情報処理学会論文誌　コンシューマ・デバイス＆システム　Vol.9　No.1　32–41 (Jan. 2019)

コンシューマ・システム論文

NTMobileを利用したECHONET Lite機器のセキュア遠隔制御システム

田中 久順[1,a)]　鈴木 秀和[1,b)]　内藤 克浩[2]　渡邊 晃[1]

受付日 2018年6月30日, 採録日 2018年11月14日

概要：ECHONET Lite はスマート家電や住宅設備を宅内から制御するための通信規格であり，宅外の操作端末からこれらの機器を直接制御することができない．本論文では，NAT 越えとエンドツーエンドの暗号化通信を実現する技術である NTMobile を応用することにより，既存サービスにおけるメーカの遠隔制御サーバを必要とすることなく，操作端末が宅外から宅内に存在する ECHONET Lite 機器を安心・安全に遠隔制御できるシステムを提案する．モバイルインターネット環境において提案システムの動作検証および性能評価を行った結果，ECHONET Lite の仕様で規定されたタイムアウト時間内に NAT 配下に設置された ECHONET Lite 機器を宅外から直接制御できることを確認した．

キーワード：ECHONET Lite，遠隔制御，エンドツーエンド通信

Secure Remote Control System for ECHONET Lite Home Appliances Based on NTMobile

Hisayoshi Tanaka[1,a)]　Hidekazu Suzuki[1,b)]　Katsuhiro Naito[2]　Akira Watanabe[1]

Received: June 30, 2018, Accepted: November 14, 2018

Abstract: ECHONET Lite is a communication standard for controlling smart home appliances and residential equipments from inside the house and these devices cannot be directly controlled from remote control devices. In this paper, we propose a secure end-to-end remote-control system based on NTMobile which is a technology to achieve NAT traversal and end-to-end encrypted communication. With the proposed system, the operating terminal can remotely control ECHONET Lite devices existing in the house from outside the house safely and securely without requiring a manufacturer's remote control server in the existing service. As a result of the operation verification and performance evaluation of the proposed system in the mobile Internet environment, we confirmed that ECHONET Lite devices installed under the NAT router can be directly controlled from outside the house within the timeout time specified by the ECHONET Lite specification.

Keywords: ECHONET Lite, remote control, end-to-end communication

1.　はじめに

わが国では 2014 年に「エネルギー基本計画」[1] が閣議決定され，2020 年までに日本国内の新築住宅の過半数で ZEH（Zero Energy House）の実現が要求されている．ZEH とは，宅内の消費エネルギーを，太陽光パネルなどによって発電されたエネルギーで賄うことで，宅内の総消費エネルギー量を実質 0 以下にすることが可能な住宅のことであり，省エネルギーや災害時の電力確保を実現することが可能となる．ZEH を実現させるためには，宅内の総エネルギー量を把握する必要があることから，効率的にエネルギーを管理・運用できるシステム HEMS（Home Energy Management System）が導入される [2]．宅内に設置された家電機器や住宅設備などから送信される情報を HEMS

1　名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University, Nagoya, Aichi 468–8502, Japan
2　愛知工業大学情報科学部
Faculty of Information Science, Aichi Institute of Technology, Toyota, Aichi 470–0392, Japan
a)　hisayoshi.tanaka@ucl.meijo-u.ac.jp
b)　hsuzuki@meijo-u.ac.jp

コントローラが受信することで，エネルギーの使用状況を数値やグラフにより可視化することができる．これにより，ユーザはエネルギーの使用状況を直感的に把握しやすくなり，省エネルギーに意識的に取り組めるようになることが期待されている．

日本における HEMS コントローラと家電機器間の通信規格には ECHONET Lite が採用されており，家電機器などの情報を収集するだけでなく，HEMS コントローラから ECHONET Lite 対応家電機器を制御することも可能である [3]．しかし，ECHONET Lite はホームネットワークでの利用を想定した通信規格であるため，宅外の操作端末から宅内の家電機器を直接制御することができない．

この課題を解決するために，ホームネットワーク内およびインターネット上に専用の装置を設置し，これらを利用することにより外出先から宅内の家電機器を遠隔制御する手法が提案されている [4], [5], [6], [7], [8], [9], [10]．ECHONET Lite 対応家電機器を製造している多くのメーカも同様のモデルを導入しており，ホームネットワークに設置されるホームゲートウェイ（以後，HGW と表記）とインターネットに専用のサーバ（以後，遠隔制御サーバ）が連携することにより，宅外から宅内の ECHONET Lite 機器を遠隔制御するサービスを展開している [11], [12], [13], [14], [15]．遠隔制御サービスは宅外から戸締りの確認や家電機器の電源をオフにしたり，帰宅前にエアコンを稼働させたりすることができるため，省エネルギーや防犯の実現，QoL（Quority of Life）の向上などにつながるものである．

一方で，メーカは遠隔制御サービスを提供するために遠隔制御サーバを安定して運用することが必須である．そのため，メーカのサポートが終了してしまうと，コントローラおよび家電機器が使用できる状態でも，ユーザは宅外から遠隔制御することができなくなる．また，宅外のコントローラが送信した制御メッセージは必ず遠隔制御サーバを経由し，その際にログとして蓄積されることもある．そのため，遠隔制御サーバがハッキングされてログ情報が流出してしまうと，時刻情報を含んだ家電機器の操作履歴からユーザの生活パターンを読み取ることが可能で，第三者に悪用される恐れがある．したがって，現在の遠隔制御システムはユーザのプライバシを侵害する危険をはらんでいるといえる．

筆者らは NAT 越え問題を解決し，エンドツーエンドの接続性と移動透過性を同時に実現できる技術として，NTMobile（Network Traversal with Mobility）を提案している [16], [17], [18]．NTMobile を導入することにより，端末間の通信経路に複数の NAT が存在したり，IPv4/IPv6 ネットワークが混在したりした場合でも相互接続性を実現できる．また，端末間の通信は UDP トンネルを利用して行われており，その通信内容は IP レベルで暗号化および認証されているため，第三者による通信内容の盗聴を防止したり，改ざんを検知したりすることができる．

