Info!

京都大学情報環境機構広報誌「Info!」
2026.8.3 No.34

Contents

ISSN 2188-7195

サービス紹介

Google Workspaceで変わる大学生活！ 学生・教員のための実践活用ガイド

1. はじめに：新しい共通プラットフォームの活用に向けて

2026年4月より、学生用Google Workspaceが新たに導入され、学生と教職員が同じプラットフォーム上でシームレスにつながる環境が整いました。本記事では、学生・教員それぞれの視点から具体的な活用シナリオを提案するとともに、特に注目されている最新の生成AIツールを安全に使いこなすためのポイントを解説します。皆様の学習・研究・業務の効率化にぜひお役立てください。

2. 【学生視点】研究・学習の効率化

Google Workspaceを取り入れることで、日々の学習や研究活動をどのように効率化できるか、具体的なシーン別にご紹介します。

- **通学・移動時間の有効活用**（Gemini Notebook） 移動時間は「耳からのインプット」に活用可能です。Gemini Notebookにオープンアクセスの論文を読み込ませて生成した対話型の音源を聴くことで、効率よく要点を把握できます。
- **ゼミの事前準備**（Gemini） 自身が作成したレジュメをGeminiに読み込ませ、事前に生成AIとディスカッションを行うことができます。Geminiに特定の専門家としての役割（プロンプト）を与えることで議論のレベルを調節し、想定問答を繰り返しておくことで、本番のゼミの質を格段に高めることが可能です。
- **グループワークの円滑化**（Google Chat / Meet / ドライブ） 個人のSNSアカウントを共有することなく、Google Chatで手軽に連絡を取り合えます。さらにGoogle Meetでのビデオ通話や、Googleドライブ上でのスライド・ドキュメントのリアルタイム共同編集により、常に最新のデータを共有しながらストレスなく議論を進められます。

3. 【教員視点】研究室運営・学務の効率化

学生との情報共有や指導のタイムラグを解決し、研究室運営をよりスムーズにするためのアプローチです。

- **面談の日程調整**（Googleカレンダー） 面談の日程調整には、Googleカレンダーの「予約スケジュール」機能が便利です。メールを何往復もさせることなく、学生の数クリックで空き枠の中から面談枠を確定させることができます。
- **論文指導・資料添削**（Googleドライブ / ドキュメント） Googleドライブ内に学生ごとの「共有フォルダ」を作成し、そこに論文の草稿を格納してもらう運用です。Googleドキュメントで作成すれば、ファイルは常に最新の1つに集約されます。教員は「提案モード」での修正案提示や「コメント機能」でのダイレクトな指摘が可能となり、学生側も修正作業をシームレスに行えます。
- **研究室の情報集約**（Googleサイト） 研究室専用のGoogleサイトを作成し、オリエンテーション資料や各種マニュアルを掲載しておくことで、毎年の初期指導の手間を大幅に削減できます。公開範囲を特定の個人や学内アカウント（学生・教職員等）に限定できるため、学外への情報漏洩を防ぎながら安全に共有可能です。
- **日常的な連絡の効率化**（Google Chat） メールでの連絡における「相手が読んだか分からない不安」や「返信の遅れ」を解消するため、日常の連絡をGoogle Chatに移行することもお勧めです。「研究室全体のアナウンス用」や「卒論・修論プロジェクト」といったテーマごとのスペース（グループ）を作成することで、コミュニケーションの心理的ハードルが下がり、学生側からも進捗報告や質問がしやすくなります。
- **ゼミのサポート**（Google Classroom） 授業は、原則としてKULMS（Kyoto University LMS）をご利用いただいておりますが、ゼミ等でGoogle Classroomを活用することで、課題の配付・提出等が容易になります。既存のLMSの補完としてお使いください。

4. 生成AIツール利用における注意点

今回のシステム導入により、学生の皆様も「Gemini」や「Gemini Notebook」といったAIツールが利用可能になりました。大変便利なツールですが、利用にあたっては厳守すべき重要な注意点があります。

- **機密情報・個人情報は入力しない**

生成AIを利用する際は、研究中の未発表データや個人を特定できる情報等の機密性の高い内容は入力しないでください。大学のGoogle Workspaceアカウントであっても、入力した情報が生成AIの学習に利用されないのは、「Gemini」や「Gemini Notebook」等の一部のサービスのみです。利用するサービスごとに規約が異なるため注意してください。万が一の情報漏洩を防ぐためにも、AIへの入力は一般的な知識の質問や、公開されても問題のない文章の推敲等に留めましょう。

