UPKI電子証明書発行サービスにおける ACME導入について

金沢：11月14日(金) TKP金沢カンファレンスセンター
福岡：11月21日(金) JR博多シティ
札幌：12月12日(金) TKP札幌駅カンファレンスセンター
仙台：1月 8日(木)　東北大学サイバーサイエンスセンター

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
水元 明法

© 2025 National Institute of Informatics

自己紹介

- 名前
  - 水元 明法 (MIZUMOTO, Akinori)
- 所属
  - 国立情報学研究所(NII) 学術基盤研究員
- 出身地
  - 石川県
- 経歴
  - NII 学術支援技術専門員
  - 物質・材料研究機構(NIMS) NIMSエンジニア
    を経て現職
- 現在の活動
  - **UPKI電子証明書発行サービス**
  - 次世代認証連携（認証器レジストリ）
  - 学術認証フェデレーション 学認





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)	←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

【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:** 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

UPKI電子証明書発行サービスでの用語

- 登録担当者
  - UPKIが提供する「電子証明書自動発行支援システム」を操作して、以下の操作ができる者をさします
    - 電子証明書の発行・更新・失効とこれらにかかる審査
    - 関連情報の処理
    - 発行履歴の取得
- 利用管理者
  - 電子証明書の秘密鍵の管理・保管について責任を負う
  - 当該機関に所属する常勤の教職員である
  - 利用機関が電子証明書の管理を外部委託している場合は，外部委託された者

https://certs.nii.ac.jp/manual/regulations#_492

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

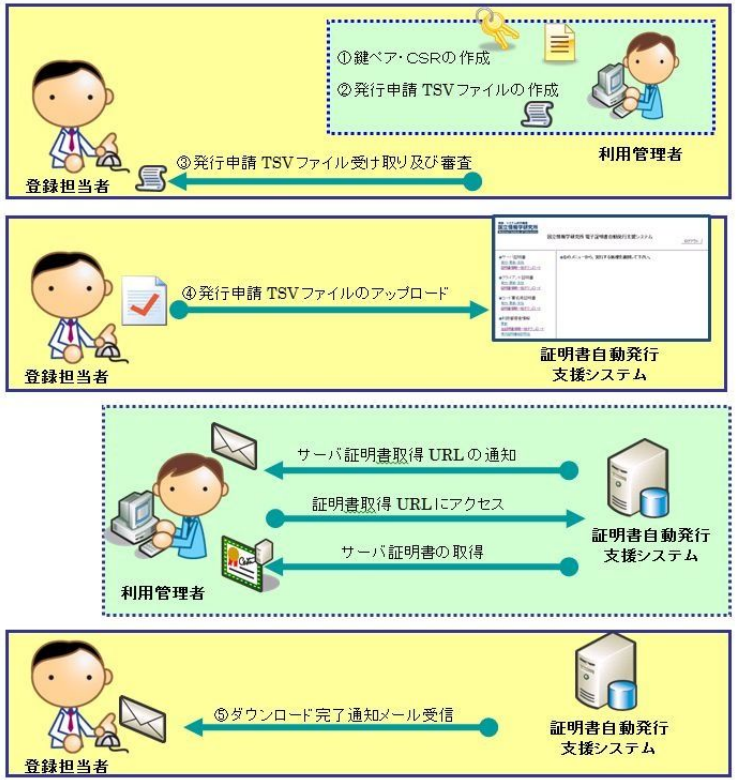
- **Certbot ＋ EAB Credential** での発行・更新・設定
- EAB(External Account Binding) Credential とは？
  - ACMEプロトコルにおいて、外部アカウントとACMEアカウントを紐付けるための認証情報のこと
    - ACMEを使って証明書を発行するために必要なアカウントを構成する情報
  - Key Identifier (KID)とHMAC Keyの組み合わせ
    - これで不正な利用を防ぎます
  - 利用管理者はEAB Credentialを用いて、UPKIのACMEサーバを利用して証明書発行・更新処理を行う
- 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



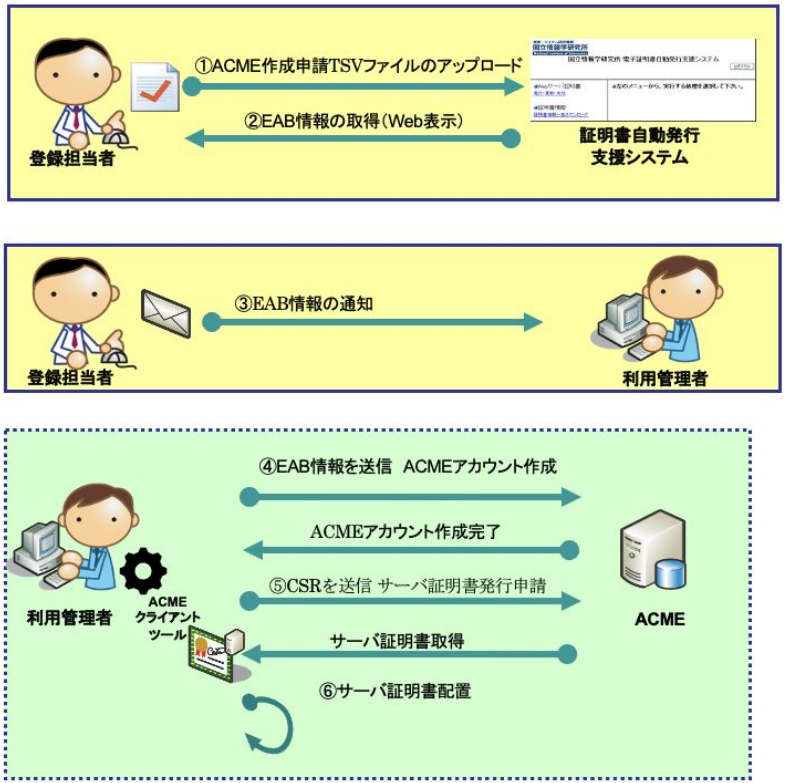
技術概要:登録担当者編

ワークフローの変化（新規発行時 1）

現行（CSRと申請用TSVファイル作成）



ACME（EAB Credential発行、CSR作成不要）



ワークフローの変化（新規発行時 2）

現行（CSRと申請用TSVファイル作成）	ACME（EAB Credential発行、CSR作成不要）
【利用管理者作業】	**【登録担当者作業】**
①サーバ証明書を申請する際に必要となる鍵ペア及びCSRの作成を行います。	①ACMEアカウント作成申請TSVファイルをアップロードします。
②サーバ証明書新規発行申請TSVファイルを作成します。TSVファイルに①で生成したCSRを貼り付けます。	② ACMEアカウントを利用するためのEAB Credentialを取得します（Web画面表示）。
【登録担当者作業】	③EAB Credential を利用管理者に通知します。
③サーバ証明書新規発行申請TSVファイルを利用管理者から受け取ります。	**【利用管理者作業】**
④サーバ証明書新規発行申請TSVファイルのアップロードを行ってください。	④EAB情報を送信し、ACMEアカウントと紐付けます。
【利用管理者作業】	⑤ACMEクライアントからサーバ証明書発行申請を行い、取得します。
サーバ証明書発行受付通知メール受信を受信します。	
サーバ証明書発行受付通知メールの情報を元に、利用管理者用証明書取得URLにアクセスします。	
サーバ証明書をダウンロードします。	
【登録担当者作業】	
⑤ダウンロード完了通知メールを受信します。	

