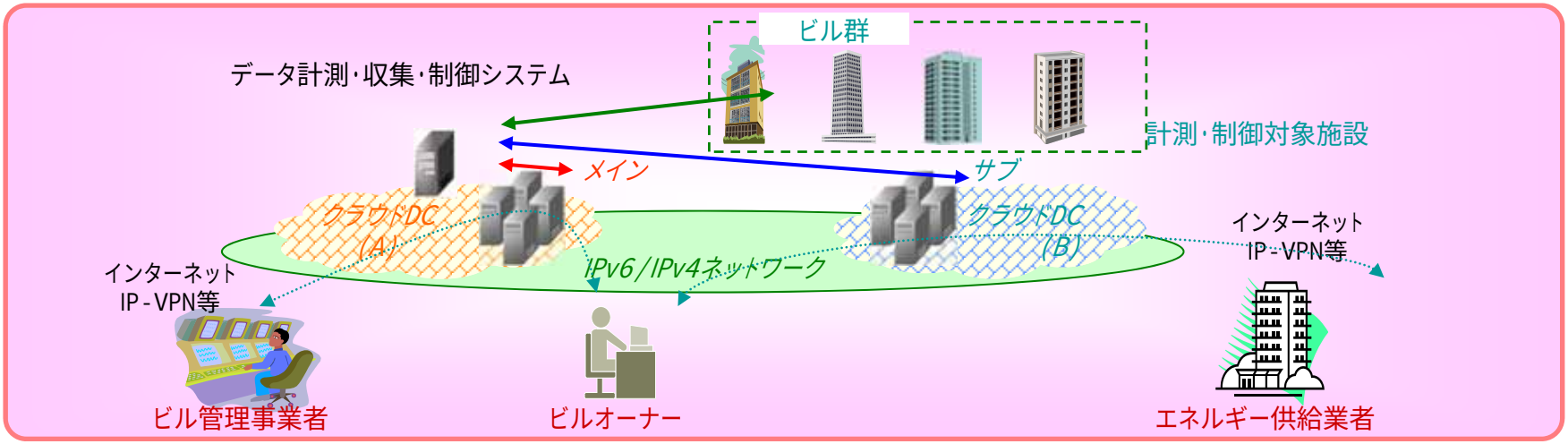
環境クラウドサービスの実証実験の実施状況等
（モデルＡ：ビル群エネルギー管理システム）

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

モデルA（ビル群エネルギー管理システム）の概要



概要･目的	**ビルオーナーが所有する複数のビル**のエネルギー効率等に基づき、エネルギー需給の制御･最適化を行うことで環境負荷（エネルギーコスト）低減への貢献を目指す
関連するプレーヤー	ビルオーナー、ビル管理事業者、エネルギー供給業者
対象エリア	広域（全国のビル展開先）
対象施設	ビルオーナー所有の複数ビル
データ特性と分析方針	**リアルタイムかつ詳細**なビル管理情報（**数千～1万程度のセンサー情報**から得られる、**大量**かつ**多種多様**なエネルギーデータ）を用い、ビル管理機器のシステム性能や、制御自体の効率性も含めた分析を行う 【データの例】各機器の成績係数、水搬送効率、空気搬送効率 【分析の例】データマイニングによる特異点抽出、可視化
データの管理方法	オーナーとの規約に準じたデータの収集･管理を行う
データの利用範囲	･オーナー（orテナント）のエネルギーコスト削減 ･オーナー（or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 ･エネルギー供給業者への提供による効率的なエネルギー需給制御
クラウド設計への影響	事業継続性の観点から、コスト要件等のために汎用的なクラウドサービスを利用する場合でも、大量の詳細データによるバースト負荷の発生に対してクラウドシステムとして柔軟にサービスを継続提供できるよう検討。

調査結果

ビル群エネルギー管理システム等に関する現状調査

①業務用ビルを対象とするエネルギー管理システムの現状

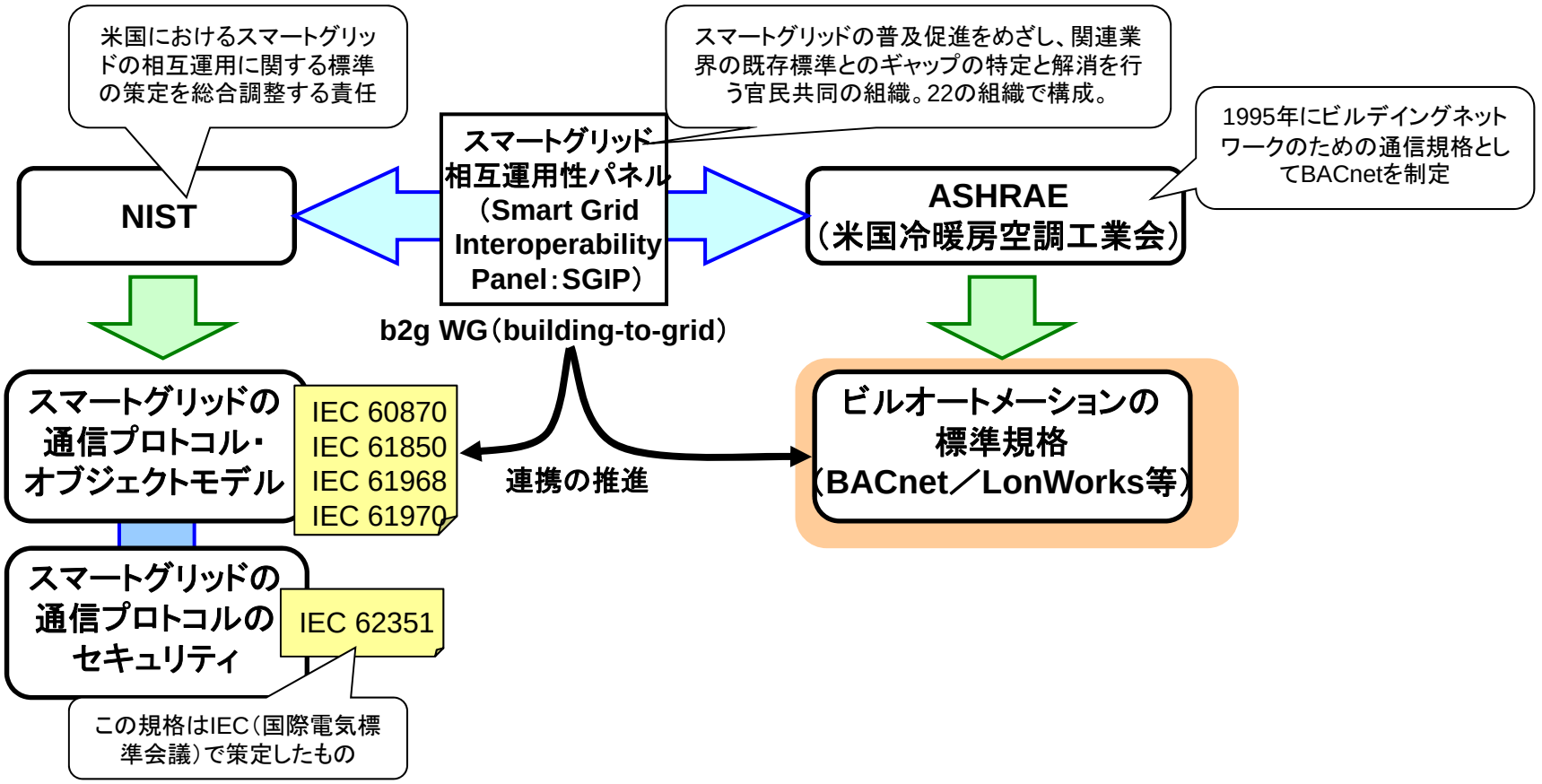
［調査項目］ 業務用ビルを対象とする最新のビル管理システム（BAS：Building Automation System／BEMS：Building Energy Management System）、モニタリングシステムに関する市場動向

