

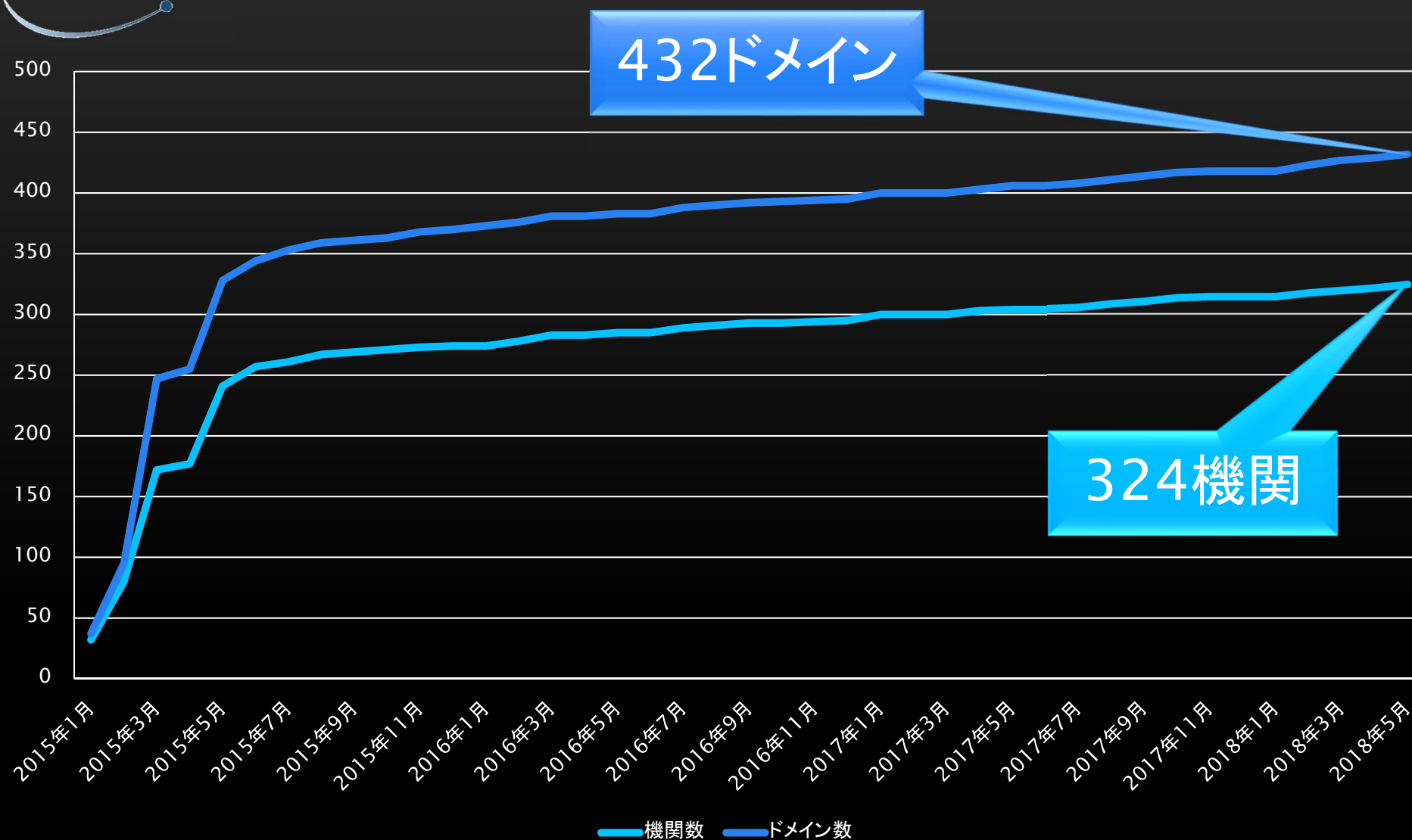


# UPKI電子証明書発行サービス 2018アップデート

学術情報基盤オープンフォーラム2018  
国立情報学研究所

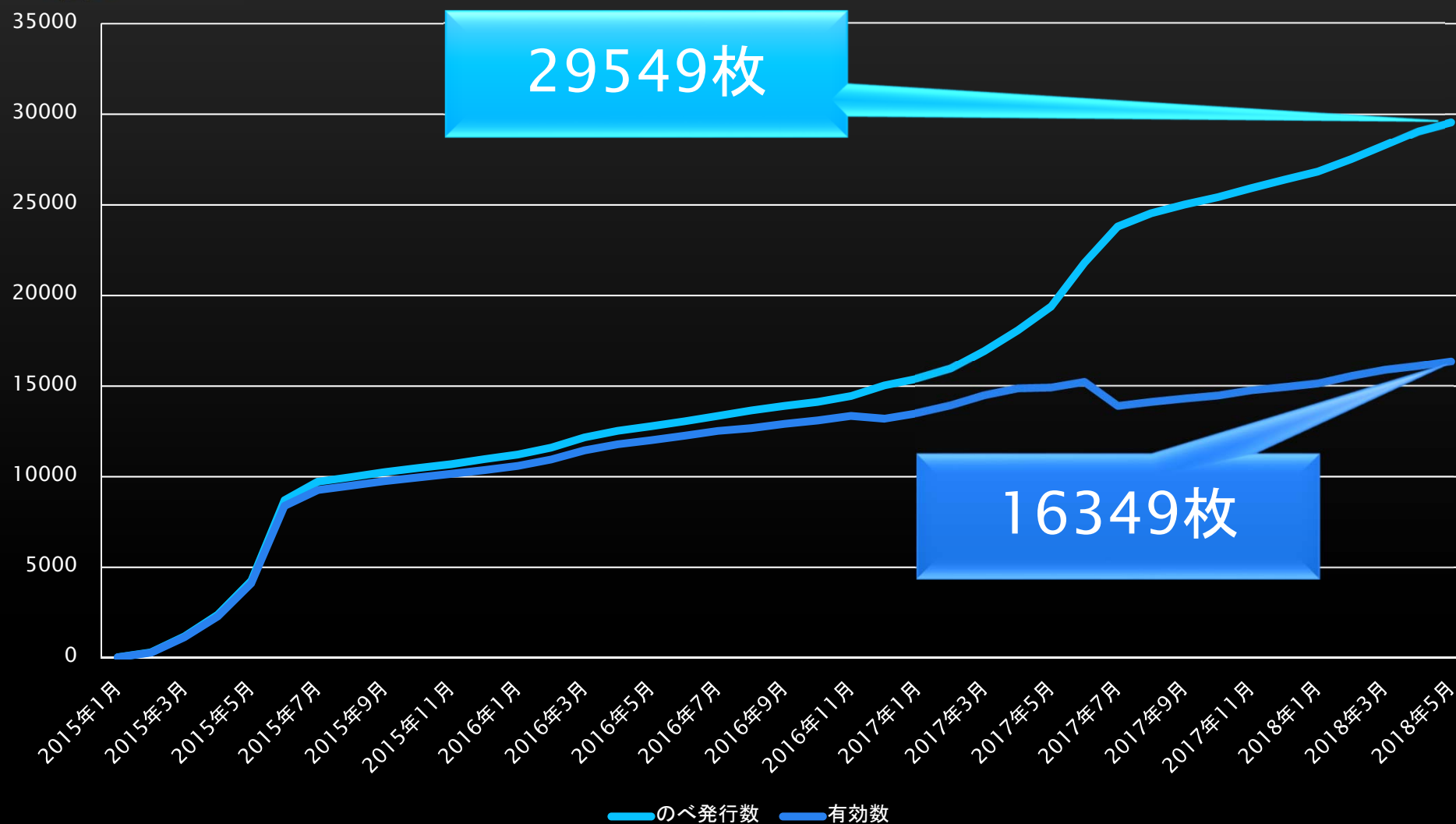


# UPKI 機関数・ドメイン数の推移





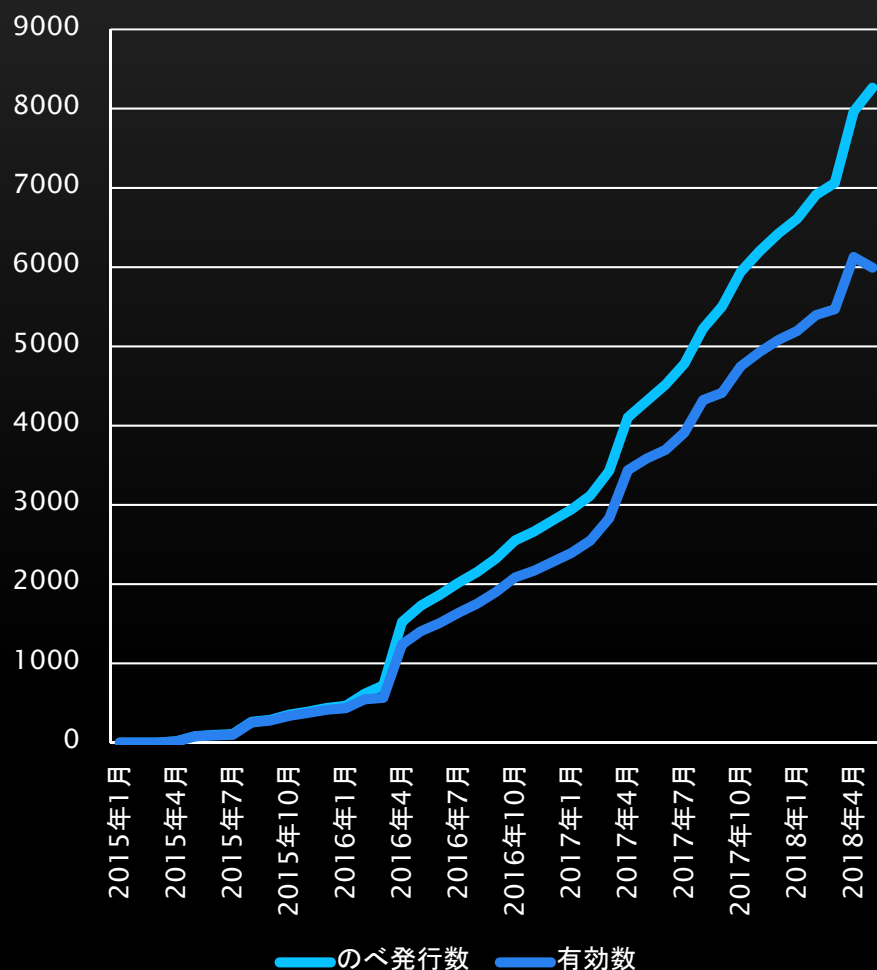
## 証明書発行状況—サーバ証明書



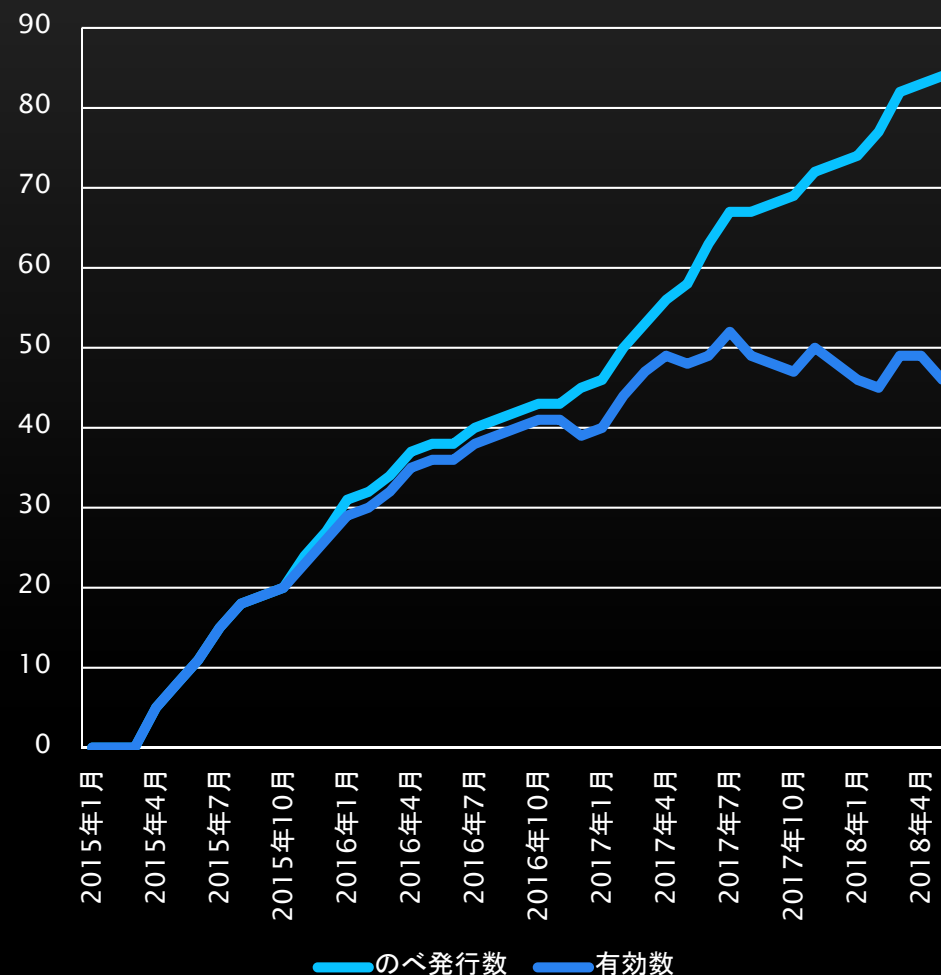


# 証明書発行状況—クライアント証明書 コード署名用証明書

## クライアント証明書



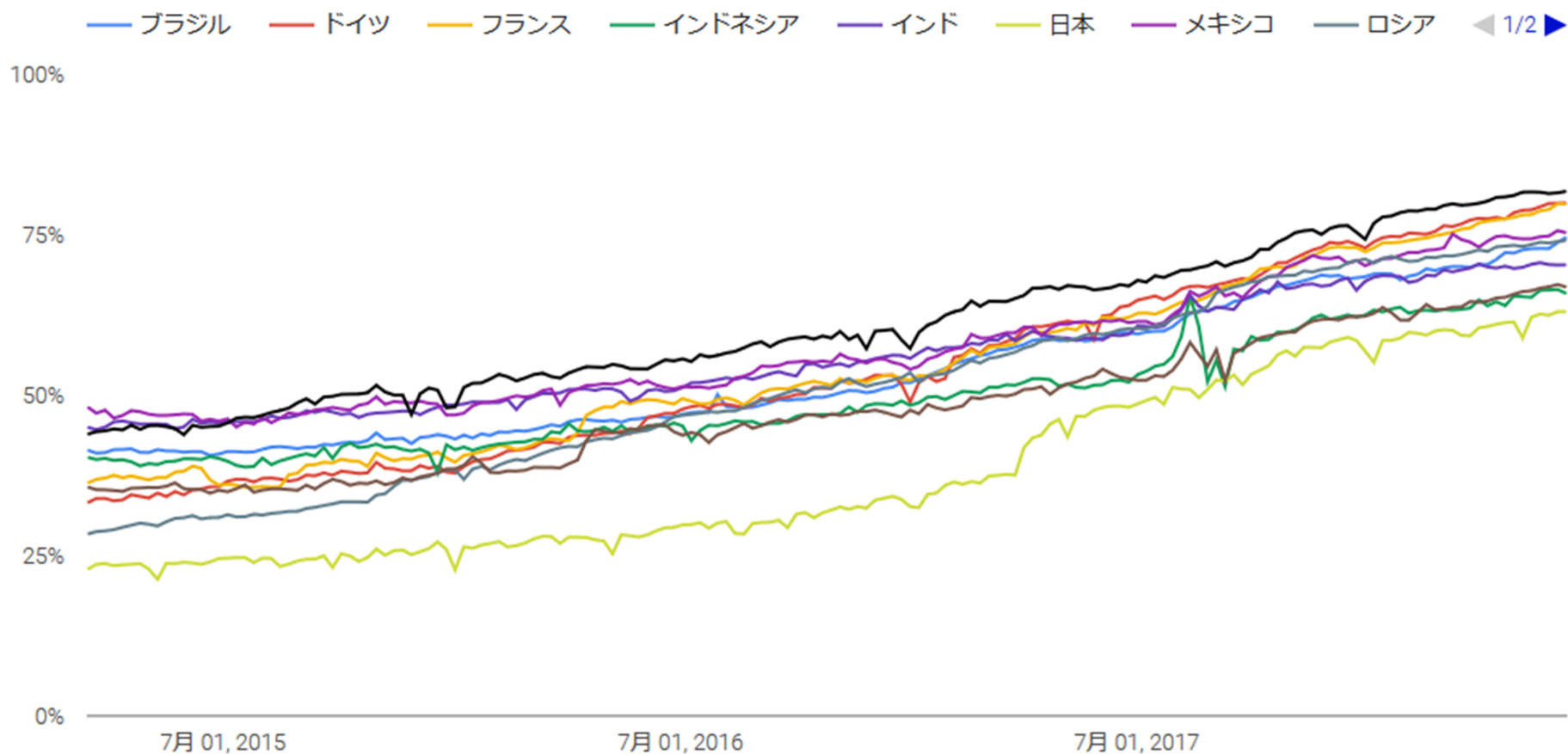
## コード署名用証明書





# HTTPSの使用状況

Chrome で HTTPS 経由で読み込まれたページの割合（国別）





# Chromeの表示変更

## ▶ Chrome 68 (7月24日)

Treatment of HTTP pages:

|                       |                            |
|-----------------------|----------------------------|
| Current (Chrome 64)   | 🔒 example.com              |
| July 2018 (Chrome 68) | 🔒 Not secure   example.com |

日本語表記:

🔒 保護されていません | www.i

## ▶ Chrome 69 (9月4日)

Treatment of HTTPS pages

|                       |                        |
|-----------------------|------------------------|
| Current (Chrome 67)   | 🔒 Secure   example.com |
| Sep. 2018 (Chrome 69) | 🔒 example.com          |
| Eventually            | example.com            |

上: <https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html>  
下: <https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html>  
より引用 2018/6/16 閲覧



