教職員のための情報セキュリティ対策ハンドブック

第1.2版

2022年12月9日

国立大学法人 和歌山大学
wakayama univ.

和歌山大学 学術情報センター

第1章　情報の取り扱い

1.1 情報の格付け

本学で取り扱われる情報は「機密性」、「完全性」、「可用性」の 3 種類の格付けで分類されます。全ての情報に格付けを認識できるように明示することが推奨されます。また、取り扱い制限を記載することで情報の取り扱い方法がより明確になります。取り扱い制限の例として「担当者限り」、「複製禁止」、「転送禁止」等適宜設定してください。

1.2 情報の利用・保存

情報の格付けが決まると、「国立大学法人和歌山大学情報セキュリティ対策のための統一基準」に記載された方法で、その情報を取り扱う必要があります。また、格付けや取り扱い制限が不明な場合は、情報の作成者、入手先に確認、または相談してください。

第2章　基本的なセキュリティ対策

正しい情報セキュリティ対策を行うためには、日常的に基本的な対策を施す必要があります。ここでは、その基本的な対策について記述します。

2.1 ID、パスワード

コンピュータを利用するためにはユーザ名とパスワードが必要になります。学術情報センターが発行するパスワードだけでなく、発注購買システム、学外のサービス、NAS（ネットワーク接続型ハードディスク）、プリンタ等色々な場面でパスワードの入力が必要になります。ユーザがどのようなパスワードを使うかは、システムのセキュリティ上非常に重要になっています。以下のチェック項目を参考に ID、パスワードの取り扱いが正しいか確認してください。

＜以下のチェック項目を確認してみましょう＞

- □パスワードは 11 文字以上です
- □パスワードは英大文字小文字、数字、記号を混在させた複雑なものにしています
- □パスワードに単語、人の名前等、類推しやすいものを使っていません
- □本学で使っているパスワードや学外サービスで用いるパスワードは全て異なっています
- □他人の目に触れる所に、メモ書きしたパスワードは置いていません
- □複数ユーザでパスワードを共有していません
- □ネットカフェ等の不特定多数が利用する PC で本学で利用している ID、パスワードを入力していません
- □受信したメールに記載されているリンク先で、ID、パスワードを入力する場合は、正しいウェブページであることを確認しています
- □NAS、Wi-Fi ルーター、プリンタ等の IoT 機器で初期パスワードが設定されている場合は、複雑なパスワードに変更しています

2.2 ソフトウェアのアップデート

日常利用している PC 上では OS（Windows 等）とアプリケーションソフトウェア（Office 等）が動作しています。これらソフトウェアは機能改善やセキュリティホール対策のために随時アップデートされます。アップデートを怠っていると、セキュリティホールを攻撃されて PC の乗っ取り、情報の漏洩につながることもあります。必ず OS やアプリケーションソフトウェアは最新のものにアップデートしてください。

また、OS が古くなるとサポートが停止されるために、以後アップデートが提供されなくなります。この場合は OS そのものを新しくする、機器を新しくする等の対応が必要となります。

PC 以外でも NAS、Wi-Fi ルーター、ネットワークカメラ、プリンタ等 IoT 機器にはファームウェアと呼ばれるソフトウェアが搭載されています。各メーカーのウェブページをチェックして、このファームウェアが更新されていないか確認し、更新されている場合は速やかにアップデート作業を行ってください。ファームウェアの更新方法は、説明書または各メーカーのウェブページ等を参考にしてください。

機種やメーカーによっては発売後一定期間が過ぎるとファームウェアのアップデートが行われなくなる事もあります。この場合は機器の買い替え、または利用中止が強く求められます。

2.3 コンピュータウィルス対策

コンピュータウィルスに感染すると、個人情報等の機密情報の漏洩や遠隔操作、ファイルの消去やランサムウェアによる重要ファイルの勝手な暗号化等、著しい被害を受け業務の遂行に支障をきたすことがあります。日頃から十分注意しウィルス対策に努めましょう。

＜以下のチェック項目を確認してみましょう＞

□全ての PC にウィルス対策ソフトを導入しています
□ウィルス対策ソフトは常に最新のものにアップデートしています
□週に1度は PC の HDD や SSD 内全てのファイルをウィルス対策ソフトで確認しています
□OS、アプリケーションソフトウェアは常に最新のものにアップデートしています
□USB メモリ、メール等で外部から持ち込んだファイルは必ずウィルス対策ソフトで確認しています
□安全性が確認できないファイルやフリーソフトをウェブ等からダウンロードしていません

