

平成 26 年度
クラウド技術調査 WG レポート

クラウドインテグレーション における SLA の検討ポイント

平成 26 年 11 月

一般社団法人 情報サービス産業協会

技術強化委員会 技術企画部会

クラウド技術調査 WG SLA チーム

はじめに

我々システムインテグレータ(以下 **SIer**)は、個々の顧客ビジネスのニーズを満たすために、多くはオンプレミス型によるシステム開発を行い、個々の顧客ビジネスのニーズを実現してきた。昨今は、顧客ビジネスのニーズをさらに短期間で実現し、柔軟に変化対応するためにクラウドサービスの利用が増えてきている。

このような背景を踏まえ **JISA** クラウド技術調査 **WG** では「クラウドサービスの利用における **SLA**」に着目し、調査活動を行い、本レポートを取りまとめた。

本レポートの主なターゲットは、パブリッククラウドを活用する **SIer** とし、対象とするクラウドサービスは、**IaaS**(Infrastructure as a Service)としている。プライベートクラウドや **SaaS**(Software as a Service)を検討範囲に含めるか議論したが、個社プロダクトや諸事情へ依存が大きいため対象外とした。

本レポートは一言で言うと「クラウドサービスを検討しはじめるときの手引き」である。クラウドサービスの利用を網羅的に扱うチェックリストと言うよりも、クラウドサービスを利用するにあたってのディスカッションの種本として扱って頂ければ幸いである。

本レポートの **SLA** 検討ポイントはすべてを満たさないといけないわけではないし、この検討ポイントを参考に **SLA** の標準化を提唱しているわけでもない。この手引きが、**SIer** にとってクラウドの活用に前向き取り組むための一助となれば幸いである。

平成 26 年 11 月
技術強化委員会 技術企画部会
クラウド技術調査 **WG** **SLA** チーム
主査 鬼頭 豊和

執筆者名簿

座長	吉成	安宏	富士通エフ・アイ・ピー株式会社 テクニカルソリューション統括部長
主査	鬼頭	豊和	株式会社野村総合研究所 (エヌ・アール・アイ・セキュアテクノロジーズ 株式会社 MSS 事業本部 MSS 開発部 出向)
委員	高橋	博幸	株式会社網屋 amigram 事業部
委員	加茂	宏一	鉄道情報システム株式会社 営業推進本部 事業開発推進室 主任
委員	伊藤	悦雄	株式会社東芝 クラウド&ソリューション社 グローバル統合事業戦略室 業務担当 参事
委員	川幡	和利	富士通エフ・アイ・ピー株式会社 ソリューションサービス本部 第二システム事業部長
委員	飯沢	篤志	リコーITソリューションズ株式会社 経営企画本部 STC
事務局	鈴木	律郎	一般社団法人情報サービス産業協会 企画調査部 次長

目次

第1章	クラウドインテグレーションにおける SLA の目的	1
1	クラウドインテグレーションにおける SLA	2
1.1	クラウドの SLA を扱った背景と目的	2
1.2	SLA の検討ポイントと選定理由	3
1.3	クラウドサービス事業へのヒアリング	3
第2章	SLA 指標	5
2	SLA 指標	6
2.1	サービスの継続性	7
2.1.1	SLA の定義	7
2.1.2	アプリケーション動作保証	7
2.1.3	不具合対応	8
2.1.4	メンテナンス対応	8
2.1.5	EOSL 対応	9
2.1.6	サービス提供終了	9
2.1.7	ディザスタリカバリ (DR)	10
2.2	バックアップデータ、保存	11
2.2.1	バックアップサービスの有無	11
2.2.2	仮想サーバのイメージコピー	12
2.2.3	データの保証	12
2.3	OS/ミドルウェアの動作保証、マイグレーション	14
2.3.1	ベンダ動作保証	14
2.3.2	既存システムのマイグレーション	14
2.3.3	仮想サーバのインポート	15
2.3.4	OS の ESOL	15
2.4	性能保証	17
2.4.1	ハードウェアの選定基準	17
2.4.2	拡張制限	17
2.4.3	時間帯による負荷対策	18
2.4.4	大量データ移行サービス	18
2.4.5	禁止事項について	19
2.5	運用関連	20
2.5.1	リソースの稼働状況監視と枯渇予知・通報	20
2.5.2	監視内容通知とヘルプデスク	21
2.5.3	顧客情報管理	21

