UPKI電子証明書発行サービス最新情報

2025年6月18日　学術情報基盤オープンフォーラム 2025

トラスト・デジタルID基盤研究開発センター 水元 明法

おかげさまで10周年

2015年1月1日に提供開始したUPKI電子証明書発行サービスは、
10周年をむかえました

UPKI電子証明書発行サービスの概要

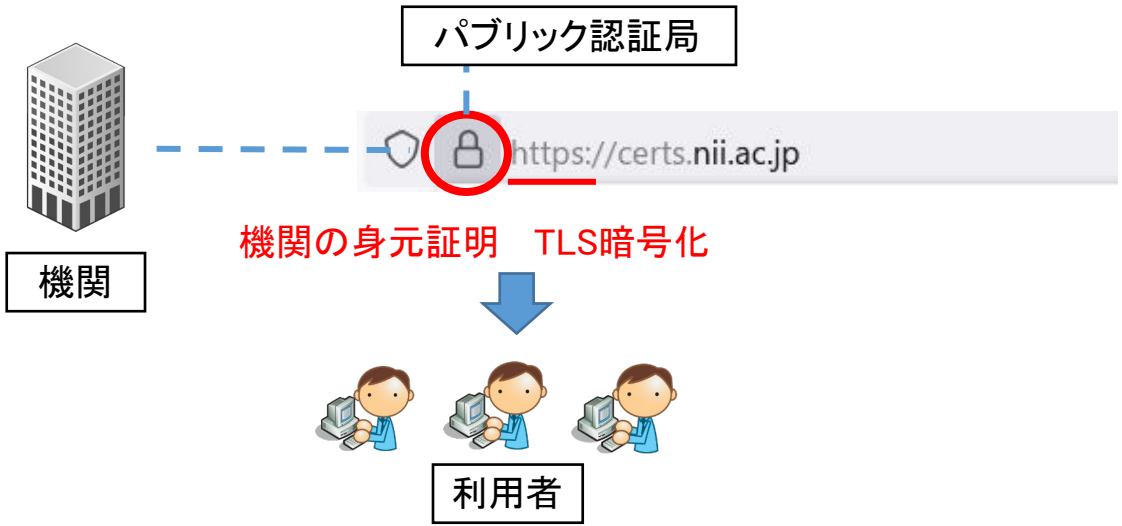
UPKI電子証明書発行サービス

- UPKI電子証明書発行サービス
- 高等教育・研究機関を対象に電子証明書を発行するサービス
  - 実情にあった契約と発行手順
  - 比較的安価で効率的

UPKI電子証明書発行サービス
提供する証明書

サーバ証明書(OV)

- Webサイトを提供する機関の身元を証明できます
- パブリック認証局で発行される公的な証明書です。
- TLSで、サーバと利用者間の通信を暗号化し、盗聴を防ぐことができます



UPKI電子証明書発行サービス
提供する証明書

個人認証用証明書

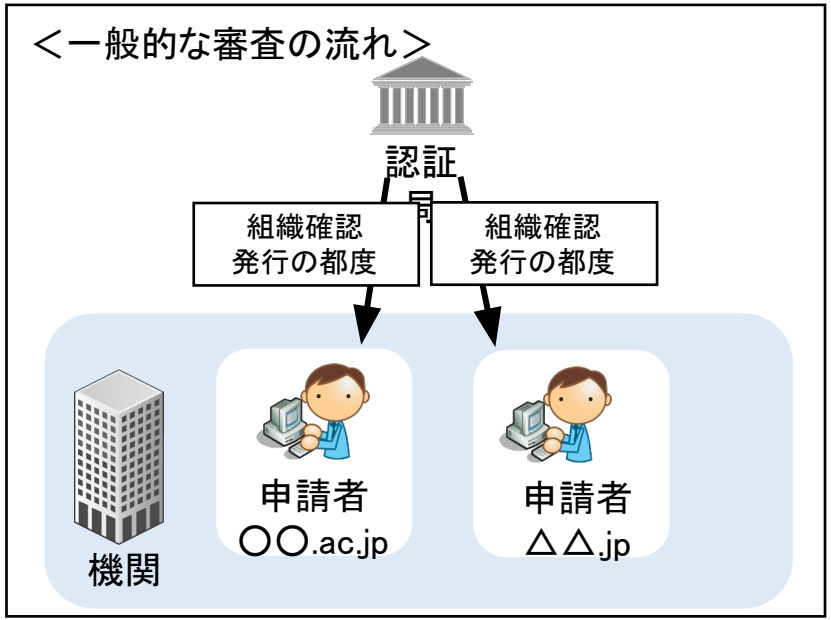
- 証明書を持つ者（利用者）がにWebサービス等にアクセスする際に身元を証明
  - プライベート認証局で発行
  - UPKIでは、プライベート認証局でも、パブリックで運用しているCP/CPSに準拠し運用

