Vol.2019-MBL-93 No.28
Vol.2019-ITS-79 No.28
2019/11/22

FNACを用いた屋外IoT機器に対するFQDN自動生成法に関する検討

柳瀬 知広[1,a)]　鈴木 秀和[1,b)]

概要：IP ネットワークに直接繋がる IoT（Internet of Things）機器が普及し始めており，今後，IPv6 の利用機会が増加すると見込まれている．IPv6 アドレスが割り当てられた IoT 機器と通信する際，FQDN（Fully Qualified Domain Name）の利用が不可避になると考えられる．筆者らは IoT 機器情報に基づいて FQDN を自動生成する FNAC（Flexible Name Autoconfiguration）を提案してきた．しかし，利用する標準化プロトコルの制約上，FNAC は屋内 IoT 機器のみを対象としており，ホームネットワーク以外に設置された IoT デバイスに対しては FQDN を自動生成できない．本稿では FNAC を応用した屋外 IoT 機器の FQDN 自動生成法について検討する．

A Study on Automatic FQDN Generation Method for Outdoor IoT Devices Using FNAC

Tomohiro Yanase[1,a)]　Hidekazu Suzuki[1,b)]

1. はじめに

インターネット技術や各種センサー・テクノロジーの進化等を背景に，パソコンやスマートフォンなど従来のインターネット接続端末に加え，家電や自動車，ビルや工場など，世界中の様々なモノがインターネットへつながり，先進的なサービスを可能とする IoT（Internet of Things）が世界規模で注目を集めている．文献 [1] によると，インターネットにつながるモノ，IoT デバイスの世界で普及している数は 2015 年時で 154 億台であり，2025 年には 754 億台と爆発的に増加すると予測されている．

IoT サービスを実現するためには，現実世界をセンシングし，あらゆるデータをサイバー空間へ送信，蓄積し，AI（Artificial Intelligence）技術によりデータを分析する必要がある．このような IoT サービスを構成するセンサノードやウェアラブルデバイス，スマート家電などの IoT デバイスは，今後エッジコンピューティングの台頭によりインターネットに直接接続することが考えられる．これらの IoT デバイスには，通信を行うために IP アドレスが割り当てられるが，現在主流である IPv4 グローバルアドレスは枯渇状況にあるため，IoT デバイスの普及に対する方策として IoT 社会では，無尽蔵なアドレス空間を有する IPv6 アドレスを用いることが不可避となる [2].

IPv6 アドレスは従来の IPv4 アドレスよりアドレスサイズが大きく，アドレスの表記も IPv4 アドレスと比較して 16 進数で桁数が多いため，可読性が悪く，ユーザにとって扱いにくい．そのため，ユーザが IPv6 アドレスを利用する際には FQDN（Fully Qualified Domain Name）のようなユーザフレンドリな識別子を利用して通信や管理を行うことが一般的である．しかし，現在普及している多くの IoT デバイスは一般的に FQDN を動的に設定する機能を有していないため，ユーザ自身で IoT デバイスの FQDN を設定して DNS サーバへ登録する必要がある．そのため，今後，IoT デバイスの普及が進み，宅内や屋外に多くの IoT デバイスが設置されることを考えると，ユーザや管理者らが手動で FQDN を設定する行為は煩わしいものになる．

[1] 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
[a)] tomohiro.yanase@ucl.meijo-u.ac.jp
[b)] hsuzuki@meijo-u.ac.jp

筆者らはこれまで，“BRAVIA” のような機器のシリーズ名から機種や製造業者を特定することのできない一般ユーザを対象とし，IoT デバイスの仕様を変えることなく，IoT デバイスから得られる情報を基に FQDN を自動生成し，かつ設置場所に関する情報などを付与してユーザが機器を特定する際に認識しやすい表記に柔軟に変更可能な FNAC（Flexible Name Autoconfiguration）[3,4] を提案してきた．しかし，従来の FNAC はホームネットワーク内に設置された IoT デバイスを対象としており，インターネットに直接繋がる屋外 IoT デバイスに対して FQDN を生成することができない．

