セキュア無線 LAN ローミング基盤 Cityroam サービス技術・運用基準

一般社団法人無線認証連携協会

2024 年 9 月 20 日 制定

1 概要

本技術・運用基準 (以下、本基準という) は、一般社団法人無線認証連携協会 (以下、協会という) が実施するセキュア無線 LAN ローミング基盤 Cityroam のサービス (以下、本サービスという) について、上位文書の「セキュア無線 LAN ローミング基盤 Cityroam サービス実施要領」を補う、技術面および運用面での基準ならびに仕様を定める。

2 規程類・基本仕様

Cityroam 関連のシステムを構築し、サービスを提供しようとする組織は、「セキュア無線 LAN ローミング基盤 Cityroam サービス実施要領」および本基準に従う必要がある。また、構築するシステムやサービスは、原則として Wireless Broadband Alliance (WBA)が定める無線 LAN ローミングの標準化文書である WRIX (Wireless Roaming Intermediary Exchange) に準拠する必要がある。例外がある場合は、本基準に明記される。

Cityroam は、The eduroam Architecture for Network Roaming (RFC 7593) を基本とする認証連携アーキテクチャを採用している。また、学術系ローミング基盤 eduroam と WBA OpenRoaming を一本化して扱えるような統合アーキテクチャを採用している。

- The eduroam Architecture for Network Roaming (RFC 7593)
  https://datatracker.ietf.org/doc/rfc7593/

Cityroam サービスのうち、OpenRoaming に関する部分については、WRIX に加えて、Passpoint (Hotspot 2.0) および OpenRoaming 関係の仕様に従う必要がある。

- Wireless Broadband Alliance (WBA) Wi-Fi Roaming Standard – WRIX
  https://wballiance.com/resource/wi-fi-roaming-standard-wba-wrix/
- Wi-Fi CERTIFIED Passpoint
  https://www.wi-fi.org/ja/discover-wi-fi/passpoint/
- WBA OpenRoaming Standards
  https://wballiance.com/wba-openroaming-standards/
- OpenRoaming End-User Privacy Policy
  https://wballiance.com/openroaming/privacy-policy/

現時点での WRIX はバージョン 3.4.0、OpenRoaming Framework & Standard Architecture はバージョン 4.4 である。これらの文書は WBA メンバー限定のため、Cityroam サービス加入組織に対して協会より提示する。

Cityroam サービスのうち、eduroam に関する部分については、eduroam (GÉANT)および eduroam JP の規程に従う必要がある。大元の規程は、Global eduroam Governance Committee (GeGC)により作成された eduroam Compliance Statement (現時点で v2、以下、eCS という) である。

・eduroam Documentation (eCS の原文があるサイト)
https://eduroam.org/support/eduroam-documentation/

・eduroam JP の加入規程、実施要領、技術・運用基準
https://www.eduroam.jp/for_admin/366

その他、Cityroam サービスのローミングパートナーが独自の制限を課している場合は、これに従うものとする。

3 認証方式

Cityroam では、利用者 (またはクライアントデバイス) の認証に、IEEE 802.1X に対応した RADIUS を使用する。利用者 (クライアント) 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。

安全上の問題があるため、IEEE 802.1X 用に発行されたクレデンシャルをウェブ認証で使用することは禁止する。

4 システムの構築

Cityroam に関連するシステムおよびサービスの要件については、前述のように eCS、WRIX、並びに、本基準の定めに従うものとする。内容に非互換性がある場合は、原則として本基準の方を優先する。協会は非互換性を解消できるような調整に努める。

5 IdP (Identity Provider)

5.1 使用する機器またはソフトウェア

IdP は、Cityroam の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、および、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またはソフトウェアを用いなければならない。EAP では TLS 1.2 および TLS 1.3 をサポートする必要がある。TLS 1.1 やこれよりも古いプロトコルは、安全上の観点から、原則として使用してはならない。

