資料 14-6

環境クラウドサービスの構築・運用ガイドライン（案）

平成２３年７月７日

目次

1. はじめに

1.1. 背景及び目的

近年、スマートグリッドやスマートシティ等のCO_2排出量削減に向けたICTを活用した取組が国内外において活発化しており、政府の「新成長戦略（平成22年6月18日閣議決定）」においては「情報通信技術の活用等を通じて日本の経済社会を低炭素型に革新する」旨が掲げられている。

また、平成23年3月11日に発生した東日本大震災の影響による電力会社の電力供給力の大幅な低下に伴い、国民・産業界等すべての電力需要家において節電に対する取組みが求められているとともに、生産性を維持した省エネ型社会経済活動の重要性とこれに対するICTの貢献への期待が高まっている。

さらに、当該分野におけるクラウド技術やIPv6技術の活用は効率的なシステム導入だけでなく、エネルギー需給、気温、湿度等の環境情報の高度な分析や、大量機器の効果的な管理・制御を可能にすると見込まれている。

このような状況を踏まえると、クラウド技術やIPv6技術等の高度なICTを活用することにより効率的に環境負荷軽減を実現する環境クラウドサービスの進展が期待されるところである。

総務省においては、「IPv6 によるインターネットの利用高度化に関する研究会」（座長：齊藤 忠夫 東京大名誉教授）に、「IPv6 を用いた環境分野のクラウドサービスワーキンググループ」（主査：江﨑 浩 東京大学大学院教授）を設置し、平成 22 年 3 月から平成 23 年 6 月まで、クラウド技術及び IPv6 技術を活用した環境クラウドサービスの健全な発展のため、環境クラウドの構築・運用に関わる事業者等が満たすことが推奨される要件等について検討を行った。この検討に当たっては、平成 21 年度第 2 次補正予算施策「環境負荷軽減型地域 ICT システム基盤確立事業」における実証実験の成果・課題等を参考とした。本実証実験では、環境クラウドサービスを実現する典型的な 3 つのモデル（ビル群エネルギー管理システム、都市型エネルギー管理システム、地域型エネルギー管理システム）について実証実験環境を構築し、環境クラウドのネットワーク要件等を検証した。

本書は、環境クラウドの構築・運用に関わる事業者等によって指針・知見として活用されることにより、同サービスの健全な普及を促進するため、本研究会の検討の結果を「環境クラウドサービスの構築・運用ガイドライン」（以下「ガイドライン」という。）としてまとめたものである。

1.2. ガイドラインの基本的な考え方

1.2.1. 環境クラウドサービスについて

環境クラウドサービスとは、環境情報（エネルギー需給、気温、湿度、等）を収集・可視化・解析し、その結果に基づき、環境負荷軽減に資するよう機器・設備を制御する機能を、クラウド、ＩＰｖ６等のＩＣＴ技術を活用して実現するサービスの総称であり、効果的に環境負荷軽減を実現するものとして、今後の普及が期待されている。

環境クラウドサービスの主な特徴は以下のとおり。

＜主な特徴＞

- クラウド技術の活用により、ネットワーク上に効率的に ICT システムを集約することが可能
- 環境情報をクラウド上に収集することにより、高度な可視化、解析、制御が可能
- インターネット上にオープンな仕様で構築することによりシステムの拡張性や高度なサービス連携が期待
- インターネット等の通信インフラを介して効率的に膨大な数のセンサーを利用するには IPv6 技術の活用が重要

1.2.2. 本ガイドラインが想定している主な読者

本ガイドラインは、主に以下の読者を想定している。

＜環境クラウドの構築・運用に関わる事業者等＞

環境クラウドサービスを提供する者（複数の者が連携してサービス提供される場合も想定）。

本ガイドラインを環境クラウドの構築・運用する際の指針として活用することにより、効率的かつ適切な環境クラウドサービスの構築・運用に資することを期待している。

＜環境クラウドサービス利用者＞

ビルオーナー、ビル管理者、施設管理者、店舗責任者、一般家庭、自治体、エネルギー供給業者、等。

サービスの提供を受ける事業者を選定する際に、IPv6 環境クラウドの構築・運用に関わる事業者等が実施・導入しているセキュリティ対策等の状況を確認するための指標として活用することを期待している。

1.2.3. 本ガイドラインの特徴

本ガイドラインでは、環境クラウドの構築・運用に関わる事業者等が、環境クラウドの構築・運用する際に推奨されるセキュリティ等に関するネットワーク要件等を解説している。実証実験等により得られた具体的な対策事例や留意が必要な点等の知見を紹介することにより、事業者等にとって実践的な内容となるよう工夫している（実証実験の詳細は2.1を参照。）。

なお、環境クラウドサービスは、複数の事業者の垂直連携により提供される場合がある。このため、利用者からは、直接契約を締結しない基盤レイヤー（プラットフォーム、インフラ等）の事業者の存在を意識されない場合があるが、本ガイドラインでは、環境クラウドサービスに関わる事業者がそれぞれ何をすべきか、あるいは、上位レイヤーを担う事業者が基盤レイヤーを担う事業者に何を要求すべきかがわかるようにレイヤーごとの要件を記載している。

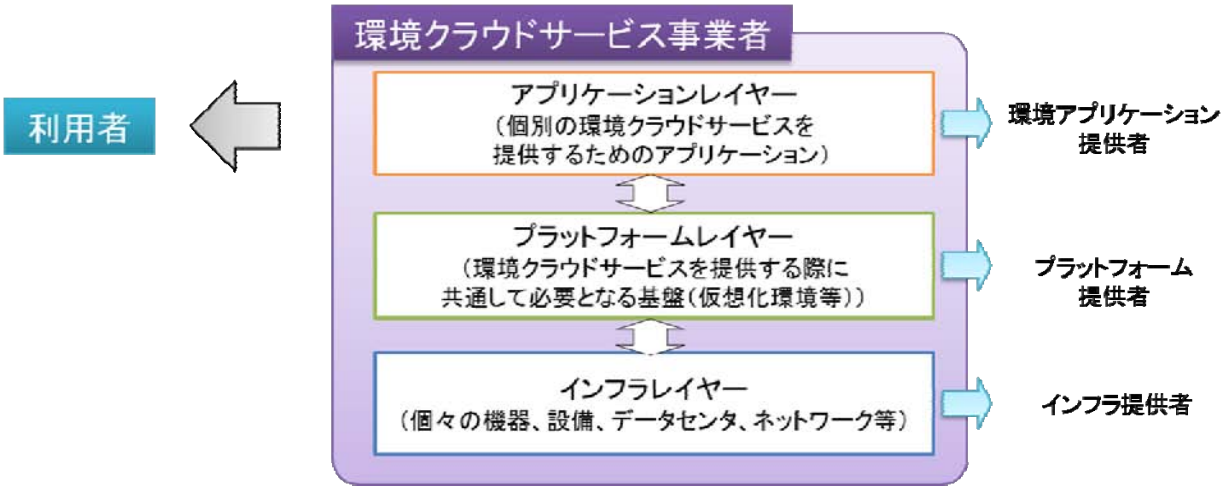


図 1-1　環境クラウドシステムのレイヤー構成

1.2.4.　本ガイドラインの構成

本ガイドラインは、主に「3. システム構成に係る要件」及び「4. システム構築・運用に係る要件」の２つの柱により構成される。以下にそれぞれの考え方を示す。

＜「3. システム構成に係る要件」について＞

環境クラウドサービスを提供する「システム構成要素」に必要とされる機能、技術要素等を解説するとともに、新たに環境クラウドサービスを開始する者の参考となるよう実証実験において採用した詳細な構成・標準技術等を記述し、具体的な実現方法例を提供している。

また、「構成要素間のインタフェース」について、標準的なプロトコルを例示するとともに、既存システムやインターネットに接続する際の留意点など考慮すべき項目を記述し、さらに具体的な対処例を提供している。

その他、IPv6 技術を活用する際の優れた点や留意すべき点について記述している。

＜「4. システム構築・運用に係る要件」について＞

（１）拡張性の確保、（２）情報セキュリティの確保及び（３）環境負荷軽減効果の評価について、アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤーごとに推奨要件を記述している。

新たに環境クラウドサービスを開始する多様な業界の事業者が本ガイドラインの読者となることを想定し、各要件の記述については一通り網羅的に解説するように努めているが、クラウドサービスや情報セキュリティ等の分野についてより具体的な内容を理解する場合には、当該分野に特化した法令・基準・ガイドライン等を参照することが望ましい。

また、環境クラウドサービスの特徴といえる事項については、環境クラウドサービス構築の際の参考となるよう、実証実験等により得られた具体的な対策事例や留意が必要な点を紹介するなど記述内容の充実化に努めている。

2. 対象となるモデル

2.1. 実証実験について

本ガイドラインにおける「実証実験」とは、総務省の平成 21 年度第 2 次補正予算施策「環境負荷軽減型地域 ICT システム基盤確立事業」に係る実証実験を指す。クラウド技術及び IPv6 技術を活用した環境クラウドサービスを普及・促進することを目的として、環境クラウドサービスの構築・運用に関わる事業者等が満たすべきセキュリティ等に関するネットワーク要件の検証を行い、得られた結果・知見等を本ガイドラインにおいて参照している。

なお、環境クラウドを活用した環境アプリケーションの多様性に対応するため、典型的な 3 つのモデル（ビル群エネルギー管理システム、都市型エネルギー管理システム、地域型エネルギー管理システム）に注目し、検証を行っている。

各モデルに係る実証実験の概要は以下のとおり。

＜モデル A：ビル群エネルギー管理システム＞

ビル管理事業者やエネルギー供給業者と連携して、複数ビルのエネルギー消費を一括して管理･制御（詳細かつ大量のビルエネルギー消費情報の管理）することを目的とし、東京、横浜、名古屋のビルにおいて実証実験を実施。

＜モデル B:都市型エネルギー管理システム＞

省エネサービス事業者や地方公共団体等と連携して、多様な施設ごとのエネルギー消費を管理･制御（多様な利用者へのサービス提供を考慮したエネルギー情報の管理） することを目的とし、広島市中心部において実証実験を実施。

＜モデル C:地域型エネルギー管理システム＞

地方公共団体等と連携して、地域の発電設備等のエネルギー供給に係る情報を管理（エネルギー供給及び関連する環境情報の管理）することを目的とし、広島市を含む広域において実証実験を実施。

2.2. モデルの特徴

本ガイドラインの対象として、環境クラウドサービスを実現する典型的な 3 つのモデルの特徴を以下、図 2-1 及び表 2-1 に示す。

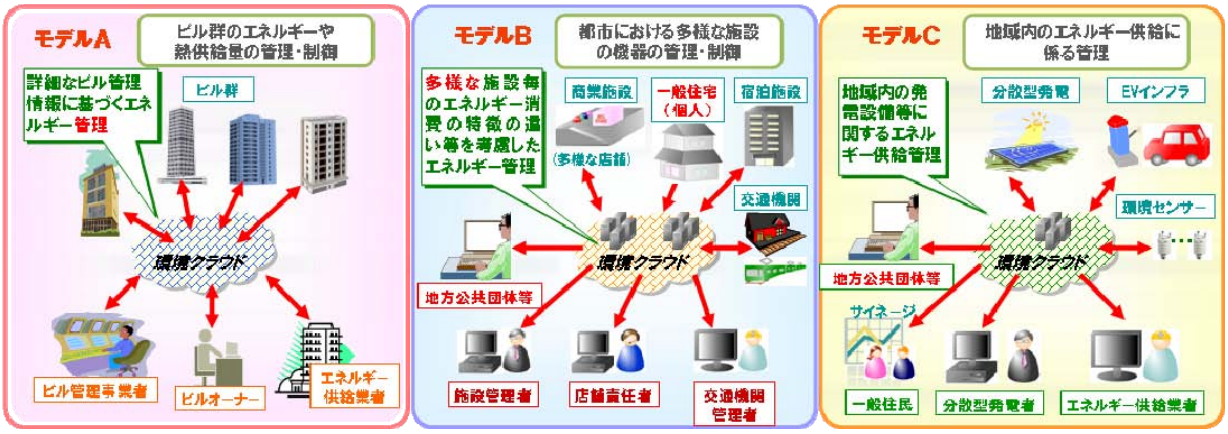


図 2-1　各モデルのイメージ

表 2-1　各モデルの特徴

	モデルA （ビル群エネルギー管理システム）	モデルB （都市型施設エネルギー管理システム）	モデルC （地域内エネルギー供給管理システム）
概要	ネットワークを通じて複数のビルのエネルギー管理を一括して行うシステム	都市部においては、施設毎のエネルギー消費の特徴の違いを考慮したエネルギー管理サービスを、様々な施設に対してネットワークを通じて提供するシステム	地域内の発電設備、蓄電設備等のエネルギー供給に係る情報を管理するシステム
主なサービス利用者	ビルオーナーあるいはビル管理事業者（単一業）、エネルギー供給者	1次利用者：事業者/施設管理者 2次利用者：有識者（大学/行政等）	1次利用者：市民等 2次利用者：有識者（大学/行政等） アプリケーション事業者等
サービス提供者	環境クラウドサービス事業者（環境アプリケーション提供者、プラットフォーム提供者に分けることが可能）		
主な特徴	エネルギーの消費に関する情報の収集を行うとともに、設備等の制御に関する情報の配信を行う	都市に存在する多様な設備についてエネルギー消費に関する情報の収集等を行う	エネルギーの消費に関する情報に加え、エネルギーの供給に関する情報の収集を行う
システム構成要素	✓ ビル群エネルギー管理システム（クラウドサービス） ✓ IPv6インターネット ✓ エネルギー情報計測・収集・制御システム	✓ 都市型施設エネルギー管理システム（クラウドサービス） ✓ IPv6インターネット ✓ エネルギー情報計測・収集・制御システム	✓ 地域内エネルギー供給管理システム（クラウドサービス） ✓ IPv6インターネット ✓ エネルギー情報計測・送信システム

2.3.　事業者と利用者の関係

環境クラウドサービスを提供する上で想定される事業形態は、例えば以下のように類型化される。

＜事業形態①：環境アプリケーション提供者とプラットフォーム提供者が同じ事業者の場合＞

環境アプリケーション提供者とプラットフォーム提供者が１つの事業者（環境クラウドサービス事業者）の中に内包され、一体化して環境クラウドサービスを提供する事業形態。

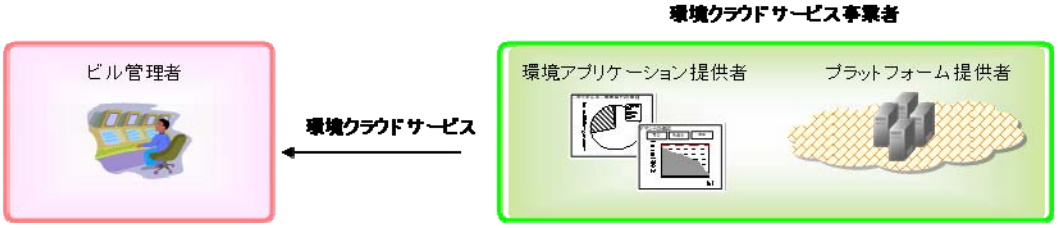


図 2-2　事業形態①のイメージ図

＜事業形態②：環境アプリケーション提供者とプラットフォーム提供者が異なる事業者の場合＞

環境アプリケーション提供者とプラットフォーム提供者が異なる事業者に分かれており、環境アプリケーション提供者がプラットフォーム提供者のプラットフォームを利用して、環境クラウドサービスを提供する事業形態（この場合、利用者からは環境アプリケーション提供者が環境クラウドサービス事業者として見えており、基本的にはプラットフォーム提供者を意識する必要はない。）。

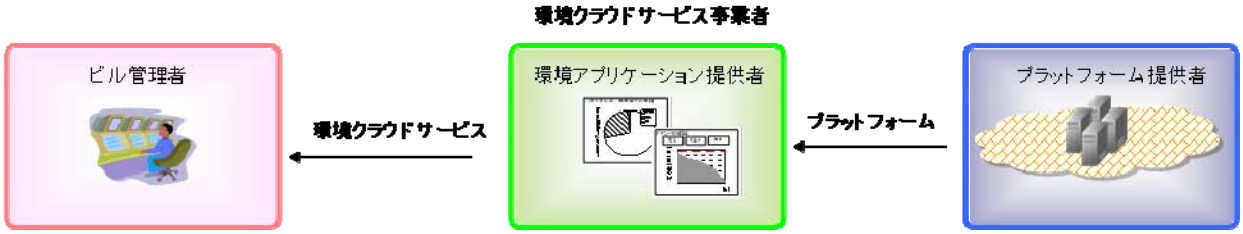


図 2-3　事業形態②のイメージ図

なお、本ガイドラインでは、この事業形態に係わらず、レイヤーごとに環境アプリケーション提供者、プラットフォーム提供者が構築・運用の際の行動指針になるようまとめている。

以下、各モデルの事業者と利用者の関係の詳細を解説する。

2.3.1.　モデル A:ビル群エネルギー管理システム

ビル群エネルギー管理システムにおいて想定される事業者・利用者の関係は以下のとおり。

表 2-2　ビル群エネルギー管理システムに係わる事業者・利用者

環境クラウドサービス事業者	ビルオーナー、ビル管理事業者、エネルギー供給事業者等に対して、環境クラウドサービスを提供する事業者。環境クラウドサービス事業者は、実体として以下の環境アプリケーション提供者、プラットフォーム提供者に細分化することができる。
環境アプリケーション提供者	プラットフォーム提供者が提供するプラットフォーム上に環境アプリケーションを構築し、環境クラウドサービスをビル管理者に提供する組織(SaaS ベンダー相当)。
プラットフォーム提供者	ハードウェア、ネットワーク、オペレーティングシステム、ミドルウェア等のインフラ、プラットフォームを環境アプリケーション提供者へ提供する組織(PaaS、IaaS ベンダー相当)。
環境クラウドサービス利用者	ビルオーナー、ビル管理事業者、エネルギー供給事業者等、ビル管理業務に携わる事業者。

2.3.2. **モデル B:都市型施設エネルギー管理システム**

都市型施設エネルギー管理システムにおいて想定される事業者・利用者の関係は以下のとおり。

表 2-3　都市型エネルギー管理システムに係わる事業者・利用者

環境クラウドサービス事業者	施設管理者（オーナー、テナント、地方自治体、一般家庭等を含む。）に対して、環境クラウドサービスを提供する事業者。環境クラウドサービス事業者は、実体として以下の環境アプリケーション提供者、プラットフォーム提供者に細分化することができる。
環境アプリケーション提供者	プラットフォーム提供者が提供するプラットフォーム上に環境アプリケーションを構築し、環境クラウドサービスを施設管理者に提供する組織(SaaS ベンダー相当)。
プラットフォーム提供者	ハードウェア、ネットワーク、オペレーティングシステム、ミドルウェア等のインフラ、プラットフォームを環境アプリケーション提供者へ提供する組織(PaaS、IaaS ベンダー相当)。
環境クラウドサービス利用者	施設管理者(商業施設、宿泊施設、交通機関など)、地方自治体、テナント、一般家庭等、都市において施設を管理、利用する法人もしくは個人。

2.3.3. **モデル C:地域内エネルギー供給管理システム**

地域内エネルギー供給管理システムにおいて想定される事業者・利用者の関係は以下のとおり。

表 2-4　地域内エネルギー供給管理システムに係わる事業者・利用者

環境クラウドサービス事業者	設備保有者（民間企業、電力供給会社や地域行政（地方自治体)、地域内市民を含む。）に対して、環境クラウドサービスを提供する事業者。環境クラウドサービス事業者は、実体として以下の環境アプリケーション提供者、プラットフォーム提供者に細分化することができる。
環境アプリケーション提供者	プラットフォーム提供者が提供するプラットフォーム上に環境アプリケーションを構築し、環境クラウドサービスを設備管理者に提供する組織(SaaS ベンダー相当)。
プラットフォーム提供者	ハードウェア、ネットワーク、オペレーティングシステム、ミドルウェア等のインフラ、プラットフォームを環境アプリケーション提供者へ提供する組織(PaaS、IaaS ベンダー相当)。
環境クラウドサービス利用者	民間企業、電力供給会社や地域行政（地方自治体)、地域内市民等。

2.4. データ利用に対する考え方

2.4.1. 環境クラウドサービスが取扱う環境情報

環境クラウドサービスでは、表 2-5 に示すような環境情報を計測・収集し、クラウド上のデータ計測・収集・制御システムで管理する。これらの情報は、利用者の需要に応じて可視化し、エネルギー消費の無駄の削減、環境負荷軽減に資する普及啓発、研究利用（２次利用）等に活用されることが想定される。

以下、各モデルのデータ利用に対する考え方及びデータの利用に当たり推奨される要件等について解説する。

表 2-5　環境クラウドサービスが取扱う環境情報（例）（モデルによる整理）

＜モデルA（ビル群エネルギー管理システムの場合）＞

測定対象施設	大規模ビル	中規模ビル
測定情報	（建物全体部） ・受電電力量 ・冷水消費量 ・蒸気消費量 ・外気温度 ・外気湿度 （各フロア） ・照明コンセント電力量 ・空調機消費電力 ・冷水消費熱量 ・温水消費熱量 ・室内温度・湿度	（各フロア） ・消費電力

＜モデルB（都市型施設エネルギー管理システム）＞

測定対象施設	商業施設		宿泊施設（ホテル）		交通機関		住宅	
					駅	車両	学生寮	社宅
測定情報	• 空調電力 • 照明電力	• 電力量 • 熱源熱量 • 空調機 • 冷温水器モード 他	• 空調電力 • 照明電力	• 電力量 • 室温 • 空調設定 • 温度 • 空調モード	• 電力量	• 電力量 • 温度 • 湿度	• 建物全体の電力量 • 各コンセントの使用電力	• 各コンセントの使用電力

＜モデルC（地域内エネルギー供給管理システム）＞

測定対象施設	太陽光パネル	EVインフラ	環境センサー
測定情報	• 電力・電圧・電流（直流、交流） • 動作モード • 日照強度	• 使用電力量	• 温度・湿度 • 風向・風速 • 雨量 • CO_2濃度

2.4.2.　モデル A（ビル群エネルギー管理システム）

ビル群エネルギー管理システムでは、ビルオーナーが所有する複数のビルのエネルギー消費・効率等を可視化することにより、エネルギー需給を制御・最適化し、環境負荷（エネルギーコスト）軽減への貢献を目指すことが想定される。データの収集・管理はビルオーナーとの規約に沿った範囲で行われ、データは主に

・ビルオーナー（又はテナント）のエネルギーコスト削減

・ビルオーナー（又はテナント）の CSR 活動や、法令によるエネルギー管理義務・報告の実施

・エネルギー供給事業者への提供による効率的なエネルギー需給制御

等の目的で利用される。

ビル群エネルギー管理システムにおけるデータ利用の流れを以下に示す。

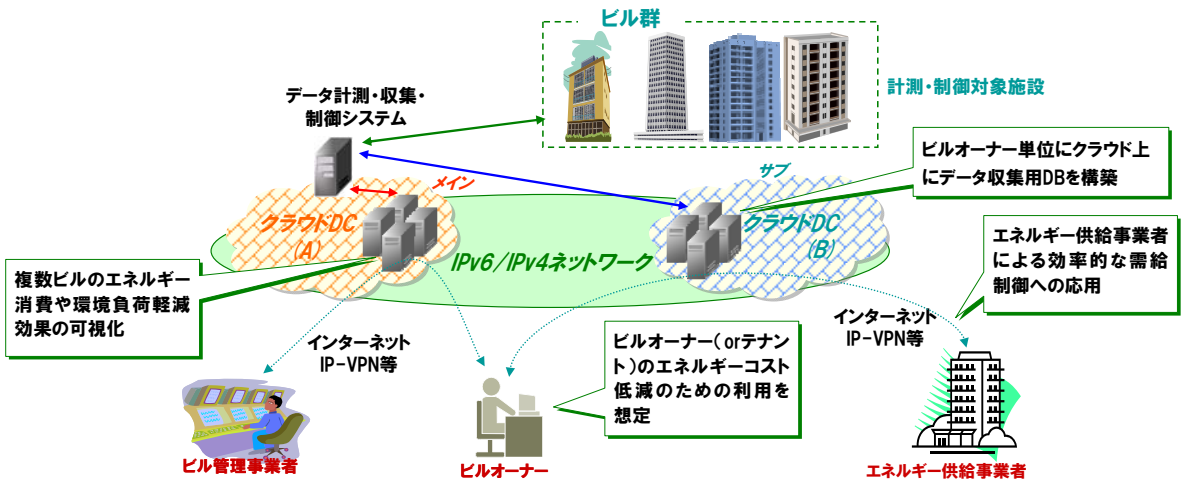


図 2-4　ビル群エネルギー管理システムにおけるデータ利用の流れ

2.4.3. モデルB（都市型施設エネルギー管理システム）

都市型施設エネルギー管理システムでは、多様な施設・事業者を対象として、データを集計/分析し、電力利用の効率化やネットワーク型の空調制御による省エネ/コスト削減を支援するサービスを提供することが想定される。データは主に

・サービス利用者の保有施設における環境負荷軽減策の実施

・研究者等の分析による、都市、事業者、施設管理者等に対する環境負荷軽減策等の提案

等の目的で利用される。

都市型施設エネルギー管理システムにおける詳細化した利用者の例及びデータ利用の流れを以下に示す。

表 2-6　都市型施設エネルギー管理システムに係わる利用者の詳細例

サービス利用者	事業者	各事業者が保有する施設における消費エネルギーを計測、分析するサービスを利用し、エネルギー消費のムダを把握し、施設におけるエルギー消費量を適正化する。
２次データ利用者	有識者大学、行政関係等）	クラウド事業者がデータ保護等の必要な加工を施した２次データを利用し、都市における消費エネルギーの傾向析、当該都市おける都市計画の策定等を実施する。
その他	設備情報保・任者	各施設に設置されている設備機器のエネルギー消費情報、稼働情報、保守・運用情報を収集し、設備機器のメンテナンス等を実施する。サービス利用者からの委託を受け、事業者が管理する施設のエネルギー情報を収集し、分析を行う。

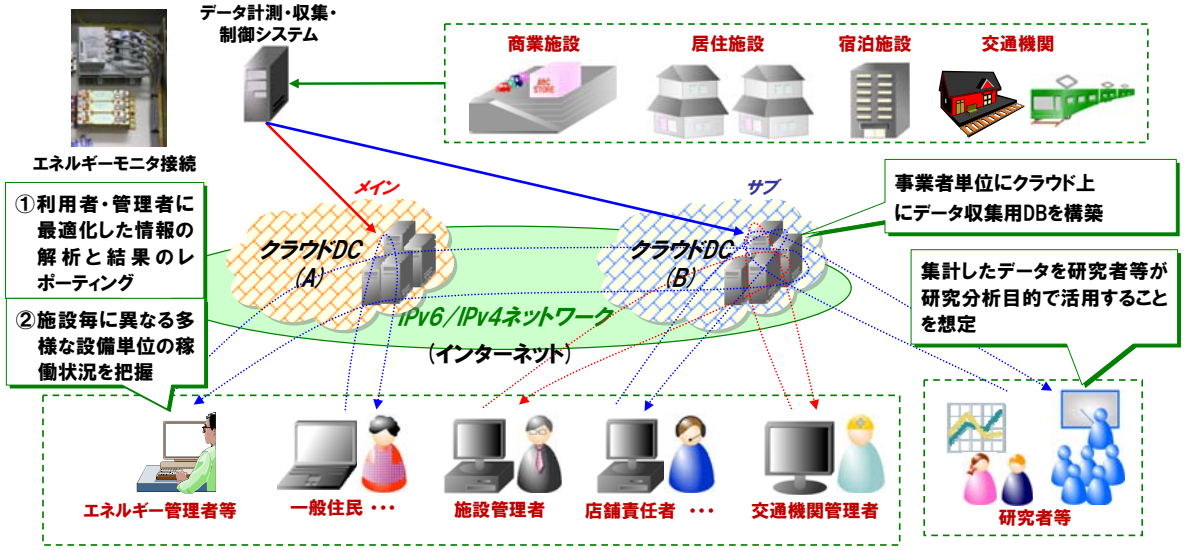


図 2-5　都市型施設エネルギー管理システムにおけるデータ利用の流れ

2.4.4. モデルC（地域内エネルギー供給管理システム）

地域内エネルギー供給管理システムでは、地域のエネルギー需給に係る情報を公共向けに提供する

ことにより、再生可能エネルギーの普及・促進やエネルギー利用に関する啓蒙に利用することが想定される。データは主に、

・サービス事業者のエネルギーの効率利用の普及啓発を目的とした分析
・研究者等の分析による都市計画等の作成
・エネルギーの効率利用を促進するアプリケーションや普及啓発のためのデジタルサイネージ等との連携

