

2011 年 12 月 2 日

送付先:ccroadmap.comments@nist.gov.

Robert Bohn, National Institute of Standards and Technology,

100 Bureau Dr., Stop 2000, Gaithersburg, MD 20899-2000.

Tel (301) 975-4731

[No. 111027658-1659-01]

NIST Special Publication(SP)500-293

US Government Cloud Computing Tehnology Readmap Volume I, II Release1.0(Draft)に関する
JEITA コメント

JEITA は日本の電子情報産業技術産業や経済の発展と文化の興隆に寄与することを目的とした業界団体です。JEITA の情報・産業社会システム部会 ソリューションサービス事業委員会では、日本のソフトウェアおよびサービス市場規模の把握、日本政府における情報システム調達制度の在り方、クラウドビジネスモデルの定義の明確化やクラウドサービス契約上の留意点を整理する等の調査活動のほかに、SLA/SLMWG を設けて、可視化ツールとしての SLA の活用について「民間向け IT システムの SLA ガイドライン」を出版する等、SLA/SLM の普及に努めています。このたび、NIST より発行された標記、技術ロードマップ を委員会で検討いたしました。

「Volume I 」の「2.3 Requirement 3: Technical Specifications for High-Quality Service-Level Agreements」および「Volume II」の「6.2 Service-Level Agreement Taxonomy」に SLA についての記述がありますが、そこにリスクマネジメントの視点を加える良いと思いました。

また、「Volume I 」2.3 の要件 3 で「SLA は測定可能」と定義されていますが、クラウドの特異性を考えると測定可能な項目だけでなく、契約書や合意書で定義される項目もサービスレベルを定義する要素として追加すればより SLA が明確になります。

参考に当委員会でまとめた「クラウドサービスのリスクコントロール手段としての SLA 適用に関する報告書(2011 年 3 月発行)」の該当部分の概要を添付します。

一般社団法人 電子情報技術産業協会
ソリューションサービス事業委員会
委員長 鈴木 英彦

SLA/SLM ワーキンググループ
主査 銅 玄 智 昭

S L A適用領域拡大に関する調査報告書—概要—

本委員会は、ソリューションサービス分野におけるビジネス環境の調査・整備、提言を目的として、ITサービスの利用者と提供者が共通認識をもちながら品質・コスト・リスクのバランスをとっていくことの重要性がますます高まっていくとの認識の下、SLA/SLMを中核テーマとして調査・研究活動を行っている。ITサービスの機能や範囲、品質、性能などを「見える化」し、コスト及びリスクとサービス品質との適正なバランスをとるためのツールとしてSLAを位置づけ、「民間向けITシステムのSLAガイドライン」（以下、「SLAガイドライン」と称す。）を日経BP社から出版し、SLA/SLMの普及に努めてきた。

1. クラウドサービス活用時のリスクコントロール

1.1 背景

経済産業省「クラウドコンピューティングと日本の競争力に関する研究会」報告書（2010年8月16日発行）によると、『クラウド・コンピューティングとは「ネットワークを通じて、情報処理サービスを、必要に応じて提供／利用する」形の情報処理の仕組み（アーキテクチャ）をいう。』と紹介されている。

クラウドに関する定義として米国国立標準技術研究所（NIST）の定義が広く引用されている。NISTの定義にある「three service models」とは①Software as a Services（SaaS）、②Platform as a Services（PaaS）、③Infrastructure as a Services（IaaS）のことであり、提供するものが何であるかによって分けられている。「four deployment models」とは①プライベートクラウド、②コミュニティクラウド、③パブリッククラウド、④ハイブリッドクラウドのことであり、クラウド利用者側の違いによって分けられる。

第5のモデルとして、プライベートクラウドとパブリッククラウドの良い点を組合せたバーチャルプライベートクラウドが着目されるようになっている。バーチャルプライベートクラウドでは、別組織の利用者や一般利用者が利用するリソースと物理的または論理的に分離したリソースを利用する形態である。

1.2 クラウドサービスとは

(1)クラウドサービスの定義

本委員会ではこれまで、サービスにはサービス提供者と利用者の視点が重要であると考え、各々の視点でサービスを定義してきた。クラウドサービスについてもサービス提供者と利用者の視点を追加し以下の定義とした。

