国立情報学研究所 eduroam JP サービス技術基準・運用基準

（平成２９年６月２３日
制　　定）
改正　平成３０年１月９日
改正　令和４年７月２５日
改正　令和６年７月１８日

eduroam JP サービス 技術基準

1　eduroam JP の認証方式

eduroam JP では利用者の認証方式として、IEEE802.1X に対応した RADIUS を使用する。利用者は利用者 ID とパスワードのペアあるいはクライアント証明書等のクレデンシャルを用いて認証を行うものとする。
キャプティブポータルによる Web 認証の使用は安全性の問題から禁止とする。

2　eduroam 関連システム

2.1　eduroam Compliance Statement への準拠

eduroamに関連するシステムの 要件については、Global eduroam Governance Committee（以下、「GeGC」という。）によって作成された eduroam Compliance Statement（以下、「eCS」という。）に準拠する必要がある。
eCSは、GÉANTのウェブサイトで公開されている[1]。

2.2　eduroam 関連システムの構築

eduroam IdP(ID プロバイダ)およびeduroam SP(サービスプロバイダ)を含め、eduroam 対応のシステムを構築する場合は、eCSに記された要件に従うものとする。
eCSについては別添の「Compliance Statement(参考訳)」を参考にしてもよいが、内容に齟齬がある場合は国内法令等に反しない限り原則として原文が優先される。現在のeCSのバージョンは2.0である。

2.3　eCS 更新への対応

eCSに更新があったときはeduroam JP はその更新内容について、eduroam JPサービス技術基準、eduroam JPサービス運用基準、および Compliance Statement(参考訳)への反映をおこなう。これらeduroam JP管理文書とeCSが相反する場合は、国内法令等に反しない範囲でeCSを優先する。

3　eduroam IdP

3.1　使用する機器

eduroam IdPは、eduroam 認証連携ネットワークに接続するため、RADIUSインタフェースを実装し、EAP メソッドへの対応と相互認証及びクレデンシャルのエンドツーエンドの暗号化をサポートした機器を用いなければならない。

3.2　認証と応答

eduroam IdPは、eduroam SPから送られてくる認証要求(Access-Request)に対し

[1] eduroam Documentation：https://www.eduroam.org/support/eduroam-documentation/

て、認証に成功した利用者についてAccess-Acceptメッセージを応答として返さなければならない。無効な利用者あるいは認証に成功していない利用者に対してはAccess-Reject を返さなければならない。

3.3 アカウント管理方法

eduroam JPサービスでは、アカウント管理方法として、自機関でのRADIUSサーバ運用と、集中管理型IdPとしてeduroam JP 認証連携 ID サービスおよび業者の提供する認証サービスなどを利用することができる。また、この中から複数の方法を組み合わせて利用してもよい。

3.3.1 認証基盤と連携するRADIUS 認証サーバ

eduroam IdPとして、自機関が運用するRADIUSサーバを利用することができる。また、RADIUSに対応したアプライアンス製品を利用してもよい。

eduroam JPでは参考資料としてFreeRADIUSを用いたRADIUS 認証サーバの構築例を提示している[2]。

3.3.2 代理認証システム

代理認証システムは、2024年3月で廃止され、eduroam JP認証連携IDサービスの代理認証機能で代用される。

3.3.3 eduroam JP 認証連携 ID サービス

eduroam JP 認証連携 ID サービスは、eduroam JP が提供し、学術認証フェデレーション「学認」に対応した SP として運用されている、集中管理型 IdP である。

