

サーバー証明書の基本知識

～そのWebサイトは安全ですか？～

2025年6月11～13日

Interop Tokyo 2025



<https://△△△.jp>

この話です

講演者について (1/2)

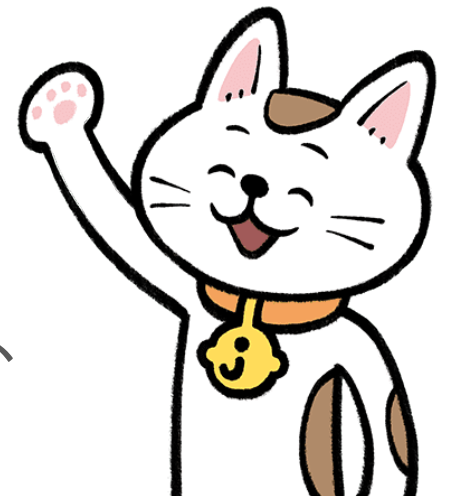
株式会社 日本レジストリサービス

JaPan Registry Services

jPRS

■ 主な役割

- JPドメイン名 (.jp) の登録管理
- 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. 「https://」 と 「http://」 の違い
2. 「https://」 にする方法
3. 「サーバー証明書」 の選び方

うちのWebサイト
安全じゃないの？



「https://」 と 「http://」
何が違う？



こんな警告を見かけたことはありませんか？

ブラウザでWebサイトを
閲覧しているときに……



保護されていない通信

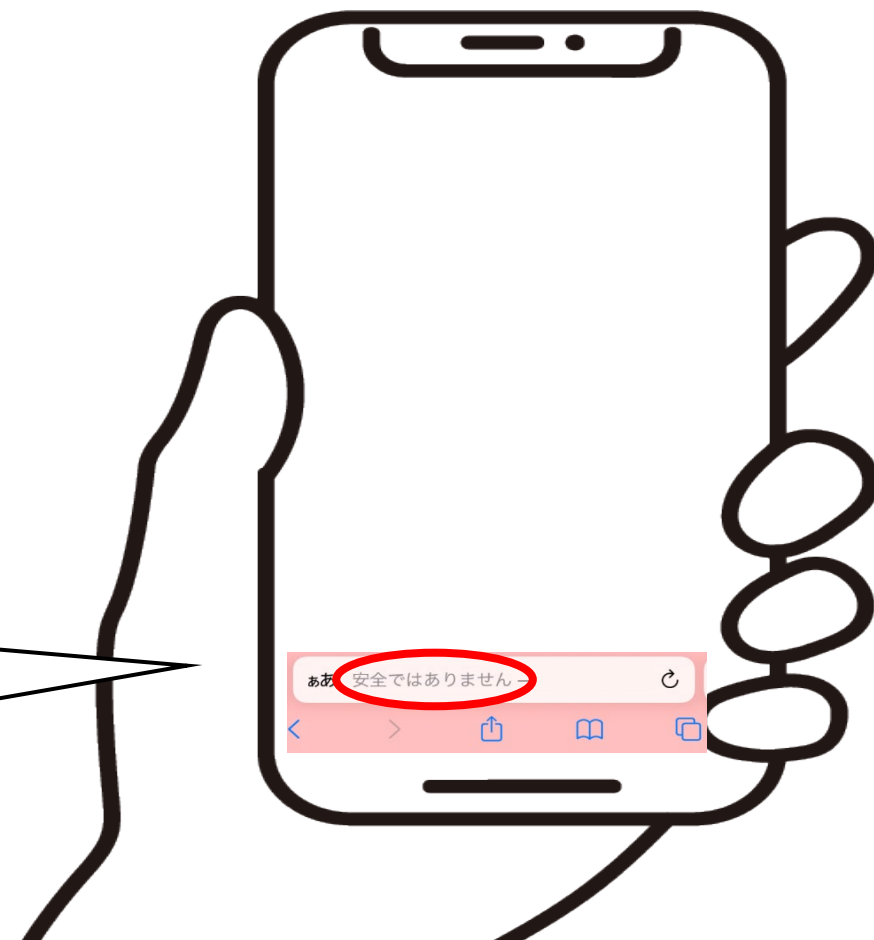


Google Chrome(グーグルクローム)の表示例

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」だと、
個人情報流出してしまう？

「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時に
表示される警告です。

通信の暗号化とは？

ショッピングサイト(ECサイト)

http://△△△.jp



リンゴを1つ
買います

通信

受け付けました

システム側



通信の暗号化とは？

ショッピングサイト(ECサイト)