2.5.4	問合せ時の本人確認	22
2.6	契約関連	23
2.6.1	契約申込手段	23
2.6.2	契約者の制限の有無	23
2.6.3	損害賠償規定の有無	24
2.6.4	最小契約の単位、期間	24
2.6.5	初期費用と有無と課金体系	25
2.6.6	決済手段	25
2.6.7	サービスの再販可否	26
2.6.8	個別対応の可否	26
2.7	拡張性	28
2.7.1	機器持ち込み、ネットワーク接続形態	28
2.7.2	専用サーバ、専用ネットワーク	29
2.8	セキュリティ	31
2.8.1	センターファシリティのセキュリティレベル	31
2.8.2	クラウドサービスに対するセキュリティ対策	31
2.8.3	利用者が遵守すべきセキュリティ要件	32
2.8.4	利用者の監査法人に対する対応	32
2.8.5	セキュリティ攻撃に対する対処	32
2.8.6	ペネトレーションテストの実施	33
2.8.7	サービス基盤内ネットワーク分離について	33
第3章	新たな観点	35
3	新たな観点	36
3.1	サービス継続性	36
第4章	参考文献ほか	37
4	参考文献ほか	38
4.1	クラウド事業者へのアンケート票	38
4.2	主なSLAガイドラインリスト(2014年3月現在)	41

第1章

クラウドインテグレーションにおける SLA の目的

1 クラウドインテグレーションにおける SLA

1.1 クラウドの SLA を扱った背景と目的

SIer はクラウドサービスを活用する SI においても、従来同様の品質や信頼性を確保する必要がある。クラウドを利用するからと言って、顧客ニーズに合ったシステムを構築するという SI の本質が変わるわけではない。

では、SIer がクラウドサービス上においても円滑なシステム構築を推進するにあたっては、SLA をどのような観点から検討すればよいただろうか。

広く公開されている多くのガイドラインは、クラウドサービス事業者や顧客ユーザ向けに提供されているものが多く、SIer 向けに書かれたガイドはほとんどない。また、昨今国内外のパブリッククラウドサービス事業者から提供されているガイドラインもあるが、SIer から見れば別業種から発行されているものであるため、そのまま SIer がシステム構築に利用するのは難しい。

