

インタークラウドのユースケースと機能要件

目次

1	はじめに	1
2	クラウドの定義	2
3	サービスに対する品質要件とクラウド事業者の SLA	5
3.1	サービスに対する品質要件とは	5
3.2	クラウド事業者における SLA とは	6
4	インタークラウドの必要性とねらい	7
4.1	End to End でのサービス毎の品質保証	7
4.1.1	性能保証	7
4.1.2	可用性保証	8
4.2	サービス連携による利便性	8
5	インタークラウドによるユースケース	9
5.1	End to End でのサービス品質保証	9
5.1.1	性能保証	9
5.1.2	可用性保証	11
5.2	サービス連携による利便性向上	12
5.3	サービス継続	13
5.4	ブローカー介在による市場取引	14
6	インタークラウドのユースケースにおける手順	15
6.1	クラウドシステム間の連携により、性能を保証する手順	15
6.2	クラウドシステム間の連携により、サービスを復旧し可用性を保証する手順	19
7	インタークラウドの機能要件	22
7.1	サービス利用者の品質要件と SLA のマッチング	22
7.2	監視(リソース、サービス、死活)	22
7.3	プロビジョニング	23
7.4	リソース発見・確保	23
7.5	リソース管理	24
7.6	サービスセットアップ	25
7.7	認証連携	25
7.8	ネットワーク連携	27
7.9	利用者からのアクセスルートのデータ変更と戻し	27
7.10	リソース解放	27
8	インタークラウドにおけるクラウドシステムの機能構成とインタフェース	28
8.1	機能構成	28
8.2	インタフェース	29
9	おわりに	30

10 参考文献..... 30

◎免責事項:

本ホワイトペーパーはGlobal Inter-Cloud Technology Forum(以下「GICTF」)が作成したものです、GICTFは本ドキュメントで提供される内容に関し、その正確性、有用性、確実性その他いかなる保証もするものではありません。本ドキュメントで提供される内容を利用する場合は、利用者の責任において行ってください。本ドキュメントに記載された内容のご利用により万が一何らかの損害が発生したとしても、GICTFは一切責任を負いません。

本ドキュメントの著作権は、GICTFに帰属します。本ドキュメントの全部または一部の「プリントアウト」「コピー」「無料配布」は可能ですが、GICTFの許諾なく無断で改変、公衆配信、販売、出版、翻訳／翻案することなどは営利目的、非営利目的に関わらず禁じられています。

以上の点をご了承の上、ご利用ください。

◎本ドキュメントに関する問い合わせ先

Global Inter-Cloud Technology Forum

inquiries-090717@gictf.jp

1 はじめに

クラウドシステムは、新たな価値を創造するITインフラストラクチャとして、その潜在能力に期待が高まっている。今後企業の基幹業務や電子行政や社会インフラサービスへ適応領域を広げていくためには、クラウドシステムのコンピューティング資源(リソース)のみならず、ネットワークも含めたEnd to Endのサービス品質保証の考慮や、コンプライアンス/ガバナンス等も含めた信頼性要求、さらには省電力要求に応じていく必要がある。

1つのクラウドシステム(シングルクラウド)によりサービスが提供されている状況では、クラウドシステムへの想定外の過負荷(インターネットからのトラフィックなど)や自然災害などの発生により、予備のリソースの補填が求められるかもしれない。しかし、シングルクラウドが保有する利用可能な予備リソースには限りがあることから、サービス継続に限界が出ることが考えられる。そのような場合にもサービスの可用性や性能などの品質保証の要求に応え続けるためには、ブロードバンドネットワークで結ばれた他のクラウドシステム間と連携(インタークラウド)してリソースを調達する といった相互に補完する仕組みが必要不可欠となる。

今日まで各クラウド事業者は独自仕様でクラウドシステムを構築して来ている。システム間のインターフェースの標準化を行うことは、クラウドシステム間の連携を進め、より高信頼、高品質なクラウドサービス提供を実現可能とする。その結果として、企業活動や行政活動といった社会活動全般も活性化されることが期待できる。

本ドキュメントでは、インタークラウドのシステムに対する機能要件やインタークラウドのインターフェース要件について記載する。

2 クラウドの定義

本ドキュメントにおけるクラウドシステム間連携の対象として扱う“クラウド”に関する定義は、NIST (National Institute of Standards and Technology)から公開されているドキュメントの定義を用いる。その定義(基本的な特徴、サービスモデル、配備モデル)を抜粋し、以下に示す。

クラウドコンピューティングとは、複数の利用者によって共有される設定・調節可能なコンピュータリソース(ネットワーク、サーバ、ストレージ、アプリケーション、サービス等)プールに、オンデマンドにネットワークからアクセスが可能な、利便性のあるモデルのことである。リソースは、管理する労力やプロバイダの関与を最小限に抑えつつ迅速に提供・リリースすることができる。このクラウドモデルは可用性を促進するものであり、5つの基本的な特徴、3つのサービスモデル、及び4つの配備モデルから成り立っている。

基本的な特徴:

オンデマンド・セルフサービス:

利用者はサービスプロバイダの人的関与無しに、必要に応じて自動的にサーバタイムやネットワークストレージ等のコンピューティング能力を利用することができる。

幅広いネットワークアクセス:

種々のクライアントプラットフォーム(携帯、ラップトップ、PDA等)による利用を促進する標準メカニズムを介して、ネットワーク上でのアクセスが可能である。

リソース・プーリング:

プロバイダのコンピューティングリソースは、マルチテナントモデルを利用する複数の利用者には供給され、その物理・仮想リソースは利用者の需要に応じて動的に割り当てられる。一般的に顧客は、提供されるリソースの正確な位置は認識・管理せず、より抽象的なレベル(国、州、データセンタ等)で位置特定が可能であるように位置的に独立している感がある。リソースの例として、ストレージ、処理能力、メモリ、ネットワーク帯域幅、及び仮想マシンなどがある。

迅速な柔軟性:

素早いスケールアウトやスケールインにより、場合に応じて自動的に、迅速かつ柔軟に能力の提供が可能である。利用者にとっては、必要時に必要な量を購入することができることにより、無制限に提供されているように見える。

管理されたサービス:

クラウドシステムは、サービスの種別(ストレージ、処理能力、帯域幅、アクティブなユーザーアカウントの数等)に適したレベルでの能力測定により、リソースを自動的に管理し、最適な利用ができる。リソースの利用状況は監視・管理され、サービスのプロバイダと利用者双方に透明性のある報告が行われる。

サービスモデル:

SaaS:

プロバイダが提供するクラウド基盤上のアプリケーションを利用する形態のサービス。そのアプリケーションは様々なクライアントのデバイスからWebブラウザ(Webメール等)のようなシンクライアントのインタフェースを介してアクセスされる。利用者は、ネットワーク、サーバ、OS、ストレージ、または個々のアプリケーションを含めクラウド基盤の管理は行わない。ただし特定のユーザ向けアプリケーションの設定を除く。

PaaS:

プロバイダが提供するプログラム言語・ツールを用いてユーザ自身が開発・調達したアプリケーションをクラウド基盤上で動作させる形態のサービス。利用者は、ネットワーク、サーバ、OS、またはストレージを含めクラウド基盤の管理・制御は行わないが、導入したアプリケーションや、おそらくアプリケーションの動作環境構成は制御する。

IaaS:

利用者が OS やアプリケーションを含めた任意のソフトウェアの導入・運用を可能とする、処理能力、ストレージ、ネットワーク、及び他の基本的なコンピューティングリソースを提供する形態のサービス。利用者は基本的なクラウド基盤の管理は行わないが、OS、ストレージ、導入したアプリケーションや、おそらく選ばれたネットワークコンポーネント(ホストのファイアウォール等)も制限付きで制御する。

配備モデル:

プライベートクラウド:

1つの組織のために運用されるクラウド基盤。第三者によって運用される場合もあり、自社運用／社外運用がある。

コミュニティクラウド:

複数の組織によって共有されたクラウド基盤。共通の意識(ミッション、セキュリティ要件、ポリシー、コンプライアンス要件等)を持つ特定のコミュニティを維持する。第三者によって運用される場合もあり、自社運用／社外運用がある。

パブリッククラウド:

一般公衆または大きな産業団体によって利用されるクラウド基盤。1つのクラウドサービス提供事業者によって所有されている。

ハイブリッドクラウド:

2 つ以上のクラウド(プライベート、コミュニティ、またはパブリック)からなるクラウド基盤。それらのクラウドは各特性を残しつつ、データやアプリケーションの移行を可能にする標準的または固有の技術によって結び付けられている。(クラウド間の負荷分散のためのクラウドバースト等)

上述の定義のもとで、インタークラウドは、以下のように定義される。

サービス毎の性能、可用性などの品質要件の保証を目的に、各利用者のサービス品質要件とクラウド事業者毎のSLAの間を調整し、標準的なインタフェースを利用することで、異なるクラウド事業者のクラウドシステムとの間を連携してオンデマンドでのリソース融通やワークロードの移行を可能とするクラウドのモデル。

3 サービスに対する品質要件とクラウド事業者のSLA

3.1 サービスに対する品質要件とは

クラウド事業者がサービスの品質(QoS:Quality of Service)のレベルを保証しようとする場合、利用者のサービスに対する品質の要件を満たす必要があり、それは表1のようにサービス毎に複数の品質項目の組み合わせで多様にクラウド事業者へ提示される。その中で重視する品質項目もサービス毎に異なる。

例えば、下表における○×証明サービスではセキュリティを重視しているため、性能(レスポンス)や通信品質の保証よりは、日本の法規遵守とFISMA Mediumの利用が優先され、他方、××追跡サービスではサービス利用者は即時対応に関心があるため、性能(レスポンス)の品質要件を優先して、クラウド事業者へ要求することになる。

