証明書が47日に短縮されます

2026/07/16

JANOG58

Naoki Ebisawa

自己紹介

名前: 海老澤 直輝

担当: Akamai製品の実装、導入支援、トレーニング等を担当しています。

JANOG歴: JANOG51が初オフライン参加で、そこからはほとんど参加

今回の資料は社内コミュニティで発表した資料を利用修正しております。
元資料作成者の**Atsushi Suzuki-san Special thanks !**

証明書の有効期限が 段階的に **47日** に短縮されます。

自動化の検討、組織内での連携などが必要になっていきます。

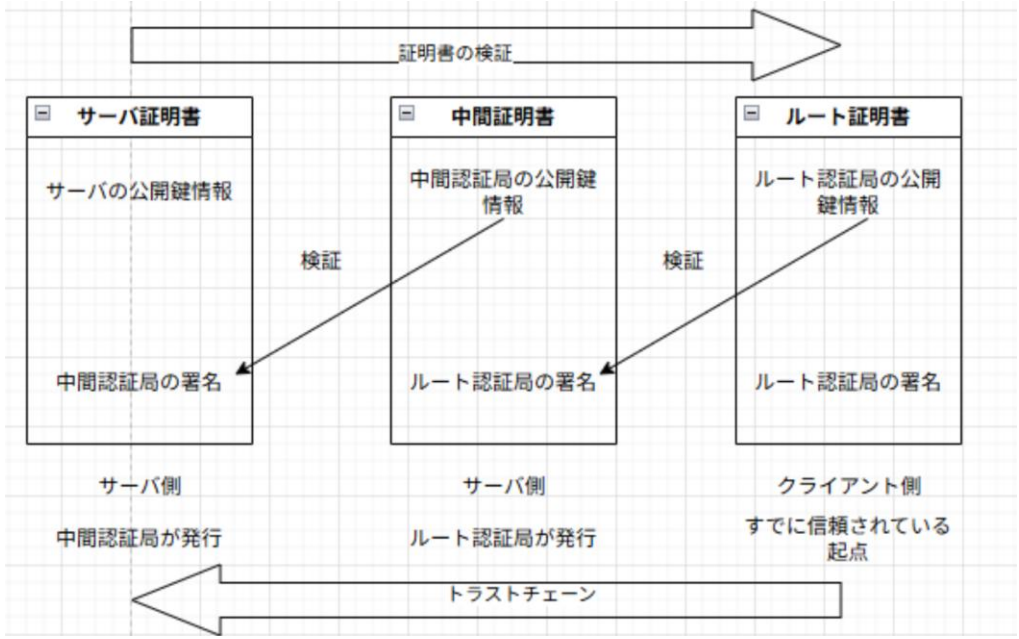
まだ情報が少ない中ですが、可能なところから自動化を検討する必要があります。

インタラクティブLTとのことで、実際にどのような取り組みをしているかコメントいただけると嬉しいです。(質問も嬉しいです。)

そもそも証明書とは？

HTTPSの通信を行う際に相手が本物である(真正性)を担保するために必要なもの

信頼できる第三者(認証局(CA))にデジタル署名されることで、本物であることを証明します。



たかが証明書されど証明書

証明書の更新を忘れて、証明書の期限が切れてしまうとどうなるでしょうか？

→ **ブラウザ上でうまくサイトが表示されず、偉い人に怒られます！**

そのため証明書の更新対応は必須になります！

アジェンダ

1. 証明書の有効期限短縮の概要と背景
2. 業界としての方向性
3. これからの証明書運用

証明書の有効期限短縮の概要と背景

証明書の有効期限短縮の概要と背景

CA/Browser Forum にて、Ballot SC-081 v3 が承認

- **2029年3月** までに、段階的に**証明書の有効期間を 47日 まで短縮**
- 合わせて、ドメイン認証、組織認証の有効期間を短縮

⇨
- **証明書の手動管理は困難**となり、**自動化が必要**となる
- 業界として自動化に向けた仕組みを整備中

参考: https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/

証明書の有効期限短縮の概要と背景
- 業界標準の短縮タイムライン

＊ 段階的に短縮される各種有効期限（Ballot SC-081 v3）

	証明書 有効期間	ドメイン認証 有効期間	組織認証 有効期間
これまで	398日	398日	825日
2026年3月15日	200日	200日	398日
2027年3月15日	100日	100日	398日
2029年3月15日	47日	10日	398日