## 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



利用管理者



登録担当者



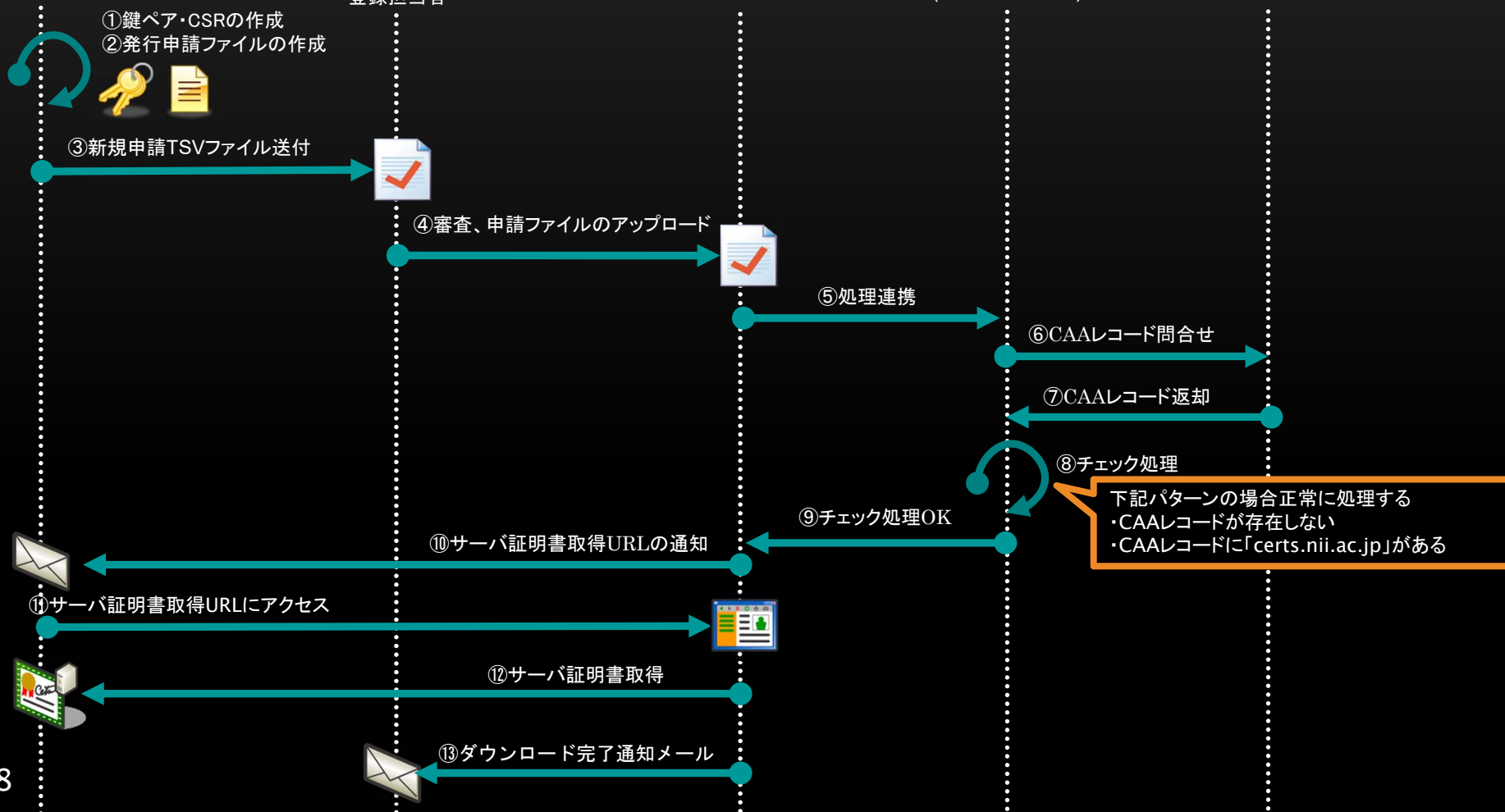
証明書自動発行  
支援システム



STS証明書発行  
システム  
(申請中継サーバ)

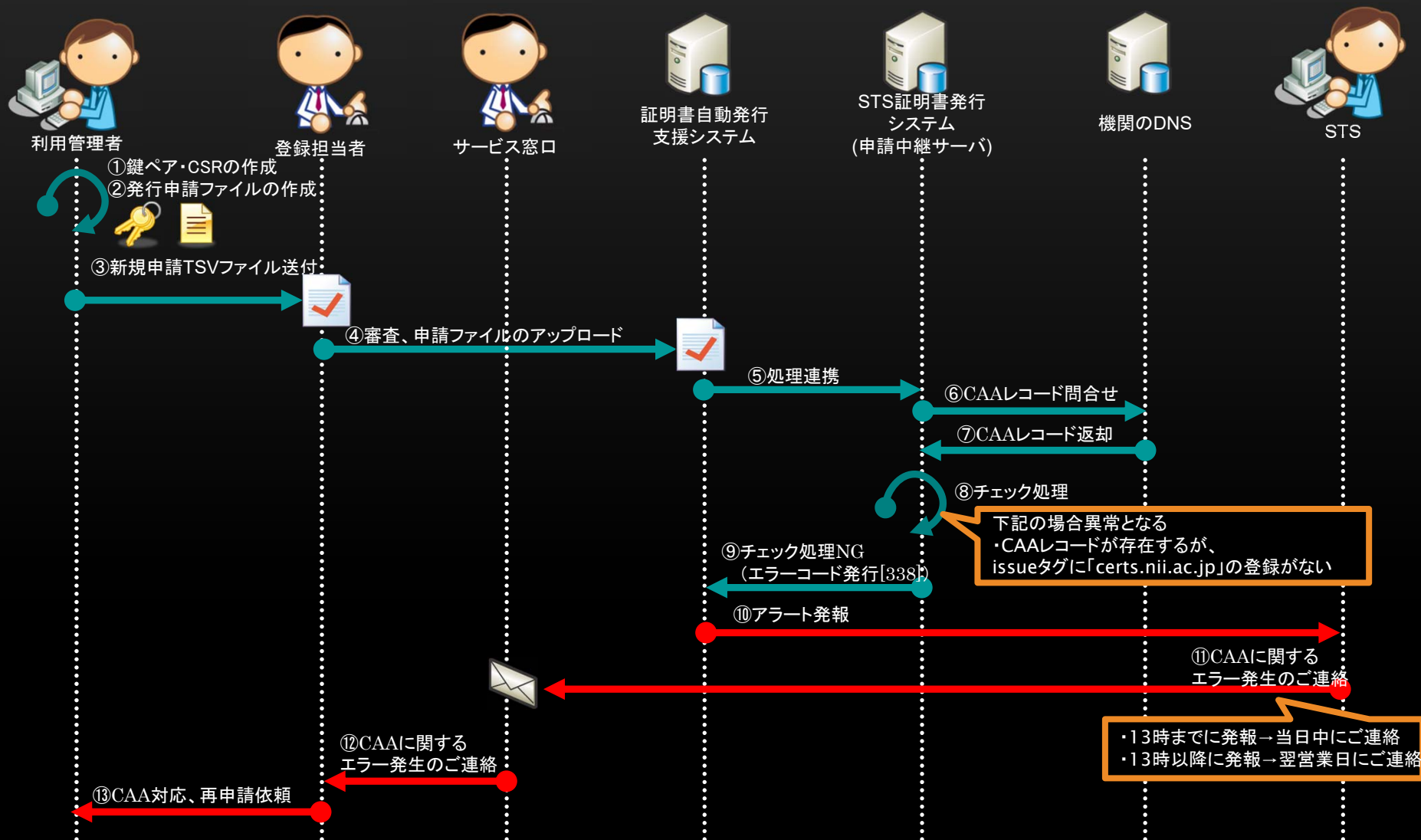


機関のDNS





# 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

# UPKI電子証明書発行サービス 2018 アップデート



## アップデートで対応したもの

- ▶ サービス利用機関のご要望
- ▶ CA/B Forum のBRでの定めによるもの
- ▶ ブラウザベンダの要求
- ▶ 環境のアップデートに付随するもの
  - ▶ ミドルウェア群



## 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



## 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

# —対応Webサーバ・ミドルウェア **Update!**

- ▶ Apache httpd 2.2
- ▶ Apache httpd 2.4.8~ **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 一対応環境 **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 一用途

- ▶ 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 Update!

