

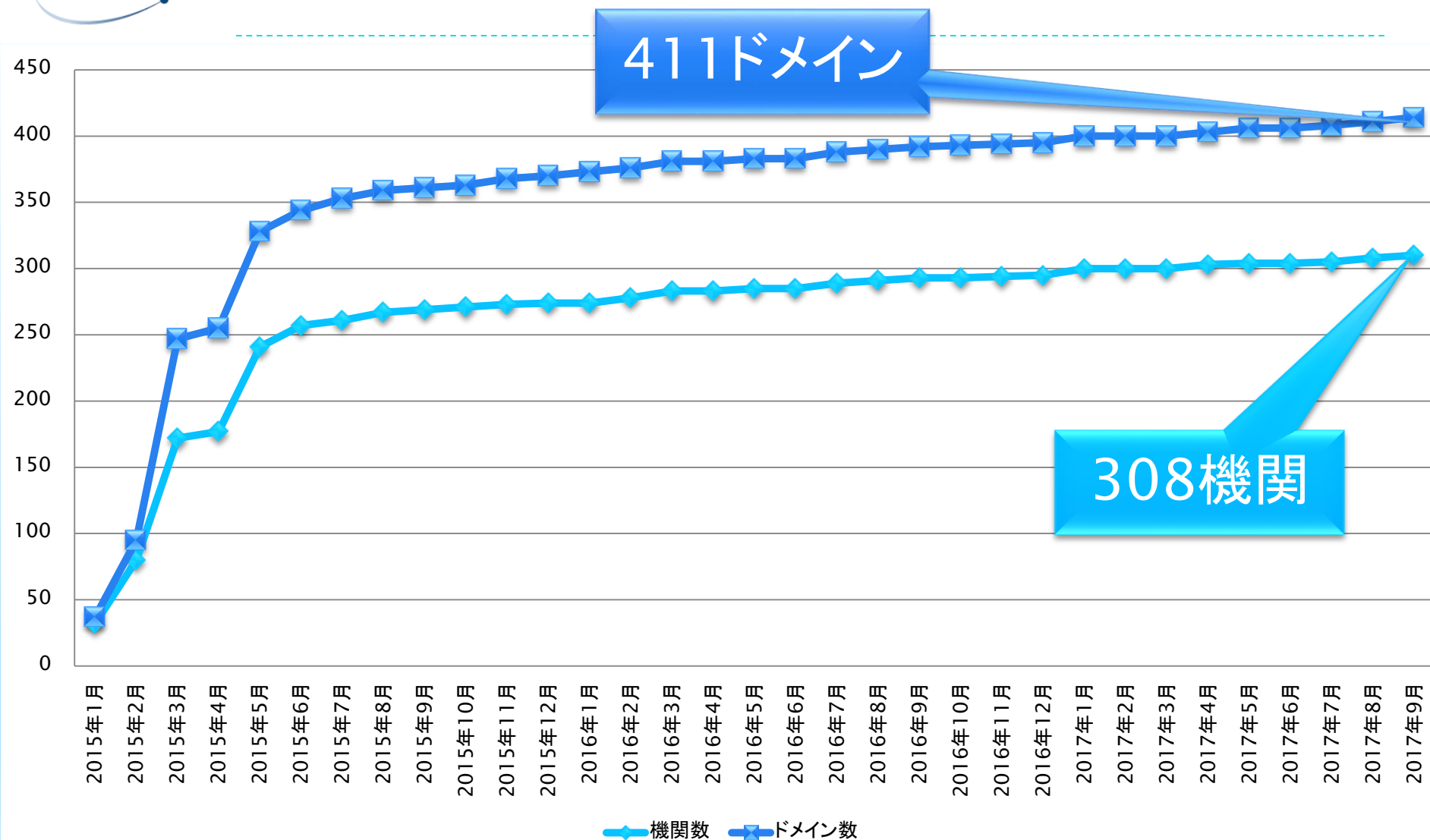


UPKI電子証明書発行サービス アップデート

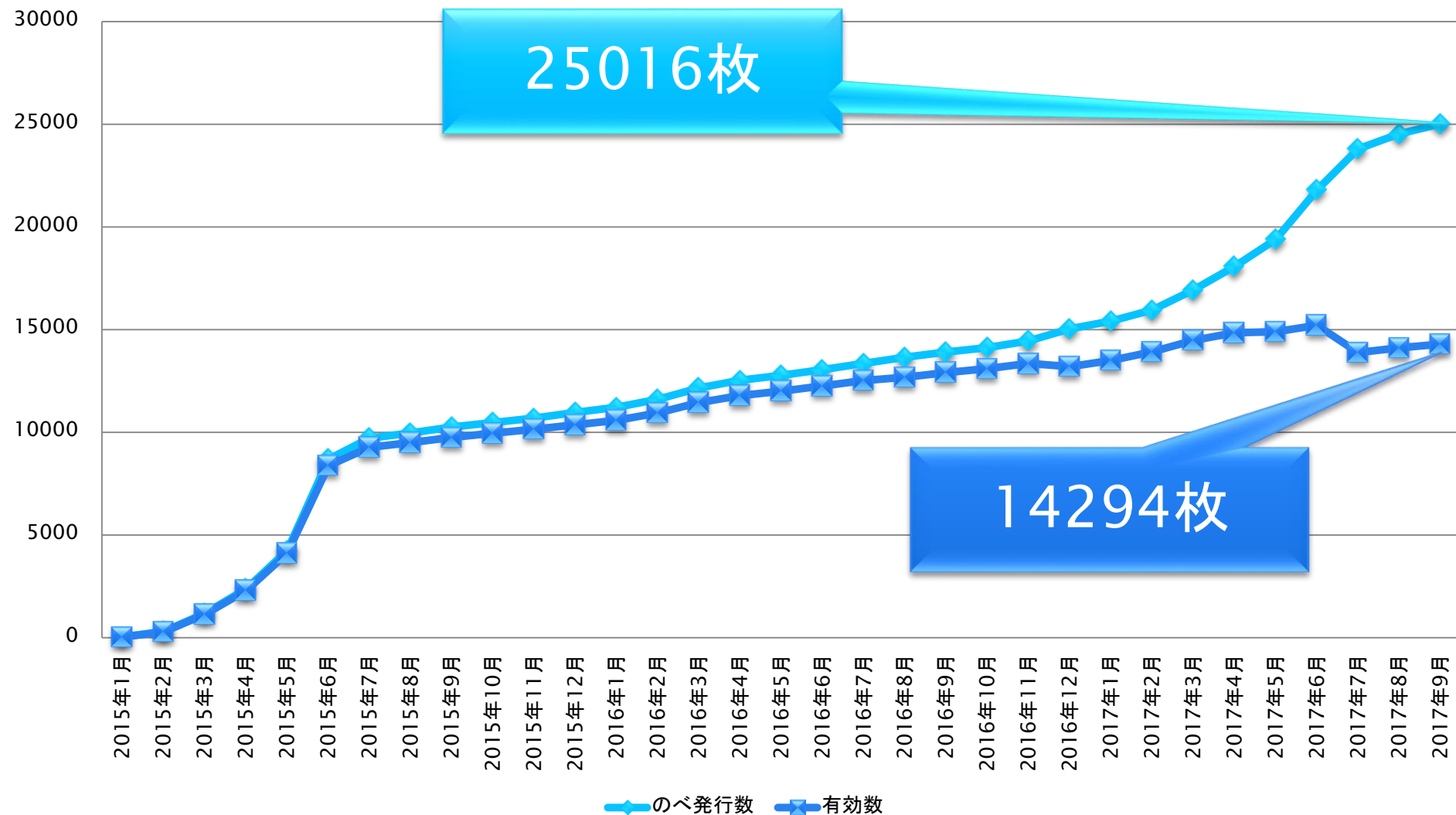
平成29年度 SINET・学術情報基盤サービス説明会
国立情報学研究所



UPKI 機関数・ドメイン数の推移



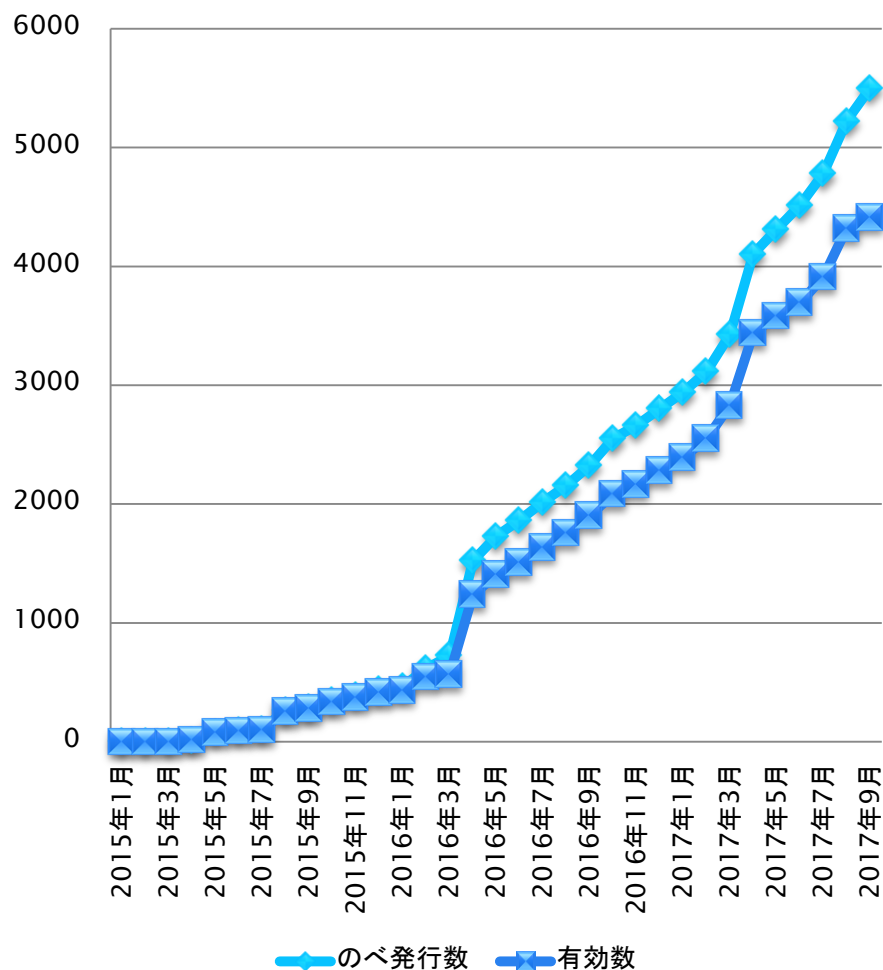
証明書発行状況—サーバ証明書



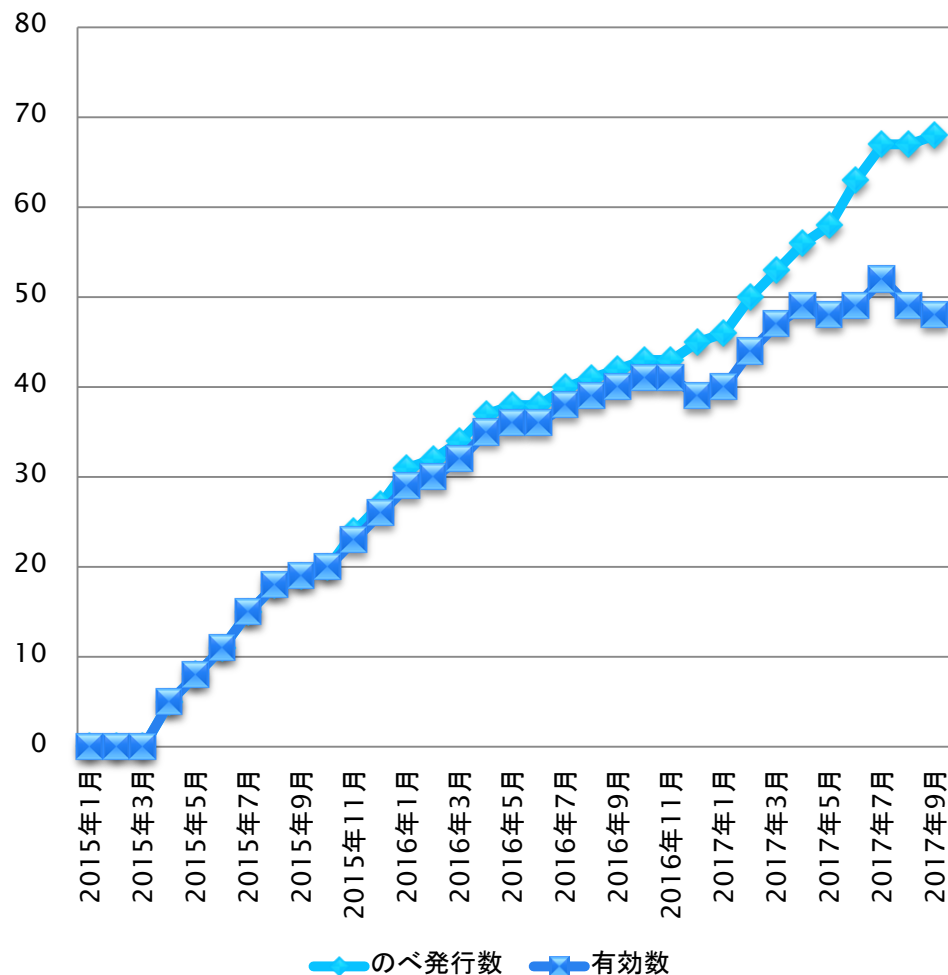


証明書発行状況ークライアント証明書 コード署名用証明書

クライアント証明書



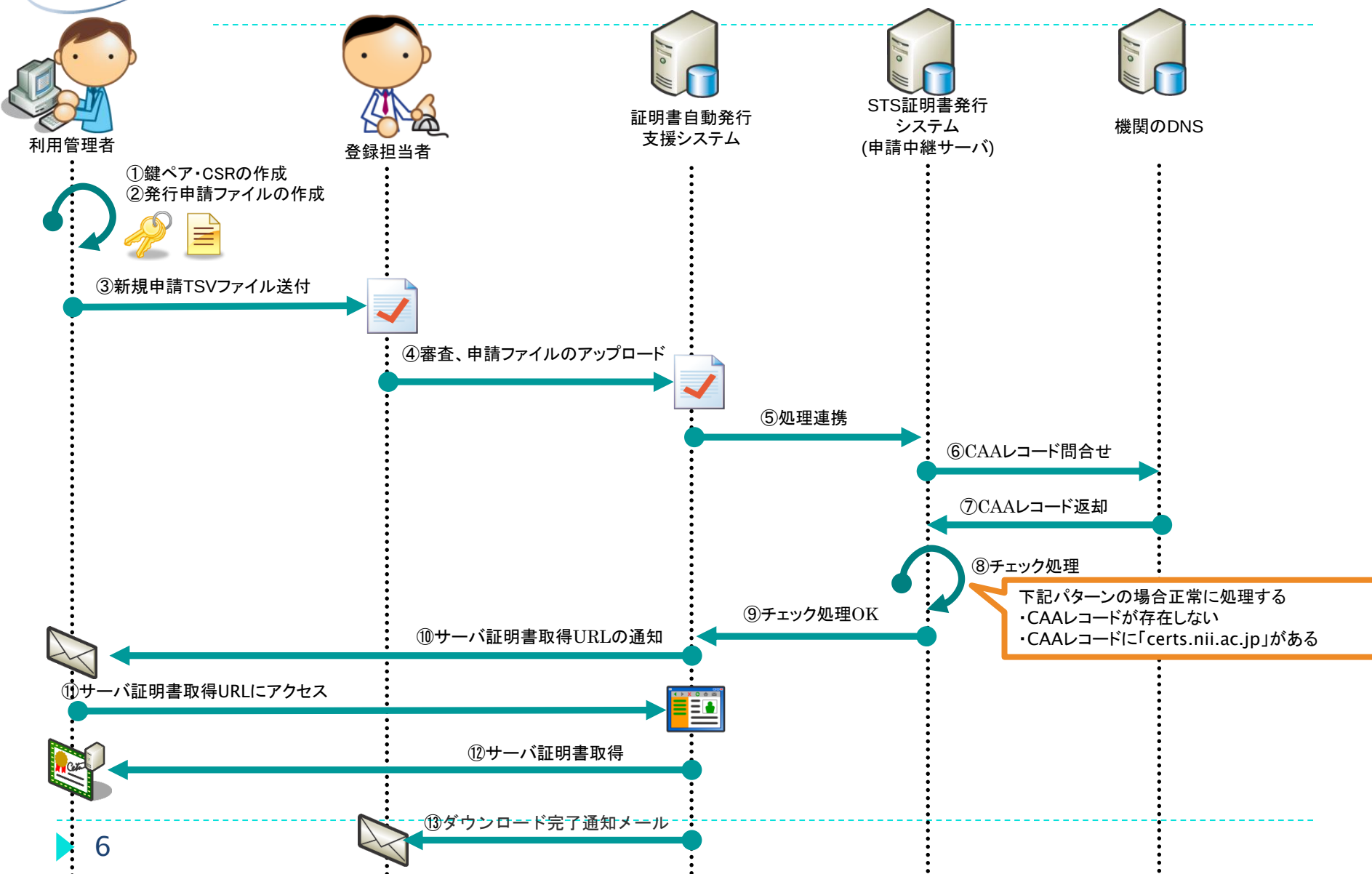
