
「安全」を引き寄せる
8つの情報セキュリティ対策
佐賀大学総合情報基盤センター

はじめに

大学の教育研究が ICT への依存度を高めている中、情報セキュリティがますます重要となっています。その中で全構成員が情報セキュリティポリシーに則って、対策を講じることが求められますが、日々変化するセキュリティ問題への対応は容易ではありません。
本学では種々の情報セキュリティ対策を実施しており、その一環として、教職員、学生に向けた基本的なガイドブックを作成しました。
つきましては、本学においてはこのガイドブックを参考に、情報セキュリティ対策を確実に実施するようお願いします。

佐賀大学最高情報セキュリティ責任者（CISO）
理事　渡　孝則

セキュリティ対策を日常生活から考える

次ページで紹介する 10 大脅威における攻撃の手口はどれも巧妙ですが、セキュリティ対策としては、すぐに実践できることが多く含まれています。中には自動で（私たちが仕事をしている間に）実行できるものさえあります。

このガイドブックでは、ちょっとした注意や作業でセキュリティのレベルが向上する８つの基本的対策を紹介します。この８つの対策を全て実施して、各人の ICT 環境の安全性を高め、大学全体の ICT 環境をより安全なものにしていきましょう。

このガイドブックで紹介する８つの基本的対策

01　OS やアプリを最新の状態にしましょう
02　ウイルス対策ソフトを確実に使いましょう
03　パスワードを適切に管理しましょう
04　情報の持ち運びに気をつけましょう
05　メールのリンクや添付ファイルに注意しましょう
06　SNS は気をつけて使いましょう
07　Wi-Fi の利用に気をつけましょう
08　情報媒体を廃棄するときは一工夫しましょう

脅威！リスクは知らない間に忍び寄る

私たちの仕事や生活において、インターネットへの依存度が日々高まっています。
その中でパソコンやタブレット端末、スマホが活躍する場も広がり続けています。
これらは大変便利ですが、その一方私たちが気付かない間に、下記の「2023 年 10 大脅威※1」に見られるような様々な脅威が出現しています。どの脅威も私たちの身近でいつ起きてもおかしくないものばかりです。
このような状況の中で、私たちは自分自身にどのようなリスクがあるのか正しく知り、適切に対応することが求められています。

2023 年 10 大脅威

１位　ランサムウェアによる被害（前年 1 位）
２位　サプライチェーンの弱点を悪用した攻撃（前年 3 位）
３位　標的型攻撃による機密情報の窃取（前年 2 位）
４位　内部不正による情報漏えい（前年 5 位）
５位　テレワーク等のニューノーマルな働き方を狙った攻撃（前年 4 位）
６位　修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）（前年 7 位）
７位　ビジネスメール詐欺による金銭被害（前年 8 位）
８位　脆弱性対策の公開に伴う悪用増加（前年 6 位）

９位　不注意による情報漏えい等の被害（前年 10 位）
１０位　犯罪のビジネス化（アンダーグランドサービス）（前年圏外）

※1　2023 年 10 大脅威：2022 年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約 200 名のメンバーからなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。
https://www.ipa.go.jp/security/10threats/10threats2023.html

佐賀大学にとっての３大脅威

- **情報セキュリティ関連規程・ガイドラインの理解不足**
- **メール等によるウイルス感染**
- **USB メモリ紛失などによる情報漏えい**

０１　OS とアプリを最新の状態にしましょう

現実　OS やアプリの脆弱性への攻撃法が日々続々と出現

世間を騒がせているマルウェア※2、ランサムウェア※3は、オペレーティングシステム（OS：Windows、Mac OS、iOS、iPad OS、Android など）やアプリケーションソフトの脆弱性（いわゆる弱点）をついてきますが、その多くはパッチ※4 を適用していれば防ぐことができます。

対策　OS やアプリのアップデートをチェックし適用しましょう！

この対策は、パソコン・タブレット端末・スマホに共通です。

Windows パソコンの場合

Windows OS は、自動的にアップデートが行われます。
なお、サポート期限が切れた Windows OS は、セキュリティ更新プログラムは提供されませんので、必ず、サポート期間中の Windows OS にアップグレードしてください。
Windows OS のサポート期限
　Windows 8.1：2023 年 1 月 10 日

