訪問者の身元と目的を保証する訪問者認証システムの提案

平田 宗一郎[1]　丸山 一貴[1]　土屋 英亮[2]

概要：水道や電気といった重要なインフラの点検等で，自宅や会社へ当該企業のサービスマンを名乗る者が訪れる場合を考える．提示された身分証が確実に本物か判断するのは難しいが，正規のサービスマンであれば迎え入れて点検を行ってもらわなくてはならない．訪問者の身元をその所属組織に問い合わせて明らかにする訪問者認証を行う必要があるが，一般的な電話を用いた訪問者認証では時間がかかり，また音声でしか情報を伝達することができない．そこで，本論文ではスマートフォンを用いた訪問者認証システムを提案する．この方式では特別な機器を利用せず，訪問者がスマートフォンを用いて所属組織から認証用のトークンを取得・提示し，訪問を受けた者が自身の PC やスマートフォンで独立にこれを検証することで，訪問者の身元確認を実現する．訪問者の所属組織では，訪問先が妥当である場合のみトークンを発行することで，身分を悪用した訪問を防ぐことが可能である．本論文では，提案の詳細と試作システムの実装方法，それを用いた具体的な利用例を示す．

キーワード：訪問者認証，ホームセキュリティ，トークン，ワンタイムパスワード

Visitor authentication system to confirm visitor's identity and purpose

Abstract: Suppose that a service engineer of a water board or an electric power company comes to our home or office and he shows his ID card. We cannot make sure that the card is genuine, and if the engineer is genuine we have to accept the visit to get a maintenance service. If we could call the company which employs the engineer, his identity would be confirmed. The call takes a long time and provides a limited information based on the talk. Now, we propose a visitor authentication system using smartphones. It enables us to identify a visitor without any special devices. A visitor retrieves a *token* for a certain visit from his company by using his smartphone and shows it to the resident. A resident starts an application of the system, which is already installed to his PC or smartphone, to send the token to the company in order to verify it. A company issues a token if and only if a visitor, an employee, stays near a valid customer to prevent a wrongful visit. In this paper, we describe the detail of our proposal. An implementation of our pilot system and a use case are also included.

Keywords: Visitor authentication, home security system, token, one-time password.

1. はじめに

自宅や職場に訪問者が訪れた場合，知人や取引先等ではないにもかかわらず受け入れざるを得ないものとして，生活インフラや各種サービスに関わるものが挙げられる．例えば電力会社や水道局，郵便や宅配便，NHK 等である．これらの訪問者は，見覚えのある制服を身に着けて不自然ではない用件を述べるため，我々は玄関の鍵を開けて対面して対応している．玄関の向こう側にいる人間が本当にその通りの所属で，業務上の行為として訪問しているかどうかを確かめるには，訪問を受けた側（以下，住人という）が口頭で述べられた訪問者の所属組織の電話番号を独自に調べ，そこに問い合わせることが必要だが，訪問を受けたその場で行うことは時間的にも，手間の観点からも困難である．

安ら [1] は，独居高齢者がモニター付きインターフォンを介して訪問者に対応する場合の不安感について調査を行っている．訪問者に対して抱く不安感は独居女性や，児童に留守番をさせている保護者でも同様であり，訪問者との会

[1] 明星大学 情報学部
School of Information Science, Meisei University
[2] 国立大学法人 電気通信大学 情報基盤センター
Information Technology Center, University of Electro-Communications

話とは別の手段によりその身分等を確認することができれば，合理的に不安感を解消できる可能性があると我々は考えた．一方で，外来者が示す所属等の情報により自動的に本人確認を行う仕組みは，外来者にネットワーク利用を許可するための国際無線 LAN ローミング基盤 eduroam[2] として実用化されており，同様の方法により訪問者を認証することは可能である．

