無線 LAN ローミングにおける個人データ活用と認証負荷削減のためのオフライン属性共有手法

後藤英昭 [1)]，　原田寛之 [2)]，　漆谷重雄 [3)]

1) 東北大学 サイバーサイエンスセンター
2) 札幌学院大学 情報処理課
3) 国立情報学研究所

Offline Attribute Sharing Method for Personal Data Utilization and Authentication Load Reduction in Wireless LAN Roaming

Hideaki Goto[1)], Hiroyuki Harada[2)], Shigeo Urushidani[3)]

1) Cyberscience Center, Tohoku University
2) Information Processing Division, Sapporo Gakuin University
3) National Institute of Informatics

概要

著者らは，教育・研究機関向けの無線 LAN ローミング基盤 eduroam を含む市民向けのセキュア無線 LAN ローミング基盤 Cityroam を開発し，2020 年からは OpenRoaming も統合して，全国の商業施設や公共施設，鉄道駅などに展開してきた．近年では東京都や京都市，函館市，姫路市，大阪府などの自治体 Wi-Fi にも採用され，キャンパス外 eduroam サービスの大幅な拡大に寄与している．このようなローミング基盤では，アカウント（利用者 ID）を提供する組織とネットワーク接続サービスを提供する組織が基本的に分かれており，アカウント発行時にデータ利用の許諾や個人の属性を取得できても，ローミング先でこれらを活用することが難しい．従来のフリー Wi-Fi では属性値や行動情報の取得が広く行われてきたが，これが困難になるという理由で，ローミング基盤の導入が難しくなることがある．特に自治体 Wi-Fi の場合は，防災・減災や都市デザインのために行動情報を利用したいというニーズがある．本研究では，ローミング環境においても許諾情報や属性情報を安全に通信事業者間で相互利用できるような枠組みを検討し，基礎となる手法を開発した．この実用化ができれば，セキュア無線 LAN ローミング基盤の普及を通じて，安全な学習・研究環境の整備や，社会全体の ICT 推進に貢献が期待される．

1　はじめに

教育・研究機関向けの無線 LAN ローミング基盤である eduroam (エデュローム) は，執筆時点 (2024 年 9 月) で世界 104 か国 (地域)，国内 439 機関に導入されるに至っている [1]．初等・中等教育機関についても，海外では既にいくつかの国で導入が進んでいる [2]．学生や生徒，教職員の学習・教育・研究環境を改善するために，キャンパスのみならず市街地でも eduroam のサービスを提供したいという要求があり [3, 4]，近年では “off-campus eduroam” のキーワードの下，国内外で展開が活発化している．国内では，eduroam JP の発足から間もない 2010 年から，通信事業者の厚意によって市街地 eduroam のサービスが提供された例がある [5]．しかしながら，長年に渡って各所に働きかけたものの，他事業者や全国への波及には至らなかった．

著者らは，教育・研究機関向けの無線 LAN ローミング基盤 eduroam を含む市民向けのセキュア無線 LAN ローミング基盤 Cityroam [6] を開発し，2020 年からは OpenRoaming [7] も統合して，全国の商業施設や公共施設，鉄道駅などに展開してきた．近年では東京都や京都市，函館市，姫路市，大阪府などの自治体 Wi-Fi にも採用され，キャンパス外 eduroam サービスの大幅な拡大に寄与している．このようなローミング基盤では，アカウントを提供する組織（IdP, Identity Provider と呼ぶ）とネットワーク接続サービスを提供する組織（eduroam では SP, Service Provider と呼ぶ．OpenRoaming などでは，ANP, Access Network Provider と呼ぶ）が基本的に分かれている．利用者が無線 LAN に接続する時，利用者認証の要求が，図 1

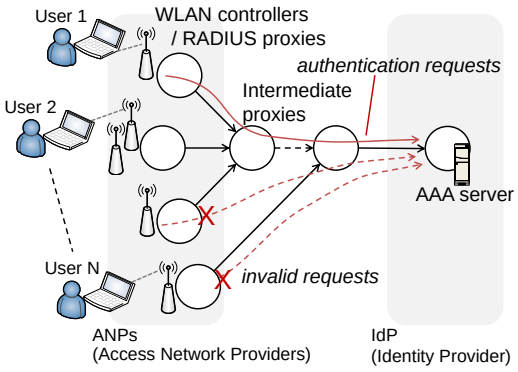

図 1　ローミングシステムにおける認証要求の流れ

のようにいくつかのプロキシを介して ANP から IdP に届けられる．アカウント発行時に利用者からデータ利用の許諾や個人の属性情報を取得しても，IdP と ANP の間にデータを安全に交換する仕組みがなければ，ローミング先でこれらを活用することが難しい．従来のフリー Wi-Fi では利用者属性の利用や行動情報の取得が広く行われてきたが，これが困難になることが，ローミング基盤の普及の障壁になっている．特に自治体 Wi-Fi の場合は，防災・減災や都市デザインのために行動情報を利用したいというニーズがあり，データ利用の仕組みの実現が急務である．