現在は 200 日に短縮されている状態。

参考: https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/

証明書の有効期限短縮の概要と背景
補足: Akamai 対応 CA の短縮タイムライン

	証明書有効期間	ドメイン認証 有効期間	組織認証 有効期間
現在	Let's Encrypt = 90日 DigiCert = 397日 業界標準 = 398日	Let's Encrypt = 30日 DigiCert = 397日 業界標準 = 398日	業界標準 = 825日 DigiCert = 825日
2026年2月24日	DigiCert = **199日**	DigiCert = **199日**	DigiCert = **397日**
2026年3月15日	業界標準 = 200日	業界標準 = 200日	業界標準 = 398日
2027年2月10日	Let's Encrypt = **64日** DigiCert = **99日** (日付未定)	Let's Encrypt = **10日**	
2027年3月15日	業界標準 = 100日	業界標準 = 100日	
2028年2月16日	Let's Encrypt = **45日** DigiCert = **46日** (日付未定)	Let's Encrypt = **7時間**	
2029年3月15日	業界標準 = 47日	業界標準 = 10日	

Let's Encrypt: https://letsencrypt.org/2025/12/02/from-90-to-45
DigiCert: https://www.digicert.com/blog/tls-certificate-rule-changes

証明書の有効期限短縮の概要と背景
- 47日への短縮により何が起こるか

これまで (398 days)

更新頻度

年 0 ~ 1 回

ドメイン認証の再利用

398 日間

更新失敗時の対応

年に 1 回かつ猶予あり

これから (47 days)

更新頻度　年 8 ~ 9 回

▶ 更新にかかる運用コストが 9倍 に増加

ドメイン認証の再利用　10 日間

▶ 再利用が難しく毎回ドメイン認証が必要

更新失敗時の対応　年に複数かつ猶予なし

▶ クリティカルな対象として監視が必要

証明書の有効期限短縮の概要と背景 - なぜ47日へ短縮するのか？

長期利用に起因
非自動化に起因
失効確認の限界に起因

実態との乖離

・陳腐化した企業情報
・過去のドメイン認証結果の再利用

古い証明書の悪用

・証明書の悪用
・悪用状態の長期化

認証局の誤発行

・証明書の誤発行
・誤発行状態の長期化

失効確認の限界

・CRL の肥大化
・CRL/OCSP のパフォーマンス問題

手作業でのミス

・誤情報の登録
・更新忘れやミス

Crypto Agility の欠如

・危殆化した暗号への対応遅延

参考: https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/

証明書の有効期限短縮の概要と背景 - なぜ47日へ短縮するのか？

長期利用に起因
非自動化に起因
失効確認の限界に起因

~~実態との乖離~~

更新頻度が短くなり、平均的な**証明書の信頼度が向上**

~~古い証明書の悪用~~

更新頻度が短くなり、窃取された**証明書の悪用期間が短縮**

~~認証局の誤発行~~

更新頻度が短くなり、誤発行された**証明書の放置期間が短縮**

~~失効確認の限界~~

失効確認への依存が減り、**パフォーマンスやリアルタイム性が向上**

~~手作業でのミス~~

自動化が必須となり、証明書**管理の品質や安定性が向上**

~~Crypto Agility の欠如~~

更新頻度が短くなり、**危殆化した暗号の放置期間が短縮**

参考: https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/

業界としての方向性

業界としての方向性
- 証明書管理の自動化に向けた取り組み

CA にて以下の対応が進行中。

自動化機能の提供

2027年3月15日までに、ACME または同等の自動化機能を提供予定。

手動ドメイン認証方式の廃止

2028年3月15日までに、人間の介入が必要なドメイン認証方式 (メール, 電話) を廃止予定。

永続的なドメイン認証の標準化

定期的な更新不要でドメイン認証を完了する方式 (DNS-PERSIST-01) を標準化予定。
※時期未定

業界としての方向性
- 自動化機能の提供

ACME とは
(Automated Certificate Management Environment)