そこで本論文では，NTMobile を応用することにより，宅内に設置された ECHONET Lite 機器を宅外から安心・安全に遠隔制御できるシステムを提案する．提案システムでは NTMobile の仕様を拡張することにより，ECHONET Lite プロトコルに対応させる．また，宅外の操作端末と宅内の ECHONET Lite 機器の通信を中継する装置として，RCA（Remote Control Agent）を宅内に設置する．操作端末は NTMobile を利用して RCA との間に UDP トンネルを構築し，ECHONET Lite 機器を制御するメッセージを暗号化 UDP トンネルを用いて転送する．これにより，ユーザはメーカの遠隔制御サーバを必要とすることなく，宅内に設置されている市販の ECHONET Lite 機器を宅外から遠隔制御することができる．提案システムのプロトタイプを Android タブレットと Linux PC に実装し，モバイルインターネット環境において既存の遠隔制御サービスと性能の比較評価を行った．

以下，2 章で既存の遠隔制御システムとその課題を示し，3 章で提案している遠隔制御システムの概要について述べる．4 章で提案システムの実装および評価について述べ，5 章でまとめる．

2.　既存の遠隔制御システム

ホームネットワークにおいて ECHONET Lite 機器を制御する場合，まずコントローラは宅内に存在する ECHONET Lite 機器を探索するため，機器探索パケットをマルチキャストで送信する．これを受信した ECHONET Lite 機器は，機器探索に対する応答メッセージをコントローラにユニキャストで返信する．コントローラは応答メッセージを受信することにより，ホームネットワークに存在する ECHONET Lite 機器を発見する．コントローラは発見した機器に向けて制御メッセージをユニキャストで送信することにより，ECHONET Lite 機器の制御が行われる．ここで，機器探索時に送信されるメッセージはローカルスコープアドレスを用いているため，外出先からホームネットワークに存在する ECHONET Lite 機器を直接探索することができない．

上記の課題を解決するために，一般的な遠隔制御サービスでは図 **1** に示すようにインターネット上に専用の遠隔制御サーバを設置し，ホームネットワークに設置する HGW と連携するシステムモデルが採用されている．本論文ではこのような既存の遠隔制御システムを遠隔制御サーバ利用方式と表記する．遠隔制御サーバ利用方式では，宅外のコントローラは ECHONET Lite で規定されている機器探索メッセージを直接送信することはせず，HTTPS などの Web 技術を用いて遠隔制御サーバにアクセスし，メーカが定義した独自の制御メッセージを送信する．遠隔制御サーバから HGW へ制御メッセージを渡す方法としては，

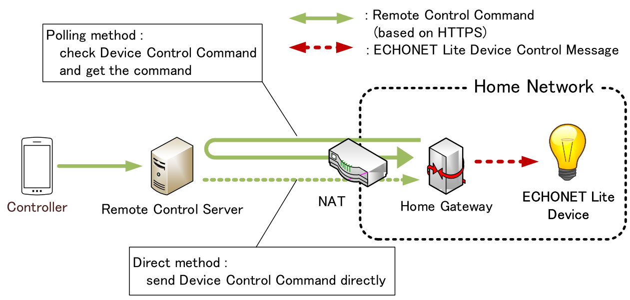


図 1　既存の遠隔制御システムの概要
Fig. 1　Overview of existing remote control system.

ホームネットワークのブロードバンドルータにポートフォワーディングを設定して遠隔制御サーバから直接送信する手法と，HGW が定期的に遠隔制御サーバにポーリングして蓄積された制御メッセージを取得する手法がある [19]．制御メッセージを入手した HGW はメッセージに従って ECHONET Lite による通信（機器探索や機器制御）を開始し，その応答を遠隔制御サーバ経由でコントローラに返す．

遠隔制御サーバ利用方式はコントローラからの制御メッセージがすべて遠隔制御サーバに届くため，メーカはユーザの操作履歴を取得することができる．これにより，遠隔制御時に問題が発生した際にログ情報から原因の特定を行うことが可能である．また，ログ情報を解析することにより，ユーザが主にどのような機器をどのように制御しているのかを知ることができるため，新製品の開発や新しいサービスの創出につなげることが可能になる．

しかし，ユーザは宅内では ECHONET Lite 対応のコントローラアプリケーション（以後，コントローラアプリ）を，外出先では Web ブラウザなどを利用したコントローラアプリを利用することになり，場所に応じてアプリケーションを使い分ける必要がある．メーカ側も 2 種類のコントローラアプリと遠隔制御サービスをそれぞれ提供する必要があり，開発コストの増加につながっている．また，メーカが遠隔制御サービスを終了してしまうと，ユーザは外出先から宅内の ECHONET Lite 機器をいっさい制御できなくなってしまうため，遠隔制御サーバの安定的かつ継続的な運用が求められる．さらに，ユーザの制御履歴が遠隔制御サーバに蓄積されると，そのログ情報が流出した際，第三者に悪用される恐れがある．これにより，ユーザの生活パターンが読み取られてしまい，プライバシの侵害や犯罪などにつながる懸念がある．

3.　提案システム

既存サービスの課題を解決するために，本論文では遠隔制御サーバ利用方式ではなく，外出先のコントローラと宅内の ECHONET Lite 機器をエンドツーエンドで接続するアプローチで遠隔制御システムを実現する．そこで，提案システムでは NAT 越えを実現する技術である NTMobile を利用する．

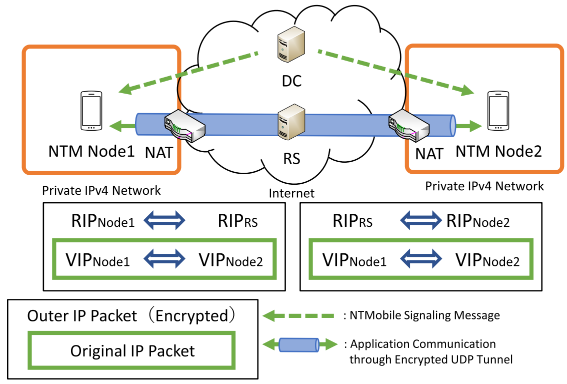


図 2　NTMobile におけるエンドツーエンド通信の概要
Fig. 2　Overview of end-to-end communication in NTMobile.

