

インターネットの通信に安全を！

押さえておきたい

# HTTPS化とサーバー証明書の基本

2023年6月14～16日

Interop Tokyo 2023

jPRS



 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**



## ■ 主な役割

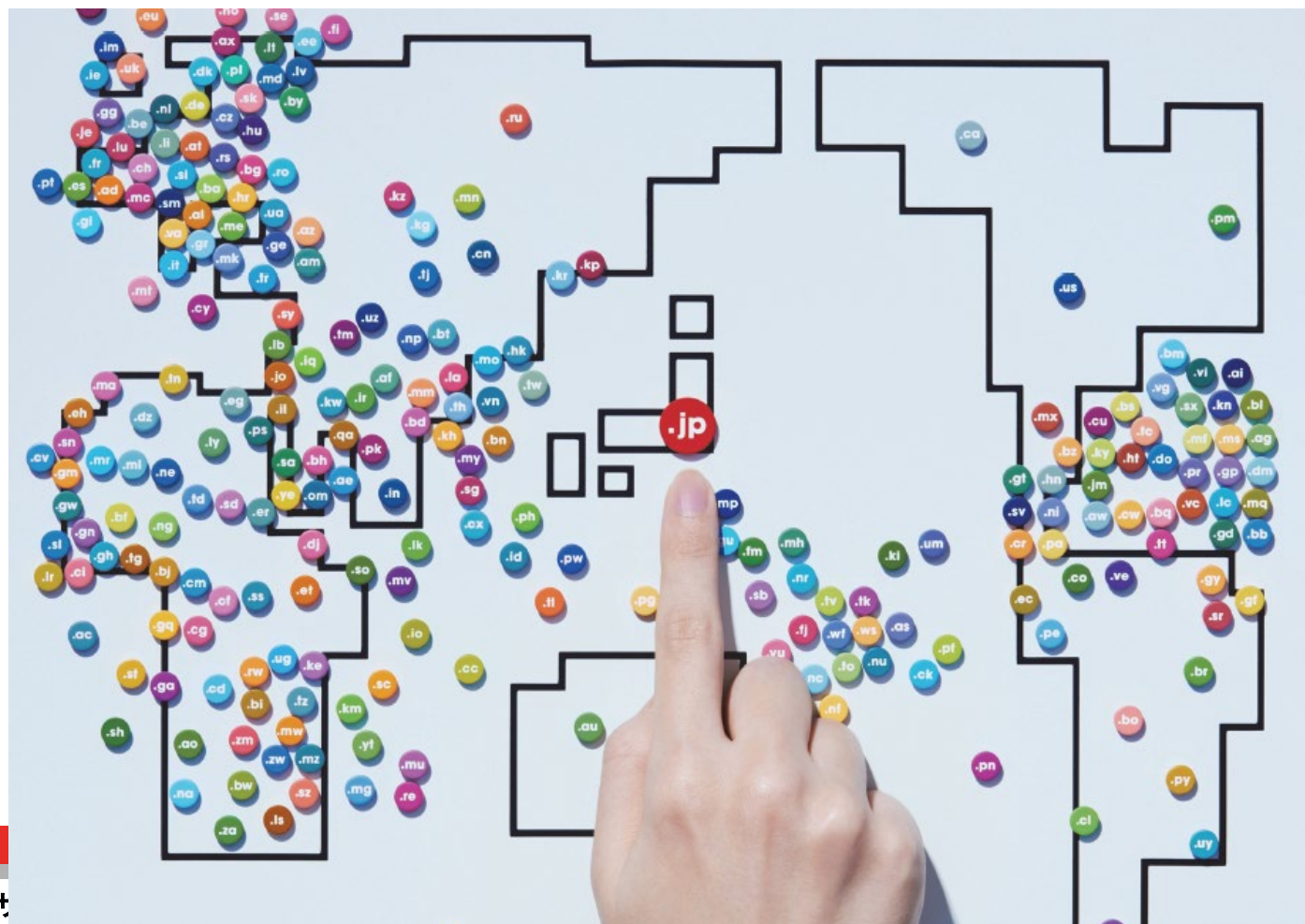
- JPドメイン名 (.jp) の登録管理
- サーバー証明書認証局
- インターネットのポリシー策定や技術の標準化など、国際活動・研究開発への貢献

