京都大学情報環境機構広報誌「Info!」

2026.2.13 No.33

Info!

Contents

ISSN 2188-7195

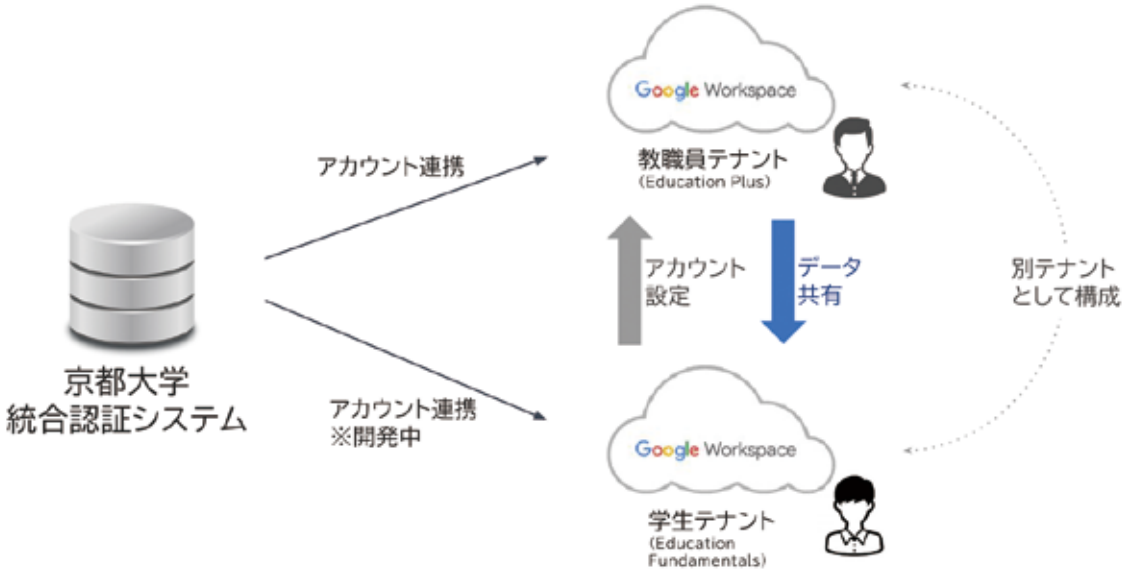
お知らせ

【2026年4月開始】学生用Googleアカウントの提供について ～Google ドライブ、カレンダーに加え、最新の生成AI『Gemini』も安全な環境で利用可能に～

情報環境機構では、2026年4月より、全学生・非常勤講師・名誉教授等のECS-ID保有者を対象に「学生用Googleアカウント」の提供を開始します。これまで教職員にはグループウェアとしてGoogle Workspaceを提供してきましたが、今回、新たに学生用の環境（テナント）を構築し連携させることで、セキュリティを担保しつつ、データ共有の利便性向上や教育・研究活動の効率化を推進します。

1. 導入の背景と仕組み

これまで、学生と教職員間でのファイル共有やスケジュール調整において、プラットフォームの違いによる不便さが課題となっていました。今回、教職員用テナントとは独立した「学生用テナント（ドメイン：st.kyoto-u.ac.jp）」を構築することで、既存の教職員データへのアクセス権限を明確に分離し、安全な連携を実現します。教職員と学生間のデータ共有は、教職員が利用しているGoogle Workspaceの各種サービスに学生のアカウントを共有設定することで行います。



2. 提供する主なサービス

学生用アカウントで利用できるサービスは、コラボレーションに必要な機能に厳選して提供します。

- Google ドライブ　　：資料の保存・共有
- Google カレンダー　：研究室やゼミでの予定共有、共同管理
- Google Chat / Meet　：グループディスカッションやクイックな連絡
- Gemini / NotebookLM：生成 AI の活用による学習・研究支援
- Google Classroom　　：授業課題の共有など（教職員テナント側で提供）

⚠ 重要：Gmailは提供されません。学生用メール（KUMOI）は、引き続きMicrosoft 365を利用してください。

3. 具体的な活用シーン

教職員と学生が同じGoogle Workspaceプラットフォームを利用できるようになることで、以下のような活動がスムーズになります。

【研究室・ゼミ】資料共有と共同編集
教職員が作成した共有ドライブやフォルダに学生を招待することで、論文指導や資料の共有、共同編集がシームレスに行えます。また、Google カレンダーでの予定共有により、ミーティング調整が容易になります。

【授業】Google Classroom の活用
教職員テナントで Google Classroom を利用し、学生を招待することで、課題の配付・提出や連絡事項の共有が可能になります。LMS（学習管理システム）の補完的なツールとしても活用が期待されます。

【研究・学習支援】生成 AI ツールの利用
Gemini や NotebookLM といった Google の最新 AI ツールが安全に利用可能になります。文献の要約やアイデア出しなど、研究・学習活動の補助として活用できます。

4.【重要】既存アカウントに関する注意点

すでに「@st.kyoto-u.ac.jp」で個人のGoogleアカウントを作成している方へ
現在、大学のメールアドレス（@st.kyoto-u.ac.jp）を使用して、独自に個人のGoogleアカウントを作成・利用している場合、2025年12月以降のテナント設定時に競合が発生します。対象となる学生には別途詳細を案内しますが、別のメールアドレスに変更するなど、データの退避・移行が必要となりますのでご注意ください 。

5. スケジュール（予定）

2026年3月頃 ： 在学生・新入生のアカウント作成・案内
2026年4月　 ： サービス正式リリース・運用開始

利用マニュアル等、詳細については、2026年3月頃に改めてお知らせします。
この新しい環境が、皆様の教育・研究活動のさらなる活性化につながれば幸いです。2026年4月より、ぜひご活用ください。

（ 澤田：情報環境機構 IT基盤センター 電子事務局グループ ）

お知らせ

PandAのサービス終了と、あらたなLMSの運用について

本学のLMS（学習管理システム：Learning Management System）は、情報環境機構が提供するPandA（呼称）を2013年度より運用してきましたが、2026年3月より新たなLMS（Kyoto University LMS：KULMS（仮称））を運用する予定です。

KULMSは、PandAと同じオープンソースのLMS Sakaiをベースにしており、慣れ親しんだ画面構成を維持しつつ、操作性の改善、アクセス集中にも対応できるシステム強化を図っています。

なお、PandAは2027年2月末まではKULMSと並行して運用を行いますが、2026年3月以降は原則としてKULMS主体の運用へ移行する予定です（※）。

今後KULMSに関するお知らせや操作マニュアルなどは、学務部で準備中のWebサイトに掲載する予定ですが、掲載先については、情報環境機構のPandAのご案内ページでもお知らせする予定としています。見落としのないようにご注意ください。
情報環境機構 学習支援システムPandA : https://www.iimc.kyoto-u.ac.jp/ja/services/education/lms

※並行運用期間中（2026年3月～2027年2月末）のPandAの利用について
データ移行期間として、過年度の授業資料をダウンロードすることが可能です。2026年度開講科目については、原則としてPandAは利用できませんのでご注意ください。

