Info!

京都大学情報環境機構広報誌「Info!」

2025.3.4 No.31

Contents

ISSN 2188-7195

特集

全学アカウントでの多要素認証における FIDO/パスキー認証の利用について

情報環境機構では、教職員および学生をはじめとする大学構成員に対してSPS-ID/ECS-IDと呼ぶ全学アカウントを発行し、様々なサービスでご利用頂いているところですが、昨今の不正アクセスの増加・高度化に対するセキュリティ対策として、多要素認証の導入を進めています。SPS-IDについては2020年度から、ECS-IDについては2024年度から導入を開始し、これまで、メールおよびアプリを利用するワンタイムパスワード（One-Time Password; OTP）を用いた多要素認証についてご案内してきているところです。

多要素認証をECS-IDに拡大するにあたり、2024年7月に認証システム更新をおこないましたが、それに伴い、近年普及が進んでいるFIDO/パスキー認証機能もご活用頂けるようになりました。

本解説では、FIDO/パスキー認証の利用方法について簡単に紹介します。（記載内容は、2024年12月時点の動作に基づいています。）

本解説を読むにあたっての注意事項：

- ここでは、ワンタイムパスワードによる多要素認証の設定は済んでいる（ワンタイムパスワードによる多要素認証を利用中である）ことを前提としていますので、ワンタイムパスワードについての説明は行いません。

1. FIDO/ パスキーとは

FIDO (Fast IDentity Online; ファイド) とは、携帯端末を活用した生体認証技術などの標準化を目指す非営利団体であるFIDOアライアンスが策定している標準規格であり、それをさらに使いやすく拡張したものはパスキー(Passkey)と呼ばれています。AppleやGoogle、Microsoftもパスキーに対応しており、携帯端末でもパスキーへの対応が急速に進められています。WindowsやMacといったPC端末も、Windows 11やMacOS 13など最近のOSで対応しており、多要素認証の標準としての地位を築きつつあります。ここでは、FIDOとパスキーの厳密な区別には触れずに、以下ではまとめてパスキーと呼ぶこととします[1]。（操作手順や画面上ではFIDO表記になっていますが、パスキーと同じ意味だと考えてください。）

多要素認証とは、性質の異なる3つの認証要素（知識情報、所持情報、生体情報）のうちから2つ（以上）を組み合わせた認証方式のことを指しますが、パスキーは、所持情報としての携帯端末と、その携帯端末に登録されている生体情報または知識情報の組み合わせによって認証を行う方式であり、それ自体で多要素認証を実現する安全な認証方式となっています。これを全学アカウントにおける多要素認証でのワンタイムパスワードの代わりに利用することで、安全かつ手間なく認証を行うことができるようになります（ワンタイムパスワードを確認して入力するという操作が必要ありません）。全学アカウントの新しい認証システムでは、パスキーとして複数の端末を登録・管理することができるため、複数の端末を併用している場合でもそれぞれの端末における認証が便利になります。ただし、これまでと同様、端末自体のセキュリティ対策（スクリーンロック設定など）はしっかり行い、端末の紛失や盗難が発生しても簡単に他人に不正利用されないようにしておくことが重要です。

1　FIDO という用語は覚えづらいためか、最近では FIDO の意味も含めパスキーという用語で広く広報が行われているように感じられます。

2. パスキー認証に必要なもの

以下では、パスキーを利用して認証を行うことをパスキー認証と呼びますが、パスキー認証を利用するためには、次の A/B/C の 3 つが揃っている必要があります。

A) パスキー認証に対応した認証サイト

ここでは、全学アカウントの認証システムがこれにあたります。

B) パスキー認証に対応した端末（Web ブラウザ）

上記 A の認証サイトにアクセスする際に利用する端末の Web ブラウザがパスキー認証に対応している必要があります。Windows/Mac/Android/iPhone/iPad/ChromeBook など主要な端末の標準ブラウザはパスキー認証に対応しています。

C) 端末（Web ブラウザ）から利用可能なパスキー認証器

上記 B のブラウザから A の認証サイトにアクセスした際に利用可能なパスキー認証器が必要です。パスキー認証自体は A と C の間で行われますが、それを B が仲介するという関係になります。一般的には、B の端末自身が C（パスキー認証器）の機能を備えている場合が多いですが、B と連携可能な（外付けの）パスキー認証器を利用する方法もあります。後者では、共用端末からのアクセスの際にも、パスキー認証を利用して安全にログインできます（使用後は確実にログアウトする等のセキュリティ上の配慮は引き続き必要です）。

- 端末自身がパスキー認証器の機能を備えているもの[2]
  - ✓ 顔認証や指紋認証によるサインイン設定を行った Windows (Windows では、この設定機能のことを Windows Hello と呼びます) (Windows 10 以降で利用可能ですが、Windows 11 22H2 以降を推奨)
  - ✓ タッチ ID の設定を行った Mac (MacOS 13 以降)
  - ✓ 顔認証や指紋認証による画面ロック解除の設定を行った Android（Android 9 以降)
  - ✓ タッチ ID やフェイス ID による画面ロック解除の設定を行った iPhone や iPad（iOS 16 以降、iPadOS 16 以降)
- 端末以外の（外付けの）パスキー認証器（セキュリティキー）
  - ✓ FIDO/ パスキー対応 USB セキュリティキー（指紋認証つき / なし）
  - ✓ FIDO/ パスキー対応 NFC セキュリティキー（指紋認証つき / なし）
  - ✓ QR コードのスキャンによるクロスデバイス認証（後述）に対応したスマートフォン（B と C の機能を兼ね備えたパスキー認証可能なカメラ付きスマートフォンは、他の端末 (B) と組み合わせることで、その端末に対する C の機能として利用できる場合があります。詳細は 5 に後述。）

なお、指紋認証なしで利用可能なセキュリティキーは、所持していることのみの確認となる可能性があるため（実装に依存）、紛失・盗難にさらなる注意が必要です。

2　記載のバージョンより古くても WebAuthn に対応しているもの（Android 7 以降、iOS 14 以降など）であれば、認証器として登録できる可能性がありますが、パスキーとして紹介されている様々な機能が制限されます。

3. 初期設定（登録）の方法

ここでは Windows での登録の方法を示します。他の OS でも同様にして端末からのメッセージの指示に従いながら登録することができます。なお、この登録の操作を開始する前に、端末側でパスキーが利用できるように設定が完了している必要があります。Windows 端末の場合は、事前に Windows の設定の中のサインインオプションにおいて、Windows Hello の設定を行い、顔認証や指紋認証で Windows 自体にサインオンできるようにしておく必要があります。（ここでは、Windows Hello の設定方法の詳細は省略します。）

