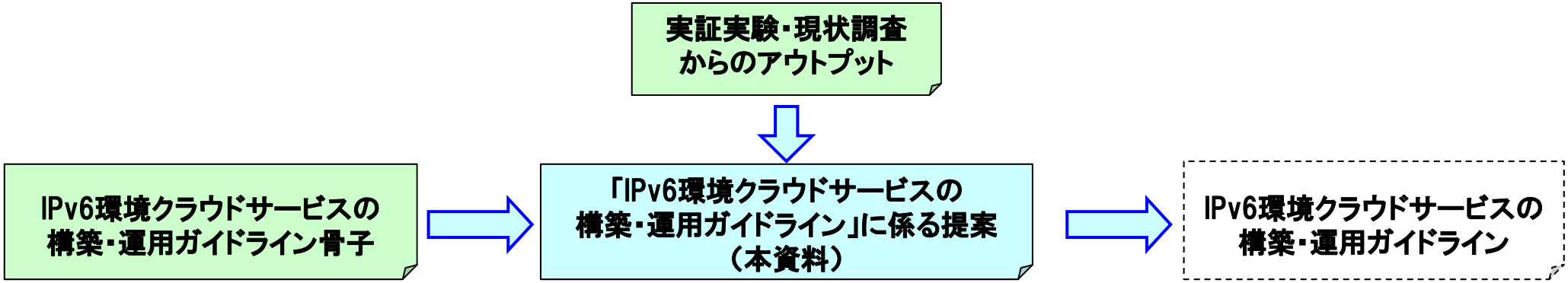
「IPv6環境クラウドサービスの構築・運用ガイドライン」に係る提案

平成23年2月24日
エヌ・ティ・ティ・コミュニケーションズ株式会社
三井情報株式会社

本提案の位置づけ

ガイドライン骨子記載事項	• 今後、平成21年度第二次補正予算施策「環境負荷軽減型地域ICTシステム基盤確立事業」における実証実験結果を踏まえ、それぞれの項目について推奨要件を設定するとともに、必要な具体化、詳細化を行い、ガイドラインを策定する予定である。

本提案は、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で取りまとめられた「IPv6環境クラウドサービスの構築・運用ガイドライン骨子」に基づき、平成21年度第二次補正予算施策「環境負荷軽減型地域ICTシステム基盤確立事業」における実証実験及び現状調査からのアウトプットを踏まえ、ガイドラインの素案として議論に供するために作成したものである。



なお、ガイドライン骨子の構成は

1. ガイドラインの目的
2. 用語の定義
3. ガイドラインの基本的な考え方
4. 対象となるモデル
5. システム構成に係る要件
6. システム構築・運用に係る要件

となっているが、実証実験や現状調査からのアウトプットが寄与できる項目としては上記の5及び6であることから、本提案のスコープは「システム構成に係る要件」及び「システム構築・運用に係る要件」とする。

「システム構成に係る要件」の具体化について（提案）

ガイドライン骨子記載事項	• それぞれのシステムの構成要素において使用可能な技術、規格等について記述する。 • それぞれの構成要素間のインターフェースについて、考慮すべき項目について記述する。

