資料WG環6-2

環境クラウドサービスの実証実験の実施状況等
（モデルB：都市型施設エネルギー管理システム）

2011年2月24日

三井情報株式会社
www.mki.co.jp

目次案

１　実証実験の概要 ―― 2

２　調査結果 ―― 3
　２．１ エネルギー管理システムの現状 ―― 5
　２．２ クラウドサービスに関するセキュリティの現状 ―― 9

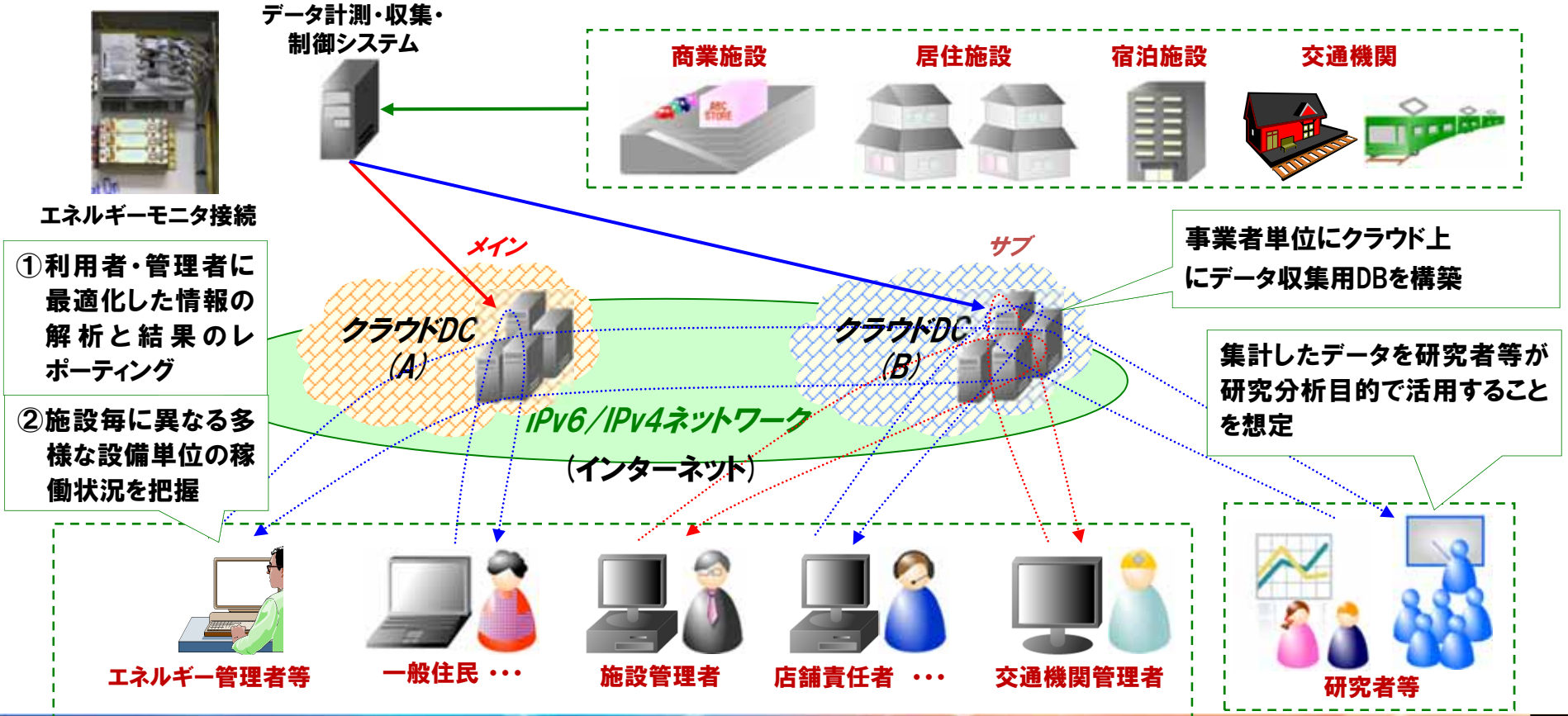
３　検証経過報告 ―― 10
　３．１ 想定するビジネスモデル ―― 12
　３．２ 検証項目と検証方法 ―― 13
　３．３ モデルBの特徴 ―― 15

４　参考資料 ―― 18
　４．１ 検証結果 ―― 19
　４．２ その他必要となる事項 ―― 28

三井情報株式会社
www.mki.co.jp

1、実証実験の概要について

実証実験の目的	多様な施設に対して、エネルギー管理サービスをネットワークを通じて提供 （多数の事業者/施設管理者にサービスを提供することを考慮したエネルギー管理）
関連するプレイヤー	民間企業、施設管理者、ビルオーナー、テナント、自治体、大学教授 等
対象エリア	主に広島市中心部の施設
対象施設	●商業施設　●宿泊施設　●居住施設　●交通機関



