様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月　 ９ 日現在

機関番号：１１３０１
研究種目：基盤研究(B)（一般）
研究期間：2019～2021
課題番号：１９Ｈ０４０９０

研究課題名（和文）耐障害性・耐災害性と回復力を有する大規模無線LAN認証連携基盤に関する研究

研究課題名（英文）Study on Disruption- and Disaster-tolerant, Resilient Identity Federation Infrastructure for Large-scale Wireless LAN

研究代表者
後藤　英昭（Goto, Hideaki）

東北大学・サイバーサイエンスセンター・准教授

研究者番号：４０２７１８７９

交付決定額（研究期間全体）：（直接経費）　　4,900,000円

研究成果の概要（和文）：現在の公衆無線LANにおける利用者認証の処理は、広域ネットワークの常時接続に依存している。このため、ネットワーク障害の際に、局所的なサービスさえも使用不能に陥ることが多い。本研究では、多数の通信事業者が無線LANの相互利用を提供するローミング環境において、ネットワークの一時的・部分的な途絶が生じても安定して認証処理が行えるシステムを開発した。大規模なローミング環境でも利用できるような、電子証明書を用いたローカル認証方式、及び、その運用方式を開発した。本システムは、被災地などで上流のネットワークが失われても動作し、様々な局所サービスを利用可能にできる。航空機内の無線LANサービスにも有用である。

研究成果の学術的意義や社会的意義
大規模災害における被災地や、航空機内の無線LANなど、ネットワークの分断がやむを得ない状況においても、安定かつ安全な利用者認証を実現する技術を開発した。これにより、公衆無線LANに限定されず、様々な情報システムの耐災害性・耐障害性の向上に役立つ学術的な枠組みを与えた。安全性と利便性に優れた公衆無線LAN及び大学・学校等キャンパス無線LANの普及を通じて、ICT時代の社会の情報インフラの構築と教育・研究に貢献する。

研究成果の概要（英文）：The user authentication process in the current public wireless LAN (WLAN) is dependent on always-on connection to the wide-area network. Network disruptions often lead to service interruptions even in local network use. We looked into a roaming environment in which many telecom operators provide mutual use of WLANs and have developed a new system that enables stable user authentication even during temporary/partial network disruptions. We have developed a certificate-based local authentication method that works in a large-scale roaming environment and also its operation method. The system works even when the back-haul network is disrupted in a disaster affected area, and enables various local services. The system is also useful in in-flight WLAN services.

研究分野：情報セキュリティ

キーワード：認証連携　次世代ホットスポット　公衆無線LAN　耐災害ネットワーク　eduroam　利用者認証　機内無線LAN

１．研究開始当初の背景

第 5 世代移動通信システム(5G)の登場により、通信容量の大幅な向上が期待されている。一方、移動体通信の年々急激に増大する通信量に対応するには 5G だけでは足りないと世界の業界では考えられており、“Convergence”のキーワードのもと、無線 LAN との融合が推進されている。これに伴い、公衆無線 LAN も社会の重要インフラの一つに位置付けられるようになってきたが、それに相応しい品質を実現するには、利用者認証と個人ごとの暗号化、ローミング(相互利用)の実現に加えて、大規模なネットワーク障害や災害にも対応できる基盤が必要である。

現在の利用者認証の仕組みは、広域ネットワークの常時接続を前提としており、一時的なネットワーク障害にも弱く、認証失敗によって局所的なネットワーク利用すら不可能になるという欠点がある。例えば、大規模災害により孤立した地区において、局所的な電子サービスの提供すら難しくなる。これを改善しようとすると、

- 一時的に孤立したコミュニティの中でいかに相手を認証し信用できるか
- 全体が俯瞰できる環境といかにして情報の整合を図れるか

という、一般化された学術的な「問い」が生じる。このような問いに答えられるような調査・研究と、実用的な大規模認証連携アーキテクチャおよび関連要素技術の開発が必要である。

