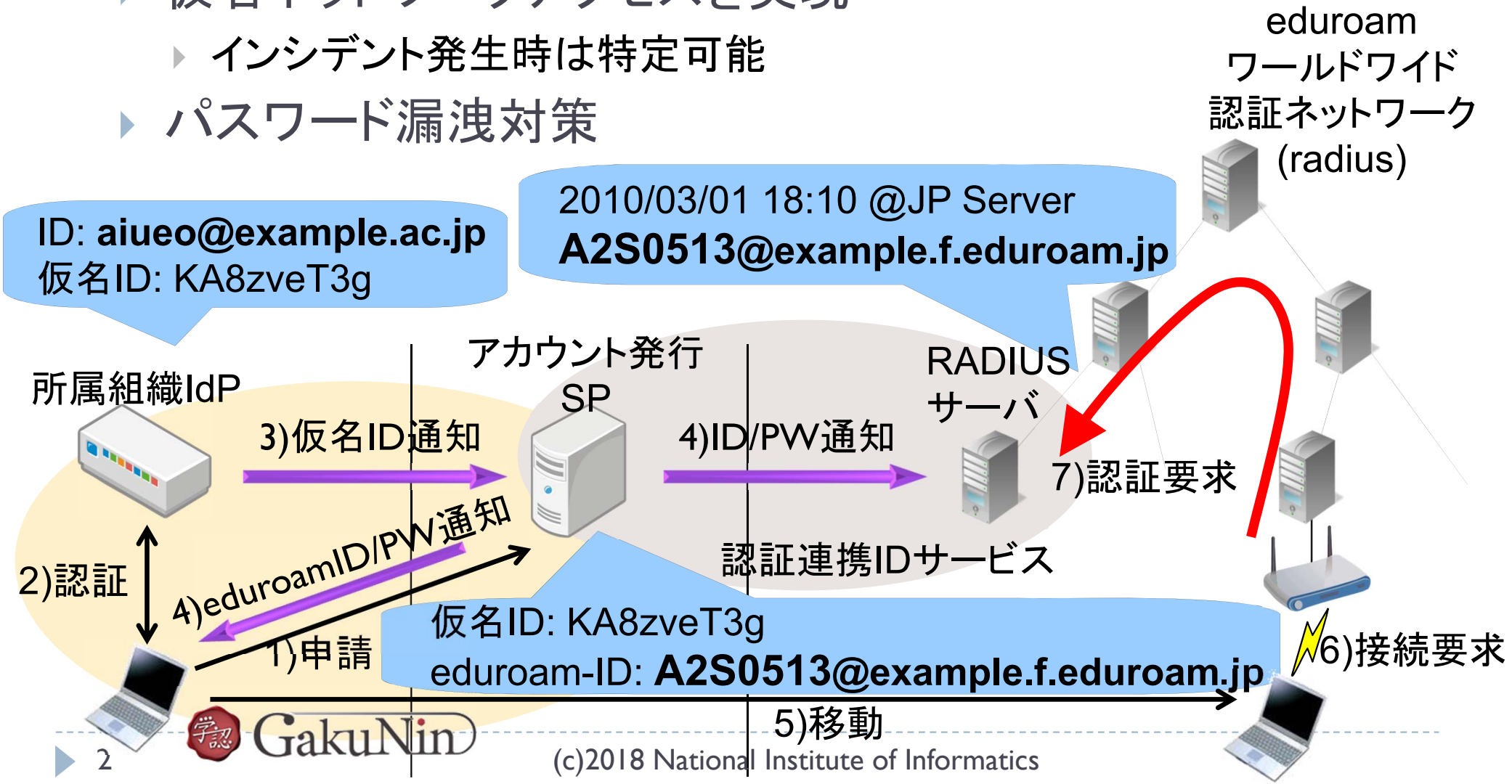
eduroam JP認証連携IDサービス新機能 (Federated-ID new feature introduction)

