サーバー証明書の基礎知識

～そのWebサイトは安全ですか？～

2024年6月12～14日

Interop Tokyo 2024

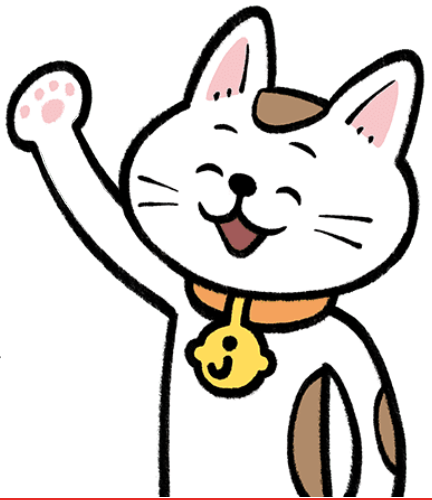
講演者について（1/2）

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



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

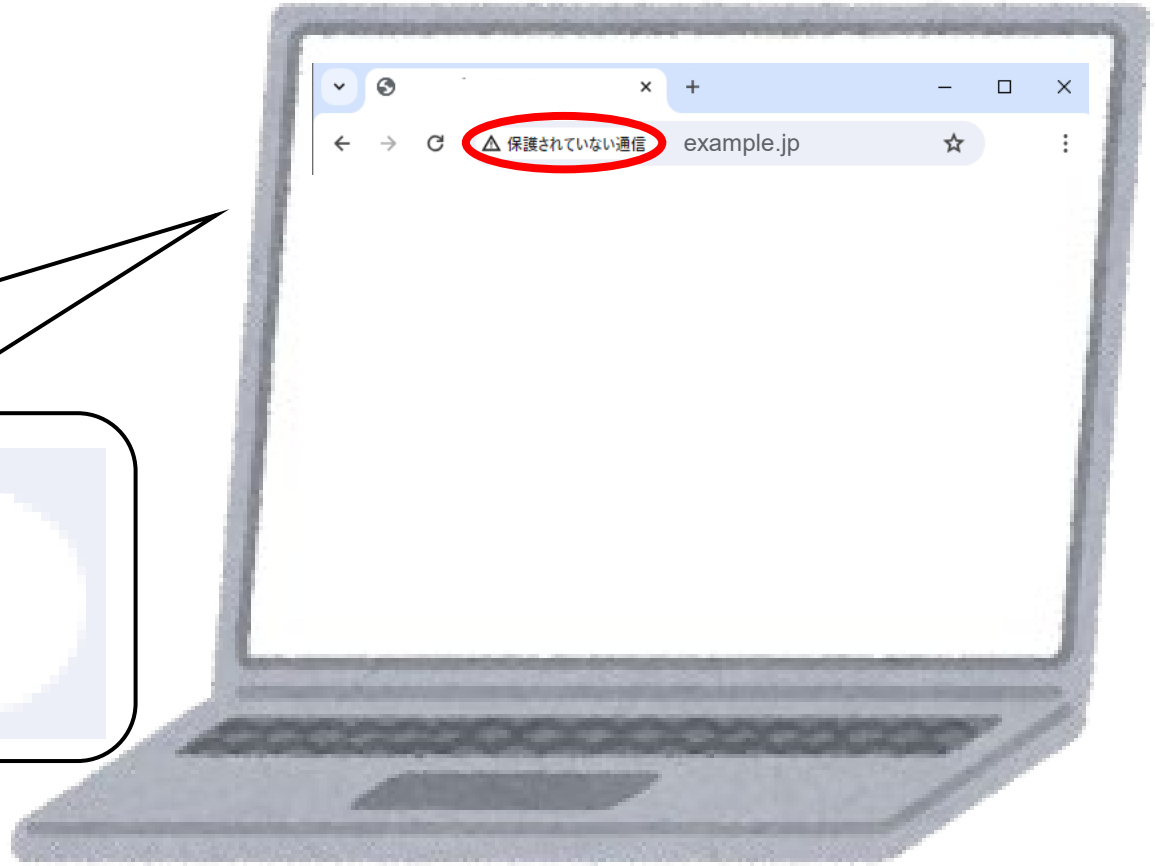
「サーバー証明書も解説」篇
https://youtu.be/WoFUvOYjO88