（ 学務部教務企画課教育情報推進室 ）

お知らせ

2026年3月に京都大学から 離籍（卒業・修了、 退職・離職など）、身分変更の方へ

京都大学から発行している全学アカウント（ECS-ID/SPS-ID[*1]）は、京都大学に籍がなくなれば利用できなくなります。また、身分変更で全学アカウントが切替わる場合があります。
全学アカウントが利用できなくなると、各アカウントに紐づく提供サービス[*2]も利用できなくなります。

【サービスの一例】

- 全学メール[*3]　KUMOI/KUMail
- 統合型クラウドサービス[*4]　Google Workspace/Microsoft365
- オンラインミーティング[*5]　Zoom/Google Meet
- データ保存・ストレージ[*6]　GoogleDrive/OneDrive(Microsoft365)/KUMailストレージ/RDM Driveなど

離籍・身分変更などが予定されている場合は、時間の余裕がある間に各サービスの案内を確認して、データのバックアップ・移行・引継ぎなどをご自身で行ってください。
また、生涯メール[*7]の利用、メールの転送・不在通知などの設定についても離籍・身分変更などの前に検討ください。

対象者となる方の種別に応じた対応を纏めました。下記をご確認ください。

（学生向け）卒業時の対応
https://www.iimc.kyoto-u.ac.jp/ja/guide/students/graduate-guide.html
（非常勤講師・その他の方向け）身分終了時の対応
https://www.iimc.kyoto-u.ac.jp/ja/guide/others/leave-guide.html
（教職員向け）退職・異動時の対応
https://www.iimc.kyoto-u.ac.jp/ja/guide/faculty-staff/retire-guide.html

離籍・身分変更などのご不明な点につきましては、まず所属の各部局にお問い合わせください。
全学アカウントやサービスについてのご不明な点につきましては、下記からお問い合わせください。時期によっては、問い合わせが集中し、回答まで時間をいただく場合がありますので時間に余裕をもってご相談ください。

情報環境機構　お問い合わせ
https://www.iimc.kyoto-u.ac.jp/ja/inquiry/

---

*1 全学アカウント（ECS-ID/SPS-ID）
https://www.iimc.kyoto-u.ac.jp/ja/services/account/
ECS-ID 学生・非常勤講師等のアカウント
SPS-ID 教職員のアカウント

*2 提供サービス
https://www.iimc.kyoto-u.ac.jp/ja/services/
情報環境機構が提供しているサービス一覧

*3 全学メール（KUMOI/KUMail）
https://www.iimc.kyoto-u.ac.jp/ja/services/mail/
KUMOI 学生・非常勤講師等のメール
KUMail 教職員用メール

*4 統合型クラウドサービス
https://www.iimc.kyoto-u.ac.jp/ja/services/cloud-service/
Google Workspace/Microsoft365

*5 オンラインミーティング
https://www.iimc.kyoto-u.ac.jp/ja/services/online-meeting/
Zoom/Google Meet

*6 データ保存・ストレージ
https://www.iimc.kyoto-u.ac.jp/ja/services/storage/
GoogleDrive/OneDrive(Microsoft365)/KUMailストレージ/RDM Driveなど

*7 京都大学同窓生向けサービス、生涯メールアドレス
https://www.alumni.kyoto-u.ac.jp/static/service.html

（ITサービスデスク：情報環境機構）

お知らせ

生成AIサービスにおける情報セキュリティ上の注意点と学内の各種生成AIサービスについて

※本記事は、2025年12月15日時点の情報に基づいて執筆しています。

1. はじめに

近年、ChatGPTの出現を発端として、生成AI (Generative Artificial Intelligence) 技術を活用した様々なサービスが社会的に急速に広まっています。当初はチャット型のテキスト生成サービスが中心でしたが、画像や動画、音声などデータの種別を超えたマルチモーダルな情報を統合的に扱うことができるように進化してきています。今後、こうした生成AIサービスは、研究、教育、学習、諸業務など大学においても必要不可欠なものになっていくことと予想されます。
生成AIサービスは便利である一方、その性質を理解した上で取り扱いに十分注意する必要があります。特に、情報セキュリティの観点においては、生成AIサービスを介した意図しない情報漏洩に注意を払うことが求められます。
本稿は、情報セキュリティの観点から、本学における情報の取り扱いに関する一般的なルールをふまえつつ、生成AIサービスの利用にあたっての注意点や選定の原則を簡潔にまとめたものです。また最後に、現時点で本学環境において利用可能な主な生成AIサービスについて紹介します。

2. 生成AIにおける情報の流れ

生成AIにおいて扱われる情報の流れを理解する上で、文化庁から公開されている「AIと著作権」の資料(https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html)で示される例が一般的な概念としてわかりやすく参考になります。ここでもその資料の図や用語に基づいて説明することとします。

生成AIは非常に高度で複雑な処理が行われているという印象がありますが、その他の様々な情報サービスと同様に、入力された情報に対して処理が行われ、処理された結果としての情報が出力される、という関係に一般化して整理することができます。高度化が進む生成AI技術も、基本的にはこの一般的な例を原則として整理することが起点となります。

情報の機密性（公開情報か機密情報か）を意識した図に描きなおしたものを図1（「生成AIにおける情報処理プロセス」）に示しますが、生成AIにおける処理は、「AI開発・学習段階」と「生成・利用段階」の2段階に分けることができます。

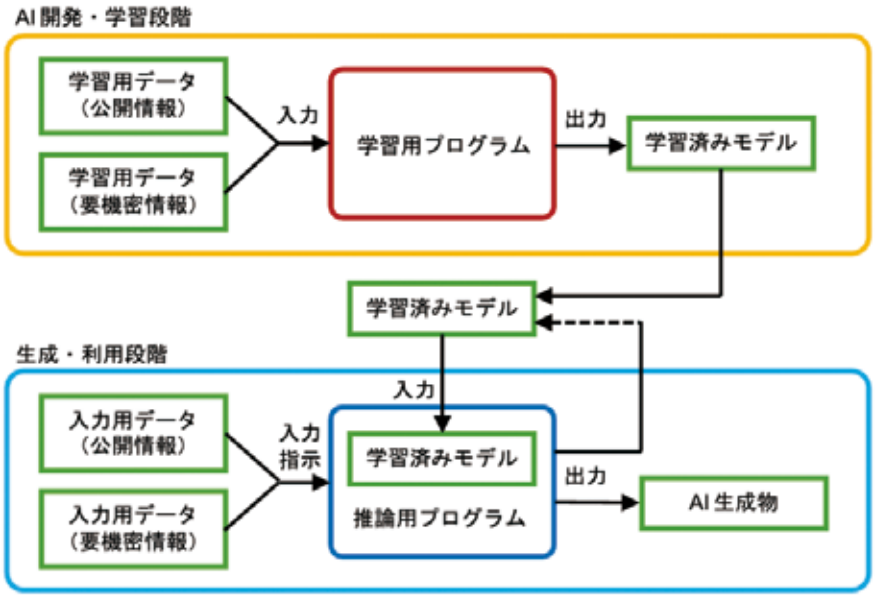


図1：生成AIにおける情報処理プロセス

また、それぞれの段階において、情報の入力と出力が存在します。このように、生成AIにおいても、その処理は入力された情報に対して加工して出力する仕組みとして整理することができ、入力に機密情報が含まれていると、出力にも入力された情報に由来する機密情報を含む可能性があります。機密情報が含まれるかどうかを明確に判断できないのは、学習済みモデルやその取扱いが（利用者から見て）ブラックボックスであり、生成AIの処理の中で情報がどのように加工されるかという挙動を容易に予測することができないためです。このため、生成AIにおいては「可能性を持つ」という曖昧な特性を強く意識した取り扱いが求められます。なお、この図では、後半の「生成・利用段階」においても出力として学習済みモデルへの反映処理を含んでいるところが、文化庁の図より少し複雑になっています（後の説明に関連します）。

