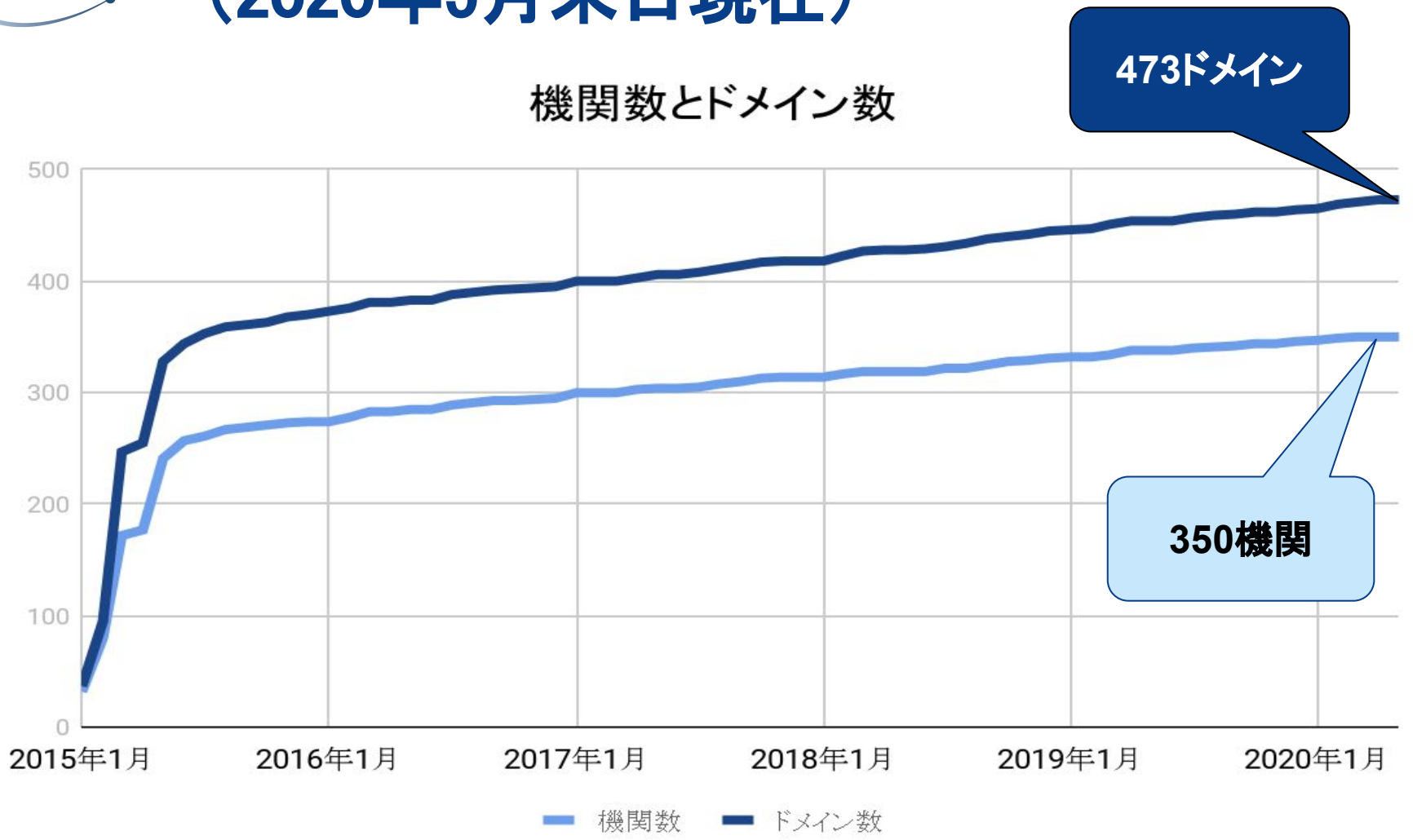
UPKI電子証明書発行サービスについて

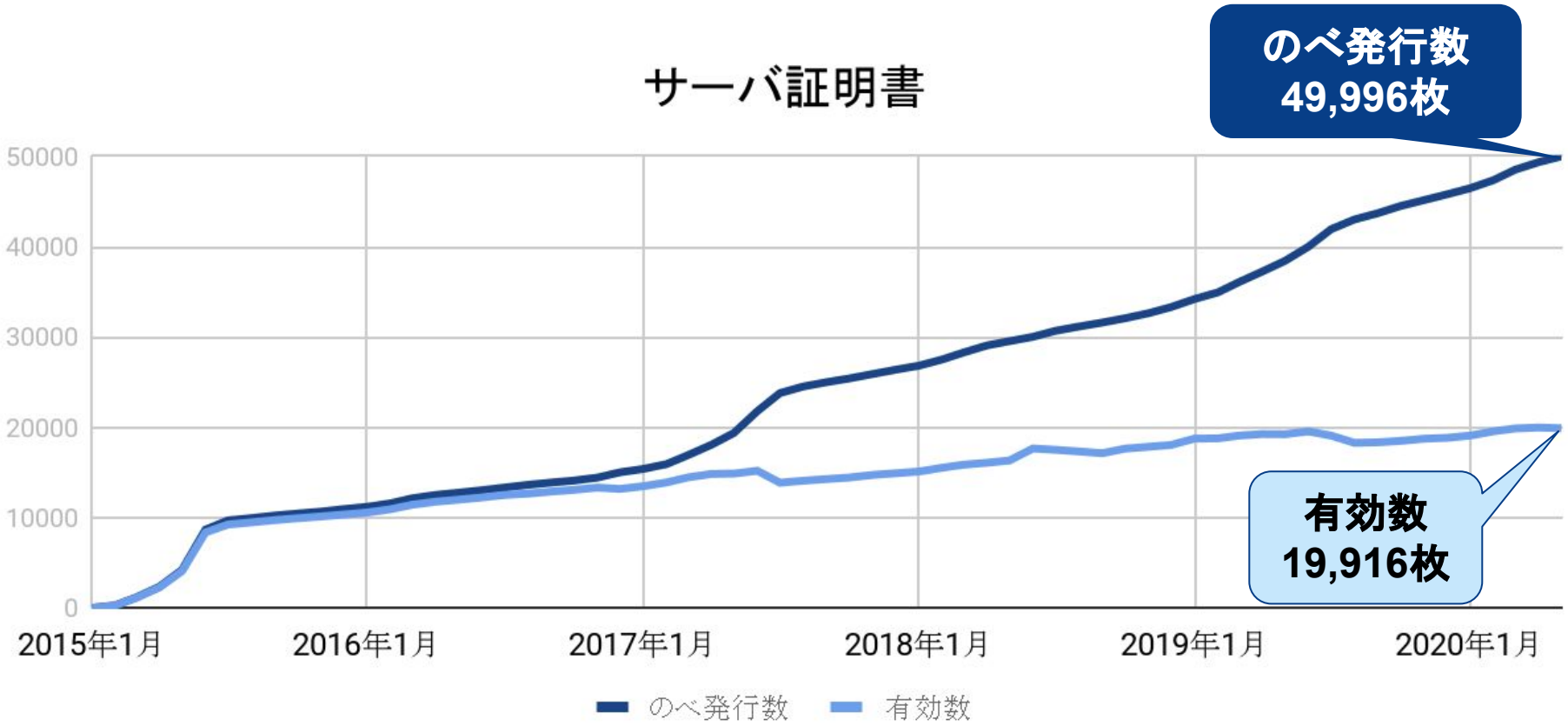
学術情報基盤オープンフォーラム2020

統計情報

サービス利用機関数とドメイン数（2020年5月末日現在）



発行数の推移（2020年5月末日現在）



発行数の推移（2020年5月末日現在）

CA/B Forum BR対応

CA/B Forum BR対応

- CA/Browser Forum の Baseline Requirements における、運用業務に関する変更と厳格化への対応を実施中です
  - UPKIの証明書についてBR違反・抵触を発見またいは指摘されると、場合によって、これに該当する証明書の全失効が有り得ます
  - UPKIの認証局についてBR違反・抵触を発見または指摘され、それに対処できない場合、UPKIの証明書はブラウザから信頼されない証明書として扱われます
- こういった事態を避けるため、ご協力をお願い申し上げます