②業務用ビルが利用するクラウドサービスのセキュリティの現状

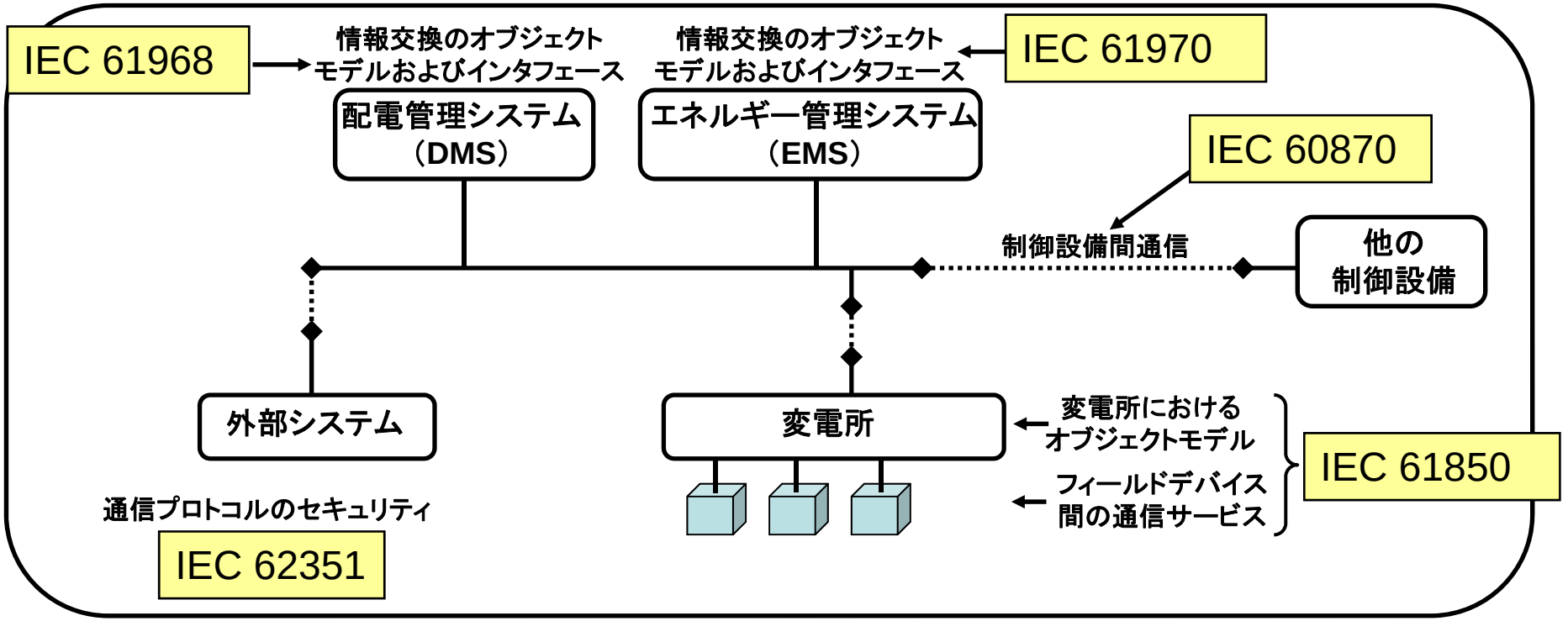
［調査項目］ 業務用ビルのエネルギー管理で利用されるクラウドに関する標準化動向、市場・技術動向

業務用ビルを対象とするエネルギー管理システムの現状

ビル管理における標準規格としては、BACnet/LonWorksがあるが、これらはASHRAEの標準規格として採用されている。スマートグリッドとの関連については、NISTの管轄下にある民間標準化団体であるスマートグリッド相互運用パネルが、スマートグリッドと、ASHRAE等が採用している既存標準とのギャップに対処する。



（参考）NISTスマートグリッド基礎規格の内容



IEC60870：電力制御設備間通信の標準を記述したもので、計測、状態、制御メッセージの通信に用いられる。リアルタイムデータ表示、制御操作、時系列データ、スケジューリングと課金情報、遠隔制御、イベント通知などを含む。

IEC61850：変電所内のシステム自動化のためのオブジェクトモデル、フィールドデバイス（メーターや電圧調整器など）間の通信サービスを規定したもの。

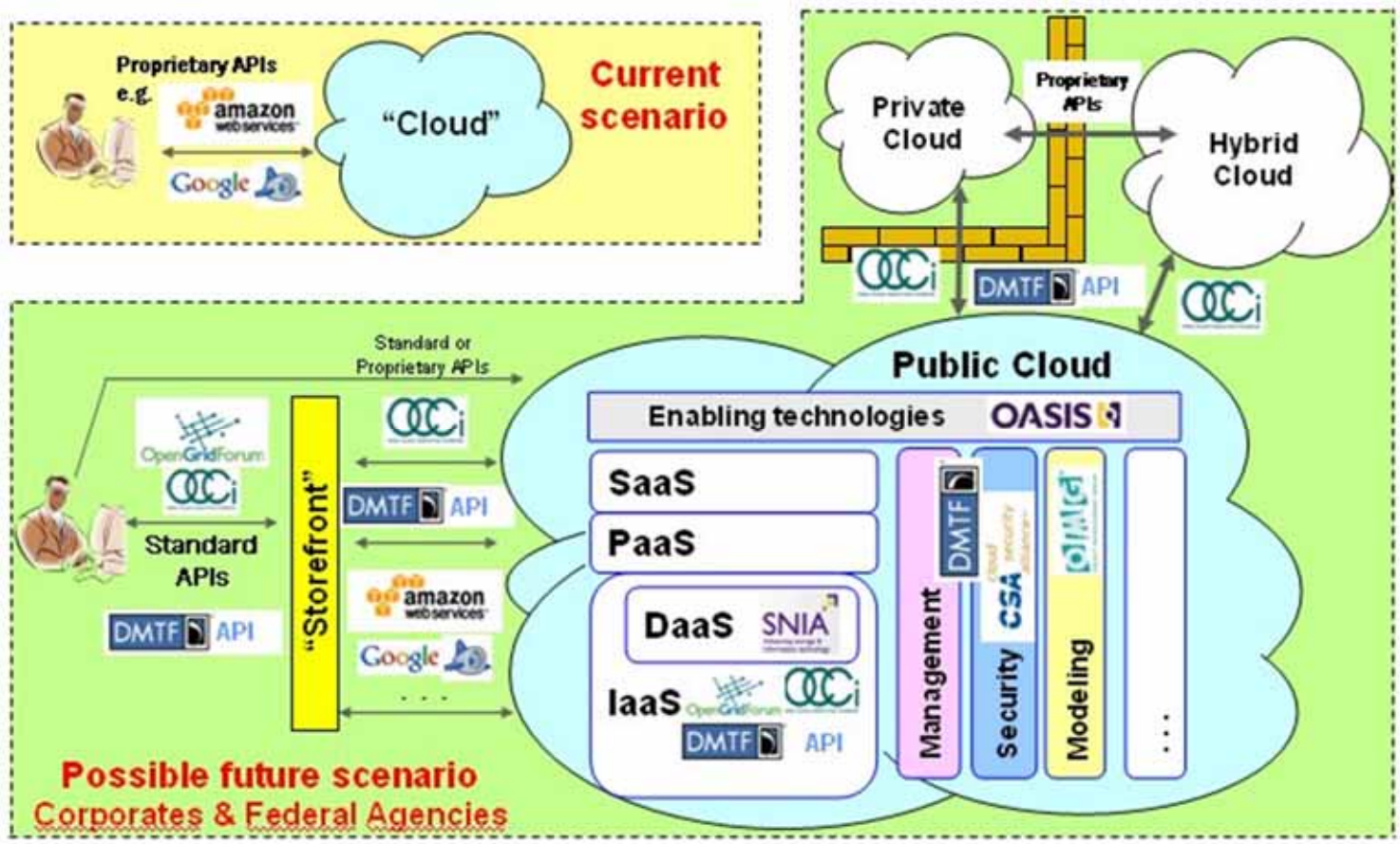
IEC61968：配電管理システムにおける、情報交換のオブジェクトモデルおよびそれに基づいたアプリケーションの通信インタフェース、すなわちアプリケーション間の相互運用性について規定したもの。

IEC61970：エネルギー管理システムにおける、情報交換のオブジェクトモデルおよびそれに基づいたアプリケーションの通信インタフェース、すなわちアプリケーション間の相互運用性について規定したもの。

IEC62351：電力システム制御操作のための情報セキュリティをスコープとし、上記IEC4標準で定義された通信プロトコルのセキュリティ標準が規定されている。

業務用ビルが利用するクラウドサービスのセキュリティの現状（標準化動向）

クラウド標準化に関わる組織が連携を模索する動きがあり、Cloud Standards Coordination（クラウド標準化団体OMGの呼びかけで2009年7月に立ち上がった標準化団体同士の情報交換の場）に各組織が参加し、議論が行われている。下図は、Cloud Standards Coordinationが整理した各組織の役割である。ここではセキュリティに関しては、CSA（Cloud Security Alliance)がマッピングされている。