3. 情報の取り扱いにおける一般的な注意点

まず最初に、生成AIに限らない、情報を取り扱う上での一般的な注意点について整理します。この整理は、生成AIサービスを分類する上での基本事項となるものです。

3. 1　情報の格付け

情報には、誰もが自由にアクセスすることが可能な公開情報と、関係者以外が自由にアクセスできてしまうと不都合な情報（非公開情報、機密情報）の区別があります。後者は要機密情報とも呼ばれますが、情報が関係者以外に公開されて（漏洩して）しまった場合に、どのような（どの程度の）損害が発生するのかについて、あらゆる状況を想定し（リスク評価）、それらを踏まえたうえで、情報を保護するためにどのような（どの程度厳しい）取り扱い方が必要かを定め、その取扱い方を徹底することが求められます。

要機密情報を守るための手段としては、様々な取り扱い条件（ルール）が考えられますが、取り扱い条件が取り扱う情報ごとに多岐にわたると情報の取り扱いが煩雑になるため、組織としての標準的な要機密情報の分類と、分類に応じた取り扱い方法を定めることが一般的です。その標準は組織ごとの「情報格付け基準」として定められ、組織に所属する者が守るべき規程（ルール）となっています。

情報の内容や重要度に応じて、取り扱い条件を標準に基づき分類を行うことを情報の「格付け」と呼び、京都大学において教職員等は、情報を作成または入手する際に格付けを行うものとされています（「京都大学情報セキュリティ対策基準」第62条）。また、その情報に触れる者は、指定された格付けに対応した取り扱いを行うことを徹底するものとされています（同基準第66条）。情報の格付けの具体的な分類や取り扱い、各種情報の標準的な内容に応じた格付けの例は、「京都大学情報格付け基準」にて示されており、実際の手順等は部局ごとに決定し周知徹底することが求められています。

本学においては、「機密性1情報」は要機密情報でない情報のことを指し、機密情報は「機密性2情報」または「機密性3情報」に分類されます。

例えば、公表されている天気予報の情報、公共施設の住所や営業時間などであれば、取り扱いに気を遣うことはないと思いますが、これらは機密性1情報にあたります。一方、家族や友人の住所や氏名となれば、ある程度気を遣い他人に伝えるときは慎重に判断すると思います。金融機関のIDやパスワードとなれば、他人に漏れないように厳重に扱っているのではないかと思います。これらは機密性2情報（パスワードは場合によっては機密性3情報）にあたります。こうした、皆さんの日常的な感覚に基づく情報の取り扱いと同様に、組織の中の情報についても、組織として関係者が協力しながら慎重に扱うことが求められています。

前述の情報格付けに基づく情報の取り扱いの徹底は、当然のことながら生成AIの利用においても求められます。生成AIにおいて、入力された情報がどのように扱われる可能性があるかを確認し、情報格付けで求められる取り扱いに違反するような意図しない情報漏洩が発生しないよう注意しながら利用する必要があります。

3．2　クラウド型サービスの利用

近年、Google WorkspaceやMicrosoft 365をはじめとするクラウド型サービスの普及が急速に進んでおり、クラウド型サービスを利用しない日はないほどの状況となっています。このようなクラウド型サービスに代表されるような、他者（他組織）が運用管理するシステムは外部サービスとも呼ばれますが、クラウド型サービスを利用する場合には、そのシステムに入力した情報がどのように扱われる可能性があるかについて意識しておく必要があります。具体的には、システムのおおまかな構成やサービス内容を理解した上で、構成要素のどの部分が自分や自組織専用として扱われ、どの部分が他者（多組織）と共用されるのかを確認しておくことが重要です。特に生成AIにおいては「学習」という仕組みを持つことから、どのような情報（データ）が学習に利用され、その学習結果を誰が利用しうるのかを意識する必要があります。自分が入力した情報をもとに学習が行われ、その学習結果が他者の生成AI利用において使用される可能性があるならば、そこから情報漏洩が発生する可能性があります。

3．3　外部サービスとの契約形態

生成AIやクラウド型サービスに限らず、自分が入力する情報を他者の管理下に置く形となる外部サービスを利用する場合、そのような情報の取り扱いは「第三者提供」と「業務委託」の2つにおおまかに分類されます。第三者提供では、他者に情報を提供した場合、他者は受け取った情報を自由に利用することができます（他者への情報提供の際に可否の判断が必要となります）。一方、業務委託では、あくまでも提供された情報に関する権利は委託元（提供元）にあり、委託する作業を委託元の代理として委託先が行うという関係になります（委託先が情報を自由に扱うことはできません）が、そのような関係を実現するためには、委託元と委託先の間で何らかの（業務委託）契約を交わしておくことが必要です。委託先がどのように情報を取り扱うべきかは契約において明示することになりますが、たとえ契約が存在してもその内容が不十分であれば、（一部であっても）第三者提供と同様に見做される要因が含まれてしまうことになり、情報漏洩につながる可能性が生じます。

外部委託については、委託先において情報の不適切利用や漏洩が生じぬよう、適切に委託仕様を定めるとともに、随時委託先における情報の取り扱い状況を定期的に確認し、最終的に情報の返却や消去が確実に行われるようにすることが求められます（「京都大学情報セキュリティ対策基準」第56条～第58条）。しかしながら、契約の形態としては、アカウント作成時にサービス提供者が事前に定めた約款（利用規約等）に同意する形で契約行為を行う約款型サービスも存在し、そのような契約形態においては、情報の取り扱い方法について細かく調整することは困難です。また、たとえ個別の契約書が存在する場合であっても、特にGoogleやMicrosoftのような国際的な巨大企業が提供する組織向けサービスの利用では、契約書の内容を修正してより厳しい情報の取り扱いを求めるような対応は容易でないことが多いため、約款型サービスと同様に、外部サービスにおける情報の取り扱い方針を確認した上で、入力しようとする情報の格付けと突き合わせて、意図しない情報漏洩が発生しないよう、入力するデータに配慮することが求められます（「京都大学情報セキュリティ対策基準」第59条）。

なお、上述に沿って外部サービスにおける契約上の情報の取り扱いについて注意を払ったとしても、必ずしも万全ということはありません。不慮の事故（システムトラブル、操作ミス、不正アクセス等による侵入、マルウェア感染、内部犯による情報の持ち出しなど）による意図せぬ情報漏洩が発生する可能性についても想定し、それらも見込んだリスク評価を行った上で、取り扱う情報に対して許容しうるかどうかを判断する必要があります。

