2016年10月20日
第57回JPドメイン名諮問委員会
資料4

サーバー証明書について

2016年10月20日（木）

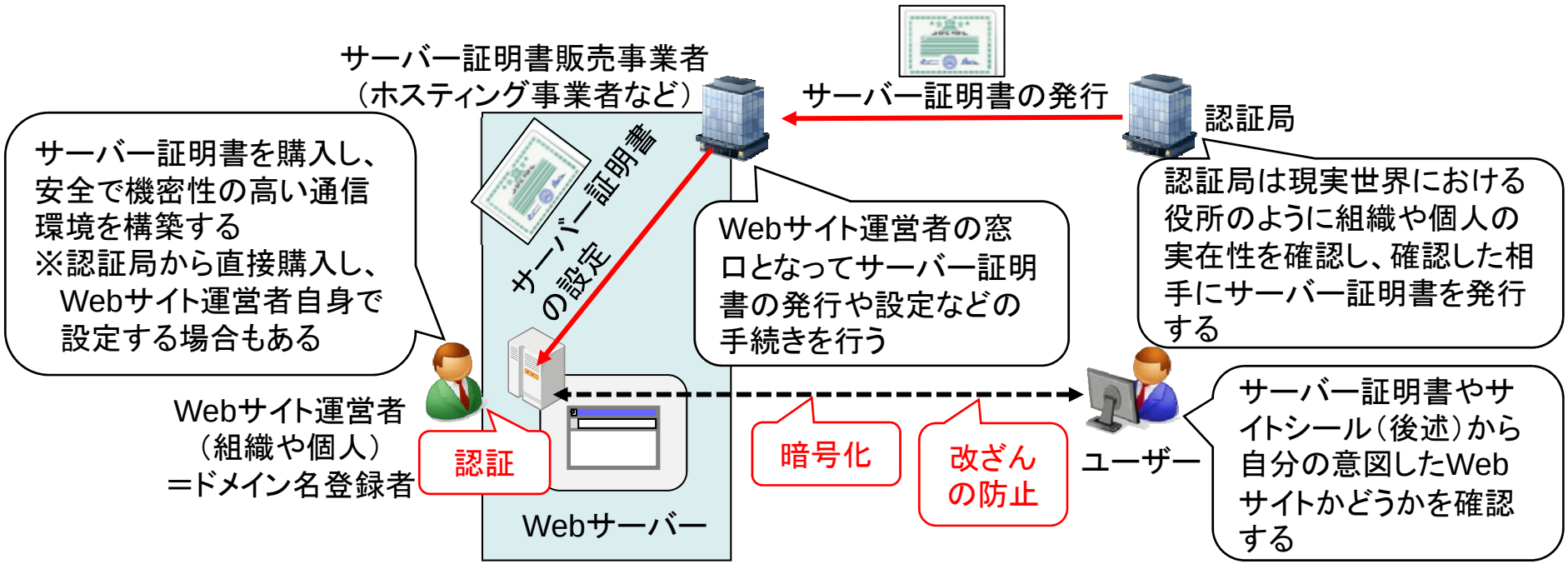
株式会社日本レジストリサービス

JPRSサーバー証明書発行サービス

- 2016年4月から、ドメイン名利用の安全性・信頼性を向上させる新サービスとして提供開始
- サービス開始の背景
  - サーバー証明書に対する社会のニーズの高まり
    - インターネット利用における、より高い安全性・信頼性の確保
- 当社が指定事業者を通じてドメイン名とサーバー証明書の双方を併せて提供することで、より高い安全性・信頼性を実現可能に
- その結果、インターネット全体の安全性・信頼性にも貢献

サーバー証明書の仕組み

- サーバー証明書
  - 認証局（CA）と呼ばれる第三者機関がドメイン名の登録者や組織の実在性を確認し、サーバー証明書を発行
  - サーバー証明書がWebサイトに設定されることにより、ユーザーは、そのWebサイトの内容が期待するWebサイト運営者のものであることが確認できる