業務用ビルが利用するクラウドサービスのセキュリティの現状（市場・技術動向）

センサー機器の実装制限を考慮した上で、仮想環境でのセキュリティ課題やインターネットを含む通信回線における攻撃に対処するための市場技術として、下記のようなUTM（Unified Thereat Management)製品が挙げられる。ファイアウォール、IDS/IPS（侵入検知・防御）、アンチウィルス、Webフィルタリング（フィッシング対策）等の機能を利用して、外部からの攻撃を防御する。

販売元	製品名	主な特徴
トレンドマイクロ	Deep Security	仮想化対応、パッチ管理、IDS/IPS、Webフィルタリング、FW、変更監視、管理システム連携
VMWare	vShield App／vShield Edge	仮想化対応、FW、管理システム連携、フロー監視/VPN、LB
IBM	Security Network Intrusion Prevention System	仮想化対応、IDS/IPS、仮想パッチ、Webフィルタリング
マクニカ	Altor	仮想化対応、FW。AP監視、IDS/IPS
FORTINET	FORTIGATEシリーズ	仮想化対応、FW、VPN、IDS/IPS、AV、Webフィルタリング
CheckPoint	Security Gateway Virtual Edition	仮想化対応、FW、IDS/IPS、VPN、AV、Webフィルタリング、標準規格ログ
McAfee	McAfee MOVE Anti-Virus	仮想化対応、AV

業務用ビルが利用するクラウドサービスのセキュリティの現状（市場・技術動向）

仮想環境でのセキュリティ課題に対処するため、市場にある下記のような暗号化製品を適用することができる。データベースを暗号化する製品であるが、仮想アプライアンスとしてハイパーバイザー上で動作させることが可能となっており、クラウドのユーザ企業の管理者が、自社のリソースに関するセキュリティ設定の権限を独自に持つことが出来る。これにより、クラウド側の管理者は生データに触れることはできず、データの秘匿性を確保することが出来る。

販売元	製品名	主な特徴
セーフネット	DataSecure	AP暗号化、DB暗号化、ストレージ暗号化、暗号鍵管理、事業者・利用者のデータ参照権限分離

業務用ビルが利用するクラウドサービスのセキュリティの現状（市場・技術動向）

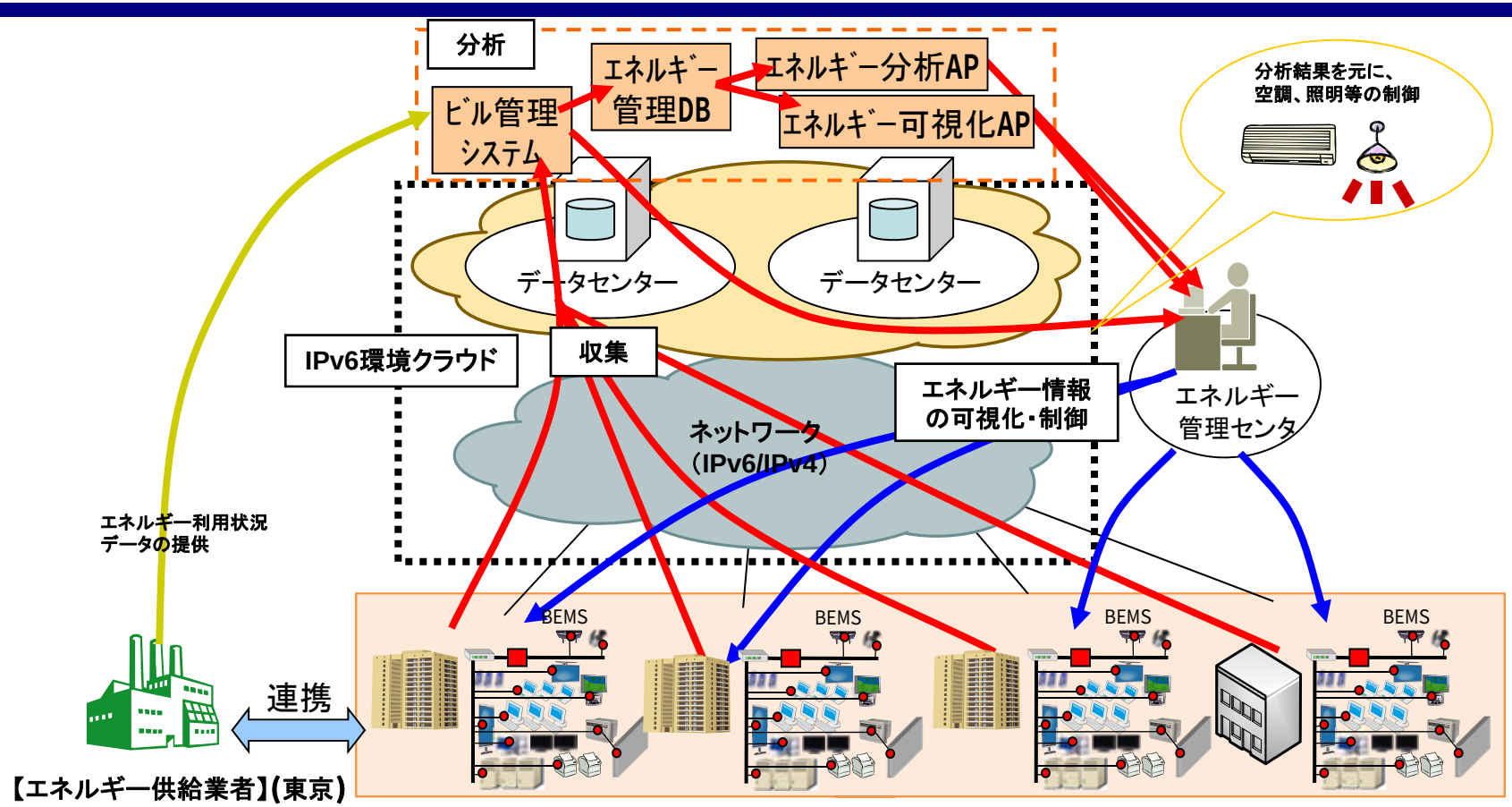
認証認可によるセキュリティの確保を行うために、市場にある下記のようなID管理製品を適用することができる。トークン等のID/PWに代わる認証手段を用いて、企業システムとクラウド間の認証連携機能を提供する。クライアント端末へのドライバインストールやクラウド上へのユーザー情報の展開を不要とし、WAN回線をレイヤー2で暗号化するといった特徴も備える。

販売元	製品名	主な特徴
セーフネット	eToken PRO Anywhere（利用者用認証トークン）	ドライバレス、証明書ベース認証
ノベル	Novell Cloud Security Service（事業者向け認証基盤）	シングルサインオン、監査ログ、ID管理

10

実証経過報告

モデルA　実証実験システムの全体構成



測定対象施設	大規模ビル			中規模ビル
	田町（19フロア）	横浜（14フロア）	名古屋（12フロア）	大塚（3フロア）
測定点	8639	4460	6830	69
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Ａの特徴について

モデルAでは、大量かつ多種多様なビル管理情報を用い、ビル管理機器のシステム性能や、制御自体の効率性も含めた分析を行うという特徴があるため、例えば以下のような観点で検証項目に特色が現れる。

✓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、リアルタイム処理への要求

⇒ 関連する検証項目：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**分析と可視化を行うための適切な設計**（定量評価指標、計測ポイントの設定等）