[2] FreeRADIUS 3 の導入：https://meatwiki.nii.ac.jp/confluence/x/bYefBQ

eduroam JPサービスが提供する集中管理型IdPである。加入機関は自機関の所属者がeduroamに接続するための認証システムとして利用することができる。

代理認証機能 は、eduroam JP認証連携IDサービスのサブセットとして提供する、学認加入を要しないeduroam JPサービスアカウント発行機能である。

3.3.4 業者の提供するサービス

機関の IdP を代行する目的で、業者が認証サービスを提供している場合、機関は業者との契約に基づいてそのサービスを利用することができる。

4 eduroam SP

4.1 RADIUS への対応

eduroam SP は、eduroam 認証連携ネットワークに接続するため、RADIUS プロトコルに対応した機器を用いなければならない。

4.2 アクセスポイントのセキュリティ

ネットワークアクセスを提供するアクセスポイントは、IEEE802.1X の EAP に対応し、セキュリティ機能の仕様として WPA2+AES をサポートする、すなわち WPA2 Enterprise (AES)相当の機器を使用しなければならない。なお、WPA2+TKIPはセキュリティ機能として業界団体から非推奨となっている。

4.3 アクセスポイントの機能

ネットワークアクセスを提供するアクセスポイントは、ESSID ごとに異なる RADIUS サーバを指定可能なものを使用することを推奨する。アクセスポイントの選定においては、当該機能を実装していない機器があることについて留意すること。

将来的に、市民向けのローミング基盤であるOpenRoamingを導入する可能性がある場合は、OpenRoamingでは、Passpointの機能が必須であることから、Passpoint (Hotspot 2.0) Release 3以上の基地局を選定することが望ましい。。

4.4 DNS および DHCP の提供

eduroam SP が利用者に提供するネットワークにおいては、DNS キャッシュサーバ（DNS サーバ）および IP アドレスの自動設定基盤（DHCP サーバ）を提供しなければならない。

4.5 eduroam SP ネットワークで提供する IP アドレス

eduroam SP ネットワークで提供する IP アドレスはインターネットに対してルーティング可能なものでなければならない。NAT を用いてルーティングを行うネットワークを構築してもよい。

eduroam SP ネットワークで用いるルーティング可能な IP アドレスは、原則として自機関が保有する IP アドレスブロックから割り当てる。また、ゲスト用に提供されるネットワークからのアクセスであることを明確にするために、新規契約などにより新たに割り当てられた IP アドレスを使用してもよい。

なお、SINET 加入機関については、eduroam JP より、SINET 接続用の最小限の eduroam 接続用 IP アドレスの割り当てを受けることができる。eduroam 接続用 IP アドレスの申請および利用形態については、ドキュメント「SINET における eduroam ア

クセスネットワークの収容について」に従うこと。

4.6 EAP パケットの転送

eduroam SP は利用者および eduroam 加入機関宛のすべての EAP メッセージを改変せずに転送しなければならない。

4.7 RADIUS Proxy サーバ

eduroam SP は利用者の認証要求をJP RADIUS Proxyに転送するRADIUS Proxyサーバを運用しなければならない。なお、JP RADIUS Proxyの負荷の観点から、認証要求はキャンパス単位など合理的な範囲で機関のRADIUS Proxyサーバで集約すること。

アクセスポイントあるいはアクセスポイントを管理するコントローラ等に同様の機能がある場合、その機能を用いてもよい。

eduroam JPでは参考資料としてFreeRADIUSを用いたRADIUS Proxyサーバの構築例を示している[2]。

eduroam JPサービス 運用基準

1　eduroam JPの提供するサービス等

eduroam JPは、その運用のために加入機関に以下を提供する。

1.1　JP RADIUS Proxy

eduroam JPサービスが提供する、各加入機関からの認証要求や認証応答を中継するサーバ。本サーバについては冗長構成をもち、地理的分散を考慮して運用されるものとする。

1.2　代理認証システム

代理認証システムは、2024年3月で廃止され、eduroam JP認証連携IDサービスの代理認証機能で代用される。
なお、これまでに代理認証システムで発行したアカウントについては、外部からのインシデント照会に対応する必要があるため各加入機関の責任において適切に管理すること。

