役職員のための
情報管理・セキュリティ
ハンドブック

Ver. 1.3

国立大学法人 富山大学

目　次

Ⅰ．「情報」の取り扱い 1
1.個人情報
2.学生情報
3.研究情報

Ⅱ．基本的な情報セキュリティ対策 3
1.認証情報（ID，パスワード）の管理
2.OS•ファームウェアのアップデート
3.管理者IDの設定•管理
4.コンピュータウイルス対策
5.アプリケーションソフトの使用
6.アクセス制限
7.紛失•盗難対策
8.情報（データ）の保存
9.情報の持ち出し

Ⅲ．電子メールの利用 8
1.業務でのフリーメールアドレスの利用禁止について
2.メール送信前の確認
3.学外メールへの自動転送禁止
4.メールによるサイバー攻撃

Ⅳ．クラウドサービス等利用時の注意事項 11
1.クラウドサービスの利用
2.サーバやクラウドサービスの運用•管理
3.WEB会議サービスの利用
4.SNSの利用

Ⅴ．その他の注意事項 14
1.テレワーク（在宅勤務）時の情報機器の利用
2.出張先等学外での情報機器の利用
3.外部電磁的記録媒体の取扱い
4.不正アクセスの禁止
5.パソコン等を処分するとき
6.情報（データ）の廃棄
7.セキュリティに対する情報収集
8.クリアデスク•クリアスクリーン

Ⅶ．富山大学セキュリティ情報 Web サイト 16
Ⅷ．セキュリティに関する問い合わせ先 16

Ⅰ．「情報」の取扱い

大学における教育・研究活動や各種業務はすべて，情報を取り扱う活動であり，そこで扱われる情報は資産的価値を有するものです。これら情報の取扱い方法は，規則や法律で厳格に定められており，本学における主な関連規則には，以下のものがあげられます。

○情報資産保護に関する基本方針
○法人文書管理規則
○個人情報保護方針／個人情報保護規則
○情報の格付け及び取扱制限に関する規則

この他，契約書等により，情報の取扱いが規定されている場合も多く，その内容を正しく理解し，適切に取り扱う必要があります。

1．個人情報

本学では，「独立行政法人等の保有する個人情報の保護に関する法律」に基づき，「国立大学法人富山大学個人情報保護規則」を定め，本学が保有する個人情報の適正な取扱い，管理，維持に努めています。

この規則において，「職員は，個人情報を保有するに当たっては，業務を遂行するため必要な場合に限るものとし，かつ，その利用の目的をできる限り特定しなければならない。」としており，目的の業務が終了した場合，当該個人情報を適切に消去し，不用意に保有し続けてはいけません。また，人種，信条，社会的身分，病歴等の要配慮個人情報は，取扱いによって差別や偏見，その他の不利益が生じるおそれがあるため，情報の取得・利用・管理に関して，特に注意を払う必要があります。

2．学生情報

学生の成績や身上書など本学の教職員が職務上作成又は取得したこれらの情報についても個人情報が含まれており，本学において組織的に用いるものとして本学で保有する場合は，「法人文書」に該当する可能性があります。

法人文書に該当した場合は，「国立大学法人富山大学個人情報保護規則」のほか「国立大学法人富山大学法人文書管理規則」に従い取り扱う必要があります。

3．研究情報

「富山大学研究者倫理・行動規範」の研究活動における遵守事項において，以下のとおり定められています。

・自らの研究活動において，研究・調査データの記録の厳正な取扱いを徹底するとともにそれらを一定の期間（個々の分野の特性に応じて適切と考えられる期間，それが判然としない場合にあっては 5 年間）は保存しなければならない。
・調査や実験を通じて知り得た被験者の個人情報等を漏洩させてはならない。