等の目的で利用される。

地域内エネルギー供給管理システムにおける詳細化した利用者の例及びデータ利用の流れを以下に示す。

表 2-7　地域内エネルギー供給管理システムに係わる利用者の詳細

エネルギー情報提供者	設備保有者	サービス事業者に対して、自らが保有管理する設備機器におけるエネルギー需給情報の提供を行う。
２次利用事業者	有識者（大学・行政等）	地域内エネルギー供給管理システムサービスに蓄積された情報をもとに、市民に対次世代エルギーの普及啓発を目的としたデジタルサイネージ等のデータ公開や、都市計画の基礎データとしての街づくり構想等を検する。
	アプリケーション事業者	EV インフラ等の利用状況のモバイルへの配信や、太陽光発電量をもとにした教育用コンテンツの配信等、アプリケーション提供を行う。
一般市民		地域内エネルギー供給管理システムサービス提供者や行政が提供する地域の次世代エネルギーに関する情報をデジタルサイネージやモバイルデバイスを介して閲覧する

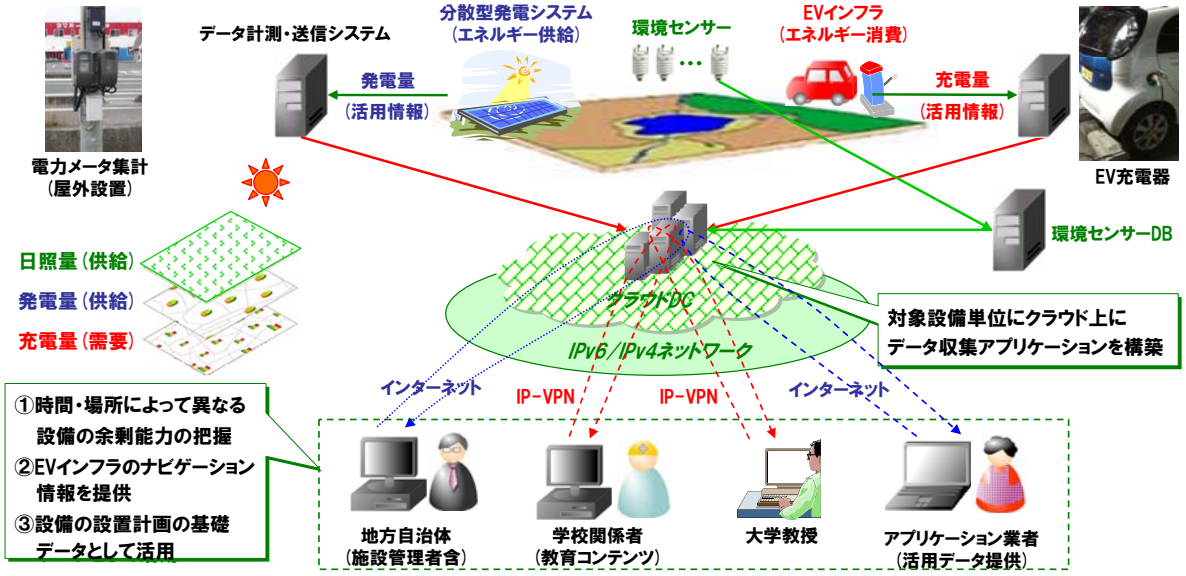


図 2-6　地域内エネルギー供給管理システムにおけるデータ利用の流れ

3. システム構成に係る要件

3.1. モデル A：ビル群エネルギー管理システムの構成要件

本項では、ビル群エネルギー管理システムを構成する以下の要素について、必要とされる機能、技術要素等の例、構築するに当たって推奨される要件、実証実験において採用した詳細な構成・標準技術等の例を解説する。

3.1.1. ビル群エネルギー管理システム（クラウドサービス）

3.1.2. エネルギー情報計測・収集・制御システム

3.1.3. IPv6 インターネット

3.1.4. 構成要素間のインタフェース

3.1.5. システム構成の詳細（例）

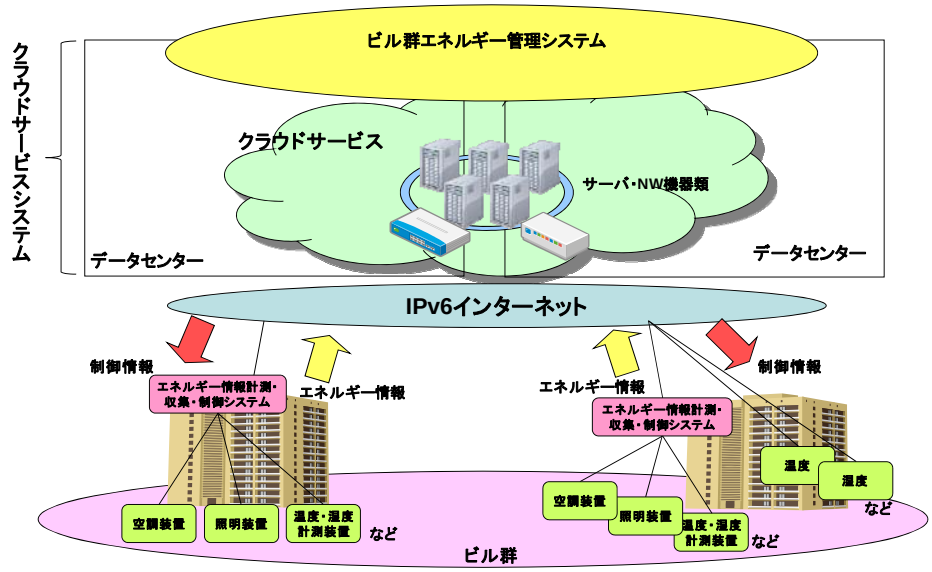


図 3-1 ビル群エネルギー管理システムの全体構成例

3.1.1. ビル群エネルギー管理システム（クラウドサービス）

ビル群エネルギー管理システムは、複数のビルのエネルギー情報（温度、湿度、エネルギー消費量等）を受信・保存・加工し、エネルギー情報計測・収集・制御システムに対してビル内の機器・設備を制御するために必要な情報を送るシステムである。

ビル群エネルギー管理システムの構成要素として必要とされる機能､技術要素等の例を以下に示す。

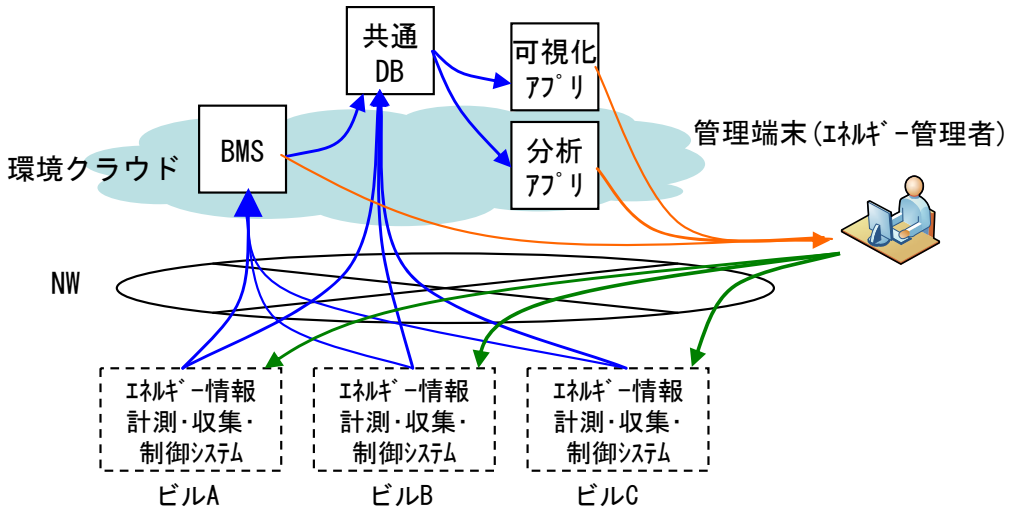


図 3-2　ビル群エネルギー管理システムの構成例

表 3-1　ビル群エネルギー管理システムの構成要素

構成要素名	機　能
ビル管理システム（Building Management System：BMS）	環境クラウド上に配置され、ビルのエネルギー関係データを集約し現在のエネルギー消費状況の可視化を行う。
共通データベース（DB）	環境クラウド上に設置され、BMS やエネルギー情報計測・収集・制御システムから得られるエネルギー関係データを保管及び管理するための機能を持つ。
可視化アプリケーション	環境クラウド上に配置され、共通 DB に収集されたビルのエネルギー関係データを元に中長期のエネルギー情報を可視化するための機能を持つ。
分析アプリケーション	環境クラウド上に設置され、共通 DB に収集されたビルのエネルギー関係データを元に日常や定期のエネルギー使用状況を可視化し、エネルギー管理を支援するための機能を持つ。
管理端末	エネルギー管理者が利用する端末。ビルのエネルギー消費状況を確認し、遠隔でエネルギー情報・計測・収集・制御システムにアクセスする。

3.1.2.　**エネルギー情報計測・収集・制御システム**

エネルギー情報計測・収集・制御システムは、ビル内のエネルギー情報を計測・収集・送信し、ビル群エネルギー管理システムから得られる情報に基づき、ビル内の機器・設備を制御するシステムである。

エネルギー情報計測・収集・制御システムの構成要素として必要とされる機能、技術要素等の例を以下に示す。

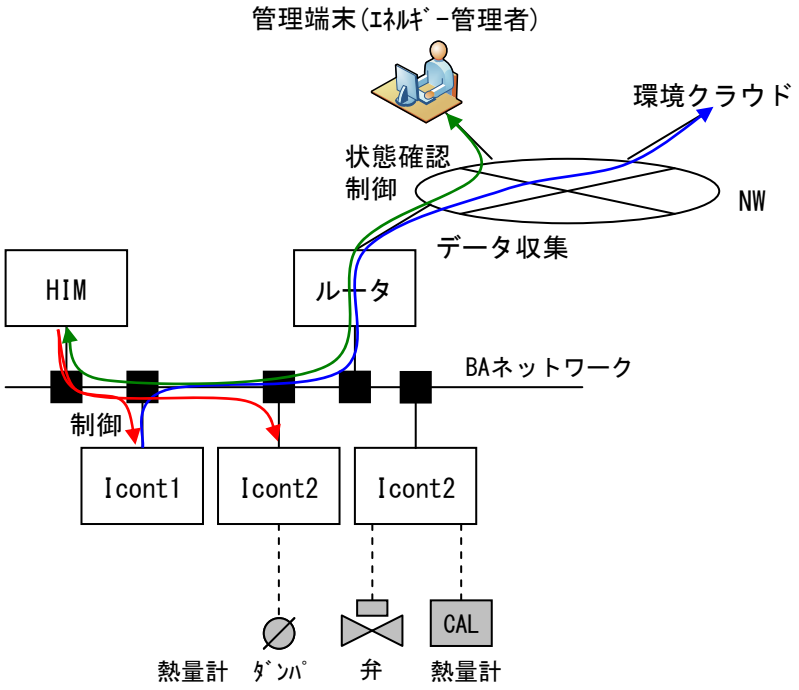


図 3-3　エネルギー情報計測・収集・制御システムの構成例

表 3-2　エネルギー情報計測・収集・制御システムの構成要素

構成要素名	機　能
HIM (Human Interface Module)	エネルギー情報計測・収集・制御システムを構成する要素（デバイス）。管理者がビル設備の監視、制御を行うためのもの。
Icont (Intelligent Controller)	エネルギー情報計測・収集・制御システムを構成する要素（デバイス）。実際のビル設備機器が接続されており、制御の実施や、エネルギーデータの一次保存を行うためのもの。
ルータ	エネルギー情報計測・収集・制御システムのネットワークと、クラウドを接続する機器。
BA ネットワーク	エネルギー情報計測･収集･制御システムを構成する BACnet プロトコルで通信を行うネットワーク。

3.1.3.　IPv6 インターネット

ビル群エネルギー管理システムでは、管理・制御ビル内に設置されたエネルギー情報計測・収集・制御システムとクラウド上に構築されたエネルギー管理のための環境アプリケーションの間で IPv6 通信が行われることが想定される。

システム構成の検討に当たり、IPv6 インターネットの利用に係る留意点を以下に示す。

＜システム構成の検討に当たっての留意点＞

・ 環境アプリケーション、データセンターのネットワーク設備等のプラットフォーム、インターネット、ビル内のネットワーク設備やエネルギー情報計測・収集・制御システムは、大量の機器（センサー等）を取り扱うことに伴う管理コストの低減等の観点から、IPv6 に対応している

ことが望ましい。

・ IPv6 への移行期においては、IPv4/IPv6 の併存環境が想定されるため、IPv6 インターネットの利用において、IPv4/IPv6 を変換するための中間ノードを介在させることが望ましい。

3.1.4. 構成要素間のインタフェース

ビル関連の情報を通信するための規格として BACnet や LonWorks など標準化されたプロトコルを搭載した製品が市場に出てきているものの、いまだ独自のプロトコルのシステムを使っているビルが多いため、各インタフェースは、マルチプロトコル・マルチベンダサポートで対応している場合が多い。また、従来ビル内に閉じていた通信を IPv6 インターネット経由で行うという特徴がある。

3.1.5. システム構成の詳細（例）

実証実験により得られた知見等を踏まえ、具体化・詳細化したビル群エネルギー管理システム及びエネルギー情報計測・収集・制御システムの構成の例を以下に示す。

＜モデル A 実証実験を踏まえたシステム構成の例＞

・ビル内の機器からの情報収集には BACnet/IPv6（一部 IPv4）を利用

・従来ビル内に設置されていた BMS（ビル群エネルギー管理システム）をクラウド上に配置

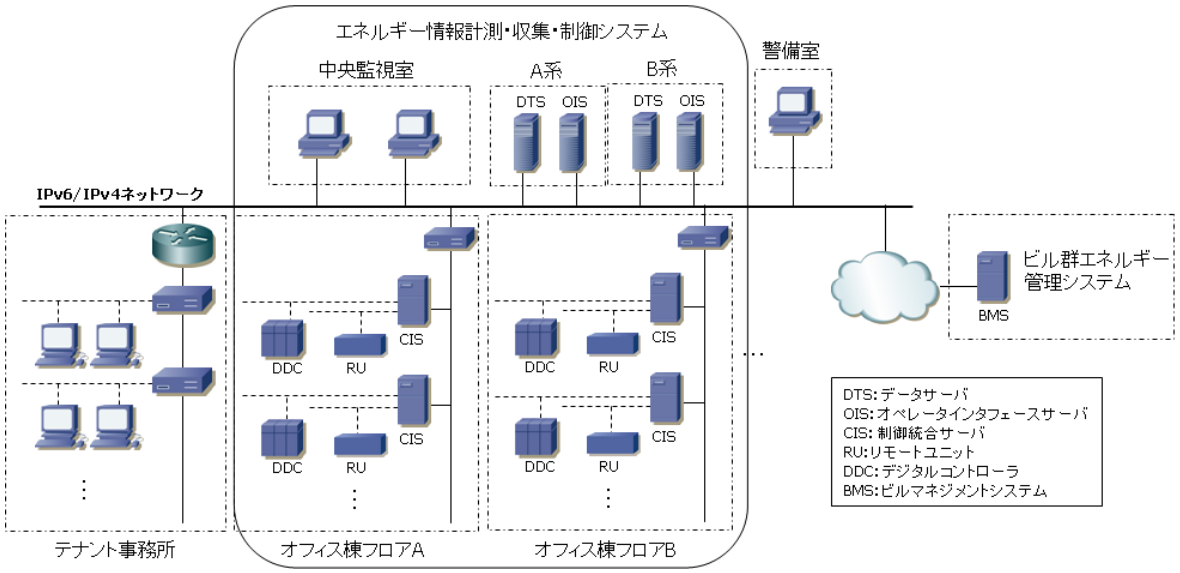


図 3-4　ビル群エネルギー管理システムの構成例

3.2. モデル B：都市型施設エネルギー管理システムのシステム構成要件

本項では、都市型施設エネルギー管理システムを構成する以下の要素について、必要とされる機能、技術要素等の例、構築するに当たって推奨される要件、実証実験において採用した詳細な構成・標準技術等の例を解説する。

3.2.1. 都市型エネルギー管理システム（クラウドサービス）

3.2.2.　エネルギー情報計測・収集・制御システム

3.2.3.　IPv6 インターネット

3.2.4.　構成要素間のインタフェース

3.2.5.　システム構成の詳細（例）

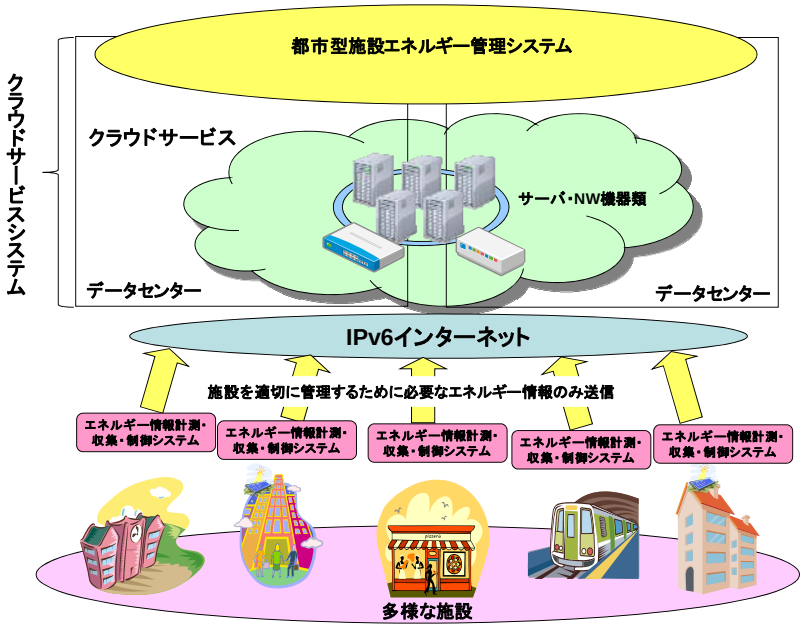


図 3-5　都市型施設エネルギー管理システムの全体構成例

3.2.1.　**都市型エネルギー管理システム（クラウドサービス）**

都市型施設エネルギー管理システムは、都市内に存在する多様な施設（商業施設、宿泊施設、居住施設、交通機関等）を対象に、施設内に設置されている設備機器（空調、照明など）のエネルギー消費に係る情報を収集､分析し､環境負荷軽減を実現するために必要な制御を実施するシステムである。

都市型施設エネルギー管理システム及びエネルギー情報計測・収集・制御システムの構成要素として必要とされる機能、技術要素等の例を以下に示す。

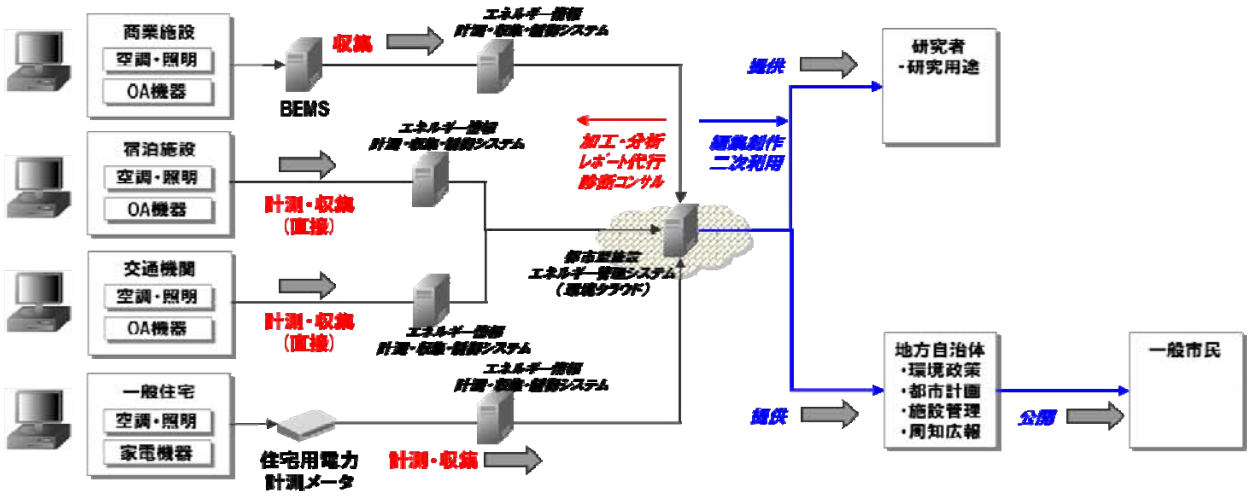


図 3-6　都市型施設エネルギー管理システムにおけるサービスモデル（例）

表 3-3　都市型エネルギー管理システム及びエネルギー情報計測・収集・制御システムの構成要素

構成要素名		機　能
都市型施設エネルギー管理システム（環境ラド）	環境クラウドアプリケーション	エネルギー情報の収集・制御を実施するアプリケーション。Linux 等の汎用的な基盤上のアプリケーションで構築される。外部連携用 API 等を有し、SOAP 等標準化されたプロトコルで利用することができる。
	環境クラウドデータベース（DB）	エネルギー情報を蓄積する DB。事業者用及び分析用の DB を有する。
	認証モジュール	環境クラウドを利用する利用者共通基盤。
エネルギー情報計測収集・制御システム	ゲートウェイ	設備機器の独自通信プロトコルについて、LonWorks 等を介することで、IP に変換し、情報を収集するアプリケーション。環境クラウドから発信された制御情報を設備機器に発信する役割も持つ。
	家電電力計測装置	一般居住施設内に設置される機器であり、家電機器の接続することで、機器の消費電力量を計測する。取得されたデータは Bluetooth 等でゲートウェイに対して送出する。
その他	計測・制御置（BEMS）	既設のビル管理システム。BACnet や LonTalk 等のプロトコルを有し、設備器の運転情報の収や制御監視等を行っている。

3.2.2.　**エネルギー情報計測・収集・制御システム**

エネルギー情報計測・収集・制御システムは、都市型施設エネルギー管理システムから得られる情報に基づき、サービスの提供対象である商業施設、居住施設、宿泊施設、交通機関等の各施設内の機器・設備を制御するシステムである。エネルギー情報を送信し施設内の機器・設備を制御する「エネルギー情報収集・接続・制御装置」及び施設内のエネルギー情報を計測する「エネルギー情報計測装置」により構成される。

システム構成の検討に当たっての留意点及びシステムのイメージ（例）を以下に示す。

システム構成の検討に当たっての留意点

エネルギー情報計測・収集・制御システムには、相互運用性を確保する観点から、BACnet、LonWorks、oBIX 等の汎用的なビルオートメーション用データ通信プロトコルを利用可能な機器を利用することが望ましい。

図 3-7　エネルギー情報計測・収集・制御システムのイメージ（例）

3.2.3.　IPv6 インターネット

都市型施設エネルギー管理システムでは、都市型施設エネルギー管理サービスが対象とする施設及び機器におけるエネルギー情報をエネルギー情報計測・収集・制御システムを介して直接収集し、収集した情報の分析に基づき、機器の制御を行う。

環境負荷軽減に向けた意識の高まりから、計測・収集の対象となる機器が今後飛躍的に増大することが想定される。このため、施設内に設置された機器の制御を、都市型施設エネルギー管理システムから直接行う場合には、都市型施設エネルギー管理システムと施設内に設置された機器との間でエンド・ツー・エンドでの通信を確保することが必要になり、現在一般的に利用されている IPv4 アドレスでは対応しきれなくなる可能性がある。

システム構成の検討に当たり、IPv6 インターネットの利用に係る留意点を以下に示す。

＜システム構成の検討に当たっての留意点＞

・ 都市型施設エネルギー管理システムと施設内に設置された機器との間でエンド・ツー・エンドでの通信を確保するため、IPv6 アドレスを介した通信基盤を提供することが望ましい。

3.2.4.　構成要素間のインタフェース

都市型施設エネルギー管理システムは、都市型施設エネルギー管理システム、エネルギー情報計測・

収集・制御システム、IPv6 インターネットにより構成される。

エネルギー情報計測･収集･制御システムと監視･制御対象の機器との間の通信については､BACnet、Lontalk などの標準化されたプロトコルが存在する（BEMS や中央監視装置が既に導入されている場合に導入可能。）。また、エネルギー情報計測・収集・制御システムと都市型施設エネルギー管理システムとの間の通信については、SOAP 等標準化されたプロトコルが存在する。

システム構成の検討に当たり、構成要素間のインタフェースに係る留意点を以下に示す。

＜システム構成の検討に当たっての留意点＞

・ 構成要素間のインタフェースには、相互運用性を確保する観点から、可能な限り標準化された通信プロトコルを利用することが望ましい。

3.2.5. **システム構成の詳細（例）**

実証実験により得られた知見等を踏まえ、具体化・詳細化した都市型施設エネルギー管理システム及びエネルギー情報計測・収集・制御システムの構成の例を以下に示す。

＜モデル B 実証実験を踏まえたシステム構成の例＞

・ 施設内に設置されている設備機器からの情報収集にはLonTalk 等の標準化されたプロトコルを利用

・ 施設に既設の BEMS が導入されている場合には、セキュリティ面を考慮し、NetBIOS を介した CSV によるファイル渡しを実施

・ 家庭の電力の収集に際しては、Bluetooth 等無線を介したセンサーとゲートウェイの間でのデータの授受を実施

・ エネルギー情報計測・収集・制御システムと都市型施設エネルギー管理システムとの間の通信には、汎用的なウェブサービスを利用

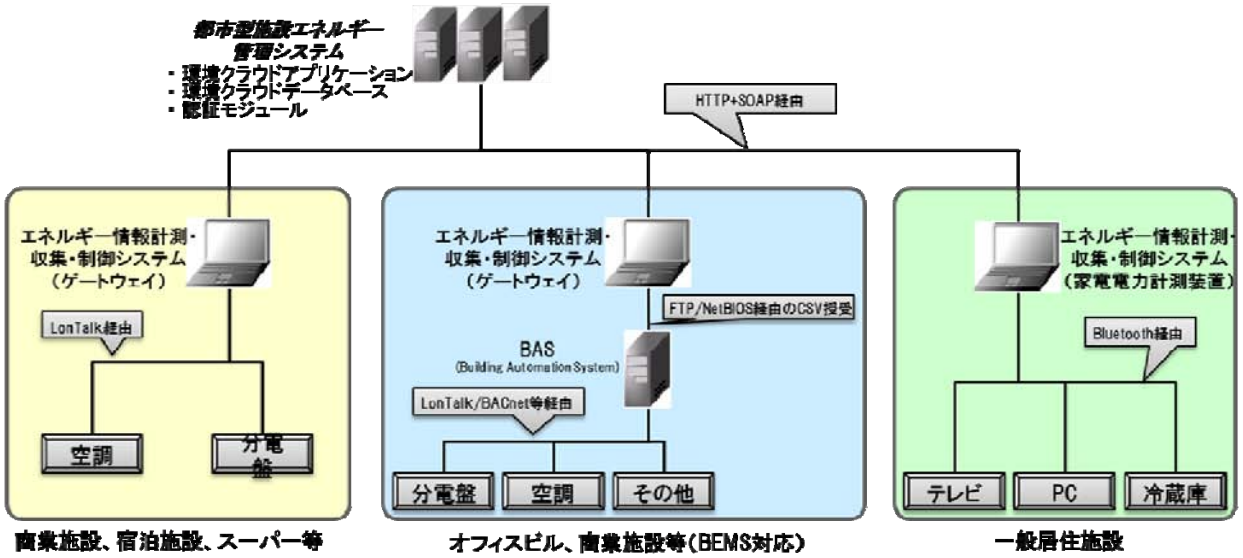


図 3-8　都市型施設エネルギー管理システムの構成例

3.3.　モデル C：地域内エネルギー供給管理システムのシステム構成要件

本項では、地域内エネルギー供給管理システムを構成する以下の要素について、必要とされる機能、技術要素等の例、構築するに当たって推奨される要件、実証実験において採用した詳細な構成・標準技術等の例を解説する。