「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

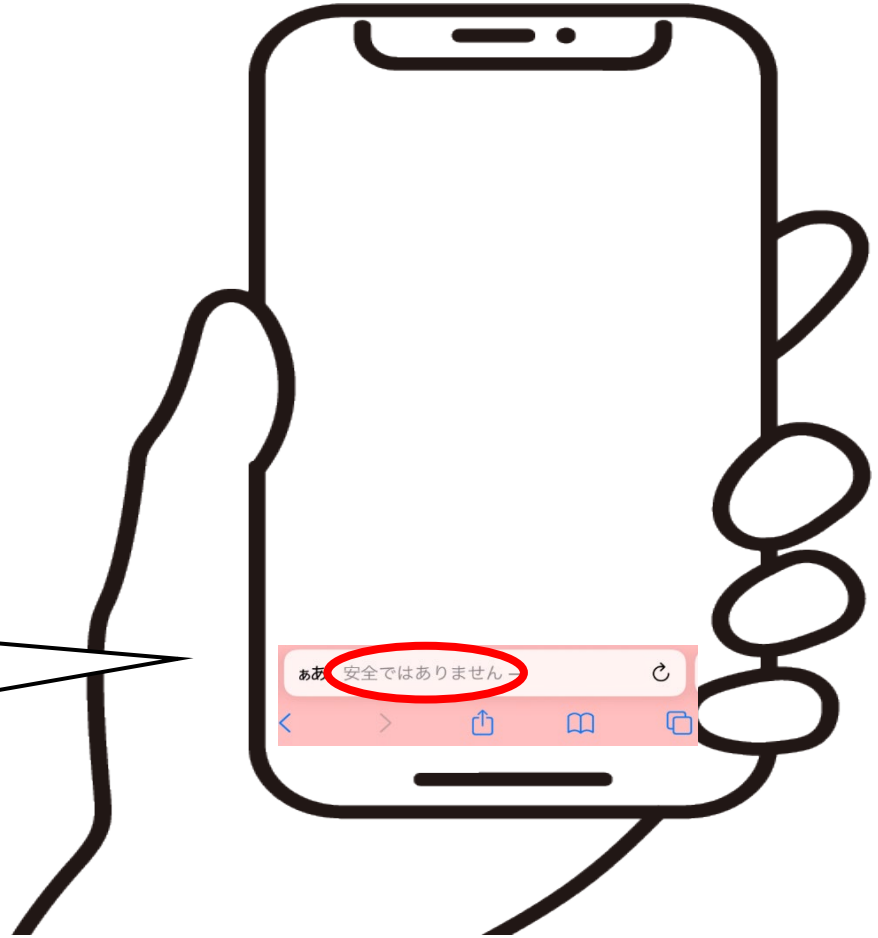


Google Chrome（グーグルクローム）の表示例

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？

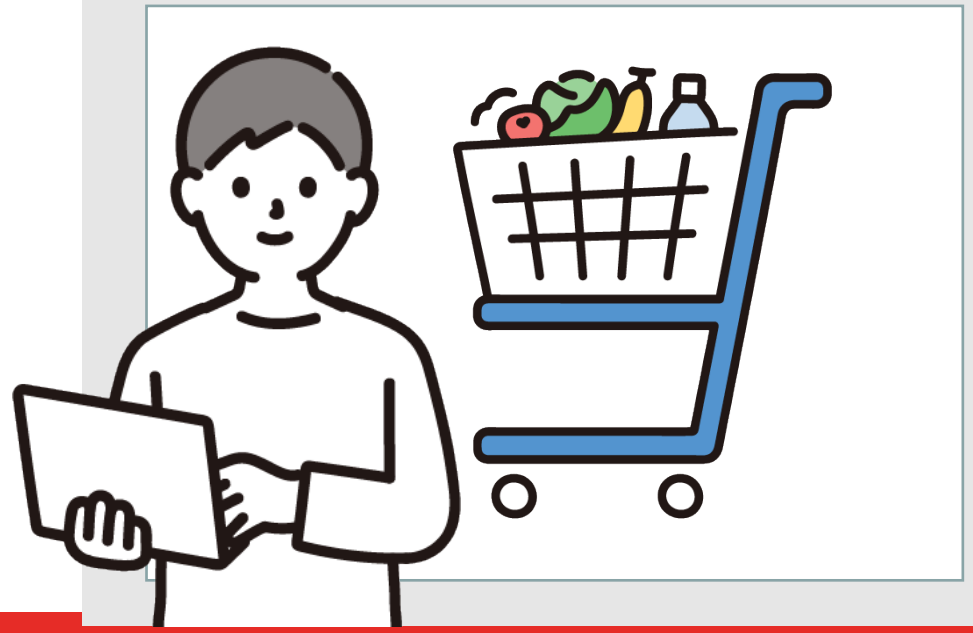
「安全ではありません」だから、