「システム構成に係る要件」を以下のように具体化する。

□　それぞれのシステムの構成要素において必要とされる機能、技術要素等について記述する※

・モデルA：
- ビル群エネルギー管理システム（クラウドサービス）
- エネルギー情報計測・収集・制御システム

・モデルB：
- 都市型施設エネルギー管理システム（クラウドサービス）
- エネルギー情報計測・収集・制御システム

・モデルC：
- 地域内エネルギー供給管理システム（クラウドサービス）
- エネルギー情報計測・送信システム

・モデル共通：
- IPv6インターネット

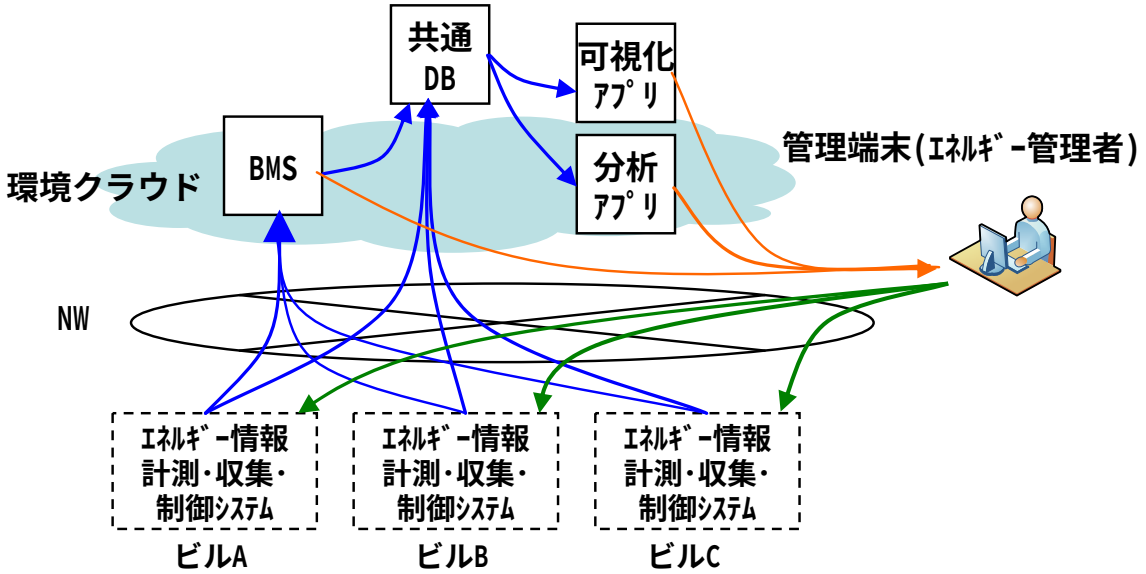
□　「構成要素間のインターフェース」について考慮すべき項目を記述する

□　環境クラウドにおけるIPv6技術の重要性について記述する

※なお、それぞれのシステムの構成要素において使用可能な技術、規格等については、ガイドライン本文で扱う性質のものではないため、参考情報として別紙で扱うものとする。

システム構成に係る要件（モデルA）

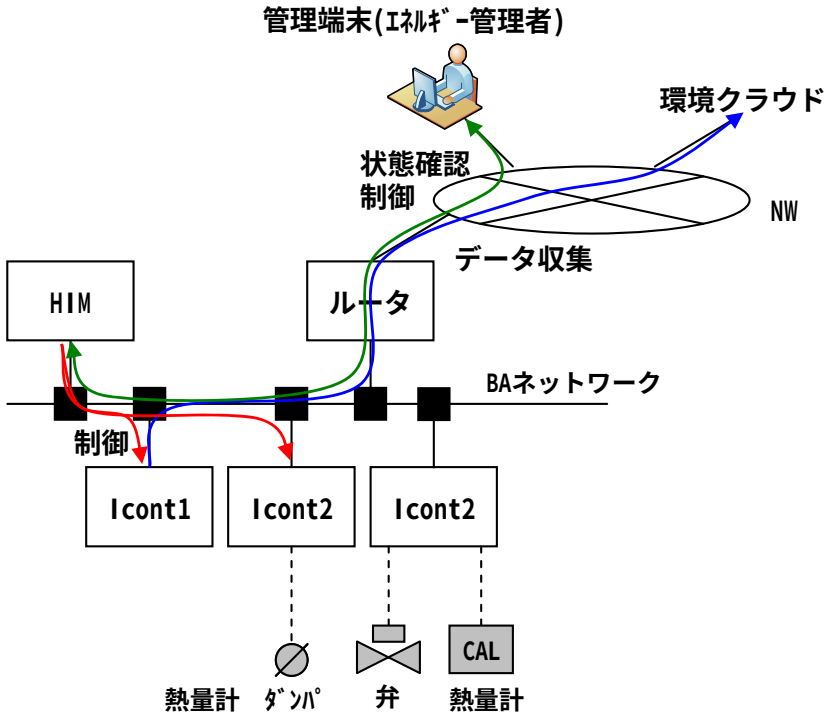
- ビル群エネルギー管理システムの構成要素(例)



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)	環境クラウド上に配置され、BMSやエネルギー情報計測・収集・制御システムからの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で収集されたビルのエネルギー関係データから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	環境クラウド上に配置され、共通DBで収集されたビルのエネルギー関係データから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で、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。

システム構成に係る要件（モデルA）

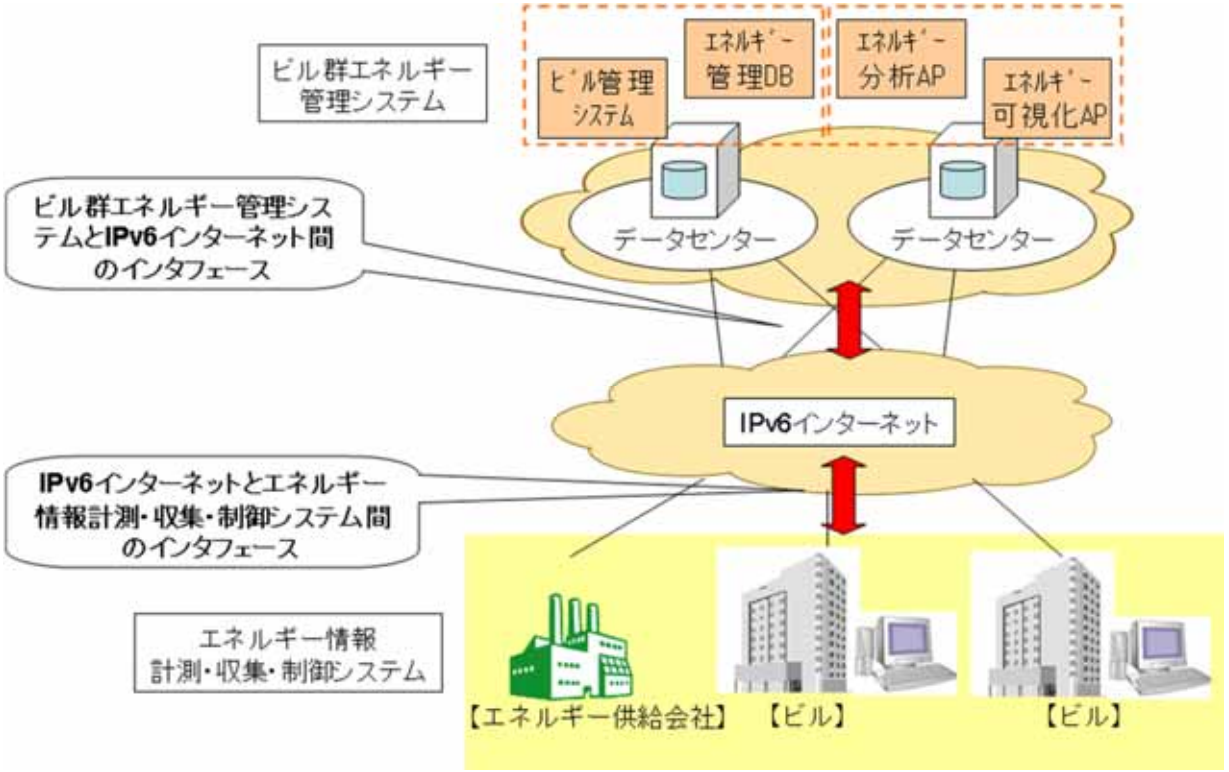
- エネルギー情報計測・収集・制御システムの構成要素（例）



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）で、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）で、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ためのもの。
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。

