eduroam コンプライアンス・ステートメント

(参考訳第二版)

(原文：eduroam Compliance Statement v2.0 – Issued October 2023)

注：この文書はあくまでも参考訳です。正確な内容については必ず原文を参照し、確認してください。

1.1. この文書では、グローバルな eduroam サービスを提供するため、ローミング・オペレータ(RO: Roaming Operators)およびローミング連合(RC: Roaming Confederations)についての最低限の技術的・組織的標準について概説する。この最低限の標準を実現するためには、ローミング・オペレータ(RO)とローミング連合(RC)の間の調整が必要である。

1.2. この文書は、RO や RC、個々の eduroam 利用者からのフィードバックに基づいて Global eduroam Governance Committee (GeGC)により変更されることがある。あらゆる変更はバージョン管理、および、GÉANT における適切な変更管理手順を経て行われる。この文書は、さらに具体的な合意によって拡大または変更されることがある。

1.3. GÉANT のコーディネーションの下で運営される GeGC は、RO および RC の代表から構成され、GeGC がこの文書の作成に携わった。この文書についてのあらゆるフィードバックは、その検討のために、gegc@lists.geant.org に送付いただきたい。GeGC と GÉANT の関係については、GeGC Charter でさらに記載されている。

1.4. eduroam サービスにおける、各エンティティ(IdP、SP、RO)の運用状態に関する紛争について、責任のある RO または RC によって解決できない場合は、GeGC が最終的な裁定を下す。

1.5. eduroam core Operational Team または Roaming Operator に適用される外部の法律または法的要件の遵守のため、IdP、SP、RO または RC の削除が求められる場合がある(MAY)。そのような決定は、eduroam コミュニティに通知される。

1.6. すべての eduroam SP、IdP、RO および RC は、該当するデータ保護規制を遵守しなければならない(MUST)。

1.7. この文書におけるキーワード「MUST」、「MUST NOT」、「REQUIRED」、「SHALL」、「SHALL NOT」、「SHOULD」、「SHOULD NOT」、「RECOMMENDED」、「MAY」、「OPTIONAL」は、RFC2119[RFC2119] の記述に従って解釈される。

1.8. 以下の定義を使用する：

eduroam	eduroam とは、IdP により発行された利用者ごとのクレデンシャルを用いて利用者を認証することにより、セキュアなネットワーク接続を提供する、認証連携されたローミングサービスである。
eduroam core Operational Team	eduroam サービスのうち、すべてのローミングオペレータに代わって運用される要素を担当するチーム。この core Operational Team は GÉANT によって任命される。
eduroam Identity Provider (IdP)	利用者のクレデンシャル、および利用者の eduroam への接続に責任を持つエンティティのこと。IdP は、一部の地域では Home Institution としても知られている。
eduroam Service Provider (SP)	eduroam 利用者が IdP によって認証に成功することで、それらの利用者がインターネットに接続するために収容される、アクセスネットワークを運用するエンティティのこと。SP は、一部地域では訪問先機関 Visited Institution としても知られている。
Roaming Operator (RO)	一つの国や経済圏のために eduroam サービスを運用するエンティティのことであり、その RO が属する RC によってそのように認められている国や経済圏、あるいは RC が全く設立されていない地域の場合には GeGC によってそのように認められているものを指す。RO は、例えば国の研究・教育ネットワーク(NREN: National Research and Education Network)の運用者が担当する。RO は eduroam operator とも表記されることがある。
RADIUS Proxy Server (RPS)	RPS は、グローバルな eduroam サービスを実現するための技術的基盤(すなわち、RADIUS サーバの階層構造)を提供する目的で構築され、維持されるものである。 地域のトップレベル RPS は、対応する RC によって運用される。RC が構築されていない地域においては、GeGC がその地域の RO のアドバイスを受け、その地域のためのトップレベル RPS を運用する RO を任命する。
Roaming Confederation (RC)	ある地域にサービスを提供する、まとまりのある RO 群として構成され GeGC によりそのように認められているエンティティのこと。“European eduroam Confederation”はその一例である。

2　RO、RC、IdP および SP における管理および技術コンプライアンス

2.1. eduroam では、eduroam SP ネットワークに接続するすべての利用者を個別に識別することが可能な技術を用いる。RO は、利用者の一意識別可能性を保証する責任を負う。

2.2. 認証機構は、相互認証を用いたエンドユーザ検証のため利用者と eduroam IdP の間で定義される。eduroam IdP は、セキュアな方法 (できればアウト・オブ・バンド) で利用者の一意識別性が保たれたクレデンシャルを配布し、利用者が相互認証を用いた IdP の真性性を検証できるようにする責任を負う。

2.3. 利用者識別プロセスでは、Roaming Operator、eduroam SP、および eduroam IdP において、十分なログ情報の記録が求められる。このプロセスには、利用者識別情報が eduroam SP 側のログに含まれる、あるいは送信されることを明示的に含んでいない(利用者のプライバシーを守るため、匿名外部アイデンティティ、あるいは EAP メカニズムが推奨される)。