Windows 10 Home and Pro（22H2）：2025 年 10 月 14 日
Windows 11 Home and Pro（21H2）：2023 年 10 月 10 日
Windows 11 Home and Pro（22H2）：2024 年 10 月８日
アプリもバージョンを確認し、最新バージョンにしておきましょう。

Mac OS パソコンの場合

Mac OS の古いバージョンは、セキュリティ更新プログラムは提供されませんので、常に最新バージョンにしておきましょう。
アプリも App Store にアクセスして更新の有無を確認しましょう。

タブレット端末やスマホの場合

iOS、iPad OS、Android OS の古いバージョンは、セキュリティ更新プログラムは提供されませんので、常に最新バージョンにしておきましょう。
アプリも App Store や Google Play ストアにアクセスして確認しましょう。

※２　マルウェア（Malware）：有害な機能をもったプログラムの総称。ウイルス、ワーム、トロイの木馬などに分類されます。
※３　ランサムウェア（Ransomware）：暗号化などによってファイルを利用不可能にし金銭（身代金）を要求するマルウェア
※４　パッチ：ソフトウェアのベンダー（開発元）から配布される更新プログラム

０２　ウイルス対策ソフトを確実に使いましょう

現実　ウイルス対策ソフトをインストールしているのに機能していない

ウイルス対策ソフトをインストールしているにもかかわらず、ウイルス定義ファイルを日々更新していなかったり、ウイルスチェックをしていなかったり、ウイルス対策ソフト自体の有効期限が切れているケースがあります。これではセキュリティ対策になりません。

対策　毎日ウイルス定義ファイルの更新と週に１回はウイルスチェック

Windows10 以降であれば、Windows Defender により最低限の対策が可能ですが、ウイルス対策ソフトを別途インストールすることを推奨します。Mac OS も同様です。ウイルス定義ファイルの更新やウイルスチェックの開始時間を設定して、自動的に実行するようにすると良いでしょう。

タブレット端末やスマホもセキュリティ対策が必要です

セキュリティ対策は、タブレット端末やスマホにおいても必須です。特にスマホについては、フィッシングメールによる被害が多発していますので、迷惑メール対策などをしっかり行っておきましょう。

０３　パスワードを適切に管理しましょう

現実　パスワード設定の不備による成りすまし事件が多発

ID、生年月日、氏名といった公開情報をはじめ、他人にわかりやすい、推測しやすいパスワードを設定したことが原因で、第三者が成りすます事件が起きています。また、同一のID・パスワードの使い回しにより、ID・パスワードが盗まれて、成りすましの被害に遭う事件も発生しています。

対策　他人に推測されないパスワードで同じパスワードを使い回ししない

- 強度が強い（推測しにくい）パスワードにする
- パスワードは絶対に人に教えない
- パスワードの使い回しをしない
- パスワードを適切に保管する

また、下記のような場所で、ID、パスワードが盗まれることがありますので、注意しましょう。

- ホテル、ネットカフェなどの共用パソコン
- ホテル、駅、空港などのフリーWi-Fi

０４　情報の持ち運びに気をつけましょう

現実　USB メモリ紛失などによる情報漏えい事故が頻発しています

USB メモリなどの小型記憶媒体は情報の持ち運びに便利ですが、個人情報など重要なデータを入れた USB メモリを紛失、盗難にあうなどして、情報漏えい事故に発展するケースが後を絶ちません。

対策　本学アカウントの OneDrive を活用しましょう。

本学アカウントの OneDrive（Microsoft365 オンラインストレージ）を活用しましょう。
但し、下記のような使い方は、データの持ち出しとみなされる場合がありますので、注意しましょう。

- OneDrive に保存しているファイルを自宅などのパソコンにダウンロードすること
- 個人アカウントのオンラインストレージにファイルを保存すること

ファイルを共有して編集するような場合は、Teams のファイル共有を活用しましょう。
学外者とデータのやり取りが必要な場合は、OneDrive のリンク URL を活用し、リンク URL の作成時に有効期限とパスワードを設定するようにしましょう。

０５　メールのリンクや添付ファイルに注意しましょう

現実　メールを発端とする標的型攻撃が脅威となっています

標的型攻撃は特定の個人や組織を狙った攻撃で、おおむね以下の過程で攻撃が行われます。

❶ メールの添付ファイルやリンクをクリックしてウイルスに感染
❷ ウイルスが他のウイルスをダウンロードして進化
❸ 進化したウイルスが組織内の他のパソコンから情報を集めて外部に送信