2.4 アプリケーションソフトウェアの利用

PC 等にアプリケーションソフトウェアをインストールする場合は、以下の点に注意してください。

＜以下のチェック項目を確認してみましょう＞

□ソフトウェアは、ライセンスで定められた範囲内でインストールしています

□フリーソフトは、正規のウェブサイトからダウンロードし、ウィルスチェック等で安全性を確認した上で、利用しています。

□業務に関係ないソフトウェアをインストールしていません

□OS に機能がある場合は、必要に応じてソフトウェアが利用できる機器のデバイス（カメラやマイク等）や連絡先等のデータへのアクセス制限を行っています

第3章　電子メールの利用

業務で電子メール利用が増えていますが、うっかりミスによってインシデントに直結する場合もあります。本章の内容をよく理解して正しい電子メール利用に心掛けてください。

3.1 電子メールで気をつける事

電子メールは便利なコミュニケーション手段ですが、注意点があります。

＜以下のチェック項目を確認してみましょう＞

□宛先が正しいか確認しています

□一斉送信等で誰に送信したか受信者に知られては困る場合は BCC を使っています

□フリーメール（Gmail、Yahoo!メール等）に業務メールを転送していません

□勝手に転送先が追加されていないか、時々確認しています

3.2 機密情報の添付

電子メールは葉書と同様に、第三者にのぞき見される可能性があります。最近は、送信先のメールアカウントが乗っ取られていて、メールが見放題ということもあります。また誤送信した場合に漏洩リスクとなります。機密情報の添付は原則禁止ですが、やむを得ない場合は次の方法を取ってください。

① Office のファイルへのパスワード設定機能を使い、複雑なパスワードを用いる。

② テキストファイル等パスワード機能の利用できないファイルはアタッシェケース等の暗号化ソフトウェアを用い、複雑なパスワードを用いる。

③ パスワードの伝達に電子メールは用いない。事前に取り決めておくか、ショートメッセージサービス（SMS）、電話等別媒体を利用し伝達する。

＜参考＞

機密情報を交換する場合には、ファイル交換用にオンラインストレージ（Proself）を用意しておりますので活用してください。さらに Proself の認証が破られた場合等に備えてファイルを暗号化しておけばさらに安全です。

Proself ： https://proself.center.wakayama-u.ac.jp（要認証）

3.3 標的型攻撃メール

特定の大学、企業、組織を狙ってコンピュータウィルスを添付したメールを送りつける標的型攻撃が多発しています。添付ファイルに仕込まれたウィルスを実行させるために、数々の騙しのテクニックが使われています。標的型攻撃メールに騙されないように次の点に注意してください。

＜受け取ったメールは、以下のような点が無いか注意しましょう＞

① 件名や本文が拙い日本語である。
② 知らない差出人・企業または、Yahoo、Gmail 等のフリーメールが使用されている。
③ 自分の業務と無縁の内容である。
④ あからさまに添付ファイルを開かせようとする内容である。
例:【大事なお知らせ】、【緊急】、【重要】等
⑤ 添付ファイルの拡張子が ZIP、LZH、RAR 等、圧縮されている。
⑥ 身に覚えのない事に対する支払いを要求している。(取引先に成りすましている場合もあるので注意する。)

＜うっかり添付ファイルを開いてしまったら＞

うっかり添付ファイルを開いてしまったら、至急以下の行動をとってください。

① 速やかに PC をネットワークから切断する(LAN ケーブルから抜く、または無線 LAN から切断)。電源は落とさない。
② 同様のメールが来ていないか同じ課内で情報共有する。
③ CSIRT にすぐに連絡する。 ※連絡先は最終頁

3.4 フィッシング

フィッシング(Phishing)とは、金融機関、日本郵便、宅配便等を装った電子メールや SMS(ショートメッセージサービス)で偽の URL へ導き、個人情報、クレジットカード情報、ID・パスワード等を搾取する行為です。

本学でも過去に被害例がありますので以下の点に気をつけてください。

＜以下のチェック項目を確認してみましょう＞

□個人情報の入力を求めるメールを信用しない
□メールに記載される差出人名称を信用しない
□電子メールのリンクは、送信者の組織のウェブページからたどるか、組織のドメイン等と同じかどうか確認したうえで、利用している