システム側

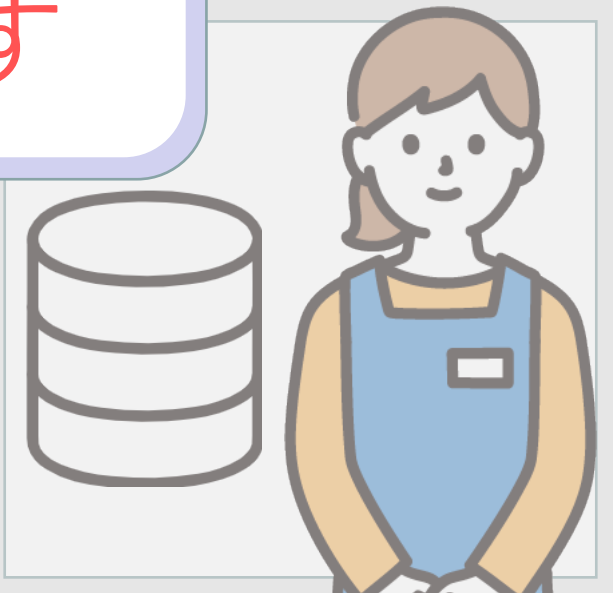
http://

暗号化されていない状態で
情報が送信されています



通信

受け付けました



つまり、悪意を持った
第三者がその通信を

- ・ のぞき見る
- ・ 改ざんする

ことが可能な状態です

インターネット上の通信のことを
はがきを使ってご説明します。

表面

裏面

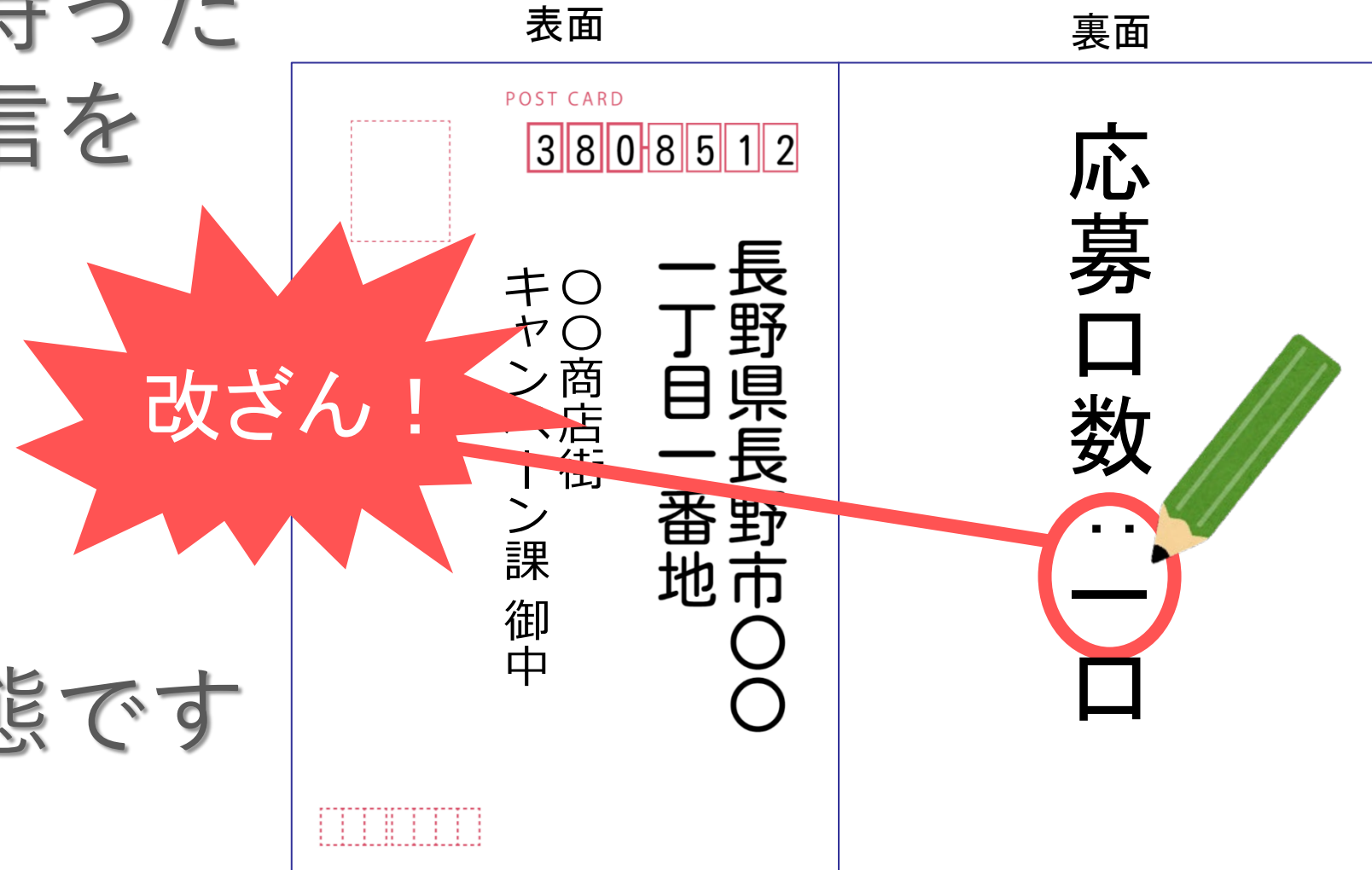
POST CARD 3 8 0 8 5 1 2 長野県長野市〇〇 一丁目一番地 〇〇商店街 キャンペーン課 御中	応募口数 .. 一口
--	-------------------