IdP は、RADIUS のトランスポートとして、TLS 1.2 と TLS 1.3 の両方に対応した RadSec エンドポイントを実装しなければならない。Cityroam の認証連携ネットワークにおいて、UDP を用いる従来の RADIUS プロトコルによる接続は、段階的に廃止の予定である。

UDP を用いる従来の RADIUS プロトコルによる接続を行う場合、加入組織は最大 2 台までの IdP を Cityroam の認証連携ネットワークに接続できるものとする。試験などの一時的な用途を除き、原則として、3 台以上の接続は認められない。

5.2 認証と応答

IdP は、ANP (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は 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失敗した利用者に対しては Access-Reject メッセージなどで応答し、Access-Accept メッセージを返してはならない。

認証に成功した利用者については、不正利用者の特定などに利用できる情報を含んだ Chargeable-User-Identity (CUI)属性を応答に含める。この値は IdP と ANP でログを突き

合わせるために用いられ、利用者 ID を含むデータのハッシュ値でもよい。

5.3 アカウント管理方法

アカウント発行の主体となる組織は、アカウント発行方法として、自組織が運用する RADIUS サーバや、他の組織がホスティングサービスやクラウドサービスとして提供する RADIUS サーバを用いてもよい。

5.4 利用者の紐づけとアカウント発行の責任

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、不正利用などのインシデント発生時に利用者本人を割り出すのに有用な、本人確認または何らかの本人紐づけを実施した上で、発行されなければならない。

しかしながら、現時点では電子的手段による本人確認が容易ではないという事情に鑑み、例えば SMS を利用した電話番号の確認・紐づけや、信頼できるプロバイダのメールアドレスとの紐づけ、信頼できる SNS のアカウントとの紐づけなどを行う方式も暫定的に認める。やむを得ずこのような方式を採用する場合、捜査において有用な情報を取得するように努めること。

不正利用などにより利用停止とすべき利用者については、すみやかにアカウントの利用を停止しなければならない。

無効になったアカウントについては、すみやかに端末から削除するように、利用者に指導することが望ましい。頻繁に認証失敗を繰り返す端末があった場合は、アカウントが無効になっているか、設定ミスや端末の不具合の恐れがあるので、端末から設定を削除するように当該利用者に指導することが望ましい。

5.5 利用者への対応・啓発活動

IdP は、自組織が発行したアカウントの利用者に対して、問い合わせを受け付ける窓口を設置、開示しなければならない。問い合わせの内容が、他の Cityroam 加入組織にも影響する場合は、必要に応じて運用連絡会などで報告・連絡するものとする。

利用者が不正行為等を行わないよう、啓発活動と指導に努めるものとする。

法令、および、総務省のガイドラインなどを参考にして、セキュリティ対策と青少年保護に留意すること。これを元に、利用者にも注意喚起を行うこと。

サイトブロックを実施するには利用者の同意が必要となることに注意が必要である。一般に、公衆無線 LAN ではネットワーク側で確実にフィルタリングを行うことが難しいことから、必要に応じて端末側でフィルタリングを行うことを利用者に推奨していく。

- [総務省] 無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について
  https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
- [e-Gov 法令検索] 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://elaws.e-gov.go.jp/document?lawid=420AC1000000079

5.6 ログの保存

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 か月とする。ただし、国内法令や、利用者の居住地の法律と齟齬がある場合は、適切な法に従うものとする。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、協会や他の加入組織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) 認証要求の User-Name 属性 (Outer-Identity と Inner-Identity がある場合は両方)

(3) 利用者の識別子 (Inner-Identity など)と実利用者を紐づける情報

(4) ANP から通知された端末の MAC アドレス (Calling-Station-Id 属性)

(5) 認証応答のタイプ (Accept, Reject)

(6) Operator-Name 属性が存在する場合はその値

(7) RadSec による接続の場合は、クライアント証明書の Common Name (CN) (取得できる場合のみ)