EABクレデンシャル発行時に必要な情報

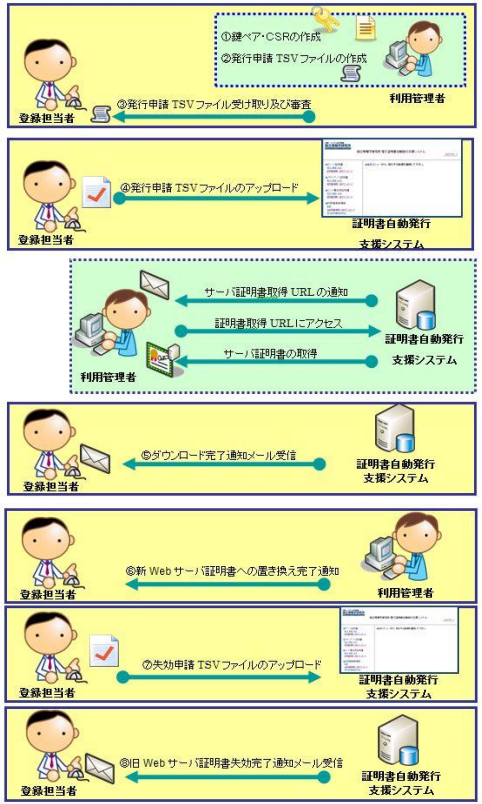
- 以下の項目をTSVファイルに記載して、電子証明書自動発行支援システムにアップロード
  - **主体者DN**
    - CN=test01.upki.jp, O=National Institute of Informatics, L=Chiyoda-ku, ST=Tokyo, C=JP
  - **証明書プロファイルID**
    - 3:サーバ証明書（sha256WithRSAEncryption）
    - 11:サーバ証明書（ecdsa-with-SHA384）
  - **利用管理者氏名**
    - MIZUMOTO, Akinori
  - **利用管理者所属**
    - 国立情報学研究所
  - **利用管理者メールアドレス**
    - mailaddress@upki.jp
  - **利用管理者FQDN**
    - test01.upki.jp
  - **利用管理者ソフトウェア名・バージョン**
    - Nginx 1.29.1
  - **dNSName**
    - dNSName=test01.upki.jp
- 詳しいフォーマットはマニュアルを参照

TSVファイル記載項目の比較（TSV/CSR発行とEAB Credential）

現行（CSRと申請用TSVファイル）	ACME（EAB Credential発行）
主体者DN	主体者DN
証明書プロファイルID	証明書プロファイルID
CSR	**（CSR不要）**
利用管理者氏名	利用管理者氏名
利用管理者所属	利用管理者所属
利用管理者mail	利用管理者mail
利用管理者FQDN	利用管理者FQDN
利用管理者ソフトウェア名・バージョン	利用管理者ソフトウェア名・バージョン
dNSName	dNSName

ワークフローの変化（更新発行時）

現行（CSRと申請用TSVファイル作成）



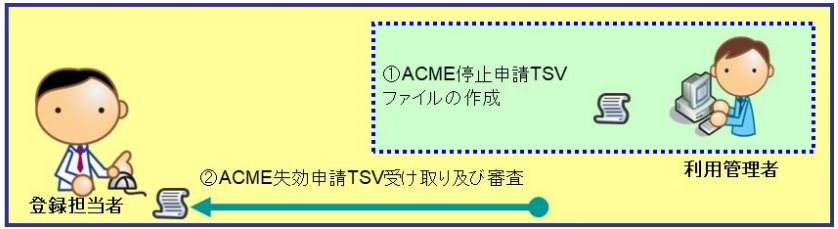
ACME

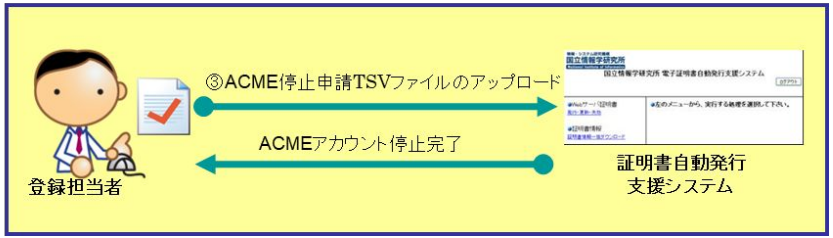


- 更新用のコマンドを実行
  - # certbot renew
- またはcronで自動実行（Nginxでの例）
  - 0 5 * * * certbot renew --quiet --deploy-hook "systemctl reload nginx"
  - 残りの有効期間（2/3経過後）に基づいて更新フローの実行要否が判断される
- EAB Credential が失効されている場合は更新不可
- 発行済みの証明書は登録担当者の操作で失効可

ワークフローの変化（EAB Credential の失効）

- 現行のTSV発行形式では当該サーバ証明書の失効のみでよかった
- ACMEにて自動更新を設定している場合、失効しても新たにまた更新発行されてしまう
- **EAB Credential 自体の停止も必要**





登録担当者用マニュアル

- ACMEプロトコルによる認証情報管理手順（登録担当者向け）
  - 1-1.ACMEプロトコル認証情報登録
    - 新規にEAB Credentialの登録を必要とする場合
    - サーバ証明書の記載内容（主体者DN）を変更する場合
  - 1-2.ACMEプロトコル認証情報更新
    - 登録済みのEAB Credentialの利用者変更を必要とする場合
    - サーバ管理者を変更する場合
  - 1-3.ACMEプロトコル認証情報停止
    - EAB Credentialの停止を必要とする場合
  - 1-4.ACMEプロトコル情報一括ダウンロード
    - 登録済みのEAB Credentialに関する諸情報の取得（全件）を必要とする場合

TSVツール

- TSV作成ツール ACME対応アップデート版提供中
  - https://certs.nii.ac.jp/tsv-tool/
- TSVツール操作手順書
  - オンラインマニュアルを提供中
  - EAB Credentialの新規・更新・停止申請用TSVファイル
  - ACMEで発行した証明書の失効申請用TSVファイル
    - 既存の証明書の失効申請用TSVファイルと同じ
    - ACMEプロトコルでの失効は可能だが、登録担当者の操作でも証明書失効が必要なケースがある



技術概要：利用管理者（サーバ管理者）編

利用管理者（サーバ管理者）用マニュアル

- ACMEクライアントツールによるサーバ証明書管理手順（利用管理者向け）
  - 1-1.サーバ証明書の新規申請手続き
    - 新規にサーバ証明書を発行する場合
    - サーバ証明書の記載内容（主体者DN）を変更する場合
  - 1-2.サーバ証明書の更新申請手続き
    - サーバ証明書の(主体者DN以外の)記載内容を変更する場合
    - 有効期限内の証明書を継続利用したい場合
    - 有効期限の切れた証明書を継続利用したい場合
    - 有効期限の切れた証明書を継続利用したい場合
  - 1-3.サーバ証明書の失効申請手続き
    - サーバ証明書が不要になった場合や秘密鍵が危殆化した場合