3.3.1.　地域内エネルギー供給管理システム（クラウドサービス）

3.3.2.　エネルギー情報計測・送信システム

3.3.3.　IPv6 インターネット

3.3.4.　構成要素間のインタフェース

3.3.5.　システム構成の詳細（例）

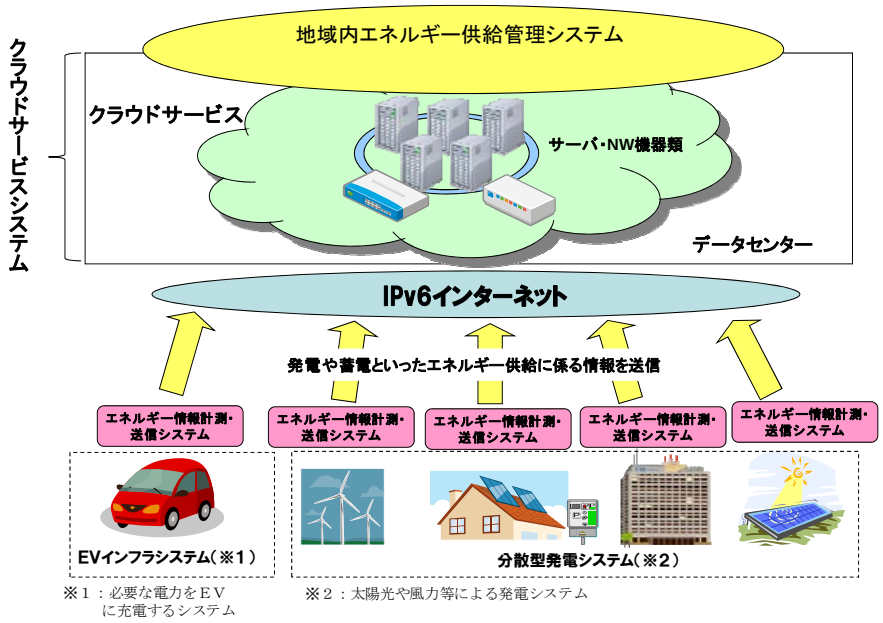


図 3-9　地域内エネルギー供給管理システムの全体構成例

3.3.1.　地域内エネルギー供給管理システム（クラウドサービス）

地域内エネルギー供給管理システムは、発電や蓄電といったエネルギー供給に係る情報を受信・保存・加工し、エネルギー情報計測・送信システムに対して、蓄電・放電を制御するために必要な情報を送るシステムである。

地域内エネルギー供給管理システム及びエネルギー情報計測・収集・制御システムの構成要素として必要とされる機能、技術要素等の例を以下に示す。

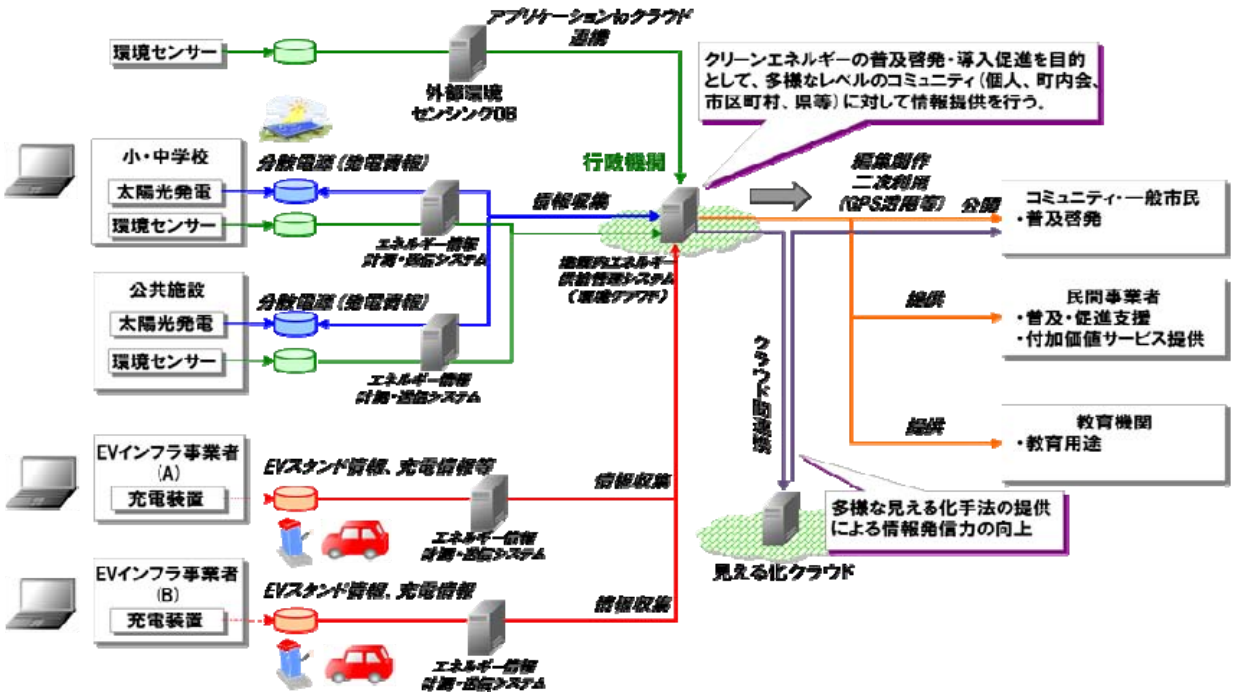


図 3-10　地域内エネルギー供給管理システムにおけるサービスモデル（例）

表 3-4 地域内エネルギー供給管理システム及びエネルギー情報計測・収集・制御システムの構成要素

構成要素名		機　能
地域内エネギー供給システム（環境クラウド）	環境クラウドアプリケーション	エネルギー情報の収集・制御を実施するアプリケーション。Linux 等の汎用的な基盤上のアプリケーションで構築される。外部連携用 API 等を有し、SOAP 等標準化されたプロトコルを利用することができる。
	環境クラウドデータベース（DB）	エネルギー情報を蓄積する DB。事業者用及び分析用の DB を有する。
	認証モジュール	環境クラウドを利用する利用者共通基盤。
エネルギー情報計測・収集・制御システム	ゲートウェイ	分散電源（太陽光パネル）に使われている RS485 や EV 充電器用の分電盤等からデータを取得し、機器の発電量や充電量等を、環境クラウドデータベースに送出する。
その他	環境センサー	気温・湿度・CO_2 濃度等の地域の気象状況を修正するセンサー。IEEE1888 等標準化されたプロトコルでの通信が可能。

3.3.2.　エネルギー情報計測・送信システム

エネルギー情報計測・送信システムは、太陽光パネル等分散型発電設備における発電容量及び EV インフラ等充電蓄電設備における充電量を計測し、計測データを地域内エネルギー供給管理システムへ送信するためのシステムである。システムのイメージ（例）を以下に示す。

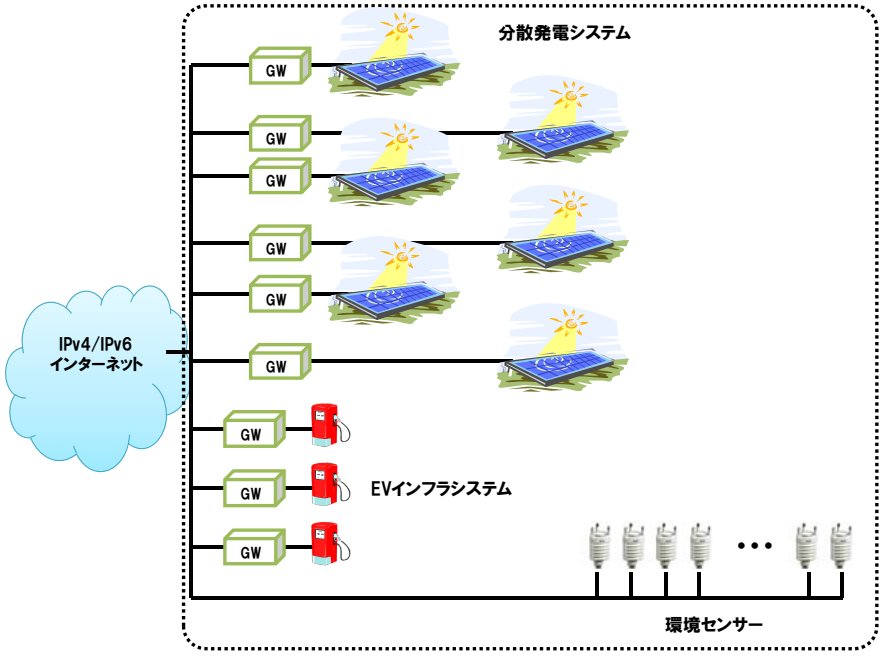


図 3-11　エネルギー情報計測・送信システムのイメージ（例）

3.3.3.　IPv6 インターネット

地域内エネルギー供給管理システムでは、地域内エネルギー供給管理サービスが対象とする機器のエネルギー情報をエネルギー情報計測・送信システムを介して直接収集する。

環境負荷軽減に向けた意識の高まりから、計測・収集の対象となる機器が今後飛躍的に増大することが想定される。この対象機器の増加は、ビル群エネルギー管理システムや都市型施設エネルギー管理システムが対象とする機器の増加と比較しても、大幅に大きくなる可能性があり、現在一般的に利用されている IPv4 アドレスでは対応しきれなくなる可能性がある。

システム構成の検討に当たり、IPv6 インターネットの利用に係る留意点を以下に示す。

＜システム構成の検討に当たっての留意点＞

- 計測・収集の対象となる機器の増大に対応するため、IPv6 アドレスを介した通信基盤を提供することが望ましい。

3.3.4.　構成要素間のインタフェース

システム構成の検討に当たり、構成要素間のインタフェースに係る留意点を以下に示す。

＜システム構成の検討に当たっての留意点＞

- 地域内エネルギー供給管理システムが対象とする機器については、現状では標準化された通信プロトコルが存在していないため、エネルギー情報計測・送信システムにおいて地域内エネルギー供給管理システムが解釈可能な通信プロトコルに変換した上で、計測データを地域内エネ

ルギー供給管理システムに送信することが望ましい。

3.3.5. システム構成の詳細（例）

実証実験により得られた知見等を踏まえ、具体化・詳細化した地域内エネルギー供給管理システム及びエネルギー情報計測・送信システムの構成の例を以下に示す。

＜モデル C 実証実験を踏まえたシステム構成の例＞

- 分散電源の発電量に係る情報の収集に際しては、既設のパワーコンディショナーと接続し、RS485 経由でデータ授受を実施
- EV インフラの電力供給量の収集に際しては、EV インフラが接続されている専用分電盤の電力量を計測・収集
- 環境センサーの収集に際しては、IEEE1888 に準拠したセンサーネットワークプロトコルを利用
- エネルギー情報計測・収集・制御システムと都市型施設エネルギー管理システムとの間の通信には、汎用的なウェブサービスを利用

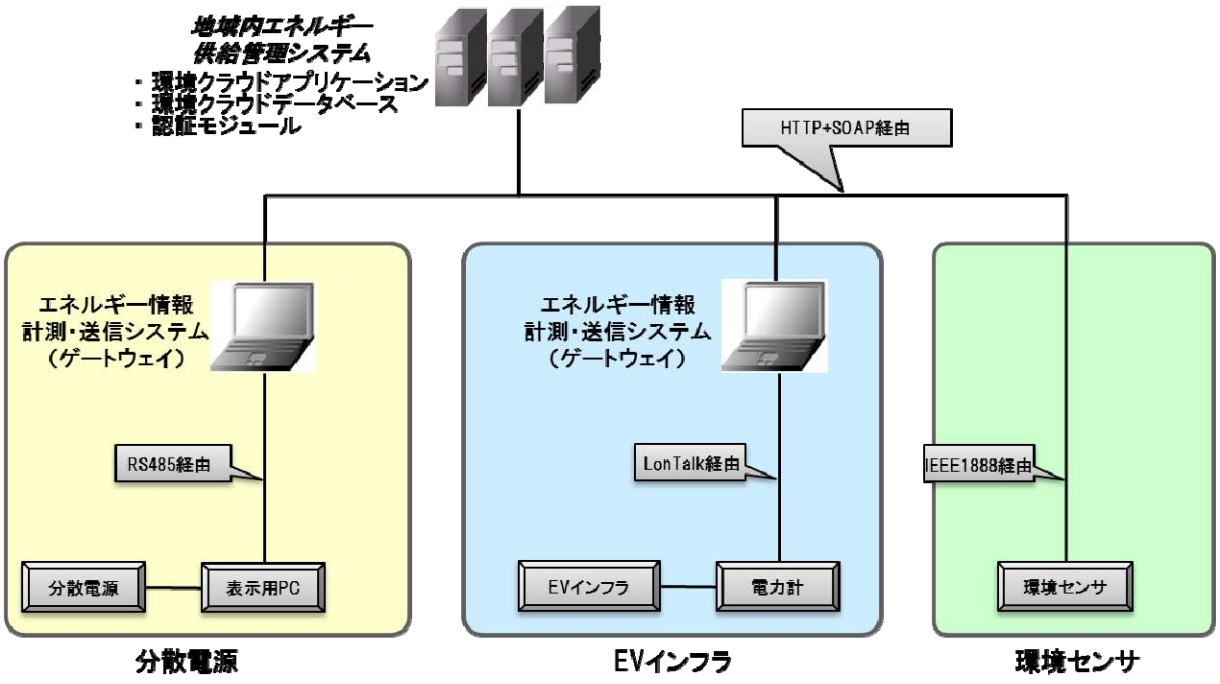


図 3-12　地域内エネルギー供給管理システムの構成例

3.4. 環境クラウドサービスにおける IPv6 技術の導入

環境負荷軽減型地域 ICT システムが普及するにしたがい、管理・制御を実施する機器や設備の数も大きく増加することが予期される。インターネット等の通信インフラを介して膨大な数のノードを管理する際、従来の IPv4 技術に依存したネットワーク設計では効率的・効果的な管理を行うことはできない。

一般的に効率的・効果的な管理・制御を行うためには、対象のノードに対してエンド・ツー・エンドの通信到達性が必要とされる。情報を収集･制御する側が自らスケジューリングしたタイミングで、情報を収集・制御される側にアクセスすることがしばしば要求されるためであり、ここでエンド・ツー・エンドの通信到達性がない場合、通信方式が複雑なものになり、特殊な機器やソフトウェアを導入･管理する等、システム全体のコストに影響を与えることにつながる。仮に IPv4 に依存したネットワーク設計を行う場合､限られた IP アドレス空間で膨大な数のノードとの通信到達性を確保するために IP アドレスを集約する NAT やプロキシサーバを導入することになるが､このような中間ノードの存在を意識せずに透過的に末端ノードを管理･制御することは難しく､コストの上昇を招くことになる。加えて、中間ノードを介在させることによる通信のパフォーマンスの低下も懸念される。

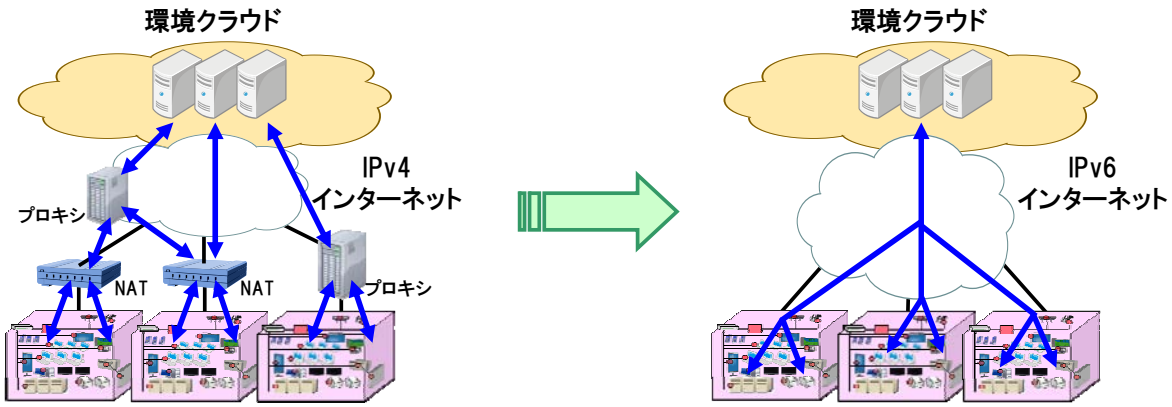


図 3-13　IPv4 と IPv6 における環境クラウドの構成

また、現在利用されている IPv4 アドレスは既に不足状態に陥っており、2011 年 2 月 3 日をもって IANA(Internet Assigned Numbers Authority)管理の IPv4 アドレスは枯渇し､また､APNIC(Asia Pacific Network Information Centre) /JPNIC (Japan Network Information Centre: 社団法人日本ネットワークインフォメーションセンター)における IPv4 アドレスの在庫も 2011 年 4 月 15 日をもって枯渇したと発表されており、今後 IPv4 アドレスの新規取得は困難になると見込まれる。

環境クラウドサービスに IPv6 技術を導入する際の共通的な留意点を以下に示す。

IPv6 導入の考え方

- 環境クラウドにおいては IP アドレス空間の制約を考慮する必要のない､IPv6 技術を活用することが望ましい。
- IPv6 を活用することにより、エンド・ツー・エンドでの通信に係るパフォーマンスが上昇するとともに管理コストの低減につながり、環境クラウドサービスの普及を後押しすることができる。
- IPv6 をサポートしていないクラウド事業者のプラットフォームを環境クラウドで利用する場合には、IPv6 対応を要求していくことが望ましい。

IPv6 の導入手段

環境クラウドサービスを展開する事業者は、JPNIC 等から IPv6 アドレスの割当を受けるか、IPv6 対応の ISP と契約して IPv6 アドレスの割当を受けることにより、IPv6 ベースのサービスを展開することが求められる。

IPv6/IPv4 併存環境への対応

センサーデバイス等が IPv6 対応をしておらず、環境クラウドを構築する際、やむを得ず IPv4 ネットワークを部分的に利用せざる得ない状況が考えられる。また、IPv4 ベースで構築された既存システムは、全て IPv6 化されるまでにいくつかのシステム更改ステップが想定される。このため、環境クラウドを構築する際には、このような IPv6 /IPv4 の併存環境への対応も重要。例えば、ビル群エネルギー管理システムでは、以下のように IPv6 環境へ移行していくことが考えられる。

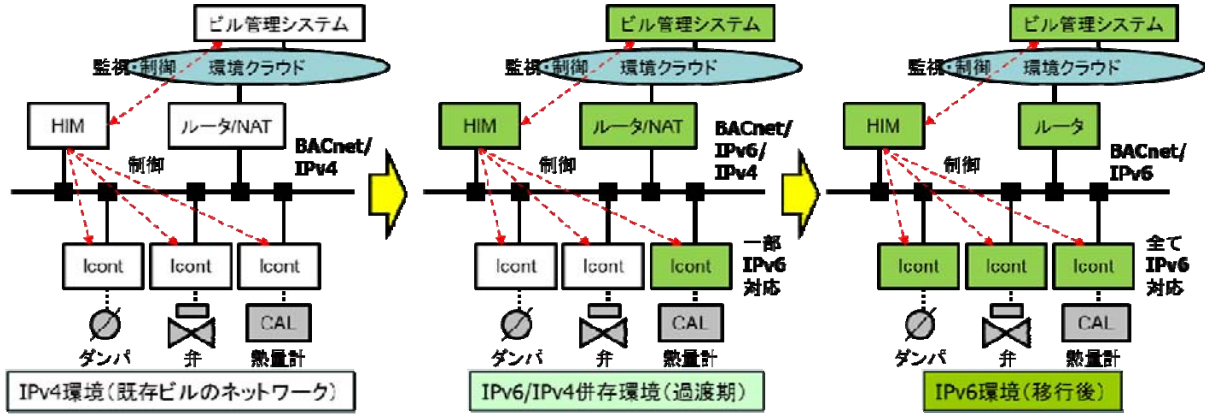


図 3-14　ビル群エネルギー管理システムにおける IPv6 への移行シナリオ（例）

IPv6 フォールバック問題への対処

環境クラウドを構成する際に既存の IPv4 インターネットアクセスに加え IPv 6 閉域網を新規導入する場合には、マルチホーム環境での IPv6 フォールバック問題※１が発生する懸念があり、必要な対処※２を行うことが重要。環境クラウドを構築する際には、このような IPv6 導入に関わる諸問題に対処することが重要である。

※１　IPv6 閉域網とマルチホーミングした端末が、インターネット上のノードにアクセスする際に閉域網側へアクセスを開始してしまう問題。

※２　IPv6 で外部接続性を確保する、または端末にルーティング情報を設定する等の対処が必要になる。

4.　システム構築・運用に係る要件

4.1.　拡張性の確保

本項では、拡張性を確保するために留意することが望ましい要件について、4.1.1.　移植性及び相互

運用性、4.1.2. 事業継続性、4.1.3. 情報管理、4.1.4. 仮想化及び 4.1.5. アプリケーションの開発・運用管理の観点で留意することが望ましい要件を解説する。

4.1.1. **移植性及び相互運用性**

目的：環境クラウドでは、レガシー環境からクラウド環境への移行、異なる環境クラウド基盤やサービスへの移行、他システムとの連携等が想定される。こうした移植性及び相互運用性について、環境クラウドサービス事業者、利用者が満たすことが推奨される要件を明確化する。

環境クラウドサービス利用者の対象施設の管理方針の改定改変等により、環境アプリケーションに新たな機能やより高い処理能力が必要になる場合がある。この際、環境アプリケーション提供者が独自性の高いモジュールを用いた場合には、ていると、環境クラウドサービス利用者は他の環境クラウドサービスへの移行が簡易にできないおそれ可能性がある。また、環境アプリケーションへの新たな機能追加や、環境クラウドサービス利用者の増大等に伴うサービス規模の拡大によって、より高い処理能力のプラットフォームが必要になる場合がある。この際、プラットフォーム提供者が独自性の高いモジュールを用いた場合には、ていると、他のプラットフォームへの移行が簡易にできないおそれ可能性がある。このような状況は環境アプリケーション提供者、プラットフォーム提供者にとっても、ベンダーロックインを避ける利用者の獲得を逃すことになる。

このため、環境クラウドサービス事業者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.1.1.1　異なる仮想化基盤間における移植方法の提供（モデル A 実証実験より得られた知見等）
4.1.1.2　汎用性の高い移植手法の提供（モデル B 実証実験より得られた知見等）
4.1.1.3　標準的なデータ連携用 API の提供（モデル C 実証実験より得られた知見等）
4.1.1.4　セキュリティ対策の文書化
4.1.1.5　多様なデータ移行手段の提供
4.1.1.6　処理能力の確認
4.1.1.7　システムテストの実施

4.1.1.1. **異なる仮想化基盤間における移植方法の提供（モデル A 実証実験より得られた知見等）**

概要

ベンダーロックインを回避し、異なる環境クラウドサービス間での移植性を確保するため、一般的な仮想化基盤の違いを把握し移植方法を提供することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・ 仮想サーバのイメージ形式の変換等仮想化環境の違いを吸収出来るツールの利用

（プラットフォームレイヤー）

・ プラットフォームで利用している仮想化方式における、仮想サーバのイメージ形式の変換ツ

ール等の提供

実証実験により得られた知見

＜モデル A 実証実験を踏まえた知見＞

・環境アプリケーションの設計・構築時に OS やミドルウェアの移植性が考慮されることはあっても、仮想化方式の選定までは考慮されてこなかった。異なる環境クラウドサービス間でのマイグレーションを容易に実現するためには、移設手段が明確化されている仮想化方式を選定することも重要な要素となる。

＜実証内容＞

ベンダーロックインを避けるため、異なる環境クラウドサービス間での移植性を確保することは重要である。実証実験では、環境アプリケーションの導入に際して移植性に関する実験を行った。（図 4-1）。

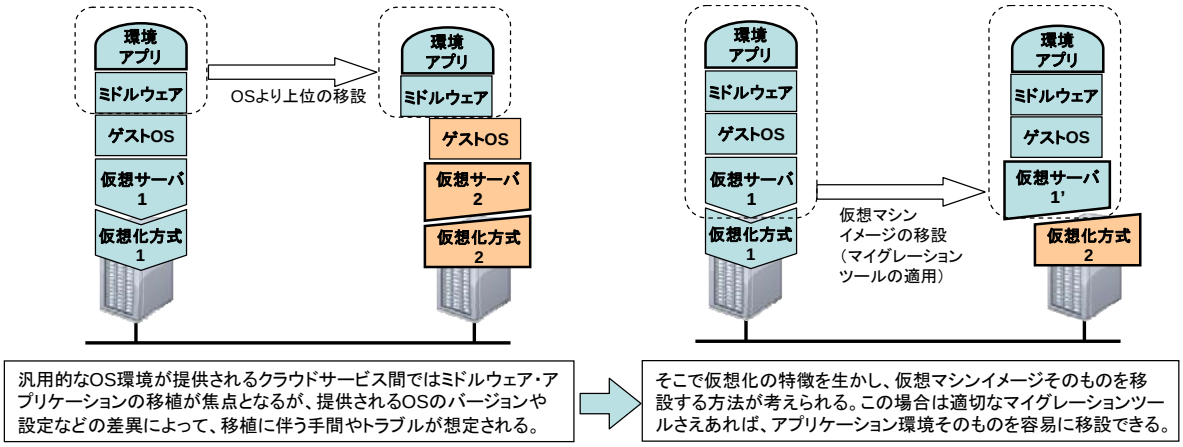


図 4-1　モデル A における異なる仮想化方式への移植の実証

＜実証結果＞

同じ仮想化方式であっても商用とフリーのバージョンの違い等でマイグレーションツールが動作しない場合があった。そのような場合、仮想マシンイメージの移設の際に OS の修復インストールが必要になる等、独自のノウハウが必要になり、かえって移植性が損なわれることが判明した。

4.1.1.2. 汎用性の高い移植手法の提供（モデル B 実証実験より得られた知見等）

概要

環境クラウドサービス利用者の需要に応じた柔軟なサービス移行のため、汎用性の高い移植手法を提供することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・データの種類に依存しない標準化（汎用化）された API を介したデータ移行手段の提供（プラットフォームレイヤー）

・プラットフォーム単位でのサービス移行を想定した汎用的なプラットフォームで動作可能なアプリケーションの提供

実証実験により得られた知見

＜モデル B 実証実験を踏まえた知見＞

・環境クラウドサービスの利用者がサービスを移行する際には、環境クラウドサービス上で蓄積・管理されているデータを取得し、新しいサービスにスムーズに移行できる仕組みが必要となる。この場合、クラウドサービス事業者は、データの移植手法を提供することが重要となる。

＜実証内容＞

都市型施設エネルギー管理システムでは、利用者企業が、環境クラウドサービスから、自社システム及び他社サービスへ移行するニーズをあらかじめ想定する必要がある。そこで、実証実験では、利用者による柔軟なサービス移行を想定した汎用性の高い移行方法について検証を行った。（図 4-2）

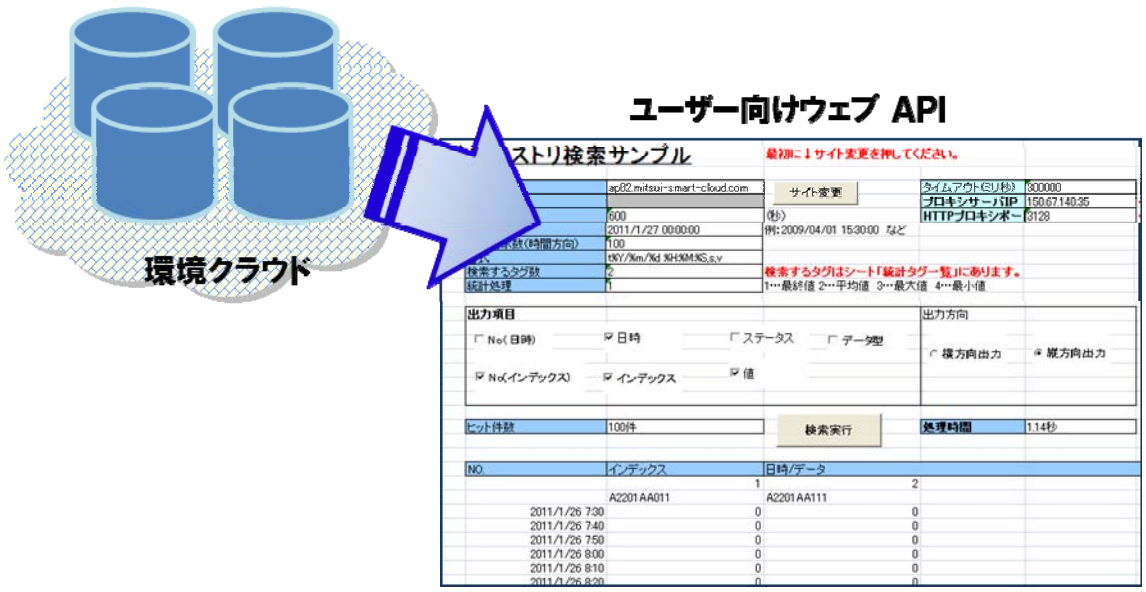


図 4-2　ウェブサービス経由での環境クラウド上のデータの取得に関する実証実験

＜実証結果＞

標準化されている SOAP を活用したデータ移行ツールを開発し、サービス利用者及び分析用データベースを利用者に配布し、利便性を検証した。また、汎用性の高い OS である Linux を用いてアプリケーションを実装し、本番用のクラウド環境から、別環境への OS イメージの移植を実施し、利便性を検証した。標準的なウェブサービスによるデータのダウンロードや汎用性の高い OS を利用したシステムの構築は、サービスの移行を想定した場合、そのデータの移行性の観点から有効であることが明らかとなった。