つまり「契約上、情報が守られることになっている」としても、「どのような事態においても情報が守られる」ことを保証するものではないことに注意する必要があります。情報の利活用とその保護は、利便性と秘匿性の天秤であるともいえます。もしその情報が、利便性より秘匿性を重視すべき情報であったなら、外部サービス（クラウド型サービス）での利用は控えることが適切です。

4. 生成AIサービスの利用

4.1　生成AIサービスの分類

前述の生成AIにおける情報の流れや外部サービスの利用等の説明を踏まえると、生成AIサービスは、その特徴から次の表のように大まかに4つに分類することができます。

サービス種別	データの保存場所	他者向け学習利用	クラウド利用リスク	備考
個人向けクラウド型サービス	学外	あり（原則）	高	有償であっても学習利用されるケースがある
組織向けクラウド型サービス	学外	なし（原則）	中	契約で保護されるとしても、絶対に漏洩しないとは限らない（意図しない漏洩や外部攻撃）
クラウド独自環境構築型サービス	学外	なし	低	IaasSで専用環境を構築すると、アクセス者やネットワーク範囲を限定しやすい
ローカル独自環境構築（ローカルLLM）	学内	なし	なし	LLMやライブラリ自体の汚染に注意（サプライチェーンリスク）

以下では、この4つのそれぞれの特徴を順に見ていきます。

①個人向けクラウド型生成AIサービス

- 個人としての利用を想定しており、原則として約款に基づく契約の形態を採る。
- 約款の内容はサービス提供側の都合で勝手に変更されることがあるため、定期的に約款の内容を確認する必要がある。
- 無償で提供されているものが多いが、有償オプションとしてより高機能なサービスを提供するものもある。
- 基本的に、入力した情報は生成 AI の学習に用いられる（学習結果を他者も利用する）とされているが、中にはオプションにより学習に利用させないように設定を変更することが可能なものもある（オプトアウト）。
- 有償オプションを契約することで、同一クラウドサービス内のストレージ機能と連携した生成 AI 機能の利用が可能なものがある。（さらに、他社のクラウドストレージサービス等と連携させて利用することが可能な場合があるが、組織契約のクラウドストレージサービスと連携させる場合には、そのような形での情報の取り扱いが認められているかどうかの確認が必要である。）
- 同様に、有償オプションを契約することで、クラウド型サービスとして一括して提供される一連のサービス（電子メール、オンラインミーティング、オフィス系文書作成ツール等）と連携した生成 AI 機能の利用が可能な場合がある。
- あくまでも個人契約に基づく利用であり、組織（大学）としての情報の取り扱いにおいて、個人向けサービスを利用しても良いかどうかの判断は別途必要となる。

②組織向けクラウド型生成AIサービス

- 組織（大学）として契約されているサービス。組織としての情報のアクセス範囲の制限がある程度考慮されているため、①より組織外への情報漏洩のリスクは低いが、組織内での情報漏洩の可能性については別途確認が必要。
- 入力した情報は生成 AI の学習には用いないとされている場合が多いが、利用するサービスごとに確認が必要である。
- 基本的に約款による契約でないとしても、契約に記載のない事項について、サービス提供側の都合でサービス内容が変更されることがある。約款に基づく契約の形態を採るものもある。
- クラウド型サービスに含まれるストレージ機能等と連携し、組織の中で共有されるファイルを情報源に含めて生成 AI の機能を利用することが可能な場合がある。
- クラウド型サービスとして一括して提供される一連のサービス（電子メール、オンラインミーティング、オフィス系文書作成ツール等）の中のオプションの一つとして生成 AI 機能が提供される場合が多い（Microsoft 365 や Google Workspace など）。生成 AI オプション自体は無料であっても、クラウド型サービスの基本契約は原則として有償である。また、より高度な生成 AI 機能との連携機能が利用可能な有償オプションもある。

③クラウド独自環境構築型生成AIサービス

- 汎用クラウド基盤（IaaS 等）の上に専用の生成 AI 環境を構築して利用する形態。
- 生成 AI 環境の構築や運用を支援するサービスもある（業務委託）。
- 独自環境なので、情報源とするファイルの範囲やアクセス可能な利用者を限定しやすく、クラウドサービスそのものにアクセスさせる利用者が限定できるという点において、情報漏洩の可能性が②よりも低い。
- 生成 AI の大規模言語モデルの利用形態としては、次の 2 つがある：
    1. 既存の生成 AI サービスの機能（API）を利用する方法
        - 原則として入力した情報は生成 AI の学習には用いられない
    2. 公開されている生成 AI の大規模言語モデル等を利用する方法（④に近い方式）
- 入力した情報を生成 AI の学習に利用することが可能な場合もある
- 大規模言語モデルの定期的なアップデートが必要となる

④ローカル独自環境構築型生成AIシステム（ローカルLLM）

- 学内にハードウェアを含めて独自の生成 AI 環境を構築して利用する形態。
- 他者を関与させずに運用可能なので、機密性の高い情報を扱いやすい。
- 公開されている生成 AI の大規模言語モデルを利用する方法であるため、大規模言語モデルの定期的な更新が必要となる。
- 入力した情報を生成 AI の学習に利用することが可能な場合もある。

以下に、生成AIサービスを利用する際の考慮点について補足します。

4．2　外部生成AIサービスに入力する情報に対する留意点

外部生成AIサービスの利用は、以下の通り、情報の取り扱いの一般ルールにおける、学外サービス利用時の注意をそのまま当てはめることにより、情報セキュリティ上の問題を回避することができると考えられます。

- 高い機密性が求められ、学外に出してはならない情報は入力しない。
- 外部サービスの利用が認められている情報であっても、契約や約款により、それが守られることを確認する。
- 誤った生成を防ぐため、入出力双方において情報の正確性を確認する。

高い機密性が求められ、学外に出してはならない情報は、生成AIサービスであろうと、それ以外のサービスであろうと、学外へ流れるようなことがあってはなりません。そうした情報は、学外者とのメールに添付することが認められないのと同様に、生成AIサービスに利用することも認められません。とりわけ格付けにおいて機密性3情報とされる情報が、誤って生成AIサービスに投入されることのないよう、注意する必要があります。（機密性3情報において暗号化した上で学外サービスを利用することが認められている場合、生成AIサービスにも暗号化された状態で入力することになりますが、暗号化された状態では生成AIの機能を活用することはできません。また、たとえ暗号化されている状態であっても、それが漏洩すると解読のリスクが高まるため、暗号化されたままの状態であっても安易に扱うべきではありません。）

4．3　機関内他者からの参照可能性について

前述のとおり、生成AIにおいて実際に入力した情報が学習に利用されるかどうかは、それぞれの生成AIとの契約内容を確認する必要があります。本学とサービス提供者との契約に基づいて提供される生成AIサービス（後述の「Google WorkspaceにおけるGemini」や「Microsoft365におけるCopilot Chat」など）の場合、Google社、Microsoft社より、入力内容がAIの学習に利用されない設定となっているとの説明を受けています。