利用可能なACME「チャレンジ」

- UPKIでは、ACMEでの証明書発行時に以下の2つの「チャレンジ（ドメイン所有権確認の方法）」を選択できます
  - **HTTP-01チャレンジ**
    - 通常のWebサイトでは HTTP-01チャレンジ が**簡単でおすすめ**です
    - が、ネットワーク・サーバ構成上、選択できないこともあります
  - **DNS-01チャレンジ**
    - Webサーバーを外部に公開できない場合は DNS-01チャレンジ を選択してください

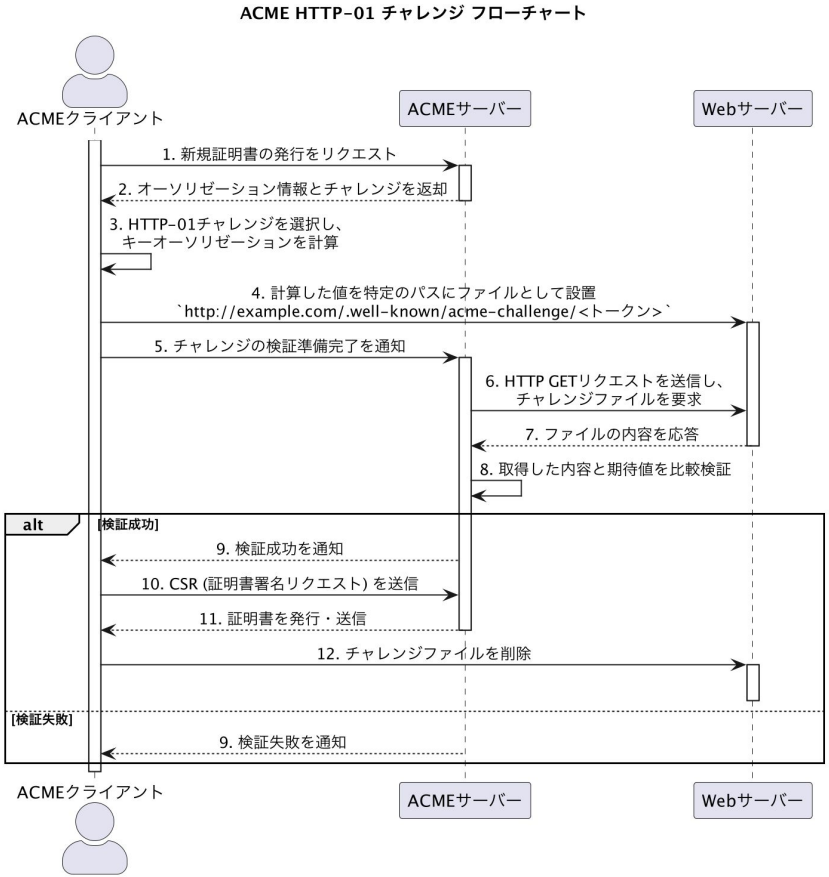
HTTP-01チャレンジ（1）

- **仕組み:**
  - 認証局（CA）は、指定されたトークン（ランダムな文字列）をWebサーバーの特定のURLパス（/.well-known/acme-challenge/）に設置するよう要求します
  - CAはそのURLにHTTPでアクセスし、トークンが正しく配置されていることを確認してドメインの所有権を検証します
- **要件:**
  - 証明書発行対象がWebサーバーを指している必要があります
  - 外部からHTTP（ポート80）でサーバーにアクセスできる必要があります
    - ポート80からポート443へのリダイレクトを許容します
- **メリット:**
  - 設定が比較的簡単で、多くのACMEクライアントが自動化に対応しています
  - 特別な権限（DNSの編集権限など）が不要です
- **デメリット:**
  - Webサーバーが公開されていない環境（開発環境や内部ネットワークなど）では利用できません

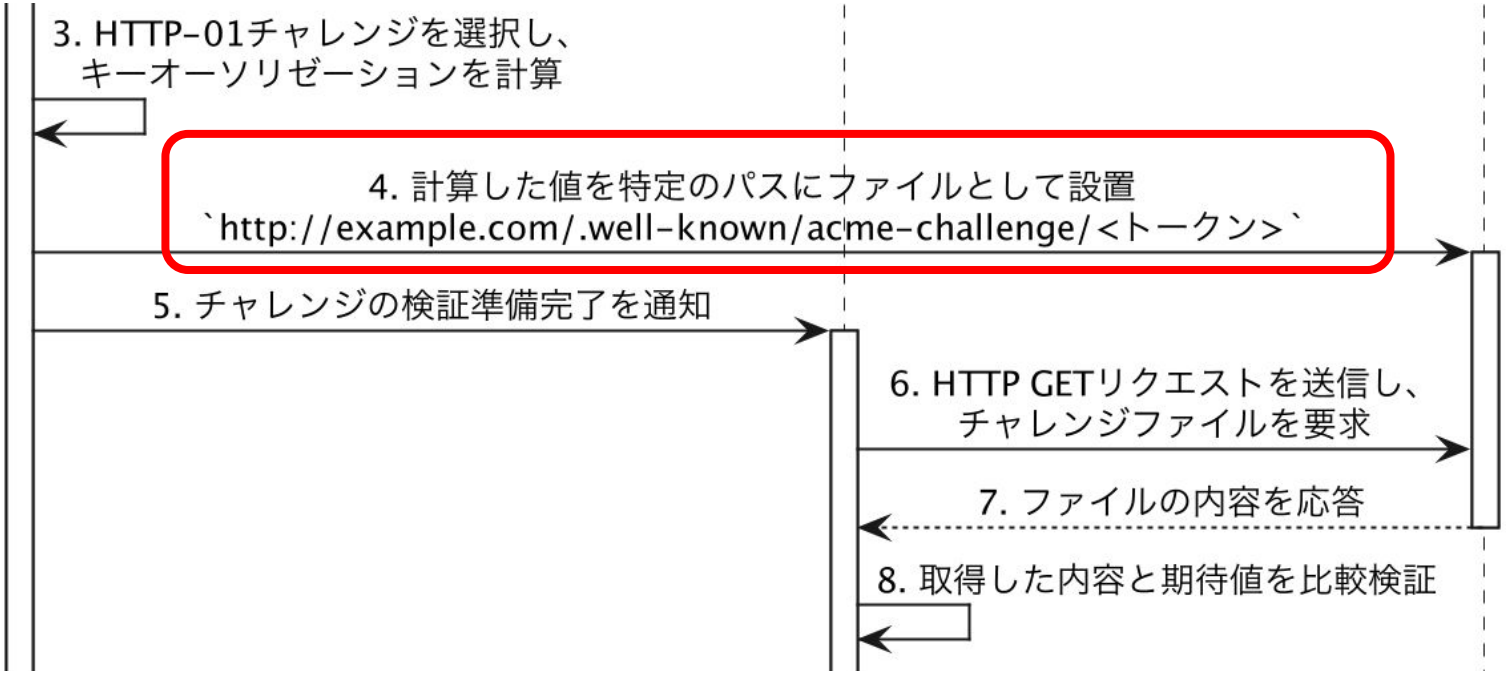
HTTP-01チャレンジ(2)

- **チャレンジ成功のキャッシュ:**
  - 30日間キャッシュされる
  - 発行直後に強制的に更新発行した場合など、再チャレンジが省略される場合がある
  - 関連する条件が変更された場合、再チャレンジが必要になる
    - EAB Credentialの変更
    - サーバの変更
    - 認証局側でキャッシュが強制無効化された場合
    - SANsの値が変更された場合