ここで買うと危険なのかな？

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

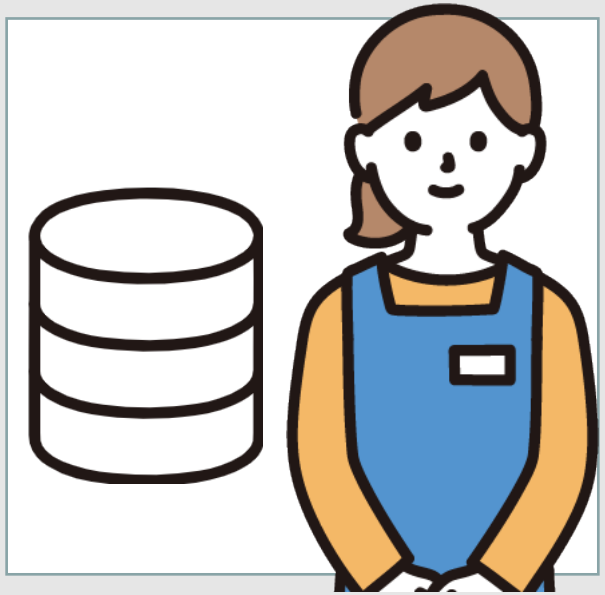


リンゴを1つ
買います

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）

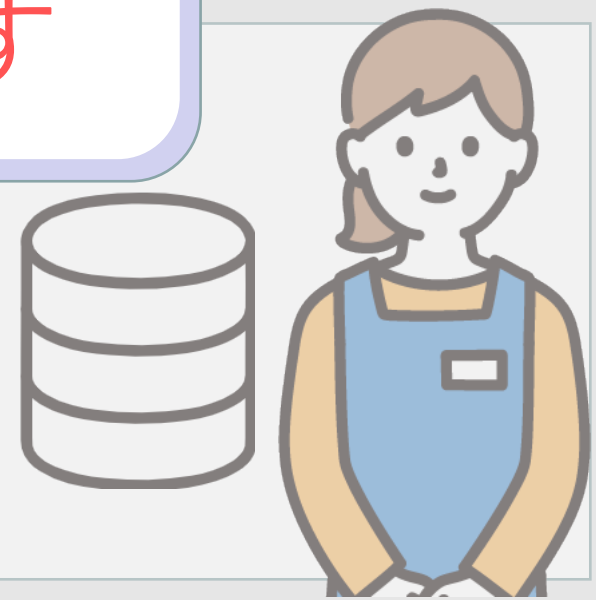
システム側

http:/

暗号化されていない状態で