第4章　ネットワークサービスの利用

オンラインストレージサービスや SNS（ソーシャル・ネットワーキング・サービス）は広く普及しており、うまく使うと強力なツールになります。しかしその特性を理解せずに利用すると思わぬトラブルに巻き込まれる可能性もあります。特に秘匿情報が一度ネットワークに拡散すると消去不可能になる場合もあります。ここでの注意点に気をつけてネットワークサービスの安全な利用に心掛けてください。

4.1 オンラインストレージサービスの利用

Google Drive や Dropbox、OneDrive などのオンラインストレージサービスは職場、出張先に関わらずファイルの保存、参照や外部の人とファイル交換ができるために非常に便利です。しかし使い方を誤ると情報漏えいの危険もあります。次の点に注意して利用してください。

＜以下のチェック項目を確認してみましょう＞

□パスワードは 2.1 で記載した複雑なものを利用しています
□パスワードを本学のものを含め他のパスワードと同じものを利用していません
□オンラインストレージサービスのトラブルに備え、他の場所にファイルをバックアップしています
□共有の設定は、一般公開されないように慎重に行っています
□秘匿情報を保存する場合は複雑なパスワードで暗号化を行っています

4.2 SNS の利用

LINE、Facebook、Twitter、Instagram 等でのコミュニケーションは非常に便利ですが、不用意な発言や利用法を誤ると思わぬトラブルに巻き込まれることがあります。

＜以下のチェック項目を確認してみましょう＞

□機密情報や本学の品位を落とすような投稿は行っていません
□公開／非公開設定の特性は十分理解しています
□見知らぬ人からの友達申請には十分注意しています
□非公開設定をしていても、グループの誰かが他のグループや他の SNS へ転送する危険性があることを認識しています
□サービス連携には十分注意しています
□友人、知人、学生等のプライベートな情報などの無許可投稿は行っていません
□誹謗中傷や事実と異なる内容の投稿は行っていません

第5章　こんなときには

5.1 学外での PC 等の利用

国内、海外の出張に業務で利用している PC を持ち出すと紛失・盗難のリスクがあります。原則持ち出しはお勧めしませんが、やむを得ない理由で持ち出す場合は以下の点に気をつけてください。

＜以下のチェック項目を確認してみましょう＞

□Wi-Fi を利用する場合は、セキュリティ保護の表示や鍵(🔓)マークのあるネットワークを利用しています

□ホテル、公共の場所で Free Wi-Fi 等を利用する場合は https で始まるサイトのみ利用しています

□PC に機密情報を保存していません

□やむを得ない理由で機密情報を持ち出す場合は複雑なパスワードで暗号化しています

□OS 起動前の BIOS のパスワードを設定しています

□機密情報を持ち出した場合はその内容を正確に把握しています

□機密情報が不要になったら、速やかに削除しています

OS 標準の機能でファイルを削除した場合、**ファイルを復元できてしまう**可能性があります。機密情報を削除する場合は**復元が困難な方法でファイルを完全に消去**してください。

□ USB メモリからファイルを消去する場合

USBメモリに保存した機密情報を完全に消去する場合は、USBメモリを**フォーマット(初期化)**してください。(※USB メモリ内の**全てのファイルが消去**されます。)

✓　クイックフォーマットでは不十分ですので、ご注意ください

参考: Data Rescue Center https://www.rescue-center.jp/elementary/vol04.html

□ HDD からファイルを消去する場合

HDD などの磁気記憶装置から機密情報を完全に消去する場合は、ファイル消去ソフトウェアをご利用ください.

参考ソフトウェア: ERASER (Windows, 英語) https://eraser.heidi.ie/download/

□ SSD からファイルを消去する場合

OS 標準のファイル削除を行ってください。(ごみ箱に移動させた場合は, ごみ箱を空にしてください。) Trim 機能により, 定期的にファイルの痕跡が消去されます.