HTTP-01チャレンジ フローチャート



HTTP-01チャレンジ フローチャート



※実際にはcertbotが自動処理します

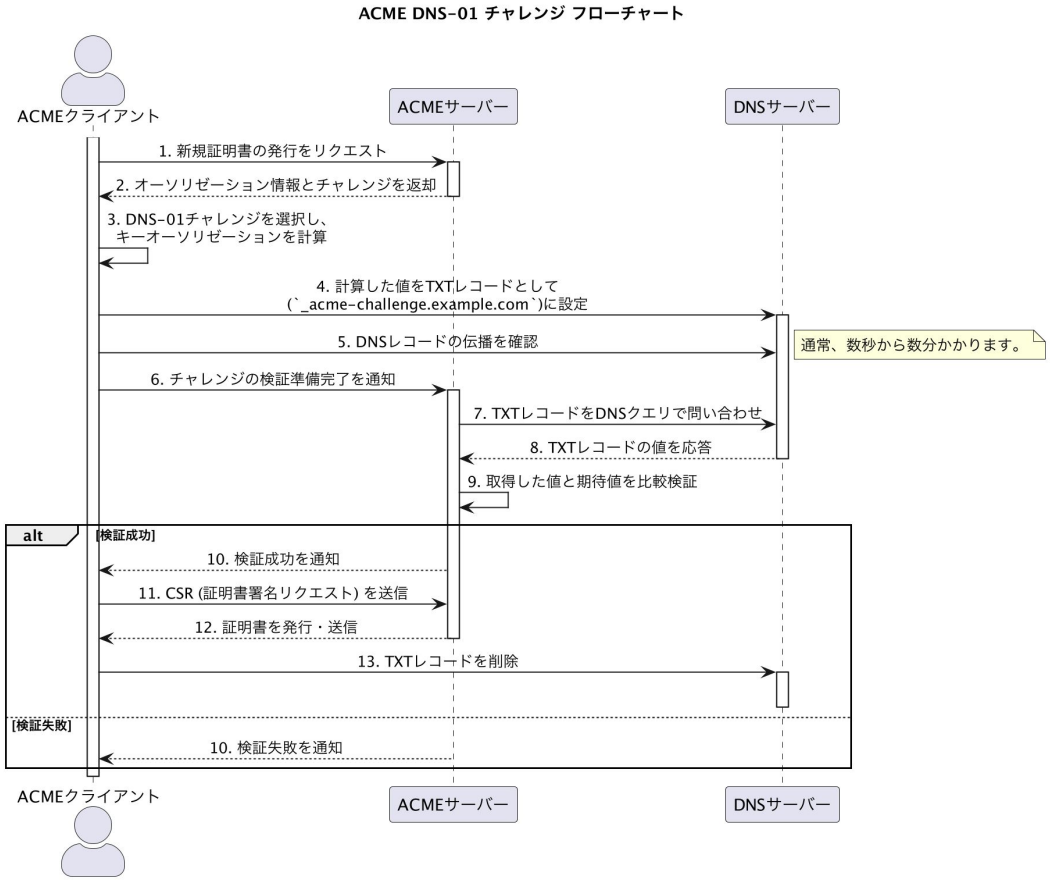
DNS-01チャレンジ（1）

- **仕組み:**
  - 認証局（CA）が、指定されたトークンをドメインのDNSレコード（具体的にはTXTレコード）に設定するよう要求します
  - CAはDNSに問い合わせを行い、指定されたTXTレコードが存在することを確認してドメインの所有権を検証します
- **要件:**
  - DNSレコードをAPIなどを通じてプログラムで編集できる必要があります
  - 手動対応は不可ではないのですが、非常に煩雑です
- **メリット:**
  - Webサーバーを外部に公開する必要がなく、HTTPサーバーが稼働していなくても証明書を取得できます
  - ファイアウォールの内側にあるサーバーでも利用可能です
- **デメリット:**
  - DNSプロバイダがAPIに対応している必要があり、設定がHTTP-01に比べて複雑になる場合があります
  - DNSの変更がインターネットに反映されるまでに少し時間がかかることがあります

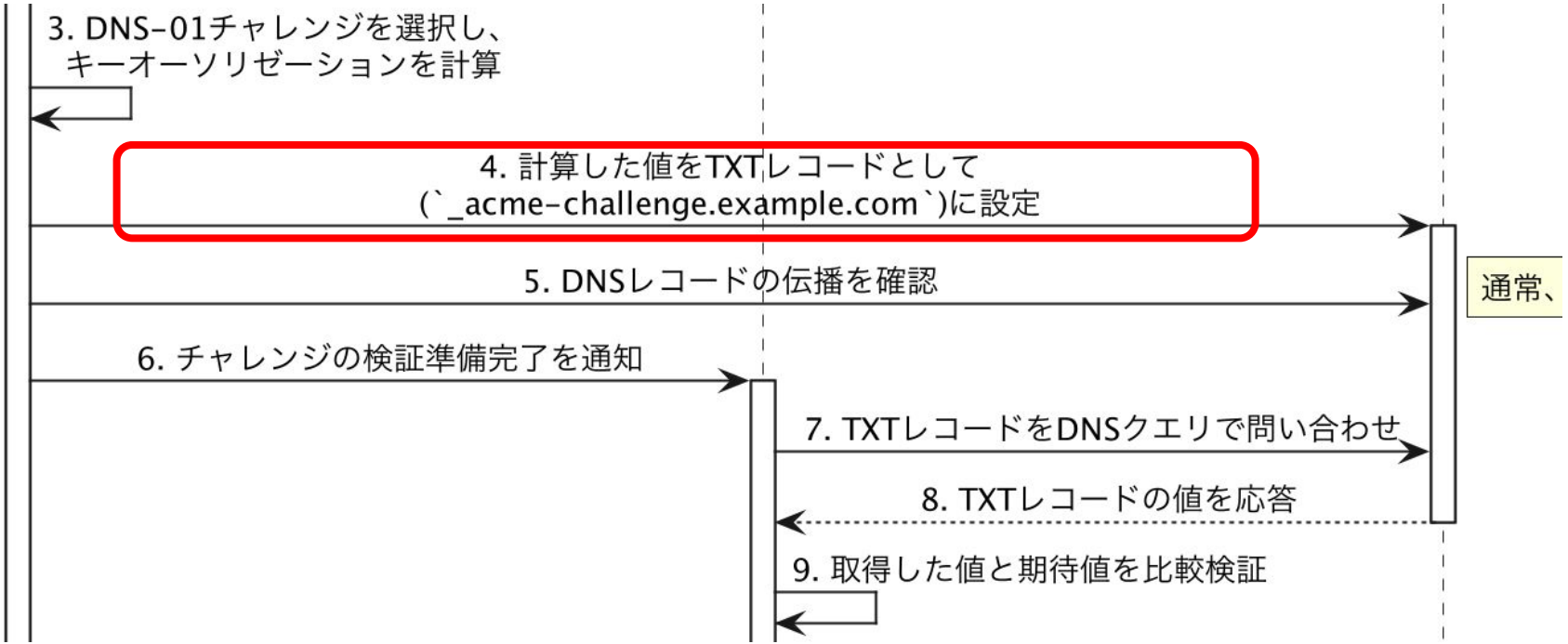
DNS-01チャレンジ(2)