研究代表者らは、無線 LAN ローミング環境の耐災害性・耐障害性を向上させることを目的として、電子証明書を利用したローカル認証方式を開発、提案した(文献[1])。しかし、これを応用した世界規模の環境で利用できるような認証連携アーキテクチャやその運用方式の開発は未着手である。また、現在、実用化された大規模な無線 LAN ローミング環境として学術系の eduroam(エデュローム, 90 か国, 国内 233 機関が参加)があるが、商用サービスでは、少数の通信事業者が個別に契約を結びあう小規模なものに留まっている。世界各地の都市の公衆無線 LAN をセキュア化し、認証連携で結ぼうとするプロジェクトが、2016 年より業界団体において始まっている。しかし、まだ大規模認証連携のアーキテクチャも確立されていない、開発の初期段階であり、前述のような耐障害性や高可用性についての検討はほとんど行われていない。

ネットワークアクセスのための認証連携は、従来、業者間の独自方式や、インターネット RFC などを元に実装されてきており、学術的な取り扱いはそれほど多くない。しかし、優れた基本アーキテクチャやシステム、運用方式などの開発には、運用現場のニーズや利用状況などの分析が不可欠である。複数のローミングシステムの連携を考える場合、学術的な扱いを重視しつつ、ローミングシステム全体を俯瞰したアーキテクチャの設計や分析が必要である。

[1] S. Kinoshita, T. Watanabe, Y. Yamasaki, H. Goto, H. Sone, “Fault-Tolerant Wireless LAN Roaming System Using Client Certificates,” COMPSAC2013, pp.822-823, 2013.

２．研究の目的

本研究は、研究代表者による「耐障害性・耐災害性を有する認証連携ネットワークの自動構築に関する研究」(挑戦的萌芽研究, H27-28)を発展させたものである。

前研究では、ネットワーク障害の際にも継続利用できるような認証連携方式を開発したが、障害中に局所的な設定変更・アカウント追加などは行えず、復旧するまでの「短期間のつなぎ」に留まっていた。また、連携できる機関の数が十分ではなかった。これらの制約を取り払おうとすると、以下のような学術的な「問い」が生じる。

- セキュリティとプライバシを維持しつつ、いかに認証の分散協調処理を実現できるか。
- 広域ネットワークの障害中に変更された状態(認証データ等)の最適な同期・調停方法は何か。それらをどのように実現できるか。
- システムの規模と運用コスト(労力, 費用)の関係はどうか。運用コストを下げられる構成はどのようなものか。
- スケーラビリティ確保の要件はどのようなもので、どのような制約がありうるか。

これらを明らかにしつつ、耐障害性・耐災害性と回復力を有する大規模無線 LAN 認証連携に適したアーキテクチャを模索し、要素技術を開発することが、本研究の課題である。

公衆無線 LAN およびキャンパス無線 LAN は、社会の重要なインフラになりつつあることから、日常的なネットワーク混雑・途絶や、自然災害等被災時の避難所においても、高い可用性が必要となる。このような要求に応えられる認証連携システムを構築するためには、認証およびセキュリティ維持の分散協調モデルや、機関間のトラスト(信頼関係)形成・維持、ポリシー調整などのモデルを学術的、理論的に導き、システムの骨格となるアーキテクチャを実用的な形で設計する必要がある。これらの背景と要求を踏まえて、本研究では、「耐障害性・耐災害性と回復力を有する大規模無線 LAN 認証連携基盤」の開発を目的とする。

３．研究の方法

各年度当初の研究予定を記す。初年度は、概ね以下のように研究を進める。

(1) 学術系無線 LAN ローミング基盤の eduroam や、政府系の govroam、市民向け公衆無線 LAN の国内外の展開動向、技術動向、運用状況を調査し、関係者との情報交換を通じて、耐

災害性・耐障害性の観点で現行システムの課題を整理する。特にネットワークの信頼性が低い新興国の事例は、システム設計に重要な知見をもたらすと考えられることから、より詳しく調査を行う。また、欧州 GÉANT 主催の国際会議 TNC をはじめ、APAN ミーティング、COMPSAC などの国際会議において、情報収集、意見交換、成果報告を行う。