参考:EaseUS:Windows 11/10 で SSD の TRIM を無効/有効にする方法

https://jp.easeus.com/knowledge-base/how-to-enable-disable-trim-on-ssd.html

5.2 PC がウィルスに感染した、または感染した疑いがある

PC がウィルスに感染した場合は以下の手順に従って行動をしてください。

① 速やかに PC をネットワークから切断する（LAN ケーブルから抜く、または無線 LAN から切断）。電源は落とさない。

② 直ちに CSIRT に連絡し、指示に従う。※連絡先は最終頁

5.3 PC 等端末等を紛失した、または盗まれた

PC や機密情報の保存されている USB メモリ等が盗まれた、または紛失したと判明した場合、以下の手順に従って対応してください。

① 以下の内容を上司および CSIRT に連絡する。

※盗まれた時、または最後に確認した時の状況

※個人情報を含む機密情報が保存されている場合はその詳細な内容、および複雑なパスワードで暗号化されているか

② 紛失した PC 等が発見された場合にはすぐに上司および CSIRT に報告する。

5.4 NAS、Wi-Fi ルーター、ネットワークカメラ、複合機等の IoT 機器を購入した

NAS、Wi-Fi ルーター、ネットワークカメラ、複合機等 IoT 機器はそれ自身ネットワーク機能を持ったコンピュータです。設置後の管理を怠ると外部から侵入され、文書や写真、映像が流出したり、IoT 機器を踏み台に外部組織を攻撃する事もあります。外部からの侵入を防ぐためには以下の点に気をつけてください。

＜以下のチェック項目を確認してみましょう＞

□IoT 機器のパスワードは購入・設置後すぐに初期設定パスワードから複雑なものに変更している

□ファームウェア（IoT 機器に組み込まれたソフトウェア）は常に最新のものに更新している

□IP アドレスは、過去に取得したものを使いまわさず、新たに申請しなおしている

5. 5 ソフトウェアと著作権

ソフトウェアには著作権があり、ライセンスに記載された条件で利用することができます。不正に取得したソフトウェアやライセンスに違反した状態でソフトウェアを使用する行為は法律違反になり、犯罪や損害賠償請求のリスクとなります。また、適正なアップデートを受けることができないため、セキュリティリスクとなります。ソフトウェアの適正利用を行ってください。

＜以下のチェック項目を確認してみましょう＞

□ソフトウェアは正規の販売店から購入している

□ライセンス条項を読んで違反しないように注意している
□体験版のソフトウェアを利用した後は必ずアンインストールしている

5.6　その他、困ったことがある場合

PC 等を利用していて不安に思うこと、おかしいと思う事があれば学術情報センターに相談してください。

第6章　付録

参考リンク集

・和歌山大学　学術情報センター　セキュリティ情報
https://www.wakayama-u.ac.jp/aic/security/index.html

・内閣サイバーセキュリティセンター（略称:NISC） 情報セキュリティハンドブック
https://www.nisc.go.jp/security-site/files/handbook-all.pdf

・独立行政法人情報処理推進機構（略称:IPA） 重要なセキュリティ情報
https://www.ipa.go.jp/security/

・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」
https://www.ipa.go.jp/security/technicalwatch/20150109.html

・IPA 対策のしおり シリーズ
https://www.ipa.go.jp/security/antivirus/shiori.html

・一般社団法人コンピュータソフトウェア著作権協会　ソフトウェアユーザーの皆さんへ
https://www2.accsjp.or.jp/sam/user.php

改訂履歴

版数	発行日	改訂履歴
第 1 版	2020 年 1 月 21 日	初版発行
第 1.1 版	2021 年 3 月 25 日	5.5 ソフトウェアと著作権を追加
第 1.2 版	2022 年 12 月 9 日	5.1 ファイル完全消去の具体例を追記

情報セキュリティ事故発生もしくは、その疑いがある場合には、
速やかに対象機器をネットワークから隔離（例　LAN ケーブルを抜く）
した上で、直ちに以下まで連絡してください。

情報セキュリティについて

和歌山大学 CSIRT(Computer Security Incident Response Team)

TEL：073-457-7177（内線 7177）

E-mail：csirt@ml.wakayama-u.ac.jp

また、日常のお問い合わせについては、以下に気軽にご相談ください。

技術的なご質問・ご意見

学術情報センター（技術担当者）

E-mail：query@ml.wakayama-u.ac.jp

その他、PC・ネットワークの利用について

学術情報センター（情報管理係）

TEL：073-457-7177（内線 7177）

E-mail：aic@ml.wakayama-u.ac.jp