



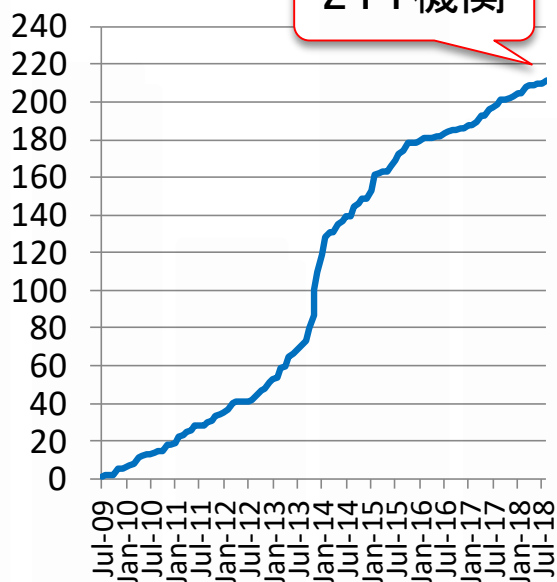
学認について

国立情報学研究所 2018年

IdP/SPの推移(2018/9現在)

IdP機関数

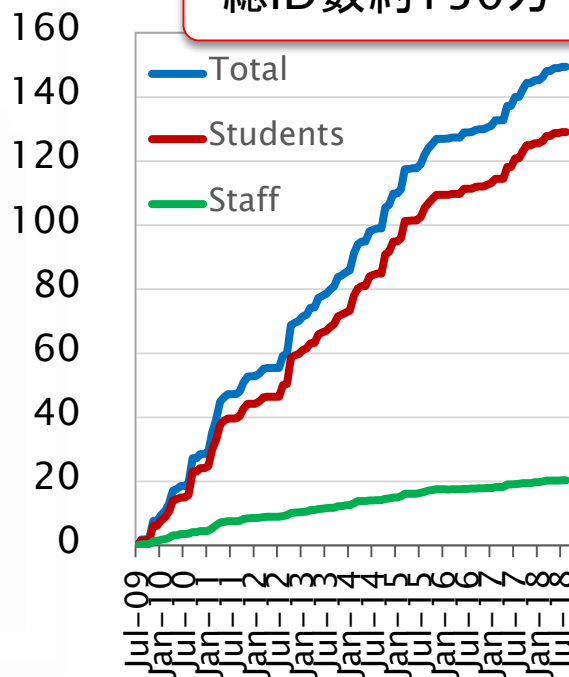
211機関



IdPユーザ数

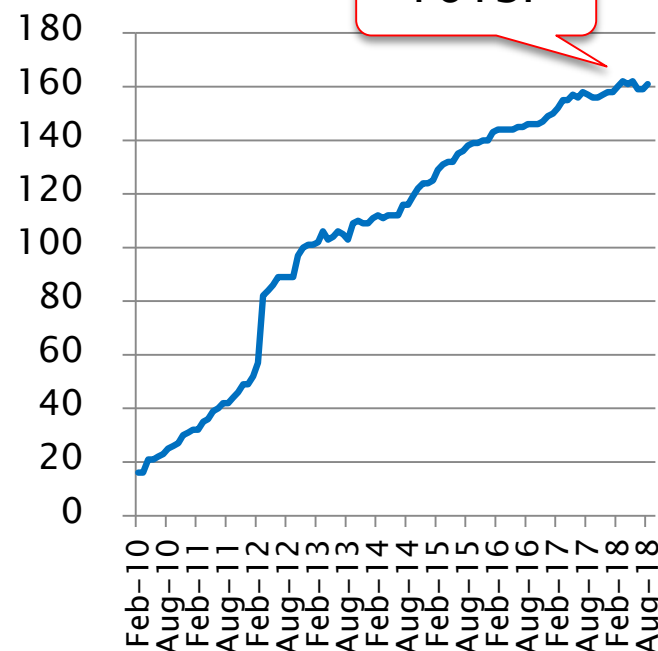
(万人)

総ID数約150万



SP数

161SP



	国立大学	公立大学	私立大学	短期大学	高等専門学校	共同利用機関	その他	合計
学認参加数	73	17	59	0	51	2	9	211
カバー率	85%	19%	9.8%	0%	89%			
総機関数	86	91	600	343	57			