(2) 前研究(挑戦的萌芽研究, H27-28)で開発した、耐災害性・耐障害性を有するメッシュネットワーク向けの認証連携システムを研究室に再構築するとともに、長期・大規模ネットワーク障害における限界と課題を、実験と机上検討で明らかにする。

(3) Wireless Broadband Alliance (WBA)が主催する City Wi-Fi Roaming トライアルに参加、世界の次世代ホットスポット(NGH)基盤に接続し、世界の公衆無線 LAN 業界の動向・技術調査、および、通信事業者との情報交換や業界への技術提供を行う。

(4) 電子証明書を利用したローカル認証方式(既開発)を発展させ、平時の認証情報分散方法や分散協調処理、障害下での局所的アカウント管理の実現可能性と信頼性、効率などを机上で分析し、必要となる基本アーキテクチャおよび処理を設計・開発する。

(5) 既存の認証連携システムを元に、新規設計のアーキテクチャに基づいた改良型のプロトタイプを開発する。ノート PC やスマートフォンなどの多種多様な端末を用いて機能・性能評価を行い、問題点と課題を整理する。

第二年度は、概ね以下のように研究を進める。

(1) 前年度に引き続いて、様々なキャンパス無線 LAN・公衆無線 LAN の展開動向、技術動向、運用状況を調査し、耐災害性・耐障害性の観点で実装・機構の課題を整理する。

(2) WBA の Global Roaming Federation/OpenRoaming や、関連仕様・技術の開発に参画し、技術提供を行う。世界の公衆無線 LAN 業界の動向・技術調査、情報交換を行う。

(3) 前年度に引き続いて、既開発のローカル認証方式の発展のための技術開発を行う。

(4) 既存の認証連携システムを元に、新規設計のアーキテクチャに基づいた改良型のメッシュネットワーク向け認証連携システム(プロトタイプ)を開発する。ノート PC やスマートフォンなどの端末を用いて、機能・性能評価を行い、問題点と課題を整理する。

(5) 研究代表者らが開発し、2008 年より国内の eduroam 基盤でサービス提供している集中型認証システムに、ローカル認証の機能を追加し、評価を行う。

(6) 上記の改良型の認証システムを元に、ネットワーク障害時に局所的にアカウント管理の機能を提供する、縮小型認証システムを開発する。設計した認証連携アーキテクチャに基づいて、分散協調機能を開発し、多数の認証システムが連携動作できるようにする。

最終年度は、概ね以下のように研究を進める。

(1) 前年度と同様の調査を継続する。特に、コロナ禍におけるリモートワーク、遠隔授業などの普及や、観光需要の低迷により、無線 LAN の利用形態に大きな変化が起きていることから、新たな課題の抽出と整理を行う。

(2) WBA OpenRoaming の仕様策定・技術開発に、参画を継続する。世界の公衆無線 LAN 業界の動向・技術調査、および、通信事業者との情報交換を行う。

(3) 平時の認証情報分散方法や分散協調処理、障害下での局所的アカウント管理の実現可能性と信頼性、効率などについて、前年度までの分析結果を基に、無線 LAN サービスの新たな応用や利用形態を反映し、整理する。開発中の基本アーキテクチャの微修正を行う。

(4) 航空機内の無線 LAN サービスにおいて、ローミングのための利用者認証のニーズが生じている。本研究の成果がこの課題解決にも適合することから、早期実用化のためのアーキテクチャを並行して開発する。

(5) 新規設計のアーキテクチャに基づいたメッシュネットワーク向け認証連携システム(プロトタイプ)の開発を継続する。前年度までの機能・性能評価結果を元に、改良を行う。国内の eduroam 基盤に仮想機関として接続し、参加機関に試験サービスを提供し、フィードバックを得る。

