巻頭言

AI の利便性とコスト

吉浦紀晃
情報メディア基盤センター長

ここ数年、情報メディア基盤センターの年報の巻頭言を書いています。そのたびにセンターでの出来事を書こうとするのですが、何を書いても差し障りがあり、結局、そのときに考えていたことを書いています。今回もそうなりました。

ここ数年は AI の話題が持ちきりで、最近では「Claude Mythos」が話題です。私自身も AI を日常的に利用しており、調べ物や業務の軽減に役立てています。その一方で、Google などの検索エンジンを使う頻度や、検索結果の Web ページを開く回数は相当に減りました。

ここ数ヶ月、私は主に ChatGPT と Claude を利用しており、使い勝手という点では Claude に分があると感じています。実際の業務では、その効果をさまざまな場面で実感しています。ネットワーク管理では、障害時のログの分析を任せると瞬時に結果を返してくれるため、システムトラブル発生時の原因究明の速さが格段に向上しました。講演や授業の資料作成でも、PowerPoint に要点を書き込むだけで体裁よく清書してくれます。試験問題の作成にも利用しており、誤りを含む問題が生成されることはあるものの、作成作業そのものの負担は確実に軽減されました。ファイル形式の変換も可能で、たとえば MS Word で書かれた文書を、TeX と呼ばれる組版システムの形式へ変換してくれます。とりわけ印象的なのは、簡単なプログラムであれば細かな指示を与えなくても作成してくれる点です。ファイル変換プログラムであれば、変換元と変換先のサンプルを渡すだけで作成してくれます。従来は変換ルールを人間が定義する必要がありましたが、その手間すら不要です。

もっとも、これだけ便利であっても費用対効果から見れば、利用を続けるかどうかは悩ましい問題です。現在の私は「AI を使ってみよう」という興味が動機になっていますが、業務軽減の効果と利用料金とを純粋に天秤にかけたとき、その判断は必ずしも容易ではありません。例えばファイル変換プログラム作成が 100 円で済むなら迷いはありませんが、これが 1 万円ともなれば、自分でファイル変換プログラムを書いてしまうかもしれません。

この費用対効果という視点は、AI を企業や組織の業務に本格的に組み込もうとする際にも、なおさら重要になるはずです。今は、国内外を問わず、企業が社員に AI の利用を推奨し、使わなければそのこと自体を指摘されるような状況にあります。これは、AI によって何が可能になるのかを各社が見極めようとするトライアル期間だからであり、いわば費用対効果を度外視して利用が奨励されている段階だと言えます。しかし、このトライアル期間が終わり、AI を恒常的な業務に組み込む段階に至れば、最終的には費用対効果が重要な判断基準になるでしょう。AI への巨額の投資を思うと、それを回収するために設定される利用料金がどの水準に落ち着くのか、一抹の不安を覚えます。あるいは、いずれは AI が広告を出すようになるのかもしれません。

令和７年度 活動一覧

月	日	活　動　内　容	月	日	活　動　内　容
4	8	第1回センタースタッフ打合せ	10	1	第22回センタースタッフ打合せ
	15	第2回センタースタッフ打合せ		8	第23回センタースタッフ打合せ
	22	第3回センタースタッフ打合せ		15	第24回センタースタッフ打合せ
	29	第4回センタースタッフ打合せ		22	第25回センタースタッフ打合せ
5	13	第5回センタースタッフ打合せ		25	法定停電対応
	20	第6回センタースタッフ打合せ		29	第26回センタースタッフ打合せ
	27	第7回センタースタッフ打合せ	11	12	第27回センタースタッフ打合せ
6	3	第8回センタースタッフ打合せ	12	10	第28回センタースタッフ打合せ
	10	第9回センタースタッフ打合せ		17	第29回センタースタッフ打合せ
	17	第10回センタースタッフ打合せ		24	第30回センタースタッフ打合せ
	24	第11回センタースタッフ打合せ	1	7	第31回センタースタッフ打合せ
	26	第22回 国立大学法人情報系センター協議会総会（広島大学）		14	第32回センタースタッフ打合せ
7	1	第12回センタースタッフ打合せ		19	第2回東京大学情報基盤センター スーパーコンピューティング専門委員会（オンライン開催）
	8	第13回センタースタッフ打合せ			
	15	第14回センタースタッフ打合せ		21	第33回センタースタッフ打合せ
	22	第15回センタースタッフ打合せ		28	第34回センタースタッフ打合せ
	29	第16回センタースタッフ打合せ	2	4	第35回センタースタッフ打合せ
8	5	第17回センタースタッフ打合せ		18	第36回センタースタッフ打合せ
	26	第18回センタースタッフ打合せ		25	第37回センタースタッフ打合せ
9	2	第19回センタースタッフ打合せ	3	4	第38回センタースタッフ打合せ
	8	第1回東京大学情報基盤センター スーパーコンピューティング専門委員会（オンライン開催）		11	第39回センタースタッフ打合せ
				18	第40回センタースタッフ打合せ
	9	第20回センタースタッフ打合せ		25	第41回センタースタッフ打合せ
	16	第21回センタースタッフ打合せ		27	第1回情報メディア基盤センター会議 (オンライン開催)

