Vol.2015-ITS-61 No.10
Vol.2015-CDS-13 No.10
2015/5/22

ビル設備向け遠隔サービスにおける ゲートウェイ装置の運用支援システム

川崎 仁[1,a)]　北上 眞二[1]　田畠 広泰[1]　追川 修一[2]

概要：M2M/IoT と呼ばれるシステムの活用が広がっており，ビル設備向けの遠隔サービスとして，使用電力量の見える化やデマンドレスポンスによる需給調整などへの関心が高まっている．これらのサービスを提供するために，ビル設備やビル設備コントローラなどのビル機器とサーバをゲートウェイ装置を介して接続し，ビル機器からのデータ収集，分析，ビル機器の制御を行うことが求められている．このようなシステムにおいては，ビル機器とサーバの接続を維持するために，ゲートウェイ装置の設置から運用中の設定変更に至るまで，ビル側での設定作業が必要となる．しかし，多数のビル機器をサーバと接続するためには，そのような運用上必要となる設定作業に精通したエンジニアを育成する必要があり，サービスの拡大において課題となる．本稿では，センタに運用支援サーバと鍵管理サーバを設置し，ゲートウェイ装置とサーバで事前に共有した鍵を用いて，運用上必要となる設定作業を支援する方式を提案した．提案方式を実装，評価し，ビル設備向け遠隔サービスを提供するシステムにおいて有効であることを示した．

1. はじめに

M2M (Machine-to-Machine) [1], [2], [3] あるいは IoT (Internet-of-Things) [4] と呼ばれるシステムの活用が広がっている．M2M/IoT を活用したシステムは，遠隔地にある多数のデバイスとセンタにあるサーバをネットワークを介して接続し，サーバがそれらのデバイスを制御することで，様々なサービスを提供する．M2M は ETSI[5] や oneM2M[6] などが標準を提案し，IoT については ITU-T[7] が勧告を出しており，いずれも基本的な構成は類似している．遠隔地にあるデバイスは，ゲートウェイ装置を介してあるいは直接，3G/LTE や xDSL/FTTH などのアクセスネットワークに繋がっている．センタには，それらのデバイスと通信をするサーバがあり，アクセスネットワーク経由でデバイスから情報を収集したり制御したりすることでサービスを実現する．この M2M/IoT を活用する分野として，自動車，制御システム，農業，コンシューマ機器，医療など，様々な産業が想定されている．

ビル設備向けの遠隔サービスにおいても，M2M/IoT を活用したシステムの構築が進められている．例えば，消費電力の見える化やデマンドレスポンスによる需給調整などのサービスが提供されている [8]．こうしたサービスを実現するためには，ビル設備が持つエネルギーデータを分析したり，分析した結果を元にしてビル設備を制御したりすることが必要である．このため，複数のビルとセンタをネットワークで接続し，データの収集やビル機器の制御を行うシステムを構築しなければならない [9]．

本稿では，このようなビル向けの遠隔サービスを対象として，ビル側のゲートウェイ装置とセンタ側のサーバを接続する場合のゲートウェイ装置の運用支援について検討する．ゲートウェイ装置とは，ビル設備やビル設備コントローラなどのビル機器とサーバを接続するためにビルに設置する装置であり，プロトコル変換などの機能によってビル機器とサーバの通信を中継する機能を有している．ビル機器とサーバの接続を開始し，維持するためには，両者の通信を中継するゲートウェイ装置について，その設置から運用中の設定変更に至るまで，ビル側での設定作業が必要となる．しかし，多数のビル機器をサーバと接続するためには，そのような運用上必要となる設定作業に精通したエンジニアを育成する必要があり，サービスの拡大において課題となる．そこで，我々は，ゲートウェイ装置の運用上必要となる設定作業を支援する運用支援システムを提案する．

2 章では，課題と提案方式を述べ，3 章では提案方式の実装を示す．4 章で性能を評価し，5 章で評価結果を考察

[1] 三菱電機ビルテクノサービス (株)
Mitsubishi Electric Building Techno-Service Co., Ltd.
7–19–1 Arakawa, Arakawa–ku, Tokyo 116–0002, Japan
[2] 筑波大学
University of Tsukuba.
1–1–1 Tennodai, Tsukuba, Ibaraki 305–8577 Japan
[a)] kawasaki.jin@meltec.co.jp

して提案方式が有用であることを述べる．6 章では，関連研究を示す．そして，7 章でまとめる．

2. 課題と提案方式

本章では，ビル設備向けの遠隔サービスを提供するシステムにおいて，ゲートウェイ装置とサーバを接続して運用する場合の課題を述べ，その後に課題を解決するために我々が提案する方式を述べる．

2.1 ビル設備向け遠隔サービス

ICT 技術の進歩と社会情勢の変化により，ビル設備向け遠隔サービスの提供が進められている．従来より，省エネルギーを実現するために，BEMS(Building Energy Management System) と呼ばれるシステムがビルに導入されてきた [10]．現在は，経済産業省が中心となって，エネルギー利用情報管理運営者（BEMS アグリゲータ）やエネルギーマネジメント事業者の取り組みを補助金で支援することも行われている [11]．