(6) ネットワーク回復時に柔軟に認証情報の同期・調停処理を行う処理を開発する(継続)。研究室内の実験用ネットワークおよび実際のインターネットの上で評価実験を行う。

第二年度(2020 年度)よりコロナ禍の影響があり、国際会議が縮小されて調査が難しくなったことや、通学および対面作業の制限により大学院生の研究補助を得るのが難しくなったことなどから、応用技術としてのメッシュネットワーク向け認証連携システムの開発を割愛することとなった。一方で、WBA において機内無線 LAN サービスのローミング対応と高度化のニーズが高まったことから、研究成果の早期応用と社会貢献を重視した開発を計画に盛り込んだ。

４．研究成果

(1) 耐災害・耐障害無線メッシュネットワークのためのローカル認証方式

従来のローカル認証方式では被災地などでの基地局の臨時設置に制約が大きかった点に着目し、基地局間での電子証明書の効率的な配布を実現する改良型の耐災害・耐障害無線メッシュネットワークのアーキテクチャを開発した。複数の通信事業者の間で基地局を融通、相互接続

でき、上流ネットワークが途絶時も臨時アカウントを発行できる仕組みを実現した（図 1）。

局所的な認証が行えるようにするため、無線 LAN の認証方式の一つである EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)を用い、電子証明書と秘密鍵は予めすべての無線アクセスポイントに配布しておく。複数の通信事業者が提供するアクセスポイントを相互接続・相互利用できるように、利用者認証と同様に、アクセスポイントの接続にも EAP-TLS を用いる。ネットワークの途絶時にも、新規のアクセスポイントを認証、接続許可することができ、ローカルネットワークが容易に拡張できる。

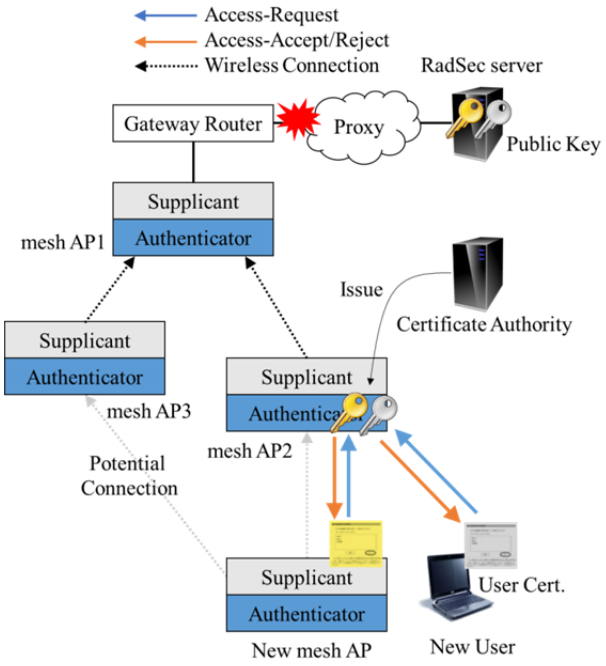

図 1. ローカル認証方式における利用者認証・アクセスポイント認証

(2) 大規模無線 LAN ローミング基盤の開発

Wireless Broadband Alliance (WBA)における NGH の仕様策定・実証実験に参画した。耐災害性・耐障害性の観点での貢献はまだないが、大規模なローミングフェデレーションを複数接続するインターフェデレーションのためのアーキテクチャの提案や、課題抽出・整理を行った。