表 1 サービス毎の品質項目の例

アプリケーション処理とそれ以外(ネットワーク遅延等)を含めたEnd to Endのレスポンス。サービス毎の特性に応じて設定する。例えば、即時対応重視型では処理が軽く反応が早いなど。

品質項目	○×証明サービス (セキュリティ重視)	△□協働サービス (監査重視)	××追跡サービス (即時対応重視)	...
可用性(稼働率)	99.9%	99.5%	98%	
性能(レスポンス)	5s	1s	0.1s	
通信品質	ベストエフォート	帯域保証	ベストエフォート	
セキュリティ	FISMA Medium	—	—	
監査	—	SAS 70 Type II	—	
コスト	☆☆☆	☆☆☆☆☆	☆	
法令順守	日本法	EU法	—	
⋮				

3.2 クラウド事業者におけるSLAとは

クラウド事業者はサービスの品質保証の指標となるSLA(Service Level Agreement)を規定する。表2はSLAの項目例を示す。SLAの内容は事業者毎に異なる。

表 2 SLA(Service Level Agreement)項目の例

SLA項目		
可用性	サービス稼働率 稼働率	サービスを利用できる確率 ((計画サービス時間-停止時間) ÷ 計画サービス時間)
	平均復旧時間	障害発生から修理完了までの平均時間 (修理時間の和 ÷ 故障回数)
	サービス中断時間	想定できる障害からの業務継続対策(クラスタ構成等)ありの再開時間 ディザスタリカバリ時に、どれくらいで復旧させるかの目標
	データリカバリ復旧時点時間	障害発生時のデータをどこまで復旧するか
性能	オンライン応答時間	オンライン処理の応答時間
	オンライン応答時間遵守率	目標時間内に完了したオンライントランザクションの割合
	バッチ処理時間	バッチ処理の応答時間
	バッチ処理時間遵守率	目標時間内に完了したバッチ処理の割合
	単位時間あたり最大処理件数	単位時間あたり最大処理件数
	単位時間あたり最大処理件数遵守率	単位時間あたりの最大処理件数が目標を達成した割合
セキュリティ	事業者セキュリティ基準取得状況	情報セキュリティ基準「ISMS認証基準 (Ver.2.0) ISO27001」を取得しているか
	管理権限を持つ主体の認証実施状況	攻撃者が管理権限を手に入れることによる情報漏洩の脅威への対策有無
	管理システム上の対策における操作制限状況	情報漏洩の元となる不正ソフトウェアのインストール、不要アクセス経路設定防止のためのアクセス制限有無
	クラウドシステム間の伝送データ秘匿	クラウド間で伝送されるデータ秘匿有無
	データ配置場所	データの国内配置
	不正行為検知のためのログの取得状況	不正アクセス発生を検知し、その後の対策のためのログが取得できるか
	不正行為検知のためのログの保管期間	不正行為の確認、正しく処理された証跡保持期間
	不正通信遮断のための通信制御状況	踏み台攻撃等の脅威や情報の持ち出し抑止のための通信制御の実施有無
	DoD/DDoS攻撃回避のためのネットワーク輻輳対策状況	サービス停止攻撃の回避対策有無
	マルウェア対策の実施	マルウェア感染防止する対策の実施有無

4 インタークラウドの必要性和ねらい

電子行政、医療・金融などのミッションクリティカルな分野にもクラウドシステムによるサービスを適用するためには、End to Endでのサービス品質保証、コンプライアンスなどの信頼性、あるいはクラウドシステムの省電力化などの要求に応えていくことが不可欠である。

しかしながら、クラウドシステムへの想定外の過負荷や自然災害などの発生により予備のリソースが必要となった場合に、シングルクラウドが保有する利用可能な予備リソースには限りがあることから、安定的なサービス継続が困難になることが考えられる。そのような場合においてもサービスの可用性や性能などの品質要件を保証するためには、インタークラウドにより、リソースを相互に融通しあう仕組みを提供することが必要になると考えられる。特に中小企業が構築するプライベートクラウド等は、仮想化技術によりぎりぎりまでサーバが集約され、急激な負荷変動を想定した設備設計が考慮されないことが想定されるため、一時的に他クラウドシステムと連携する重要性は高くなる。

実際に、インタークラウドを市場のクラウドシステムに適用する際は、End to Endでのサービス品質保証(性能、可用性など)、サービス連携による利便性といった要求に応えることが重要となる。以下に、それぞれの要求事項について説明する。

4.1 End to Endでのサービス毎の品質保証

4.1.1 性能保証

サービスを提供しているクラウドシステムに対して、想定外の急激なトラフィック増加などが発生し、クラウドシステムへの過負荷により性能が低下するような事態においても、自律的に利用者の要求を満たすSLAを持つ事業者を適切に選択し負荷分散などを行うことにより、利用者にとってのサービスの性能(レスポンスなど)を保証すること。また、優先度の低い処理のワークロードを一時的に他クラウドシステムへ退避して、優先度の高い処理の性能を保証すること。

4. 1. 2 可用性保証

災害による被害で、クラウドシステムが提供するサービスの継続性に影響を及ぼした際に、被災エリア外のクラウドシステムと連携してサービス復旧(ディザスタリカバリ)を行うことにより、被災前と同様にサービスを提供することでサービスの可用性を保証すること。また、全てのサービスの品質要件を保証して復旧することが困難な場合は、優先度の高いサービスの品質を保証しながら、低い優先度のサービスにはベストエフォートで一部の品質要件を満たすような、サービス毎の優先度に応じて復旧できることも重要である。

4. 2 サービス連携による利便性

サービス連携による利便性とは、パスポート申請のように、複数の手続きを踏む必要があるような場合に、申請サービスと全ての関連手続きサービスを利用者からワンストップサービスとして見えるように連携することで、利便性を高めること。

また、上記の要求事項以外にもインタークラウドを適用するケースとして、サービス利用者の要請や事業の停止などによりサービス自体を他のクラウドシステムへ移行するケース、またはサービスを利用する際に仲介業者(ブローカー)が利用者とクラウド事業者の間に介在にして市場取引が行われるといったケースが考えられる。

5 インタークラウドによるユースケース

クラウドシステムを電子行政、医療・金融などのミッションクリティカルな分野へ適用するには、End to Endでのサービス品質保証などの要求事項をインタークラウドで応えることが重要となる。

本節では、これらの要求事項を満たすために複数のクラウドシステムが連携するユースケースと、各ユースケースでのクラウドシステムの動作について示す。

5.1 End to Endでのサービス品質保証

5.1.1 性能保証

－ 急激な負荷増加に対して性能を保証するユースケース

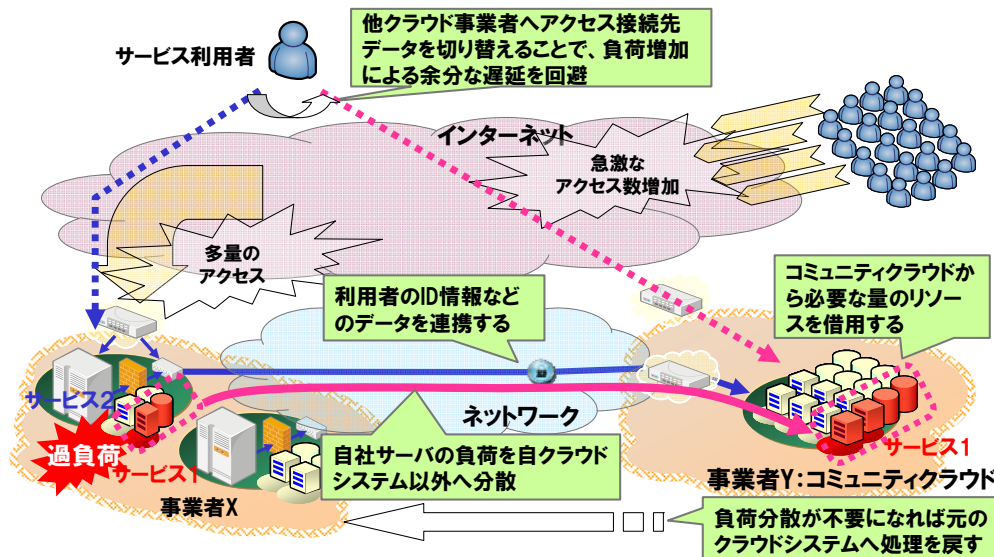


図 1 急激な負荷増加に対して性能を保証するユースケース

サービスの利用者は、インターネット経由で事業者 X のクラウドシステムが提供しているサービス1の WEB サービス(WEB 通販サイトなど)へログインしていたが、あるポータルサイトの広告などを契機に他の利用者からのアクセスが増大し、サービス1への負荷が増加した。

そのため、クラウドシステムは自律的に負荷増加によるサービス1の性能低下を判断し、クラウド事業者 Y が提供するコミュニティクラウドからリソース(WEB サーバなど)を借用、コミュニティクラウドとの間で利用者の ID 情報やアプリケーションなどのデータを転送し、利用者からサービス1へのアクセスのみを切り替えることで、負荷の分散を行った。そのことにより利用者は、同一のログイン ID を利用して、アクセス先変更を意識せず、同様の性能での WEB サービスが利用可能となる。また、サービス1が巨大なDBを持ち大量アクセスが発生しているような状況では、上記のようにサービス1を他のクラウドシステムへ分散することが困難なため、サービス2を分散することでサービス1の性能を保証することも考えられる。

