進展があるからといって，情報通信機器を駆使して，安易に利用者のプライバシ情報の収集を推進することが，必ずしも情報セキュリティの確保や，教育等の充実に有効であるとは考えない．そこで，本学の情報資産における個人属性情報およびプライバシに関する情報の安全を確保し，プライバシを保護するために，次の（１），（２），（３）を対策基準として定め，利用者に周知し，理解を求めることとする．

（１）特定個人を推定したり特定したりするために情報を収集し利用する場合

個人属性情報やプライバシに関する情報を取扱う場合で，ＩＰアドレス，ＭＡＣアドレス，座席番号など，個人情報でない符号や番号を単独で収集し，特定個人を推定

したり特定するための情報として利用する場合がある．このような場合，個人情報と同様の対策基準で取扱うのが自然であり，運用に混乱がなく，的確な対策基準となる．特定個人を推定したり特定したりするために情報を収集し利用する場合について，以下の各号を対策基準として定め，利用者に周知し，理解を求めることとする．但し，収集された情報が，匿名加工され，かつ平均値や合計値のように統計処理された後でのみ使用される場合は除外する．

一．特定個人を推定したり特定したりするために情報を収集し利用する場合は，収集された情報は，個人識別符号であるとして取り扱う．

二．「**４．２　**個人情報の取扱いに関する対策基準」および「**４．３　**本学の情報資産における機密情報や個人情報の学外持ち出しに関する対策基準」が定める対策基準を用いる．

（２）個人の私的領域に踏み込んだ情報を収集し利用する場合

教育や，情報セキュリティの確保や，学術研究目的などで，アンケート，生体情報収集，行動情報収集を実施するなど，個人属性情報やプライバシに関する情報を収集する場合がある．例えば，授業中の受講態度やパソコン等の操作履歴等を，教員がよく観察し指導するのは，学生の健全な育成のために当然のことであるが，観察と指導にとどまらず，データの収集まで行うとき，収集したデータを不適切に利用しているかのような誤解を与えることや，収集したデータが漏えいするなどの事態が発生することは，本学の教育等の発展を阻む可能性がある．情報通信機器を用いて収集できる情報は，今や，単独の個人識別符号等よりも多種，多様で，ち密であり，個人の私的領域に踏み込んだ情報を容易に収集できる．こうした場合，個人情報には該当しなかったり，あるいは個人情報を匿名加工した上で利用するような場合であっても，慎重な取り扱いが必要になる．個人の私的領域に踏み込んで，個人属性情報やプライバシに関する情報を収集し利用する場合について，以下の各号により，取扱う情報の最大限の範囲を明示的に限定するとともに，情報を取扱う者の標準的な行動を対策基準として定め，利用者に周知し，理解を求めることにより，本学の情報資産における情報セキュリティの確保と，情報の適切な利用を推進するものとする．但し，収集された情報が，匿名加工され，かつ平均値や合計値のように統計処理された後でのみ使用される場合は除外する．

なお，利用目的や，取扱う情報の種類・性質に応じて，適切な取扱い法は変わるべきものである. 適切な取扱い法は, 個々の情報を管理する者の責任において定められ，適切に実施されるものとする．当然ながら，本ポリシーで定める対策基準を実施してさえいれば何を行ってもよいということではなく，こうした誤解が生じないように，個々の情報を管理する者は，情報を取扱う者に適切な指導を行うものとする.

一．収集され利用される情報が個人情報に該当する場合には，本節の対策基準とあわせて,「**４．２**　個人情報の取扱いに関する対策基準」および「**４．３**　本学の情報資産における機密情報や個人情報の学外持ち出しに関する対策基準」が定める対策基準を用いる.

二．プライバシに関する情報を取扱う場合には，関連法令等ならびに本法人や本学が定める規程等を正しく理解して，プライバシに関する情報を取扱うことは当然のことである．当該情報を管理する者は，その責任において，当該情報を取扱う者全員に適切な指導を実施する.

三．情報を収集する者は，情報の収集において本学の情報資産のき損や消失を可能な限り防ぐ責任を十分に理解する.

四．情報を管理する者は，万一の情報セキュリティ事故発生時の再発防止策の策定と実施，信頼の保持の重要性を，十分に理解する.

五．情報通信機器の操作履歴を収集でき，他の情報通信機器で第三者が閲覧できるようにするための操作履歴監視装置あるいは操作履歴監視ソフトウェアを設置するときは，次の通りに取扱う.

- 真にやむを得ない場合を除き，操作履歴監視装置あるいは操作履歴監視ソフトウェアの利用目的を，学生の健全な育成に限定する．それら以外の目的に利用するときは, 利用目的を, 監視対象者全員の知り得る状態に置き，監視についての監視対象者全員からの合意を得ることとし，合意が得られないときは，その者の監視データを確実に消去するか，本人が特定できないように匿名加工するなどの措置を講ずる.
- 利用目的を変更した場合は，該当者全員からの合意を取得する.
- 収集される監視データを管理する者は，監視データがプライバシに関する情報であることを正しく理解し，慎重に取扱う.
- プライバシ保護を確実なものにするために，監視時間を授業中に限定する，

監視対象者を受講者に限定するなど，利用目的に合致しないデータを収集することが無いように，必要な対策を講じる．

六．学生や部外者が往来しえる通路や，利用することがありえる教室，居室，実験室等で，個人を顔貌やＭＡＣアドレスやＩＰアドレスや個人に割り当てられた符号や番号で特定しながら，個人の位置を計測や測位できる位置計測・測位装置あるいは位置計測・測位ソフトウェアを設置するときは，次の通りに取扱う．

- 真にやむを得ない場合を除き，位置計測・測位装置あるいは位置計測・測位ソフトウェアの利用目的を，学生の健全な育成に限定する．それら以外の目的に利用するときは，利用目的を，位置計測・測位対象者全員の知り得る状態に置き，位置計測・測位についての位置計測・測位対象者全員からの合意を得ることとし，合意が得られないときは，その者の位置計測・測位データを確実に消去するか，本人が特定できないように匿名加工するなどの措置を講ずる．この場合は，顔貌全体が残っている場合，ＭＡＣアドレスやＩＰアドレスが残っている場合には，匿名化できていないものとみなす．
- 利用目的を変更した場合は，該当者全員からの合意を取得する．
- 収集される位置計測・測位データを管理する者は，位置計測・測位データがプライバシに関する情報であることを正しく理解し，慎重に取扱う．
- プライバシ保護を確実なものにするために，位置計測・測位時間を限定するなど，利用目的に合致しないデータを収集することが無いように，必要な対策を講じる．

七．学生や部外者が往来しえる通路や，利用することがありえる教室，居室，実験室等で，個人を特定せずに，個人の通過や接近等を計測できる感知装置あるいは感知ソフトウェアを設置するときは，次の通りに取扱う．

- 利用目的を，容易に知りえる状態に置く．
- 収集される感知データを管理する者は，感知データがプライバシに関する情報であることを正しく理解し，慎重に取扱う．

八．情報通信機器のデータを収集でき，他の情報通信機器で第三者が閲覧できるようにするためのデータ監視装置あるいはデータ監視ソフトウェアを利用して，本人の了解なくデータを監視することは行わない．情報セキュリティの確保のため

に必要な場合であっても，必ず，本人の許可を得るものとする．但し，データをバックアップして，障害回復に用いるための装置は，データ監視にはあたらないので，除外する．また，第三者が閲覧できないように適切に設定され使用される場合には除外する．また，情報セキュリティの確保にために，真にやむを得ず，一時的に，データを利用できない状態に置くような措置を行うことも，データ監視にはあたらないので除外する．

九．本学の情報資産を用いて，次の情報を収集しない．例外は，十号，十一号，十二号で定める．

- 信書の差出人および本文に関する情報．
- 通信パケットのヘッダおよび本体に関する一切の情報．

十．情報セキュリティを確保するために，次のいずれかに該当する場合は，九号の例外とする．

- ファイヤウオールシステムがパケットフィルタリングを行う目的で，通信パケットのヘッダを取得する場合．
- ウイルス対策システムがコンピュータウイルス等のスキャンを行う目的で，通信パケットのヘッダおよび本体を取得する場合．
- 侵入検知システムが侵入を検知する目的で，通信パケットのヘッダおよび本体を取得する場合．

十一．十号の定めにより，情報を収集する場合には，次の対策によって，利用者のプライバシ保護を行う．

- 保存や表示される情報は，フィルタリングやスキャンや検知の結果に限定する．
- フィルタリングやスキャンや検知の結果に関係しないパケットの情報は直ちに破棄する．
- フィルタリングやスキャンや検知の結果に関係するパケットであっても，パケットの本体，パケットのＩＰアドレス，パケットのＭＡＣアドレスなどは，利用者のプライバシに関わる．パケットの中で，フィルタリングやスキャンや検知に直接関係しない部分は，当該ファイヤウオールシステムや当該ウイルス対策システムや当該侵入検知システムの管理者以外の目に触れないようにする．

十二．教育目的あるいは学術研究目的で，通信パケットのヘッダおよび本体を収集する場合には，九号の例外とする．その場合，情報を収集し，利用する者は，次の事項をすべて遵守するものとする．

- 利用目的を，収集対象者全員の知り得る状態に置き，収集についての収集対象者全員からの合意を得る．
- 合意を得ていない者の通信パケットを傍受することが無いように，適切な技術的対策を講じる．
- 収集されるデータを管理する者は，データがプライバシに関する情報であることを正しく理解し，慎重に取扱う．

十三．可能な限り，収集し利用する情報の利用目的を特定する．

十四．Ｗｅｂサイト等でプライバシに関する情報を取得し，利用する場合には，データの規模やデータの利用期間を勘案しながら，可能な限り，次の事項を行う．

- 「**付録６**．個人情報等の収集を行うサイト等での個人情報保護方針のひな形」を参考にしながら，独自のプライバシ保護方針を定め，プライバシに関する情報を取扱う者に適切な指導を実施する．
- プライバシ保護方針をできるだけプライバシに関する情報の該当者本人の知り得る状態に置くことにより，関係者の理解を得る．

十五．文書等でプライバシに関する情報を取得し，利用する場合には，データの規模やデータの利用期間を勘案しながら，可能な限り，次の事項を行う．

- 「**付録７**．個人情報保護規範のひな形」を参考にしながら，独自のプライバシ保護規範を定め，プライバシに関する情報を取扱う者に適切な指導を実施する．
- プライバシ保護規範をできるだけプライバシに関する情報の該当者本人の知り得る状態に置くことにより，関係者の理解を得る．

十六．可能な限り，情報の収集において，本人からの合意を取得するか，情報を収集していることを，対象者から分かりやすい状態にしておく．

十七．利用目的を変更した場合は，可能な限り，該当者全員からの合意を取得するか，利用目的を変更したことを，該当者全員から分かりやすい状態にしておく．

十八．情報の収集における本人からの合意の取得では，次の項目のいずれかを実施する．

- 収集対象者全員と対面できる場合には，利用目的，収集対象者，収集される情報の種類，利用期間，保存期間，情報漏えい等の脅威について，収集対象者全員に，文書等で分かりやすく説明し，収集対象者全員の合意を得る．
- Ｗｅｂサーバなど，サイトを用いて，情報を取集する場合は，利用目的，収集対象者，収集される情報の種類，利用期間，保存期間，情報漏えい等の脅威について，プライバシ保護方針を文書で定め，対象者が容易に知り得る状態に置く．
- 上記以外の手段で情報を取集する場合は，利用目的，収集対象者，収集される情報の種類，利用期間，保存期間，情報漏えい等の脅威について，プライバシ保護方針を文書で定め，対象者が容易に知り得る状態に置くか，利用者の求めに応じて直ちに開示できる状態に置く．

十九．情報の収集における本人からの合意の取得において，正課の単位取得や報酬について説明を行う場合には，説明内容を文書で記述し，誤解が生じないようにする．説明に用いた文書は，収集を実施する者の責任において保存し，可能な限り，第三者からの開示請求に応じる．

二十．プライバシに関する情報の収集を行うときは，次に掲げる場合を除くほか，いかなる場合，いかなる種類の情報であっても，秘密には行わない．

- 人の生命，身体もしくは財産の保護のために必要がある場合であって，情報収集を行っている事実を明示できないほどの緊急性を要する場合．
- 本学の教職員が，国の機関もしくは地方公共団体の委託を受け，法令の定める事務を遂行することに対して協力する必要がある場合であって，秘密にしないことにより当該事務の遂行に支障を及ぼすおそれがあるとき．

二十一．隔離された情報ネットワーク内で収集を実施するなどの技術的な対策を実施することで，同意を得ていない者の情報を収集したり，同意を得ていない種類の情報を収集したりすることが無いようにする．

二十二．同意を得ていない者の情報を収集したり，同意を得ていない種類の情報を収集した場合には，直ちにその部分を破棄する．

二十三．収集した情報が漏えいしないための，技術的対策を講じる．

二十四．情報を匿名化するにあたっては，可能な限り，元の個人情報を推定，算出

ができなくなるような最大限の技術的な対策を講じるものとする.

