Wi-Fi プロファイルを用いた eduroam/OpenRoaming のパスワードレス設定

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

Passwordless Configuration of eduroam/OpenRoaming Using Wi-Fi Profile

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

教育・研究機関向けの無線 LAN ローミング基盤である eduroam は，これまで多くの機関で，ID・パスワードを使う形で運用されてきた．利用者が ID・パスワードを記憶または記録しておく必要性があり，手作業での入力の負担が大きかった．また，打ち間違いによる接続不良も，利便性を損ねていた．一方，市民一般向けのローミング基盤である OpenRoaming の開発と並行して，OS ベンダ各社は近年，Wi-Fi プロファイルを用いたウェブベースのプロビジョニング (準備，設定投入) の仕組みを提供するようになった．プロファイルは，無線 LAN の設定に必要なパラメータや証明書などを埋め込んだファイルである．これにより，WPA2 Enterprise の無線 LAN であっても，利用者が複雑な手順を踏まずに設定できるようになった．本研究では，主要な OS の対応状況を調査した．また，機関の情報システムに組み込んで Wi-Fi プロファイルを発行できるようにするためのツールキットを開発し，GitHub で公開した．これを用いると，組織のアカウントなどを用いてログイン済みのウェブサイトから，プロファイルを電子的手段で端末に流し込み，ID・パスワードレスな eduroam/OpenRoaming 設定を実現できる．利用者による入力ミス・設定ミスの可能性を極力排除することで，サービスの利便性と安定性の向上が期待される．

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 [1] は，これまで多くの機関で，ID・パスワードを使う形で運用されてきた．利用者が ID・パスワードを記憶または記録しておく必要性があり，手作業での入力の負担が大きかった．また，打ち間違いによる接続不良も，利便性を損ねていた．一方，市民一般向けのローミング基盤である OpenRoaming [2] の開発と並行して，OS (Operating System) ベンダ各社は近年，Wi-Fi プロファイルを用いたウェブベースのプロビジョニング (準備，設定投入) の仕組みを提供するようになった．これにより，WPA2 Enterprise の無線 LAN であっても，利用者が複雑な手順を踏まずに設定できるようになった．

本報告では，主要な OS のウェブベース Wi-Fi プロビジョニングの対応状況を解説する．また，機関の情報システムに組み込んで Wi-Fi プロファイルを発行できるようにするためのツールキットを開発したので，紹介する．これを用いると，組織のアカウントなどを用いてログイン済みのウェブサイトから，プロファイルを電子的手段で端末に流し込み，ID・パスワードレスな eduroam/OpenRoaming 設定を実現できる．利用者による入力ミス・設定ミスの可能性を極力排除することで，サービスの利便性と安定性の向上が期待される．

本稿では，初めに，eduroam の接続設定の現状と課題を説明する．続いて，最近の各種 OS におけるウェブベース Wi-Fi プロビジョニングの動向と技術を説明する．最後に，ID・パスワードレス設定を実現するた

めのツールキットを紹介する．

2　eduroam CAT と geteduroam による eduroam 設定の容易化

2.1　eduroam の手動設定の課題

eduroam は WPA2 Enterprise (IEEE 802.1X) による安全な利用者認証と接続方法に基づくシステムである [1]．eduroam では幾つかの認証方式が利用できるが，ID とパスワードを使う EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) と PEAP (Protected Extensible Authentication Protocol) が広く利用されている．この他，電子証明書を用いる EAP-TLS (-Transport Layer Security) を採用している機関もある．

EAP-TLS の場合は，電子証明書を端末にロードする必要があるため，機関内のウェブサイトなどを通じて端末の設定を行う必要がある．一方，ID・パスワード方式は，他にネットワーク接続手段のない場所でも，手動設定のみで無線 LAN に接続できるという利点がある．例えば，自分の所属機関が eduroam に参加していないが，参加した国際会議でビジター用の eduroam アカウントが配布されているようなケースが，これに該当する．しかしながら，eduroam を十分に安全に利用できるようにするためには，本来はサーバ認証の設定も必要で，手作業での接続設定は煩雑である．