つまり、悪意を持った
第三者がその通信を

- ・のぞき見る
- ・改ざんする

ことが可能な状態です

インターネット上の通信のことを
はがきを使ってご説明します。



こういった行為への
対応策として

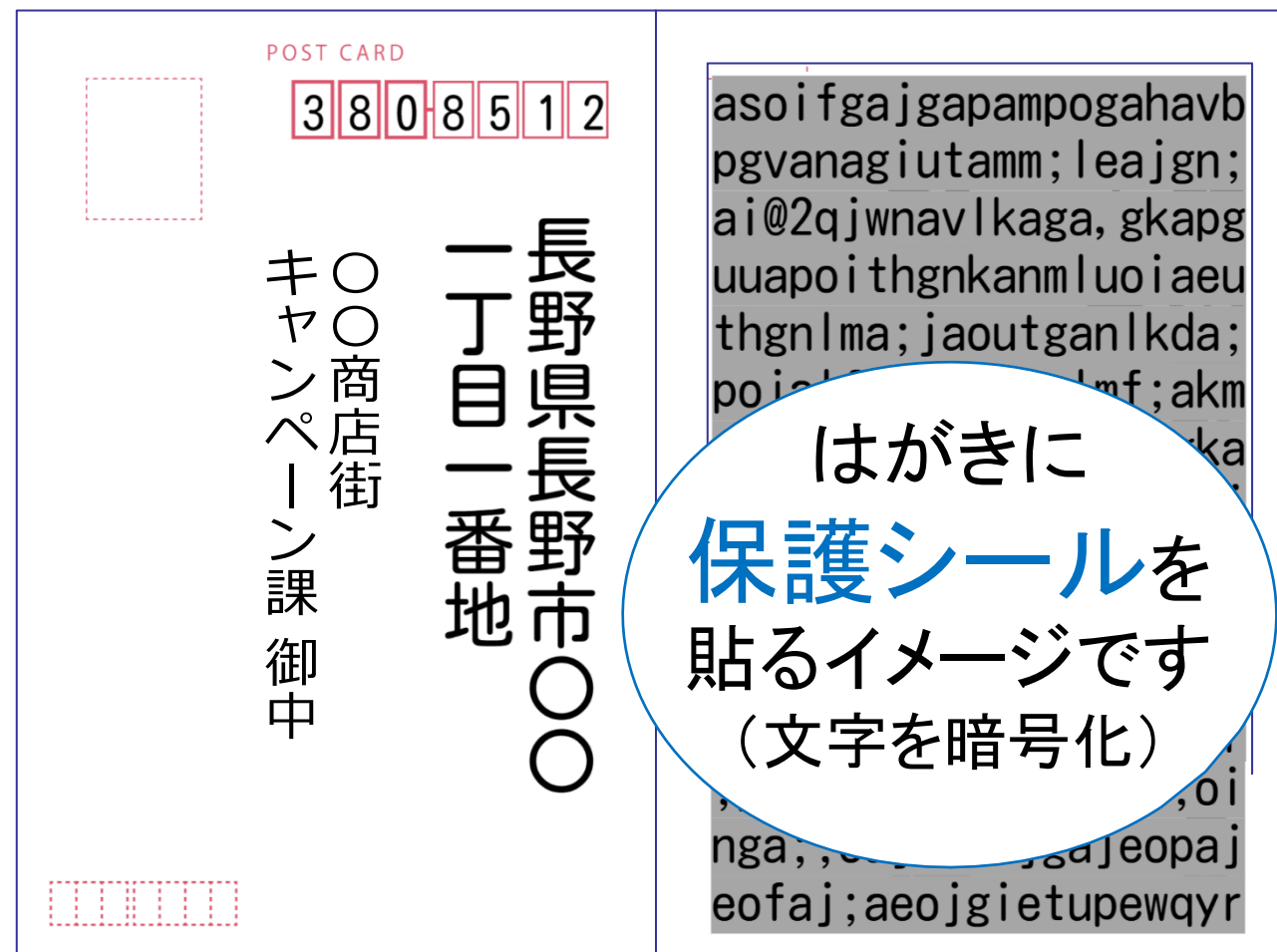
通信の暗号化
(SSL/TLS対応)