3.1　NTMobile の概要

NTMobile とは，実際のネットワーク環境に依存しない仮想的な IPv4/IPv6 アドレス（以後，仮想 IP アドレス）と，端末間に構築される UDP トンネルを用いた暗号化通信により，NAT 越えと移動透過性を実現する技術である．NTMobile を実装した端末（以後，NTM 端末）は起動時に DC（Direction Coordinator）に対して自身の IP アドレスを通知する制御メッセージを送信し，DC は NTM 端末との通信に利用するグローバル IP アドレスとポート番号を登録する[*1]．その後，NTM 端末は DC から仮想 IP アドレスを取得し，NTM 端末上のアプリケーションはこの仮想 IP アドレスを用いて通信を行う．

仮想 IP パケットを実ネットワークでルーティングするために，アプリケーションが通信相手 NTM 端末の名前解決を行う際の DNS 問合せをトリガとして NTMobile のトンネル構築シグナリングを開始する．シグナリング処理の際，DC は NTM 端末に対して通信相手のグローバル IP アドレスとポート番号を通知することにより，NAT の外側から通信相手 NTM 端末へ通信できる．DC は通信ペアとなる NTM 端末のネットワーク位置に基づいて，エンドツーエンド通信が可能な通信経路となるように両 NTM 端末にトンネル構築指示を行うことにより，UDP トンネルの構築および暗号鍵の共有を行う．これにより，通信経路上の NAT の影響を受けることなく，NTM 端末はエンドツーエンド暗号化通信を実現することができる．

なお，**図 2** のように NTM 端末が各々異なる NAT 配下に存在するときは，NTMobile の中継サーバである RS（Relay Server）を経由する．その際，双方の NTM 端末と RS 間で UDP トンネルが構築されるが，仮想 IP パケットを含むメッセージ部は NTM 端末間で暗号化されるため，RS

[*1] DC は受信した制御メッセージの送信元 IP アドレスとポート番号を登録する．そのため，NTM 端末が NAT 配下に存在する場合は，NAT 外側のグローバル IP アドレスとマッピングされたポート番号となる．

が通信内容を傍受することはできない．なお，NTMobile では経路最適化機能があり，これを適用すると異なる NAT 配下に存在する NTM 端末どうしであっても，RS を経由することなくエンドツーエンドで暗号化通信することが可能である [20]．

DC や RS はインターネット上に分散配置することが可能で，使用するアプリケーションやサービスに依存することがないため，NTMobile は高いスケーラビリティとフレキシビリティを兼ね備えたシステムとして運用することが可能である．

3.2　NTMobile 利用時の技術的課題と解決方法

NTMobile と ECHONET Lite を単純に組み合わせただけではまったく動作せず，提案システムを実現するうえで次の技術的課題を解決する必要がある．

課題 1：ECHONET Lite 機器への実装の制約

NTMobile でエンドツーエンド通信を行うには，両エンド端末に NTMobile を実装することが必須だが，ユーザが市販の ECHONET Lite 機器に NTMobile をインストールすることはできない．なお，NTMobile では Web サーバなど一般端末との通信に RS を利用することができるが，RS はどの端末からでもアクセスできるインターネット上に設置しなければならない．そのため，RS と ECHONET Lite 機器との間には必ず NAT が存在することになる．したがって，RS から ECHONET Lite 機器に対して通信を開始することができない．上記の点から，従来の NTMobile における構成装置だけでは市販の ECHONET Lite 機器への遠隔アクセスは実現できない．

課題 2：トンネル構築処理の開始条件

NTMobile は DNS 名前解決処理をトリガにトンネル構築を開始して，通信相手端末の仮想 IP アドレスを取得する．一方，ECHONET Lite では DNS の仕組みではなく，マルチキャストでホームネットワークに存在する ECHONET Lite 機器を探索する．したがって，従来の NTMobile を ECHONET Lite と単純に組み合わせても，NTMobile の機能はまったく動作しない．

これらの課題に対して，本論文では次のようなアプローチで解決する．

課題 1 の解決策：RCA の導入

ECHONET Lite のコントローラはスマートフォンやタブレットなどのモバイル端末を想定しているため，コントローラ側に NTMobile の機能を実装することは可能である．そのため，RS が ECHONET Lite 機器と同じホームネットワーク内に存在すれば，コントローラがその RS を介して一般端末である ECHONET Lite 機器と NTMobile の仕組みによりエンドツーエンド通信することができる．ただし，コントローラと RS 間にはホームネットワークを構成する NAT が存在するため，NAT 越え問題を解決する必要がある．

そこで宅内に設置する RS に NTM 端末の NAT 越え機能を追加することにより，RS をインターネット空間ではなくホームネットワークに設置しても宅外からアクセスできるようにする．さらにこの拡張した RS に ECHONET Lite 通信処理部を実装することにより，ECHONET Lite 機器との通信を仲介する機能を保持させる．本論文ではこの拡張した RS を RCA（Remote Control Agent）として定義する．

課題 2 の解決策：NTMobile の仕様拡張

まず，NTMobile を実装したコントローラが ECHONET Lite の機器探索パケットの送信をトリガとして，RCA 間でトンネル構築ができるように NTMobile のシグナリング開始条件を拡張する．ここで，トンネル構築後に ECHONET Lite 機器の仮想 IP アドレスをコントローラに提示する必要があるが，ECHONET Lite 機器は NTMobile を実装していない一般端末のため，仮想 IP アドレスは保持していない．そこで，RCA に複数の仮想 IP アドレスをプールさせ，RCA は発見した ECHONET Lite 機器のプライベート IP アドレスに対して未使用の仮想 IP アドレスを対応付ける．このアドレスの対応関係を記録するために，アドレス割当てテーブル AAT（Address Allocation Table）を定義する．これにより，従来の NTMobile における一般端末との通信スタイルと同じ仕組みで，宅外のコントローラから宅内の ECHONET Lite 機器へ通信を開始できる．

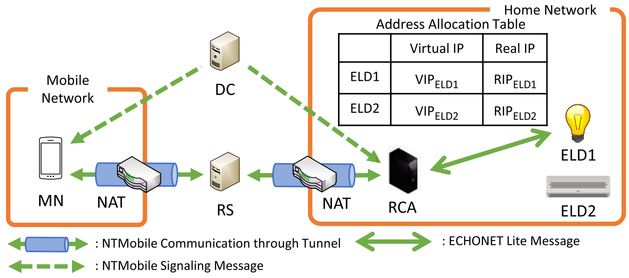


図 3　提案システムの概要

Fig. 3　Overview of the proposed system.