以上に加えて，現行のローミングシステムには，多数の不正な認証要求によって，認証サーバや中間プロキシの負荷が高くなるという問題がある．不正な認証要求の中には，卒業生の端末が発する，期限切れアカウントの認証要求が多く含まれる．この問題は，アカウントの有効期限を属性値とみなせば，前述の問題と同じ機構で対処できると考えられる．

本報告では，初めに，認証負荷の削減を取り上げる．続いて，改ざん対策を含む，汎用性の高い属性共有手法を提案する．本研究では，航空機や船舶，被災地のネットワークなど，上流ネットワークが不安定な環境における無線 LAN ローミングの利用も重要視しながら，オフラインでも利用できるような属性共有手法を開発した．この実用化を進めることで，ローミング基盤の導入障壁を下げられる可能性がある．自治体 Wi-Fi などの eduroam 対応の促進も期待される．

2　認証負荷の削減のための有効期限共有

2.1　問題と関連技術

eduroam や OpenRoaming，Cityroam は，いずれも RFC 7953 の eduroam アーキテクチャ [8] に基づいている．これらのローミングシステムでは，無線基地局（Access Point，AP）が認証連携ネットワークを介して IdP 機関の認証サーバ（Authentication, Authoriziation and Accounting (AAA) サーバ）に接続されている（図 1）．一般に，AP と認証サーバは常時通信可能な状態が想定されている．AP と認証サーバの間には，ANP やハブ事業者の RADIUS (Remote Authentication Dial-In User Service) プロキシが存在し，これらが認証連携ネットワークを構成している．国内の eduroam の場合，eduroam JP のプロキシを運用している国立情報学研究所がハブ事業者に，ANP (SP) と IdP が加入機関に該当する．

eduroam では，大学から大勢の卒業生が出ていくたびに，期限切れのアカウントが多数生じる．卒業生は eduroam の設定を外すように求められているが，それでもなお多くの端末に設定が残っており，期限切れアカウントによる不正な（認証に失敗する）認証要求が多数，プロキシと認証サーバで観測されている．現状ではまだサーバ類の負荷に余裕があり，差し迫った危機はないものの，失敗した認証要求によってログファイルが肥大化して，不正利用や接続トラブルなどの分析の負担になっている．OpenRoaming は，2020 年に立ち上がった比較的新しいシステムであるが，eduroam と比べて格段に多い市民が対象のため，同様の問題が早晩出てくると予想される．

利用者認証が成功した場合，プロキシや認証サーバには 1, 2 行のログが残る．これに対して，認証が失敗した場合は，端末の再認証機能によって短時間に何度も認証要求が送られてくる．一般に，端末には back-off timer の機能が備わっており，10 回程度の試行でも認証が失敗するようならば，一定時間（例えば数分間）再認証を控えるようになっている．しかしながら，しつこく再認証を繰り返す端末も世の中に存在しており，特に，多くの機関から認証要求が集まるハブ事業者のプロキシの負荷上昇が問題になりうる．認証失敗は，必ずしも設定ミスや期限切れアカウントの問題ばかりではなく，攻撃の可能性もある．このため，実際に eduroam JP 事務局から幾つかの大学に調査依頼が出されたことがある．

期限切れアカウントの問題に対処するために，幾つかの機構が用意されている．その一つは，無線 LAN の設定に使うプロファイルに有効期限の情報を持たせておき，期限に到達した時点でプロファイルを無効化する方法である．例えば，Apple の各種（macOS, iOS, iPadOS）で用いられる .mobileconfig 形式のプロファイルには RemovalDate という項目があり，ここに有効期限を埋め込むことができる．有効期限に

達すると，プロファイルの削除を促すポップアップが利用者に提示される．しかしながら，他の多くのオペレーティングシステム（OS）では有効期限が設定できず，また，利用者が手動で無線 LAN の接続設定を行った場合には問題に対処できない．認証要求に対する応答で認証サーバが期限切れを端末や ANP に通知する仕組みも提案されているが，端末に実装されて広く普及するまで年数がかかると考えられる．