ー 遅延に対して性能を保証するユースケース

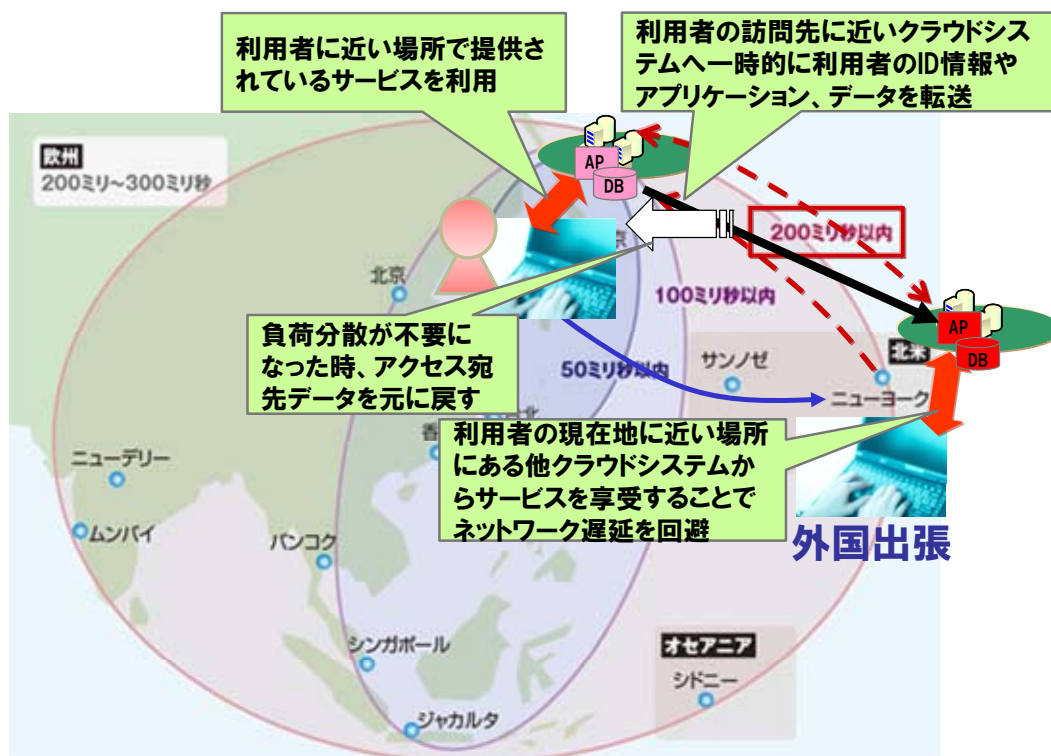


図 2 遅延に対して性能を保証するユースケース

あるクラウドシステムが提供するサービスの利用者が遠隔地のロケーションへ移動(海外出張など)した。それまでのサービスの拠点からの物理的距離が長くなることで(ネットワーク遅延の増大)、利用者にとってはサービスの応答性能が低下する。

クラウドシステムが応答の性能低下を検出し、移動先でも同じサービスをそれまでと同様の性能で提供するために、移動先に近い拠点のクラウドシステムからリソースを借用し、利用者の ID 情報やアプリケーション、データなどを転送することで、利用者は移動先に近い拠点から提供されたサービスが利用できる。そのことにより利用者は、一時的に同一の ID による同様の性能のサービスが利用可能となる。

5.1.2 可用性保証

－ 災害や大規模故障発生に対して可用性を保証するユースケース

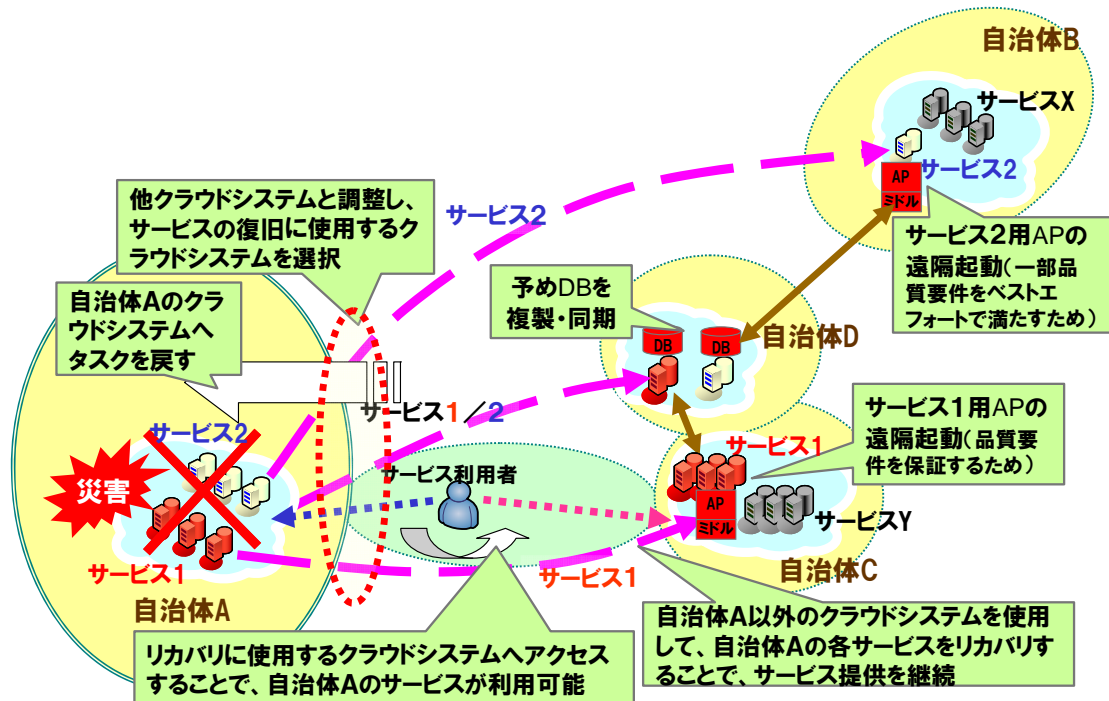


図 3 災害や故障発生に対して可用性を保証するユースケース

自治体Aのクラウドシステムが自然災害を被災し、自治体Aが提供しているサービスの継続が不可能となった。

そのため、自律的に災害発生による影響を調べ、サービス継続不可を判断し、あらかじめサービスの復旧(リカバリ)先となっている遠距離の自治体B、C、Dのリソース(アプリケーション、ミドルウェア、DBサーバなど)を利用し、ディザスタリカバリを行う。そのことにより、通常自治体Aにより提供されていたサービスが一時的に他の自治体から提供され、利用者はサービスを継続して利用可能となる。リカバリを行うに際し、全てのサービスの品質要件を保障するのに必要なリソース量が膨大な場合に、サービス1のようにサービスの品質要件の保証を最優先とするようなサービスは、品質要件の保証が可能な自治体でのリカバリを行い、サービス2のように一部品質要件をベストエフォートとしても早期復旧を優先とするサービスは、早期復旧が可能な自治体でのリカバリを行う。

5. 2 サービス連携による利便性向上

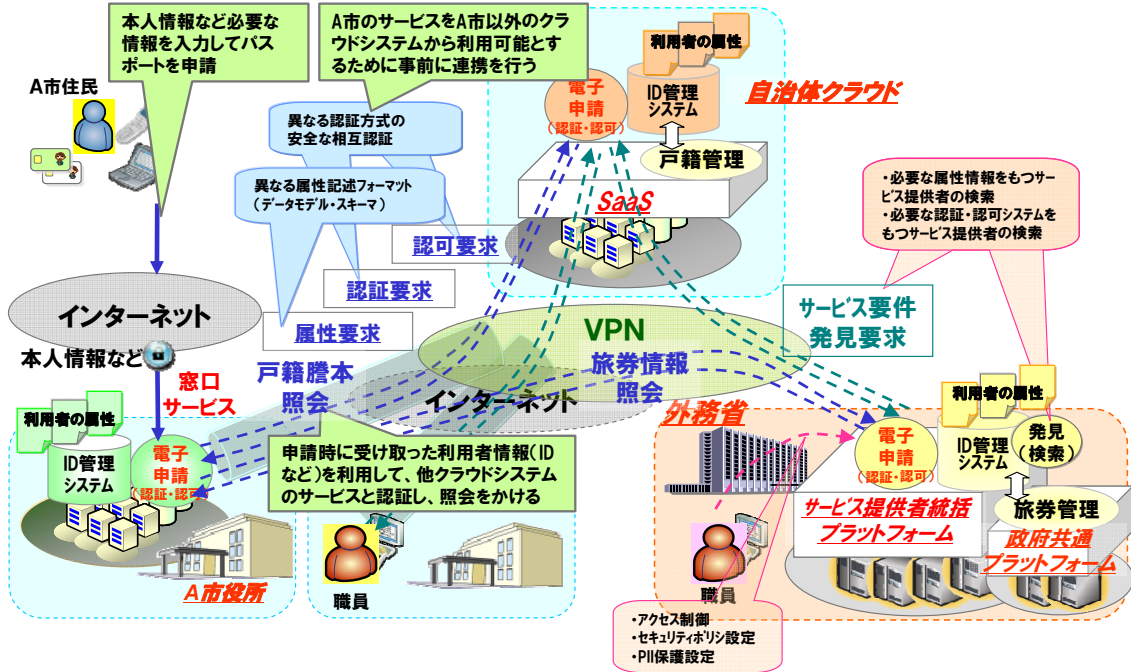


図 4 サービス連携により利便性を高めるユースケース

A市の自治体が提供する電子申請サービスは、ID情報やセキュリティ基準を調整する交渉により、他事業者のサービス(自治体クラウドの戸籍管理サービスや中央省庁の旅券管理サービスなど)との連携動作を予め可能としていた。

A市の住民が、自治体Aの提供する電子申請サービスを利用してパスポート申請などを行う際、申請に必要な情報(本人情報など)が投入されると、入力情報はアプリケーションへ入力する利用者のID情報を認証し共有するために他クラウドシステムのサービス(戸籍管理や旅券管理など)へ転送され、情報の取得や照会が行われる。そして、連携したサービスの利用結果を利用者へ提供することで、利便性が向上したワンストップサービスが利用可能となる。