【BR対応】
機関所在地とドメイン所有権の確認

- 全サービス利用機関の**所在地**確認を特定記録郵便にて実施（書類の到達と返送）
  - サービス利用開始時に確認を実施します

- 対象ドメインの**所有権**確認を、WhoisDB記載の連絡先メールアドレスを対象に実施（メール到達と返信）
  - こちらは毎年、サービス利用機関を対象に実施します
  - WhoisDBのメンテナンスをお願い申し上げます

【BR対応】STおよびLの値の固定1

- 認証局よりSTおよびLの値を各機関ごとに統一する必要があると要請されました
  - Lのみ、STのみ、LとST双方、の3通りの指定が可能
    - 今後も変更なし
  - 認証局で確認した機関所在地を記載しなければなりません
    - これまで：各機関の登録担当者で確認
      - STは候補から選択（システムでチェック）
      - Lはシステムでのチェックなし
    - 対応実施後：システムでSTとLそれぞれ1つずつ
      - 利用機関から指定および変更の届け出が可能
- L=Default Cityとしてサーバ証明書が発行されたケース有り

【BR対応】STおよびLの値の固定2

- UPKIで発行済の証明書におけるLとSTの値を機関ごとに集計し、登録担当者宛にご連絡しました
  - 下記URLでご確認いただけます
    - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=59022761
- 多くの機関で、STとLの値は統一された同じものが使われていました
  - 複数（大文字・小文字表記ゆれは許容します）ある場合は、発行数の最も多いものを固定値として採用しました
  - ただし、認証局からの指摘で、下記変更点があります
    - STのみ無い場合、確認済み所在地をもとにSTを追加しました。
    - Lのみ無い場合、そのままにしました。
    - 両方ない場合は、両方追加しました。
    - ST、Lは、先日認証局からの郵便物で確認した機関所在地としています。
    - 市区町村名以外が指定されている場合、本部所在地の市区町村名としました。
  - 別のものに指定したい場合は、必ずご連絡ください
    - 一旦、対応実施日（7月中頃）までといたします
    - その後も随時変更の届け出が可能です（確認済み所在地と突合します）
    - 一時的・短期的な変更はお請けできません

【BR対応】STおよびLの値の固定3

- これまで発行された証明書について
  - STおよびLの値の固定実施日までに発行された証明書は、全て有効期限までご利用いただけます
  - 新しく発行しなおす必要はありません

【BR対応】L=Default City として発行された証明書

- 一部利用機関において L=Default City と指定した証明書が発行されていました
- 2019年にセコムトラストシステムズがブラウザベンダより指摘され、全て失効する対応を実施しました
  - こういった、確認が取れていない設定値で証明書を発行することが、重大な問題であると指摘されました
- STおよびLの固定は、この指摘への対応措置としての実施となります