が必要になっています

インターネット上の通信のことを
はがきを使ってご説明します。

表面

裏面



SSL/TLS対応（暗号化）した ショッピングサイト（ECサイト）



Vnhprubvmz;uah
apdaufpaj;gavam

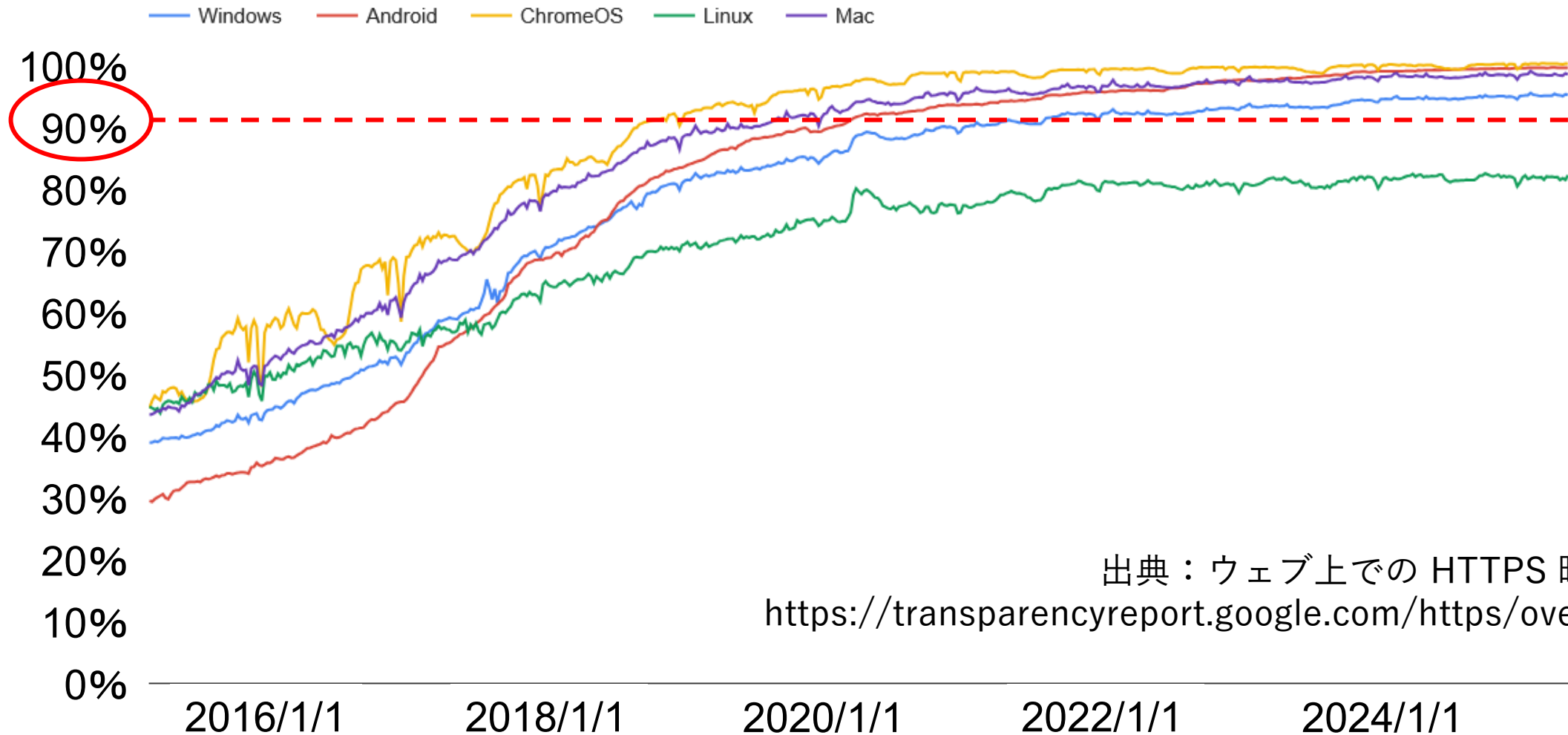
通信

Awoqgrnvzlu]1na

システム側



Chrome で HTTPS 経由で読み込まれたページの割合（プラットフォーム別）



出典：ウェブ上での HTTPS 暗号化
<https://transparencyreport.google.com/https/overview>

ここまでのまとめ

- 「https://」は通信が暗号化されている
「http://」は通信が暗号化されていない
- 通信が暗号化されていないとWebブラウザーが
「保護されていない通信」「安全ではありません」
と警告を表示する
- WebブラウザーのChromeで読み込まれたページの
うち、主要なOSでは90%以上が「https://」である