二十五. 情報セキュリティ事故の調査において, 個人属性情報やプライバシに関する情報を取得するにあたっては, 取得の目的を, 被害状況の把握, 事実の裏付けの取得, 被害拡大の防止, 再発防止策の策定, 本学の社会的信用の維持に限定し, 調査対象者の理解を得るものとする.

二十六. 情報セキュリティ事故の調査において, プライバシに関する情報の取得は, 本人の同意の上での聞き取り調査, インターネットサービス公開を行っているサーバでのインターネットサービスへのアクセス履歴データの読み取りなど, 適正な手段で行うことは当然のことである. このとき, 適正に取得が行われたこと自体も記録し, あとで確認ができるようにする. この記録は, 調査対象者の求めに応じて内容の確認と内容の訂正が遅滞なく行えるようにする.

（３）学術研究目的で個人属性情報データベースを作成する場合

本学の教職員が, 本学の情報資産を用いて, 目的の全部または一部として学術研究の用に供する目的で, 電子計算機を用いて検索することができるように体系的に構成された個人属性情報データベースを作成する場合について, 関係する法令などで, 義務等が定められていないとしても, 多数の個人属性情報の集合体を取扱うことから, 慎重な取扱いが必要になる. 当該個人属性情報データベースが, ＭＡＣアドレス等の個体番号, ＩＰアドレス, クレジットカード番号, メールアドレスなど, 単体では個人を識別することはできなくても, 他の情報と組み合わせることにより, 容易に個人を識別するのに利用できる個人属性情報を含むとき, これら個人属性情報は, 原則個人情報にはあたらないものの, 情報セキュリティの確保のために, 本ポリシーの「**４. ２** 個人情報の取扱いに関する対策基準」が定める対策基準を用いる.

５．情報資産の区分と各々の対策基準

５．１　情報通信機器

情報通信機器には，個人利用機器とそれ以外の機器がある．

（１）個人利用機器

もっぱら１名で使用する，あるいは，共同利用機器であっても，特定の少ない人数で利用する個人利用機器については，利用者自身が，当該情報通信機器のシステム管理者となり，コンピュータウイルスへの対策，不正侵入への対策，情報漏えいの対策，データ消失等に対する対策など，情報セキュリティの確保に責任を持つという自己責任原則になる．

（２）個人利用機器でない機器

個人利用機器でない機器は，複数名で共同利用される．その利用者は，一般利用者とシステム管理者に分かれる．システム管理者は，当該情報通信機器を適切に管理し，コンピュータウイルスへの対策，不正侵入への対策，情報漏えいの対策，データ消失等に対する対策など，情報セキュリティの確保を行う．システム管理者は，一般利用者のユーザアカウントの管理，アクセス権限の管理も行う．一般利用者は，当該情報通信機器を適切に利用し，情報セキュリティの確保に努めるとともに，システム管理者の助言や指示や指導に従う．当該情報通信機器に利用規則等が定められている場合には，それを遵守するのは当然のことである．

５．２　ソフトウェア

（１）アップデートとバージョンアップ

情報セキュリティ対策としては，ソフトウェアのアップデートを適切に行い，最新の状態を保ち続けることが有効な対策になる．また，サポート期限の切れたバージョンのソフトウェアは使わずに，バージョンアップするか，同等機能の別のソフトウェア等に交換する必要がある．以上のことを利用者はよく理解する．あわせて，システム管理のために，アップデートやバージョンアップの作業，バージョンアップ後に業務等に支障

が無いかの確認作業も重要であることを，利用者はよく理解する.

今後，本学では，下記に例示するソフトウェアを候補として，一般利用者を対象として，アップデート情報およびバージョンアップ情報を提供するサービスを段階的に整備していくことにより，情報セキュリティ対策を推進することを検討する．ここでは特定のソフトウェア製品についてのみ，アップデート情報およびバージョンアップ情報が利用者に情報提供されることになるが，特定のソフトウェア製品の推奨ではないこと，本学としてソフトウェア製品の優劣を判断したわけでないこともあわせて周知し，利用者の理解を求めることとする．情報提供を行うソフトウェアには，インターネットのクラウドサービスとＷｅｂブラウザ等が連携して動作する形態のものも含めることにする.

- オペレーティングシステム
- ウイルス対策ソフトウェア
- データバックアップソフトウェア
- オフィスソフトウェア
- 電子メールソフトウェア
- Ｗｅｂブラウザ
- パスワード管理ソフトウェア
- ＰＤＦビューワ
- Ｆｌａｓｈプレーヤ
- 通話／ビデオ会議ソフトウェア
- 圧縮・解凍ソフトウェア
- 暗号・復号ソフトウェア
- カレンダー／日程表ソフトウェア
- 施設予約ソフトウェア
- スケジュール調整／出欠管理ソフトウェア
- 掲示，通知，情報共有用ソフトウェア
- アンケートソフトウェア

（２）公開データ

インターネット上で配布，公開されている公開データ（例えば，テンプレート，イラスト，クリップアートなど）の利用では，著作権を侵害しないことが絶対に必要である.

公開データの利用に関する調査や情報収集については，必要に応じて，全学レベルで行う．その結果は，利用者に周知し，理解を求めることとする．

（3）全学ソフトウェア

有償ソフトウェアで，全学で広く利用されるソフトウェアについては，全学単位で一括導入することにより，ソフトウェアのバージョンを維持して，情報セキュリティ対策を推進することを検討する．以下の各号を，今後の検討課題とする．

一．全学ソフトウェアの制定，充実を検討する．

二．全学ソフトウェアのインストール，アップデート，標準的な使用法に関する情報の提供サービスを段階的に整備していくことにより，情報セキュリティ対策を推進することを検討する．

三．全学ソフトウェアのバージョンアップについて，情報収集の上，可能な範囲で，全学レベルでの，長期的なバージョンアップ計画の策定を検討する．このバージョンアップ計画の策定の目的は，各部局において，当該部局の判断により，必要に応じて，全学ソフトウェアを動作させる情報通信機器等の更新を計画的に行うための，当該情報通信機器等の中長期調達計画の立案のための参考資料とするためのものである．バージョンアップ計画の策定は，教育等のために随時，情報通信機器等を調達することを妨げるものではない．

（4）情報通信機器の調達計画

下記の情報通信機器については，時間経過により，使用するファームウェアやオペレーティングシステムが古くなった上に，それらをアップデートやバージョンアップできるための支援がメーカー等から受けられなくなる可能性がある．

- デスクトップパーソナルコンピュータ
- ノートパーソナルコンピュータ
- タブレット
- ルータ
- ネットワークアクセスストレージ

そのような場合，情報セキュリティ対策を実施することなく使い続けることは，情報セキュリティの脅威になる．とりわけ，個人情報を含む情報の集合物である個人情報デ

ータベースに対して，高レベルのアクセス権限を持つ事務部門においては，ファームウェアやオペレーティングシステムが古いままで，アップデートやバージョンアップが実施できず，その他の情報セキュリティ対策を何ら実施することなく放置することは，情報セキュリティの大きな脅威となる．高レベルのアクセス権限を持つ事務部門においては，事前に，必要な情報通信機器の台数や調達更新に関する中長期計画を立てることを検討する．このとき国税庁がパーソナルコンピュータ（サーバー用のものを除く．）の耐用年数は４年，その他の電子計算機の耐用年数は５年と定めていることを勘案し，これら耐用年数をはるかに超えて情報通信機器を使い続けることを避けることにより，ファームウェアやオペレーティングシステムの古さに起因する情報セキュリティの脆弱性を軽減することを今後検討する．

５．３　本学の教職員，学生等が業務上又は修学上取得及び作成した情報

（１）個人情報データベースにおける個人情報の明示

個人情報を含む情報の集合体である個人情報データベースを取扱う教職員に対しては，取扱う情報が個人情報であることが適切に明示されるようにするために，以下の対策基準を定め，利用者に周知し，理解を求めることとする．

一．取扱う情報が，個人情報で無いと誤認することが無いように，個人情報の定義や，本学が取扱う個人情報の種類について，個人情報を取扱う者に適切に分かりやすく明示し，指導を行う．

二．個人情報ではないのに個人情報であるかのように取扱うこと，個人情報ではないのに第三者や関係者などに個人情報であると誤った説明を行うことも，情報管理上の問題を招く可能性があるので，そのようなことが起きないように，個人情報を取扱う者に，適切に指導を行う．

要配慮個人情報を取扱う場合は，取扱う者に対して，誤解の余地が無いようにその範囲等を明示する．あわせて，個人情報ではなくても，本学の規定等により機密として取扱うべき機密情報を取扱う場合についても，取扱う者に対して，誤解の余地が無いようにその範囲等を明示する．

但し，情報の種類の明示法として，単純にファイル名に「機密重要」のような文字列

を含めてしまうような明示法だと，不正アクセス者に手がかりを与えてしまうことになるので，不正アクセス者への手がかりにならないように，明示は適切に行う．

機密情報や個人情報の取扱いにおける事故を理由として利用者を処分等するときなどは，事前に，機密情報や個人情報であることが分かる明示を行い，理解を得られていたかをあわせて確認する．

（２）情報の管理法の区分け

情報セキュリティマネジメントに従事する者は，本学の情報資産で情報を取扱うとき，次の４形態がありえることを理解する．さらに，情報セキュリティ事故に関する調査や処置を実施するときは，それぞれの形態にあった調査，被害拡大防止策の実施，事実の公表，再発防止策の策定と実施，本学の社会的信用の維持のための適切な行動を実施する．

一．情報通信機器を情報ネットワークにつなぐことは無い．外部の電磁的記録媒体を接続することはできないようになっている．プリントアウトもできない．

この場合，不正アクセスや不正使用を行うには，当該情報通信機器を使用するか，当該情報通信機器が発する電磁波を解析するなどしかなく，不正アクセスや不正使用の痕跡を保全し，調査することは，４形態の中では一番容易である．