- Google Workspace の生成 AI に関するプライバシー ハブ
  https://support.google.com/a/answer/15706919?hl=ja
- Microsoft 365 Copilot と Microsoft 365 Copilot Chat でのエンタープライズ データ保護
  https://learn.microsoft.com/ja-jp/copilot/microsoft-365/enterprise-data-protection

しかしながら、クラウド上で提供されるサービスである以上、同一機関の利用者間で意図せず情報が共有・漏洩するリスクがゼロとは言えません。生成AIは発展途上の技術であり、その発展も日進月歩どころか、分進秒歩と言ってよいほど目覚ましいものとなっていますが、いずれにしても情報の取り扱いが不透明であることには変わりはありません。また、事前に問題がないと説明を受けていたとしても、不慮の事故や操作ミス、突然の仕様変更等で情報漏洩が発生してしまう可能性を考慮しておく必要があります。生成AIを利用する側に立てば、情報の取り扱いを始めとする各種ルールの整備にまだまだ課題があるというのが現状です。

したがって、たとえ機関契約であっても、入力してよい情報は「同一機関の他者の目に触れても差し支えない内容」に限定しておくことが望ましいでしょう。とりわけ、所属機関内でも限られた担当者のみが扱うべき要機密情報は、生成AIに入力すべきではありません。

4．4　クラウドサービス選定のための参考情報

生成AIに限らず、クラウド型サービスの選定においては、政府情報システムのためのセキュリティ評価制度（ISMAP）で提供されているクラウドサービスリスト(https://www.ismap.go.jp/csm)や、国立情報学研究所の学認クラウド導入支援サービスで提供されているチェックリスト(https://cloud.gakunin.jp/foracademy/)が参考になります。高い要件を満たすサービスほど費用も高くなる傾向があるため、不必要に高い要件を求めるのではなく、取り扱う機密情報の内容やサービスに求められる耐障害性等の品質等に見合うサービスを選定すると良いでしょう。

4．5　生成AIサービスと連携するストレージサービスの利用上の注意

生成AIサービスによっては、別のクラウドストレージに保存されているファイルを参照して生成AI機能を利用することができる場合があります。このような形で異なるクラウドサービスを連携させて利用するためには、参照される側のクラウドストレージサービスにおいて、他からのアクセスが許可されている必要があります。

前述の情報の格付けの項の説明にあるように、機密情報には情報の格付けと取り扱い制限が指定されることになっており、その指定は、一般に、機密情報（すなわちファイル）ごとに異なります。クラウドストレージにおいて機密情報を扱う場合、それぞれの機密情報に対して意図しない情報漏洩が発生しないようにするための継続的な管理が求められます。

別のクラウドストレージと連携させて生成AIサービスが利用できること（以下「連携利用」と表記。）は便利ではある一方、連携させることで生成AIから様々な機密情報にアクセスできるようにしてしまうことで、意図しない情報漏洩が発生するリスクが高くなります。そのため、大学として契約するGoogleやMicrosoft等のクラウドストレージでは、別の生成AIサービスからの連携利用は現時点では許可されていません。将来的に、ファイル単位等でのきめ細かなアクセス制御機能が充実してくれば許可される可能性がありますが、その場合でも、引き続き意図しない情報漏洩が発生しないよう生成AIの利用者自身も継続して最新の注意を払うことが求められます。

4．6　生成AIのローカル運用におけるリスク

クラウド型の生成AIサービス利用のように、サービス事業者側での学習、情報漏洩や窃取されるリスクを懸念する場合、学内のローカルPC等の専用環境で生成AIを動かし、そこに情報を入力するような運用（いわゆるローカルLLM）が考えられます。この場合、クラウド型サービス利用の観点からのリスクは軽減されますが、その他のリスクは依然として存在します。

利用する生成AI環境を完全に独自開発することは不可能ではありませんが、多くの場合、既存のソフトウェアや生成AIモデルを利用することになるため、それらの安全性についても注意を払う必要があります。信頼性の低いモデルや関連ライブラリをインターネットから入手し、組み込むことで、それらに仕込まれた悪意のあるコードや脆弱性が専用環境に持ち込まれるといったリスクがあります。このようなリスクは、サプライチェーンリスクと呼ばれます。例えば、以下のような可能性が考えられます。

- 【モデル自体の汚染】公開されている生成 AI モデルを使用する場合、その中に機密情報を窃取するコード等が仕込まれている可能性
- 【開発環境の脆弱性】モデルの運用に必要なオープンソースソフトウェア (OSS) やライブラリに、意図的なバックドアや不注意によるセキュリティホール等が存在する可能性

このように、サプライチェーンを構成するコンポーネントの安全性が欠如していれば、情報をローカルに閉じた専用環境で入力したとしても、不正なコードを通じて情報が外部に流出する危険性が残ります。

したがって、運用者側には、クラウドサービス利用時とは異なり、組織がモデルやソフトウェアの出所、およびその後の更新・修正が継続的に安全であるかを自ら担保する責任が生じることにも留意が必要です。

4．7　生成AIサービスにおけるその他のリスク

生成AIを利用する上で、情報セキュリティ（情報漏洩）以外の観点においても注意が必要です。例えば、以下のようなリスクに対する考慮も必要となります。

- 既存の著作物と同一または類似した内容が出力される可能性
- ハルシネーションによる誤った内容や根拠が不明な内容が出力される可能性
- 社会的多数派に偏った回答、画一的な回答が出力される可能性
- バイアスのある出力、差別や偏見等につながる内容が出力される可能性
- 生成 AI への入力としてデータが扱われた際に、意図しない行動（例：直前の会話履歴に含まれる機密情報を出力するなど）をとるように仕向ける攻撃を受ける可能性（プロンプトインジェクション等と呼ばれる、生成 AI が利用されることを想定したデータの作りこみ）
- 自分自身の調査、研究、創作等の成果としてみなされない可能性

ここでは、これ以上の詳細には触れませんが、生成AIを利用する場合には様々なリスクが存在することを踏まえたうえで利用する必要があります。

5．学内の各種生成AIサービス

ここでは、本学において教職員や学生が利用可能な生成AIサービスについて紹介します（2025年10月現在の情報）。
以下は、②の「組織向け生成AIサービス」に分類されるものです。

- 情報環境機構提供の Google Workspace における Gemini（教職員限定）
  https://www.iimc.kyoto-u.ac.jp/ja/services/cloud-service/google#02
- 情報環境機構提供の Google Workspace における NotebookLM（教職員限定）
  https://www.iimc.kyoto-u.ac.jp/sites/default/files/2025-03/info31_0.pdf
- 情報環境機構提供の Microsoft365 における Copilot Chat（チャットツールであり Office との連携機能なし）
  https://docs.google.com/document/d/1UIVX4xS6d1r8VVR8Tbcc53yt9PCeRW6mAjz65MGWVdU/edit?tab=t.0#heading=h.sk0m2l9k6vbg
- 情報環境機構提供の Microsoft365 の追加有償サービス「Copilot for Microsoft 365」（Office に内包して動作する有償のソフト）
  https://docs.google.com/document/d/1UIVX4xS6d1r8VVR8Tbcc53yt9PCeRW6mAjz65MGWVdU/edit?tab=t.0#heading=h.sk0m2l9k6vbg
- DX 推進室提供の「exaBase」（職員限定）
  https://sites.google.com/kyoto-u.ac.jp/dx-portal/dx-activity/gai-for-adm