クラウドコンピューティングを活用して、サービス提供者から利用者に提供されるITサービス

(2)クラウドサービスのメリット

クラウドサービスのメリットを利用者視点で定義した（表1参照）。

表1 クラウドサービスのメリット（利用者視点）

	区分	内容
1	導入期間短縮メリット	①必要な時にすぐに利用することができる。 ②必要な期間だけ利用することができる。
2	コストメリット	①ハードウェアやソフトウェアは共有されるため、投資コストを抑えることができる。 ②従量課金で使った分だけ支払うことができる。
3	リソースメリット	①アップグレードやバージョンアップをサービス提供者側が実施してくれることから、利用者は最新の環境を利用できる。 ②セキュリティ管理をサービス提供者側が実施してくれる。
4	システム拡張性のメリット	クラウドサービスは一般的に仮想化されており、利用者のサービス利用頻度や範囲の拡大に柔軟に対応できる。

(3)クラウドサービスの検討対象領域

クラウドサービスへのSLAの適用を検討するにあたり、検討対象領域を定義した。

クラウドコンピューティングのデプロイモデルは、「プライベート」「コミュニティ」「パブリック」「ハイブリッド」「バーチャルプライベート」の5種類ある。本委員会では、サービス提供者と利用者が別々の企業のように独立性が高いモデルを検討対象領域とした。