本論文では，自宅に訪問者が訪れた場合，訪問者自身が提示する情報に基づいて訪問者の所属組織に本人確認を行うことを，訪問者認証と呼ぶこととする．訪問者認証では，訪問者が住人に対して (1) 所属組織，(2) 氏名，(3) 顔，(4) 訪問理由を提示し，住人は所属組織から送信された情報と照合することにより本人確認を行う．本研究の目的は，訪問者認証に加えて，訪問理由を検証することにより，訪問の正当性を確認して受け入れの認否を決める仕組みを実現することである．また，本提案は住人側の安心感を高めるだけでなく，所属組織が訪問者の業務遂行状況を監督することも可能とするものである．以下，第 2 章で関連研究との比較を述べ，第 3 章で提案方式の詳細と試作システムの実装，具体的な利用方法を示す．第 4 章で検討すべき点について議論を行い，第 5 章でまとめを述べる．

2. 関連研究

現時点で一般的な枠組みによる訪問者認証の方法について述べる．住人は訪問者の所属組織を確認し，偽装のおそれのない信頼のおける電話帳（以下，電話帳という）から所属組織に対して電話をかけ，訪問者が実在し，現在正当な理由で住人の下に訪問しているか確認する．電話帳を用いるとは，例えば自宅のインターネット回線を通じて所属組織の社名を検索し，問い合わせ先を確認することを意味する．この方法の利点は，一般に普及している固定電話・携帯電話を用いて認証を行うことができ，訪問者認証のために別途機材を購入することが必要ないという点である．欠点は，電話帳から訪問者の所属組織の連絡先を調べて電話をかけ，訪問者の情報を電話口で聞き出す行為に手間と時間がかかることである．また，この方法では訪問者の顔を確認できないため，悪意のある第三者が訪問者の訪問先，訪問時間，訪問者の氏名・所属組織等を知っていた場合には，偽装が可能である．本研究では，住人が所属組織から訪問者の情報を聞き出す部分を自動化すると共に，顔情報の提示を追加することでより確実な訪問者の確認を実現する．

中井 [3] は，あらかじめ住人宅にフェムトセル基地局と専用の表示装置を設置して，訪問者の携帯端末と組み合わせて訪問者認証を実現する方式について提案している．この方式における訪問者認証の手順は以下の通り：(1) 携帯端末が基地局のカバーエリアに入った際，(2) 端末が基地局に対して自動的に通信を行い，認証サーバへ情報提示のリクエストを送信する．(3) 認証サーバは端末に紐付いた訪問者の情報をレスポンスとして送信し，(4) 表示装置がこれを提示する．訪問者と住人が端末の操作などを必要とせずに認証結果を得ることができるという利点はあるが，各住戸に基地局及び専用の表示装置を設置する必要がある．本研究では，訪問者・住人とも認証のために若干の操作を要するが，訪問者は携帯するスマートフォンを，住人は自宅の PC もしくはスマートフォンを利用するため，汎用的な装置と一般的な通信路を利用することができるので，導入コストは低いと言える．

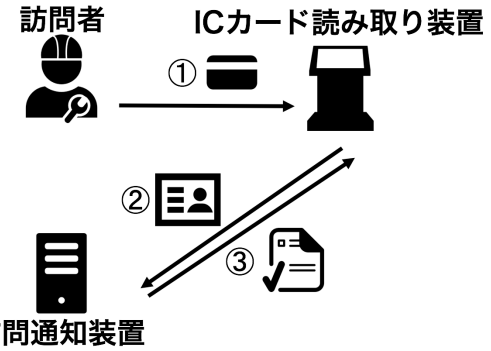

図 1 籠田 [4] による訪問者認証の手順
Fig. 1 Visitor authentication procedure by Kagota[4].

籠田 [4] は，訪問者の所属組織が訪問の正当性を保証するシステムを提案している．ネットワーク接続された IC カード読み取り装置を訪問先に設置し，訪問者が IC カードをかざしてパスワードを入力すると，読み取り装置が自身の設置場所と時刻を付加して所属組織に設置された認証サーバへ送信する．認証サーバは訪問先と訪問時刻が正しい場合にのみ読み取り装置に承認の信号を送る（**図 1**）．本研究と同じく，権限を悪用した不正な訪問を防ぐことを目的としているが，専用の読み取り装置を設置することが必要である．本研究では読み取り装置に相当する手続きを住人が行うことになる．訪問者が所属組織とあらかじめ通信を行って，住人に必要とされるサーバ上の情報にアクセスするためのトークンを生成することで，住人が伝達すべき情報を圧縮していると言える．