情報が送信されています

通信

受け付けました

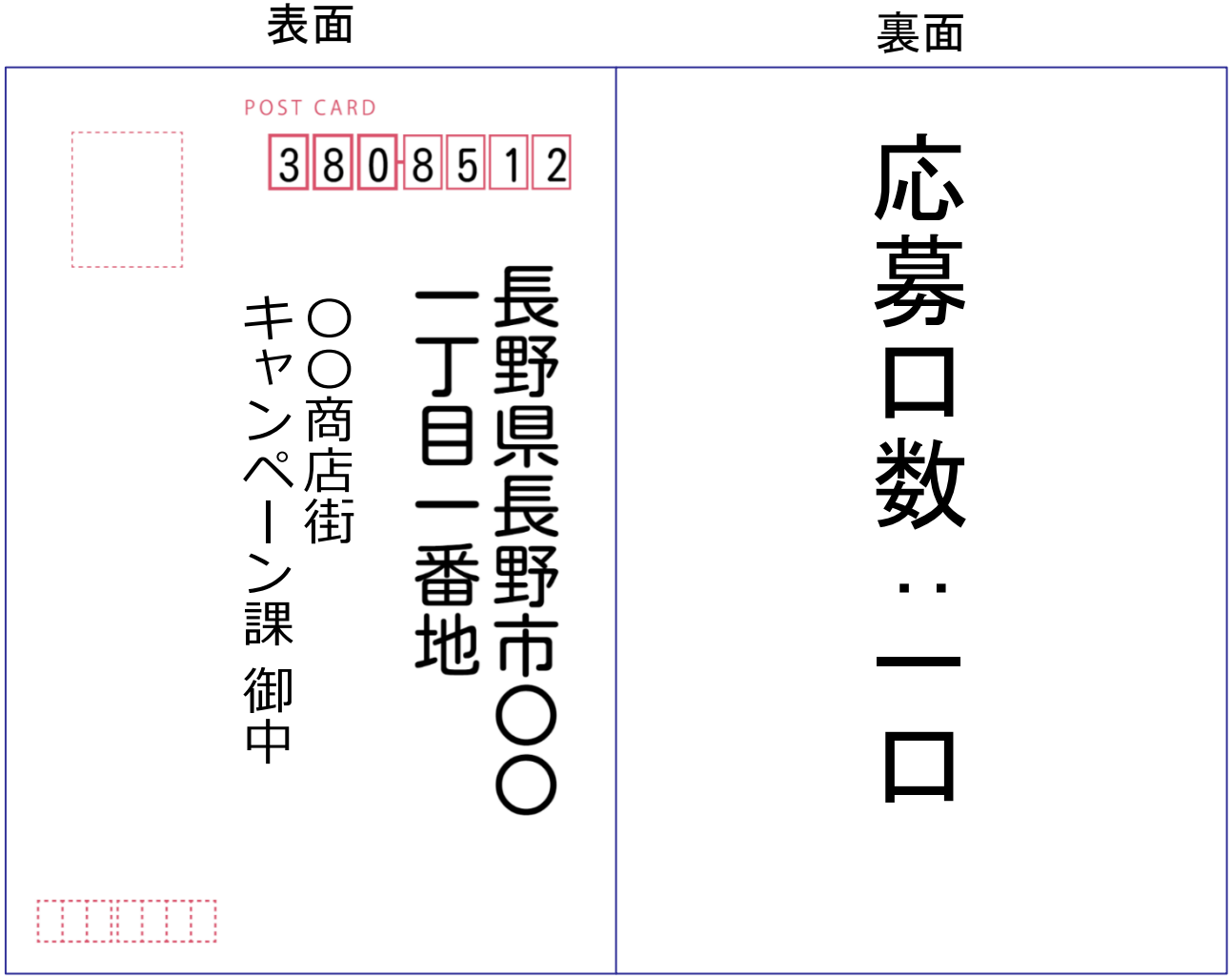


インターネット上の通信のことを
はがきを使ってご説明します。

つまり、悪意を持った
第三者がその通信を

- のぞき見る
- 改ざんする

ことが可能な状態です

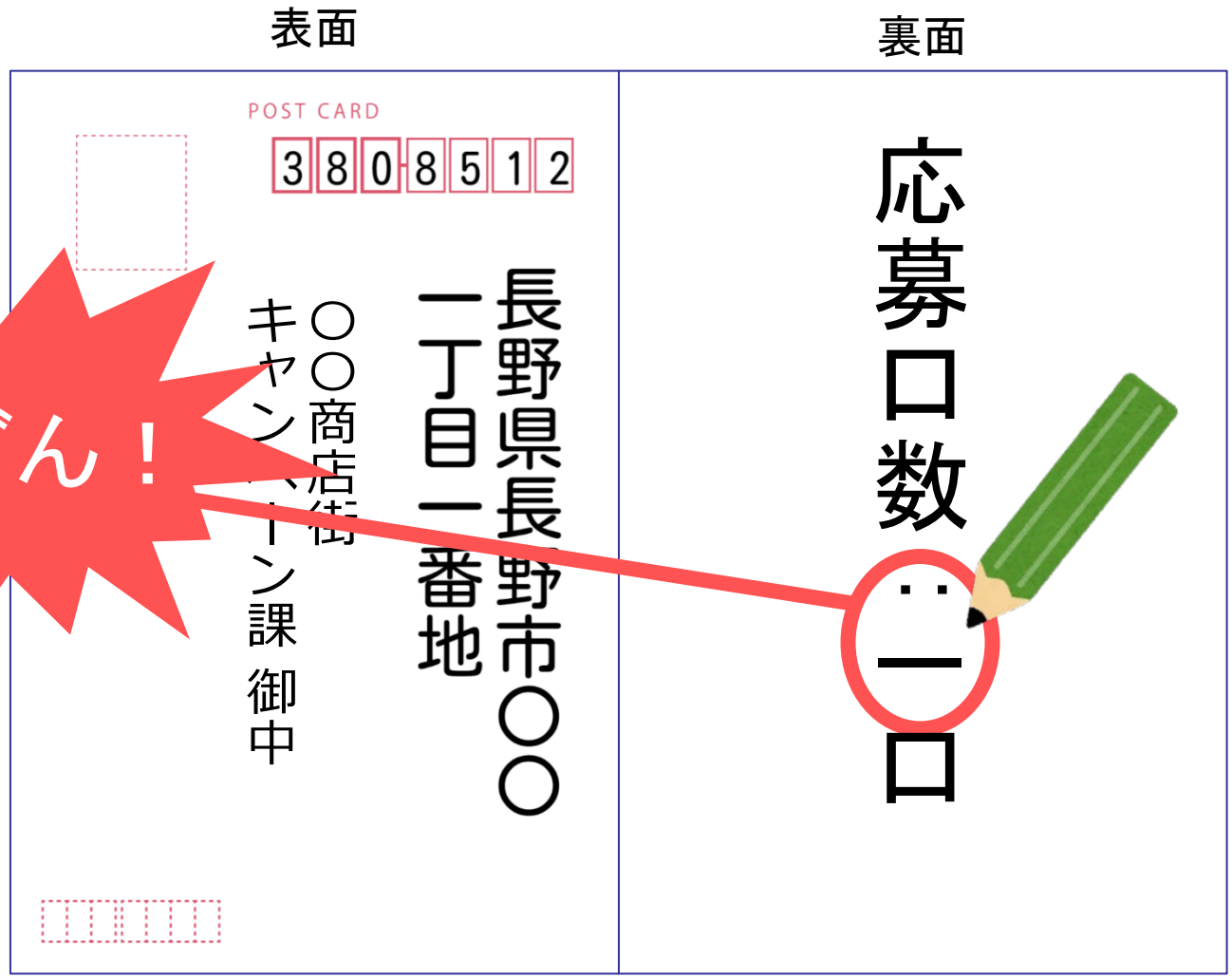


インターネット上の通信のことを
はがきを使ってご説明します。