2.4. RC、RO、eduroam IdP、あるいは SP によって運用される RPS は、受け取った eduroam 参加機関宛の EAP メッセージ (外部アイデンティティを含めて) を、GeGC により定義・合意された eduroam ルーティングメカニズムによって決定されたとおりに、適切な RADIUS サーバ(RC、RO または IdP)に向けて改変せずに転送しなければならない(MUST)。

3　RO における管理および技術コンプライアンス

3.1. RO は特定の国または経済圏内において、eduroam サービスの動作を保証する責任をもつ。

3.2. RO はまた、適切なエンティティが存在しない他の国や経済圏内において、eduroam サービスを運用が可能であり、その運用を望む場合、その eduroam サービス動作を保証する責任をもってもよい。ただし、その国や経済圏を含む地域の RC による、もしくは、RC が構築されていない場合においては GeGC による、明確な承認が必要である。

3.3. RO は、その国または経済圏において、研究や教育に携わっている組織が eduroam IdP として適格かどうかを決定する権限を持つ。

3.4. RO は、その国または経済圏において、eduroam SP の適格性を決定する権限を持つ。eduroam SP の技術要件が満たされ、すべての eduroam 利用者に対してその所属に関わらず、料金なしに接続が提供される限りにおいて、eduroam SP としての適格性には制限がないものとする。

3.5. RO は、他のすべての RO と連絡が取れるようにしなければならない (MUST)。これは、RC あるいは地域の eduroam 運用者リストを介して可能である。RO は eduroam データベース内 (https://monitor.eduroam.org/) のデータが完全かつ最新であることを保証しなければならない(MUST)。RO は適切な通信チャネルを用いて、合理的な時間内に連絡が取れるようにしなければならない (MUST)。

3.6. RO は、GeGC によって定義された適切な方法で、その国や経済圏において利用可能な eduroam SP の位置情報(SP サイト)を公開すべきである(SHOULD)。

3.7. RO は、要件の変更の伝達のため、あるいは問題の解決をはかるために、その国や経済圏における

eduroam SP と連絡がとれるようにしなければならない(MUST)。

3.8. RO は、専用の Web ページにおいて、次の最低限の情報を含む eduroam サービスに関する情報を公開しなければならない(MUST)。

- RC ポリシーの遵守を確認する文書と，その文書への URL リンク (該当する場合)
- IdP のリストと、各々の eduroam SP の Web ページへのリンクを含んだ eduroam 接続サービスエリアを示すリストあるいはマップ
- eduroam サービスやメーリングリストに責任を持つ適切な技術サポートの連絡先についての詳細

3.9. RO は、利用者識別プロセスを確実に完結させるために、その国あるいは経済圏の eduroam IdP および eduroam SP に対して十分なログ情報を保持させなければならない(MUST)。そのための方法は、付録 A および B に記述されている。

3.10. その国または経済圏において、eduroam の名称とロゴが GÉANT の商標として登録されていない場合、RO は、eduroam の名称とロゴを登録しなければならない。あるエンティティが、その国や経済圏を含む地域の RC から RO として認識されなくなった場合、あるいはその地域に RC が確立されておらず、GeGC から RO として認識されなくなった場合は、そのエンティティは商標の所有権を GÉANT に譲渡しなければならない(MUST)。

4 eduroam IdP および SP における管理および技術コンプライアンス

4.1. eduroam IdP および SP に対する要件はこの文書の付録Ａおよびｂに列挙する。それらの要件は、技術的な更新や、各 RO、RC、IdP、SP または個々の eduroam 利用者個人からのフィードバックを受けて改訂されうる。GeGC の過半数の合意によるいかなる変更も、バージョンコントロールを経て管理され、かつ、そのような変更は、その変更が効力を生じる 10 日前までに電子メールで RO および RC に通知されなければならない(MUST)。変更は、eduroam を利用するすべての関係者(RO、RC、IdP、SP など)に適用される。

4.2. この文書に署名することにより、RO または RC は、ここに定められた規則を実施し、従うことを一方的に宣言したものとする。この文書に署名することによって、RC は、RC を構成する RO に本文書に記述された規則を実施させ、従うことを保証する責任を負うものとする。この文書に署名することによって、RO は、その国や経済圏における eduroam IdP および eduroam SP に本文書に定められた規則を実施させ、従うことを保証する責任を負うものとする。この文書に署名することによって、RO または RC は、この eduroam コンプライアンス・ステートメントが、RO または RC が以前に同意したすべての eduroam コンプライアンス・ステートメントに優先することに同意したものとする。

4.3. これに従わない場合、eduroam の名称、ロゴおよび商標についての使用の権利の剥奪を含め、RC や RO などのエンティティの認定がはく奪される場合がある。

Acting as RC/RO for: (country, economy / multiple of)

Signed by: (Name of RO / RC)