5.7 使用するレルムと加入組織側での終端

レルム (realm)は利用者の所属を識別するための符号であり、RADIUS プロトコルの User-Name 属性においてアットマーク (@) の後ろ (右側) に設定される。Cityroam で使用する基本的なレルムを基本レルムと呼び、cityroam.jp を用いる。加入組織は原則として組織の英字略称を基本レルムの前に付けたものを使用するものとする (例：exampleinc.cityroam.jp)。これを組織基本レルムと呼ぶ。

使用する英字略称は、組織が一般的に DNS ドメイン名などで使用しているものを原則とするが、別のものを希望する場合は、先願主義により、協会と協議の上で決定する。

基本レルム以外のもの (3GPP など) を使用する場合は、組織が登録した DNS ドメイン名と整合するものを原則とし、協会と協議の上で決定する。

レルムは DNS のドメイン名としても使われるため、case-insensitive (大文字小文字を区別しない) である。

加入組織は、協会に通知することなく随時、組織基本レルムの左側に任意のサブレルムを付与してもよい。(例： subrealm1.exampleinc.cityroam.jp)

Cityroam の認証連携ネットワークから送られてくる認証要求のうち、自組織の組織基本レルムが末尾に付いているものは、IdP においてすべて終端し、認証連携ネットワークに戻すような転送は行わないこと。もし、他の組織から自組織以外の組織基本レルムが付いた認証要求を受け取った場合は、破棄してよい。

加入組織がサブレルムを使用せず、組織基本レルムのみを使用する場合であって、RADIUS proxy でワイルドカードによるマッチングができない場合は、proxy の接続前に協会に申し出ること。これを怠った場合、認証要求のループが発生することがある。

6 ANP (Access Network Provider), SP (Service Provider)

6.1 RADIUS proxy

ANP (SP)は、アクセスポイントを介して利用者端末から送られてくる認証要求を Cityroam の認証連携ネットワークに転送するために、RADIUS proxy を運用しなければならない。RADIUS proxy 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、これを用いてもよい。

UDP を用いる従来の RADIUS プロトコルによる接続を行う場合、組織は最大 2 台までの RADIUS proxy を Cityroam の認証連携ネットワークに接続できるものとする。試験などの一時的な用途を除き、原則として、3 台以上の接続は認められない。RadSec を用いた接続の場合は、4 台程度まで接続してよい。

6.2 使用する機器またはソフトウェア

ANP は、Cityroam の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、および、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またはソフトウェアを用いなければならない。EAP では TLS 1.2 および TLS 1.3 をサポートする必要がある。TLS 1.1 やこれよりも古いプロトコルの使用は、安全上の観点から、原則として認められない。

ANP は、RADIUS のトランスポートとして、TLS 1.2 または TLS 1.3 に対応した RadSec を実装しなければならない。Cityroam の認証連携ネットワークにおいて、TLS 1.2 は近く廃止される可能性があるため、TLS 1.3 に対応することが強く推奨される。UDP を用いる従来の RADIUS プロトコルによる接続は、段階的に廃止の予定である。

6.3 認証要求の転送

ANP は、他組織の IdP に向けて送出されるすべての EAP メッセージを、改変せずに転送しなければならない。基地局やコントローラ、プロキシなどで、EAP メッセージを終端してはならない。

User-Name 属性を改変してはならない。

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。

6.4 アクセスポイントのセキュリティ

無線 LAN サービスを提供するアクセスポイントは、WPA2 Enterprise に対応した機器を使用しなければならない。暗号方式には CCMP (AES) を用いる必要があり、TKIP を使用してはならない (有効化も禁止)。

2.4GHz 帯と 5GHz 帯では、PMF (IEEE 802.11w) の transition mode (optional mode)を有効にした WPA2 Enterprise を用いる必要がある。PMF を無効化する、あるいは、PMF を必須にした WPA3 Enterprise モードで動かしてはならない。