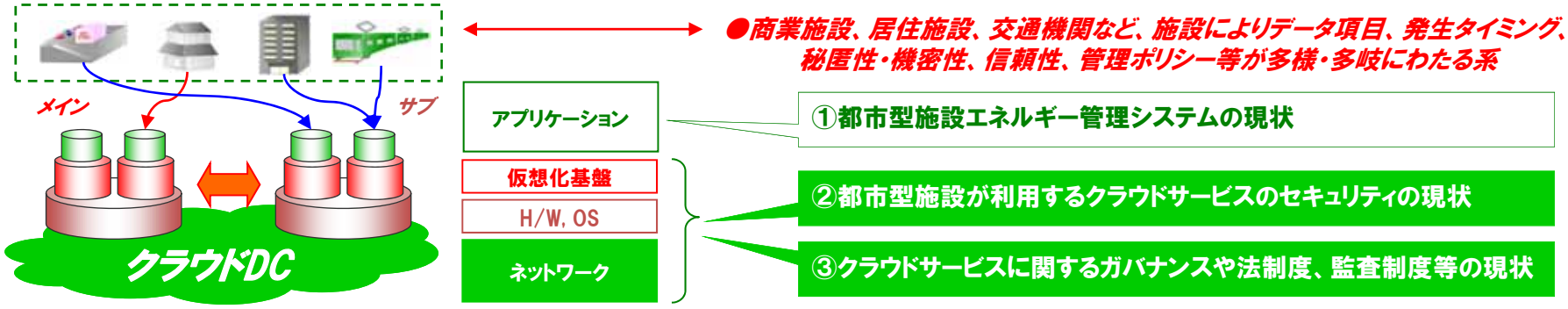
2. 調査結果

2. 都市型施設エネルギー管理システム等に関する現状調査

■ 都市型施設エネルギー管理システム等の現状について国内外の動向調査を実施する。調査の視点は下記の2項目となるが、調査により把握された内容を以降に整理する。

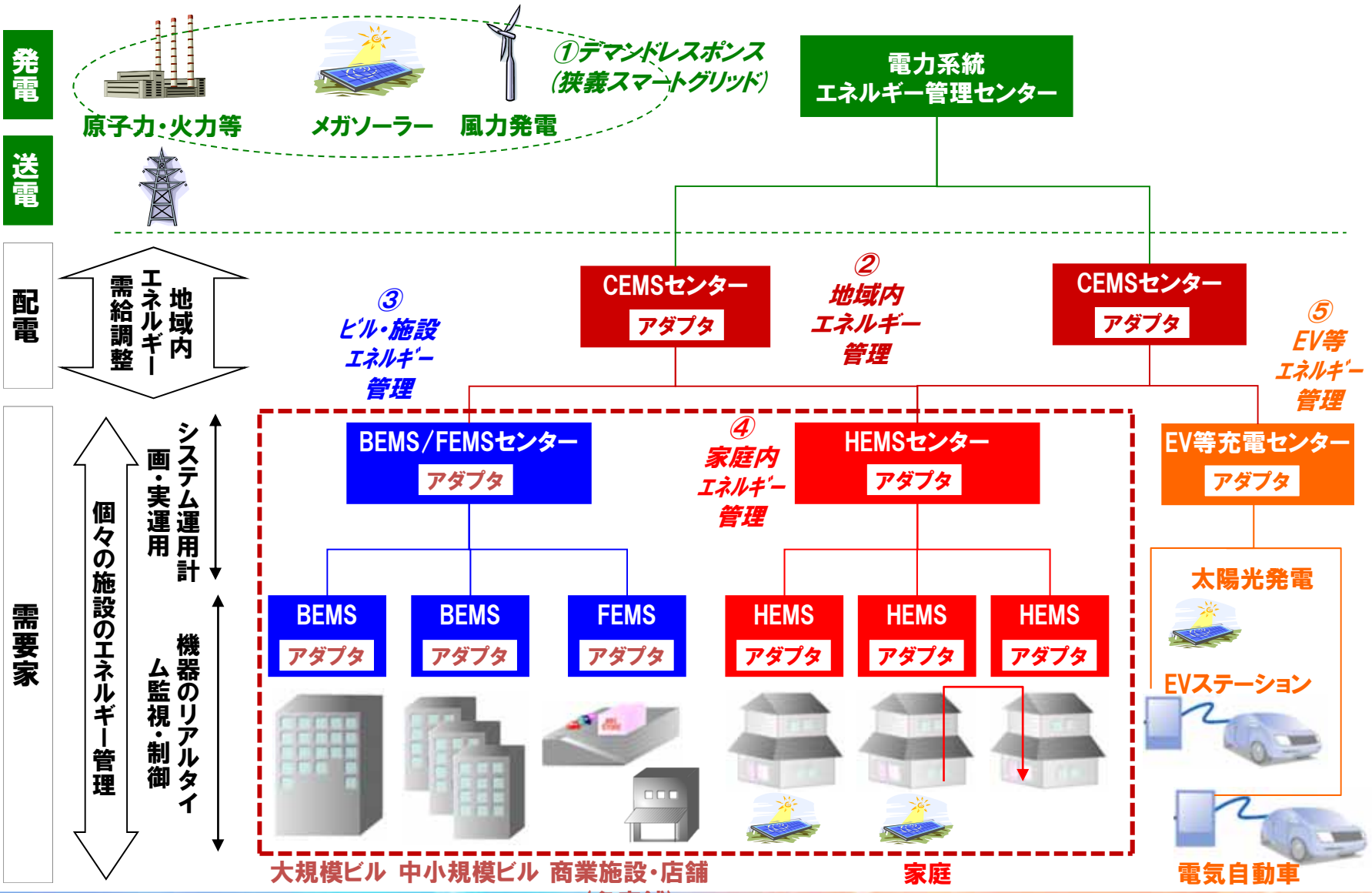
①商業施設、居住施設、交通機関等の施設を対象とするエネルギー管理システムの現状
［調査項目］ 都市型施設エネルギー管理システムの市場、技術・標準化、政策の動向及び関連事項

②商業施設、居住施設、交通機関等の施設が利用するクラウドサービスのセキュリティの現状
［調査項目］ クラウドサービスのセキュリティに関する市場、技術・標準化、政策の動向及び関連事項



2－1．エネルギー管理システムの現状

■ 都市型施設エネルギー管理システムは③及び④に該当する。



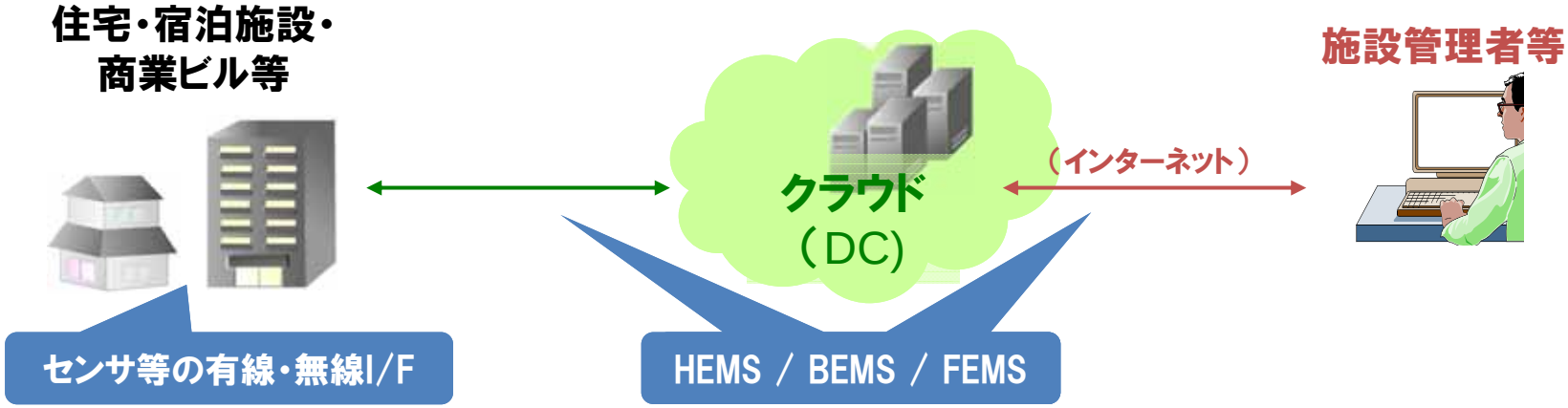
2－1. エネルギー管理システムの海外事例

■ 米国では、ECA（Enterprise Carbon Accounting）をキーワードに、以下に示すような領域のベンダーがクラウド環境を活用した炭素管理・エネルギー管理等のサービスを提供している。
■ 特に新興企業ではSaaS型サービスを提供しているケースが多く、ユーザインタフェースや多拠点の効率的管理を行う等の工夫を行っている。

ECA Software Vendor of Enterprise Carbon Accounting in each category			
EHS (Environmental, Health and Safety)	ERP (Enterprise Resource Planning)	Startups	Energy Management
Dakota Software Enablon* Enviance IHS ProcessMAP*	CA SAP* SAS	C3 Carbonetworks Hara* PE International* TRIRIGA Viewlocity*	Advantage IQ EnerNOC Johnson Controls* Pace* Summit Energy Verisae

主要ECAベンダー*	主な顧客
Enablon	ANZ, Bombardier, Centrica / Direct Energy, Woolworths
ProcessMAP	Allergan, Bunge Limited, CareFusion
SAP	Autodesk, Hitachi Consulting, University at Buffalo
Hara	Aerojet, Akamai, Brocade, City of Palo Alto, City of San Jose, Coca-Cola, News Corp
PE International	Carnival, Gerresheimer, Thyssen Krupp Elevators
Viewlocity	Avaya
Johnson Controls	Catholic Healthcare West
Pace	Bayer, Dresser-Rand, Kinross Gold, Sapa Extrusions, Savvis, Titanium Metals

2－1．エネルギー管理システムの技術・標準化動向



標準化テーマ	標準化機関	概要	備考
HEMS	IEC/TC100, IEC/SG4, IEEE, EIA	家庭を対象としたエネルギー管理システムの要素技術の規格として、ECHONET（ISO/IEC62480、ミドルウェアアダプタインタフェース：家電機器のアダプタのネットワークI/F仕様）、CEBus（EIA-600）、ISO/IEC1802（インターオペラビリティ標準ガイドライン）、ISO/IEC15054（ゲートウェイガイドライン）、ISO/IEC1567（エネルギーマネジメントモデル・スタンダード）等が公開されている。	
BEMS / FEMS	ISO/TC205, IEC/TC57, IEEE	IEC60870, BACnet/ANSI/ ISO16484, ANSI C12, OpenADR, AMI-SEC system BACnet ANSI ASHRAE 135-2008/ISO 16484-5 LonWorks ANSI/EIA709.1-B EN14908 ISO/IEC14908	
センサ等の有線・無線I/F	各フォーラム団体等	Zigbee（IEEE802.15.4）、WiFi、UPA、HD-PLC等のさまざまな有線・無線技術規格が提案されている。また、2009年、米国より、Zigbee、WiFi、FlexNet（AMIメータ通信規格）と互換性を実現するI/FとしてU-SNAPが提案された。	