- ▶ 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!**



# 第一次アップデート 2018/2/26

- ▶ 証明書発行状況の統計表示
  - ▶ 証明書発行支援システムにて、各ドメインごとに発行状況の統計を表示する機能を提供
- ▶ メール通知機能の変更
  - ▶ 登録担当者が受信する通知メールのうち、まとめられるもの（有効期限の通知等）をダイジェスト版に変更
    - ▶ ただし件数が多く、メール1通の容量が10MBを超える場合は分割されます
  - ▶ 利用者向けの通知メール本文については、英文を併記
- ▶ クライアント証明書取得時の英語インタフェース等追加
  - ▶ 証明書取得時のWebインタフェースに、英語版を追加
    - ▶ ブラウザの言語設定によって自動的に切り替わります
    - ▶ リンクをクリックすることで、手動で切り替えることもできます
    - ▶ クライアント証明書利用者向けインストールマニュアルに、英語版を追加
- ▶ クライアント証明書の有効期間変更
  - ▶ 有効期間を25ヶ月から52ヶ月に変更



## 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



## 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
  - ▶ クライアント証明書
    - ▶ **Update!** 発行日から52ヶ月
  - ▶ コード署名用証明書
    - ▶ 発行日から24ヶ月+30日間



## マニュアル Update!

- ▶ オンラインマニュアルの提供
  - ▶ これまでPDF、Wordで提供していましたが、meatwikiに記述し、ブラウザから参照できる形式に変更します
    - ▶ <https://meatwiki.nii.ac.jp/confluence/x/IYKPAQ>
    - ▶ 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
    - ▶ 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を用いて提供中
- ▶ 「meatwikiが見られなくなっちゃうと困るのだけど・・・？」→法定停電の対策を講じています



## 第二次アップデート 2018/3/26

- ▶ サーバ証明書のCertificate Transparency対応
  - ▶ Certificate Transparency（以下CTといいます）対応のSHA-2認証局を新設し、これを中間認証局とするサーバ証明書の発行が可能になりました
  - ▶ CTに対応したサーバ証明書が必要な場合は、新規あるいは更新申請を行ってください
  - ▶ 3月26日のメンテナンス後に発行する証明書は、全てCT対応となります
    - ▶ 2018年3月26日 19:00以降に新規発行または更新発行した証明書では、**中間証明書が変更になりました**
    - ▶ 「国立情報学研究所 オープンドメイン SHA-2認証局 CT対応版 CA証明書(nii-odca3sha2ct.cer)」を取得してインストールしてください
  - ▶ 非対応の認証局からのサーバ証明書発行は停止しました



## サーバ証明書 —Certificate Transparency対応 **New!**

- ▶ Certificate Transparency ( RFC6962 )
  - ▶ 2018年4月30日移行発行された証明書において、CT対応要件を満たすことが必須になりました(Chrome)
  - ▶ UPKIのサーバ証明書でも対応しました
- ▶ 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
- ▶ **中間証明書が変更になりました**
  - ▶ <https://repo1.secomtrust.net/sppca/nii/odca3/index.html>
    - ▶ 国立情報学研究所 オープンドメイン SHA-2認証局 CT対応版 CA証明書(nii-odca3sha2ct.cer)



## CT対応の必須化—Apple(2018/10/15)

- ▶ Appleのプラットフォームでも、CT対応が必須化されます
  - ▶ 2018年10月15日以降に発行された証明書は、CTポリシーを満たす必要がある
  - ▶ <https://support.apple.com/en-us/HT205280>  
6月8日公開



## Certificate Transparency 対応の利点は？

- ▶ 悪意ある者が nii.ac.jp の証明書を、管理者に知られずに正規のCAに発行させたら・・・？
- ▶ CTログがなかった過去
  - ▶ 認証局は、とにかくそういうことがないように頑張る
  - ▶ NIIは、知らないところで勝手に発行されていても気づきにくい
- ▶ CTログがある今
  - ▶ 認証局は、証明書発行時に必ずCT Log Serverに登録する
  - ▶ すべてのCT Log Server は公開されており、NIIはそれを監視できる



## CTログを監視するには

- ▶ censys
  - ▶ <https://censys.io>
  - ▶ 検索項目が充実
  - ▶ ユーザ登録すると、無償で 250 Queries/月
- ▶ Cert Spotter
  - ▶ <https://sslmate.com/certspotter/>
  - ▶ sslmate の1サービス
  - ▶ ユーザ登録すると、Watch listを作成できる
    - ▶ ドメインを Watch listに登録すると、日次でCTログに新しく登録された証明書一覧をメールで通知してくれる
    - ▶ 無償利用の場合、有効な証明書のみ検索可
- ▶ Facebook 開発者ツール
  - ▶ <https://developers.facebook.com/tools/ct/>
  - ▶ こちらもWatch listを作成し、メール通知を受けられる
    - ▶ 期限切れ、失効済みの証明書も検索可



# 画面イメージ : Facebook 開発者ツール

facebook for developers

Docs

Tools

Support

My Apps

Search developers.facebook.com

## Certificate Transparency Monitoring

Certificate Transparency is an open framework which helps log, audit and monitor publicly-trusted TLS certificates on the Internet. This tool lets you search for certificates issued for a given domain and subscribe to notifications from Facebook regarding new certificates and potential phishing attacks.

