～なぜ必要？有効期間短縮にどう対応する？～

サーバー証明書の基礎知識

2026年6月10～12日

Interop Tokyo 2026

株式会社 日本レジストリサービス

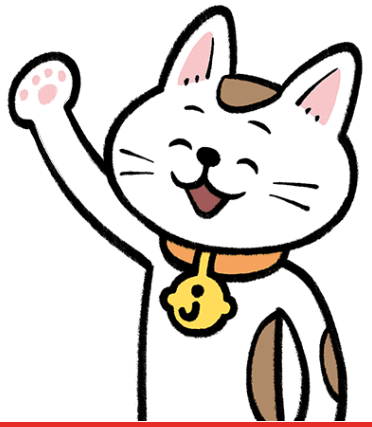
JaPan Registry Services

■ 主な役割

- JPドメイン名（.jp）の登録管理
- gTLD（.com、.netなど）の登録取り次ぎ
- サーバー証明書認証局
- インターネットのポリシー策定や技術の標準化など、国際活動・研究開発への貢献

このセミナーでわかること

1. サーバー証明書でできること
2. サーバー証明書の入手・設定方法
3. サーバー証明書の有効期間短縮への対応



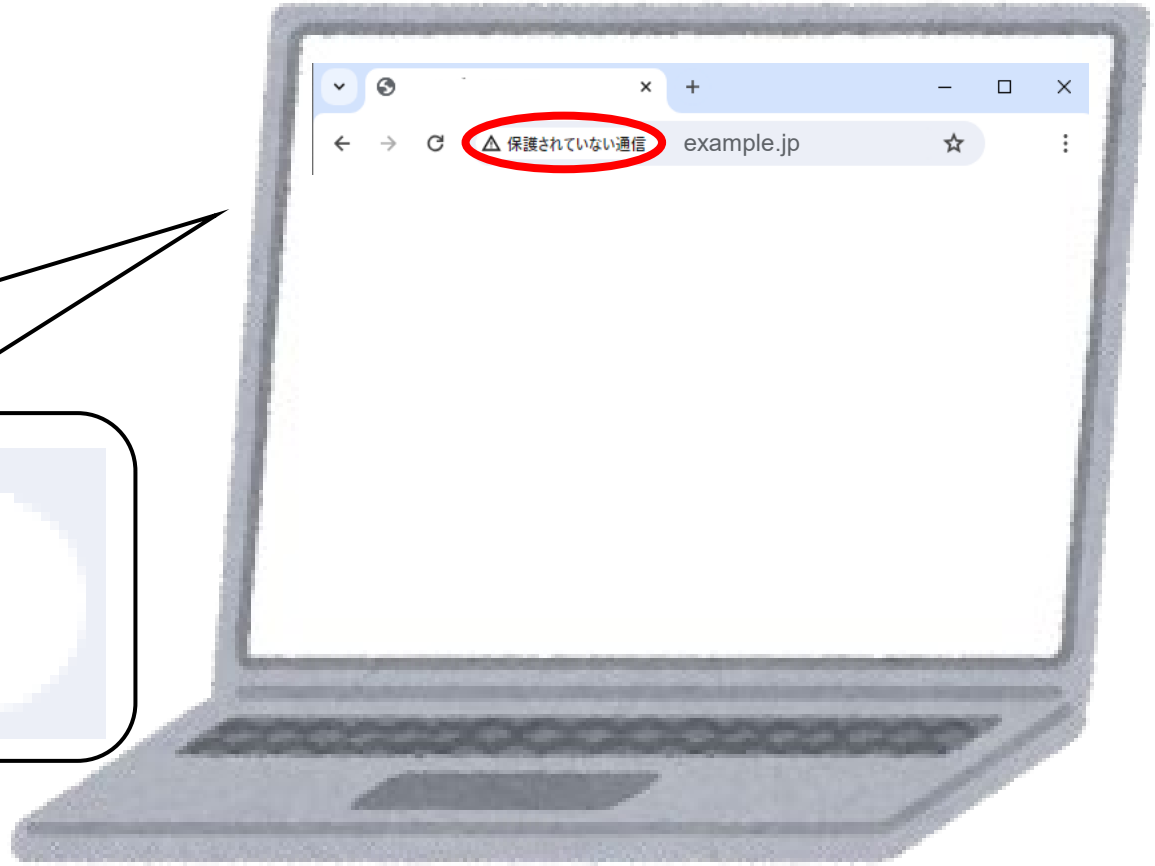
「サーバー証明書も解説」篇
https://youtu.be/WoFUvOYjO88