大学のような教育研究機関では通常の構成員に加えて，非常勤講師や客員研究員など，限定された権限でシステムを利用できるユーザが存在する．清水ら [6] は非常勤講師等が所有する一般的な IC カードを認証に用いる方法を提案している．非常勤講師等は訪問者と位置づけることができ，住人による本人確認に応用することは可能である．しかし，本研究が対象とする環境では住人が事前に訪問者を特定することや，一般的な住宅の玄関に IC カードリーダを設置することは困難である．

大学ではこの他に，学会や研究打ち合わせ等のイベントで来訪する利用者に，一時的なネットワーク利用権を与えたい場合がある．eduroam[2] は教育機関の間でキャンパス

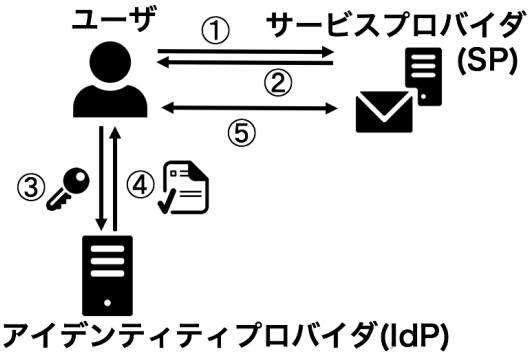

図 2 Shibboleth 認証の手順
Fig. 2 Shibboleth authentication procedure.

無線 LAN の相互利用を目的としたローミングサービスであり，伊東ら [5] は大学での具体的な導入について報告している．eduroam に参加している教育機関の所属である者（本論文における訪問者）が，別の eduroam に参加している教育機関のキャンパス無線 LAN に接続したい場合，自分の所属などを付加した認証情報を含めて IEEE802.1X にて接続を試みる．無線アクセスポイントに接続すると認証サーバ（本論文における住人）へ認証を要求し，最終的に接続者の所属元の RADIUS サーバ（本論文における所属組織）で認証が行われ，結果がキャンパス無線 LAN 側へ返り，適切であれば接続を許可する．本研究で採用した，訪問者の所属組織に住人から問い合わせを行うという方式は，eduroam におけるそれと同じ考え方である．

組織内に複数のサービスが存在し，かつサービスの利用者を認証したい場合に，セキュリティを維持したまま利用者の手間を軽減させたい場合がある．Shibboleth 認証 [8] はシングルサインオンを実現するための認証基盤であり，別のサービスを利用する度に利用者へ認証を要求するのではなく，一度の認証処理により複数のサービスが利用可能となる機能を提供する．サービスプロバイダ（SP）（本論文における住人）と呼ばれるサービスを提供するシステムへ，認証が行われていないユーザ（本論文における訪問者）がアクセスした場合，SP は認証を管理するアイデンティティプロバイダ（IdP）（本論文における訪問者認証システム）へリダイレクトさせる．ユーザは IdP で認証を行い，IdP は認証結果を含んだ SP へのリダイレクトをユーザに返す．以降ユーザは対応する SP に対してアクセスする際に，認証結果を付与してアクセスし，ユーザから認証結果を受け取った SP は，そのユーザに応じたサービスを提供する．（**図 2**）本研究で採用した，認証情報を認証をされる側に渡し，その後自らの認証情報を確認したい側へ渡すという方式は，Shibboleth 認証におけるそれと同じ考え方である．SP と本論文における住人，認証を要求するユーザと本論文における訪問者，IdP と本論文における訪問者認証システムはそれぞれ対応した関係にある．

佐藤ら [7] は利用者の認証に Facebook を利用して，その所属グループごとに異なるアクセス制御を適用する方法を提案している．外部の認証サーバを利用者の本人確認だけでなく，種別判定にも利用している．この考え方は本研究にも応用可能であり，例えば所属組織が訪問者の属性として訪問目的等の付加情報を登録しておくことで，住人に対してより細やかな情報提供が可能になると考えられる．

