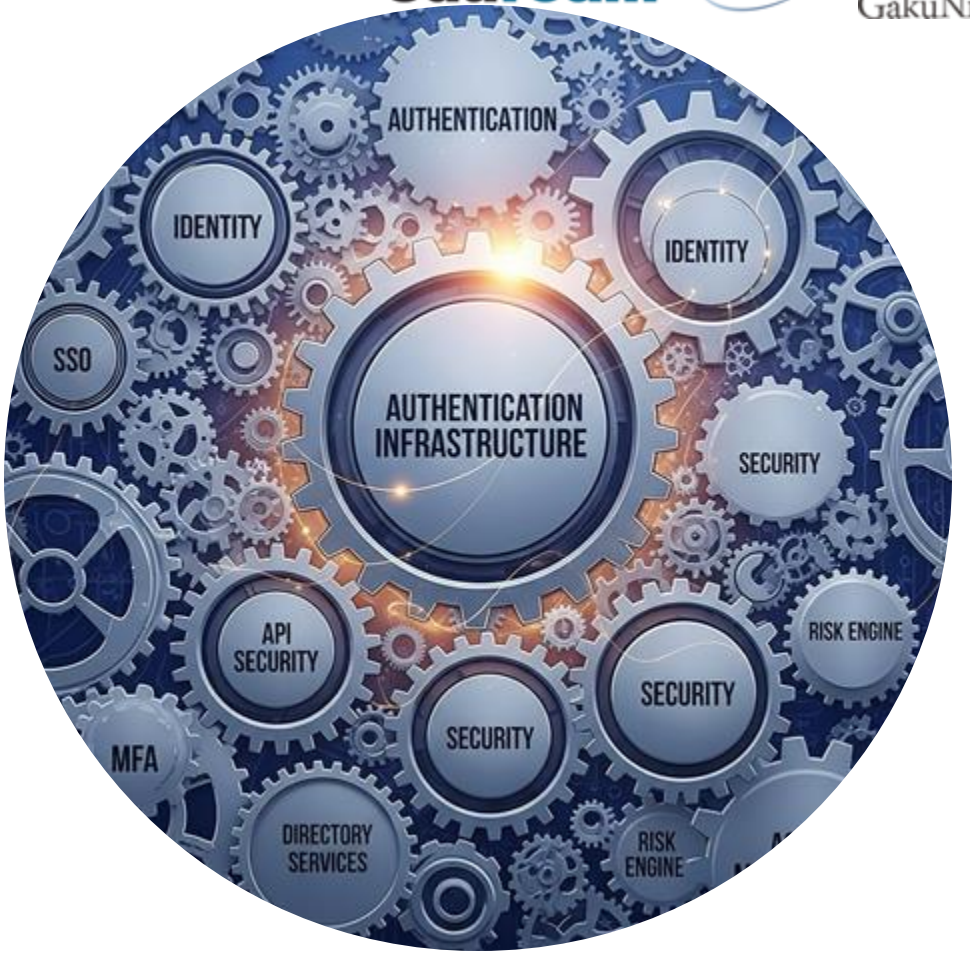
認証
―学認・UPKI・eduroamの最新動向

NIIサービスキャラバン2025

国立情報学研究所
トラスト・デジタルID基盤研究開発センター

本日お話すること

- 認証基盤の重要性と私たちが直面する現状
- 現状の課題に対するNIIの取り組み
- 電子証明書の有効期間短縮について
- お知らせ



大学・研究機関における被害の現状

- 近年、大学・研究機関で”強固とは言えない認証”に起因する被害が多発
- フィッシング詐欺によるID/パスワード窃取で**情報漏洩やなりすまし**が発生
- 乗っ取られたアカウントが悪用され、迷惑メール大量送信などの二次被害も
- 特にMicrosoft 365を狙った攻撃が複数報告されており、多要素認証の導入が急務
- 大学や研究機関での被害は他人事ではない

教員のMicrosoft 365アカウントが乗っ取られ、フィッシングメール送信

2024年5月、教員のMicrosoft 365アカウントがフィッシング詐欺により乗っ取られました。
攻撃者はこのアカウントを悪用し、学生や卒業生、他の教職員など学内外の関係者に対し、偽のメールを送信しました。
この結果、学生が偽サイトに自身のIDとパスワードを入力してしまう二次被害が発生しました。
原因は、教員がフィッシングサイトに認証情報を入力してしまったことでした。

複数アカウントへの不正アクセス、大量のフィッシングメール送信の再発

2025年1月、大学は教職員と学生のメールアカウントがフィッシング攻撃を受け、不正アクセスされたと発表しました。
これにより、学内外のアドレスに対し、フィッシングメールが送信されました。
同大学では2023年にも大規模なスパムメール送信事案が発生しており、パスワード認証のみに依存するリスクと、継続的な対策の重要性が改めて示された形となります。