2.2 有効期限情報を用いた認証要求の抑制

認証サーバや認証連携ネットワークの負荷を下げる方策の一つとして，図 1 中に×印で示したように，ANP におけるプロキシで期限切れアカウントの認証要求の転送を止めることを考える．利用者認証のたびに IdP に問い合わせるのでは認証負荷の削減にならないので，あらかじめ認証情報の中に属性値として有効期限を埋め込んでおく必要がある．

無線 LAN ローミングでは，ID・パスワード方式の認証方式が広く使われている．具体的には，EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security) [9] や Microsoft PEAP (Protected Extensible Authentication Protocol) などである．これらの方式では，ユーザ ID とレルム（realm）を連結した “`alice@example.com`” のような形式の User-Name が用いられる．この例では，“`alice`” がユーザ ID，“`example.com`” がレルムである．EAP-TTLS や PEAP には，EAP トンネルの外で使われる outer-identity と，保護されたトンネル内で使われる inner-identity の区別があり，プライバシ保護のため，outer-identity の方は匿名化された “`anonymous@example.com`” のような User-Name を用いることが強く推奨されている．従って，属性情報を埋め込むのは，レルム部分に限定される．

ANP が構文解析しやすい形で，有効期限をレルムに埋め込むことを考える．例えば，

“`alice@vu250331.example.com`”

のような User-Name を使うことが考えられる．この例では，2025 年 3 月 31 が有効期限である．ANP や中間プロキシは，この有効期限を越えた認証要求を転送せず，Access-Reject で終端してよい．サブレルムが追加されているが，eduroam や OpenRoaming ではワイルドカードを用いたレルムベースのルーティングが採用されているため，現行の認証連携ネットワークの変更は不要である．ただし，どのような形式で有効期限を埋め込むのかを，すべての ANP と IdP，ハブ事業者の間で標準化しておく必要がある．

ローミングシステムでは，クライアント証明書を用いる認証方式の EAP-TLS [10] も広く用いられている．クライアント証明書には若干の属性値を埋め込むことができるが，必ずしも ANP がこれを読み取ることはできないという制約がある．最近は，プライバシ保護のためにクライアント証明書の内容を保護したいという要求が高まっており，対策が進められている．従って，EAP-TLS を使用する場合でも，レルムに属性値を埋め込むのが現実的である．

2.3 認証負荷削減の評価

提案手法による認証負荷の削減効果を，既存のデータを用いて評価した．この評価には，第一著者らが開発して，2008 年から全国の大学等にサービス提供してきた「eduroam 代理認証システム」を用いた．当システムは IdP as a Service の形をとり，2024 年度末時点で 134 機関（会議利用分を除く）に利用されていた．多数の機関に利用されていることから，大学ごとの IdP に比べて利用者数が格段に多く，提案手法の効果を見るのに適していると考えられる．また，実際に期限切れアカウントによる負荷上昇が可視化されたシステムでもある．2024 年 3 月末にサービス終了したため，今回が唯一の機会であった．

大学の学期の関係で，毎年 4 月頃と 10 月頃に，大量の期限切れアカウントが発生する．古いデータは利用できないことから，本研究では 2023 年度の統計データのみを用いた．同システムが受け取った認証要求の総数のうち，期限切れが理由で Access-Reject となったものは 9.6% であった．この値は，すべての ANP (SP) 機関が提案手法を導入したときに達成される，削減割合の最大値に相当する．

上記の割合は，ログファイルの見た目から受ける印象よりも小さい．サーバのソフトウェアに FreeRADIUS を用いた場合，認証成功した端末に対しては，inner-identity と outer-identity に相当する 2 行がログに残る．一方，認証失敗の場合は端末が再認証を試みるため，複数回の認証試行が記録される．ログファイル中で “Login incorrect” のメッセージが含まれる行（パスワードの入力ミスも含む）は，全体の 20.4% であった．認証失敗は，“Login incorrect” の下にさらに追加の情報が出力されるため，ログファイルの肥大化の影響が大きい．

なお，代理認証システムは eduroam JP のプロキシから認証要求を受け取っている．一般に，RADIUS プロキシは頻繁に認証に失敗する端末からの要求を一時的に抑制する機能を持っている．このため，eduroam

JP のプロキシや，ANP (SP) 機関のプロキシが，再認証の認証要求の多くを叩き落していた可能性がある．一方で，前段にあるプロキシは，IdP が Access-Reject を返した際に，それが期限切れによるものか他の原因によるものかを，区別できない．このため，同様の分析を AP に近いところで実施することは困難である．