サーバー証明書でできること

こんな警告を見かけたことはありませんか？

ブラウザーでWebサイトを
閲覧しているときに……

⚠ 保護されていない通信

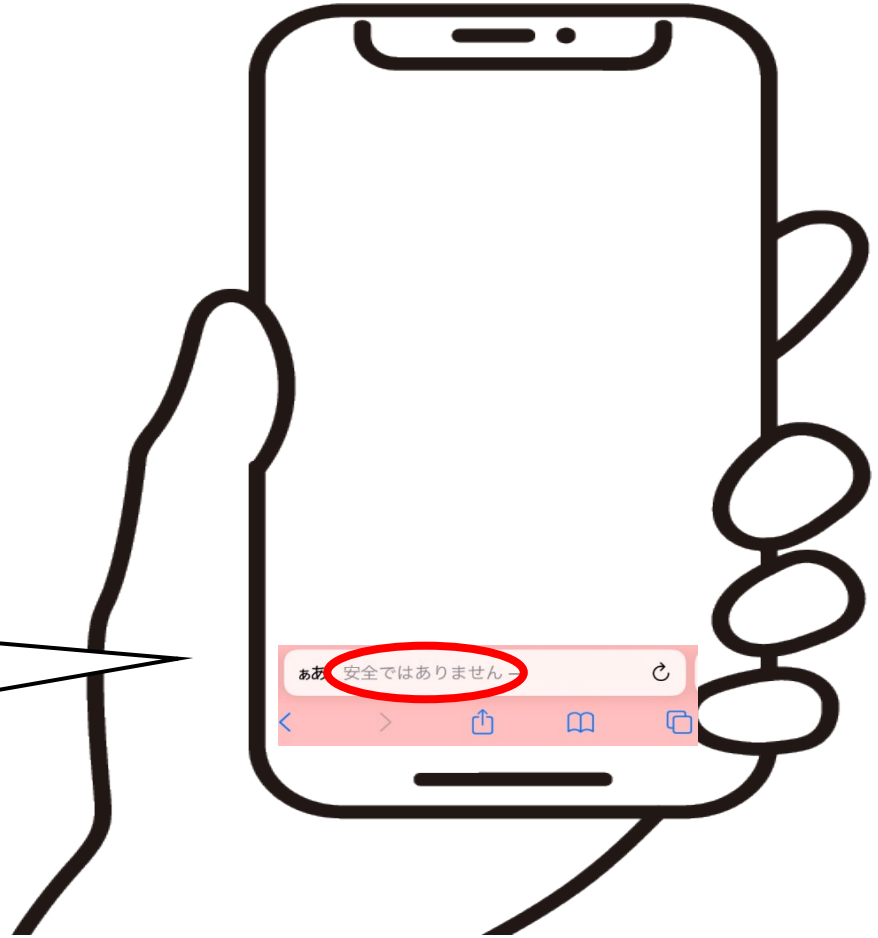


Google Chrome（クローム）の表示例

こんな警告を見かけたことはありませんか？

スマートフォンでWebサイトを
閲覧しているときに……

安全ではありません



Apple Safari（サファリ）の表示例

これってどういうことなんだろう？

「保護されていない通信」だから、
個人情報が流出してしまう？

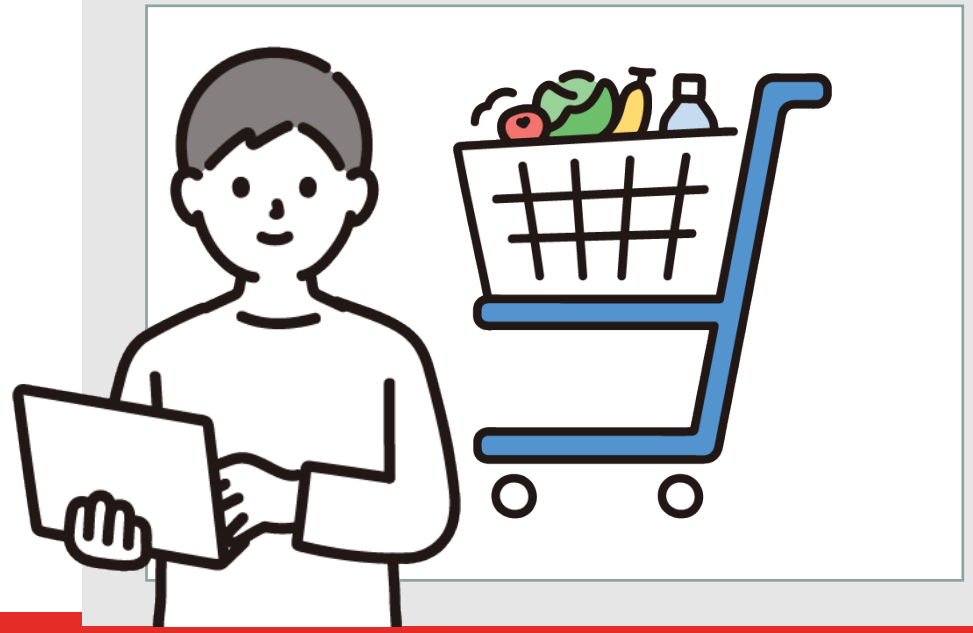
「安全ではありません」だから、
ここで買うと危険な