様々な官公庁、民間企業が被害にあっていますが、❶のメールの文章が巧妙なため、攻撃に気付き難いというのが現状です。

対策　怪しいメールは疑い、総合情報基盤センターに確認を取りましょう

メールは簡単にニセモノを作ることができますので、知った相手からのメールと思っても、簡単に信用しないようにしましょう。特に知らない差出人から届いたメールにおいて、以下の場合は要注意です。

- 件名に緊急、重要、限定などと書かれている。
- 本文にリンクや添付ファイルが含まれている。

佐賀大学では、毎年、標的型攻撃メール訓練を実施しています。

０６　SNS は気をつけて使いましょう

現実　投稿内容や設定の不備でトラブルに発展することがあります

Facebook や X（Twitter）で不適切な投稿による「炎上」や、アカウントの乗っ取りによる不正使用などのトラブルが起きています。更に、プライバシー設定への配慮不足により、自他の情報を必要以上にネットに晒したり、投稿した写真から、自分の行動範囲を特定されたりするケースもあります。

SNS で問題となる投稿

教職員：不適切発言、誹謗中傷、学生の個人情報・成績等の漏えい、セクハラ、パワハラ（アカハラ）、非違行為

学　生：不適切発言、誹謗中傷、情報漏えい、非行行為自慢（カンニング、万引きなど）

SNS の利用に伴う炎上リスク（大学の評判に関するリスク）

- いたずら、悪ふざけ
- 違法な行為の暴露・自慢
- 大学内での不満、愚痴
- 大学内における違法な行為の告発
- 大学、学生、保護者、他大学等に対する批判、悪口
- 他者の名誉やプライバシーを侵害する書込み

対策　自分の設定を確認し、不適切な公開をしないように注意しましょう

以下の注意点に沿って、適切に SNS を利用するようにしましょう。特にスマホから気軽に利用できるので、より注意が必要です。

❶ 常に公開・引用・記録されることを意識して利用しましょう。
❷ 成りすまし防止のため複雑なパスワードを利用し、さらにセキュリティを高める設定を行いましょう。
❸ プロフィールや投稿内容の公開範囲を設定し、不必要な露出を回避しましょう。
❹ 知らない人とむやみに“友達”にならないようにして、知っている人でも本人かどうか確認しましょう。
❺ SNS の“友達”に迷惑をかけない設定を行いましょう。
❻ “友達”からの削除は慎重にして、制限リストなどの利用も考えましょう。
❼ 写真の位置情報やチェックインなど、技術的なリスクを正しく理解しましょう。
❽ むやみに“友達”のタグ付けや投稿をしないようにしましょう。
❾ セキュリティ対策ソフトを利用し、危険なサイトを利用するリスクを減らしましょう。

佐賀大学ソーシャルメディア利用に関するガイドライン（令和３年３月３０日制定）
https://www.saga-u.ac.jp/koho/sns.html

０７　Wi-Fi の利用に気をつけましょう

現実　Wi-Fi の利用で ID・パスワードなどが盗まれる被害が多発

今、学内外を問わず Wi-Fi が必要不可欠な世の中になっています。それに伴って Wi-Fi の通信を盗聴、のぞき見され ID・パスワードなどの個人情報が盗まれる被害も増えています。
特に暗号化などセキュリティ対策がされていないフリーWi-Fi（公衆無線 LAN）の利用には注意が必要です。

対策　暗号化などセキュリティ対策がされている Wi-Fi の利用

学内及び自宅で Wi-Fi 機器を設置する場合は、下記のセキュリティ対策を行いましょう。

- 通信の暗号化（WPA3 に対応した Wi-Fi 機器にする）
- Wi-Fi 機器の管理用 ID とパスワードを変更する
- SSID を変更して Wi-Fi 機器の機種を特定されないようにする
- 接続時のパスワードを設定する（初期パスワードから変更する）
- 接続する端末を制限する（端末の MAC アドレスを登録する）

ホテル、駅、空港などの暗号化されていないフリーWi-Fi に接続して ID、パスワードなどの個人情報を送信しないようにしましょう。

０８　情報媒体を廃棄するときには一工夫しましょう

現実　不用意に情報媒体を廃棄し、重要な情報が盗まれる被害

適切に処理されずに廃棄された情報媒体（紙、CD-ROM、USB メモリ、NAS、外付け HDD ほか）や情報端末（パソコンやタブレット端末など）から重要情報が漏えいする事故が起こっています。ゴミあさりによる情報収集（トラッシング）は現実の脅威です。