今回は，認証サーバで観測されるログのみを分析に用いたが，前段のプロキシのログを見る権限があれば，より高い精度で削減効果の予測ができる可能性がある．そのような分析は今後の課題であるが，複数機関の協力が必要である．

2.4 有効期限の改ざんの問題

提案手法では，有効期限を平文でレルムに埋め込んでいる．有効期限を延ばすなどの目的で，利用者がレルムを改ざんする可能性がある．

有効期限が改ざんされて，認証要求が認証サーバまで到達しても，真の有効期限の情報を持っている認証サーバが正しく認証を失敗させることができる．

3 改ざんを防止できる属性共有手法

3.1 属性共有の用途と課題

本章では，様々な属性を扱えるような，汎用的な属性共有の枠組みを示す．ただし，共有する属性値の具体的な定義は取り扱わない．属性共有の実現のためには，ローミング基盤全体での標準化が必要であり，属性値の定義だけでも広い議論が必要になる．

従来型のフリー Wi-Fi では，IdP と ANP の区別がなく，一つの事業者がアカウント発行と基地局の提供を行っている例が多い．例えば，以下のような情報が収集されている．

- 年齢層
- 性別
- 国籍
- 言語 (ブラウザの設定値などから取得)
- 利用環境 (アプリ等の開発に反映)
- 無線 LAN の利用場所，滞在時間
- 移動経路 (ショッピングモール内で立ち寄った店舗や，観光スポットの分析，防災・減災のためのデータ収集など)

取り扱いに注意が必要な個人情報も含まれているが，それらのデータ取得・利用については，アカウント発行時に利用者に許諾を得ておく必要がある．幾つかの情報は利用者から事前に取得しておく属性値であり，利用許諾もフラグとして属性値の一種とみなせる．

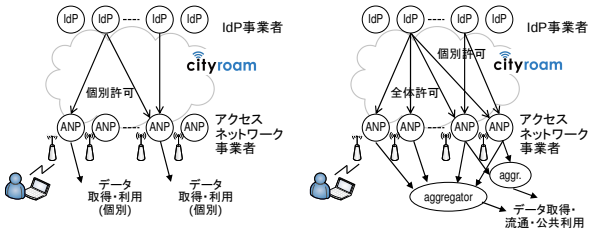

図 2　データ取得・利用の個別許可 (左) と全体許可 (右)

ローミング環境においても，図 2 の左のように，IdP と ANP の間で個別の契約に基づいてデータ取得・利用を許可し，また，属性値を共有することは可能である．しかしながら，1 対 1 の契約では利用範囲が限られてくる．例えば，ある IdP が利用者から取得した利用許諾に基づいて，属性値をどの ANP でも利用できるようにしたいことがある（図 2 右）．年齢に応じたコンテンツ制限などが該当する．自治体 Wi-Fi では，複数の事業者が取得した行動情報を集約したいというニーズがある．これは，防災・減災を含む都市デザインの観点でも重要である．

eduroam の場合は，詳細な属性値や行動情報の利用は好まれないかもしれない．eduroam における重要な属性利用の例として，コンテンツ制限が挙げられる．自治体 Wi-Fi では，法令等 [11] に基づいて，青少年保護のためのフィルタリングの実装が求められることがある．eduroam は，国内外とも初等・中等教育機関への導入も進められており，セキュア無線 LAN ローミングが生徒にとって有用な学習環境になることが予想される．フィルタリング機能をネットワーク側ではなく端末上に実装することが望ましいと考えられるが，自治体 Wi-Fi ではそれとは別にフィルタ実装の要望がある．一方，公衆無線 LAN において一律にフィルタリングを実施することは，「通信の秘密」との関係があり難しい．利用者の属性や事前の同意によってフィルタリングを制御できるようになれば，このように相反する問題の一部を解消できる可能性がある．

利用者属性の中には，利用者や他者が変更できてはいけないものがある．属性値を保護するために，改ざん防止の仕組みも必要である．

3.2 オフライン処理の有用性

2 章で述べた，期限切れアカウントの対策では，オフラインで属性共有する必要があった．利用者認証が成功する場合は，通常は認証サーバまで認証情報が届けられているので，IdP から ANP に対して属性値を送ることができる．これには，RADIUS の VSA (Vendor-Specific Attribute) を使うことが考えられ