EAP-TTLS と PEAP では，利用者認証に先立って，これから接続しようとする基地局とネットワークが偽物ではないことを確認するための，サーバ認証が行われる．PEAP ではサーバ認証の省略もできるが，利用者認証に用いられる MS-CHAPv2 のセキュリティが十分ではないため，巧妙に細工された偽基地局に誘導されるとパスワードが解析・窃取される恐れがある．このため，サーバ認証の有効化が強く推奨されている．

さらに，プライバシー保護のために，実際に利用者認証に使われる Inner Identity とは別に，Outer Identity に匿名 ID を設定することが望ましい．機関のポリシーに依って，匿名 ID を設定しない運用も可能である．

以上をまとめると，認証方式の選択の後，ID・パスワードに加えて，サーバ認証のための情報 (サーバ証明書の検証に使う CA (Certificate Authority) 証明書の名前と，サーバ証明書の SAN (Subject Alternative Name) など)，および，Outer Identity の入力が必要であり，これを利用者が手作業で行うことは難しい．

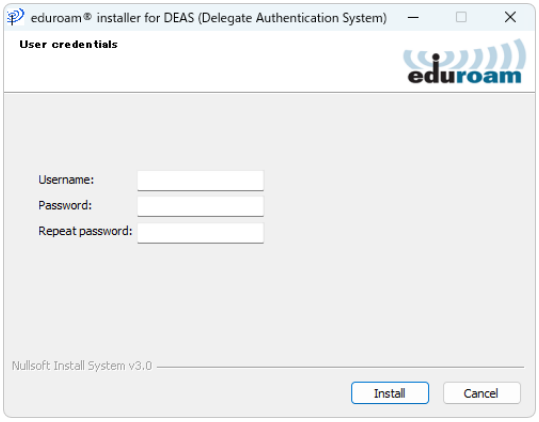

図 1　eduroam installer (CAT) による接続設定．

ID とパスワードの入力においても，画面に表示されたり紙に書かれたものを端末に入力する際に，1 (イチ) と l (エル) のように似た文字を間違えたり，末尾に余計なスペースを入れてしまう，ハイフン (–) とよく似た他の記号を入れてしまうなど，入力ミスによる認証失敗に多くの利用者と管理者が悩まされている．類似した文字を排除するなど，システム設計の工夫もあるが，手動設定の負担と誤入力の問題は残る．

2.2　eduroam CAT

eduroam の接続設定を容易にするために，eduroam CAT (Configuration Assistant Tool) [3] が運用されている．eduroam の IdP (Identity Provider) となる機関の管理者が，ID・パスワードを除く設定情報を仕込んだプロファイルを，予め eduroam CAT のサーバに登録しておく．利用者は，eduroam CAT からこのプロファイルをダウンロードして，eduroam installer に読み込ませる．これにより，図 1 のように ID・パスワードを入力するだけで，安全な eduroam 接続設定が可能である．

eduroam CAT は幅広い OS に対応している．Apple の iOS, iPadOS, macOS では，MDM (Mobile Device Management) 向けの共通のプロファイル形式 (.mobileconfig) が利用でき，端末に特別なアプリを導入しなくても無線 LAN 設定が可能である．一方，Android と Windows については，eduroam CAT 独自の .eap-config 形式のプロファイルが発行され，利用者がこれをダウンロードして eduroam installer に読み込ませることで，端末の無線 LAN 設定が行われる．

執筆時点で，eduroam CAT のサーバ周りのシステムは運用継続されているが，アプリのメンテナンスが行われておらず，後述する geteduroam [4] への移行が進められている．

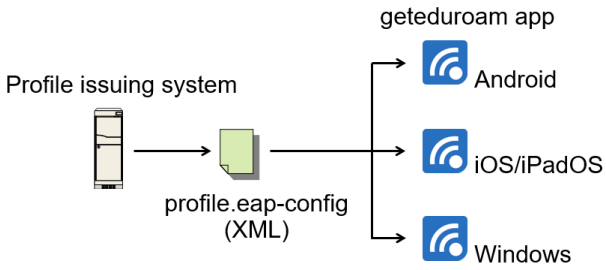

図 2　.eap-config と geteduroam app による無線 LAN 設定.