非常勤講師のPCがサポート詐欺に、学生の成績情報漏洩の恐れ

2024年5月、大学の非常勤講師が所有する私物のパソコンが、偽のウイルス感染警告（サポート詐欺）をきっかけに不正アクセスを受けました。
このPCには、担当科目を履修する学生の氏名、学籍番号、メールアドレス、成績情報などが保存されており、これらの情報が漏洩した可能性が報告されています。
個人のデバイスが起点となり、重要な教育情報が危険に晒されるという、脅威の形を示唆する事例です。

教育・研究分野はサイバー攻撃の主要ターゲット、前年比119%増

個別の事例だけでなく、より大きな視点での脅威も報告されています。サイバーセキュリティ企業のチェック・ポイント・ソフトウェア・テクノロジーズが2024年10月に発表した調査によると、2024年第3四半期において、教育・研究部門は最もサイバー攻撃の標的とされた分野であり、1組織あたりの週平均攻撃数は前年同期比で119%も増加しています。これは、アカデミア全体が攻撃者から極めて高い関心を寄せられていることを示す憂慮すべきデータです。

私たちが直面する現状

- 攻撃の巧妙化と高度化が進行中
- パスワード認証だけではセキュリティに限界
- 利便性とセキュリティの両立が喫緊の課題

さらなる信頼性向上のために

- より機微な情報（個人情報、研究データ、人事情報など）を扱うサービスの増加
- 現行のパスワード認証だけでは、アクセスを許可するには不十分なケースが出てきている
- 「パスワード認証だけ」の世界から、
  「より確かな身元確認と当人認証」が求められる世界への変化
- NII認証担当では、継続して以下のサービスを整備中
  - 学認：認証/認可を制御
  - UPKI：安全な通信インフラの基盤
  - eduroam JP：無線LANローミング

次世代認証連携の検討を進めています

- 学認の仕組みの中でAAL2/IAL2を実現するための技術検討
- 次世代認証連携に向けた技術標準仕様策定、公開、国際的相互運用性の担保
  - IAL2/AAL2規準文書
- 認証プロキシサービス
  - Orthros：学認外（企業など）からのアクセス手段の確保
  - 認証Proxy
- 認証器レジストリ
  - AAL2をみたす多要素認証用認証器のリスト公開
  - 簡易かつフィッシングへの耐性を確保した認証へ
- 次世代認証連携中規模実証実験
  - 保証度の高い認証を要求するSPと保証度の高い認証を提供するIdPが集まって行うサービスイン前提の実証実験

UPKI電子証明書発行サービス－安全な通信の土台

- 通信の安全を守る「身分証明書」：電子証明書
  - **暗号化:** 通信内容を盗み見から守る (SSL/TLS)
  - **認証:** 通信相手が本物かを確認する
  - サーバ証明書（Webサイトの身分証）とクライアント証明書（利用者の身分証）の2種類を提供

サーバ証明書 有効期間段階的短縮について

【何が起きるのか？】 変更の概要

TLSサーバ証明書の最大有効期間が、段階的に大幅短縮されます

- CA/Browser Forumにて、TLSサーバ証明書の最大有効期間を現行の**398日**から最終的に**47日**へ短縮することが決定しました

【何が起きるのか？】 具体的なスケジュール

2026年3月から段階的に短縮が開始されます

発行日	最大有効期間	
～ 2026年3月14日	398日 (現行)	←2025年度末まで
2026年3月15日 ～ 2027年3月14日	200日	←2026年度末まで
2027年3月15日 ～ 2029年3月14日	100日	←2028年度末まで
2029年3月15日 ～	47日	

※ドメイン名などの検証データの再利用期間も同様に短縮され、最終的には最大10日となります
※サーバ証明書のみであり、クライアント証明書は影響を受けません
※UPKIでは、2026年3月4日実施のメンテナンス終了後から有効期間を198日間とする予定です

【どう対応するのか？】 ACMEプロトコルとは？

ACME (Automatic Certificate Management Environment) が、この課題を解決する鍵となります

- 概要
  - 証明書の発行・更新・失効といった管理プロセスを自動化するための標準プロトコル（RFC 8555）です
  - 認証局（CA）とサーバが直接対話し、人手を介さずに証明書のライフサイクルを管理します
- なぜACMEが必要か？
  - 有効期間が47日という短期間になると、手動での管理は非現実的です
  - ACMEによる自動化は、この頻繁な更新に対応するための最も効果的で中心的な役割を果たします

UPKI電子証明書発行サービスでの対応

現在の電子証明書発行形態→当面維持

- 現行のTSVファイルによる申請（TSV申請）
  - 利用管理者が鍵ペアとCSRを生成し、申請用TSVファイルを作成
  - 登録担当者が発行・更新・失効処理
  - 利用管理者は証明書をファイルとして受け取り、インストール操作を行う
- 現行の発行形態は**当面（年単位）維持**します
  - サーバ証明書利用環境における、ACMEへの対応は十全とは言えない
    - 対応していないものも沢山
    - 対応した製品が出たとして、それを機関で導入するまでのラグ（調達の周期などに起因）も存在
  - ACMEへの全証明書の移行が難しい現状、現行の発行形態は維持する必要があります