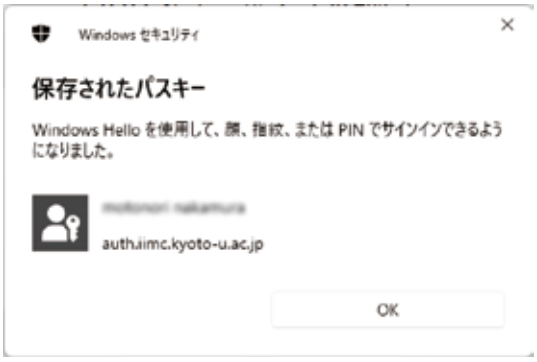
① パスキー認証を利用したい端末から、全学アカウントの多要素認証設定ページにログインします。（ログインには、すでに設定済みの多要素認証が必要です。）
多要素認証設定ページ : https://auth.iimc.kyoto-u.ac.jp/user/

② ログインできたら、画面右上の横三本線のメニュー（ハンバーガーメニュー）のアイコンをクリックします。

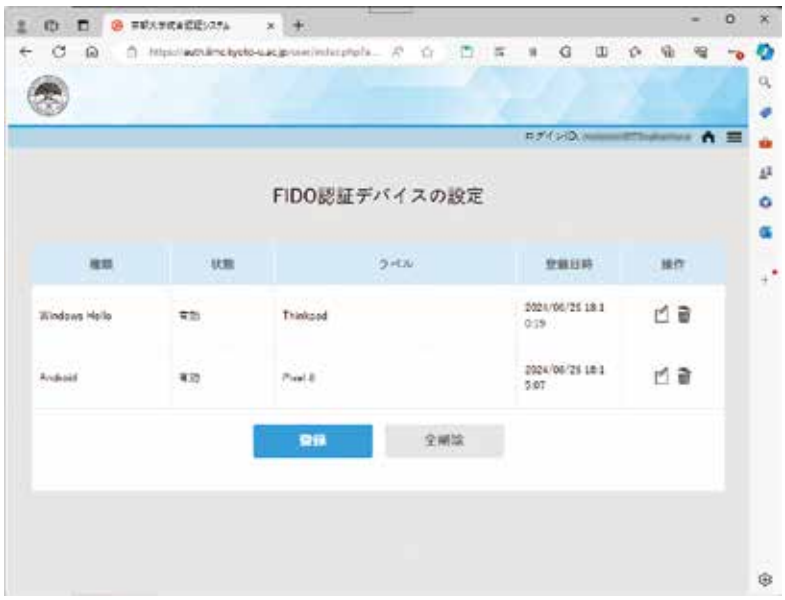
③ 現れたメニューから「FIDO 認証デバイスの登録」を選択します。

④ 「FIDO 認証デバイスの登録」を選択すると、登録されている FIDO 認証デバイスの一覧が表示されます。最初は未登録の状態なので、一覧は表示されません。

⑤　「登録」ボタンを押すと、操作をしている当該端末のパスキー機能を用いて認証が行われます。認証が成功すると、「保存されたパスキー」の画面が表示され、ここで OK を選択することで、FIDO 認証デバイスとしての登録が完了します。（最後の OK 選択まで進まないと、登録が完了しません。）



⑥　①～⑤と同様の操作を他の端末で行うことにより、複数の端末を登録することができます。同じ種類の端末を複数登録する場合（Windows 端末を複数、Android 端末を複数など）は、一覧表示で Windows Hello や Android、FIDO としか表示されないため、どの端末の登録であるかを区別できるように、ラベルに機種名などを設定しておくとよいでしょう（右端の操作のところで、メモ書きのアイコンをクリックします）。ラベルを設定しておくことで、使わなくなった端末の設定削除なども容易になります。この例では、Thinkpad や Pixel 8 のラベルを設定しています。登録したい端末がこの一覧に表示されれば、登録完了です。
（登録完了後に引き続き、登録した端末の FIDO 認証の動作確認をする場合は、ハンバーガーメニューから一旦ログアウトした上で、後述の 4 に進みます。）

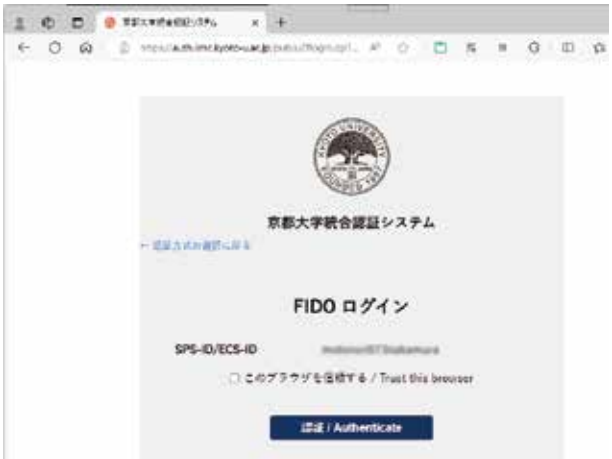


4. 認証時の操作

① 全学アカウントでログインする際に多要素認証が必要なサイトにアクセスします。(「全学アカウントの多要素認証設定ページ」も、そのようなサイトの一つです。)

② 最初に、これまでどおり、ECS-ID/SPS-ID とパスワードを用いて認証します。次の画面で、認証方式として「FIDO 認証」を選択します。(FIDO 認証デバイスが登録済みの場合は、認証方式の選択画面がスキップされて、次の「FIDO ログイン」の画面がいきなり表示されます。ワンタイムパスワードによる認証に切り替えたい場合は、「認証方式の選択に戻る」をクリックしてください。)

③ 「FIDO ログイン」の画面で「認証」のボタンをクリックすると、当該端末でサポートされている認証方式が提示されます。その中から端末側で設定済みの方式を選択して認証操作を行うことで、FIDO 認証が完了し、アクセスしようとしていたサイトにログインできます。Windows の場合、Windows Hello と呼ばれる機能が FIDO に対応していますが、顔認証、指紋認証、PIN 認証などが併用でき、それらのいずれかで認証できます。



5. 別端末（スマートフォン）を用いた認証（上級者向け）

FIDO 認証デバイスとして登録していない端末から多要素認証でログインする場合にも、ワンタイムパスワードを使用する代わりに、「全学アカウントの多要素認証設定ページ」で登録済みのスマートフォンを用いた認証を行うことができます。このような方法を、「クロスデバイス認証」と呼びます。クロスデバイス認証では、Web ブラウザが動作する端末と認証デバイスが近くに存在していることを確認するために Bluetooth (BLE: Bluetooth Low Energy) が利用されます。ここでは、Windows 端末とスマートフォンを組み合わせた例で説明します。