5.3 サービス継続

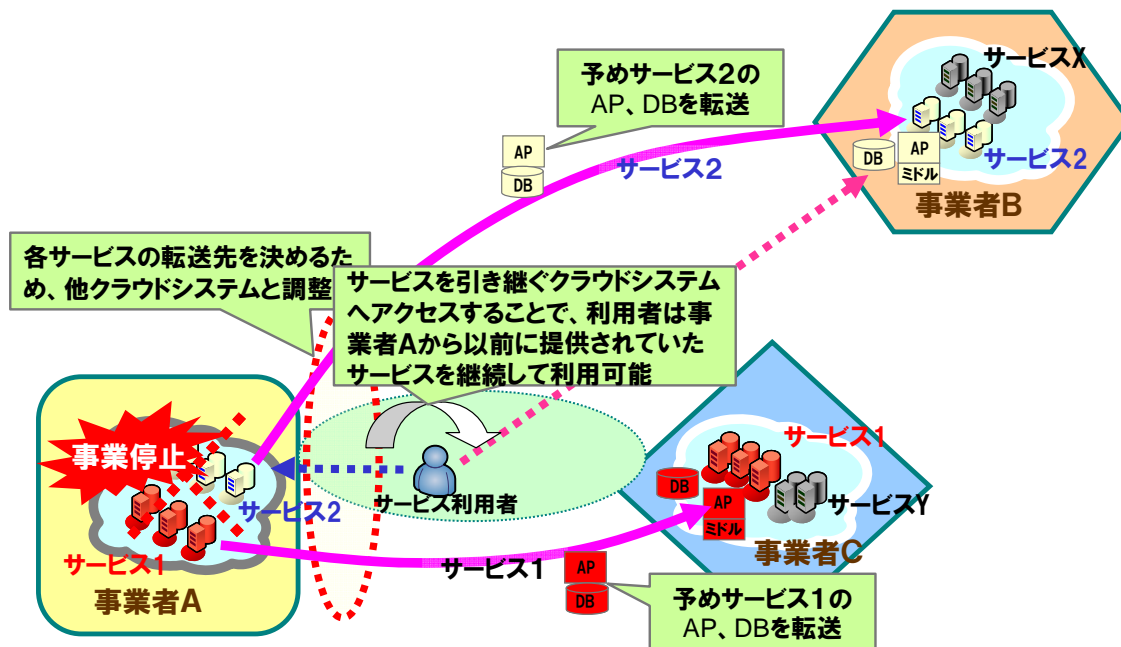


図 5 サービスを継続するユースケース

サービス提供事業者Aの事業が停止してしまうと、利用者が同じクラウドサービスを利用するには、他事業者が提供する同種のクラウドサービスに再度利用者登録などが必要となる。

そのような状況を回避するため、あらかじめ事業者Aの提供しているリソース、アプリケーション、利用者のID情報などを事業者B、Cのクラウドシステムへ転送する。これにより、利用者は事業者Aの事業の停止においても、事業者B、Cから同様のサービスを継続して利用可能となる。また、サービス利用者がサービス移行を要求するときにも適用できる。

5.4 ブローカー介在による市場取引

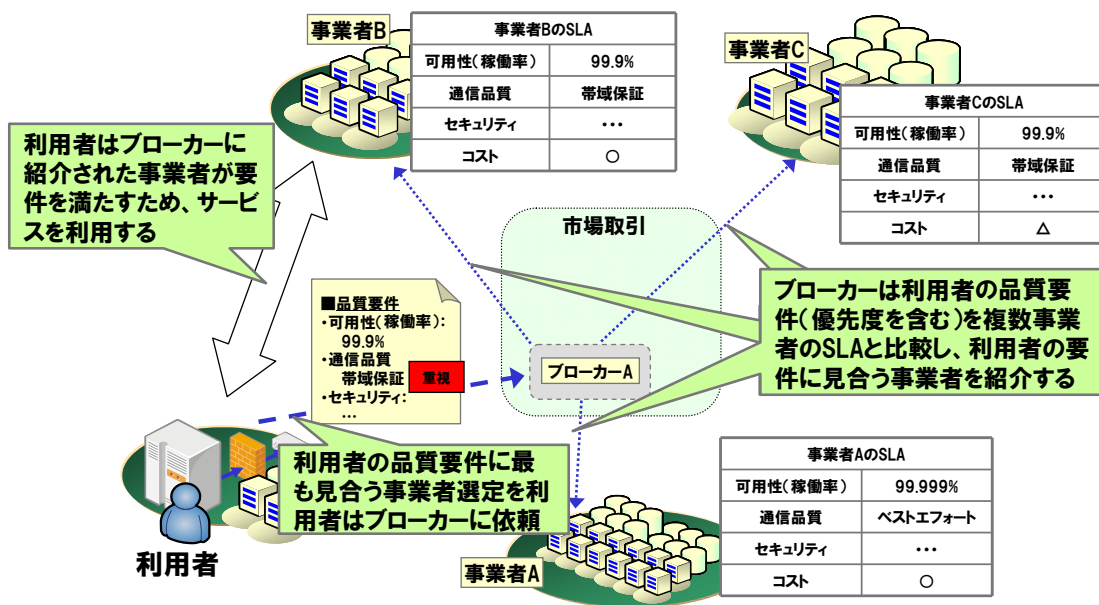


図 6 ブローカー介在による市場取引

利用者がクラウドシステムのサービスを利用する際は、利用者が提示するサービスの品質要件と複数事業者のSLAを比較して、適した事業者のクラウドシステムを選択する必要がある。

そのため、利用者は求めるサービスの品質要件をブローカーAに提示し、ブローカーAから利用者の品質要件に見合うSLAを持つ事業者Bの情報を提供してもらうことで、最も品質要件に見合ったサービスを利用することが可能となる。利用者は、ブローカーにより提供された事業者の一覧から利用するクラウド事業者Bを選定し、サービスを契約する。

6 インタークラウドのユースケースにおける手順

本節では、前掲のユースケースの中でインタークラウドを利用するために、それぞれのクラウドシステムに求められる手順を示す。

6.1 クラウドシステム間の連携により、性能を保証する手順

5.1.1 項に挙げているユースケースでは、各サービスのトラフィック量や TAT(Turn Around Time)などのリソース使用状況をクラウドシステムが監視し、サービスの性能低下によって負荷分散が必要と自律的に判断した場合に、負荷分散のためのリソースを自もしくは他クラウドシステムから確保し、動的にサービスリソースを再構成する。確保したリソースは監視され、負荷分散の必要がないと判断した時に解放される。

以下は、初期構成のシングルクラウドシステムでサービスを提供するところから始まり、他のクラウドシステム上にリソースを確保し、そのリソースが必要なくなって解放するまでのライフサイクルの手順(a) ~ (d) を例示している。インタークラウドに関わるクラウドシステムの各手順の動作概要を以下に説明する。概要には対応する 7 章の節番号を記載する。

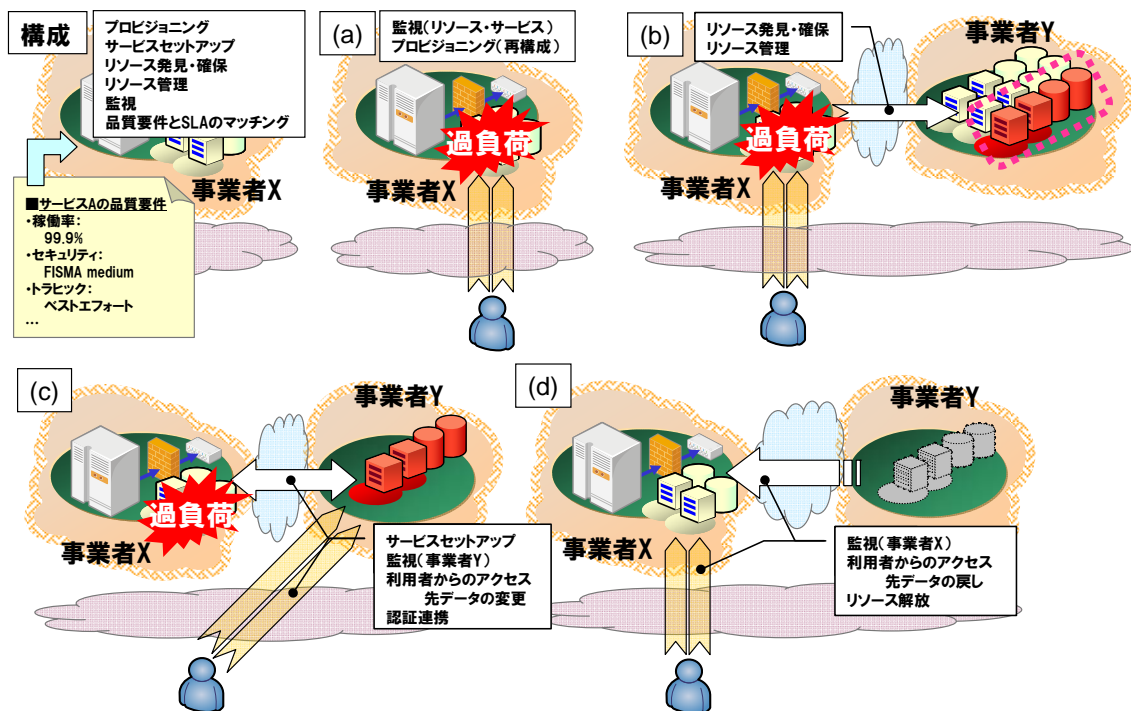


図 7 クラウドシステム間の連携により、性能を保証する手順と機能

初期構成

[プロビジョニング] シングルクラウドにおける初期構成に必要なリソース要件を求める

[リソース発見・確保] プロビジョニングにより必要とされる利用可能なリソースを検索し、確保する

[リソース管理] シングルクラウドシステムが、確保したリソースを各サービスのリソース構成情報として管理する

[サービスセットアップ] 確保したリソースの起動及びネットワークを含めた接続などを行う

[監視] クラウドシステムの監視(リソース・サービス・死活)を開始する

[サービス利用者の品質要件と SLA のマッチング] 各サービスへの利用者のサービス品質要件とクラウドシステムの SLA を比較し、リソースの確保先候補となるクラウドシステムを予め選択する【7.1 項】