また，「富山大学における研究データの保存等に関する指針」では，以下のとおり定められてます。

・資料（文書（実験ノート等を含む），数値データ，画像等）の保存期間は，原則として，当該論文等の発表後 10 年間とする。電子化データについては，メタデータの整理・管理と適切なバックアップの作成により，再利用可能な形で保存するものとする。
・個人データ等その取扱いに法的規制があるもの，契約等により別に定めがあるもの又は倫理上の配慮を必要とするものについては，それらの規制，契約，指針等に従うものとする。
・研究者が退職，他機関への異動等した場合は，当該研究室等の代表者等が，当該研究者の研究活動に係る資料のうち保存すべきものについて，この指針で定める期間内は，バックアップをとって保存する，所在を確認し追跡可能としておく等，適切に保存しなければならない。

Ⅱ． 基本的な情報セキュリティ対策

情報を安全に取り扱うためには，情報機器の日常管理の徹底が不可欠です。電子化されたデータは，ネットワークを通じて世界中に瞬時に伝わり，簡単に複製が作られます。便利な半面，その取扱いには十分に注意する必要があります。

本学のネットワークの利用に際しては，「富山大学情報ネットワーク・システム利用細則」を遵守してください。

1． 認証情報（ID，パスワード）の管理

認証情報が漏洩した場合，悪意のある第三者に悪用され，犯罪に巻き込まれる場合もあります。情報の保護やセキュリティ確保のため，認証情報の管理には十分注意してください。パスワードの管理については，本学の「利用者パスワードガイドライン」を遵守してください。

※「利用者パスワードガイドライン」からの抜粋

2．2（1）パスワードとして使用する文字列は，解析ツールで容易に解析できないよう，半角文字で 8 文字以上とし，次の文字集合のうち，（ア），（イ），（ウ）からそれぞれ最低 1 文字以上を含むこと。また，当該システムで使用可能な場合には，（エ）も加えること。

（ア）英大文字：A ～ Z

（イ）英小文字：a ～ z

（ウ）数字：0 ～ 9

（エ）記号：プラス (+)，マイナス (-)，アスタリスク (*)，スラッシュ (/)，イコール (=)，ドット (.)，アンダーバー (_) など

2．2（2）容易に推察可能である次の文字列は，パスワードとして使用しないこと。

（ア）アカウント情報や個人情報から推測できる文字列（ユーザ ID，名前，生年月日，電話番号等）

（イ）前記（ア）を並べ替えた文字列又は数字や記号を追加した文字列

（ウ）キーボードの文字配列上，並んでいる文字列

（エ）辞書の見出し語，著名人の名前等を含む文字列

2．4（3）認証システムが異なる複数の情報システムにおいて，同一パスワードの使い回しはしないこと。

複雑なパスワードの設定には，覚えやすいフレーズや言葉遊びを取り入れる等の方法が有用です。（参考）パスワードの作り方（IPA「チョコっと＋パスワード」）

⚠ インシデント事例（A 大学）

メールアカウントに簡易なパスワードを設定していたことにより，第三者から大学 Web メールに不正ログインされ，外部に大量のフィッシングメールが送信される事態に（加害者に）なっていた。

2．OS･ファームウェアのアップデート

パソコンはもちろんのこと，プリンタ，スキャナ，NAS（ネットワークハードディスク），無線 LAN アクセスポイント，ルータなども，搭載されている OS・ファームウェアの脆弱性や設定の不備により，不正侵入やデータの詐取，改ざん，他の攻撃の踏み台とされることがあります。これらの機器のOS・ファームウェアについても常に最新のものにアップデートしてください。

一般的に使用されている代表的な OS 等のアップデート方法については，以下の富山大学セキュリティ情報 Web サイトを参考にしてください。

「基本的なパソコンのセキュリティ対策について」

「各製品の EOL（製品寿命）情報について」

その他情報機器のファームウェアアップデートについては，機器のマニュアルやメーカー Web サイトの情報を確認してください。

なお，ファームウェアの更新サポートが終了している機器は，利用しないでください。

> ⚠ インシデント事例（B 大学）
> ネットワーク機器のファームウェアのバージョンが古かったことにより，第三者から該当機器に不正アクセスされ，機器の ID•パスワードが漏洩した。

3．管理者 ID の設定･管理

パソコンやプリンタ，スキャナ，NAS などの管理者 ID は，初期状態ではパスワードが設定されていなかったり，初期パスワードがメーカーマニュアル等で公開されている場合が多く，そのまま使用することはセキュリティ上，大変危険ですので，パスワードの設定，管理を適切に行ってください。