そこで，本稿では従来の FNAC の機能を拡張し，屋外 IoT デバイスに対して FQDN を自動生成する手法を検討する．既存の FNAC の機能を拡張し，その機能を有したサーバをインターネット上に設置することで屋外 IoT デバイスに対する FQDN の自動生成を実現する．

以下，2 章で既存研究とその課題，3 章で提案手法について述べる．4 章で提案手法の評価結果について示し，5 章でまとめる．

2. 既存研究

2.1 DNSNA

2.1.1 概要

DNSNA（DNS Name Autoconfiguration）[5] は，グローバルネットワークまたはローカルネットワークに存在する IoT デバイスの FQDN を動的に生成し，DNS サーバに登録するシステムである．**図 1** に IPv6 ネットワークにおける DNSNA システムの構成を示す．DNSNA では IoT デバイスに FQDN を自動で生成する機能を搭載する．

IoT デバイスはネットワークに接続すると，自身の IPv6 リンクローカルアドレスを生成し，ローカルリンク上に存在するルータに RS（Router Solicitation）メッセージを送信する．RS メッセージを受信したルータは，RA（Router Advertisement）メッセージをブロードキャストする．RA メッセージにはネットワークのドメイン情報が含まれているため，IoT デバイスは受け取った RA メッセージより IPv6 アドレスとモデル名や製造メーカを表す機器情報を利用した FQDN を自動生成する．その後，IoT デバイスは自動生成した IPv6 アドレスがネットワーク上で一意か確認するためにルータに対して DAD（Duplicate Address Detection）[6] を実施する．IPv6 アドレスの一意性が保証された後，IoT デバイスの FQDN を DNS サーバに登録するために，ルータは IoT デバイスに対して NI Query（Node Information Query）[7] を送信し，IoT デバイスの FQDN を問い合わせる．NI Query を受け取った IoT デバイスは，自動生成した自身の FQDN と IPv6 アドレスのペア情報が含まれた NI Reply（Node Information Reply）をルータに返信する．IoT デバイスの FQDN と IPv6 アドレスの情報

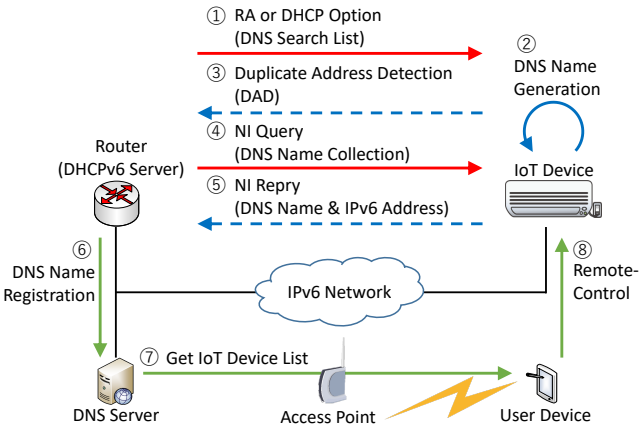

図 1 DNSNA のシステム構成
Fig. 1 The structure of DNSNA system.

を入手したルータは IoT デバイスが生成した FQDN の一意性を確認するために，DNS サーバに対して DNS Query を送信する．DNS サーバからの応答により FQDN が一意であることを確認できたら，DDNS（Dynamic Domain Name System）[8] の機能を利用し，IoT デバイスの FQDN と IPv6 アドレスのペアを AAAA レコードとして DNS サーバに登録する．

生成された FQDN は IoT デバイスの IPv6 アドレスと共に AAAA レコードとして DNS サーバに登録されるため，ユーザは FQDN を用いて宅外から IoT デバイスにアクセスすることが可能となる．

2.1.2 FQDN の構成

DNSNA における FQDN の構成は “`unique_id.object_identifier.OID.domain_name`” となる．“`unique_id`” は FQDN の一意性を保証するための識別子で，製品名の末尾にシーケンス番号を加えたものなどが使われる．“`object_identifier`” はデバイスの機器情報を表す識別子で，製造業社 ID，デバイスのモデル ID，シリアル ID，拡張 ID の 4 つの内容を組み合わせて構成される．“`OID`” は “`object_identifier`” が利用されていることを表す識別子である．“`domain_name`” は IoT デバイスが存在するネットワークのドメインを表す識別子である．

