科学研究費助成事業　　研究成果報告書

平成　２６　年　　５　月　１５　日現在

機関番号：　１１３０１
研究種目：　挑戦的萌芽研究
研究期間：　2012～2013
課題番号：　２４６５００２３

研究課題名（和文）高度ポリシー適用を実現するネットワークローミング・認証連携基盤に関する研究

研究課題名（英文）Development of network roaming and identity federation infrastructure realizing high-degree policy application

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）　　2,700,000円、（間接経費）　　810,000円

研究成果の概要（和文）：世界規模の学術系無線LANローミング基盤であるeduroam(エデュローム)や、公衆無線LANなどの環境において、ID発行者と無線LANサービス提供者で個別にポリシーを設定し、それらを突き合わせることで、個人レベルの高度なアクセス制御を実現可能な、認証連携機構を開発した。また、耐災害・耐障害の機構を導入することによって、大規模災害時などのネットワーク途絶時にも利用可能な、頑強なアクセスネットワークシステムを実現した。

研究成果の概要（英文）：We have developed an identity federation mechanism that realizes personalized high-level access controls based on the combination of policies provided from both the ID provider and the service provider. The federation system is specially designed for Wireless LAN (WLAN) roaming systems such as "eduroam," the world-wide academic WLAN roaming system, and other public WLAN services. We have also developed an access network architecture tolerant of network disruptions that could be caused under large-scale disasters by introducing some disaster- and fault-tolerant mechanisms.

研究分野：　総合領域

科研費の分科・細目：　情報学・計算機システム・ネットワーク

キーワード：　ネットワークローミング　認証連携　ユビキタスネットワーク　インターネット高度化　無線LANローミング　eduroam

１．研究開始当初の背景

現在の公衆無線 LAN などにおけるネットワークローミング環境においては、無線 LAN サービスの提供側と享受側(利用者のアカウントを発行する機関) で個別にポリシーを適用する仕組みが不十分であり、ネットワーク利用の安全性の確保や、サービスの細やかなアクセス制御が行えないという問題がある。国際的な学術系無線 LAN ローミング基盤である eduroam(エデュローム)を、研究代表者らが中心となって 2006 年に日本に初導入、現在その運用主体を担っているが、その普及過程において、サービス提供側となるホスト大学と利用者の ID を発行するホーム機関で、それぞれが希望するアクセス制御が実現できないことが、eduroam 導入の障害の一つになっていることが明らかになってきた。複数のオペレータによるローミングは、ユビキタスネットワーク環境においては必要不可欠なものであり、商用系・学術系を問わず、柔軟なポリシーの適用が必要である。特に、会議場などにおいては、その場の機材やサービスといったリソースに対するアクセス権限をオンサイトで付与したいという場面もあり、動的なアクセス制御が望まれている。

２．研究の目的

ネットワークローミングにおいて配慮が必要となるポリシー、および、サービス提供側と享受側のポリシーの違いについて詳細な調査を行い、複数ポリシーの整合方法や動的なポリシー設定を実現するための手法について検討する。無線 LAN ローミング基盤 eduroam をアプリケーションの一例として取り上げ、上記の調査・検討結果を基にして、認証連携基盤における属性情報の持たせ方およびネットワークにおける高度なアクセス制御の実現方法を検討する。プロトタイプシステムを実装し、実証実験による評価を行い、知識(知見) の蓄積を行う。

３．研究の方法

はじめに、当初の研究予定を記す。2012 年度は、概ね以下の順序で研究を進める。

(1) 国内外の eduroam 参加機関および参加検討中の機関の聞き取りなどを通して、無線 LAN ローミング基盤に求められる様々なアクセス制御やアクセスネットワークの運用ポリシーを調査するとともに、将来のローミング環境に必要になるであろう新しいアプリケーションと動的ポリシー適用について検討する。海外の動向については、TERENA 主催の国際会議やワークショップ、ミーティング(TF-MNM, TF-EMC2 など) をはじめ、APAN ミーティング、TNC、SAINT などの国際会議において情報収集を行い、また意見交換を行う。