4.1.1.3. 標準的なデータ連携用 API の提供（モデル C 実証実験より得られた知見等）

概要

外部データベースとの連携やデジタルサイネージ/モバイル端末等への配信等環境クラウドサービスにおけるデータの利活用を円滑にするため、事業者間での柔軟なデータ連携を想定した汎用性の高いデータ連携手法を提供することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・ 外部のデータベースやアプリケーションと連携を行うことを想定した汎用的かつ一般的な API を介してデータアクセス手段の提供

実証実験により得られた知見

＜モデル C 実証実験を踏まえた知見＞

・環境クラウド上で蓄積・管理する情報は、外部のデータベースやアプリケーションと連携することにより、更に有効活用できる可能性がある。この場合、環境クラウドにおいて汎用的な API の提供を行うことによって、こうした外部連携を容易に行えるようになる。

＜実証内容＞

地域内エネルギー供給管理システムでは、EV インフラ等の稼働状況等をウェブ公開するような新規事業者への２次利用目的でのデータの提供を想定する必要がある。また、データ分析を目的とした他の環境データベースとの連携を想定する必要がある。そこで、実証実験では、汎用的なウェブ API により環境クラウド上で蓄積・管理するデータを取得できる仕組みを構築し、その有効性を検証した。（図 4-3）

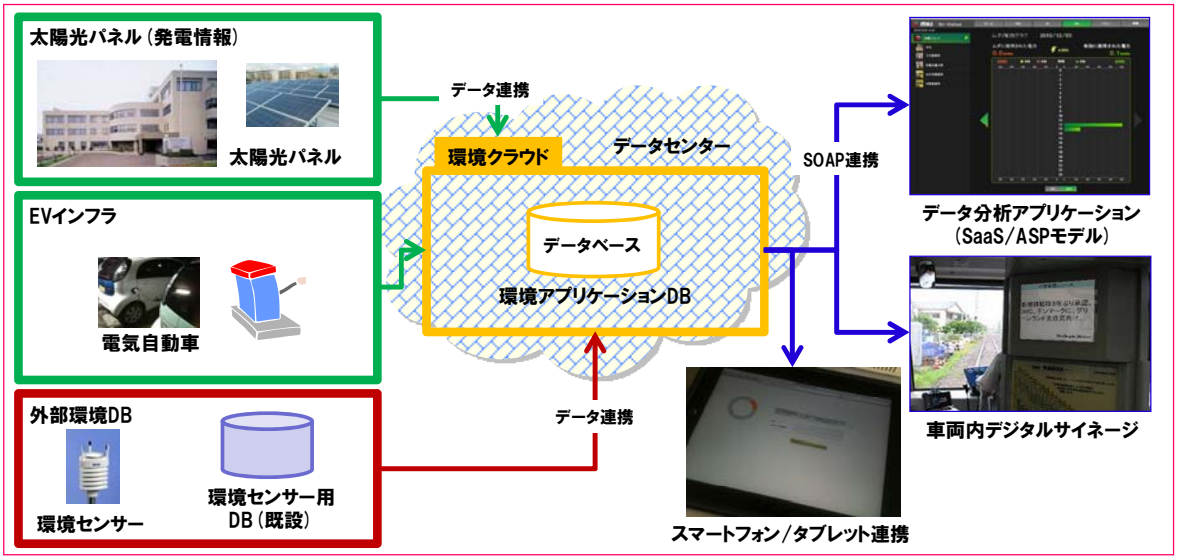


図 4-3　環境クラウドと外部データベース・アプリケーションの連携に関する実証実験

＜実証結果＞
様々なアプリケーションや他の環境データベースとの連携を考えた場合、環境クラウド側でそれらとの連携を考慮した汎用的なウェブ API を提供することが、データ利用の利便性を向上させることが明らかとなった。これにより、データを活用したサイネージ等のアプリケーションが提供され、市民への情報提供という観点で効果があった。環境クラウド上で蓄積・管理する情報を広く一般に提供し、より効果的に分析するためには、外部のアプリケーションやデータベースとの連携が有効であり、その際には汎用的なウェブ API により、環境クラウド上で管理するデータにアクセスできる環境を提供することが重要となる。

4.1.1.4. **セキュリティレベルの比較**

概要

環境クラウドサービスでは、環境クラウドサービス基盤の運営を他社に委託する場合があるため、基盤の移行の必要性が生じた際には、移行先のセキュリティレベルの妥当性を自社の基準等と比較・評価できることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・ 環境アプリケーションで扱うデータの種類、データに対するセキュリティ対策、アプリケーション自体のセキュリティレベルの結果の文書化

（プラットフォームレイヤー）

・ プラットフォームで提供するミドルウェアにおけるセキュリティ対策の文書化

（インフラレイヤー）

・ インフラで提供するオペレーティングシステム、機器、ネットワーク、データセンター設備におけるセキュリティ対策の文書化

【環境クラウドサービス利用者】

・ 事業者のセキュリティレベル及び対策の確認

4.1.1.5. **多様なデータ移行手段の提供**

概要

環境クラウドサービスを円滑に移行するため、センサー数や施設の規模に応じた収集データの容量、データの機密性等に適した多様なデータ移行手段を提供し、選択できることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー）

・ネットワーク経由又は外部媒体等によるデータ移行、データの暗号化等、様々な移行手段の提供

【環境クラウドサービス利用者】

・利用状況に応じたデータ移行手段の確認と選択

4.1.1.6. **処理能力の確認**

概要

環境クラウドサービスでは､大量のデータを収集し､多種多様なデータ分析を行う場合があるため、移行先のプラットフォームで必要とされる処理能力を確保できか確認することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者利用者】

(アプリケーションレイヤー)

・環境アプリケーション提供者による、環境アプリケーションが正常に動作するために十分なパフォーマンスが発揮されるプラットフォームの利用

【環境クラウドサービス利用者】

・事業者の処理能力が十分であることの確認

4.1.1.7. **システムテストの実施**

概要

環境クラウドサービスの移行先において、正常にサービスが動作することを確認するため、システムテストを事前に実施することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

(アプリケーションレイヤー)

・環境アプリケーション提供者による、移行先のプラットフォームのシステムテストの実施

・施設のセンサー等のシステムと環境クラウドサービスの連携を確認するためのシステムテストの実施

【環境クラウドサービス利用者】

・事業者によるシステムテストの実施の有無と結果の確認

4.1.2. **事業継続性**

目的：環境クラウドでは、関連する事業者と利用者（ビル管理事業者、施設管理者、地方自治体等）の要請に基づいて、事業継続性や災害復旧に関わる要件や、それらを実現するためのシステムの信頼性について、特有の留意事項が想定される。こうした事業継続性について事業者等が満たすことが推奨される要件を明確化する。

災害時には、ビジネス中断が長引けば長引くほどビジネスチャンスの喪失による減収、企業評価・信用の失墜が大きくなる。特に環境クラウドサービスは公共性の高いビジネスであるため、その影響度は大きい。また、事業継続性を維持するためには、リスクの把握・想定や、災害復旧計画の導入・運用・見直しなどのプロセスを継続的に行うことが重要となる。

このため、主に環境クラウドサービス事業者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.1.2.1　ディザスターリカバリ機能の確認（モデル A 実証実験より得られた知見等）
4.1.2.2　安定的な制御の実施（モデル B 実証実験より得られた知見等）
4.1.2.3　安定的なデータ収集基盤の提供　（モデル C 実証実験より得られた知見等）
4.1.2.54　無線ベースでのネットワークセキュリティのあり方（モデル C 実証実験より得られた知見等）
4.1.2.5　事業継続計画(BCP)の項目検討
4.1.2.6　BCP の継続的な見直し
4.1.2.7　妥当性のある目標復旧時間

4.1.2.1. **ディザスターリカバリ機能の確認(モデル A 実証実験より得られた知見等)**

概要

ビル群の管理では、特に迅速なサービス復旧が求められる場合があるため、システム障害や自然災害によるサービス中断が発生することに備え、あらかじめディザスターリカバリについて検討することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

(アプリケーションレイヤー)

・環境アプリケーション提供者によるプラットフォームのディザスターリカバリ機能の有無・正常性の確認

(プラットフォームレイヤー)

・プラットフォーム提供者によるプラットフォームレベルでのディザスターリカバリ機能の提供

【環境クラウドサービス利用者】

・事業者によるディザスターリカバリ機能の提供の有無・正常性の確認

実証実験により得られた知見

＜モデル A 実証実験を踏まえた知見＞

・環境クラウドにおいては、リアルタイムのサービス引継ぎが可能なバックアップ体制を用意しておくことが重要であるが、その設計にあたっては、コスト効果の観点からパブリッククラウドを活用することも視野に入れながら検討を行うことが可能である。

＜実証内容＞

環境クラウドでは大量のセンサー情報の収集・分析を伴うため、クラウド基盤のサービス停止が起きた場合、データロスなどの損害も大きい。実証実験では、特定のデータセンター上に障害が発生した場合にも、クラウド上の他のデータセンターにおいてリアルタイムのサービス引継ぎを実施する検証を行った。また、バックアップサイトとしてはプライベートクラウドだけでなく、パブリッククラウドも対象とした。(図 4-4)

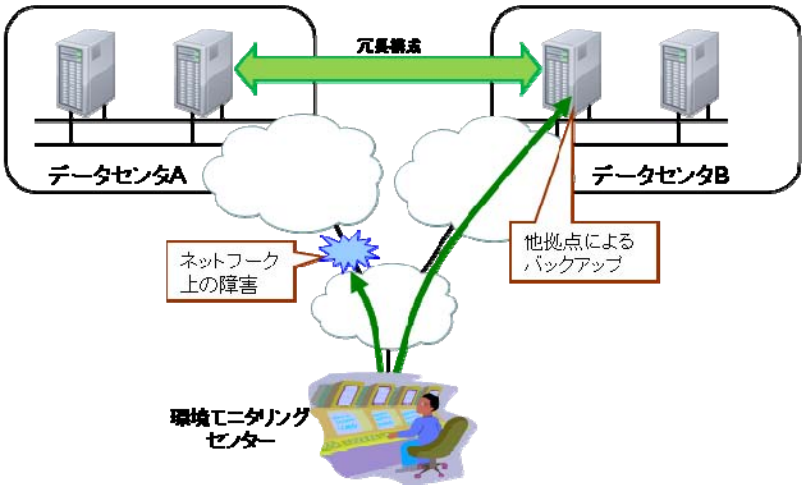


図 4-4　異なるデータセンターを利用した異常時のサービス引継ぎ

＜実証結果＞

地理的に離れた 2 つのデータセンター間で、負荷分散機能を活用した障害時の切り替えを実現した。これにより、片方のデータセンターで障害が発生した場合でもウェブインタフェースを介した環境アプリケーションの利用に影響を与えることなく、高い可用性を維持したサービス提供ができることが明らかになった。また、バックアップサイトはコスト削減のためパブリッククラウドが利用されるケースも想定されるが、プライベートクラウド・パブリッククラウドを横断したサービス引継ぎも実現できた。

4.1.2.2. 安定的な制御の実施（モデル B 実証実験より得られた知見等）

概要

施設設備を監視・制御を環境クラウドサービスからネットワークを通じて実施する場合には、必ずしも既設の有線ネットワークを活用できるとは限らず、無線ネットワーク及び携帯網を利用したネットワークを構成する場合があるため、このようなネットワークにおいて障害が発生した場合であっても、安定した施設の監視・制御が行える仕組みを提供することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー）

・環境クラウドシステムと監視・制御対象の施設の間のネットワーク環境に依存しない安定的な施設の監視・制御の実現

実証実験により得られた知見

＜モデルＢ実証実験を踏まえた知見＞

・環境クラウドサービスを提供する際には、環境クラウドと監視・制御対象の間のネットワークにおいて障害等が発生し、環境クラウドから監視・制御を行えなくなる可能性がある。こうした事態に備え、施設内にゲートウェイを設置し、一時的な監視・制御を行える仕組みを提供することが事業継続性を高めることになる。

＜実証内容＞

施設の機器制御を必要とするサービスでは、ネットワーク状況によらずサービス継続性の確保が求められることを想定する必要がある。そこで、実証実験では、通信回線の障害等が発生した場合にも、安定した制御を実現する手法について検証を行った。（図 4-5）

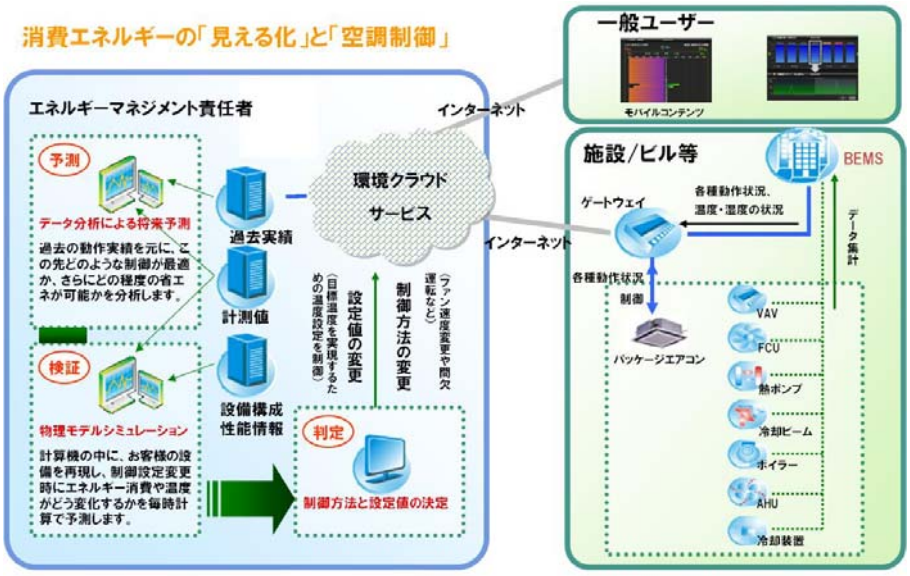


図 4-5　ゲートウェイモデルによる安定的な施設設備機器の監視・制御に関する実証実験

＜実証結果＞

サービス利用者の施設に設置したゲートウェイを介して、ゲートウェイと環境クラウドアプリケーション間の通信が遮断された場合でも安定した制御が行えることを確認した。また、ゲートウェイについては、実証実験参加企業（特に設備管理担当）より、施設側に設置する場合、機器がコモディティハードウェアで構成されていること、事前に既設設備ネットワーク（BEMS 以外では課金システム等）に影響が出ないことを求められるケースが多い。ゲートウェイにおけるベンダーロックインを避ける観点からも、事業者がゲートウェイのオープン性と汎用性を担保することが重要である。

4.1.2.3. **安定的なデータ収集基盤の提供（モデル C 実証実験より得られた知見等）**

概要

環境クラウドサービスでは、監視の対象となる施設において、設備機器が不定期に更新される場合があるため、設備機器が更新された場合であっても引続き利用できる仕組みを検討することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・設備機器が更新された場合であっても利用者が継続してサービスを利用可能なアプリケーションの設計

実証実験により得られた知見

＜モデル C 実証実験を踏まえた知見＞

・回線障害等の理由により、計測データに欠損が発生すると環境クラウドサービスが提供するデータの信頼性に問題が発生する可能性がある。設備機器に設置する計測装置において、データの送出リトライ機能を実装し、定期的に送出できなかったデータを自動的に再送出する仕組みを取り入れることにより、データの欠損を軽減することができる。

＜実証内容＞

廉価に環境クラウドを構築しつつも、高い事業継続性を求められることを想定したシステムを構築するため、実証実験では、計測機器と環境クラウド間の通信における事業継続性の向上を目的とし、機器とサーバの通信が途切れた場合であっても、回線復旧時に自動的にデータの再送を行える仕組みの検証を行った。（図 4-6）

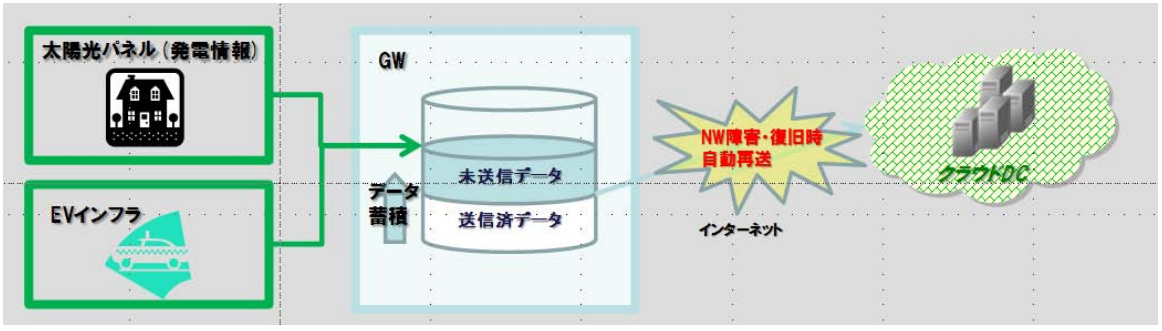


図 4-6　回線障害によるデータ欠損の軽減に関する実証実験

＜実証結果＞

ネットワーク障害復旧時に自動的にデータをリトライ出来るプログラムを実装することで、データの欠損を軽減できることを検証した。これにより、回線障害が発生し、定期的なデータの送出ができなかった場合でも、ネットワーク障害回復後にデータを再送し、欠損を軽減できることを確認した。

このような仕組みは、外部アプリケーションとデータ連携している場合、環境クラウドとアプリケーションの間の通信にも適用することが重要である。

4.1.2.4. 無線ベースでのネットワークセキュリティのあり方(モデルC実証実験より得られた知見等)

概要

環境クラウドサービスでは、屋外に設置された設備機器の監視・制御などに際して、有線 LAN を利用できず、無線 LAN 及び携帯網を利用してシステムを構築する場合があるため、そのようなシステムを構築する際の情報セキュリティの在り方をあらかじめ検討することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（インフラレイヤー）

・無線ネットワークを活用したシステム構築を想定したセキュアな設備機器の監視システムの在り方の検討

4.1.2.5. 事業継続計画（BCP）の項目検討

概要

環境クラウドサービスでは、環境アプリケーション提供者、プラットフォーム提供者に責任が分かれ、BCP が複雑になる場合があるため、レイヤーごとに網羅的に BCP を検討することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・国際標準規格（例えば、BS25999 等）を用いた網羅的な BCP の検討及び認証の取得

【環境クラウドサービス利用者】

・事業者による BCP 検討や認証取得の確認

4.1.2.6. BCP の継続的な見直し

概要

環境クラウドサービスでは、環境アプリケーション提供者、プラットフォーム提供者に責任が分かれる場合があり、BCP をより実効性の高いものにするため、継続的に BCP の見直しを行うことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・最新の事業状況や技術動向を考慮した BCP の継続的な見直し

【環境クラウドサービス利用者】

・事業者における BCP 見直しの確認

4.1.2.7. **妥当性のある目標復旧時間**

概要

環境クラウドサービスでは、環境アプリケーション提供者、プラットフォーム提供者に責任が分かれる場合があり、サービス品質を保証するため、各レイヤーでの復旧施策を考慮して、妥当性のある目標復旧時間を設定することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・技術、運用側面から検討された妥当性のある目標復旧時間の設定

【環境クラウドサービス利用者】

・事業者が設定した目標復旧時間の妥当性の確認

4.1.3. **情報管理**

目的：環境クラウドでは、利用者から収集したデータを加工し、事業者間で共有することや、加工して２次利用等を行ことが想定される。また、収集する環境情報は、プライバシー情報や企業の機密情報等に間接的あるいは直接的に関わる可能性を有する。こうした情報管理について事業者等が満たすことが推奨される要件を明確化する。

環境アプリケーション提供者とプラットフォーム提供者では、実施している情報管理施策が異なることが考えられるため、収集したデータを提供者間で共有する場合には、それぞれが実施している情報管理施策について確認し、データセキュリティライフサイクルである作成→保存→利用→共有→アーカイブ→廃棄の過程を踏まえて考慮しなければならない。

このため、主に環境クラウドサービス事業者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.1.3.1　定期的なバックアップ・リストアの実施による分離保存の確認（モデル A 実証実験より得られた知見等）

4.1.3.2　蓄積データの暗号化によるデータ安全性の確保（モデル A 実証実験より得られた知見等）

4.1.3.3　２次利用データの適切な情報提供の合意形成（モデル B 実証実験より得られた知見等）

4.1.3.4　情報提供及び２次データ利用者との合意形成　（モデル C 実証実験より得られた知見等）

4.1.3.5　データの完全性の確保と証明

4.1.3.6　データへのアクセス制御による適切なデータ利用権限の付与

4.1.3.7　ログや監視ツールを用いたアクセスモニタリングによるアクセス制御効果確認

4.1.3.8　マルチテナント環境を考慮したバックアップデータ分離保存及びアクセス制御

4.1.3.9　契約終了、中途解約時の情報の扱いの明確化

4.1.3.1. 定期的なバックアップ・リストアの実施による分離保存の確認（モデル A 実証実験より得られた知見等）

概要

環境クラウドサービスに用いられる技術の更改が行われる場合があるため、定期的にバックアップ・リストアを実施し、データの論理的な分離や管理が継続して有効に機能していることを確認することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーションで扱うデータの定期的なバックアップの実施及びバックアップデータが他の利用者と適切に分離されていることの確認

【環境クラウドサービス利用者】

・事業者によるバックアップ・リストアの方法、定期性等の妥当性の確認

実証実験により得られた知見

＜モデル A 実証実験を踏まえた知見＞

・環境クラウドで大規模なビル群を一括管理するためには、ログの出力レベル等の情報保持の粒度や、クラウドのストレージ確保等、注意深い設計・運用が必要になると考えられる。

＜実証内容＞

実証実験では、管理対象の 4 棟のビルのセンサー情報等を環境クラウド上に配置したビル群エネルギー管理システムへ集約し、クラウド上で分析・可視化を行う運用を 3 ヶ月に渡って実施した。（図 4-7）

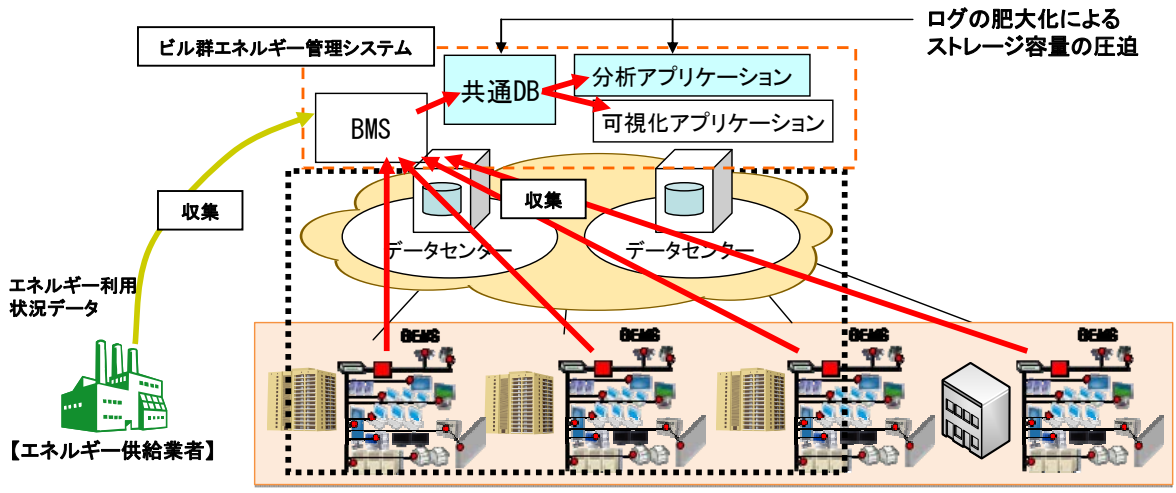


図 4-7　モデル A における情報管理に関わる実証

＜実証結果＞

ビル群エネルギー管理システムの主要コンポーネントである共通データベース（DB)、分析アプリケーションにおいてそれぞれ運用データのトランザクションログ（MSSQL)、アプリケーションログ（テキスト）が肥大化し、当初想定していたストレージ容量を大幅に上回ったため、定期的なメンテナンスが必要となった。これは４棟のビルのセンサー情報の一元管理、さらにその広範な分析という規模の大きさによって引き起こされた設計・運用上の課題点と言える。また、ビルごとにビル管理システムが独立して設計・運用されていた時には顕在化しなかった問題点が、環境クラウドによるビル群一元管理によって表出してきた１つの例でもある。

4.1.3.2. **蓄積データの暗号化によるデータ安全性の確保（モデルＡ実証実験より得られた知見等）**

概要

環境クラウドサービスでは、ビル施設に関するセンサー情報だけではなく、オーナーやテナントの情報も扱う可能性があるため、蓄積データに対する安全性を確保することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者によるアプリケーションデータへの適切な暗号化の実施

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者によるプラットフォームレベルでの暗号化の実施及び強力なストレージ暗号の利用

【環境クラウドサービス利用者】

・事業者によるデータに対する暗号化等の安全性確保手段の確認

4.1.3.3. **２次利用データの適切な情報提供の合意形成（モデルＢ実証実験より得られた知見等）**

概要

環境クラウドサービスでは、サービス事業者が異なる複数の施設から情報を収集・管理する場合があるため、収集情報の２次利用を行う場合にはあらかじめサービス利用者の許諾に基づいて適切に情報の加工・編集を行うことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・収集データの見方によっては企業活動を推測出来る可能性があること等に留意した目的外の活用方法に対する事前検討

【環境クラウドサービス利用者】

・情報の２次利用に関する事業者の方針及び合意形成手段の確認

実証実験により得られた知見

＜モデル B 実証実験を踏まえた知見＞

・環境クラウド上で蓄積・管理するデータの２次利用を行う際には、あらかじめ利用用途、利用範囲、利用期限等を明確にした上で、データの提供者、サービス事業者、分析用データ利用者の間で合意形成を行っておくことが重要となる。

＜実証内容＞

利用者に対する見える化/分析/制御サービスの提供とともに、都市レベルでの更なる環境負荷軽減目標達成を目的とした研究目的での分析用データベース（DB）の提供を想定されるため、実証実験の実施に当たっては、サービス提供者と利用者間での合意形成が重要となる。また、研究目的で利用するに辺り、分析の有効性が損なわれない機密情報隠蔽等の加工が求められる。これらの要件について、検証を行った。（図 4-8）

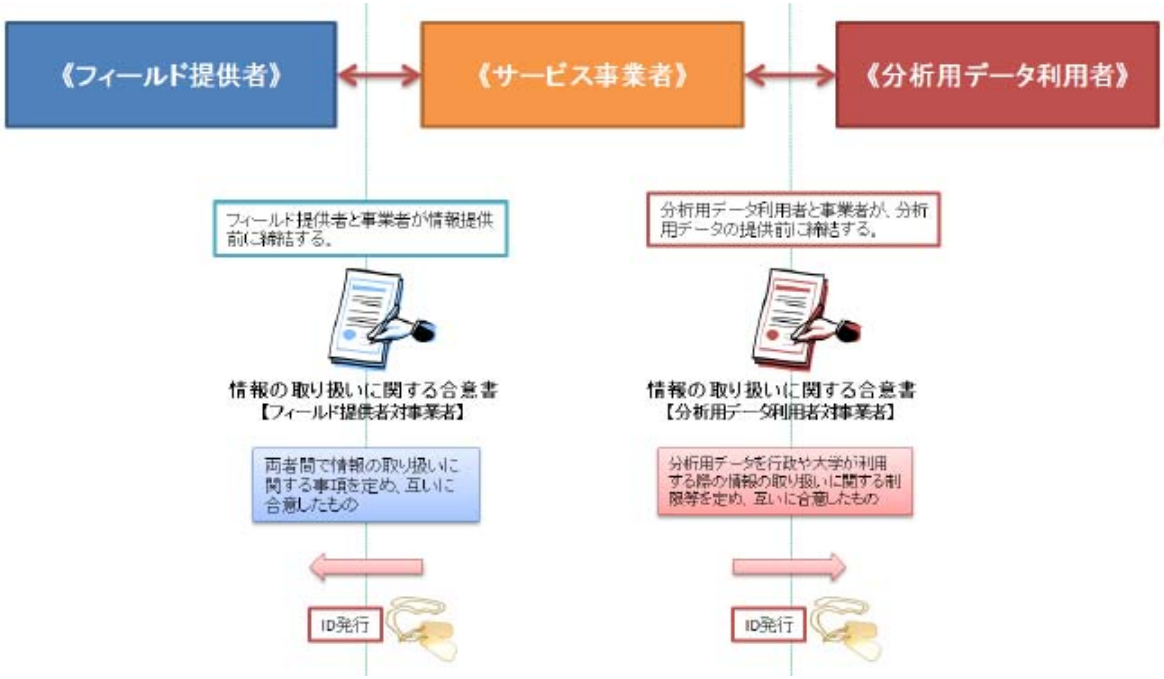


図 4-8　データの２次利用時における権利処理に関する実証実験

＜実証結果＞

実験参加者へのヒアリングを通じて、情報の出し手と受け手で双方の合意に基づき、情報の取り扱いを定めるケースについて検討した。また、企業帰属データに対して、個別施設情報等が特定されない形での分析用データベース（DB）構築の在り方を検討した。