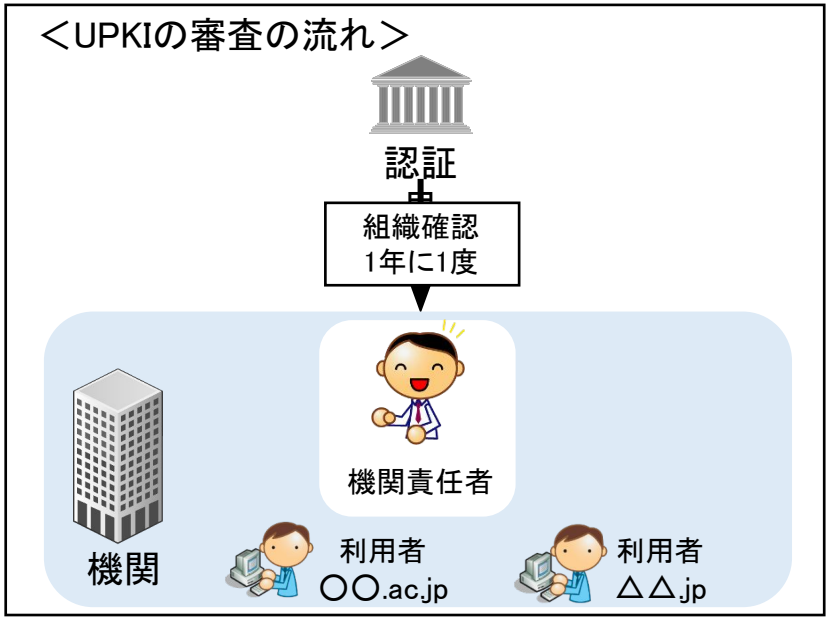
S/MIME証明書

- 文書や電子メールにデジタル署名
  - 文書作成者や送信元メールアドレスを保証し、なりすましや改ざんを防止
  - パブリック認証局で発行
  - 電子メールを暗号化し、盗聴を防ぎ、情報漏洩などを防ぐことができます