また，FQDN に位置情報を含めることも可能となっており，その場合の名前は “`unique_id.object_identifier.OID.mic_loc.mac_loc.LOC.domain_name`” となる．新たに追加された “`mic_loc`” はデバイスが存在する場所の詳細な箇所を示す識別子で，部屋の中央や淵といった内容が入る．“`mac_loc`” はデバイスが存在する場所を表す識別子で，キッチンやリビングルームといった部屋の名称であったり，道路であれば交差点などの内容が入る．“`LOC`” は “`mic_loc`” と “`mac_loc`” が利用されていることを表す識別子である．

2.1.3 課題

DNSNA はローカルネットワークだけでなく，グローバ

ルネットワーク上の IoT デバイスに対しても FQDN の自動生成を行うことが可能である．しかし，次に示す 2 つの課題が存在する．

(1) IoT デバイスと IPv6 ルータに機能追加が必要
IoT デバイスに DNSNA を実装し，かつルータにも NI Query を利用するために DHCPv6 サーバを兼ねたり，DNS サーバに Dynamic Update を行う機能を追加する必要がある．市販の IoT デバイスに対してユーザが機能追加することは不可能な場合がほとんどであり，DNSNA の標準化などの作業が必須になると考えられる．

(2) FQDN がわかりにくく，変更できない
FQDN の構成にはデバイスのシリアル番号などのユーザが通常意識しない情報が含まれており，ドメイン名が長くなってしまう．また，製造業社 ID から社名を判断することは困難であり，FQDN だけで IoT デバイスを特定できない場合がある．仮にユーザがわかりやすい FQDN に変更したとしても，IoT デバイスは DNSNA で定められている手続きに従って所定の FQDN を再度自動生成してしまう．そのため，ルータが再度自動生成された FQDN で DNS サーバの AAAA レコードを上書きして更新してしまうため，ユーザが設定した FQDN は解決できず，ユーザフレンドリではない．

2.2 FNAC

2.2.1 概要

FNAC は，IoT デバイスの仕様を変えず，デバイスから得られる情報を基に FQDN を自動生成し，かつ自動生成後の FQDN をユーザが認識しやすい形式に柔軟に変更可能な IoT デバイスのための FQDN 自動生成手法である．

図 2 にホームネットワークにおける FNAC のシステム構成と仕組みを示す．ホームネットワーク内に FNAC を搭載したホームゲートウェイ（HGW : Home Gateway）および ECHONET Lite [9] 対応スマート白物家電，DLNA（Digital Living Network Alliance）[10] 対応スマート黒物家電などの市販 IoT デバイスを設置する．DNS サーバはサービスプロバイダが提供している DDNS 対応 DNS サーバを利用する．また，ホームネットワークのドメイン設定はユーザ自身でドメイン名取得サービスを利用して設定を行う．

HGW は既存の IoT デバイスが採用している DLNA や ECHONET Lite などで定義されている機器探索メッセージ等を用いて IoT デバイスの機器情報を取得する．HGW は取得できた機器情報に基づいてホームドメインと組み合わせることで，ユーザが認識しやすい形式をした FQDN を自動生成し，DNS サーバへ動的に登録する．また，FNAC ではユーザが Web ブラウザで HGW にアクセスし，自動生成された IoT デバイスの FQDN を認識しやすい名前に設定することが可能である．

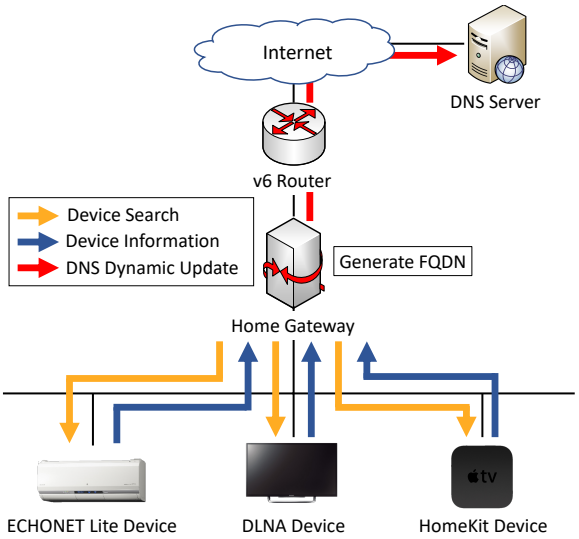

図 2 ホームネットワークにおける FNAC のシステム構成と仕組み
Fig. 2 A configuration and mechanism of FNAC system in home network.

