eduroam コンプライアンス・ステートメント

(参考訳 2018.03.13 版)

(原文：eduroam Compliance Statement v1.0, TSec(11)043 – Issued 4th October 2011)

注：これ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．

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・オペレータとローミング連合の間の調整が必要である．

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，TERENA[1] における適切な変更管理手順を経て行われる．

TERENA[1] 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 からの代表により構成され，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@terena.org>[2]に送付いただきたい．

eduroam サービスにおける，IdP，SP，RO の運用状態に関する紛争について，責任のある RO や 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. 用語

1.1 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た利用者認証により，セキュアなネットワーク接続を提供する，認証連携された無線 LAN ローミングサービスである．

1.2 eduroam Identity Provider (eduroam IdP)

利用者のクレデンシャル，および，それらの利用者が eduroam に接続するための認証サーバの運用に責任をもつエンティティ [3]のこと．IdP は，一部の地域ではホーム機関(Home Institution)としても知られている．

1.3　eduroam Service Provider（eduroam 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[3]のこと．SP は一部の地域では訪問先機関(Visited Institution)としても知られている．

1.4　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[3]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 オペレータ(eduroam operator)とも表記されることがある．

1.5　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な基盤(すなわち，RADIUS サーバの階層構造)を提供することを目的として構築され，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 が設立されていない地域おいては，GeGC はその地域の 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．

1.6　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 群により構成され，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．欧州 eduroam 連合がその一例である．

2.　利用者識別プロセス

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．この利用者識別プロセスは，利用者の EAP 内部の識別子の同一性を確認するために，eduroam SP とユーザの eduroam IdP の通信で定義される．利用者識別プロセスでは，eduroam IdP および SP の双方において，十分なログ情報の記録が求められる．利用者識別プロセスの結果は，責任を持つ IdP が，eduroam SP ネットワークにおいて，特定の使用を引き起こした利用者を識別するためのものである．利用者識別プロセスには，この利用者識別情報が eduroam SP 側に送信されること

を明示的に含んでいない.

3. eduroam EAP パケット転送に関する技術的コンプライアンス

3.1 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 メッセージを, GeGC によって定義・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.

4. RO における管理および技術コンプライアンス

4.1 RO は特定の国や経済圏の中で eduroam サービスの動作を保証する責任をもつ.

4.2 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において eduroam サービスの運用が可能であり, その運用を望む場合, その eduroam サービスの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.

4.3 RO は, その国や経済圏において, 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.

4.4 RO は, その国や経済圏の 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かかわらず, 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.

4.5 RO は他のすべての RO との連絡がとれるようにしなければならない. 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 には合理的な時間内で連絡がとれなければならない.

4.6 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 の位置情報を公開すべきである.

4.7 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.

4.8 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.

4.8.1 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)

4.8.2 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

4.8.3 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

4.9 RO は，利用者識別プロセスを確実に完結させるため，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．そのための方法は，付録 A および B に記述されている.

4.10 もしも eduroam の名称とロゴが TERENA[1]の商標として登録されていない場合は, RO はその国または経済圏における商標として eduroam の名称とロゴを登録しなければならない．もし，あるエンティティがその国や経済圏を含む 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 TERENA[1] に譲渡しなければならない.

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

5.1 eduroam IdP と SP のための要件はこの文書の付録 A と B に列挙する．それらの要件は，技術的な更新や，各 RO，RC，または eduroam 利用者個人からのフィードバックによって改訂されうる．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行われ，このドキュメントの，より以前のバージョンに署名したすべての参加機関に対して効力を生じるものとする.

この文書に署名することにより，RO や RC はここに記述された規則を実施し，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 や eduroam SP に本文書に記載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.

これに従わない場合，eduroam の名称，ロゴ，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[3]の認定がはく奪される場合がある.

付録

A. eduroam IdP 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 ルーティングファブリックに接続するための RADIUS インタフェースを実装しなければならない.

A2. eduroam IdP は，すべてのローカルユーザに対して，有線のみならず，無線ネットワークに適合している 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.