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



こういった行為への
対応策として

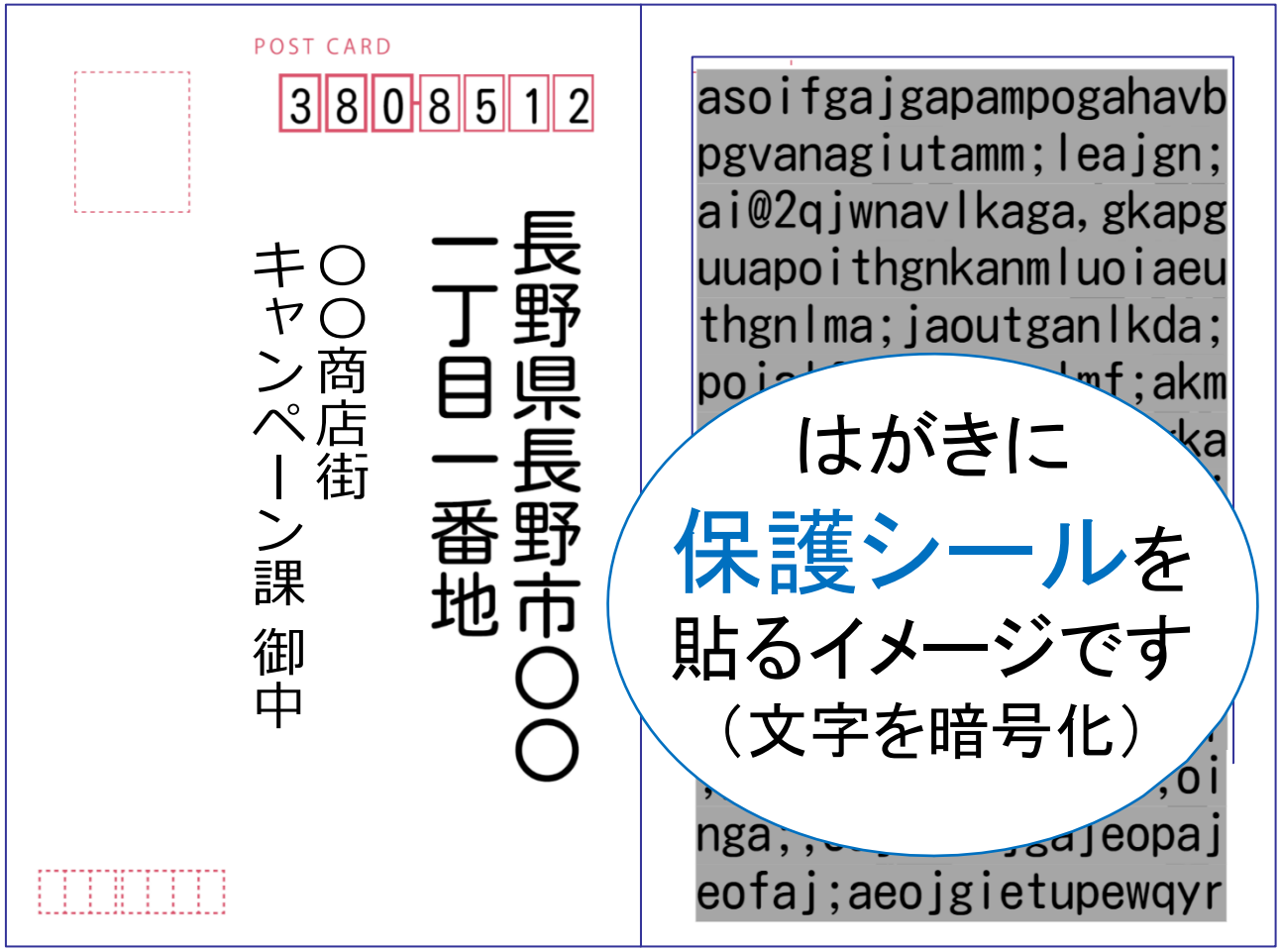
通信の暗号化
（SSL/TLS対応）

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）

https://△△△.jp

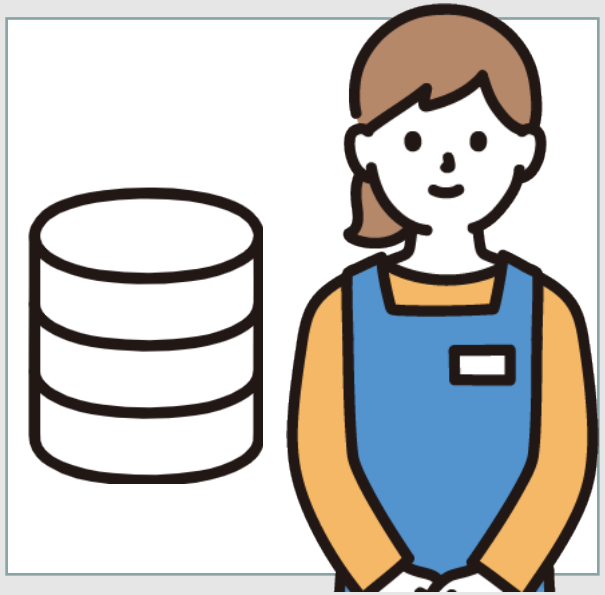
セキュアの「s」