二．情報通信機器を情報ネットワークの DMZ の内側にあり，学内ネットワークの限られた IP アドレスからしかアクセスできない．プリントアウトはできる．外部の電磁的記録媒体を接続することはできないようになっている．

この場合，ネットワーク経由での不正アクセスがあり得る．アクセス履歴等の痕跡を保全し，侵入手段の特定を行うことから調査が始まる．不正アクセスの結果として，内蔵の全データが漏えいし，また，他への不正アクセスへの踏み台等として利用されている可能性もある．学内ネットワークの調査，当該機器の管理者権限に関する調査によって，不正アクセスされたデータの範囲が限定できる証拠が得られる可能性がある．

三．一及び二以外の学内システム

学内に設置された情報通信機器に情報を格納する場合が該当する．学内に置く場合には，盗難や紛失や自然災害に備えて，情報通信機器を適切に管理する必要がある．データのバックアップ，ソフトウェアのアップデート，共同利用機器のアカウント管理などのシステム管理も適切に実施される必要がある．不正アクセスの結果として，内蔵の全データが漏えいし，また，他への不正アクセスへの踏み台等として利用されている可能性もある．不正アクセスされたデータの範囲を限定することは難しい．

四．学外システム

学外に置く場合には，信頼できる外部業者を使う必要がある．必要に応じて，データの痕跡を一切残さずに，データを確実に消去できるような情報サービスを慎重に選択する必要がある．外部業者がシステム管理のサービスを提供しないときは，適切にシステム管理を実施する必要がある．情報セキュリティ事故時の調査手段については，事前に検討しておく必要がある．

いずれの場合であっても，情報ネットワークにつながっている限り，不正アクセス等の脅威は当然ある．従って，ログインのためのパスワードは安全に使用する必要があるし，重要なデータは，暗号化するなど，安全に利用する必要がある．

なお，情報の性質や用途に応じて，情報セキュリティ上最適な情報通信機器の形態は変わるものである．情報セキュリティを確保しながら，サービスの即時立ち上げやコストを重視する場合などは，外部業者が提供するサービスを使うのが最善になる可能性がある．可用性を特に重視する場合などは，学内の情報通信機器と外部業者が提供するサービスを組み合わせることになる可能性もある．従って，情報通信機器の形態について，何らかの制限を行うのは，情報セキュリティ上好ましくない．特定の利用形態について規則や手続きを定めるときは，想定されるリスクを具体的にリストアップし，他の利用形態についても相当の規則や手続きを定める．

６．利用者の対策基準

本章では，情報セキュリティを確保するための，一般利用者やシステム管理者が行う標準的な行動等を，利用者の対策基準として定める．本章では，下記の脅威を想定して，それらへの対策として適切と判断される標準的な行動等を，網羅的かつ体系的に記述する．これにより，情報セキュリティを確保しながら，本学の教育等のさらなる発展を推進する．

- 情報通信機器の不正利用や不正アクセス
- コンピュータウイルスやスパイウェアやボットなどの不正なソフトウェア
- 情報漏えい
- 電子メールの不適切な利用による事故
- Ｗｅｂブラウザの不適切な利用による事故
- インターネットサービスの不適切な利用による事故
- データの消失等により業務が継続できなくなること

本章に記述される対策基準は網羅的かつ体系的なものであるが，当然ながら，一般利用者やシステム管理者が行う行動の全てを記述することはできない．一般利用者やシステム管理者は，本章に記述されている標準的な行動に不備があると判断するときや，そのまま実行しては効率が良くないなどの問題があると判断するときは，各自，適切な行動により情報セキュリティの確保を行うものとする．

個人利用機器については，利用者は，当該個人利用機器を適切に利用し，情報セキュリティの確保に努めるとともに，当該個人利用機器のシステム管理も行う．利用者自身がシステム管理を行うので，情報セキュリティの確保は自己責任原則になる．さらには，情報セキュリティ事故が発生したときは，自ら被害の拡大の防止，事故の再発防止のための行動を求められる．

個人利用機器でない共同利用機器の場合には，システム管理者と，一般利用者に分かれる．一般利用者は，当該情報通信機器を適切に利用し，情報セキュリティの確保に努めるとともに，システム管理者の助言や指示や指導に従う．システム管理者は，当該情報通信機器を適切に管理し，情報セキュリティの確保に努める．

なお，利用者の遵守事項は，関係法令等や学内規則等で定められており，これらを遵守することは当然のことであるので，本章で，これらを重ねて記述することは行わない．本章の記述は，遵守事項であると特に断りのない限り，一般利用者やシステム管理者が

行う標準的な行動を記述したものである. 情報セキュリティマネジメントに従事する者が，本ポリシーを運用するにあたって，本ポリシーの標準的な行動を，遵守事項であるかのように誤解し，そのように利用者に指導を行ったり，報告等を求めるだけの形式的なだけの運用を行ったりすることは，利用者を委縮させ，混乱を招き，無用な手間を増やし，情報資産の有効な活用を減退させ，情報セキュリティマネジメントの失敗を招く可能性があるので，情報セキュリティポリシーに従事する者は，そのような誤解を助長することが無いように十分に注意する.

情報セキュリティマネジメントに従事する者は，常に，最新の情報セキュリティ技術に関する調査を行いながら，本学の情報セキュリティ施策に対する利用者の不満や改善点の収集を行い，ときには，利用者に対して，本ポリシーに記述された標準的な行動に替わる適切な行動を具体的に提示することによって，本学の教育等をさらに発展させ充実させるものとする. 情報セキュリティマネジメントに従事する者が，本章の記述に不備が見つかったときや，より簡素な手続きがあるときに，すみやかに学内に周知できるようにするために，学内向けの周知手続きは，別途定める.

６．１　パスワードの使用

（目的）

パスワードは，本人確認のための大切なものである. 不正利用，不正アクセス等の可能性を軽減し，情報セキュリティの確保を行うために，パスワードの適切な使用に関する対策基準を定め，利用者に周知し，理解を求めることとする.

（対象）

情報通信機器やインターネットサービスの利用者.

（項目）

一. パスワードは，英語の大文字，英語の小文字，数字等を組み合わせた８個以上の文字列とし，推測されにくいようにする. 可能な限り，パスワードの中に英記号を含める. 但し，サービスの提供者がパスワードについて別に定めている場合にはそれに従う.

二. インターネットサービスの利用で，インターネットサービスにパスワードが設定

できない場合には，不特定多数からのアクセスの可能性があるので，同等の機能を持った，他のサービスを利用する．合理的な理由があり，パスワードを設定せずにインターネットサービスを利用するときは，必要のないデータは格納しない，必要がなくなった時点でデータはすぐに消す，たとえ暗号化をしていたとしても，ファイル名等が不正攻撃の手掛かりになる可能性があるので，機密情報や個人情報は極力格納しないなどの，十分に安全が確保できる対策を講じる．

三．パスワードは，他人に知られないように，適切な方法で保管する．本体やディスプレイなどにパスワードを書いた紙を張り付けておくようなことは避ける．

四．パスワードを適切に管理するために，可能な範囲で，パスワード管理ソフトウェアを利用する．

五．ログイン時にパスワード以外にセキュリティコードを入力しないとログインできない仕組みである二段階認証が利用できるときは，可能な限り，二段階認証を利用する．このときのセキュリティコードも，他人に知られないように，適切な方法で保管する．

六．操作の代行を依頼するなどで，他人に自分のパスワードを一時的に貸す場合にも，適切にパスワードを管理する．貸し出しが終わった後は，パスワードを変更する．

七．離席するなどで，情報通信機器を手放す場合には，可能な限りログアウトを行い，システムの不正アクセスやパスワードの漏えいを防ぐ．

八．パスワードの漏えいが確認できた場合には，直ちに当該情報通信機器の停止，学内情報サービスの利用の停止，インターネットサービスの利用の停止などで，それ以上の不正利用や不正アクセスが発生しないような対策を行う．その後，パスワードの変更などの適切な対策を行う．機密情報や個人情報を扱っている情報通信機器や学内情報サービスやインターネットサービスで，パスワードの漏えいが確認できた時には，情報セキュリティ事故として取扱い，当事者は，調査や対策などに協力する．

６．２　電子メールソフトウェアの使用

（目的）

電子メールソフトウェアは，情報交換に欠かせない．一方で，宛先の設定ミスによる情報漏えい，同一文面を複数の宛先に同報するときの宛先情報の漏えいの危険がある．

さらには，詐欺的な電子メールを送り付けてくることにより，コンピュータウイルス等に感染させたり，情報を漏えいさせたりすることを試みる外部からの攻撃などの危険もある．情報セキュリティの確保を行うために，電子メールソフトウェアの適切な使用に関する対策基準を定め，利用者に周知し，理解を求めることとする．ＳＮＳなどを用いて外部との情報共有や情報交換を行う場合にも，本節の電子メールソフトウェアについての標準的な行動と同様の行動をとる．

（対象）

情報通信機器やインターネットサービスの利用者で，それらで，電子メールソフトウェアを使用する場合．

（項目）

一．利用者自身で，コンピュータウイルスが添付された電子メールに対処する．怪しい電子メールが届き，添付ファイルが添付されていた場合には，安易に，添付ファイルを開く操作を行わない．添付ファイルについては，ウイルス対策ソフトウェアでスキャンするか，自動でスキャンするように設定する．ウイルス対策ソフトウェアは，１００％の精度で漏れなく検出できるわけではないことを理解して，添付ファイルを開いた後の挙動にも十分に注意を払う．

二．利用者自身で，不当な勧誘や不当な広告を行う電子メールに対処する．怪しい勧誘や広告が載った電子メールが届いたときは，安易に，返信したり，本文中の勧誘に従ったりしない．

三．利用者自身で，偽サイト（フィッシングサイト）への誘導を行う電子メールに対処する．電子メールの差出人はどのようにでも詐称でき，メールの件名なども自由に設定できる．特に，銀行，クレジットカード会社，信販会社，オンラインショッピング，懸賞など金銭や商取引に関わるような電子メールが届き，特定サイトへの誘導を行っている場合には，偽サイト（フィッシングサイト）への誘導である可能性に十分に注意し，自らのプライバシを安易に開示しない．電子メールが記載している会社名などに直接連絡を取り，確認などを行う．

四．利用者自身で，コンピュータウイルス等に感染させることが目的のサイトへの誘導を行う電子メールに対処する．メール本文中のリンクなどを安易にクリックする

操作を行わない．電子メールの本文中に見知らぬ URL が記載されている場合，こうした URL が業務や修学等に役立つ可能性は確かにあるものの，偽サイト（フィッシングサイト）への誘導である場合もある．必要の無い限り，当該サイトにアクセスしない．必要な場合でも，十分に安全を確認する．

五．利用者自身で，偽メール（フィッシングメール）に対処する．機密情報や個人情報の提供を要求する電子メールに対しては，十分に確認を行う．電子メールでの依頼に対して，電子メールの差出人などに，機密情報や個人情報を提供するときは，依頼が書いてある電子メールの本文や，差出人のメールアドレスなどをよく確認する．差出人に直接電話で確認したり，本人に情報を直接手渡しするなどの方法も検討する．

六．本学の学生や第三者の複数の宛先に，同一の内容で電子メールを同報するときは，宛先メールアドレスそのものがプライバシにあたる可能性があるため，ＢＣＣに設定する．但し，教職員のメールアドレスは公知の個人情報として取扱うので，ＢＣＣに設定する必要はない．