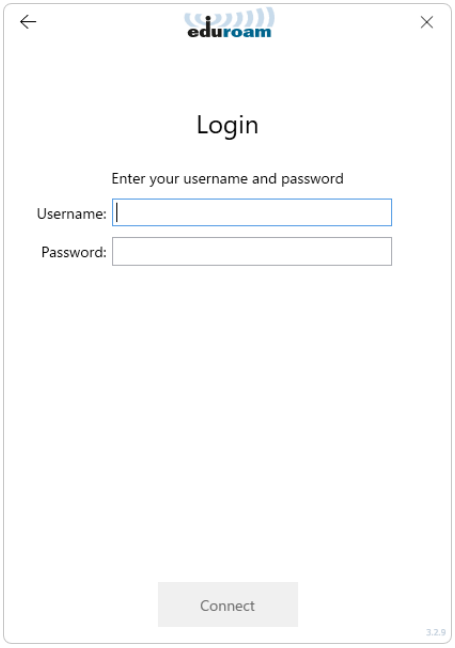

図 3　geteduroam による接続設定.

2.3　geteduroam

eduroam の接続設定をさらに容易にするために，geteduroam という名前のアプリが開発されている [4]．geteduroam では，eduroam CAT と同じ .eap-config 形式のプロファイルが利用できる．

執筆時点で，geteduroam の基本機能は eduroam CAT のアプリと同様であるが，インタフェースの洗練が進められている．対応 OS は，Android，Windows，iOS/iPadOS である (図 2)．iOS/iPadOS と macOS については，eduroam CAT のウェブサイトで発行されるプロファイルのみを用いて設定が可能なため，実質的には Android と Windows で特に有用なアプリとなっている．

geteduroam は基本的に eduroam CAT のシステムをバックエンドに利用しており，ID とパスワードの入力はあいかわらず必要である (図 3)．また，eduroam の接続設定の際に，eduroam CAT のウェブサイトにアクセスするためのネットワーク接続が別途必要である．Apple 以外の端末では，予めアプリを導入しておく必要もある．

3　ウェブベース Wi-Fi プロビジョニングの最新動向

3.1　プロファイルを用いた無線 LAN 設定

教育・研究機関向けの eduroam に加えて，市民一般向けのセキュアな無線 LAN ローミング基盤の実現が望まれるようになり，国内では著者らによる Cityroam [5] が 2018 年に，世界では Wireless Broadband Alliance (WBA) による OpenRoaming [2] が 2020 年に運用開始された．OpenRoaming では Passpoint [6] と呼ばれる仕組みが導入されているが，これは eduroam における WPA2 Enterprise と同様の設定に加えて，さらに細かいパラメータを端末に設定する必要がある．このため，手作業による設定は困難であり，設定に必要な情報をまとめたプロファイルを端末に電子的に流し込む，プロビジョニングの仕組みが開発されるようになった．ウェブベースの Wi-Fi プロビジョニングの機能を使うことで，利用者はオンラインサインアップ (OSU, Online Sign-Up) の機能を用いて，煩雑な手順を踏まずにセキュアな無線 LAN に接続できるようになった．Passpoint に対応したプロファイルは，特に，Passpoint プロファイルと呼ばれている．

一部のプロファイルには有効期限を設定する項目もあり，期限切れのアカウントによる大量の認証要求の発生を抑制することも可能である．eduroam では大勢の卒業生の端末に設定が残っていることがローミング基盤の負担になっており，有効期限が設定できることは負荷軽減に貢献すると考えられる．

次節より，代表的な OS のウェブベース Wi-Fi プロビジョニングの対応状況と仕組みを説明する．

3.2　Android (PPS MO)

Android では，Passpoint [6] で定義された PPS MO (Per-Provider Subscription Management Object) と呼ばれる形式のプロファイルが利用される．このプロファイルは XML (eXtensible Markup Language) 形式で記述されている．利用者がウェブサイトで Passpoint 設定などのボタンをタップすると，Passpoint プロファイルが端末にダウンロードされて，自動的に無線 LAN 設定のメニューに遷移する (図 4)．利用者が入力しなければならないようなパラメータは一切なく，数タップの操作のみで設定が完了する．

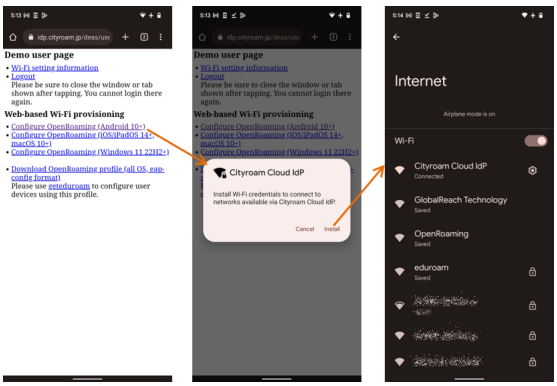

図 4　PPS MO による Android の Passpoint 設定.