(2) 上記の調査・検討結果を基にして、ポリシーの汎用的な記述方法や、属性情報としての定義、属性情報の交換方式、ポリシーの整合方法などについて机上で検討を行う。この際、様々な認証連携基盤に応用できるような汎用性を確保しつつ、特に eduroam の認証連携基盤に組み入れられるような設計を行う。

(3) 現行の eduroam の認証連携システムを基にして、データセンターや学術クラウドでの利用に適した、導入障壁の低い認証連携アーキテクチャを設計する。また、実証実験用のサーバを構築して、国内で eduroam の参加を準備中または検討中の機関にサービスを提供し、フィードバックを得る。(実証実験後に正規運用として継続できるように配慮し、国内の学術情報基盤の高度化に貢献する。)

(4) 動的ポリシー設定の機能をユーザに提供するため、オンサイトでアクセス権を変更できるような仕組みについて検討する [1]。管理者権限の一時的付与やグループ設定などを認証連携基盤上で実現できるような、安全でスケーラブルな枠組みを開発する。ウェブサービスなどの形でプロトタイプを実装し、実証実験によりフィードバックを得て、改良を行う。

(5) 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、開発した認証連携システムの評価を行い、問題点や課題を整理する。

2013 年度は、概ね以下の順序で研究を進める。

(1) 前年度同様に、TF-EMC2、TF-MNM などの TERENA 主催のミーティングや、APAN ミーティング、TNC や COMPSAC などの国際会議において、認証連携およびネットワークアクセス制御に関する情報交換と資料収集を行う。

(2) 前年度に開発した認証連携アーキテクチャをベースとして、静的属性情報に加えて動的な情報も利用できる手法を開発する [2]。ポリシーに基づいてアクセス権限をネットワークに反映させる方法として、ファイアウォールの自動制御と、仮想ネットワーク (VLAN) による通信経路分離の二種類を組み合わせたアクセス制御機構を開発する。

(3) 動的なポリシー設定が可能なファイアウォール機能を備えた、評価用のネットワークを実験室内に構築し、様々な OS の端末を用いてシステムの機能・性能の評価を行う [3]。

(4) スケーラブルで効率の良い VLAN を構築するために、OpenFlow 技術を応用したアクセスネットワークとその制御方法を開発し、実証実験用のシステムを構築する。様々な種類の端末を用いて、システムの機能・性能の評価を行う。

(5) 海外の研究者に協力を依頼し、二つ以上の国にまたがる無線 LAN ローミングシステムを試作して、国際的なネットワーク環境において実証実験を行う [4]。実験で得られた知見を元に、アーキテクチャやプログラムの改良をさらに進める。また、TERENA のミーテ

ィングなどを介して国際的に技術提案を行っていく。

以上が当初の研究計画であるが、1)～4)について、耐災害性・耐障害性の実現を優先させるように、一部計画を変更した(具体的には「研究成果」に記す)。

４．研究成果

国際的な学術系無線 LAN ローミング基盤 eduroam や商用の公衆無線 LAN サービスなどのネットワークローミング環境において、配慮が必要となるポリシー、および、サービス提供側と享受側のポリシーについて調査を行い、複数ポリシーの突き合わせによって高度なアクセス制御を実現するための基礎技術を開発した。主たる成果を以下に示す。

(1) 柔軟なアクセス制御が可能なネットワークローミングシステムの実現

初めに、国内外の eduroam の運用状況分析などを通して、無線 LAN ローミング基盤に求められる様々なアクセス制御やアクセスネットワークの運用ポリシーについて検討を行った。ID 発行側のポリシーを静的な属性値として利用者の認証情報に付与し、これを RADIUS プロトコルの上でサービス提供側に通知する手法を開発した。また、サービス提供側のポリシーと利用者の属性値を照らし合わせて、アクセス制御ルールを生成・適用する手法を考案した。