2－1．エネルギー管理システムの政策動向及び関連事項

日米欧のエネルギー管理システムに係る主要な政策動向

- ■ 日米欧ともに、さまざまな方法で省エネルギー設備の導入・普及促進施策を実施。
- ■ 日本では、エネルギー設備の導入に係る補助金・助成金施策が比較的多いが、米国・欧州では、省エネルギー設備の導入投資コストに対する税制優遇施策が比較的多い。

		補助金・助成金	税制優遇	規制
	エネルギーマネジメント	省エネルギー設備等導入リース事業支援、温室効果ガス排出削減支援補助金、省エネルギー対策導入補助金	（・住宅エコポイント）	RPS法、非化石エネルギー法、エネルギー供給構造高度化法、改正省エネ法
	エネルギーマネジメント	省エネ技術等の導入助成	エネルギー優遇税制	連邦政府への再生可能エネルギーの導入義務、家電・照明の省エネ基準強化
	エネルギーマネジメント	家庭への断熱スキーム、省エネ・リフォーム補助金等	企業の省エネプロジェクト投資に無利子融資、省エネ家電・家具の買い替えへの税制優遇 、省エネ改築費用の長期低利子貸付・税制優遇　等	エネルギー効率指令、ErP指令

2－2. クラウドセキュリティに関する技術、政策及び関連事項

■ クラウドサービスの普及促進を支援するための活動（ベストプラクティス、標準化等）が行われている。

海外事例
●Open Cloud Manifesto【宣言文】 • IBM、Cisco、SAP、EMC、AT&T、Red Hat、VMware 等250社以上が参加、クラウド間のオープン化、互換性確立を盛り込んだ6原則の宣言文を公開。 ●Cloud Security Alliance（CSA）【ベストプラクティス】 • eBay、PGP、Qualysなどの企業が2009年3月に設立、クラウドおけるセキュリティのベスト・プラクティスの普及促進を目指す。 ●ENISA – Securing Europe's Information Society • “欧州ネットワーク情報セキュリティ庁”は、ユーザー・電子政府の観点でクラウドコンピューティングのリスクアセスメントを実施。
●Open Cloud Consortium（OCC）【標準化】 • 大学中心、Cisco、Yahooなどが参加、クラウド同士をつなぐ枠組みの策定、ベンチマーク策定を行う。 ●Distributed management task force（DMTF）【標準化】 • オープンなクラウドリソース管理についてOpen Cloud Standards Incubator を創設。 ●Open Grid Forum（OGF）【標準化】 • クラウド間のオープンなAPI提供を目的にWGを創設（OCCI）

3. 検証経過報告

3. 検証シナリオ

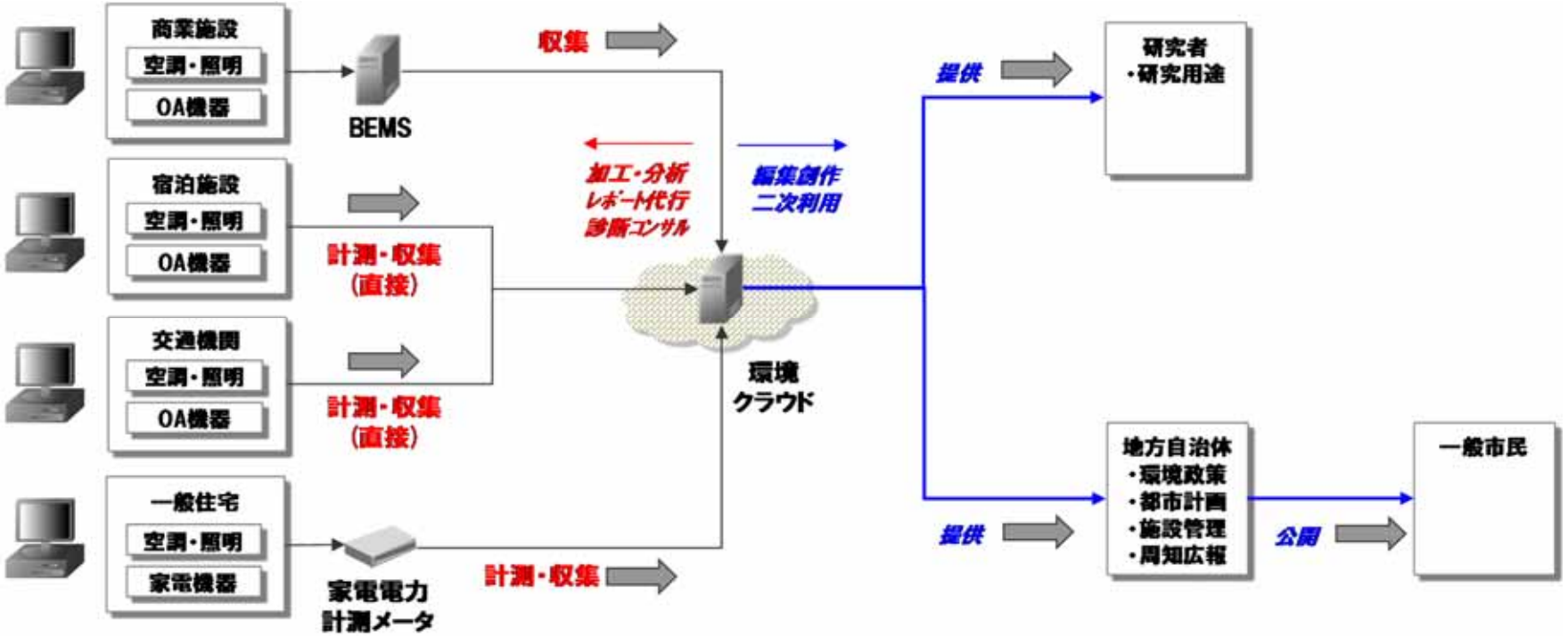
本実証実験では、実証実験を通じて、以下にあげるネットワーク要件について検証を行い、各項目において求められるセキュリティ要件、留意すべき事項等について取りまとめを行う。

（1）セキュリティを意識した拡張性の確保	（2）情報セキュリティの確保
(a) 移植性及び相互運用性 アプリの移植性確保のための要件、方策、注意点、課題等	(a) ID管理とアクセス管理 センサー等非人間的要素も加味した認証・認可管理等
(b) 事業継続性 障害時や災害時の対応の要件、方策、注意点、課題等	(b) 暗号化及び鍵管理 センサーネットワークを前提とした暗号化、鍵管理の方策等
(c) 情報管理 情報ライフサイクル各段階でのセキュリティ要件等	(c) インシデント対応 環境クラウドアーキテクチャに特有のインシデントへの対応
(d) 仮想化 仮想化によって新たに生じる攻撃可能性への対応等	(d) データセンターの安全性確保、運用管理 異なるサービスを組み合わせた際の運用安定性の確保等
(e) アプリケーションの開発・運用管理 共通基盤に影響する各種規約、仕様等への対応等	(e) 責任分界点の設定 異なるサービス間での有効な責任分解点の定義方策等
	(f) ガバナンス及びエンタープライズリスクマネジメント クラウド特有のセキュリティガバナンス、リスク管理等
	(g) 法制度及び電子情報の開示 IT関連の法制度や基準への対応可能度、限界の評価等
	(h) コンプライアンス及び監査 クラウドにおける監査の実現方法、限界の評価等

3－1．想定するビジネスモデル

◆想定ビジネスモデルを仮説し、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」を実証

仮説	【ビジネスモデル（仮説）】 都市部における多様な施設・事業者を対象として、データ集計／分析による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
	単一企業の省エネ努力では、CO2削減目標の達成は困難と想定し、ユーザー合意のもと取得した地域特性の高い消費エネルギーデータを研究者や地方自治体向けに提供することでフィードバック効果を得ることも想定。



