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

平成　２９　年　　５　月　２２　日現在

機関番号：　１１３０１
研究種目：　挑戦的萌芽研究
研究期間：　2015～2016
課題番号：　１５Ｋ１２０１５

研究課題名（和文）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

研究課題名（英文）Development of automatic authentication network configuration method for disruption and disaster-tolerant identity federation systems

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）　　2,600,000円

研究成果の概要（和文）：認証連携は現在、様々なサービスに利用されている。大多数のシステムがネットワーク接続に依存しているため、ネットワーク障害の際は、局所的なサービスでさえも利用不能に陥ることが多い。本研究では、動的に構造が変化する無線メッシュネットワーク(WMN)のような環境においても、認証ネットワークを自動的に構築できる手法を開発した。電子証明書を用いたローカル認証方式をWMNと組み合わせ、基地局と利用者両方の認証に用いた。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。また、被災地のみならず、会議場・イベント会場などでの一時的な基地局設置にも有用である。

研究成果の概要（英文）：Identity federation has been adopted in various web and network services including Public Wireless LAN (WLAN). Network disruptions often lead to service interruptions, even for local applications, since most identity federation systems depend on network connectivity. We have developed an automatic authentication network configuration method which works well even on dynamically changing networks such as Wireless Mesh Network (WMN). Local authentication method using client certificates has been combined with a WMN, and used for both access point and user authentications. The system works even when the back-haul network is disrupted in a disaster affected area, and enables various local services. The new system will also be useful for temporary and quick deployment of WLAN systems at conference/event sites as well as in affected areas.

研究分野：　総合領域

キーワード：　認証連携　無線LANローミング　eduroam　利用者認証　無線メッシュネットワーク　耐災害性　耐障害性

１．研究開始当初の背景

認証連携は、インターネット上の様々なサービスに導入され、その依存性が強まっている。学術コミュニティにおいても、Shibboleth を代表として世界的に立ち上げの時期にあり、日本でも「学術認証フェデレーション(学認, GakuNin)」(研究代表者が参画)や、学術系無線 LAN ローミング基盤「eduroam」(研究代表者が主導)などの基盤構築が進められている。学術・商用の両サービスとも、認証連携基盤においては、認証サーバやそれらを結ぶネットワークなどの部分的な障害がシステムの広範囲に影響を及ぼすことにより、サービスの可用性の低下が日常的に問題となっている。その早急かつ根本的な解決のためには、基盤を俯瞰した調査・研究が必要である。

現在の様々な認証連携基盤は、冗長化などの対策に留まり、広域停電や自然災害による障害に対して、アーキテクチャ上の対策やその研究が不十分である。人々の生活が電子的なサービスに強く依存する現在、システムの一部損壊にも耐えられるような、耐障害性・耐災害性を備えた認証連携アーキテクチャが必要と考えられる。また、我々は過去の研究において、被災地やイベント会場の端末過密環境などにおいて DTN(遅延耐性ネットワーク)が有効であることを示したが、安全かつ迅速な認証サービスを展開するには、DTN 上でも利用できる認証連携ネットワークを安全に自動構築・修復する技術が必要である。

２．研究の目的

インターネット上の各種サービスや公衆無線 LAN に導入が進み、依存が高まっている認証連携基盤について、認証機材の故障や過負荷、停電、自然災害による機材喪失などの障害においても、サービス全体ないし一部を継続利用できる「耐障害性・耐災害性を有する認証連携ネットワーク」の実現と、サービス提供の「場所と規模に柔軟に適応して、安全に自動構築できるアーキテクチャ」の開発を目的とする。ネットワークや電源のインフラが不安定な新興国や、被災地・避難所、イベント会場等の端末過密空間における安全な無線 LAN サービスを想定し、調査と理論により認証連携の高可用化と自動構築への要求要件を導いた上で、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)を利用した実証実験を通して分析や考察を行い、世界的に方式提案を行ってゆく。