▶ IdP of the Year 2017

- ▶ 近畿大学（6月のNIIオープンフォーラム2018にて表彰）
- ▶ 多要素認証の導入や, Shibboleth以外のミドルウェアを用いたIdPを構築・運用し, 学認の多様性に貢献

▶ 大学ICT推進協議会（11/19～21@札幌）

- ▶ AXIES認証連携部会企画セッションは 11月19日 午前開催

▶ 学認申請システムアップデート

- ▶ eduGAINへの参加の自動化
 - ▶ 「eduGAINに参加する」にチェックを入れて申請するとメタデータ自動登録
- ▶ テンプレート外メタデータアップロード機能
 - ▶ テンプレート外メタデータをアップロード・自動適用する機能を追加、これまでのようなメールでのやりとりは不要

▶ eduGAINについて

- ▶ 各国/地域のフェデレーション間でメタデータを共有する仕組み
- ▶ 参加すると海外のフェデレーションから登録されたSPを使える
- ▶ IdP登録数:2500以上 SP登録数:1700以上
- ▶ 参加するには、学認申請システムで「eduGAINに参加する」にチェック
 - ▶ **注意**:連絡先種別は「**support**」または「**technical**」としてください

▶ eduGAINに参加すると使える海外SPの例

- ▶ eduroam Visitor Access : eduroam利用時の接続支援
- ▶ British Online History : 英国・アイルランドの歴史資料提供
- ▶ CareKnowledge : 社会福祉関係の情報提供
- ▶ CERN : サービスリスト
<http://information-technology.web.cern.ch/services>
- ▶ DROPBOX
- ▶ monitor.eduroam.org : 各地域・国ごとのeduroam関連情報提供
- ▶ ORCID
etc.....

IdP/SPリスト:<https://met.refeds.org/met/federation/edugain/>

▶ 学認参加IdP運用状況調査

- ▶ 今年も実施していますので、全参加機関様のご回答をお待ちしております
- ▶ ご回答いただけない場合、メタデータの出力停止措置もあります

▶ ROCA脆弱性への対応

- ▶ メタデータ切替にご協力いただきありがとうございました。
- ▶ SPの利用に不具合があるようでしたらご連絡ください。
- ▶ 詳細な経過は次ページ

メタデータ署名証明書移行に関するまとめ

- ▶ 2018年10月19日に最後のSPの移行が完了し、全てのIdP/SPの移行が完了
(事務局判明分のみ、提供終了を除く)

▶ 時系列によるまとめ

2017年

- ▶ 10/16 RSA鍵生成ライブラリ脆弱性 (CVE-2017-15361) 公表
- ▶ 11/2 新トークン入手
⋮ 動作検証
- ▶ 11/14 新証明書生成

- ▶ 11/17 新メタデータを並行公開・
IdP/ SP管理者宛移行案内
⋮ メール・電話による状況確認・督促

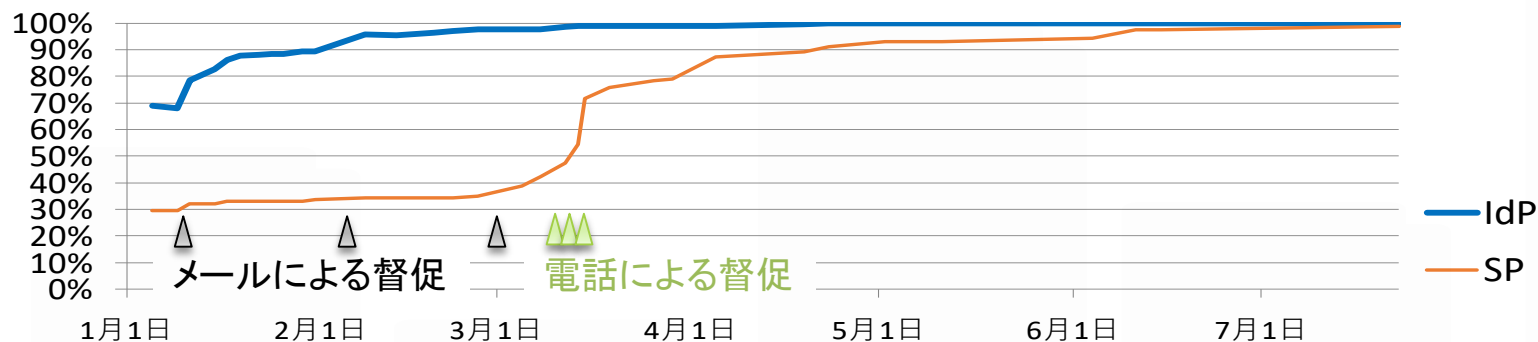
2018年

- ▶ 7/24 旧メタデータ公開停止
⋮ 事後調査で問題があったSPに連絡
- ▶ 10/19 最後のSPの対処が完了

▶ 移行期限の変遷

- ▶ 12/18→1/19→2/16→...→3/31→5/18→7/24(確定)