⇒ 関連する検証項目：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が行われる仕組み

⇒ 関連する検証項目：移植性及び相互運用性、ID管理とアクセス管理

モデルＡの検証項目と検証方法

	特徴点	想定される要件	検証方法
1．拡張性の確保に関する検証			
1－1．移植性及び相互運用性	一般的なクラウド基盤への移植性の高いビル管理モジュールが求められる	アプリケーション導入の際、複数のクラウド基盤での動作確認の実施	VMware、Xen等複数の仮想基盤間でのアプリケーション移設を実証する
1－2．事業継続性	障害発生時のロスを防ぐためにはリアルタイムなバックアップや迅速なリストアが重視される	特定のデータセンターの障害時にもクラウド全体としてサービスの継続性を担保すること	基盤レベルの負荷分散機能を活用しながらデータセンター間のサービス引継ぎを実証する
1－3．情報管理	ビルオーナーやテナントの内部情報を扱うため高い情報セキュリティが求められる	複数ビルのデータの集中管理・分析を行うが、第三者によるデータの2次利用は通常行われない	データの退避・保全・復元を定期的に実施し、可用性保全の機能・水準を明らかにする
1－4．仮想化	ビルの利用状況に即した柔軟な管理システムを、仮想化技術を活用して実現する	仮想化された、論理基盤上における情報セキュリティの確保	仮想サーバの通信のモニタリングを実施し、高いセキュリティレベルの確保を実証する
1－5．アプリケーションの開発・運用管理	単一ユーザーによるクラウドアプリケーション利用のモデルとなる	基盤だけでは補償しきれない、アプリケーションレベルでのデータの安全性確保	サーバ間の通信チャネルをIPsecで保護することでアプリケーションのセキュリティ強化を実証する
2．情報セキュリティの確保に関する検証			
2－1．ID管理とアクセス管理	既存の管理システムのクラウドへの統合シナリオが考慮される	既に展開されている認証セキュリティが、クラウドとシームレスに連携すること	クラウド上の複数のアプリケーションサーバに対するシングルサインオンを実証する
2－2．暗号化及び鍵管理	暗号化を活用して内部情報を安全に取り扱うことが求められる	センサ情報の機密性・完全性確保および適切なアクセスコントロールに基づく管理・制御	インターネット経由、VPN経由に関わらず、暗号化・鍵管理によって通信の保護を実証する
2－3．インシデント対応	マルチテナント環境に対応した運用監視システムによってクラウドが管理される	複数のユーザに対する包括的な監視・管理が可能であること	市中技術を利用した統合監視システムを構築し、監視・インシデント対応の運用を実証する
2－4．データセンターの安全性確保、運用管理	ビル管理アプリケーションや多種多様なセンサーネットワークを収容するクラウド基盤である	基盤リソースの動的増強、ビル群管理に特化したシステム設計、IPv6等によるNWのEnd-to-End到達性など	バースト負荷に対する動的リソース供給や、ビル内計測ポイントの評価を実施する
3．環境負荷軽減効果の評価に関する検証			
3－1．環境負荷軽減効果の可視化	ビルオーナーが望む要求性能に準じた定量評価が求められる	定量評価指標、計測ポイントの設定等、ビル群管理アプリに特化したシステム設計	評価指標・計測ポイントの有効性について実証を通して評価を行う

1－1．移植性及び相互運用性

想定される要件

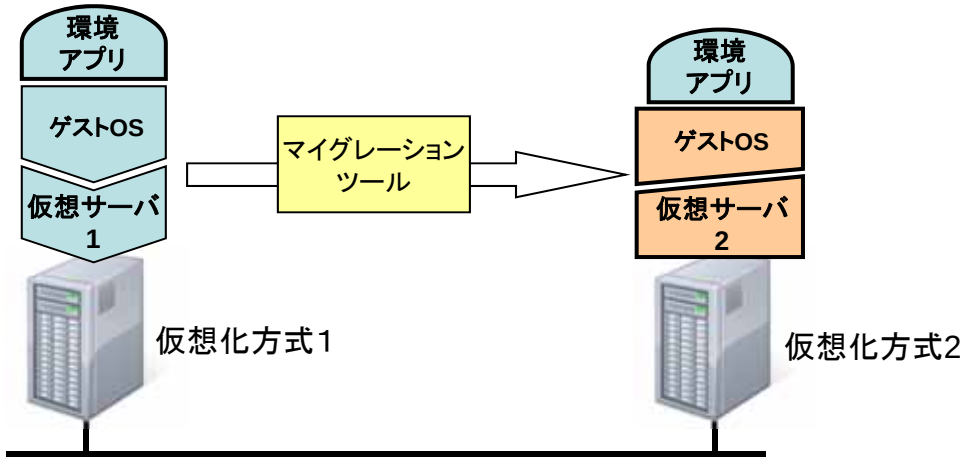
環境アプリケーションを導入する際、異なる仮想化方式を用いたクラウド基盤間での移植性の確保を考慮しなければならない。従って、異なる複数の仮想化方式上で環境アプリケーションを動作させるためのプロセスについて検証を行った。

検証方法

異なる複数の仮想化方式では、仮想サーバのイメージの形式が異なるためことが想定されるため、マイグレーションツールを利用してイメージ形式を変換する等により、異なる仮想化方式を用いた基盤への移植性を検証した。

実証実験の内容

仮想化方式が異なる環境クラウド基盤へ環境アプリケーションを移行することを想定し、異なる仮想化環境への移行プロセスについて検討した。



実証実験の結果

実証実験において以下を実施した

・マイグレーションツール等による異なる仮想化方式に移植する方法の検討および実証環境での移行後の環境アプリケーションの運用状況の確認

実証実験を行う中で、以下が明らかになった

・仮想化方式によっては、移植の際にマイグレーションツールが必要になること

・移行後は、移行前の状態から継続して環境アプリケーションを正常に運用できることが確認でき、特定のプラットフォームへの依存性を軽減可能であること

1－2. 事業継続性

想定される要件

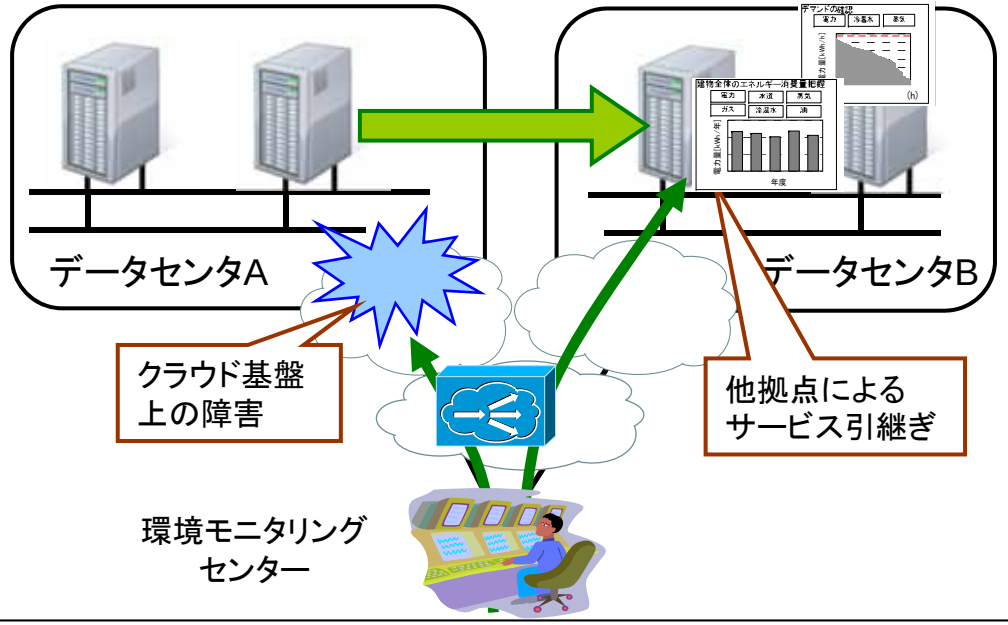
環境クラウドサービスでは、大量のセンサ情報を収集し制御を行うため、クラウド基盤のサービス停止が起きた場合、データロスなどの損害も大きい。従って、特定のデータセンター上に障害が発生した場合にも、クラウド上の他のデータセンターにおいて**リアルタイムのサービス引継ぎ**を実施することが重視される。

検証方法

本実証では、地理的に離れた2つのデータセンターを用意し、負荷分散機能を活用して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、Web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。