以下は、③のクラウド独自環境構築型生成AIサービスに分類されるものです。

- 情報環境機構が直接提供する文字起こしサービス「kWhisper」（教職員限定）
  https://kwhisper.rd.iimc.kyoto-u.ac.jp/

これらは入力したデータが学習用に利用されないものとされていますが、前述の注意点のとおり、入力しようとする情報の取り扱いとして差し支えないかどうか適宜判断いただき、慎重に扱うべき要機密情報は入力しないようにしてください。

（ 中村 素典／中元 崇：情報環境機構 IT基盤センター 情報基盤グループ ）

サービス紹介

手軽にウェブサイトを作成！ Google サイトの活用と「カスタムURL」の設定

情報環境機構が提供する京都大学のアカウント（～@kyoto-u.ac.jp）では、教職員グループウェアに付随するツールとして、Google サイトが利用可能です。
本記事では、Google サイトと「カスタムURL」の機能について紹介します。

Google サイトとは

Google サイトは、プログラミング知識なしで手軽にウェブサイトを作成し、情報を共有できるツールです。
部署内での情報集約やプロジェクトの共有ポータル作成などに活用できます。
目的に応じて、3段階でサイトの公開範囲※1※2を設定することが可能です。
「制限付き」：共有した特定のユーザのみ閲覧できます。
「京都大学」：教職員アカウント（SPS-ID）保有者のみ閲覧できます。
「公開」　　：学外の誰でも閲覧できます。
※1 2026年4月から「学生・非常勤講師等」を対象にした公開範囲の設定も可能になる予定です。
※2 Google サイトでは公開範囲のほか、共同編集権限の範囲も設定可能です。これらの設定を誤ると、意図せず情報が外部に漏れてしまうリスクが発生します。
情報漏洩を防ぐため、内容に応じて最も厳重な設定になっているか、必ず確認したうえで設定してください。

独自性・公式性を高める「カスタムURL」

Google サイトで作成したページのURLは、標準では「https://sites.google.com/kyoto-u.ac.jp/任意の文字列」という形式になります。
Google サイトのリリース当初は利用できませんでしたが、サイトの公式性や認知度を高めたい場合は、このURLを独自のドメインに変更する（カスタムURLを設定する）ことが2025年1月より可能になりました。

- **カスタム URL の形式と条件**
  カスタム URL として設定できるのは、kyoto-u.ac.jp のサブドメイン、またはサブサブドメインに限られます。
  例：example.kyoto-u.ac.jp や example1.example2.kyoto-u.ac.jp など
- **設定のための必須条件**
  カスタム URL を利用するためには、サイトの公開範囲を「公開」に設定している必要があります。
- **申し込み方法**
  カスタム URL の設定を希望される場合は、部局のドメイン管理者の許可を得たうえで、以下のワークフローからお申し込みください。
  [Google サイト カスタム URL 設定依頼]
  https://ku1.cybozu.com/g/workflow/send.csp?cid=701

本記事で紹介した内容は「京都大学教職員グループウェアマニュアル」に記載しております。是非ご確認いただき活用ください。

[京都大学教職員グループウェアマニュアル]
https://docs.google.com/document/d/1FTCLyu2cEmNCx8n4bYUZNF5bjxlYy5pa598SuXzCCpo/edit?tab=t.vd9rge5rox81#heading=h.yqnk3uji6dto
[Chatbot]
https://notebooklm.google.com/notebook/22a347e6-a761-44bd-97ca-284bf0a03a32

（新村：情報環境機構 IT基盤センター 電子事務局グループ）

サービス紹介

学術情報メディアセンターが提供する データを活用した研究を支援するサービス

学術情報メディアセンターでは、全国共同利用サービスとしてスーパーコンピュータを利用した大規模計算サービスを提供しており、本学を含む全国の研究者の皆様に、大規模なシミュレーションや可視化のアプリケーション等、大規模計算を必要とする幅広い用途でご利用いただいています。一方、データを活用した研究においては、実験機器・センサーやWebページ等からのデータの収集と集積・管理、収集したデータの解析、データセットとしての公開等、スーパーコンピュータによる大規模計算サービスではカバーできない多様な処理が必要とされます。また、データの性質によっては隔離された環境での分析が必要になる等、従来のスーパーコンピュータが利用できないケースも想定されます。本稿では、本センターで提供するデータを活用した研究を支援するサービスをご紹介します。

データ活用社会創成プラットフォーム mdx

mdxは仮想化技術を用いて研究プロジェクト毎に分離したプライベートな計算機環境を提供するIaaS型の学術向けクラウドサービスです。mdx上で研究プロジェクト毎に異なる仮想ネットワークを構成し、サーバ仮想化技術を用いた高性能な仮想マシン（GPUを含む）を接続して隔離された高性能な計算環境を構築したり、大規模で高速なストレージを利用したりすることができます（図 1）。これらの計算資源は利用者向けのWebポータルからセルフサービスで設定することが可能です。また、国立情報学研究所が運用する学術ネットワークSINETのL2VPNサービスと連携することで、研究室のVLANや遠隔の観測機器等を同一の仮想ネットワークに接続することが可能な場合があります（本センター又は各システムの担当にご相談ください）。mdxは本センターが参画するデータ活用社会創成プラットフォーム協働事業体が運用しており、mdx Iは東京大学情報基盤センターに、mdx IIは大阪大学D3センターに設置されています。現在非常に需要が高いGPUについては、mdx IはNVIDIA Tesla A100、mdx IIはNVIDIA H200 SXMを備えています。また、ストレージについても数百TB以上の利用が可能です。詳細はhttps://mdx.jp/をご参照ください。