このセミナーでわかること

- ①完了 1. 「https://」 と 「http://」 の違い
- 2. 「https://」 にする方法
- 3. 「サーバー証明書」 の選び方

どうやって「http**s**://」にする？



HTTPS化するためには…ヒントはここ



サーバー証明書を
Webサーバーに
設定する必要があります。

サーバー証明書は、誰が何を証明するの？

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

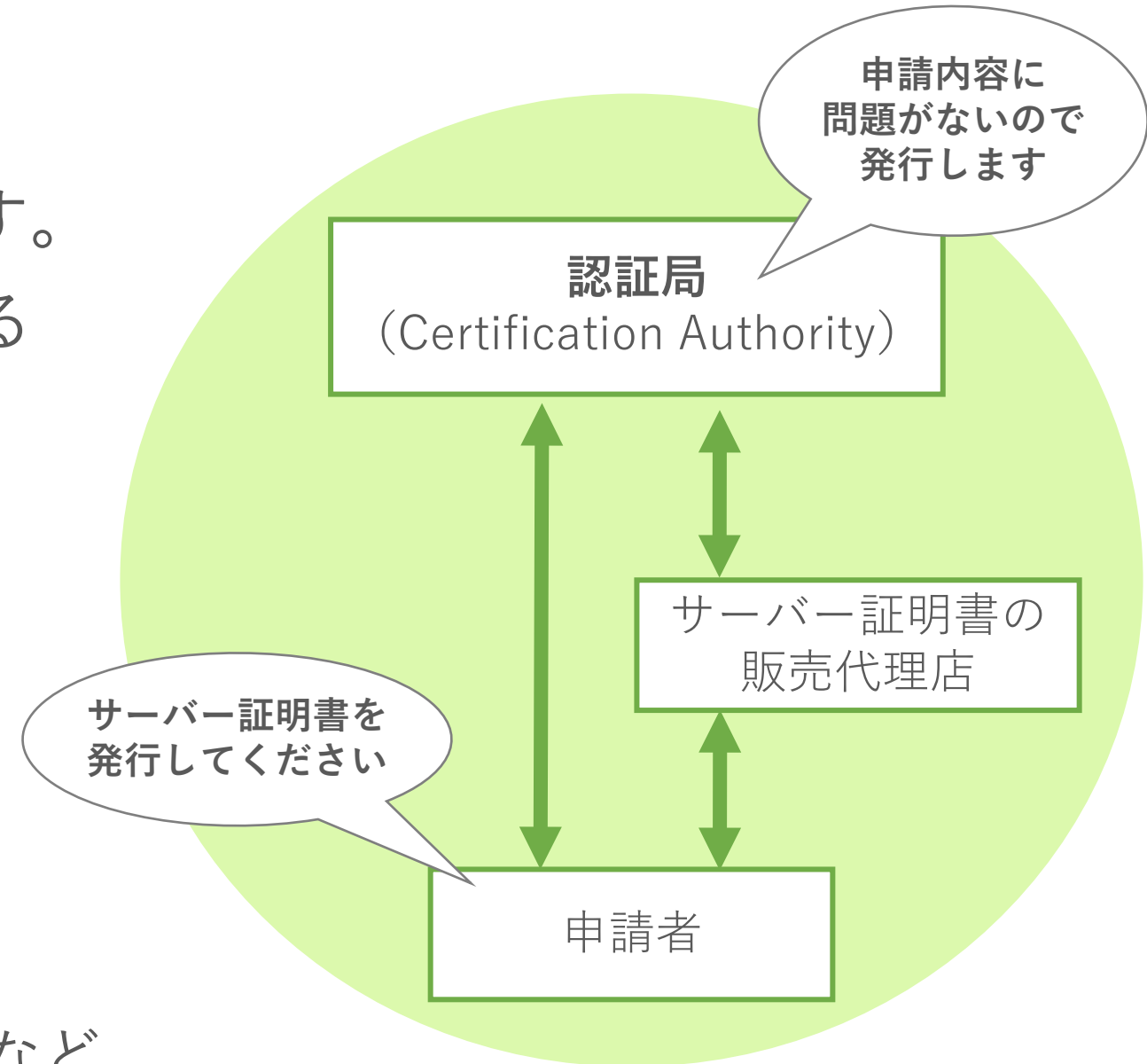
申請元の組織や企業が実在していることを

証明するものです。

認証局って何者？

- 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

①

CSRの作成

秘密鍵の生成や
署名前の証明書
情報の作成

②

サーバー証明書
の申し込み

取り扱い事業者に
サーバー証明書発
行の申し込み

③

認証局による
認証手続き

ドメイン名管理権
限の確認や電話な
どによる認証

④

サーバー証明書
のインストール

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

サーバー
の申請

CSRのサンプル

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICdzCCAIECAQAwZzEQMA4GA1UEAxMHbHJhLXRmczEQMA4GA1UECjMHbHJhLXRmczESMBAGA1UEBjMUTW10YWthc2hpMQ4wEwYub2t5bzELMAkGA1UEBhMC
SIAwXDANBgkqhkiG9w0BAQEFAANLADBIAktF2t+iHqA2nWqt7U'YwApptgs'YVFrknXIUH
tZifBz8F0hsBelFbCT33po+9zrWzmRga8DDhxSdujmwGZH0wlDAQABolIBUzAaBgorBg
EEAYI3DQIDMQwWCjUuMC4LjIwN0YKKwyBBAGCNwlBDjEnMCUwDgxYDVROPAQH/BAQDAgT
wMBMGA1UCCsGAQUFBwMBMIH9BgorBgEEAYI3DQIDCMYHUMIHRAgEBHloATQBpAGMAcbwB
mAHQAIABSAFMAQQAgAFMAQwBoAGEAbg