Search

Subscriptions

certs.nii.ac.jp

Search

| Domains                  | Subject                                                                                                                                | Issuer                                                                           | Validity                    | Certificate                         |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-----------------------------|-------------------------------------|
| pramanam.certs.nii.ac.jp | C=JP, L=Academe, O=National Institute of Informatics, CN=pramanam.certs.nii.ac.jp                                                      | C=JP, O=National Institute of Informatics, CN=NII Open Domain CA - G5            | Apr 26, 2018 - May 27, 2020 | Show Details<br>(CT Precertificate) |
| certs.nii.ac.jp          | C=JP, L=Academe, O=National Institute of Informatics, OU=Cyber Science Infrastructure Development Department, CN=certs.nii.ac.jp       | C=JP, L=Academe, O=National Institute of Informatics, CN=NII Open Domain CA - G4 | Jun 21, 2017 - Jul 22, 2019 | Show Details                        |
| check.certs.nii.ac.jp    | C=JP, L=Academe, O=National Institute of Informatics, OU=Cyber Science Infrastructure Development Department, CN=check.certs.nii.ac.jp | C=JP, L=Academe, O=National Institute of Informatics, CN=NII Open Domain CA - G4 | Dec 01, 2016 - Jan 01, 2019 | Show Details                        |
| check.certs.nii.ac.jp    | C=JP, L=Academe, O=National Institute of Informatics, OU=Cyber Science Infrastructure Development Department, CN=check.certs.nii.ac.jp | C=JP, L=Academe, O=National Institute of Informatics, CN=NII Open Domain CA - G3 | Dec 17, 2015 - Dec 31, 2016 | Show Details                        |
| certs.nii.ac.jp          | C=JP, L=Academe, O=National Institute of Informatics, OU=Cyber Science Infrastructure Development Department, CN=certs.nii.ac.jp       | C=JP, L=Academe, O=National Institute of Informatics, CN=NII Open Domain CA - G4 | Jun 18, 2015 - Jul 18, 2017 | Show Details                        |
| check.certs.nii.ac.jp    | C=JP, L=Academe, O=National Institute of Informatics, OU=Cyber Science Infrastructure Development Department, CN=check.certs.nii.ac.jp | C=JP, L=Academe, O=National Institute of Informatics, CN=NII Open Domain CA - G3 | Mar 20, 2015 - Dec 20, 2015 | Show Details                        |
| certs.nii.ac.jp          | C=JP, L=Academe2, O=National Institute of Informatics, OU=Cyber                                                                        | C=JP, L=Academe2, O=National Institute of Informatics, OU=UPKI NII               | Oct 07, 2014 - Mar 06, 2016 | Show Details                        |



# 画面イメージ : Facebook 開発者ツール

facebook for developers Docs Tools Support My Apps Search developers.facebook.com

Certificate Transparency Monitoring

Certificate Transparency Monitoring for certificate transparency. This tool lets you search for certificates that have been added to the public transparency log to help detect potential phishing attacks.

Search

Serial Number

1742485494025967131

Signature (sha256WithRSAEncryption)

07ba7da3a0fe8b84613e8761565d1854398bfd3aa620230e14243c71329d324d69d820a62

Certificate PEM Download

```
-----BEGIN CERTIFICATE-----
MIIE5jCCA86gAwIBAgIIGC6NUyGwVhswDQYJKoZIhvcNAQELBQAwWzELMAkGA1UE
BhMCS1AxKjAoBgNVBAoTIIU5hdGlvbmFsIEluc3RpdHV0ZSBvZiBjb2Vcm1hdG1j
czEgMB4GA1UEAxMXTk1JIE9wZW4gRG9tYW1uIEIENBIC0gRzUwHhcNMjgwNDIy
NzA3WhcNMjAwNTI0MDIyNzA3WjBuMQswCQYDVQQLGwJKUdEQMA4GA1UEBxMHQW5h
ZGVtZTEqMCgGA1UEChMTM0akw9uYWwgSW5zdG10dXR1IG9mIEluc3RpdHV0ZSBv
ZiBjb2Vcm1hdG1jMSEwHwYDVQQDExhwcMFTtYw5hbS5jZjZjZjZjZjZjZjZjZjZj
DQEBQUAA4IBDwAwggEKAoIBAQC6xnYqt6DMcsgMauCorCLU2d9psTz+ZNRyE2s8
PTXUGuLqDcI6Q9CVEEoyV7H56+1A9LzMp5tab9nIY46IMIm2rWkdzEqsoy0C+hw7
LcGzMxPKZVkk0PbV61FL18i+t23k3rtnd4ruZJ1+uWEX610IjfiQbPKIHm2RhnXH
vEngvYVRRfpmJhgE+UplfHnd117W870kM4ew17/rf10uYH91A0ESuAoZY0iOL9
-----
```

| Domain                | Issued To                                                               | Issued By                                                          | Issued At    | Expires At   | Details      |
|-----------------------|-------------------------------------------------------------------------|--------------------------------------------------------------------|--------------|--------------|--------------|
| certs.nii.ac.jp       | Science Infrastructure Development Department, CN=check.certs.nii.ac.jp | Domain CA - G3                                                     | Oct 07, 2014 | Mar 06, 2016 | Show Details |
| check.certs.nii.ac.jp | C=JP, L=Academe2, O=National Institute of Informatics, OU=Cyber         | C=JP, L=Academe2, O=National Institute of Informatics, OU=UPKI, MI | Oct 07, 2014 | Mar 06, 2016 | Show Details |