中村 素典 / 国立情報学研究所

NII学術情報基盤オープンフォーラム2018

eduroam認証連携IDサービス

- 「学認」で認証し、eduroam一時アカウントを発行
  - 仮名ネットワークアクセスを実現
    - インシデント発生時は特定可能
  - パスワード漏洩対策



eduroam認証連携IDサービスの提供開始

- 廃止された「仮名アカウント発行システム」の後継
  - 2017年6月より運用開始
  - IDの形式が変更されました（所属機関がわかる）
    - XXX@DDD.f.eduroam.jp （本人用アカウントの形式）
    - VVV@DDD.v.eduroam.jp （ビジター用アカウントの形式）
      - DDDの部分は、機関毎に異なるサブドメインです
        - 機関が保有するドメイン名ac.jpなどを除いたもの
      - XXX、VVVの部分はID発行時に自動生成されます
      - 所属機関名を示すサブドメインを利用しないこともできます
- クライアント証明書（プライベート証明書）も利用可能
- 0/O/o、1/l/I等の紛らわしい文字の不使用（2018年より）

- 「仮名アカウント発行システム」は2018年3月末で終了
  - XXX@upki.eduroam.jp形式のIDは廃止

IdPから送信すべき属性情報

- o (organization)
  - 機関の識別に利用（必須）
- eduPersonTargetedID
  - 利用者の識別に利用（必須）
- eduPersonAffiliation
  - 教職員・学生を識別した発行のために利用（選択）
    - **学生**：発行制限の適用（有効期限短縮、継続利用確認の対象、ビジター用アカウント発行不可）
    - **教職員**：ビジター用アカウントが発行可能
    - **その他**：ビジター用アカウントは発行不可だが、学生向け制限の適用なし
- eduPersonEntitlement
  - 機関管理者権限の確認に利用（選択）
  - 設定方法については、利用ガイドを参照ください

ビジター用アカウントのエリア制限（新）

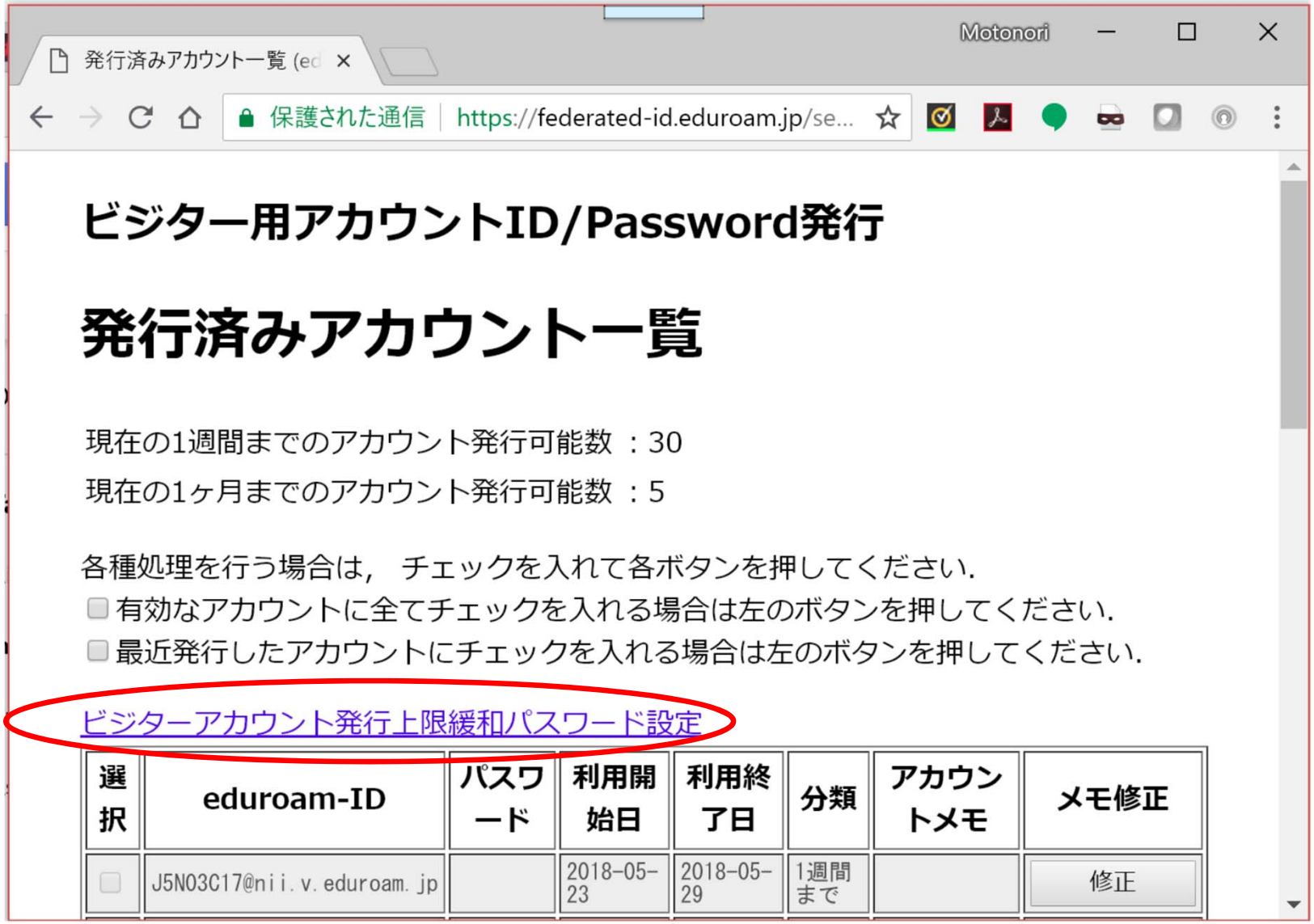
- ビジター用アカウントは、IDが発行された機関のアクセスポイントでのみ利用可能となります
  - 2018年4月以降、各機関のプロキシサーバが、新JPプロキシへの接続に切り替わると、本制限が適用開始となります
  - 切り替えが未実施の場合でも、ビジター用アカウントは海外での利用ができなくなります