2.3 FQDN の構成

FNAC における FQDN の構成は “unique_id.maker_name.location_name.home_domain” である．“unique_id” は，FQDN の一意性を保証するための識別子で，デバイスの型番やカテゴリ名に加えてシリアル番号の一部や通し番号などが付与される．“maker_name” はデバイスの製造メーカの名称を表す識別子である．“location_name” はデバイスが設置されている部屋名など場所を表す識別子である．“home_domain” はデバイスが存在するホームネットワークのドメインを表す．

FNAC の FQDN における “unique_id” と “home_domain” は必須の識別子であるが，“maker_name” と “location_name” はプロトコルによっては IoT デバイスから取得できない場合があるため省略することが可能である．

2.3.1 課題

従来の FNAC は IoT デバイスの各プロトコルで定められた機器探索を用いて，機器情報を取得し FQDN を自動生成している．これらのプロトコルはホームネットワークでの利用を想定しているため，ホームネットワークに接続していない屋外 IoT デバイスに対しては機器探索を用いての機器情報の取得を行うことが困難となり，FQDN を自動で生成することができない．そのため，屋外 IoT デバイスに対して FQDN を自動生成するための新たな方法を検討する必要がある．

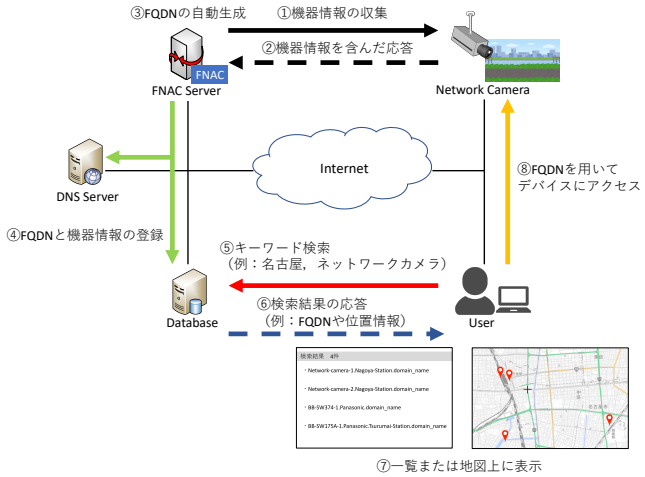

図 3　提案手法におけるシステム構成と仕組み

Fig. 3　A system configuration and mechanism of the proposed method.

3. 提案手法

3.1 概要

本稿では，屋外 IoT デバイスに対して FQDN を自動生成するために FNAC の機能を拡張する方法を検討する．前述の通り，インターネットに直接繋がる IoT デバイスに対して，IoT デバイスの各プロトコルで定義されている探索メッセージをマルチキャストし，機器情報を収集することは困難である．そのため，特定の IoT デバイスに対して直接機器情報を問い合わせ，収集する方法が必要となる．**図 3** に提案手法におけるシステム構成と仕組みを示す．インターネット上に設置された IoT デバイスに対して FQDN を自動生成するには FNAC の機能を有したサーバ（以下，FNAC サーバ）をインターネット上に設置する必要がある．また，ユーザが IoT デバイスに設定された FQDN を活用しやすくするために，インターネット上に機器の種類名や設置場所といった IoT デバイスの機器情報を登録することのできるデータベースを設置する．データベースには以下の項目を登録する．

- FQDN
- UUID（Universally Unique Identifier）[11]
- IoT デバイスの種類名
- 型番
- シリアル番号
- 製造業者名
- サービス（https など）
- ポート番号
- プロトコル（TCP または UDP）
- 位置情報
  - 市町村名
  - 番地
  - 設置場所名（建物名など）
  - 詳細な設置場所名（○階や○○部屋など）
  - 緯度
  - 経度
- ユーザ情報
  - ユーザ名
  - 組織名
  - 部署名
  - 電話番号
  - メールアドレス