- **指定すべきTXTレコードの有効期間:**
  - TXTレコードに指定すべき値は、作成から7日間有効
- **チャレンジ成功のキャッシュ:**
  - 30日間キャッシュされ、再チャレンジが省略される場合がある
  - 関連する条件が変更された場合、再チャレンジが必要になる
    - EAB Credentialの変更
    - サーバの変更
    - 認証局側でキャッシュが強制無効化された場合
    - SANsの値が変更された場合

DNS-01チャレンジ フローチャート



DNS-01チャレンジ フローチャート



※DNSの設定は、手動もしくはcertbotの対応プラグイン利用が必要です。

EAB Credential 設定コマンド例

```
certbot register \
--eab-kid 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx' \
--eab-hmac-key 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxXXXXXXX' \
--server 'https://secomtrust-acme.com/acme/'
```

※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

サーバ証明書発行用コマンド例

```
certbot run \
--nginx \
-d xxxx.test.com \
--key-type rsa \
--server 'https://secomtrust-acme.com/acme'
```

※ --server オプションでACMEサーバの指定必須

EAB Credential設定と証明書発行を1行で

```
certbot --server https://secomtrust-acme.com/acme/ \
--eab-hmac-key xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx \
--eab-kid xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx \
-d test01.upki.jp \
--key-type rsa
```

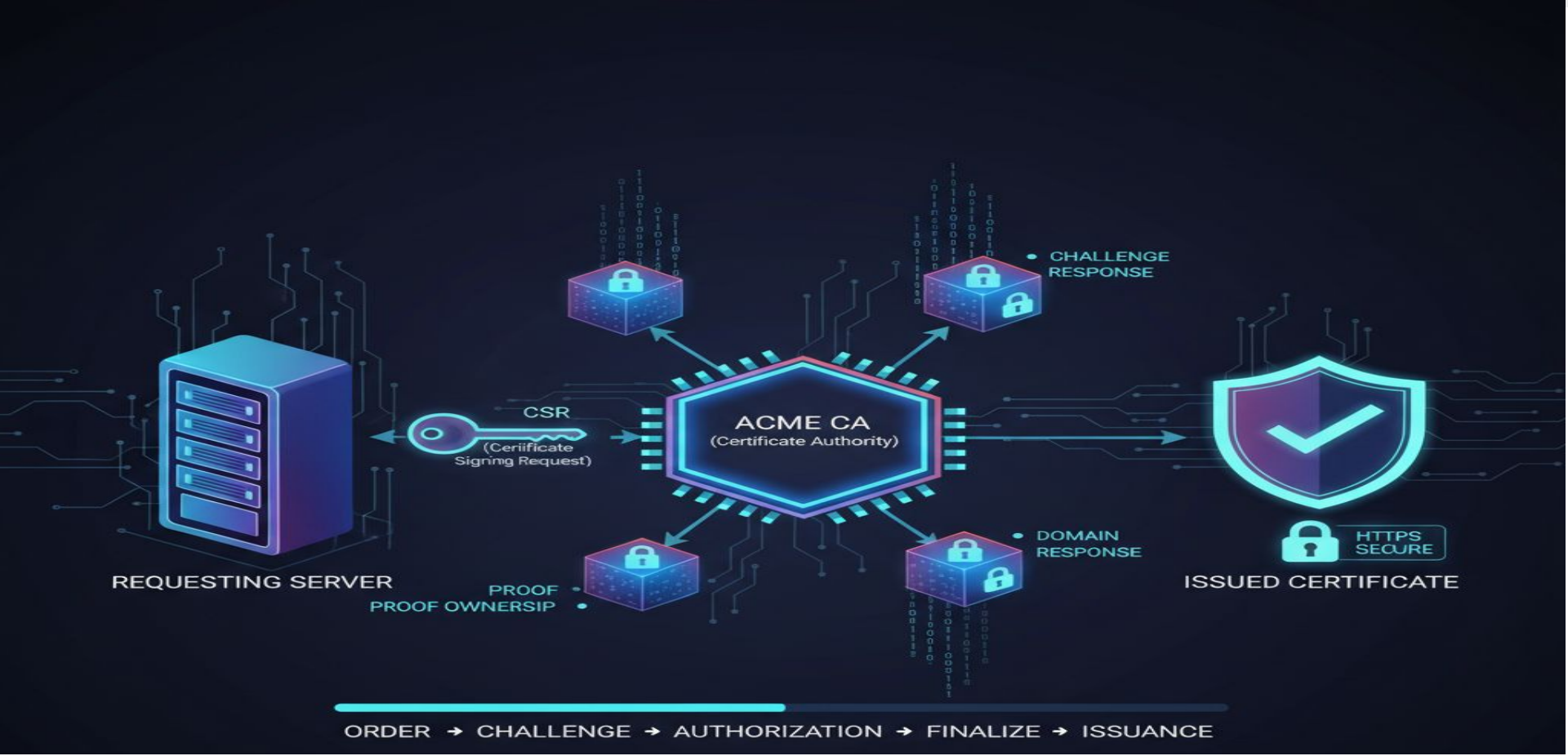
監視

- 証明書の残有効期間を監視し、更新が正しく動作しているか確認する必要がある
- よく使われるものを例示します

名称	備考
AWS CloudWatch	ACMまたはLambda関数で有効期限情報を取得し、CloudWatchアラームを設定
GCP Cloud Monitoring	Uptime CheckでSSL検証を有効にし、アラートポリシーを策定して通知を受け取る
Azure Monitor	Key Vaultが生成するイベントをAzure Monitorなどで補足して処理
Zabbix	有効期限を出力するスクリプトを作成し、エージェントから値を取得して処理
Red Sift	Webサービス、Let's Encrypt推奨、無償利用の上限あり

補足事項

- 2025年10月30日から先行利用開始
- 2026年3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3月から、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



ACMEによる証明書発行の詳細（HTTP-01チャレンジ）

前提条件

- HTTP-01チャレンジを使用する場合、サーバの80番ポートが利用可能である
- 外部の複数拠点（5つ）から、当該サーバ証明書発行対象のFQDNがDNSで名前解決出来ること
- certbot 4.0.0 を利用する
- 登録担当者から、当該証明書に紐付けたEAB Credentialが発行され、それを受領済みである
- 当該サーバにSSHでアクセス可能である
- 当該サーバはWebサーバとして利用予定のものであり、80番ポートと443番ポートが利用可能である
- 当該サーバはインターネット側からアクセス可能である

環境：OSの詳細

```
$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 13 (trixie)"
NAME="Debian GNU/Linux"
VERSION_ID="13"
VERSION="13 (trixie)"
VERSION_CODENAME=trixie
DEBIAN_VERSION_FULL=13.1
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

環境構築

```
$ sudo apt update && sudo apt upgrade #パッケージマネージャ更新
$ sudo apt install nginx certbot python3-certbot-nginx # nginx、certbot、プラグインをインストール
```

ACMEによる証明書取得

