UPKI証明書について

NIIサービス説明会 2021年1月19日

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

CA/B Forum BR対応
中間認証局変更

- BRの変更により、UPKIの中間認証局は以下のいずれかの対応が必要になりました
  - 技術的制約を施す
  - 外部監査を受けたものに切り替える
    - BRに定められた、WebTrust準拠性を確認する監査です
- サービス利用機関のご負担が少なくなる前者での対応を検討してきましたが、この場合、中間CA証明書が肥大化し、IEでの検証不能や一部OSでの検証時にハングアップするなどの問題が生じ、これらの不具合を回避する手段はありませんでした
- このため、外部監査を受ける対応をとることになりました
- サービス利用機関の皆様には、多大なご負担をお願いすることになり、申し訳ありません

中間認証局変更

変更点1:サーバ証明書 中間認証局の名称と主体者DN

項目	新中間認証局 （2020年12月25日0:00から）	旧中間認証局 （2020年12月24日まで）
中間認証局の名称	RSA: **NII Open Domain CA - G7 RSA** ECDSA: **NII Open Domain CA - G7 ECC**	RSA: **NII Open Domain CA - G5** ECDSA: **NII Open Domain CA - G6**
中間認証局証明書の主体者DN	RSA: **CN=NII Open Domain CA - G7 RSA** **O=SECOM Trust Systems CO.,LTD.** **C=JP** ECDSA: **CN=NII Open Domain CA - G7 ECC** **O=SECOM Trust Systems CO.,LTD.** **C=JP**	RSA: **CN=NII Open Domain CA - G5** **O=National Institute of Informatics** **C=JP** ECDSA: **CN=NII Open Domain CA - G6** **O=National Institute of Informatics** **C=JP**

変更点2：サーバ証明書 リポジトリ・CP・CRL

項目	新中間認証局 （2020年12月25日0:00から）	旧中間認証局 （2020年12月24日まで）
リポジトリURL	https://repo1.secomtrust.net/sppca/nii/odca4/	https://repo1.secomtrust.net/sppca/nii/odca3/
証明書ポリシ（CP）	https://repo1.secomtrust.net/sppca/cp/ovcp.pdf	https://repo1.secomtrust.net/sppca/nii/odca3/NIIODCA3.pdf
発行する証明書のCRL	RSA: http://repo1.secomtrust.net/sppca/nii/odca4/fullcrlg7rsa.crl ECDSA: http://repo1.secomtrust.net/sppca/nii/odca4/fullcrlg7ecc.crl	RSA: http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlg5.crl ECDSA: http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlg6.crl

変更点3:サーバ証明書 OCSPレスポンダ

項目	新中間認証局 （2020年12月25日0:00から）	旧中間認証局 （2020年12月24日まで）
発行する証明書のOCSPレスポンダ	RSA: http://niig7rsa.ocsp.secom-cert.jp ECDSA: http://niig7ecc.ocsp.secom-cert.jp	RSA: http://niig5.ocsp.secomtrust.net ECDSA: http://niig6.ocsp.secomtrust.net

- ネットワーク的に接続先を制限しているマシンでは、許可リストにこれらURLを加えていただく必要があるケースがございます
  - お問い合わせいただいた例ですと、図書館の書誌情報検索専用マシンなどがあります

変更点4:サーバ証明書 主体者DN OUの値

項目	新中間認証局 (2020年12月25日0:00から)	旧中間認証局 (2020年12月24日まで)

OUの値	• 任意、ただし事前登録が必要
	  • 発行済みの証明書で使用しているOUの値は登録作業不要(登録済みです)
	  • 詳しくは UPKI証明書 主体者DNにおける OUの値一覧 をご参照ください
		• 任意

- OUの値一覧
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=67609949
- OUの値については、他の認証局では廃止されるなど、取り扱いが流動的です
  - セコムトラストシステムズでの取り扱いが変更になった場合、そちらに準ずることになります