6GHz 帯では、WPA3 Enterprise を用いる必要がある。

有線部分での盗聴や中間者攻撃から利用者の通信内容を保護する必要がある。基地局システムで VPN を用いるか、オーナーや利用者が容易に割り込めないように配線を物理的に保護するといった対策が必要である。モバイル網のように既に保護が有効な回線では、追加の保護は必要ではない。

6.5 アクセスポイントの機能要件

Passpoint (Hotspot 2.0) Release 1 以上に対応したアクセスポイントを用いなければならない。

Passpoint Release 3 には有用な機能が幾つかあり、協会が段階的に有効化を推奨していくため、Release 3 以上に対応したアクセスポイントの導入が推奨される。具体的には、Venue URL と Roaming Consortium Selection element の機能を有することが望ましい。

SSID ごとに異なる RADIUS サーバを指定できることが望ましい。

RADIUS accounting の機能が必要である。

Calling-Station-Id と Called-Station-Id の送出機能が必要である。Called-Station-Id は、MAC アドレスの後ろにコロン (:) と SSID が付加された形式で送出できる必要がある。(例： de-ad-be-ef-01-23:cityroam)

迅速な設定変更とインシデント対応のため、リモート管理機能のあるアクセスポイントの採用が強く推奨される。VPN を用いてリモート管理を実現してもよい。

6.6 DNS および DHCP の提供

ANP が利用者に提供する無線 LAN サービスのネットワークにおいて、DNS による名前解決、および、DHCP による IP アドレスの自動設定の機能を提供しなければならない。

6.7 ネットワークで提供する IP アドレス

利用者端末に配布する 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。NAPT を用いてもよい。

NAPT を用いる場合、一人で複数端末を利用することが一般化した最近の状況に鑑み、十分なセッション数を捌けるようなシステム構成にする必要がある。

6.8 SSID と Passpoint の設定

ANP は、原則として、以下の二つの SSID を送出しなければならない。これらに加えて、ANP 独自の SSID を提供してもよい。

(1) cityroam (Cityroam の基本の SSID で、すべて小文字)

(2) eduroam (eduroam の基本の SSID で、すべて小文字)

標準的な構成では、SSID “cityroam”のみに、Passpoint の設定を付与する。SSID “eduroam”で Passpoint を有効にしてはならない (接続できない端末が多数あるため)。

SSID “eduroam” と Passpoint のいずれか一方のみを送出する設定は禁止とする。

ANP 独自の SSID に Cityroam 用の Passpoint を設定する場合、その SSID を通じた認証要求を Cityroam の認証連携ネットワークに転送する必要がある。この場合、SSID “cityroam”には Passpoint の設定を付与しなくてもよいが、Passpoint 非対応の端末も WPA2/WPA3 Enterprise でローミング利用できるようにするため、原則として“cityroam”の併設が必要である。

Passpoint の設定内容については、別途定める。

以下のすべての条件が満たされる場合に限り、ANP から協会への申請および審査の上で、”cityroam”の送出を割愛することが許される。ただし、調達等の都合により、サービスエリアや SSID を事前に開示できない場合は、審査時に具体的な名称を求めない。

1) 自治体 Wi-Fi などの無線 LAN サービスにおいて、当該サービス独自の SSID を定め、

それを共通の SSID として広域で使用し、その SSID に Passpoint の設定を付与する。(注：Passpoint に対応できない端末でもある程度広い範囲でローミングの効果が得られるようにするため、施設ごとや店舗ごとに別の SSID を使用することは「広域」とみなされない)

2) Passpoint の Domain Name に “cityroam.jp” を設定する。

3) Passpoint に対応していない端末では、ローミング利用が 1)の独自 SSID の範囲に限られることになるため、自治体などオーナーがこの制約について事前に了承している。

4) Passpoint に対応した端末であっても、OS のバグにより Passpoint が使用できない状況が発生することがあり、”cityroam”を吹いていない場合は代替の接続手段が提供できなくなる。自治体などオーナーがこの制約について事前に了承している。