3－2. 検証項目と検証方法

	特徴点	想定される要件	検証方法
移植性及び相互運用性	事業者が利用するサービスを変更したり、自社システムへ移行したりするケースが増加する可能性がある。	事業者による柔軟なサービスの移行を想定した、汎用性の高い移行手法について検証を行う。	取得情報をWEBサービス経由でユーザーが利用しやすいAPIの在り方を検証。
事業継続性	施設の機器制御を必要とするサービスでは、ネットワーク環境によらずサービスの継続性が求められるケースが想定される。	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う。 複数DCを利用した場合の可用性の検証を行う。	エージェント型制御の在り方を検討し、通信障害時でも適切な制御を実現する仕組みについて検証。 アプリケーションレベルでレプリケーション機能を実装し、システム可用性の向上について検証。
情報管理	管理事業者が異なる複数の施設から情報を収集・管理し、許諾に基づいて収集情報の二次利用を行う。	収集情報の二次利用において、許諾に基く適切な情報の加工・編集が求められ、その取り決めについて検証を行う。	実験参加者へのヒアリングを通じ合意形成の在り方について検討。 プライバシー加工された分析用DBの在り方について検証。
仮想化	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可能性がある。	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ついて検証を行う。	シミュレーション環境を用意しサイジングについて検証。 疑似攻撃シュミ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。
アプリケーションの開発・運用管理	クラウド上で管理する情報をサービスを利用する事業者や二次利用情報を活用する主体が取得、加工、分析する。	サービスを利用する事業者の一次利用や研究用途等の二次利用を想定した、標準的なAPI提供手法の在り方及び耐脆弱性について検証を行う。	ダウンロード用WEB APIを実装し、利用可能性について検証。 代表的な不正アクセス攻撃（例：XSSやSQLインクジェクション等）に対するシステムの耐性について検証。

3－2. 検証項目と検証方法

	特徴点	想定される要件	検証方法
ID管理と アクセス管理	セキュリティポリシの異なる事業者に対応し、適切な認証方式の在り方が重要。	セキュリティポリシーの異なる事業者へのサービス提供を想定した、認証基盤の在り方について検証を行う。	端末インストールが不要な認証基盤を構築し、導入可能性を検証。認証基盤からログを取得し、アクセスログの監査ができることを検証。
暗号化及び 鍵管理	事業サイト・クラウド間、DC間で授受される事業者保有情報について安全に取り扱うことが重要。	多様な通信手段でのアクセス、DC間のデータ同期等を想定した、クラウドにおける適切な暗号化・鍵管理及びセキュアなDC間通信について検証を行う。	シミュレーション環境を用意し、環境アプリケーションの脆弱性について検証。 盗聴及び改竄の疑似攻撃に対し、通信の安全性について検証。
インシデント対応	契約に基づいて合意されたインシデント対応を尊守した、システム、体制の構築が重要。	システム稼働状況を監視し、障害発生時に必要な連絡・復旧を行える体制について検証を行う。	管理サーバーを実装し、パフォーマンス/リソース使用状況の監視の在り方を検証。 障害時の通知機能を実装し、同システムの有効性について検証。
その他	複数の施設及び拠点に設置された機器の故障を想定し、遠隔から効率的に監視できることが重要。	多様な施設に設置された機器の故障・異常の発生を検出できる仕組みについて検証を行う。	疑似的に発生させた故障情報の検知可能性について検証。

3－3. モデルBの特徴　-ユーザーの増加に伴うスケールアウト性能-

事業者増加ケースを予め想定した環境の構築

取得情報の管理については、十分な情報セキュリティを求められたため、環境クラウド上に、サービスを事業者毎に構築し運用が求められると想定した。事業者増加時を予め想定したクラウド環境のサイジングが重要と想定。

仮想化

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立ち上げ、CPU/ネットワーク/ディスク等の負荷を検証。	スケールアウトの性能評価及び悪性データの混入に関して問題ないことが確認できた。

ID/アクセス管理

共通認証基盤におけるセキュリティ評価を実施し、アクセス制御の迂回可能性や認証機能の悪用可能性を検証。	Cookieを利用した認証方式に関しては、アクセス制御並びに認証機能の悪性用に関しても問題ないことを確認。サービス利用者からも認証基盤に関する特筆すべき指摘は無かった。

ID/アクセス管理

Cookieを活用した共通認証基盤を開発し、サービス利用者が共通利用できる仕組みを配布し有効性を検証。	クライアントにモジュールを導入する方式は、導入しずらい企業もあり、また企業の個別ネットワークと認証連携することはコスト要因になるという意見が出た。

検証項目と求められる要件

① 仮想化：サービス利用者増加に対するアプリケーションのスケールアウトを予め検討しておくこと
② IDおよびアクセス管理：環境クラウドサービス利用者共通の認証基盤を考慮すること
　　ユーザーIDのなりすまし等WEBの脆弱性に対する評価を予め実施すること

3－3．モデルBの特徴　-インターネット回線によるサービス提供-

安価な回線を利用した場合の事業継続性の確保

複数の事業者及び施設が対象となるため、専用線等の利用が難しく、安価なインターネット及び携帯網を利用したケースにおけるビジネス面での事業継続性が重要になると想定

事業継続性	環境クラウドとゲートウェイ間の通信が遮断された場合でも安定した制御が行える仕組みを開発し検証。	既存インフラを活用できるケースは少なく、そのため、信頼性の低いインターネット回線の利用を余儀なくされた。そのため、信頼性の低い回線の中でも安定した制御が求められた。
事業継続性	ゲートウェイは、コモディティのハードを利用しオープン性を確保。サービス事業者からのリモートメンテナンスを検証。	施設管理者から、ゲートウェイの構成に関しては、詳細な説明が求められ、設置することで既存設備に影響がでないかの技術的検証が求められた。
事業継続性	サービス利用者の設備機器等が更新されたケースを想定し、データ取得の継続性に関する機能を開発し検証。	計測対象によっては、定期的に設備更新等があるケースもあり、都度メンテナンスする必要のない構成が求められた。

検証項目と求められる要件

① 事業継続性：信頼性の低い回線を使うことを前提としたうえで、適切な制御が実施されること
ゲートウェイ等の機器についてはコモディティなハードウェアを採用し、オープン性を担保すること
設備更新を視野に入れたサステナビリティを担保すること

3－3. モデルBの特徴　-データの2次利用-

想定するデータ利用モデル（BtoBモデルとして）

個別企業の省エネ努力では、CO2削減には限界がある為、ユーザー合意のもと取得した地域特性の高い消費エネルギーデータを地域の環境負荷軽減を目的に、研究者等に分析用データとして提供することが特徴。

情報管理 分析用DB利用者に対して、情報の取り扱いに関する運用マニュアル案を提示し、運用時の課題について整理。	利用期間の明確化、データの出所の明記、情報提供者の不利益を生じさせない加工について、サービス事業者と分析用DB利用者間で事前に協議・合意することが必要との意見が出た。
移植性及び相互運用性 データダウンロード用のAPIを開発し、サービス利用者や分析用DB利用者に提供。	API利用者は必ずしも、ITリテラシーの高い人材になるとは限らない為、極力プログラムレスのデータ取得方法があると良いという意見が出た。
ガバナンス及びエンタープライズリスクマネージメント 取得データの2次利用の可能性に関し、サービス利用者にヒアリング調査を実施し課題点を整理。	環境エネルギーデータより企業活動が推測される可能性があるため、情報提供のタイミングについては予め合意が必要との意見が出た。

検証項目と求められる要件

① 情報管理：分析用のデータに関しては、予め利用目的をサービス事業者と分析用DB利用者間で合意しておくこと。
② 責任分解点：サービス事業者から分析用DB利用者へデータ移行がされた時点で適切な管理責任は移行すること合意すること
③ ガバナンス及びエンタープライズリスクマネジメント：企業活動が推測される可能性もあるため、開示タイミングについて合意すること

4. ご参考資料

4－1. 検証結果①（移植性及び相互運用性）

想定される要件

ユーザー企業が、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。

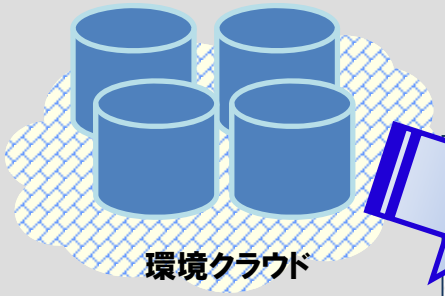
ユーザーによる柔軟なサービス移行を想定した汎用性の高い移行方法について検証を行う。