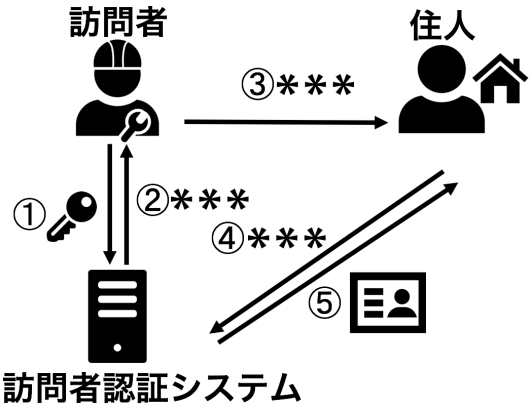

図 3 訪問者認証の手順
Fig. 3 Procedure of our proposal.

3. 提案方式

本章では，提案方式の詳細と試作システムの実装方法，想定する具体的な利用例について述べる．

3.1 提案方式の詳細

本方式では次のことを前提としている：

- 住人及び訪問者は，通信先である訪問者認証システムへのアクセス方法を，あらかじめ安全な手段で入手しているものとする．
- 住人と訪問者認証システム間と，訪問者と訪問者認証システム間の通信は暗号化がなされており，改ざんや盗聴のおそれはないものとする．
- 訪問者認証システムに置かれている訪問者の情報は所属組織の権限で適切に管理されているものとする．
- 玄関を解錠することなく訪問者の顔と提示されたトークンを光学的に確認できるよう，住人宅にはドアスコープやカメラ付きインターホン等が設置されているものとする．

本論文で提案する訪問者認証は，**図 3** のような手順で認証を遂行する．

(1) 訪問者は訪問先へ訪問する直前に，スマートフォンを利用して所属組織の訪問者認証システムへログインし，訪問先を選択してトークンを要求する（発行リクエスト）．この際，スマートフォンが測定した GPS の位置情報を添付する．
(2) 訪問者認証システムは訪問者を認証した後に，位置情報をあらかじめ登録された情報と比較し，近くにある

訪問先一覧を訪問者に提示する．訪問者が一覧から訪問先を選択することで，トークン（図中の＊＊＊）が発行され訪問者へと送信される．

(3) 訪問者は訪問先へ行き，ID カードを提示して所属と氏名を明らかにした上で，住人へトークンを伝達する．

(4) 住人は訪問者認証システム用アプリケーションに，訪問者から伝達されたトークンを入力して送信する．

(5) 訪問者認証システムはトークンを受け取り，これに紐付けられた訪問者の所属・氏名・顔写真・訪問理由（訪問者情報）を住人に送信する．同時に (2) で発行したトークンを無効化して，再利用を防止する．

(6) 住人は受信した情報を訪問者と比較して，訪問者認証を行う．

訪問者認証システムは訪問者の所属組織が運用しており，社員である訪問者の ID とパスワード，部署や顔写真といった情報を管理している．各訪問者がその日に訪問する予定の行き先について，位置情報と訪問先の名前と訪問理由（以下，訪問先情報という）をあらかじめ登録しておく．訪問者がトークン発行のために接続すると，訪問者本人か確認するためにログイン認証を実施し，訪問者が申告する訪問先情報に基づいてトークンを発行する．

提案方式で交換される情報を**表 1** にまとめる．発行リクエストでは，どの訪問者がどこへ訪問しようとしているかを明らかにするため，訪問者からは 2 つの情報を訪問者認証システムへ提示する．1 つは訪問者の ID であり，システムへのログインにより通知される．もう 1 つは訪問先を特定するための訪問先情報である．トークンとは，訪問者が住人へ伝達する情報をハッシュ値としたものである．トークンと結びついている情報は，電話を利用した訪問者認証では住人が口頭で所属組織に伝えなければならないものであり，提案方式では訪問者が代理で事前に所属組織に伝えることにより，住人の負担を軽減していると考えられる．トークンを受け取った訪問者認証システムが住人に送信する訪問者情報は，所属と氏名に加えて，所属組織が保持する訪問者の顔と訪問理由を送信する．これにより，電話では難しかった住人による訪問者の本人確認が実現される．