七．利用者は，機密情報や個人情報を電子メールで送信するときは，宛先にミスがないことを十分に確認する．

八．電子メールソフトウェアに，電子メールの送信操作後に，送信取消ができる機能のある場合には，可能な限りその機能を有効化しておく．そのことで，宛先ミスなどの問題に気付いたときに，送信取消ができるようにしておく．

九．紙形式で配布・回覧された機密情報や個人情報を，電子化して電子メールで送信することは可能な限り避ける．どうしても必要な場合には，当該情報の作成者あるいは配布者の事前了解を得る．

十．学生の健全な育成のために，学生本人やその保護者，保証人，代理人などに，授業の出席状況のプライバシに関する情報を電子メールで知らせたり，登校できない理由等（健康上の理由，経済上の理由，事件・事故など）のプライバシに関する情報を電子メールでやり取りすることはありえるものの，いかなる形であれ，学生のプライバシに関する情報が第三者に漏えいしないように，十分に注意する．例えば，電子メールのプリントアウトなどを，第三者に見える状態で放置するようなことは避ける．なお，学生の個人情報を取扱う場合には，当該学生の保証人，保護者，代理人については第三者から除外する．

十一. 機密情報や個人情報の集合体の全てまたは一部分を電子メールの添付ファイルで送信するときは，パスワードで暗号化された暗号化ファイルで送信する．パスワードは，英語の大文字，英語の小文字，数字等を組み合わせた８個以上の文字列とし，推測されにくいようにする．可能な限り，パスワードの中に英記号を含める．その場合，復号のためのパスワードは，添付ファイルを添付した電子メールの本文の中には記述せずに，別の電子メール等で伝えたり，電子メールソフトウェアに付随する本人通知・確認機能を利用したりなどで，宛先の設定ミスによる事故の可能性を軽減する．

十二. 電子メールの宛先の設定ミスに対する対策として，ストレージの利用がありえる. 学内のファイルサーバ, 学内の情報サービスが提供するオンラインストレージ, インターネットのオンラインストレージなどのストレージで, 下記の機能などがあるときは, 電子メールの宛先の設定ミスに対する対策として有効である可能性がある．

- パスワードによる認証機能が付いていて，本学の利用者だけがログインしてデータにアクセスできるように，データのアクセスを制限できる機能がある．
- ストレージに置いたファイルの読み取り時に，開示要求のメッセージがストレージの保有者に送られて，開示の拒否ができる機能がある．

電子メールでの送付よりも，ストレージを利用する方が，宛先の設定ミスに起因するデータ漏えいの可能性が少ないと判断する場合には，当該ストレージの利用を検討する．このときも，機密情報や個人情報のファイル自体を暗号化するなどで，安全を確保する．

十三. 宛先に設定ミスをして，機密情報や個人情報を送付したときは，直ちに，当該宛先にその消去を依頼する．

十四. 詐欺的な電子メールの求めに応じて，電話，手紙，ＦＡＸ，電子メール，Ｗｅｂページのフォーム等で，関係の無い学生や，関係の無い外部の第三者に機密情報や個人情報を漏えいさせたときは，それ以上，安易に，詐欺先に直接連絡を試みることは，被害の拡大を防ぐために避ける．

十五. 機密情報や個人情報の集合体の全てまたは一部分を，暗号化を行わずに，関係の無い学生や，関係の無い外部の第三者に送信したときは，情報セキュリティ事故

として取扱う．当事者は，送付内容，宛先を報告するとともに，調査や対策などに協力する．

十六．本学で，電子メールソフトウェアの種類とバージョン，メールソフトの設定，メーリングリスト等の利用手順などについて指示することがある．その場合は，指示に従うこと．

６．３　Ｗｅｂブラウザの利用

（目的）

Ｗｅｂブラウザは，情報収集等に欠かせないだけでなく，ゼルコバやセレッソなどの学内の各種情報サービスの利用にも必要不可欠である．一方で，偽サイト（フィッシングサイト）による情報の漏えいや，Ｗｅｂブラウザの誤操作により意図せぬソフトウェアのインストールを行ってしまうなどの危険がある．情報セキュリティの確保を行うために，Ｗｅｂブラウザの適切な使用に関する対策基準を定め，利用者に周知し，理解を求めることとする．

（対象）

Ｗｅｂブラウザを使用する利用者．

（項目）

一．Ｗｅｂブラウザを用いて，ソフトウェアを探し，インストールを行うとき，利用者自身で，コンピュータウイルスを含んだソフトウェアをインストールしないように対処する．インターネットで，ソフトウェアをダウンロードして，使用するときは，ウイルス対策ソフトウェアでスキャンするか，自動でスキャンするように設定する．ウイルス対策ソフトウェアは，１００％の精度で漏れなく検出できるわけではないことを理解して，インストール後の挙動にも十分に注意を払う．

二．本来有料である映画，音楽，アニメ，漫画，アプリ等が無料でダウンロードできるかのようなＷｅｂページがあった場合，著作権侵害の危険，コンピュータウイルス等の感染の危険があるので，当該Ｗｅｂページを使用しない．誤ってダウンロードを行い，送金の指示，連絡の指示，情報通信機器をロックしての身代金の要求等があった場合には，慌てずに，本学の共同利用センターの相談窓口等に相談する．

本学の共同利用センターは，この種の相談の場合には，特に本学が定める場合を除き，相談の秘密を守るものとするとともに，必要に応じて，匿名での相談にも応じるものとする．

三．Ｗｅｂブラウザの利用時に，不正請求を行う表示やポップアップウインドウが現れた場合には，利用者自身で適切に対処する．利用者は不正請求やそれに伴う自らの個人情報の提供には応じない．不安を感じる場合には，Ｗｅｂブラウザの画面をスマートフォンのカメラ等で撮影し，本学の共同利用センターの相談窓口等に相談する．本学の共同利用センターは，この種の相談の場合には，特に本学が定める場合を除き，相談の秘密を守るものとするとともに，必要に応じて，匿名での相談にも応じるものとする．

四．Ｗｅｂブラウザの利用中に，そのつもりがないにも関わらず，ソフトウェアのインストール等に関する表示が現れた場合には，慌てずに，ソフトウェア名等を確認し，ダウンロードやインストールの要求の表示を消すなどで，覚えのないソフトウェアはインストールしない．そのとき，「ウイルス対策ソフトウェア」，「システムの問題解消」のような警告が表示されたとしても，偽物のソフトウェア（偽装ウイルス対策ソフトウェア等）である可能性がある．警告を鵜呑みにはせずに，信頼できるウイルス対策ソフトウェア等のみを使用するようにする．

五．Ｗｅｂブラウザの使用中，あるいはそれ以外のときにも，「ウイルスへの感染」，「スパイウェアへの感染」などのポップアップウインドウによる警告表示が出て，サイトへの誘導や，ソフトウェアのインストールの表示が表示されたとき，それが見慣れない表示である場合には，偽物のソフトウェア（偽装ウイルス対策ソフトウェア）である可能性がある．激しい色，点滅表示，ことさらに「マイクロソフト」，「Windows オペレーティングシステム」，「ウイルス」，「スパイウェア」，「問題発見」，「このままでは危険」などの危険をあおる場合ほど，偽物の可能性が高い．警告を鵜呑みにはせずに，信頼できるウイルス対策ソフトウェア等のみを使用するようにする．

六．Ｗｅｂブラウザでの表示はどのようにでも詐称できる．ＨＴＭＬの機能により，ポップアップウインドウを表示することもできる．これらは，正当なＷｅｂページ，オペレーティングシステムの正当なポップアップウインドウと見分けがつかないほど巧妙な場合がある．以上のことを，利用者は，十分に理解する．Ｗｅｂブラウ

ザで「同意」や「送信」等のボタンを押す場合は十分に注意する．Ｗｅｂブラウザのフォームで機密情報や個人情報を記入する場合にも十分に注意する．

七．偽サイト（フィッシングサイト）により，機密情報や個人情報を漏えいさせたときは，それ以上，安易に，詐欺先に直接連絡を試みることは，被害の拡大を防ぐために避ける．

八．Ｗｅｂブラウザを利用していて，機密情報や個人情報の集合体の全てまたは一部分を，暗号化を行わずに，関係の無い学生や，関係の無い外部の第三者に提供したときは，情報セキュリティ事故として取扱う．当事者は，提供内容，提供先を報告するとともに，調査や対策などに協力する．

九．本学で，Ｗｅｂブラウザの種類とバージョン，Ｗｅｂブラウザの設定について指示することがある．その場合は，指示に従うこと．

６．４　データのバックアップの実施

（目的）

個人利用機器では，必要なデータのバックアップは各自で行うことになる．バックアップが無い場合には，誤操作や情報通信機器の故障などによってデータが消失し，業務や修学に支障が出る可能性がある．従って，バックアップは重要である．一方で，ＣＤ－Ｒ，ＤＶＤ－Ｒ，外付けのハードディスク，ファイルサーバ，オンラインストレージ等にバックアップした場合，そこからの情報漏えいの危険もある．情報セキュリティの確保を行うために，データのバックアップの実施に関する対策基準を定め，利用者に周知し，理解を求めることとする．

（対象）

情報通信機器やインターネットサービスで，データを取扱う場合．

（項目）

一．利用者は，可能な限り，業務や学修に必要なデータのバックアップを行う．特に，内蔵ハードディスク等の動作に，異常や不安を感じる場合などは，適宜バックアップを実施する．

二．身代金要求ウイルス（ランサムウェア）のような，悪意を持ってデータを暗号化

もしくは破壊し，身代金を要求するようなソフトウェアがある．身代金を払ったとしてもデータの復活が出来る保証は無いし，身代金要求ウイルス（ランサムウェア）等によって業務が長期間中断した場合などは，本学の社会的信用を損なう可能性がある．そこで，業務の継続等に関わる重要なデータは，バックアップの実施後に電磁的記録媒体を情報通信機器から切り離し，鍵のかかる容器などで厳重に管理するなどで，身代金要求ウイルス（ランサムウェア）等によるデータの破壊や消失を防ぐ．

三．誤操作によってデータを消失した場合や，機器の故障によってハードディスク全体等が読めなくなった場合でも，適切な処置によってデータを復活できる場合がある．慌てて操作を試すのではなく，本学の専門家あるいはデータ救出を専門とする外部業者に落ち着いて相談する．そのときは，業務継続について，部局等で適切に措置し，余裕を持ってデータの回復が行えるようにするとともに，業務を中断させないことだけに固執するあまり，誤った手順での業務を行わないように十分に気を付ける．そのための，人的・組織的対策を講じる．

四．外部業者にデータの復活作業を依頼するときは，外部業者が不適切な作業等を行うことにより情報漏えいを起こさないように十分に監督する．外部業者にデータの復活作業を依頼するために，情報通信機器を外部に持ち出すときは，信頼できる業者に依頼を行い，本学の関連規則に従う．

五．学内のファイルサーバ，学内の情報サービスが提供するオンラインストレージ，インターネットのオンラインストレージなどのストレージは，一般の電磁的記録媒体に記録する場合と違って，紛失・置忘れや盗難の危険が少ない可能性があるもの．一方で，不正アクセスによる情報漏えい，不適切な設定による情報漏えい，インターネットのオンラインストレージ業者等によるデータの読み取り（例えばクロール操作）の危険があるので，適切なパスワードの設定と管理，データアクセス権限の適切な設定，データの暗号化などに十分に気を付ける．

六．インターネットのオンラインストレージにバックアップをする場合には，次のことに気を付ける

- 信頼できる業者のオンラインストレージにバックアップする．
- 突然，オンラインストレージサービスが廃止され，データが利用できなくなる場合があるので，そのための対策を事前に行っておく．