る．一方，無線 LAN ローミングの新しい応用先として，上流ネットワークが一時的に不通になるような航空機や船舶などがあり，オフラインでも利用できるような認証手法が考えられている [12]．被災地においても上流ネットワークが寸断されることがあり，このような状況でも地域内のネットワークサービスを安全に利用できるようにするためには，オフライン認証が有効である．

3.3 ローカル認証方式を用いた属性共有

本研究では，ローカル認証方式 [12] を基にして，改ざん防止機能を持つ属性共有手法を実現した．

2 章に示した手法と同様に，属性値を RADIUS User-Name のレルム部分に埋め込む．埋め込む属性値の具体的な種類や形式については，今後の研究や標準化の議論に譲る．本稿では，User-Name の最大長が許す範囲内で，任意のデータの埋め込みを想定する．図 3 に，属性情報共有の機能を盛り込んだローカル認証の仕組みを示す．従来手法 [12] では，パスワードと署名の生成にユーザ ID のみを使用していたが，新しい手法ではレルム部分も含めた User-Name 全体を用いる．本手法のローカル認証の処理の内容は，以下のとおりである．

アカウント発行時に，IdP は有効期限などを埋め込んだユーザ ID を生成する．これにレルムを連結したものを User-Name とする．User-Name に HMAC (Hash Based Message Authentication Code) アルゴリズム [14] と Base64 符号化を適用して，パスワードを生成する．ANP 側にあるプロキシにも同様の処理を実装しておくことで，端末から送出された User-Name を元にして同じパスワードが生成できるので，これを端末が提示したパスワードと比較することで，ANP 側だけでローカルに認証処理が完了する．ハッシュ値を用いてパスワードを生成する方法は，古村らによる先行研究 [13] を参考にした．

[12] の手法では，これに加えて，ECDSA (Elliptic Curve Digital Signature Algorithm) で求めた署名を User-Name に埋め込んでいる．ローカル認証には，機内 Wi-Fi のように，多数のプロキシが HMAC 用の共通鍵を持つような応用がある．HMAC のみを用いる手法では，ANP もアカウントを発行できるが，ローミング基盤の用途によってはこの性質が問題になることがある．正規の IdP から発行されたアカウントのみを有効にできることが望ましい．署名を User-Name に埋め込むことによって，このような制限が実現できる．

属性値はバイナリデータの可能性もあるため，User-Name で使用可能な文字セットに符号化する．RADIUS プロトコルでは，ユーザ ID 部分は大文字小文字を区別する，すなわち case sensitive として扱うことができる．レルム部分は，DNS (Domain Name System) でも用いられることがあり，大文字小文字を区別しない (case insensitive) 符号化が必要である．例えば Base32 符号化が利用できる．属性値のレルム部分への埋め込みは，属性部分だと判断しやすいようなマジック文字列と属性値（符号化後の文字列）を連結する方法が考えられる．

属性値を埋め込んだ後の User-Name は，例えば，
“CYEPBcv7T|MCUCEQC3SwoCbmNfPno3KRvZP7qLAhBg+cHjunGEo6CwKPzHeNz7@xattrjeztqpof52n2xxm7vphkeocp5aqbil43.example.com”
のように表される．これだけ長い文字列を人手で入力するのは困難であるが，近年はウェブサイトから無線 LAN の設定情報を電子的手段で端末に流し込む web-based provisioning が普及してきており，本手法でもこれを用いることを想定している．

3.4 実装と制限事項

提案手法は，FreeRADIUS の Perl モジュールを用いて実装できることを確認している．User-Name の仕様上の最大長は 253 オクテットであり，埋め込むことのできる属性値のビット数は，この値の制約を受ける．従って，詳細な属性をオフラインで共有することは難しい．どのような属性値を優先して埋め込むかは，応用に依存する．プライバシ保護のために属性値の暗号化が必要である．埋め込み可能なビット長の具体的な値について，暗号の強度と併せて議論する必要があり，分析を進めている．

実際にレルムに埋め込まれる符号化後の文字列が，利用者ごとにユニークなものになると，ANP による行動分析を制限する目的で業界がランダム化を強化している MAC アドレスの代わりに，行動分析に利用される恐れがある．共通の属性値を持つ利用者が複数存在するように，埋め込む属性値を取捨選択する必要があると考えられる．

3.5 改ざんに関する評価

利用者が属性値を改ざんした場合，HMAC によって求まるパスワードの値が変わることになる．利用者は HMAC の鍵を知らないので，パスワードの偽造は困難であり，利用者認証が失敗する．