A3. eduroam IdP は，受信したアクセス要求に対して，認証できた有効なローカルユーザに対して RADIUS アクセプトメッセージを送信しなければならない.

A4. 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 アクセプトメッセージを送ってはならない.

A5. eduroam IdP はユーザサポートを提供しなければならない. どのようなサポート案件も，調整と解決のために，RO や RC までエスカレートされることがある.

A6. 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．ログには以下の情報が記録されなければならない.

・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)
・認証応答のタイプ(すなわち，Accept や 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 6 か月とする.

B. eduroam SP における管理および技術コンプライアンス

B1. 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.

B2. eduroam SP の IEEE 802.1X 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．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.

B3. eduroam SP の IEEE 802.11 無線ネットワークは WPA2+AES をサポートしなければならない. また，それに加えてレガシーハードウェアを用いるユーザのため，WPA/TKIP をサポートしてもよい．例外的に，2012 年 1 月 1 日より前に構築された SP に限り，2013 年 1 月 1 日までは WPA/TKIP のみのサポートとしてもよい.

B4. 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.

B5. 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べきである．また，NAT を提供してもよい.

B6. eduroam SP は eduroam 基盤に対し，eduroam 参加機関宛のすべての EAP メッセージを改変せずに転送すべきである．

B7. 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 に対して課金してはならない．

B8. 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．

B9. eduroam SP は，ログの記録により，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，十分なログを保持すべきである．

・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)
・認証応答のタイプ(すなわち，Accept や Reject)
・クライアントのレイヤ 2(MAC)アドレスと，パブリックアドレスが使用されている場合の，ログイン後に発行されたレイヤ 3(IP)アドレスとの相関情報(例えば，ARP sniffing ログまたは DHCP ログ)

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 6 か月とする．

コンプライアンス・ステートメントに関する FAQ

Q. 3.1 によると，EAP メッセージは変更せずに転送しなければならない．この規定は，VLAN 属性を取り除くことや，ブルートフォースアタックを止めることについても制限するものか？

A. RADIUS パケットには EAP メッセージと，VLAN 割り当て属性などの他の属性が含まれている．変更しない必要があるのは EAP メッセージのみである．つまり，VLAN 属性については必要に応じて変更や除去が可能である．
この条項はプロキシサーバについてのみ当てはまることに注意すること．もしブルートフォースアタックが起きている場合，それはホットスポット，すなわち eduroam SP ネットワークから来る．eduroam SP はそのようなことが発生しないように阻止できる可能性がある(関連する条項は B6 であり，「すべき」との規定となっている)．もし SP が，その認証リクエストを IdP に転送することを望むと判断した場合，間にある他の

どんなプロキシも干渉しないものと想定する．
コンプライアンス・ステートメントのこの条項の意図は，プロキシサーバが EAP セッション自体を終端(すなわち, 転送せずにトンネルを終端させるなど)しないことを確認することである．この動作は許容されていない．

Q. 4.6 において，アクセスポイントの情報は特定の形式である必要があると規定されている．なぜ有名なフォーマットに固執することが必要なのか？

A. この情報は，グローバルなホットスポットマップのようなエンドユーザ向け文書のいくつかの部分を編集するために用いられる．もしホットスポットについての情報がいくつかの別々のフォーマットで断片的に管理される場合，統一感のある世界全体のマップを作成することは不可能であるか，技術的な問題によりとても難しい．

Q. 5.1 では「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 や eduroam SP に本文書に記載された規則を実施させ，従うことを保証する責任を負う．」と記述されている．この誓約を RO が遵守するための適切な方法はあるか．

A. RO がこの誓約を遵守するための良い方法の一つは，その国あるいは経済圏において，eduroam IdP と eduroam SP に対して，規則を実施し従うことを承諾する文書に署名させることである．もし，その国や経済圏の IdP や SP が規則に従わないことによって RO の目にとまることになった場合，RO はその IdP や SP に対して適切な行動を起こすことが期待される．

---

[1] 現 GÉANT

[2] 現在は gegc@lists.geant.org 宛とすること

[3] ここでは「組織」の意味