- オンラインストレージのサービスにログインするための適切なパスワードを設定し，適切に管理する．
- 機密情報や個人情報を含むファイルをオンラインストレージにバックアップするときは，パスワードで暗号化する．パスワードは，英語の大文字，英語の小文字，数字等を組み合わせた８個以上の文字列とし，推測されにくいようにする．可能な限り，パスワードの中に英記号を含める．
- 機密情報や個人情報を含むファイルをオンラインストレージにバックアップするときは，たとえファイルが暗号化されていたとしても，ファイル名そのものなどが攻撃者への手掛かりとなる可能性があるので，ファイル名は適切に設定する．機密情報や個人情報を含むファイルをオンラインストレージにバックアップするときは，オンラインストレージの保有者のみか，保有者と特定の関係者のみがアクセスできるように設定する．データファイルのリンクを知っていれば誰でもアクセスできたり，サーチエンジンなどで検索すればだれでもアクセスできたりする機能である自動共有機能等の有無を必ず確認し，その機能を解除する．機能が解除できないときは，当該オンラインストレージの使用を避ける．

６．５　本学の情報ネットワークの利用とインターネットサービス利用

（目的）

本学の情報ネットワークは，ゼルコバやセレッソなどの学内の各種情報サービスの利用にも必要であるし，Ｗｅｂブラウザ，電子メールソフトウェア，各種インターネットサービスの利用などにも必要である．一方で，本学の情報ネットワークの利用並びにそれを用いたインターネットサービス利用では，次の４つが問題である．

１．学内の定期試験等，重要な行事において本学の情報ネットワークを用いる場合，本学の情報ネットワークの障害が発生すると，当該行事の運営に支障が出る．
２．無線ＬＡＮは，通信パケットを盗聴できる危険がある．盗聴によりパスワード等の重要な情報が漏えいする危険がある．
３．本学の情報ネットワークのインターネットへの接続については，本学が定めるフ

ァイヤウオール機器の運用基本方針により，ファイヤウオールが運用されている．さらにはネットワークの要所にはファイヤウオールが設置されている場合がある．しかし，ファイヤウオールは万能ではなく，サイバー攻撃等を確実に防げるということはない．さらには，個々の利用者の業務上もしくは修学上の必要に応じた適切なファイヤウオールの設定を行うには，個々の利用者からの適切な情報提供と協力が必要となる．

４．時には，情報通信機器を外部に持ち出して使用する場合がある．ファイヤウオール等で守られた本学の情報ネットワークのときと同じ設定で，公衆ＬＡＮを使う場合に，本学の情報ネットワークでは問題にならなかった当該情報通信機器の脆弱性が問題になる可能性がある．

そこで，情報セキュリティの確保を行うために，本学の情報ネットワークの適切な利用とインターネットサービスの適切な利用に関する対策基準を定め，利用者に周知し，理解を求めることとする．

（対象）

次のいずれかに当てはまる者を対象者とする．

- 学内の定期試験等，重要な行事において本学の情報ネットワークを利用する利用者
- 無線ＬＡＮを使用する情報通信機器の利用者
- 本学の情報ネットワークを利用して，インターネットサービス利用を行う利用者

（項目）

一．本学の情報ネットワークは，計画的な停止や，予期せぬ障害が不可避であることを理解する．重要な行事を，本学の情報ネットワークを用いて行うときは，学内ネットワークの障害により，当該行事の実施が出来なくなるような事態や，学生の不利益が生じるような事態を避けるために，当該行事実施者の責任において，学内ネットワーク障害時の行動計画や，適切な代替手段（定期試験の場合であれば，紙形式での問題・解答用紙などを代替手段として準備しておくなど）を用意する．必要

に応じて，予備の情報通信機器を用意する．

二．入学試験や本学の正課の定期試験を本学の情報資産を用いて行い，その途中で本学の情報資産の障害によって，それらの実施が出来なくなったり，特定の学生に不利益が生じる可能性が生じたりなどの問題が起き，適切な対処あるいは代替手段が何ら実施されず，事故に至った場合には，情報セキュリティ事故として取扱う．

三．本学の情報ネットワークで，無線ＬＡＮを使用するときは，通信内容をＷＰＡ方式，ＷＰＡ２方式，ＴＫＩＰ方式，ＡＥＳ方式などで暗号化して通信を行う．学外に情報通信機器を持ち出して公衆無線ＬＡＮを使用するときも，同じく暗号化して通信を行う．

四．本学の情報ネットワークでの，無線ＬＡＮの使用について，本学が，無線ＬＡＮの暗号方式等について指示することがある．その場合は，指示に従うこと．

五．利用者は，インターネットサービス利用について，学内からポート８０番でのインターネットサービスへの接続を行え，外部への電子メール発信が行えるようなファイヤウオール設定を行っている以上，他のポートをいかに遮断しようが，情報流出のリスクが存在していることを正しく理解する．

六．利用者は，本学が定めるファイヤウオール機器の運用基本方針の目的として，学外からのアクセス集中による障害を防ぐ，非常時に学内から大量のパケットが爆発的に放出されるような異常を防ぐ，情報セキュリティ事故の発生時に被害の拡大を防ぐ，外部からのサイバー攻撃を防ぐというような情報セキュリティ上の目的があることを正しく理解する．

七．利用者は，本学が定めるファイヤウオール機器の運用基本方針の運用において，プライバシが尊重されていることを正しく理解する．

八．本学の常勤教職員は，インターネットサービス利用において，インターネットサービスに接続できないなどのインターネットサービス利用上の支障を感じるときは，本学が定めるファイヤウオール機器の運用基本方針により運用されているファイヤウオールに関する設定の変更を共同利用センターに申請できるものとする．このことにより，本学におけるインターネットサービス利用をさらに発展させる．

九．八で定める申請を円滑に実施するため，申請には次の項目を含めることとする．

- 氏名
- 所属

- 職名
- 内線番号
- メールアドレス
- ＩＰアドレス
- ポート番号
- プロトコル

十. 八で定める申請は遅滞なく処理される. 八で定める申請が不許可になる場合には, 理由と異議申立先が申請者に遅滞なく連絡される.

十一. 八で定める申請によりポートが解放された場合, そのポート経由での情報流出を防ぐための技術的対策は申請者自身が行う.

十二. 学内の管理されたネットワークとは違って, 学外のネットワークは適切に管理されていない可能性がある. 情報通信機器を学外の情報ネットワーク（例えば, 公衆のＷｉ－Ｆｉアクセスポイントに接続するなど）で使用するときは, 利用者は, 不正アクセスやサイバー攻撃に対する次の技術的対策を講じる.

- 情報を漏えいさせる危険を軽減するために, ＬＡＮ内の他の利用者がアクセスできるディレクトリ共有機能／フォルダ共有機能は必要が無ければ解除する.
- 重要な情報は適切に暗号化する.
- 適宜, コンピュータウイルスのスキャンを行う.

十三. インターネットサービスの利用において, 見知らぬ人からの氏名, 住所, 電話番号, 写真等の要求が来たときは, 利用者は, それが悪用される危険性を十分に意識し, これらの要求は, 利用者自身で, 慎重に検討する. 不安を感じるときは, 本学の共同利用センターの相談窓口等に相談する.

６．６　共同利用機器の利用

（目的）

共同利用機器の情報セキュリティの確保のためには, 共同利用機器のシステム管理者が, 種々の機能制限や設定を行うことを, 共同利用機器の一般利用者は, 十分に理解し, 支持し, 協力する必要がある. 共同利用機器の利用における一般利用者の行動に関する対策基準を定め, 利用者に周知し, 理解を求めることとする.

（対象）

共同利用機器を利用する一般利用者.

（項目）

一．一般利用者は，共同利用機器の本来の機能が制限されていたり，自由な設定変更が行えない場合であっても，それらが情報セキュリティの維持のための実施されていることを理解し，支持する.

二. 一般利用者は，共同利用機器の設定が事前の予告なく変更された場合であっても，それらが情報セキュリティの維持のため緊急措置等である可能性を理解し，支持する.

三．一般利用者は，自らのデータファイル等が事前の予告なく隔離されたり，削除されたりした場合であっても，その措置が情報セキュリティの維持のための緊急措置等である可能性を理解するとともに，システム管理者はプライバシの保護に十分な配慮を行っていることを理解し，支持する.

四．一般利用者は，システム管理者が発行するパスワードを適切に使用する．システム管理者の事前了解なくパスワードを貸し借りすることは避ける.

五．一般利用者は，共同利用機器に，データファイルを保存するとき，適切なアクセスモードを設定する．また，必要に応じて，データファイルを暗号化する.

六．共同利用機器のハードウェアやソフトウェア，共同利用機器が提供するサービスは，適宜，見直しが行われることを理解し，支持する.

６．７　情報通信機器のシステム管理

情報セキュリティの確保のために，情報通信機器のシステム管理において，システム管理者が行う標準的な行動を対策基準として定め，システム管理者を含む利用者に周知し，理解を求めることとする．個人利用機器については，個々の利用者が，当該個人利用機器のシステム管理者になり，本節の対策基準を用いる.

６．７．１　ソフトウェアのアップデートとバージョンアップ

（目的）

情報セキュリティの確保のために，ソフトウェアのアップデートやバージョンアップを適切に行い，最新の状態を保ち続けることが有効である．特に，サポート期限の切れたバージョンのソフトウェアは使用せずに，バージョンアップするか，同等機能の別のソフトウェア等に交換する必要がある．一方で，バージョンアップに伴って，操作感が変化して業務等の効率が一時的に低下する可能性があったり，旧バージョンにおいて使用していたデータが正常に扱えなくなる可能性があるなどの問題がある．ソフトウェアを最新の状態に保ちながら，業務等に支障が出ないようにするために，ソフトウェアのアップデート，バージョンアップに関する対策基準を定め，利用者に周知し，理解を求めることとする．

（対象）

ファームウェア，オペレーティングシステム，アプリケーションソフトウェア（オフィスソフトウェア，ウイルス対策ソフトウェア，Ｗｅｂブラウザ，ＰＤＦビューワ，Ｆｌａｓｈプレーヤ等）などのソフトウェアが搭載されていて，それらがアップデート，バージョンアップ可能な情報通信機器を管理するシステム管理者．

（項目）

一．システム管理者は，不要なソフトウェアを削除する．

二．システム管理者は，適宜，ソフトウェアのアップデートを行うか，自動でアップデートが行われるように設定し，ソフトウェアを最新の状態に保つ．

三．システム管理者は，授業中等にソフトウェアの自動アップデート等が始まり，授業等の実施に支障が出るなどの事態がなるべく起きないように，可能な限り，事前にアップデート操作を済ませておくなどの対策を行う．

四．サポート期限の切れたバージョンのソフトウェアを，適切な対策を行うこと無しに使い続けることは，情報セキュリティの脅威を増大させる．システム管理者は，余裕をもってバージョンアップあるいは同等機能の別のソフトウェア等に交換することができるように，計画的に準備する．止むを得ず，サポート期限の切れたバージョンのソフトウェアを使う場合には，適切な技術的対策を講じる．

五．ソフトウェアのバージョンアップは，機能が増え，情報セキュリティの脆弱性が減ることが期待できるという効果がある．一方で，ソフトウェアのバージョンアッ

プにより，以前動作していた周辺機器が動作しなくなる可能性，操作感が変わる可能性，旧バージョンにおいて使用していたデータ（マクロ等）が正常に扱えなくなる可能性，バージョンアップ時の操作ミスによりデータを消失する可能性などの危険がある．そこで，システム管理者は，以下を技術的対策として実施する．

- ソフトウェアのバージョンアップ作業は，余裕をもって計画的に行う．
- ソフトうウェアのバージョンアップの前に，重要なデータをバックアップする．
- 可能であれば，事前にバージョンアップ後に支障がないことの調査や検証を実施しておく．
- 可能であれば，万一の場合のための代替機を準備しておく．

六．バージョンアップに伴って問題が発生したときは，システム管理者が旧バージョンに戻すか，代替機でバックアップデータを使用するなどの措置により，業務等を継続する．

６．７．２　パスワードの適切な管理とアクセス権限の設定

（目的）

パスワードは，本人確認のための大切なものである．パスワードによる認証の上，適切なアクセス権限を設定することも，データの不適切なアクセスを防ぐのに重要である．不正利用，不正アクセス等の可能性を軽減し，情報セキュリティの確保を行うために，パスワードの適切な管理や，アクセス権限の設定に関する対策基準を定め，利用者に周知し，理解を求めることとする．

（対象）

次のいずれかに該当する情報通信機器

- パスワードが設定できる機能が搭載されている情報通信機器のシステム管理者
- 利用者が作成し利用するファイルについてのアクセス権限の設定が出来る機能が搭載されている情報通信機器のシステム管理者．

（項目）

一．情報通信機器の不正利用を防ぐために，システム管理者は，システムの利用時に，

パスワードによる認証を行うようにシステムを設定する.