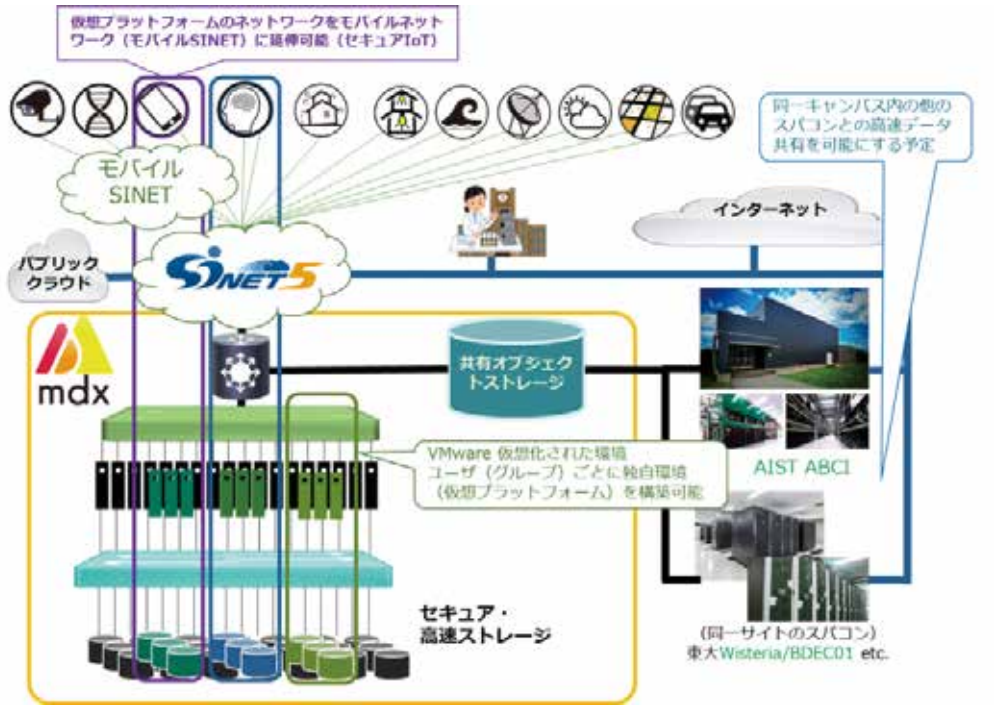


図 1 mdxの概要（2021年3月9日付広報発表資料より引用）

エッジコンピューティング基盤

研究者がデータを活用した研究において利用可能な主な計算資源として、従来から提供しているスーパーコンピュータに加え、前述のmdxや、情報環境機構が提供する研究データ用ストレージサービスであるRDM Drive及びRDMオブジェクトストレージ等があります。実際の研究においては、これらのシステムを各研究室やフィールドに存在する研究機器やセンサー、計算機等と組み合わせて利用されることが想定されます。例えば、研究機器やセンサーからデータを収集しRDM DriveやRDMオブジェクトストレージに機微なデータを保存するとともに、スーパーコンピュータで大規模解析を実行するケースを考えると、研究機器やセンサーが接続されている隔離ネットワークとRDM Drive又はRDMオブジェクトストレージをブリッジする機能や、RDM Drive又はRDMオブジェクトストレージに保存されたデータから機微なデータを削除しつつスーパーコンピュータのストレージにデータを転送する機能が求められると考えられますが、このようなシステム間の橋渡しの処理に利用しやすいサービスはありませんでした。そこで、本センターでは、「研究DXを創発する横断型データ駆動のためのデータ運用支援基盤センターの創設」事業（2023年度～2027年度、情報環境機構・学術情報メディアセンター・図書館機構）とその関連プロジェクト「mdx連携・データ駆動基盤」の一環として、2024年度末にエッジコンピューティング基盤を導入しました。本システムは、昨今利用が広がっているコンテナの実行環境を提供します。コンテナは、コンテナイメージという形でアプリケーションとその実行に必要なファイルをまとめることにより、可搬性の高いソフトウェア実行環境を実現する技術です。コンテナイメージが広く公開されているソフトウェアは多数あり、そのようなソフトウェアを利用するケースでは、仮想マシンの利用時は必要であったソフトウェアのセットアップの手間を省くことができると期待されます。また、コンテナの実行形態として、常時実行や定期実行、一回のみの実行など、多様な実行形態をサポートします。

本システムは、コンテナオーケストレーションツールとして事実上の標準であるKubernetesを採用し、利用者の皆様にKubernetesのAPIへのアクセスを提供します。そのため、橋渡しの処理に限らず一般的なコンテナの実行環境として利用することが可能です（図 2）。また、利用にあたり、Web上にある多くのノウハウが利用できると期待されます。 本システムは本学のキャンパスネットワークKUINSに200Gbpsで接続しており、本システム上で動作するコンテナは他のシステムに高速にアクセスすることができます。さらに、KUINSのVLANを引き込むことで、研究機器やセンサーが接続されている隔離ネットワークと通信することが可能な設計になっています（詳細はご相談ください）。加えて、本システムは停電の影響を受けないよう無停電電源装置及び発電機で電源をバックアップしており、メンテナンス及び障害時を除き24時間365日運用します。 本システムは原稿執筆時点（2025年12月）でサービス提供に向けた準備中であり、今後、2026年度に試行サービスを経て正式なサービスの開始を予定しています。

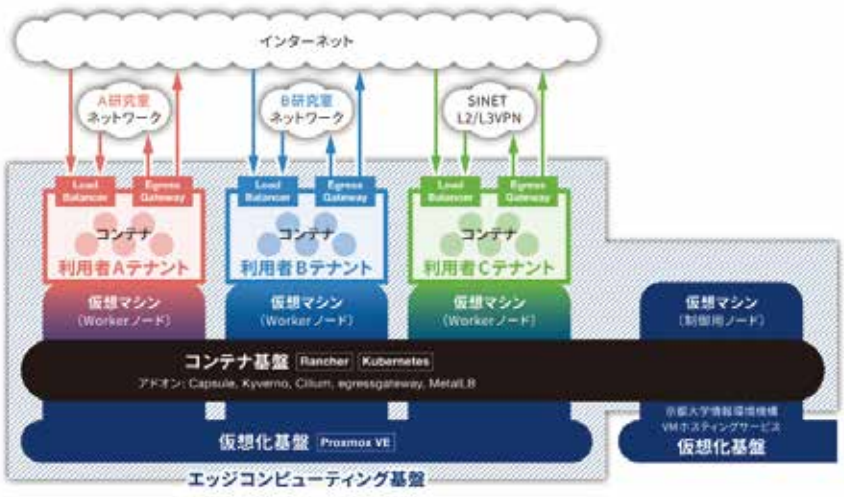


図 2 エッジコンピューティング基盤の概要

（小谷大祐：学術情報メディアセンター 准教授）

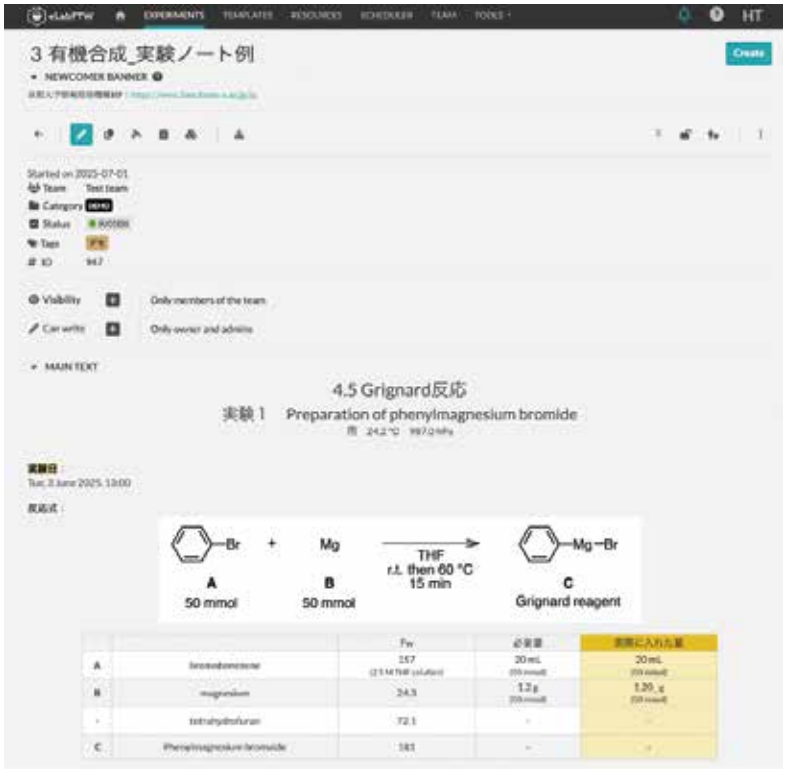
サービス紹介

電子実験ノートeLabFTWの試行サービス

情報環境機構では、2025年7月より、Campus ICT Labsにて電子ラボノート「eLabFTW」試行サービスの提供を開始しました。教職員・学生・非常勤講師等のSPS-IDおよびECS-IDを保有する方が利用可能です。