3.3　提案システムの概要

図 3 に提案システムの概要を示す．以後，NTMobile を実装したコントローラを MN（Mobile Node），操作対象となる宅内の ECHONET Lite 機器を ELD（ECHONET Lite Device）と表記する．また，端末 N の実 IP アドレス*2を RIP_N，仮想 IP アドレスを VIP_N と表記する．インターネット上には NTMobile プロバイダにより DC および

*2　接続しているネットワークから割り当てられる IP アドレス．

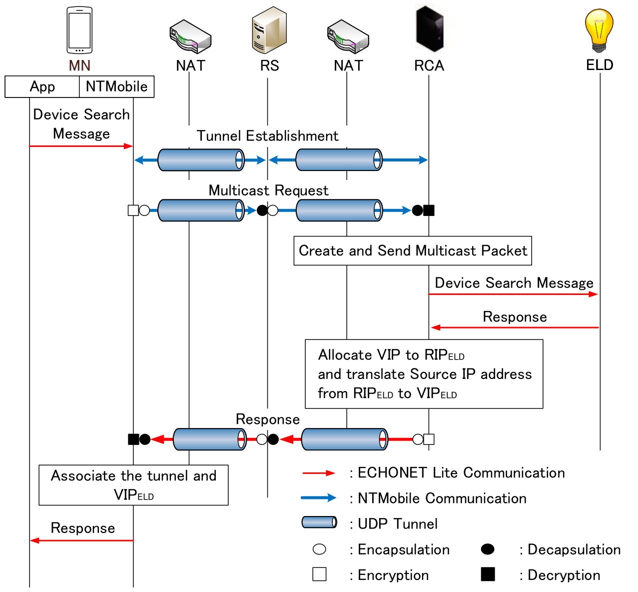


図 4　機器探索シーケンス
Fig. 4　Device search sequesnce.

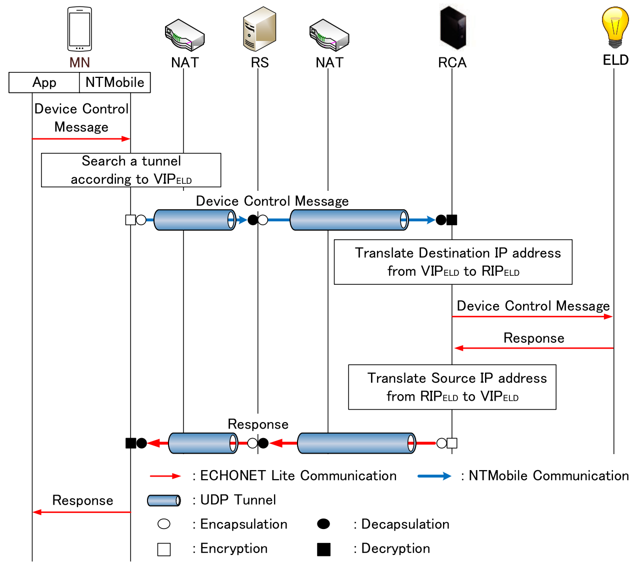


図 5　機器制御シーケンス
Fig. 5　Device control sequesnce.

RS が提供されているものと仮定し，MN はモバイルネットワークや滞在先の LAN など NAT 配下のネットワークに存在するものとする．また，MN と RCA は起動時に IP アドレスを登録する制御メッセージを DC へ送信し，DC は各 NAT のグローバル IP アドレスとポート番号を記録しており，仮想 IP アドレスが配布されているものとする．

このような環境下において，MN はホームネットワーク内にある RCA との間に暗号化 UDP トンネルを構築し，宅内の ELD を制御する際は RCA が割り当てた仮想 IP アドレス宛に制御メッセージを送信する．RCA は MN から受信した制御メッセージをデカプセル化および復号したあと，送信元 IP アドレスを VIP_{MN} から RIP_{RCA}，また宛先 IP アドレスを AAT に従って VIP_{ELD} から RIP_{ELD} に変換して転送する．応答メッセージは逆の手順で MN まで到達させることにより，既存システムで必須であった遠隔制御サーバを用いることなく，ECHONET Lite 機器の遠隔制御を実現する．

3.4　通信シーケンス

3.4.1　機器探索シーケンス

図 4 に機器探索の流れを示す．MN のユーザがコントローラアプリを起動して機器探索を行うと，コントローラアプリは機器探索メッセージを含んだマルチキャストパケットを生成する．MN はこのパケットを送信する前に，NTMobile のトンネル構築シグナリングを開始する．このとき，DC からの経路指示を受けて，MN と RS 間および RS と RCA 間でトンネルが構築され，以降，MN と RCA は RS を経由して通信を行う．

その後，MN は RCA にホームネットワーク内の ELD の探索を依頼するために，新たに定義する NTMobile の制御メッセージ Multicast Request を RCA に送信する[*3]．RCA は受信した Multicast Request を基に ECHONET Lite の機器探索メッセージ（送信元 IP アドレスは VIP_{MN}）を生成し，ホームネットワークにマルチキャストすることにより ELD の代理探索を行う．

ELD は機器探索メッセージを受信後，ECHONET Lite で制御可能な家電機器情報が含まれた応答メッセージを VIP_{MN} 宛に返信する．RCA は ELD からの応答メッセージを代理で受信すると，構築済みのトンネルを用いて MN に転送する．このとき，RCA は複数所持している仮想 IP アドレスの中から未使用のアドレスを探索時に得た各 ELD の実 IP アドレス RIP_{ELD} に対応付け，AAT で管理する．その後，RCA は AAT に基づいて応答メッセージの送信元 IP アドレスを RIP_{ELD} から VIP_{ELD} に変換後，暗号化およびカプセル化してから MN へ送信する．

MN はカプセル化された応答メッセージを受け取るとデカプセル化および復号の処理を行う．このとき，MN は RCA との間で構築した UDP トンネルを VIP_{ELD} 宛のパケットを伝送するために再利用するべく，MN が保持するトンネルテーブルを設定する．これにより，MN のコントローラアプリに発見した ELD の IP アドレスとして VIP_{ELD} が通知される．