システム構成に係る要件（モデルA）

- 構成要素間のインターフェース

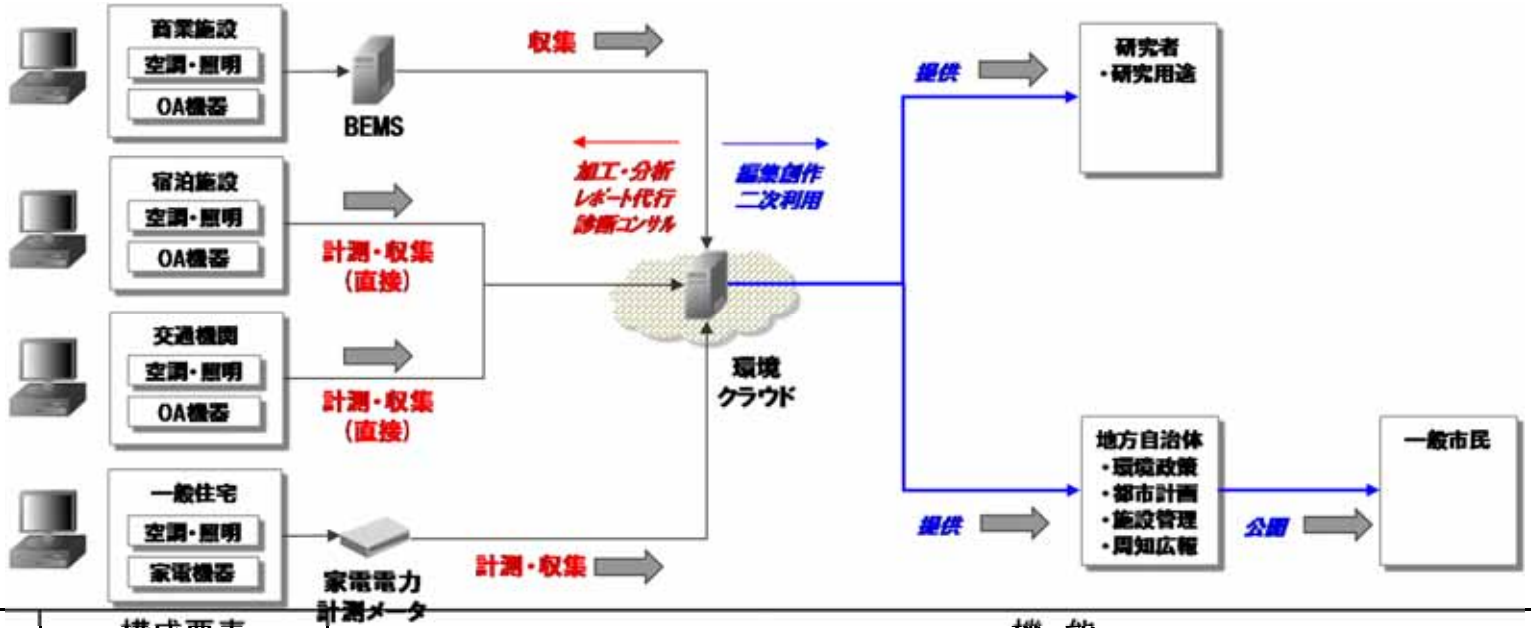


■ エネルギー情報計測・収集・制御システム、ビル群エネルギー管理システムでは、業界で普及が進んでいるプロトコルを搭載した製品が市場に出てきているものの、いまだ独自のプロトコルのシステムを使っているビルが多いという現状がある。そのため、各インタフェースは、マルチプロトコル・マルチベンダサポート対応により、接続性を確保することが望ましい。

■ 従来のエネルギー管理システム、エネルギー情報計測・収集・制御システムでは主にビル内での通信に閉じていたが、環境クラウドサービスではインターネットを経由した通信が行われる。 そのため、IPv6対応を実施するとともに初期段階ではIPv4との混在環境を想定して接続性を確保すること望ましい。

システム構成に係る要件（モデルB）

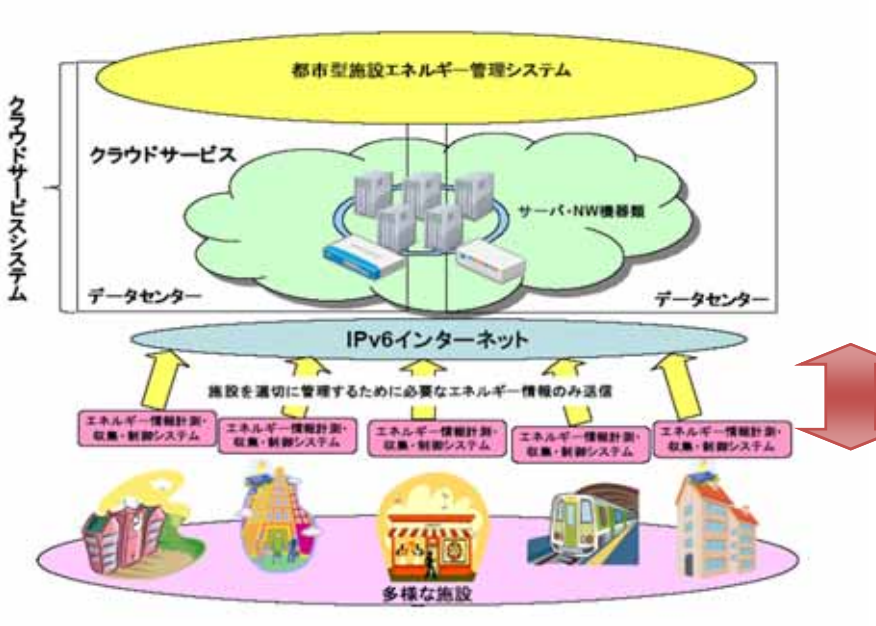
- 都市型施設エネルギー管理システム及びエネルギー情報計測・収集・制御システムの構成要素(例)



	構成要素	機　能
都市型施設 エネルギー管理 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等標準的なプロトコルで利用で利用することができる。
	環境クラウド データベース	エネルギー情報を蓄積するDB。事業者用及び分析用のデータベースを有する。
	認証モジュール	環境クラウドを利用するユーザー共通基盤。
エネルギー情報 計測・収集・制御 システム	ゲートウェイ	設備機器の独自言語を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・制御装置(BEMS)	既設のビル管理システム。BACnetやLonTalk等の独自のプロトコルを有し、設備機器の運転情報の収集や制御監視等を行っている。