Vnhprubvmz;uah
apdaufpaj;gavam

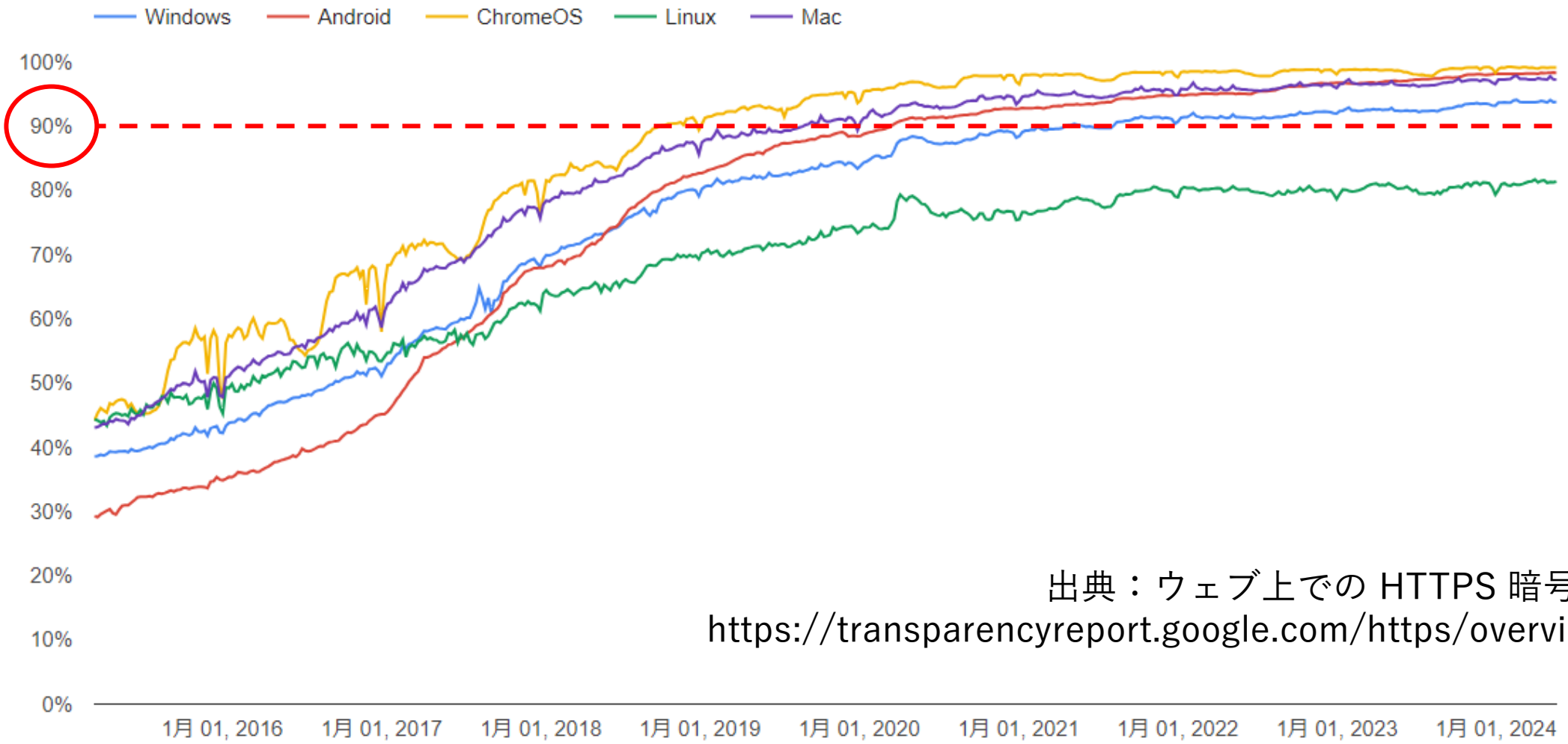
通信

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 「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「https://」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