FNAC サーバは特定の IoT デバイスに対して機器情報を要求し，IoT デバイスの機器情報を取得する．取得できた機器情報に基づいて，ユーザが認識しやすい形式をした FQDN を自動生成し，DNS サーバへ動的に登録する．この際，データベースに対しても IoT デバイスの FQDN および機器情報を登録する．

ユーザが IoT デバイスにアクセスする際には，データベースに登録されている機器情報を用いる．例えば，名古屋市に設置されているネットワークカメラにアクセスしたい場合には，「名古屋，ネットワークカメラ」とキーワードを用いて検索をする．データベースに一致する情報があった場合，該当する FQDN の一覧やネットワークカメラが設置されている場所を登録されている緯度と経度の情報を用いてマップ上に表示される．そこからアクセスしたい項目を選択することで，DNS サーバに対して FQDN を利用した正引きを行いネットワークカメラの IP アドレスを解決し，アクセスすることができる．

3.2 FQDN の自動生成と登録

図 4 に屋外 IoT デバイスに対する FQDN 自動生成および登録シーケンス図を示す．なお，FNAC サーバにはドメイン名が設定されているものとする．本稿では，インターネット上に存在する IoT デバイスに対して機器情報を収集する方法として，SNMP（Simple Network Management Protocol）[12] を用いた手法と IoT デバイスに筆者らが提案する独自プロトコルを搭載させる手法を検討する．

3.2.1 SNMP を用いた手法

FNAC サーバを SNMP マネージャ，IoT デバイスを SNMP エージェントとして構築する．IoT デバイスが所持する機器情報の集合体である MIB（Management Information Base）[13] 内のベンダー独自の管理情報を定義できる拡張 MIB には，IoT デバイスの機器情報が定義されている．

ユーザは FNAC サーバに監視対象とする IoT デバイスを登録する．FNAC サーバは登録された監視対象の IoT デバイスに対して，機器情報の取得要求を送信する．要求を受け取った IoT デバイスは機器情報を含んだ応答を FNAC サーバに返す．この際，FNAC サーバには過去に FQDN

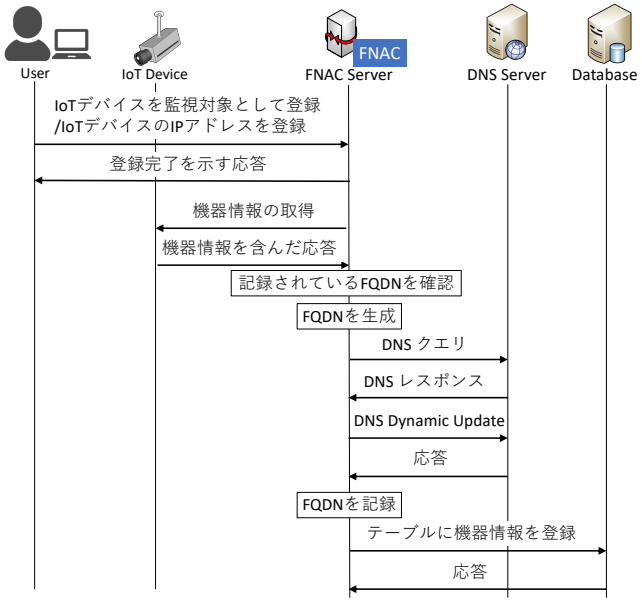

図 4 屋外 IoT デバイスに対する FQDN 自動生成および登録シーケンス

Fig. 4 Automatic FQDN generation and registration sequence for outdoor IoT devices.