# JPドメイン名とは

「.jp」は、日本を表すドメイン名です。

<https://△△△.jp>

ココのハナシです。→



# このセミナーでわかること

1. 「HTTPS」 とは何か？  
なぜ必要とされているか？
2. 「SSL/TLS対応」のために必要な  
「サーバー証明書」の概要

「サーバー証明書も解説」 篇  
<https://youtu.be/WoFUvOYj088>



「https://」と「http://」の  
違いは？


# 最近こんな表記を見かけませんか？

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」と表示されている。



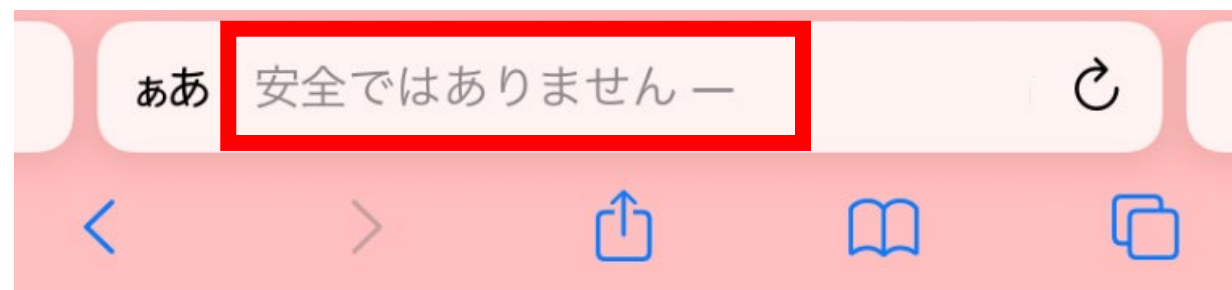
Google Chrome(グーグルクローム)の表示例

# 最近こんな表記を見かけませんか？



安全ではありません

iPhoneなどのスマートフォンでWebサイトを閲覧しているときに「安全ではありません」と表示されている。



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



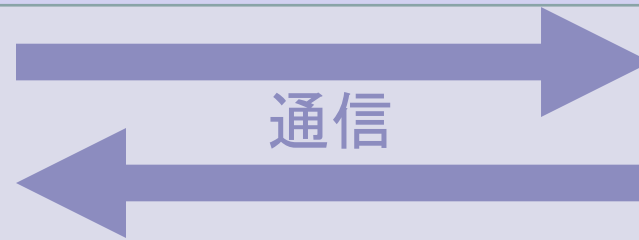
# 通信の暗号化とは？

ショッピングサイト(ECサイト)