証明書のライフサイクル (CSR生成, 認証, 発行 等) を自動化するための標準プロトコル。

ACME 対応の要件
- From Chrome Root Program

2027年3月15日までに ACME または同等の自動化機能を提供することが義務付けられている。

⇨ 既に ACME 対応済みの CA も多いが、業界のデッドラインは **2027年3月15日** であり、**自動化を検討する際の目安**となる。

参考: https://googlechrome.github.io/chromerootprogram/#133-promote-cryptographic-agility-and-resilience

業界としての方向性
- 手動ドメイン認証方式の廃止

2026年3月15日	IP アドレスを用いたドメイン認証を廃止 ※元々脆弱性が指摘されており、このタイミングで廃止
2027年3月15日	電話・FAX・郵送によるドメイン認証を廃止
2028年3月15日	メールによるドメイン認証を廃止 ▶特に OV/EV 証明書で普及しており、影響が大きい

⇨ 既存の手動ドメイン認証が難しくなるのが、**2028年3月15日** であり、**自動化を完了する期日の目安**となる。

参考: https://www.digicert.com/jp/blog/ca-bf-ballot-sc-090-closer-to-fully-automated-validation

参考: ドメイン認証方式のラインナップ

HTTP / TLS ベース

HTTP-01
/.well-known/ 配下に一時的なトークンを配置して認証する方式

TLS-ALPN-01
TLS handshake 時に専用の ALPN 拡張で一時的なトークンを応答する方式

DNS ベース

DNS-01
TXT や CNAME レコードに一時的なトークンを配置して認証する方式

DNS-ACCOUNT-01
DNS-01 をベースに同一ドメインで複数証明書が必要な場合に対応した方式

DNS-PERSIST-01
New

永続的なレコードを配置し、
書き換え不要で認証を完了する方式

参考: https://cabforum.org/2025/10/09/ballot-sc-088v3-dns-txt-record-with-persistent-value-dcv-method/

業界としての方向性
- 永続的なドメイン認証方式 (DNS-PERSIST-01)

DNS-PERSIST-01 は **DNS レコードの書き換え不要**でドメイン認証を永続的に完了させる新しい方式。

従来のドメイン認証方式の課題

- 更新のたびにトークン発行が必要
- DNS レコード書き換えが必要

→ 特に DNS ベースの認証では、自動化する場合に**ゾーン管理用の API Key が漏洩するリスク**があった

DNS-PERSIST-01 による解決

- 初回のみ CA と ACME アカウント情報をレコードに記載
- 以降は書き換え不要で更新可能

→ **レコード書き換えの手間やゾーン管理用の API Key が不要**となり、安全かつ簡素な自動化が可能になった

 参考: https://cabforum.org/2025/10/09/ballot-sc-088v3-dns-txt-record-with-persistent-value-dcv-method/

業界としての方向性
- 永続的なドメイン認証方式 (DNS-PERSIST-01)

RFC はドラフト段階であるが、以下の様なレコードになる予定。

```
_validation-persist.example.com. IN TXT "letsencrypt.org;
accounturi=https://acme-v02.api.letsencrypt.org/acct/12345678; policy=wildcard"
```

Issuer Domain Name

CA を識別するためのドメイン名を指定。

accounturi

証明書を要求する ACME アカウントの識別子を指定。

(参考) ACME アカウントは CA 毎に払い出され、要求者の公開鍵と共に CA で保存。証明書発行時は対応する秘密鍵で署名してリクエストする。

 参考: https://www.certkit.io/blog/dns-persist-01 , https://datatracker.ietf.org/doc/draft-ietf-acme-dns-persist/01/

業界としての方向性

業界として、自動化に向けて急ピッチで仕組みを整備しています。

期限が短く情報が少ない中ではありますが、**業界のスケジュールやロードマップを抑えて、可能なところから自動化の検討を進めて行く**必要があります。

これからの証明書運用

これからの証明書運用
- 47日への短縮により何が起こるか

これまで (398 days)

更新頻度

年 0 ~ 1 回

ドメイン認証の再利用

398 日間

更新失敗時の対応

年に 1 回かつ猶予あり

これから (47 days)