収集情報自体は、個人情報、機密情報、プライバシー情報のいずれにも該当しないが、間接的に企業の活動状況を把握することができる可能性があるため、分析用 DB 利用者への開示タイミングについてはあらかじめ合意が必要という意見がでた。分析用 DB 利用者に対しては、あらかじめ提供の合意、利用期間の明確化、データの出所の明記、サービス利用者の不利益を生じさせないプライバシーの加工について、事前に協議・合意することが必要との意見が出た。

4.1.3.4. **情報提供及び２次データ利用者との合意形成（モデルＣ実証実験より得られた知見等）**

概要

環境クラウドサービスでは、分散電源やEVインフラ等から環境情報を収集し、許諾に基づいて収集情報の２次利用を行う場合があるため、収集・管理データの市民への一般公開や有識者等の２次利用時には適切に情報を加工・編集することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー／インフラレイヤー）

・ 環境クラウドサービス上で蓄積・管理されるデータの市民への一般公開及び将来的な商用アプリケーションでの利用を想定した情報の利用範囲、権利に対する合意形成の在り方の検討

【環境クラウドサービス利用者】

・情報の２次利用に関する事業者の方針及び合意形成手段の確認

実証実験により得られた知見

＜モデルＣ実証実験を踏まえた知見＞

・収集・蓄積するデータは、広く市民に提供されるが、２次加工情報をアプリケーション事業者が次世代エネルギー利用促進等の目的で利用する可能性があることも想定する必要がある。

＜実証内容＞

収集・管理データの市民への一般公開や事業者等の２次利用等において、公開・提供情報における適切な情報の加工・配信が求められるため、その取り決めについて検証を行った。（図 4-139）

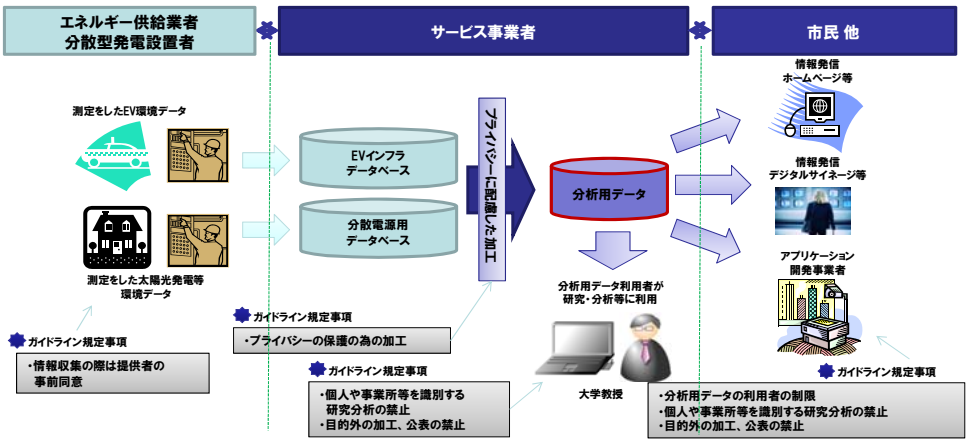


図 4-9　データの２次利用時における権利処理に関する実証実験

＜実証結果＞

参加者へのヒアリングを通じ、データ公開時の合意形成の在り方について検討した。また、集計さ

れたデータの他事業者(アプリケーション業者等)が利用する場合の合意形成の在り方について検討した。

太陽光発電量、EV インフラ、環境情報に関しては公共性の高いデータであり、公開に関しては特に問題ないのではという意見もあった。しかしながら、初期のデータ蓄積段階では、データボリュームの少なさから意図しないデータ分析がされる可能性について留意すべきではという意見が出た。また、データ提供者に関しては、提供するインセンティブが必要であり、また、提供に関して契約で管理することは難しいと予想されるため、どのような形で合意形成を図るかが重要という意見が出た。

また、今回の実証実験では、設備機器情報に ID を付け、2 次利用者に提供を行った。事業展開の際、対象設備機器が増加することを考えるとネーミングルール等のルール化が必要と言う意見が出た。IPv6 アドレスをユニークなキーとして管理することで設備機器の管理面だけではなく、分析の効率性が上がる可能性があるという意見もあった。

4.1.3.5. **データの完全性の確保と証明**

概要

環境クラウドにおいて収集されたデータは、エネルギー消費量の報告書に記載される元データとなることや、環境アプリケーションによる分析・可視化によって今後の運転計画に反映されるだけでなく、監査の際に求められる場合があるため、情報管理においてデータの完全性が保たれることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者によるデータの完全性を検証するための施策の実施

【環境クラウドサービス利用者】

・事業者によるデータの完全性を保証するための施策の実施の確認

4.1.3.6. **データへのアクセス制御による適切なデータ利用権限の付与**

概要

環境クラウドサービスでは、環境クラウドサービス利用者、環境アプリケーション提供者、プラットフォーム提供者の複数の利用者・事業者が存在する場合があり、第三者による不正なデータ利用を防止するため、それぞれの利用者・事業者間で、データへのアクセス権限の所有者を明確にし、その権限に沿ってアクセス制御が行われることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー、インフラレイヤー）

・環境アプリケーション提供者とプラットフォーム提供者の間におけるデータ参照、追加、変

更、削除等アクセス権限に関する責任の明確化

【環境クラウドサービス利用者】

・事業者との間におけるデータ参照、追加、変更、削除等アクセス権限に関する責任分担の確認

4.1.3.7. **ログや監視ツールを用いたアクセスモニタリングによるアクセス制御効果確認**

概要

環境クラウドサービスでは、施設の管理情報など機密性の高い情報を扱う場合があるため、データに対して環境クラウドサービス利用者、環境アプリケーション提供者、プラットフォーム提供者の適切なアクセス権限を設定し、データアクセスのモニタリングを行い、意図通りに権限を持った利用者のみが利用可能であることを確認することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者による環境アプリケーションで利用するデータへのアクセスのモニタリングとアクセス制御の正常動作確認

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者によるプラットフォームへのアクセスのモニタリングとアクセス制御の正常動作確認

4.1.3.8. **マルチテナント環境を考慮したバックアップデータ分離保存及びアクセス制限**

概要

環境クラウドサービスでは、仮想化によるマルチテナント環境においてエネルギー管理情報等機密性の高い情報を利用する場合があるため、不用意に他の利用者のバックアップデータにアクセスできないようにすることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者による利用者ごとのデータバックアップ機能の分離

（プラットフォームレイヤー）

・プラットフォーム提供者による環境アプリケーション提供者ごとのデータバックアップ機能の分離

4.1.3.9. **契約終了、中途解約時の情報の扱いの明確化**

概要

環境クラウドサービス利用者が委託先の事業者を円滑に変更・中途解約できるようにするため、契約終了時の情報の取り扱いを明確化しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス利用者】

・契約終了、中途解約時における情報資産の消去、廃棄に関する事項の契約書への明記

4.1.4. **仮想化**

目的：仮想化技術に由来するセキュリティリスクに加え、計測・制御対象の機器/設備数の増加や関係する事業者の要請等への対応等、仮想化基盤のスケーラビリティの観点での留意事項が想定される。こうした仮想化について事業者等が満たすことが推奨される要件を明確化する。

環境クラウドサービスで提供されるサーバリソースは、仮想化技術を用いることによって必要に応じて柔軟に供給される。これらのサーバリソースはハイパーバイザーと呼ばれる OS によって管理・制御が行われため、仮想化環境特有の新たなセキュリティリスクとして、悪意を持った利用者がハイパーバイザーを攻撃し、サービス停止に陥らせることや、仮想マシンを不正に操作することが考えられる。また、仮想化によりハードウェアの内部に仮想マシン間のネットワークが隠蔽されるため、従来と異なるネットワーク監視方法が運用者に求められる。一方で、環境クラウドでは計測・制御対象の機器/設備数の増加が見込まれ、関係する事業者の要請等への対応等、仮想化基盤のスケーラビリティの観点での留意事項も想定される。

このため、環境クラウドサービス事業者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.1.4.1　利用者の増加に対するスケールの確保（モデル B 実証実験より得られた知見等）

4.1.4.2　計測対象の増加に対するスケールの確保（モデル C 実証実験より得られた知見等）

4.1.4.3　仮想ネットワークのモニタリングによる仮想マシン間通信の安全性の確保

4.1.4.4　ゲスト OS へのセキュリティ技術の適用による多層防御

4.1.4.5　仮想マシンイメージの完全性の確保

4.1.4.6　認証に基づく仮想マシン管理機能へのアクセス制限

4.1.4.1. **利用者の増加に対するスケールの確保（モデル B 実証実験より得られた知見等）**

概要

環境クラウドサービスでは、サービスの普及に伴い、事業者数・施設数が飛躍的に増加することが想定されるため、サービスを利用する事業者数の増加に対応した可用性、脆弱性等のセキュリティ要件に留意することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・同一サービスを利用する事業者間でのデータ漏えいを防止するためのデータ管理手法の在り方の検討

（プラットフォームレイヤー）

・ 事業者単位でデータベースを構築する際におけるプラットフォーム（仮想化システム）のCPU、メモリ、ディスク等のサイジング方法の検討

実証実験により得られた知見

＜モデルB実証実験を踏まえた知見＞

・環境クラウドサービスの普及を見越して、システムがスケーラブルかつセキュアであることをあらかじめ検証しておくことが重要である。

＜実証内容＞

サービスの普及に伴い、対象となる都市内の施設を管理するサービス利用事業者が増加（＝事業者単位データベース（DB））を想定したシステムを構築する必要がある。そこで、実証実験では、①事業者DBの増加を想定したスケールアウト（可用性）、②外部からの不正アクセス及び不正アクセスの検知（脆弱性）、③制御を想定したアプリケーションの脆弱性（脆弱性）について検証を行った。（図 4-1310）

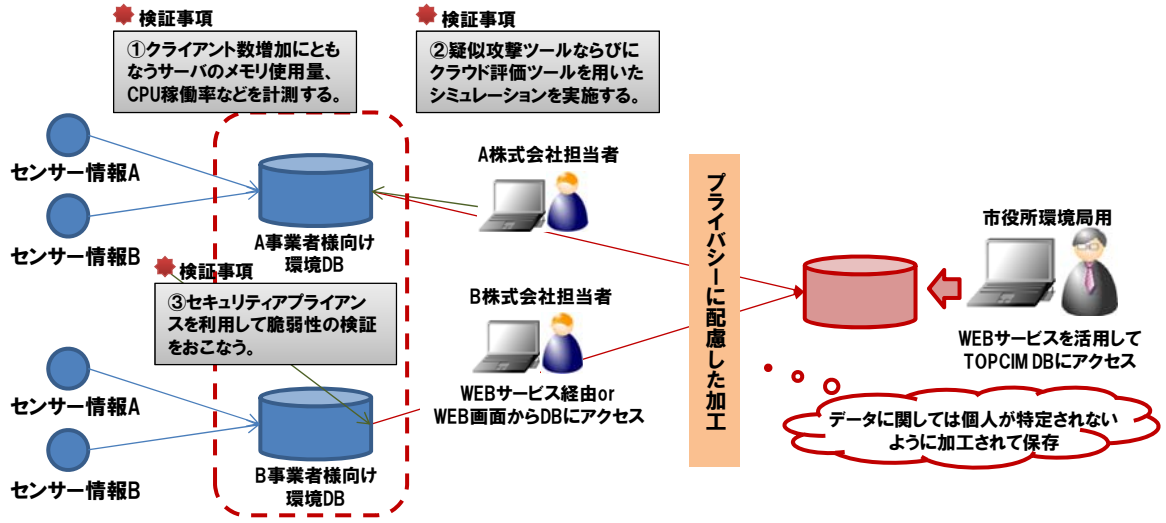


図 4-10　サービス利用者の増加に対応した仮想システムの構築に関する実証実験

＜実証結果＞

本番環境とは別のシミュレーション環境に 100 事業者分のアプリケーションを構築し、データ登録・ダウンロード等を仮想クライアント 100 台からランダムに行うシステム耐性の検証を行った。この際、シミュレーション環境を用意し、利用者数増加に伴う、例えばメモリ使用量、CPU 稼働率などを計測し環境構築時のサイジングについて検証した。また、疑似攻撃シミュレーションの実施によりシステム耐脆弱性について検証した。これらの検証をあらかじめ十分に行なっておくことで、サービス利用者が増加した場合であっても、安全かつ安定的にサービスを提供できることが明らかとなった。

4.1.4.2. 計測対象の増加に対するスケールの確保（モデル C 実証実験より得られた知見等）

概要

今後、環境クラウドサービスにおいて計測対象設備として利用される EV インフラや分散電源の急速な普及が見込まれるため、それらの機器から安定的に情報を収集可能なシステムを構築することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー）

・対象設備の急激な増加想定した安定的なデータ収集環境及びそのシステム環境(主にネットワークとトラヒックに関するサイジング等)の実装

実証実験により得られた知見

＜モデル C 実証実験を踏まえた知見＞

・環境クラウドサービスを介して計測・監視する設備機器の増加を見越して、システムがスケーラブルかつセキュアであることをあらかじめ検証しておくことが重要である。

＜実証内容＞

分散電源や EV インフラの急速な普及に伴い、計測ポイント数が急激に増加することをあらかじめ想定する必要がある。実証実験では、①計測ポイント数が急激に増加したケースを想定した場合のスケールアウト（可用性）、②外部からの不正アクセス及び不正アクセスの検知（脆弱性）、について検証を行った。（図 4-1311）

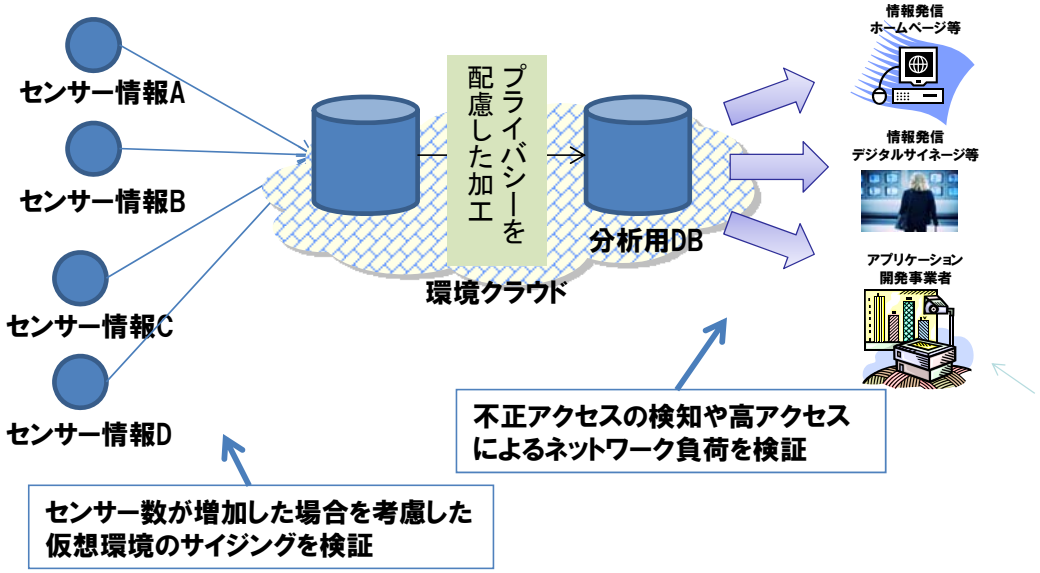


図 4-11　監視対象の増加に対応した仮想システムの構築に関する実証実験

＜実証結果＞

シミュレーション環境を構築し、計測ポイントが増加した場合のサイジングを行い、システムの可用性を検証した。また、ファイアウォールの実証及びセキュリティアプライアンスを利用してのシステムの耐脆弱性を検証した。これらの検証をあらかじめ十分に行なっておくことで、サービス利用者が増加した場合であっても、安全かつ安定的にサービスを提供できることが明らかとなった。

4.1.4.3. **仮想ネットワークのモニタリングによる仮想マシン間通信の安全性の確保**

概要

環境クラウドサービスでは、複数の利用者が仮想化技術を活用して単一の物理サーバを利用する場合がある。従来の監視システムにより、論理的に存在する仮想ネットワーク上のトラヒックを直接監視することは困難なため、仮想ネットワークのモニタリングの手段を確保し、仮想マシン間通信の安全性を確保することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（インフラレイヤー）

・プラットフォーム提供者による仮想アプライアンス製品の導入等による不正トラヒックの監視・検知

実証実験により得られた知見

＜モデル A 実証実験を踏まえた知見＞

・仮想アプライアンス製品等の導入により、仮想ネットワーク上のセキュリティの確保が可能であること。

＜実証内容＞

クラウドサービスの普及に伴い、仮想化環境のセキュリティ対策に特化した仮想アプライアンス製品がセキュリティベンダーから提供されている。そのようなセキュリティ製品を利用することで、仮想ネットワーク上の通信をモニタリングすることが可能になる。実証実験では、環境アプリケーションを展開している仮想化環境に、仮想ネットワーク上の通信のモニタリング・フィルタリングが可能となる仮想アプライアンスを導入し、不正トラヒックへの対策を実証した。(図 4-1312)

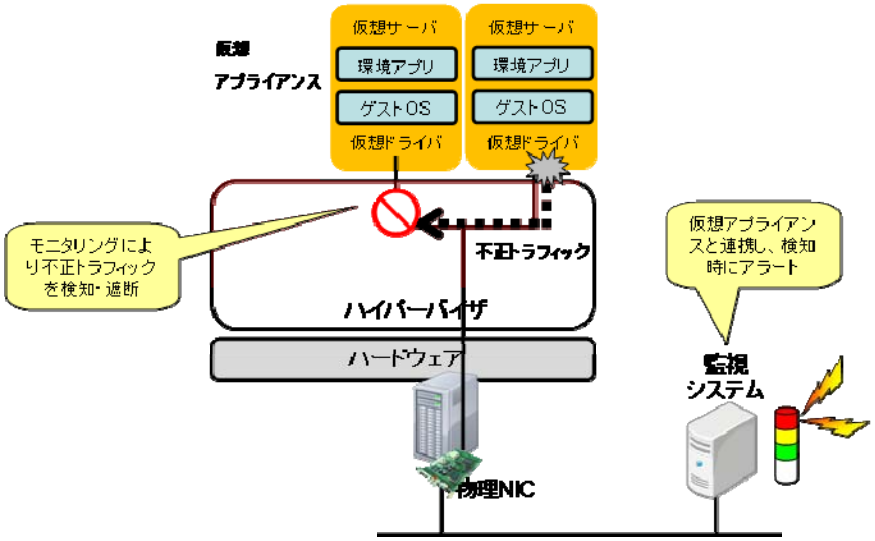


図 4-12　環境クラウドサービスにおける、仮想サーバ間の通信の監視

＜実証結果＞

実証実験により、仮想ネットワーク上の不要なトラヒックを検知・遮断できることが確認でき、高いセキュリティレベルでの環境クラウドサービスの運用が可能であることが明らかとなった。

4.1.4.4. **ゲストＯＳへのセキュリティ技術の適用による多層防御**

概要

環境クラウドサービスでは、環境アプリケーション提供者、プラットフォーム提供者が分かれる場合があるため、プラットフォームのセキュリティ施策に依存せずにセキュリティレベルを確保できるよう、多層的な防御を実施することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーションで扱うデータやプラットフォーム上の既存のセキュリティ対策を考慮したアンチウイルスソフト、IDS/IPS、暗号化機能などの多層防御の導入

4.1.4.5. **仮想マシンイメージの完全性の確保**

概要

環境クラウドサービスでは、公共性の高い情報を取り扱う場合があり、サービス停止による利用者への影響が大きいため、第三者による改ざんにさらされないよう、仮想マシンイメージファイルの完全性を確保することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（インフラレイヤー）

・プラットフォーム提供者によるバックアップ・リストア時のイメージファイル同一性の保証

4.1.4.6. 認証に基づく仮想マシン管理機能へのアクセス制限

概要

環境クラウドサービスでは、エネルギー管理に関する機密性の高いデータや設備オーナーやテナント等の情報を扱う場合があるため、万全なセキュリティを確保するために仮想マシンの管理機能へのアクセス制限を厳格に行うことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（インフラレイヤー）

・プラットフォーム提供者による仮想マシン管理機能への強固な認証方式の実装

4.1.5. アプリケーションの開発・運用管理

目的：環境クラウドでは、その普及促進を図る上で、ネットワーク上で動作するアプリケーションの開発・展開のベストプラクティス等を提示することが重要と想定される。こうしたアプリケーションの開発・運用管理について事業者等が満たすことが推奨される要件を明確化する。

環境アプリケーションをクラウド上で利用することで発生する新たなセキュリティリスクに対応することのプライオリティは高い。このため、環境クラウドサービス事業者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.1.5.1 標準的なウェブ API を介したデータアクセス手段の提供 （モデル C 実証実験より得られた知見等）

4.1.5.2 不要なサービスの停止

4.1.5.3 アプリケーションログの管理

4.1.5.4 アプリケーションのセキュリティ評価

4.1.5.5 プラットフォームへの攻撃に対する防御の実施

4.1.5.1. 標準的なウェブ API を介したデータアクセス手段の提供（モデル C 実証実験より得られた知見等）

概要

環境クラウドサービスでは、多様な端末（モバイル端末やデジタルサイネージ等）に対して情報提供を行うことが想定されるため、事業者はモバイルやサイネージ用コンテンツを作成可能となる API を提供することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者による複数のデバイスからの参照に対処するための標準的なAPIの提供

・環境アプリケーション提供者による参照・統計処理の際のデータアクセスに対するシステム耐性評価の実施

4.1.5.2. **不要なサービスの停止**

概要

外部公開サーバ上で稼働している他のサービスの脆弱性を利用した環境情報の改ざん等のリスクを軽減するため、不要なサービスを停止することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境クラウドサービス運用に必要なアプリケーションのみでの運用

4.1.5.3. **アプリケーションログの管理**

概要

環境アプリケーションが出力するログやシステムログにより環境アプリケーションが扱うセンサーや施設等の情報が第三者に推測されるおそれがあるため、その機密性に留意することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者によるアプリケーションログの取得及び安全な場所への隔離

（プラットフォームレイヤー）

・プラットフォーム提供者によるシステムログの取得及び安全な場所への隔離

4.1.5.4. **アプリケーションのセキュリティ評価**

概要

環境アプリケーションの完成時点で内在する脆弱性や、アプリケーション更改時点で発生する脆弱性、運用中に発現する新たなセキュリティ脅威に係る脆弱性等に対処するため、適切な時点でアプリケーションのセキュリティ評価を実施することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者による適切な時点でのアプリケーションの脆弱性評価の実施

（プラットフォームレイヤー）

・環境アプリケーション提供者による適切な時点でのプラットフォーム上での脆弱性評価の実施

4.1.5.5. **プラットフォームへの攻撃に対する防御の実施**

概要

環境クラウドサービス上で蓄積・管理されるデータを活用する際、環境クラウドサービス利用者に提供される汎用的な API がプラットフォームに対する攻撃を引き起こす可能性があるため、その防御を行うことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー）

・汎用的な API の提供に当たっての XSS や SQL インジェクション等代表的な攻撃手法に対するシステム耐性評価の実施

4.2. **情報セキュリティの確保**

本節では、情報セキュリティを確保するために、4.2.1. 責任分界点の設定、4.2.2. ガバナンス及びエンタープライズリスクマネジメント、4.2.3. 法制度及び電子情報の開示、4.2.4. コンプライアンス及び監査、4.2.5. ID 管理とアクセス管理、4.2.6. 暗号化及び鍵管理及び 4.2.7. インシデント対応、データセンターの安全性確保、運用管理の観点で留意することが望ましい要件を解説する。

4.2.1. **責任分界点の設定**

目的：環境クラウドサービスが委託等により複数の事業者によって提供される場合、環境情報の管理の責任分界点が設定されていなければ、インシデント発生時の賠償等に関する紛争の発生や、インシデント対応の遅延、不十分なセキュリティ施策等環境クラウドサービスのセキュリティレベルへ深刻な影響が出る可能性もある。こうした責任分界点の設定について事業者等が満たすことが推奨される要件を明確化する。

環境クラウドサービスにおいては、環境アプリケーション提供者とプラットフォーム提供者の 2 つのサービス提供者と、環境クラウドサービスを利用する環境クラウドサービス利用者が存在する。それぞれ提供者、利用者の責務の範囲を明確にし、あらかじめ責任分界点を設定することが重要となる。

このため、主に環境アプリケーション提供者、プラットフォーム提供者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.2.1.1. 既設施設管理システムとの接続（モデル A 及びモデル B 実証実験より得られた知見等）

概要

既設の施設管理システムの中には、インターネットなど外部ネットワークへの接続をあらかじめ想定しないシステムも多数存在しているため、このようなシステムを環境クラウドと接続する際には、システム連携に係る責任分界点を明確にしておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・既存システムの環境要件、外部システムに接続する際のセキュリティリスク及びそれらの対策の明確化
・外部との連携に関わる責任分界の環境クラウドサービス利用者への明確な説明の実施
・最適なデータ接続方法の選択
・既設設備への影響度の事前確認（主に施設管理者及び設備管理業者に対して）

【環境クラウドサービス利用者】

・環境クラウドサービス事業者との間の外部との連携に関わる責任分界の十分な理解
・データ取得頻度の設定
（高頻度に取得するほど省エネ効果は高いが、既設システムへ負荷が係ることに留意）
・既設システムからのデータ取得範囲の指定
（例えば、BEMS 等ではエネルギー情報以外の情報も保持しているケースが多い。）

実証実験により得られた知見

＜モデル A 実証実験を踏まえた知見＞

・パブリッククラウド基盤では利用者が制御可能な範囲に制約がある。クラウドサービスの仕様（ネットワーク帯域を含む。）や扱うソフトウェアとの相性、運用手順によっては不具合を引き起こす可能性があるため、パブリッククラウドを活用する場合は慎重な運用試験やバックアップサイトとしての活用を通して実績のある安定した構成を洗い出し、適切な責任分界点を見出すことが重要になると考えられる。

＜実証内容＞

一般的に安価に環境クラウドを構築するための選択肢の 1 つとして、汎用的なパブリッククラウドを活用することが考えられる。パブリッククラウドを用いた場合、プライベートクラウドのように環境アプリケーションのために安易に基盤のチューニングをすることができない中で必要なセキュリティ・品質レベルを担保する仕組みを実装する必要がある。そこで、実証実験では海外の商用パブリッククラウドサービスを活用し、相互接続性も含めた運用実験を行った（図 4-13）。

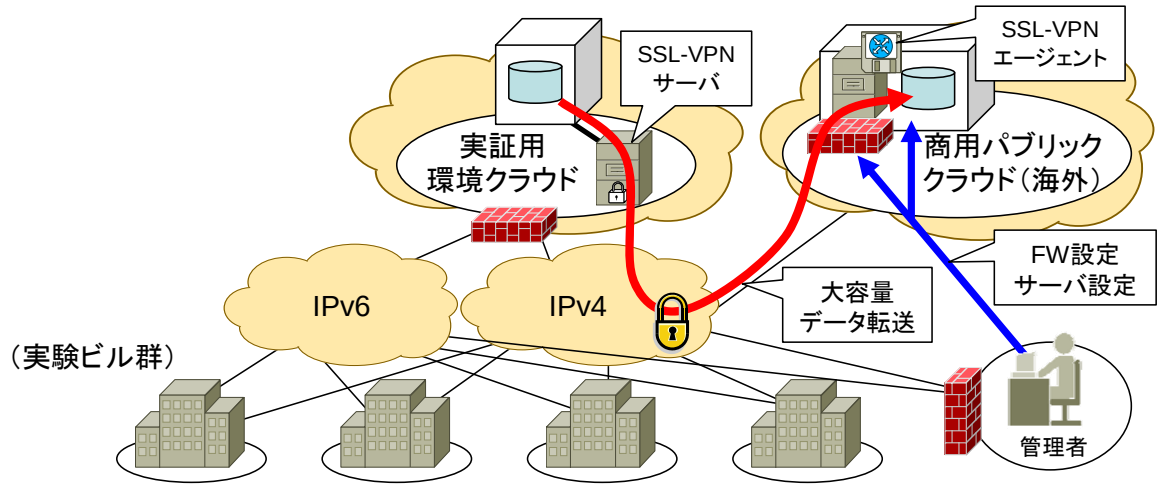


図 4-13　モデル A におけるパブリッククラウドを活用した実証

＜実証結果＞

商用のパブリッククラウドへ大容量の運用データを転送する際、実証用の複数データセンター間での転送に比べて非常に多くの時間を要した。管理対象のビル群の規模が大きくなれば、データ転送の帯域も含めたクラウド設計が重要になると考えられる。またパブリッククラウドとの間を VPN で接続する場合、パブリッククラウド上に VPN エージェントをインストールする必要があるが、パブリッククラウド側の IP アドレスがしばしば消失し､復旧にエージェントの再インストールが必要になるケースがあった。また、パブリッククラウド上におけるファイアウォール設定を誤ると、サーバ操作性を失い、結果としてサーバの OS を再インストールしなくてはならないケースもあった。