令和７年度研究会・研修会等参加報告

Microsoft 大学ユーザー会
～大学×AI 活用の今と未来～

日　程:　6 月 3 日（火）
主　催：日本マイクロソフト株式会社
会　場：日本マイクロソフト株式会社 品川本社
参加者：杉田　吉弘
内　容：　大学×AI 活用がタイトルということで、Microsoft 製の生成 AI である Microsoft 365 Copilot を、各大学でどのように導入し、どのように活用し、どのように展開していくか、が主なテーマであった。

構成としては、まずは Microsoft 社員の方から Copilot の最新の動向や活用方法について講演があり、続いて、活用の方向性毎に、①主に事務業務への活用、②論文のオープンアクセス化に対応した活用、③学修成果の可視化への活用、の３つについて、それぞれの大学から事例共有があった。全体を通じて「エージェントの活用」について一番興味を惹かれたので、それについて記載する。

エージェントとは、Microsoft 365 Copilot のライセンスにより利用できる Copilot Studio で作成が可能な、“特定の仕事・役割に特化した専門の係”として動いてくれる AI のことだという。ブラウザ（最近だとアプリ版がいつの間にかインストールされる）ベースの Copilot Chat を総合相談窓口だとすると、エージェントは専門窓口というイメージになるだろうか。エージェントの利用する情報ソースをナレッジと呼ぶようであるが、このナレッジには、Web サイト、ファイル（PDF, Word, Excel, PPT, テキストファイル等）、SharePoint 等を指定することができ、FAQ やマニュアルが既にあるのであれば、それらをナレッジとして指定するだけでもある程度の回答を生成できるようになるようである。

これらのことから、エージェントを活用し、情報メディア基盤センター/情報基盤課の問合せ対応業務を効率化することが可能かもしれないと感じた。特定の業務に特化したエージェントを構築することで、職員や教職員からの問い合わせに対して、迅速かつ的確な対応が可能になると考えられる。

第 22 回 国立大学法人情報系センター協議会

日　程：6 月 26 日（木）
開催校：広島大学
会　場：広島大学 霞キャンパス

(電子会議システム利用によるハイブリット開催)

参加者：杉田 吉弘

（オンライン参加者：南雲 浩二、原口 史之、渋谷 大智、杉浦 徹志）

内　容：　国立大学法人の情報系センターにおける諸課題について、文部科学省、国立情報学研究所（以下、NII という。）による講演、各地区からの報告、オープンディスカッションが行われた。オープンディスカッションは初めての試みとのこと。

文部科学省からは情報科学技術分野に係る施策の動向について、NII からは、提供中のサービスの概要と今後の展望、次期 SINET、研究データ基盤としてのクラウドサービス、認証事業、NII-SOCS の現状と展望について紹介があった。次いで、各地区から報告があり、ICT インフラ維持管理という情報系センターの基本的な使命を全うするにも、サービスや機器の価格上昇、知見豊富な教職員の定年退職等によりぎりぎりの状況（もしくは立ち行かない状況）であることに加えて、DX 推進や ICT 人材育成、全学的な ICT 戦略企画立案等の新たなミッションが加わることで従前からの人材不足に拍車がかかり、大変厳しい状況にある大学が多い中、いくつかの大学（香川大学等）では全学の DX 推進や人材育成、経営層を巻き込んだ改革に着手しており、やり始めている大学がある一方で、踏み出せない大学も多くある、という印象を受けた。

本学においては DX や ICT 人材育成は主に事務局の経営企画推進課を筆頭に、各種プロジェクトチームやワーキンググループによる推進が始まって３～４年経過しており、着実に進んで来ている印象を持っているが、情報メディア基盤センター及び情報基盤課が積極的な関与を行っていない状況のため、今後は協力体制を作ることが必要になるかもしれない。

最後に、次回の協議会について、福岡教育大学が開催校となるが、大学の立地として、福岡市と北九州市に挟まれており、交通アクセスが良いとはいえないことから、対面であれば福岡市で実施、もしくはオンライン開催も視野に入れて検討していることが報告された。開催方法については、今後の幹事会で決定する予定とのことであった。