3.4.2　機器制御シーケンス

図 5 に機器制御の流れを示す．MN は制御したい ELD を選択して制御を開始すると，VIP_{ELD} を宛先として ECHONET Lite 機器の制御メッセージを送信する．このとき，MN では宛先 IP アドレス VIP_{ELD} をキーとして

[*3] NTM 端末と RCA がトンネルを構築する際に NTMobile の Tunnel Request/Response の制御メッセージを交換しており，そのチャネルを利用することにより，NAT を越えて RCA まで送信することができる．

トンネルテーブルを検索し，機器探索時に構築した暗号化 UDP トンネルの情報を取得する．その後，MN は機器制御メッセージを暗号化，カプセル化して RCA に送信する．

RCA はカプセル化された機器制御パケットを受信した後，パケットのデカプセル化および復号処理を行う．その後，RCA は AAT に従って宛先 IP アドレスを VIP_{ELD} から RIP_{ELD} に変換し，機器制御パケットを ELD に転送する．機器制御メッセージに対する ELD からの応答メッセージ（宛先 IP アドレス VIP_{MN}）は，再度 RCA で送信元 IP アドレスを RIP_{ELD} から VIP_{ELD} に変換し，暗号化およびカプセル化して MN へ転送する．MN は応答メッセージを取得後，コントローラアプリに渡す．

以上により，遠隔制御サーバを中継することなく，宅外のコントローラからホームネットワークに設置された ECHONET Lite 機器を遠隔制御することができる．

4. 実装・評価

4.1 実装

従来の NTMobile を拡張し，MN と RCA のプロトタイプ実装を行った．

4.1.1 MN のプロトタイプ実装

図 6 に MN のモジュール構成を示す．MN はモバイルデバイスを想定しているため，NTMobile の実装には root 権限が不要な VpnService 利用型 NTMobile [21] を利用した．コントローラアプリからマルチキャストされる機器探索メッセージを検知できるように，VPN API を利用したルーティングテーブルの設定とパケット判断モジュールの拡張を行った．また，NTMobile トンネルサービスは機器探索メッセージを受け取ると，あらかじめ設定された RCA に対して UDP トンネルを構築後，機器探索メッセージの情報を基に Multicast Request を生成して送信する機能を追加した．なお，ECHONET Lite の制御メッセージの暗号化/復号およびカプセル化/デカプセル化処理は従来の NTMobile の機能をそのまま利用した．

4.1.2 RCA のプロトタイプ実装

図 7 に RCA のモジュール構成を示す．従来の RS および NTM 端末のモジュールを組み合わせて RCA デーモンを開発した．RCA デーモンには，Multicast Request を受信した際，ECHONET Lite の機器探索メッセージを生成し，ホームネットワークにマルチキャストする機器探索機能を実装した．また，ELD の実 IP アドレスと仮想 IP アドレス間のアドレス変換には Linux 標準の NAT 機能である Netfilter を利用するため，iptables によるアドレス変換ルールの追加を行った．複数の仮想 IP アドレスを保持し，ECHONET Lite 機器に仮想 IP アドレスを動的に割り当てるため，AAT を実装した．

なお，ELD が送信する VIP_{MN} 宛の応答メッセージを RCA が代理受信するために RIP（Routing Information

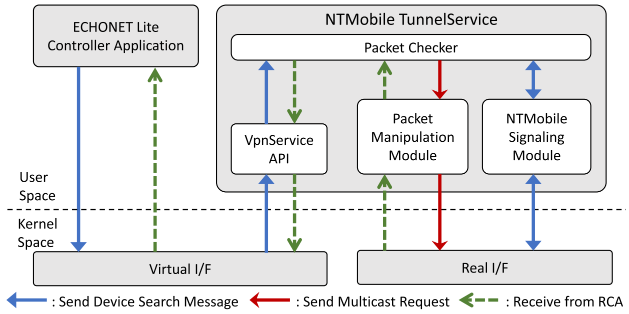


図 6　MN のモジュール構成
Fig. 6　Module structure of MN.

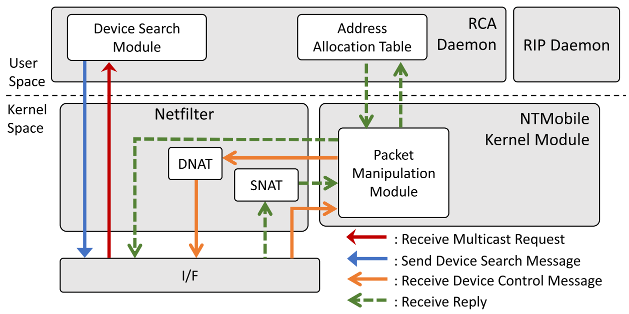


図 7　RCA のモジュール構成
Fig. 7　Module structure of RCA.

Protocol）デーモンを起動させた．RIP デーモンにより，仮想 IP アドレス宛のパケットを RCA へ転送するよう記述された RIP Request が送信される．これをデフォルトゲートウェイであるブロードバンドルータが受信すると，RIP Request に則りルーティングテーブルに追加する．以降，ELD から VIP_{MN} 宛の応答メッセージは 1 度ブロードバンドルータに送られるが，その後，RCA へ転送されるようにした．

4.2 実験環境

図 8 に動作検証および評価実験を行ったネットワーク構成を，**表 1** に各装置のスペックを示す．DC および RS は Linux サーバとして VPS（Virtual Private Server）上に構築した．コントローラアプリとして「えねぽた」[*4]を利用し，ECHONET Lite 準拠の電文を MN から送信させた．MN は Android タブレット（Nexus 9，Android 7.0）を，RCA は Ubuntu 12.04 LTS をインストールした Intel 製のミニ PC（DN2820FYKH）を利用した．Nexus 9 は Wi-Fi モデルであったため，docomo 回線に接続している Android スマートフォンのテザリングを利用してインターネットに接続した．研究室 LAN をホームネットワークと見立て，ECHONET Lite 機器として東芝ライフスタイル株式会社製のエアコン 1 台（RAS-B806DRH）と HGW（HEM-GW26A）および RCA を設置した．

[*4] http://www.10fw.co.jp/enepota/

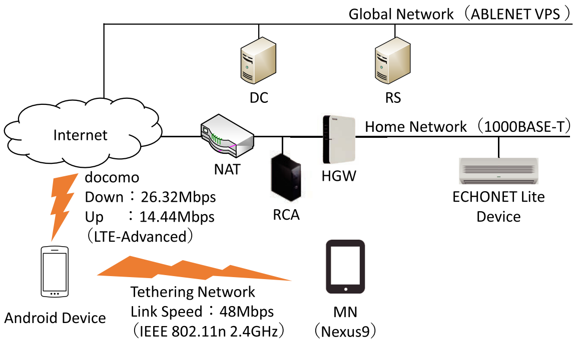


図 8　動作検証用ネットワーク構成
Fig. 8　Network configuration for operation verification.