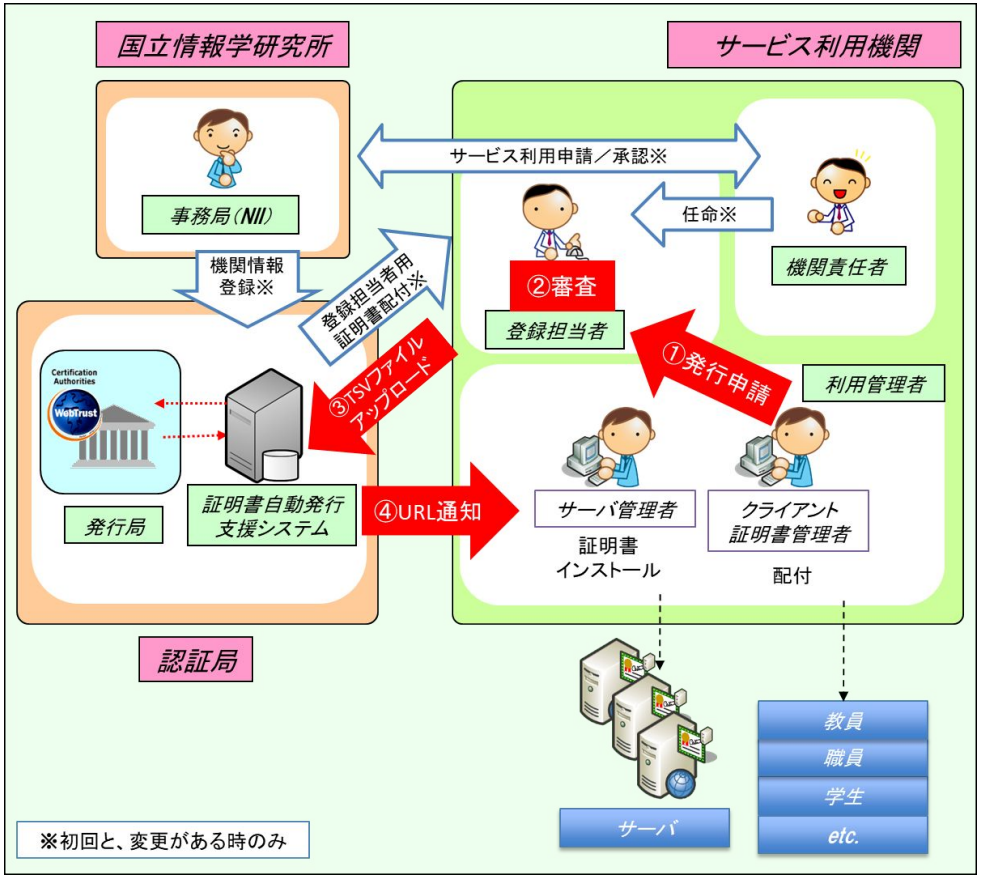
UPKI電子証明書発行サービス
証明書発行における審査

・証明書で機関の身元証明を可能とするために、審査を行います。
・UPKIでは、申請のあったドメインに対して、申請受付時とその後1年毎に認証局から機関責任者へ連絡し、組織の確認を行っています。





UPKI電子証明書発行サービス
証明書発行の流れとメリット



- 本サービスでは、**年間定額料金**で、枚数に制限なく、電子証明書を発行することができます。
- 各サービス利用機関内に担当者を設定し、それぞれの業務を担当していただくことで、比較的安価な料金設定を実現しています
  - 例：構成員数1-200人の場合、￥30,000（1ドメイン含む・枚数制限なし）
  - 詳細は「利用細則」をご参照ください

機関責任者：機関責任者は、所属する機関の長より委嘱を受け、本サービスの利用に関する責任を負います。

登録担当者：機関責任者から任命を受け、機関内で証明書発行・失効・更新等にかかる申請の審査とその業務を担当します。

利用管理者：NIIが定める各種規定に合意し、証明書に記載された公開鍵と対になる秘密鍵を管理します。登録担当者を介して証明書の発行を行います。

UPKI電子証明書発行サービス
規定・マニュアル

各種規定、マニュアルは、以下のUPKI電子証明書発行サービスのホームページに掲載しています。

https://certs.nii.ac.jp/manual

UPKI電子証明書発行サービスからのお知らせ

Security Communication ECC RootCA1
ブラウザ搭載状況

対象：証明書プロファイル11 サーバ証明書ecdsa-with-SHA384

【OS・ブラウザ搭載状況】

- Microsoft Windows
- Chrome105（2022/08/30・Windows版）
- Firefox 106（2022/10/19）
- Chrome107（2022/11/07・Mac版）
- Android14（2023/10/05）
- macOS Sequoia Ver.15.0、Safari バージョン18.0 、iOS 18（2024/09/17）

