国立情報学研究所
eduroam JP サービス技術基準・運用基準

令和4年7月25日

改訂履歴		
版数	日付	内容
1.00	2017/06/23	初版発行
	2018/01/09	IdPおよびSPの提供目的の明確化
	2022/07/25	eduroam JP サービスに登録できるレルムの明確化

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 関連システムの構築

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 Compliance Statement が、GÉANT のウェブサイトで公開されている。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、Compliance Statement に記された技術要件に従うものとする。Compliance Statement 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原則として原文が優先される。現在の Compliance Statement のバージョンは 1.0 である。Compliance Statement の原文は、次のウェブページにある。

eduroam Documentation：

https://www.eduroam.org/support/eduroam-documentation/

Compliance Statement に更新があったときは、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）への反映が行われ、公開されたときから、更新後の Compliance Statement に従うものとする。eduroam JP サービス技術基準、eduroam JP サービス運用基準、Compliance Statement (参考訳)の更新以前に、更新後の Compliance Statement に準拠することについては、これを妨げない。

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し、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-Accept メッセージを返してはならない

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 として代理認証システムおよび eduroam JP 認証連携 ID サービス、業者の提供する認証サービスなどの方法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。当該ソフトウェアを用いて RADIUS サーバを構築・運用する場合は、以下の Web ページを参照のこと。

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

3.3.2 代理認証システム

自機関での RADIUS サーバの運用を行わず、eduroam JP が提供する代理認証システムを利用することができる。eduroamJP サービス加入時あるいはその後に代理認証システムの利用を申請することで、申請の承認後に代理認証システムを用いた利用者へのアカウント発行が可能である。代理認証システムで発行した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。

代理認証システムの利用にあたっては、代理認証システム利用規約を遵守すること。

代理認証システム利用規約：
https://www.eduroam.jp/deas/#_149

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。

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 認証連携 ID サービス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。

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

3.3.4 業者の提供する認証サービス

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 をサポートする機器を使用しなければならない。

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。

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、自機関が保有する IP アドレスブロックから割り当てる方法を基本とする。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、新規回線契約などにより新たに割り当てられた IP アドレスブロックを使用してもよい。

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「SINET4 および SINET5 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。ただし、VLAN 属性等のヘッダ情報については、必要に応じて除去および変更することができる。

4.7 RADIUS Proxy サーバ

eduroam SP は利用者の認証要求を転送する RADIUS Proxy サーバを運用しなければならない。RADIUS Proxy サーバではなく、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、FreeRADIUS 3 を用いた RADIUS Proxy サーバの構築方法を提示している。当該ソフトウェアを用いて RADIUS Proxy サーバを構築・運用する場合は、以下のウェブページを参照のこと。

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

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

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。代理認証システムの詳細については eduroam JP サービス技術基準 3.3.2 を参照のこと。

1.3　eduroam JP 認証連携 ID サービス

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。eduroam JP 認証連携 ID サービスの詳細については eduroam JP サービス技術基準 3.3.3 を参照のこと。

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，高等教育機関における教育研究活動等及び高等教育機関に対する教育研究支援活動に限ること。

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。

また、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。

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 6 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）　認証応答のタイプ（Accept, Reject）

4.5　レルムの運用

eduroam JP サービスに登録できるレルムは日本の ccTLD、すなわち .jp、に属し、且つ機関が所有する 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。二名の技術担当者については、機関ごとに別の者をおくことが望ましいが、認証システムにおけるアカウント管理が適切に行われる限り、同一の二名の担当者をおいてもよい。

5　eduroam SP

5.1　サービスの提供は，高等教育機関における教育研究活動等及び高等教育機関に対する教育研究支援活動に限ること。

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。マップデータのフォーマットおよび提出方法については，次のウェブページを参照のこと。
基地局マップデータの提出について：

https://www.eduroam.jp/for_admin/#_74

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 6 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)　認証応答のタイプ（Accept, Reject）
(5)　クライアントの MAC アドレス、および割り当てられた IP アドレスの対応が判別できる情報（ARP sniffing ログ、DHCP ログ等）
(6)　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利用者に広報すること。

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。

以上