【BR対応】中間CA証明書の月次更新（サーバ証明書・クライアント証明書）

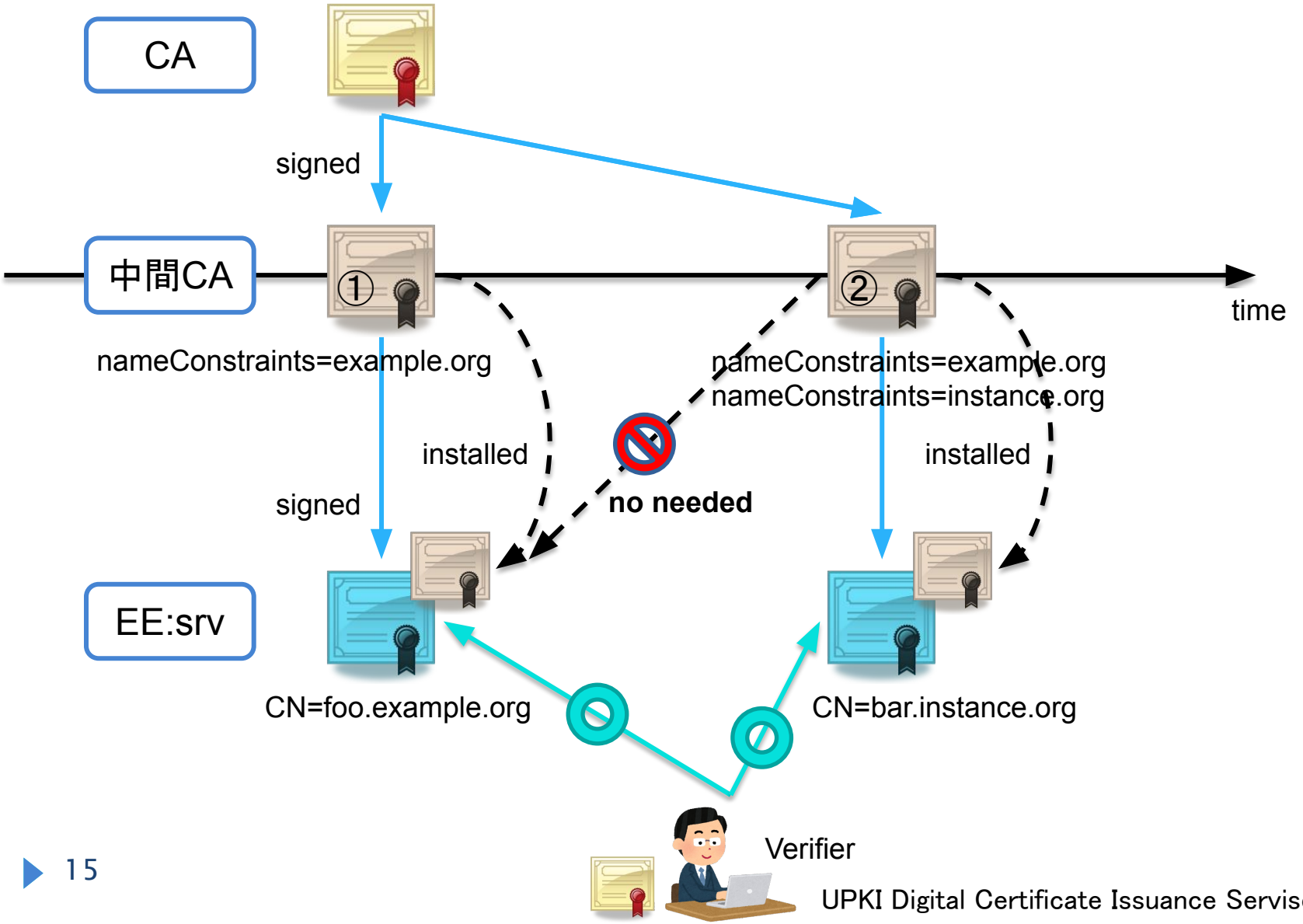
- サーバ証明書用中間CA証明書に、発行対象のドメイン（=本サービスに登録された全ドメイン）を記載します
  - 「名前の制限」フィールド（Name Constraints）
  - 月次で、鍵交換を伴わない中間CA証明書の更新を行い、新規参加機関のドメインを上記フィールドに追加
  - エンドエンティティ証明書のFQDNドメインが中間証明書に記載されていれば検証可能
- リポジトリには、その時点の最新版までを掲載します
- 本対応開始までに発行した証明書は、有効期限満了まで利用可能です
- S/MIME用中間CAにも同様に名前の制限フィールドの追加を計画しておりましたが、クライアント認証等に甚大な影響が生じることが報告され、当面保留しています

したがって・・・

- UPKI登録済みのドメインで発行済の証明書
  - 発行済証明書に影響なし
  - 更新時はリポジトリから中間CA証明書を取得してインストール
- UPKI登録済みのドメインで新たに発行する証明書
  - これまで通りリポジトリから中間CA証明書を取得
  - 更新時、インストール済の中間CA証明書再利用可能
- UPKIに新たに登録するドメインで発行する証明書
  - 中間CA証明書の取得時期に注意
  - 利用開始月の前月末頃にリポジトリに掲載

- インストール済の中間CA証明書を毎月更新する必要はありません

具体例:サーバ証明書


CA
signed
中間CA
①
②
time
nameConstraints=example.org
nameConstraints=example.org
nameConstraints=instance.org
installed
installed
signed
no needed
EE:srv
CN=foo.example.org
CN=bar.instance.org
Verifier