を自動生成済みの IoT デバイスの IP アドレスと FQDN が記録されているため，この記録より FQDN が割り当て済みでない事を確認できれば，FNAC サーバは受信した機器情報を基に FQDN を自動生成する．

自動生成した FQDN がインターネット上で一意であるかを確認するために，FNAC サーバは生成した FQDN の AAAA レコードを DNS サーバに問い合わせる．DNS サーバからの応答で IPv6 アドレスが取得できなかった場合は自動生成した FQDN に重複がないということが確認できるため，IoT デバイスの FQDN と IPv6 アドレスのペアを DDNS の機能を使って DNS サーバに登録する．なお，DNS サーバからの応答で IPv6 アドレスが取得できた場合は自動生成した FQDN に重複があるため，FQDN が一意なものになるまで繰り返す．そして，自動生成した FQDN と IP アドレスを FNAC サーバに記録する．最後に，FNAC サーバはデータベースに自動生成した FQDN と取得した機器情報を登録する．

しかし，この手法は，IoT デバイスが SNMP プロトコルに対応している必要がある．

3.2.2 IoT デバイスに独自のプロトコルを搭載させる手法

3.2.1 で示した手法は，IoT デバイスが SNMP プロトコルに対応している必要がある．そこで，SNMP プロトコルに対応していない IoT デバイスに対して FQDN を自動生成する手法として，独自のプロトコルを IoT デバイスに搭載する方法を検討する．前提として，IoT デバイスは UUID や機器の種類名，メーカ名などの機器情報が記述された JSON ファイルを所有している．

ユーザはインターネット上に設置された IoT デバイスの IP アドレスを FNAC サーバに登録する．FNAC サーバは登録された IP アドレスをもとに IoT デバイスを特定し，機器情報の含まれた JSON ファイルを取得する．FNAC サーバは記録されている IP アドレスと FQDN の情報を確認し，FQDN が生成済みでなければ取得した JSON ファイルを解析，機器情報の抽出を行い FQDN を自動で生成する．以下のシーケンスは，3.2.1 と同様である．

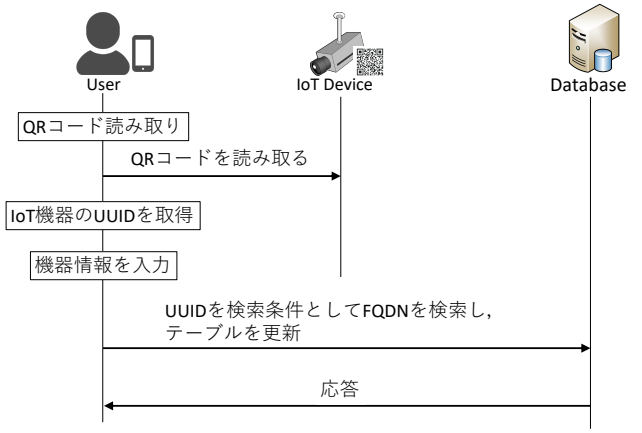

図 5 IoT デバイスの機器情報をデータベースに追加登録する際のシーケンス

Fig. 5 Sequence for additionally registering device information of IoT devices in the database.

3.3 IoT デバイスの機器情報の追加登録

図 5 に IoT デバイスの機器情報をデータベースに追加登録する際のシーケンス図を示す．この手法は，3.2.2 で FQDN 登録時に IoT デバイスの UUID が登録されていることを前提条件とする．また，IoT デバイスには UUID を埋め込んだ QR コードを所持させておく．

ユーザはスマートフォンやタブレットなどの端末で IoT デバイスが所持している QR コードを読み取り，IoT デバイスの UUID を取得する．次に，ユーザはデータベースに新たに追加したい設置場所名や所有ユーザなどの機器情報を入力する．この際，ユーザが所持する端末が位置情報の取得を許可していた場合，QR コードを読み取った場所の緯度，経度の情報を GPS から取得する．機器情報の入力完了後，UUID を検索条件としてデータベース内のテーブルを検索し，該当する IoT デバイスのレコードに追加情報を登録する．

4. 評価

4.1 アンケート調査による評価

筆者らは，2019 年 7 月 25 日から 8 月 2 日までの期間で，FNAC および DNSNA で自動生成された FQDN がユーザにとって IoT デバイスを特定可能なわかりやすい FQDN となっているかを明らかにするため，IoT デバイスの名前に関するアンケート調査を行った．本評価では，このアン