WBA では、市民一般向けのセキュアなローミング基盤を構築する構想があり、Passpoint 技術を用いた NGH の実現が模索されていた。これとは独立に、研究代表者らは、セキュア公衆無線 LAN ローミングを実現するために、国内の基盤として Cityroam を立ち上げ(2018 年 6 月)、運用を開始していた。2019 年度に Cisco OpenRoaming が公表され、WBA における開発はこれに合流することになった。一方で、eduroam などのその他のローミングフェデレーションとの接続性が課題となっていたことから、本研究ではこの設計に参画して、技術供与を行った。第二年度(2020 年度)に OpenRoaming が WBA に移管され、正式に発足するのに合わせて、Cityroam も初期メンバーとして OpenRoaming に参加し、技術開発に参画した。特に、欧州 GÉANT における Global eduroam Governance Committee (GeGC) 委員としての立場を生かして、eduroam の代表的として開発に携わった。これらの活動により、eduroam のアカウントを用いて世界各地の OpenRoaming 基地局に安全に端末を接続できる仕組みを実現した。

eduroam では、アカウントに含まれるレルム名 (@example.jp のように DNS のドメイン名に類似) を見ただけでは、eduroam に属するアカウントか他のフェデレーションのものなのかを判別できないという問題がある。このため、端末からアクセスポイントに送られた認証要求を、どのフェデレーションに転送するかという、ルーティング(経路選択)の問題があった。この問題を解決するために、インターフェデレーション接続のための技術を開発した。

レルムの自動学習を用いた認証要求転送先の自動選択手法を、図 2 に示す。端末がアクセスポイントに接続され、未知のレルムを含む認証要求が送られてきた場合、プロキシは端末の再認証機能を利用して転送先を順次切り替え、正しい転送先となるローミングフェデレーション(またはコンソーシアム)を見付けて、当該レルムをデータベースに記録する。次回以降に同じレルムを持つ認証要求が届いた場合は、即座に正しい宛先に認証要求が転送されるようになる。

この手法には、本研究のテーマである耐災害性・耐障害性の観点がまだ含まれていない。両者を組み合わせられるような技術の開発は、将来の課題である。

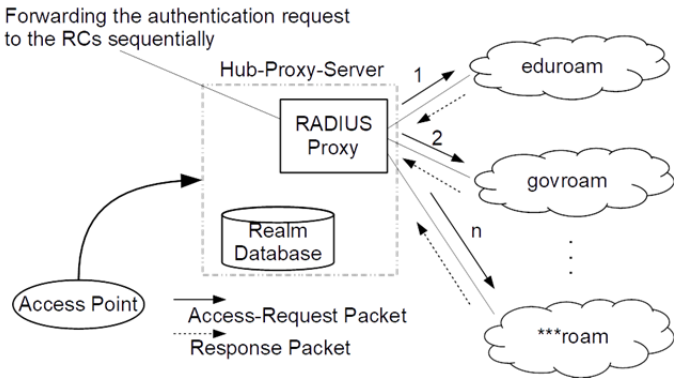

図 2. レルムの自動学習による認証要求転送先の選択

(3) 機内無線 LAN サービス向けの認証連携技術の開発

耐災害性・耐障害性の観点で現行システムの実装・機構の課題を整理し、また、大規模ローミング基盤の応用を調査していく過程で、航空機内の無線 LAN サービスで、被災地のネットワーク途絶環境と共通する課題が多いことを導き出した。これを受けて、早期実用化が急務の機内無線 LAN ローミングを題材として、研究開発を進めた。

機内無線 LAN サービスは、従来はインターネット接続が主体であったが、近年では航空機に搭載されるメディアサーバなどを使用して、音声・映像メディアなどの機内エンターテイメントの提供や、フライト情報、到着地情報、観光ガイドなどの提供、機内ショッピングなどの、重要なサービスとなっている。しかしながら、現行の機内無線 LAN は、暗号化のないオープンネットワークが利用されており、盗聴や、偽基地局を用いた中間者攻撃が可能となる問題を抱えている。また、利用者が飛行機に搭乗するごとに無線 LAN の接続設定を行う必要があり、利便性が低いという問題もある。このような課題に取り組むため、WBA では OpenRoaming を機内無線 LAN サービスに応用する計画が立ち上がった。