Signature: Date:

eduroam コンプライアンス・ステートメント付録

A　eduroam Identity Provider における管理および技術コンプライアンス

A.1. eduroam IdP は、eduroam 基盤に接続するための、RADIUS インタフェースを実装しなければならない(MUST)。

A.2. eduroam IdP は、すべての機関ユーザ に対して、有線のみならず無線ネットワークに適合した EAP メソッドを実装し、相互認証と、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なければならない(MUST)。

A.3. eduroam IdP は、Access-Request を受信し、認証できた有効な機関ユーザに対して RADIUS Access-Accept メッセージを送信しなければならない(MUST)。

A.4. eduroam IdP は、無効なユーザや認証されていないユーザに対して、RADIUS Access-Reject を送信しなければならない(MUST)。

A.5. eduroam IdP は、自機関ユーザをサポートしなければならない(MUST)。いかなるサポート案件も、調整と解決のために、RO または RC にエスカレートすることができる。

A.6. eduroam IdP はすべての認証試行についてログに記録しなければならない(MUST)。ログには以下の情報が記録されなければならない(MUST)。

- 認証要求とそれに対応する応答のタイムスタンプ
- 認証要求における外部 EAP アイデンティティ(User-Name 属性)
- 内部 EAP アイデンティティ(実際のユーザの識別子)
- 接続しているクライアントの MAC アドレス(Calling-Station-Id 属性)
- Operator-Name 属性が存在すれば、訪問先 SP
- eduroam-SP-country 属性が存在すれば、認証要求の訪問国
- 認証応答のタイプ(すなわち、Accept または Reject)

当該国内における規制により別途定めがない限り、最少保持期間は 3 か月とする。

eduroam SP は、訪問先ネットワークの eduroam SP における利用者識別のために、Chargeable-User-Identity(CUI RADIUS 属性)を提供すべきである(SHOULD)。

B　Eduroam Service Provider における管理および技術コンプライアンス

B.1. eduroam SP ネットワークは、eduroam 基盤に接続するための RADIUS インタフェースを備えた 802.1X を実装しなければならない(MUST)。

B.2. eduroam SP の IEEE 802.11 無線ネットワークは、SSID として“eduroam”をブロードキャストしなければならない(MUST)。もし、一つ以上の eduroam SP が同じ場所にある場合、“eduroam-”で始まる SSID を使用してもよい(MAY)。

eduroam SP が IdP のホームネットワークでない(例えば他のローミング基盤の一部)場合は、

001BC50460 内の GÉANT の Roaming Consortium Organization Identifier (RCOI)、または GÉANT によりローミングネットワークに対して割り当てられた(RCOI)を使用して、Passpoint/Hotspot 2.0 経由でネットワークを提供してもよい (MAY)。

B.3. eduroam SP は eduroam Passpoint/Hotspot 2.0 クライアントのすべての認証を eduroam 基盤に向けて転送する必要がある (SHOULD)、基盤の検出に(NAPTR レコードを介した) (RADIUS)動的ピア検出を利用してもよい(MAY)。

B.4. eduroam SP IEEE 802.11 無線ネットワークは WPA2+Enterprise(後方互換を含めて)をサポートしなければならない(MUST)。

B.5. eduroam SP ネットワークは IP アドレスおよび DNS 解決の自動設定基盤を提供しなければならない (MUST)。

B.6. eduroam SP ネットワークはルーティング可能な IP アドレスを提供する必要がある (SHOULD)。また、NAT を提供してもよい(MAY)。

B.7. eduroam SP は外部識別子を含む eduroam 参加機関宛のすべての EAP メッセージを改変せずに Outer Identity を含めて、eduroam 基盤に向けて転送しなければならない(MUST)。

B.8. eduroam SP は、eduroam SP ネットワークに収容した 利用者あるいはその eduroam IdP に課金してはならない(MUST NOT)。

B.9. eduroam SP サービスは SP ローカルポリシに基づいて提供される。ただし、利用者接続の内容を変更すること(例えば、アクセスリストまたはファイアウォールのフィルタルールにより、任意のポートまたはアプリケーション層のプロキシを拒否するなど)は強く非推奨であり、変更する場合は、各々の RO に報告しなければならない(MUST)。

B.10. eduroam SP は、ログを記録および/あるいは転送により、ログインしたユーザについて責任を負う IdP を識別することができるよう十分な(以下の)ログを保持すべきである(SHOULD)：

- 認証要求とそれに対応する応答のタイムスタンプ
- 認証要求における外部 EAP アイデンティティ(User-Name 属性)
- 接続しているクライアントの MAC アドレス(Calling-Station-Id 属性)
- 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、利用できない場合もあり)
- Operator-Name 属性の SP 識別子(RO によって付与されてもよい[MAY])
- 認証応答のタイプ(すなわち、Accept または Reject)
- IdP が返せば、Chargeable-User-Identity(CUI 属性)
- パブリックアドレスが使用されている場合は、クライアントのレイヤ 2(MAC)アドレスとログイン後に発行されたレイヤ 3(IP)アドレスの相関情報(DHCP ログなど)

当該国内における規制により別途定めがない限り、最少保持期間は 3 か月とする。