結果として2010年度のクラウドサービスの検討対象領域は「パブリック」と「バーチャルプライベート」の2種類とした。

1.3 クラウドサービス活用のリスク

クラウドサービスへのSLAの適用を検討するにあたり、まず、サービス特有のリスクも含めたクラウドサービス活用のリスクを定義した。

(1)クラウドサービス特有のリスクと洗い出し

クラウドサービスの仕組みを考えた場合、従来のITサービスとは異なる、独自のサービスリスクが存在する。

そのクラウドサービスリスクを以下の手順で洗い出した。

<手順1>参考となる報告書から、クラウドサービスの課題を抽出した（図1参照）。

<手順2>当委員会独自に課題に対応するリスクを定義した。

<手順3>定義しきれていないリスクを独自に補った。

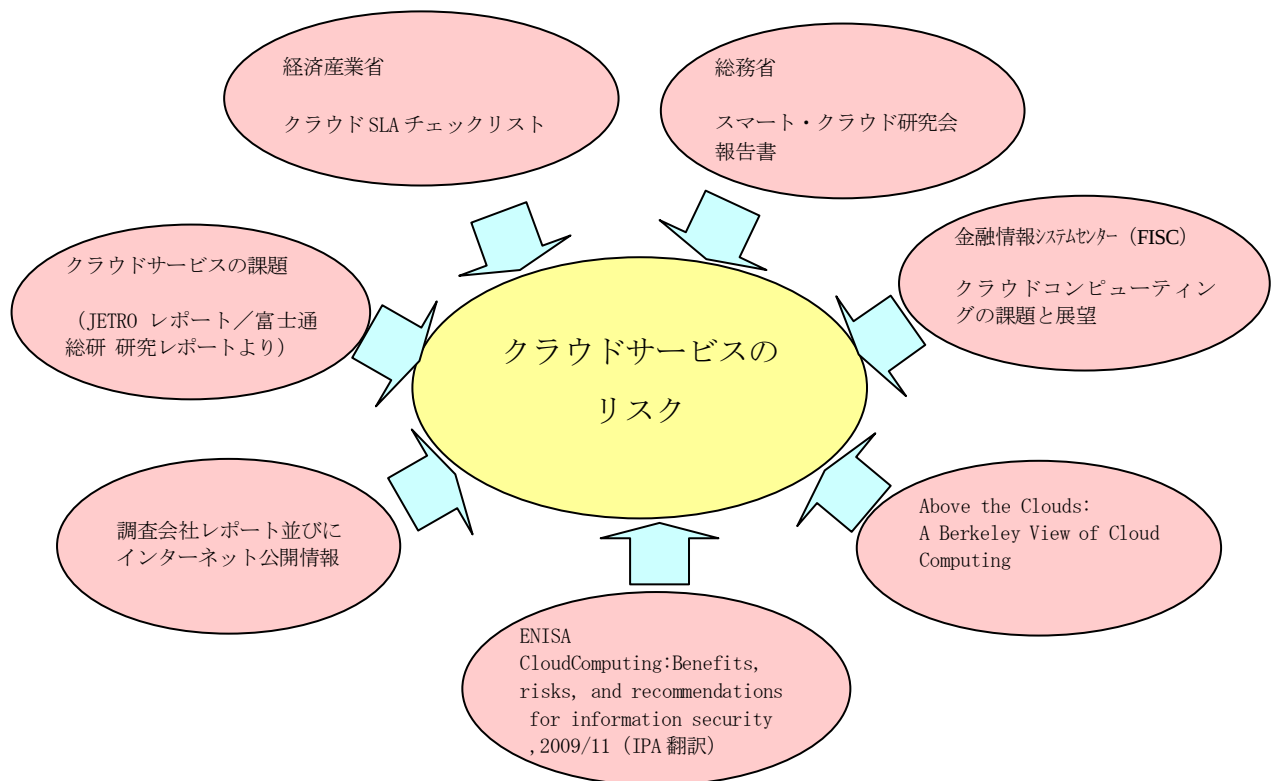


図1 参考となる報告書からのクラウドサービスリスク洗い出し

1.4 クラウドサービスへのSLAの適用

企業のIT担当者が、企業の情報システムへクラウドサービスを適用する場合に、クラウドサービスの課題をリスクとして捉え、そのコントロール手段としてSLAを定義し、サービス提供者、利用者間で合意することによりクラウドサービスとそのリスクが見える化することを目的に、検討を行った。

(1) クラウドサービスへのSLA適用の考え方

クラウドサービスの利用は、クラウドサービスを自社の情報システムへ適用する場合においては、通常の外部委託と同様に、サービス提供者、利用者の関係性が生まれる。

またクラウドサービスの特性により、提供を受けるサービスは見えるが、提供されるサービスの環境については、利用者から見えにくく関与が薄くなる傾向にある。

このような場合において、利用者とサービス提供者間でサービスの見える化ツールとしてのSLAが有効である。

本委員会で検討するSLAは、サービスレベル項目だけではなく、サービス仕様での定義や契約での取り決めも含む広義のSLAとして考える。

今回の検討においては、クラウドサービスを適用する場合のリスクを洗い出し、そのコントロール方法として広義の SLA を位置づける。

以下の表にクラウドサービスの SLA によるコントロール方法を示す（表 2 参照）。

表 2 SLA によるコントロール方法

デプロイモデル SLA によるコントロール		バーチャルプライベートクラウド		パブリッククラウド
		物理的分離	論理的分離	
狭義 SLA	標準のサービスレベル項目	○	○	◎
	標準のサービスレベル項目へ追加	◎	○	△
広義 SLA	チェック項目	○	○	◎
	仕様／RFI	◎	○	△

1.5 サービスレベル項目の考え方と適用方法

(1) サービスレベル項目の考え方

クラウドサービスのリスクに対して SLA を適用することで、クラウドサービスのリスクコントロールを可視化し、リスクの回避／低減／移転を実現することを目的に、コントロール方法の実現手段としてふさわしいサービスレベル項目について検討した。しかしながら、以下に示すような問題があることがわかった。

- ・ SLA で規定できるサービスレベル項目だけでは、クラウドサービスにおけるリスクコントロール全体に対応することができない。
- ・ 定性的な（定量的には表現できない）サービスレベル項目を用いないと、コントロールすることができないリスクがある。
- ・ リスクコントロール方法の実現方法の中には、SLA で規定すべきサービスレベル項目としてふさわしくないものがある。

そこで、サービスレベル項目を、クラウドサービスのリスクをコントロールするための実施手段として広く捉えることにした。リスクコントロール手段としてのサービスレベル項目を考えると、その特性から以下の 3 つに区分することができる。

- ・ 自動：定量的に表現でき、自動的にツールで測定可能なもの
- ・ 手動：定量的に表現するのではなく、出来た／出来なかった、ある／ない等を人により確認するもの

- ・仕様：SLA で規定するのではなく、サービス要求、契約条項、サービス仕様として規定されるもの

(2) サービスレベル項目の適用方法

クラウドサービス活用のライフサイクルの各段階に応じて、サービスレベル項目の適用方法は異なる、以下に適用方法を記載する（表 3 参照）。

表 3 サービスレベル項目の適用方法

ライフサイクル	コントロール方法の実装区分		
	自動	手動	仕様
事前検討	チェックリスト	チェックリスト	チェックリスト
サービス要求提示	RFI/RFP	RFI/RFP	RFI/RFP
契約	SLA	SLA／サービス契約	サービス契約
運用	SLA	SLA／契約事項確認	契約事項確認
終了	—	契約事項確認	契約事項確認