ルートCA証明書・中間CA証明書更新

- 2025年10月～2026年3月1日までの期間に、TLS用中間CAの切り替えを実施予定
  - NII Open Domain CA – G8 RSA（現行はG7）
- 新中間CA証明書(G8)は、新ルートCAから発行される
  - SECOM TLS RSA Root CA 2024
  - https://crt.sh/?caid=363595
- 現在Mozillaに搭載申請中
  - https://bugzilla.mozilla.org/show_bug.cgi?id=1943001
- スケジュール定まり次第お知らせ致します
  - 新中間CA証明書は、公開され次第お知らせします
  - https://crt.sh/?q=NII+Open+Domain+CA
    - 現在G7まで

ドメイン認証におけるMPIC対応

- 2025年3月15日より、ドメイン認証におけるMulti-Perspective Issuance Corroboration（MPIC）への対応を実施
  - Baseline Requirements（BR）の改定に伴う対応
- **MPIC：**証明書発行対象のFQDNに対するDNS検証を、世界各地の複数のネットワーク拠点から実施し、その結果の一致を確認することで、ドメイン名の所有権確認をより強化する仕組み
  - **発行要件:** プライマリーのDNS検証において、世界各地に設置されたリモートネットワーク5箇所中4箇所以上で、対象FQDNの名前解決結果が一致した場合にのみ、証明書が発行される
  - **発行抑止:** 上記要件を満たさない場合（DNS検証結果の一致が3箇所以下の場合）、証明書の発行は抑止される
  - **エラー通知:** 発行が抑止された場合、エラーコード 338 が記録される
- この変更に伴い、証明書発行対象とするFQDNは、インターネット上で複数の視点から正しく名前解決可能な設定にする必要がある

CAAレコードチェック

CAは、証明書を発行しようとしているドメイン名（例：`child.parent.example.co.jp`）に対して、そのドメインを管理する権威DNSサーバーにCAAレコードを問い合わせます。

- **CAAレコードが存在する場合**：その内容に従い、許可されたCAのみが証明書を発行できます。
- **CAAレコードが存在しない場合**：権威DNSサーバーは、**該当するレコードが存在しない** ことを示す応答（`NOERROR`ステータスコードと、空もしくはCAAやTEXTなどの何らかのAnswerセクション）を返す必要があります。応答がない、あるいはエラー（`SERVFAIL`など）を返すと、CAAレコードチェックが失敗し、証明書は発行されません。

内部FQDNへの証明書発行におけるDNS設定

- 証明書を発行したいFQDNを管理する権威DNSサーバーに対して、digコマンドを用いてCAAレコードを問い合わせ、以下のような応答が返ってくることを確認してください。
- 期待される応答例

```
$ dig @203.0.113.53 CAA child.parent.example.co.jp

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12345
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0 <= Answerセクションは空でも良い

;; QUESTION SECTION:
;child.parent.example.co.jp.     IN    CAA

;; AUTHORITY SECTION:
parent.example.co.jp. 3600 IN    SOA ns1.parent.example.co.jp. admin.parent.example.co.jp.
2025042401 ... <= SOAレコードが含まれる
```

status: NOERROR が返ってくれば、CAAレコードが存在しない場合でもチェックは成功します。

BINDによる設定例 named.conf

ここでは、権威DNSサーバーとしてBINDを使用し、parent.example.co.jp ゾーンを管理しており、そのサブドメイン child.parent.example.co.jp に証明書を発行したい場合の具体的な設定例を示します。

```
// named.conf

acl "trusted" {
    any;
};

options {
    directory "/var/named";
    allow-query { trusted; };
    recursion no;                  // 再帰問い合わせは無効に（権威サーバーの役割）
};

// 管理するゾーンの定義
zone "parent.example.co.jp" IN {
    type master;                    // プライマリDNSサーバー
    file "/var/named/parent.example.co.jp.zone"; // Zoneファイルへのパス
    allow-query { any; };          // このゾーンへの問い合わせを許可
};
```