5) サービス提供の開始に際して、事前に、Passpoint の設定を付与した独自 SSID を協会に通知する。

6.9 設定変更・修正のすみやかな対応

Cityroam やローミング先事業者の仕様に変更があり、協会が設定変更依頼を発行した場合、ANP はすみやかにこれに対応する必要がある。基準としては、三週間以内を完了の目標とすること。ただし、セキュリティ上の問題がある場合は、一週間以内のできるだけ早い時期を目標とする。緊急性が必要なセキュリティ上の問題が発覚した場合、協会が ANP の対応を待たずに認証連携を遮断することがある。

ANP の設定不良などがみつかった場合、協会は修正依頼を発行する。ANP はこれにすみやかに対応する必要がある。基準としては、二週間以内を完了の目標とすること。

ANP の負担を減らすため、協会は、設定変更の頻度を極力減らすように努める。

6.10 アクセス制限の原則禁止、セキュリティ対策、青少年保護

セキュリティ対策上制限が慣例とされているもの (OP25B など) 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。特定のプロトコル等について制限を行う場合は、制限内容について協会に届け出ること。また、制限の内容について利用者に広報すること。

統一的な利便性を確保するために、利用可能なサービス(プロトコル)にはできるだけ制限をかけないことが望ましい。

特に、http/https、ssh、各種 VPN プロトコルは、公衆無線 LAN という利用形態において有用なため、アクセス制限は原則として認められない。この他、eduroam JP や GÉANT などから提供されている最低限提供すべきサービス (開放すべきポート) の内容を最大限尊重すること。

・[eduroam JP] eduroam として提供すべきサービスについて
https://www.eduroam.jp/for_admin/85

法令、および、総務省のガイドラインなどを参考にして、セキュリティ対策と青少年保護に留意すること。しかしながら、サイトブロックを実施するには利用者の同意が必要となることに注意が必要である。一般に、公衆無線 LAN ではネットワーク側で確実にフィルタリングを行うことが難しいことから、必要に応じて端末側でフィルタリングを行うことを利用者に推奨していく。

・[総務省] 無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

・[e-Gov 法令検索] 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://elaws.e-gov.go.jp/document?lawid=420AC1000000079

6.11 品質確保と帯域確保の努力義務

モバイル網に対する無線 LAN の高速性を生かし、安定に利用できるように、通信品質と帯域の確保に努めること。

上流回線にモバイル網を使用することは、移動体や屋外フィールドなどでやむを得ない場合に限り、電波状況のよい場所において基地局あたり 10Mbps 以上の帯域が得られるように努めること。

6.12 ログの保存

ANP は、無線 LAN の不正利用などのインシデント発生に備えて、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 か月とする。ただし、国内法令や、利用者の居住地の法律と齟齬がある場合は、適切な法に従うものとする。

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、協会や他の加入組織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) 認証要求の User-Name 属性 (Outer-Identity)

(3) 接続した端末の MAC アドレス (Calling-Station-Id 属性)

(4) 端末が接続したアクセスポイントの MAC アドレスと SSID (Called-Station-Id 属性)

(5) 認証応答のタイプ (Accept, Reject)

(6) IdP から Chargeable-User-Identity (CUI)属性が返された場合はその値

(7) 端末の MAC アドレス、および、割り当てられた IP アドレス (DHCP ログなど)

(8) NAPT を使用している場合、アドレス変換およびポート変換のログ

6.13 基地局マップデータの提供義務

ANP は、実施要領の規定に従い、基地局の設置場所の情報を基地局マップデータとしてまとめ、協会に提出する必要がある。

提出に用いるデータ形式、および、提出先については、協会より別途提示される。

6.14 障害情報の公知

ANP は、自組織が Cityroam 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組織外からも確認できるよう、ウェブサイトなどを通じて広報するように努めること。

以上