サイトなのかな？

これらはWebサイトとの通信が
暗号化されていないことを知らせる
警告メッセージです。

通信の暗号化とは？

Webブラウザー

安全ではありません　△△△.jp



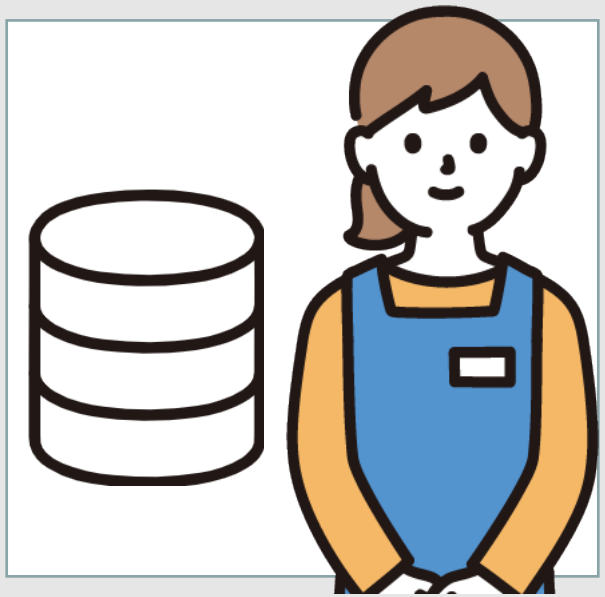
リンゴを1個
買います

通信

受け付けました

ショッピングサイト

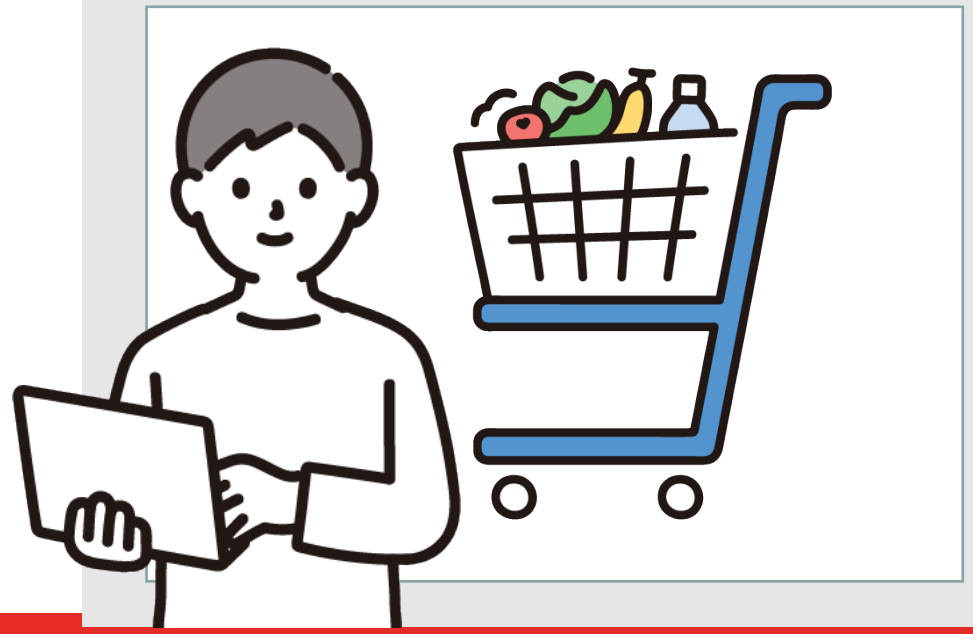
△△△.jp



通信が暗号化されていないと…

Webブラウザー

安全ではありません　△△△.jp



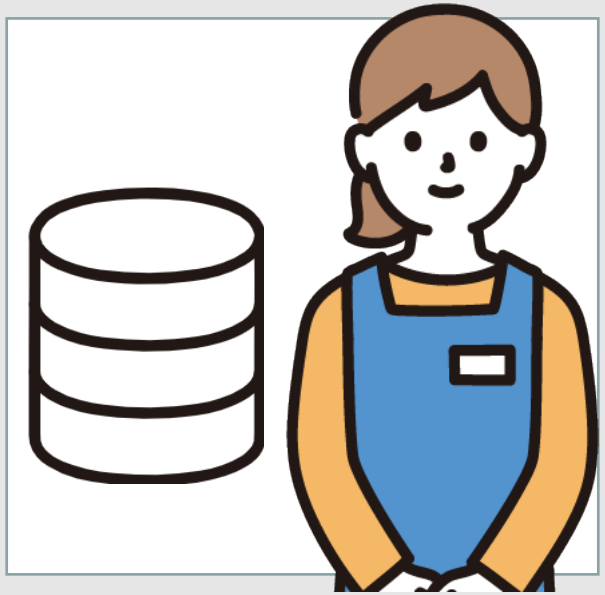
リンゴを100個
買います

覗き見！
書き換え！

受け付けました