- **ハルシネーションに注意する**

AIは非常に便利ですが、万能ではありません。時には「もっともらしい嘘（ハルシネーション）」を、まるで正しい事実かのように出力することがあります。AIが出した回答をそのまま鵜呑みにせず、必ず本や信頼できる論文でファクトチェック（事実確認）を行うことを徹底してください。 また、レポートや論文作成における生成AIの利用ルールについては、必ず各授業や学会が提示する指示やガイドラインに従ってください。

5. Google Workspace利用における注意点

- **学生用のGmailは提供なし**

学生用Google Workspaceでは、Gmailは提供されません。**学生用メールは、引き続きMicrosoft 365（KUMOI）を利用してください**。Googleカレンダーでの会議への招待や、Googleドライブのファイル共有通知等は、システムを通じて皆様のMicrosoft 365（KUMOI）のメールアドレス宛に届きます。通知メールは常にMicrosoft 365側でチェックするようご注意ください。

- **卒業・退職時のデータバックアップ**

大学から提供されるアカウントは永続的なものではありません。卒業や退職によって籍を離れる際には、アカウントおよびドライブ内のデータにアクセスできなくなります。研究成果や重要な資料は、各自で定期的に個人のストレージ等へバックアップを取るよう心がけてください。

6. おわりに

Google Workspaceは、単なる便利なITツールの集まりではありません。学内の全員が同じプラットフォームを利用することで、学生と教職員、あるいは学生同士のコミュニケーションの壁を取り払い、学問や研究をよりスムーズに進めるための共通基盤です。ぜひ皆様の活動にご活用ください。

※ 利用可能なGoogle Workspaceのサービスが教職員と学生で異なります。詳細は下記サイトをご確認ください。
https://www.iimc.kyoto-u.ac.jp/ja/services/cloud-service/google/index
※ 学生用Google Workspaceへのログイン方法は、下記サイトをご確認ください。
https://sites.google.com/kyoto-u.ac.jp/stgwman/%E5%AD%A6%E7%94%9F%E7%94%A8gws%E6%A6%82%E8%A6%81#h.n9q73ngix7on

（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

UPKIサーバ証明書の自動更新サービスの提供開始 ～有効期間短縮への対応をお願いします～

ウェブサイトの信頼性を担保する認証局とブラウザベンダーで構成される「CA/Browser Forum」において、セキュリティ向上を目的に、TLSサーバ証明書（サイトの身元証明と通信暗号化のための電子証明書）の最大有効期間を段階的に47日間へ短縮する方針が決定されました。UPKIサーバ証明書を運用する国立情報学研究所（NII）もこれにしたがい、下記のスケジュールで有効期間を短縮することを公表しています。

発行日	有効期間
～2027年3月14日	198日
2027年3月15日～2029年3月14日	100日
2029年3月15日～	47日

有効期間が47日になると年に7～8回の更新が必要となり、従来の手動更新では更新漏れによるサービス停止リスクや作業コストの増加が懸念されます。これに対応するため、NIIではUPKIサーバ証明書をACME（Automatic Certificate Management Environment）プロトコルで自動更新する機能（以下、ACMEサービス）の提供を開始しており、京都大学でも利用可能となりました。なお、従来のサーバ証明書サービスは将来的に縮小・廃止予定ですので、今後は本サービスをご利用ください。

■ACMEサービスの利用方法

ACMEは、証明書を利用する「サーバ」と証明書を発行する「認証局」が直接対話し、発行・更新・失効を自動的に行う標準的な手順です。サーバにインストールしたクライアントソフトが認証局とやり取りして証明書を取得します。証明書を発行する際には、対象ドメインを管理していることを示す「ドメイン所有権の確認」が必要で、確認方法には次の2種類があります。

HTTP-01チャレンジ（簡単おすすめ）

- DNSのAレコード、AAAAレコードまたはCNAMEレコードの指すサーバに対しHTTP（80/TCP）接続
- 検証時に生成したランダム値が /.well-known/acme-challenge/ の値と一致すればOK

DNS-01チャレンジ

- 検証時に生成したランダム値がDNSの _acme-challenge.[ドメイン名] のTXTレコードと一致すればOK
- 都度DNSレコードの登録が必要だがDNS登録APIがあれば自動化は可能

■UPKIのACMEサービスの利用方法

UPKIでは上記のドメイン所有権の確認に加えて、アカウント発行のためのEAB情報（External Account Binding：認証局にアカウントを紐づける鍵情報）が必要です。京都大学ではKUINSDBにログインして下記の手順でEAB情報を申請してください。