① FIDO 認証デバイスとして登録していない端末からログインする際に、認証方式として FIDO を選択します。また、端末の Bluetooth を ON にしておきます。

② 「FIDO ログイン」の画面で「認証」のボタンをクリックすると、当該端末でサポートされている認証方式が提示されますが、そこで「別のデバイスを使用する」を選択します。

③ FIDO 認証デバイスとして登録されているもののうち利用可能なものが一覧に表示されるので、その中から「iPhone、iPad、または Android デバイス」を選択します。

④ ログイン画面に QR コードが表示されるので、FIDO 認証デバイスとして登録済みのスマートフォンでカメラアプリ（あるいは Google Lens）を起動して QR コードをスキャンします。QR コードが認識されると、スマートフォンの画面に「Passkey を使用する」という表示が現れるので、そこをタップします[3]。このとき、スマートフォンはネットワークに接続されている状態にし、さらに Bluetooth も ON にしておきます[4]。（Bluetooth を後から ON にするとうまく動作しないことがあるようです。）

⑤ さらに、Android の場合は、このタイミングで「次回の QR コードをスキップしますか？デバイスをお互いに記憶させることができます」という表示が出るので、ここでは「後で」をタップします。（「OK」をタップすると、同じ端末・スマートフォンの組み合わせで、次回以降の QR コードのスキャン操作が省略できるようになり、上記③の「iPhone、iPad、または Android デバイス」の並びで当該スマートフォンが直接選択できるようになります[5]。次回以降の FIDO 認証において当該スマートフォンを選択すると、QR コードを読み込まなくても当該スマートフォンに認証が転送されます。）

⑥ QR コードを読み込んだスマートフォンで認証処理が始まるので、指示に従ってして、スマートフォンで認証操作を行うことで FIDO 認証が完了します。

3　Google Authenticator では、ワンタイムパスワード一覧の下にある「＋」のボタンをタップして、スマートフォンのカメラで QR コードをスキャンします。QR コードが認識されると、「パスキーを使用 続行」という確認メッセージがアプリ上に表示されるので、「続行」をタップします。

4　ログインしようとする端末とスマートフォンは、Bluetooth を ON にしておくだけでよく、ペアリングされている必要はありません。

5　この設定のリセットは、Android の Google Play 開発者サービス（「設定」→「Google」すべてのサービス→「デバイス、共有」→「パスキーがリンクされたデバイス」）で「他のデバイスへのリンクを消去する」から行うことができます。消去の操作をした後に改めて当該 Android に対してクロスデバイス認証の操作を行うことで、Windows 側の一覧から削除されるようです。

以上、新認証システムにおけるパスキー認証の使用方法を簡単に紹介しました。パスキー認証機能はまだまだ発展途上にあり、各端末における対応状況も変化が激しいと考えられますが、非常に便利な機能ですので、最新の情報を確認しつつ是非ともご活用頂けましたら幸いです。

（IT基盤センター：情報環境機構）

京都大学Microsoft 365の文字起こし機能について

京都大学 Microsoft 365 のサービスの一つとして提供されている Microsoft Teams では、運用上の理由からその機能を十分にご活用頂ける状態にはなっておらず、皆様にはご不便をおかけしているところですが、このたび、文字起こし（トランスクリプション）機能がご利用頂けるようになりましたので、その利用方法について簡単にご紹介いたします。

1. Microsoft Teams の文字起こし機能

京都大学 Microsoft 365 の Microsoft Teams では、チームを作成しての利用ができませんが、チームが作成されていなくても、次のようにして Teams 会議を開催して文字起こし機能を利用することができます。

① 会議の開催
Microsoft Teams (https://www.microsoft365.com/launch/teams) にアクセスし、Teams ホーム画面にあるメニューの「カレンダー」において「今すぐ会議」あるいは「新しい会議」で会議を作成します。この Teams 会議への招待リンクを他の参加者に伝えた上で会議を開始することで、Teams 会議を開催することができます。

② レコーディングと文字起こしの開始
Teams 会議が開始されると、会議の主催者（同じ会議に参加する京都大学 Microsoft 365 のユーザを含む）の Teams 会議画面において、メニューの「その他」の中に「レコーディングと文字起こし」を見つけることができます。その中にある「レコーディングを開始」あるいは「文字起こしの開始」を選択すると、文字起こしの処理が開始されます。文字起こしの内容は、トランスクリプションとして、画面横のエリアに表示されます。

③ ライブキャプションの表示
Teams 会議画面において、メニューの「その他」の中にある「言語と音声」で、ライブキャプションをオンにすると、画面の上または下のエリアにライブキャプションとしての文字起こしが表示されます。前述のトランスクリプションは、会議主催者にのみ表示される機能ですが、ライブキャプションは参加者も自身の画面に表示させることができます。

④ 言語の変更
トランスクリプションやライブキャンプションのエリアにある設定（歯車アイコン）を開くと、表示する言語（認識させたい言語）を変更することができます。話されている言語と一致していないと正しく文字起こしが行われないことに注意が必要です。

⑤ 終了した会議のトランスクリプション
終了した Teams 会議のレコーディングやトランスクリプションは、主催者の Teams ホーム画面にあるメニューの「チャット」から参照することができます。レコーディングされたビデオをクリックして開くと、文字起こしされたトランスクリプションとともに表示されます。また、ビデオを再生し、ビデオ画面内のメニューにある CC アイコンでキャプションを有効にすると、ビデオ画面上にキャプションが表示されます。Teams 会議のビデオは、後述の Microsoft Stream からもアクセスすることが可能です。

詳しくは Microsoft のサイトをご確認ください。
https://support.microsoft.com/ja-jp/Search/results?query=teams+文字起こし

2. Microsoft Stream の文字起こし機能

Microsoft Teams で開催された会議でなくても、Zoom 等の他のツールで作成されたビデオファイルなどを Microsoft Stream (https://www.microsoft365.com/launch/stream) にアップロードして、トランスクリプトを生成させることができます（生成には、ビデオのレコーディングと同程度～ 2 倍程度の時間が必要なようです）。また、動画の再生時にキャプションを表示させることもできます。

詳しくは Microsoft のサイトをご確認ください。
https://support.microsoft.com/ja-jp/Search/results?query=stream+文字起こし