３．研究の方法

当初の研究予定を記す。

平成 27 年度は、概ね以下の順序で研究を進める。

(1) 様々な認証連携の機構を調査した上で、国内外の運用状況の調査や、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実装・機構の限界を明らかにする。また、障害の影響範囲や、制限付きの運用を想定した場合に必要とされる属性などのクラス分けなどを行う。特に、学術系の国際無線 LAN ローミング基盤 eduroam は、研究代表者が運用主体を担っていることから、実運用のログなどを利用して、詳細な状況分析を行う。

(2) 国内外の学術系認証連携基盤や eduroam の参加機関、参加検討中の国・機関の聞き取りなどを通して、認証連携基盤に求められる様々な運用ポリシーや、将来の高度アクセス制御に必要な属性などを調査する。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, REFEDS など)をはじめ、APAN ミーティング、TNC、COMPSAC 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。特に新興国においては、学術情報基盤の信頼性がまだ十分ではない地域が多数あることから、現状および想定される障害について調査する。

(3) 上記の調査・検討結果を基にして、認証サーバや広域ネットワークの障害で問題となる機構部分、可能な回避策などを洗い出す。孤立したネットワークや DTN(遅延耐性ネットワーク)上でも利用できる認証連携のフレームワークを開発する。研究代表者らが先行研究で開発した方式は無線 LAN 専用であり、また、電子証明書の更新処理などの検討が未だであることから、当方式を基本とするか新規に、汎用性と実用性の高いフレームワークを設計する。

(4) 認証サーバや属性プロバイダ、広域ネットワークなどの一時的な高負荷・障害にも耐性がある、属性交換方式について検討する。負荷状況・障害状況に応じた機能縮退を実現する方法論を導出するとともに、制限環境の実装方法について検討する。

(5) 無線 LAN ローミングへの応用を想定して、耐障害性・耐災害性を有する認証連携システムのプロトタイプを開発し、国内の eduroam 基盤に仮想機関として接続する。予算に計上したノート PC や、スマートフォン(個人所有)、現有の Mac、タブレットなどの多種多様な端末を用いて、実装したプロトタイプの機能・性能評価を行い、問題点や課題を整理する。eduroam に参加中、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。

平成 28 年度は、概ね以下の順序で研究を進める。

(6) 前年度同様に、TERENA 主催のミーティングや、REFEDS Meeting、InCommon CAMP、APAN ミーティング、TNC や COMPSAC などの国際会議において、認証連携基盤の認証および属性交換に関する情報交換と資料収集を行う。

(7) 前年度に開発した耐障害・耐災害認証連携フレームワークを基に、無線 LAN ローミ

ング以外の認証連携基盤への応用を想定して、実装を開発する。この際、既存の機構に追加(アドオン)できるような仕組みを想定してアーキテクチャ設計を行うが、既存システムに大幅な変更が許される場合についても併せて検討する。

(8) 現有および予算に計上した PC を用いて、Shibboleth に基づく認証連携システムを研究室内に構築し、耐障害・耐災害の機能を追加したプロトタイプを実装する。様々なオペレーティングシステムの端末を用いて、システムの機能・性能の評価を行い、問題点や課題を整理する。

(9) 認証連携ネットワークの自動構築・修復を実現するために、これまでの調査結果を基にして、自動構築への要求要件を導く。続いて、最寄りのプロキシサーバを見つける探索機構や、安全に接続するためのサーバ間相互認証、死活監視などの機構を開発する。

(10) 上記の機構をプロトタイプとして実装し、無線 LAN への応用を想定して、研究代表者らが開発した端末過密環境向けの無線 LAN システムと組み合わせて、実証実験・評価を行う。従来の認証連携機構では、接続するプロキシサーバが静的に固定されているという制限があったが、本研究ではこの部分を自動化する。

(11) 評価実験で得られた知見を基に、フレームワークやアーキテクチャ、実装の改良をさらに進める。TERENA や Internet2 のミーティングなどを介して国際的に技術提案を行う。