> ⚠ インシデント事例（C 大学）
> 複合機（プリンタ，スキャナ等）の管理者パスワードを設定せずに運用していたことにより，スキャナで読み込んだ個人情報を含んだデータが第三者から閲覧可能になっていた。

4．コンピュータウイルス対策

最近のコンピュータウイルスは，利用者に気付かれないように重要なデータを盗み出しインターネット上に公開したり，遠隔からパソコンを操作できるようにしたりします。そのため知らないうちに犯罪に巻き込まれることもあります。このような被害を避けるため， 以下の対策を必ず実施してください。

・パソコンには，コンピュータウイルス対策ソフトをインストールし，常に最新の定義ファイルを取得して，定期的なウイルスチェックを行うこと。

・心当たりのない差出人からのメールに添付されたファイルを開いたり，メール本文に記載されたURLを安易にクリックしないこと。

・業務に不要なWebサイトの閲覧をしないこと，また，安全性が確認できないWebサイトからファイルやアプリケーションソフトをダウンロードしないこと。

・他者から入手したファイルを利用する際や他者にファイルを送信する際には，事前にファイルのウイルスチェックを行うこと。

ウイルス感染もしくは，その疑いがある場合

速やかにパソコン等のLANケーブルを抜いてネットワークから切り離し（無線LANの場合には無線LANを無効にし），直ちに以下の連絡先まで連絡してください。

情報政策課（五福）
内線：6058／外線：076-445-6058

⚠ インシデント事例（D大学）

不審なメールの添付ファイルを開いたことによりウイルス感染し，この職員を騙るウイルス付のメールが，過去にこの職員とメールのやり取りをした人に送信される事態に（加害者に）なっていた。

5．アプリケーションソフトの使用

アプリケーションソフトを使用する際には，以下のことに注意してください。

・アプリケーションソフトもOS同様，常に最新版へアップデートする。（アップデートの方法は，ソフトのマニュアルやヘルプ，メーカーWebサイト等で確認してください。）

・商用ソフトの場合，認められているライセンス数を超えてインストールしない。また，違法にコピーされたソフトは，重大な著作権侵害となるので，絶対に使用しない。

・フリーソフトを使用する場合は，安全性を十分に確かめ，正規の配布サイトからダウンロードする。

・フリーソフトをインストールする際，意図せず不要なソフトが同時にインストールされることもあるので，十分に確認のうえ実施する。

・大学で利用可能なソフトかどうか利用規約をよく確認する。（家庭内での使用に限定されているソフトは大学では利用できません。）

・ソフトに連絡先，カメラ，ストレージ，位置情報等へのアクセス権限を付与できる場合，不要な権限を付与しない。また，Webサイト閲覧時に「通知機能」の許可を求められた場合，安易に許可しない。

6．アクセス制限

複数名が共有して使用する機器や共有フォルダ等には，適切なアクセス権を設定してください。また，スキャナで読み取った保存先のフォルダには必ずパスワードを設定してください。アクセス権の設定等については，役職員が責任を持って実施し，学生等に絶対に任せないようにしてください。

> ⚠ インシデント事例（E 大学）
> スキャナの保存先フォルダのパスワードを設定しなかったことにより，個人情報が第三者から閲覧できる状態になっていた。

7．紛失･盗難対策

パソコンが盗難・紛失にあった場合，ログインパスワードが設定されていても，パソコン内部の HDD（SSD 含む。以下同じ。）が抜き取られ，データを読み取られてしまう可能性があります。しかし，パソコン内の HDD に暗号化処理を行っていれば，万が一盗難にあったとしても，暗号化鍵がわからない限り，データを読み取られることはありません。このため，パソコン内の HDD に対して，BitLocker 等のソフトにより，暗号化処理を行うことを推奨します。

8．情報（データ）の保存

使用しているパソコンに保存するデータは最小限にしてください。

また，特に機密性の高い重要な情報は，パソコン上で処理が終わり次第，暗号化して外付けの HDD に移動もしくは暗号化 HDD に移動してください。これらの HDD は必要なときのみ接続し，それ以外のときはネットワークやパソコンに接続しないようにしてください。