検証方法

取得情報をWEBサービス経由で**ユーザーが利用しやすいAPI**を実装し、実証実験関係者に配布することでその在り方を検証した。

実証実験の内容及び仮説

データ加工を希望する事業者に対して、WEBサービスを公開し、データの加工ができる環境を提供。



ユーザー向けWEB API

実証実験の結果

実証実験において下記の対応を実施した。

・データダウンロードツールをSOAP手順にて開発し、サービス利用者及び分析用DB利用者に配布し、利便性を検証。
・汎用性の高いOSであるLinuxを用いてシステムを実装し、本番用のクラウド環境から、別環境のシミュレーション環境への移植を実施し、利便性を検証。

実証実験を行う中で、以下の留意事項が明らかとなった。

・サービス利用者は、ITリテラシーの高い人材とは限らない為、極力プログラムレスの機能を求められた。
・仮想化されたイメージをどのようなタイミングでバックアップをするか等に関してはSLA等で明記する必要があると考える。

4－1. 検証結果②（事業継続性）

想定される要件

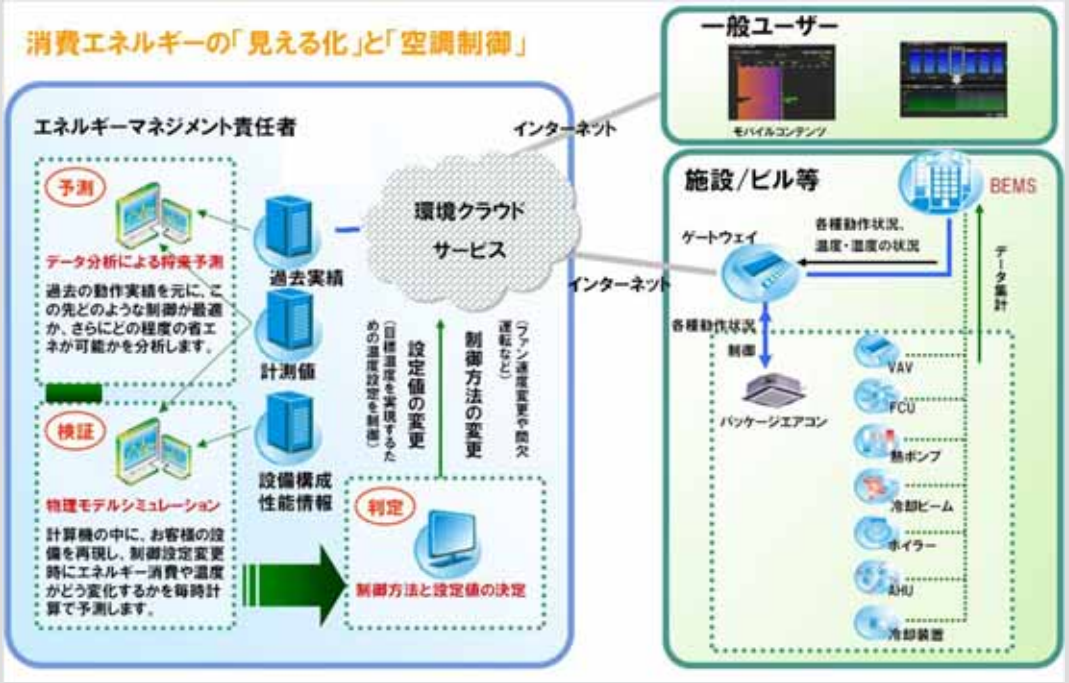
施設の機器制御を必要とするサービスでは、**ネットワーク状況によらずサービス継続性の確保**が求められることを想定する必要がある。

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う。

検証方法

ゲートウェイ型の制御クライアントを実装し、ネットワーク障害が発生した場合でも適切な制御を行えることを検証した。

実証実験の内容及び仮説



実証実験の結果

実証実験において下記の対応を実施した。

- 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。
- ゲートウェイについては、コモディティのハードウェアを利用し、オープン性と汎用性を担保した。

実証実験を行う中で、以下の留意事項が明らかとなった。

- ゲートウェイを設置する場合、設置場所によっては、既存の有線ネットワークが利用できないケースがある。そのため、有線と無線を両方考慮したネットワーク構成を予め検討する必要がある。
- ゲートウェイ等、施設側に新たに設置する場合、施設管理者等から説明を求められるため予め資料を準備することが望ましい。

4－1. 検証結果③（情報管理）

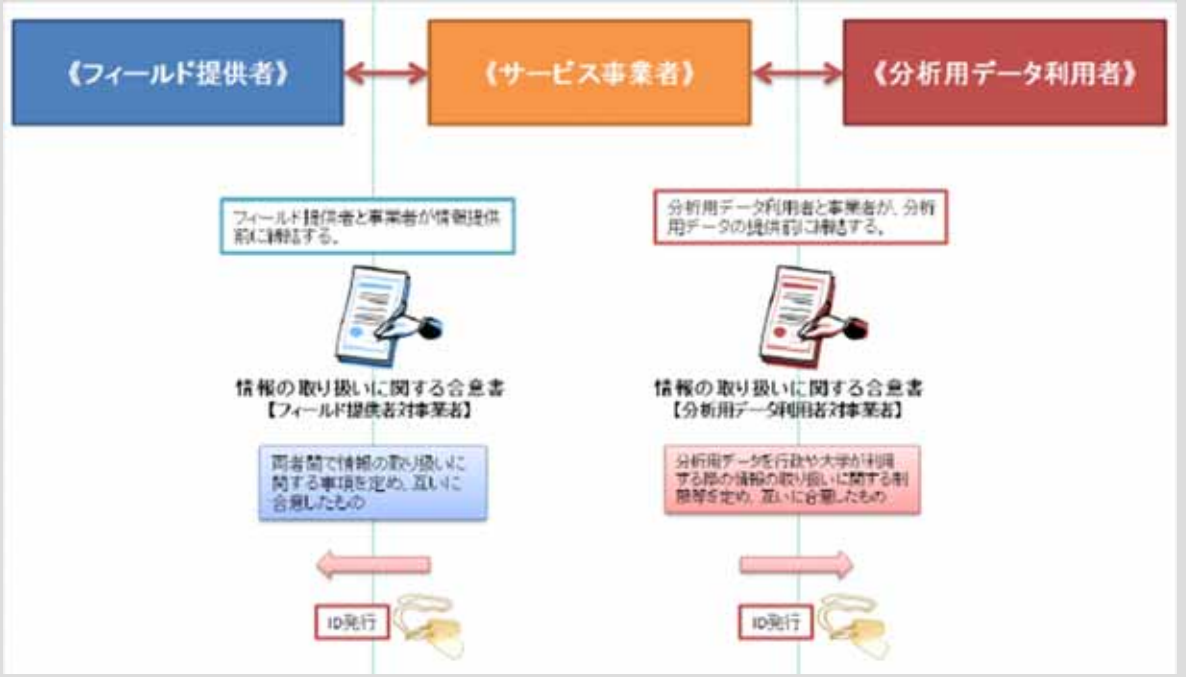
想定される要件

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、**都市レベルでの環境負荷軽減を目的とした研究目的での分析用DB**の提供を想定する必要がある。
この場合、**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、検証を行う。

検証方法

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。
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DB**構築の在り方を検討した。

実証実験の内容及び仮説



実証実験の結果

実証実験において下記の対応を実施した。

・サービス利用者及び分析用DB利用者に対し、情報取り扱いガイドライン（案）を配布し、情報管理における留意事項をヒアリング調査を実施した。

実証実験を行う中で、以下の留意事項が明らかとなった。

・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予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、予め提供の合意、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. 検証結果④（仮想化）