また，電力を安定供給することを目的として，従来よりスマートグリッドやデマンドレスポンスの取り組みが進められてきた [12], [13]．そうした取り組みの成果として，OpenADR と呼ばれるデマンドレスポンスを自動化する規格の整備が世界的に進んでいる [14]．OpenADR では，電力会社と需要家の間にアグリゲータと呼ばれる事業者が入り，電力会社からの節電依頼を元に需要家へ電力使用量の負荷分散をするなどの調整を行う．

さらに，ビルの多数を占める中小規模ビルにおいては，ビル内に追加の機器を設置することは，設置場所やコストの面で難しい場合が多い．そのため，センターに設置したサーバに情報を収集して，顧客に対しては，インターネット経由でサービスを提供することも行われている [15]．

このようなサービスは，次の理由からビル内で閉じたシステムだけでは実現することができない．まず，ビルで取得できるデータを分析したり，分析した結果を元にしてビル設備を制御したりすることが必要なためである．こうした処理は負荷が大きいためビル機器の様な比較的低スペックの機器で実現することが難しい．加えて，複数拠点を管理している管理者にとっては，遠隔にある複数のビルの情報をまとめて管理することが望ましい．複数のビルの情報をまとめるために，サーバにデータを収集することが求められる．そして，デマンドレスポンスのように，サービス提供の形態そのものが他のシステムと連携して動作することを前提にしている．

2.2 ビル設備向け遠隔サービス提供システム

本稿で対象とするビル設備向けの遠隔サービスを提供するシステムは，ビルに設置された機器とセンタに設置されたサーバ，そしてビルとセンタを繋ぐネットワークから成る．このシステムの構成図を**図 1** に示す．ビルの規模や提供するサービスによって違いはあるものの，一般的には次のとおりに構成される．

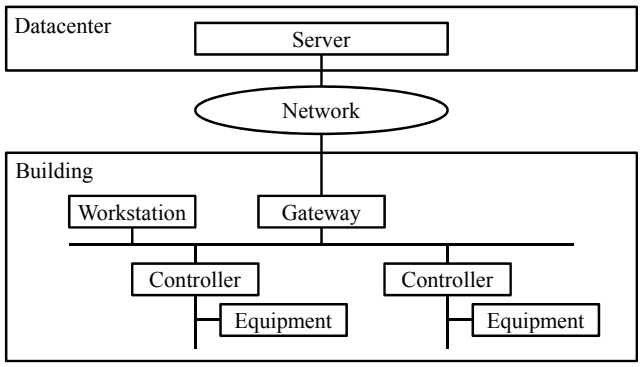

図 1 ビル設備向け遠隔サービス提供システムの構成図
Fig. 1 Overview of remote service for building device.

センタには，サービスを実現するためのサーバが設置されている．例えば，ビルに設置された機器と通信してデータ収集や機器制御を行うサーバ，収集したデータを蓄積する DB を搭載するサーバ，利用者が操作するための Web ページを提供するサーバなどがある．

ビルには，ビル設備とビル設備を制御し，管理するための機器が設置されている．ビル設備とは，空調機，照明設備，入退室管理設備などを指す．これらのビル設備を制御し，管理する機器をビル設備コントローラと呼ぶ．ビル設備は種類ごとにまとめられて，対応するビル設備コントローラにより管理されている．ビル設備とビル設備コントローラは，有線や無線などのネットワークで接続されている．

前述のとおり，ビル設備コントローラが種類ごとにビル設備を管理している．ビルには複数種類の設備があるため，全ての種類のビル設備を管理し，情報を集約するために中央監視装置が設置される．中央監視装置は，BACnet 等のネットワークでビル設備コントローラと接続されており，各ビル設備コントローラが収集したデータを集約したり，ビル管理者向けのビル設備管理画面を提供したりする．

センタとビルはネットワークにより繋がる．ネットワークとしては，一般に，3G/LTE などの無線通信や，xDSL/FTTH などの有線通信がある．このネットワークにより，ビル機器とサーバを接続する構成として，2 つのモデルがある．1 つは，デバイスとサーバを直接接続するモデルであり，もう 1 つは，デバイスとサーバの間に，通信を中継するゲートウェイ装置を置くモデルである．本稿では，ゲートウェイ装置を置くモデルを前提として議論を進める．なお，ゲートウェイ装置については，次節で取り上げる．

2.3 ゲートウェイ装置の機能と運用における課題

前節で，デバイスとサーバの間に，通信を中継するゲー

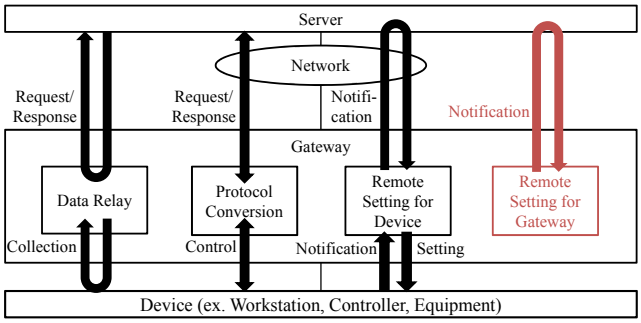

図 2 ゲートウェイ装置の機能
Fig. 2 Functions of gateway.