## 第三次アップデート 2018/7/9予定

- ▶ ECDSA（楕円曲線暗号）サーバ証明書を提供
  - ▶ ECDSA認証局を新設し、これを中間認証局とするサーバ証明書（ecdsa-with-SHA384）の発行が可能になります
- ▶ タイムスタンプサービス
  - ▶ UPKIのコード署名用証明書およびクライアント証明書で利用できる、タイムスタンプサービスが提供されます
  - ▶ UPKI電子証明書発行サービス利用機関は、追加料金なく、タイムスタンプを用いた署名が可能です
  - ▶ タイムスタンプを使用する回数に上限はありません
- ▶ 主体者DNの制限緩和
  - ▶ STが使用可能になります
  - ▶ ただしSTは都道府県名を用いることとします
  - ▶ Lの値としてこれまでは Academe を指定していましたが、この制限は廃止となります。市町村名を入れてください
- ▶ アクセスPIN指定機能の提供
  - ▶ クライアント証明書の一括発行申請時に、アクセスPINを指定できるようになります
  - ▶ これにともない、クライアント証明書の申請用TSVに、アクセスPINを指定する列が1つ追加されます



## 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
    - ▶ 国立情報学研究所 オープンドメイン ECC認証局
    - ▶ CA証明書(nii-odca3ecdsa.cer)
- ▶ **New!**サーバ証明書の鍵ペアにも、RSAに加えてECCが使用可能です
  - ▶ 鍵はECC384ビットとします
    - ▶ secp384r1



## ECCの鍵とCSR生成

### ▶ 鍵生成

- ▶ `$ openssl ecparam -genkey -name secp384r1 |  
openssl ec -out ec384.key -aes128`

### ▶ CSR生成

- ▶ `$ openssl req -new -key 【秘密鍵ファイル名】 -out  
【CSRファイル名】 -sha384`



## 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
  - ▶ →詳しくはこのあとで
    - ▶ 「タイムスタンプの概要・動向および活用事例」



## 主体者DNの制限緩和 Update! — ST が指定可 L=Academe固定を廃止

- ▶ サーバ証明書とクライアント証明書の主体者DNの仕様を下記の通り変更します
  - ▶ L=Academe 固定を廃止 → 市区町村名を入力してください
    - ▶ 値として、Academeは使えなくなります
    - ▶ 7月9日のメンテナンス以降、更新前と同じ主体者DNは使えません
      - 新規発行申請を行ってください
  - ▶ ST=が指定可能に → 都道府県名を入力してください
    - ▶ 入力できる値の一覧は、マニュアルページをご参照ください
    - ▶ STは、いくつかの表記パターンを許容します
      - 例：Tokyo や Toukyou など
  - ▶ **LとSTのいずれかが必須**、両方を指定することもできます
    - ▶ LとSTには、本サービスの利用申請書に記入した所在地を用いてください



# 主体者DNの制限緩和 Update!

## — ST が指定可 L=Academe固定を廃止

- ▶ 主体者DNの例は、下記の通りです。
  - ▶ 既存の主体者DNの例
    - ▶ CN=certs.nii.ac.jp,O=National Institute of Informatics,L=Academe,C=JP
  - ▶ 7月9日以降の主体者DNの例
    - ▶ CN=certs.nii.ac.jp,O=National Institute of Informatics,L=Chiyoda-ku,C=JP
    - ▶ CN=certs.nii.ac.jp,O=National Institute of Informatics,ST=Tokyo,C=JP
    - ▶ CN=certs.nii.ac.jp,O=National Institute of Informatics,L=Chiyoda-ku,ST=Tokyo,C=JP



## クライアント証明書 PIN指定発行 New!

- ▶ クライアント証明書発行時、PINを指定できるようになります
- ▶ クライアント証明書発行・更新申請用TSVの仕様が変更されます
  - ▶ これまで14列で構成されたTSVファイルに1列足され15列となり、15列目でアクセスPINが指定できるようになります
  - ▶ 入力は任意で、値なしでも問題ありませんが、TSVファイルとしては15列が必須になります
- ▶ 7月9日を以て、TSV作成ツールでもこの仕様変更にあわせたアップデートを行います



## 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**以外も**対象です

- ▶ 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](mailto: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

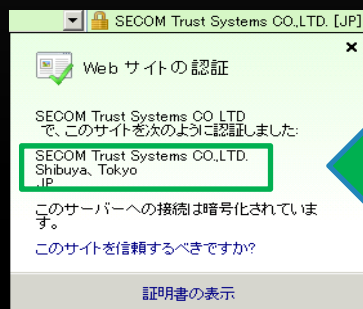
OV(組織認証)証明書(セコムパスポートforWeb SR3.0)では、https://でアクセスしてもアドレスバーの色は白色のままです。



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



- ▶ 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](mailto:certs@nii.ac.jp)
    - ▶ Web : <https://certs.nii.ac.jp/contact/>
  - ▶ 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