以上が当初の研究計画であるが、無線 LAN 以外の現行の認証連携システムではアーキテクチャ上の困難さがあること、及び、無線 LAN システムの耐災害性・耐障害性の早期実現を優先させた方がよいと判断されたことから、(7)(8)については割愛し、代わりに、公開鍵基盤(PKI)の運用及びそれを利用する認証処理を効率化するための手法を開発することとした(具体的には「研究成果」に記す)。

４．研究成果

本研究では、インターネット上の各種サービスや公衆無線 LAN に導入が進み、依存度が高まっている認証連携基盤について、認証機材の故障や過負荷、停電、自然災害による機材喪失などの障害においても、サービス全体ないし一部を継続利用できる「耐障害性・耐災害性を有する認証連携ネットワーク」の実現と、サービス提供の「場所と規模に柔軟に適応して、安全に自動構築できるアーキテクチャ」の開発を目的として、研究を進めた。

平成 27 年度は、世界規模の学術系無線 LAN ローミング基盤である eduroam への応用を想定して、手法開発や実践的な分析・考察を行った。

初めに、国内外の eduroam および学術系認証連携基盤の運用状況の調査や、関係者との情報交換などを通じて、認証連携基盤に求められる様々な運用ポリシーや、セキュリティ要件、大規模イベントや自然災害の被災地などで想定される利用形態やシステム障害などの情報収集を行った。得られた知見を基に、従来は現場での手作業に大きく依存していた認証連携ネットワークの構築作業を大幅に簡素化できる、「認証連携ネットワーク自動構築手法」を開発した。また、本手法を B.A.T.M.A.N. による無線メッシュネットワーク(WMN)と組み合わせることによって、可搬型無線基地局システムのプロトタイプを開発した(図 1)。このシステムは、世界の認証連携基盤の接続点となるサーバと、それに関連付けられた電子証明書を一度だけ各基地局に登録しておくことによって、現場では複数基地局の配置と電源投入だけで、様々な規模の公衆無線 LAN サービスを構築可能にする。

基地局の認証と利用者認証の両方で、電子証明書を利用したローカル認証処理を実現した(図 2)。これにより、上流のネットワークが途切れてインターネットから孤立した被災地でも、電子掲示板・連絡網を実現するための局所的なネットワークを、迅速に敷設できる。

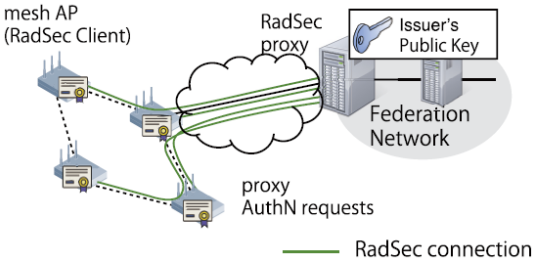

図 1 無線メッシュネットワークを利用した可搬型基地局システム

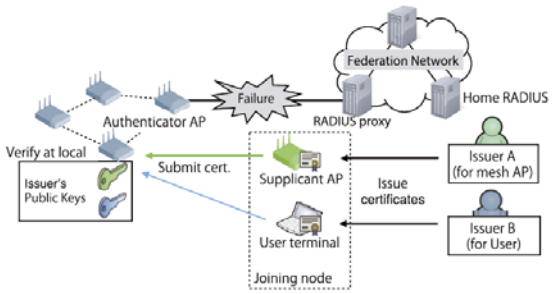

図 2 電子証明書を利用した端末・利用者ローカル認証

平成 28 年度は、前年度に学術系無線 LAN ローミング基盤 eduroam への応用を想定して開発した「認証連携ネットワーク自動構築手法」及びそのプロトタイプを基に、実用化に必要となる要件や処理を抽出・検証し、そのための手法を開発・評価した。