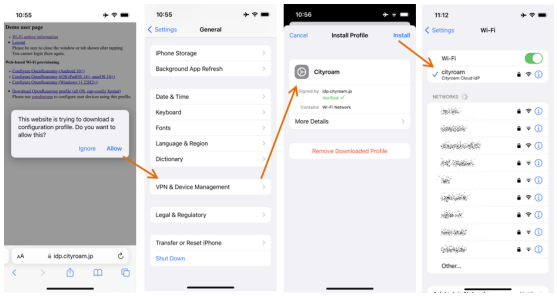

図 5　.mobileconfig による iOS の Wi-Fi 設定.

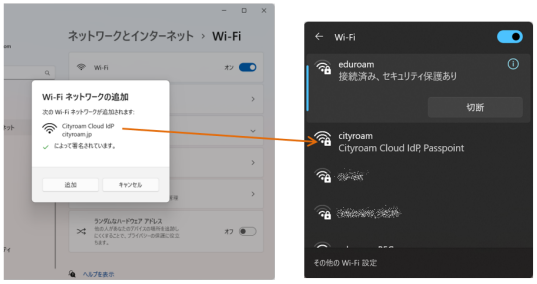

図 6　ms-settings: URI スキームによる Windows 11 の Wi-Fi 設定.

Android のリファレンス実装では，EAP-TTLS, EAP-TLS, EAP-SIM, EAP-AKA, EAP-AKA' の形式がサポートされている．PPS MO 形式は，Passpoint の機能を伴わない従来の WPA2 Enterprise のみの設定には対応していない．すなわち，eduroam の設定には利用できないという問題がある．

Android の Passpoint 周りの実装は，ほぼ実用的と言えるレベルに達したのが Android 10 であり，調査した限りにおいて，安定な動作には 11 以降が必要である．プロファイルには有効期限を示す ExpirationDate の定義も含まれているが，Android 12 以前では機能しないようである．

3.3　iOS/iPadOS/macOS (.mobileconfig)

Apple の iOS, iPadOS, macOS の各 OS では，MDM 向けの.mobileconfig 形式のプロファイルが共通のプロファイル形式 (.mobileconfig) が利用される．この形式では，無線 LAN の一通りの設定が網羅されており，WPA2 Enterprise だけでも，Passpoint を組み合わせても，いずれでも利用できる．

利用者がウェブサイトで Passpoint 設定などのボタンをタップすると，プロファイルが端末にダウンロードされる．続いて，プロファイルをインストールする操作が必要である (図 5)．利用者が入力しなければならないようなパラメータは一切なく，数タップの操作のみで設定が完了する．

プロファイルには有効期限の埋め込みも可能であり，期限切れのプロファイルを削除するように，利用者に操作を促すことができる．

.mobileconfig 形式のプロファイルは，XML 形式で記述されており，S/MIME (Secure / Multipurpose Internet Mail Extensions) による署名に対応している．署名付き・署名なしのいずれでも利用できるが，署名なしの場合はプロファイルのインストールの際に赤字で警告が表示される．署名に用いる証明書は，OS が標準対応しているパブリック CA から発行されたものが必要である．制約条件は厳しくないので，利用者に無用な心配をさせないためにも，署名付きのプロファイルを発行することが望ましい．

3.4　Windows (ms-settings: URI スキーム)

Windows 10 および Windows 11 では，ms-settings: URI スキームを用いて，プロファイルによる無線 LAN の設定が可能になっている．XML で記述されたプロファイルをウェブサイトからダウンロードする際に，URL の前に ms-settings:wifi-provisioning?uri= を付けることで，Windows の「ネットワークとインターネット > Wi-Fi」メニューが自動的に立ち上がり，プロファイルを取り込む仕組みになっている．図 6 のように，利用者が Wi-Fi ネットワークの追加を承認するだけで，接続設定が完了する．