ノートパソコン，外付けHDD，USBメモリ等は，鍵のかかるキャビネット等に保管し，施錠してください。

9．情報の持ち出し

重要な情報を保存したノートパソコン，タブレット端末，USBメモリ，外付けHDD，CD 等の電子媒体及び重要書類を持ち出すときには，以下のことを徹底してください。

・個人情報が含まれる場合は，本学個人情報保護規則に従う。
・ノートパソコンまたはタブレット端末に保存するデータは必要最小限にする。
・電子媒体はケース等に入れ，USBメモリはタグ，ストラップ，鈴などを付け紛失を防止する。
・書類はひも付き封筒等に入れ，容易に目に触れないようにする。

・ノートパソコン，タブレット端末に必ずログインパスワードを設定し，可能なら生体認証を設定する。
・ノートパソコン，タブレット端末は HDD を暗号化する。またはデータを暗号化する。
（参考）IPA「情報漏えいを防ぐためのモバイルデバイス等設定マニュアル」
・ログイン，暗号化等に用いるパスワードには，適切なパスワードを設定する。
・ブラウザに本学業務システムの ID・パスワードを保存しない。
また，携行時には以下のことに注意してください。
・電車内では網棚に置かない。
・自動車内には保管しない。
・離席する場合は携行する。
・他者から覗き見できない状態で使用する。

⚠ インシデント事例（F 大学）
個人情報を含むノートパソコンが出張中に盗難に遭い，情報漏洩の危険が発生した。（個人情報は出張業務に必要なものではなく，学外への持ち出しに管理者の許可をとっておらず，パスワード設定等の対策もなかった）

Ⅲ. 電子メールの利用

業務で利用機会の多いメールは，大変便利な反面，サイバー攻撃の標的とされることや，情報漏洩につながる可能性があります。利用時には，以下の内容に注意してください。

1. 業務でのフリーメールアドレスの利用禁止について

本学においては，メール利用によるインシデントが万が一発生した場合に，発生原因，拡散経路などを迅速に調査，対応することが困難となるため業務でのフリーメールアドレスの利用を禁止しております。

本学の業務等で使用するメールアドレスは，本学で提供する末尾が「u-toyama.ac.jp」であるメールアドレス（本学ドメインメール）を利用するよう徹底をお願いします。

⚠ インシデント事例（G 大学）

•教員が，学生に誤ったフリーメールアドレスを課題提出先に伝え，学生が提出。実在するフリーメールアドレスでそのまま送信され個人情報が漏洩。大学で管理しているメールアドレスではなかったため，送信先の人物の特定等調査できなかった。

2. メール送信前の確認

送信の際は以下のことを確認してください。

・メールの宛先は正しいか。
・添付ファイルは正しいか。
・個人情報が含まれる場合は，本学個人情報保護規則に従う。
・メールの本文に本来送信してはいけない情報を記載していないか。

⚠ インシデント事例（H 大学）

•間違ったファイルをメール送信したことにより，個人情報が漏洩した。
•メールの宛先を間違えて送信したことにより，個人情報が漏洩した。
•添付ファイルに本来送信してはいけない情報が非表示となっていたことにより，（Excel のシートが非表示となっている，トリミング前の非表示箇所が削除されていない，画像を貼り付けて非表示としただけで適切なマスキング処理がされていない等）個人情報が漏洩した。

3. 学外メールへの自動転送禁止

本学で取得したメール（学内メール）を学外で取得した私用のメール等（学外メール）に自動転送した場合，以下の問題が生じます。

・学内メールで受信した内容がすべて学外に保存される。
・学外メールに用いるIDとパスワードが何らかの理由で流出した場合，第三者に学内

メールの内容も覗き見られて意図しない情報漏洩に繋がる。

・インシデントが発生した場合に拡散経路などを追跡することができない。

このため，本学では，学内メールを学外メールに自動転送することを禁止しています。

⚠ インシデント事例（I 大学）

大学のメールのバックアップを取るために，私用メールに自動転送していたところ，私用メールがフィッシング被害を受けて ID とパスワードが漏洩し，第三者から私用メールにログインされて，大学のメールに含まれる個人情報が漏洩した。