1.3　eduroam JP認証連携IDサービス

eduroam JPサービス加入時あるいはその後に利用を申請することで、eduroam JPと学認の双方に参加している機関の利用者は、eduroam JP認証連携 ID サービスより、eduroam JP サービスの利用者アカウントを発行し利用することができる。
また、利用者アカウントの発行に用いる学認ユーザアカウントについては、各加入機関の責任において適切に管理すること。発行されたアカウントについては、利用者アカウントを発行したユーザおよびその所属機関が責任を負うものとする。

eduroam JPサービス加入時あるいはその後に利用を申請することで代理認証機能により、eduroam JP サービスの利用者アカウントを発行し利用することができる。
また、発行されたアカウントについては、その所属機関が責任を負うものとする。

eduroam JP 認証連携 IDサービス（代理認証機能を含む）の利用にあたっては、eduroam JP認証連携 ID サービス利用規約を遵守すること[3]。

2　変更申請書の提出

申請内容に変更があった場合は、eduroam JP申請システムより変更を申請するものとする。
特に、機関責任者あるいは技術担当者に交代が生じるときは、速やかに変更申請を行うこと。

3　ネットワークおよび機器の運用

eduroam JP サービス加入機関は、サービスに供するネットワーク及び機器について、健全な運用と信頼性維持に努めなければならない。

4　eduroam IdP

4.1　サービスの提供は、国立情報学研究所 学術無線LANローミング基盤サービス加入規程および関連文書の範囲に限ること。

4.2　アカウント管理

eduroam IdP は、利用者のアカウント発行および管理に責任を持つものとする。全ての

[3] eduroam JP 認証連携 ID サービス利用規約：
https://meatwiki.nii.ac.jp/confluence/x/SVhHAQ

アカウントは、当該の機関が管理する有効な利用者情報に基づかなければならない。無効となった利用者については遅滞なく当該利用者に対するアカウントの利用を停止しなければならない。

4.3　利用者への対応

eduroam IdPは本サービスに関する問い合わせを受け付ける窓口を設置し、自機関に所属する利用者に対して開示しなければならない。利用者から受け付けた問い合わせについては、必要に応じてeduroam JPあるいは eduroam JP運用連絡会のメンバーに対して報告・連絡するものとする。

eduroam IdPは、利用者が不正行為等を行わないよう、指導および啓蒙に努めるものとする。また、利用者に無効となったアカウント情報は端末からすみやかに (1ヶ月以内) 削除するよう指導しなければならない。頻繁に認証失敗を繰り返す端末等があれば、当該利用者に対して、アカウント情報を端末からすみやかに削除するように指導すべきである。

4.4　ログの保存

eduroam IdPは、すべての有効な認証試行について、ログを記録・保存しなければならない。ログの保存期間は原則として最短3ヶ月とする。インシデントの報告またはインシデントに関連する調査依頼があった場合は、eduroam JP や他の加入機関の eduroam IdP・SPが行う調査に誠意をもって協力すること。保存すべき最低限の情報は以下のものとする。

(1)　認証要求とそれに対応する応答のタイムスタンプ
(2)　認証要求における外部 EAP アイデンティティ(User-name属性)
(3)　内部 EAP アイデンティティ(実際の利用者識別子)
(4)　接続しているクライアントの MAC アドレス(Calling-Station-ID属性)
(5)　Operator-Name属性が存在すれば、訪問先 SP 情報
(6)　eduroam-SP-country属性が存在すれば、認証要求の訪問国情報
(7)　認証応答のタイプ(Accept, Reject)

4.5　レルムの運用

eduroam JP サービスが運用・管理するレルムは、日本のccTLD、すなわち.jp、に属し、かつ機関が所有する DNSドメイン名に基づいたものに限る。機関は必要に応じて、複数のレルムを運用することができる。運用するすべてのレルムについて事務局に届け出ること。このとき、主たるレルムを一つ指定するものとする。

4.6　レルムの階層化

eduroam IdP は eduroam JP サービスに登録しているレルム下位のDNSドメイン名に対応するレルム名を下位レルムとして運用することができる。eduroam JP サービスでは、特に機関からの要望がない限り、下位レルムを考慮せずに全ての認証要求を当該加入機関のサーバへ転送する。下位 レルムに関する認証要求については、下位レルムの有効・無効を 問わず、機関内ですべて終端し、eduroam JP のサーバに戻らないようにすること。