このプロファイルは，WPA2 Enterprise のみでも，Passpoint との併用でも利用できる．EAP-TTLS や EAP-AKA などに対応しているが，実機で検証したところ，PEAP は利用できなかった．EAP-TLS にも対応していない．Passpoint の場合でも SSID の設定が省略できないなど，まだ仕様が十分に固まっていないように見える．

プロファイルには XML 署名が必須で，省略はでき

ない．また，この署名には EV (Extended Validation) 対応のコード署名用証明書が必要であり，非 EV の署名では赤字で「署名が無効です。」というエラーが表示されて，ネットワークが追加できない．Windows 11 22H2 アップデートでは，この制約が緩和されて，非 EV の署名も受け付けられるようになった．

現在は Windows 10 の端末も数多く使われているため，当面の間，EV 証明書を用いた運用が望まれる．

Windows 用のプロファイルには，有効期限を設定する項目が見当たらなかった．

3.5 .eap-config の利用

OS の仕組みではないが，代用品として優れた性質を持っているので，2.2 で説明した .eap-config についてここで補足説明しておく．

.eap-config は eduroam CAT や geteduroam で用いられているプロファイル形式であり，XML で記述される．この形式は，WPA2 Enterprise の EAP-TTLS, EAP-TLS, PEAP に対応しており，Passpoint にも限定的ながら対応している．標準的な eduroam では世界で統一された SSID “eduroam” が用いられるが，Passpoint による接続も規定されており，後者では RCOI (Roaming Consortium Organization Identifier) によって接続先の基地局が選ばれる．OpenRoaming でも RCOI が使われていることから，この .eap-config 形式は OpenRoaming にも応用できる．しかしながら，SIM 認証に対応していないという制約がある．

2 で述べたように，現在の eduroam CAT や geteduroam の運用では，ID・パスワードを手作業で入力ないしコピー・ペーストすることが多い．.eap-config 形式には UserName, Password の項目も定義されており，予めこれらを埋め込んでおけば，手作業が不要な，ID・パスワードレスな接続設定が実現できる．これを実現するには，無線 LAN のアカウントを保有している各機関，すなわち IdP が，自前で UserName, Password を埋め込んだプロファイルを生成・発行する必要がある．

.eap-config 形式には ValidUntil の項目があり，有効期限の埋め込みも可能である．

4 Provisioning Tools を用いた ID・パスワードレスな無線 LAN 設定

無線 LAN 設定に用いるプロファイルの形式が OS ごとに異なる上に，形式や署名方法に関する公開情報が十分ではなく，正しく動作する条件や環境が見出しにくいという問題があった．無線 LAN 業界でも，プロファイルの生成に各社が苦労している状況であった．そこで，十分に洗練されていなくても，まずは正常に動作する基本的なものが必要と考え，プロファイルの生成を用意にするツールキットを開発して，GitHub でオープンソースソフトウェアとして公開した．初めに，OpenRoaming 用のシステムを開発する事業者のために，Passpoint/OpenRoaming 向けのツールキットを Passpint Provisioning Tools の名称で開発，公開した [7]．続いて，同じコードをベースにしながら，学校・大学でも利用しやすいように，eduroam 専用にパッケージ化した eduroam Provisioning Tools を開発，公開した [8]．

Provisioning Tools は，IdP となる機関で自前のプロファイル発行システムを開発しやすいように，CGI (Common Gateway Interface) Perl スクリプトとして開発した．Perl スクリプトなので，CGI 以外の組み込みの用途でも，適応のための書き換えは難しくない．生成されるプロファイルの形式は OS ごとに異なるが，埋め込むパラメータは共通のものが多いため，共通の設定ファイルにまとめた．このツールキットを利用するには，ウェブサーバ上にコードを置き，設定ファイルを自機関向けにカスタマイズし，無線 LAN のアカウントをデータベースから読み出すための自前のコードを追加する．