4．メールによるサイバー攻撃

近年，メールを用いたサイバー攻撃が頻繁に行われています。本学においても，標的型攻撃メールやフィッシングメールが日々確認されています。

【標的型攻撃メール】

近年の標的型攻撃メール等は非常に巧妙化しており，以下のように様々方法で添付ファイルや本文中のリンクを開くよう仕向ける手口が確認されています。

・実在している企業や職員を騙い，研究や業務に関連する本文で信用させ，添付ファイル等を開くように仕向ける。

・過去にやり取りしたメールの内容を用いて，やり取りしていた相手になりすます。

・メールでやり取りを行っている中で，やり取りしている相手になりすます。

これらのメールは文章も自然な日本語で書かれており，よく知る人からのメールや自分が送ったメールに対する返信であれば，あまり注意せずに添付ファイル等を開いてしまう可能性があります。本当に本人からのメールかどうかを判別することは非常に困難になってきてはいますが，以下の対策を行ったうえで，普段から標的型攻撃メールが届く可能性があるという意識を持つことが重要です。

【対策】

・コンピュータウイルス対策ソフトを必ず入れておく。

・ファイル名の拡張子，偽装対策のため，OS の設定で，ファイルの拡張子を表示する。

・不用意にマクロを有効化しない。

（添付ファイルをオフィスソフトで開いた際に，セキュリティの警告が表示された場合，不用意にマクロの有効化「コンテンツの有効化」のクリックをしないでください。オフィスファイルのマクロを有効化することでウイルスに感染する場合もあります。）

・知り合いからの情報こそ疑う。

少しでも不自然に思うことがあれば，先方に別の手段（電話等）で確認するなど，安全を確認してからファイルを開くようにしてください。

判断がつかない場合は，以下の富山大学セキュリティ情報 Web サイト等も参考にしてください。

「不審なメールや添付ファイルを確認する方法」

「IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」」

【フィッシングメール】

フィッシングメールの典型的な手口として，メール管理者，クレジットカード会社や銀行，宅配便業者などからのお知らせと称してメール本文中のリンクをクリックさせ，本物のWebサイトとそっくりな偽サイトに誘導し，ID やパスワードを入力させ，入力された情報を詐取します。以下の点に注意してください。

・メール本文中のリンクをクリックせず，その会社等の正規の Web サイトにアクセスし，確認する。

・メール本文中に表示されている URL（アンカーテキスト）と実際のリンク先のURLが異なっていないか，リンク先 URL が正式な Web サイトかどうかを確認する。

メールのIDとパスワードを偽サイトに入力してしまった場合

直ちに以下の連絡先または最寄りの総合情報基盤センターまで連絡してください。

情報政策課（五福）

内線：6058 ／外線：076-445-6058

また，富山大学セキュリティ情報 Web サイトにおいて，フィッシングメールに関する情報を随時更新していますので参考にしてください。

「セキュリティ Web サイト（TOP）(随時更新)」

「フィッシング被害への対処法等について」

Ⅳ. クラウドサービス等利用時の注意事項

1. クラウドサービスの利用

クラウドサービスを利用することで，高機能なサービスを迅速かつ容易に利用(提供)できるようになってきましたが，学生の個人情報や本学の重要情報，秘密情報等の情報資産を外部のクラウドサービス上で管理することは，情報漏洩等のセキュリティ上のリスク増加をもたらします。クラウドサービス上で本学業務に関係する情報を取り扱う場合は，「国立大学法人富山大学におけるクラウドサービス利用要項」及び「富山大学クラウドサービス利用ガイドライン」遵守し，対策の徹底をお願いいたします。

また，保存したファイルが外部に公開する設定になっていたり，サービスが突然終了し，その結果データが消失してしまう可能性もあります。各サービスの利用規約，利用方法を確認し，適切に運用願います。