実証実験の内容

環境クラウドサービスを運用しているデータセンターでの障害を想定し、バックアップサイトのデータセンタへサービスを引き継ぐ方法を検討した。



実証実験の結果

実証実験において以下を実施した
- プライベートクラウド内のサービス引継ぎ
- プライベートクラウドからパブリッククラウドへの引継ぎ

実証実験を行う中で、以下が明らかになった
- バックアップサイトがプライベートクラウド、パブリッククラウドに関わらずサービス引継ぎが可能であること

1－3. 情報管理

想定される要件

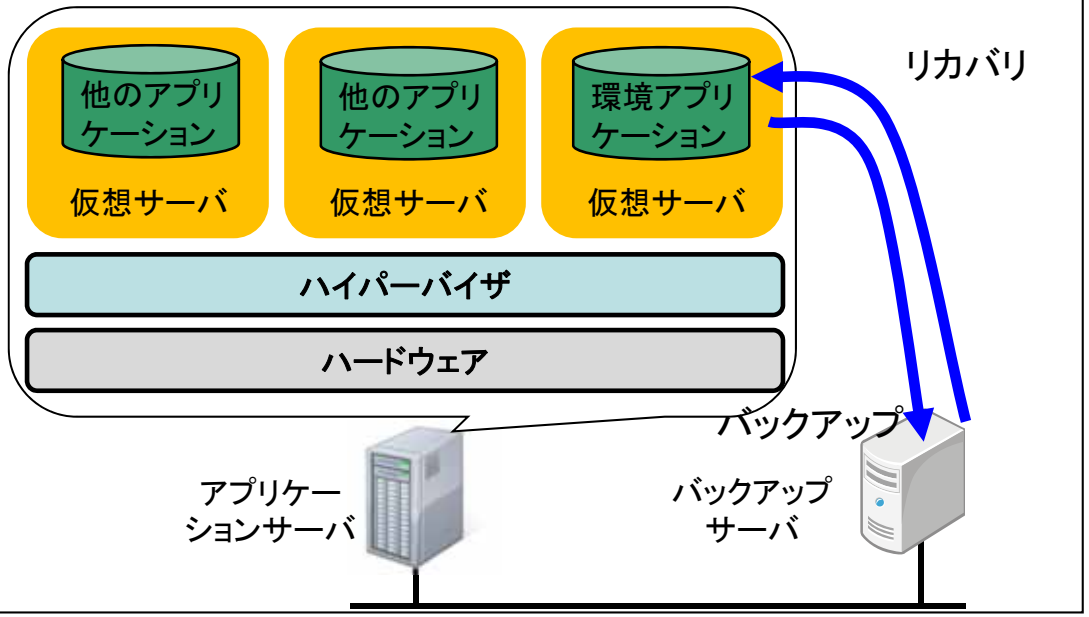
データバックアップにおいては、万が一の流出に備え、データは暗号化されることが望ましい。このとき、第三者が利用している仮想サーバが存在しているマルチテナント環境でデータが保存されることを考慮しなければならない。従って、マルチテナント環境においても、安全に暗号化してデータを保存する方法を実証を行う。

検証方法

マルチテナント環境を考慮したデータ保存を行うためには、暗号化する際に利用者ごとに暗号鍵を分ける方法が有効である。本実証では、ストレージ管理ソフトウェアを利用し、データバックアップの際に利用者ごとに暗号鍵を変える運用で検証した。

実証実験の内容

データ流出時に備え、バックアップする際、暗号化を施し、暗号化されたデータは正規のユーザのみがリカバリできる方法を検討した。



実証実験の結果

実証実験において以下を実施した

・環境クラウドサーバを設置し、ストレージ管理ソフトウェアによるデータの定期的なバックアップ

・正規の暗号鍵を有している利用者、有していない第三者のリストア時の効果を検証

実証実験を行う中で、以下が明らかになった

・マルチテナント環境でも利用者ごとに暗号鍵を使い分けて暗号化を行うことで、正規の利用者のみが正常にリストアでき、安全なデータ管理が可能なこと

1－4. 仮想化

想定される要件

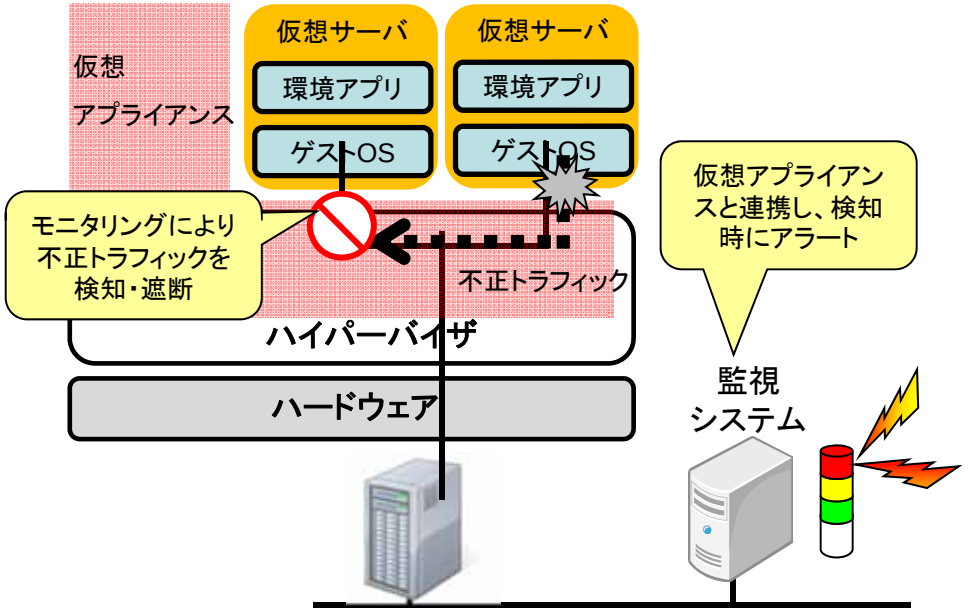
仮想化技術を用いたサービス基盤では、同一物理サーバ上で複数の仮想マシンが動く。そして、仮想マシン同士が物理サーバ内に論理的に存在する仮想ネットワークを経由して通信を行う場合がある。そのため、物理サーバ外部のネットワークのトラフィック監視のみならず、仮想ネットワーク上のトラフィック監視も必要となる。

検証方法

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を利用することで、仮想ネットワーク上の通信のモニタリングを検証した。

実証実験の内容

仮想サーバ間で不正なトラフィックが発生することを想定し、不正トラフィックへの対策方法を検討した。



実証実験の結果

実証実験において以下を実施した

・仮想アプライアンスを用いた、仮想ネットワーク上のトラフィックのモニタリング

・モニタリングしたトラフィックの中で、不要なトラフィックの検知・遮断

実証実験を行う中で、以下が明らかになった

・仮想アプライアンスにより、従来にはなかった仮想ネットワーク上のセキュリティも確保が可能

１－５．アプリケーションの開発・運用管理

想定される要件

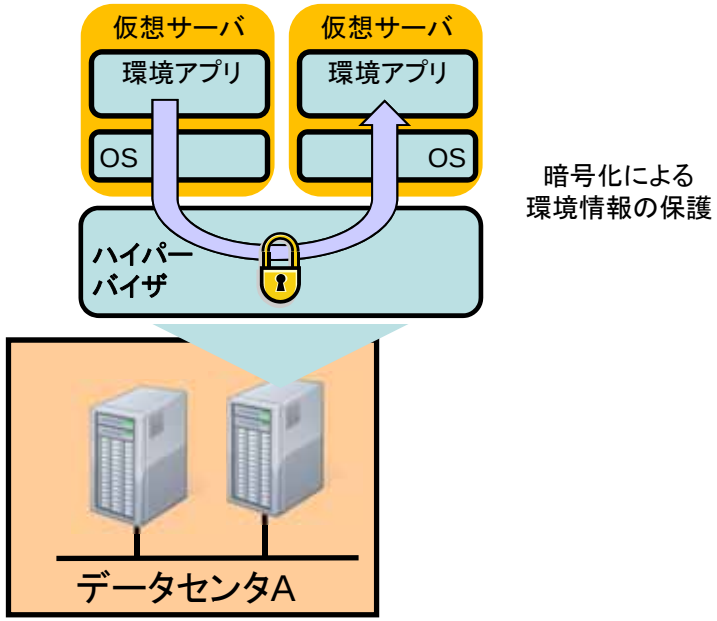
環境クラウドサービスでは、複数の仮想サーバ間でアプリケーションが連携する場合がある。このとき、仮想サーバ間で通信が発生するが、同一のネットワーク内には第三者が利用する仮想サーバが存在する可能性があるため、通信の盗聴のリスクがある。
従って、仮想サーバ間の通信の安全性を確保する必要がある。