悪意の第三者が，正規の訪問者を装って訪問者認証を回避しようとする場合を考える．第三者が訪問者のスマートフォンを入手してトークンの発行を試みた場合，訪問者認証システムへのログイン認証ができず，トークンを入手できない．第三者が発行済みのトークンを入手した場合，訪問者認証システムが住人に提示する顔画像と異なるため，住人の判断により訪問者認証はエラーとなる．仮に第三者が訪問者認証システムに不正にログインできたとしても，訪問者は訪問先の選択しかできず，住人を欺くためのトークンは入手できない．

このシステムにより，住人は専用の装置を取り付けることなく，また，電話による確認よりも容易に，訪問者認証に必要な訪問者の情報を入手することができる．訪問者の顔写真を提示することにより，より正確に認証を行うことができるだけでなく，住人の心理的な安心感にも寄与すると考えられる．訪問者の所属組織は訪問者認証システムを通じて，訪問者がいつ，どの訪問先のトークンを要求したか，住人からトークンの確認要求があったかを把握することができるので，職権の乱用を監視することができる．また訪問者の不正行為を抑止することに繋がると言える．ただし，提案方式は専用の装置や通信路を用いないため，職務を放棄しようとする訪問者が正規の手続きでトークンを入手し，私物のスマートフォンを用いて住人と同様の手順でトークンを検証した場合，この不当行為を所属組織が検出することができない．これについては第 5 章で述べる．

3.2 実装

提案方式の具体的な利用手順を確認するため，試作システムの実装を行った．訪問者認証システムに相当する機能は，Web サーバ上に Ruby on Rails を利用した Ruby プログラムとして実装した．住人及び訪問者が使用する，訪問者認証システムと HTTP で通信してトークンを扱う機能は，Java を用いて Android アプリケーションとして作成し，住人用と訪問者用にそれぞれ別個のアプリケーションとなっている．訪問者認証システムは OS X 10.10.5 上で Ruby 2.2.2 及び標準添付の WEBrick ライブラリを用いて，住人用と訪問者用の両 Android アプリケーションは Android 5.1.1 上で動作確認を行った．フレームワークに必要な分を除いて独自に実装したコードは，訪問者認証システムで 100 行弱，訪問者用アプリケーションで約 80 行，住人用アプリケーションで約 50 行であるが，試作システムでは以下を省略している．

- GPS を使用した位置情報の取得．
- 訪問先の名前．

訪問者認証システムのデータベースには，訪問者のアカウントに紐付けられた「氏名」「顔写真」「訪問理由」「その他説明文」が格納されている．訪問者認証システムが HTTP を介して提供する機能として，「訪問先リストの取得」「トークンの取得」「トークンに紐付けられた情報の取得」の三つがあり，Android アプリケーションはこれらを利用する．「訪問先リストの取得」「トークンの取得」は訪問者用 Android アプリケーションで用いられ，個々の訪問者に割り当てられてた ID とパスワードが必要である．「トークンに紐付けられた情報の取得」は住人用 Android アプリケーションで用いられ，認証は必要ない．

訪問者用の Android アプリケーションは，起動すると訪問者認証システムへのログインを求められる．ログインを行うと訪問先一覧が表示され（**図 4**），一つを選択すると確認画面の後にトークンが表示され（**図 5**），訪問者はこれを住人へと伝達する．住人用の Android アプリケー

表 1 訪問者認証で交換される情報
Table 1 Information transferred through the procedure.

図 3 の手順	情報の名称	含まれる情報
(1)	発行リクエスト	訪問者の ID
(2)–(4)	トークン	訪問者情報と結びついたハッシュ値
(5)	訪問者情報	所属と氏名 訪問者の顔 訪問理由

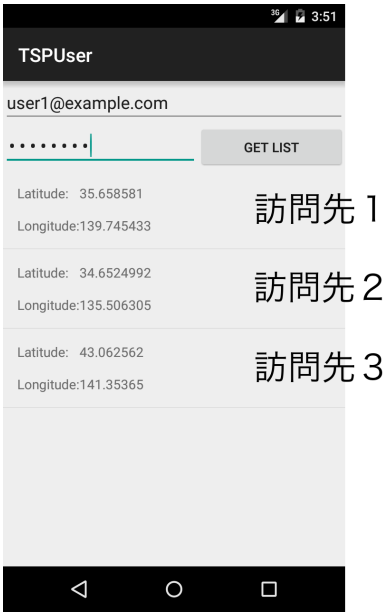

図 4 訪問先のリスト
Fig. 4 List of targets to be visited.