ショッピングサイト

△△△.jp

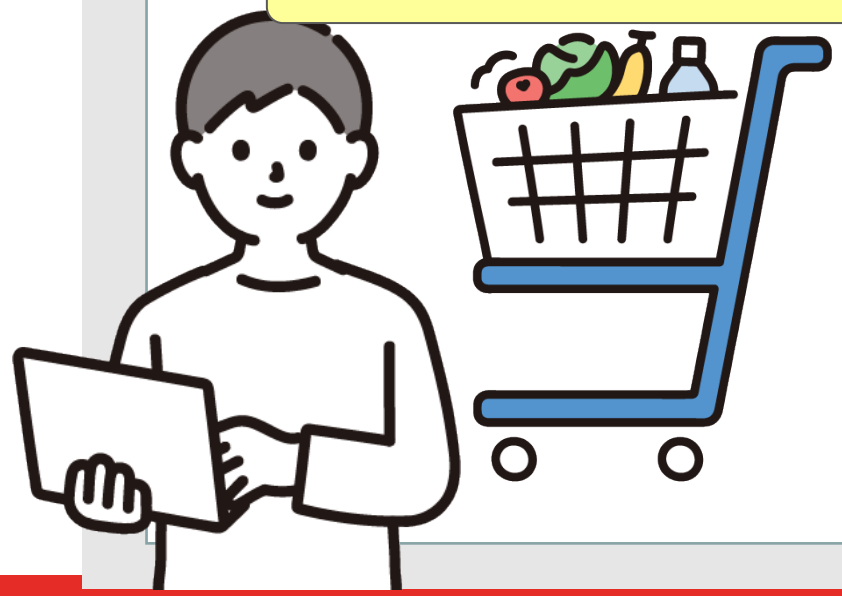


サーバー証明書を入れることで…

Webブラウザー

△△△.jp

「安全ではありません」が表示されなくなる



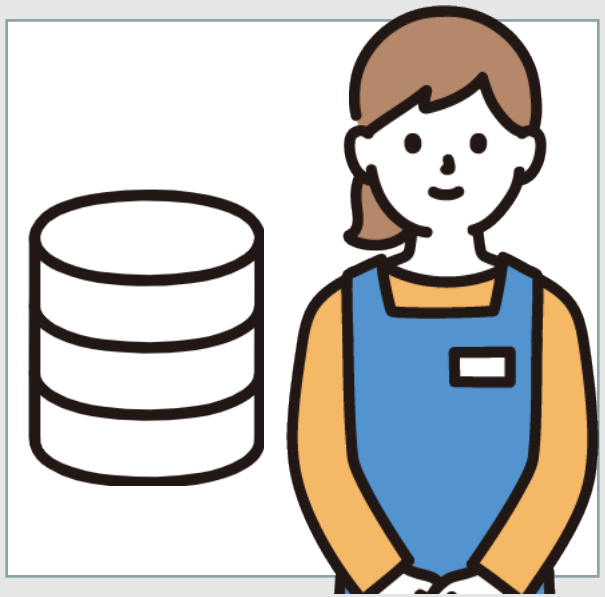
覗き見・書き換え
不可！

サーバー証明書で
通信を暗号化！

ショッピングサイト

サーバー証明書

△△△.jp



ここまでのまとめ

- 通信が暗号化されていないと、第三者が通信内容を覗き見たり、改ざんしたりできる
- こういった行為への対応策として、サーバー証明書を使った通信の暗号化が必要になっている
- サーバー証明書は、Webサイトの管理者が入れる

