サーバ証明書の有効期限における自動化対応について

現在、Web サーバ等の運用において管理者は 1 年に一回 HTTPS の対応のために、UPKI のサーバ証明書を情報基盤センター/医学情報センターに申請し、そのサーバ証明書を受領し、入れ替え作業を行い、適切に管理しています。しかしながら、セキュリティを大幅に高めるために、UPKI を運用している機関より、今後そのサーバ証明書の有効期間が以下のように段階的に大幅短縮となることが報告されました。

【短縮予定】

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 14 日～	47 日

上記の予定でサーバ証明書が短縮されると、サーバ管理者にとっては一層大きな作業負荷が発生することになります。そこで、本センターではこのような課題に対処するために、以下の 3 つの場合において、サーバ証明書の有効期間を自動的及び手動で更新することを推奨する。

【さくらインターネット上の Web サーバ：学外における Web 運用】

情報基盤センターにおいて、Let‘s Encrypt という自動的にかつ、永続的な無料のサーバ証明書を利用する方法を実施（サーバ管理者は作業不要）

【学内オンプレミス上の Web サーバ：購入したサーバで Web 運用（学外公開 Web）】

ACME というプロトコルで自動化（一度、実施すると今後これまでのように手動で更新する必要なし）

・手順　今後公開予定

【学内オンプレミス上の Web 以外のサーバ（特別なアプリサーバ）で証明書を利用】

・既存の 1 年間に 1 回行っている作業を短縮期間に基づいて、サーバ証明書を手動で更新