サイバー攻撃対策セミナー（ハンズオン形式）

～サイバー攻撃への対処　能力の強化に資する教養訓練～

日　程：10 月 20 日（月）、21 日（火）

主　催：埼玉県警察

会　場：埼玉会館７Ａ会議室

参加者：杉浦　徹志、渋谷　大智、金澤　英雄

内　容：　本セミナーは、サイバー攻撃の最新情勢や対策に関する講演に加え、イン

シデント発生を想定したハンズオン演習及びロールプレイングを通じて、実際の対応手順を学ぶ内容であった。講演では、ランサムウェア、APT グループ、サプライチェーン攻撃、VPN 機器の脆弱性悪用など、近年の攻撃事例や注意すべきポイントについて説明があり、組織として平時からログ取得、バックアップ、連絡体制、インシデント対応フローを整備しておく重要性を再確認した。

特に有用であったのは、インシデント発生時に端末から必要な情報を収集し、プロキシログ、Web アクセス履歴、ファイルアクセス、RDP 接続履歴等を確認するハンズオンである。講習で紹介された端末情報取得・証跡保全の考え方やツールは、実際に学内利用端末でマルウェア感染が疑われる事案が発生した際にも参考となり、状況把握や初動対応に役立った。机上の知識だけでなく、実際にどの情報を確認し、どのように切り分けを行うかを体験できた点は、日常業務に直結する内容であった。

また、隔離された演習環境においてランサムウェアの動作を確認できたことも非常に貴重であった。通常業務の中でランサムウェアの挙動を実際に見る機会はなく、ファイル暗号化の流れや、被害発生時にどのような痕跡が残るのかを具体的に理解することができた。さらに、被害発生後の情報共有、警察機関への連絡、関係者への報告、公表の考え方についても扱われており、技術的対応だけでなく、組織としての判断や連携の重要性を学ぶ機会となった。

各層別サイバーセキュリティ研修　CSIRT 研修（初級編）

日　程：11 月 11 日（火）～13 日（木）（第 1 回）
　　12 月 17 日（水）～19 日（金）（第 2 回）
主　催：文部科学省
会　場：オンライン
参加者：渋谷　大智（第 1 回）、杉浦　徹志（第 2 回）
内　容：　CSIRT 構成員としての役割を担い始めた人員を対象に、インシデント対応を含むセキュリティ対策の基礎技術や、ネットワークセキュリティ技術の習得を目的として実施された研修であった。

内容は情報セキュリティ全般にわたり、攻撃手法やアクセス制御、ログ分析、ネットワーク境界セキュリティなどが体系的に解説された。研修は教材の内容を中心に進められたが、講師がセキュリティ担当者としての実務経験を踏まえ、実践で役立つコマンドやツールを紹介していた点が有益であった。

仮想環境を利用した実習では、セキュリティ設定の実践や攻撃手順の再現、フォレンジック演習を通じて理解を深めることができた。特にファイアウォール設定やフォレンジックに関する内容は、今後の業務において活用可能な

知見であると感じた。（渋谷　大智）

本研修は、CSIRT の役割やインシデント対応の基本思想を中心に、組織的なサイバーセキュリティ対策の運用に必要な基礎知識を体系的に学ぶ内容であった。

講師の実務経験に基づき、攻撃の発生から検知、初動対応、封じ込め、復旧、再発防止に至る一連のフローが具体例とともに解説され、座学でありながら実運用を強く意識した深い理解を得ることができた。技術的なテーマについては、OWASP Top 10 をはじめとする Web アプリケーション脆弱性の概念、スキャンツールによる定期診断の重要性、IDS/IPS による通信監視の位置付けなどが取り上げられた。これにより、個別の技術要素を「点」ではなく、対策全体という「面」で捉える視点を養えたことは大きな収穫であった。また、Windows 環境における調査手法として、Sysinternals ツールを用いたプロセス・ファイル操作の可視化や、Security Compliance Toolkit (SCT) によるセキュリティベースラインの確認など、実務に直結する具体的な手法が紹介された点も非常に有用であった。特に、公開鍵・秘密鍵や電子証明書に関する解説は、単なる暗号技術の理論に留まらず、認証や通信の信頼性確保というインシデント対応の観点から再定義されており、既存知識をより実戦的なものへと昇華させる機会となった。（杉浦　徹志）