・以下の図では、品質要件の形状がSLAの形状に含まれるもしくは一致する場合にマッチングした(品質要件を満たした)とする(品質要件、SLAの形状の違いは、サービス毎、事業者毎の品質項目、SLA項目の違いを表している)
 ・マッチングした場合でも、品質要件とSLAの形状の差分が大きいほど余剰なSLA項目が含まれることを意味する

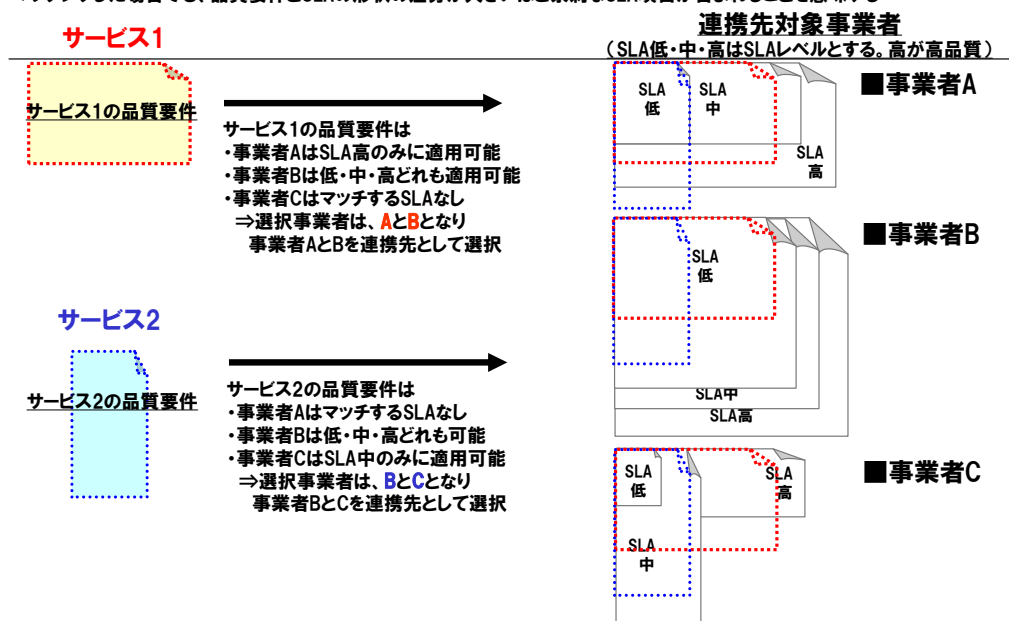


図 8 品質要件と SLA のマッチングの概念図

手順 (a)

[リソース監視] コンピューティングやネットワークのリソース使用状況を収集する【7.2 項】

[サービス監視] 各サービスの性能を監視し、それを元にサービスの性能低下による負荷分散が必要かどうかを、自律的に判断する【7.2 項】

【急激なアクセス増加などによるサービスへの過負荷が発生】

[プロビジョニング] 負荷分散するためのリソース再構成に必要なリソースを求める【7.3 項】

手順 (b)

[リソース発見・確保] 自クラウドシステムに対して、プロビジョニングにより必要とされる要件の利用可能なリソースを検索し、リソースを発見した場合は該当のリソースを確保する【7.4 項】

[リソース発見・確保] リソース要件の全部もしくは一部が自クラウドシステムで発見できない場合は、品質要件とSLAのマッチングにより選択された他クラウドシステム群に対して同様に動的な検索を行い、利用可能なリソースを発見・確保する【7.4 項】

[リソース管理] 他のクラウドシステムから確保したリソースを含め、サービスのためのリソース構成情報を更新する【7.5 項】

手順 (c)

[サービスセットアップ] 確保したリソースの起動及び接続などを行い、負荷分散のためにクラウドシステム間でワークロードを移行する【7.6 項】

[監視(事業者 Y)] リソースを確保したクラウドシステムの監視(各リソース状態・各サービス状態・死活)を開始する【7.2 項】

[認証連携] リソースを確保する前と同じ条件で利用者がサービスを利用できるようにするために、クラウドシステム間で ID 情報やデータを連携する【7.7 項】

[接続先データの変更] 利用者からのサービス接続先データを、当初のサービス接続先からリソースを確保した他のクラウドシステムに変更する【7.9 項】

手順 (d)

[監視(事業者 X)] 連携したクラウドシステムを含めた各サービスの性能を監視する【7.2 項】

【 負荷分散によりサービスへの過負荷が収束 】

[サービスアクセスデータの戻し] 負荷分散が不要となった場合は、ワークロードやデータを元のクラウドシステムへ戻し、利用者からのサービス接続先データを当初のサービス接続先データに戻す【7.9 項】

[リソース解放] 戻しにより不要となったリソースの解放やデータクリアを行う【7.10 項】

上記の手順は、クラウドシステム間の連携モデルを用いて示したものであるが、これを 5.1.1 項のユースケースに以下のように当てはめることにより、以下の (a) ~ (d) のような手順として対応させることができる。

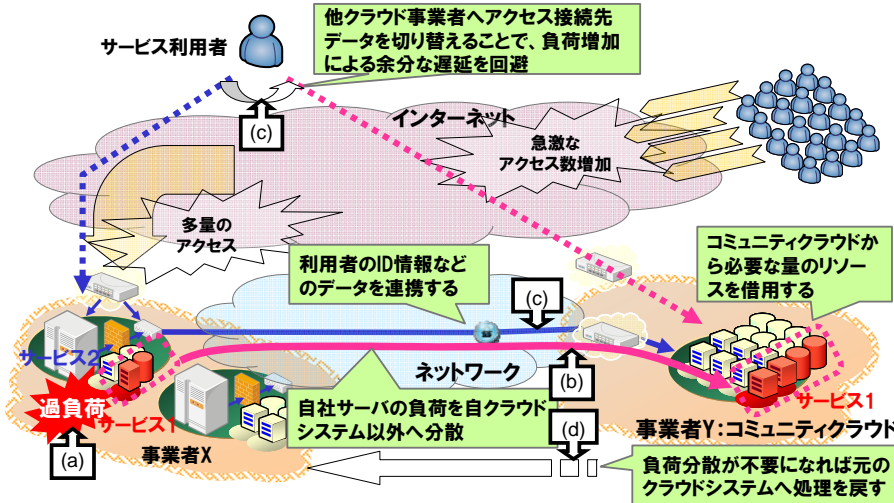


図 9 負荷増加に対して性能を保証する手順

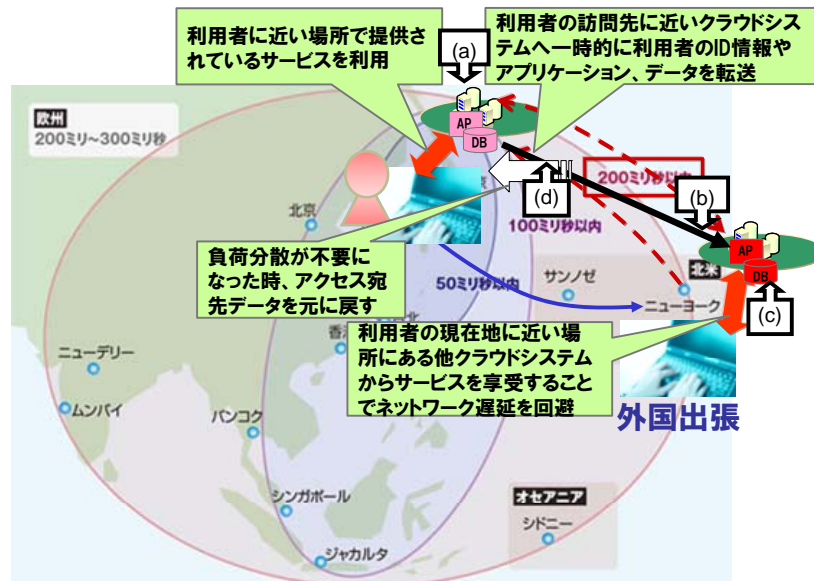


図 10 ネットワーク遅延に対して性能を保証する手順

6. 2 クラウドシステム間の連携により、サービスを復旧し可用性を保証する手順

5.1.2 項に挙げているユースケースでは、災害発生によりクラウドシステムのサービス提供の継続が不可能となった場合に、そのクラウドシステムは他クラウドシステムと連携してディザスタリカバリを行う。また、ディザスタリカバリ後に、被災した元のクラウドシステムからのサービス提供が再開可能となった際は、元のクラウドシステムへ負荷が戻される。

ディザスタリカバリでは、データの復旧規模も大きいことが考えられるため、効率的な復旧のために予めディザスタリカバリのためのバックアップ先を設定し、そのクラウドシステムに定期的なバックアップをすることが重要である。また、被災したクラウドシステム自身による自律的な復旧が不可能な場合(システムが全壊した場合)も考えられることから、被災したクラウドシステムがサービス復旧できないことを他クラウドシステムが検出し、検出した他クラウドシステムが代理としてリカバリ動作を統制し、サーバ・ストレージ、ネットワークのリソース確保などを行うことも重要となる。

以下に、シングルクラウドシステムが初期構成でサービスを提供開始するところから、他クラウドシステム上に確保したリソースを利用してクラウドサービスを復旧し、罹災したクラウドシステムが修復後に自リソースでサービス提供を再開するライフサイクルの手順(a) ~ (d) を図示し、インタークラウドを含むクラウドシステムの各動作手順の概要を説明する。概要には 7 章の対応する節番号を記載する。