プロファイルを生成するスクリプトは，ウェブサイト上の利用者用ポータルなど，何らかの利用者認証によってアクセス制御されている場所に設置する．これにより，ウェブサイトにログイン中の利用者を判別して，その利用者の無線 LAN アカウントをプロファイルに埋め込むようにする．ウェブサイトのログインには，ウェブアクセス用の認証方式を利用することを想定しており，SSO (Single Sign On) や，最近普及してきた FIDO2 [9] などのパスワードレス認証も利用できるだろう．EAP-TTLS では，もちろん内部的に ID・パスワードが利用されるが，これらは利用者の目に触れることはなく，無線 LAN 認証用のトークンとみなすことができる．つまり，この意味で，「無線 LAN の ID・パスワードレス設定」が実現できる．

Passpoint Provisioning Tools は，ほぼそのままの形でフリー Wi-Fi 向けの OpenRoaming (settlement-free model) に利用できるように設計した．対応 OS は，Android 10 以上 (11 以上を推奨)，iOS/iPadOS 14 以上, macOS 10 以上，Windows 10 以上である．

eduroam Provisioning Tools は，ほぼそのままの形

で eduroam に利用できるように設計した．対応 OS は，iOS/iPadOS 14 以上, macOS 10 以上，Windows 10 以上であり，geteduroam で使える.eap-config 形式のプロファイルも生成できるようにした．先に説明したように，PPS MO 形式が Passpoint 専用のため，Android では OS 単体でウェブベースの eduroam 設定ができない．geteduroam などの外部プログラムに頼る必要がある．

図 4, 5, 6 はいずれも，Provisioning Tools で生成したプロファイルを用いて，実際の端末画面をキャプチャしたものである．

ウェブベースの無線 LAN 設定には，他にネットワーク利用手段のない場所では使えないという不利な点がある．しかしながら，現在はネットワークの常時利用が一般化しており，短時間ならば他の接続手段が利用できることもある．最近の学生ならば，キャンパス無線 LAN に接続する前に，自宅のネット回線や携帯電話のテザリングを利用できるのが普通だろう．無線 LAN ローミングが社会に普及するにつれて，オンサイトでの接続設定が必要な機会は減ってくるものと考えられる．

5 むすび

本研究では，最近の主要な OS に組み込まれている，ウェブベースの無線 LAN 設定機能について，技術と対応状況を調査した．また，機関の情報システムに組み込んで Wi-Fi プロファイルを発行できるようにするためのツールキットを開発した．組織のアカウントなどを用いてログイン済みの情報システムから，プロファイルを電子的手段で端末に流し込み，ID・パスワードレスな eduroam/OpenRoaming 設定を実現できる．利用者による入力ミス・設定ミスの可能性を極力排除することで，サービスの利便性と安定性の向上が期待される．

現時点では，OS や利用者端末の仕様や実装にまだ流動的なところが多く，現場で欲しい機能が十分に実装されているわけではない．今後も引き続き，実際のニーズに即した技術仕様の検討を進めて，OS ベンダや無線 LAN 業界に改良を働きかけていく予定である．

本研究の一部は，令和 4 年度国立情報学研究所公募型共同研究の助成を受けた．Passpoint および OpenRoaming に関する調査と開発は，国立研究開発法人情報通信研究機構 (NICT) の委託研究 Beyond 5G 国際協働研究型プログラムにより実施した．

参考文献

[1] eduroam JP: https://www.eduroam.jp/ (2022 年 9 月 30 日参照)

[2] WBA OpenRoaming: https://wballiance.com/openroaming/ (2022 年 9 月 30 日参照)

[3] eduroam CAT: https://cat.eduroam.org/ (2022 年 9 月 30 日参照)

[4] geteduroam: https://www.geteduroam.app/ (2022 年 9 月 30 日参照)

[5] Cityroam: https://cityroam.jp/ (2022 年 9 月 30 日参照)

[6] Wi-Fi Alliance, “Passpoint – Wi-Fi ホットスポットネットワークへのシームレスでセキュアな接続を実現.” https://www.wi-fi.org/ja/discover-wi-fi/passpoint/ (2022 年 9 月 30 日参照)

[7] Passpoint Provisioning Tools: https://github.com/hgot07/PasspointProvisioningTools/ (2022 年 9 月 30 日参照)

[8] eduroam Provisioning Tools: https://github.com/hgot07/eduroamProvisioningTools/ (2022 年 9 月 30 日参照)

[9] FIDO Alliance: https://fidoalliance.org/ (2022 年 9 月 30 日参照)