eLabFTWとは

電子ラボノート「eLabFTW」はフランスのある研究室の一角で始まり、研究者を支援するために作られたオープンソースのソフトウェアです。ブラウザでアクセスするだけでご利用できます。研究室および講義での利用が可能です。実験ノートの作成をはじめ、研究室内の備品管理、機器予約、構造式描画ソフト、DNAクローニング、APIなど様々な機能が実装されています。



eLabFTWの主な機能

Campus ICT Labsで提供しているバージョン 5.3.11 の代表的な機能は以下の通りです。

- EXPERIMENTS：実験ノートの作成など
- TEMPLATES：実験ノートやリソースのテンプレート作成
- RESOURCES：資料や試薬、実験機器、備品、部屋の管理など
- SCHEDULER：RESOURCES に登録したものの予約
- TOOLS
    - Compounds：全てのチーム・ユーザーが登録・閲覧可能な化合物データベース
    - Chemical Structure Editor：構造式描画ソフト Ketcher が利用可能
    - DNA Cloning：OpenCloning が利用可能

カテゴリーやタグにより、実験ノートの管理、検索が楽になります。また、RFC 3161準拠のタイムスタンプ署名や監査ログ、変更履歴、暗号署名なども利用可能です。作成したノートやスケジューラの利用履歴はPDF、PDF/A、JSON、ZIP、ELN、CSV形式で書き出しが可能です。
詳細については下記の文書をご参照ください。

eLabFTW機能紹介：https://u.kyoto-u.jp/elabftwinformation

利用方法

下記のGoogleフォームより利用申請をしてください。チーム作成は講義単位、研究室単位での申請をお願いいたします。

利用申請フォーム：https://forms.gle/mVHmeqhDPEnxK6k59

また、利用申請をする前にeLabFTWの機能を試したい方は、お試し用のチーム「Playground」にてお試しいただけます。下記のURLよりログインしてください。

eLabFTWログインURL：https://eln.rd.iimc.kyoto-u.ac.jp

本試行サービスは、すでに学生実験や研究活動で実際に活用いただいております。利用イメージがつかないなどありましたら、お気軽にお問い合わせください。
皆様の研究・教育活動のさらなる活性化につながれば幸いです。ぜひご活用ください。

（ データ運用支援基盤センター：情報環境機構 、システムデザイングループ：IT基盤センター ）

コラム

その警告はニセモノです！『サポート詐欺』にご注意を

ウェブサイトを閲覧中に、突然パソコンの画面いっぱいに「ウィルスに感染しています」「サポート窓口に電話してください」と表示されたり、大きな警告音が鳴り響いた経験はありませんか？これは、利用者の不安を煽ってパソコンの遠隔操作や金銭の詐取を狙う「サポート詐欺」と呼ばれる手口です。今回は、もしもの時に慌てないための知識をお伝えします。

サポート詐欺の手口とは？

サポート詐欺は、「人の心理的な隙」を狙うサイバー攻撃（ソーシャルエンジニアリング）の一種です。攻撃者は以下のような手順で罠を仕掛けてきます。

- **偽の警告**：突然「ウィルス感染」の警告画面を表示し、大音量で不安を煽ります。
- **操作不能**：画面を閉じられないように細工し、焦りを誘います。
- **偽の解決策**：実在する企業を装い、「〇〇サポートセンターへ電話してください」と偽の解決策を提示します。

「優しくサポートしてもらえるなら…」と電話をしてしまうと、巧みな話術で遠隔操作ツールをインストールさせられ、情報を盗まれたり、「サポート代金」として高額な金銭を請求されたりする被害に繋がります。

もし遭遇してしまったら

まずは落ち着いてください。ウェブサイトの閲覧中に突然表示される「ウィルスに感染しています」「サポート窓口に電話してください」といったメッセージは、ほぼ100%ニセモノです。実在する企業が、このような形で警告を出したり、電話を求めたりすることはありません。

＜基本的な対処法＞

- **画面の指示は無視する**：絶対に電話をかけてはいけません。
- **ブラウザを閉じる**：落ち着いて、閲覧中の Web ブラウザを閉じてください。
- **閉じられない場合**：無理に操作せず、部局のセキュリティ窓口や情報部 情報基盤課 情報セキュリティ掛（旧称：セキュリティ対策掛）（ https://www.iimc.kyoto-u.ac.jp/ja/services/ismo/efforts#02 ）までご連絡ください。画面の写真があると対応がスムーズになる可能性があります。

＜もし電話をかけて、遠隔操作ソフトを入れてしまったら＞

パソコンの中の情報が盗み出されている可能性がありますので、以下の3点のご対応をお願いします。

1. すぐにインターネット接続（LAN ケーブルや Wi-Fi）を切断する
2. ウィルス対策ソフトでパソコンの中をチェックする
3. 情報セキュリティ掛へ連絡する。

また、オンラインバンキング等の情報を入力してしまった場合は、各サービスの正式な問い合わせ窓口や連絡先を確認した上で、「詐欺に遭った可能性がある」とご相談ください。 犯人から金銭を要求されても、絶対に支払わないでください。「助けてもらったのに…」という罪悪感を持つ必要はありません。

被害に遭わないために

インターネット上で「過剰に不安を煽る」あるいは「親切すぎる」メッセージを提示することは攻撃者の常套手段のため注意が必要です。画面に表示された内容を鵜呑みにしない習慣をつけましょう。

また、手口を知り、体験しておくことも有効です。そのためのWebサイトを紹介しておきますので、一度ご覧になってください。

- **手口を知る その 1**：情報処理推進機構（IPA）の注意喚起ページ
  https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20241119.html
- **手口を知る その 2**：JC3 コラム ーサポート詐欺編
  https://www.jc3.or.jp/threats/topics/article-396.html
- **体験する（学内限定）**：疑似体験型セキュリティ訓練
  https://www.iimc.kyoto-u.ac.jp/ja/ku_internal/services/ismo/simulated

（ 津田 侑：情報環境機構 セキュリティアーキテクト ）

京都大学 情報環境機構 iimc
Institute for Information Management and Communication

編集・発行：京都大学情報環境機構
〒606-8501 京都市左京区吉田本町
Webサイト　https://www.iimc.kyoto-u.ac.jp

掲載記事に関するご質問やご意見・ご感想などありましたら、ぜひ下記までお寄せください。

【総合窓口】
ITサービスデスク
E-mail：support@iimc.kyoto-u.ac.jp