システム構成に係る要件（モデルB）

- 構成要素間のインターフェース



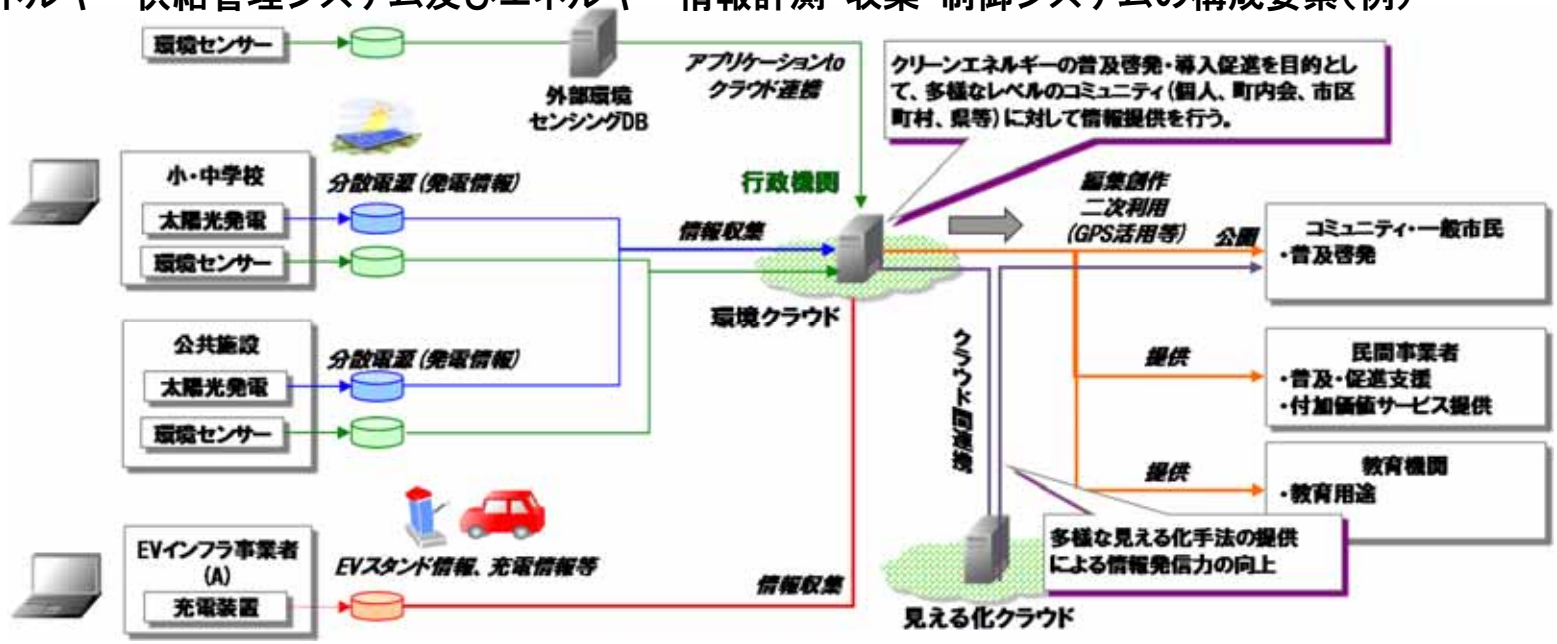
■ 都市型施設エネルギー管理システム（環境クラウド）とエネルギー情報計測・収集・制御システム間は、インターネットを介して接続される。その際、サービス利用施設の増加、セキュリティ面を考慮し、インターフェースはIPv6インターネットに対応していることが望ましい。初期段階ではIPv4との混在も必要となる。

■ エネルギー情報計測・収集・制御システム（ゲートウェイ）と施設内に設置されている家電電力計測装置間の通信に際しては、無線ベースでの情報収集を想定し、インターフェースは、BluetoothやZigbee等に対応していることが望ましい。

■ エネルギー情報計測・収集・制御システム（ゲートウェイ）と既存のBEMS等の設備管理システム間での通信に関してはデータ授受に際しては、LonWorksやBACnet等のプロトコルへの対応及びNetBIOSやFTPなどを介したCSVでの受け渡しに対応していることが望ましい。

システム構成に係る要件（モデルC）

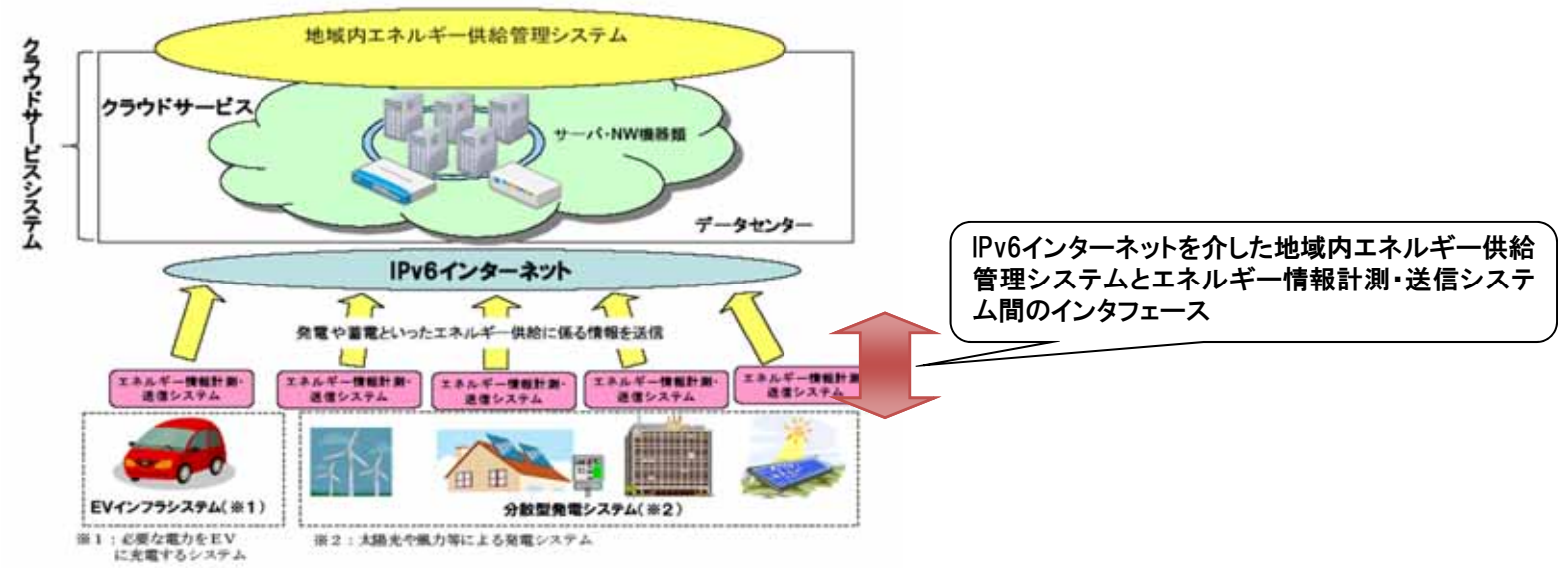
-地域内エネルギー供給管理システム及びエネルギー情報計測・収集・制御システムの構成要素（例）