コード署名用証明書



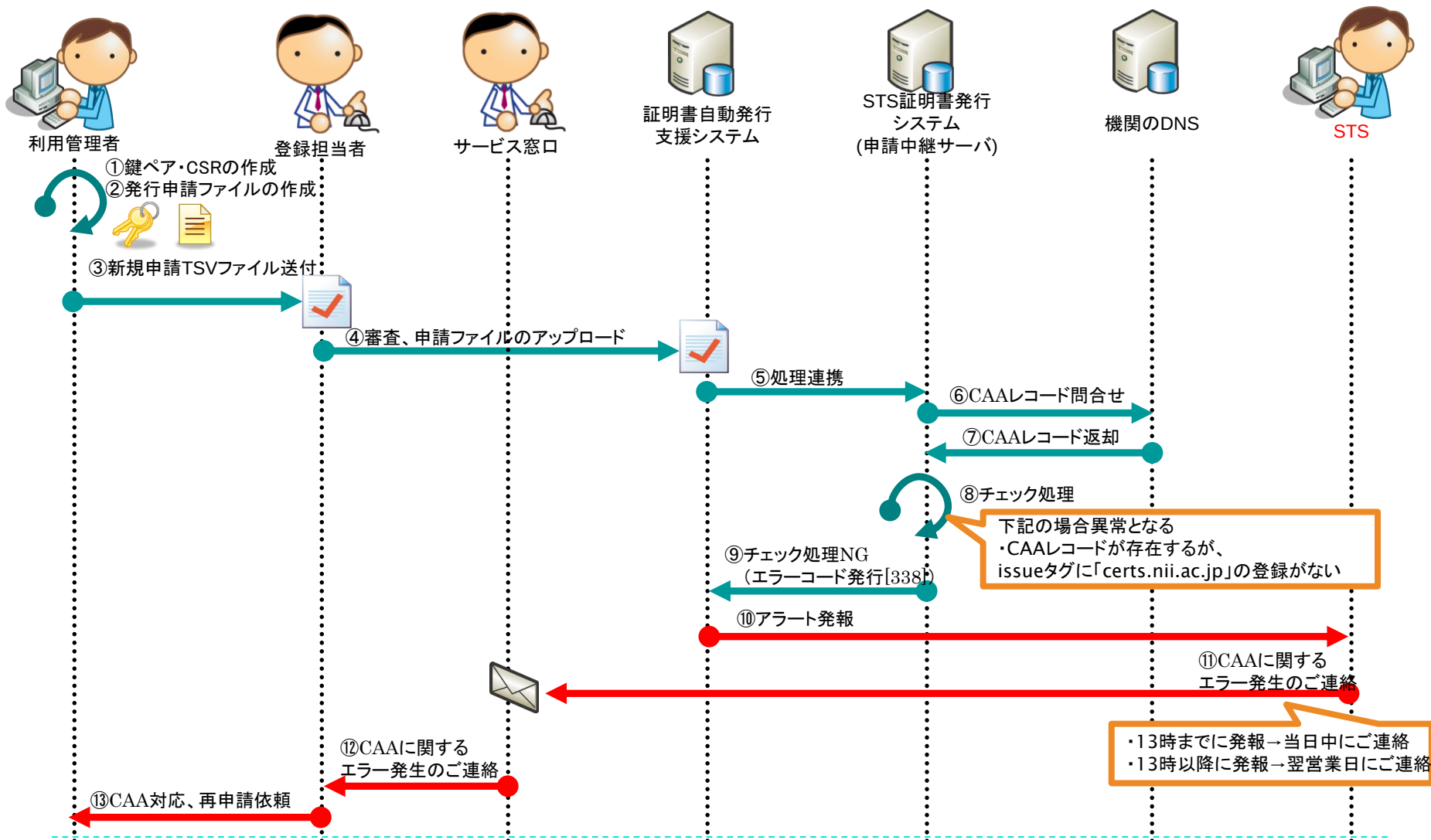
DNS CAAレコードの検証

- ▶ CA/B Forum BRにおいて、証明書発行時に、DNS CAAレコードの検証が義務付けられました
- ▶ これにあわせて、CPを改定しました
 - ▶ 4.2.4 CAAレコードの確認
 - ▶ 本CAは、申請情報の審査時にCAAレコードを確認する。本CAをDNSのCAAレコードに記載する場合、Issuer Domain Name は“certs.nii.ac.jp”とする。
- ▶ 下記のいずれかの場合、発行可能です
 - ▶ CAAレコードが存在しない
 - ▶ CAAレコードが存在し、かつ certs.nii.ac.jp が 記載されている