このセミナーでわかること

1. サーバー証明書でできること（完了）
2. サーバー証明書の入手・設定方法
3. サーバー証明書の有効期間短縮への対応

サーバー証明書の入手・設定方法

サーバー証明書は誰が発行するの？

誰が：

信頼のおける第三者機関である「認証局」

が

何を：

ドメイン名（サーバー）の管理権限があること

や

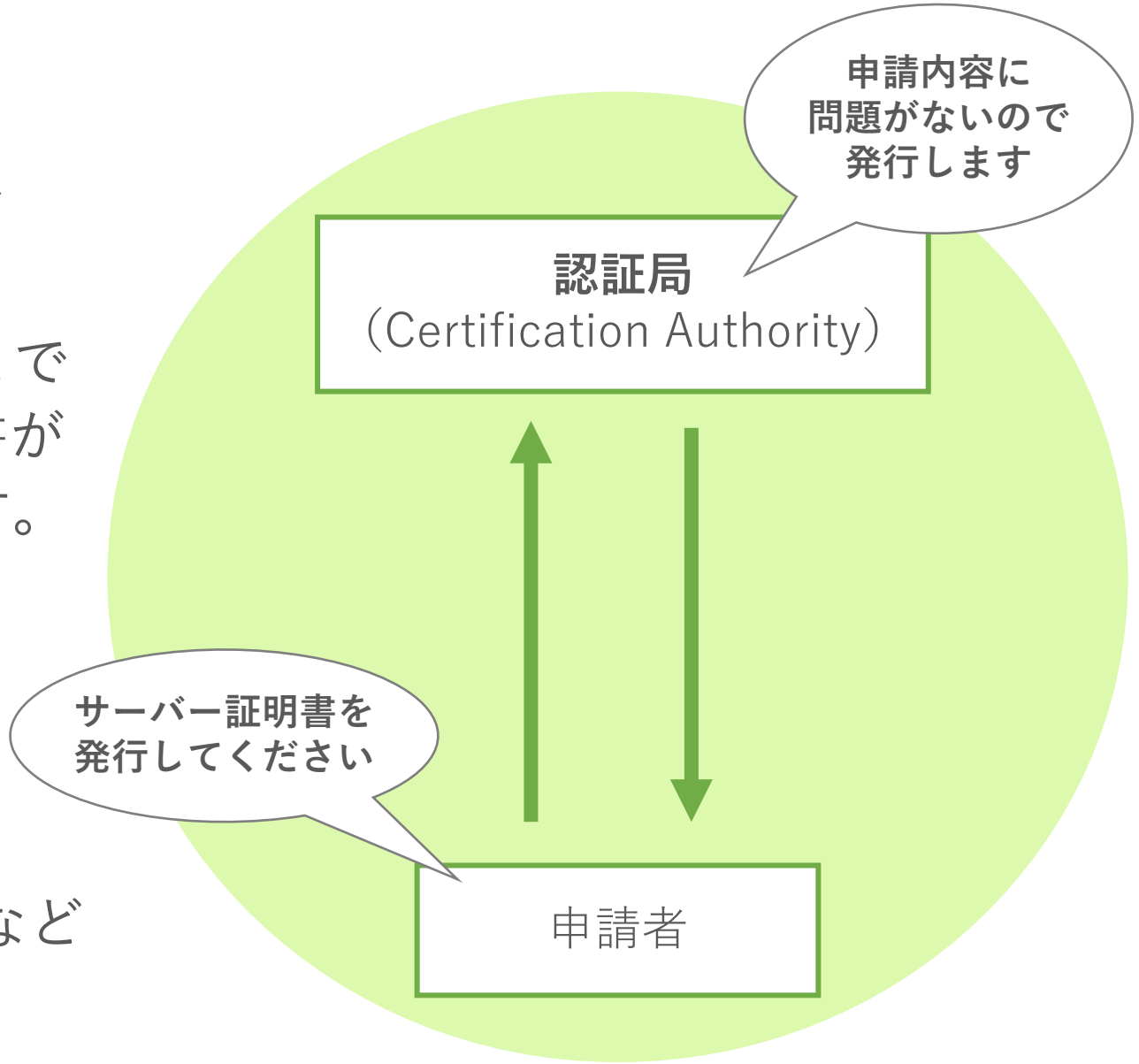
申請元の組織や企業が実在していること

を

証明するために発行します。

認証局って何者？

- 申請者からの依頼を受けて、証明書を発行・失効する機関です。
- Webブラウザが認証局を信頼することでその認証局が発行したサーバー証明書が信頼され、Webサイトが信頼されます。
- 認証局が信頼を確保するための、審査プログラムや仕組みが存在します。
  - WebTrust（ウェブトラスト）
  - 認証局運用規程（CPS）　　… など



設定までの基本的な流れ

秘密鍵の生成や署名前の証明書情報の作成

取り扱い事業者にサーバー証明書発行の申し込み

ドメイン名管理権限の確認や電話などによる認証

Webサーバーに証明書を設定

※ レンタルサーバーをご利用の場合は、設定方法や作業内容が異なる場合があります。
ご利用のサービス提供事業者さまに直接ご確認・お問い合わせください。

① CSRの作成

① CSRの作成

CSRのサンプル

```
----BEGIN NEW CERTIFICATE REQUEST-----
MIICdzCCAiECAQAwZzEQMA4GA1UEAxMHbHJhLXRmczEQMA4GA1UECxMHczEQMA4GA1UE
ChMHbHJhLXRmczESMBAGA1UEBxMJTWlOYWthc2hpMQ4wEwVUb2t5bzELMAkGA1UEBhMC
SlAwXDANBgkqhkiG9w0BAQEFAANLADBIAktF2t+iHqA2nWqt7UYwApptgsYvFrkmXIUH
tZifBz8FOhsBelFbCT33po+9zrWzmRga8DDhxSdujmxGZHOwIDAQABoIIBUzAaBgorBg
EEAYI3DQIDMQwWCjUuMC4LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYDVR0PAQH/BAQDAgT