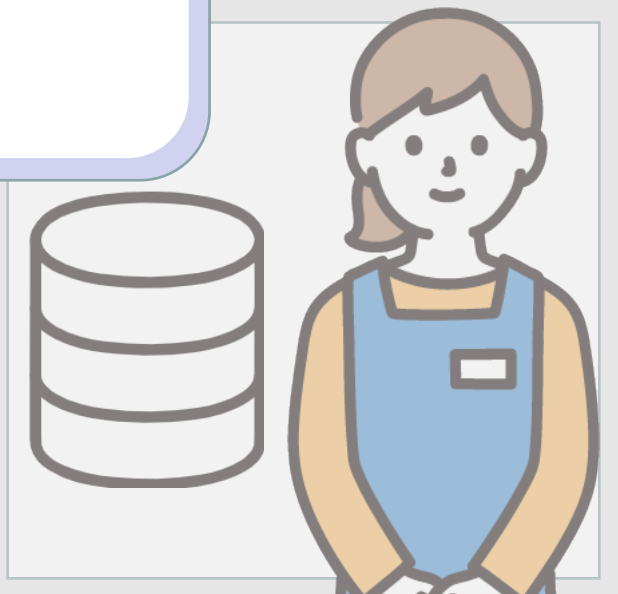
システム側

http://

暗号化されていない状態で  
送信されています



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

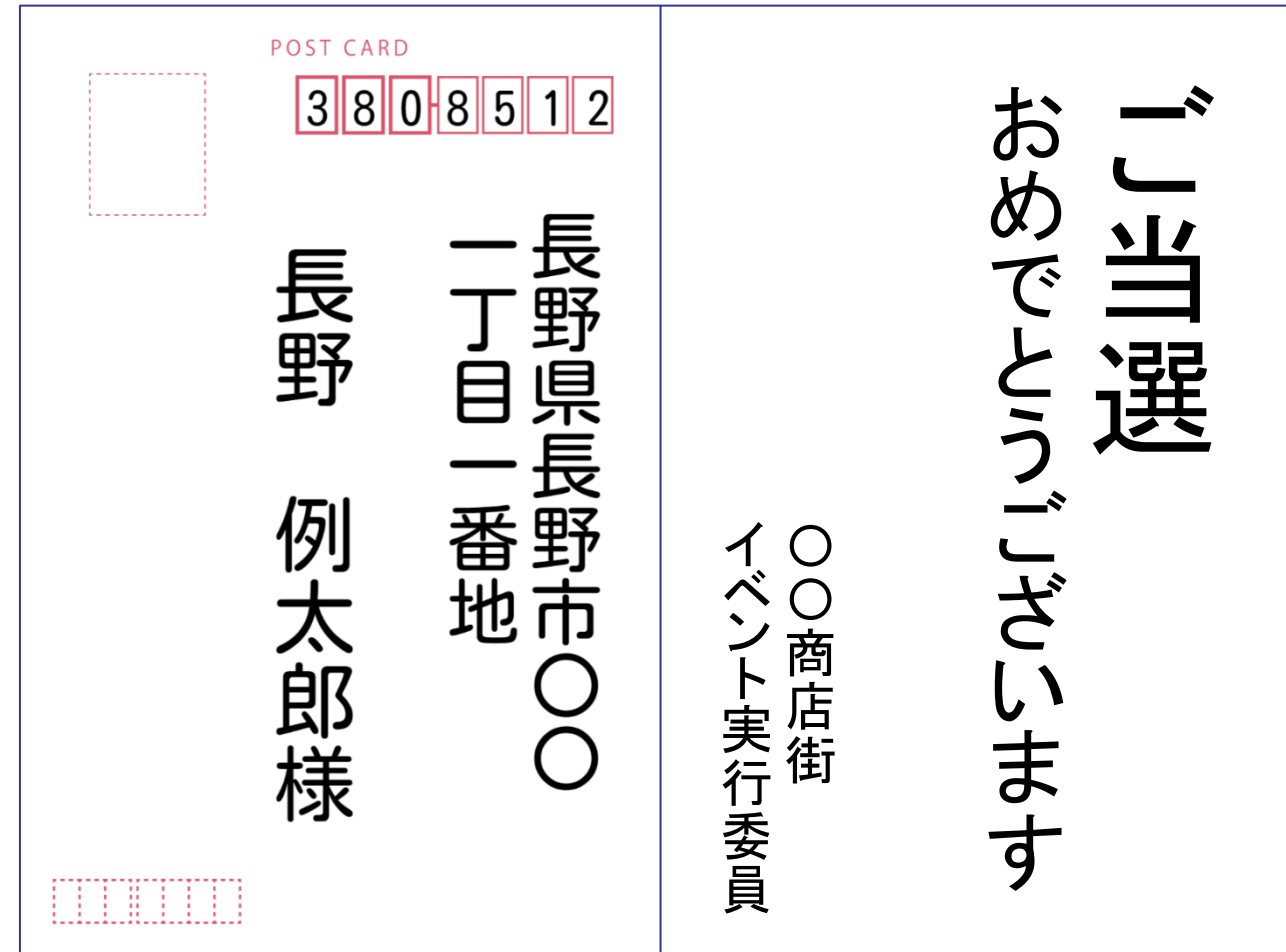
- ・覗き見る
- ・改ざんする

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



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。

つまり、悪意を持った  
第三者がその通信を

- ・覗き見る
- ・改ざんする

ことが可能な状態です



表面	裏面
<p>POST CARD</p> <p>3 8 0 8 5 1 2</p> <p>長野 例太郎様</p> <p>長野県長野市〇〇 一丁目一番地</p>	<p>〇〇商店街 イベント実行委員</p> <p><b>落選です</b> またご応募ください</p>

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)