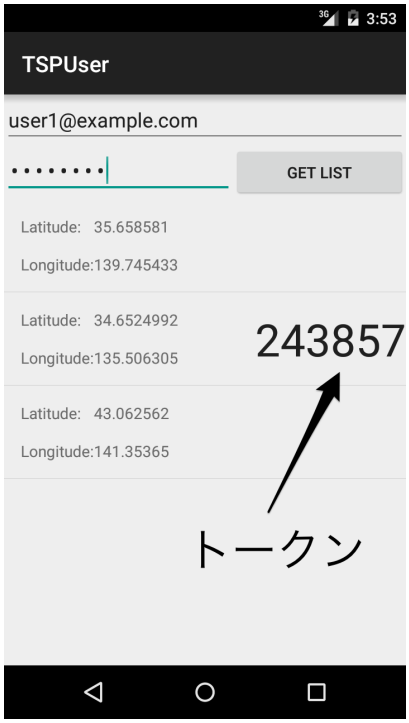

図 5 トークンの表示
Fig. 5 Token sent from the visitor authentication server.

ションは，起動するとトークンの入力を求められる．訪問者から提示されたトークンを入力すると，訪問者認証システムから対応する訪問者の情報を受信し，画面に表示する（**図 6**）．住人はこれを対象の訪問者と比較して訪問者認証を行う．試作システムではトークンを 6 桁の数値として実装している．

3.3 想定する利用シーン

訪問者の所属組織は，訪問者認証システムへあらかじめ訪問者の名前と顔写真，訪問先の住所を登録しておき，訪問者に対して訪問する住所と訪問理由の対を登録しておく．また，訪問者に対して訪問者用アプリケーションを配布し，使用方法の教育を行い，このシステムについて住人へ伝達を行っておく．住人は，あらかじめ本提案の Android アプリケーションを Google Play ストアなどの信頼できるアプリケーション配信サービスからインストールしておき，操作方法について習得しておく．アプリケーションは，訪問者の所属組織のウェブサイトからリンクされているものをインストールすることで，不正なアプリケーションのインストールを回避する．訪問者は事前に，訪問者用 Android アプリケーションにて住人の住所を選択してトークンを入手する．訪問者はインターホンを鳴らし，所属と氏名を告げてドアスコープ等にトークンを提示する（**図 7**）．その後，住人の操作中はドアスコープ等の前で顔が住人から見えるよう待機する．住人は住人用 Android アプリケーションを起動し，トークンを入力して対応する訪問者の情報を画面へ表示させる．もしトークンを入力しても訪問者の情報が画面に表示されない場合，つまり対応する訪問者の情報が存在せず，有効でないトークンを訪問者から受け取っている場合は，正規の訪問者でないと判断して訪問者を追い払い，訪問者認証を終了する．住人は Android アプリケーションにて対応する訪問者の情報を表示させることに成功した場合，ドアスコープ等から確認できる訪問者と，Android アプリケーションに表示されている訪問者の情報とを比較し，同一人物であると判断して，訪問理由も正当であると判断した場合はドアを開けて訪問者を迎え入れ，訪問者認証を終了する．訪問理由に不自然な点がある場合

図 6 訪問者情報の表示
Fig. 6 Visitor's identity.

図 7 ドアスコープを用いたトークンの提示
Fig. 7 Token shown via a door scope.