更新頻度　　年 8 ~ 9 回

▶ 更新にかかる運用コストが 9倍 に増加

ドメイン認証の再利用　　10 日間

▶ 再利用が難しく毎回ドメイン認証が必要

更新失敗時の対応　　年に複数かつ猶予なし

▶ クリティカルな対象として監視が必要

これからの証明書運用
- 求められる運用

人間の介入を排除した **完全自動化**

カレンダー通知等の手作業からの脱却

ソフトウェアと同様の CI/CD, DevOps による運用

クリティカルな **監視**と**インベントリ**

証明書を可視化するインベントリの構築

更新失敗時のアラートに対応できる体制

これからの証明書運用
- 人間の介入を排除した完全自動化

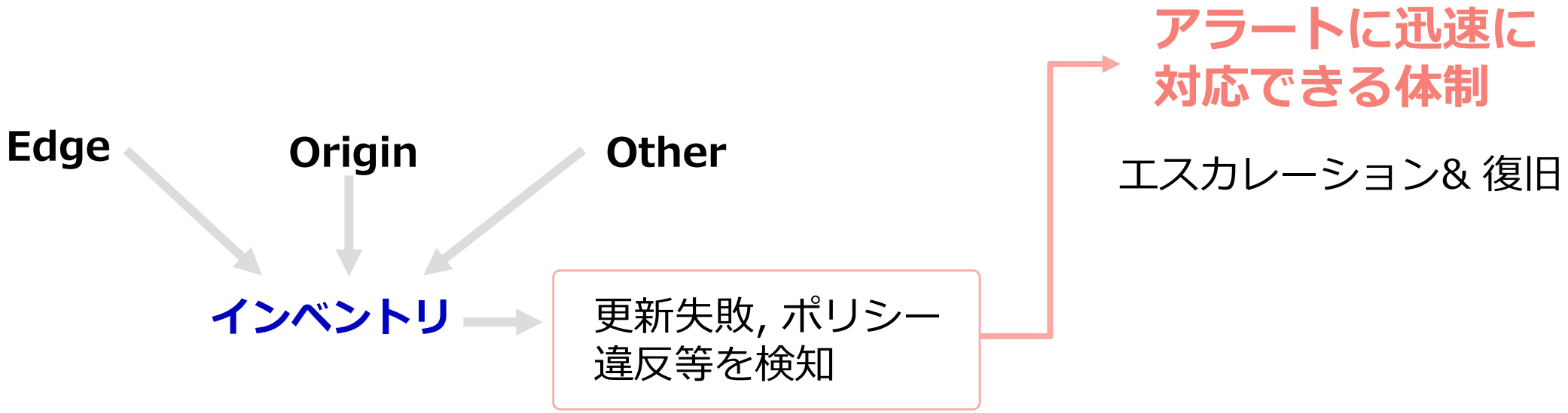
ソフトウェアと同様に構成を定義し、ビルドから検証まで自動化

1. **コード定義 (IaC)** — Terraform 等で証明書要件をコードで定義
2. **自動取得 (Build)** — CSR 取得や証明書生成、ポリシー準拠の確認等を自動で実施
3. **自動展開 (Deploy)** — 証明書のアップロード、展開を自動で実施
4. **検証 (Validate)** — エンドツーエンドの疎通テストや死活監視を自動で実施

参考: https://www.akamai.com/resources/white-paper/tls-certificate-lifecycles-white-paper

これからの証明書運用
- クリティカルな監視とインベントリ

証明書を可視化するインベントリを構築, 監視し、
更新失敗時のアラートに対応できる体制も整備。



参考: https://www.akamai.com/resources/white-paper/tls-certificate-lifecycles-white-paper

これからの証明書運用
- 今からできること

有効期限短縮による影響について組織内で理解を得る

影響が大きく短期間での整備が必要になる点の理解を得る

CI/CD, DNS, サイトオーナー等、各チームの協力を得る

証明書を棚卸し、インベントリ構築を検討

証明書がどこに、いくつあるかを洗い出す

証明書を集中的に管理/監視するインベントリを構築

最後に

JANOG62-63あたりで、CDN事業者、企業目線での証明書自動化の取り組みの話ができる、聞けたら面白そうだなと思ってます。

最後に

証明書の有効期限が 段階的に **47日** に短縮されます！

これだけ知ってもらえたら満足です！