前年度と同様に、国内外の eduroam および

学術系認証連携基盤の運用状況の調査や、関係者との情報交換などを通じて、認証連携基盤に求められる様々な運用ポリシーや、セキュリティ要件、大規模イベントや自然災害の被災地などで想定される利用形態やシステム障害などの情報収集を行い、知見を蓄積した。前年度に開発したプロトタイプを基に、被災地等、上流のネットワークが一時的に途絶する環境においても安全な認証とアクセス制御が可能となる機構を理論的・実験的に検証した。従来のローカル認証方式に加えて、証明書失効リスト(CRL)を効率的に各基地局に配布する手法を取り入れることで、不正利用が明らかになった人物による利用を早急に停止したり、機能不全となった基地局を迅速に切り離したりできるようになった。

CRL を各基地局が個別にサーバからダウンロードするとネットワークの混雑を招く。これを避けるため、WMN に含まれる木構造を利用して、CRL をサーバ側からプッシュし、各基地局が隣接ノードにリレーする仕組みを開発した(図 3)。6 ノードから成る直線状の WMN を用いた評価実験により、開発したリレー型 CRL 配信システムでは、CRL の転送データ量と通信時間のいずれも従来の約 1/4 に削減できることを確認した。

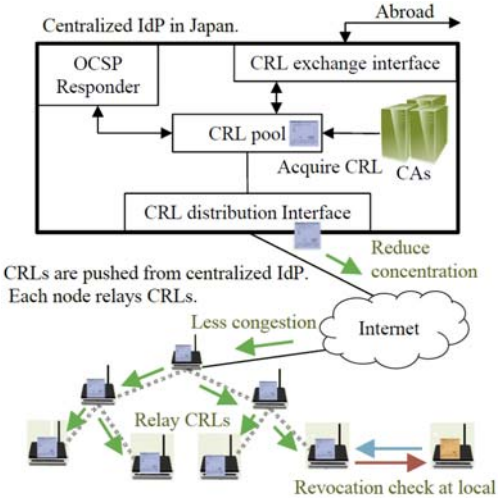

図 3 WMN 上におけるリレー型 CRL 配信

本研究により開発した手法及びプロトタイプを実用レベルまで洗練することにより、被災地等においても高い安全性と安定性を有する公衆無線 LAN システムを構築し、電子掲示板・連絡網を実現するための局所的なネットワークを迅速に敷設できるようになると考えられる。開発した手法は、被災時に限らず平時においても有用と考えられ、イベント会場や学校等における迅速かつ柔軟な基地局設置にも貢献が期待される。

本研究では、基地局を提供・運用する組織が複数あるケースも部分的に想定していたが、システム全体の運用方法については、まだ検討の余地が残されている。評価実験を行った WMN の規模も小さい。複数組織にまたがるような、数十～数百ノード規模の巨大 WMN への拡張・応用、及び、その評価が、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）

〔雑誌論文〕（計１件）
[1] Tomo NIIZUMA and Hideaki GOTO, “Easy-to-Deploy Wireless Mesh Network System with User Authentication and WLAN Roaming Features,” IEICE TRANSACTIONS on Information and Systems, Vol.E100-D, No.3, pp.511-519, 2017. 査読有
DOI: 10.1587/transinf.2016EDP7123

〔学会発表〕（計３件）
[1] Tomo Niizuma and Hideaki Goto, “Quick- and Easy-to-Deploy Wireless Mesh Network System for WLAN Roaming Services,” Asian Internet Engineering Conference (AINTEC) 2015, pp.9-16, 2015. (2015.11.18-20, Bangkok, Thailand). 査読有
DOI: 10.1145/2837030.2837032

[2] Tomo Niizuma and Hideaki Goto, “Easily and Fast Deployable Wireless Mesh Network System for eduroam,” The TNC15 Networking Conference (poster), 2015. (2015.5.15-18, Porto, Portugal). 査読有

[3] Hideaki Goto, Tomo Niizuma, Motonori Nakamura, and Hideaki Sone, “eduroam IdP as a Service - benefits and operational experiences -,” The TNC15 Networking Conference (poster), 2015. (2015.5.15-18, Porto, Portugal). 査読有

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