-----END NEW CERTIFICATE REQUEST-----
```

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。

- ・ 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

② サーバー証明書の申し込み



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



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

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

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

- ①完了 1. 「https://」 と 「http://」 の違い
- ②完了 2. 「https://」 にする方法
- 3. 「サーバー証明書」 の選び方

認証局を選ぶ際のポイント



Q. HTTPS化できるならどの認証局でもOK？



A. そんなことはありません。

認証局のトラブルにより、
せっかく導入した証明書が

無効化されてしまった事例もあります。



無効化された事例 その1

- Symantecが発行したサーバー証明書が、
主要Webブラウザで無効化（2017～2018年）
 - Symantecは世界最大シェアの認証局だったが、
証明書発行において不手際を繰り返していると指摘
 - Chrome 70以降とFirefox 64以降において、Symantecが発行した
証明書を導入したWebサイトの閲覧がブロック

無効化された事例 その2

- Entrustが発行したサーバー証明書が、
主要Webブラウザで無効化（2024年）
 - 数年間にわたる誤発行の多さ・業界標準に従わない不適切な対応が問題視され「認証局としての能力・信頼性・完全性に関する信頼が損なわれた」として、Google・Mozillaが無効化
 - Chrome 131以降とFirefox 133以降において、Entrustがルート認証局となっている証明書を導入したWebサイトの閲覧がブロック

サーバー証明書の自動更新

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