サーバー証明書の三つの役割

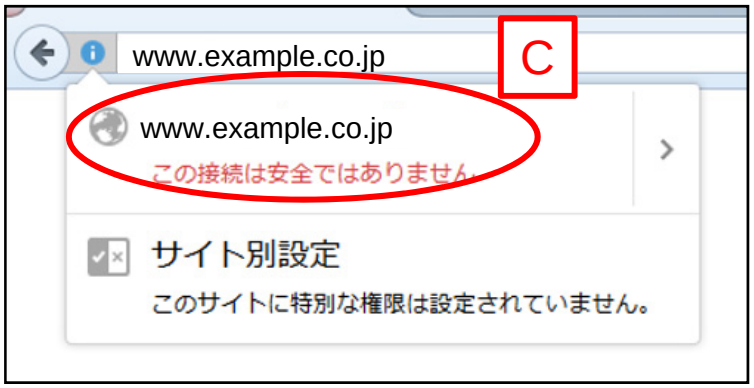
- サーバー証明書には、次の三つの役割がある
  1. 認証
     - Webサイト運営者の身元を証明し、なりすましを防止する
  2. 通信の暗号化
     - WebサーバーとWebブラウザーの間のデータとのやりとり（通信）を暗号化し、第三者がそのやりとりを盗み見ること（盗聴）から保護する
  3. 改ざんの防止
     - 受け取ったデータが途中で書き換えられたり、一部が失われたりしていないことを確認する

（参考）サーバー証明書の種類

- Domain Validation（DV）
  - 当該ドメイン名の登録者であることのみを確認
- Organization Validation（OV）
  - その組織が確かに存在すること（実在性）を、電話調査や登記簿確認など、所定の手段で確認した上で発行される証明書
  - DV証明書よりも一段上の信頼性を確保
- Extended Validation（EV）
  - 業界の統一基準に基づく厳密な認証を経て発行
  - EV証明書用の特別な表示
    - Webブラウザーのアドレスバーが緑色になり、組織名がその横に表示されるなど
  - OV証明書よりも一段上の信頼性を確保

アクセスしているWebサイトにサーバー証明書が付されているかの確認方法（1/2）

- 以下のような形で視覚的に確認可能
  - アドレスバーに鍵（南京錠）マークが表示されている（A）
  - アドレスバーのURLが「https://」で始まっている（B）
  - Webブラウザーに警告メッセージが表示されていない（C）