現在の機内無線 LAN サービスでは、インターネットへの接続（バックホール接続）が衛星や地上基地局との通信に依存している。通常、乗客の搭乗から離陸を経て、一定高度(通常 10,000 ft.)に達するまでは、様々な制約によって、インターネット接続を利用できない。このため、常時接続を前提とした従来型の認証システムでは、バックホール接続が切れている間に乗客はアクセスポイントに接続できず、一定高度に達するまで機内サービスが受けられないことになる。さらに、巡航中においても、気象条件や空域における制限によってバックホール接続が途切れることがあり、利用者認証に失敗することで、無線 LAN の接続が切れる問題が生じる。

図 3 に、機内無線 LAN 向けのローカル認証・ローミングシステムの仕組みを示す。EAP-TLS における「サーバ認証」と「端末(利用者)認証」で、異なる公開鍵基盤(PKI)を使用する。乗客は異なる航空会社の便を乗り継ぐこともあるので、便が変わっても安全な自動接続が可能になるように、ローミング機能を実現した。複数のアカウント発行者に対応する電子証明書をすべて、予め航空機内のサーバに搭載しておく。世界の膨大な数の航空会社から電子証明書を集めるような運用は、現実的ではない。本研究では、多くの航空会社がアライアンスに属していることを利用して、アライアンスごとに証明書グループを構成することを想定した。

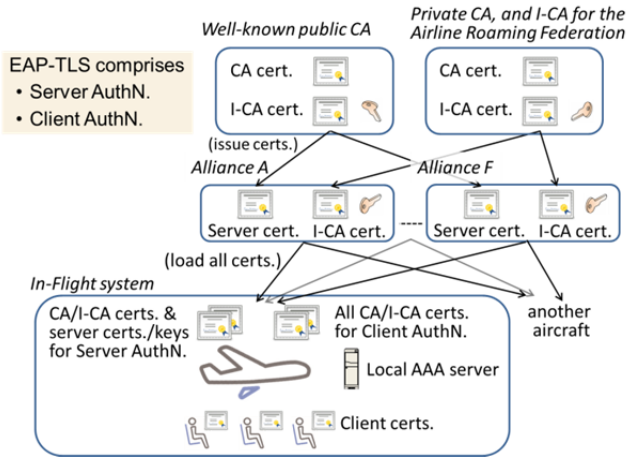

図 3 機内無線 LAN のためのローカル認証・ローミングシステム

多数の航空機への効率的かつ確実な証明書配布が必要なため、その技術の開発が今後の課題である。また、機材盗難などによる証明書の流出の恐れもあることから、影響範囲を抑制できるような対策技術の開発も必要である。

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　2件）

１．著者名 Kazunari Irie, Hideaki Goto	４．巻 28
２．論文標題 Automatic Roaming Consortium Discovery and Routing for Inter-federation Wireless LAN Roaming System	５．発行年 2020年
３．雑誌名 Journal of Information Processing (JIP)	６．最初と最後の頁 378-386
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.28.378	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Hideaki Goto	４．巻 29
２．論文標題 Inter-federation Roaming Architecture for Large-scale Wireless LAN Roaming Systems	５．発行年 2021年
３．雑誌名 Journal of Information Processing (JIP)	６．最初と最後の頁 103-112
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.29.103	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 Kazunari Irie, Hideaki Goto, Takuo Suganuma
２．発表標題 Certificate-based Local Authentication System for Wireless Mesh Networks in Disaster Areas
３．学会等名 The 6th International Conference on Information and Communication Technologies for Disaster Management（国際学会）
４．発表年 2019年

１．発表者名 Hideaki Goto
２．発表標題 Continuous and Secure In-Flight Wireless LAN with Roaming
３．学会等名 Asian Internet Engineering Conference (AINTEC) 2021（国際学会）
４．発表年 2021年

１．発表者名
Hideaki Goto

２．発表標題
Disruption-tolerant Local Authentication Method for Continuous and Secure In-Flight Wireless LAN

３．学会等名
The 5th IEEE International Workshop on Secure Digital Identity Management (SDIM 2022)（国際学会）

４．発表年
2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

Cityroam
https://cityroam.jp/
セキュア公衆無線LANローミング研究会
https://nghsig.jp/

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関