- ▶ 下記に該当する場合、発行不可となります
 - ▶ CAAレコードが存在し、かつ certs.nii.ac.jp が 記載されていない

発行可能なケース



発行不可のケース



主体者DNの値チェック厳格化

- ▶ CA/B Forum BRに準拠するため、主体者DNの値のチェックを厳格化します
 - ▶ CN
 - ▶ 記号で始まったり、".."のように記号が連続する場合、申請時にエラーとなります
 - ▶ OU
 - ▶ 記号と半角スペースのみが記入されている場合、申請時にエラーとなります
- ▶ 現在発行済みのものに、これらに該当する証明書があったとしても、直ちに失効とはなりません
 - ▶ 将来的に、失効・新規発行をお願いする可能性があります



次期調達について

- ▶ 次期認証局調達を実施しました
 - ▶ 現在の認証局での証明書発行契約（セコムトラストシステムズ）は、2017年12月末日までとなっています
 - ▶ 次期認証局も、引き続きセコムトラストシステムズから提供されることに決まりました
- ▶ これまで発行した証明書は？
 - ▶ 全て、継続して有効期限まで利用可能です

現サービスからの変更点（抜粋）

- ▶ 認証局
 - ▶ SHA2継続（SHA1廃止）
 - ▶ ECDSA新設
- ▶ 対応Webサーバ・ミドルウェア追加
- ▶ 署名に用いるタイムスタンプサーバの提供
- ▶ サーバ証明書のCT対応
- ▶ クライアント証明書の有効期間を48ヶ月以上に設定可能に
- ▶ 通知メールのダイジェスト版