BINDによる設定例 Zoneファイル

```
; /var/named/parent.example.co.jp.zone
$TTL 3600 ; デフォルトのTTL（Time To Live）秒

@   IN  SOA ns1.parent.example.co.jp. admin.parent.example.co.jp. (
        2025042401 ; Serial number (ゾーン更新時にインクリメント)
        3600       ; Refresh (セカンダリDNSが更新を確認する間隔)
        1800       ; Retry (リフレッシュ失敗時の再試行間隔)
        604800     ; Expire (セカンダリDNSがデータを無効とみなす期間)
        86400 )    ; Minimum TTL / Negative Cache TTL

; --- Name Server Records ---
; このゾーンの権威DNSサーバーを指定します。
    IN  NS  ns1.parent.example.co.jp.
;   IN  NS  ns2.parent.example.co.jp. ; 複数のNSサーバーがある場合

; --- Name Server Address Records ---
; NSレコードで指定したサーバー名のIPアドレスを定義します。
; グローバルIPアドレスである必要があります。
ns1.parent.example.co.jp. IN A 203.0.113.53
; ns2.parent.example.co.jp. IN A 203.0.113.54 ; 複数のNSサーバーがある場合

; --- Other Records ---
; 証明書を発行したいホストのAレコード（必須ではない）
; child   IN  A   203.0.113.100
; その他の必要なレコード（MX, TXTなど）
; ...
```

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？】変更の概要と背景

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

- 決定事項
  - 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。
- 背景と目的
  - セキュリティの向上: 証明書の不正利用リスクを低減し、エコシステム全体を保護することが目的です。
  - 失効メカニズムの補完: 主要ブラウザはリアルタイムの失効検証を常時行っておらず、短命な証明書によって失効チェックへの過度な依存を減らします。
  - 自動化の促進: 証明書管理の自動化を促し、運用の安定化とインシデント（例：Heartbleed脆弱性）発生時の迅速な対応を目指します。

【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)
2026年3月15日 ～ 2027年3月14日	200日
2027年3月15日 ～ 2029年3月14日	100日
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。

【何が起きるのか？】想定される問題点

証明書の更新頻度増大により、手動管理は限界に達します

- サービス停止リスクの増大
  - 手動更新では、更新忘れやミスによる証明書切れの可能性が高まります。
  - 自動化を導入しても、スクリプトエラーやネットワーク障害による更新失敗のリスクが懸念されます。
- 管理コスト・負荷の増大
  - 単純計算で、年1回だった更新作業が年8回以上必要になります。
  - 大量の証明書発行が、認証局（CA）のインフラに大きな負荷をかける可能性があります。
- 対応が困難な環境の存在
  - 自動化プロトコルに対応していないソフトウェアやハードウェア（IoTデバイス、レガシーアプリ等）が多数存在します。

【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

【どう対応するのか？】
メリット：ACME導入で得られる効果

ACMEによる自動化は、単なる効率化以上の価値をもたらします

- メリット1：運用効率化とサービス停止リスク低減
  - 証明書のライフサイクル管理を完全に自動化し、担当者の負担を劇的に軽減します
  - 更新忘れなどのヒューマンエラーをなくし、証明書切れによるサービス停止のリスクを大幅に低減します
- メリット2：セキュリティの向上
  - 万が一、秘密鍵が漏洩しても、有効期間が短い（短く変更されていく）ため不正利用される期間を限定できます（攻撃の持続性低減）
  - 新しい暗号アルゴリズムへの移行などを迅速に行えるようになります。
- メリット3：インシデントへの迅速な対応
  - Heartbleedのような大規模な脆弱性が発生した際も、影響を受ける証明書を迅速に入れ替えることが可能です