トウェイ装置を置くモデルを前提として議論を進めると述べた．本節では，ゲートウェイ装置の機能を**図 2** に従って述べる．

ゲートウェイ装置の機能として，(1) データ中継，(2) プロトコル変換，(3) デバイスの遠隔初期設定の支援が知られている [16]．

まず，データ中継機能とは，デバイスが保持しているデータを収集する機能である．ゲートウェイ装置でデータを中継するメリットとして，ゲートウェイ装置の配下に多数のデバイスが設置されている場合に，サーバがデバイスに対して 1 台ずつ収集するのではなく，ゲートウェイが集約してサーバに応答することで，負荷を低減できることが示されている．次に，プロトコル変換機能とは，サーバとデバイスとで対応するプロトコルが異なる場合に，ゲートウェイ装置がプロトコルを相互に変換することで，サーバとデバイスを接続可能にする機能である．ビル設備管理においても，ビルに設置されている全ての機器が，サーバのプロトコルに対応している訳ではない．全ての機器にサーバとのプロトコルに対応する改修を行うことは難しいため，プロトコル変換機能を搭載したゲートウェイ装置がプロトコルを変換することで，サーバと機器を接続できる．そして，デバイスの遠隔初期設定の支援機能は，多数のデバイスを一斉に導入する際の初期設定をゲートウェイ装置とサーバが連携して行うことで自動的に実行する機能である．

本稿では，前述の 3 つの機能に加えて，運用支援機能を挙げる．遠隔サービスを安定的に提供し続けるためには，据付から機能維持，撤去に至るまで，日々の運用を考慮しなければならない．ビル向け遠隔サービス提供システムを例にとると，まず，サービスの提供に先立って，ビルにゲートウェイ装置を設置し，ゲートウェイ装置とサーバが通信するための設定作業を行わなければならない．また，ネットワークの設定変更によりサーバと機器の接続に問題が生じた場合は，現地で情報を確認してサーバ側に反映しなければならない．

しかし，ビル設備管理の分野においては，ビル設備の据付，保守を担当するエンジニアは機械や電気を専門としている場合が多く，必ずしも ICT 技術に精通している訳ではない．そのため，遠隔サービスを安定的に提供するために実施するゲートウェイ装置の運用業務は，エンジニアにとって負荷となる．M2M/IoT を活用して，多数のビル機器をサーバと接続していくためには，エンジニアの負荷を低減していくことが必要である．エンジニアの負荷を低減するために作業を容易にしていくことが課題である．

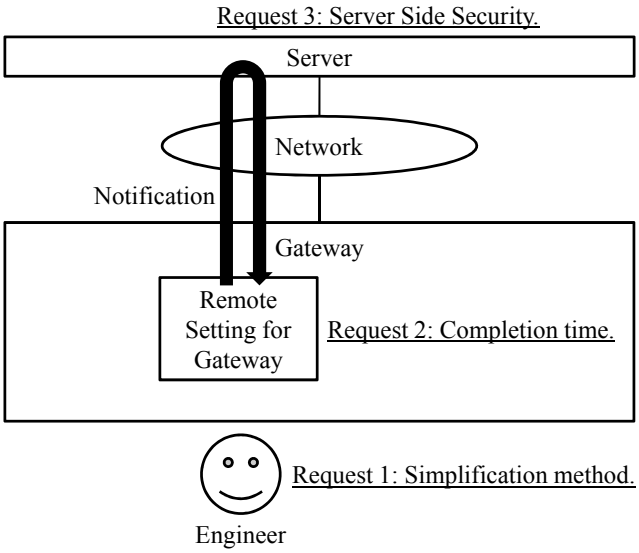

図 3 システムの要件
Fig. 3 Requirements of system.

2.4 システムの要件

本節では，前節で述べた，遠隔サービスを安定的に提供することを目的とした，ゲートウェイ装置の運用業務を容易にするためのシステム要件を述べる．

まず，検討にあたっての前提条件として，本稿では，エネルギーの見える化やデマンドレスポンスのようなサービスを提供することを想定している．これらのサービスにおいては，ビル外部の要求に基づいて，ビル設備の情報収集やビル設備の制御を任意の時点で実行する必要がある．したがって，処理の主体はセンタ側であり，通信の方向は，センタからビルに対する要求を送信する方向（つまり，センタからビルに対するポーリング）を想定する．また，センタの通信プロトコルには，広く用いられている HTTP と TCP/IP を利用する．HTTP およびその派生プロトコルはビル機器とのプロトコルにも採用されている他，M2M/IoT を実現するプロトコルとしても利用されているため，検討対象は多くのシステムを包含する．

2.4.1 要件 1

システムの要件の 1 つ目は，ゲートウェイ装置設置時のサーバとの通信設定作業を簡易化できることである．ビル設備向けの遠隔サービスを提供するためには，ゲートウェイ装置とセンタ側の装置との接続を有効にするための設定をしなければならない．例えば，センタに設置した装置からゲートウェイ装置にポーリングによる通信を行うために