検証方法

本実証では、仮想サーバ間の通信においてIPSecを用いた暗号化を行うとともに通信のモニタリングを検証した。

実証実験の内容

アプリケーションごとにセキュリティレベルが異なることを想定し、画一的にアプリケーション運用におけるセキュリティを確保する方法を検討した。



実証実験の結果

実証実験において以下を実施した
・仮想サーバ間の通信におけるIPSecを用いた暗号化
・暗号化された通信のモニタリングによる、仮想サーバ間の通信の秘匿性の確認

実証実験を行う中で、以下が明らかになった
・仮想環境上の環境アプリケーションの連携においても、暗号化によるデータ転送の安全性確保が重要となること

2－1．ID管理とアクセス管理

想定される要件

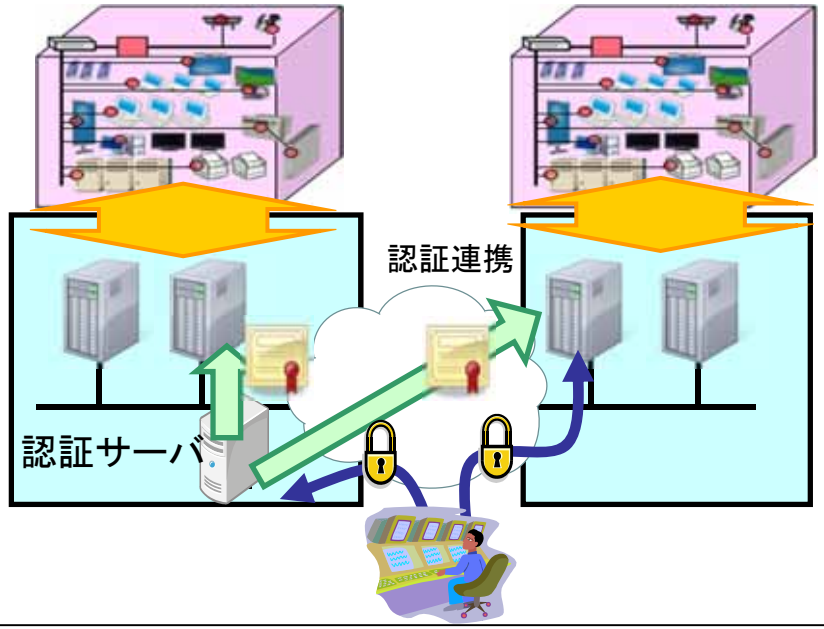
ビル管理者が、自拠点からクラウド上のビル群管理システムへアクセスする際に要求される認証は、既存の管理システムの認証セキュリティ（ID・パスワードやハードウェアトークン等）とシームレスに連携することが求められる。従って環境クラウドにおける認証連携機能（**複数のサーバ間での認証情報の引継ぎ**）が必要となる。

検証方法

複数のデータセンターに認証サーバを設置し、認証連携機能を持たせることで複数の環境アプリケーションの間でシングルサインオンを検証する。

実証実験の内容

既存のシステムと環境クラウドサービス等の複数のドメインでもシームレスに連携することを想定して、認証連携について検討した。



実証実験の結果

実証実験において以下を実施した

・東京の2つのデータセンターに認証連携機能を持った認証サーバを設置し、環境アプリケーション間でのシングルサインオンを確認

実証実験を行う中で、以下が明らかになった

・認証連携機能により、高い認証セキュリティを保ったまま、複数の環境アプリケーションのシームレスな利用が可能

・アプリケーション個別に認証連携機能の追加が必要であったことから、開発時から認証連携を想定した実装を意識することが望ましい

2－2. 暗号化及び鍵管理

想定される要件

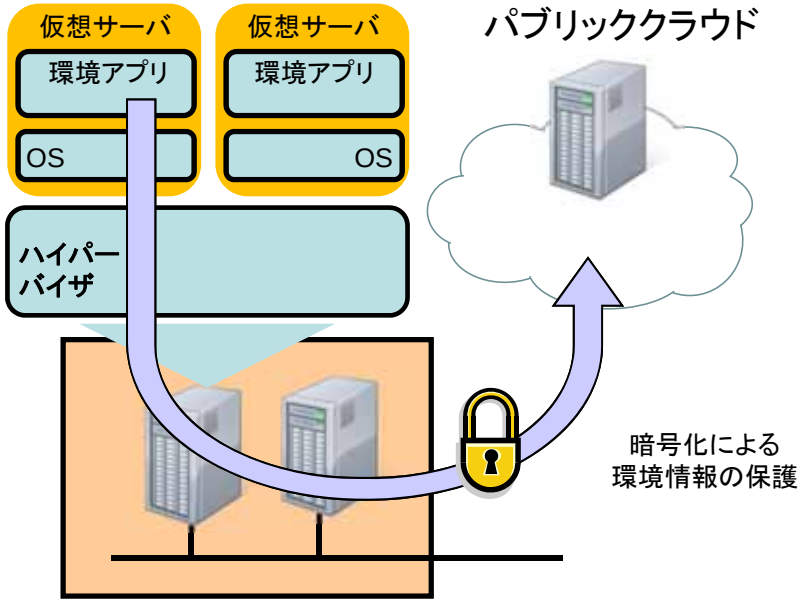
環境クラウドサービスをパブリッククラウド上で運用する際、データはインターネット上を転送されることになるため、セキュリティの確保が重要になる。

検証方法

パブリッククラウド上で運用される環境クラウドサービスの通信において、適切な暗号化を行う。そして、パケットデータのモニタリングを行い、暗号化により機密性が確保されることを確認する。

実証実験の内容

パブリッククラウド利用時に、データがインターネット上で転送される際、経路上での盗聴等のデータ漏洩を想定し、安全にデータを転送する方法を検討した。



実証実験の結果

実証実験において以下を実施した

・インターネットを経由した通信における、SSL-VPNによる暗号化およびパケットデータのモニタリング

実証実験を行う中で、以下が明らかになった

・パブリッククラウドをプラットフォームとして選定する場合、SSL-VPN等のセキュリティ施策により安全性が確保されること

・一方で、クラウド側に物理的にVPN機器を導入することが必ずしもできないため、ソフトウェアによるソリューションが一部必要になること

2－3. インシデント対応

想定される要件

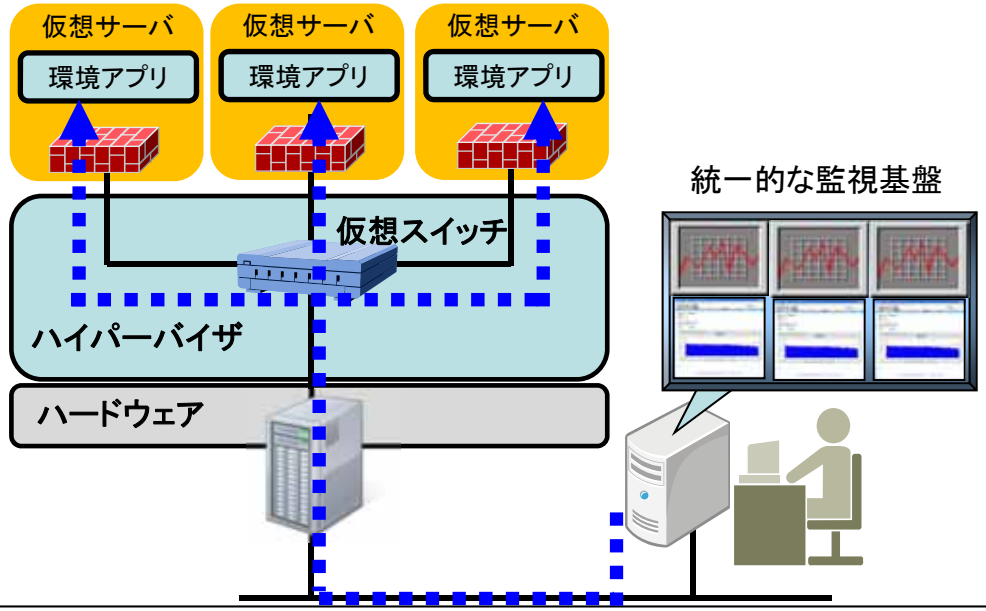
サーバの仮想化により監視対象の可視性が下がるため、クラウド基盤の運用の観点では、マルチテナント環境下においても一貫した運用監視システムにより管理できることが重要となる。

検証方法

マルチテナント環境でも一貫して、生死監視、プロセス監視等を行うことができる運用監視システムを構築し、複数の環境アプリケーションの停止および復旧を検知できることを検証する。