想定される要件

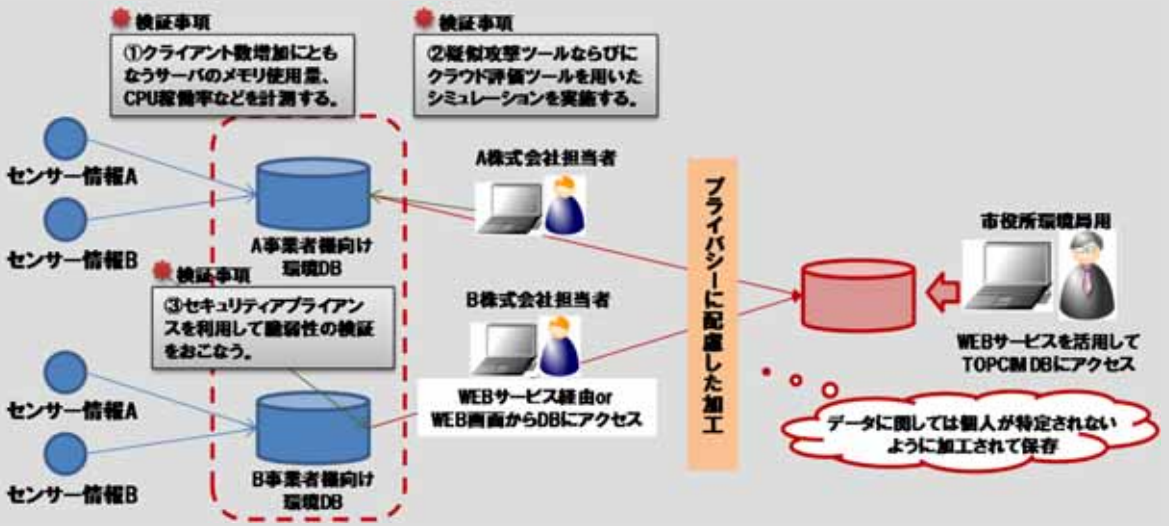
サービスの普及に伴い、対象となる都市内の施設を管理するサービス利用事業者が増加（＝事業者単位DB）を想定したシステムを構築する必要がある。
この際、①事業者DBの増加を想定したスケールアウト（可用性）、②外部からの不正アクセス及び不正アクセスの検知（脆弱性）、③制御を想定したアプリケーションの脆弱性（脆弱性）について検証を行う。

検証方法

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。
疑似攻撃シュミ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。

実証実験の内容及び仮説

クラウド上に事業者単位でサービスを構築し、協力事業者にシステム構成の説明と同意を得て運用を実施した、



実証実験の結果

実証実験において下記の対応を実施した。
- データ保全の安全性を考慮し、サービス利用者単位（＝法人単位）でアプリケーションを構築/運用を実施。
- 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台からランダムに負荷をシステム耐性の検証を行った。

実証実験を行う中で、以下の留意事項が明らかとなった。
- サービス利用者より環境クラウドのシステム構成（特にデータ保持方法）の説明を求められた。
- アプリケーションのスケールアウト方法に関しては予め想定したサイジングの実施が重要と想定される。

4－1．検証結果⑤（アプリケーションの開発・運用管理）

想定される要件

サービス利用事業者が社内情報発信目的でのデータ利用や、研究用途での分析用DBへのアクセス、ダウンロード、データの加工等のニーズを予め想定する必要がある。
WEBサービス等標準的手法を用いたデータのダウンロード機能が求められるため、その手法について検証する。また、WEBサービス提供時の耐脆弱性について検証を行う。

検証方法

データダウンロード用WEBサービスの機能を実証しユーザーへ配布し有効性を確認した。
また、XSSやSQLインクジェクション等、プラットフォームに対する代表的な攻撃に対するシステムの耐性を検証した。

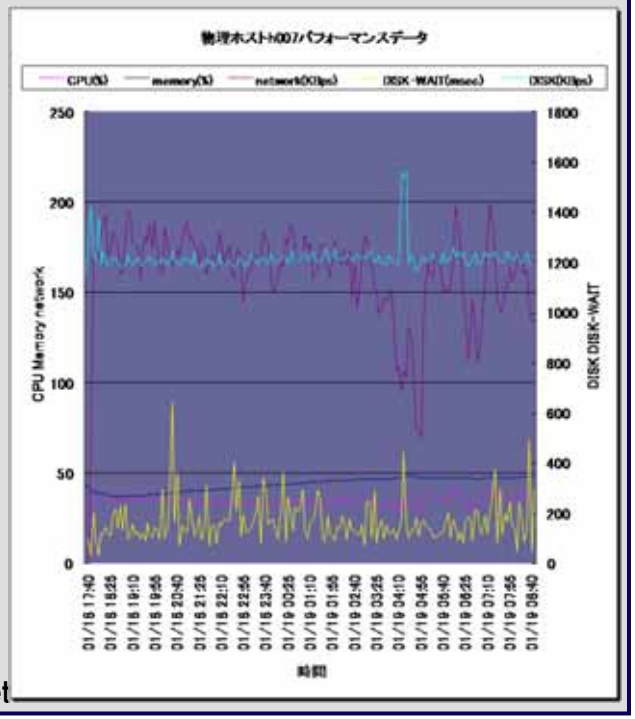
実証実験の内容及び仮説

100台のサーバに対し100台のクライアントからランダムにサーバを選択し連続でアクセスを行う。

【結果】
DISK性能以外はやや余裕あり。

・CPU使用率は30%台で推移
・メモリ使用率は約47%に収束
・NWは帯域の約0.1%を使用
・DISKの転送量は最大性能の約0.8%使用
・DISK待ち時間が長く、最大で600msecを記録しており、大きなオーバーヘッドと考えられる。
・サーバダウンなどはなし。

【ハードウェアスペック】
HP DL320 G5（2006/11モデル）CPU:
QuadCore Xeon X3350 2.66GHz
Memory:8GB HDD:SATA160GB
MAX150MBps 7200rpm NIC:Gigabit Ethernet



実証実験の結果

実証実験において下記の対応を実施した。
・WEBサービスを活用した（プロトコルはSOAP）データダウンロードAPIを開発し、有効性の検証。
・データダウンロードツール等の開発により環境クラウドアプリケーションに、多数のユーザーがアクセスすることを想定し、応答時間等のパフォーマンスについてシュミレーションを実施。

実証実験を行う中で、以下の留意事項が明らかとなった。
・データの検索等については特に問題となる負荷はみられなかった。ただし、データを統計処理して取り出すケースでは負荷が高くなるケースもあり、アプリケーション特性に応じて負荷分散する等考慮が必要になると思われる。

4－1．検証結果⑥（ID管理とアクセス管理）

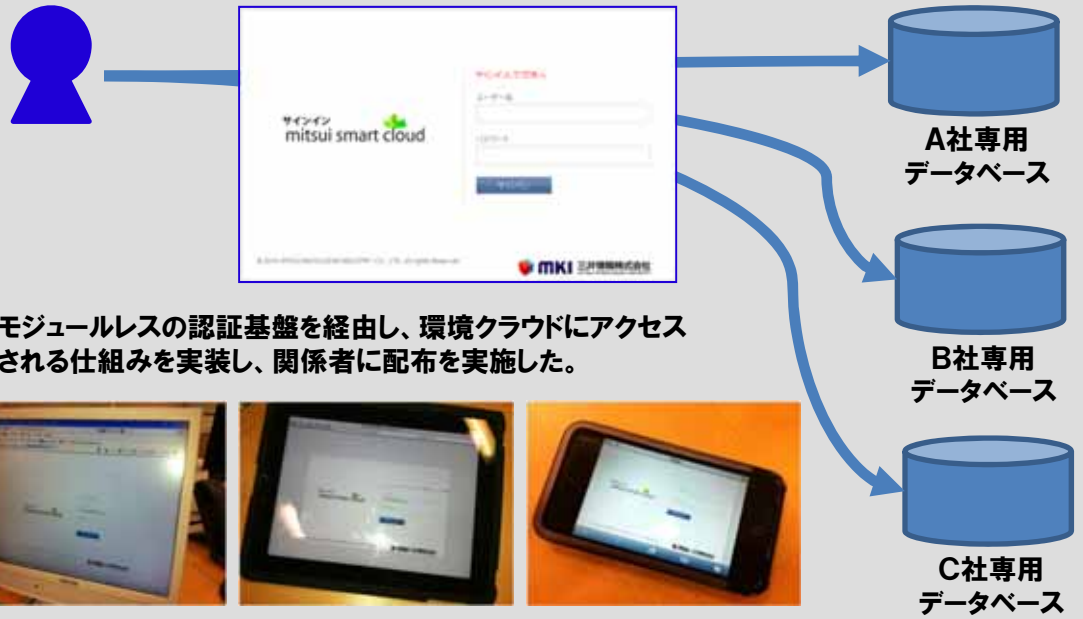
想定される要件

複数事業者が共同利用する場合、事業者毎に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。
異なる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う。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う。