4.7　学校法人等の名義による申請

複数の高等教育機関を運営する学校法人等が、運営する各機関の eduroam JP サービスへの加入にあたり、各機関で異なるレルムを用いる場合、機関ごとに加入申請書を提出しなければならない。申請書に記載する機関名、機関責任者については、同一の法人名、責任者とすることができる。

5　eduroam SP

5.1　サービスの提供は、国立情報学研究所 学術無線LANローミング基盤サービス加入規程および関連文書の範囲に限ること。

5.2　基地局マップデータの提出

eduroam SPは、eduroam基地局の位置情報をeduroam JPに提出すること[4]。

5.3　課金の禁止

eduroam SPは利用者およびeduroam IdPに対して使用料を請求してはならない。

5.4　ログの保存

eduroam SPはログインした利用者に対して責任を負うeduroam IdPにおける利用者識別を可能とするため、ログを記録・保存しなければならない。保存期間は原則として最短3ヶ月とする。インシデントの報告またはインシデントに関連する調査依頼があった場合は、eduroam JPや他の加入機関のeduroam IdP・SPが行う調査に誠意をもって協力すること。保存するべき最低限の情報は以下のものとする。

(1)　認証要求とそれに対応する応答のタイムスタンプ
(2)　認証要求における外部EAPアイデンティティ（User-name属性）
(3)　接続しているクライアントのMACアドレス（Calling-Station-ID属性）
(4)　接続しているアクセスポイントのMACアドレスとSSID(Called-Station-Id属性、利用できないこともある)
(5)　Operator-Name属性中のSP識別子(ローミング事業者によって付与される)
(6)　認証応答のタイプ（Accept, Reject）
(7)　IdP が返せばChargeable-User-Identity(CUI属性)
(8)　クライアントのレイヤ2(MAC)アドレス、および割り当てられたレイヤ3(IP)アドレスの対応が判別できる情報（DHCPログ等）
(9)　NAT を利用している場合、アドレス変換およびポート変換の履歴

5.5　eduroam SPにおけるアクセス制限

eduroam SP は、セキュリティ対策上制限が慣例とされているものを除き、原則として全てのポートについて通信を制限しないものとする。利用可能なプロトコル等について制限を行う場合は、制限内容についてeduroam JPに届け出ること。また、制限の内容について来訪者を含む利用者に広報すること。

やむを得ず制限を課す場合でも、eduroam JP, GÉANT などから提供されている最低限提

[4] 基地局マップデータの提出について：https://www.eduroam.jp/for_admin/#_74

供すべきサービス(開放すべきポート)の内容を最大限尊重すること[5]。

5.6　障害情報の公知

eduroam SPは、自機関がeduroam JPサービスに供するネットワークや機器に障害が生じた場合、その障害情報について当該障害の発生している機関外から確認できるよう、ウェブサイトなどを通じて広報するよう努めること。

5.7　eduroam SP機器更新にあたって

サービス断を避けるため既存機器を稼働させたままあらたにRADIUSの接続機器を追加登録し、新旧の機器を並行運用することができる。なお、サービス無停止での機器交換等をSPに求めるものではない。

5.8　Operator-Name属性

JP RADIUS Proxyは、eduroam JP加入機関 SP からの認証要求転送にあたってはeduroam JPが機関に割り当てたOperator-Name属性を追加、あるいは上書きする。

ただし、国立情報学研究所学術無線 LAN ローミング基盤サービス加入規程、3条七の機関は、複数機関の運用を受託することがあることから、eduroam JPが割り当てるOperator-Name属性を自身で追加、あるいは上書きして転送すること。委託元SPからの認証要求には委託機関に割り当てられた Operator-Name を、それ以外は自身のものを使用すること。

以上

[5] eduroamとして提供すべきサービスについて: https://www.eduroam.jp/for_admin/85
eduroam Service Definition and Implementation Plan: https://eduroam.org/wp-content/uploads/2020/02/GN2-07-327v2-DS5_1_1-_eduroam_Service_Definition.pdf[5]