二. 管理の都合上，一時的にパスワードを紙に書いて張り付けるなどで，権限の無い者にパスワードを周知してしまった場合には，当該情報通信機器にパスワードを設定していないのと同じになることを正しく理解する. 貼り付けが終わった後，適切にパスワードを再設定する.

三. システム管理者は，アクセス権限については，個々の利用者が必要とする最小限のアクセス権限を設定する.

四. システム管理者は，ファイルアクセス，データベースアクセス，Ｗｅｂアクセス等のための匿名利用者のアカウントを作成する場合にも，個々の匿名利用者が必要とする最小限のアクセス権限を設定する.

五. システム管理者は，利用者のアクセス権限に変更があったときや，利用者がシステム利用資格を失ったときは，直ちに，アカウントの変更を行い，適正な利用者のみがシステムを利用できるようにする.

六. システム管理者は，パスワードの作成やアクセス権限の設定のために情報通信機器が保持する個人情報を最小限に留める.

七. 遠隔から telnet，ssh，リモートデスクトップ等での操作ができる情報通信機器のシステム管理者は，サイバー攻撃による危険の軽減のため，可能な限り管理者権限での遠隔からのログインが直接できないような技術的対策，可能な限りログイン時のパスワードが盗聴されないための技術的対策を実施する.

６．７．３　コンピュータウイルス等への対策

（目的）

コンピュータウイルス等への感染により，情報通信機器が不正に利用されたり，データが破壊されるだけでなく，感染した情報通信機器が新たな感染源になってしまうという危険がある. コンピュータウイルス等の脅威に関する対策基準を定め，利用者に周知し，理解を求めることとする.

（対象）

- ウイルス対策ソフトウェア等がインストールできる情報通信機器のシステム管理者

- ＵＳＢメモリなどの電磁的記録媒体を差し込んだときに，その中のプログラムを自動実行できる機能を有する情報通信機器のシステム管理者

（項目）

一．システム管理者は，情報通信機器に，ウイルス対策ソフトウェア等をインストールできる場合には，適切なものをインストールする．システム管理者は，適宜，ウイルス対策ソフトウェアのパターンファイル等のアップデートを行うか，自動でアップデートが行われるように設定し，パターンファイル等を最新の状態に保つ．

二．インターネットで配布されているソフトウェアに，コンピュータウイルスが混入している可能性がある．システム管理者は，インターネットで配布されているソフトウェアのインストールを行う前に，可能な限りコンピュータウイルス等のスキャンを行う．

三．パーソナルコンピュータの利用中にポップアップウインドウが開き「コンピュータウイルスを発見したので，対策ソフトウェアをインストールしますか？」のような表示が出ることがある．このような表示は偽物の可能性があるので，安易に「合意」や「続行」などのボタンを押さない．このような表示が出た場合には，使い慣れたウイルス対策ソフトウェアで情報通信機器をスキャンする．

四．システム管理者は，ウイルス対策ソフトウェアは１００％の検出率ではないことを理解する．

五．ＵＳＢメモリ等の電磁的記録媒体を使い，他の人とデータをやり取りするときは，可能な限り，当該電磁的記録媒体のコンピュータウイルス等のスキャンを行う．

六．パーソナルコンピュータにＵＳＢメモリ等の電磁的記録媒体を差し込んだときの自動再生機能は，可能な限り解除しておく．

七．コンピュータウイルス等に感染した可能性があると判断される場合には，可能な限り，直ちに当該情報通信機器をネットワークから切り離し（ＬＡＮケーブルを抜いたり，無線ＬＡＮの機能を切るなど），感染を広めることを防ぐ．その後，可能であれば，コンピュータウイルス等のスキャンを行ない，コンピュータウイルスの有無を確認する．そのとき，ウイルス対策ソフトウェアが表示するウイルス名などの情報を，その後の調査のためにメモ等に書き写しておく．

八．機密情報や個人情報の集合体であるデータベースの全てまたは一部分を，暗号化

を行わずに，ファイルとして格納している情報通信機器で，コンピュータウイルスの感染が確認でき，さらに，関係の無い学生や，関係の無い外部の第三者に機密情報や個人情報の集合体であるデータベースの全てまたは一部分が漏えいした可能性が合理的に疑われるときは，情報セキュリティ事故として取扱う．当事者は，調査や対策などに協力する．

６．７．４　情報通信機器の紛失・置忘れや盗難への対策

（目的）

情報通信機器の紛失・置忘れや盗難により，情報漏えいが発生する危険がある．教育等の発展のため情報通信機器の積極的な利用の推進と，万一の紛失・置忘れや盗難時の被害状況の把握や，再発防止策の策定の容易さを両立させるために，情報通信機器の紛失･置忘れや盗難に関する対策基準を定め,利用者に周知し,理解を求めることとする．

（対象）

紛失・置忘れや盗難の可能性がある情報通信機器のシステム管理者

（項目）

一．ノート型のパーソナルコンピュータ，タブレット，ＵＳＢメモリなどの電磁的記録媒体等，簡単に持ち運べる情報通信機器で，機密情報や個人情報の集合体であるデータベースの全てまたは一部分を，暗号化を行わずに，格納している場合には，システム管理者は，セキュリティチェーン等を使う，ある程度長期間使用しないときは施錠できるキャビネットに格納する，施錠できる居室で保管するなど，実施可能な盗難対策を実施する．

二．情報通信機器の紛失・置忘れや盗難が発生した場合には，システム管理者は，捜査機関等に紛失・置忘れや盗難を届け出る．不要な混乱等を避けるために，届け出は，速やかに，適切に行うとともに，捜査機関等に適切に協力する．その後，紛失・置忘れあるいは盗難したと考えられていた情報通信機器が発見できた場合などは，速やかに，届け出る．

６．７．５　情報通信機器の破棄におけるデータ消去

（目的）

情報通信機器を破棄するとき，適切にデータを消去しないことにより，情報漏えいが発生する危険がある．情報通信機器の破棄に関する対策基準を定め，利用者に周知し，理解を求めることとする．

（対象）

破棄される情報通信機器のシステム管理者

（項目）

一．システム管理者は，ファイル消去ソフトウェア等を用いて，適切に，ファイルを消去する．あるいは，信頼できる外部業者等に消去を依頼する．

二．ファイル消去ソフトウェアの実行が難しい場合，内蔵の電磁的記録媒体を取り出して，ハンマー等で破壊する．破壊する作業では，作業者の安全に十分に気を付ける．

６．８　インターネットサービス公開における対策基準

（目的）

インターネットを利用して，学外に種々のサービスを提供するインターネットサービス公開では，次の背反しがちな２つの目標を両立させる必要がある．

- インターネットサービス公開の促進が，本学の教育等の充実と発展に必要不可欠である．
- 不正アクセス，情報漏えい，データの消失，インターネットサービス公開に利用している情報通信機器が他への攻撃への踏み台に使用されるなど，情報セキュリティの危険がある．

そこで，インターネットサービス公開を促進し，本学の教育等の充実と発展を進めるとともに，情報セキュリティの確保が容易に行えるようにするために，インターネットサービス公開に関する対策基準を定め，利用者に周知し，理解を求めることとする．

（対象者）

インターネットサービス公開を行うシステムのシステム管理者．

（項目）

一. 本学の常勤教職員は, インターネットサービス公開において支障を感じるときは, 本学が定めるファイヤウオール機器の運用基本方針により運用されているファイヤウオールに関する設定の変更を共同利用センターに申請できるものとする. このことにより, 本学におけるインターネットサービス公開をさらに促進し, 発展させる.

二. 一で定める申請には, 次の項目を含める.

- 氏名
- 所属
- 職名
- 内線番号
- メールアドレス
- ＩＰアドレス
- ポート番号
- プロトコル
- 使用するオペレーティングシステム
- 使用するサーバソフトウェア

三. 一で定める申請は遅滞なく処理される. 一で定める申請が不許可になる場合には, 理由と異議申立先が申請者に遅滞なく連絡される.

四. 一で定める申請によりポートが解放された場合, そのポート経由でのサイバー攻撃を防ぐための技術的対策は, システム管理者が行う.

五. インターネットサービス公開において, 本学の統合認証システムを利用したい場合には, 準備, 運用, 費用負担等について協議する必要があるので, 相当の準備期間をとって, 本学の共同利用センターと事前協議を行うこととする.

六. システム管理者は, 使用するオペレーティングシステムやサーバソフトウェア等の脆弱性に関する情報を常に収集し, 適切な対策を心掛ける.

七. システム管理者は, 可能な限り, インターネットサービス公開へのアクセス記録を残し, それが改ざんされないような技術的対策を実施する.