検証方法

端末インストールが不要な認証基盤を構築し、導入可能性を検証した。
また、認証基盤からログを取得し、アクセスログの監査ができることを検証した。

実証実験の内容及び仮説



モジュールレスの認証基盤を経由し、環境クラウドにアクセスされる仕組みを実装し、関係者に配布を実施した。

PC、iPad、iPhone等のマルチデバイスに対応した認証基盤

実証実験の結果

実証実験において下記の対応を実施した。

- Cookieを活用した共通認証基盤を開発し、サービス利用者に提供。認証基盤については、サービス利用者の要望もありPCだけではなく、iPhone/Android/iPad等のマルチデバイスに対応。

実証実験を行う中で、以下の留意事項が明らかとなった。

- 認証基盤を利用する場合にクライアントモジュールをクライアントPCに導入することが必須の場合、導入しずらいケースもあるとの意見が出た。
- 企業ネットワークと認証連携（LDAP等）については、コストメリットとの比較になるが、既存システム等の変更が必要なケースでは個別対応をすることは難しいのではという意見が出た。

4－1. 検証結果⑦（暗号化及び鍵管理）

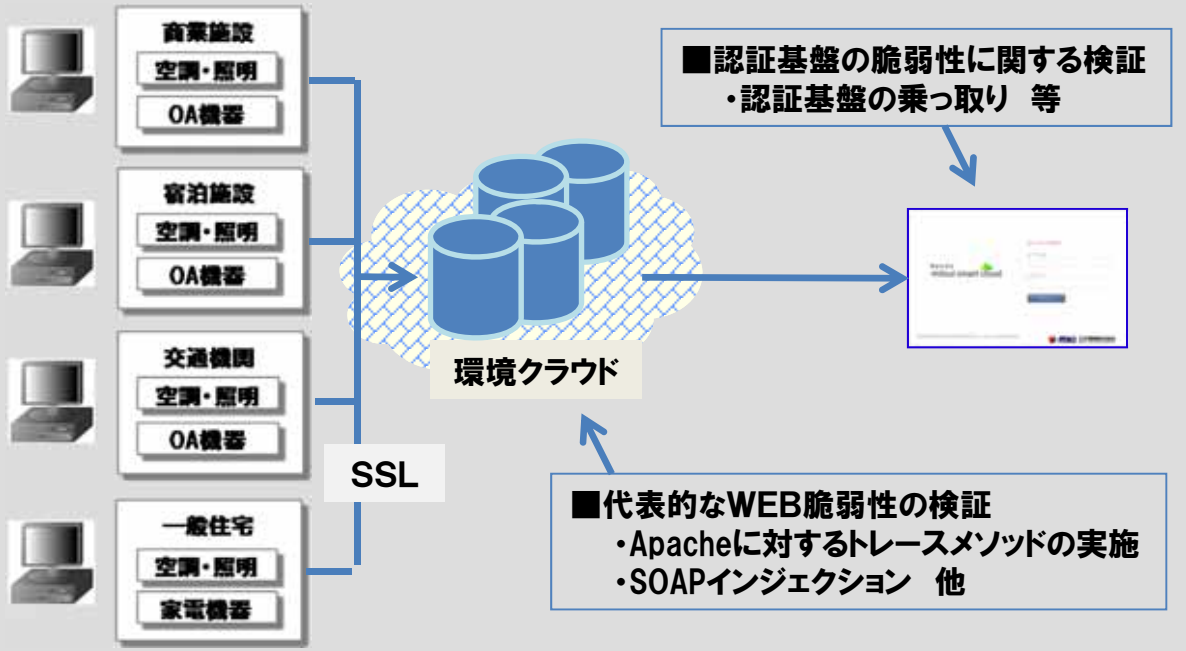
想定される要件

多様な利用者が**様々な通信手段**を介してシステムを利用することを想定する必要がある。
クラウド⇔サービス利用事業者間の**通信の安全性の確保**及びクラウドにおける適切なデータ暗号化と鍵管理について検証を行う。

検証方法

アプリケーションへのアクセスを対象としたWEBアプリの脆弱性に関するシミュレーションを実施した。
通信対する盗聴及び改竄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。
HTTPSで使用されるSSLサーバー証明書を認証ゲートウェイのサーバ内に保存する構成で実装し、その有効性を検証した。

実証実験の内容及び仮説



実証実験の結果

実証実験において下記の対応を実施した。

- ゲートウェイ、環境クラウド間の通信に関してSSL通信を実施。
- ゲートウェイについては、ID/パスワードで認証管理を実現。
- 環境クラウドアプリケーションに対して、代表的なWEB脆弱性の検証を行い、安全性を確認。
- 認証基盤に関して、ID/パスワードのなりすまし等の脆弱性を確認するための検証を行い安全性を確認した。

実証実験を行う中で、以下の留意事項が明らかとなった。

- 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に対する攻撃が脅威となるため、十分な対策が必要となる。

4－1. 検証結果⑧（インシデント対応）

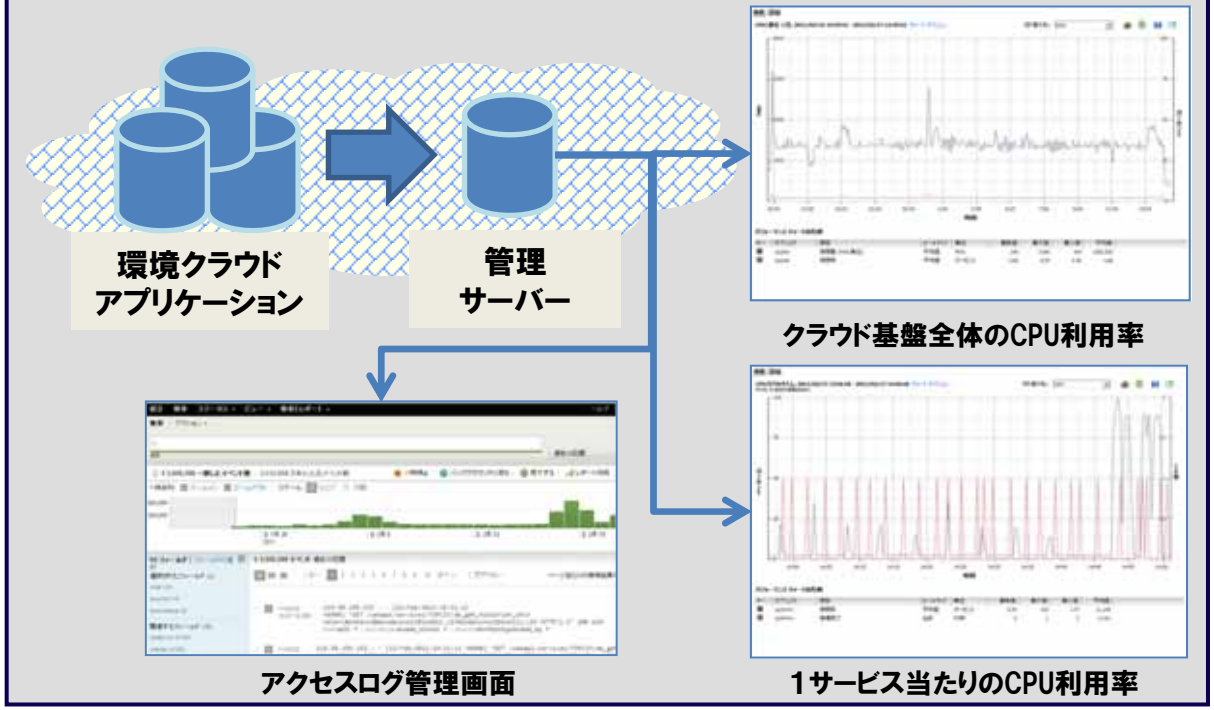
想定される要件

法人対法人の契約によって提供されるサービスであり、契約に基づいてSLA、インシデント対応等が明文化されることになると想定されるため、それを尊守する必要がある。
予め**定めたSLA等に基づきシステムの稼働状況を監視**し、障害発生時に必要な連絡を行うと同時に復旧を行える体制が必要となる。そのような体制の在り方を検証する。