表 1　各装置のスペック
Table 1　Device specifications.

	CPU	Memory
MN	NVIDIA Tegra K1 2.3 GHz	2 GB
RCA	Intel Celeron N2830 2.16 GHz	8 GB
DC	Virtual CPU 1 Core 3.3 GHz	512 MB
RS	Virtual CPU 2 Core 3.1 GHz	1,536 MB

4.3　提案システムにおける処理時間

提案システムにおける応答時間を明らかにするため，次の処理時間を測定した．

- トンネル構築処理：MN と RCA 間でトンネル構築が確立するまでに要した時間
- 機器探索処理：MN から ECHONET Lite 機器の探索を開始してからエアコンからの応答パケットを受信するまでに要した時間
- 機器制御処理：MN からエアコンの機器制御パケットを送信してからエアコンからの応答パケットを受信するまでに要した時間

MN 上で，各パケット送受信処理の直前にタイムスタンプを取得し，それらの差分を算出することによりパケットの送受信時間を解析した．なお，制御対象であるエアコンはリモコンで電源 OFF の状態とした．

表 2 に提案システムによりエアコンを 50 回遠隔制御したときの各処理時間を示す．平均値に着目すると，いずれの処理も短時間で完了することを確認した．このうち，トンネル構築処理は初めて機器探索を行うとき，または MN が別のネットワークへ移動して IP アドレスが変化した際に 1 回だけ発生する処理である．また，機器探索処理にかかる時間は最長でも約 3.3 秒で完了する．ECHONET Lite の規格書によると，制御メッセージを送信してから応答メッセージを受信するまでのタイムアウト時間は 5,000 [ms] と定義されている [22]．したがって，提案システムにより発生するオーバヘッドが ECHONET Lite 通信に悪影響を及ぼすことはなく，実際のモバイルインターネット環境においても問題なく動作することが分かった．

表 2　各通信処理における応答時間
Table 2　Response time in each communication process.

	Min. [ms]	Avg. [ms]	Max [ms]
Tunnel establishment	503.24	1,108.72	1,871.14
Device discovery	113.24	530.85	1,386.75
Device control	131.57	559.82	1,495.29

表 3　提案システムと既存サービスの遠隔制御時間の比較
Table 3　Comparison of remote control time between proposed system and existing service.

	Min. [ms]	Avg. [ms]	Max [ms]
Proposed system	200	543	1,264
Existing service	1,032	1,514	2,201

4.4　既存サービスとの比較評価

提案システムが既存サービスと比較してどの程度の時間で ECHONET Lite 機器の遠隔制御が可能かを評価するため，提案システムと既存サービスで機器制御を開始してからエアコンが制御されるまでの時間を比較した．既存サービスとして，東芝ライテック社から提供されている家電の遠隔制御サービスである「フェミニティ倶楽部」[11] を利用した．

既存サービスは HTTPS による通信を行っているため，機器制御パケットとその応答パケットを完全に特定することが困難なため，パケットキャプチャによる応答時間を算出できない．そこで，各手法による機器制御の様子を撮影し，機器制御を開始した時点からエアコンが反応した時点の差分から，機器制御に掛かる時間を算出する．なお，動画は Android スマートフォンを利用し，フレームレートを 30 fps，保存形式を MP4 として撮影を行った．

表 3 に提案システムと既存サービスの機器制御にかかる時間を 10 回ずつ測定した結果を示す．提案システムの結果はすでに MN と RCA 間にトンネルが構築されている状態であるが，表 2 のトンネル構築処理が平均 1 秒程度で完了することを考慮しても，両者を比較した結果，提案システムは既存サービスと同等以上の性能が得られることが分かった．

4.5　既存システムとの定性評価の比較

既存システムでは遠隔制御サーバが停止またはサービスが終了した際，宅外からの制御ができなくなることに加え，複数の家庭において同様の問題が発生する．提案システムでは，コントローラと RCA が直接通信を行うため，既存システムのような課題は発生しない．また，提案システムでは，コントローラアプリは宅内用のものをそのまま利用すればよく，宅外用アプリケーションへの切替えが不要になり，メーカ側も宅外用アプリケーションを開発する必要がなくなる．提案システムで利用されるサーバは NTMobile 通信全般で使用され，遠隔制御サービス以外の用途にも利

用可能である．そのため，既存システムのように遠隔制御専用サーバを開発して運用することが必須でなくなる．以上より，提案システムはユーザの管理外となる機器やサービスの影響を受けず，かつ従来よりプライバシの観点で優れているといえる．

宅内への遠隔制御を実現するうえで必要となるセキュリティ機能の1つとして，ユーザ認証がある．既存システムでは，遠隔制御サーバにおいてユーザ認証やアクセス制御機能を実装しており，認証されたユーザ以外から遠隔制御できない仕組みとなっている．提案システムの基盤となっているNTMobileでは，文献[23]において通信開始時にユーザ認証を行う機構を導入している．パスワード認証方式とOpenID認証方式の2種類が存在し，認証に失敗した場合はNTMobileの通信自体が行えない仕組みとなっている．また，文献[24]のアクセス制御機能をRCAに導入することにより，特定のNTM端末のみRCAとトンネル構築およびトンネル通信を許可したり，その他の端末からの通信を拒否したりするなどの制御を容易に設定することができる．したがって，提案システムは既存システムと同様，ユーザ認証およびアクセス制御を実現することが可能である．