は，センタ装置がゲートウェイ装置の IP アドレスを管理しておく必要がある．通信事業者のネットワークを利用する場合，ゲートウェイ装置の IP アドレスは，設置時まで分からない仕様となっていることが多い．そのため，遠隔サービスの立ち上げを行うエンジニアは，ビルでゲートウェイ装置の IP アドレスを確認してセンタ装置に設定し，その後にゲートウェイ装置とセンタ装置の通信が正常に行えることを確認するために通信試験を行う．上記の作業は，ビル設備やビル設備コントローラの据付と設定の作業に加えて行う必要があり，エンジニアにとっては現地作業における負担となっている．特に，ICT 技術に精通していないエンジニアにとっては負担が大きい．そこで，ゲートウェイ装置設置時とセンタ装置との接続を有効にするために行うネットワークの設定作業を，簡易化することが要件となる．

2.4.2 要件 2

2 つ目の要件は，稼働中に発生したネットワークの設定変更を一定の時間内にサーバへ反映することである．ビル向け遠隔サービスを安定的に提供するためには，ネットワークの設定変更によりセンタ装置とビル機器の接続に問題が生じた場合は，現地で情報を確認してセンタ側に反映しなければならない．例えば，ゲートウェイ装置に割り当てられる IP アドレスが変更されると，センタ装置から当該ゲートウェイ装置宛の通信がタイムアウトしてエラーとなり，サービスを提供できなくなる．通信エラーを検出すると，エンジニアが対象のビルを訪問し，ゲートウェイ装置の IP アドレスを確認して，再度センタ側に設定し，ゲートウェイ装置とサーバの通信が正常に行えることを通信試験により確認する．しかし，エンジニアが現地を訪問するためには一定の時間を要するため，サービスレベルを維持できない可能性がある．エネルギーの見える化では，30 分単位で使用電力量を表示することが一般的である．また，デマンドレスポンスは，電力会社からの節電依頼に応えるため，将来的に数分単位でビル設備を制御する可能性があるとされている．

2.4.3 要件 3

3 つ目の要件は，センタ装置のセキュリティを確保することである．近年，サイバー攻撃が増加すると共に，その手段も高度化していることが報告されている．M2M/IoT はビル機器とセンタ装置をネットワークで繋ぐため，サーバ機密性，完全性，可用性といった一般の情報セキュリティで考慮すべき事項も満足する必要がある．センタには，ビル設備やお客様の情報を蓄積しているため，サーバのセキュリティを確保することは重要な要件となる．特に，外部からの接続を受け付けるサーバについては，セキュリティを考慮する必要がある．

本稿では，上記の要件を満足する認証システムを提案する．

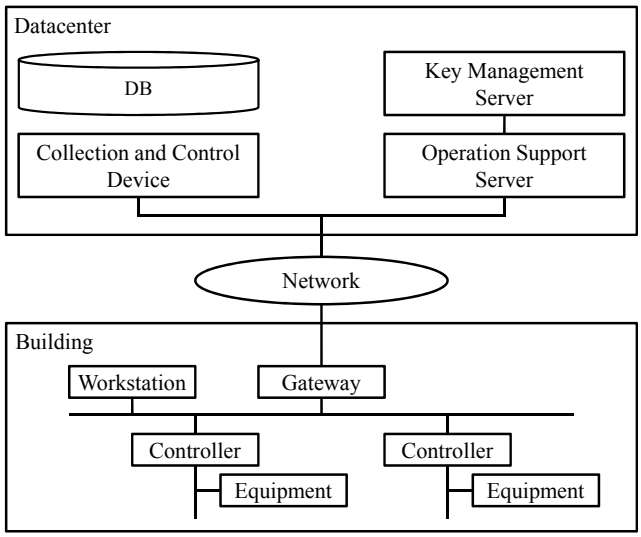

図 4 提案方式のシステム構成図
Fig. 4 Overview of the proposed system.

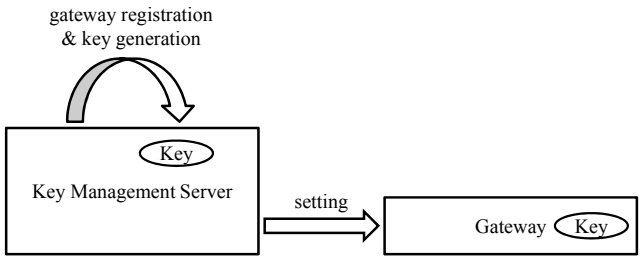

図 5 事前共有鍵の設定
Fig. 5 Setting of pre shared key.