wMBMGA1UCCsGAQUFBwMBMIH9BgorBgEEAYI3DQICMYHuMIHrAgEBHloATQBpAGMAcbwB
mAHQAIABSAFMAQQAgAFMAQwBoAGEAbg
-----END NEW CERTIFICATE REQUEST--
```

・コモンネーム（例: jprs.co.jp）

・組織名　・部署名　・公開鍵の情報

…などの情報が書かれている

CSRとは？

「Certificate Signing Request」の略で、
サーバー証明書の発行を申し込む際に必要です。
CSRは、申し込み情報と一緒に認証局に提出します。

※CSRの生成方法については認証局のWebサイトでご確認ください。

② サーバー証明書の申し込み

①	②	③	④
CSRの作成	サーバー証明書の申し込み	認証局による認証手続き	サーバー証明書のインストール

希望する認証局の証明書を取り扱っている事業者に
サーバー証明書発行の申し込みをします。

申し込みは、オンラインもしくは書面で必要情報を入力して提出します。
費用は、取り扱いの事業者や、サーバー証明書の種類によって異なります。

サーバー証明書の【種類】？

② サーバー証明書の申し込み

① CSRの作成 → ② サーバー証明書の申し込み → ③ 認証局による認証手続き → ④ サーバー証明書のインストール

サーバー証明書は3種類ある！

	DV（ドメイン認証型）	OV（組織認証型）	EV（拡張認証型）
通信の暗号化	○	○	○
サーバー証明書が認証する対象	ドメイン名の管理権限	管理権限+組織の法的実在性	管理権限+組織の法的実在性

③ 認証手続き

発行までにかかる時間は
即日～2週間程度

メール・電話・公的書類の確認などによる認証が行われます。

サーバー証明書の種類により、認証方法や手続きにかかる期間が異なります。

④ サーバー証明書のインストール

インストール方法は、Webサーバーアプリケーションや
レンタルサーバー／クラウドサービスの種類によって異なります。

一般的なWebサーバーアプリケーション
（Apache、 Microsoft IIS、nginx、Tomcatなど）における手順であれば、
主な認証局のWebサイトでマニュアルが公開されています。