実証実験の内容

サーバの仮想化により監視対象の可視性が下がることを想定して、仮想サーバも含めて統一的に監視する方法を検討した。



実証実験の結果

実証実験において以下を実施した

・運用監視システムを構築し、仮想サーバ上で運用される複数の環境アプリケーションの停止、復旧時の検知。

実証実験を行う中で、以下が明らかになった

・マルチテナント環境下の仮想サーバの監視においても、従来の物理端末の監視と同様に、統一的な監視を行え、障害の発生・復旧の検知ができること

2－4. データセンタの安全性確保、運用管理

想定される要件

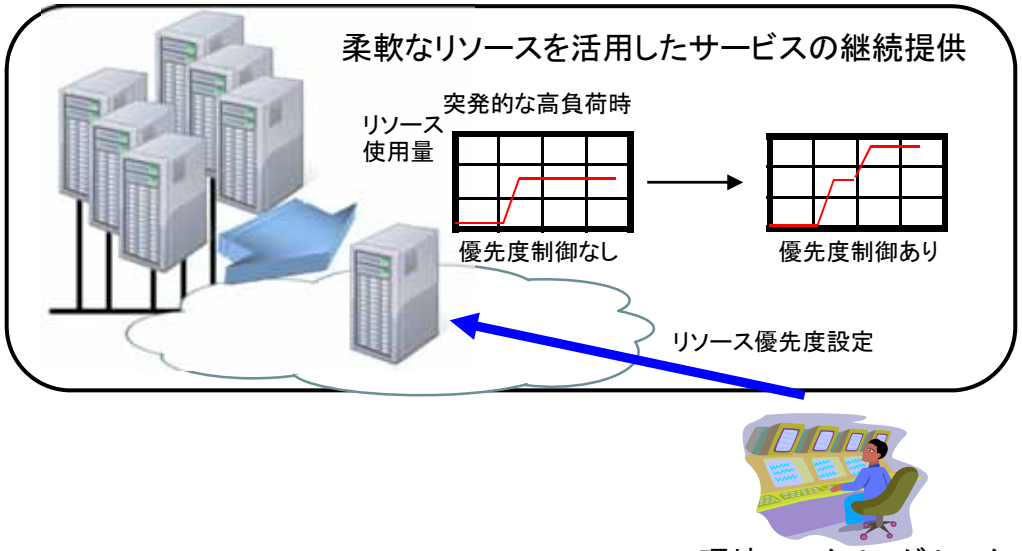
1箇所のビルで大量のセンサ情報の収集分析を行う場合、災害、障害などイベント発生時の警報や、日次のデータ分析などの計算負荷が突発的に発生し、クラウドのリソースを圧迫する可能性がある。
従って本実験ではクラウドの**リソースを動的に増強する仕組み**が必要である。

検証方法

クラウドのプロビジョニング機能を活用することで、仮想マシン上でバースト負荷が発生した際にも、動的に処理のためのリソースが追加されることを検証する。これにより、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を確認する。

実証実験の内容

突発的に負荷がかかる状況を想定し、リソースを動的に増強する仕組みを検証した。



実証実験の結果

実証実験において以下を実施した
・仮想マシンに優先度を設定し、特定の仮想マシンにバースト負荷を発生させたときのリソース状況を確認

実証実験を行う中で、以下が明らかになった
・リソースの動的制御をするためには、環境アプリケーションの種類に応じてリソース追加の優先度をあらかじめ決めておく必要があるため、事前にアプリケーションの処理の重要度や想定される負荷発生タイミングを検討することが必要

3－1．環境負荷軽減効果の可視化

想定される要件

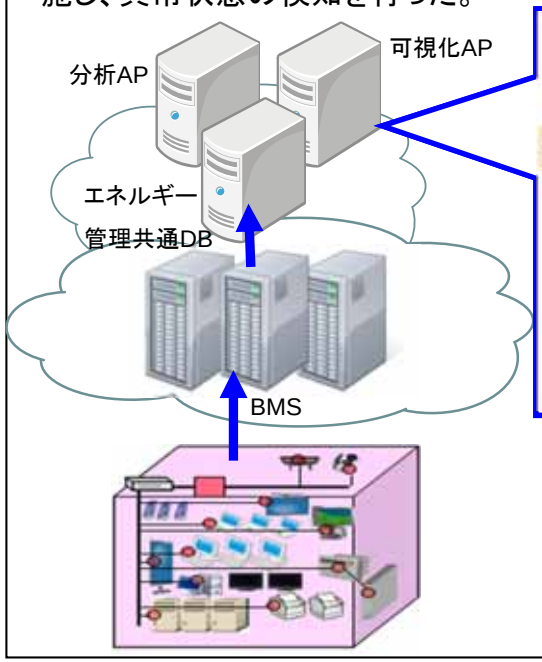
ビルオーナーが望む要求性能に準じた定量評価指標、計測ポイントの設定等、ビル群管理アプリケーションに特化したシステム設計が要件として求められる。

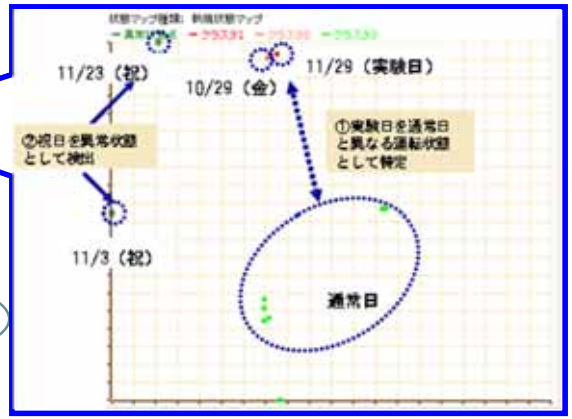
検証方法

実証実験に先立って、環境アプリケーションが効果的に動作するための評価指標・計測ポイントの設計を行い、実証を通してその有効性について評価を行う。

実証実験の内容

収集したエネルギー消費データをもとに環境アプリケーションによる分析を実施し、異常状態の検知を行った。





エネルギー消費状態マップ（特徴点抽出）

実証実験の結果

実証実験において、以下を実施した

・照明の消し忘れを想定した実験を実施し、通常日の消灯状態と実験日の点灯状態についての蓄積されたエネルギー消費データから特徴点抽出を行い、正しく異常状態の検知が行えることを確認

さらに詳細な分析のため、引き続き継続分析中

ネットワーク要件以外に検討が必要な事項

環境クラウドを活用したビル群エネルギー管理システムを実現するためには、法制度に関する事項など、ネットワーク要件以外にもセキュリティ上の検討項目が存在する。ここでは、実験では検証できないが、環境クラウドのセキュリティを考慮する上では不可欠な事項について調査を行った

事項	検討内容
４－１．責任分界点の設定	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検討する
４－２．ガバナンス及びエンタープライズリスクマネジメント	強固なガバナンスを達成するために必要となる事業者と利用者の連携について検討する
４－３．法制度及び電子情報の開示	環境クラウドサービスにおいて、意識すべき法制度について言及し、顧客の電子情報を開示しなければならないケースについて検討する
４－４．コンプライアンス及び監査	クラウド環境下では、監視の複雑化が懸念されることから、コンプライアンスの徹底や、それを監査するために必要な事項を検討する

4－1. 責任分界点の設定

セキュリティインシデントに関して、利用者と事業者の間に、セキュリティ関連の役割と責務についての明確な定義が必要である。欧州のENISA*1では、運用における合理的な責務の範囲として、下記の表のように、SaaS、PaaS、IaaSにおいて、利用者および事業者ごとに整理している。

*1 ENISA:European Network and Information Security Agency(欧州 ネットワーク情報セキュリティ庁)

利:利用者　事:事業者

№	責務	SaaS		PaaS		IaaS	
		利	事	利	事	利	事
1	収集および処理されたクラウド環境クラウドサービス利用者のデータに関するデータ保護法への適合	○					
2	ID管理システムの維持管理	○		○		○	
3	ID管理システムのマネジメント	○		○		○	
4	認証プラットフォームのマネジメント（パスワードポリシーの実施を含む）	○		○		○	
5	物理的サポートインフラストラクチャ（設備、ラック空間、電力、空調、配線等）		○		○		○
6	物理的なインフラストラクチャのセキュリティと可用性（サーバ、ストレージ、ネットワーク帯域等）		○		○		○
7	OSのパッチ管理と強化手順（環境クラウドサービス利用者の強化手順とプロバイダのセキュリティポリシーとの矛盾の有無の確認）		○		○		
8	セキュリティプラットフォームの設定（ファイアウォールルール、IDS/IPSのチューニング等）		○		○	○	
9	システムの監視		○		○		
10	セキュリティプラットフォームのメンテナンス（ファイアウォール、ホスト用IDS/IPS、ウイルス対策、パケットフィルタリング）		○		○		
11	ログの収集およびセキュリティの監視		○		○	○	
12	ゲストOSのパッチ、および強化手順の管理（環境クラウドサービス利用者の強化手順とプロバイダのセキュリティポリシーとの矛盾の有無の確認）					○	
13	ゲストセキュリティプラットフォームの設定（ファイアウォールルール、IDS/IPSのチューニング等）					○	
14	ゲストシステムの監視					○	
15	ホストシステム（ハイパーバイザー、仮想ファイアウォール等）						○