	構成要素	機　能
地域内エネルギー供給管理システム（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等標準的なプロトコルで利用で利用することができる。
	環境クラウドデータベース	エネルギー情報を蓄積するDB 事業者用及び分析用のデータベースを有する
	認証モジュール	環境クラウドを利用するユーザー共通基盤。
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・CO2濃度等の地域の気象状況を修正するセンサー。FIAP等の標準化されたプロトコルでの通信が可能。

システム構成に係る要件（モデルC）

- 構成要素間のインターフェース



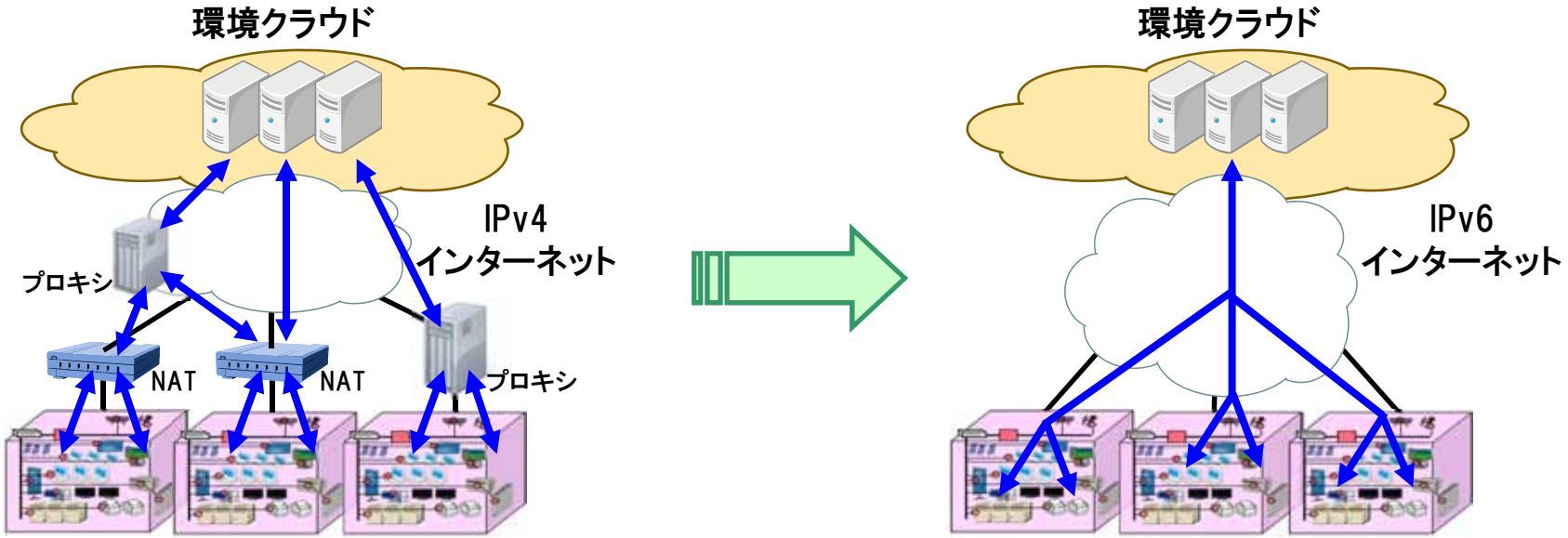
■ 地域内エネルギー供給管理システム（環境クラウド）とエネルギー情報計測・送信システム間はインターネットを介して接続される。計測対象機器の増加、センサー管理を考慮し、インターフェースはIPv6インターネットに対応していることが望ましい。初期段階ではIPv4との混在も必要となる。

■ エネルギー情報計測・送信システム（ゲートウェイ）と太陽光発電装置間の通信に関しては、屋外に設置されているため、基本的に無線での通信が必要となる。インターフェースは、RS485等に対応していることが望ましい。
ただし、メーカー毎にデータの配列が異なることを予め考慮しておく必要がある。

■ エネルギー情報計測・送信システム（ゲートウェイ）と環境センサー間の通信に関し、インターフェースは、FIAP等に対応することが望ましい。

環境クラウドにおけるIPv6技術の重要性

- インターネット等の通信インフラを介して環境クラウドで扱われる膨大な数のノードを管理する際、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
- IPv4を用いた場合、管理・制御対象のノードに対する通信方式が複雑なものになり(NATやプロキシサーバ、またそれらの間の通信を管理する特殊な機器やソフトウェアの導入・管理等)、システム全体のコスト上昇を招く他、中間ノードを介在させることによる通信パフォーマンスの低下も懸念される
- 従って、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重要であり、IPv6を活用することでシステムの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



「システム構築・運用に係る要件」の具体化について（提案）

- 「システム構築・運用に係る要件」を以下のように具体化する
  - ・推奨要件の具体化、詳細化に当たっての考え方：
    環境クラウドサービスの特性を考慮し、「ガイドライン骨子」の項目ごとに、推奨される要件を設定する際の考え方を記載
  - ・モデル共通：
    環境クラウドサービスに共通的に推奨される要件を記載
  - ・モデル別：
    モデルの特徴に基づいて個別に推奨される要件を記載（次ページにモデルの主な特徴と関連する項目を記載）
- 基本的に、事業者に推奨される要件を記載するものとし、必要に応じて、利用者がサービスを選択する際に有用な情報を記載する
- 推奨要件には該当しないが、実証実験等により得られた構築・運用に有用な情報を別途記載する

（参考）各モデルの主な特徴

	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
モデルの主な特徴と関連する項目	• 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）	• 省エネサービス事業者や地方公共団体等と連携して、多様な施設毎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） • 環境負荷軽減効果の分析を目的としたデータの2次利用	• 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） • 環境負荷軽減効果の分析や普及啓発を目的としたデータの2次利用
	✓ 計算負荷のバースト的な発生に対する柔軟な対処、リアルタイム処理 → 事業継続性、仮想化、データセンターの安全性確保、運用管理 ✓ ビルオーナーの要求を満たすエネルギー消費の分析と可視化 → 環境負荷軽減効果の可視化 ✓ 既存のビル管理システムからクラウドへのシームレスなマイグレーション → 移植性及び相互運用性、ID管理とアクセス管理	✓ 利用者の増加を想定した設計 → 仮想化、ID及びアクセス管理 ✓ インターネットを利用したサービス提供 → 事業継続性 ✓ 環境負荷軽減効果の分析を目的とした研究者等へのデータの提供（2次利用） → 情報管理、責任分解点、ガバナンス及びエンタープライズリスクマネジメント	✓ 急激な対象設備数の増加を想定した設計 → 事業継続性、仮想化、インシデント管理 ✓ 環境負荷軽減効果の分析を目的とした外部アプリケーションとのデータ連係 → 移植性及び相互運用性、ID及びアクセス管理、情報管理 ✓ 環境負荷軽減の普及啓発を目的として公共向けに情報提供（2次利用） → 移植性及び相互運用性、アプリケーション開発/運用管理、情報管理