3. その他の文字起こしの方法

上記で紹介した Microsoft Teams や Stream を利用する方法以外にも、Word や OneNote のディクテーション機能やトランスクリプション機能も利用することができます。状況に応じて使いやすい方法を選択してください。Word、OneNote はいずれにも、PC にインストールして利用するアプリ版とブラウザで利用可能な Web 版があります。Web 版はそれぞれ次の URL からアクセスできます。

Word: https://www.office.com/launch/Word

OneNote: https://www.office.com/launch/OneNote

4. Copilot との関係について

文字起こしの機能を利用するために Copilot のライセンスは不要です。また文字起こしの結果が Copilot の学習などに使用されることはないことを Microsoft に確認しています。逆に、Copilot のライセンスがあれば、文字起こしされたトランスクリプションに基づいて動画の要約を簡単な操作で作成させることができます。

（中村素典：情報環境機構　IT 基盤センター　教授）

事務改革がさらに進化！
DXワーキンググループ第2期がスタート

2024年10月1日、京都大学の事務業務のDXを加速させるため、DXワーキンググループ（以下、DXWG）の第2期が始動しました！メンバーは公募や事務本部等からの推薦で集まったやる気満々の事務職員たち。任期は2年間で、それぞれの経験や得意分野を活かしながら、新しいアイデアをどんどん形にしていきます。

～事務改革のこれまでの取組～

京都大学の事務改革の取組みとして、事務改革推進本部会議（事務職員による会議体）のもとに2022年11月に立ち上がった「DXWG」と「業務デザインワーキンググループ（以下、業務デザインWG）」が、2024年3月に第1期の活動を終えました。この2つのWGは、事務の効率化とデジタル化を目指して、それぞれの得意分野を活かしながら取り組んできました。

DXWGでは、「押印の一部廃止」や「電子決裁の導入」で、これまで面倒だった手続きをスムーズに。また、一部の経理業務に「RPA（ロボティック・プロセス・オートメーション）」を導入し、繰り返し作業を自動化。事務作業の手間を大きく減らすことに成功しました。一方、業務デザインWGでは、事務全体の課題を整理し、教職協働を実現するための事務側の改革の礎となる「5つの業務デザインポリシー」を策定し、事務改革推進本部会議において提言を行いました。このポリシーは、第2期DXWGの活動方針としても活用されています。

【5つの業務デザインポリシー】

～第２期活動開始～

第1期では、業務を効率化するための提言や試行が行われましたが、第2期ではその成果をさらに深め、学内で「使える」施策を実現するフェーズに突入します。例えば、手間のかかる作業を簡単にするデジタルツールや、部局同士のスムーズな情報共有をサポートする仕組みづくりなど、教員や学生のみなさんも「便利！」と思える変化を目指します。DXWGの取り組みが事務職員だけでなく、教員や学生のみなさんにとってもより良い環境づくりにつながるよう取り組んでいきますので今後の活動に、ぜひご注目ください！

【業務デザインWGの様子】

【DXWG（II期）の様子】

（DXWG（II期）情報発信チーム）

サービス紹介

KURENAI: 研究データ（論文の根拠データ）をDOI付きで公開できます

論文投稿の際、論文の根拠データ（研究データ）の登録・公開場所に困ったことはありませんか？
→「KURENAI」では論文の根拠データ（研究データ）も登録・公開することができます。

1. KURENAI とは？

京都大学学術情報リポジトリ「KURENAI」[*1] では、オープンアクセスを推進するプラットフォームとして、京都大学で日々創造される研究・教育成果（学術雑誌掲載論文、学位論文、紀要論文など）をインターネット上で公開しています。「KURENAI」はすでに 20 万件以上の論文等を公開し、年間 600 万回を超える論文ダウンロード数を誇る、世界中でも第 7 位、国内 1 位の論文プラットフォームです [*2]。

2. KURENAIに研究データ（論文の根拠データ）を公開するメリットは？

研究データ（論文の根拠データ）にDOI[*3]を付与することができます。DOIを付与することで引用されやすくなり、研究成果の可視性向上が期待できます。

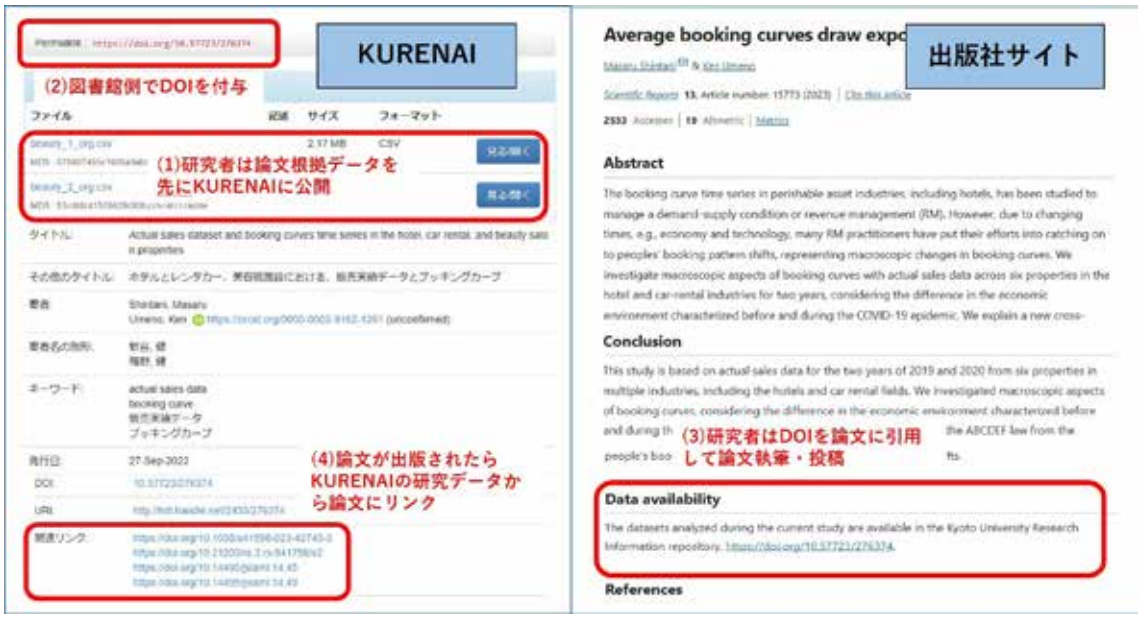
近年、学術ジャーナルの投稿規定や執筆要領で、論文の根拠データの公開が求められることが多くなってきています。その際、KURENAIを論文根拠データの登録・公開場所として利用していただくことが可能です。