八. インターネットサービス公開を行っている情報通信機器に対して, 遠隔から telnet, ssh, リモートデスクトップ等での操作ができる場合, 当該情報通信機器の

システム管理者は，サイバー攻撃による危険の軽減のため，可能な限り管理者権限での遠隔からのログインが直接できないような技術的対策，可能な限りログイン時のパスワードが盗聴されないための技術的対策を実施する．

九．システム管理者は，可能な限り遠隔からのアクセスをポート単位，ＩＰアドレス単位で遮断するファイヤウオールソフトウェアを稼働させ，適切に設定する．

十．フォームの記入などのデータ操作を行うサービスを提供する場合には，システム管理者は，可能な限り，SQL インジェクション等の不正なデータ操作への技術的対策を実施する．

十一．外部とのＶＰＮ（仮想プライベートネットワーク）を構成する場合には，システム管理者は，可能な限り，送信元及び宛先ＩＰアドレスや，プロトコルや，通信ポートや，利用時間帯や，総通信量について制限を行うように設定する．

十二．システム管理者は，可能な限り不正なアカウントの検知や，システムファイルの不正な書き換えの検知ができる技術的対策を実施する．

十三．システム管理者は，必要なデータのバックアップを実施し，サービスの可用性を維持する．

十四．システム管理者は，身代金要求ウイルス（ランサムウェア）によるデータの破壊に備え，可能な限り，身代金要求ウイルス（ランサムウェア）によるデータの破壊が困難な方式でのデータのバックアップを実施する．

十五．システム管理者は，可能な限りデータの改ざんの検知ができる技術的対策を実施する．

十六．システム管理者は，データファイルのアクセス権限を適切に設定する．

十七．システム管理者は，可能な限り，サーバソフトウェアの実行権限を，管理者の権限ではなく，専用の匿名利用者の権限に設定する．

十八. システム管理者は, インターネットサービス公開によって知り得た秘密は守る．そのことをサービスの利用者に明言する．

十九．インターネットサービス公開で，機密情報や個人情報を取扱う場合には，機密情報や個人情報の利用目的を特定し，公開する．

付録１．インターネットサービス利用申請書

本学の専任教職員がインターネットサービスを利用し，本学のファイヤウオールの設定に変更の必要を感じたときのためのインターネットサービス利用申請書を定める．

但し，本学のシステム管理上のため，記載事項が変更になったり，管理用の欄が増えることがある．また，インターネットサービス利用申請書の書式は，適宜，改訂される可能性がある．

インターネットサービス利用申請書

年　　月　　日

共同利用センターICT サービス部門長　殿

所属：＿＿＿＿＿＿＿＿職名：＿＿＿＿＿＿氏名：＿＿＿＿＿＿＿＿

内線番号：＿＿＿＿＿＿電子メールアドレス：＿＿＿＿＿＿＿＿＿＿＿＿

下記の通りインターネットサービス利用を申請します．申請にあたり，共同利用センターが定める Internet サービス利用ガイドラインを遵守します．

(1) **通信経路**

学内	**IP アドレス**（1 つを記入）	
学外	**ホスト名もしくは IP アドレス** （複数のときは「/」などで区切る）	
	ポート番号	□ 22 (ssh) □ 9418 (git) □ 110 (pop) □ その他（ポート番号：　　　　　　）
	プロトコル	□ TCP □ UDP

(2) **利用目的および特記事項**

(3) **利用期間**

開始日：　　　年　　月　　日　**終了日**：　　　年　　月　　日

※　利用期間を無期限にしたい場合には，終了日を記入しないこと．また，利用停止を共同利用センターICT サービス部門に通知すること．

付録２．インターネットサービス公開申請書

本学の専任教職員がインターネットサービスを公開し，本学のファイヤウオールの設定に変更の必要を感じたときのためのインターネットサービス公開申請書を定める．

但し，本学のシステム管理上のため，記載事項が変更になったり，管理用の欄が増えることがある．また，インターネットサービス利用申請書の書式は，適宜，改訂される可能性がある．

インターネットサービス公開申請書

年　　月　　日

共同利用センターICT サービス部門長　殿

所属：＿＿＿＿＿＿＿＿職名：＿＿＿＿＿＿氏名：＿＿＿＿＿＿＿＿

内線番号：＿＿＿＿＿＿電子メールアドレス：＿＿＿＿＿＿＿＿＿＿＿＿

下記の通りインターネットサービス公開を申請します．申請にあたり，共同利用センターが定める Internet サービス公開ガイドラインを遵守します．

(1) **サーバ機器と通信経路**

サーバ機器	IP アドレス（1 つを記入）	
	設置場所（建物名，部屋番号など）	
	オペレーティングシステム名	
	公開サービスに使用するサーバソフトウェア名とバージョン番号	
	ポート番号	□ 80 (http) □ 443 (https) □ 22 (ssh) □ その他（ポート番号：　　　　　　）
	プロトコル	□ TCP □ UDP
学外	公開先 IP アドレス	□ 任意の IP アドレスに公開 □ 公開する IP アドレスを下記の通り限定

(2) **サーバ機器における機密情報や学生の個人情報の有無**

□ 機密情報や学生の個人情報はない

□ 機密情報や学生の個人情報を格納する

□ 機密情報や学生の個人情報を格納するだけでなく，収集も行う

(3) **利用目的および特記事項**　（機密情報や学生の個人情報を取扱う場合には，その利用目的も記述）

(4) **利用期間**

開始日：＿＿＿＿年＿＿＿月＿＿＿日　　**終了日**：＿＿＿＿年＿＿＿月＿＿＿日

※　利用期間を無期限にしたい場合には，終了日を記入しないこと．また，利用停止を共同利用センターICT サービス部門に通知すること．

付録３．インターネットサービス公開でのチェックリスト

本学の教職員がインターネットサービスを公開するときに，システム管理者が自ら確認を行うためのチェックリストを定める．

但し，チェックリストの中身は，情報セキュリティ技術の進展，本学の情報通信技術の利活用のさらなる進展等に応じて，適宜，改訂される可能性がある．

インターネットサービス公開でのチェックリスト

□　**オペレーティングシステム**と，公開サービスに利用する**サーバソフトウェア**は，自動的に**アップデート**されるように設定するか，常に手動でアップデートすること.

□　可能な限り，**ウイルス対策ソフトウェア**を常駐させ，ファイルの自動スキャンを行うように設定すること.

□　可能な限り，公開されたインターネットサービスへの**アクセス記録**が残るように，技術的対策を実施すること.

□　可能な限り，**管理者権限**で**遠隔から直接ログインができない**ような技術的対策を実施すること.

□　可能な限り，**遠隔からのアクセス**を**ポート単位**，**ＩＰアドレス単位**で**遮断**する**ファイヤウオールソフトウェア**を稼働させ，適切に設定すること.

□　フォームの記入などのデータ操作を行うサービスを提供する場合には，可能な限り，**SQL インジェクション**等の不正なデータ操作への技術的対策を実施すること

□　データの**バックアップ**を実施すること. 身代金要求ウイルス（ランサムウェア）によるデータの破壊に備え，可能な限り，身代金要求ウイルス（ランサムウェア）によるデータの破壊が困難な方式でのデータのバックアップを実施すること.

□　可能な限り，**データの改ざんの検知**ができる技術的対策を実施すること.

□　公開サービスに扱うサーバソフトウェアが扱うファイルは，可能な限り，**所有者**，**ファイルモード**（書き込み不可など）を**適切に設定**すること.

□　可能な限り，**サーバソフトウェアの実行権限**は，管理者の権限ではなく，**専用の匿名利用者**の権限に設定すること.

□　機密情報や個人情報を取扱う場合には，**機密情報や個人情報の利用目的を特定**し，いつでも開示できるように準備しておくこと.

□　**個人情報を収集するようなサイト**を公開する場合には，可能な限り，本ポリシーの「**付録６**．個人情報等の収集や利用を行うサイト等での個人情報保護方針のひな形」を参考に，個人情報保護方針を定め，当該サイト等で**公開**すること.

付録４．インターネット VPN 設置申請書

本学の専任教職員がインターネットＶＰＮを設置し運用するときのための，インターネットサービスＶＰＮ設置申請書の検討を今後進める．

但し，本学のシステム管理上のため，記載事項が変更になったり，管理用の欄が増えることがある．また，インターネットＶＰＮ設置申請書の書式は，適宜，改訂される可能性がある．

インターネット VPN 設置申請書

年　　月　　日

共同利用センターICT サービス部門長　殿

所属：＿＿＿＿＿＿＿＿＿＿＿＿　職名：＿＿＿＿＿＿　氏名：＿＿＿＿＿＿＿＿＿＿

内線番号：＿＿＿＿＿＿＿＿　電子メールアドレス：＿＿＿＿＿＿＿＿＿＿＿＿＿＿

下記の通りインターネット VPN の設置を申請します．申請にあたり，共同利用センターが定める関連規則を遵守します．

(1) **インターネット VPN 機器と接続設定**

機器	IP アドレス（１つを記入）		
	設置場所（建物名，部屋番号など）		
	オペレーティングシステム名		
	VPN サービスに使用するソフトウェア名とバージョン番号		
接続設定	接続する曜日	□　平日および土曜日午前中のみ □　曜日で制限しない	
	接続する時間帯	時　　分　～　　時　　分	
	接続を許可する学外 IP アドレスの範囲（任意の IP アドレスへの公開は原則認められません）		
	VPN 通信する通信データの元のパケット	プロトコル	□ TCP　□ UDP
		ポート番号	
	VPN で使用するリスナポート	□ 443 □ 992 □ 1192 □ 5555 □ その他（ポート番号：　　）	
	データリンク層トンネリング方式	□ SSH □ TLS □ SSL □ IPsec　□ PPTP □ L2TP □ L2F □ MPLS □ その他（　　）	
	VPN 接続の前の認証方式	□ ワンタイムパスワード方式 □ 電子証明書による方式 □ その他（　　）	

(2) **インターネット VPN の利用者**

(3) **インターネット VPN の接続を行う場所**

(4) **インターネット VPN を使用する情報機器と，そのセキュリティ対策**

(5) **インターネットカフェなど不特定多数が使用する情報機器から利用できる場合は，当該情報機器からの VPN 用パスワード漏えいを防ぐ技術的対策**

(6) **インターネット VPN 機器における機密情報や学生の個人情報の有無**

- □ 機密情報や学生の個人情報はない
- □ 機密情報や学生の個人情報を格納する
- □ 機密情報や学生の個人情報を格納するだけでなく，収集も行う

(7) **利用目的および特記事項**　（機密情報や学生の個人情報を取扱う場合には，その利用目的も記述）

(8) **利用期間**

開始日：　＿＿＿＿年　＿＿＿月　＿＿＿日　　**終了日**：　＿＿＿＿年　＿＿＿月　＿＿＿日

※　利用期間を無期限にしたい場合には，終了日を記入しないこと．また，利用停止を共同利用センター ICT サービス部門に通知すること．

※　審査において追加情報の提出を求めることがある．

付録５．不特定多数がアクセス可能な無線アクセスポイントの設置申請書

本学の専任教職員が，不特定多数によるアクセス可能な無線アクセスポイントを設置し運用するときのための，申請書の検討を今後進める．ここでいう「不特定多数」とは，本学の情報システムの利用資格の無いものが利用でき，かつ，１つのパスワードを複数の利用者で共有して利用する（つまり，無線アクセスポイントへの利用者の特定が不可能であるもの）ものをいう．

但し，本学のシステム管理上のため，記載事項が変更になったり，管理用の欄が増えることがある．また，書式は，適宜，改訂される可能性がある．

不特定多数がアクセス可能な無線アクセスポイントの設置申請書

年　　月　　日

共同利用センターICT サービス部門長　殿

所属：＿＿＿＿＿＿＿＿＿＿職名：＿＿＿＿＿＿氏名：＿＿＿＿＿＿＿＿＿＿

内線番号：＿＿＿＿＿＿＿電子メールアドレス：＿＿＿＿＿＿＿＿＿＿＿＿＿＿

下記の通り不特定多数がアクセス可能な無線アクセスポイントの設置を申請します．申請にあたり，共同利用センターが定める関連規則を遵守します．

(1) **無線アクセスポイント機器と設定**

機器	IP アドレス（１つを記入）	
	MAC アドレス（１つを記入）	
	設置場所（建物名，部屋番号など）	
	機器名	
	設置期間	年　　月　　日　～ 年　　月　　日
接続設定	SSID	
	暗号化方式	

(1) 不特定多数がアクセス可能な無線アクセスポイントを必要とする理由

(2) 利用者の範囲

(3) パスワードを不正利用されないための手立て

(4) 学内ネットワークへの影響等を緊急に調査する必要が出てきた場合の緊急連絡先

(5) 無線アクセスポイントに接続された他のパーソナルコンピュータのファイル（例えば Windows の共有フォルダ）へのアクセスを抑止する技術的方策

※　無線アクセスポイントを複数人に利用させる場合で，利用者ごとに個別のパスワードを発行せずに，共通のパスワードを使わせる場合には，不特定多数がアクセス可能であるとして，この申請書で申請を行ってください．利用者が 1 名に限られる場合には，利用者が特定されているので，本申請の必要はありません．

付録６．個人情報等の収集や利用を行うサイト等での個人情報保護方針のひな形

サイトを用いて個人情報を取得し，利用する場合には，サイト管理者は，可能な限り，個人情報の取扱いに関する規範である個人情報保護方針を，できるだけ個人情報の該当者本人の知り得る状態に置くことにより，関係者の理解を得る．

個人情報保護方針のひな形を下記に示す．下のひな形を利用する場合には，個人情報の利用目的を適切に記入するとともに，適切に加筆や変更を行うものとする．なお，文書等を用いて個人情報を取得し，利用する場合には，「**付録７**．個人情報保護規範のひな形」のひな形を用いる．

当サイトで取扱う個人情報に関する個人情報保護方針

当サイトでは，以下の通り個人情報保護方針を定め，個人情報保護の取り組みを行っています.