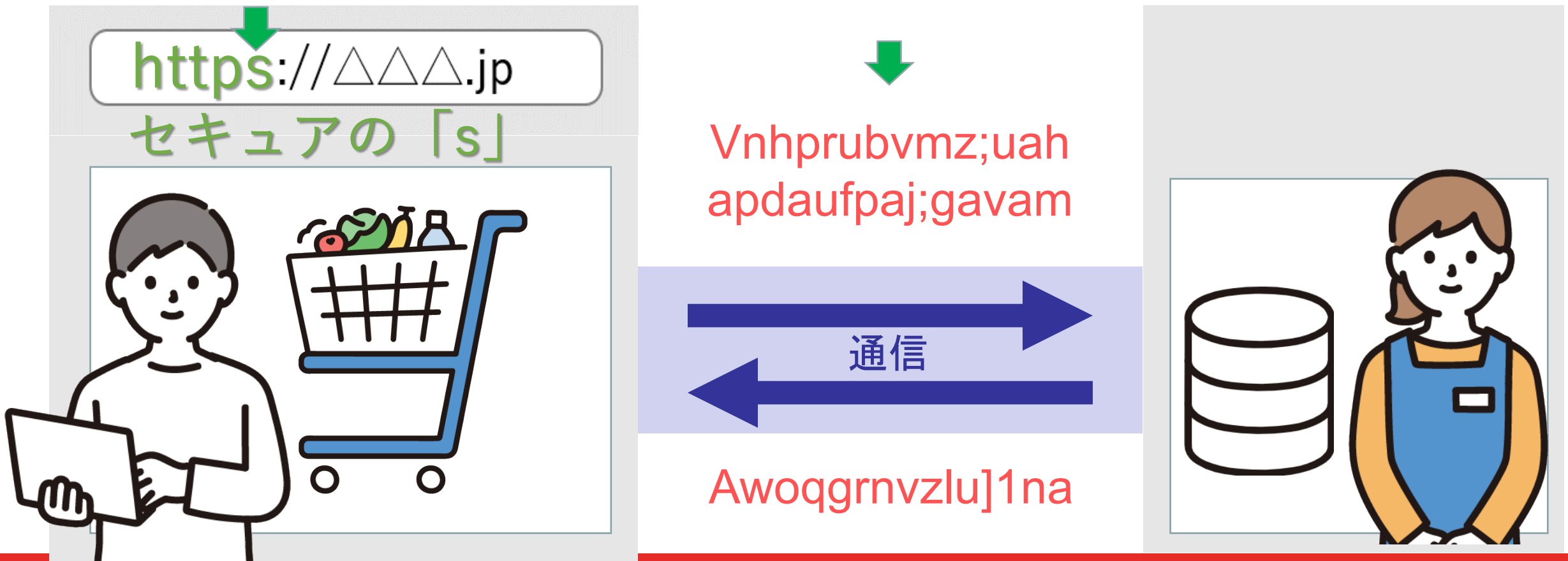
が必要になっています

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
<p>POST CARD</p> <p>3 8 0 8 5 1 2</p> <p>長野 例太郎様</p> <p>長野県長野市〇〇 一丁目一番地</p>	<p>asoifgajgapampogahavb pgvanagiutam; leajgn; ai@2qjwnavlkaga, gkapg uuapoi thgnkanmluoiaeu thgnlma: iaoutganlkda; pp: f: akm ka</p> <p>はがきに <b>保護シール</b>を 貼るイメージです (文字を暗号化)</p> <p>r ,oi nga; ,ou; ,arjgajeopaj eofaj; aeo; jgietupewqyr</p>