1.6 サービスレベル項目によるリスクコントロール

サービスレベル項目を使ってリスクをコントロールする方法を、「クラウドサービス・リスクコントロール表」としてまとめた。

(1) 目的

「クラウドサービス・リスクコントロール表」は、クラウドサービスの利用者がビジネス要求に適合した最適なクラウドサービスを活用するためのガイドとして利用することを目的としている。

(2) 構成

「クラウドサービス・リスクコントロール表」の構成は以下の通りである（図 2 参照）。

① 分類

クラウドサービス活用時の発生リスクを、その性質から以下の 9 つに分類した。

ー可用性、信頼性、セキュリティ、性能、データ管理、移行、責任範囲、法令、拡張性

② クラウドサービス活用時のリスク

クラウドサービス活用時の発生リスクを記載した。

③ リスク評価

リスクが発生したときの影響度と発生の可能性を、「大・中・小」で評価した。

④ コントロール方法

リスクをコントロール（回避／低減／移転）するために、クラウドサービスの利用者が

実行することが望ましい事柄を記載した。

⑤ 実装区分

リスクのコントロール方法を実装するためのサービスレベル項目を、その特性から3つに区分した。「自動」、「手動」、「仕様」

⑥ サービスレベル項目例

具体的なサービスレベル項目の例を提示した。

⑦ 備考

上記の各項目の記載内容についての補足説明などを記載した。

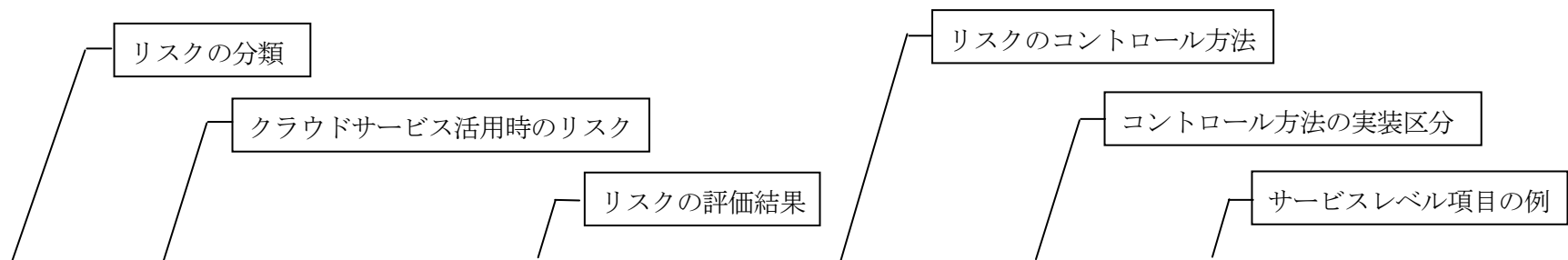
(3) 期待効果

本委員会では、「クラウドサービス・リスクコントロール表」を以下のような形で活用することで、様々な効果を期待できると考えている。

①クラウドサービスの活用を検討する際に、事前のチェックリストとして活用できる。

②クラウドサービスあるいはサービス提供者を選定するときに、リスクを評価することで自社のビジネス要求を満足するサービス要求を提示することができる。

③サービス提供者とサービス契約するときに、SLAで合意する事柄とサービス契約あるいはサービス仕様として合意する事柄を見分けることができる。



No.	分類	クラウドサービス活用時のリスク	リスク評価		コントロール方法	実装区分			サービスレベル項目例	備考
			影響度	可能性		自動	手動	仕様		
1	可用性	サービス提供者の突然のサービス提供終了により、利用者の業務遂行に支障をきたす。	大	小	サービス提供者のサービス提供が突然終了した場合でもサービスを継続できるように、あらかじめプログラム・データを第三者に預託しておく。			○	突然のサービス提供終了に対する取り決め プログラム・データの第三者預託	
2	可用性	サービス提供者の突然のサービス内容の変更・停止等により、利用者の業務遂行に支障をきたす。	大	小	サービス内容の変更・停止等がある場合は、サービス提供者がその旨を事前に利用者に連絡することを契約で定めておく。			○	突然のサービス提供変更・停止に対する取り決め サービス時間 計画停止予定通知	
3	可用性	サービスが安定して提供されないと利用者の業務遂行に支障をきたす。	大	中	サービスレベルを取り決め、定期的にモニタリングし、評価する。	○			稼働率 平均復旧時間(MTTR) 目標復旧時間(RTO) 障害発生件数 サービス提供時間帯(障害対応) サービス提供時間帯(一般問合せ)	