Vol.2019-MBL-93 No.28
Vol.2019-ITS-79 No.28
2019/11/22

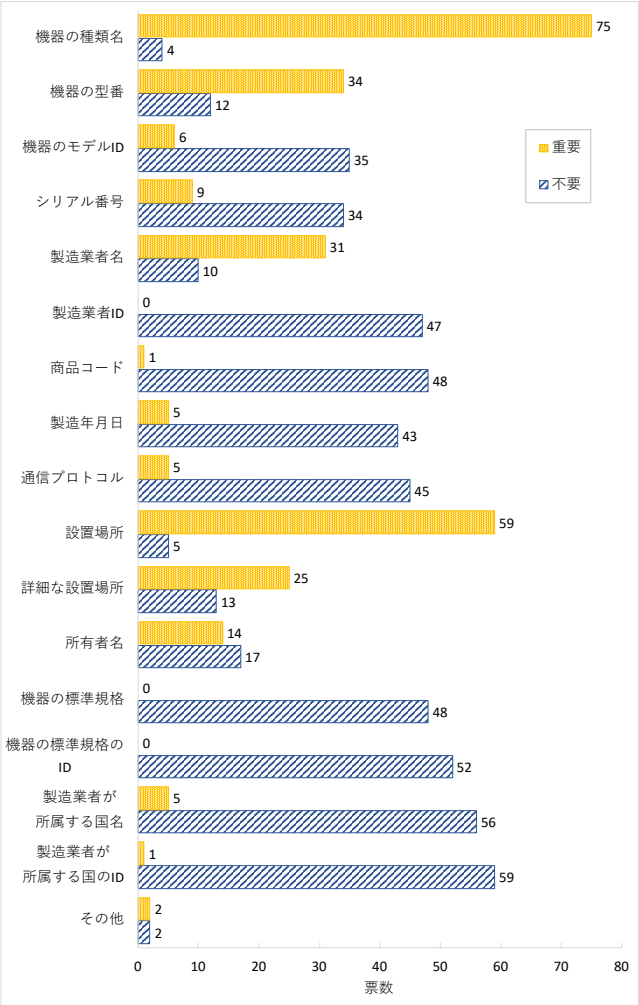

図 6 アンケート調査の回答結果
Fig. 6 Results of questionnaire survey.

ケート調査結果の一部を利用する．

4.1.1 調査内容

DLNA などの各プロトコルで取得できる機器情報に加え，DNSNA の FQDN に用いられる情報のリストを提示し，その中から回答者が IoT デバイスを特定するために重要または不要だと思う情報をそれぞれ複数選択する．

4.1.2 調査方法

アンケートを Google フォームで作成し，オンラインで調査を行った．なお，本アンケート調査は無記名式で行い，回答者の性別，年代および日常的な IoT デバイスを利用の有無を併せて確認した．

4.1.3 調査結果と考察

アンケートの有効回答数は 81 件で，回答者の内訳および回答結果は下記のとおりである．

- 男性：70 名，女性：11 名
- 20 代：56 名，30 代：12 名，40 代：9 名，50 代：4 名
- IoT デバイスの日常利用あり：男性 26 名，女性 8 名

図 6 にアンケート調査の回答結果を示す．回答者が IoT デバイスを特定するために重要視する情報として，機器の種類名や設置場所，型番や製造業者名といった直感的に機器を特定できる内容が上位に選ばれた．これらの 4 つの情報は FNAC における FQDN を構成する情報に全て含まれており，FNAC の FQDN はユーザにとって有用な FQDN であると言える．また，上位 4 つの情報に次いで詳細な設置場所や所有者名，シリアル番号が選ばれた．これらの情報は上位 4 つの情報と共に提案手法のデータベースで管理することの可能な情報である．そのため，提案手法を用いることでユーザが意識する情報から IoT デバイスを特定可能だと言える．一方，製造業者が所属する国や機器の標準規格，それらを表す ID などの情報は必要とされていないことがわかった．これらの ID は DNSNA における FQDN を構成する必須の識別子となっており，ユーザが直感的に IoT デバイスを特定しにくいことを意味している．

表 1 既存研究との比較
Table 1 Comparison with existing researches.