 - ▶ 有効期限間近の通知など、期日の定まったものを1メールに
- ▶ 発行統計の表示
- ▶ マニュアルのWebページ化
 - ▶ meatwikiに掲載

次期認証局調達にともなう UPKI電子証明書発行サービスの変更点



発行可能な証明書—変更なし

- ▶ サーバ証明書
- ▶ クライアント証明書
 - ▶ 個人認証用証明書
 - ▶ S/MIME証明書
 - ▶ クライアント証明書のうち、S/MIME署名の機能を有するものを特にS/MIME証明書と呼びます
 - ▶ 証明書にメールアドレスが記載されます
- ▶ コード署名用証明書



有効期間

▶ 各証明書の有効期間

▶ サーバ証明書

- ▶ 発行日から24ヶ月+30日間
- ▶ CA/B Forum BRでは、下記の通り定めています
 - 2018年3月1日以降発行する証明書では、有効期間825日を超えないこと
- ※現在は最大39ヶ月を超えないこと

▶ クライアント証明書

- ▶ **Update!** 発行日から48ヶ月もしくはそれ以上

▶ コード署名用証明書

- ▶ 発行日から24ヶ月+30日間



証明書の署名アルゴリズム

- ▶ sha256WithRSAEncryption
- ▶ 廃止 : sha1WithRSAEncryption
- ▶ **New!** サーバ証明書については、加えて下記が使用できるようになります
 - ▶ ecdsa-with-SHA384 (楕円曲線暗号)
- ▶ サーバ証明書の鍵ペアにも、RSAに加えてECDSAが使用可能です



サーバ証明書 対応ブラウザ Update!