2.5 提案方式

前節で述べた 3 つの要件を満足するために，本稿では，運用支援サーバを導入し，運用支援サーバとゲートウェイ装置で事前共有した鍵を用いた運用支援システムを提案する．

提案方式のシステム構成図を**図 4** に示す．提案方式のシステムでは，センタに 3 つの装置を設置する．収集制御クライアントは，ゲートウェイ装置に要求を送信し，ビル設備のデータを収集したり，ビル設備を制御したりする機能を提供するクライアントである．運用支援サーバは，ゲートウェイ装置からの通知を受信し，ゲートウェイ装置を認証し，ゲートウェイ装置の設定情報を記録するサーバである．鍵管理サーバは，ゲートウェイ装置と運用支援サーバで事前に共有する鍵データを生成し，管理するサーバである．鍵データの取得は，鍵管理サーバへ要求を送信して実行する．ゲートウェイ装置の情報や鍵の情報はデータベースに保存する．

遠隔サービスの運用者は，あらかじめ鍵管理サーバを用いて，ゲートウェイ装置の固有情報から鍵を生成する．ここでは，ゲートウェイ装置の MAC アドレスを固有情報として扱う．そして，生成した鍵を事前共有情報として，ゲートウェイ装置に設定する．鍵管理サーバによる鍵の生

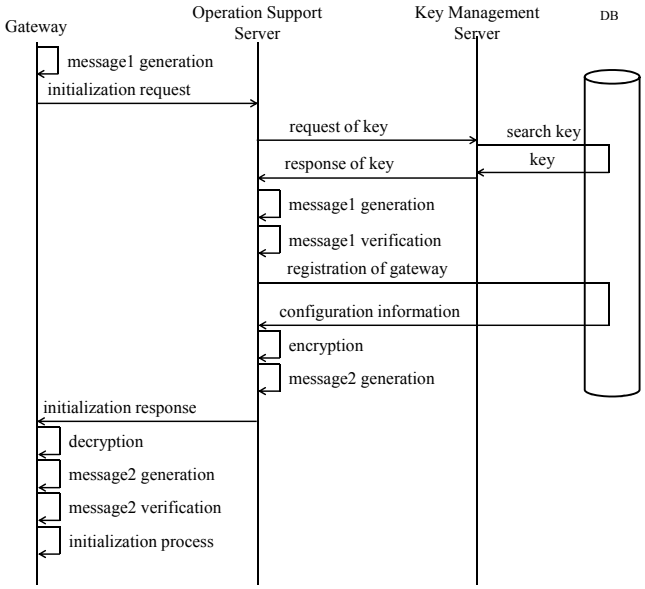

図 6 初期設定のシーケンス
Fig. 6 Sequence of initial setting.

成からゲートウェイ装置への設定までの一連の処理を**図 5** に示す.

提案方式の運用システムでは，ゲートウェイ装置とセンタ装置をネットワークで繋ぐために必要な設定を，ゲートウェイ装置から運用支援サーバに通知することで実現する．ビルにゲートウェイ装置を設置した際にゲートウェイ装置から初期設定を実行するためのシーケンスを**図 6** に示す.

2.5.1 ゲートウェイ装置 → 運用支援サーバ

まず，ゲートウェイ装置は，次の処理を実行する.

(1) メッセージ 1 生成：
事前共有鍵で固有情報と時刻情報を用いてメッセージ 1 を生成する.

(2) 初期設定要求：
メッセージ 1 と固有情報およびサーバに設定する情報を運用支援サーバに送信する.

2.5.2 運用支援サーバと鍵管理サーバ

次に，運用支援サーバと鍵管理サーバは，次の処理を実行する.

(1) 鍵要求と鍵応答：
事前共有鍵を鍵管理サーバに要求し，鍵管理サーバからの応答として事前共有鍵を取得する.

(2) メッセージ 1 生成：
事前共有鍵と固有情報と時刻情報を用いてメッセージ 1 を生成する.

(3) メッセージ 1 検証：
受信したメッセージ 1 と生成したメッセージ 1 を比較し，検証する.

(4) 登録要求と登録応答：
ゲートウェイ装置のネットワーク設定情報を登録する．また，ゲートウェイ装置に設定する必要のある情報を応答する.

(5) 暗号化：
ゲートウェイ装置に初期設定する情報を暗号化する.

(6) メッセージ 2 生成：
事前共有鍵で固有情報と時刻情報を用いてメッセージ 2 を生成する.

2.5.3 運用支援サーバ → ゲートウェイ装置

最後に，ゲートウェイ装置が次の処理を実行する.

(1) 初期設定応答：
ゲートウェイ装置が運用支援サーバから暗号化された初期設定情報とメッセージ 2 を受信する.

(2) 復号：
暗号化された初期設定情報を複合する.

(3) メッセージ 2 生成：
事前共有鍵で固有情報と時刻情報を用いてメッセージ 2 を生成する.

(4) メッセージ 2 検証：
受信したメッセージ 2 と生成したメッセージ 2 を比較し，検証する.

(5) 初期化処理：
複合した初期設定情報を反映する.

2.6 提案方式とシステム要件との対応

提案方式は，ゲートウェイ装置の設置時に，ゲートウェイ装置と運用支援サーバとの間で初期設定に必要な情報を交換するため，エンジニアがサーバへの設定作業を行う必要がない．したがって，ゲートウェイ装置設置時のサーバとの通信設定作業を簡易化することができるため，1 つ目の要件を満足する.