このような状況から、SIer 自身がクラウド上でシステム構築するためのガイドラインが必要であると考えた(図 1-1)。

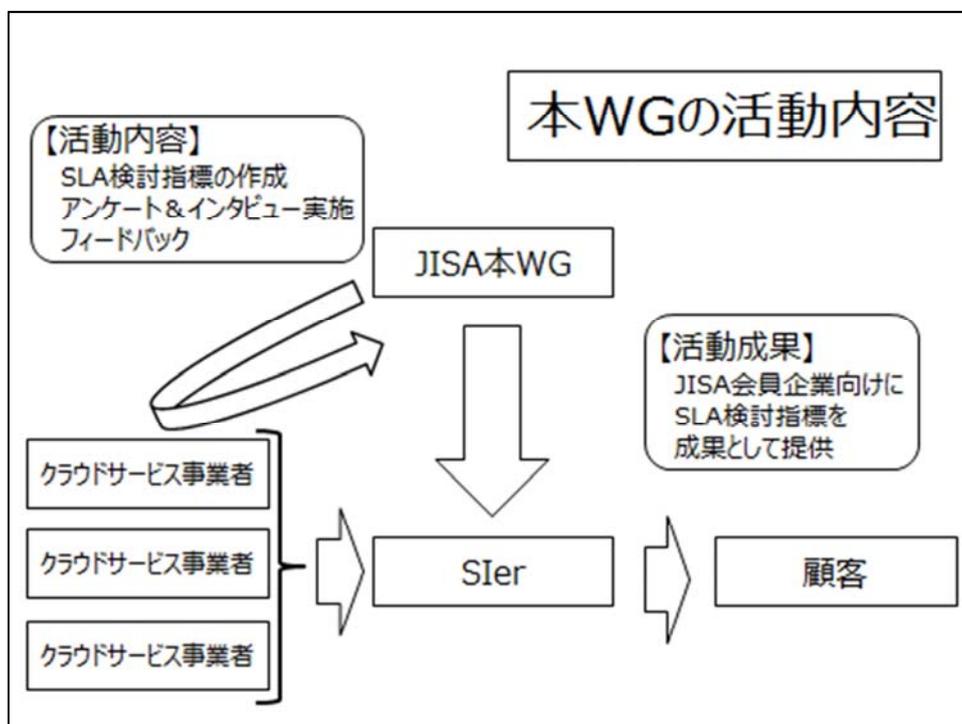


図 1-1. 本 WG の活動概要

1.2 SLA の検討ポイントと選定理由

本 WG メンバーでは、検討ポイントを表 1-1 の通り 8 つに分類し、40 個の検討ポイントを選定した。

表 1-1 SLA 検討ポイント

分類	概要
サービスの継続性	メンテナンス作業やサービス終了を想定した運用、クラウドサービスの災害対策
バックアップ データ保全	適切なデータ保存
OS/ミドルウェアの 動作保証マイグレーション	稼働する OS/ミドルウェアの動作保証、既存システムとクラウドサービス間の移植性
性能保障	他の利用者とリソースを共用することに起因する処理性能の揺れ、スケールアウト可否
運用	稼働状況の可視化と、障害発生時の利用者への通知内容、ヘルプデスクの内容
契約	クラウドサービス事業者との責任分界点、従来の契約可否や法人契約の例
拡張性	既存システムとの専用線接続やリソースを占有できる専用サーバ、利用者の機器持込みと言ったニーズが多い為、確認する必要がある。
セキュリティ	セキュリティ対策、「パブリック」なサービスであるが故のユーザ別の情報分離のためにどのような対策

実際のところ、開発するシステムの要件はさまざまである。次章で取り挙げる検討ポイントは、プロジェクトの状況や特性に応じて取捨選択を行うのが望ましい。

1.3 クラウドサービス事業へのヒアリング

本 WG が作成した 8 分類 40 個の SLA 検討ポイントをアンケート形式にして、国内クラウドサービス事業者数社にインタビューを行った。社名や個社を特定する回答は非公開の扱いの条件でご協力いただいた。実際に用いたアンケート票を第 4 章に掲載した、参照されたい。

第2章

SLA 指標

2 SLA 指標

本章では、8 分類 40 個の各検討ポイントについて Q&A 方式で解説している。各検討ポイントは「質問」、「質問の主旨」、「回答と考察」で構成される。

2.1 サービスの継続性

SIerは、クラウドサービスを利用する上で、クラウドサービス事業者によるメンテナンス作業やサービス終了を想定して、システム構築と運用を行う必要がある。また、BCP(Business Continuity Planning、事業継続計画)の観点で、クラウドサービスがDR(Disaster Recovery、災害対策)に対応しているかも確認する必要がある。

2.1.1 SLAの定義

	クラウドサービスにおける稼働率(SLA)の定義はありますか？(Yes/No)
	SLAの定義は一般公開されていますか？(Yes/No)

(1) 本質問の趣旨

SLAは保証(Assurance)ではなく合意(Agreement)である。そのため、設定値を下回った場合、月額料金の一部返金などの合意規定がある。また、SLAの定義範囲(期間、範囲、例外事項)は各社各様であることから、SLAの定義と内容が一般に公開されているか確認する。

(2) アンケート回答と考察

SLO(目標値)としている事業者も一部あるが、各社SLA定義は概ね一般に公開されていると回答があった。公開された内容には過去の稼働実績も含まれていることもあるため、SI対象のシステムに求められるサービスレベルとの乖離がないか十分に確認する。

2.1.2 アプリケーション動作保証

	クラウドサービスで提供される仮想サーバ上で動作するアプリケーションの動作保証は、行われますか？(Yes/No)
--	---

(1) 本質問の趣旨

システム導入時、各種アプリケーションを活用するにあたり、クラウド事業者が事前にアプリケーションの動作確認を行った上での動作保証をしているのか、あるいはメーカーとのサポートパスを持っているかを確認する。