2. クラウドサービスの運用･管理

Webサーバやクラウドサービス（レンタルサーバ含む。）を利用してシステムの運用・管理を行う場合には，適切に管理するためのセキュリティ対策を行う必要があります。

以下の富山大学セキュリティ情報 Webサイトを確認し，対策の徹底をお願いします。

「Webサイト／サーバの運用管理について ／ ✓Webサイト／サーバチェックリスト」

「CMSにおける一般的なセキュリティ対策について 」

「CMSの運用管理について ／ ✓CMSチェックリスト」

また，公開 Web サイトに掲載するファイルについては，個人情報等が含まれていないか，掲載してはいけない情報が非表示となっていないか，十分に確認をお願いします。

⚠ インシデント事例（J大学）

- Web サーバの CMS（Contents Management System）の設定不備により，Web サーバが第三者からログインされ，外部に迷惑メールが送信される事態に（加害者に）
- Web サイトに掲載した Excel ファイルの非表示シートに個人情報が残っていたことにより，個人情報が漏洩

3. クラウドストレージの利用

漏洩や消失のリスクを防ぐため，重要な情報はクラウドストレージに保存しないでください。

利用する際は，以下の点に注意して利用してください。

・利用に際し，学内規則や研究上定められたルール等に違反していないか確認する。

・本学総合情報基盤センターのオンラインストレージサービスの利用を検討する。

「総合情報基盤センターオンラインストレージサービス「Proself」」

・ファイルのアクセス範囲，公開範囲を制限し，適切に管理する。

・適切なパスワードを設定し，他のサービスと同一パスワードの使い回しはしない。

・ファイルの暗号化，アクセス記録の取得等の対策を行う。

⚠ インシデント事例（K大学）
クラウドストレージのアクセス範囲の設定を怠ったことにより，保存していたデータがインターネットから誰でも閲覧可能な状態になっていた。

4．Web 会議サービスの利用

本学では Microsoft Teams を会議や授業等で利用していますが，以下の点に注意してください。

・会議の URL は参加者だけに公開する。
・画面共有や録音・録画等の機能で参加者に必要のない機能は，Web 会議の設定で，参加者が利用できないように制限する。
・やりとりするファイルやその録画データに重要な情報が含まれている場合，Web 会議サービスのサーバにデータを保存しない，またはファイル共有や録画機能を使用しない。
・意図しない個人情報等の映り込みを避けるため，カメラ使用時は映像の背景に配慮したり，画面共有時は会議に関係のないファイルを閉じておく。
・画面共有するファイルは，事前にファイルに個人情報等が含まれていないか，共有しても問題がないファイルか確認する。

⚠ インシデント事例（L 大学）
リモート授業実施時に資料を間違って共有したことにより，個人情報が漏洩した。

5. SNS の利用

LINEやTwitter，Facebook等のSNSは学内外の人とコミュニケーションをとるには非常に便利である反面，不用意な情報発信で思わぬトラブルに巻き込まれる場合があり，最悪の場合，懲戒などの罰則を受けることもあります。利用時には，「国立大学法人富山大学ソーシャルメディアポリシー」を守ってください。

注意すべき点
・悪意のない情報発信のつもりでも他人を不快にする場合がある。
・想定していない人にも閲覧される場合がある。
・匿名の利用であっても実名が判明する場合がある。
・一度投稿した内容は消えない。
・著作権や肖像権の侵害のおそれがある。

Ⅴ. その他の注意事項

1．テレワーク（在宅勤務）時の情報機器の利用

テレワーク（在宅勤務）を実施する場合は，基本的なセキュリティ対策の他に，以下の点に注意してください。

・テレワークは，原則自宅にて大学資産のパソコンで実施してください。
・事務パソコンにソフトウェア等のダウンロードは勝手に行わないでください。
・テレワークで使用するパソコンには，所有者が不明もしくは自信で管理していないUSBメモリ等の外部記憶媒体を接続しないでください。
・自宅等のルーター等は，メーカーのサイトを確認のうえ，最新のフォームウェアを適応（ソフトウェア更新）してください。
・個人情報又はその他の重要情報を含む文章の学外持ち出し又は自宅等における印刷は行わないでください。
・テレワークで使用するパソコン内に，データは保存しないでください。