各層別サイバーセキュリティ研修　CSIRT 研修（応用編）

日　程：11 月 17 日（月）～21 日（金）
主　催：文部科学省
会　場：オンライン
参加者：吉浦　紀晃
内　容：　サイバーセキュリティにおける攻撃者の手法などを、演習形式で習得する研修であった。5 日間という長期の研修であったが、演習対象は脆弱性分析からクラウドコンピューティングまで広範囲にわたり、技術的な知見を深めることができた。

各層別サイバーセキュリティ研修　CISO・戦略マネジメント層研修

日　程：11 月 10 日（月）（第 2 回）、11 月 27 日（木）（第 4 回）
主　催：文部科学省
会　場：オンライン
参加者：伊藤　和人（第 2 回）、吉浦　紀晃（第 4 回）
内　容：　実効性のあるサイバーセキュリティ体制構築には、技術的な防御システム

の構築にとどまらず、組織文化の変革、人材育成、継続的な学習サイクルの確立を含む総合的な取り組みが必要であることについて、最高情報セキュリティ責任者(CISO)と戦略マネジメント層の理解を深めることを目的とする研修である。座学では、ランサムウェア被害が増加しているトレンド、サイバーセキュリティ犯行の手口は鍵開け、なりすまし、詐欺の組み合わせであること、インシデント対応体制の準備の重要性が説明された。

演習では大学でインシデントが発生したことを想定して、被害状況把握、対策、再発防止策の策定のグループワークを行い、インシデント発生後のCISO、戦略マネジメント層の役割について理解を深めた。

Microsoft 基盤で始める、AI エージェントの業務実装に向けた準備ポイント

日　程：2 月 12 日（木）
主　催：日本マイクロソフト株式会社
会　場：オンライン
参加者：渋谷　大智
内　容：　本研修では、AI を業務に活用していくうえで、生成 AI やツールを導入するだけでは十分な効果は得られず、組織としての基盤づくりが重要であるとの内容であった。

AI 活用は、個々の作業を効率化する段階から、業務プロセス全体を見直し、人と AI が協働して価値を生み出す段階へと移行しつつあり、人材育成や業務プロセスの再設計、AI 活用を前提とした組織体制や技術基盤の整備を、個別ではなく一体的に進める必要があるとのことであった。特に、既存業務を前提とした部分的な AI 導入では効果が限定的なので、業務全体を俯瞰した見直しが不可欠である点が示唆されており、今後は、自組織においても AI 導入そのものを目的とせず、業務の在り方や体制を含めた整理から検討していく必要があると感じた。

Microsoft Copilot 活用セミナー
～Copilot Chat だけでここまで変わる！日々の業務を圧倒的に効率化する方法～

日　程：2 月 25 日（水）
主　催：日本マイクロソフト株式会社
会　場：オンライン
参加者：齋藤　広宣
内　容：　Microsoft 365 ライセンスに含まれる Copilot Chat は「調べもののアシスタント」で情報収集に向き、アドオンライセンスが必要な Microsoft 365 Copilot は「仕事のパートナー」であり業務の効率化に力を発揮する、とい

う違いをふまえ、Copilot Chat の使い方に関するウェビナーが行われた。

生成 AI による出力は推測が入ることにより情報が発散ぎみになりがちなので、収束し安定した情報を得られるよう意識することが業務には必要であることが説かれていた。またそのための手法としてロール・プロンプティングや Few-Shot learning、また AI と対話を繰り返すことで回答のプロセスを踏ませること（Chain of Thought）などが、業務で直ちに使える手法として紹介された。

情報メディア基盤センター利用案内

令和 8 年 3 月現在

情報メディア基盤センター（以下、「センター」）では、以下のシステムの管理運営を行っています。利用には申請が必要な場合がありますので、詳細はセンターの Web サイトを参照してください。

https://www.itc.saitama-u.ac.jp

1. 全学情報基盤システム＝SERN

（**S**aitama university **E**ducation and **R**esearch **N**etwork）

1) 全学統一認証アカウント／Microsoft365 大学アカウント

全学生および教職員に、学内のシステム利用に必要なアカウントの発行を行っています。このアカウントで、センターが提供している学内 LAN の利用および学内の各部局で管理運営している様々なシステムへのログインが可能となります。なお、学外者が本学のネットワークを利用できる「一時アカウント」の発行も行っています。

2) Web ホスティングサービス

教育・研究・業務用のホームページ公開を目的とする Web ホスティングサービスを提供しています。令和 6 年度にサーバを更新し、システム変更とセキュリティの向上が行われました。