証明書自動発行・更新 ACME対応

- ACMEプロトコル対応
  - 証明書有効期間短縮のスケジュール決定により急務と認識
  - **UPKI認証局でもACME対応を実施**
  - →自動発行・更新・設定が可能になります
    - 自動設定は対応した環境が必要
- certbotを利用可能
  - certbot ?→certbotは、手動で管理されている Web サイトで電子証明書を自動的に取得・設定してHTTPSを有効にする、無料のオープンソースソフトウェアツール
  - 多くのACME対応認証局でも使われる
  - UPKIでも、マニュアルや手順説明ではcertbotを推奨ツールとする
  - また、他のACME対応ツールでの利用を妨げない

UPKIでのACME利用

- **Certbot + EAB Credential** での発行・更新・設定
- EAB(External Account Binding) Credential とは？
  - ACMEプロトコルにおいて、外部アカウントとACMEアカウントを紐付けるための認証情報のこと
    - ACMEを使って証明書を発行するために必要なアカウントを構成する情報
  - Key Identifier (KID)とHMAC Keyの組み合わせ
    - これで不正な利用を防ぎます
  - 利用管理者はEAB Credentialを用いて、UPKIのACMEサーバを利用して証明書発行・更新処理を行う
- 登録担当者は、エンドエンティティ証明書に紐付いたEAB Credentialを発行管理する
  - 証明書自動発行支援システムで管理
  - 専用フォーマットのTSVファイルを利用→TSVツールで作成可能

小まとめ：目的と概要

- なぜACME対応を行うのか？ (目的と概要)
  - 証明書の有効期間短縮への対応として、証明書発行・更新プロセスの自動化が急務です
  - UPKIではこの課題に対応するため、certbot等のツールで利用可能なACMEプロトコルを導入します
  - セキュリティを確保するため、EAB (External Account Binding) Credential という認証情報を用いて安全に利用できる仕組みを提供します

特記事項

- 2025年10月後半からの先行利用開始を予定(**昨日より可**)
- 2025年12月頃まで、認証局側の制限により、指定可能なFQDNは1つ（CN=dNSName）
  - 2026年から、複数指定可能になる予定
- ACMEで発行されるサーバ証明書の有効期間は**89日間**
  - TSVファイル（CSR）での発行による有効期間と異なることに留意ください
  - 2029年3月15日からは**47日間**になります
- certbot 利用時にACMEサーバの指定が必要
  - --server https://secomtrust-acme.com/acme/
  - デフォルトでLet's encryptを参照するので、指定必須

お願い：サービス利用料金の変更について

- 今回のACME導入は、電子証明書の有効期間短縮に対応するための重要な機能強化であり、サービスの安定運用とセキュリティ確保に不可欠です。
- つきましては、大変恐縮ではございますが、本機能強化に伴う費用を賄うため、サービス利用料金の変更をお願いしたく存じます。
- 何卒ご理解ご協力のほどお願い申し上げます。

変更後の利用料金（令和8年度より）

構成員数(*1)	変更後	変更前	追加ドメイン料金
1-200	**48,000**	30,000	20,000 （変更なし）
201-400	**64,000**	40,000	
401-600	**80,000**	50,000	
601-800	**96,000**	60,000	
801-1000	**112,000**	70,000	
1001-1200	**128,000**	80,000	
1201-1400	**144,000**	90,000	
1401-1600	**160,000**	100,000	
1601-1800	**176,000**	110,000	
1801以上	**192,000**	120,000	

*1 構成員数：教員・研究者数の合計

- 金額は**消費税別**
- 証明書新規発行・更新発行数に制限なし

お知らせ

UPKIからのお知らせ

- さらに詳細な内容や具体的な対応方法につきましては、今後開催する以下のイベント等でご説明いたします
- UPKI全国説明会
  - 札幌 12月12日(金) 14:00-16:00
    - TKP札幌駅カンファレンスセンター カンファレンスルーム2H
  - 仙台（TOPICと共催、日程・会場は調整中）
  - 金沢 11月14日(金) 14:00-16:00
    - TKP金沢カンファレンスセンター カンファレンスルーム3C
  - 福岡 11月21日(金) 14:30-16:30
    - JR博多シティ 9階会議室(4)
- 大学ICT推進協議会2025年度 年次大会
  - 2025年12月1日(月)～3日(水)
  - 認証基盤部会企画セッション

第4回 学認SP研究会 in AXIES 2025 (12/3)

ー多様なサービスプロバイダーと機関が集い
認証連携の実践知を共有する場ー

概要

学認SP研究会は、学認に参加・連携するサービスプロバイダーに関心を持つ関係者が集まり、最新動向や課題を共有・議論する場です。多様なSP事例を通じて安全で利便性の高い認証連携を探り、参加者同士で技術や運用の知見を交換・蓄積します。

キーワード

学認、サービスプロバイダー、認証連携、情報共有、教育・研究サービス

https://spedu-catalog.jp/