4－2. ガバナンス及びエンタープライズリスクマネジメント

ITの統制においては、COBITのITガバナンスのフレームワークが最も用いられる。COBITのフレームワークの観点から、クラウド利用の場合のITガバナンスを当てはめると、”IT資源”, “ITプロセス”の殆どが、利用者から事業者に移行するため、利用者にとって重要となるのは、企画・事業者選定段階におけるリスクマネジメント、その後の運用段階におけるリスクマネジメントである。

COBITのITガバナンスフレームワークを元にした、利用者、事業者のガバナンス

ITプロセス		主管	
		利用者	事業者
計画と組織	PO1 IT 戦略計画の策定	○	
	PO2 情報アーキテクチャの定義		○
	PO3 技術指針の決定		○
	PO4 IT プロセスと組織及びそのかかわりの定義		○
	PO5 IT 投資の管理	△	○
	PO6 マネジメントの意図と指針の周知		
	PO7 IT 人材の管理		○
	PO8 品質管理		○
	PO9 IT リスクの評価と管理	△	○
	PO10 プロジェクト管理		○
調達と導入	AI1 コンピュータ化対応策の明確化	○	
	AI2 アプリケーションソフトウェアの調達と保守		○
	AI3 技術インフラストラクチャの調達と保守		○
	AI4 運用と利用の促進		○
	AI5 IT資源の調達		○
	AI6 変更管理		○
	AI7 ソリューションおよびその変更の導入と認定		○
サービス提供とサポート	DS1 サービスレベルの定義と管理		○
	DS2 サードパーティのサービスの管理		○
	DS3 性能とキャパシティの管理		○
	DS4 継続的なサービスの保証		○
	DS5 システムセキュリティの保証		○
	DS6 費用の捕捉と配賦		○
	DS7 環境クラウドサービス利用者の教育と研修	○	
	DS8 サービスデスクとインシデントの管理		○
	DS9 構成管理		○
	DS10 問題管理		○
	DS11 データ管理		○
	DS12 物理的環境の管理		○
	DS13 オペレーション管理		○
モニタリングと評価	ME1 IT 成果のモニタリングと評価	○	○
	ME2 内部統制のモニタリングと評価		○
	ME3 外部要件に対するコンプライアンスの保証		○
	ME4 IT ガバナンスの提供	○	○

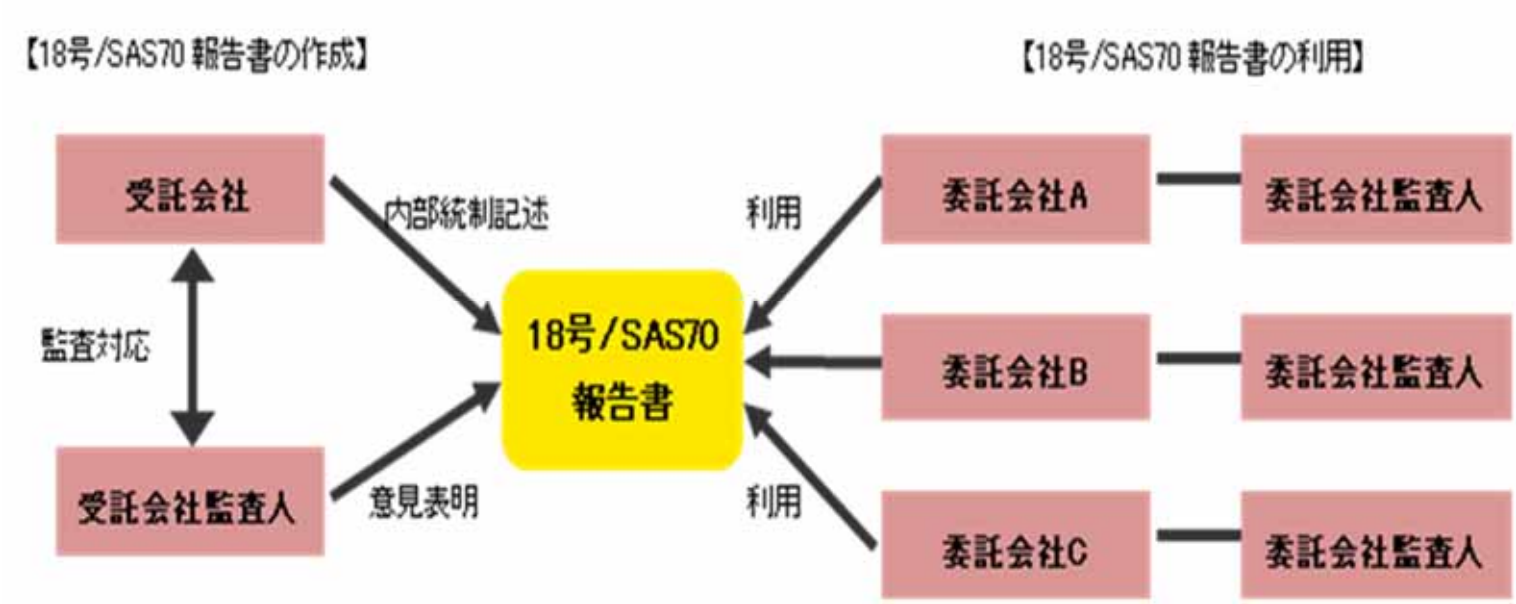
４－３．法制度及び電子情報の開示

日本の法制度においては、データの保全義務や電子情報開示を明文化したものはなく、条件付きで個人情報保護法が適用される。しかし、海外の国や州によってはEUデータ保護条例やe-ディスカバリに関する制裁規定等の、データに関する法律や条例が存在する。環境クラウドサービスが海外のデータセンターで運用される場合は、扱うデータに対してその国の法律が適用されるため、法律の適用関係を十分に検討し、契約時にはデータ取り扱いの方法や責任を明確化し、必要に応じてSLAを盛り込むことが求められる。

日本および海外の法制度

	法制度	概要
日本	エネルギーの使用の合理化に関する法律（省エネ法）	エネルギー使用量が一定値以上の企業やフランチャイズ本部に、国への報告書の提出義務を課す。
	地球温暖化対策の推進に関する法律（温対法）	温室効果ガスの排出量が多い場合、国への報告を義務を課す。
	東京都環境確保条例	燃料、熱及び電気等のエネルギー使用量が原油換算で年間1500キロリットル以上をしている企業に対して、対策計画書の提出や、温室効果ガスの削減(8%)の義務を課す。
	個人情報の保護に関する基本方針	データベース等で5000件を超える体系的に整理された個人情報を保有する企業は個人情報取扱事業者となり、この法律の対象となる。
	J-SOX法	法律ではないが、外部に委託しているIT業務の内部統制についても経営者評価を行うことが必要な内部統制報告制度。
海外	e-ディスカバリに関する制裁規定(米国)	訴訟状態になった場合、適正な情報開示がなされていないとみなされた場合、強制的に情報開示の制裁が課される。
	EUデータ保護条例(EU)	EU内の住民の個人情報に関して十分なデータ保護レベルを確保していない第三国へのデータの移動を禁じている。
	カリフォルニアデータセキュリティ法（米国)	民間企業に対し、暗号化されていない個人情報の漏えいがあった場合、あるいは漏えいが疑われる場合に、原則としてカリフォルニア州の住民に通知することを義務づけている。暗号化されている場合は通知の必要性はない。

クラウド環境の利用によって事業者側へ移管されたガバナンスにおいては、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。そのとき、事業者が外部監査を活用し、ISMS/ITSMS，18号/SAS70報告書の認証をとることが効果的である。利用者はSLAや契約書の内容が順守されていることを確認するために事業者が持つ認証により監査を行うことができ、また、事業者も利用者個別の監査対応による負荷の軽減が可能になる。ただし、認証範囲に利用者がカバーしたい評価項目がない場合は、追加を交渉することが望ましい。



18号/SAS70報告書を利用した認証の仕組み