```
sudo certbot --server https://secomtrust-acme.com/acme/ \ #ACMEサーバ指定
--eab-hmac-key XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX \ # EAB Credential
--eab-kid XXXXXXXXXX \ # EAB Credential
-d test07.upki.jp \ # 証明書発行対象の主体者DN
--nginx # certbot プラグインを指定して、自動設定を行う
```

- プラグインの指定で自動設定が可能(リロード含む)
- --key-type オプションを省略した場合、ECDSAが優先される
  - EAB Credential発行時に指定した証明書プロファイルIDにあわせて指定する
    - 3:サーバ証明書(sha256WithRSAEncryption)
    - 11:サーバ証明書(ecdsa-with-SHA384)

証明書確認

```
$ openssl s_client -connect test07.upki.jp:443 -showcerts
Connecting to 18.181.152.206
CONNECTED(00000003)
depth=2 C=JP, O=SECOM Trust Systems CO.,LTD., CN=Security Communication ECC RootCA1
verify return:1
depth=1 C=JP, O=SECOM Trust Systems CO.,LTD., CN=NII Open Domain CA - G7 ECC
verify return:1
depth=0 C=JP, ST=Tokyo, C=JP, L=Chiyoda-ku, O=National Institute of Informatics,
CN=test07.upki.jp
verify return:1
---
略
```

更新動作確認

```
$ sudo certbot renew --dry-run
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Processing /etc/letsencrypt/renewal/test07.upki.jp.conf
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Account registered.
Simulating renewal of an existing certificate for test07.upki.jp

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations, all simulated renewals succeeded:
  /etc/letsencrypt/live/test07.upki.jp/fullchain.pem (success)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

- --dry-run オプションは、証明書を実際に更新しないが、更新のプロセスをシミュレートして確認する

自動更新確認（systemdタイマーの確認）

```
$ sudo systemctl list-timers | grep certbot
Fri 2025-10-17 19:29:44 UTC 8h - - certbot.timer certbot.service
```

- certbotをインストールすると、自動でsystemdタイマーが設定される
- 自動更新の設定が内包される（後述）

systemdによる更新設定ファイルの所在

```
$ sudo ls -l /usr/lib/systemd/system | grep certbot
-rw-r--r-- 1 root root  243 Apr 16  2023 certbot.service
-rw-r--r-- 1 root root  156 May 26  2018 certbot.timer
```

- 自動で設置されるので、有無を確認するだけでよい

更新設定ファイルの中身 certbot.service

```
$ sudo cat /usr/lib/systemd/system/certbot.service
[Unit]
Description=Certbot
Documentation=file:///usr/share/doc/python-certbot-doc/html/index.html
Documentation=https://certbot.eff.org/docs
[Service]
Type=oneshot
ExecStart=/usr/bin/certbot -q renew --no-random-sleep-on-renew
PrivateTmp=true
```

- **ExecStart** ：実行するコマンド
- **-q** ：不要なログ抑制
- **renew --no-random-sleep-on-renew** ：certbotはrenew実行時にランダムに数分待機する。systemdのタイマーでの分散設定をしているので、不要として待機しない。

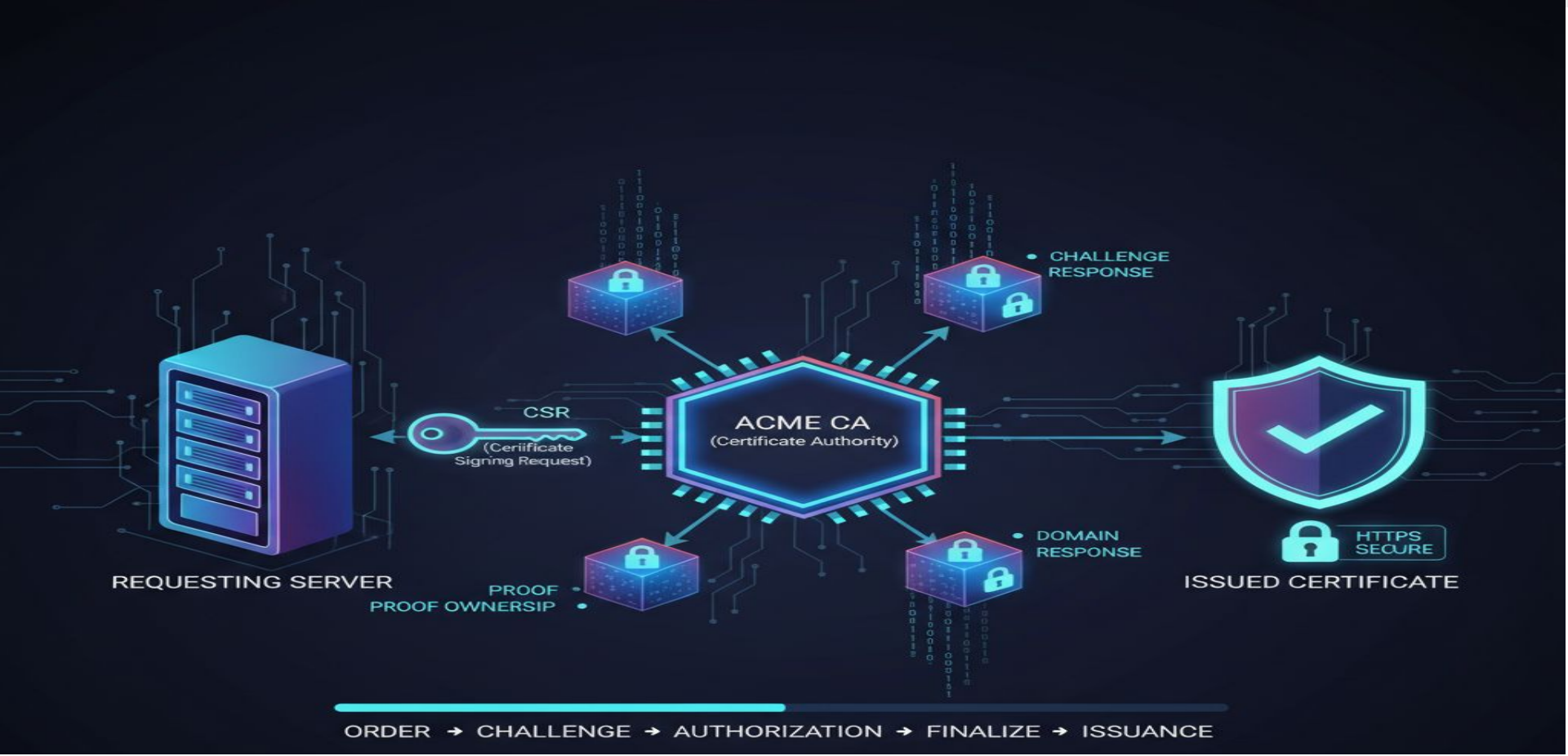
更新設定ファイルの中身 certbot.timer

```
$ sudo cat /usr/lib/systemd/system/certbot.timer
[Unit]
Description=Run certbot twice daily

[Timer]
OnCalendar=*-*-* 00,12:00:00
RandomizedDelaySec=43200
Persistent=true

[Install]
WantedBy=timers.target
```

- **OnCalendar=*-*-* 00,12:00:00**　：毎日0時と12時に実行
- **RandomizedDelaySec=43200**　：それぞれ12時間以内のディレイを設定
- **Persistent=true**　：実行時にシステムが停止していた場合、起動時に1回実行