実証実験により得られた知見

＜モデル B 実証実験を踏まえた知見＞

・既設設備管理システムは、インターネット環境との接続を想定していないケースもあるため、連携時の情報セキュリティリスクについては、あらかじめオーナー、設備管理者と協議を行い明確化しておくことが望ましい。特に、既設の設備・システムに与えるリスクについては、あらかじめオーナー、設備管理者と合意するとともに、契約などによる責任分解点の明確化をしておくことが望ましい。

＜実証内容＞

エネルギーデータの取得には、BEMS 等既設施設管理システムとの接続、ゲートウェイを活用した設備機器との直接連携が考えられる。BEMS 等に関しては、インターネットとの接続を前提に構築されているものもあるが、安全性の観点から、クローズな環境で運用されているものも多い。こうした既存環境も考慮し、エネルギーデータの取得について連携方法について実証した。（図 4-14）

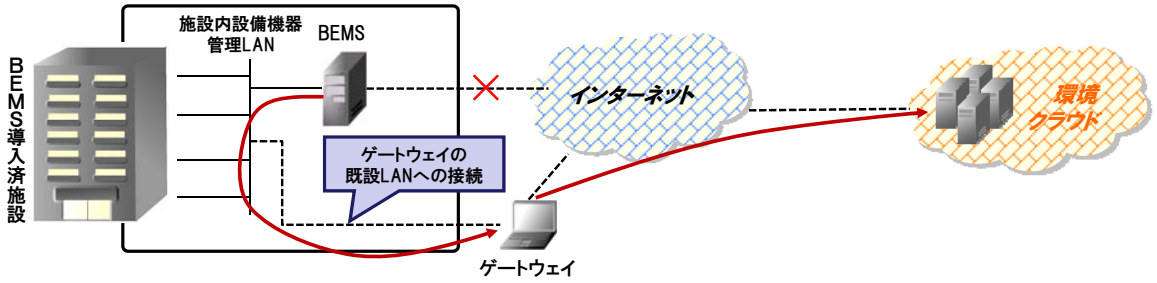


図 4-14　既設の施設管理システムとの連携実証

＜実証結果＞

BEMS 等で管理されるデータは、エネルギーデータ以外にも多岐にわたるため、安全性を考慮し、BEMS 専用ネットワークを敷く施設も少なくなかった。施設設備担当者との調整の結果、安全なデータ連携を実現するために、BEMS から CSV ファイルをネットワーク上のファイルサーバに定期的に送出し、ゲートウェイが定期的にそのファイルを取得、環境クラウドへ送出することで当該施設のエネルギー情報を環境クラウド上で管理した。

BEMS 未導入の施設に関しては、ゲートウェイを活用し、分電盤や電力系、空調設備と接続しエネルギーデータを環境クラウドに送出した。このケースにおいても事前にオーナー、施設整備担当者等との調整の中で既設ネットワークに影響がでないことを確認しながら進める必要がある。

4.2.1.2. ２次利用データベースの利用範囲と権利関係の明確化（モデル C 実証実験より得られた知見等）

概要

環境クラウドサービスでは、第三者にデータを提供する場合や公共向けに情報を提供する場合があるため、情報の提供・公開に際しては、合意形成や権利関係について明確化しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・データの収集及び活用に関する契約書又は合意書の検討・明確化

・利用に関するガイドラインの事前の明文化

【環境クラウドサービス利用者】

・事業者から提供される契約書、合意書、ガイドライン等の妥当性の確認

4.2.1.3. 責任分界点の契約書への明記

概要

環境クラウドサービス上でサービスの提供・利用を行う際、環境クラウドサービス事業者（環境アプリケーション提供者やプラットフォーム提供者）や環境クラウドサービス利用者、更には監視対象となる施設や機器等の保有者、管理者等、様々な人々がサービスにステークホルダーとして関与する

可能性がある。この場合、それぞれの間で交わされる契約書において、責任分界点について明確化しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・データが正しく環境クラウド上に蓄積されなかった場合

（センサーからデータの送出がされたのに､データベースに正しく格納されなかった場合等）

・データの完全性が損なわれた場合

（メタデータが不完全なまま流通してしまった場合等）

・情報処理プロセスで事故が発生した場合

（データベースに誤ったデータが蓄積されたもしくは上書きされた場合等）

・不正利用や攻撃の被害が発生した場合

（刑事訴訟の原告となるべき主体を特定する場合等）

【環境クラウドサービス利用者】

・上記のような事態の認識及び責任分解点が契約書に明記されていることの確認

4.2.1.4. **委託における通常運用時の責任分界点の設定**

概要

環境クラウドサービスでは、環境クラウドサービス基盤の運営を他社に委託する場合があるため、委託先との間で通常運用における責任分界を事前に明確にしておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境クラウドサービス利用者に対する環境情報保護の仕組みに関する説明責任、運用の見直し・改善実施責任の明確化

【環境クラウドサービス利用者】

・事業者と委託先との業務上の責任分解点が明確化されていることの確認

4.2.1.5. **委託におけるインシデント発生等の事後の責任分界点の設定**

概要

環境クラウドサービスでは、環境クラウドサービス基盤の運営を他社に委託する場合があるため、インシデント発生後における説明責任、善後策等の責任分界を明確にしておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境クラウドサービス利用者に対するインシデント発生時の事実及び原因と対処法に関する説明責任の明確化

・環境クラウドサービス利用者との情報共有及び善後策の検討

【環境クラウドサービス利用者】

・事業者と委託先とのインシデント発生時の責任分解点が明確化されていることの確認

4.2.1.6. **データの収集、管理時の責任分界点の設定**

概要

環境クラウドサービスでは、管理事業者が異なる複数の施設から情報を収集し、許諾に基づいて収集情報を２次利用する場合があるため、データの２次利用に関する責任分界を明確にしておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・分析用データベースを利用する際における責任分界点の事前設定

・利用に関するガイドラインの事前の明文化

【環境クラウドサービス利用者】

・データの２次利用に関する責任分界点の設定、規定の有無及びその内容の確認

4.2.2. **ガバナンス及びエンタープライズリスクマネジメント**

目的：十分な情報セキュリティ対策が講じられていない事象者のクラウドサービスを利用すること等により、利用者が情報セキュリティガバナンスを喪失してしまい、リスクの測定・管理が困難になってしまうおそれがある。こうしたガバナンス及びエンタープライズリスクマネジメントについて事業者等が満たすことが推奨される要件を明確化する。

環境クラウドサービスを利用する際の懸念事項として、利用者がガバナンスを喪失してしまうことや、利用者自身のリスクの測定が困難になってしまうこと、及びそれらの解決策が未成熟であるという点が挙げられる。そのため、事業者は、提供するサービスに応じたリスクマネジメント体制を確立するだけではなく、、必要に応じて第三者によるリスク評価を実施・利用者への結果開示が求められ、また同時に利用者もこれらが適切に行われていることを確認することが求められる。

このため、環境クラウドサービス事業者、利用者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.2.2.1　サービスの特性に応じた情報セキュリティ対策の実施

4.2.2.2　データの所在地・国の明示

4.2.2.3　マルチテナントの影響の把握

4.2.2.1. **サービスの特性に応じた情報セキュリティ対策の実施**

概要

環境クラウドサービスでは、事業者・利用者によって提供・要求される情報セキュリティレベルが異なるため、サービスの特性を考慮した上で情報セキュリティ対策を実施するようことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者によるデータの即時性・機密性をもとにしたプラットフォームのセキュリティ効果・リスク分析及び最適なプラットフォームの選択

（プラットフォームレイヤー）

・プラットフォーム提供者によるプラットフォームの潜在リスクの把握

・プラットフォーム提供者によるプラットフォームのリスク対策・受容リスクの明示及び情報提供

（インフラレイヤー）

・プラットフォーム提供者によるインフラの潜在リスクの把握

・プラットフォーム提供者によるインフラのリスク対策・受容リスクの明示及び情報提供

【環境クラウドサービス利用者】

・サービスの各レイヤーにおける情報セキュリティ対策の内容の確認

4.2.2.2. **データの所在地・国の明示**

概要

環境クラウドサービスが取り扱うデータは保存される場所によって適用される法律が異なるため、その影響を考慮した対応を行うことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・データの所在地、所在地が国外である場合の法律の留意事項及び行政執行への対応の明示

【環境クラウドサービス利用者】

・サービスで扱うデータの所在地・国、及び国外の場合の留意事項の確認

4.2.2.3. **マルチテナントの影響の把握**

概要

環境クラウドサービスは、マルチテナント環境で利用される場合があるため、共同利用者のインシデントに対するリスクに備えることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・利用者に対する他の共同利用者のインシデント発生時の影響の開示

【環境クラウドサービス利用者】

・共同利用者によるインシデント発生への事業者の対応方法の確認

4.2.2.4. **セキュリティ評価**

概要

環境クラウドサービスを提供するに当たってのリスクを適切に管理するため、事業者を選択する際には、事業者が満たしているセキュリティレベルを指標として考慮することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・情報セキュリティポリシーや実施しているセキュリティ対策の状況の開示

・必要に応じた第三者による客観的な評価の実施

【環境クラウドサービス利用者】

・事業者のセキュリティ対策や外部評価の内容の確認

4.2.2.5. **デューデリジェンスの実施**

概要

環境クラウドサービス事業者の破綻や撤退は、利用者に大きな影響を与えるため、事業者に対するデューデリジェンスをあらかじめ考慮することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・サービスの継続的提供のために必要な財務基盤の確保

【環境クラウドサービス利用者】

・事業者の財務状況や社会的信用度等の確認

4.2.2.6. 再委託先の把握

概要

環境クラウドサービスでは、環境アプリケーション提供者がプラットフォーム提供者に対してクラウド基盤の運用管理を再委託する場合があるため、安全管理や監査の観点から再委託先の把握に留意することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・委託する業務内容、委託先の選定手続、委託先に求める安全管理措置、委託先の監査等のサービス説明への記述

【環境クラウドサービス利用者】

・利用者：事業者による再委託先の把握・管理状況の確認

4.2.2.7. SLA の締結

概要

環境クラウドサービスの品質を利用者に保証するため、環境クラウドサービス事業者と利用者の間で SLA について合意をしておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・利用者に対するサービス利用契約書等を用いた保証するサービスレベル及び保証しない項目の説明

【環境クラウドサービス利用者】

・複数の事業者のサービス利用契約書等の比較・参照

・保証するサービスレベル及び保証しない項目を考慮した事業者の選定

・必要に応じた特約条項の設定

4.2.2.8. リスク評価の継続的実施

概要

環境クラウドサービスに係る情報セキュリティガバナンスやリスク管理を適切かつ恒常的に行うため、企画段階だけでなく運用段階においても継続的にリスク評価を行うことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・セルフチェックや内部監査、外部の第三者による評価の継続実施によるシステム管理体制の維持・向上

【環境クラウドサービス利用者】

・事業者のシステムリスクの評価・見直しの実施内容、頻度等の妥当性の確認

4.2.2.9. **委託事業者の監査**

概要

環境クラウドサービスに係る業務を再委託する場合において、委託した業務が適切な情報セキュリティ施策の下で実施されていることを確認するため、SLA に記載された項目の実施状況を確認することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・システム開発・運用、ヘルプデスク、外部媒体等配送・保管、記録媒体廃棄等業務の外部委託時における監査項目を記載した調査表の活用

【環境クラウドサービス利用者】

・事業者による再委託先の監査の実施状況と結果の確認

4.2.3. **法制度及び電子情報の開示**

目的：国外のクラウド上で環境クラウドサービスに係るデータが扱われる場合、その取り扱いに対して当該国の法律が適用され、電子情報の開示を求められる等、情報管理のシナリオが多岐に渡ることが想定される。こうした法制度及び電子情報の開示について事業者等が満たすことが推奨される要件を明確化する。

環境クラウドサービスでは情報管理のシナリオも多岐に渡り、そのシナリオに法制度がどのように適用されるか注意する必要があるため、事業者と利用者の間において契約等で定めておくべき重要な項目がある。

このため、環境クラウドサービス事業者、利用者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.2.3.1　監査権の確保

4.2.3.2　個別要求事項の明確化

4.2.3.3　訴訟要求対応の明確化

4.2.3.4　適応法令の明確化

4.2.3.5　データ開示リスクの明確化
4.2.3.6　国外へのデータ移送・保存の明確化
4.2.3.7　情報漏えい時の通知

4.2.3.1. **監査権の確保**

概要

環境クラウドサービスでは、環境アプリケーション提供者がプラットフォーム提供者に対してクラウド基盤の運用管理を再委託する場合がある。この場合外部に委託する IT 業務の内部統制の評価を行うことが求められるため、委託先との契約書に監査権を要求することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・利用者からの監査要請に対する他の利用者の情報保護を目的とした立ち入り範囲の限定

【環境クラウドサービス利用者】

・契約書に監査権を要求することによる SLA を基準とした監査実施の体制確保

4.2.3.2. **個別要求事項の明確化**

概要

環境クラウドサービス利用者の要求事項が、必ずしも事業者の契約書に全て記載されているとは限らないため、記載されていない要求事項に関しては個別に契約条項を含めるよう交渉することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・他サービスと特異な点に係る契約書での明文化及び説明

【環境クラウドサービス利用者】

・SLA の締結、プライバシー保護、国外へのデータ移送・保存の禁止、訴訟要求への対応、監査権の確保、契約終了、中途解約時の情報の取り扱い等要求事項の明確化
・事業者の契約条項に要求事項が含まれていることの確認
・事業者の契約条項に含まれていない要求事項に係る必要に応じた個別交渉

4.2.3.3. **訴訟要求対応の明確化**

概要

捜査機関への協力依頼や裁判所の命令等に適切に対応するため、システム情報の開示等の要請に対する対応策を事前に明確化しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・情報提出を要請された際における正式な法的手続きに従った要請・命令であることの確認

・要請を受けた際の対応に関する利用者との事前合意

【環境クラウドサービス利用者】

・事業者が情報提出を要請された際における利用者への適時通知の契約条項の追加

4.2.3.4. **適応法令の明確化**

概要

環境クラウドサービス事業者は、情報管理シナリオを明確化するため、利用者の要請に応じて、データの保管場所及び適応法令の明確化を行うことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー）

・情報の保管場所及びその安全性についての開示

・データセンターについて事業者が保有する認証（例えば、ISO/IEC27001 等）の明示及びそれに基づく安全管理の説明

【環境クラウドサービス利用者】

・データの保管場所及び適応法令の内容の確認

4.2.3.5. **データ開示リスクの明確化**

概要

環境クラウドサービスが国外で運用される場合、所在地によっては当該国の法律の適用によりデータの開示等が求められるおそれがあるため、そのリスクを明確化することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・データの所在国又は所在地域及びデータ開示の発生リスクに係る情報の開示

【環境クラウドサービス利用者】

・データの所在地域・国及びデータ開示の発生リスクの内容・程度等の確認

4.2.3.6. **国外へのデータ移送・保存の明確化**

概要

環境クラウドサービスが国外で運用される場合、所在地によっては捜査のためにデータが保存された機器を押収されるおそれがあるため、国外へのデータ移送・保存について契約書等に明確化しておくのが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者によるプラットフォーム提供者の運用データセンターの国・所在地の把握

・契約書にデータ押収の可能性がある国へのデータ移送・保存の禁止条項の追加

（プラットフォームレイヤー）

・プラットフォーム提供者によるデータを移送・保存する可能性がある地域の明示

・データ所在地が国外になる場合における法律の違いや行政執行を受けた場合のリスクに関する説明

【環境クラウドサービス利用者】

・契約書に記載された国外へのデータ移送・保存の可能性の有無及びその内容の確認

4.2.3.7. **情報漏えい時の通知**

概要

環境クラウドサービスが取り扱う情報漏えいが起こった場合に対応を適切に行うため、データの所有者等に対する事実関係等の通知手順について明確化することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・情報漏えい時のデータの所有者への通知手順、サービスの共同利用者への通知手順の開示

【環境クラウドサービス利用者】

・事業者による情報漏えい時の通知手段の内容と妥当性の確認

4.2.4. **コンプライアンス及び監査**

目的：クラウド環境の利用によって事業者側へガバナンスが移管されると、利用者の見えないところでセキュリティ対策が行われる。そのため、利用者はコンプライアンス維持のための監査方法を検討する必要があり、また、事業者もコンプライアンスを保証する必要がある。こうしたコンプライアンス及び監査について事業者等が満たすことが推奨される要件を明確化する。

環境クラウドサービスはデータセンター等の遠隔地で運用されるため、利用者にとっては扱われるデータに適切なセキュリティ対策が実施されているかを監視するためのプロセスがより複雑・困難になる。

このため、環境クラウドサービス事業者、利用者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.2.4.1　データの重要度に応じた分類

4.2.4.2　データ所在の確認

4.2.4.3　認証の取得

4.2.4.4　外部監査の活用

4.2.4.5　認証範囲の適切性確認

4.2.4.1. **データの重要度に応じた分類**

概要

環境クラウドサービスが取り扱うデータの内容により、求められるセキュリティレベルが異なるため、データを重要度に応じて分類し、適切な保護を行うことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者によるセンサー情報等のデータの重要度を考慮した分類とデータ保護

【環境クラウドサービス利用者】

・事業者によるデータの分類に応じたセキュリティレベルの設定、対策内容及びその妥当性の確認

4.2.4.2. **データ所在の確認**

概要

データ保護条例が存在する国では、不用意に第三国にデータを移動した場合、法令違反になるおそれがあるため､環境クラウドサービスが取り扱うデータの物理的な所在地を確認することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者による、プラットフォーム提供者のストレージ運用地域・国の確認

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者による、ストレージ等の運用・データ保管実施地域・国の明示

【環境クラウドサービス利用者】

・ストレージ運用、データ保管等の地域・国の確認

4.2.4.3. **認証の取得**

概要

環境クラウドサービス利用者から監査要求された際に、セキュリティポリシーの内容及びその実施状況を円滑に報告するため、環境クラウドサービス事業者は第三者機関の認証を取得することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者による情報セキュリティマネジメントシステム(ISMS)/IT サービスマネジメントシステム（ITSMS）適合性評価制度、日本公認会計士協会監査基準委員会報告書第 18 号（18 号監査）/米国公認会計士協会（AICPA）監査基準書第 70 号（SAS70）に基づく報告書等を利用した認証取得

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者による ISMS/ITSMS 適合性評価制度、18 号監査/SAS70 報告書等を利用した認証取得

【環境クラウドサービス利用者】

・事業者における第三者機関による認証の取得状況の確認

4.2.4.4. **外部監査の活用**

概要

環境クラウドサービスに係る業務の監査を実施する技術・経験を持った要員の確保や環境クラウドサービス利用者の求めに応じた個別の監査の受入れが困難な場合があるため、外部監査を活用することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・第三者専門機関による監査実施によるコンプライアンス維持、監査対応の負荷軽減

（プラットフォームレイヤー）

・第三者専門機関による監査実施によるコンプライアンス維持、監査対応の負荷軽減

【環境クラウドサービス利用者】

・事業者による外部監査の活用の有無と結果の確認

4.2.4.5. **認証範囲の適切性確認**

概要

環境クラウドサービス事業者ごとに提供サービスの特性が異なり、また、第三者認証機関の認証範囲も当該機関ごとに異なる場合があるため、認証を希望する項目が認証範囲に含まれていることを確認することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者による監査対象範囲の明確化及びその要件下で認証を受けるための第三者機関との折衝

・利用者から環境アプリケーション提供者への監査項目追加要望に対して、項目拡大の検討

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者による監査対象範囲の明確化及びその要件下で認証を受けるための第三者機関との折衝

・環境アプリケーション提供者からプラットフォーム提供者への監査項目追加要望に対する、項目拡大の検討

4.2.5. **ID 管理とアクセス管理**

目的：環境クラウドでは、既存のエネルギー管理システムからの連携・マイグレーションや新規構築等のシナリオにおいて、特有の認証セキュリティの在り方が想定される。こうした ID 管理とアクセス管理について事業者等が満たすことが推奨される要件を明確化する。

ID 管理とアクセス管理は、機密性が求められる企業用アプリケーションでは特に重要なセキュリティ項目である。例えば、環境クラウドサービスのモデル A では、企業が利用しているビルにおいてセンサー情報等が収集されるが、これは企業活動にかかわる情報であり、高い機密性が求められる可能性がある。その一方で、既存のエネルギー管理システムからの連携・マイグレーションや新規構築等のシナリオにおいて、利用者に対してシームレスなサービスを提供するための認証連携機能も考慮する必要がある。

このため、環境クラウドサービス事業者、利用者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.2.5.1　多様なシステム間での認証連携（モデル A 実証実験より得られた知見等）

4.2.5.2　汎用的な認証基盤の提供（モデル B 実証実験より得られた知見等）

4.2.5.3　共通認証基盤の提供（モデル C 実証実験より得られた知見等）

4.2.5.4　認証ログ取得による適切なアクセス管理の確認

4.2.5.5　強固な利用者認証方式の提供

4.2.5.1. **多様なシステム間での認証連携（モデル A 実証実験より得られた知見等）**

概要

環境クラウドサービス利用者が、複数のアプリケーションを利用する際の認証を円滑に行い、シームレスにサービスを提供するため、シングルサインオンを用いた認証連携機能を導入することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者によるプラットフォーム提供者のプラットフォーム上の IDP（認証を管理するシステム）の有無の確認

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者による IDP の設定及び認証連携機能の提供

・利用者からの求めに応じた他アプリケーションサーバとの信頼関係拡張

・プラットフォーム提供者による標準化された認証連携方式及び暗号化の提供

実証実験により得られた知見

＜モデル A 実証実験を踏まえた知見＞

・NAT は、エンド・ツー・エンドの通信確保やアドレス設計だけでなく、ID 連携にも影響を及ぼすため、環境クラウドに NAT を導入する場合には、システム・ネットワーク設計に留意するとともに、システム更改による IPv6 化も含めて検討する必要がある。

＜実証内容＞

ビル管理事業者がアクセスする必要のある環境クラウド上のシステムは BMS、分析アプリケーション、可視化アプリケーション等、多岐に渡る。既存のビル管理システムから環境クラウドへのマイグレーションを図る場合、既存の認証セキュリティ（ID・パスワードやハードウェアトークン等）とシームレスに連携し、システム間で ID 連携が行われることが求められる。そこで、実証実験では複数のサーバ（データセンター）間での認証連携（シングルサインオン）の実験を行った（図 4-15）。

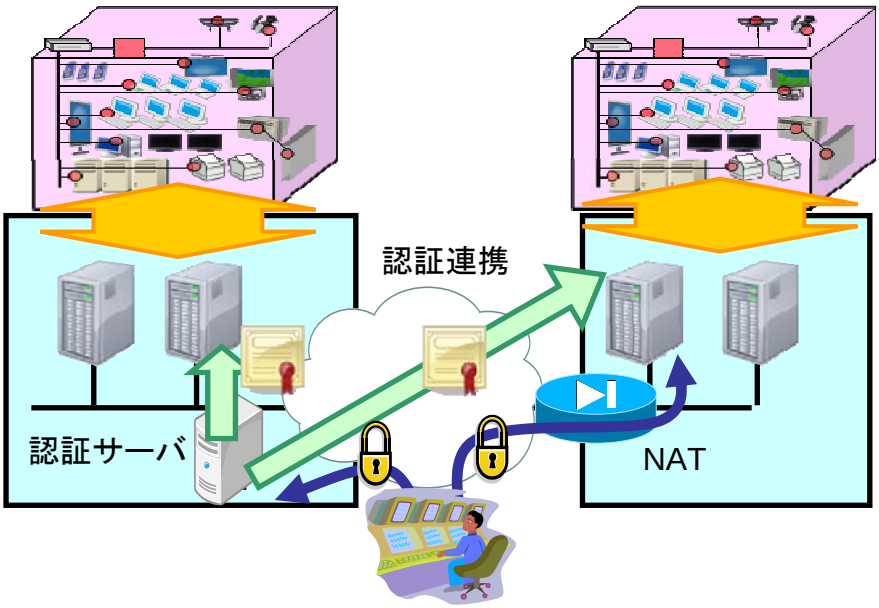


図 4-15　環境クラウドサービス内におけるサーバ間の認証連携

＜実証結果＞

実証実験では、アクティブディレクトリフェデレーションサービスを用いたシングルサインオンを導入し、直接連携していない複数のアプリケーションを続けて利用した際に、認証連携機能によりシームレスなサービス利用が実現できることを実証し、その有効性を明らかにした。一方で、クラウド上に NAT が配置された環境では正常に動作しないケースがあった（アクティブディレクトリを NAT 環境で使用する場合には慎重な調査・検証が必要となるが、BMS が Windows ベースのシステムとなっている場合、このようなケースは決して珍しくないと想定される）。

4.2.5.2. 汎用的な認証基盤の提供（モデル B 実証実験より得られた知見等）

概要

環境クラウドサービスでは、多様な事業者がサービスを利用する場合があるため、情報セキュリティポリシーの異なる事業者に対応し、適切な認証方式を提供することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー）

・情報セキュリティポリシーの異なる企業ごとに個別に認証基盤を構築・提供することが困難な場合における認証方式の在り方の検討

実証実験により得られた知見

＜モデル B 実証実験を踏まえた知見＞

・情報セキュリティポリシーが異なり、また認証モジュールのインストールが困難な事業者に対して、環境クラウドサービスを提供することにも留意する必要がある。

＜実証内容＞

複数事業者が共同利用する場合、事業者ごとに情報セキュリティポリシーが異なることを想定した認証基盤の構築を行う必要がある。そこで、実証実験では、異なる情報セキュリティポリシーの利用者を想定したクライアントモジュールレスの認証基盤の在り方について検証を行った。また、監査対応を意識したアクセスログ取得の在り方について検証を行った（図 4-16）。

図 4-16　モジュールインストールレス認証基盤に関する実証実験

＜実証結果＞

ゲートウェイにおいて ID/パスワードでの認証管理機構を実装し、通信を SSL で暗号化することにより、認証の安全性確保を行った。また、その評価を行うために、アプリケーションへのアクセスを対象としたウェブアプリの脆弱性に関するシミュレーションを実施した。また、通信対する盗聴及び改ざんの疑似攻撃による通信の安全性に関するシミュレーションを実施した。これらの検証をあらかじめ十分に行なっておくことで、サービス利用者が増加した場合であっても、安全かつ安定的にサービスを提供できることがわかった。一方で、ゲートウェイ型の構成を組んだ場合、ゲートウェイの脆弱性が攻撃の脅威となるため、十分な対策を行う必要がある。

4.2.5.3. **共通認証基盤の提供（モデル C 実証実験より得られた知見等）**

概要

環境クラウドサービスでは、多様な事業者がサービスを利用する場合があるため、情報セキュリティポリシーの異なる事業者に対応し、適切な認証方式を提供することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー）

・多様なデータベースやアプリケーションとの連携、エンジニアのコミュニティの成熟度及びエンジニアのスキル・経験を考慮した標準認証基盤の提供

実証実験により得られた知見

＜モデルＣ実証実験を踏まえた知見＞

・環境クラウド上で蓄積・管理する情報を利用した多様なアプリケーションが開発・提供されることが想定される。このような場合におけるアプリケーション開発の負荷を軽減するための一つの手法として、環境クラウド上で統合認証基盤を提供する方法が考えられる。