▶ 移行が確認できたIdP/SPの割合の推移



- ▶ Shibboleth SP ver.3リリース
 - ▶ 最新は3.0.2
 - ▶ 基本的にyum updateで問題なし
 - ▶ 情報はGakuNin Shareに随時追加

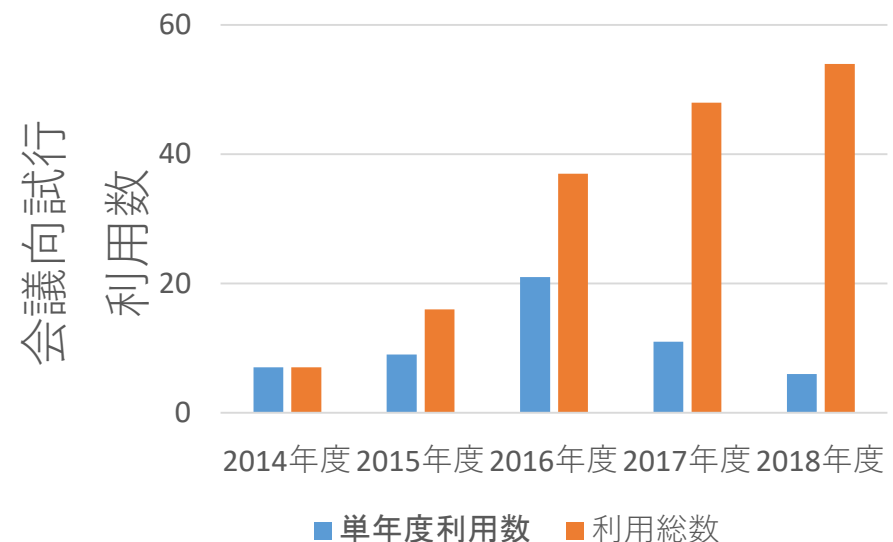
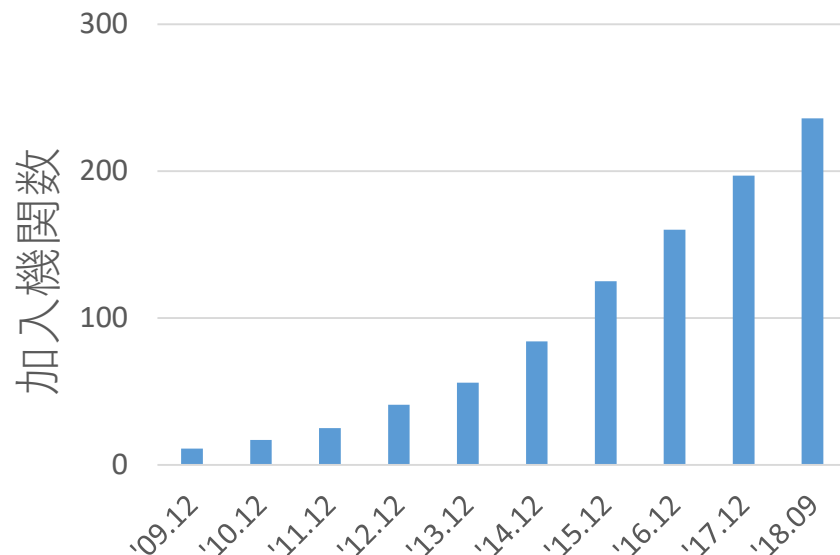
- ▶ Shibboleth IdP ver.3.4(10/10リリース)と今後の変更予定について
 - ▶ **v4.0で名前空間のフラット化が強制され**、プレフィックスが使用できなくなる
 - ▶ v3.4ではフラット化していないとDEPRECATEDのwarningとしてログに出力
 - ▶ フラット化についてはこちら
 - <https://meatwiki.nii.ac.jp/confluence/x/F4Z7AQ>
 - ▶ その他にもDEPRECATEDのwarningとなる対象が複数あり
 - ▶ 影響が大きいものとしては、<DEPENDENCY>要素は内容によって<InputAttributeDefinition>と<InputDataConnector>に変更が必要
 - ▶ 詳細は本家参照: <https://wiki.shibboleth.net/confluence/x/PgLKAg>
 - 変更のある要素の置き換え方法へのリンク等含めて記載
 - ▶ v4.0準備としてwarningが出なくなるまで設定ファイルを修正することを推奨