Firefoxの場合

※Webブラウザーによって、サーバー証明書が付されているかの確認方法は異なる場合がある

アクセスしているWebサイトにサーバー証明書が付されているかの確認方法（2/2）

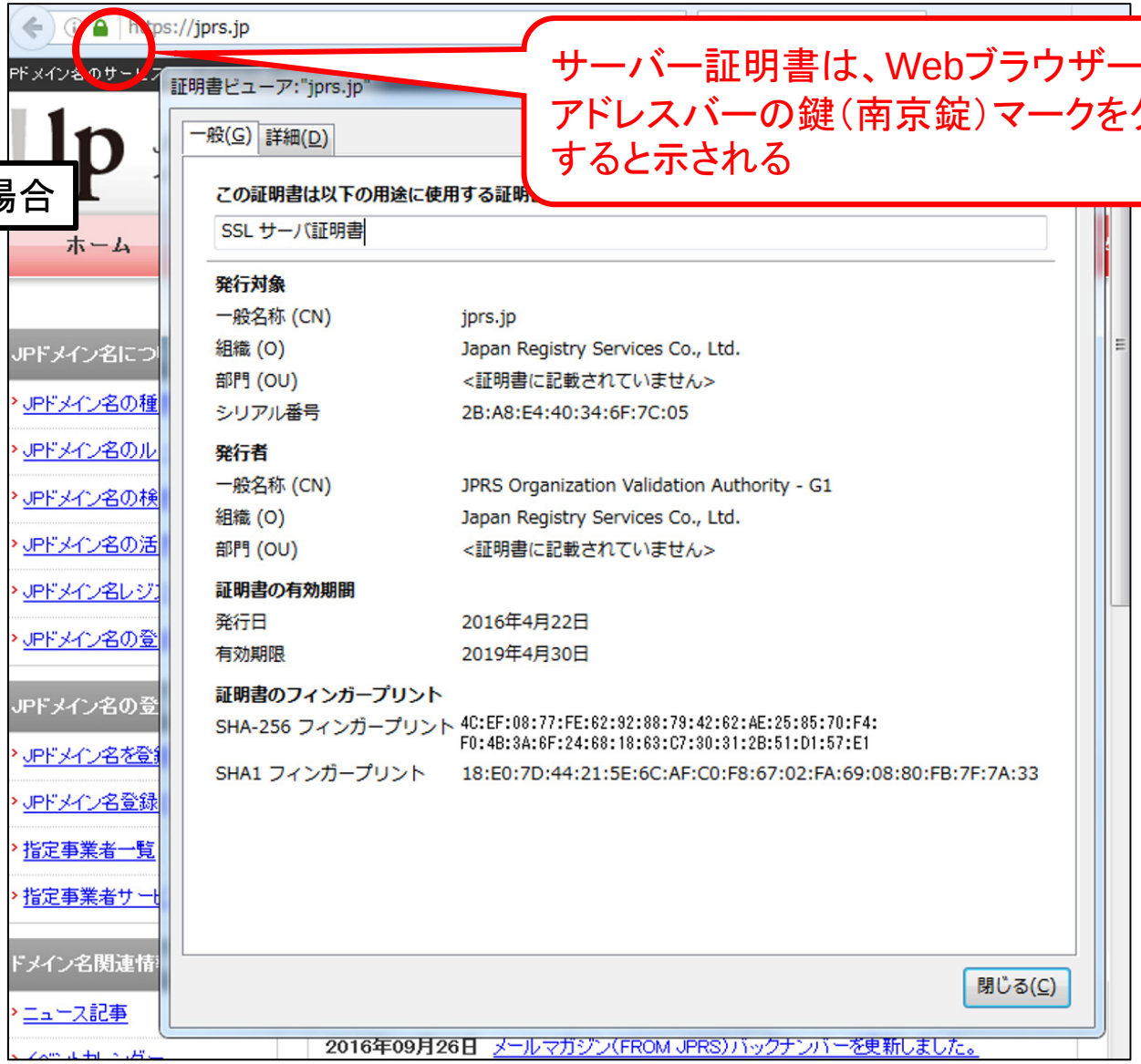
- 確認できること
  - アクセス先のWebサーバーは本物である
    - サーバー証明書の情報を表示・確認するとより確実
  - WebサーバーとWebブラウザーの間の通信が暗号化されている
  - Webサーバーから受け取ったデータが改ざんされていない

- サーバー証明書の内容の確認方法
  - Webブラウザーのアドレスバーの鍵（南京錠）マークをクリック
  - Webサイトのサイトシールが設置されている場合にはそれをクリック

※Webブラウザーによって、サーバー証明書が付されているかの確認方法は異なる場合がある

サーバー証明書の事例：JPRSのWebサイト

Firefoxの場合



サーバー証明書は、Webブラウザーのアドレスバーの鍵（南京錠）マークをクリックすると示される

サイトシールとは

- Webサイト運営者がユーザーに対し、Webサイトの安全性やセキュリティに配慮したWebサイトであることをより強くアピールできるようにするために画面に表示するシール
- サーバー証明書の発行者がサービスとして提供
- ユーザーがサイトシールをクリックすることで、インストールされているサーバー証明書の詳細を確認可能

（例：JPRSのサーバー証明書のサイトシール）

ドメイン認証型（DV）

組織認証型（OV）

サイトシールの事例：JPRSのWebサイト

サーバー証明書の詳細が、サイトシールをクリックすると示される
（一部の認証局では画像を表示させるだけでクリックできないものもある）

Web Site Profile

このWebサイトのサーバー証明書は有効です

サーバー証明書の内容は以下の通りです

コモンネーム	jprs.jp
上記以外のコモンネーム	www.jprs.jp
有効期限	2016年04月22日～2019年04月30日
ステータス	有効
証明書の種類	組織認証（OV）
組織名	Japan Registry Services Co., Ltd.
住所	JP TOKYO CHIYODA