また，IP アドレスが変更されるといったゲートウェイ装置のネットワーク設定の変更が運用中に発生した場合であっても，初期設定と同様のシーケンスにより，変更された情報を通信支援サーバに通知し，センタで管理している設定情報を変更することができる．したがって，エンジニアがビルを訪問してゲートウェイ装置の設定を確認し，サーバの設定を変更するまでの処理に要していた時間に比べて，サーバへの設定反映までの時間を削減することができる．よって，2 つ目の要件である，設定変更から一定の時間内にサーバへの設定反映を完了していること，という点を充足する.

最後に，事前に共有した鍵とゲートウェイ装置固有の情報を入力としてメッセージを生成することで，運用支援サーバが，通知をあげてきたゲートウェイ装置が正当な装置であることを確認することができた．したがって，サーバのセキュリティを確保するという 3 つ目の要件を満たすことができる.

3. 実装

本節では，前節で述べた，運用支援サーバと事前共有した鍵を用いたゲートウェイ装置の運用支援システムの実装を述べる．

3.1 運用支援サーバ

運用支援サーバは，ゲートウェイ装置からの通知を受信して，認証し，通信設定の変更があれば適用する．運用支援サーバは，CPU が Intel Xeon E5-2603 1.80GHz，メインメモリが 4GB であり，OS として RedHat Enterprise Linux 5 系を利用して，Apache2.2 系，Tomcat5 系により構築した．

3.2 鍵管理サーバ

鍵管理サーバは，事前共有鍵の生成，鍵の取得の機能を提供している．他の装置は，鍵管理サーバに要求を送信して，それらの機能を実行することができる．運用支援サーバは，API を利用して鍵を取得して，ゲートウェイ装置の認証を行っている．仮想マシン上に構築し，CPU として Intel Xeon L5520 2.27GHz，メインメモリとして 3GB を割り当てた．OS には，RedHat Enterprise Linux 5 系を利用して，その上に Apache2.2 系，Tomcat5 系を利用して構築した．

3.3 収集制御クライアント

収集制御クライアントは，ゲートウェイ装置と通信を行って，ビル設備のデータ収集やビル設備の制御を要求する．本稿で対象とする遠隔サービスは，収集制御サーバからゲートウェイ装置に対するポーリングにより実現する．宛先であるゲートウェイ装置の IP アドレスは，運用支援サーバが保存した情報を参照して通信する．収集制御サーバは，CPU が Intel Core2 Duo P8400 2.26GHz，メインメモリが 4GB であり，Linux2.6.28 系の OS とその上で動作するアプリケーションにより実現した．

3.4 ゲートウェイ装置

ゲートウェイ装置は，ビル機器とサーバの間に設置し，相互の通信を中継する．ゲートウェイ装置は，Linux 上で JavaVM を実行しており，JavaVM 上で OSGi Framework を実行している．事前共有鍵をあらかじめ設定し，ゲートウェイ装置で実行するソフトウェアは，その事前共有鍵を取得して各処理を実行する．事前共有鍵による暗号化には AES 暗号を用い，メッセージの生成には HMAC-SHA を用いる．

表 1 通知処理の処理時間の測定結果
Table 1 Measurements of processing time on notice sequense.

	(1) – (3) [s]	(4) – (6) [s]	Total [s]
1st time	0.076	0.205	0.281
2nd time	0.072	0.164	0.236
average	0.074	0.185	0.259

表 2 鍵管理サーバの処理時間の測定結果
Table 2 Measurements of processing time on key management server.

	search key time [s]
1st time	0.078
2nd time	0.058
3rd time	0.071
average	0.069

3.5 ネットワーク

センタに設置した運用支援サーバと収集制御クライアントと，ビルに設置するゲートウェイ装置を繋ぐネットワークには，通信事業者が提供する有線ネットワークを利用している．通信速度は，最大 100Mbps のベストエフォートサービスである．運用支援サーバ，収集制御クライアント，鍵管理サーバは LAN で接続されている．

4. 評価

本章では，前章で実装を示した運用支援システムの性能を測定した結果を示す．

4.1 運用支援サーバの処理性能

運用支援サーバがゲートウェイ装置からの初期設定要求を受信してから，ゲートウェイ装置に応答を返すまでの処理時間を 2 つの区間に分けて計測した．1 つ目の区間（1）–（3）は，鍵管理サーバから鍵を取得して，メッセージ 1 を生成し，メッセージ 1 を検証するまでである．2 つ目の区間（4）–（6）は，鍵管理サーバにゲートウェイ装置を登録して，ゲートウェイ装置へ返す初期設定情報を暗号化し，メッセージ 2 を生成するまでである．

計測した処理時間の結果を**表 1** に示す．（1）–（3）は，平均で 0.074 秒であり，（4）–（6）は，平均で 0.185 秒であった．

4.2 鍵管理サーバの処理性能

他の装置からの要求に基づいて，鍵管理サーバが鍵を検索するのに要する時間を計測した．計測した処理時間の結果を**表 2** に示す．平均値は，0.069 秒である．

前節で示した運用支援サーバへの初期設定処理の処理時間の内，（1）–（3）の処理中に鍵管理サーバからの鍵の取得を行っている．したがって，鍵取得処理の処理時間が，（1）–（3）の処理の内の 93.2%を占めている．