1. サーバのホスト管理者またはドメインのドメイン管理者がKUINSDBにログイン後、申請対象のホスト情報またはドメイン情報を開いてください。ホスト管理者が申請した場合はドメイン管理者の承認が必要になります。

2. ACME申請マニュアルを参考に申請してEAB情報を取得します。EAB情報が不要になった場合の「失効」や、紐付けるDNSレコードなどが変更になった場合の「引継」も可能です。

EAB情報の申請はKUINSDBマニュアル（ https://db.kuins.kyoto-u.ac.jp/manual/user/part2/part2_17.html ）でご確認ください。

■ACMEクライアントツール「certbot」の利用方法

以下に、代表的なクライアントツール「certbot」の簡単な利用例を示します。

（インストール）

Redhat系 （EPELリポジトリを有効にすること）

```
sudo dnf install certbot
```

Debian系

```
sudo apt install certbot
```

（アカウント登録）

```
sudo certbot register \
 --server 'https://secomtrust-acme.com/acme/' \
 --eab-kid xxxxxxxxxxxx --eab-hmac-key xxxxxxxxxxxx \
 --email server-admin-name@example.kyoto-u.ac.jp --agree-tos --no-eff-email
```

※ --eab-kid と--eab-hmac-key はKUINSDBで取得したEAB情報、--email は連絡先メールアドレス

（HTTP-01証明書取得）

```
sudo certbot certonly \
 --server 'https://secomtrust-acme.com/acme/' \
 --webroot -w /var/www/webroot -d host1.example.kyoto-u.ac.jp --key-type rsa \
 --deploy-hook 'systemctl reload nginx.service'
```

※ -w はWeb公開するルートディレクトリパス、-d は証明書のドメイン名、--deploy-hook は証明書取得後に実行するコマンド

（証明書更新）

```
sudo certbot renew
```

※ systemd timerにて自動実行できます。
※一度設定すれば、それ以降の更新は自動で行われます。これがACME移行の最大のメリットです。

■その他の利用ケース例

● Webサービス以外のサーバ

- メールサーバなどWebサーバ未使用の場合は --pre-hook や --post-hook オプションで証明書取得の直前・直後に実行コマンドを設定でき、Webサーバの起動・停止やファイアウォール許可・制限のような処理を追加できます。

● ロードバランサなどのアプライアンス機器

- 対応状況はUPKIマニュアル（ https://certs.nii.ac.jp/acme/appliances/ ）でご確認ください。非対応機器でも下記の処理で対応可能です。
  - HTTP接続が複数台に分散する場合は、HTTP-01チャレンジ用URLに限り特定サーバで受信するよう設定し、当該サーバでcertbotを実行します。
  - 証明書を取得したら --deploy-hook の処理でexpectコマンドによるCLI操作（またはcurlによるGUI操作）でロードバランサを更新します。
- クラウドサービスのロードバランサなら、クラウドが提供するサーバ証明書サービスの利用をおすすめします。

● KUINS-IIIサーバ

- 学外から接続不可でHTTP-01チャレンジが使えない場合は、DNS-01チャレンジで取得可能です。KUINSDBのDNS登録APIによる直接登録機能を使えば自動取得ができます。APIの利用方法はKUINSDBマニュアル（ https://db.kuins.kyoto-u.ac.jp/manual/user/part1/part1_11.html ）でご確認ください。

（DNS-01証明書取得）

```
sudo certbot certonly \
 --server 'https://secomtrust-acme.com/acme/' \
 --manual --preferred-challenges dns -d host2.example.kyoto-u.ac.jp --key-type rsa \
 --manual-auth-hook '/path/to/auth_script.sh' --manual-cleanup-hook '/path/to/cleanup_script.sh' \
 --deploy-hook 'systemctl reload nginx.service'
```

※ -d は証明書のドメイン名、--manual-auth-hook は、APIレコード登録処理、--manual-cleanup-hook は、APIレコード削除処理、--deploy-hook は、サービスをリロードするコマンド
※ APIレコード登録処理や削除処理は、curlコマンドなどを使ってJSON形式でPOSTするスクリプトを作成してください。

その他certbotの詳細はUPKIマニュアル（ https://certs.nii.ac.jp/acme/clients/certbot/ ）をご確認ください。