悪意のある ANP は，属性値を改ざんすることによって，「許諾情報が含まれていたので利用者の詳細な行動分析を実施した」というような，虚偽の主張 (false

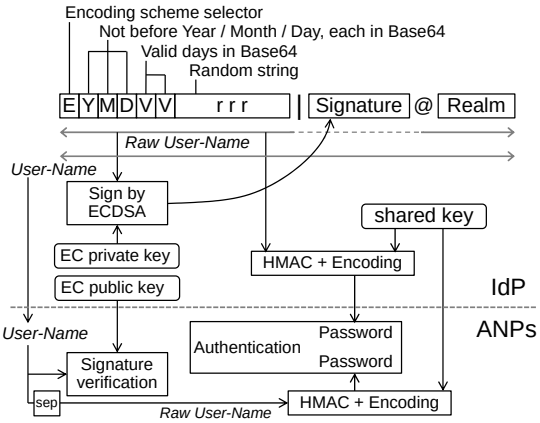

図 3　属性情報共有を考慮したローカル認証方式

claims) を試みようとするかもしれない．ANP が偽造したアカウントを根拠として提示しようとしても，IdP による署名を偽造することは ECDSA の強度の範囲で困難である．IdP が提供している署名検証用の公開鍵を用いることで，第三者でも，不正な署名を見破ることができる．

4　むすび

アカウント発行とネットワーク提供の事業者が分かれている無線 LAN ローミング基盤においても，利用者による明確な許諾が必要な行動解析や属性利用を含め，多くの通信事業者にまたがるデータ利用が可能となるように，安全な属性共有手法を開発した．本研究では特に，今後ローミングの応用が広がると予想される，航空機や船舶，被災地のようにネットワークが途切れる環境も重視した．また，オフラインでアカウントの有効期限を ANP に伝えることで，期限切れアカウントが認証連携システムに及ぼす負荷を軽減できる可能性を示した．

実際のローミング基盤への組み込みや，汎用性の高い属性値の取捨選択，業界における標準化などが，今後の課題である．

本研究の一部は，令和 6 年度国立情報学研究所公募型共同研究の助成を受けた．

参考文献

[1] eduroam JP: https://www.eduroam.jp/ (2024 年 9 月 27 日参照)

[2] 後藤英昭, 原田寛之, 漆谷重雄, “キャンパス外 eduroam と大学における OpenRoaming 導入,” 大学 ICT 推進協議会 2021 年度年次大会 論文集 FC1-3, 2021.

[3] eduroam Everywhere: https://www.heanet.ie/services/connectivity/eduroam-everywhere (2024 年 9 月 27 日参照)

[4] Metro eduroam: https://renu.ac.ug/metro-eduroam/ (2024 年 9 月 27 日参照)

[5] INTERNET Watch, “ライブドアと NII、学術無線 LAN ローミング基盤の共同実験を開始,” https://internet.watch.impress.co.jp/docs/news/353536.html (2024 年 9 月 27 日参照)

[6] Cityroam: https://cityroam.jp/ (2024 年 9 月 27 日参照)

[7] WBA OpenRoaming: https://wballiance.com/openroaming/ (2024 年 9 月 27 日参照)

[8] K. Wierenga, S. Winter, and T. Wolniewicz, “The eduroam Architecture for Network Roaming,” https://datatracker.ietf.org/doc/html/rfc7593 (2024 年 9 月 27 日参照)

[9] P. Funk and S. Blake-Wilson, “Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0),” https://datatracker.ietf.org/doc/html/rfc5281 (2024 年 9 月 27 日参照)

[10] D. Simon, B. Aboba, and R. Hurst, “The EAP-TLS Authentication Protocol,” https://datatracker.ietf.org/doc/html/rfc5216 (2024 年 9 月 27 日参照)

[11] “青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律,” https://laws.e-gov.go.jp/law/420AC1000000079 (2024 年 9 月 27 日参照)

[12] H. Goto, “Disruption-tolerant Local Authentication Method for Network Roaming Systems,” Journal of Information Processing (JIP), Vol.32, pp.407–416, 2024.

[13] 古村隆明, 岡部寿男, 中村素典, “SAML 連携を用いてロケーションプライバシを守る eduroam アカウント利用方式,” 信学技報 SITE2009–57, pp.153–158, 2010.

[14] H. Krawczyk, M. Bellare, and R. Canetti, “HMAC: Keyed-Hashing for Message Authentication,” https://datatracker.ietf.org/doc/html/rfc2104 (2024 年 9 月 27 日参照)