図書館、KURA、情報環境機構データ運用基盤センターが協力し実施した研究データ管理・公開状況についてのインタビューの中で、学内研究者からも「研究データにDOIを付与でき、データ自体は大学（KURENAI）で保持できることはとても良いですね」との声もいただいています。

3. データファーストな OA 研究サイクルを実践してみましょう

論文の根拠データを先にKURENAIに登録・公開しておくことで、そのDOIを執筆論文に引用して論文投稿する、データファーストなオープンアクセス(OA)研究サイクルが可能になります。実際に実践されている情報学研究科・梅野健教授の実践例でその手順をご紹介します。

(1)研究者は論文根拠データを先にKURENAIに登録・公開申請
(2)図書館側でDOIを付与
　KURENAIの論文根拠データ：https://doi.org/10.57723/276374
(3)研究者はDOIを論文に引用して論文執筆・投稿
　出版社サイトの論文：https://doi.org/10.1038/s41598-023-42745-3
(4)論文が出版されたらKURENAIの論文根拠データから論文にリンク
(5) 研究者は論文原稿ファイルもKURENAIに登録し公開
　KURENAIの論文原稿：http://hdl.handle.net/2433/285297



より詳しくは案内ページ[*4]をご覧いただき、KURENAIで研究データの公開を希望する場合は、図書館に申請をお願いします。

4. 国の OA 基本方針にも対応できます

2024(令和6)年2月、内閣府統合イノベーション戦略推進会議において「学術論文等の即時オープンアクセスの実現に向けた基本方針(以下、国のOA基本方針)」が決定されました。国のOA基本方針のポイントおよび京都大学における支援内容については解説ページ[*5] を設けましたので、こちらをご覧ください。

国のOA基本方針では論文の根拠データもリポジトリ公開対象となっていますので、その点でも一足早くKURENAIでの研究データ公開、データファーストなOA研究サイクル手順をお試しいただければと思います。

なお、現在、より簡便にKURENAIへの登録・公開申請ができるように、KURENAI公開支援システム[*6] を改修中です。改修が終わりましたら、査読のために査読者とのみ論文根拠データを共有できる機能も提供開始する予定です。

*1 京都大学学術情報リポジトリ「KURENAI」
https://repository.kulib.kyoto-u.ac.jp/

*2 TRANSPARENT RANKING: Institutional Repositories by Google Scholar
https://repositories.webometrics.info/en/institutional

*3 DOI (Digital Object Identifier) : 学術コンテンツの電子データに付与される国際的な識別子です (https://doi.org/***/****) 。①グローバルに一意な識別子としての役割をはたし、かつ②恒久的なアクセスを保証する (リンク切れを防ぐ) ことができます。

*4 研究データ (論文の根拠データ) をDOI付きでKURENAIに公開する
https://www.kulib.kyoto-u.ac.jp/researchdata/1395273

*5 科研費等に対する国のオープンアクセス基本方針に対応するには
https://www.kulib.kyoto-u.ac.jp/content0/1402213

*6 KURENAI公開支援システム
https://www.kulib.kyoto-u.ac.jp/content0/1370229

(附属図書館研究支援課)

お知らせ

京都大学におけるMicrosoft 365サービスの個別ライセンス追加購入について

京都大学では、EES 包括契約に基づく Microsoft 365 サービスを、大学が発行する SPS-ID および ECS-ID を保有するユーザに対して提供しています。このサービスには、インストール版 Microsoft Office である Microsoft 365 Apps などが含まれますが、Microsoft 365 Apps 等をご利用頂けるのは、A3 ライセンスが付与されているユーザに限定されます。

そのため、A3 ライセンスの契約範囲に含まれない一部のユーザ（非常勤講師、名誉教授、客員研究員、医療系職種の教職員の一部などの A1 ライセンスのみが付与されるユーザ）については Microsoft 365 Apps 等をご利用頂くことができず、これまでは別途 Microsoft Office のパッケージ製品をご購入頂くなどのご対応を頂く必要がありました。

また、Microsoft Copilot 等の有償の拡張機能を京都大学の Microsoft 365 サービスと組み合わせて利用したいという要望に対しても、これまでお応えすることができませんでした。

このたび、日本マイクロソフト社および京都大学生活協同組合と京都大学とで検討を行い、以下については個別ライセンスを追加購入頂く形での対応が可能になりましたのでご案内いたします。

1. 京大 M365 A3 個別追加ライセンス

インストール版 Microsoft Office である Microsoft 365 Apps が利用可能な A3 ライセンスを生協経由で購入いただけます（購入後、生協からのオーダーが Microsoft に届くと、京大 Microsoft 365 サービスで利用可能な A3 ライセンス数が追加されます。その後、大学側で SPS-ID/ECS-ID に対して割り当てを行うことで、購入したユーザが利用可能となります）。購入単位は最長 1 年（購入月～直近 6 月末までの期間）となり、価格は 6 月末までの月額の合計となります。継続して利用する場合は 7 月までに次の 1 年分を購入頂く必要があります。詳細については、京大生協にお問い合わせください。

2. 京大 M365 Copilot 個別追加ライセンス

京都大学の Microsoft 365 アカウントに Microsoft Copilot のライセンスを追加することで、インストール版 Microsoft Office である Microsoft 365 Apps や Web 版 Office で AI アシスタント機能が利用できるようになります。また、Copilot in OneDrive を利用することで、OneDrive に保存したファイルを AI アシスタントに参照させることができます。京大 M365 Copilot 個別追加ライセンスの購入要領は、京大 M365 A3 個別追加ライセンスと同じです。詳細については、京大生協にお問い合わせください。なお Copilot には、Microsoft 365 Copilot Chat（旧称 Bing Chat あるいは Microsoft Copilot）と呼ばれるサービスもありますが、これは質問応答や情報検索、アイデア出し、文章作成サポート等を支援する生成 AI 技術を用いたサービスで、無料でご利用いただくことができます（「Info!」No.30 で紹介しています）。ここで紹介している Office と連携して利用可能なものは、Copilot for Microsoft 365 と呼ばれるものです。両者の違いにご注意ください。

参考：アカウントに割り当てられているライセンスの確認方法

次の URL で「マイアカウント」にアクセスして、左のメニューから「サブスクリプション」を選択すると、自身のアカウントに割り当てられているライセンスを確認することができます。

https://portal.office.com/account/

ここで、Microsoft 365 A3 for faculty や Microsoft 365 A3 for Students Use Benefit が表示されず、Microsoft 365 A1 for Faculty や Microsoft 365 A1 for Student が表示される場合は A3 ライセンスが付与されていません。

