UPKI サーバー証明書の自動更新対応に向けた運用検証と考察

○尾形かおり[A)]，永井謙芝[B)]，伊勢谷陽一[C)]

[A,B,C)]北海道大学 学術情報部 情報企画課 ICT 運用・支援グループ 情報セキュリティ担当

1. はじめに

本学では、国立情報学研究所（NII）が提供する UPKI 証明書発行サービスと包括契約を締結しており、hokudai.ac.jpドメインに属するサーバーに対して、利用管理者の金銭的負担なくサーバー証明書を発行できる体制を整えている。筆者は本サービスの登録担当として、申請に基づく証明書の発行・更新・変更・失効等の手続きを担っている。

SSL/TLS サーバー証明書は、通信の暗号化と安全性を担保する上で不可欠であり、特にウェブサイト閲覧時においては、証明書の有無がアクセス可否に直結する重要な要素である。2025 年 4 月 11 日に、国際的業界団体である CA/Browser Forum では、SSL/TLS サーバー証明書の最大有効期間を現在の 398 日から段階的に短縮することが可決された(表 1 参照)。これにより、証明書の更新頻度は年 1 回程度から、年 8 回以上に増加する見込みである。

この動向を受け、NII は 2025 年 6 月 18 日のオープンフォーラムにおいて、UPKI 証明書発行サービスにおいても証明書の自動発行・自動更新に対応する方針を発表した(参考文献[1])。本論文では、この変更に伴う本学の運用上の影響について、検証結果を踏まえながら課題と対応策について考察する。

日程	有効期間
2026 年 3 月 15 日以降	最大 200 日
2027 年 3 月 15 日以降	最大 100 日
2029 年 3 月 15 日以降	最大 47 日

表 1. 有効期間の短縮スケジュール

2. 現行の取得・更新における課題

現行の UPKI サーバー証明書の運用には、複数の課題が内在している。まず、申請から発行・インストールに至るまでの各工程は、利用管理者による手動作業を前提としており、申請内容の確認は登録担当者が一件ずつ目視で行っている。この作業は時間を要するうえ、各工程に不備があった場合には、利用管理者による再作業と再提出が必要となる。特に、鍵の生成や CSR ファイルの作成、TSV 形式でのファイル提出など、技術的な知識を要する作業が含まれており、利用管理者にとっては大きな負担となっている。

また、証明書の更新は手動で行われるため、利用管理者の異動や引継ぎが不十分な場合には、更新が漏れるリスクがある。実際に、更新が間に合わず、サーバーが一時的に利用不能となった事例もあり、学内サービスの継続性に影響が懸念される。

さらに、利用管理者の IT スキルにばらつきがあることから、証明書更新関連の作業を外部業者に委託するケースも見られる。この場合、更新の度に追加の費用が発生する可能性があり、コスト面でも課題が残る。

加えて、今後は年 8 回以上の更新が必要となる見込みであり、現行の手動運用では対応が困難となることが予想され、証明書の取得・更新プロセスの自動化は、今後の運用における喫緊の課題となっている。

3. 新しい取得・更新方法

NII オープンフォーラムにて発表された UPKI 証明書発行サービスの新運用方針について、その技術的特徴と本学における導入検討事項を整理する。

3.1 技術的要件と認証方式

UPKI では、証明書の有効期間短縮対応として、取得・更新を自動化するため、ACME (Automatic Certificate Management Environment)プロトコルを導入する。UPKI が推奨する ACME クライアントは Certbot であり、Linux 環境を中心に広く利用されている。初期設定を行うことで、証明書の取得・更新が自動化され、手動更新と比較して作業負荷を大幅に削減できる。さらに、UPKI ではセキュリティ強化の一

環として、アラートシステムの導入も予定しており、更新処理の失敗時には利用管理者へ通知が行われる。このアラートシステムは、他の一般的な ACME サービスとは一線を画す高信頼な設計といえる。

加えて、UPKI では、認証局が証明書発行対象アカウントを事前に認識・制限するための仕組みである EAB (External Account Binding)によるアカウント登録を行う。EAB は、一般的な ACME サービスでは省略可能なステップであるが、UPKI ではセキュリティ強化の観点から必須としている。具体的には、UPKI が発行する「アカウント ID（EAB-KID）」と「秘密鍵（EAB-HMAC-KEY）」を用いて、ACME クライアントからの登録要求を認証する。このプロセスにより、証明書の発行対象となるサーバーが、正規の機関に属していることを事前に確認可能となり、学術機関向けサービスとしての信頼性と安全性を高めている。

```
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>
```

表 2. EAB コマンド例

3.2 認証方式と学内運用上の課題

UPKI が推奨する ACME クライアントである Certbot では、証明書発行時のドメイン所有確認において HTTP-01 チャレンジ、DNS-01 チャレンジの 2 方式が利用可能である。

HTTP-01 チャレンジは、対象サーバーの 80 番ポートに対して認証局がアクセスし、指定された URL に応答することでドメイン所有を確認する方式である。しかし、本学では情報セキュリティ対策室のインバウンド通信制限解除の規定により、学外からの 80 番ポート通信を原則禁止しており、許可している場合でも HTTPS へのリダイレクトのみが認められている。このため、本学では HTTP-01 方式の展開する場合は、このインバウンド通信制限の規定(参考文献[2])を改める必要がある。

一方、DNS-01 チャレンジは、対象ドメインの DNS に特定の TXT レコードを設定することで認証を行う方式であり、HTTP-01 に比べて柔軟性が高いとされる。しかし、本学では DNS 登録作業は情報ネットワーク担当による手動運用であるため、証明書の発行・更新の度に依頼が必要となり、現行と同等あるいはそれ以上の運用負荷がかかる。DNS-01 方式を円滑に運用するには、学内の運用規定との整合性を確保しつつ、運用体制の見直しが求められる。

よって、どちらの認証方式を採用するにしても、技術的な適合性だけでなく、学内の運用体制やセキュリティ方針との調整が不可欠であり、今後の UPKI の仕様公開に注視しながら、柔軟に対応を検討する。

3.3 プライベート環境下のサーバー対応

証明書の自動取得・更新をプライベート環境下のサーバーに適用する場合、追加の配慮が必要となる。HTTP-01 方式では、対象 FQDN に対して A レコードの登録が必要であり、DNS-01 方式では TXT レコードの登録または更新権限の付与が求められる。また、UPKI では MPIC (Multi-Perspective Issuance Corroboration)の対応も進めており、A あるいは TXT レコードが登録しない場合であっても、空の CAA レコードを登録するなどし、DNS サーバーに問い合わせた際に NOERROR を返す必要があるとしている。しかし、これらの情報が外部 DNS に公開されることで、プライベート環境の存在が外部から認識される可能性があり、セキュリティ上の懸念が生じるため、学内の運用を慎重に検討する必要がある。

4. まとめと今後の課題

UPKI 証明書の自動化対応は 10 月に導入予定である。本学では、今後も検証作業を進め、試験運用を実施し、運用体制を整えた上で利用管理者への展開を予定している。今後は技術資料や支援体制を活用し、安定的かつ安全な証明書管理の確立を目指す。

参考文献

[1]NII オープンフォーラム［UPKI サービス最新情報］
https://www.nii.ac.jp/openforum/upload/n04_02.pdf
[2]情報セキュリティ対策室[インバウンド通信制限]
https://www.security.hokudai.ac.jp/inbound-blocking/