は，権限を悪用した訪問者であると判断して訪問者を追い払い，訪問者認証を終了する．それ以外の場合は訪問者を追い払い訪問者認証を終了する．

4. 議論

4.1 信頼できる電話帳

住人は提示されたトークンの正当性を確認する際に訪問者の所属組織と通信を行うが，(1) 信頼できる電話帳を用いて通信の接続先を特定し，(2) 接続確立後に対向が正当であることを確かめる必要がある．

(1) に関して，住人向けアプリケーションでは接続先をホスト名や URL の形で保持しており，提案方式では住人の住宅にインターネット接続可能な通信サービスがあるか，スマートフォン等により携帯電話網が利用でき，接続先を特定するための DNS 等が汚染されていないことを前提としている．訪問者は住人の環境を事前に十分調査し，悪意を持って準備し攻撃することでこの前提を破壊することができる．しかしながら，FTTH 等の固定回線と携帯電話網が併用可能な状況は多いと考えられ，より攻撃が困難な通信路を使ったり，両方の通信路で認証を行うことにより安全性を高めることが可能と言える．

(2) に関して，提案方式では (1) を前提とした上で SSL 証明書により接続先の正当性を保証する．携帯電話網のような特殊なネットワークの基地局を設置することなく，一般的なインターネット通信を利用する場合，事実上この方法に限定されると言える．本研究で対象とするような訪問者の所属組織は，公的な機関であるか，それに準ずる企業であることが想定されることから，EV SSL 証明書に限定することで安全性をより高めることが可能である．

4.2 住人によるトークンの再利用

提案方式では，訪問先ごとに異なるトークンを発行し，提示された住人はそれを用いて直ちに認証を行い，当該トークンが無効化されることを前提としている．しかし，住人が悪意を持って，トークンを認証に用いないままこれを保存した場合，近隣の住宅に対してなりすましの攻撃を行う余地が生まれる．トークンに基づいて住人に表示される情報には，訪問者の顔写真を含めているため攻撃を防げるはずだが，安全性をより向上させる方法として，一定時間で自動的にトークンを無効化したり，訪問者が訪問完了を申告することで無効化する方法が考えられる．

4.3 トークンの紛失

訪問者がトークン発行済みであり，未訪問状態のスマートフォンを第三者に盗用された場合，訪問者になりすまして訪問先で悪用される可能性がある．第 4.2 章で述べたように，住人はトークンに紐付いた訪問者の顔写真から，悪用を防ぐことができるはずだが，安全性をより向上させるために，スマートフォンからトークン発行サーバへの通信はクライアント側の証明書で暗号化し，スマートフォンを紛失した場合は速やかに所属組織に連絡することで，クライアント側の証明書を無効化する方法が考えられる．

4.4 トークンと紐付ける情報

トークンと紐付ける情報として必須事項になるものは，訪問者の名前，訪問者の顔写真，住人の位置情報である住所，訪問者の訪問理由の 4 点である．次に必須事項となる理由を挙げる．

訪問者の名前は，個人を完全に特定する要素ではなく，個人の肉体と見ず知らずの人間が確認できるように関連付けられているわけではない．しかし，現在個人を識別するうえで日々人間が利用しているものであるため，住人の安心に繋がるのではないかと考えられる．訪問者の顔写真は，顔は人間の目で確かめることができる身体情報であり，変更することが難しいと考えられるため，認証の正答率に関

わる重大な要素の一つとして挙げた．住人の位置情報である住所は，他人の家と紐付けられたトークンを住人が発見することにより，トークンの使い回しによって他人の家へ訪問する，という不正な利用を防ぐことができる．訪問者の訪問理由は，家の外に設置されているメータの数値を読むのみの訪問であるのに，家の内部に入り込もうとする攻撃を牽制することができると考えられる．

以上の 4 点で，目の前にいる訪問者と訪問者認証システム上にある訪問者の情報との結びつきの確認ができるものと考える．他に考えられる情報として，所属組織での部署などが考えられるが，住人が確認した場合でも住人がどのような部署か理解できず，認証の合否に関わらないと考えたため，必須事項から除いた．その他に指紋や静脈を使った生体情報を，訪問者の情報として利用することが考えられるが，住人に特殊な機材が必要とされるため，必須事項から除いた．

4.5 複数の認証システム

提案方式では，所属組織と住人向けアプリケーションとの関係が一対一であるが，複数の所属組織がこのシステムを利用するようになった場合，住人向けアプリケーションにて住人に訪問者の企業を選択を行わせるのは，負担になる可能性がある．解決策として，トークンを情報量の多い二次元バーコードなどに決め，住人へ掲示するトークン自体に，認証システムを一意に決める URL などを載せるという方法が考えられる．