システム構築・運用に係る要件（１）拡張性の確保

1. 移植性及び相互運用性

ガイドライン骨子記載事項	• 環境クラウドサービスにおいて、アプリケーションを構築するプラットフォームを変更する場合や、プラットフォームを構築するインフラを変更する場合があり、移植性・相互運用性は非常に重要な要素となる。従って、アプリケーション、プラットフォーム等のレイヤーに応じて注意を払うべき相互運用上の検討項目について記述する。

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			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事業者等が満たすことが推奨される要件を以下のとおり明確化。
推奨要件	モデル共通		• セキュリティ対策の文書化 （環境クラウドサービスの移植先のセキュリティレベルを評価・比較するため） • 処理能力の確認 （環境クラウドサービスの移植後に初期の処理能力を確保するため） • システムテストの実施 （環境クラウドサービスの移植先でのサービスの正常動作を事前に確認するため） • 多様なデータ移行手段の提供 （環境クラウドサービスの移植時に、データ容量に適した移行手段を選択し円滑に移植するため）
	モデル別	モデルA	• 異なる仮想化基盤間における移植方法の提供 （基盤として一般的なクラウドサービスの使用が想定されるため）
		モデルB	• 汎用性の高い移植手法の提供 （多様な施設毎の利用者のニーズに応じて、柔軟にサービスを移植するため）
		モデルC	• 標準的なデータ連係用APIの提供 （外部への情報発信や他のデータベースとの連携が想定されるため）

2. 事業継続性

ガイドライン骨子記載事項	• 事業継続性や災害復旧（ディザスタリカバリ）は極めて重視されることから、これらについて注意を払うべき項目について記述する。 • システムの信頼性について記述する

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			環境クラウドでは、関連する事業者とユーザ（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以下のとおり明確化。
推奨要件	モデル共通		• 事業継続計画（BCP）の項目検討 （リスクと影響を洗い出し、対応の優先度、手順を計画するため） • BCPの継続的な見直し （実効性を高く保つためには、BCPが現状に即していることが必要なため） • 妥当性のある目標復旧時間 （目標復旧時間が技術、運用面から根拠のあるものとして設定される必要があるため）
	モデル別	モデルA	• ディザスターリカバリ機能の確認 （ビル群管理の性質上、迅速なフェイルオーバーが求められるため）
		モデルB	• 安定的な制御の実施 （信頼性の低い回線の利用時でも、安定した監視・制御を行うため）
		モデルC	• 安定的なデータ収集基盤の提供 （データの欠損による情報への信頼性低下を防ぐため）

3. 情報管理

ガイドライン骨子記載事項	• 環境クラウドサービスにおいて利用者から収集したデータを事業者間で共有する際に考慮すべき項目を記述する。 • 環境クラウドサービスにおいて重要な情報を守るために、データセキュリティライフサイクル（作成→保存→利用→共有→アーカイブ→廃棄）のそれぞれの過程で考慮すべき項目について記述する。

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			環境クラウドでは、利用者から収集したデータを加工し、事業者間で共有したり、加工して二次利用等を行うケースも想定される。また、収集する環境情報は、プライバシ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以下のとおり明確化。
推奨要件	モデル共通		• データの完全性の確保と証明 （監査やデータ利用時には正しいデータが求められるため） • 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 （第三者のデータ利用防止のため） • 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 （意図通りにアクセス制御が機能しているかを確認するため） • 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 （マルチテナント環境では同じストレージを共有するため） • 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 （分離保存の機能が有効かを確認するため） • 契約終了、中途解約時の情報の扱いの明確化 （サービス利用終了時もデータが意図しない利用をされることを防ぐため）
	モデル別	モデルA	• 蓄積データの暗号化によるデータ安全性の確保 （ビル施設に関する内部情報を扱うため）
		モデルB	• 二次利用データの権利関係の整理 （二次利用データの利用目的、利用範囲を予め明確化する必要があると想定されるため）
		モデルC	• 情報の提供／利用者間での合意形成 （データの利用範囲が契約などで予め制限できない可能性があるため）

4. 仮想化

ガイドライン骨子記載事項	• 仮想化技術を用いたSaaS、PaaS、IaaSにおいて、仮想マシンを制御するハイパーバイザへの攻撃や、従来ネットワーク上で発生していた攻撃がハードウェアの内部へ隠蔽される等、仮想化に由来する様々なセキュリティリスクに対応するために考慮すべき項目について記述する。

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			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以下のとおり明確化。
推奨要件	モデル共通		• ゲストOSへのセキュリティ技術の適用による多層防御 （プラットフォームに依存しないセキュリティ施策を実施するため） • 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 （仮想化により新たに発生した監視すべき対象であるため） • 仮想マシンイメージの完全性の確保 （仮想マシンイメージが改ざんされる可能性があるため） • 認証に基づく仮想マシン管理機能へのアクセス制限 （管理機能を管理者以外の第三者に利用できないようにするため）
	モデル別	モデルA	• 仮想ネットワークのセキュリティ確保 （クラウド上に複数の環境アプリを展開・連携させることが想定されるため）
		モデルB	• 利用者の増加に対するスケールの確保 （サービス利用者の増加した場合であっても、安定的なサービスを提供するため）
		モデルC	• 計測対象の増加に対するスケールの確保 （計測対象の増加した場合であっても、安定的なサービスを提供するため）

5．アプリケーションの開発・運用管理

ガイドライン骨子記載事項	• 環境クラウドサービスのネットワーク（クラウドネットワーク、センサーネットワーク等）上で動作するアプリケーションを開発・運用する際に考慮すべきセキュリティ項目について記述する。