- ▶ Microsoft Internet Explorer 11
- ▶ Microsoft Edge 38以上
- ▶ Firefox 52.0以上
- ▶ Opera 40以上
- ▶ Apple Safari 10.0以上
- ▶ Google Chrome 56以上
- ▶ iOS9.3.5以降に対応したSafari
- ▶ Android 4.4以降に対応したGoogle Chrome



サーバ証明書 一対応Webサーバ・ミドルウェア Update!

- ▶ Apache httpd 2.2
- ▶ Apache httpd 2.4 **New!**
- ▶ Microsoft Internet Information Server 7.5
- ▶ Microsoft Internet Information Server 8.0
- ▶ Microsoft Internet Information Server 8.5
- ▶ Microsoft Internet Information Server 10.0 **New!**
- ▶ IBM HTTP Server 7.0
- ▶ Nginx 1.2.0 **New!**
- ▶ Apache Tomcat 7
- ▶ Apache Tomcat 8 **New!**
- ▶ Apache Tomcat 8.5 **New!**
- ▶ OpenLDAP 2.4 **New!**



クライアント証明書 対応環境 Update!

- ▶ Microsoft Internet Explorer 11
- ▶ Microsoft Edge 38以上
- ▶ Firefox 52.0以上
- ▶ Opera 40以上
- ▶ Apple Safari 10.0以上
- ▶ Google Chrome 56以上
- ▶ iOS9.3.5 以上
- ▶ Android 4. 4以上



クライアント証明書 —用途

- ▶ SSL/TLSクライアント認証用証明書
- ▶ S/MIME証明書
 - ▶ Microsoft Office Outlook 2013以上
 - ▶ Apple Mail 10 以上
 - ▶ Mozilla Thunderbird 52.0 (Windows, macOS) 以上



コード署名用証明書 一対応環境

- ▶ Windows用 .exe形式
- ▶ Windows用 .cab形式
- ▶ Windows用 .dll形式
- ▶ VBAマクロ形式
- ▶ Windows PowerShell用スクリプト形式
- ▶ JAVA .jar形式
- ▶ Android用アプリケーション .apk形式
- ▶ Adobe AIR 形式



OCSPレスポнда

- ▶ OCSP(Online Certificate Status Protocol)による
証明書ステータス確認機能の提供
 - ▶ サーバ証明書
 - ▶ コード署名用証明書 **New!**



タイムスタンプサービス New!

- ▶ UPKIの証明書を用いた長期署名(RFC5126)に利用できる、タイムスタンプサーバを提供
 - ▶ 電子署名のみでは、署名検証が可能な期間は署名に用いた証明書の有効期間内となります
 - ▶ 電子署名にタイムスタンプを組み合わせると、署名検証が可能な期間をより長期間確保できます



サーバ証明書 —Certificate Transparency対応 New!

- ▶ Certificate Transparency (RFC6962)
 - ▶ 2018年4月より、Google Chromeにて対応が義務化される予定です
 - ▶ UPKIのサーバ証明書でも対応します
- ▶ 既存の証明書を失効する必要はありませんが、CT対応版が必要な場合は、更新申請を行ってください
 - ▶ 既存の証明書は、有効期限まで利用可能です



証明書発行支援システム

- ▶ 基本的にこれまでの機能はそのまま備えます
 - ▶ 発行・失効・更新の受付
 - ▶ これまで通りTSVファイルにて受け付けます
 - ▶ 一覧の取得
 - ▶ 各証明書情報の一覧を取得できます
 - ▶ 登録担当者用クライアント証明書による認証必須
 - ▶ 登録担当者用証明書を再発行する必要はありません。これまで発行したものは、継続して有効期限まで利用できます



証明書発行支援システム ー発行統計

New!

- ▶ 証明書発行状況の統計情報を表示できるように
- ▶ たとえばこんな項目
 - ▶ 発行状況
 - ▶ 各証明書 のべ発行数・失効数、有効数
 - ▶ 取得状況
 - ▶ ダウンロード・取得操作完了数
 - ▶ 同未了数
 - ▶ 有効期限間近（30日未満）な証明書の数



証明書発行支援システム メール通知 Update!