【どう対応するのか？】
デメリット：導入時の課題と対策

すべての環境ですぐに使えるわけではなく、事前の検討が必要です

- 課題（デメリット）
  - **非対応な環境:** レガシーなシステム、一部のネットワーク機器、IoTデバイスなど、ACMEをサポートしない環境が存在します
  - **自動化失敗のリスク:** スクリプトの不具合やネットワーク障害で更新が失敗し、サービス停止につながる可能性があります
  - **特定サービスへの依存:** Let's Encryptのような特定のACME対応サービスへの依存が集中するリスクが指摘されています
- 推奨される対策
  - **非対応環境:** リバースプロキシやWAFを導入し、システムの前面で証明書を代理で更新・終端する方法が有効です
  - **失敗への備え:** 証明書の有効期限を監視し、更新失敗時に管理者に通知するアラートシステムを構築します
  - **依存リスクの分散:** 複数のACME対応CAサービスを検討・併用することも選択肢です

小まとめ

- **現状認識:** セキュリティ向上のため、TLSサーバ証明書の最大有効期間は2029年3月までに47日へ短縮されます。 これにより、手動での証明書管理は事実上不可能になります
- **打つべき手:** ACMEプロトコルを導入し、証明書の発行・更新プロセスを自動化することが不可欠な対応策となります
- **得られる未来:** 自動化により、運用負担の軽減、サービス停止リスクの低減、そしてより高いレベルのセキュリティを実現できます

計画的な自動化への移行が、今後のセキュアなウェブ環境を維持する鍵です

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

- 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予定
  - 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

EAB Credential 設定例

```
certbot register \
  --server <UPKI_ACME_SERVER_URL> \
  --email your_email@example.com \
  --agree-tos \
  --eab-kid <YOUR_EAB_KID> \
  --eab-hmac-key <YOUR_EAB_HMAC_KEY>
```

※初回のみ。
※EAB Credentialは証明書を要求するサーバに保存。

設定後は、certbotの標準的な使い方と同様の操作が可能

後日提供予定の情報

- 実際の証明書発行・更新時に用いるコマンド例
  - certbot renew, certbot certonly, …
- ACMEサーバURL
- EAB Credential 発行フロー、ライフサイクルの管理等
- FAQ

ACME導入に向けて

ACME導入へのハードル

- certbotの導入・設定
- DNS設定にかかる担当部署との調整
- 担当部局のスキルセット
- 担当者への技術伝達
- 予算サイクル
- 管理対象サーバの多様性
- 他…

→導入障壁となる課題は少ないとは言えない

UPKIからのご支援

- 文書整備
  - 導入・設定マニュアル
  - 学内へのご説明資料
  - 導入へのチェックリスト
- 技術情報の伝達
  - 技術セミナー実施
  - 動画コンテンツ（実際の画面や操作をいつでも視聴可能）
- 導入サポート
  - お問い合わせへの対応
  - FAQ整備

ACME導入に向けて

- 「ACME対応、どうやって機関内に展開していくといいのだろう？」
  - 証明書有効期間が100日間になるまでに、8割がACMEでの管理に移行するには？と仮に目標設定したスケジュール案
    - 必ずしもこの通りにすべきものではありません
    - 工数が許容できる範囲に収められるよう進めるのも一案です
  - 2025年10月から6ヶ月を1期として、3期構成
    - 事前準備：2025年10月～2026年3月（有効期間200日）
    - 段階的導入と評価：2026年4月～2026年9月
    - 本格展開と定着化：2026年10月～2027年3月（有効期間100日）