5. 考察

本稿では，ビル設備向けの遠隔サービスを安定的に提供するために必要な運用を支援する方式を提案した．本章では，サーバの処理性能とシステムの有用性の 2 つについて考察した結果を述べる．

5.1 処理性能の考察

通信支援サーバへの初期設定処理の処理時間は，平均で 0.259 秒で完了している．稼働中に IP アドレスが変更された場合も，初期設定と同様の処理シーケンスを実行するため，処理時間もほぼ同じであると考える．

この結果から，本稿で対象としたビル設備向け遠隔サービスの安定した提供について考察する．IP アドレスが変更されると，センタ側装置からゲートウェイ装置に対するポーリングがタイムアウトしてエラーとなる．ここで，ゲートウェイ装置から運用支援サーバにネットワーク設定の変更を通知する．処理時間は，平均で 0.259 秒であり，人の体感からすると遅延なく反映される．

しかし，運用支援サーバへの通知が完了するまでの 0.259 秒の間，収集制御クライアントから通信ができない可能性があることには注意しなければならない．その区間に通信を行った場合でもサービスを安定して提供するために，収集制御クライアントにはリトライ処理を実装するなどの対応が必要である．

5.2 システムの有用性の考察

本節では，提案方式をビル設備向け遠隔サービス提供システムに適用する場合の有効性を議論する．

まず，本稿で提案した方式によって，遠隔サービスを提供するにあたって必要となるゲートウェイ装置の初期設定作業，稼働中のネットワークの設定変更作業を，サーバの安全性を確保した上で，ゲートウェイ装置が自律して実行できるようになる．本稿では，ゲートウェイ装置の運用を対象としたが，提案方式は，直接サーバと通信をするビル設備コントローラやビル設備に対しても適用可能である．

提案方式は，事前共有鍵を利用しており，ゲートウェイ装置が初期設定を開始するよりも前に，鍵をゲートウェイ装置へ設定しておく必要がある．設定するタイミングとしては，(1) 製造段階，(2) 事務所での事前作業段階，(3) ビルへの設置段階がある．(2) と (3) の段階で設置する場合，エンジニアの設定作業が生じるため，作業負荷を軽減するという観点では，(1) 製造段階で鍵を設定することが望ましい．

提案方式では，ゲートウェイ装置の IP アドレスが変更されたり，証明書の有効期限が切れた場合を想定して，サーバへ通知を行い，必要な設定情報を受信することで，収集制御装置とゲートウェイ装置の通信を維持できるようにしている．ゲートウェイ装置から運用支援サーバへの通知は，いつ，どの程度発生するか分からないため，運用支援サーバは十分な性能を確保しておかなければならない．また，災害時など，サーバとの通信が途絶えた状態であっても，ゲートウェイ装置は自律して動作を継続したい．このような要求を満足するためには，ゲートウェイ装置の機能を拡張し，自律的に処理を実行する仕組みが必要となる．

6. 関連研究

ネットワークカメラを対象として，動作に必要なプロファイル情報をネットワーク経由で設定する方式が提案されている [17]．この方式においては，暗号化処理に ID ベース暗号を用いており，マスターパブリックキーと機器固有の ID（サーバ：顧客 ID，ネットワークカメラ：MAC アドレス）から，対向機器の公開鍵を生成し，その公開鍵を用いてプロファイル情報を暗号化して対向機器へ送信している．本稿の提案手法の暗号化処理は，ID ベース暗号ではなく，より高速かつ一般的である AES 暗号による共通鍵暗号方式を用いている．AES は，ゲートウェイ装置と運用支援サーバ間で初期設定を行う際にデータを暗号化するために使用している．初期設定が完了すると，証明書がゲートウェイ装置に設定された状態となるため，以降は HTTPS による安全な通信を利用できる．また，この方式では，サーバから HTTP/POST によりネットワークカメラに初期設定を要求しており，サーバがネットワークカメラの IP アドレスを前提としている．一方，本稿では，ビルでの据付作業時に，ゲートウェイ装置からサーバに初期設定を行うことを前提としており，前提が異なる．

スマートデバイスの運用中にスマートデバイスが設定変更を検知すると，サーバへ変更を通知して新しい設定に対応するコンテンツを取得することを目的とした研究がある [18]．この方式においては，別のアクセスポイントに入ったことを設定変更の契機としており，SSID と MAC アドレスをスマートデバイスの属性 ID としている．別のアクセスポイントに入ると，サーバから暗号化された設定情報（機能制御ファイル/コンテンツ）を取得すると共に，属性 ID に対応する復号鍵を取得する．スマートデバイスは，取得した設定情報を復号，設定して利用する．本稿の提案手法は，事前に共有した鍵を用いて，ゲートウェイ装置側の設定情報をサーバにも通知する際にゲートウェイ装置の認証を行うと共に，ゲートウェイ装置に設定する情報の暗号化も行っている．