また、certbot以外にも下記のACMEクライアントがございますので、必要に応じてご利用ください。

- 「acme.sh」 Pythonモジュールに依存しないシェルスクリプトの軽量ACMEクライアント
- 「win-acme」 Windows Serverで動作するACMEクライアント

ACMEクライアントの詳細はUPKIマニュアル（ https://certs.nii.ac.jp/acme/clients/ ）をご確認ください。

■無償TLSサーバ証明書「Let's Encrypt」との比較

同じくACMEで無償の証明書を提供する「Let's Encrypt」との差異を下表にまとめました。EVサーバ証明書を扱う有償サービスやクラウドのオプションサービスなども含めて検討し、用途に応じた最適なサービスを選んでください。

	UPKI	Let's Encrypt
種別	OV（組織名 Kyoto University あり）	DV（ホスト名のみ。ワイルドカードやIPアドレスも可）
有効期間	89日	90日
EAB認証	要	不要
サービス開始	2025年11月	2016年4月
サポート	窓口（情報環境機構経由）	コミュニティ

（情報環境機構 IT基盤センター 情報基盤グループ）

お知らせ

アカデミッククラウドシステムのシステム更新について

アカデミッククラウドシステム（ARCS：Academic Research Cloud System）は、2026年8月末をもって現行システムの運用を終了し、2026年9月から新システムとして運用を開始します。

新システムのコンセプト

近年の研究活動における計算需要や研究データ活用の拡大を踏まえ、新システムでは従来の仮想マシン（VM）ホスティングサービス中心の構成から、研究用計算基盤を中心としたサービスへと発展させます。これまで提供してきたWebサーバやメールサーバ向けのVMサービスについては、稼働させているシステムの特性に応じて、ARCSとは異なる基盤の活用し、ARCSは研究活動を支える計算・データ活用基盤としての役割を強化します。

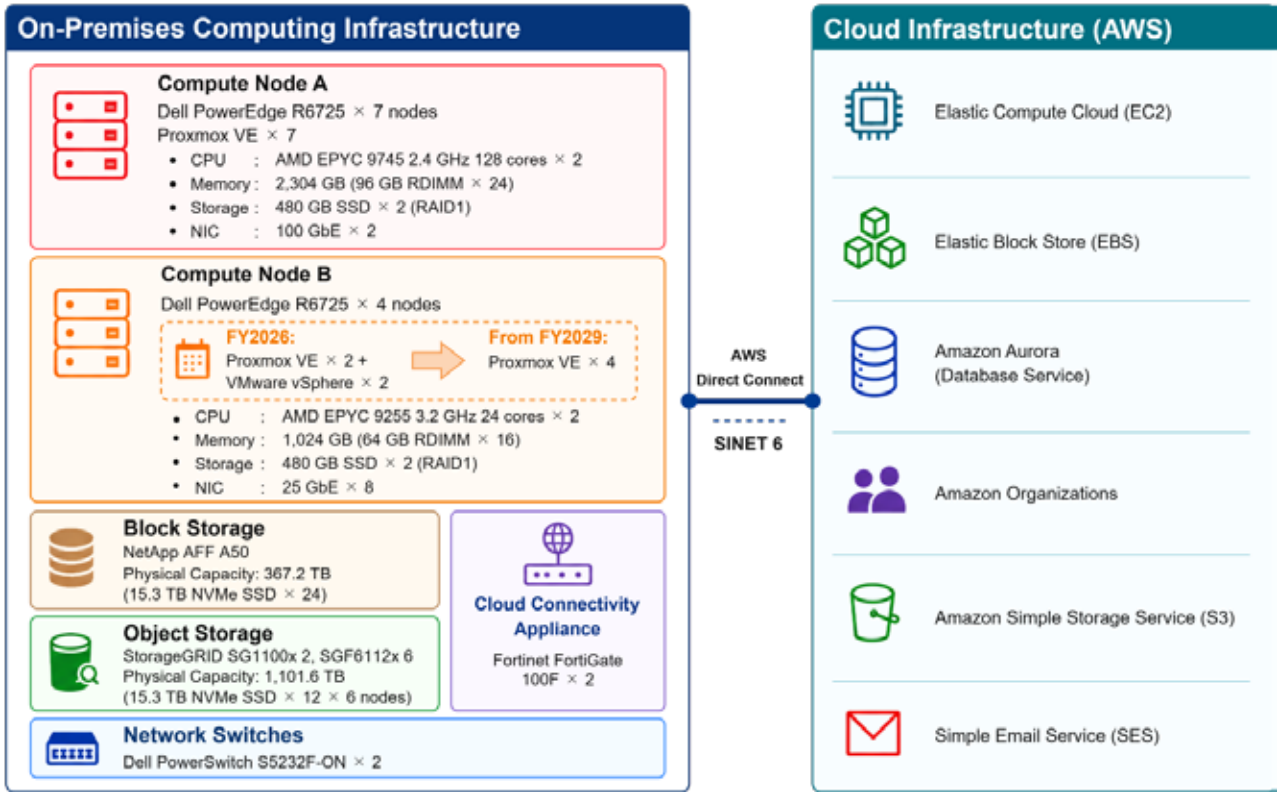
また、学内の計算システムやストレージとの高速な連携を実現するとともに、機密性の高い研究データや学外への持ち出しが困難なデータを安全に処理できる研究基盤を提供します。具体的には、新システムでは、オンプレミスストレージ基盤であるRDM Drive[※1]・RDM ObjectStorage[※2]や、コンテナ技術を中核とした計算サービスとして準備を進めているエッジコンピューティング基盤[※3]との連携も予定しています。コンテナ技術を利用することで、研究環境の再現性や移行性を高めるとともに、OSやソフトウェアのインストール・更新などの管理負担を軽減します。