5. おわりに

本論文では，住人が不利益を被らないために不可欠な訪問者認証について，電話での認証より手間と時間が少なく，専用の装置を設置する必要がない新たなシステムについて提案した．提案方式では，訪問者があらかじめ訪問者認証システムを用いて，住人が所属組織に問い合わせるべき情報をトークンとして圧縮することにより，住人の負担と所要時間を削減した．また一般に普及しているスマートフォンを用いて，訪問者（所属組織）と住人がそれぞれ保有する通信路を用いて認証を行うため，特殊な機材やネットワークの敷設を必要としない．顔写真を添付できることにより悪意のある第三者による正規の訪問者へのなりすましを防ぎ，訪問者が組織を退職した場合も訪問者認証システムによりアカウントを失効させ，退職後のシステムの不正な利用を防ぐことができる．

今後の課題として，本論文の提案方式は，一つの所属組織が運用するシステムとして設計されているが，第 4.5 章で述べたように，複数の所属組織がこのシステムを利用するようになった場合，住人からすると訪問者の所属組織ごとにアプリケーションを使い分けなければならないことは，非常に不便である．eduroam や Shibboleth 認証では，複数の認証システムが連携して動作している．これらのシステムと同様に，複数の所属組織の訪問者認証システムを連携し，住人は一種類のアプリケーションだけで認証が行えるよう拡張していきたい．また，トークンを二次元バーコード等にして所属組織の情報を含め，住人用アプリケーションがカメラを用いて取り込むことが挙げられる．一般的に用いられているドアスコープやカメラ付きインターホン等で，二次元バーコードの送受信が行えるかを検証する．また，住人は電力会社等と契約していることから，事前にアカウント登録を行うことで，トークンを払い出した時に住人用アプリケーションへプッシュ通知するといった，更なる利便性の向上が可能であると言える．請求額確認や登録情報変更のため利用者にアカウント登録を求めている企業もあり，新規に作成する必要がない場合もある．第 3.1 章では，所属組織が訪問者によるサボタージュを検出できないことを述べたが，住人が事前にアカウント登録を行うことで，訪問者がトークンを検証できないよう改善できると考えられる．また，本論文では個人宅にいる住人を対象としたが，今後法人向けに追加の認証要素や，建物や部屋のセキュリティ区分なども考慮したシステムも考えていきたい．

参考文献

[1] 安 俊相，吉田 哲，宗本 順三：戸建住宅団地における独居高齢者の訪問者に対する不安感の研究，日本建築学会計画系論文集，Vol.74，No.638，pp.735–742，2009.
[2] 国立情報学研究所：eduroam JP - Home (オンライン)，入手先〈http://www.eduroam.jp/〉(参照 2015/08/09).
[3] 中井 誠樹：訪問者認証システム及びそれに用いる訪問者認証方法，入手先〈http://www.google.com/patents/WO2012164826A1?cl=ja〉，Google Patents，2012 (WO Patent App. PCT/JP2012/002,968).
[4] 籠田 将慶：訪問管理システム，および，その方法，特開 2008-009977，2008/1/17.
[5] 伊東 栄典，笠原 義晃，のぎ田 めぐみ，鈴木 孝彦：認証連携による無線 LAN ローミング環境 －九州大学における UPKI ・ eduroam の連携－，情報処理学会研究報告 マルチメディア通信と分散処理（DPS），Vol.2007，No.91(2007-DPS-132)，pp.141–146，2007.
[6] 清水 さや子，岡部 寿男，吉田 次郎：一般カードを使った一時利用者向け認証システムの設計と実装，情報処理学会論文誌コンシューマ・デバイス＆システム（CDS），Vol.3，No.1，pp.34–45，2013.
[7] 佐藤 聡，櫻井 孝一，吉田 健一，新城 靖：高度な利用者認証が利用可能なネットワークを対象とした柔軟なアクセス制御の一実装，情報処理学会論文誌，Vol.54，No.3，pp.1099–1108，2013.
[8] Shibboleth Consortium：shibboleth，入手先〈https://shibboleth.net/〉(参照 2015/10/31).