検証方法

管理サーバーを実装し、パフォーマンス/リソース使用状況の監視を実施し、障害時にはSNMP TRAPやメールで通知を行える機能を実装した。これに対して、人為的なインシデントを発生させ、これらのシステムの有効性を検証した。

実証実験の内容及び仮説



実証実験の結果

実証実験において下記の対応を実施した。
- 環境クラウド上に、管理用サーバーを構築し、CPU・ネットワーク・メモリ・ディスク等のインシデント管理を実施。
- 認証基盤にアクセスログ管理機能を実装し、アクセス元のIPアドレス（IPv6,IPv4）、ログインユーザー、アクセス日時、アクセス先URL等をアクセス毎に取得

実証実験を行う中で、以下の留意事項が明らかとなった。
- 特筆すべき留意事項は見当たらなかった。一般的な技術を採用すれば十分対応可能と思われる。

4－1. 検証結果⑨（その他）

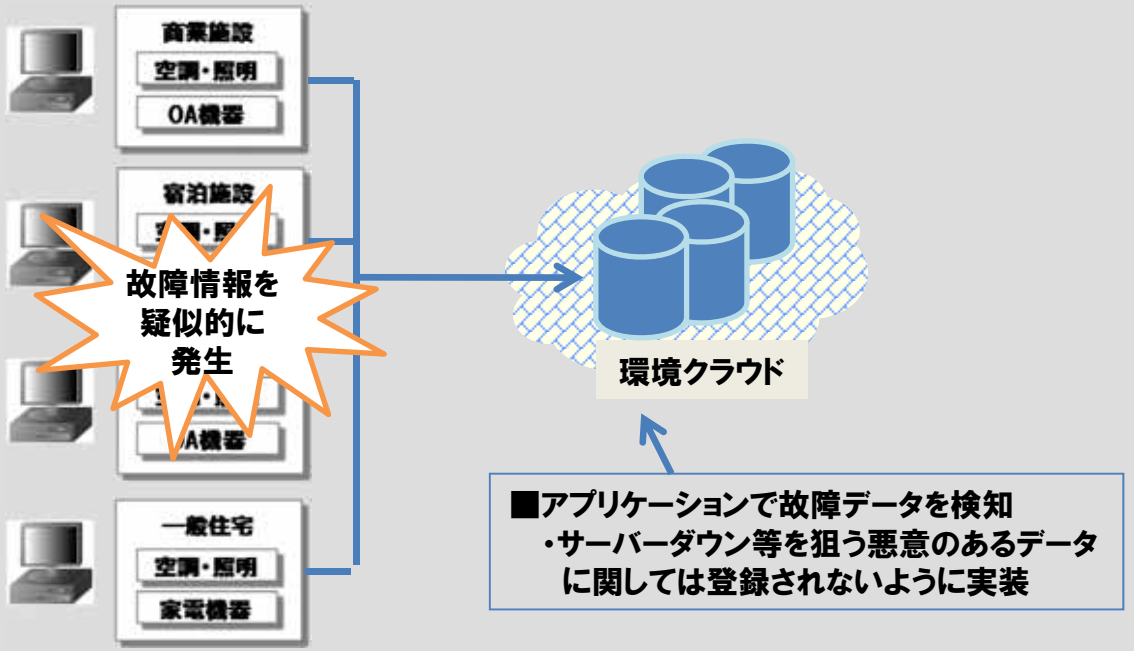
想定される要件

施設内に設置した機器が経年劣化等により故障することが想定した機器監視を行う必要がある。
施設内**計測機器の故障**発生を**検出**できる仕組みについて検証を行う。

検証方法

故障情報を疑似的に発生させ、それを検知できることを検証した。

実証実験の内容及び仮説



実証実験の結果

実証実験において下記の対応を実施した。
・シミュレーション環境上で、疑似的に故障データを発生させ、環境クラウド側で検知可能か検証を実施

実証実験を行う中で、以下の留意事項が明らかとなった。
・設備機器ごとのIDがすべて複製され、数字だけが異なるケースは、システムで回避することは難しい。
制御等を実施するケースでは、平均値から明らかにずれるデータに関しては分析から外す等の考慮が必要と思われる。

4－2. その他必要となる事項 ①（責任分界点）

明確にすべき事項	環境クラウドサービスのアーキテクチャフレームワークとして、環境クラウドサービス事業者、アプリケーション事業者、サービスに係る情報の提供者、サービス利用者など多様なプレイヤー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を整理する。
調査結果の整理	実証実験において下記の対応を実施した。 ・分析用データの取扱いに関して、分析用DB利用者に対してヒアリング調査を実施した。 実証実験を行う中で、以下の留意事項が明らかとなった。 ・分析用DBの再配布等に関しては、すべてをサービス事業者が管理することは難しいため、予め分析用DB利用者に対して利用範囲を明確化した、契約条項／利用規約を定めておくことが望ましいという意見がでた。 ・データを閲覧だけではなく、ダウンロードして分析用DB利用者が保有するケースでは、データをダウンロードした時点で、管理責任がサービス事業者から分析用DB利用者に移行する等、予め決めておく必要があるのではという意見がでた。

4－2. その他必要となる事項 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）

明確にすべき事項	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、クラウド事業者、及びデータセンター事業者が相互に連携してサービスを提供することになる。この際、エンタープライズリスクに対応するに対応し、サービスの提供が相互に依存せず継続可能な仕組みの在り方について整理する。
調査結果の整理	**実証実験において下記の対応を実施した。** ・今回の実証実験において利用したデータセンターに関しては、MKIがハウジング契約を締結し利用している。そのため、アプリケーション、プラットフォーム、データセンターの管理責任はすべて1社で実施している。 **実証実験を行う中で、以下の留意事項が明らかとなった。** ・ サービス利用者が増えた場合やサービス利用者の管理データ数が増えた場合、連携アプリケーションが増えた場合等は、アプリケーション側の変更だけではなく、インフラ側の変更も必要になる。こういったケースも予め考慮し、事業者がわかれる場合は役割分担を明文化しておく必要があると思われる。 ・ データ開示のタイミングについて、エネルギーデータより企業活動が推測される可能性を考慮してほしいという意見が出た。ホテル等の場合、他ホテルでの運転状況と比較しつつ、価格を決定する等の商習慣があり、そのためリアルタイム開示については難しいという意見がでた。

4－2. その他必要となる事項 ③（法制度及び電子情報の開示）

明確にすべき事項	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。そのため、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や開示すべき項目を整理する必要がある。
調査結果の整理	**実証実験において下記の対応を実施した。** 情報保管並びに警察等第3者への開示について、サービス利用者、分析用DB利用者へヒアリング調査を実施した。 **実証実験を行う中で、以下の留意事項が明らかとなった。** ・情報の保管に関しては、データセンターの位置により、関連法令がことなる可能性を考慮し、どこに保管されるのか明示してほしいという意見がでた。 ・警察からの捜査協力への要請等、第3者からの開示要請に対しては、やむを得ない理由であれば原則合意と思うが、その際、サービス事業者は、サービス利用者に対して連絡を入れる等の運用を検討してほしいという意見がでた。

4－2. その他必要となる事項 ④（コンプライアンス及び監査）

明確にすべき事項	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・監査上の注意事項について整理する。具体的には、クラウドにおいては、データの一意性や真正性の証明が困難になる中で、監査に耐えうるログデータの取得方法やSLA等の契約面での担保範囲等を整理する。
調査結果の整理	**実証実験において下記の対応を実施した。** プライバシーマークの取得やISO/IEC27001認証を取得済のデータセンターを選定し、環境クラウドの運用を実施。 サービス利用者へは、データセンターの位置を事前に説明し合意を得ている。 ログ管理については、アクセスログを管理する等、内部統制に求められる対応をとった **実証実験を行う中で、以下の留意事項が明らかとなった。** サービス利用者からは、特筆すべき指摘はなかった。 ログについては、社内でどの様なシステムと位置付けられるか判断がつかないが、J-SOX法等で会計システムに求められるレベルを実現ということではないのではという意見もあった。