このセミナーでわかること

完了 1. サーバー証明書でできること

完了 2. サーバー証明書の入手・設定方法

3. サーバー証明書の有効期間短縮への対応

サーバー証明書の
有効期間短縮への対応

有効期間の段階的な短縮

サーバー証明書の最長有効期間が2026年3月15日から段階的に短縮され、最終的に47日になることが決定されました。

証明書の発行日	最長有効期間
～2026年3月15日	398日
2026年3月15日～2027年3月15日	200日
2027年3月15日～2029年3月15日	100日
2029年3月15日～	47日

イマココ！

→有効期間が短縮されると更新頻度が増え、コストや更新漏れのリスクが増加します。そのため、サーバー証明書の管理の自動化への対応が推進されています。

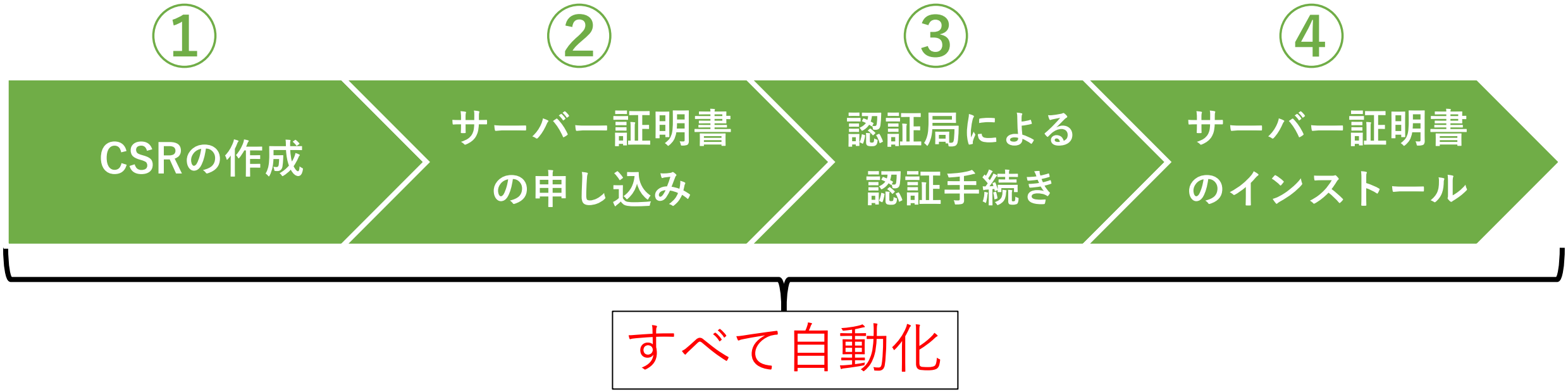
自動化への対応

- サーバー証明書の管理を自動化するプロトコルとして、ACME（アクミー）が開発され、普及が図られています。
- ACME は RFC として標準化されており、対応クライアントや連携ツールも多く提供されています。
- ACMEに対応することで、証明書の発行・更新に関する一連の手続きを自動化できます。

※サービス事業者によっては、ACME 以外の方式（独自の自動化手順）の場合があります。利用中のサービス仕様をご確認ください。

ACMEの公式ロゴ
（引用元：<https://www.ietf.org/blog/acme/>）

ACMEで自動化される範囲



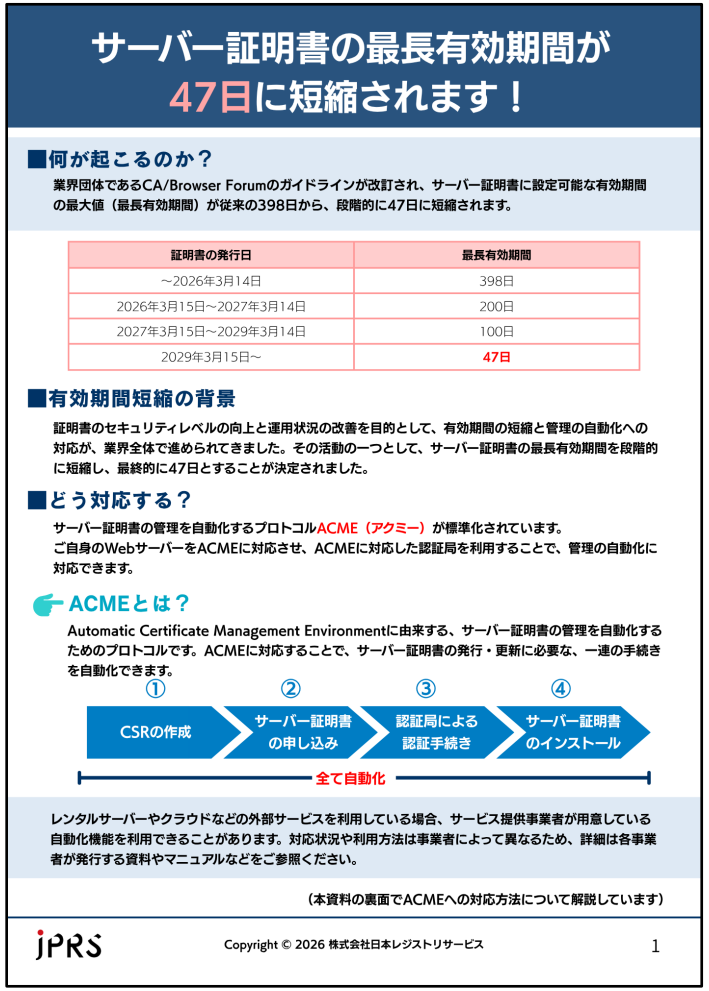
- ①～④の一連の手続きが自動化されます。
  - 電話での確認など、自動化の対象外となる手続きもあります。
- ①②④は**利用者**が、③は**認証局**が対応する必要があります。