利用の形態は下記の 2 種類から選択することができ、コンテンツは利用者が自由に作成可能です。

・ディレクトリ型

・ホスト型

https://www.itc.saitama-u.ac.jp/services/hosting/webhosting2024.html

3) メーリングリストサービス

システム老朽化のため従来の GNU Mailman によるメーリングリストサービスを終了し、令和 6 年 8 月より「ニュースメール配信」サービスを新たに開始しました。イベント告知など学外の方への情報発信用の有料サービスです。

https://www.itc.saitama-u.ac.jp/services/mail/newsletter-delivery.html

4) ハウジングサービス（新規受付は停止しています）

5) 全学情報教育システム

ノートパソコン必携化(BYOD)実施に伴い、令和 7 年度より Windows 端末の設置を終了しました。計 120 台の中間モニタは引き続き設置し、講義および自習利用に提供しています。

https://www.itc.saitama-u.ac.jp/services/PCroom/

6) 情報倫理と情報セキュリティ e ラーニング

本学の学生・教職員全員が利用できる情報倫理および情報セキュリティを学ぶための e ラーニング教材「INFOSS 情報倫理」を用意しています。

https://www.itc.saitama-u.ac.jp/services/e-learning.html

2. マイクロソフト包括ライセンス契約

平成 28 年度より日本マイクロソフト株式会社と包括ライセンス契約を締結しており、実際の利用にあたっての窓口をセンターが担当しています。詳細はマイクロソフト包括ライセンス利用案内をご覧ください。

3. クラウド DNS コネクトサービス

令和 4 年度より旧 DNS ホスティングサービスに代わり、クラウド利用によるサービスを提供しています。ドメイン管理者はセンターに対して、自ドメイン（ゾーン）の全レコード情報の閲覧およびレコードの修正・追加・削除作業を依頼することができます。

4. 証明書発行サービス

国立情報学研究所の「UPKI 電子証明書発行サービス」を利用して、必要なサーバ証明書の発行を受けることができます。

5. 学術認証フェデレーション「学認（GakuNin)」

学術認証フェデレーション（以下、学認）とは、学術 e-リソースを提供する機関と、これを利用する大学等で構成された連合体です。学認が定めたポリシーの下、相互に信頼しあうことにより Web 上の認証連携が可能となっています。

埼玉大学は平成 30 年度より学認に参加しており、下記のサービスを提供しています。

・大容量ファイル転送サービス「NII FileSender」
・学術クラウドゲートウェイ
・eduroamJP 認証連携 ID サービス

6. 東京大学スーパーコンピュータの利用

東京大学情報基盤センターが提供している各種スーパーコンピュータシステムを利用する場合の利用料の一部を負担しています（令和 8 年 3 月で利用料の一部負担は終了しました)。

7. 大判プリンタ

学会のポスター等に利用可能な B0 サイズまで印刷できるプリンタを用意しています。
学生が使用する場合は指導教員の許可が必要です。
詳細は大判プリンタ利用案内をご覧ください。

1SERN

Saitama University Education and Research Network

(全学情報基盤システム)

有線認証画面

学内無線

1)全学統一認証アカウント/
Microsoft365 大学アカウント

5)全学情報教育システム

中間モニタ

クラウドプリントサービス

2)Web ホスティングサービス
3)メーリングリストサービス
(News Letter)
4)ハウジングサービス

6)情報倫理と情報セキュリティ
(e ラーニング)

3 クラウド DNS
コネクトサービス

4 UPKI
電子証明書発行サービス

5 学術認証フェデレーション
(GakuNin)

6 東大スーパーコンピュータ

7 大判プリンタ × 2

Designjet T930

Designjet T1700dr

2 マイクロソフト
包括ライセンス契約
Microsoft365 Education

マイクロソフト包括ライセンス　利用案内

埼玉大学では平成28年度より日本マイクロソフト株式会社と包括ライセンス契約を締結しています。Office ソフトやクライアントアクセスライセンス（CAL）等のマイクロソフト製品の利用が可能なほか、本契約に付随する特典としてマイクロソフトのクラウドサービス Microsoft365 Education を利用することができます。

情報メディア基盤センターでは、ユーザーが本契約によるサービスを享受できるようにソフトウェアの整備と管理を行い、契約に則した適切なアカウント（Microsoft365 大学アカウント）を発行するとともに利用要項の整備を行っています。

定期的に契約を締結し直すため、契約内容は変更される可能性があります。利用の際は情報メディア基盤センターのホームページにて、利用資格や手順を確認してください。

◆Microsoft 365 大学アカウントの発行

本学の学生および教職員に Microsoft 365 大学アカウントを付与しており、本学在籍中は下記サービスを利用することができます。

1) クラウド電子メールサービス “Exchange Online”（旧称：Office365 メール）
本学の学生および教職員のメールシステムとして採用しています。
https://www.itc.saitama-u.ac.jp/services/mail/CloudMail.htm