4.6　VPN利用方式との比較

一般的な宅内へのリモートアクセス手法として，VPN（Virtual Private Network）がある．VPNを利用することによりECHONET Lite機器の遠隔制御を実現することは技術的に可能ではあるが，機器探索に関するマルチキャストパケットを伝送するためにはL2-VPNのように同一サブネットに参入するタイプでなければならない．または，L3-VPNであってもマルチキャストルーティングをサポートする必要がある．しかし，VPN関係のパケットを宅内に設置するVPNゲートウェイに転送するよう，ブロードバンドルータにポートフォワーディングの設定が必須となる．そのため，ユーザはVPNゲートウェイのIPアドレスおよびVPNパケットのポート番号を把握しなければならない．また，IPsecとL2TPを利用する場合は，IPsecパスルーなどの設定も必要となる．

また，メーカがECHONET Lite機器の遠隔点検や遠隔診断を行うようなサービスを行う場合，VPNを利用するとメーカがECHONET Lite機器以外の端末にもアクセスすることができてしまう．ファイアウォールを導入してアクセス制御することで解決可能だが，一般的に宅内機器はDHCPにより動的にIPアドレスが設定されていることを考慮すると，専門知識を持たない一般ユーザが動的に割り当てられるIPアドレスを把握してフィルタリングルールを設定することは敷居が高い．

これに対して，提案方式はブロードバンドルータに対してRCAへのポートフォワーディングの設定は必要ない．また，文献[24]のアクセス制御を実現する際のルールは，IPアドレスではなく固定のFQDNを採用している．そのため，提案システムはVPN利用方式と比較して，専門知識がない一般ユーザでも導入がしやすいと考えられる．

4.7　残された課題

提案システムではNTMobileが普及し，ユーザがDCやRSなどのNTMobileサーバ群を利用できる環境を想定している．そのため，NTMobileの可用性の有無が提案システムの実現にとって重要になる．文献[24]において，NTM端末に対して通信制御機能を導入している．この機能をDCなどのサーバ側にも導入することにより，不正なユーザからのアクセスを拒否したり，特定のユーザのみをアクセスを許可したりすることができる．また，文献[25]ではVRRP（Virtual Router Redundancy Protocol）を利用することにより，RSの二重化および障害発生時に高速フェイルオーバを実現する手法を提案している．文献[26]ではZabbixを利用したNTMobileサーバ群の統合的管理システムを検討しており，インターネット上に分散配置されたDCやRSなどのNTMobileサーバ群が安定かつ継続的に動作しているか監視することが可能で，高負荷なサーバにトンネル構築処理や通信中継処理が集中しないように分散させるタイミングを把握することが可能になると考えられる．

一方，DCはDNSサーバとしての役割も担っているため，通常のDNSサーバと同様にマスターとスレーブを構築し，冗長化することを想定している．複数台のDCを地理的，ネットワーク的に異なる場所に配置してダイバーシティを確保することにより，可用性を向上させることができる．また，DNSの可用性を維持するための仕組みをDCにも応用することができると考えられる．たとえば，複数のDNSサービスプロバイダを利用して権威DNSサーバを分散配置することにより，あるサービスプロバイダのDNSサービスが停止になったとしても，別のサービスプロバイダのDNSサービスが利用できれば，完全なサービス停止を回避することができる[27]．

今後はNTMobileサービスを提供するプロバイダが複数登場することを想定し，NTMobileのダイバーシティを実現するために異なるDCを利用する仕組みを検討し，検証することが必須である．さらに，StarBED [28]などを利用して大規模環境における負荷実験などを行うことにより，NTMobileの高可用性の検証を行うことが必要と考えられる．

5.　まとめ

本論文では，NTMobileを応用して宅外から宅内に存在するECHONET Lite機器を直接遠隔制御できるシステムを提案した．また，実際のモバイルインターネット環境に

において動作検証および性能評価を行った．その結果，提案システムはメーカが運用する専用のサーバを利用せず，既存の遠隔制御サービスとほぼ同じ応答時間でECHONET Lite機器を直接遠隔制御できることを確認した．

提案システムはECHONET Lite以外のプロトコルにも適応できるように設計されているため，今後はUPnP（Universal Plug and Play）やHomeKitなどに対応した機器を遠隔制御できるか検証を行っていく．

謝辞　本研究は平成28年度公益財団法人内藤科学技術振興財団研究助成金を受けて実施したものである．

参考文献

[1] 経済産業省資源エネルギー庁：エネルギー基本計画，経済産業省（オンライン），入手先 ⟨http://www.enecho.meti.go.jp/category/others/basic_plan/pdf/100618honbun.pdf⟩（参照 2018-07-07）．

[2] 株式会社富士経済広報部：HEMS・MEMSの国内市場を調査，株式会社富士経済（オンライン），入手先 ⟨http://www.group.fuji-keizai.co.jp/press/pdf/150218_15016.pdf⟩（参照 2017-05-10）．

[3] エコーネットコンソーシアム：ECHONET Liteの概要(2015). 入手先 ⟨https://echonet.jp/wp/wp-content/uploads/pdf/General/Standard/ECHONET_lite_V1_12_jp/ECHONET-Lite_Ver.1.12_01.pdf⟩．

[4] 江坂直紀，安次富大介：スマート家電の遠隔制御技術，東芝レビュー，Vol.70, No.6, pp.23–26 (2015).

[5] Saito, S., Ishikawa, N. and Tsuchiya, Y.: Development of ECHONET Lite-Compliant Home Appliances Control System Using PUCC Protocols from Smart Devices, *2015 IEEE 39th Annual Computer Software and Applications Conference*, Vol.3, pp.200–204 (2015).

[6] 田添宏治，南　圭祐，川添博史，安次富大介，会津宏幸：IoT機器開発を簡単化するクラウド集約型遠隔制御システムの提案，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.6, No.1, pp.1–10 (2016).

[7] 森下太一郎，中村雅也，三木一浩：シャープのHMSクラウドプラットフォーム，シャープ技報，Vol.109, pp.9–12 (2015).

[8] Kawazoe, H., Ajitomi, D. and Minami, K.: Design and evaluation of large-scale and real-time remote control architectures for home appliances, *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, pp.820–825 (2015).

[9] Papadopoulos, N., Meliones, A., Economou, D., Karras, I. and Liverezas, I.: A Connected Home Platform and Development Framework for smart home control applications, *2009 7th IEEE International Conference on Industrial Informatics*, pp.402–409 (2009).

[10] Sumino, H., Ishikawa, N., Tsutsui, H., Ochi, H., Nakamura, Y. and Uchida, Y.: Home Appliance Control from Mobile Phones, *2007 4th IEEE Consumer Communications and Networking Conference*, pp.793–797 (2007).