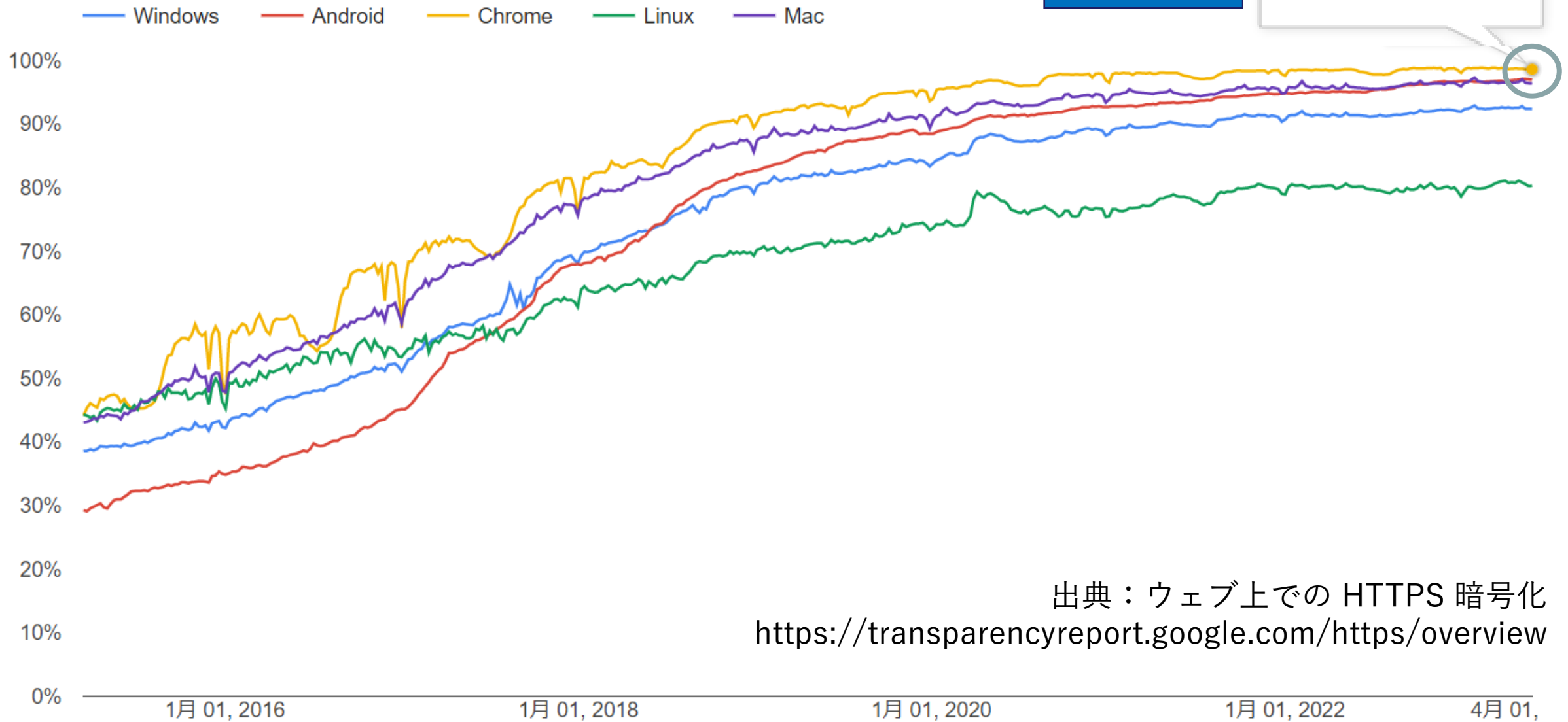
# SSL/TLS対応 (暗号化)した ショッピングサイト(ECサイト)