eduroam JPについて

国立情報学研究所

加入機関数

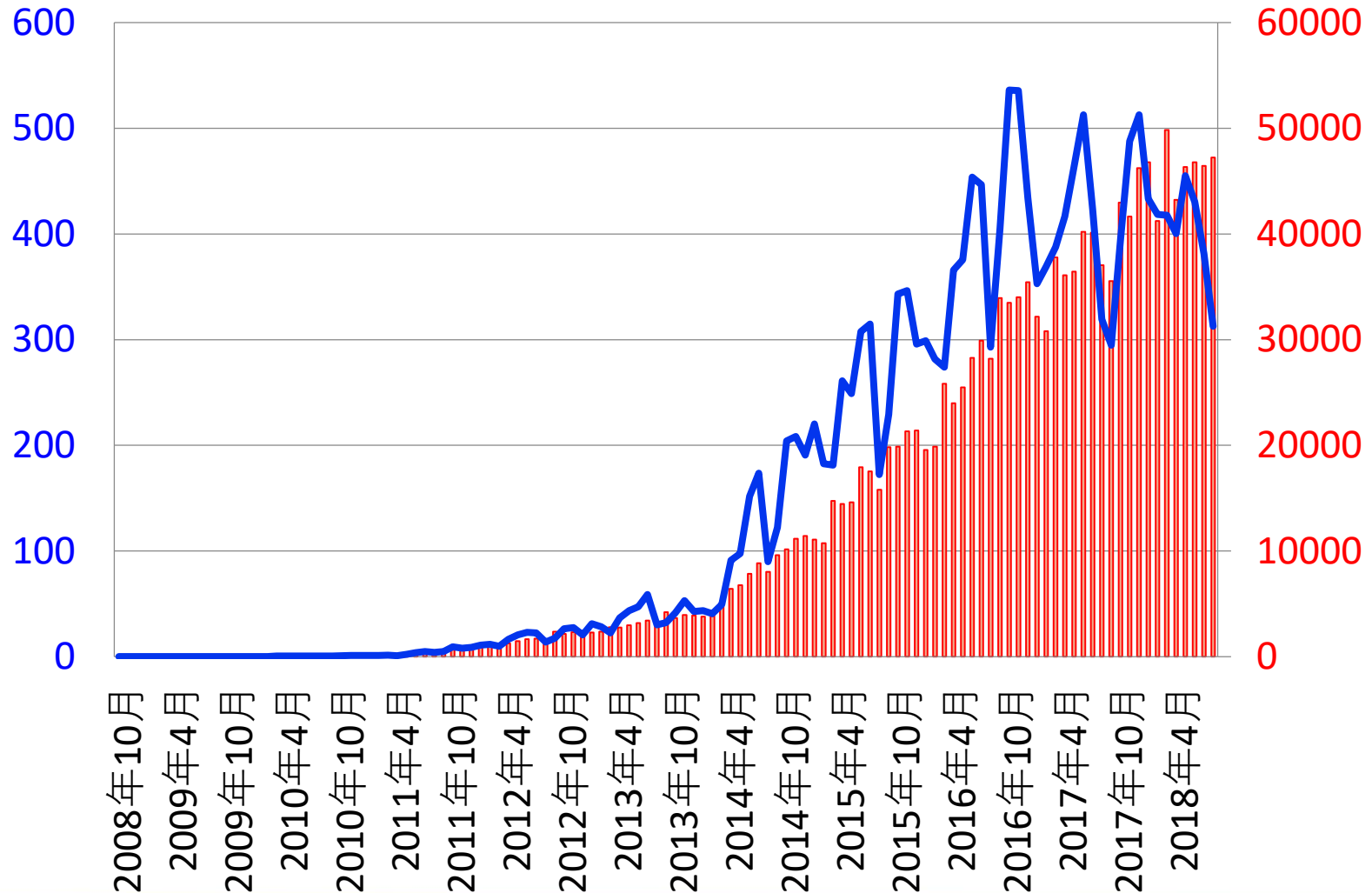
- 232機関がeduroam加入申請済み
- 代理認証システム利用機関数：68 (2018/9/30時点)
- 認証連携IDサービス利用機関数：70 (2018/9/30時点)
- 会議向け期間限定eduroamアカウントの試行：54会議



eduroam月間アクセス数(国内全アクセス)