以下をご確認ください

1. ブラウザに証明書に関する警告が表示されていないこと
2. アクセス先のURLが https://jprs.jp/ または https://www.jprs.jp/ から始まっていること
3. 本ページのURLが https://sitesealinfo.pubcert.jprs.jp/SiteSealReference から始まっていること

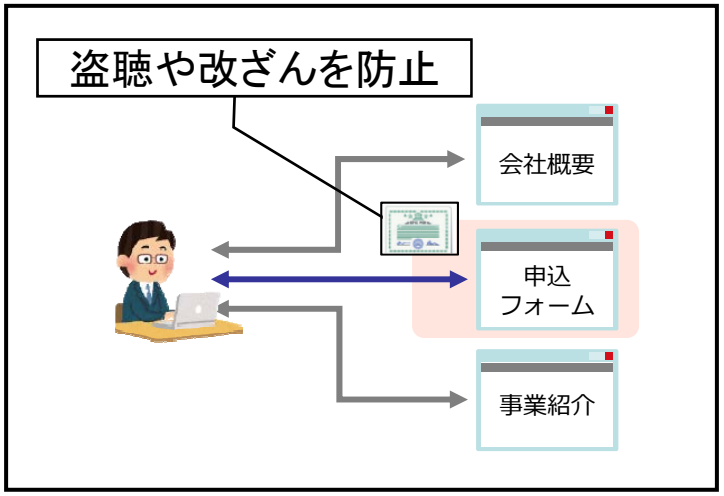
上記3点が確認できた場合、JPRS認証局は以下の内容を証明します。

通信の暗号化	https://jprs.jp/ または https://www.jprs.jp/ で始まるページは、ブラウザとサーバー間の通信が暗号化されていること
サイト運営者	jprs.jp ドメインのWebサイトが、Japan Registry Services Co., Ltd. によって運営されていること
運営者の法的実在性	Japan Registry Services Co., Ltd. が法的に実在する組織であり、jprs.jp またはwww.jprs.jp を運営していること

※コモンネームに「*」が含まれている場合、当該箇所は任意の文字列となります。

サーバー証明書導入のメリット（通信の暗号化・改ざん防止）

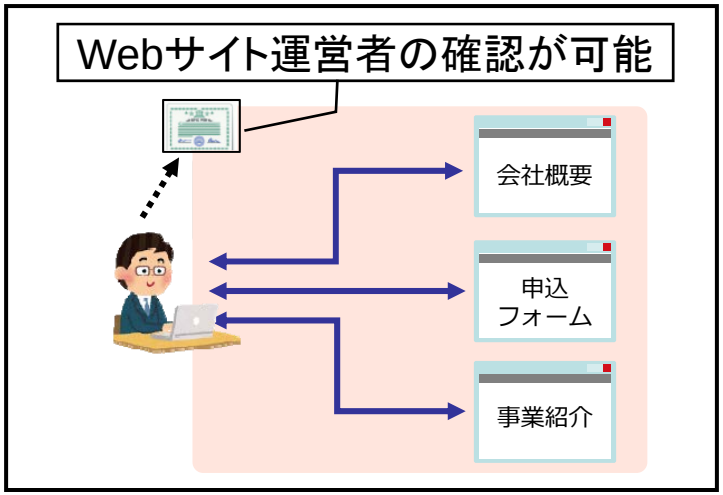
- 通信路における機密情報の保護ができ、また、データの改ざんを防止できる
  - 暗号化された通信方式（HTTPS）が利用可能
  - 従来からECサイトやネットバンキングサービスを中心に、広く使われている