ネットワークの動的なアクセス制御の実現のために、OpenFlow 技術を利用したアクセスネットワークのプロトタイプを開発し、機能の検証を行った。提案システムを用いることで、例えば利用者の所属や身分などに応じた柔軟なアクセス制御が、訪問先のネットワークでも実現可能である。TERENA のミーティング TF-MNM においてこれらの手法・システムを紹介し、意見を募り、今後追加すべき機能や配慮が必要な問題について有用な情報を得た。

(2) クライアント証明書を用いた耐障害ローカル認証方式の開発

研究開始当初は、サービス提供者(SP)と ID 発行者(IdP)の間が常にネットワークで接続される、一般的な認証連携の仕組みを想定していた。しかしながら、東日本大震災の経験およびその後の研究開発過程において、公衆無線 LAN 等のアクセスネットワークにおいては耐災害性・耐障害性が重要であり、このような性質を有する認証連携機構の開発が急務であると判断された。

例えば、図１のように避難所のネットワークが孤立している状態でも、利用者または端末の認証が可能ならば、各種情報の局所配信が可能となり、避難所における連絡網が実現できる。このような仕組みは、減災や早期復興の観点でも有効であると考えられる。

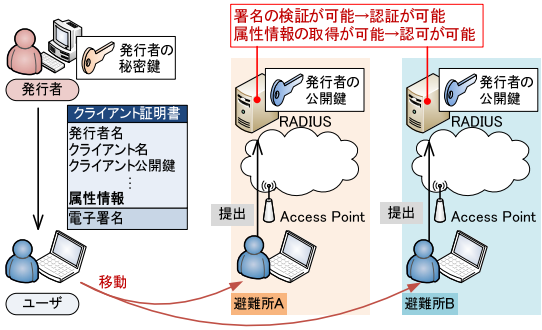

図１．クライアント証明書を用いた耐障害ローカル認証方式

本研究では、RADIUS プロトコルの EAP-TLS 認証方式を利用して、ネットワーク途絶時にもローカル認証を実現できるフレームワークを開発した(図 1)。クライアント証明書に属性情報を含めることにより、アクセス制御(認可)に必要な属性の交換も可能である。提案方式では予めすべての IdP 側の公開鍵を SP 側に登録しておく必要があるが、IdP の数を抑制できるようなアーキテクチャを採用し、鍵を自動配布とすることで、スケーラビリティを維持できる(後述の(5)も参照)。

上記(1)と(2)で開発した手法の一部を、研究代表者が別途参画する総務省・平成 24 年度委託研究に技術提供し、「災害時避難所等におけるネットワークリソース制御技術」に応用し、課題分析結果をフィードバックとして得ることができた。また、実証実験用システムの実現に貢献した。

(3) 耐災害・耐障害無線 LAN ローミング基盤の実現

学術系無線 LAN ローミング基盤 eduroam における大学等機関の参加障壁を軽減し、普及を促進するために、研究代表者が中心となって集中型の IdP である「代理認証システム」を開発し、国内機関に 2008 年より実証実験として提供している。本研究では、ローミング環境における認証基盤の耐災害性・耐障害性向上のために、地域分散による冗長化の仕組みを代理認証システムに組み入れ、クラウド型の認証システムを開発し、国際会議で発表した。

(4) クライアント証明書発行システムの開発

EAP-TLS 認証の実現のために、ローミングの参加機関が個別にクライアント証明書の発行システムを構築・運用することは、コスト・労力の両面で負担が大きい。特に、証明書を利用者に配布する手続きが煩雑である。本研究では、利用者各自が電子的な手段で容易に証明書を取得し、端末にインストールできるようにするため、eduroam 代理認証システムにクライアント証明書発行機能を追加