- 技術的には
  - RADIUSのOperator-Name属性を参照して判定します
    - 国内機関からの認証要求に対して JPプロキシ側でOperater-Name属性を付与すています（eduroamの運用ポリシーに基づく）
    - 各機関が運用する認証サーバでは、認証要求を行った利用者がどのエリアにいるかが、Operater-Name属性を見ることで知ることができます

国際会議等のサポート（2017/11～）

- これまで「代理認証システム」を利用した「会議向け期間限定eduroamアカウントの試行」（2014～）をご利用頂いていました
- 「認証連携IDサービス」をご利用の機関では、ビジター用アカウントの発行数上限を一時的に緩和する機能を利用して、同様のアカウント発行が可能になりました
- 管理者は以下の項目を入力して、「発行数上限一時緩和機能」を有効にします
  - 上限緩和有効化パスワード：この機能を利用してアカウント発行を行うモードに入るためのパスワード。一度この機能を有効にした利用者は、管理者がこの設定を削除するまで、通常のビジター用アカウントの発行ができなくなります。
  - 発行数上限緩和値：発行可能なアカウント数（～1000）
  - 緩和可能ユーザ数：この機能を利用してアカウント発行を行う者の数（それぞれに、上限緩和値が適用されます）
  - メモ：用途（会議名）などを記載
- 通常時のビジター用アカウント発行数の上限が0（発行不可）となっていても、本機能による発行許可が可能です

ビジター用アカウントの発行数上限一時緩和機能の利用（発行済みアカウント一覧画面から）



学生発行アカウントの継続利用確認機能

- 学生が発行したeduroamアカウントが、卒業後も年度を越えて利用できてしまうことに対する対応策として、「継続利用確認」機能を提供しています。これに伴い、学生発行のアカウント有効期限を最大1年まで設定が可能となっています（デフォルトは3か月）。
- 継続利用確認の手順
  - 管理者が継続利用確認機能を開始する（確認期間に入る）
  - 有効な発行済みアカウントを持つ各学生に対して、ログイン後に継続利用の確認が行われる
    - 「継続利用する／しない」の選択は、期間中に何度でも変更可能
  - 管理者が継続利用確認機能を終了すると、継続利用を希望すると回答していない学生の発行済みアカウントが全て失効される
    - 管理者は、別途、継続利用確認を実施することの広報を行う必要があります