  - セキュリティやプライバシーに対する意識の高まりにより、通常のWebサイトにおいても、利用が広まり始めている

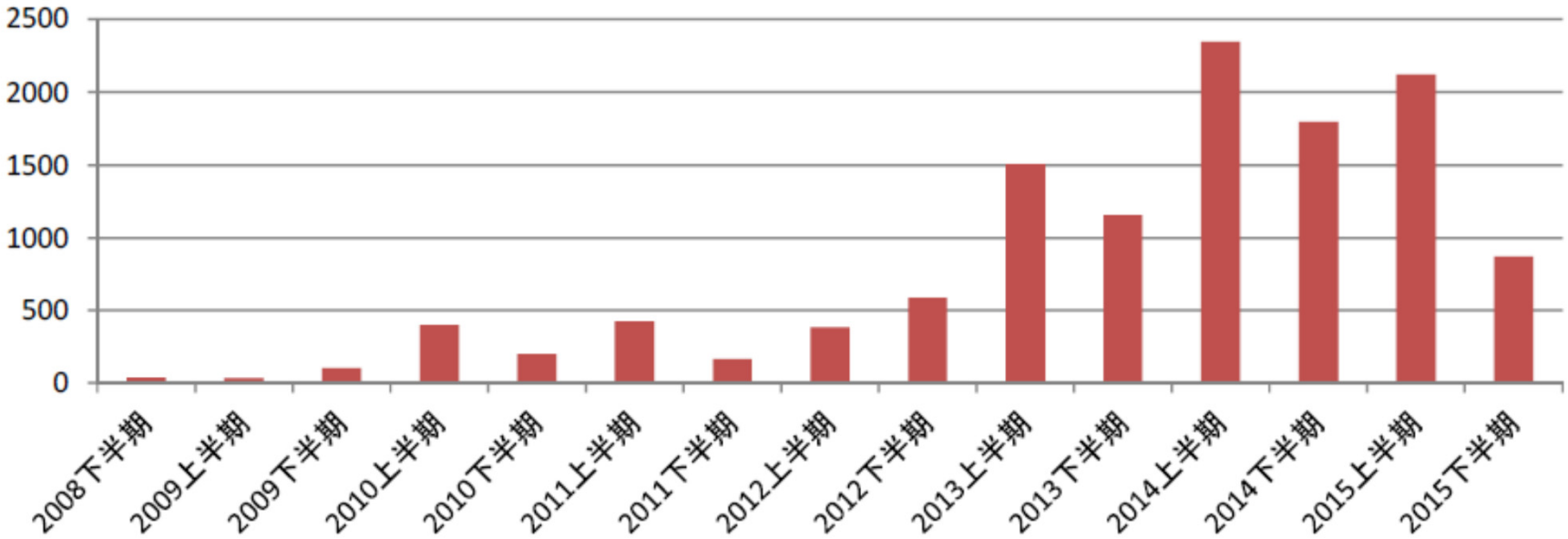
サーバー証明書導入のメリット（サーバーの認証）

- アクセスしたWebサイトが誰によって提供されているかを、ユーザーが確認できる
  - フィッシングなどにより偽のWebサイトに誘導されたことに気付くことができる可能性が高まる
  - 2015年に発見されたフィッシング詐欺サイトの件数は過去最多を記録