全体像

カテゴリ	実施内容	2025-10	2025-11	2025-12	2026-01	2026-02	2026-03	2026-04	2026-05	2026-06	2026-07	2026-08	2026-09	2026-10	2026-11	2026-12	2027-01	2027-02	2027-03
事前準備	プロジェクトキックオフ	■																	
	現状分析と要件定義	■	■																
	ACMEプロバイダ選定・検証		■	■															
	技術検証（PoC実施）			■	■	■													
	詳細導入計画策定と承認					■	■												
	関係者への説明会・研修準備						■												
段階的導入と評価	パイロット導入							■	■										
	サーバー管理者向け研修実施							■	■	■	■	■	■	■	■	■	■	■	■
	パイロット導入結果評価と計画見直し									■									
	段階的導入拡大										■	■	■						
	モニタリング体制の構築と運用開始										■	■	■	■	■	■	■	■	■
本格展開と定着化	全学的な本格展開													■	■	■	■	■	
	導入サポート体制の強化													■	■	■	■	■	■
	最終展開と目標達成（導入率80%達成）																		■
	運用体制の確立とドキュメント整備																■	■	■
	プロジェクト評価と報告																		■

事前準備

プロジェクトキックオフ	2025/10上旬	2025/10上旬
現状分析と要件定義	2025/10	2025/11
ACMEプロバイダ検証	2025/11	2025/12
技術検証（PoC実施）	2025/12	2026/02
詳細導入計画策定と承認	2026/02	2026/03
関係者への説明会・研修準備	2026/03	2026/03

ACME導入プロジェクトを本格的に開始するため、現状分析から技術検証、詳細な導入計画の策定と関係者への説明準備までを入念に行う段階

段階的導入と評価

パイロット導入	2026/04	2026/05
サーバー管理者向け研修実施	2026/04	(継続)
パイロット導入結果評価と計画見直し	2026/06	2026/06
段階的導入拡大	2026/07	2026/09
モニタリング体制の構築と運用開始	2026/07	(継続)

まずは一部のサーバーへ先行導入（パイロット導入）を行い、そこで得られた知見や評価を基に計画を見直しながら、着実に導入範囲を拡大していく段階

本格展開と定着化

全学的な本格展開	2026/10	2027/02
導入サポート体制の強化	2026/10	(継続)
最終展開と目標達成（導入率80%達成）	2027/03	2027/03
運用体制の確立とドキュメント整備	2027/01	2027/03
プロジェクト評価と報告	2027/03	2027/03

先行導入の結果を踏まえて全学的に展開を完了させ、サポート体制や運用ルールを整えることで、ACMEによる証明書管理を組織全体に定着させる最終段階

まとめ1：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。

まとめ2：計画と移行

- どのように導入を進めるのか？（計画と移行）
  - 3つのフェーズを設けた段階的な導入計画案（2025年10月～2027年3月）を提示しています。
    - 事前準備（～2026/3）: 現状分析、技術検証、計画策定
    - 段階的導入（～2026/9）: パイロット導入と評価、範囲の拡大
    - 本格展開（～2027/3）: 全学的な展開と運用の定着化
  - このようにしなければならない、というものではありません。機関の利用実態にあわせ、検討をお願いします。
- 従来のTSV申請方式も当面は維持しますので、ご安心ください。

まとめ3：UPKIからの支援

- 安心して導入を進めていただくために
  - ACME導入には技術的な課題などが想定されるため、UPKIは以下の支援を提供します。
    - 文書整備: 導入・設定マニュアル、学内向け説明資料、チェックリスト
    - 技術情報伝達: 技術セミナーの実施、動画コンテンツの提供
    - 導入サポート: FAQの整備、お問い合わせへの対応

- 引き続き、情報提供を進めて参ります。

ご連絡・お問い合わせ先

国立情報学研究所
学術基盤課 認証基盤・クラウド推進チーム（認証担当）

お問い合わせフォーム： https://certs.nii.ac.jp/contact/form

お問合せは、お問い合わせフォーム（Jira Service Management）で管理しております。お問い合わせフォームの利用についてご協力いただけますと幸いです。メールアドレス宛にいただいたお問合せは、Jira Service Managementに転送させていただく場合がありますので、ご了承ください。

原則、サービス利用機関または利用予定機関の機関責任者・登録担当者・経理担当者からお願いします。