サーバ証明書有効期間短縮とその対応

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

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

【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

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

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 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 を選択してください

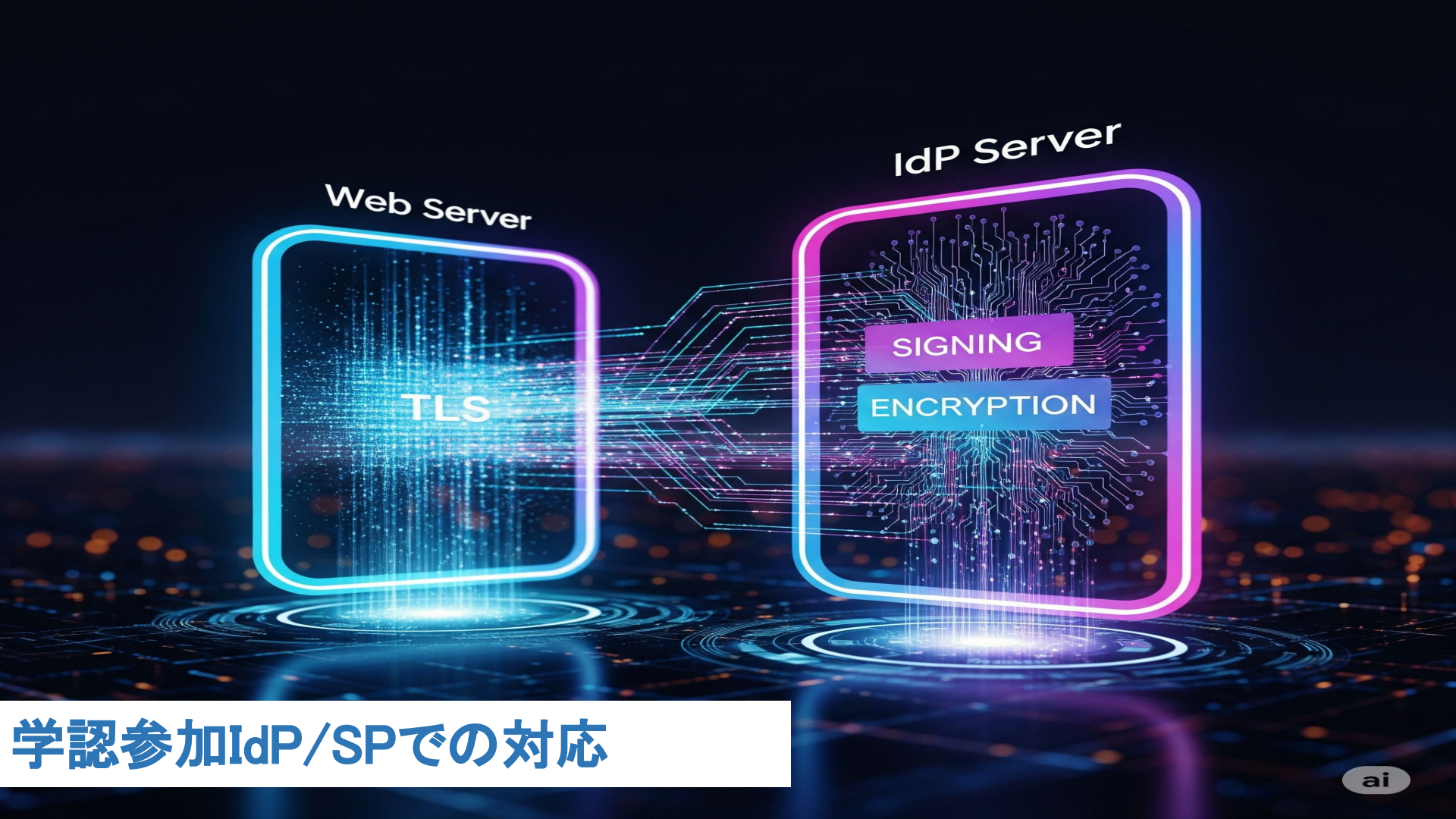
監視

- 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

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

特記事項

- 2025年10月後半からの先行利用開始を予定
- 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



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
```

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等、詳細なマニュアル
  - certbot renew, certbot certonly, …
- EAB Credential 発行フロー、必要なTSVファイル、ライフサイクルの管理等
- TSV作成ツール ACME対応アップデート版
  - https://certs.nii.ac.jp/tsv-tool/
- FAQ

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