対策　中身の情報を読めないようにして廃棄しましょう

印刷物など紙媒体の場合

シュレッダーにかけるなどして内容が分からない形で捨てるようにしましょう。特に個人情報が含まれている場合は必須です。郵便物の宛名を墨塗りにするのも（プライベートを含めて）有効です。

CD-ROM や DVD-ROM などのメディアの場合

ディスクを壊してから廃棄しましょう。総合情報基盤センターにメディアシュレッダー（CD や DVD を粉砕する装置）がありますので、それをお使いになるのが最も手軽でしょう。

USB メモリ、SD カードなどの場合

金槌などで破壊し、物理的に利用できないようにしましょう。

パソコンの場合

消去ツールを使って削除しましょう。少々時間がかかりますが、確実に消去できます。フォーマットやファイル消去では、データが復元できる場合があるので注意が必要です。パソコンの記憶装置が HDD ならば、総合情報基盤センターに磁気破壊装置がありますので、この装置で HDD の磁気を破壊しデータを読めないようにできます。

NAS、USB 外付け HDD の場合

HDD を取り出して金槌などで破壊し、物理的に利用できないようにしましょう。または、総合情報基盤センターの磁気破壊装置で磁気を破壊しデータを読めないようにしましょう。

タブレット端末やスマホの場合

OS にデータ消去の機能がありますが、写真や履歴情報などが残ることがあります。タブレット端末やスマホに特化した消去ツールを使用しましょう。

佐賀大学情報セキュリティポリシーによって目指すもの

佐賀大学では情報セキュリティポリシー（第５版、令和２年８月）を策定しています。これは情報セキュリティの大切さを日頃から十分意識し、本学の情報資産を適切に管理運用するために、必要な取り決めを定めたものです。本学は情報セキュリティポリシーによって以下のことを目指しています。

❶ 本学の情報セキュリティに対する侵害を阻止。
❷ 学内外の情報セキュリティを損ねる加害行為を抑止。
❸ 情報資産に関して、重要度による分類とそれに見合った管理。
❹ 情報セキュリティに関する情報の取得を支援。
❺ 本学の構成員等による学内外への情報セキュリティの侵害を防止し、構成員等に対する教育を実施すること。
❻ 本学のセキュリティレベルの達成度について、セキュリティ監査を実施し随時見直しを行うこと。

佐賀大学情報セキュリティポリシー（教職員限定）
https://www.saga-u.ac.jp/jyoho/gakunai/policy/SecurityPolicy_20200717.pdf

佐賀大学では、下記の情報セキュリティ対策を行っています。

- e-ラーニング情報セキュリティ講習（教職員、学生）
- 教職員、学生へのウイルス対策ソフト（F-Secure）の提供
- 標的型攻撃メール訓練及び情報セキュリティ講習（教職員）
- ファイアウォール、迷惑メール・ウイルス対策システムの運用
- 学外公開サーバのセキュリティスキャン（年２回実施）
- パスワードの変更（有効期限１年）
- Microsoft365 ポータルの多要素認証
- 学外から情報システムログイン時のワンタイムパスワード
- ３大学（九工大、佐賀大、長崎大）間セキュリティ相互監査

システム及びネットワークの障害・メンテナンス情報、セキュリティ関連の情報等は、総合情報基盤センターのホームページにアップしています。
https://www.cc.saga-u.ac.jp/

IPA（情報処理推進機構）情報セキュリティの情報提供
https://www.ipa.go.jp/security/index.html

問合せ・連絡先

本ガイドブックの内容、情報セキュリティー般に関するご質問、相談など

総合情報基盤センター（本庄地区）
TEL：0952-28-8592（内線 8592）
E-Mail：cnc-office@ml.cc.saga-u.ac.jp

情報セキュリティインシデントの届出先

佐賀大学 CSIRT（本庄地区）
TEL：0952-28-8149（内線 8149）
E-Mail：CSIRT@mail.admin.saga-u.ac.jp

発行日：2022年 12 月
改　訂：2023 年 12 月
発　行：総合情報基盤センター