一方で、近年のハードウェアおよびソフトウェアの価格上昇を踏まえ、持続可能なサービス運営を実現するため、提供サービスの見直しも行います。特に仮想化基盤を構成するソフトウェアのライセンス費用が大幅に増加していることから、限られた予算の中で必要な機能を確保するため、仮想化基盤の構成を見直します。これに伴い、新システムへの移行作業にあたっては、一部の例外を除き、原則としてVMの停止を伴います。

可用性と事業継続性については、システム内での冗長構成を確保し、安定したサービス提供を実現します。一方、ARCSは研究用途に求められる計算性能やデータ活用環境の充実を優先して整備するため、遠隔地へのバックアップについては本システムの対象外とします。必要に応じて、利用者側または別サービスとの組み合わせによるバックアップ設計をお願いします。

ARCSは、研究データ、計算資源、ストレージ基盤を有機的に連携させる次世代の研究基盤として、研究活動の高度化と効率化を支援し、本学の研究力向上に貢献していきます。

システム構成



提供を終了するサービス

システム更新に伴い、以下の試行サービスについては提供を終了いたします。

- パブリッククラウドを利用したVMホスティングサービス（試行）※4
- オブジェクトストレージ（AWS S3）※5

（情報環境機構 IT基盤センター 研究支援グループ）

※1 RDM Drive https://www.iimc.kyoto-u.ac.jp/ja/services/storage/rdmdrive

※2 RDM ObjectStorage https://www.iimc.kyoto-u.ac.jp/ja/services/storage/rdmobject

※3 エッジコンピューティング基盤 https://www.iimc.kyoto-u.ac.jp/ja/info/20251209184430

※4 パブリッククラウドを利用したVMホスティングサービス（試行）
https://www.iimc.kyoto-u.ac.jp/ja/services/server/vm#06

※5 オブジェクトストレージ（AWS S3） https://www.iimc.kyoto-u.ac.jp/ja/services/server/objss

報告

京都大学研究データ管理シンポジウムを開催しました

「京都大学研究データ管理シンポジウム：オープンサイエンスに向けた研究データ管理支援の現状と課題」を、2026年2月27日に国際科学イノベーション棟 HORIBAシンポジウムホール において、オンラインとのハイブリッド形式で開催しました。シンポジウムには、会場76名、オンライン298名の合計374名が参加しました。

シンポジウムは、岡部寿男 情報環境機構長による開会挨拶と、引原隆士 理事・副学長によるオープニング・スピーチから始まりました。続いて、黒橋禎夫 国立情報学研究所長より「データ基盤から知識基盤へ」と題した基調講演が行われました。その後、伊達進 大阪大学D3センター教授および甲斐尚人 同准教授より、データ集約基盤「ONION」の経緯や分野横断的な取り組みなど大阪大学での事例が紹介されました。さらに本学から、渥美紀寿 情報環境機構教授、小谷大祐 学術情報メディアセンター准教授、井阪悠太 情報環境機構特定講師、西岡千文 情報環境機構准教授が順に登壇し、本学の研究データ管理支援体制やエッジコンピューティング基盤、オープンアクセス実現に向けた取り組みについて講演を行いました。