＜実証内容＞

２次利用目的でのデータ利用に際しては、データへのアクセス範囲を限定するために、利用者/アプリケーションの認証が必要となる。そこで、実証実験では、事業者が開発したアプリケーションとのデータ連携時の認証について検証を行った。また、一般利用者（市民）のデータダウンロード時における利用者認証の在り方について検討を行った（図 4-17）。

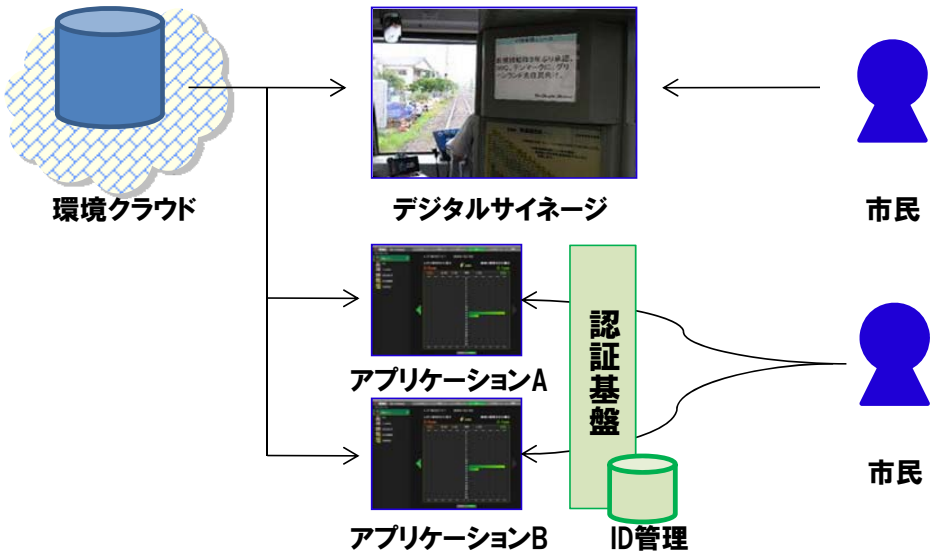


図 4-17　多様なサービス・アプリケーションとの連携を考慮した認証連携基盤に関する実証実験

＜実証結果＞

市民へのデータ公開は、デジタルサイネージ等、利用者が認証なしで利用できるのもと、認証が必要なアプリケーションがあると想定される。認証が必要なアプリケーションに対してアプリケーションごとに認証機構を提供することは利用者の利便性に影響を与える可能性がある。このことから、環境クラウドにおいて統合認証基盤を提供することが有効であることがわかった。ただし、アプリケーション開発者が同認証基盤に容易に理解出来ないことも想定し、利用ガイドを提供する等の対応が必要なると考えられる。

4.2.5.4. **認証ログ取得による適切なアクセス管理の確認**

概要

適切な利用者のみに環境アプリケーションの利用を許可し、かつ監査対応時に適切なアクセス管理が実施されていることを証明するため、認証ログを取得することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー）

・プラットフォーム提供者によるアクセス管理の証明としての認証時ログの取得（例えば、シングルサインオンを実施する場合は、IDP で認証時のログを取得することが可能）

4.2.5.5. **強固な利用者認証方式の提供**

概要

環境クラウドサービスでは、エネルギー管理に関する機密性の高いデータや設備オーナーやテナント等の情報が扱われる場合があるため、適切な利用者のみに環境アプリケーションの利用を許可できるよう強固な認証方式を用いることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者によるアプリケーション利用時の強固な認証方式の提供

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者によるプラットフォーム利用時の強固な認証方式の提供

4.2.6. **暗号化及び鍵管理**

目的：環境クラウドでは、施設内に設置された機器/設備等から送出される環境情報を正しく収集・分析し、必要な制御もしくは利用者にフィードバックするため、計測装置とクラウドとの間の通信経路の暗号化対策や環境情報の改ざん等に対応可能な仕組みを要するなど、特有の留意事項が想定される。こうした暗号化及び鍵管理について事業者等が満たすことが推奨される要件を明確化する。

環境クラウドサービス事業者と利用者は共にデータの損失・漏えいを防ぐため、特に個人情報や企業情報に係わるデータを暗号化する必要がある。そのため、強固な暗号化及び鍵管理の重要性を認識する必要がある。データは、ネットワーク、保存されているストレージ、バックアップ用メディア等、様々な箇所に存在することになるため、データが処理される全てのプロセスにおいて暗号化を行う必要がある。また、鍵管理においては、安全な鍵保管、鍵の保管場所へのアクセス管理、鍵のバックアップ及び復旧プロセスを確保し、正当な利用者のみがデータにアクセスできるようにする必要がある。

このため、環境クラウドサービス事業者、利用者が留意することが望ましい項目について、以下の

とおり細分化して解説する。

4.2.6.21　仮想化基盤内通信の安全性の確保（モデル A 実証実験より得られた知見等）

4.2.6.2　通信の暗号化の確保

4.2.6.3　強固な暗号化方式の採用

4.2.6.4　適切な鍵管理の実施

4.2.6.1. **仮想化基盤内通信の安全性の確保（モデル A 実証実験より得られた知見等）**

概要

環境クラウドサービスでは、多数の利用者のビル施設に関する情報がマルチテナント環境で扱われる場合があるため、外部ネットワーク上だけでなく仮想化基盤内においても情報漏えいに備えて安全性確保の施策を備えることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

(アプリケーションレイヤー)

・環境アプリケーション提供者によるプラットフォームでの仮想化基盤内通信の暗号化サポートの有無の確認及びサポートが無い場合におけるアプリケーションレイヤーの暗号化のサポート

(プラットフォームレイヤー)

・プラットフォーム提供者による仮想化基盤内通信の暗号化機能の提供

実証実験により得られた知見

＜モデル A 実証実験を踏まえた知見＞

・環境アプリケーションを開発するに当たっては、クラウド上への展開を想定してセキュリティ機能を実装する必要があるが、それらをサポートしていない既存のアプリケーションについても IPsec 等環境クラウドのプラットフォームレベルの機能を活用することで強固なセキュリティを確保できるケースがある。

＜実証内容＞

環境アプリケーションを環境クラウド上に展開する場合、そのネットワーク設計等に応じてアプリケーションデータ転送時の認証・暗号化を厳密に行う必要がある。実証実験では、既存のビル管理で用いられている暗号化機能のない環境アプリケーション（分析アプリケーション、可視化アプリケーション等）同士でのデータ転送に際して、セキュリティを確保した上で運用を行う実験を行った（図 4-18)。

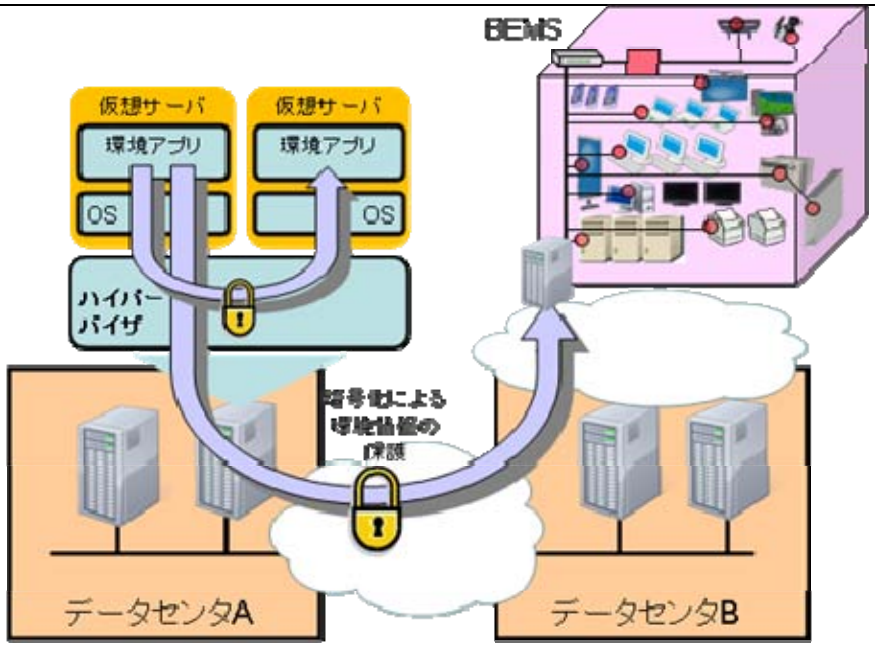


図 4-198　仮想化基盤内通信の暗号化確保の実証

＜実証結果＞

既に運用中のアプリケーションにセキュリティ機能を個別に搭載するのは容易ではないため、実証実験では、アプリケーション単位のセキュリティポリシー設定に基づく IPsec によるデータ転送保護を行い、これにより現存のアプリケーションに影響を与えることなくセキュリティ確保が可能となった。

4.2.6.2. **通信の暗号化の確保**

概要

環境クラウドサービスでは、収集したセンサー情報が定常的に外部のネットワークを経由してクラウドに集められるため、通信の暗号化を行い、第三者による盗聴によって情報が漏えいするリスクを軽減することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者によるプラットフォームでの通信暗号化のサポートの有無の確認及びサポートが無い場合におけるアプリケーションレイヤーの暗号化のサポート

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者による通信暗号化機能の提供

4.2.6.3. **強固な暗号化方式の採用**

概要

環境クラウドサービスでは、エネルギー管理に関する機密性の高いデータや設備オーナーやテナント等の情報が扱われる場合があるため、脆弱性の低い強固な暗号化方式を採用することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・暗号化の実施における電子政府推奨暗号リスト等による強固な暗号化方式の採用

（プラットフォームレイヤー、インフラレイヤー）

・暗号化の実施における電子政府推奨暗号リスト等による強固な暗号化方式の採用

4.2.6.4. **適切な鍵管理の実施**

概要

環境クラウドサービスでは、エネルギー管理に関する機密性の高いデータや設備オーナーやテナント等の情報が扱われる場合があるため、正規の利用者のみがデータを利用できるよう適切に暗号鍵を管理することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・暗号化のサポートにおける適切な鍵管理の実施（利用者ごとに暗号鍵を分ける等）

（プラットフォームレイヤー、インフラレイヤー）

・暗号化のサポートにおける適切な鍵管理の実施（利用者ごとに暗号鍵を分ける等）

4.2.7. **インシデント対応**

目的：環境クラウドでは、大規模なセンサーネットワークの複雑性に起因する脆弱性、屋外に設置されるセンサーの脆弱性、通信品質が異なることに起因する脆弱性など、ユースケースに準じた特有の留意事項が想定される。こうしたインシデント対応について事業者等が満たすことが推奨される要件を明確化する。

環境クラウドにおけるインシデント対応を行うためには、インシデントの発生場所や発生原因等の特定を行う必要があるが、クラウド環境ではデータが様々な場所に偏在することによって、調査対象が多岐に渡るほか、様々な事業者のサービスを組み合わせて運用する場合には、事業者によってはインシデント対応するためのログなどの証拠が残されていない場合もあり、インシデント対応を迅速に行うことが困難になる。

このため、環境クラウドサービス事業者、利用者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.2.7.1　計測監視対象の稼動監視（モデルＣ実証実験より得られた知見等）

4.2.7.1. **計測監視対象の稼動監視（モデルＣ実証実験より得られた知見等）**

概要

環境クラウドサービスでは、設備機器の動作状況を遠隔で監視できる等、インシデント対応に遵守したシステム、体制の構築が重要になるため、設置機器動作状況を監視し、障害発生時に必要な連絡・復旧を行える体制を構築することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（インフラレイヤー）

・故障や誤データの検知体制の構築

・屋外設置センサー等特に故障の確率が高い機器に対する管理メンテナンス体制の検討

4.2.7.2. **統一的な監視**

概要

環境クラウドサービスでは、仮想化環境も含め、多数の機器や様々な場所に偏在したデータを取り扱う場合があり、監視対象が多岐にわたるため、統一的な監視システムが準備されることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・統一的に運用可能な監視システムの導入

4.2.7.3. **インシデント定義**

概要

環境クラウドサービスに求められるセキュリティレベルは、利用者により異なるため、インシデントの定義を事前に明確化しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・発生する具体的な事象を列挙した上でのインシデント定義

【環境クラウドサービス利用者】

・インシデントの定義の確認

4.2.7.4. **利用者のためのインシデント連絡窓口の確保**

概要

環境クラウドサービスでは、公共性の高い情報を取り扱う場合があり、インシデント発生時に利用者に与える影響が大きいため、インシデント発生時において対応状況や被害状況を確認し、適切な対応をとることができる体制をあらかじめ整備しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・インシデント発生時の連絡窓口の設置及び利用者への周知

【環境クラウドサービス利用者】

・インシデント発生時の連絡窓口の有無、運用内容、連絡先情報の確認

実証実験により得られた知見

＜モデル A 実証実験を踏まえた知見＞

・環境クラウドサービスを展開するに当たり、外部のプラットフォーム提供者のクラウド基盤を活用する場合には､あらかじめプラットフォーム提供者のインシデント対応窓口やヘルプデスクとの連携手段を確保するとともに、そのサービスレベルについて確認・検討しておくことが重要である。

＜実証内容＞

環境クラウドサービスの事業者モデルにおいては、環境アプリケーション提供者が様々なプラットフォーム提供者のクラウド基盤を活用しながらサービス提供する体制が考えられる。そのため、異なるプラットフォーム提供者の基盤を用いながらシステムを構築し、統一的なサービス運用の実証を行った（図 4-19)。

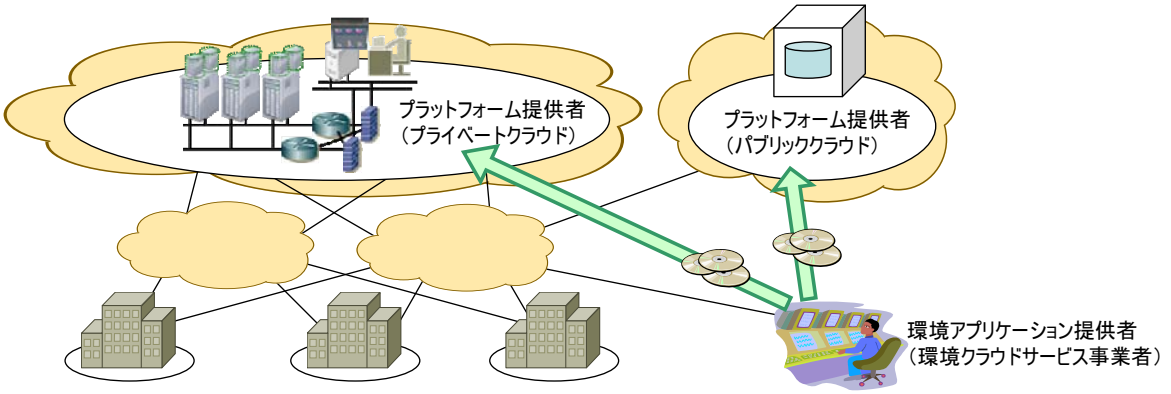


図 4-19　異なるプラットフォームを用いたシステム構築・運用の実証

＜実証結果＞

環境アプリケーションのインストールや設定変更等はリモート操作で行うことが一般的であるが、実証実験では、時にはサーバの再起動に 30 分～1 時間を要したり、データ転送に LAN 環境の数倍の時間を要したりすることもあった。その場合、障害や設定誤りによるものなのか、処理時間の問題なのか環境アプリケーション提供者には判断がつかないため、プラットフォーム提供者の窓口の協力が、その切り分けに係る効率に影響し、環境クラウドサービスそのものの品質に影響を与えることが判明した。特にサポート体制が最小限になりがちなパブリッククラウドを利用する際には注意が必要である。

4.2.7.5. **ログ取得**

概要

環境クラウドサービスでは、公共性の高い情報を取り扱う場合があり、インシデント発生時に利用者に与える影響が大きいため、インシデント発生を早い段階で検知することが望ましい。また、インシデントを検知するために参照するデータとして、アプリケーションログ、ファイアウォールのログ、IDS/IPS のログ、監視サーバのログ、ハイパーバイザーのログを取得することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者によるアプリケーションへのログ機能の実装

・環境アプリケーション提供者によるインシデントとして定義されたアプリケーション挙動発生時のアラート通知機能の実装

（プラットフォームレイヤー）

・プラットフォーム提供者によるファイアウォール、IDS/IPS、監視サーバ、ハイパーバイザーのログ取得に係る設定

・プラットフォーム提供者によるインシデントとして定義された挙動発生時のアラート通知機能の提供

4.2.7.6. **バックアップ**

概要

環境クラウドサービスでは、公共性の高い情報を取り扱う場合があり、インシデント発生時に利用者に与える影響が大きいため､インシデント発生時に環境クラウドサービスを迅速に復旧できるよう、バックアップデータを取得しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・データ、設定ファイル、仮想マシン等のバックアップの取得

4.2.7.7. **インシデント発生時の状態保存**

概要

環境クラウドサービスでは、公共性の高い情報を取り扱う場合があり、インシデント発生時に利用者に与える影響が大きいため、インシデントの発生原因を特定し、再発防止策を講じられるようインシデント発生時の状態を保存しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・詳細なオフライン分析に必要なインシデント発生時のログ等の情報取得

4.2.7.8. **優先度を考慮したインシデントレスポンス**

概要

環境クラウドでは、エネルギー管理に関する機密性の高いデータや設備オーナーやテナント等の情報が扱われる場合があり、インシデント発生時には情報資産に対し適切な対処を行い、被害を最小限に抑える必要があるため優先度を考慮したインシデントレスポンスを定義しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー、プラットフォームレイヤー、インフラレイヤー）

・情報資産に対して機密性・完全性・可用性の観点から優先度を検討した上でのインシデント対応の実施

4.2.8. **データセンターの安全性確保、運用管理**

目的：異なる事業者が提供する複数のデータセンターで環境クラウドサービスが連携する場合には、データセンター自体のセキュリティレベル向上に向けた施策や、セキュリティレベルの異なるデータセンターの活用に関する留意事項が想定される。こうしたデータセンターの安全性確保、運用管理について事業者等が満たすことが推奨される要件を明確化する。

セキュリティレベルの異なる複数のデータセンターを活用して環境クラウドシステムを構成し、仮想サーバ単位の監視項目の統一や、データセンターをまたいだ環境アプリケーションの品質管理などを実現する場合には、データセンターそのものの技術アーキテクチャとインフラの実装が環境クラウド全体のサービスレベルに与える影響を考慮する必要がある。

このため、環境クラウドサービス事業者、利用者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.2.8.1　突発的な負荷上昇に対するサービス安定性の確保（モデル A 実証実験より得られた知見等）

4.2.8.2　データセンターに関する監査

4.2.8.3　環境クラウドサービス事業者の SLA の根拠

4.2.8.4　データセンターの適正な運用管理区分

4.2.8.5　データセンターのメンテナンスポリシーの設定・確認

4.2.8.6　データセンターにおけるプロセス改善

4.2.8.7　環境クラウドサービス事業者が提供するテクニカルサポートの確認

4.2.8.1. **突発的な負荷上昇に対するサービス安定性の確保（モデル A 実証実験より得られた知見等）**

概要

環境クラウドサービス利用者のビジネス規模の拡大等によって、必要とされるサーバやネットワークのリソースの増大だけでなく、定期的なメンテナンス・日々の環境負荷分析の計算等によるバースト的な負荷が発生することに考慮することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・環境アプリケーション提供者による環境アプリケーションがクラウド基盤の柔軟なリソース変更を十分に生かせるだけのスケーラビリティを確保していることの確認

（例えばモデル A では、センサー情報に基づく環境負荷の分析・可視化において定期的にコンピュータリソースを大きく消費することを念頭に置いたアプリケーション設計が求められる。）

（プラットフォームレイヤー）

・環境アプリケーション提供者によるプラットフォーム提供者の SLA 及びリソース制御の仕組みについての把握

（例えばモデル A では、センサー情報に基づく環境負荷の分析・可視化において定期的に

コンピュータリソースを大きく消費することを念頭に置いたクラウド基盤の選定が求められる。）

実証実験により得られた知見

＜モデル A 実証実験を踏まえた知見＞

・大量のデータ収集・分析を行う環境クラウドにおいては、バースト的な負荷への柔軟な対処が必要になるため、あらかじめ利用する環境アプリケーションの処理の重要度・想定される負荷の発生タイミングに応じて、クラウド上のリソース追加の優先度を適切に設計しておく必要がある。

＜実証内容＞

1 箇所のビルで大量のセンサー情報の収集・分析を行う場合、災害、障害などイベント発生時の警報や、日次のデータ分析などの計算負荷がバースト的に発生し、サーバやネットワークのリソースを圧迫する可能性がある。そこで実証実験ではクラウドのリソースを動的に増強する仕組みについて検証を行った（図 4-20）。

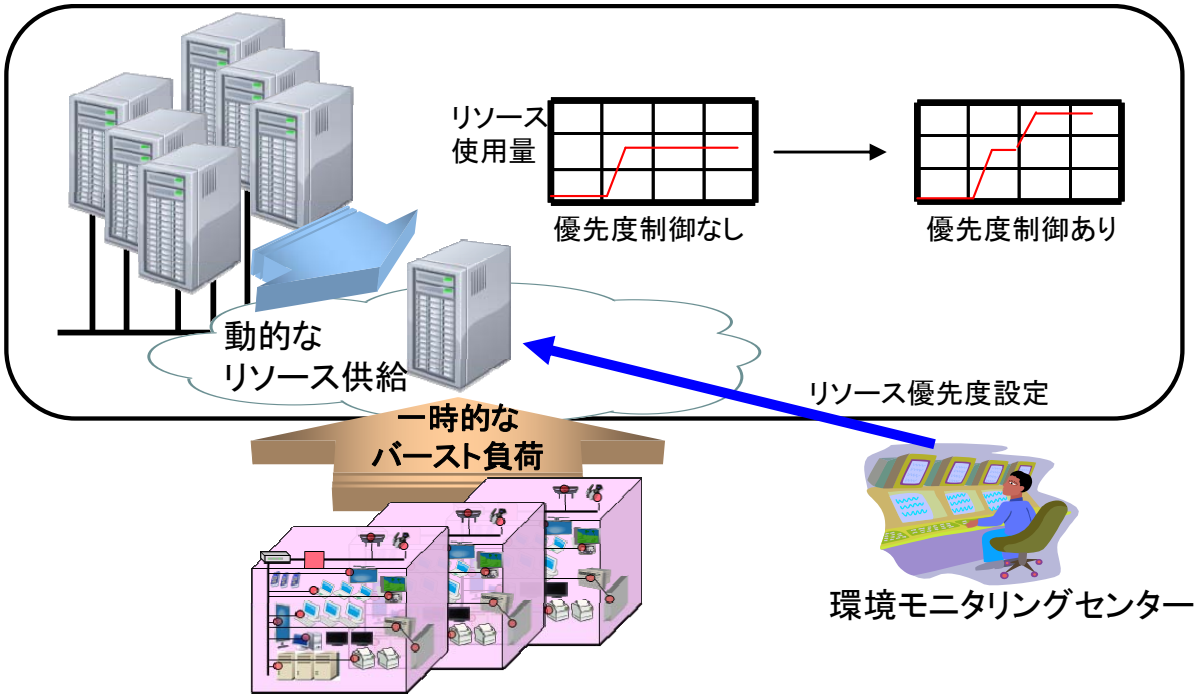


図 4-20　優先度を使ったリソース制御のイメージ

＜実証結果＞

環境クラウドサービスでは、データセンター等に設置されている物理サーバは仮想化されて、仮想マシン単位で環境クラウドサービス利用者に提供される。複数の仮想マシンは管理コンソールを通して、リソース制御を動的に行うことが可能である。例えば、ある仮想マシンが突発的に負荷が上昇する処理を行う場合、環境クラウドサービスの運用状況をモニタリングしている管理者が、あらかじめその仮想マシンに対して優先度を高く設定することで、高負荷時にリソースを集中させて処理を行うことができる。実証実験では優先度に応じたリソース制御を行う場合と行わない場合で突発的な負荷

に対する仮想マシンの稼働状況のモニタリングを行ったが、リソース制御を行う場合では仮想マシンの過負荷状態を回避することができ、正常なサービスレベルを維持できることが明らかとなった。

4.2.8.2. **データセンターに関する監査**

概要

環境クラウドサービスでは、プラットフォームの運営を他社に委託する場合があるため、データセンターのセキュリティレベルの判断に当たっては、プラットフォーム提供者がデータセンターに関する認証を取得しているかどうか、また外部業者による監査を受け入れる用意があるかどうかを一つの目安として考慮することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者のデータセンターに対する利用者又は適切な第三者機関による監査の受け入れ

【環境クラウドサービス利用者】

・データセンターへの外部監査が可能であることの確認

4.2.8.3. **環境クラウドサービス事業者の SLA の根拠**

概要

環境クラウドサービス事業者の SLA の正確性・妥当性を確認するため、クラウド基盤の技術要素と SLA の関連性を把握し、複数の事業者を比較できることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー、インフラレイヤー）

・利用者からの求めに応じた可能な範囲でのクラウド基盤のアーキテクチャ情報の開示準備

【環境クラウドサービス利用者】

・可能な範囲でのデータセンター等のクラウド基盤のアーキテクチャ情報の入手及び SLA との関連性の把握

4.2.8.4. **データセンターの適正な運用管理区分**

概要

環境クラウドサービスでは、プラットフォームの運営を他社に委託する場合があり、そのデータセンターのセキュリティレベルが脆弱であればサービスも影響を受けるため、サーバ基盤やネットワーク基盤、それらの運用基盤、あるいは運用担当者について適切な区分を規定し、責任の範囲を明確化しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者によるクラウド基盤の運用管理区分に関する適切な規定に従った運用

・利用者の求めに応じた運用管理区分の開示

4.2.8.5. **データセンターのメンテナンスポリシーの設定・確認**

概要

環境クラウドサービスでは、エネルギー管理に関する機密性の高いデータや設備オーナーやテナント等の情報が扱われる場合があるため、システムに脆弱性が見つかった場合には速やかにパッチを適用する等のセキュリティ対策を講じるとともに、環境クラウドサービスが利用するデータセンターの保守についても日々のセキュリティ維持の体制が確保されていることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー、インフラレイヤー）

・プラットフォーム提供者によるデータセンター基盤のセキュリティメンテナンスの継続実施

・利用者の求めに応じたメンテナンスポリシーの開示

【環境クラウドサービス利用者】

・データセンターメンテナンスポリシーの確認

4.2.8.6. **データセンターにおけるプロセス改善**

概要

環境クラウドサービスでは、プラットフォームの運営を他社に委託する場合があるため、プラットフォーム提供者がデータセンター運用上のプロセス改善のスキームを所持していることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー、インフラレイヤー）

・利用者の求めに応じたプロセス改善スキームの開示

4.2.8.7. **環境クラウドサービス事業者が提供するテクニカルサポートの確認**

概要

環境クラウドサービス利用者の先に別のエンド利用者が存在し、環境クラウドサービス利用者がテ

クニカルサポートを提供している場合には、データセンターを提供する環境クラウドサービス事業者のテクニカルサポートの品質が影響するため、あらかじめ環境クラウドサービス事業者が提供するテクニカルサポートを確認しておくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（プラットフォームレイヤー、インフラレイヤー）

・データセンターに関連するテクニカルサポートの品質が、利用者だけでなく、その利用するサポートサービスの品質にも影響を与えることを認識した適切なサポートの提供

【環境クラウドサービス利用者】

・事業者のテクニカルサポートの品質を踏まえた上での自身が提供する環境アプリケーションのサポート品質の規定

4.3. 環境負荷軽減効果の評価

本節では、環境負荷軽減効果を評価するために、留意することが望ましい要件を解説する。

4.3.1. 環境負荷軽減効果の可視化

目的：環境クラウドサービスは、対象施設を適切に設計・施工した上でデータを収集し、施設の適切な維持・管理に資するだけでなく、データを公開することによってエネルギー効率活用等にも貢献する。こうした環境負荷軽減効果の可視化について主に利用者等が満たすことが推奨される要件を明確化する。

環境クラウドサービスを利用することによって、どの程度環境負荷軽減効果が得られるかを利用者が把握することは重要である。

このため、主に環境クラウドサービス利用者が留意することが望ましい項目について、以下のとおり細分化して解説する。

4.3.1.1 分析評価手法と可視化方法の階層的分類（モデル A 実証実験より得られた知見等）

4.3.1.2 データ可視化によるネットワーク型制御と省エネ意識の普及啓発（モデル B 実証実験より得られた知見等）

4.3.1.3 デジタルサイネージ等での普及啓発コンテンツの発信（モデル C 実証実験より得られた知見等）

4.3.1.4 計測ポイントの設定

4.3.1.5 評価指標の設定

4.3.1.6 データ可視化方法の設定

4.3.1.1. 分析評価手法と可視化方法の階層的分類（モデル A 実証実験より得られた知見等）

概要

エネルギー消費の分析を効果的に行うため、管理対象や目的、評価指標、可視化手法等を階層化・

分類することが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス利用者】

（アプリケーションレイヤー）

・ビルのエネルギーや性能を評価する方法におけるトップダウンアプローチとボトムアップアプローチを繰り返すことの検討

（例えばモデル A では、建物全体から特定の部分やサブシステムに向けて対象を細分化しながら性能検証を行うトップダウンアプローチと、特定の部分や機器からシステムや建物全体に向けて性能検証を行うボトムアップアプローチを組み合わせて分析・可視化が行われる。）