認証回数 (万)

ユーザ数



規程類・運用体制の整備

• 規程類の改訂

- 学術無線LANローミング基盤サービス加入規程
 - 加入機関の機関区分について改訂予定
- Compliance Statement参考訳公開
 - あくまで参考訳です
 - 原文の記載に従ってください
 - FWの設定方針等が記載されているので原文と併せてご熟読ください

• eduroam JPコミュニティ

- 運用連絡会：お知らせ用ML,インシデント発生時の情報開示
- 何らかのインタラクティブなコミュニティの開設を検討中
 - 加入機関担当者同士の情報交換、eduroam JPへの質問など
 - 利用するプラットフォームについては検討中

eduroam JP各種切替作業

- 加入継続申請
 - 2018/10末で×切
- JP RADIUS Proxyサーバリプレイス
 - 4月より移行作業中
 - ~~2018/06末~~→2018/10末 ×切
 - 未対応の場合、近いうちにeduroamが使えなくなります
 - まだ対応していない場合はお急ぎください
 - 作業手順：
<https://meatwiki.nii.ac.jp/confluence/x/XrOPAQ>

eduroam関連サービス

- **eduroam JP認証連携IDサービス**

- ゲストアカウント利用範囲制限
 - 発行機関からのアクセスのみ許可するように変更
 - JP RADIUS Proxyサーバリプレイスに併せて4月より設定作業中
 - リプレイス対応済みの機関は制限実施済み

- **eduroam CAT(Configuration Assistant Tool)**

- 専用アプリやブラウザを通じて接続設定を半自動化
 - OSによりアプリ経由かブラウザ経由か異なる
 - ユーザ側はIDとパスワードのみ必要
 - 認証サーバの証明書も検証されるため、よりセキュアに
- 機関(認証サーバ)ごとにプロファイルを用意
 - プロファイルは各機関担当者が作成
 - プロファイル管理Webサイトへはeduroam JPが招待します
 - 利用をご希望の場合はeduroam JPまでご連絡ください

その他

- 加入したい場合は
 - eduroam JPウェブサイトにて参加手順等ご案内しています
 - ウェブサイトおよび規程類をご熟読の上、ご参加ください
 - <https://www.eduroam.jp/>
- 小中高の参加について
 - 附属校は大学/学校法人で一括して管理できるなら利用可
 - 大学/学校法人としての加入のみでOK
 - 大学附属校ではない小中高については小中高向けコンソーシアム経由で参加可能
 - <https://nghsig.jp/school.html>