サーバ証明書 OUの値について

- サーバー証明書の発行時に指定する主体者DN OUの値を、事前に「OU許可リスト」に登録しておく必要があります
  - 発行済みの証明書で使われているOUの値は、すでに証明書自動発行支援システムに登録済みです
    - ただし、「OUの値として使用できないもの」の条件に合致するものを除きます
- 「OU許可リスト」には、ドメイン、機関名（日・英）、OUの値、が記載されています
  - 許可されているOUの値を知りたい場合は、ドメインとOUの値を1対1で確認してください
  - 同一機関でも、ドメインごとに許可リストに登録されているOUの値は異なります
- OUの値は、大文字と小文字の区別をしておりませんので、大文字と小文字の差異のみで登録を行う必要はありません

OU許可リストに含まれていない場合の対処方法

下記1～3のいずれかの方法でご対応をお願いします。

1. OUなしで発行申請
2. OUの許可リストに登録されているOUに変更して発行申請
3. サービス窓口へ新規でOUを申請し、許可リストにセコムトラストシステムズが登録後、発行申請

※新規OU申請を受け付けてからセコムトラストシステムズで許可リストに登録するまで最大10営業日を要します。

お急ぎの場合は、1または2のご対応をお願いします

OUの値として使用できないもの

下記1～5に該当するものは、OUの値として使用できません

1. 「英字」1文字、「数字のみ」、「記号のみ」、「数字と記号の組み合わせ」
2. Organization nameと異なる組織名
   a. 明らかに別組織のものを指します。
   b. 法人傘下の大学名や、部局名、研究室名、事務局を務める学会名などは登録可能です。
3. 第三者の商号、商標（またはそれに近似する文字列）
4. URL、IPアドレス、ドメイン名、旧機関名・社名、地名（国名、都道府県名、市区町村名等）、国コード
5. 「Null, Unknown, Not Applicable, NA, N/A, None等」該当なし、不完全、適用されないことを示す文字列

変更点5:サーバ証明書 主体者DN STとLの値

項目	新中間認証局 (2020年12月25日0:00から)	旧中間認証局 (2020年12月24日まで)
ST/Lの値	• ST と L の双方が必須 • 詳しくは UPKI証明書 主体者DNにおける ST および L の値一覧 をご参照ください	• ST と L のいずれか、または双方を記入

- STおよびLの値一覧
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=59022761
- サーバ証明書の発行申請時、
  - 既存のサーバ証明書の主体者DNのうち、CNとOUの双方が完全に一致するものがある場合は更新発行申請用TSVファイルを作成してください。
  - 既存のサーバ証明書の主体者DNと、CNおよびOUが一致しない場合は新規発行申請用TSVファイルを作成してください。

変更点6:サーバ証明書 DNS CAAレコード設定値

項目	新中間認証局 (2020年12月25日0:00から)	旧中間認証局 (2020年12月24日まで)
DNS CAA レコード設定値	設定値: secomtrust.net 設定例: xxx.ac.jp. CAA 0 issue "secomtrust.net"	設定値: certs.nii.ac.jp 設定例: xxx.ac.jp. CAA 0 issue "certs.nii.ac.jp"

- CAAレコードを設定すると、証明書を発行する認証局を制限することができます
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=67610271
- 設定必須ではありません

新規または更新発行申請の判断基準

- 既存の証明書で使用している主体者DNのうち、
  - CNとOUが完全に一致する場合は、更新発行申請を行ってください
  - CNとOUが一致しない場合は、新規発行申請を行ってください
- **既存の証明書**のうち、**CNとOUが一致**しているものがある場合、**STとLが異なって**いても更新発行申請を行ってください
  - 「既存の証明書」は、これまでUPKI電子証明書発行サービスで発行したサーバ証明書全てを指します