その他、機関管理者向け機能

- 機関毎に以下の値を調整することができます
  - １人あたりの発行可能なアカウント数（同時有効最大数）
    - 教職員、学生共通
  - 学生発行アカウントの発行可否（デフォルトは発行不可）
  - 学生発行アカウントの最長アカウント有効期間
    - 3か月～1年（3か月がデフォルト）
  - ビジター用アカウントの発行可否（教職員のみが発行可）
    - 最大1か月までのアカウントの同時有効最大数
      - 0～10を指定可（デフォルト0：発行不可）
    - 最大1週間までのアカウントの同時有効最大数
      - 0～100を指定可（デフォルト0：発行不可）
      - いずれか一方のみを設定することも可能
    - 同意書PDFや、一覧CSVも出力可能
    - 同時有効最大数の一時緩和（最大1か月のもの）
- 発行済みアカウントの一覧と、個別失効
  - サブ管理者権限の新設（サブ管理者はこの機能のみが利用可）
- 継続利用確認（学生発行アカウントを対象）

発行済みアカウントの一覧

- 利用者（発行者）はeduPersonTargetedIDのハッシュ値部分で表示されます
  - eduPersonTargetedIDが以下のときの「ABCDEF1234567890」の部分
    - <IdPのentityID>!https://federated-id.eduroam.jp/shibboleth-sp/!ABCDEF1234567890
  - ハッシュ値と実IDとの対応は、IdPで確認してください
    - https://meatwiki.nii.ac.jp/confluence/display/GakuNinShibInstall/StoredID
- 有効期限が残っているアカウントのみが失効可能
- 発行済みアカウントは、発行から1年3か月後に一覧から消去されます
- 失効情報は、認証サーバに1日1回反映されます
  - すぐに反映させたい場合は「失効反映」をクリック

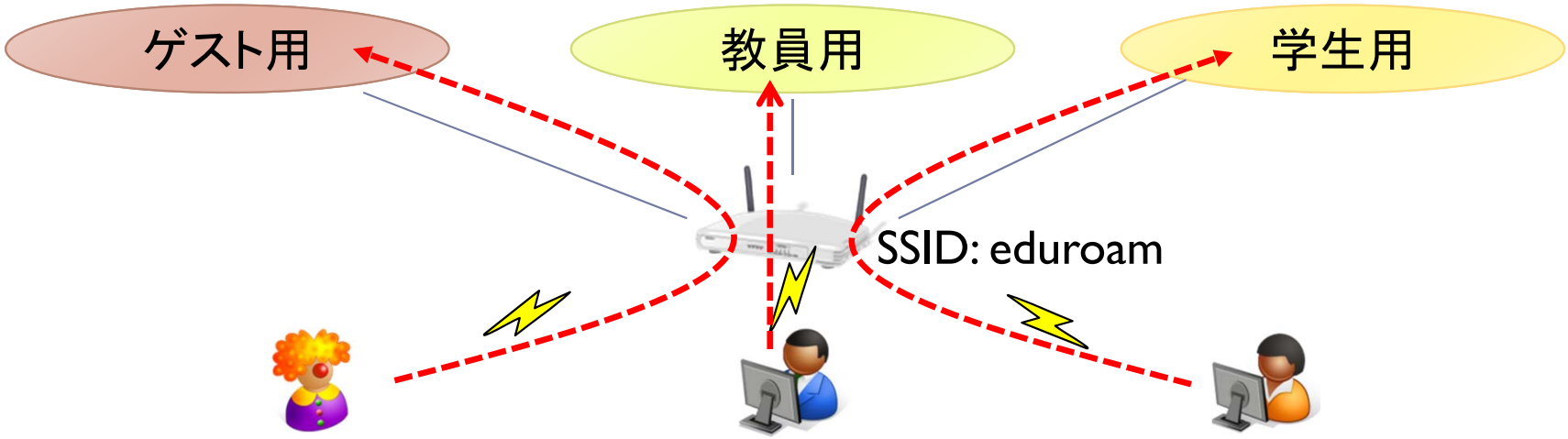
おまけ：認証テスト（Linux等の上で）

- radtest
  - radtest TEST@EXAMPLE.AC.JP PW 127.0.0.1 0 SECRET
- eapol_test (wpa_supplicant附属)
  - EAP設定によるテストツール
  - eapol_test -a 127.0.0.1 -s SECRET -c CONFIG_FILE

```
network={
    ssid="eduroam"
    eap=PEAP
    identity="TEST@EXAMPLE.AC.JP"
#   anonymous_identity="anonymous@EXAMPLE.AC.JP"
    password="PASSWORD"
}
```