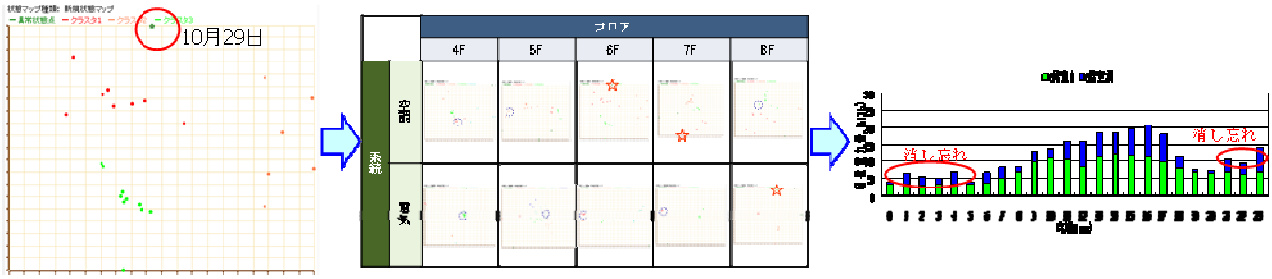
実証実験により得られた知見

＜モデル A 実証実験を踏まえた知見＞

・ビル管理においてはセンサーが多数存在するため、効率的な分析を行うことが求められる。収集したセンサー情報に対して、分析項目を階層的に分類し、トップダウンアプローチによる分析を行うことにより効率的にビル全体の分析から特定の箇所への分析を行うことが可能になる。

＜実証内容＞

ビル管理で利用されるエネルギー指標は数多く存在し、またエネルギー消費を可視化する際の切り口もエネルギー種別、用途、系統、フロア単位、機器単位、時間単位等、様々なアプローチが存在している。また、ビルの規模が大規模になるほど監視対象が増加するため、ビル管理者が分析しなければならないエネルギー情報も増える。そのため、実証実験ではエネルギーが無駄に消費されている状態（エネルギーフォルト）を効果的に検知するため、膨大なセンサー情報を階層的に分類して分析を深めていくことで普段のエネルギー消費傾向と異なる箇所を特定していくトップダウンアプローチによる分析を実証した（図 4-21）。



ビル全体の消費電力量（日別）の特異点分析　　フロア、エネルギー系統の消費電力量（日別）の特異点分析　　空調機の消費電力量（時間別）の分析

図 4-21　トップダウンアプローチによるモデル A 分析の実証

＜実証結果＞

トップダウンアプローチによる分析において、最初にクラスター分析によって特異日の抽出（上記10 月 29 日）を行うことで分析範囲を絞り、次にフロア、エネルギー系統別の消費電力量の特異点分析を行い、疑わしいフロア、エネルギー系統を絞り、さらに時間別での特異点を抽出することでエネルギーフォルトが発生している箇所・時間帯を効果的に特定することができた。

4.3.1.2. データ可視化によるネットワーク型制御と省エネ意識の普及啓発（モデル B 実証実験より得られた知見等

概要

環境クラウドサービス利用者が運用による改善、ネットワーク型制御等を実施していくため、必要な消費エネルギーのリアルタイム表示及び期間分析結果等を広く提供していくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス事業者及び利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス事業者】

（アプリケーションレイヤー）

・サービス利用者の属性に応じた可視化手段の選択

・ネットワーク型制御を実施する場合のサービス事業者とサービス利用者の合意

【環境クラウドサービス利用者】

・データによる施設管理省エネ効果の確認と省エネ意識の向上

実証実験により得られた知見

＜モデル B 実証実験を踏まえた知見＞

エネルギー消費分析のデータに関しては、対象設備ごとに利用状況が異なることを留意しなければならない（企業活動の内容、運転時間、運転目的等）。そのため、実際にネットワーク型制御を実施する場合には、データに基づき制御方針を検討し合意に至るプロセスが重要である。また、一般住宅の場合、外出先からでもモバイルデバイス等を活用し、家電等の稼働状況を確認できる仕組みを提供する等、省エネのポイントに気付きを与えることが重要である。

＜実証の内容＞

①ネットワーク型制御の実現

環境クラウドに蓄積したエネルギー消費分析のデータを活用し、環境クラウド側から空調運転の制御を行った。検証に当たっては、室温・外気温差がある場合でも、快適環境の維持しやすい方法である SAT(供給空気温設定)で制御検証を行った。

【空調制御の目的例】

種類	内容
BAU（通常制御）	快適環境を考慮しながら、エネルギー消費量の削減
デマンドコントロール	ピーク電力のカットによる基本料金の削減
PLA（ピーク負荷回避）	エネルギー消費量の平準化によるピーク負荷回避

【空調制御の方法例】

制御の種類	内容
SAT（供給空気温設定）	快適環境を考慮しながら、エネルギー消費を最小限に抑えるための設定温度の制御
LR（ロードローテーション）	快適環境を考慮しながら、空調機のオフ/オン、または、 ファン速度の制御により、個々の空調負荷を最適にすることで、エネルギーを削減
外気冷却	外気温が室温より低い場合に、外気を用い冷房のエネルギー削減に利用
動的発停	業務開始時刻に快適な温度になるよう空調機を起動する時刻を決定

サービス利用者との制御方針の打ち合わせにおいては、環境クラウドのデータ分析結果を以下のとおり整理し、利用者の合意を得た。

【制御方針案】

場所	調査結果	制御方針
オフィス内空調	空調機は停止中のものも多く、稼働中の運転モードは、暖房、冷房、自動、送風と様々。 しかも、暖房、自動では運転中であっても、設定温度と室温が乖離している。 この時期の夜間の温度が5度以下であるが、空調機のある天井裏の温度は20度以上に保たれており、断熱性の良い建物と思われる。	✓まず、各空調機設定場所において、空調機の測定する「室温」（吸気温度）と、人の高さにおける温度との差を 確認。 ✓室温が設定温度以上になる場所では、室温に合わせて空調機の停止、あるいは間歇運転制御の検討。 ✓室温が設定温度に届かない場所においては、空調機性能に合わせた設定温度幅で制御する（SAT制御） ことで、省エネを図る。 ✓その他の場所では、室温に合わせた設定温度で制御する（SAT制御） ことで、省エネを図る。

②一般住宅のサービス利用者へのフィードバック方法の検討

学生寮及び企業社宅合計 28 宅に HEMS の構成要素であるスマートタップを設置し、Bluetooth を活用してエネルギーデータの集計を実施した。 フィードバック用のアプリケーションを提供する際、スマートタップを活用した省エネ効果を以下の 2 つと仮定した。

・指定期間のエネルギー消費分析をフィードバックすることによるエネルギー利用行動の改善

・リアルタイムデータを外出先から稼働状況を確認できることによる消し忘れ防止。

実証実験では、ウェブサービスでデータ利用のトレンドを確認できる機能とスマートフォンでデータ利用状況を確認できる機能を提供した。

＜実証結果＞

ネットワーク型制御に関しては問題なく実施できることを確認した。制御方針については、利用者の活動特性を考慮すること、季節変動により見直す必要があることを確認した。アプリケーションによるフィードバックに関しては、利用者のデバイスに制限をつけることが困難なため、汎用的なアプ

リケーションでの提供が望まれた。また、スマートタップを活用してエネルギー集計を行う場合、電波干渉等の課題もあることから設置時の確認が必要になる。さらに、異常監視（使い過ぎや消し忘れ）とアラート（携帯メールなど）が提供されると、より有効であるとの意見もあった。

4.3.1.3. デジタルサイネージ等での普及啓発コンテンツの発信（モデルＣ実証実験より得られた知見等）

概要

広く地域住民に対して環境負荷軽減の啓蒙を行うため、環境クラウド上で蓄積・管理している情報や加工した情報を広く提供していくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス利用者】

（アプリケーションレイヤー）

・地域住民に対して情報提供を行う際における属性に応じた可視化の実現

実証実験により得られた知見

＜モデルＣ実証実験を踏まえた知見＞

・エネルギー需給に関して、地域住民に普及啓発を行う際には、その構成が多様であることから、属性に応じた可視化を行うことが重要であると考えられる。また、可視化する際には、可視化が住民の行動改善を促すよう情報の提供方法を工夫する必要がある。

＜実証内容＞

地域の住民に対して、環境クラウド上で蓄積・管理する情報を提供する際には、その情報の受け手を意識した情報の提供を行う必要がある。そこで、実証実験では、様々な対象者を想定し、それぞれの対象にあった情報の可視化をすることによって、エネルギー需給に係る意識啓発を行うための検証を行った。（図 4-22）。

(1)路面電車内でのサイネージ　(2)太陽光パネルの発電量　(3)発電量のグラフ

図 4-22　デジタルサイネージを活用した市民への普及・啓発

＜実証結果＞

エネルギーデータの公開に関しては、閲覧対象者、場所等によりそのコンテンツを変更すべきという意見が大半を占めた。環境クラウドで取得される太陽光発電量や EV インフラの情報と気温、CO_2濃度等の外部のデータベースのデータを組み合わせることで市民への見える化による普及啓発の効果を高められたと考えている。

4.3.1.4. **計測ポイントの設定**

概要

設備のライフサイクルにわたって情報マネジメントを効率的に実施するためには必要な情報を長期間にわたり収集・蓄積し、分析・可視化することが重要であることから、計測ポイントを設定する際には、「どのようにエネルギーや性能を管理するのか」という点を念頭におくことが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス利用者】

（アプリケーションレイヤー）

・設備の使用用途と求められる評価指標に基づく計測ポイントの設定

（例えばモデル A では、近年設備への要求が短期間で激しく変化するようになり、「いま設備に何が求められているのか」、「いま何ができるのか」ということを明確に把握することが重要である。使用用途の例には、通常の事務室/サーバ室/倉庫などがあり、評価指標の例には、夏季 26±1℃/40±5%、24 時間運転なのか 9 時－20 時運転なのか等がある。）

・設置機器の種類、機能、能力、要求される運転方法に基づく計測ポイントの設定

（例えばモデル A では、設備の設計段階での要望が実際にどのように反映されているか、またそのためにどのような機能や仕組みが用意されており、それをどのように運用するよう考えているのかを明確に把握する必要がある。機器の例には、コージェネレーションシステム/蓄熱システム/外気冷房などがあり、運転方法の例には、外気のエンタルピが室内より低いとき外気冷房する等がある。）

・計測計量されているポイントに関する情報と正確性の確認

（例えばモデル A では、計測計量されているポイントの場所と名称が一致していること、計測計量されている値が定格値や実際に計測した値と比べ正しい値を示していること、センサーが定期的に保守されていること、などが挙げられる。）

4.3.1.5. **評価指標の設定**

概要

設備のライフサイクルにわたって情報マネジメントを効率的に実施するため、計測データが評価対象であるビルの目的、要求仕様に応じた評価指標として加工されることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス利用者】

（アプリケーションレイヤー）

・定期的評価の観点からの評価指標の設定

（例えばモデル A では、エネルギー消費原単位の比較のように他の設備や過去のデータなどと「量」が比較され、1 日～1 ヶ月、1 年というように期間を設定して利用され、リアルタイム性が要求されない指標を活用している。この場合、評価結果をビルオーナーやテナントにも説明する場合があり、非技術者にも理解できるような解析や可視化が求められる。）

・日常的評価の観点からの評価指標の設定

（例えばモデル A では、機器の動的挙動や制御性の評価、ピークカット/シフトのようなデマンドの評価に利用され、リアルタイム性が求められる。この場合、指標そのものは技術者が利用しやすいように活用すればよい。）

・必要に応じた評価指標の設定

（例えばモデル A では、機器やシステムに異常や不具合が発生した場合に、その原因を特定するために利用される指標で、緊急性が求められる場合が多い。）

・計測値・制御量を直接比較する観点からの評価指標の設定

（例えばモデル A では、電力消費量や温度など、計測された値を直接比較するものであり、時系列のトレンド、同一規模/用途のものとの比較や、値自身の正確性の確認に用いられる。）

・異なる規模・種類のものを比較する観点からの評価指標の設定

（例えばモデル A では、「電力量」「冷水量」など、量で計測される値を「単位面積あたり」「化石燃料」「温暖化ガス量発生量」に換算し、規模や用途が異なるものとの比較に用いている。）

・効率や性能を比較する観点からの評価指標の設定

（例えばモデル A では、成績係数（COP）、WTF、ATF など、「仕事量」を「消費エネルギー」で除した無次元数として換算した指標を用いている。メーカーカタログ値、新設時、過去の値と比較し、機器の不具合や経年劣化の検出に用いられる。）

・制御性を比較する観点からの評価指標の設定

（例えばモデル A では、出入口温度差、設定値との差、設定値との差×時間のように設計条件との乖離を定量化し評価するものとして利用可能である。）

4.3.1.6. **データ可視化方法の設定**

概要

設備のライフサイクルにわたって情報マネジメントを効率的に実施するため、効果的なデータの可視化を行うことで改善施策の検討や情報共有に役立てることが望ましい。

推奨要件（実施の手引き）

環境クラウドサービス利用者は、例えば、次の項目に留意することが望ましい。

【環境クラウドサービス利用者】

（アプリケーションレイヤー）

・規模、用途、時間経過を確認・評価する観点からの可視化方法の設定
（例えばモデルAでは、棒/折線/円グラフ等を用いることが多く、グラフの横軸は「規模」「用途」「時間」であることが多い。主に相対的な評価に利用される。）
・データごとの相関性を確認・評価する観点からの可視化方法の設定
（例えばモデルAでは、散布図を用いることが多く、主に傾向分析やシミュレーションに利用される。）
・発生頻度やピークを確認・評価する観点からの可視化方法の設定
（例えばモデルAでは、降順グラフを用いることが多く、グラフの横軸は「時間」であることが多い。グラフから最大値、最小値、継続時間を確認することができる。）

5. その他参考事項

5.1. 用語解説

クラウドコンピューティング	本ガイドラインにおける「クラウド」とは、「クラウドコンピューティング」の略称として用いている。なお「クラウドコンピューティング」とは、データーサービスやインターネット技術などが、ネットワーク上にあるサーバ群（クラウド（雲））にあり、利用者は今までのように自分のコンピュータでデータを加工・保存することなく、「どこからでも、必要な時に、必要な機能だけ」を利用することができる新しいコンピュータネットワークの利用形態を指す。
IPv6(Internet Protocol Version 6)	IPv4の後継規格であり、IPアドレスがほぼ無限（3.4×10の38乗個）、IPv4に比べてセキュリティの強化及び各種設定が簡素化される等の特徴がある。
環境情報	エネルギーの需給に関する情報や気温、湿度等の情報。
環境クラウドサービス	クラウド技術を活用し、家庭、業務用ビル、又はそれらを含む一定の地域全体のエネルギーの需給に係る情報（消費電力、気温、湿度等）を収集・解析し、各機器や設備の制御を行う仕組み。
環境負荷軽減型地域ICTシステム	家庭、業務用ビル、又はそれらを含む一定の地域全体における、エネルギーの需給を最適化するシステム。

5.2. 関係ガイドライン

5.2.1. クラウドサービス、情報セキュリティ分野等に係る基準・ガイドライン

本ガイドラインは、環境クラウドサービスの提供や利活用を具体的に想定し、その有用性や潜在性を最大限発揮することを念頭に、関係する事業者、利用者の双方が活用することを想定してセキュリティ面の留意事項を中心に整理している。そのため、クラウドサービスや情報セキュリティ等の分野について、より具体的な内容を理解する場合には、以下に一例として示すような当該分野に特化した

法令・基準・ガイドライン等を参照いただきたい。

文書	団体	内容
・ Security Guidance for Critical Areas of Focus in Cloud Computing V2.1	CSA (Cloud Security Alliance)	2009年4月に初版が発表されたクラウドセキュリティガイダンス。CSA とはクラウドコンピューティングのセキュリティを確保するためのベストプラクティスの利用促進を行っている業界団体。
・ Cloud Computing: Information Assurance Framework ・Cloud Computing: Benefits, risks and recommendations for information security	ENISA （European Network and Information Security Agency)	2009 年 11 月に発行されたクラウドコンピューティングのセキュリティに関する文書。ENISA とは2004年3月に設立された欧州連合（EU）の機関で、ネットワークセキュリティ及び情報セキュリティに関する予防・対応能力を促進することを任務としている。
・監査基準委員会報告第 18 号	日本公認会計士協会	公認会計士又は監査法人が保証業務として報告書を提供する際に基準として用いられる文書。 主に、4.2.1(責任分界点の設定)、4.2.2(ガバナンス及びエンタープライズリスクマネジメント)、4.2.3(法制度及び電子情報の開示)、4.2.4(コンプライアンス及び監査)に関係。
・SAS70：Reports on the Processing of Transactions by Service Organizations	AICPA （American Institute of CPA s）	18 号と同様、公認会計士又は監査法人が保証業務として報告書を提供する際に基準として用いられる文書であるが、18 号との間に実質的な違いはない。 主に、4.2.1(責任分界点の設定)、4.2.2(ガバナンス及びエンタープライズリスクマネジメント)、4.2.3(法制度及び電子情報の開示)、4.2.4(コンプライアンス及び監査)に関係。

5.2.2. **情報の取り扱いに係る基準・ガイドライン**

5.2.2.1. **関係法令による制約等の存在への留意について**

本ガイドラインで対象とする環境情報は、エネルギーの需給に関する情報や気温、湿度の情報等であるが、ビルオーナーやテナントが活用するビルに係わる情報に限定されず、都市や地域における幅広い情報を対象としている。地域においては、行政に係わる情報とともに統計情報や地理空間情報と重ね合わせて提供されることもあるため、多様な情報の集合体になることが想定される。そのような場合には、情報を管理する主体が多様となり、多くの関連法令が関わることになるため留意すべき点も多くなる。

環境情報に係る関連法令としては、個人情報の保護に関する法律（平成 15 年法律第 517 号)、著作権法（昭和 45 年法律第 48 号)、統計法（平成 19 年法律第 53 号)、気象業務法（昭和 27 年法律第 165 号）等が想定されるが、場合によって情報管理や２次利用等に際し、何らかの要請や制約を受ける可能性も生じてくる。そのため、個々のケースに応じて収集する環境情報の内容を十分に判断し、関連法令による制約等の存在について留意することが必要である。

5.2.2.2. **参考となる基準・ガイドラインの例について**

環境クラウドサービスにおける情報の流通・利用に関して参考となる基準・ガイドラインの例として、「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」(座長：堀部 政男　一橋大学名誉教授）第２次提言（平成 22 年 5 月 26 日公表）及び「電気通信事業における個人情報保護に関するガイドライン（平成 16 年総務省告示第 695 号。最終改正平成 22 年総務省告示第 276 号）の解説」を紹介する。

○「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」第２次提言

総務省は、新たなサービスの登場や新技術を活用した情報の流通などによって、通信の秘密、個人情報保護、知的財産保護等といった諸権利との関係を整理する必要が生じてきたことから、平成 21 年 4 月から、「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」を開催し、様々な課題に対する具体的な対応策の検討を行っている。

平成 21 年 8 月には、「インターネット地図情報サービス」、「違法音楽配信対策」及び「電気通信事業における個人情報保護に関するガイドラインの改正」について取りまとめ、第一次提言として公表し、その後、平成 22 年 5 月に「CGM サービス」、「ライフログ活用サービス」及び「安全管理措置」について取りまとめ、第２次提言として公表している。

ここでは、特に環境情報の流通・利用に当たって参考になると考えられる「ライフログ活用サービス」に係る記述の一部を抜粋する。

＜参考：匿名化＞

行動ターゲティング広告や統計情報を提供するサービスについては、必ずしも個人を識別する必要がないことから、個人識別性を具備する情報に対して匿名化を行うことで個人識別性を喪失させ、流通や利活用を容易にする取組が検討されている。

個人識別性を備える情報には、（１）契約者情報等の、それ単独で個人識別性を有する場

合と、（２）利用者のウェブページ上における閲覧履歴、購買履歴、入力履歴等の行動履歴から生じ得る場合が存在する。

現在、個人識別性の獲得リスクを回避するために、各方面においてk-匿名化等の処理のアプローチが検討されているが、課題も指摘されており、客観的に、完全に個人識別性を喪失させるのは容易ではなく、結局、ケースバイケースの判断によらざるを得ない。

なお、匿名化を行って個人識別性を喪失させる行為は個人情報の利用に当たらないため、個人情報取扱事業者は、匿名化を個人情報保護法上の「利用目的」として、特定する必要はないと解される。

個人情報の保護に関する法律の規定する利用目的の特定（第 15 条）の趣旨は、不必要に又はみだりに個人情報を取り扱うことを制限するとともに、個人情報の取扱いの透明性を図り、本人自らが権利利益の侵害を未然に防止するために必要な対応をとることができる環境を整備しようとするものである。一方、匿名化を行って個人識別性を喪失させる行為は、個人の権利利益の侵害のおそれを小さくするものであり、利用目的の特定等の義務を課さない方がむしろ法の趣旨に沿うと考えられる。

なお、ライフログ活用サービスは、その態様によっては、プライバシーを侵害し得るし、利用者の不安感等を惹起し得る（例えば、個人識別性のない情報も転々流通するうちに個人識別性を獲得してしまうおそれ等もある。）。このため、ライフログを取得・保存・利用する事業者はライフログの取扱いにあたって利用者に対して一定の配慮をなすことが望ましいとされており、第２次提言では、各業態における自主的なガイドライン等の策定の指針となる配慮原則が示されている。具体的な配慮原則は以下の６つである。

＜配慮原則＞

①広報、普及・啓発活動の推進

対象事業者その他の関係者は、利用者のリテラシーの向上や不安感や不快感の払拭に資するべく、対象情報を活用したサービスの仕組みや、本配慮原則に基づく取組について、広報その他の啓発活動に努めるものとする。

②透明性の確保

対象事業者その他の関係者は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知り得る状態に置く（以下「通知等」という。）よう努めるものとする。通知等に当たっては、利用者が容易に認識かつ理解できるものとするよう努めるものとする。

③利用者関与の機会の確保

対象事業者は、その事業の特性に応じ、対象情報の取得停止や利用停止等の利用者関与の手段を提供するよう努めるものとする。

④適正な手段による取得の確保

対象事業者は、対象情報を適正な手段により取得するよう努めるものとする。

⑤適切な安全管理の確保

対象事業者は、その取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要かつ適切な措置を講じるよう努めるものとする。

⑥苦情・質問への対応体制の確保

対象事業者は、対象情報の取扱いに関する苦情・質問への適切かつ迅速な対応に努めるものとする。

また、上記提言を踏まえ、「電気通信事業における個人情報保護に関するガイドラインの解説」の一部が改正されている。

○「電気通信事業における個人情報保護に関するガイドラインの解説」（一部抜粋）

（利用目的の特定）

第５条　電気通信事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定するものとする。

２　電気通信事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行わないものとする。

３　前２項の規定により特定する利用目的は、電気通信サービスを提供するため必要な範囲を超えないものとする。

（解説）

（１）　（略）

（２）　「その利用の目的を…できる限り特定」するとは、個人情報がどのような目的で利用されるかをできるだけ具体的に明確にするという趣旨である。したがって、単に「サービスの提供のため」や「業務の遂行のため」といった抽象的な目的では足りず、例えば、「加入者の本人確認、料金の請求、料金・サービスの変更及びサービスの休廃止の通知のため、加入者の氏名、住所、電話番号を利用します。」のように具体的に特定すべきである。

なお、個人情報に対して、特定の個人を識別できないようにする加工（いわゆる匿名化）を行うことは、個人情報の利用に当たらず、利用目的として特定する必要はない。

（３）・（４）　（略）

5.3.　環境クラウドに使用可能な技術、規格等

環境クラウドの各モデルのシステムの構成要素においては、以下のような技術・規格等が市場に展開されており、使用可能であると考えられる。

＜モデル共通＞

IPv6（インターネットプロトコル）

＜モデル A＞

BACnet、LonWorks など（ビル管理の情報を通信するために使用可能なプロトコル）

＜モデル B＞

BACnet、LonWorks など（施設関連の情報を通信するために使用可能なプロトコル）

Zigbee、Bluetooth など（一般居住施設におけるエネルギー情報収集するために使用可能なプロトコル）

SOAP など（ゲートウェイと個別機器間で情報を授受するために使用可能なプロトコル）

NetBIOS（ゲートウェイから BEMS 内のデータ取得のために使用可能なプロトコル（Samba 利用時））

IEEE802.15.4（電車内に設置した温湿度計からデータを収集するために使用可能な無線プロトコル）

＜モデル C＞

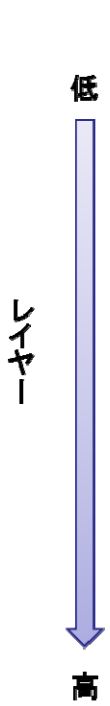
RS485（ゲートウェイと太陽光発電装置との間でエネルギー情報を授受するために使用可能なプロトコル）

IEEE1888(環境センサーと環境クラウド側で通信するために使用可能なプロトコル)

5.4. IPv6 技術を活用した施設管理に係る技術の標準化動向

環境クラウドサービスでは、施設に設置した多量のセンサーを効率的に管理することが必要となる。また、センサーから収集した情報を分析し、環境クラウドから施設内の設備機器を直接制御することが想定される。これらの場合には、センサーや設備機器を制御するためのコントローラーが IPv6 に対応していることが望ましいと考えられる。

現在、IETF 等において議論されている IPv6 センサーネットワーク、設備管理プロトコルの標準化技術動向は以下に示すとおりである。



規格/プロトコル	概要
PLC	電力線を介した通信を行うための技術 ・電力線上でIP通信を行うことが可能
IEEE802.15.4	低コスト・低消費電力かつ高信頼／セキュリティを持つ無線技術
6lowpan	IEEE802.15.4無線上でIPv6通信を行うためのプロトコル ・ヘッダの圧縮や近隣発見の最適化により低消費電力を実現
RPL	不安定な無線リンク上でのルーティングプロトコル ・トポロジの動的な変化に対する柔軟な対応 ・スケーラビリティに対する耐性
CoAP	無線などの低速リンク上で効率的にデータを転送するためのプロトコル
LonTalk	設備機器のコントローラとサブシステムとを接続するプロトコル
BACnet	サブシステムと中央監視システムとを接続するプロトコル
oBIX	ウェブサービスを介して設備監視を行うためのプロトコル ・下位層に多様な設備管理プロトコルを収容可能
UGCCnet	ウェブサービスを介して設備監視を行うためのプロトコル ・下位層に多様な設備管理プロトコルを収容可能
Zigbee (Smart Energy Profile 2.0)	802.15.4やPLC上で6lowpan/IPv6/CoAPを利用し、通信を行うためのプロトコル

5.5. サービス調達事例

環境クラウドサービスの調達に類似した事例として、公的主体がビルの中央監視装置の更改を行った際の調達仕様書の事例を紹介する。システム構成として、原則 IPv6 を利用いることや、BACnet/IP 等のオープンなプロトコルを利用することが規定されている。

第○編　BA-LAN（Building Automation-LAN）
　第○章　システム構成
　　1　基本条件
　　(1)～(8)　（略）
　　(9) 原則 IPv6 とし、既存設備との対応でやむを得ない場合は、IPv4 にも対応する。
　　(10)プロトコルは、TCP/IP を採用する。
　　(11)各ＢＡ等が BACnet/IP プロトコルで運用できるようにネットワークレイヤの５層以上はフリーとする。
　　(12)～(18)　（略）
　　(19)ネットワーク監視のために、コアスイッチ及びディストリビューションスイッチは、SNMP 及び RMON に対応すること。また、コアスイッチは、NetFlow あるいは sFlow 等を利用して、通信状態が確認できること。

第○編　BMS（ビルマネジメントシステム）
　第○章　システム構成

1　概要　一般事項

本工事の新 BA-LAN を基本通信ネットワークとして有効活用するものとし、BACnet、TCP/IP 等のオープンなプロトコルにより、各種 BA、各種システムの運転情報を収集、蓄積し管理する。

2　基本要件

(1)機能要件

ア　（略）

イ　原則 IPv6 とし、既存設備との対応で技術的に不可能な場合は、IPv4 にも対応する。

ウ～ク　（略）