例：
新規または更新発行申請の判断基準

- **更新発行申請**が必要な場合（CNとOUが一致、LとSTは一致・不一致を問わない）
  - 既存証明書：
    CN=certs.nii.ac.jp,OU=OU1,O=NII,L=Academe,C=JP
  - 発行したい証明書
    ：**CN=certs.nii.ac.jp,OU=OU1**,O=NII,L=Chiyoda-ku,ST=Tokyo,C=JP
- **新規発行申請**が必要な場合（CNもしくはOUが不一致）
  - 既存証明書：**CN=certs.nii.ac.jp,OU=OU1**,O=NII,L=Chiyoda-ku,ST=Tokyo,C=JP
  - 発行したい証明書
    ：**CN=certs.nii.ac.jp,OU=OU2**,O=NII,L=Chiyoda-ku,ST=Tokyo,C=JP
- **新規発行申請**が必要な場合（CNもしくはOUが不一致）
  - 既存証明書：**CN=certs.nii.ac.jp,OU=OU1**,O=NII,L=Chiyoda-ku,ST=Tokyo,C=JP
  - 発行したい証明書
    ：**CN=certs.nii.ac.jp,OU=OU1,OU=OU2**,O=NII,L=Chiyoda-ku,ST=Tokyo,C=JP

既存の証明書情報取得方法

- 登録担当者の方
  - 下記「サーバ証明書情報取得」の手順をご参照ください
    - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=26187929#id-%E3%82%B5%E3%83%BC%E3%83%90%E8%A8%BC%E6%98%8E%E6%9B%B8%E7%AE%A1%E7%90%86%E6%89%8B%E9%A0%86-Toc505784041
- 利用管理者の方
  - https://crt.sh/ で、ホスト名（CN）の検索がおすすめです
  - 本サービス開始時からの証明書情報が登録されています

変更点1:クライアント証明書 中間認証局の名称と主体者DN

項目	新中間認証局 （2020年12月25日0:00から）	旧中間認証局 （2020年12月24日まで）
中間認証局の名称	個人認証用･S/MIME用: **SECOM Passport for Member PUB CA8**	個人認証用: **NII Open Domain CA - G4** S/MIME用: **NII Open Domain S/MIME CA**
中間認証局証明書の主体者DN	個人認証用･S/MIME用: **CN=SECOM Passport for Member PUB CA8** **OU=SECOM Passport for Member 2.0 PUB** **O=SECOM Trust Systems CO.,LTD.** **C=JP**	個人認証用: **CN=NII Open Domain CA - G4** **O=National Institute of Informatics** **C=JP** S/MIME用: **CN=NII Open Domain S/MIME CA** **O=National Institute of Informatics** **C=JP**

変更点2：クライアント証明書 リポジトリ・CP・CRL

項目	新中間認証局 （2020年12月25日0:00から）	旧中間認証局 （2020年12月24日まで）
リポジトリURL	https://repo1.secomtrust.net/sppca/nii/odca4/	https://repo1.secomtrust.net/sppca/nii/odca3/
証明書ポリシ（CP）	https://repo1.secomtrust.net/spcpp/pfm20pub/PfM20PUB-CP.pdf	https://repo1.secomtrust.net/sppca/nii/odca3/NIIODCA3.pdf
発行する証明書のCRL	http://repo1.secomtrust.net/spcpp/pfm20pub/ca8/fullCRL.crl	個人認証用: http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlg4.crl S/MIME用: http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlsmime.crl

変更点3:クライアント証明書 OU・ST/L

項目	新中間認証局 (2020年12月25日0:00から)	旧中間認証局 (2020年12月24日まで)
主体者DN(OUの値)	• 任意	
主体者DN(ST/Lの値)	• ST と L のいずれか、または双方を記入	

- サーバ証明書と異なり、OUとST/Lのルールに変更はありません
- 新規または更新発行の判断基準は、サーバ証明書に準じます

お知らせ

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

機関所在地とドメイン所有権の確認

- 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）

- 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）
  - WhoisDBのメンテナンスをお願い申し上げます

- これらには有効期間があります
  - 2021年8月～9月頃より順次再度の確認を実施いたします
  - 機関によって実施日は異なります

関連リンク

- 中間認証局変更にともなう変更点一覧
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=67609995
- UPKI証明書 主体者DNにおける OUの値一覧
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=67609949
- UPKI証明書 主体者DNにおける ST および L の値一覧
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=59022761

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）
    - お問い合わせフォーム：　https://certs.nii.ac.jp/contact/form
  - 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