お問い合わせ先

eduroam JPの詳細については以下を参照ください
<http://www.eduroam.jp/>

eduroam全般のお問い合わせ先：
eduroam-office@nii.ac.jp



UPKI電子証明書発行サービス



登録状況および証明書発行状況

2018/9
末日現在

機関
328

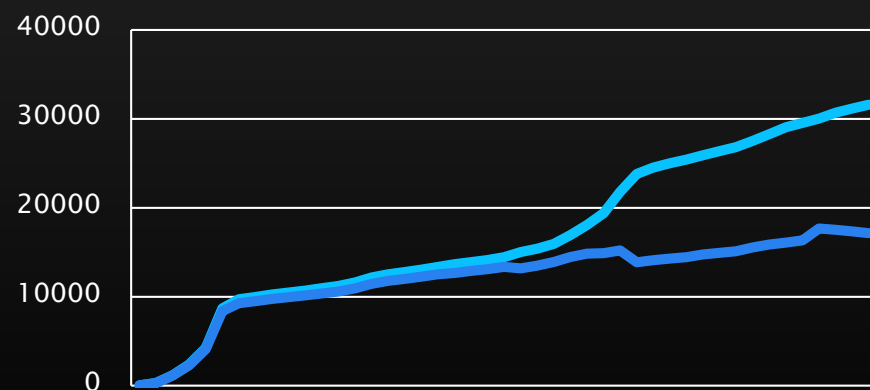
ドメイン
438



サーバ
証明書

のべ発行数
31606

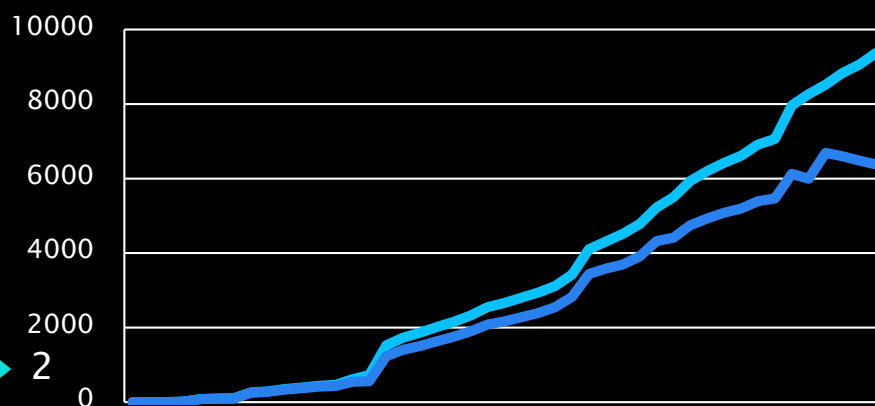
有効数
17150



クライアント
証明書

のべ発行数
9379

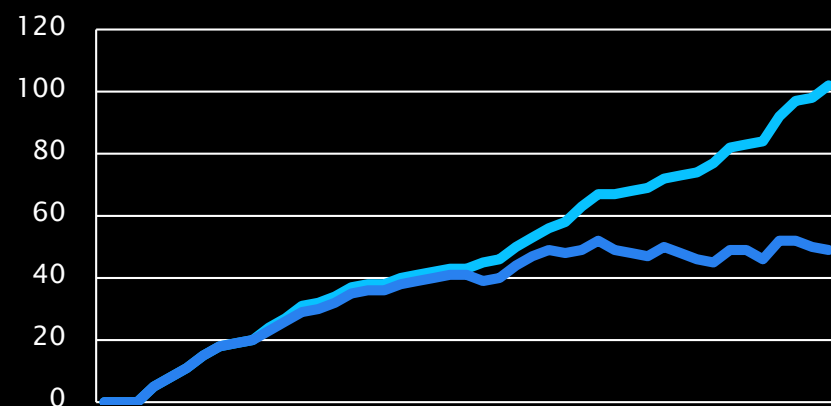
有効数
6375



コード署名用
証明書

のべ発行数
102

有効数
49





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イス等追加
 - ▶ 証明書取得時のWebインタフェイスに、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



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



第三次アップデート 2018/7/9、7/11

- ▶ ECDSAサーバ証明書を提供
 - ▶ ECC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）が発行できます
- ▶ 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を提供開始
 - ▶ 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した
 - ▶ ただしSTは都道府県名を用いることとします（マニュアルに一覧表）
 - ▶ 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した。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した
 - ▶ 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つ追加されました



主体者DNの制限緩和(1)

— ST が指定可 L=Academe固定を廃止

- ▶ 主体者DNの仕様変更
 - ▶ 旧主体者DNの仕様では、「L=Academe」固定、「ST=」使用不可としてきました
 - ▶ CA/Browser Forum の BR(Baseline Requirements) において、OV証明書では L=の値として確認可能な市区町村名を用いることとされており、さらにこれが厳格化されました
 - ▶ ブラウザベンダなどによって、適切な値が指定されているかチェックされます
- ▶ UPKIのOVサーバ証明書でもBRへの対応は必須ですので、仕様変更を行いました
- ▶ また、あわせて要望が多かったSTの値を設定できるようにしました
 - ▶ L=「Academe固定」から、「市区町村名を指定」に変更
 - ▶ 要望が多かった ST=都道府県名 を開放
 - ▶ IISのCSR作成機能が使えます
 - ▶ 主体者DNにてST=を必須とする機器で、UPKIの証明書が利用可能になります
 - Polycomの一部などが該当します



主体者DNの制限緩和(2)

— 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した
 - ▶ 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は使用できません
 - ▶ 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
 - <https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=29235860>
 - ▶ 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
 - ▶ キャンパスや施設の所在地と一致しないケースがあります