2) Microsoft365 配布グループ（メーリングリスト）
組織や係等、複数のメンバーへ同じメールを配信するためのメールアドレスを付与しています。従来の代表メールアドレス（組織メールアドレス）に代わるサービスとして、令和 5 年 3 月に旧サービスからの移行手続きと並行運用を開始しました。
https://www.itc.saitama-u.ac.jp/services/MS/M365-DistributionGroup.html

3) Microsoft365 Apps for enterprise（個人利用端末向け）
・Word　・Excel　・PowerPoint　・Access（Windows のみ）
・Outlook　・OneNote　・OneDrive　・Teams　など
https://www.itc.saitama-u.ac.jp/services/MS/CloudOffice.html

◆ソフトウェアの提供

埼玉大学の資産であるコンピュータで利用できるソフトウェアの提供をしています。

1) Microsoft Windows OS（アップグレードライセンス版）
https://www.itc.saitama-u.ac.jp/services/MS/windowsSA.html

2) Microsoft365 Apps 共用端末向け（シェア方式・ デバイスライセンス方式）
https://www.itc.saitama-u.ac.jp/services/MS/CloudOffice-special.html

大判プリンタ　利用案内

情報メディア基盤センターにて、カラー印刷のできるプリンタを２台用意しています。学会用ポスターの作成等にご活用ください。

【利用資格】　本学の教職員および教職員の許可を得た学生
【利用料金】　1 枚 1000 円
【印刷サイズ】　B0 サイズまで
※ロール紙利用につき横断幕のような長いものも印刷可能（要事前相談）
【申請方法】　事前申請は不要です。
センター窓口にお越しいただき、大判プリンタを使用したい旨をお申出ください。職員が設置場所（センター棟 2F）へご案内します。
窓口受付期間　　：平日 9:00～16:30（12:15～13:15 を除く）
プリンタ利用時間：平日 9:00～16:50※時間内にご退室ください

【プリンタについて】
現在センターでは、下記２台の大判カラープリンタを保有しています。
用紙およびインクは、必ず備え付けのものをご利用ください。
お持込みはできません。
① HP DesignjetT930　（A 判専用）
② HP DesignjetT1700dr
※大判プリンタの詳細は下記をご参照ください。
https://www.itc.saitama-u.ac.jp/services/printer.html

①

②

専用カッターを備えています
用途に合わせてご利用ください

センターより

情報セキュリティ教育の充実に向けて、情報セキュリティ・情報倫理に関するポスターを作成し、掲示しています。

情報セキュリティ・倫理マニュアル

Saitama University 埼玉大学

安心して情報システムを利用するための10か条

1. OSやソフトウェアは常に最新版にしましょう

PCやスマートフォンの基本ソフトウェア（OS）やアプリケーションソフトウェアを更新して，セキュリティ対策を最新にしましょう。

2. ウイルス対策を徹底しましょう

IDやパスワードを盗んだり，遠隔操作を行ったり，ファイルを勝手に暗号化するウイルスが増えています。PCやスマートフォンにはウイルス対策ソフトを導入しましょう。

3. ID・パスワードは適切に管理しましょう

IDとパスワードは本人であることを証明する大切な情報です。パスワードは，第三者に「教えない」「知られない」ようにしましょう。容易に推測される誕生日，名前などを使ったり，同じパスワードを使い回したりするのはやめましょう。多要素認証が利用できる場合は有効にしましょう。

4. 不審なメールは無視（削除）しましょう

不審なメールのリンクのクリックや，添付ファイルを開くとウイルスに感染する可能性があります。メールの差出人を確認し，知らない人から届いたメールは無視（削除）しましょう。差出人の「なりすまし」を防ぐため，メールソフトやスマートフォンなどのフィルタ機能を上手に使いましょう。

5. 情報管理に注意しましょう

ウイルス感染やネットワークの侵入，PCやUSBメモリの盗難・紛失により個人情報が漏洩する事件が多発しています。個人情報や機密情報を含む重要なファイルはパスワードでロックして，管理を徹底しましょう。なくなると困る重要なファイルはバックアップを作成して適切に保管しましょう。

6. Webページの通信が暗号化されているか確認しましょう

Webページでパスワードやクレジットカード番号などを入力するときは，盗聴や改ざんを防ぐため通信暗号化を確認しましょう。Webページのアドレス先頭が「https://」となっているか，Webブラウザのアドレス欄に鍵「🔒」マークが表示されていれば通信が暗号化されています。

7. 著作権などの知的財産を侵害してはいけません

著作物やデザインを無断で複製したり，WebページやSNSに掲載したりしてはいけません。
正当なライセンスのないソフトウェアを使用したり，違法ダウンロードしたりしてはいけません。