（参考）フィッシングの動向（国内の状況）

- フィッシング対策協議会が公表しているフィッシングサイトの件数

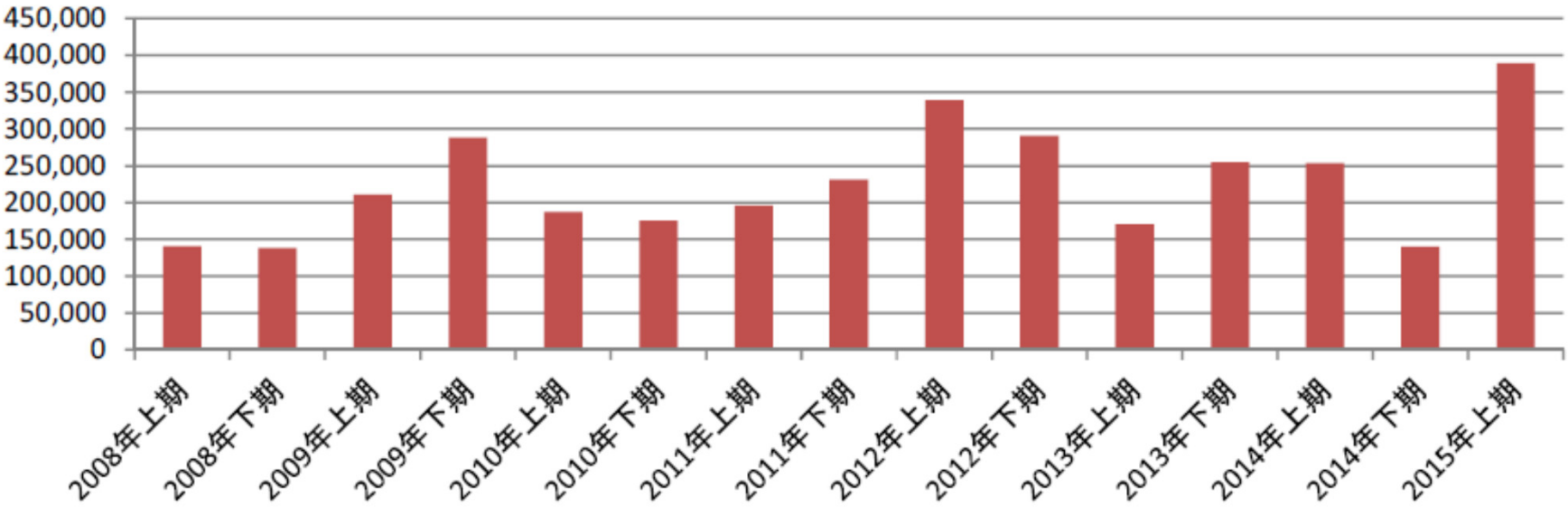


フィッシング対策協議会 ガイドライン策定ワーキンググループ,「フィッシングレポート2016」
<https://www.antiphishing.jp/report/pdf/phishing_report_2016.pdf>

（参考）フィッシングの動向（海外の状況）

- APWG（※）が公表しているフィッシングサイトの件数

  ※APWG（Anti-Phishing Working Group）は、サイバー犯罪へのグローバルな対応を統一することに焦点を当てた、グローバルな産業界、法執行機関、政府機関の連合。



フィッシング対策協議会 ガイドライン策定ワーキンググループ,「フィッシングレポート2016」
<https://www.antiphishing.jp/report/pdf/phishing_report_2016.pdf>

サーバー証明書導入の追加メリット

- 検索順位への影響
  - GoogleではWebサイト全体のHTTPS化を推奨しており、検索エンジンの順位決定の要因として、Webサイト全体をHTTPS化しているかどうかを考慮することを公表
  - Webサイト全体をHTTPS化することがSEO（※）（Search Engine Optimization：検索エンジン最適化）に効果があると言われている

※SEOとは、サーチエンジンの検索結果のページの表示順の上位に自らのWebサイトが表示されるように工夫すること。また、そのための技術やサービス。<http://e-words.jp/w/SEO.html>

- Webサイト表示の高速化
  - 主要なブラウザーの最新版では、従来よりも高速なブラウジングを実現するHTTP（通信プロトコル）の新バージョンであるHTTP/2の対応が進んでいるが、サーバー証明書を設定したWebページでしかHTTP/2は使えない
  - Webサイト表示の高速化にも、Webサイト全体をHTTPS化することが重要となる

JPRSサーバー証明書サービスの意義

- ドメイン名利用の安全性・信頼性を向上させる新サービスとして提供開始
  - ドメイン名サービスの一環として、JPRSがこれまで培ってきた高い安全性・信頼性で提供
  - ドメイン名登録者に対して、レジストリかつ認証局という立場から、サーバー証明書の発行の際に確実な確認を行い、不正なサーバー証明書の発行を検知するための枠組みを構築できる可能性（今後検討）