上記の個別追加ライセンスを購入することで、Microsoft 365 A3 や Microsoft 365 Copilot のライセンスが追加されます。

（情報基盤グループ：情報環境機構）

お知らせ

Garoon Myポータルを使いこなそう

教職員グループウェアのポータル画面を自由にカスタマイズできる、Myポータル機能について紹介します。

〇便利な使い方

特定の機能に特化したMyポータルを複数準備し、切り替えて使用します。表示するのに複数クリックする必要のあるポートレットを登録しておくとワンクリックで表示されて便利です。

（一例）

1. グループスケジュール：MY グループでグループメンバーのスケジュールを複数作成し、グループスケジュールのポートレットを登録

2. 個人スケジュール　：個人スケジュール（週、月）のポートレットを登録

3. 通知：通知関係（メッセージ・ワークフロー等）のポートレットを登録

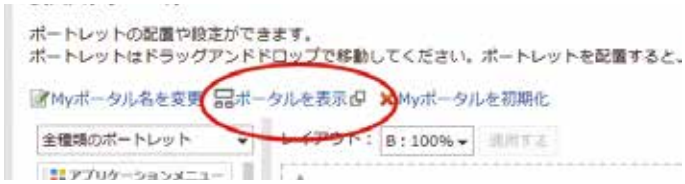
4. 1から3を必要に応じて切り替えて使用

〇Myポータルの作成

1. My ポータルの追加は教職員グループウェア右上の My ポータルの追加から行います。

2. My ポータルに名称をつけ、A、B、C、D の好みの位置にポートレット（機能）を配置できます。A、B、C、D の表示割合は「レイアウト」で変更できます。
なお、削除禁止と表示されているポートレットは、システムや緊急の通知で使用しますので削除を行わないでください。編集中に誤って削除した場合は、再度、追加してください。

3. 上部の「ポータルを表示」をクリックすると設定した My ポータルが表示されます。



〇マニュアルについて

設定方法や使用方法の詳細については、以下のマニュアルをご参照願います。

・京都大学教職員グループウェア マニュアル（個人設定ー10.MYポータル）

・掲載場所　マニュアル→教職員グループウェア の以下の場所

（電子事務局グループ：情報環境機構）

お知らせ

2次グループメールに関する仕様と注意点

教職員グループウェアでは、2次グループというグループ管理機能を備えており、Garoonのファイル管理やGoogleドライブ等の権限管理でご利用いただけます。また、Googleグループを利用したグループメールとしての役割もございます。

今回は、特にグループメール機能に関する情報をお届けします。

1. 新しい 2 次グループ検索アプリのリリース

この度、2次グループの利用を支援する新しい検索アプリをリリースしました。以下に主な機能と利点を紹介します。

- **検索機能の強化**
  高速かつ正確に2次グループアドレスやメンバーの検索が可能になりましたので、管理作業の効率が向上しました。
- **スムーズな変更申請**
  詳細画面の「2次グループ申請（編集）へ」ボタンを押すと、申請フォームに直接移動できるようになりました。また、フォームには現在の設定内容があらかじめ入力された状態になっており、変更したい項目だけを修正するだけで済むため、申請がスムーズに行えるようになりました。
- **学生用メール、学外メールアドレスの非公開化**
  学生用メールや学外のメールアドレスはローカルパート（「@」より左側）を伏せ字にして表示するようになりました。必要に応じて「Googleグループ・メンバー確認」ボタンで伏せ字部分を確認可能です。

アクセス方法

教職員グループウェア（Garoon） にて、画面上部の職員検索アイコンをクリックし、「2次グループ検索」をクリックしてください。

2. 外部からのメールの受信設定について

新しく作成した2次グループの初期設定では、学外からのメールを**受信できない**（エラーメールを返す）仕様になっています。学外からのメールを受信する場合や、推奨設定への変更についてはGoogleグループの初期設定を行う必要があります。詳しい手順は以下のマニュアルをご参照ください。

教職員グループウェアマニュアル「Googleグループ初期設定」
※設定変更は2次グループの「Googleグループオーナー」のみ実施可能です。

3. 異動時のメンバー更新のお願い

2次グループは、教職員グループウェアの様々なアプリで権限管理に利用されています。異動や所属変更があった場合は、速やかにメンバー更新をお願いします。なお、メンバーの更新申請は、Garoon の2次グループ申請（編集）フォーム経由で行う必要があります。
詳しい手順は以下のマニュアルをご参照ください。

教職員グループウェアマニュアル「2次グループ・Googleグループ」
※更新申請は2次グループの「編集権限者」のみ実施可能です。

4. 差出人アドレス（From）の書き換えについて

2 次グループへ届いたメールにおいて、送信者のメールシステムが「なりすまし防止技術（DMARC）」を利用している場合、差出人アドレス（From）が 2 次グループのアドレスに変更される場合があります。
これは、メールの配送を問題なく行うための Google グループの特性となります。
ただし、返信先（Reply-To）として元の差出人のアドレスが設定されているため、メールソフトの「返信」ボタンを押すことで正しい送信先に返信できます。

例：

差出人（From）：gaibu@example.com
宛先：group@mail2.adm.kyoto-u.ac.jp

のメールが届いた場合に、以下のように差出人が変更される場合があります。

差出人（From）：group@mail2.adm.kyoto-u.ac.jp
宛先：group@mail2.adm.kyoto-u.ac.jp

※メールソフトの返信ボタンを押すと元の差出人「gaibu@example.com」が宛先に設定されます。

メールソフトでは以下のように表示されます。

- **Gmail Web ブラウザ版の場合：**
  送信者：元の差出人 via 2 次グループ名 <2 次グループのメールアドレス >
  宛先：2 次グループのメールアドレス
- **Thunderbird の場合：**
  差出人：元の差出人 via 2 次グループ名 <2 次グループのメールアドレス >
  返信先：元の差出人 < 元の差出人メールアドレス >
  宛先：2 次グループのメールアドレス

注意事項：
迷惑メールでも同様の差出人変更が発生する場合があります。Fromが変更されていることで不正なメールだと気がつかない場合もありますので、受信したメールは内容の精査を十分行い、不審な場合は添付ファイルの開封や返信を避けてください。