4	可用性	提供されるサービスに、重大な障害が発生することにより利用者の業務遂行に支障をきたす。	大	小	サービス提供者と利用者の間で、早期復旧が不可能な場合の代替措置を事前に取り決める。			○	重大障害時の代替手段	
5	可用性	利用者間のリソース分離の不備により、サービスの中断が発生する。	大	小	マルチテナントでのデータベース管理方法、データベースの暗号化鍵管理(全テナント共通 or テナント毎)等を契約時に確認し、必要に応じてデータベースの分割・暗号鍵の個別管理を契約で定めておく。			○	マルチテナントストレージにおけるキー管理要件	
6	可用性	災害復旧訓練が適切に実施されず、災害時の業務継続が出来ない。	大	中	契約時に、災害発生時のシステム復旧/サポート体制等の災害復旧訓練の内容・実施頻度を確認し取り決める。			○	BCP コンテンジェンシープラン	

備考

図2「クラウドサービス・リスクコントロール表」の構成

1.7 「クラウドサービス・リスクコントロール表」の使い方

クラウドサービスの利用に際してリスクコントロールを検討する際の、「クラウドサービス・リスクコントロール表」の活用方法について記載する。

活用シーンとしてクラウドサービスの利用におけるライフサイクル（「事前検討」・「サービス要求提示」・「契約」・「運用」・「終了」）を想定し、各段階でのリスクマネジメント観点での主要検討事項と、検討における「クラウドサービス・リスクコントロール表」の活用方法を例示する（図3参照）。

ライフサイクル	主要検討事項 (リスクマネジメント観点)	「クラウドサービス・リスクコントロール表」の活用例
事前検討	クラウドサービス利用に伴うリスクの洗い出し・評価	✓ クラウドサービス利用に伴うリスクを俯瞰する ✓ 各リスクの影響度・可能性から重要なリスクを特定する ✓ 上記検討結果を、クラウドサービス利用に向けた企画の参考とする
サービス要求提示	クラウドサービス提供者のリスク対応方針確認	✓ 重要なリスクに対するサービス提供者の対応方針を確認する
契約	要求仕様の検討 SLAの締結	✓ 契約内容に盛り込むべき仕様を検討する ✓ 継続的に管理すべき事項で、SLAに盛り込むべき項目を検討する
運用	リスク対応方針に応じた管理状況の確認	✓ 運用状況により、契約見直し（サービスレベル項目追加・削除）を行う際の参考とする
終了	クラウドサービス終了に伴うリスク評価・対応	✓ 契約内容を再確認し、終了に伴う処置が適切に行われているか確認する

図3 「クラウドサービス・リスクコントロール表」の活用方法

2. クラウドサービスの米国調査報告

本委員会では、クラウドサービスの活用に向けたサービスレベル項目の策定を目指し、次の三つの観点から米国のクラウドサービスの利用者およびサービス提供者にヒアリング調査を行った。

(1) 日本では入手が難しい、クラウドでの基幹系利用での RFI/RFP の要求事項の入手を図る。特に、パブリッククラウドである GoogleApps に対して、厳密なセキュリティ要件を指定して活用した事例としてロサンゼルス市役所のヒアリング調査を行う。

- (2)日本に先行し利用が普及しているクラウドサービスにおいて、実際に顕在化してきたクラウドの課題の調査収集を行い、課題の解決策として、利用者とサービス提供者間で取り決めるサービスレベル項目の抽出を行う。
- (3)クラウドサービスにおいて、実際の業務を進めている利用者が、データ保持や法制度対応の為にいかなる施策をとっているかの調査を行う。特に米国愛国者法への実際の対応状況を調査し、日本でのデータ保持に関する SLA の考え方を確立する。