認証VLAN （ダイナミックVLAN）

- 同一SSID (eduroam) を用いて、
  - 大学関係者とゲストで接続先のVLANを変える
    - IPアドレス等によりアクセス可能なリソースの範囲を制御したい
  - さらに、教員と学生とで接続先のVLANを変える



- 「レルム」で接続先のVLANを選択可能
  - 教職員用レルムと、学生用レルムの分離など

RADIUSのVLANに関する属性情報

- Tunnel-Type = 13, VLAN
- Tunnel-Medium-Type = 6, IEEE 802 (802.1x)
- Tunnel-Private-Group-Id = 100 VLAN番号

ユーザ毎に異なるVLAN番号を指定する運用も可能

- 認証に成功したユーザが、指定されたVLANに接続される
  - 他機関のユーザに付随する属性情報は無視
- アクセスポイント製品に応じて、指定すべきパラメータが異なることがあるので注意が必要
  - Tunnel-TypeやTunnel-Media-Typeが省略可だったり

レルムによる識別

- 教職員のレルム
- 学生のレルム
- その他のレルム

```
sites-enabled/default:
post-proxy {
        if ("%{Realm}" == "f.example.jp") {
                update reply {
                        Tunnel-Private-Group-Id = 100
                }
        }
        if ("%{Realm}" == “s.eduroam.jp") {
                update reply {
                        Tunnel-Private-Group-Id = 200
                }
        }
        update reply {
                Tunnel-Private-Group-Id = 300
        }
```

最初に設定した値が有効

UPKIクライアント証明書の活用

- eduroamJP認証連携ID発行サービスでのクライアント証明書認証では、プライベートなクライアント証明書を提供。
  - CN=AAAAAAA@DDD.f.eduroam.jp
- パブリックなUPKIクライアント証明書を利用するには？
  - CN=Motonori Nakamura（emailはSubjectAltNameに格納）

（参考）証明書の検証

- CA証明書の取得
  - 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S/MIME用SHA-2認証局CA証明書
    - https://repo1.secomtrust.net/sppca/nii/odca3/nii-odcasmime.cer
  - 国立情報学研究所 オープンドメインSHA-2認証局CA証明書
    - https://repo1.secomtrust.net/sppca/nii/odca3/nii-odca3sha2.cer
  - Security Communication RootCA2 Certificate
    - https://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer

- 証明書を検証する際の注意点
  - 全てのS/MIME証明書は、「NII Open Domain S/MIME CA」から発行されます。
  - 用途にS/MIMEを含まないクライアント証明書は、「NII OpenDomain CA - G4」から発行されます。
  - クライアント証明書では、OCSPによる失効検証は提供されていません。

（参考）FreeRADIUSによるクライアント証明書認証の方法

- CA_file = CA証明書(PEM)を並べたファイルを指定
- check_crl = yes
  - CRLファイルは定期的にダウンロードし、毎回更新後にradiusdを再起動
    - http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlg4.crl
    - https://repo1.secomtrust.net/sppca/nii/odca3/fullcrlsmime.crl
- check_cert_issuer = "/C=JP/L=Academe/O=National Institute of Informatics/CN=NII Open Domain CA – G5"
  - 複数のCAから発行されたクライアント証明書を同時に利用する場合は、このチェックは使えない（自作スクリプトへの組み込み）
- check_cert_cn による判定はUPKIの証明書には使いにくい（→自作スクリプトでチェック）

（参考）自作スクリプトですべきこと

- CRLの定期ダウンロードとCRLに基づく確認
  - 失効されていない証明書であること
- CA証明書に基づく発行者の確認
  - 有効なUPKIクライアント証明書であること
- クライアント証明書のDNの確認
  - 自機関に属する利用者であること
    - /C=JP/L=Academe/O=××University

- UPKIクライアント証明書によるeduroam認証の例
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=25560773

おわりに

- 詳細については利用ガイドを参照ください
  - https://meatwiki.nii.ac.jp/confluence/x/8IdHAQ
  - 認証連携IDサービスのサイトからもリンクがあります
    - https://federated-id.eduroam.jp
- その他eduroamに関するtipsは次のページにまとめています
  - https://meatwiki.nii.ac.jp/confluence/x/tQaGAQ