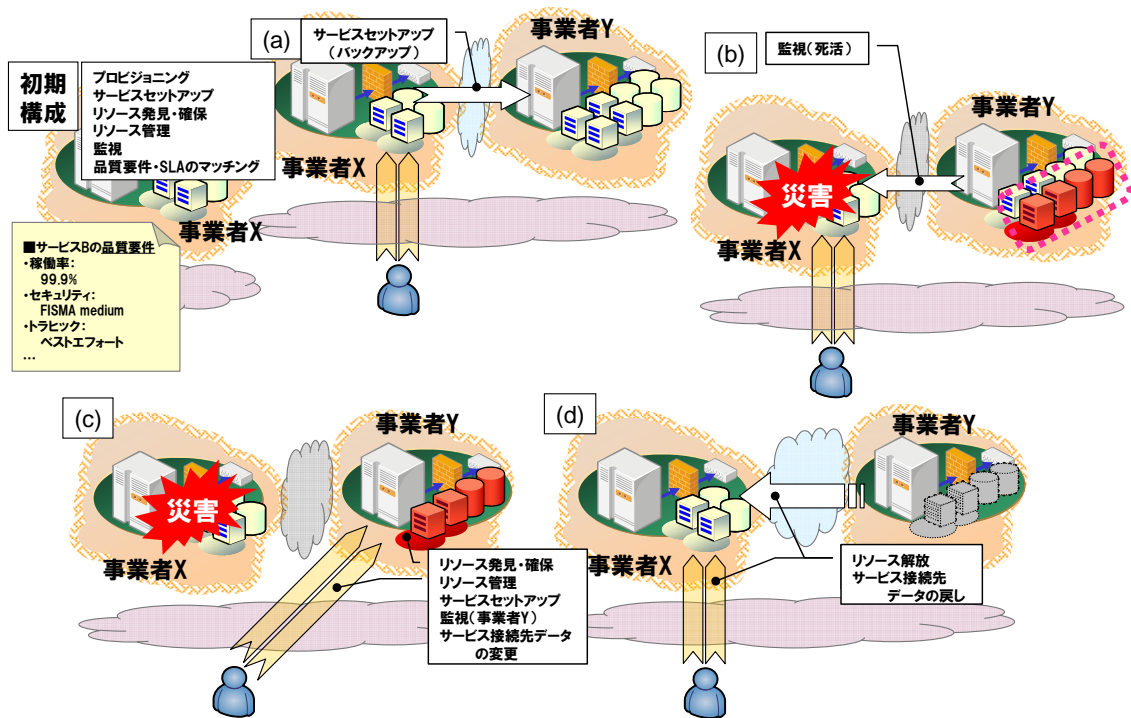


図 11 クラウドシステム間の連携により、可用性を保証する手順と機能

初期構成

[プロビジョニング] シングルクラウドにおける初期構成に必要なリソース要件を求める

[リソース発見・確保] プロビジョニングにより必要とされる利用可能なリソースを検索し、確保する

[リソース管理] シングルクラウドシステムが、確保したリソースを各サービスのリソース構成情報として管理する

[サービスセットアップ] 確保したリソースの起動及びネットワークを含めた接続などを行う

[監視] クラウドシステムの監視(リソース・サービス・死活)を開始する

[サービス利用者の品質要件と SLA のマッチング] 各サービスへの利用者のサービス品質要件とクラウドシステムの SLA を比較し、ディザスタリカバリを代理で統制するクラウドシステム、リカバリ時に必要となるリソースを確保するクラウドシステム、またはデータのバックアップ先となるクラウドシステムを予め選択する【7.1 項】

手順 (a)

[セットアップデータバックアップ] サービスの復旧に必要なデータなどを事前にクラウドシステム間でバックアップする【7.6 項】

手順 (b)

[監視(死活)] リカバリを統制するクラウドシステムは災害や大規模故障の発生によりディザスタリカバリを必要とする状況かをサービス毎に監視し、自律的にディザスタリカバリ開始を判断する【7.2 項】

【 災害発生により被災し、クラウドシステム上の全サービスが提供不可 】

手順 (c)

[リソース発見・確保] 災害を罹災したクラウドシステムの代理でリカバリを統制するクラウドシステムは、自クラウドシステムに対して、リカバリに必要な利用可能なリソースを検索し、リソースを発見した場合は該当のリソースを確保する【7.4 項】

[リソース発見・確保] 必要なリソースの全部もしくは一部が自クラウドシステムで発見できない場合は、利用者の品質要件と SLA のマッチングにより選択されたリカバリ時のリソース確保先となっている他クラウドシステム群に対して同様に検索を行い、確保可能なリソースを発見・確保する【7.4 項】

[リソース管理] 罹災クラウドシステムの代理でリカバリの統制を行うクラウドシステムは、ディザスタリカバリにより復旧したサービスのリソース構成を管理する【7.5 項】

[サービスセットアップ] バックアップしたデータにアクセスし、確保リソースの起動及びネットワークへの接続などを行い、各サービスを提供する【7.6 項】

[監視(事業者 Y)] 代用となったクラウドシステムの監視(リソース・サービス・死活)を開始する【7.2 項】

[接続先データの変更] 利用者からのサービス接続先データを、リカバリによって代用となったクラウドシステムに変更する【7.9 項】

【 被災したクラウドシステムが復旧しサービスが再開可能 】

手順 (d)

[サービスアクセスデータの戻し] 罹災したクラウドシステムがサービス提供能力を回復した場合は、代用

のクラウドシステムから運用中のデータ・ワークロードなどを引き継いでサービス提供を再開する。また、利用者からのサービス接続先データを当初のサービス接続先データに戻す【7.9 項】

【リソース解放】回復により不要となったリソースの解放やデータクリアを行う【7.10 項】

上記の手順は、クラウドシステム間の連携モデルを用いて示したものであるが、これを 5.1.2 項のユースケースに以下のように当てはめることにより、以下の (a) ~ (d) のような手順として対応させることができる。

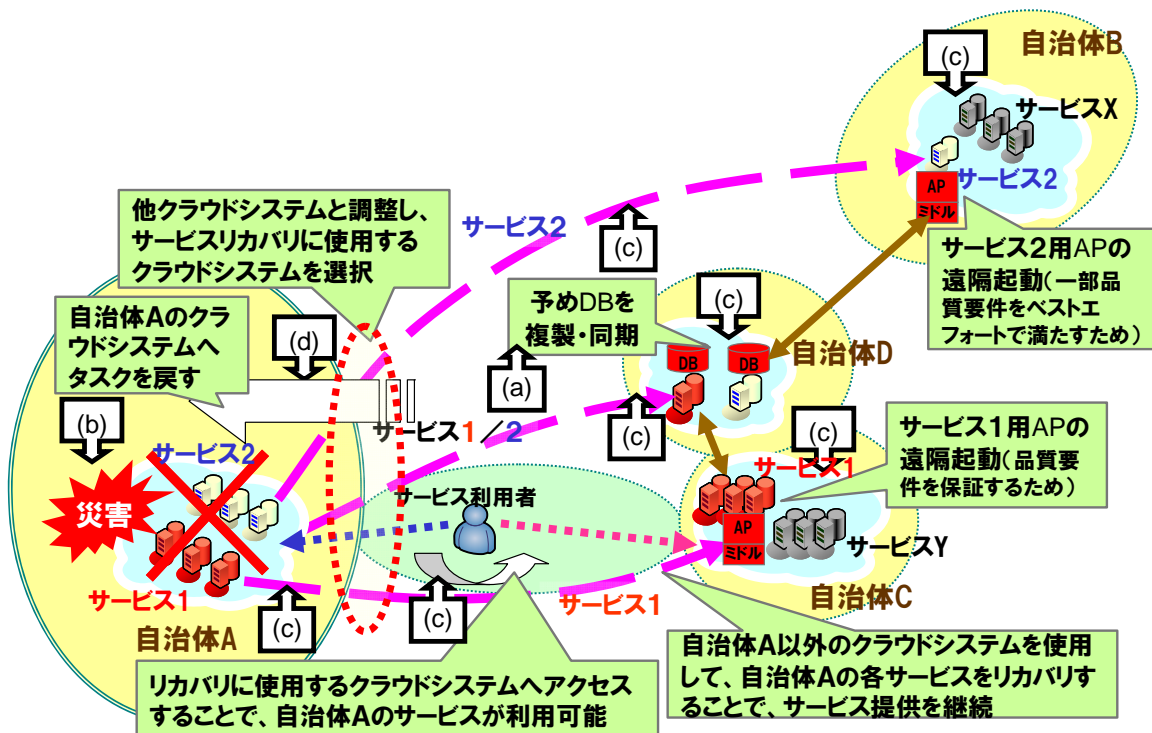


図 12 災害や故障発生に対して、サービスを復旧し可用性を保証する手順

7 インタークラウドの機能要件

本節は、前節で述べた各手順を実行するための要件を、10の機能に分けてまとめる。

7.1 サービス利用者の品質要件とSLAのマッチング

本機能は、サービスの性能低下や災害発生などにおいても他クラウドシステムと連携し、サービスの品質要件を保証するために、サービスの品質要件とクラウド事業者のSLAの内容をマッチングし、利用者の品質要件を満たして連携動作を可能とするクラウド事業者及びクラウドシステムを選択する。

以下に、利用者の品質要件とクラウドシステムのSLAのマッチングを行なうための機能要件を挙げる。

- ・ クラウド事業者やブローカーが利用者の品質要件と他クラウドシステムのSLAを比較するため、対象となるクラウドシステムのSLAは他クラウドシステムに対して標準的な様式を利用して提供(公開や配布など)すること
- ・ サービスの品質要件の項目と、他事業者が提供するクラウドシステムのSLAを比較(一致や許容範囲)することにより、連携先として適切なクラウド事業者が選択できること
- ・ 他クラウドシステムが保有しているアプリケーションやミドルウェアを含むリソースが検索できること
- ・ SLAのマッチング後に、事業者方針の変更などによりクラウドシステムのSLAが変更された場合、その変更を他のクラウドシステムが検知できるようにすること

7.2 監視(リソース、サービス、死活)