ACMEによる証明書発行の詳細（DNS-01チャレンジ）

前提条件

- 外部の複数拠点（5つ）から、当該サーバ証明書発行対象のFQDNがDNSで名前解決出来ること
- certbot 4.0.0 を利用する
- 登録担当者から、当該証明書に紐付けたEAB Credentialが発行され、それを受領済みである
- 当該サーバにSSHでアクセス可能である
- 証明書発行対象に関わる、DNS-01チャレンジで使用するDNSレコードを更新する権限を持っている
- 当該サーバはインターネット側と通信可能である

環境の前準備

```
$ sudo apt install ufw
$ sudo ufw status
Status: inactive

$ sudo ufw allow 22/tcp
Rules updated
Rules updated (v6)

$ sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)

$ sudo ufw deny 80/tcp
Rules updated
Rules updated (v6)
```

- SSH(22)を許可
- https(443)を許可
- http(80)を**不許可**

環境の前準備—設定確認

```
$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup

$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
443/tcp                    ALLOW IN    Anywhere
80/tcp                     DENY IN     Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
443/tcp (v6)               ALLOW IN    Anywhere (v6)
80/tcp (v6)                DENY IN     Anywhere (v6)
```

HTTP-01チャレンジに失敗

```
$ sudo certbot \
--server https://secomtrust-acme.com/acme/ \
--eab-hmac-key XXXXXXXXXX \
--eab-kid XXXXX \
-d test001.upki.jp \
--key-type rsa --nginx

#略

Certbot failed to authenticate some domains (authenticator: nginx). The Certificate
Authority reported these problems:
  Domain: test001.upki.jp
  Type:   malformed
  Detail: DCVチャレンジに失敗しました。[HTTP-01のチャレンジ検証に失敗。HTTPステータス: 504, URL
(HTTP/HTTPS): http://test001.upki.jp/.well-known/acme-
challenge/YRGu2HEFqIsG8du8y3T7uYl74Ee1gYonPnL9uth8XpQ]

Hint: The Certificate Authority failed to verify the temporary nginx configuration
changes made by Certbot. Ensure the listed domains point to this nginx server and that it
is accessible from the internet.

Some challenges have failed.
Ask for help or search for solutions at https://community.letsencrypt.org. See the
logfile /var/log/letsencrypt/letsencrypt.log or re-run Certbot with -v for more details.
```

DNS-01チャレンジで証明書を取得(1)

```
$ sudo certbot certonly \
--server https://secomtrust-acme.com/acme/ \
--eab-hmac-key xxxxxxxxxx \
--eab-kid xxxxx \
-d test001.upki.jp \
--key-type rsa \
--preferred-challenges dns \
--manual

Saving debug log to /var/log/letsencrypt/letsencrypt.log
Requesting a certificate for test001.upki.jp
```

DNS-01チャレンジで証明書を取得(2)

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name:

_acme-challenge.test001.upki.jp.

with the following value:

MA2Mf6MKVFNkz_vP1msW7gx4CKfP2PImCrSGI7h1S3w

Before continuing, verify the TXT record has been deployed. Depending on the DNS
provider, this may take some time, from a few seconds to multiple minutes. You can
check if it has finished deploying with aid of online tools, such as the Google
Admin Toolbox: https://toolbox.googleapps.com/apps/dig/#TXT/_acme-
challenge.test001.upki.jp.
Look for one or more bolded line(s) below the line ';ANSWER'. It should show the
value(s) you've just added.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
```

DNSレコードを更新（Route 53の例）



DNSレコードを確認（別ウインドウのターミナル）

```
% dig TXT _acme-challenge.test001.upki.jp

; <<>> DiG 9.10.6 <<>> TXT _acme-challenge.test001.upki.jp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37341
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1424
;; QUESTION SECTION:
;_acme-challenge.test001.upki.jp. IN    TXT

;; ANSWER SECTION:
_acme-challenge.test001.upki.jp. 300 IN TXT "MA2Mf6MKVFNkz_vP1msW7gx4CKfP2PImCrSGI7h1S3w"

;; Query time: 38 msec
;; SERVER: 136.187.41.216#53(136.187.41.216)
;; WHEN: Thu Nov 13 14:47:56 JST 2025
;; MSG SIZE  rcvd: 116
```

DNS-01チャレンジで証明書を取得(3)

```
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/test001.upki.jp/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/test001.upki.jp/privkey.pem
This certificate expires on 2026-02-10.
These files will be updated when the certificate renews.

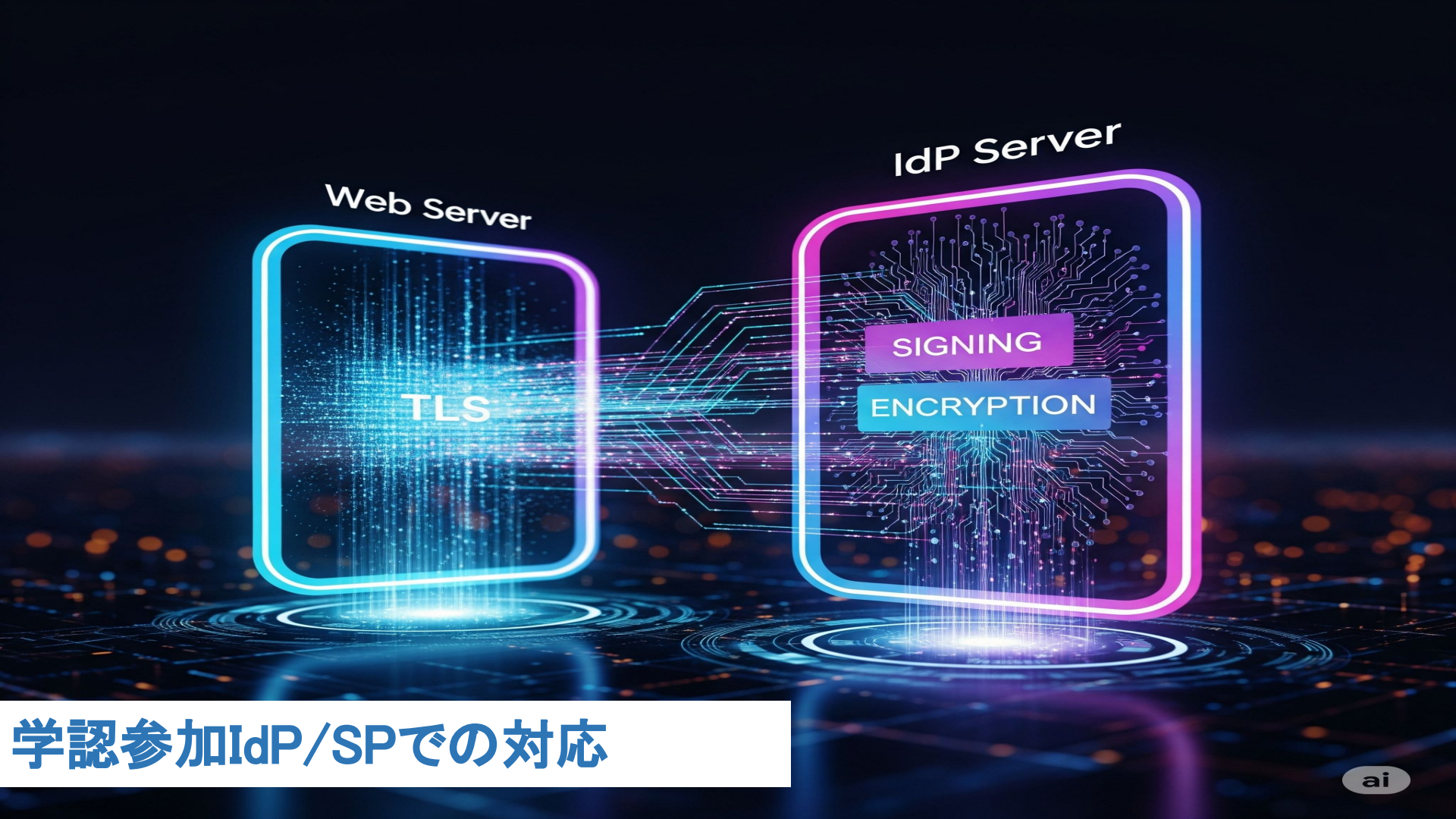
NEXT STEPS:
- This certificate will not be renewed automatically. Autorenewal of --manual
certificates requires the use of an authentication hook script (--manual-auth-hook) but
one was not provided. To renew this certificate, repeat this same certbot command before
the certificate's expiry date.
```

取得した証明書を確認