- ▶ これまで通り各種通知を登録担当者や利用管理者にメールでお届けします
- ▶ あらかじめ設定された期日に送信が決まっているメールについては、極力1通にまとめて送信します
 - ▶ たとえば
 - ▶ 証明書の有効期限の通知
 - ▶ リマインド などなど・・・
- ▶ 利用者に向けたメール本文には英文も併記します
 - ▶ 各証明書取得のための通知等



マニュアル

- ▶ オンラインマニュアルの提供 **Update!**
 - ▶ これまでPDF、Wordで提供していましたが、Webページに記述する形式にします
 - ▶ システムからPDF出力も可能です
 - ▶ 各ソフトウェアに対応したマニュアルはもちろん、証明書利用者を対象とするものについては英語版も提供 **New!**
 - ▶ クライアント証明書のインストール
 - ▶ S/MIME証明書のメーラへのインストール
- ▶ スクリーンショットについてはWindows10, macOS Sierraを用いて提供予定



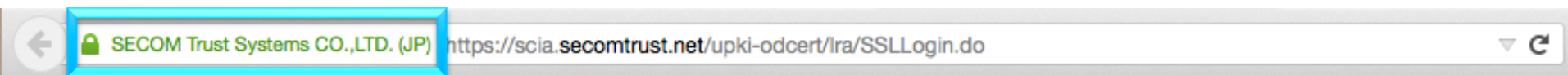
サービス利用料金について

- ▶ 本日お伝えした以上のことを実現していくには、ご負担いただいている費用について、再検討を行う必要がございます
 - ▶ たとえば・・・
 - ▶ 証明書発行・更新・失効用のAPI
 - ▶ 各機関が持つシステム、あるいはアプライアンスから証明書の各申請が可能なもの
 - ▶ または発展させてACMEプロトコル対応
 - ▶ 証明書インストール確認ツール
 - ▶ Webサービスとして提供
 - FQDNを入力すると、証明書インストール状態をチェック
 - 確認できない場合、想定される原因と対処などを表示
- ▶ 証明書発行状況の調査とあわせて、サービス利用機関の皆様へサービス利用料金変更に関するアンケートを実施します
 - ▶ ご意見をお寄せいただければ幸いです



EV証明書について

- ▶ 本サービス利用機関(※)に対し，証明書発行もとであるセコムトラストシステムズより，**EV証明書**が有償で提供されます



※サービスに登録したドメインである必要はありません

- ▶ ご希望の機関には，セコムトラストシステムズより提供された「申請ガイド」を送付いたします
 - ▶ certs@nii.ac.jp までご依頼ください！
 - ▶ 「申請ガイド」受領以降のEV証明書についてのお問い合わせ，発行手続き，お支払い等は，セコムトラストシステムズと直接行ってください

EV SSL証明書(セコムパスポートforWeb EV2.0) の特徴

◆ 機能 アドレスバーが緑色に変化し、安全性をアピール



EV SSL証明書対応ブラウザでアクセスすると、アドレスバーが緑色に変化

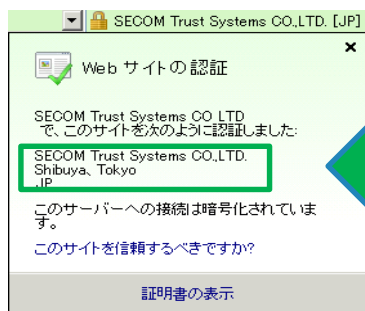
OV(組織認証)証明書(セコムパスポートforWeb SR3.0)では、https://でアクセスしてもアドレスバーの色は白色のままです。



危険なサイトはアドレスバーが赤色に変化

https://でアクセスしたとき、「失効されている」「有効期限が切れている」「WebサイトのURLと一致していない」疑わしいサイトの場合には、危険なサイトとして、アドレスバーが赤色に変化します。

◆ 効果 識別情報の表示で運営組織を確認、フィッシング対策に有効



従来、ブラウザの鍵マークをクリックしなければ確認できなかった「サーバー証明書に記載されている組織名」がアドレスバーの横に表示されます。

EV SSL証明書は、実在証明としてより一層安全性をアピールすることができます。



セコムのWebステッカーがEV SSL証明書の更なる安全性を訴求



おわりに

- ▶ ご連絡・お問い合わせ先
 - ▶ 国立情報学研究所 学術基盤課総括・連携基盤チーム
(認証担当)
 - ▶ Mail : certs@nii.ac.jp
 - ▶ Web : <https://certs.nii.ac.jp>
 - ▶ 原則, サービス利用機関または利用予定機関の機関責任者・登録担当者からお願いします