2．出張先等学外での情報機器の利用

ノートパソコン等を学外で利用する場合は，以下の点に注意してください。

・接続したネットワークからノートパソコン等に不正アクセスされることを防ぐため，パーソナルファイアウォールを導入する。
・利用中に盗み見のおそれがあるため，ノートパソコン等のパスワードやスクリーンセーバーを適切に設定する。
・利用中の情報機器から離れる際は，盗難に注意する。
・インターネットカフェ等に設置されたパソコンを利用する場合，本学情報システムへのアクセスは行わない。

3．外部電磁的記録媒体の取扱い

ここでの外部電磁的記録媒体とは，フラッシュメモリ(USB／メモリースティック等)，外付けHDD 等の記録媒体を指します。

原則，大学の情報を保存した外部電磁的記録媒体は，持ち出し禁止です。やむを得ず持ち出す場合は，以下の点に注意してください。

・個人情報が含まれる場合は，本学個人情報保護に関するルールに従う。
・学部長または所属部課長に持ち出しの許可を取る。（公開情報，またはキャンパス間の移動に伴う持ち出しを除く。）
・データは，ファイル暗号化，または暗号化機能付USBメモリを使用して暗号化する。ただし，機密性の高い重要な情報については，必ず暗号化機能付USBメモリを使用して暗号化する。
・暗号化に用いるパスワードは，適切なパスワードを設定する。

・作業目的が終了したらデータを速やかに削除する。
・不要になったら，物理的に破壊するか専用ソフトによる完全消去を行ったうえで廃棄する。

4．不正アクセスの禁止

他人の認証情報（ID，パスワード）でシステムを利用することは，不正アクセス行為になります。コンピュータの脆弱性を故意に突いて他人のパスワードを盗み出したり，他人になりすましてファイルを盗み見たり，迷惑メールをばらまくなども犯罪行為です。

5．パソコン等を処分するとき

パソコン等を処分する際には，データの漏洩を防ぐために，HDDの物理的破壊もしくは専用のソフトを用いて，データの完全消去を行ってください。パソコンのゴミ箱を空にしたり，フォーマットしたりしただけでは，データが復元されてしまうことがあります。

移管する場合なども，専用のソフトを用いてデータを完全に消去してください。

6．情報（データ）の廃棄

情報（データ）を廃棄する際は，記録された媒体に応じて，以下のいずれかの方法で行ってください。

・外付け HDD，USB メモリ
　データの完全消去もしくは物理的破壊
・CD，DVD などのディスク
　シュレッダーによる細断もしくは，CDのラベル面，DVDのディスク内面にカッターでキズを入れる
・重要書類
　シュレッダーによる細断もしくは専用BOXに入れて溶解処分

なお，総合情報基盤センターに，HDD（SSD や外付け含む。），USB メモリ，CD，DVD 等の物理破壊装置を設置しています。予約制になっていますので，内線 3803（五福以外からは 91-3803）にご相談ください。

破壊作業は各自で行っていただきます。また，HDDを破壊する場合は，パソコン本体等は持ち込まず，事前に筐体から取り外してご持参ください。

Ⅶ. 富山大学セキュリティ情報 Web サイト

富山大学セキュリティ情報

https://security.u-toyama.ac.jp

セキュリティに関する情報を随時発信しています。
不審なメールの情報やセキュリティ関連の注意事項・注意喚起の情報を掲載していますので，定期的に確認をお願いします。

Ⅷ. セキュリティに関する問い合わせ先

もしかして…と思ったら

ウイルス感染もしくは，ウイルス感染の疑いがある場合：

1．速やかにパソコン等のLANケーブルを抜いてネットワークから切り離す（無線LANの場合，無線LANを無効にする）

2．シャットダウン等の操作をせず，直ちに以下に連絡する

＜セキュリティ担当職員＞

学術情報部情報政策課（五福）

内線：６０５２／外線：０７６－４４５－６０５８

総合情報基盤センター（五福）

内線：６９４６/外線：０７６－４４５－６９４６