→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、サーバー証明書の自動更新への対応が推進されています。

これらの事例や動向から言えること

サーバー証明書はいろいろな認証局から発行されています。
信頼できる認証局を選ぶことが大切です。

証明書の中には**無料**のものもありますが、
有料の証明書は、不具合・トラブルが発生した際の
サポートや、オプション機能が充実しています。

また、有効期間の短縮に伴い、**自動更新への対応**を推進する
必要があります。

ドメイン名 + サーバー証明書 = もっと安全

JPRSはドメイン名の登録管理（主に.jp）と
DNSの運用を通して、
インターネットの基盤を24時間×365日支えています。



2016年から、ドメイン名やインターネットの安全性を
より高めるべく、サーバー証明書の提供を行っています！



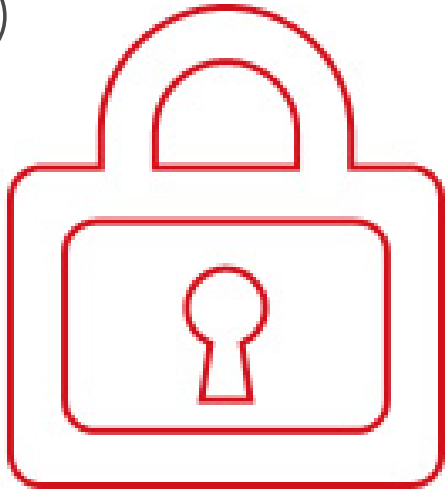
SECURED
by jPRS

HTTPS化には

安心と信頼の
JPRSサーバー証明書

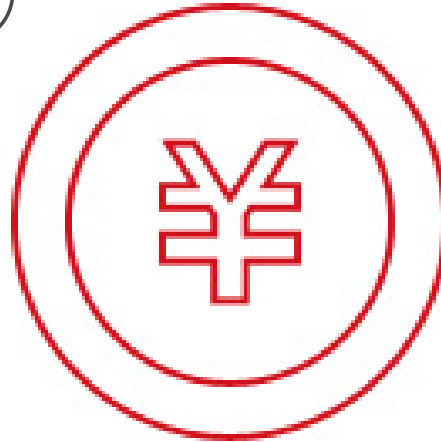
JPRSサーバー証明書の3つの特長

①



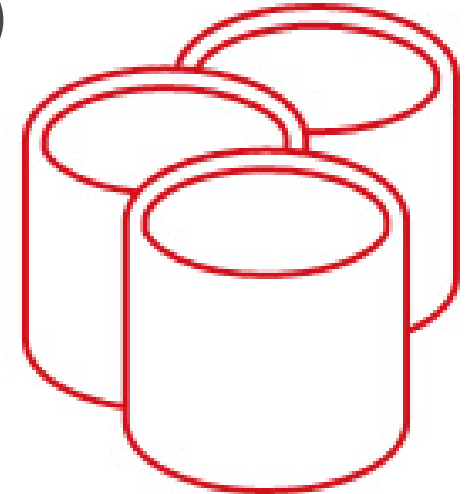
「.jp」を登録管理する
JPRSが発行する
安心と信頼の証明書

②

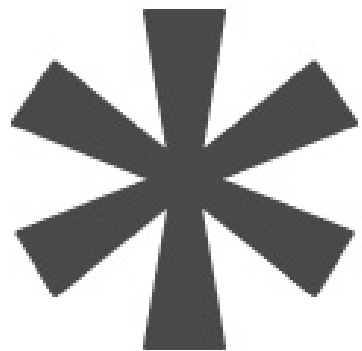


お手頃価格と
高い信頼性を
両立

③



1枚の証明書を
複数のサーバーに
導入可能



ワイルドカード対応

DV（ドメイン認証型）

OV（組織認証型）



ダブルアドレスオプションで

「www.」の有無にかかわらず
同一の証明書が利用可能



もちろん

.jp以外のドメイン名にも対応

くわしくは <https://JPRSサーバー証明書.jp> まで

JPRSサーバー証明書を取り扱い事業者は、
以下のページからご確認いただけます。



<https://JPRSサーバー証明書.jp/>

まとめ

1. 「https://」と「http://」の違い
通信が暗号化されているのが「https://」
2. 「https://」にする方法
WebサーバーにJPRSなどの認証局が発行する
サーバー証明書を設定
3. 「サーバー証明書」の選び方
信頼できる認証局を選ぶことが大切