した。これにより、国内の大学等では、同システムに管理者がサインアップするだけで、eduroam の IdP 機能および証明書発行機能が利用できるようになる。

(5) 耐災害・耐障害 eduroam アーキテクチャの開発

世界規模の学術系無線 LAN ローミング基盤である eduroam に耐災害性・耐障害性の視点を導入し、ネットワーク途絶時にも利用可能な認証連携機構、および、利用者属性に基づくアクセス制御方式を実現するために、(2)の耐障害ローカル認証方式と、集中型 IdP の代理認証システムを組み合わせた、耐災害・耐障害 eduroam アーキテクチャを開発した。

図 2 に示すように、同システムを有する国(地域)では Path A が用いられ、認証処理に必要なホップ数が大幅に削減され、長距離の通信も不要となることから、トップレベルのサーバやネットワークの障害、混雑に強い、安定な認証が可能となる。同システムを導入していない地域でも、Path B の経路で認証が可能であり、機関個別の RADIUS サーバに向かう分の経路が削減され、認証の効率化と安定化を図ることができる。

本アーキテクチャを国際会議および TERENA のミーティングなどで提案した。

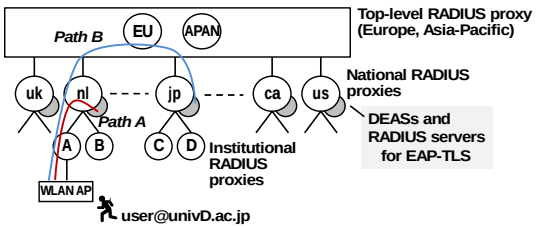

図 2. 代理認証システムを利用した耐災害・耐障害 eduroam アーキテクチャ

以上、(1)～(5)の手法・技術をすべて統合したシステムの構築と評価、および、国内機関へのサービス提供が、今後の課題である。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔学会発表〕（計 7 件）

[1] Tomo Niizuma and Hideaki Goto, “Centralized Online Sign-up and Client Certificate Issuing System for eduroam,” COMPSAC MidArch 2014 Workshop (2014.7.21-25, Sweden). 査読有, 印刷中

[2] Hao Liu and Hideaki Goto, “Certificate-based, Disruption-tolerant Authentication System with Automatic CA Certificate Distribution for eduroam,” COMPSAC MidArch 2014 Workshop (2014.7.21-25, Sweden). 査読有, 印刷中

[3] 新妻 共, 後藤英昭, “耐障害性・耐災害性を有する無線 LAN ローミング基盤のためのクライアント証明書発行システム,” 電子情報通信学会 2014 年総合大会講演論文集 B-16-2, p.554 (2014.3.18, 新潟大学).

[4] Hao Liu and Hideaki Goto, “Disruption-tolerant, Large-scale Wireless LAN Roaming Architecture for eduroam,” 信学技報 IA2013-56, pp.27-28 (2013.11.1, 広島).

[5] Hideaki Goto, Hao Liu, Shunichi Kinoshita, Motonori Nakamura, and Hideaki Sone, “DISRUPTION-TOLERANT, LARGE-SCALE WIRELESS LAN ROAMING ARCHITECTURE FOR EDUROAM,” IADIS International Conference Applied Computing 2013 (AC2013), pp.191-195 (Oct.25, 2013, USA). 査読有

[6] Hideaki Sone, Hideaki Goto, and Motonori Nakamura, “Authorization-based Flexible Network Service for Wi-Fi Roaming Systems,” TERENA Networking Conference TNC2013 (poster) (June 3-6, 2013, Netherland). 査読有

[7] Hideaki Goto and Hideaki Sone, “CLOUD-BASED, DISASTER-TOLERANT DELEGATE AUTHENTICATION SYSTEM FOR LOW DEPLOYMENT AND OPERATIONAL COSTS OF LARGE-SCALE EDUROAM SYSTEM,” IADIS International Conference Applied Computing 2012 (AC2012), pp.369-374 (Oct.20, 2012, Spain). 査読有

〔その他〕（計 1 件）

[1] eduroam 代理認証システム, http://www.eduroam.jp/

６．研究組織

(1)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