8. 掲示板やSNSは注意して利用しましょう

現実社会と同様にインターネット上でもルールやマナーを守り，掲示板やSNSで個人等を誹謗中傷してはいけません。書き込みはうのみにせず，デマやフェイクニュースでないか確認しましょう。

9. 個人情報やプライバシー情報を守りましょう

埼玉大学
マスコットキャラクター
メリンちゃん

インターネット上に，安易に個人情報やプライバシー情報を公開することは危険です。
自分や家族，友人の個人情報をSNSに掲載するときは，情報の公開範囲に注意しましょう。
写真を公開するときは、一緒に写った人に事前に許可を取りましょう。

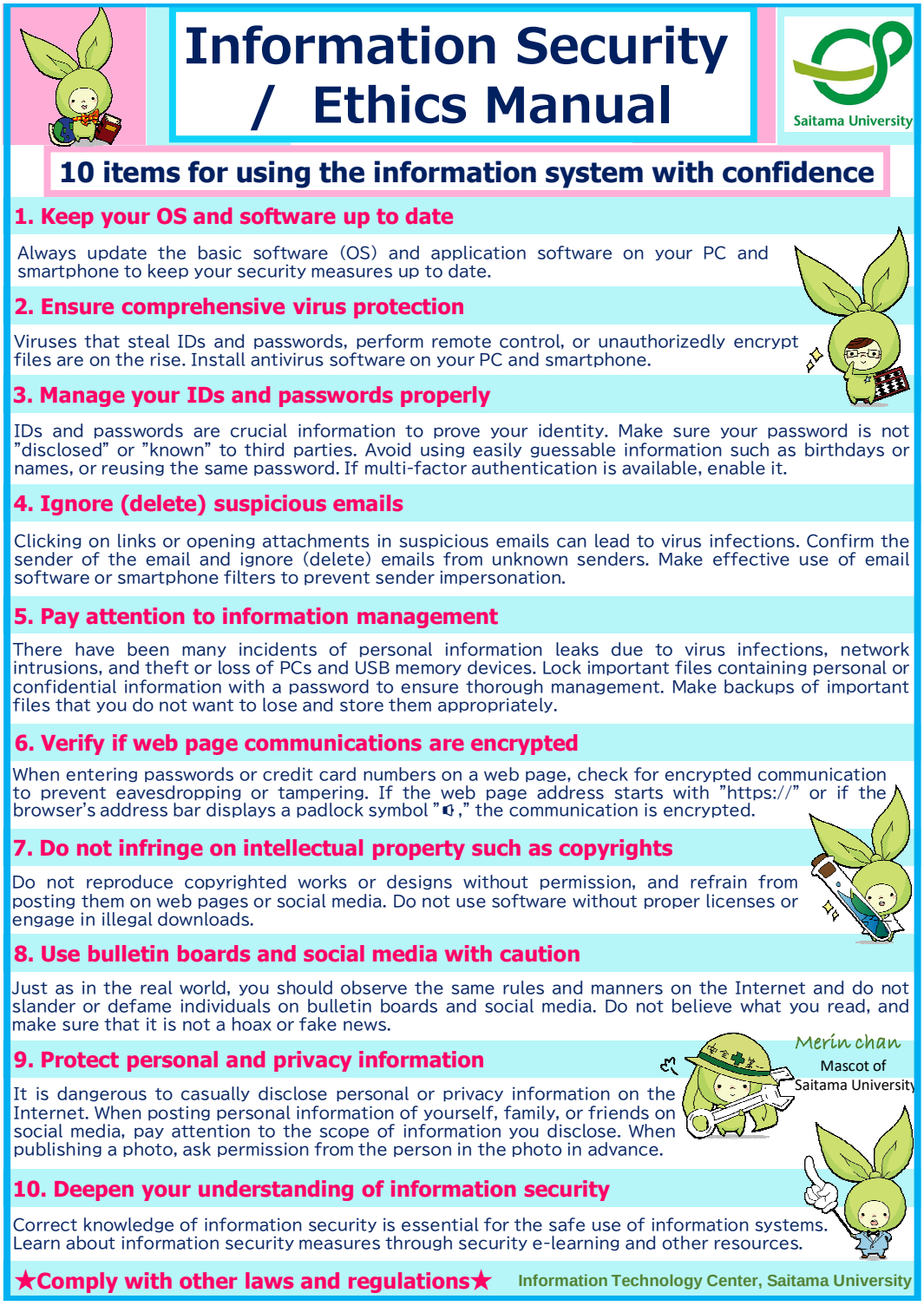
10. 情報セキュリティに関する理解を深めましょう

情報システムの安全な利用には情報セキュリティに関する正しい知識が大切です。
情報セキュリティeラーニングの受講などによって、情報セキュリティ対策を学びましょう。

★その他法令を遵守しましょう★

埼玉大学情報メディア基盤センター

情報機器やネットワークを利用する上で情報セキュリティと情報倫理について注意すべき10項目を挙げ、多様な留学生が在学することに配慮し、日本語のほかに英語のバージョンを作成、ポスターサイズに印刷したものを学内各所に掲示しています。