## 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)



拡大

2023/05/27  
Chrome: 99%

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、99%が「https://」である

# このセミナーでわかること

完了

「HTTPS」 とは何か？  
なぜ必要とされているか？

2. 「SSL/TLS対応」のために必要な  
「サーバー証明書」の概要

どうやってHTTPS化する？

# HTTPS化するために必要な「証明書」

- 運転免許証
- 社員証
- 卒業証書
- パスポート、といったもの

…ではなく **サーバー証明書** が必要です。

# 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。  
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

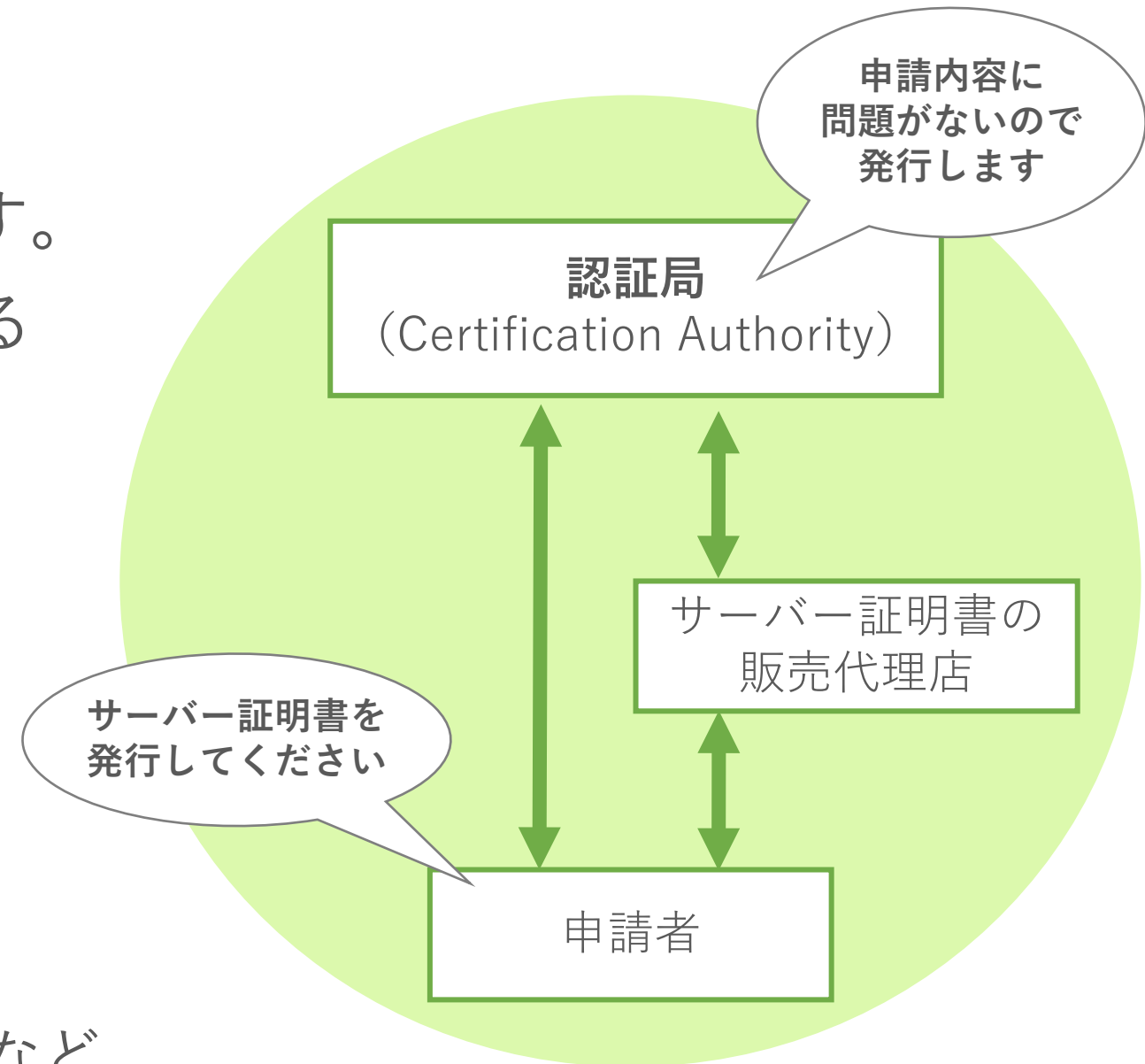
申請元の組織や企業が実在していることを

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  
申

CSRのサンプル

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIICdzCCAIECAQAwZzEQMA4GA1UEAxMHbHJhLXRmczEQMA4GA1UECzMmHbHJhLXRmczESMBAGA1UEBxMUTWl0YWthc2hpMQ4wEwYub2t5bzELMAkGA1UEBhMC
SIAwXDANBgkqhkiG9w0BAQEFAANLADBIAktF2t+iHqA2nWqt7U'YwApptgs'YVFrknXIUH
tZifBz8F0hsBelFbCT33po+9zrWzmRga8DDhxSdujmwGZH0wlDAQABolIBUzAaBgorBg
EEAYI3DQIDM0wMCjUuMC4LjIwN0YKKwYBBAGCNwIBDjEnMCUwDgYDVROPAQH/BAQDAgT
wMBMGA1UCCsGAQUFBwMBMIH9BgorBgEEAYI3DQIDM0YHUuMIHrAgEBHloATQBpAGMAcbwB
mAHQAIABSAMQQAQAFMAQwBoAGEAbg
-----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！