[11] 東芝ライテック株式会社：フェミニティ倶楽部，東芝ライテック株式会社（オンライン），入手先 ⟨http://feminity.toshiba.co.jp/feminity/⟩（参照 2018-07-07）．

[12] ニフティ株式会社：スマートサーブ，ニフティ株式会社（オンライン），入手先 ⟨http://smartserve.nifty.com/⟩（参照 2018-07-07）．

[13] ダイキン工業株式会社：ダイキンスマートアプリ，ダイキン工業株式会社（オンライン），入手先 ⟨http://www.daikinaircon.com/app/smart_app⟩（参照 2018-07-07）．

[14] パナソニック株式会社：スマートHEMS，パナソニック株式会社（オンライン），入手先 ⟨https://sumai.panasonic.jp/chikuden/smarthems/⟩（参照 2018-07-07）．

[15] 富士通株式会社：My Cloudエコ，富士通株式会社（オンライン），入手先 ⟨http://azby.fmworld.net/mycloud/apps_top/eco-dx/⟩（参照 2018-07-07）．

[16] 鈴木秀和，上醉尾一真，水谷智大，西尾拓也，内藤克浩，渡邊晃：NTMobileにおける通信接続性の確立手法と実装，情報処理学会論文誌，Vol.54, No.1, pp.367–379 (2013).

[17] 内藤克浩，上醉尾一真，西尾拓也，水谷智大，鈴木秀和，渡邊　晃，森香津夫，小林英雄：NTMobileにおける移動透過性の実現と実装，情報処理学会論文誌，Vol.54, No.1, pp.380–393 (2013).

[18] 上醉尾一真，鈴木秀和，内藤克浩，渡邊　晃：IPv4/IPv6混在環境で移動透過性を実現するNTMobileの実装と評価，情報処理学会論文誌，Vol.54, No.10, pp.2288–2299 (2013).

[19] 一色正男，河口俊朗，平原茂利夫：広がる東芝ネットワーク家電“フェミニティ”シリーズ，東芝レビュー，Vol.60, No.4, pp.23–27 (2005).

[20] 納堂博史，鈴木秀和，内藤克浩，渡邊　晃：NTMobileにおける自律的経路最適化の提案，情報処理学会論文誌，Vol.54, No.1, pp.394–403 (2013).

[21] Takayuki, Y., Hidekazu, S., Katsuhiro, N. and Akira, W.: IP Mobility Protocol Implementation Method Using VpnService for Android Devices, *Proc. 9th International Conference on Mobile Computing and Ubiquitous Networking*, Vol.2016, No.16, pp.1–2 (2016).

[22] ECHONET CONSORTIUM: ECHONET Lite, ECHONET CONSORTIUM (online), available from ⟨https://echonet.jp/spec_g/⟩ (accessed 2018-07-07).

[23] 山田貴之，上野泰輔，鈴木秀和，内藤克浩，渡邊晃：VpnService型NTMobileシステムへのユーザ認証機能の導入，第78回全国大会講演論文集，Vol.2016, No.1, pp.489–490 (2016).

[24] 金松友哉，大久保陽平，山田貴之，鈴木秀和，内藤克浩，渡邊　晃：NTMobileにおける通信制御機能の提案と実装，電気学会論文誌C（電子・情報・システム部門誌），Vol.137, No.12, pp.1571–1579（オンライン），DOI: 10.1541/ieejeiss.137.1571 (2017).

[25] 井上　卓，鈴木秀和，内藤克浩，渡邊　晃：NTMobileにおけるRS-Nの高速フェイルオーバの検討，平成26年度電気・電子・情報関係学会東海支部連合大会 (2014).

[26] 木村友輔，柳瀬知広，田中久順，鈴木秀和，内藤克浩，渡邊晃：Zabbixを用いたNTMobileサーバ群の統合的管理の検討，平成30年度電気・電子・情報関係学会東海支部連合大会，No.L2-2 (2018).

[27] 高嶋隆一：権威DNSサービスのダイバーシティ，DNSOPS.jp BoF（オンライン），入手先 ⟨https://dnsops.jp/bof/20171130/20171130-dnsops-takasima-v2.pdf⟩（参照 2018-09-24）. Internet Week 2017.

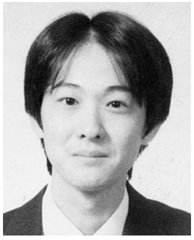
[28] 国立研究開発法人情報通信研究機構：StarBED4，入手先 ⟨http://starbed.nict.go.jp/⟩（参照 2018-09-12）．

田中 久順　（学生会員）

2017年名城大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科情報工学専攻修士課程に在学中．ホームネットワークに関する研究に従事．学士（工学）．IEEE会員．

鈴木 秀和　（正会員）

2004 年 3 月名城大学理工学部情報科学科卒業．2009 年 3 月同大学大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程修了．2008 年 4 月日本学術振興会特別研究員．2010 年 4 月名城大学理工学部助教．2015 年 4 月より同大学理工学部准教授および東北大学電気通信研究所共同研究員を兼務．ネットワークセキュリティ，モバイルネットワーク，ホームネットワーク等の研究に従事．博士（工学）．IEEE，ACM，電子情報通信学会各会員．



内藤 克浩　（正会員）

1999 年 3 月慶應義塾大学理工学部電気工学科卒業．2004 年 3 月名古屋大学大学院工学研究科情報工学専攻博士課程後期課程修了．2004 年 4 月三重大学工学部電気電子工学科助手．2007 年 4 月同大学助教．2011 年 9 月カリフォルニア大学ロサンゼルス校客員研究員．2014 年 4 月愛知工業大学情報科学部准教授．2016 年情報処理学会・長尾真記念特別賞受賞．無線ネットワーク，モバイルコンピューティングの研究に従事．博士（工学）．IEEE，電子情報通信学会各会員．

渡邊 晃　（正会員）

1974 年 3 月慶應義塾大学工学部電気工学科卒業．1976 年 3 月同大学大学院工学研究科修士課程修了．1976 年 4 月三菱電機株式会社に入社後，LAN システムの開発・設計に従事．1991 年 9 月同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティ等の研究に従事．2002 年 4 月名城大学理工学部教授．博士（工学）．IEEE，電子情報通信学会各会員．