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			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以下のとおり明確化。
推奨要件	モデル共通		• 不要なサービスの停止 （不要なサービスの脆弱性によるセキュリティ低下を防ぐため） • アプリケーションログの管理 （ログから情報推測などが行えるため） • アプリケーションのセキュリティ評価 （アプリケーションの脆弱性検査のため） • プラットフォームへの攻撃に対する防御の実施 （プラットフォームの脆弱性に対処するため）
	モデル別	モデルA	
		モデルB	
		モデルC	• 標準的なWEB APIを介したデータアクセス手段の提供 （一般市民への情報提供時に、様々なアプリケーション・デバイスとの連携が想定されるため）

システム構築・運用に係る要件（２）情報セキュリティの確保

6. 責任分界点の設定

ガイドライン骨子記載事項	• 環境クラウドサービスにおいて、複数のサービス提供者が存在する場合の責任分界点を設定する際に考慮すべき項目について記述する。

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			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など、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以下のとおり明確化。
推奨要件	モデル共通		• 委託における通常運用時の責任分界点の設定 （委託時の責任分界点の明確化のため） • 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 （委託時の責任分界点の明確化のため） • データの収集、管理時の責任分界点の設定 （二次利用の場合における、データ管理責任の明確化のため）
	モデル別	モデルA	
		モデルB	• 二次利用DBの利用範囲の明確化 （二次利用データ提供後の情報の取扱いに関する責任分界点を明確にする必要があるため）
		モデルC	

7．ガバナンス及びエンタープライズリスクマネジメント

ガイドライン骨子記載事項	• 環境クラウドサービスを提供するにあたって、情報セキュリティガバナンスやリスク管理の観点から考慮すべき項目について記述する。

ガイドラインに記載すべき事項の要点（案）		
推奨要件の具体化、詳細化に当たっての考え方		**クラウドサービスを利用することによって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ことが考えられる。 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以下のとおり明確化。**
推奨要件	**モデル共通**	• **サービスの特性を考慮した事業者の選定** （事業者・利用者によって提供・要望するセキュリティレベルが異なるため） • **データの所在地・国の把握** （所在地によってデータに適用される法律が違うため） • **マルチテナントの影響の把握** （他利用者のインシデントに対する、自身のリスクを把握するため） • **セキュリティ評価** （事業者選定のための指標となるため） • **デューデリジェンスの実施** （事業者の財務状況がリスクになる可能性があるため） • **再委託先の把握** （再委託により直接的な監視が困難になるため） • **SLAの締結** （利用者にサービス品質を保証するため） • **リスク評価の継続的実施** （運用開始後の継続的な見直しのため） • **委託事業者の監査** （委託した業務が適切なセキュリティ施策の下で実施されているか確認するため）

8．法制度及び電子情報の開示

ガイドライン骨子記載事項	• 環境クラウドサービスにおいて、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、環境クラウドサービスの提供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について記述する。

ガイドラインに記載すべき事項の要点（案）		
推奨要件の具体化、詳細化に当たっての考え方		**環境クラウドサービスにおいて、国外のクラウド上でデータが扱われる場合、その取り扱いに対してその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以下のとおり明確化。**
推奨要件	**モデル共通**	**• 監査権の確保** **（ 委託先のIT業務も内部統制を評価するため）** **• 個別要求事項の明確化** **（契約書に不足している要件を補うため）** **• 訴訟要求対応の明確化** **（訴訟発生時の対応を適切に行うため）** **• 適応法令の明確化** **（該当する法令を遵守するため）** **• データ開示リスクの明確化** **（海外の法律適用等により、データ開示を強制されるリスクがあるため）** **• 国外へのデータ移送・保存の明確化** **（海外の法律適用の可能性を確認するため）** **• 情報漏えい時の通知** **（個人情報取扱事業者に当たる場合の個人情報の保護に関する基本方針の遵守のため）**

9．コンプライアンス及び監査

ガイドライン骨子記載事項	• 環境クラウドサービスにおいて、セキュリティポリシーの遵守及びその監査プロセスがより複雑・困難になることから、利用者が認識すべきコンプライアンス・監査上の留意事項について記述する。

ガイドラインに記載すべき事項の要点（案）		
推奨要件の具体化、詳細化に当たっての考え方		**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施策が行われる。そのため、利用者はコンプライアンス維持のために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しなければならない。 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以下のとおり明確化。**
推奨要件	**モデル共通**	• **データの重要度に応じた分類** （データ種別によって求められるセキュリティレベルが異なるため） • **データ所在の確認** （データが取り決められた所在地のみで扱われているかを確認するため） • **認証の取得** （適切にセキュリティポリシーを遵守していることを証明するため） • **外部監査の活用** （第三者による客観的な監査の実施のため） • **認証範囲の適切性確認** （認証の評価項目は認証機関によって異なるため）

10. ID管理とアクセス管理

ガイドライン骨子記載事項	• 環境クラウドサービスの利用者やシステム構成要素の認証・認可、認証連携、アクセス制御に関して考慮すべき項目について記述する。

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			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以下のとおり明確化。
推奨要件	モデル共通		• 認証ログ取得による適切なアクセス管理の確認 （意図したようにアクセス管理が正常に働いているかの確認や、監査時に利用するため） • 強固なユーザ認証方式の提供 （なりすましのリスクが存在するため）
	モデル別	モデルA	• 多様なシステム間での認証連携 （既存のビル群管理システムからのシームレスなマイグレーションが求められるため）
		モデルB	• 汎用的な認証基盤の提供 （セキュリティポリシの異なる多様な事業者に対してサービスを提供する必要があるため） • WEB脆弱性に対する検証 （ユーザIDのなりすまし等が発生した場合であっても、システムに耐性があることを予め検証するため）
		モデルC	• 共通認証基盤の提供 （多数のアプリケーションとの連携を想定し、アプリケーションごとの認証負荷を軽減するため）

11．暗号化及び鍵管理

ガイドライン骨子記載事項	• 環境クラウドサービスの提供者と利用者は共にデータの損失・漏洩を防ぐ必要があり、データの暗号化及び鍵管理をそのための重要なメカニズムとして認識する必要がある。これらについて考慮すべき項目について記述する。

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			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竄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以下のとおり明確化。
推奨要件	モデル共通		• 通信の暗号化の確保 （データの機密性を確保するため） • 強固な暗号化方式の採用 （暗号化されたデータの解読を防ぐため） • 適切な鍵管理の実施 （正規の利用者のみがデータを利用できるようにするため）
	モデル別	モデルA	• 仮想化基盤内通信の安全性の確保 （クラウド上でビル施設に関する内部情報を扱うため）
		モデルB	
		モデルC	