	DNSNA	従来手法	提案手法
IoT デバイスへの機能実装	×	○	△
グローバルネットワークでの名前解決	○	×	○

4.2 既存研究との比較

表 1 に提案手法と既存技術である DNSNA および従来の FNAC との比較を示す．2 章で述べた通り，DNSNA はグローバルネットワークを含めた IoT デバイスの制御を実現しているが，IoT デバイスへの機能が必須である．従来の FNAC は IoT デバイスのプロトコルにとらわれることなく，IoT デバイスの FQDN の自動生成を実現できるが，ホームネットワーク内でしか利用することができない．

提案手法では，FNAC サーバをインターネット上に設置することでインターネットに直接繋がる屋外 IoT デバイスに対して FQDN の自動生成を実現できる．また，FQDN を自動生成するために FNAC サーバが IoT デバイスの機器情報を収集する必要があり，SNMP に対応した IoT デバイスには機能の追加は必要ないが，SNMP 未対応の IoT デバイスには提案するプロトコルを搭載する必要がある．

5. まとめ

本稿では，FNAC を用いた屋外 IoT デバイスに対する FQDN の自動生成法を検討した．提案手法では，FNAC サーバをインターネット上に設置し，SNMP や提案するプロトコルを利用して IoT デバイスの機器情報を収集することにより，屋外 IoT デバイスに対する FQDN の自動生成が可能となる．また，インターネット上に IoT デバイスの機器情報を管理するデータベースを設置することで，ユーザは機器情報から IoT デバイスに設定された FQDN の検索が可能となり，FQDN を用いた機器制御を活用しやすくな

る．アンケート調査により，FNAC の FQDN およびデータベースで管理する情報にはユーザが意識する情報が用いられているため，機器の特定に貢献できることを示した．

今後は詳細な仕様を決定し，提案手法の実装を行う予定である．

参考文献

[1] IHS Markit: IoT platforms: enabling the Internet of Things, available from ⟨https://cdn.ihs.com/www/pdf/enabling-IOT.pdf⟩.
[2] 総務省：IPv6 によるインターネットの利用高度化に関する研究会 第四次報告書 〜IoT 時代を拓く新たな戦略〜，入手先 ⟨http://www.soumu.go.jp/main_content/000388694.pdf⟩.
[3] Yanase, T., Tanaka, H. and Suzuki, H.: Flexible Name Autoconfiguration for IoT Devices, *2018 Eleventh International Conference on Mobile Computing and Ubiquitous Network (ICMU)*, IEEE Computer Society, pp. 1–6 (2018).
[4] Yanase, T. and Suzuki, H.: Evaluation of Flexible Name Autoconfiguration for IoT Devices in IPv6 Network, *2019 IEEE The 8th IEEE Global Conference on Consumer Electronics (GCCE)*, pp. 925–929 (2019).
[5] Lee, K., Kim, S., (Paul)Jeong, J., Lee, S., Kim, H. and Park, J.-S.: A framework for DNS naming services for Internet-of-Things devices, *Future Generation Computer Systems*, Vol. 92, pp. 617–627 (online), DOI: https://doi.org/10.1016/j.future.2018.01.023 (2019).
[6] Moore, N.: Optimistic Duplicate Address Detection (DAD) for IPv6, RFC 4429, IETF (2006).
[7] Crawford, M., Fermilab and Haberman, B.: IPv6 Node Information Queries, RFC 4620, IETF (2006).
[8] Vixie, P., Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136, IETF (1997).
[9] ECHONET CONSORTIUM: ECHONET Lite, ECHONET CONSORTIUM (online), available from ⟨https://echonet.jp/spec_g/⟩.
[10] DLNA Allience: DLNA, available from ⟨https://www.dlna.org/⟩.
[11] Leach, P., Mealling, M. and Salz, R.: A Universally Unique IDentifier (UUID) URN Namespace, RFC 4122, IETF (2005).
[12] Case, J., Mundy, R., Partain, D. and Stewart, B.: Introduction and Applicability Statements for Internet Standard Management Framework, RFC 3410, IETF (2002).
[13] Presuhn, R., Case, J., McCloghrie, K., Rose, M. and Waldbusser, S.: Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), RFC 3418, IETF (2002).