【BR対応】コード署名用証明書の発行元変更

- Microsoftよりセコムトラストシステムズに下記の連絡がありました
  - 「コード署名用証明書中間CAが、WebTrust取得のための外部監査対象であり、外部監査を受ける必要がある」
  - セコムトラストシステムズの判断として、当該中間CAでWebTrustを取得せず、発行元の認証局を自社提供のものに統合する対応をとることとなりました
- 現在発行済みのすべてのコード署名証明書を失効し、新しいコード署名証明書に変更する必要があります
  - 手順について、コード署名用証明書をご利用中の機関宛にご案内いたしました
  - 未完了で、また今後もご利用予定がある場合、ご対応をお願い申し上げます

お知らせ

Safari(Apple)が信頼する証明書の有効期間について1

- Appleの発表への対応
  - Apple社のブラウザSafariにおいて、2020年9月1日以降、有効期間が398日を超える証明書を信頼しない
    - 2020年8月31日までに発行された証明書（これまでの発行済を含む）には影響しません
      - 有効期限まで利用可能です
  - 現在の有効期間24ヶ月+30日のサーバ証明書プロファイルでは対応できないので、対処をセコムトラストシステムズと検討してきました

参考：About upcoming limits on trusted certificates
https://support.apple.com/en-us/HT211025

Safari(Apple)が信頼する証明書の有効期間について2

- 当初は有効期限を短縮したプロファイルの追加を検討していましたが・・・
  - 「398日を超える有効期限が設定された証明書を発行した認証局に対し、不信を含むペナルティを課すことができる」といった見解をAppleが示し、他のブラウザベンダも追随を検討しているようです
- これが確実なものとなった場合、現在の25ヶ月有効なプロファイルを変更することになります

Authority information Access について

- 現在発行されているサーバ証明書には、Authority information Access に CA Issuersとして、中間CA証明書が指定されています
  - この証明書をサーバにインストールしていると、たとえ誤った中間CA証明書をインストールしていた場合、そもそも中間CA証明書をインストールしていない場合でも、クライアント側のアクセス時、ブラウザが自動で正しい中間CA証明書を取得し、証明書検証を行います
    - ブラウザの実装に依存し、例えばFirefoxでは利用できない機能です
- ただし、これが機能するのはサポートしたブラウザのみです
  - 稼働監視を設定している場合、アクセス不能としてアラートが出る場合があります
  - たとえばGCPのMonitoringからはアクセス不能として扱われます

Firefox ESR版利用のお願い

- 現在、Firefox69以降の keygen要素廃止のため、クライアント証明書ブラウザ発行（ブラウザに直接インストールする方法）が実施できません
  - ブラウザ発行の場合は、ESR版（現在バージョン68系）のご利用を皆様にお願いしております
  - もしくはP12発行（ファイルで取得する形式）をご利用ください
- 2020年度、利用するAPIを変更し、Chrome、Edge、Safari、Firefox で利用可能な改修を実施予定です
  - 68系のESR版が9月頃にベースのバージョンを上げるので、それまでに対応予定

TSVツール 提供再開

- 証明書の各申請に用いるTSVファイル作成用のWebアプリケーション：TSVツールは、不具合発覚のため公開停止しておりました
  - 原因の究明とアプリケーションの修正が完了し、2020年6月9日より公開再開いたいました
- 今後、Webアプリケーション版に下記のアップデートを適用予定です
  - クライアント証明書プロファイルの追加
    - 有効期間13ヶ月、25ヶ月のプロファイルを指定可能になります
  - CSR読込時のチェック機能拡充
    - 読込時に修正すべき点が表示されます
  - TSVビューアの機能拡充
  - 細かな不具合の修正
- Docker Container版TSVツールでは、先行してこれらの機能をお試しいただけます

TLS1.0/1.1廃止

- 2020年3月より各ブラウザにおいて無効化され、全画面エラーが表示される予定だったが、COVID-19の影響で延期となりました。
  - Chrome 84 (2020/7/14)
  - Firefox 74 (一時的に再有効化され、延期中)
  - Safari 13 (発表ないものの、「安全ではありません」との表示で接続可)
  - Edge legacy/Internet Explorer (2020/9/8)
  - Edge Chromium Base(2020/7)
- 現在TLS1.2に対応していないサイトは3%未満といわれます
  - 猶予は得られましたが、学内システム等、この間にご確認ください。

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/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・経理担当者からお願いします