自動化のためにすべきこと

- Webサーバーを、**自動化に対応させる**必要があります。
  - 具体的な対応方法は、**Webサーバーソフトウェアやサービス事業者**が提供する、**サービスの仕様**などにより異なります。
  - 自前運用（オンプレミス）の場合は**Webサーバーソフトウェアや運用手順に合う形**で、レンタルサーバーやクラウドなどのサービスの場合はそれぞれの事業者が提供する自動更新機能や設定手順など、**サービスの仕様に沿う形**で対応する必要があります。

自動化のためにすべきこと

JPRSブースでは、サーバー証明書の
有効期間の短縮とACMEに関する
情報をまとめた**リーフレットを配布**しています。
ぜひご利用ください



サーバー証明書の最長有効期間が47日に短縮されます！

■何が起こるのか？

業界団体であるCA/Browser Forumのガイドラインが改訂され、サーバー証明書に設定可能な有効期間の最大値（最長有効期間）が従来の398日から、段階的に47日に短縮されます。

証明書の発行日	最長有効期間
～2026年3月14日	398日
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15日～	47日

■有効期間短縮の背景

証明書のセキュリティレベルの向上と運用状況の改善を目的として、有効期間の短縮と管理の自動化への対応が、業界全体で進められてきました。その活動の一つとして、サーバー証明書の最長有効期間を段階的に短縮し、最終的に47日とすることが決定されました。

■どう対応する？

サーバー証明書の管理を自動化するプロトコルACME（アクミー）が標準化されています。
ご自身のWebサーバーをACMEに対応させ、ACMEに対応した認証局を利用することで、管理の自動化に対応できます。

ACMEとは？

Automatic Certificate Management Environmentに由来する、サーバー証明書の管理を自動化するためのプロトコルです。ACMEに対応することで、サーバー証明書の発行・更新に必要な、一連の手続きを自動化できます。

① CSRの作成 → ② サーバー証明書の申し込み → ③ 認証局による認証手続き → ④ サーバー証明書のインストール

全て自動化

レンタルサーバーやクラウドなどの外部サービスを利用している場合、サービス提供事業者が用意している自動化機能を利用できることがあります。対応状況や利用方法は事業者によって異なるため、詳細は各事業者が発行する資料やマニュアルなどをご参照ください。

（本資料の裏面でACMEへの対応方法について解説しています）

JPRSサーバー証明書発行サービスのご紹介

JPRSでは2016年から、インターネットの安全性を高めるべく、**サーバー証明書発行サービス**を提供しています。

SECURED by JPRS

- JPドメイン名とDNSの管理運用で培ってきた**高い技術**と**信頼性**
- サーバー証明書の管理を自動化する**「ACME」**にも対応

本セミナーのまとめ

1. サーバー証明書でできること

- ☑ サーバー証明書を入手・設定することで通信が暗号化され、内容の覗き見・改ざんができなくなる

2. サーバー証明書の入手・設定方法

- ☑ Webサイトの管理者がJPRSなどの認証局から、所定の方法で入手・設定する必要がある

3. サーバー証明書の有効期間短縮への対応

- ☑ サーバー証明書の有効期間が、段階的に47日に短縮される
  有効期間短縮に対応するため、自動化が推奨されている

アンケートへのご協力をお願いいたします。

アンケート回答用URL

@JPRS_official　JPRSofficial