（電子事務局グループ：情報環境機構）

お知らせ

NotebookLMで業務効率をアップ！

情報環境機構では、Googleが提供する NotebookLM を利用したチャットボットの試行を開始しました。このチャットボットはグループウェアのマニュアルを学習しており、グループウェアに関する質問に答えたり、必要な情報を素早く検索したりすることで、業務の効率化をサポートします。

NotebookLMの主な特徴

NotebookLM は、以下の機能を提供します。

- **自動要約とキーポイント抽出**
  アップロードした資料を AI が解析し、重要なポイントを瞬時に要約します。膨大な文書でも短時間で内容を把握することが可能です。
- **多様な形式の資料を扱える**
  Google ドキュメント、PDF、YouTube 動画など、さまざまな形式の資料をもとに情報検索が可能です。
- **質問応答機能**
  資料をもとに、具体的な質問に答えます。例えば、「Garoon スケジュールで他のメンバーの状況を一覧で確認できる？」「教職員にアンケートを取る方法を教えて」といった質問に対し、該当箇所を引用して回答します。

ご利用にあたって

グループウェアのチャットボットは https://u.kyoto-u.jp/gwbot にアクセスしていただくか、教職員グループウェア（Garoon）にログインし、「マニュアル ＞ 教職員グループウェア チャットボット」と辿っていただくとご利用いただけます。
また、NotebookLMは教職員グループウェアのサービスとして提供していますので、教職員であればご利用いただけます。利用データはAIの学習に利用されない仕様ですので安心です。
また、2025年1月時点ではオーナー変更や複製は不可のため、作成者が退職した場合は別のユーザが新たに作成する必要があります。そのため、情報環境機構の短縮URLサービス「KNIVES」を併用して共有することをおすすめします。

全学共有や利用のご相談

作成したNotebookLMは教職員アカウントや2次グループに限り共有が可能です。もし全教職員に共有したい場合は情報環境機構までご相談ください。
NotebookLMに関するご感想・ご意見をGoogleフォーム （ https://forms.gle/yusFPgmodqu2TUuFA ）にお寄せください。また、もっと「こんなことにも使えそう！」というアイデアも募集しております。

（電子事務局グループ：情報環境機構）

お知らせ

JMPの教育コン端末での提供終了と今後の利用について

教育用コンピュータシステム（以下「教育コン」という）の固定型端末サービスでは大学向けの有償ライセンス（共有端末で利用可能）を用いて、統計解析ソフトウェア JMP Proを提供してまいりました。しかしながら、JMP Statistical Discovery LLC 社製より、この有料ライセンスの提供が2024年12月末日をもって終了となると連絡があったことから、固定型端末サービスにおいてもJMP Proの提供を2024年12月末で終了しました。すでに授業にて固定型端末を利用されている科目担当者および主要部局には連絡済みですが、ご注意頂けますようよろしくお願い致します。

2025年1月以降は、日本国内の教育機関に所属の学生、研究者、および教職員であれば、個人申込による無償ライセンス（JMP Student Edition）が提供されています。なお、この無償ライセンスは共有端末では利用できないため、各個人の所有端末（BYOD）へインストールして利用してください。詳しい内容については、次のJMP Statistical Discovery LLC 社製のホームページをご覧ください。

https://www.jmp.com/ja_jp/software/student-edition-info.html

無償ライセンスの申し込にみ関する注意点を以下のページにまとめています。

https://u.kyoto-u.jp/jmp-student-edition

（植木徹：情報環境機構　教育支援グループ　教育情報主査）

お知らせ

情報環境機構新ロゴの紹介

情報環境機構（以降、「当機構」とする）では、当機構のロゴを刷新するとともに、2024 年 1 月に設置された 2 つのセンター（IT 基盤センター、データ運用支援基盤センター）のロゴを当機構のものと連続性、関係性を持たせる形で策定しました。

新しいロゴのコンセプトは、「広がり、変化し、リンクする」です。

情報環境機構は主に学内に対して IT サービスを提供する組織です。教育や研究において使いやすい、使う価値のある IT サービスを提供するためには、学内の多くの利用者と繋がり、その関係性を広げ、また多様なニーズに対して絶えず変化していくことが重要です。変化のひとつとして、2024 年 1 月にデータ運用支援基盤センターを設置し、研究データの管理・利活用のための支援を行なっていくことになりました。こうした情報環境機構の新しい動きを踏まえつつ、また将来にわたって求められるミッションを果たすための旗印として、ロゴを刷新しました。

新しいロゴは「リンク」を想起させる形状をモチーフとし、利用者との繋がりを作っていく様子を表しています。また Input/Output 両方の方向性、つまり利用者の声やニーズに耳を傾けながら、こちらからも利用者目線で働きかけていく姿勢を表現しています。さらにリンクの形状はその配置次第で色々な形状に変化する可能性を秘めており、情報環境機構が今後も変化していく意志を込めました。同じ意図で IT 基盤センター（CITI）、データ運用支援基盤センター（CODA）のロゴも作成しています。

これらの新しいロゴとともに情報環境機構は利用者の方にとって価値のある IT サービスを提供してまいります。

（小野英理：情報環境機構データ運用支援基盤センター 准教授）

お知らせ

全学アカウント(ECS-ID/SPS-ID)の多要素化について

2020年10月15日（木）のSPS-ID（教職員のアカウント）に引き続き、2024年11月5日（火）からECS-ID（学生・非常勤講師等のアカウント）についても多要素認証が必須となりました。

アカウントを利用する場合は、**「アカウントの有効化」**および**「多要素認証の設定」**を行ってください。

※「アカウントの有効化」とは

アカウント（ECS-ID、SPS-ID）は発行直後、利用できない状態（無効化）となっています。

合わせて通知された「有効化キー」で、有効化（自身でパスワード設定）して利用可能となります。

「有効化キー」は、「アカウントの有効化」に使用するもので、有効化（自身でパスワード設定）後は利用出来なくなります。

詳しくは下記、情報環境機構サイトの案内をご覧ください。

●学生向けビギナーズガイド
https://www.iimc.kyoto-u.ac.jp/ja/guide/students/beginner-guide.html

●非常勤講師・その他の方向けビギナーズガイド
https://www.iimc.kyoto-u.ac.jp/ja/guide/others/beginner-guide.html

●教職員向けビギナーズガイド
https://www.iimc.kyoto-u.ac.jp/ja/guide/faculty-staff/beginner-guide.html

●多要素認証
https://www.iimc.kyoto-u.ac.jp/ja/services/account/mfa/

・～はじめて多要素認証の設定をする～
https://sites.google.com/kyoto-u.ac.jp/mfa-start-jp/home

・多要素認証導入の必要性
https://sites.google.com/kyoto-u.ac.jp/mfa-start-jp/about_mfa?authuser=0#h.wy8k9bycsyat