M2M/IoT において，遠隔地に設置したデバイスを管理するための標準仕様として，OMA-DM（Open Mobile Alliance–Device Management）[19] や BBF（Broadband Forum）の TR–069 CPE WAN Management Protocol[20] がある．これらの標準仕様の実装については，OSGi Alliance が標準化を行っており [21]，OSGi Release 6 が公開

されている [22]．本稿の提案手法を実現する上で，ゲートウェイ装置と運用支援サーバとの間の通信プロトコルに，これらの標準を利用することも可能である．本研究では，ビル設備向け遠隔サービスを提供する上で必要となる，ゲートウェイ装置の運用に着目して，要件を抽出し，その要件に対応するシステムを実装し，有効性を評価している．

7. まとめ

本稿では，ビル設備向け遠隔サービスを提供するシステムを対象として，ビルに設置するゲートウェイ装置の運用を支援するための運用支援システムを提案した．提案方式は，運用支援サーバをセンタに設置し，サーバとゲートウェイ装置にあらかじめ事前共有鍵情報を設定しておくことで，サーバのセキュリティも確保する．提案方式を実装し，その性能を評価して，提案方式の有用性を示した．今後は，ゲートウェイ装置だけでなくビル設備やビル設備コントローラにも対象を拡大し，運用を支援する方式の研究を進める予定である．

参考文献

[1] OECD: Machine-to-Machine Communications: Connecting Billions of Devices (2012).
[2] Geng Wu, Shilpa Talwar, K. J. N. H. and Johnson, K. D.: M2M: From Mobile to Embedded Internet, *IEEE Communications Magazine*, Vol. 49, No. 4, pp. 36–43 (2011).
[3] Kim Chang, Anthony Soong, M. T. and Xiang, Z.: Global Wireless Machine-to-Machine Standardization, *Internet Computing, IEEE*, Vol. 15, No. 2, pp. 64–69 (2011).
[4] Luigi Atzori, Antonio Iera, G. M.: The Internet of Things: A survey, *Elsevier Computer Networks*, Vol. 54, No. 15, pp. 2787–2805 (2010).
[5] ETSI: ETSI TS 102 690 V2.1.1 Machine-to-Machine communications (M2M); Functional architecture (2013).
[6] oneM2M: oneM2M Release 1 specifications (2015).
[7] ITU-T: Overview of the Internet of Things (2013).
[8] 小柳 隆，黒崎 淳，松浦友朋，潮田尚史，高橋雅仁，上野 剛，坂東 茂：オフィスビルを対象にしたデマンドレスポンス (DR) の実証試験，第 47 回空気調和・冷凍連合講演会講演論文集，No. 47, pp. 87–90 (2013).
[9] 野田 肇，関 義朗，飯野 穣：ビル群のエネルギー管理を実現する次世代の BEMS 技術 (2012).
[10] 柴 昇司：ビルエネルギーマネジメントシステム”FacimaBA-system BEMS” (2014).
[11] 経済産業省：BEMS・HEMS 補助金についてのお知らせ (2013).
[12] Albadi, M. H. and El-Saadany, E. F.: Demand Response in Electricity Markets: An Overview, *IEEE Power Engineering Society General Meeting*, pp. 1–5 (2007).
[13] Rahimi, F. and Ipakchi, A.: Demand Response as a Market Resource Under the Smart Grid Paradigm, *Smart Grid, IEEE Transactions on*, Vol. 1, No. 1, pp. 82–88 (2010).
[14] Ghatikar, G. and Bienert, R.: Smart Grid Standards and Systems Interoperability: A Precedent with OpenADR, *Proceedings of the Grid Interop Forum* (2011).
[15] 林 慧，菅原 進：ビルの省電力をサポートする遠隔省電力サービス FACiTENA-i，東芝レビュー (2014).
[16] 堀 賢治, 服部雅晴, 吉原貴仁, 井戸上彰, 山崎徳和：M2M エリアネットワーク (2013). M2M ゲートウェイ.
[17] 阿倍博信，若土剛之，中島宏一，小林信博：ID ベース暗号を用いたネットワークカメラ向けセキュアプロファイル設定方式，マルチメディア通信と分散処理ワークショップ論文集，Vol. 2009, No. 9, pp. 55–60 (2009).
[18] 佐藤亮太，知加良盛，奥田哲矢，栢口 茂：スマートデバイスにおける利用環境に応じた機能制御機構の提案とその考察，情報処理学会論文誌，Vol. 55, No. 1, pp. 267–279 (2014).
[19] OMA: OMA Device Management V1.2, , available from ⟨http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/dm-v1-2⟩ (accessed 2015/4/19).
[20] BBF: TR-069 CPE WAN Management Protocol, , available from ⟨http://www.broadband-forum.org/technical/download/TR-069_Amendment-4.pdf⟩ (accessed 2015/4/19).
[21] 山田勝彦，塩尻浩久：M2M 標準化動向と遠隔管理技術の標準化活動，NEC 技報，Vol. 64, No. 4, NEC, pp. 26 – 30 (2011).
[22] OSGi-Alliance: OSGi Alliance Specifications, , available from ⟨http://www.osgi.org/Specifications/HomePage⟩ (accessed 2015/4/19).