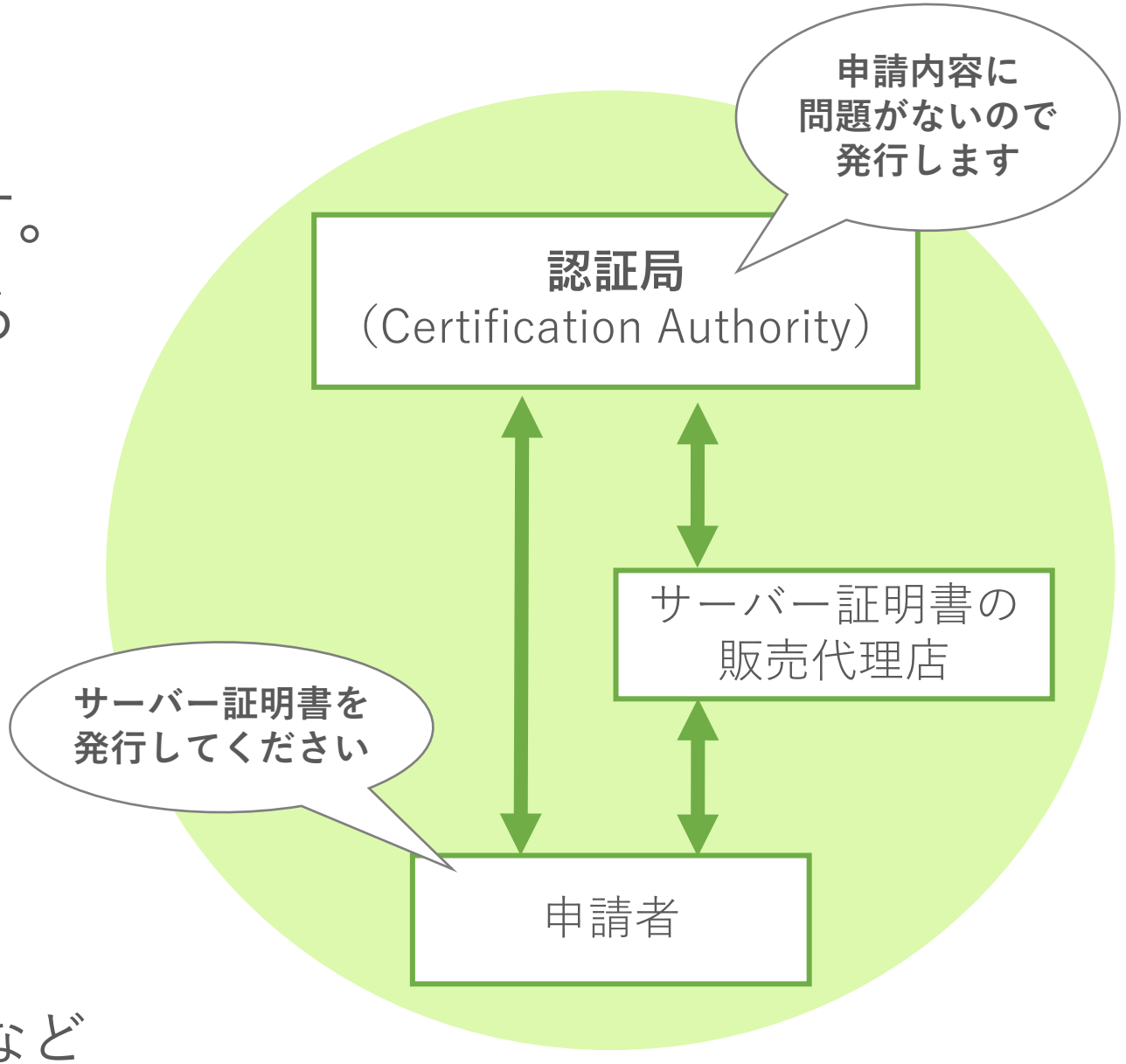
を

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	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**
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 → サーバ申