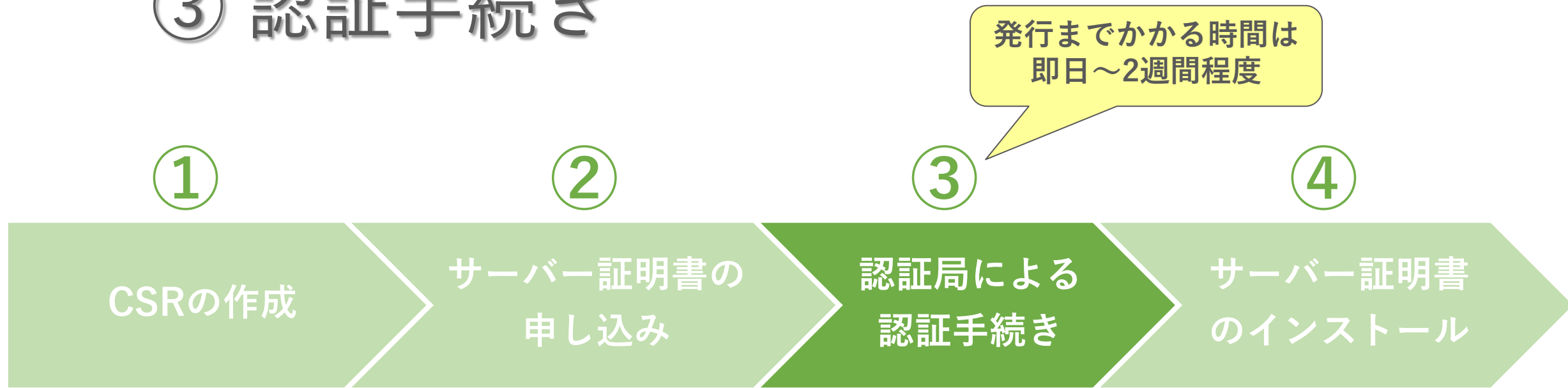
**DV**  
(ドメイン認証型)

**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。

# サーバー証明書の自動更新

サーバー証明書の有効期間が、2020年9月から、それまでの最長2年から最長1年に短縮されました。

また2023年3月にGoogleは、将来的に最大有効期間を90日間に短縮する方針を発表しました（実施時期未定）。

→有効期間が短縮されると更新頻度が増えるため、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が推進されつつあります。

# 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。



# 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！



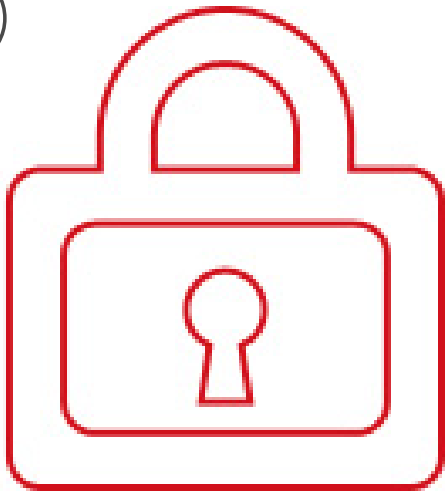
SECURED  
by jPRS

安心と信頼の  
JPRSサーバー証明書

HTTPS化には

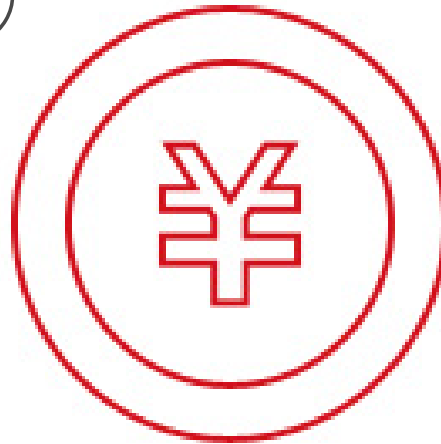
# JPRSサーバー証明書の3つの特長

①



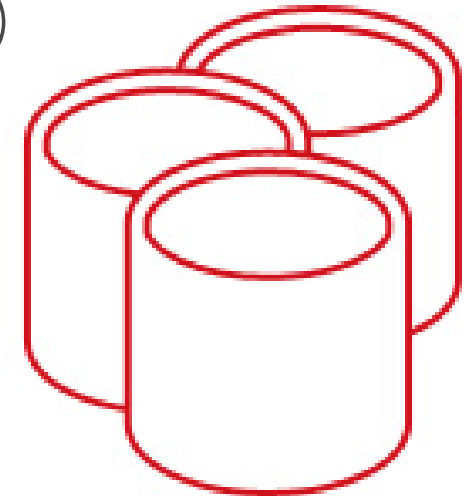
「.jp」を登録管理する  
JPRSが発行する  
安心と信頼の証明書

②

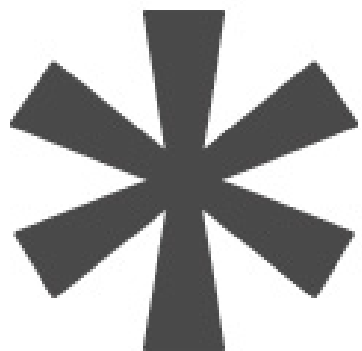


お手頃価格と  
高い信頼性を  
両立

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/>