```
$ sudo openssl x509 -noout -subject -dates -in
/etc/letsencrypt/live/test001.upki.jp/fullchain.pem
subject=C=JP, ST=Tokyo, C=JP, L=Chiyoda-ku, O=National Institute of Informatics,
CN=test001.upki.jp
notBefore=Nov 13 05:39:24 2025 GMT
notAfter=Feb 10 05:39:22 2026 GMT
```

DNS-01チャレンジ使用時に更新を自動化したい場合

- 使用しているDNSがAPI提供していることが必須
  - DNSプロバイダあるいは開発元などで確認
- よく使われるもの（Certbotチーム公式）
  - certbot-dns-route53
    - 対象サービス: Amazon Web Services (AWS) の Route 53
  - certbot-dns-cloudflare
    - 対象サービス: Cloudflare
  - certbot-dns-google
    - 対象サービス: Google Cloud DNS
  - certbot-dns-digitalocean
    - 対象サービス: DigitalOcean
  - certbot-dns-linode
    - 対象サービス: Linode
- 非公式
  - certbot-dns-azure
    - 対象サービス: Azure DNS



学認参加IdP/SPでの対応

2つの証明書

- Webサーバ用（Apache, nginxなど）
  - ブラウザで検証するため、有効期間短縮の影響を受ける
  - ACMEで更新を自動化するのが現実的
- SAMLメタデータ用（IdP, SP）
  - 高頻度で証明書を発行して学認申請システムから変更申請を行うのは非現実的
    - 現状、自動化は難しく、失敗時のリスクが大きい
  - 自己署名証明書への移行を検討してください
    - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=159744061
    - なお、技術運用基準において以下の通り定めています
      - 失効した証明書は使用すべきではない。
      - また、証明書は3年を目処に定期的に更新すべきである。

自己署名証明書の作り方（例）

```
> openssl version
OpenSSL 3.5.4 30 Sep 2025 (Library: OpenSSL 3.5.4 30 Sep 2025)

> openssl genrsa -out server.key 2048

> openssl req -new -x509 -nodes -key server.key -out server.crt -days 3650 -subj
"/C=JP/ST=Tokyo/L=Chiyoda-ku/O=GakuNin/CN=self.signed.certificate.gakunin.jp"

> openssl x509 -issuer -subject -dates -noout -in server.crt
issuer=C=JP, ST=Tokyo, L=Chiyoda-ku, O=GakuNin, CN=self.signed.certificate.gakunin.jp
subject=C=JP, ST=Tokyo, L=Chiyoda-ku, O=GakuNin, CN=self.signed.certificate.gakunin.jp
notBefore=Oct  3 10:09:52 2025 GMT
notAfter=Oct  1 10:09:52 2035 GMT
```



お知らせ

中間CAおよびルートCAの変更について（1）

- **2025年12月17日** より、RSAのサーバ証明書を発行する中間CAが新しいルートCA配下のものに変更されます
- **2026年1月20日** より、S/MIME証明書を発行する中間CAが新しいルートCA配下のものに変更されます

	RSA証明書	S/MIME証明書
変更適用日	**2025年12月17日**	**2026年1月20日**
新・中間CA	NII Open Domain CA - G8 RSA	SECOM Passport for PublicID SMIME RSA CA 2024
新・ルートCA	SECOM TLS RSA Root CA 2024 （RSAのサーバ証明書専用の新設ルートCA）	SECOM SMIME RSA Root CA 2024 （S/MIME証明書専用の新設ルートCA）
信頼性担保	新ルートCAは、各プラットフォームでの導入状況を鑑み、現行のルートCA「**Security Communication RootCA2**」によるクロスルート署名を施したものが提供されます。	

中間CAおよびルートCAの変更について(2)

- 変更適用日以降に発行した証明書をインストールする場合は、新しい中間CA証明書のインストールも忘れずに実施してください
  - ACMEプロトコルをご利用の場合は、自動で正しい中間CA証明書が取得されます
- 現在、ご利用中の各中間CAから発行された証明書(サーバ証明書、S/MIME証明書)は、**今回の変更による影響を受けません**
  - 証明書に記載された有効期限まで引き続き有効であり、強制的に失効されることはありませんのでご安心ください

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

まとめ：今後の対応とお願い

背景:なぜ今、対応が必要か？

TLSサーバ証明書の有効期間短縮

- CA/Browser Forumの決定により、サーバ証明書の最大有効期間が398日から段階的に短縮され、2029年3月15日以降は47日となります 。

手動管理の限界

- 更新頻度が年8回以上となり、手動での証明書管理は更新忘れやミスによるサービス停止リスクの増大を招き、事実上不可能になります 。

UPKIの対応：証明書管理の自動化

ACMEプロトコルの導入

- 有効期間短縮に対応するため、証明書の発行・更新を自動化するACMEプロトコルを導入します 。
- 推奨ツールとして`certbot`の利用を想定しています 。

安全な利用のための仕組み

- 不正利用を防止するため、EAB (External Account Binding) Credentialによる認証を導入し、セキュリティを確保します 。

既存発行形態の維持

- ACME非対応の環境も考慮し、従来のTSVファイルによる申請も当面は維持します 。

今後のアクション：計画的な移行のお願い

ACMEへの移行計画の策定

- 管理下のサーバや機器がACMEに対応可能か確認し、自動化への移行計画を立ててください。
- 非対応環境については、代替策をご検討いただくとともに、情報提供をお願いします。
  a. 件数あるいは影響度が高いものについては、UPKIで手順を調査してドキュメント提供したいと考えております

先行利用の検討

- 2025年10月より先行利用を開始しました 。ぜひ早期の試行をご検討ください。

重要なお知らせ：サービス利用料金の改定について

機能強化に伴う料金改定

- ACME導入をはじめとする継続的なサービス改善と安定運用のため、大変恐縮ながら利用料金の改定をお願いする次第です。

改定時期

- 令和8年度（2026年度）からの適用を予定しております。

ご理解ご協力のお願い

- 今後もセキュアなウェブ環境を維持するため、何卒ご理解ご協力のほどお願い申し上げます。

ご質問・コメントをお願いします

- お時間まで、質疑応答の時間とさせてください。