１．基本的考え方

収集した個人情報は，利用目的の範囲内で適切に取扱います.

２ 個人情報の利用目的

当サイトで取得した個人情報は，以下の目的で利用します.

- ＜利用目的を記載＞
- ＜利用目的を記載＞

３．個人情報の管理

当サイトで取得した個人情報は，次の方針により，厳重に管理します.

- 本人の申し出により，遅滞なく，正確かつ最新の状態に更新します.
- 漏えい，紛失，改ざん，不正アクセスなどの不適切な取扱いが生じないように，技術的対策などの必要な措置を講じて，適正に管理します.

４．個人情報の第三者への提供の禁止

当サイトで取得した個人情報は, 次のいずれかに該当する場合を除き, 利用目的以外のために自ら利用したり, 第三者に提供することはありません.

- 本人またはその代理人の同意が得られる場合
- 法令に基づく開示要請があった場合
- 不正アクセス，脅迫等の違法行為があった場合
- 個人情報の取扱いの全部または一部を外部業者等に委託する場合
- その他，本サイトの管理者が定める特別な理由に該当する場合

但し，統計的に処理された当サイトの利用状況情報や，利用者属性情報は公表することがあります.

５．個人情報の照会等に対する対応

当サイトで取得した個人情報に対して，照会や修正や削除などを希望される場合は，下記にお問い合わせください．本人確認の上，開示等を行うかの審査を，遅滞なく実施します.

６．適用範囲

本個人情報保護方針は，当サイトにおいてのみ適用されます.

７．その他

以上の個人情報保護方針は改定することがあります. 改定された個人情報保護方針は, 当サイトで公開します.

お問い合わせ

本サイトでの個人情報の取扱いに関するお問い合わせは，下記のサイト管理者までご連絡ください.

＜サイト管理者の電子メールアドレスや電話番号などの問い合わせ先を記入＞

付録７．個人情報保護規範のひな形

文書等で個人情報を取得し，利用する場合には，個人情報を管理する者は，可能な限り，個人情報の取扱いに関する独自の個人情報保護規範を定め，個人情報を取扱う者に適切な指示や指導を実施するとともに，個人情報保護規範をできるだけ個人情報の該当者本人の知り得る状態に置くことにより，関係者の理解を得る．

個人情報保護規範のひな形を下記に示す．下のひな形を利用する場合には，個人情報を取扱う部局名や，個人情報の利用目的を適切に記入するとともに，適切に加筆や変更を行うものとする．なお，サイトを用いて個人情報を取得し，利用する場合には，「**付録６**．個人情報等の収集や利用を行うサイト等での個人情報保護方針のひな形」のひな形を用いる．

個人情報保護規範

＜個人情報を取扱う部局名等＞では，本学の学生の健全な育成と，本学の適切な管理運営のために個人情報を取扱っています．個人情報の適正な取扱いを確保するために、個人情報の保護に関する法令等を遵守するとともに，学校法人福山大学が定める「学校法人福山大学個人情報管理基本方針」，本学が定める「福山大学情報倫理規程」を遵守します．さらに，以下の通り，個人情報保護規範を定め，個人情報保護，プライバシ保護の取り組みを行っています．

１．基本的考え方

収集した個人情報は，利用目的の範囲内で適切に取扱います．

２ 個人情報の利用目的

取得した個人情報は，以下の目的で利用します．

- **＜利用目的を記載＞**
- **＜利用目的を記載＞**

３．個人情報の管理

取得した個人情報は，次の方針により，厳重に管理します．

- 本人の申し出により，遅滞なく，正確かつ最新の状態に更新します．
- 漏えい，紛失，改ざん，不正アクセスなどの不適切な取扱いが生じないように，技術的対策などの必要な措置を講じて，適正に管理します．

４．個人情報の第三者への提供の禁止

取得した個人情報は，次のいずれかに該当する場合を除き，利用目的以外のために自ら利用したり，第三者に提供することはありません．

- 本人またはその代理人の同意が得られる場合
- 法令に基づく開示要請があった場合
- 不正アクセス，脅迫等の違法行為があった場合
- 個人情報の取扱いの全部または一部を外部業者等に委託する場合
- その他，本学が定める特別な理由に該当する場合

５．個人情報の照会等に対する対応

個人情報に対して，照会や修正や削除などを希望される場合は，下記にお問い合わせください．本人確認の上，開示等を行うかの審査を，遅滞なく実施します．

６．適用範囲

本個人情報保護規範は，**＜個人情報を取扱う部局名等＞**で**＜データ名＞**を取扱う場合にのみ適用されます．

７．その他

以上の個人情報保護規範は，改定することがあります．個人情報保護規範の改訂の有無及び内容については，下記にお問い合わせください．

お問い合わせ

個人情報の取扱いに関するお問い合わせ．

＜電子メールアドレスや電話番号などの問い合わせ先を記入＞

付録８．情報通信関連サービス取扱い誓約書について

本学の利用者に対して，情報通信関連サービスを利用するときの注意事項を周知するための誓約書について，今後検討を進める．

但し，本学のシステム管理上のため，記載事項が変更になったり，管理用の欄が増えることがある．また，誓約書の書式は，適宜，改訂される可能性がある．

福山大学

共同利用センター長　殿

情報通信関連サービス取扱い誓約書（一般利用者向け）

所属 ＿＿＿＿＿＿＿＿

氏名 ＿＿＿＿＿＿＿＿

私は，学内ネットワーク及び学内情報サービスの利用にあたって，次の事項を遵守することを誓います．

記

1. Ｐ２Ｐ型ファイル共有ソフトウェアを利用しません．

2. 学内情報サービスの ID やパスワードを，友人や家族などの第三者に貸しません．

3. 可能な限り，ソフトウェアのアップデートやバージョンアップを行います．

4. 可能な限り，ウイルス対策ソフトウェアを使用します．

5. 学内ネットワークを盗聴しません．

6. 違法なダウンロード，違法なコピー，学内ネットワーク及び学内情報サービスなどへのいたずらなどは，決して試みません．

福山大学

共同利用センター長　殿

情報通信関連サービス取扱い誓約書（教職員向け）

所属 ＿＿＿＿＿＿＿＿＿＿

氏名 ＿＿＿＿＿＿＿＿＿＿

私は，学内ネットワーク及び学内情報サービスの利用にあたって，次の事項を遵守することを誓います．

記

1.学術研究目的以外でのＰ２Ｐ型ファイル共有ソフトウェアの利用を行いません．Ｐ２Ｐ型ファイル共有ソフトウェアを利用する場合は，福山大学セキュリティポリシー，個人情報保護やプライバシ保護や著作権等に関する関係法令等や学内規則等を，十分に理解し，慎重に利用します．事故の疑いのあるときは，調査に協力します．

2. 学内情報サービスの ID やパスワードを，友人や家族などの第三者に貸しません．システム管理等の業務のために関係者に貸し出すときは，厳重に管理し，貸し出し後はパスワードを変更するなどで，適切に管理します．利用機器や利用サービスごとで定められた利用規則で，パスワード等の貸し出しが禁止されている場合にはそれに従います．

3. 可能な限り，ソフトウェアのアップデートやバージョンアップを行います．

4. 可能な限り，ウイルス対策ソフトウェアを使用します．

5. 教育や学術研究目的以外での学内ネットワークの盗聴を行いません．学内ネットワークを盗聴する場合は，福山大学セキュリティポリシー，個人情報保護やプライバシ保護等に関する関係法令等や学内規則等を，十分に理解し，慎重に行います．事故の疑いのあるときは，調査に協力します．

6. インターネットサービス利用においてポート解放等が必要になった場合には，所定の手続きで申請します．

7. インターネットサービス公開を行う場合には，所定の手続きで申請します．

8. 個人情報の収集と利用は，適切に行います．

付録９．情報漏えい調査時のチェックリスト

１．**調査における原則**

□　被害拡大防止・二次被害防止，再発防止，信頼回復に集中する

□　事実に基づく客観的な調査を進め，情報は一元管理する

□　調査過程そのものを透明にし，調査結果を開示することで，信頼回復を行う

□　全学出動

□　調査の負担による士気の低下に適切に対応する

□　事前の備えを見直すとき，手続きが増え，利用者の理解が得られず士気が低下するリスクに対応する

２．**漏えいの種類**を，事実に基づき調査する

□　置忘れ・紛失，盗難

□　Ｐ２Ｐ型ファイル共有ソフトウェア

□　電子メールでの誤送信，Ｗｅｂでの誤公開等

□　不正アクセス

□　不正プログラム（コンピュータウイルス，トロイの木馬等）

□　その他（外部の掲示板等への掲載を含む）

□　不明

３．**被害状況**を，事実に基づき調査する

□　情報の不正利用の有無（その状況）

□　置忘れ・紛失，盗難した機器のセキュリティ対策状況

□　情報漏えい後の第三者からの接触の有無

□　不正プログラム関係情報（名称，検知手順，対処法など）

□　置忘れ・紛失，盗難した機器の発見状況

４．**事故の発見方法**を，事実に基づき記録する

□　自組織内（本人からの通知を含む）

□　第三者からの指摘

□　被害者や関係者からの通知

□　警察

□　マスコミ

□　匿名の掲示板など

□　不明

５．**情報セキュリティ事故の開示方法**を適切に決定する

□　Ｗｅｂサイト

□　被害者への直接通知

□　被害者への個別訪問による通知

□ 記者会見

□ その他

6．**開示される内容**を確定し，一元的な窓口で正確に発表する．

□ 事故の原因

□ 被害の範囲

□ 経過（事故が起こるまでの事実，発見日時と発見方法，確認された事故の内容）

□ 緊急の被害拡大防止策

□ 再発防止策

□ 問い合わせ窓口

□ 補償の方法

7．**被害者救済策**を確定し，一元的な窓口で正確に発表する．

□ 問い合わせ窓口の設置

□ 個別説明の内容

□ 個別相談における想定問答

□ 補償内容

□ その他の救済策

8．**再発防止策**を確定し，一元的な窓口で正確に発表する．

□ 情報サービスの停止

□ 技術的対策

□ 人的・組織的対策

□ その他

9．**関係機関等への報告，連絡**

□ 監督官庁

□ 警察

□ その他

１０．**二次被害に関する追跡結果**

□ 被害者に対するいやがらせ，勧誘，恐喝，脅迫

□ 被害者に成りすましての犯罪行為

□ その他，漏えい情報を利用した犯罪行為