プログラムの後半には、渥美教授をモデレーターとして、「大学におけるこれからの研究データ管理支援」をテーマとしたパネルディスカッションが行われました。パネリストとして黒橋所長、伊達教授、引原理事・副学長のほか、林和弘 科学技術・学術政策研究所データ解析政策研究室長、村山泰啓 附属図書館教授が登壇し、各分野の専門家を交えた活発な議論が交わされました。最後に、引原理事・副学長の閉会挨拶をもって、本シンポジウムは閉幕しました。

また、シンポジウム後には情報交換会が開催され、学内外から集まった参加者が所属の垣根を越えて親睦を深め、新たなネットワーク構築に繋がる盛況な情報交換の場となりました。

本シンポジウムは、オープンサイエンスの実現に向けた研究大学における基盤整備の現状や課題の共有、今後進むべき方向について議論を深める重要な機会となりました。今回の議論や交流を通じて、各研究機関におけるデータ管理支援の連携が一層強化され、データ駆動型の学術研究が力強く推進されていくことが期待されます。

開会挨拶を行う岡部機構長

オープニング・スピーチを行う
引原理事・副学長

基調講演を行う黒橋所長

伊達教授

甲斐准教授

渥美教授

左から、小谷准教授、井阪特定講師

西岡准教授

パネルディスカッションの様子

(情報環境機構 データ運用支援基盤センター)

コラム

脆弱性対応の原点回帰ー「情報資産の把握」と「正しい順位付け」という基本から

日々システムを運用していく中で、次々と公表される新しい脆弱性に対して、その対応に頭を抱えている担当者も多いのではないでしょうか。今回は、限られたリソースの中での効果的なシステムの守り方を整理します。

脆弱性の対応の前に、情報資産の把握を

「新たな脆弱性が公表されたが、うちのシステムは大丈夫なのか」と組織内で大騒ぎすることは少なくありません。ここで大切なのが、自身の管理下に「どのようなシステムがあり、何のOSやソフトウェアが、どのバージョンで動いているか」を把握できているか、という点です。管理できていないサーバーや、過去に立ち上げてそのまま放置されたシステムがあれば、そこがそのまま攻撃者の侵入口になってしまいます。脆弱性対応の第一歩として、地道に自分たちの情報資産を正確に把握し、自身の管理するシステムが公表された脆弱性に該当するかを迅速に判断できるようにしておくことが大切です。

脆弱性への対応基準

情報資産を把握できたら、次は発見された脆弱性の精査です。該当する全ての脆弱性に即時対応することが理想で、自動更新可能かつ運用上支障がないシステムは自動更新を有効にしておくのが賢明です。しかし、人的・金銭的コストの面から現実的には困難な場合もあります。そこで重要になるのが、対応の優先順位付けである「トリアージ」という考え方です。

脆弱性の深刻度を測る指標として広く利用されるCVSS（Common Vulnerability Scoring System）があります。これは脆弱性の深刻度を0.0〜10.0の数値で表したもので、算出されたスコアの大きさや評価基準を参考にした優先順位付けができます。たとえば、リモートコード実行（RCE）が可能な脆弱性については、攻撃者が外部ネットワークからシステム内部に侵入する恐れもあるため、最優先で対処する必要があります。一方で、ローカル権限昇格の脆弱性については、攻撃の実行条件として「システムにアクセスする権限を既に持っていること」が前提となるため、ローカルユーザーが悪用されうる環境以外では、対応の優先順位を少し落とすことができます。このように優先順位付けの基準を組織内で準備しておくことで、素早く対応の判断ができるようになります。

一方で、脆弱性が発見されたからといって、すぐにそれを利用したサイバー攻撃が起こるとは限りません。そこで参考にしたいのが、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）が公開しているKEV（Known Exploited Vulnerabilities）です。KEVは「実際に悪用が確認され、対処方法が明らかな脆弱性」のカタログです。つまり、KEVカタログに掲載されていれば 、即時対応すべきと言えます。CISAはKEV等を指標とした優先順位付け基準としてBOD 26-04を発行していますので、こちらも参考にしてみてください。

脆弱性との上手な付き合い方を目指して

システムを運用し続ける限り、脆弱性をゼロにすることは不可能です。最近では、AIを用いた脆弱性の探索やコード解析が自動化され、新しい脆弱性がこれまで以上の頻度で発見・公表されるようになってきています。だからこそ、「脆弱性は必ず発見されるもの」という前提で、「情報資産の把握」と「対応基準の策定」という原点を見つめ直すことが重要です。基本を徹底し、脆弱性と上手につき合っていく仕組みを組織全体で作り上げていきましょう。

（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