12. インシデント対応

ガイドライン骨子記載事項	• 環境クラウドサービスにおいて、その複雑性やセンサーに起因する脆弱性によってセキュリティインシデントが引き起こされる可能性がある。また、情報収集システムと機器制御システムが連携する場合には、それぞれのシステムにおいて求められる通信品質が異なることに起因する脆弱性によってセキュリティインシデントが引き起こされる可能性があるため、その対応として考慮すべき項目について記述する。

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			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以下のとおり明確化。
推奨要件	モデル共通		• 統一的な監視 （仮想化環境も含め機器の監視対象が多岐にわたるため） • インシデント定義 （対応すべきインシデントを明確にし、迅速に対応するため） • 利用者のためのインシデント連絡窓口の確保 （インシデントの情報提供のため） • ログ取得 （インシデントを検知するため） • バックアップ （早急なインシデント復旧のため） • インシデント発生時の状態保存 （原因の特定及び再発の防止のため ） • 優先度を考慮したインシデントレスポンス （守るべき資産を把握し、被害を最小限に抑えるため）
	モデル別	モデルA	
		モデルB	
		モデルC	• 計測監視対象の稼働監視 （設置機器の故障・障害等を、クラウド上で速やかに検知するため）

13．データセンターの安全性確保、運用管理

ガイドライン骨子記載事項	• 特に、異なる事業者が提供する複数のデータセンターを活用する場合において、安全性確保及び運用管理に関して考慮すべき項目について記述する。

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			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は、データセンタ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以下のとおり明確化。
推奨要件	モデル共通		• データセンタに関する監査 （データセンターのセキュリティレベルを証明するため） • 環境クラウドサービス事業者のSLAの根拠 （ SLAの正確性を把握・証明するため） • データセンターの適正な運用管理区分 （運用担当者の責任を明確にするため） • データセンターのメンテナンスポリシーの設定・確認 （ ITシステムの脆弱性対応のため） • データセンターにおけるプロセス改善 （継続的なセキュリティレベルの維持・向上のため） • 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の確認 （利用者がサポートを受けるため）
	モデル別	モデルA	• 突発的な負荷上昇に対するサービス安定性の確保 （多種多様なセンサーネットワークやビル管理アプリを収容するため）
		モデルB	
		モデルC	

システム構築・運用に係る要件（３）環境負荷軽減効果の評価

１４．環境負荷軽減効果の可視化

ガイドライン骨子記載事項	• 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に示すことが重要であることから、環境負荷軽減効果を可視化する際に考慮すべき項目について記述する。

ガイドラインに記載すべき事項の要点（案）			
推奨要件の具体化、詳細化に当たっての考え方			環境クラウドサービスでは、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・管理に役立て、さらにはデータを公開することによってエネルギー効率活用などに貢献する。 こうした環境負荷軽減効果の可視化について事業者等が満たすことが推奨される要件を以下のとおり明確化。
推奨要件	モデル共通		• 計測ポイントの設定 （適切なデータ分析評価のため） • 評価指標の設定 （適切なデータ分析評価のため） • データ可視化方法の設定 （改善施策の検討や情報共有のため）
	モデル別	モデルA	• 分析評価手法と可視化方法の階層的分類 （ビル群管理のための分析を効率的に行うことが求められるため）
		モデルB	
		モデルC	

ガイドライン本文の記載例

13. データセンターの安全性確保、運用管理

－ 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に特徴的な留意事項）

環境クラウドサービス利用者のビジネス規模の拡大によって、必要とされるサーバやネットワークのリソースも増大していく。また日々の運用においても定期的なメンテナンス・環境負荷分析計算等により、バースト的な負荷が発生することも考慮されなければならない。環境クラウドサービスはまさにそのような条件に柔軟に対処できるクラウド基盤であるが、特に以下の点を考慮する必要がある。

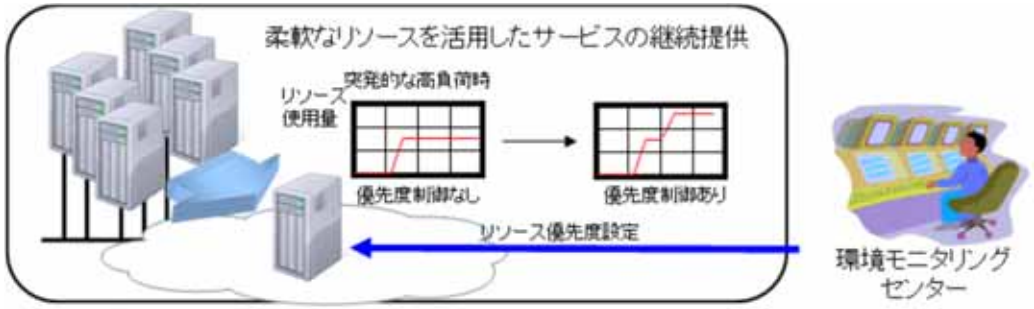
【アプリケーションレイヤー】

環境アプリケーション提供者は、自身が使用す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を確認することが望ましい。特にモデルAではセンサ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必要になるかもしれない。

【プラットフォームレイヤ、インフラレイヤ】

環境アプリケーション提供者はプラットフォーム提供者が提供するクラウド基盤のリソースについて、SLAで確認するだけでなく、リソース制御の仕組みについても把握していることが望ましい。特にモデルAではセンサ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てクラウド基盤を選定する必要があるかもしれない。

なお、コンピュータリソースの消費の変化に対する柔軟なリソース制御に関連して、以下のような実証例からもその有効性が明らかになっている。



優先度を使ったリソース制御のイメージ

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の上がる処理を行う場合、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。実証では優先度を使っ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することが可能となっている。

参考となるガイドライン等

- 環境クラウドサービスは、ビル、都市、地域における環境情報を、クラウドサービスを活用して収集・管理・制御し、環境アプリケーションを通じてサービス利用者に環境負荷軽減に資する情報を提供するものである。
- 本ガイドラインは、このような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、以下に示す、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。

団体	文書
CSA(Cloud Security Alliance)	Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
ENISA(European Network and Information Security Agency)	・Cloud Computing: Information Assurance Framework ・Cloud Computing: Benefits, risks and recommendations for information security
日本公認会計士協会	監査基準委員会報告第 18号
AICPA(American Institute of CPAs)	SAS70:Reports on the Processing of Transactions by Service Organizations

（参考情報）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（GW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（GW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（GW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）
- FIAP(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)