Information Security / Ethics Manual

Saitama University

10 items for using the information system with confidence

1. Keep your OS and software up to date

Always update the basic software (OS) and application software on your PC and smartphone to keep your security measures up to date.

2. Ensure comprehensive virus protection

Viruses that steal IDs and passwords, perform remote control, or unauthorizedly encrypt files are on the rise. Install antivirus software on your PC and smartphone.

3. Manage your IDs and passwords properly

IDs and passwords are crucial information to prove your identity. Make sure your password is not "disclosed" or "known" to third parties. Avoid using easily guessable information such as birthdays or names, or reusing the same password. If multi-factor authentication is available, enable it.

4. Ignore (delete) suspicious emails

Clicking on links or opening attachments in suspicious emails can lead to virus infections. Confirm the sender of the email and ignore (delete) emails from unknown senders. Make effective use of email software or smartphone filters to prevent sender impersonation.

5. Pay attention to information management

There have been many incidents of personal information leaks due to virus infections, network intrusions, and theft or loss of PCs and USB memory devices. Lock important files containing personal or confidential information with a password to ensure thorough management. Make backups of important files that you do not want to lose and store them appropriately.

6. Verify if web page communications are encrypted

When entering passwords or credit card numbers on a web page, check for encrypted communication to prevent eavesdropping or tampering. If the web page address starts with "https://" or if the browser's address bar displays a padlock symbol "🔒," the communication is encrypted.

7. Do not infringe on intellectual property such as copyrights

Do not reproduce copyrighted works or designs without permission, and refrain from posting them on web pages or social media. Do not use software without proper licenses or engage in illegal downloads.

8. Use bulletin boards and social media with caution

Just as in the real world, you should observe the same rules and manners on the Internet and do not slander or defame individuals on bulletin boards and social media. Do not believe what you read, and make sure that it is not a hoax or fake news.

9. Protect personal and privacy information

It is dangerous to casually disclose personal or privacy information on the Internet. When posting personal information of yourself, family, or friends on social media, pay attention to the scope of information you disclose. When publishing a photo, ask permission from the person in the photo in advance.

Merin chan
Mascot of
Saitama University

10. Deepen your understanding of information security

Correct knowledge of information security is essential for the safe use of information systems. Learn about information security measures through security e-learning and other resources.

★Comply with other laws and regulations★

Information Technology Center, Saitama University

情報メディア基盤センター教職員名簿

【情報メディア基盤センター】

センター長

吉　浦　　紀　晃	教授（併任） （理工学研究科数理電子情報部門）	

専任教員

間　邊　　哲　也	准　教　授	
松　田　　哲　直	准　教　授	

【総務部情報基盤課】

課　　長

南　雲　　浩　二		

課長代理

二　川　目　　一		令和7年7月～

技術職員

齋　藤　　広　宣	主任技師	
天　野　　直　子	技　　師（併任）	
東　　宏　樹	専門技術員（併任）	～令和7年5月
金　澤　　英　雄	専門技術員（併任）	令和7年6月～
渋　谷　　大　智	専門技術員（併任）	
杉　浦　　徹　志	専門技術員	令和7年4月～
倉　永　　直　樹	派遣職員	

事務職員

原　口　　史　之	主　　査	～令和7年8月
佐　藤　　泰　弘	主　　査	
杉　田　　吉　弘	主　　査	
田　中　　桂　太	主　　査	令和7年9月～
村　松　　美由起	事務補佐員	
中　村　　由紀子	事務補佐員	
小　峰　　麻貴子	事務補佐員	～令和7年10月
中　村　　美　樹	事務補佐員	

埼玉大学情報メディア基盤センター規程は、下記を参照してください。
https://www.saitama-u.ac.jp/houki/houki-n/reg-n/2-2-20.pdf

埼玉大学情報メディア基盤センター年報
『 さいたま 』
Vol.32　2026.6（令和 8 年）

発行者　埼玉大学情報メディア基盤センター
〒338-8570　　さいたま市桜区下大久保 255
電話　　048-858-3674