本機能は、クラウドシステム上のコンピューティングリソースやネットワークリソースの使用状況や死活情報などを収集、監視し、サービス品質状況や死活状況の監視を行い、負荷分散やディザスタリカバリの必要性を判断する。

以下に、リソースやサービス、死活に関する状況の監視を行うための機能要件を挙げる。

- ・ 各サービスの性能の監視し、各サービスの性能維持のために負荷分散の要否を判断するために、各サービスを運用している自もしくは他クラウドシステムの各サービスのリソース情報(サーバ・ストレージやネットワークの性能情報、稼動情報など)を周期的もしくは要求ベースで収集できること

- ・ 自然災害発生時における、各サービスの死活状況の監視し、災害による罹災の程度によりディザスタリカバリを行うために、自もしくは他クラウドシステムのリソースの死活情報を周期的もしくは要求ベースで収集できること
- ・ クラウドシステム間を跨ったサービスの監視を行うために、リソース監視情報(性能情報、稼動情報、死活情報)が収集でき、連携するクラウドシステム間で共通に定義された監視情報フォーマットにより、他のクラウドシステムと相互に交換ができること
- ・ サービスのセキュリティ条件を設定でき、クラウドシステム外部からクラウドシステム内部への、またはクラウドシステム内部からクラウドシステム外部への攻撃が監視でき、対処可能なこと

7.3 プロビジョニング

本機能は、サービスの品質要件に基づいてリソース要件(量や種別など)を求め、サービスの性能低下の検出時にサービスの性能を維持するためのリソース再構成に必要なリソースを求める。

以下に、サービスの提供・性能維持のプロビジョニングについての機能要件を挙げる。

- ・ 使用するアプリケーション毎に動作特性は異なるため、ネットワークのトラフィック負荷が変動したときのボトルネックを把握し、適したプランニングができること
- ・ クラウドシステムの初期リソース構成を決定するためのプロビジョニングと、サービスの性能維持のために動的再構成をするプロビジョニングとでは、リソース要件の精度や決定にかかる時間の条件が異なるため、精度重視や即応性重視など様々なプランニングを可能とすること

7.4 リソース発見・確保

本機能は、自クラウドシステムもしくはSLAマッチングによってリソース確保の対象となる他クラウドシステムに対して、リソース要件(量や種別など)を満たす確保が可能なリソースを検索・発見する。また、発見した確保可能なリソースを持つクラウドシステムに確保を要請し、リソースを確保する。

以下に、確保可能なリソースの発見と選択したクラウドシステムから確保を行うための機能要件を挙げる。

- ・ サービスの性能低下もしくは災害発生時に、サービスの性能維持や災害復旧のためのリソース確保先候補として選択されたクラウドシステム群に対して、利用可能なリソースを検索し、発見できること

- ・ リソースの第一検索先は自クラウドシステムとして、自クラウドシステムに見つけられない場合に他クラウドシステムへ検索できること
- ・ 他クラウドシステムのサーバ・ストレージをLANや広域ネットワークで接続する必要があるため、サーバ・ストレージリソースとネットワークリソースが一緒に確保できること
- ・ サーバ・ストレージ、ネットワークなど連携のためのリソースの大半は同時に確保する必要があり、他のクラウドシステムとのリソース確保の重複を防ぐ必要があるため、全てのリソース確保が終わるまでリソースの仮押さえ(予約)を可能とすること
- ・ サービス毎に異なる重視する品質項目に基づいたリソース確保を可能とすること。例えば、遅延が重要ならばまず利用者から近いサーバを確保し、次にネットワーク条件を確保する。逆に帯域容量が重要ならば、帯域容量が十分なネットワーク確保を優先し、次にネットワークと接続されているサーバを探す
- ・ 大規模災害時の災害復旧には莫大なリカバリ用のリソースを必要とするが、必ずしも必要リソースが確保できるとは限らないため、リカバリの優先度(早期復旧優先、品質要件保証など)に応じたリカバ리를可能とする仕組みが必要。例えば、ライフラインサービス用には強制的なリソース確保を可能とするなど

7.5 リソース管理

本機能は、各サービスのために自もしくは他クラウドシステムに確保したリソースの構成を管理する。

以下に、確保したリソースを管理するための機能要件を挙げる。

- ・ 複数クラウドシステム間に跨ったリソースを一元管理するために、リソースの種別や状態などの付加情報を標準的に表現できること
- ・ サーバ・ストレージとネットワークなど各サービスの様々なリソース構成を一元管理できること
- ・ 複数クラウドシステム間にまたがったリソースの構成情報を、クラウドシステム間のイベント(他クラウドシステムからのリソースの確保・解放など)に同期して更新できること

- ・ リソース構成に変更が生じた場合にその差分が分かるように、差分情報を管理すること(スナップショット等)

7.6 サービスセットアップ

本機能は、自もしくは他クラウドシステムに確保したリソースを利用可能するために、クラウドシステム間のネットワークを接続し、アプリケーションやミドルウェアの遠隔起動、データの移動やコピーなどを行い、サービス提供前のセットアップを行う。

以下に、確保したリソースを利用するための機能要件を挙げる。

- ・ 災害発生によりクラウドシステムが罹災した場合に利用するバックアップデータへのアクセスを可能とすること
- ・ 「7.4 リソース発見・確保」で述べた手順によって予約したリソース(VMやアプリケーション、ミドルウェア)を、遠隔起動ができること。その際は、リソースを確保した先のクラウドシステムの環境に依存する設定値を考慮して起動できること
- ・ 起動するVMやアプリケーション自体が選択したクラウドシステムにない場合は、コピーして起動できること
- ・ 「7.4 リソース発見・確保」で述べた手順によって確保したリソースとネットワークを通して接続ができること。必要に応じてセキュアなVLANやVPNを用いることができること

7.7 認証連携

本機能は、クラウドサービス間を連携する際に、利用者がシームレスにサービスを利用するための利用者IDやデータ連携などを行う。

以下に、クラウドサービス間で利用者IDやデータを連携するための機能要件を挙げる。

- ・ 異なるID管理方式で使用される多様な利用者情報の形式がサポートされていること
- ・ 異なるデータモデルやスキーマを使っているID管理システムと相互運用可能な機能を持つこと
- ・ 異なるID管理方式で構築されたクラウドシステムに跨るサービスに対する利用者が設定した認証または認可機関に発行された認証結果を、複数クラウドシステム間で信頼関係に基づく相互認証を可能とするための、シームレスかつ安全に利用可能な認証方式(仕様間のコンテキスト変換等)が提供できること

- 単一、あるいは複数のクラウドシステムにおけるサーバ間の信頼関係の管理機能が持てること
- 単独のクラウドシステム内のサービス利用者の ID 情報を検索できる機能が持てること
- 連携されたクラウドシステム間で、ID連携のために生成された情報の検索・発見・交換が行えること。ID管理のライフサイクル(作成・更新・解除)の管理に関するルールの生成とその実行を行うことができること。例えば、異なるクラウドを跨って管理された利用者情報の作成・更新・解約において、利用者本人あるいは本人より委任されたクラウド管理者の機能により、一斉同期、部分同期、同期解除等が行われるなど
- 異なる認証を行うクラウドシステム間の連携が行われた際、認証強度の同じサービス間ではシームレスな認証連携を行い、認証強度を変更する場合は、サービス利用者とクラウド事業者の双方の同意が取れること
- 一定のルールに従って利用者のPII(Personally Identifiable Information)の秘密保持ができること
- 無許可のアクセスから利用者情報を保護するためのアクセス制御機能が、ネットワーク機能やID管理機能にサポートされていること
- クラウドシステム間の認証連携サービス提供後の災害時の対処として、障害が発生したサービス管理サーバに対するバックアップ認証機能を同一クラウドシステム内あるいは連携クラウドシステム内に配備できること
- 他事業者環境でサービス提供を行う場合、利用者に認証環境の移行要否が確認できること
- 利用者に認証環境の移行をしてよいか確認する必要がない場合においても、移行前後の事業者間の信頼性、相互接続、保守運用、認証(シングルサインオン)が保証できるように利用者のアイデンティティ情報が管理されていること
- アイデンティティ情報を、クラウドシステムを用いて管理しサーバを跨って使用する場合(もしくは単一のサーバが複数機能をサポートする場合)、アイデンティティ情報を管理する機能間で認証情報を同期する手段により、認証情報の一貫性を保持できること

7.8 ネットワーク連携

本機能は、クラウドシステム間の連携をする際、クラウドシステムとネットワークとが連携することにより、より高品質のネットワーク能力を提供する。

以下に、クラウドシステムとネットワークが連携するための機能要件を挙げる。

- ・ サービス毎のフローを監視し、ネットワークの負荷状況に基づいて自律的にサービスのフローを変更することにより、ネットワークの安定運用ができること
- ・ ネットワーク機器のシャットダウンも考慮して、システム全体の節電効果が最大となるような省電力化ができること

7.9 利用者からのアクセスルートの変更と戻し

本機能は、災害発生やサービスの性能低下により、利用者が他クラウドシステムから提供されるサービスを利用するときに利用者からのサービス接続先データを他のクラウドシステムに変更し、元のクラウドシステムからのサービス提供が可能になった時、サービス接続先データを以前に戻す。

以下に、クラウドシステム間のサービス接続先の切り替え、戻しについての機能要件を挙げる。

- ・ 災害発生時に災害復旧を行い、リカバリを行った他クラウドシステムからサービス提供する場合、利用者が災害前と同様のサービス利用を可能とするため、利用者は何もせずとも、利用者が代用のクラウドシステムにアクセスできるようにネットワークに関するデータを変更できること
- ・ サービスの性能低下に対処するためフロントWebサーバの負荷を分散する場合においても、利用者が何もせずともサービスの接続先データを負荷分散に応じて変更できること
- ・ 災害を罹災したクラウドシステムが復旧したり、クラウドシステム間の負荷分散が必要なくなったときに、サービスを提供するクラウドシステムを以前のクラウドシステム戻すために、サービス接続先データに戻すこと