CSRのサンプル

```
----BEGIN NEW CERTIFICATE REQUEST-----
MIICdzCCAiECAQAwZzEQMA4GA1UEAxMHbHJhLXRmczEQMA4GA1UECxMHczEQMA4GA1UE
ChMHbHJhLXRmczESMBAGA1UEBxMJTWIOYWthc2hpMQ4wEwVUb2t5bzELMAkGA1UEBhMC
SIAwXDANBgkqhkiG9w0BAQEFAANLADBIAktF2t+iHqA2nWqt7UYwApptgsYvFrkmXIUH
tZifBz8FOhsBelFbCT33po+9zrWzmRga8DDhxSdujmxGZHOwIDAQABoIIBUzAaBgorBg
EEAYI3DQIDMQwWCjUuMC4LjIwNQYKKwYBBAGCNwIBDjEnMCUwDgYDVR0PAQH/BAQDAgT
wMBMGA1UCCsGAQUFBwMBMIH9BgorBgEEAYI3DQICMYHuMIHrAgEBHloATQBpAGMAcbwB
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。

- **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 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

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

発行までかかる時間は
即日～2週間程度

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

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

1. 完了 「https://」と「http://」の違い
2. 完了 「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

- 中国最大の認証局WoSignと子会社StartComが発行したサーバー証明書が、主要Webブラウザで無効化
  - ずさんな管理体制や組織ぐるみの不正行為が発覚したことによるもの

※ WoSignは2017年8月にWoTrus CA Limitedに社名を変更していますが、本資料では著名な旧社名・サービス名であるWoSignのままとしています。

無効化された事例 その2

- 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
  - Symantecは世界最大シェアの認証局だったが、Googleは証明書発行で同社が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の証明書を導入している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。

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、自動更新に対応しているサービスもあります。

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

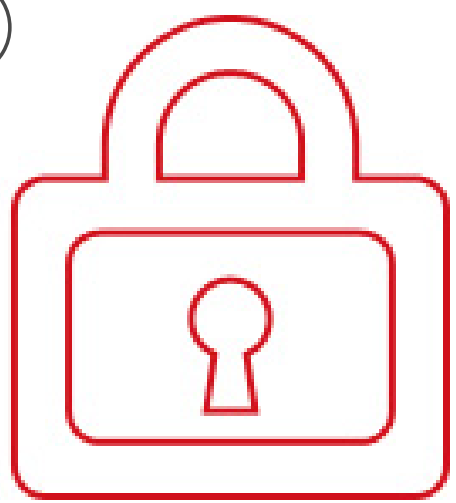
HTTPS化には

安心と信頼の

JPRSサーバー証明書

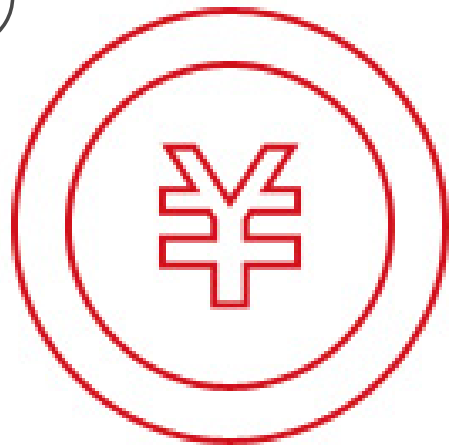
JPRSサーバー証明書の3つの特長

①



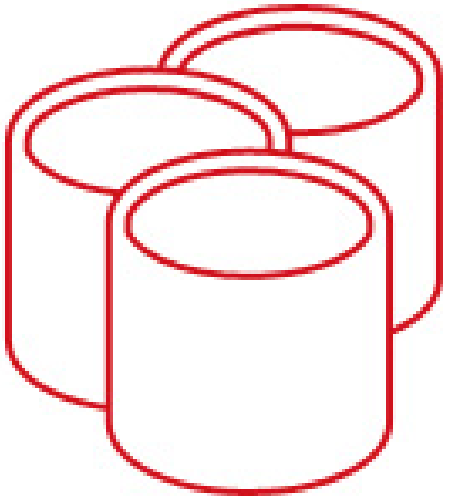
「.jp」を登録管理する
JPRSが発行する
安心と信頼の証明書

②

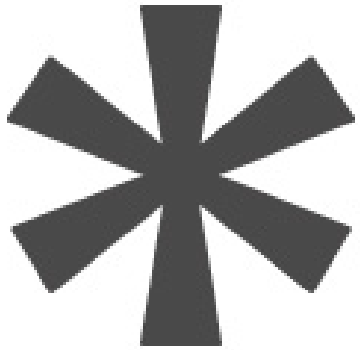


お手頃価格と
高い信頼性を
両立

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サーバー証明書の取り扱い事業者は、
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