主体者DNの制限緩和(3)

— 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



証明書記載事項について

- ▶ 不正確または誤解を招く恐れがある記載事項について
 - ▶ 証明書に表示されている情報が不正確または誤解を招く恐れがあるとCAが判断した場合、当該証明書は失効されます (CAB/F BR 4.9.1.1 項番10)
 - ▶ フィッシングによく使われる（と言われる）文字列を含む証明書発行申請を一時保留するシステム修正を2018年11月18日に実施しました
 - ▶ 例：Amazon, Microsoft, Mozilla, Google…他。
(具体的な禁止文字列リストは公開されておられません)
 - ▶ 具体的には下記の通りです
 - まず認証局で定めた文字列が SANs(Subject Alternative Names) の dNSName に合致するかシステムで判定され、合致した場合証明書の発行が保留されます
 - 認証局は、当該証明書のSANs文字列を確認します
 - フィッシングやその他不正利用のリスクが低いと判断した場合は、発行許可の処理がなされます
- ▶ なお本サービスのCP 項番3.1.6 において、第三者の登録商標や関連する名称を含む証明書発行申請は禁止されております



Whois情報メンテナンスのお願い

- ▶ WhoisDB記載事項のメンテナンスをお願いします
 - ▶ 「登録担当者」
 - ▶ 「技術連絡担当者」
- ▶ 各担当者の更新はもちろん、電話番号やメールアドレスも最新・正確なものに保ってください
 - ▶ 情報が古い場合は、レジストラに連絡して修正してください
- ▶ 今後、ドメイン所有者の確認が厳格化されます。そのために必要な情報となりますので、留意ください。



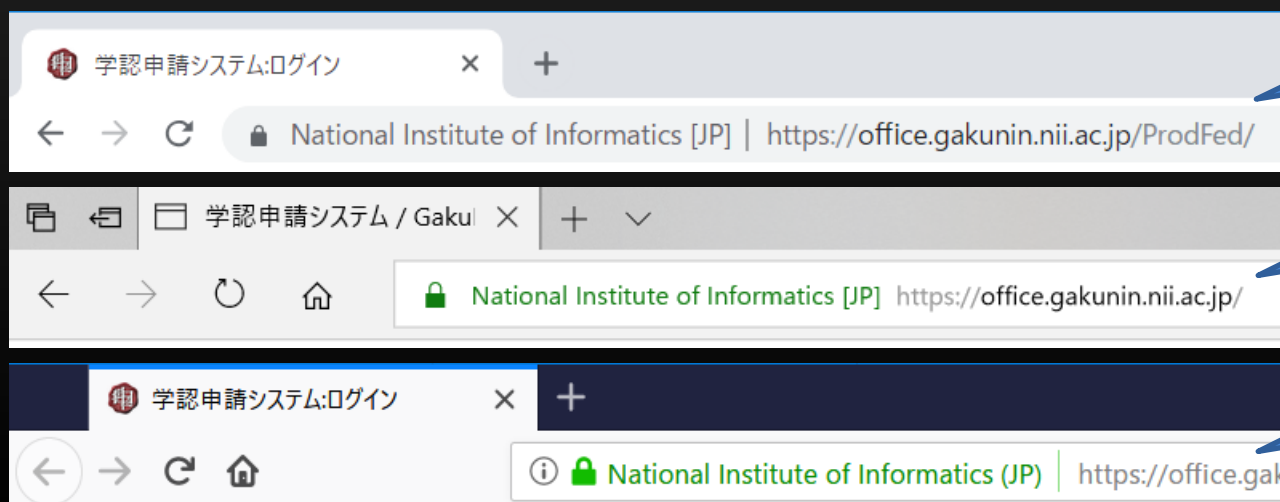
CTログサーバ

- ▶ 現在、以下の3CTログサーバに発行ログを記録しています
 - ▶ Google “Pilot”
 - ▶ Google “Rocketeer”
 - ▶ Comodo “Mammoth”
 - ▶ Symantec “WS”から変更 (2018/9/27～)
 - 9月末日で新規記録受付を終了したため
- ▶ いずれかが停止すると証明書発行が遅延するため、記録先CTログサーバの追加を検討中



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
- ▶ これまでの有効期間12ヶ月に加え、**24ヶ月の証明書も提供開始**(2018年11月～)



※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 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



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・登録担当者からお願いします