7.10 リソース解放

本機能は、ディザスタリカバリや負荷分散を行った後、監視結果から負荷分散やリカバリが不要であることを判断し、不要なリソースなどを解放する。

以下に、確保したリソースが不要となった場合に行う解放についての機能要件を挙げる。

- ・ 確保したリソースを利用開始した際に起動した VM やアプリケーションなどの停止やリソース管理情報の更新、移行したデータの完全消去もしくは回収を行えること。サーバ・ストレージのリソースの解放後は、接続したネットワークを解放できること。他クラウドシステムにワークロードが残っている場合は、ワークロードを回収もできること

8 インタークラウドにおけるクラウドシステムの機能構成とインタフェース

本節では、前掲した各機能の要件を満たすクラウドシステムの機能構成と、その機能構成に基づいてクラウドシステム間を連携するインタフェースの要件を示す。

8.1 機能構成

インタークラウドをサポートするクラウドシステムには、前節における監視やリソース発見・確保などの機能が必要となる。クラウドシステム間を連携する機能構成は、次にあげる機能エンティティによって構成することができる。

- (1) 利用者からのサービス品質要件を元にしてリソース要件を推論し、クラウドシステムを管理するリソースプランを識別する機能エンティティ
- (2) クラウドシステム間の連携をサポートし、クラウドシステムの監視・制御を行う機能エンティティ
- (3) クラウドシステムを構成するサーバ・ストレージリソースを制御・管理を行う機能エンティティ
- (4) クラウドシステムを構成するネットワークリソースを制御・管理を行う機能エンティティ

7節で述べた機能は機能エンティティの関連で図13のようにグループ化できる。

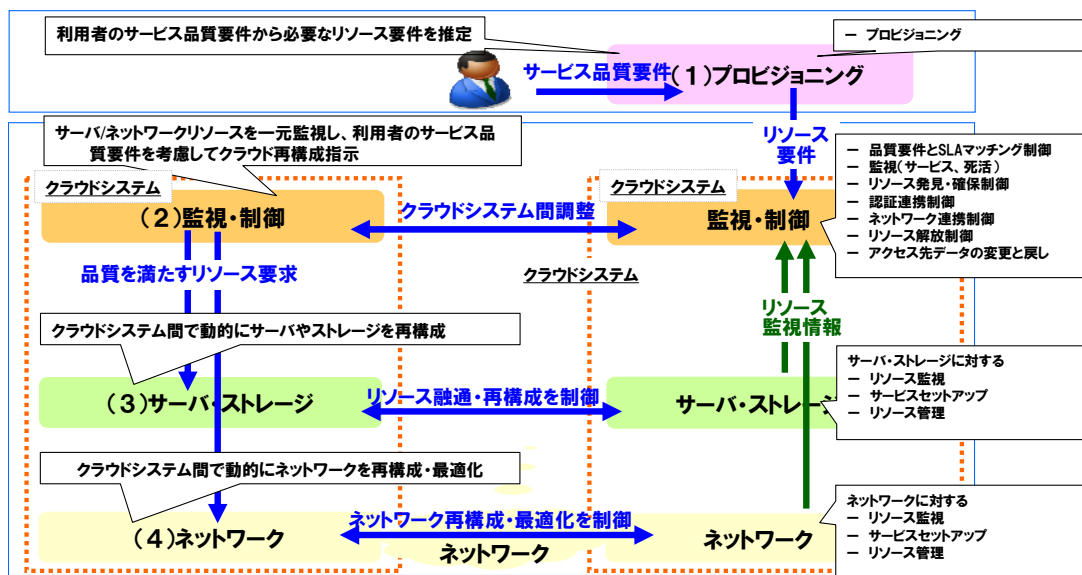


図 13 クラウド連携機能の機能エンティティのマッピングとエンティティ間の関係図

8.2 インタフェース

前掲の機能構成を基盤にクラウドシステム間を連携するには、クラウドシステム間およびクラウドシステム内の機能エンティティ間のインタフェースを用意する必要がある。

下表に、インタークラウドのクラウドシステムに必要となるインタフェースの要件を示す。表中の方向欄に記載されている(1)～(4)の数字は、図13の(1)～(4)に対応する。また、関連機能欄の記載は章番号に対応する。

表3 インタークラウドにおけるインタフェース要件

	インタークラウドにおけるインタフェース要件	方向	関連機能
1	リソース確保先となるクラウドシステムの選択などを行うために必要となるSLA情報を共有もしくは配布する	クラウドシステム間	6.1項
2	あらかじめ他クラウドシステムに対して、クラウドサービスの運用時のデータ(システムデータ、ユーザデータなど)をバックアップする	クラウドシステム間	6.6項
3	データのバックアップに必要となるクラウドシステム間のネットワークを接続・切断する	クラウドシステム間	6.6項
4	災害復旧やサービスの性能維持において、リソース要件に基づいて他クラウドシステムへリソース確保を依頼・解除する	クラウドシステム間	6.4項
5	リソース要件に基づいて、クラウドシステムにおけるサーバリソースのリソース確保(予約)と解除を依頼する	(2)⇔(3)	6.4項
6	リソース要件に基づいて、予約したサーバリソースと接続するネットワークリソースのリソース確保(予約)を依頼・解除する	(2)⇔(4)	6.4項
7	他クラウドシステムへ確保(予約)したリソース(サーバ・ネットワーク)に対して、使用開始・停止(解放)を通知する	クラウドシステム間	6.4項
8	クラウドシステム内に確保(予約)したサーバリソースに対して、使用開始・停止(解放)を通知する	(2)⇔(3)	6.4項
9	クラウドシステム内に確保(予約)したネットワークリソースに対して、使用開始・停止(解放)を通知する	(2)⇔(4)	6.4項
10	他クラウドシステムで使用したリソースのデータをクリアする	クラウドシステム間	6.10項
11	リソース確保を行ったクラウドシステムへリソース監視情報(監視項目等)を設定する	クラウドシステム間	6.2項
12	リソース確保を行ったクラウドシステム内のリソース監視情報の収集を開	クラウドシステム間	6.2項

	始する		
13	サービス利用者からクラウドサービスへのネットワーク接続の許可・禁止を 依頼する	(2)⇔(4)	6.6項
14	クラウドサービスの初期構成やサービスの性能維持のために必要となる1 つ以上のクラウドシステムのリソース要件を求める	(1)⇔(2)	6.3項

今後は、これらのインタフェースの規定を進めるが、GICTFとして独自のインタフェース仕様を定めるのではなく既存の標準化団体において検討されているインタフェース仕様(例として、OGFのOCCI、DMTFのOpen Cloud Standards Incubator、SNIAのCDMIなど)の適用及び拡張をすることとしたい。

9 おわりに

GICTFでは、グローバルなクラウドシステム間の連携を可能として、より高信頼、高品質なクラウドサービスがグローバルに提供されることを目標としている。

GICTFでは、今後クラウド間に跨って提供されるサービスの一元的な監査手法や、クラウドシステム間での精算方式等についても検討し、本ドキュメントで記載した機能やインタフェースの要件をもとに、インタークラウドをはじめとするクラウドの標準化に寄与していく予定である。

10 参考文献

[クラウド定義]

NIST - The NIST Definition of Cloud Computing

<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>

[ユースケース]

CSA - Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

<http://www.cloudsecurityalliance.org/csaguide.pdf>

DMTF - Interoperable Clouds, A White Paper from the Open Cloud Standards Incubator

http://www.dmtf.org/about/cloud-incubator/DSP_ISO101_1.0.0.pdf

OGF - Open Cloud Computing Interface-Use cases and requirements for a Cloud API

<http://www.ogf.org/documents/GFD.162.pdf>

Open Cloud Manifesto - Cloud Computing Use Cases White Paper Version2.0

http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-2_0.pdf

[SLA]

GSA - US Federal Cloud Computing Initiative RFQ

<http://www.scribd.com/doc/17914883/US-Federal-Cloud-Computing-Initiative-RFQ-G>

SA

JEITA - 民間向けITシステムのSLAガイドライン

<http://home.jeita.or.jp/is/committee/solution/guideline/080131/index.html>

SLA@SOI - Service Oriented Infrastructure

<http://sla-at-soi.eu/>

経済産業省 - SaaS 向けの SLA ガイドライン

<http://www.meti.go.jp/press/20080121004/20080121004.html>

首相官邸 - 電子政府ガイドライン

<http://www.kantei.go.jp/jp/singi/it2/guide/index.html>

総務省 - 地方公共団体におけるICT部門の業務継続計画(BCP)策定に関するガイドライン

http://www.soumu.go.jp/menu_news/s-news/2008/080821_3.html

総務省 - 電子政府の推進

http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/a_01.htm

[インタフェース、機能構成]

DMTF - Distributed Management Task Force

<http://www.dmtf.org/home>

DMTF - Virtualization Management (VMAN)

<http://www.dmtf.org/standards/mgmt/vman/>

DMTF - Open Virtualization Format Specification

http://www.dmtf.org/standards/published_documents/DSP0243_1.0.0.pdf

DMTF - CPU Profile

http://www.dmtf.org/standards/published_documents/DSP1022_1.0.pdf

DMTF - Virtual System Profile

http://www.dmtf.org/standards/published_documents/DSP1057_1.0.0.pdf

OGF - Open Cloud Computing Interface Working Group

<http://www.occ-wg.org/doku.php>

OGF - Open Cloud Computing Interface Specification(Draft)

<http://forge.gridforum.org/sf/docman/do/downloadDocument/projects.occ-wg/docman.root.drafts/doc15731/5>

Project Kenai - The Sun Cloud API

<http://kenai.com/projects/suncloudapis/pages/Home>

VMware - vCloud API

<http://communities.vmware.com/community/developer/forums/vcloudapi>