・京都大学で導入する多要素認証
https://sites.google.com/kyoto-u.ac.jp/mfa-start-jp/about_mfa?authuser=0#h.rzhuozb3rmi3

（情報環境支援センター：情報環境機構）

お知らせ

2025年3月に京都大学から離籍（卒業・修了など、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、下記のようなサービスが利用できなくなります。（アカウントに紐づく提供サービス[*2]）

- ・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ストレージなど

離籍・身分変更などが予定されている場合は、比較的時間の余裕がある間に各サービスの案内を確認、データのバックアップ・移行・引継ぎなどを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・不在通知などについても離籍・身分変更などの前に確認ください。

各詳細につきましては、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的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

（情報環境支援センター：情報環境機構）

報告

2024年度無線LANシステム更新

2024 年 9 月から 2025 年 3 月にかけて全学の無線 LAN システム（吉田・宇治・桂キャンパスに設置されたアクセスポイント 2600 台と遠隔地等に設置されたアクセスポイント 300 台および管理サーバ）の更新を実施致しました。以下に新システムより導入した新機能や新サービスなどを紹介致します。

1. Wi-Fi 6E（6GHz 帯）対応
   既存のアクセスポイントは吉田・宇治・桂キャンパスでは Wi-Fi 5、遠隔地等では Wi-Fi 4 まで対応した機器でしたが、新しいアクセスポイントはすべて Wi-Fi 6E 対応となり、これまでと比較してより効率的な通信環境が提供できるようになるとともに、新たに追加された 6GHz 帯の周波数も利用できるようになります。そのため新規で購入される端末機器は新たな 6GHz 帯を有効活用できる Wi-Fi 6E 対応機器をお勧めいたします。
2. 提供する無線 LAN サービス
   従来どおり学内構成員向けの「KUINS-Air」と学内学外の研究教育機関構成員向けの「eduroam」は現在のサービスをそのまま継続して提供いたします（設定の変更は必要ありません）。それらに加えて新たに一般利用者向けに「OpenRoaming」を提供を検討しております。
3. 端末からの利用環境確認方法の提供
   「KUINS-Air」に接続して下記 URL にアクセスすると、その時点での接続先となっているアクセスポイント名やご利用の周波数帯、同時に接続中の端末台数などをご確認いただけます。通信が不安定であったり途切れるといったお問い合わせの際には表示された情報をあわせてご提供いただくと調査が円滑にすすみます。
   https://observes.kuins.kyoto-u.ac.jp/wc2/
4. 新規アクセスポイント導入方法の変更
   部局さまでアクセスポイントを追加設置される場合は下記 URL をご確認ください。なお、現在は余剰予備機の無償提供は実施しておりません。新規購入する代わりに利用率の低い既存機器を移設する方法もございます。実際の利用状況等に基づくご提案も可能ですので必要であればお気軽にご相談ください。
   https://www.iimc.kyoto-u.ac.jp/ja/services/network/admin/ap.html

システム更新期間中はご不便をおかけして申し訳ございませんでした。また各部局の担当者さまには日程調整のご尽力をいただきありがとうございました。

（情報基盤グループ：情報環境機構）

コラム

マルウェアの流行り・廃りとサイバー攻撃対策

言葉やファッション、音楽など、時代に合わせた流行があります。過去に流行って廃れたものも、何年か経ってから再度流行ったりします。コンピュータに大きな被害をもたらす悪いプログラム（マルウェア）についても同様に流行りと廃りがあり、その時に合った対策が必要になります。今回のコラムでは、マルウェアの流行り廃りを中心に、サイバー攻撃への対策について考えていきます。

マルウェアの流行り廃り

サイバー攻撃を実行する人（攻撃者）は、新しいマルウェアを日々生み出しています。攻撃者が完全に新種のマルウェアを開発することもありますが、既に出回ったマルウェアを一部改変することで活動パターンが似たマルウェアを作り出すこともあります。後者はマルウェアの「亜種」と呼ばれます。たとえば、2016年にIoT機器をターゲットに感染拡大したMiraiというマルウェアがありますが、現在ではMioriやInfectedSlursと呼ばれるMiraiの亜種の活動が活発です。
他方で、少し前に感染爆発したマルウェアが今は活動が鈍化したり、過去に流行ったマルウェアが再度流行することもあります。こういったことから単純に「マルウェア対策」と言っても、流行り廃りを捉えた対策になっていないと、対策として全く意味のないものとなってしまいます。

流行り廃りの実例: Emotet

Emotetというマルウェアは2014年頃から活動がはじまり、2019年頃に感染拡大したことで、その被害について数多くの報道がされました。2021年1月、欧州司法機構と欧州刑事警察機構により組織された8ヶ国の共同作戦でEmotetの攻撃インフラをテイクダウンすることで一時的にEmotetの感染拡大を封じ込めましたが、2021年11月に活動を再開しました（参考:Info! No.25コラム）。さらに、2023年3月頃からEmotetによる活動が活発になりましたが、2025年1月現在ではほぼその活動は観測されなくなっています。そのため、今のところはEmotetの対策に注力しても空振りになる可能性が高く、その間に別のマルウェアによる攻撃にさらされるかもしれません。

流行り廃りを追いかけるセキュリティ

マルウェアの対策として身近なものとしてウィルス対策ソフトがあります。ウィルス対策ソフトがマルウェアに気づくきっかけのひとつに、マルウェアの通信機能による活動があります。たとえば、Emotetのように指令サーバ（C2サーバ：Command and Controlサーバ）を介して遠隔操作を実行する通信や、感染したコンピュータから次の感染先を探索する通信、別のマルウェアを追加でダウンロードする通信などがあります。
本学では、学内ネットワークとインターネットとの境にファイアウォールを設置し、このような通信を遮断する仕組みを運用しています（参考: Info !No.28コラム）。マルウェア通信を遮断するための情報はインターネット上で共有され、その内容は日々更新され、今まさに流行っているマルウェアをある程度は追いかけられるようになっています。
大学生活を送るみなさまは、まさに流行の最先端で活躍されていることかと思います。みなさまに安心・安全で楽しい大学生活を送っていただくために、情報環境機構ではサイバー攻撃の流行り廃りを把握しつつリスクを認識し、その時に置かれる状況に応じたセキュリティ体制の実現を目指していきます。

(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】
情報環境支援センター
E-mail：support@iimc.kyoto-u.ac.jp