(2) アンケート回答と考察

クラウドサービス事業者がオプション提供するアプリケーション

ンを除き、原則動作保証は利用者責任であるとの回答であった。
これは、メーカーの物理サーバを購入するときと同じである。

そのため、クラウドサービスを利用する際には利用者自身(ここでは SIer を指す)においてアプリケーションメーカーへ仮想サーバ上での動作保証の有無の確認、利用するクラウドサービス上における動作確認を行う必要がある。

2.1.3 不具合対応

物理サーバやストレージにウィルスやバグなどの不具合を検知した場合の対処方針はありますか？ (Yes/No)
サービス停止を伴うメンテナンス作業を行う場合、利用者との調整を行う際の方針はありますか？

(1) 本質問の趣旨

クラウドサービスでは、仮想サーバをベースに SI を行うことが前提であるため、物理サーバやストレージの管理はクラウド事業者へ任せられる。しかしながら、ウィルスやバグなどの不具合検知が無くなるわけではないので、検知した場合の対処方針およびサービス停止を伴うメンテナンス作業を SIer が行う場合の、日時調整などが行えるかを確認する。

(2) アンケート回答と考察

各社何かしらの手段をもって情報公開を行い、メンテナンス停止の事前告知は行うとの回答がほとんどであった。一部、利用者(SIer)側と日程調整を行う事業者もあった。

SI 対象のシステムに固定的な運転停止時間が求められる場合は、あらかじめクラウドサービス事業者側に停止日時の事前調整ができるかなどの条件を確認する。

2.1.4 メンテナンス対応

定期メンテナンスや緊急メンテナンスの実施はありますか？ (Yes/No)
利用者へのメンテナンスの通知方法は具体的にどのような方法がありますか？

(1) 本質問の趣旨

定期メンテナンスについて、事前告知があるのかどうか、通知方法は利用側にとって必要十分な方法であるのか、緊急メンテナ

ンスに関しては、基本は避けるべき事柄であるため、過去の稼働状況や、SI 対象システムの運転時間等を考慮した調整が可能かどうか確認する。

(2) アンケート回答と考察

2.1.3 質問 3 と同様に各社何かしらの手段をもって情報公開を行い、メンテナンス停止の事前告知は行うとの回答であった。

SI 対象のシステムに固定的な運転停止時間が求められる場合は、あらかじめクラウド事業者側にメンテナンス対応条件を確認する。

2.1.5 EOSL 対応

クラウドサービスのシステム基盤上で、EOSL(End Of Service Life)対応の作業を行う場合、利用者に連絡を行っていますか？ (Yes/No)
--

(1) 本質問の趣旨

クラウドサービスのシステム基盤で利用されている各種プロダクト(VMware などの仮想化基盤など)について、商用ソフトであるかオープンソースソフト(OSS)であるかにかかわらず EOSL 対応(システム基盤のバージョンアップなど)が必要となる。EOSL に対するクラウドサービス事業者のポリシーを確認する。

(2) アンケート回答と考察

EOSL 対応をすでに経験している事業者は連絡を行う、または連絡を行わないのいずれの回答もあった。また EOSL 未経験の事業者は、連絡を行う予定であるとの回答であったことから、事業者ごとに対応ポリシーが異なることが分かる。

SI 対象のサービス停止の可否にも関わるため、このポリシーに応じた運用設計が必要であり、事前に条件を確認しておく。

2.1.6 サービス提供終了

クラウドサービス事業者の都合により、クラウドサービスの提供が終了する場合、利用者へサービス停止の何カ月前に通知されますか？

(1) 本質問の趣旨

SI 対象のシステムをクラウド上で運用するにあたり、クラウドサービス事業者の倒産などによる事業者都合のサービス停止などに備える必要がある。

具体的にはサービス終了に関し過去に一部サービス終了に伴い、代替サービスの提案や実績があったのか、また、サービス自体が終了する場合、終了予告から利用停止期間はどの程度あるのかを確認する。

(2) アンケート回答と考察

サービス終了通知を規約通りのタイミングで行う事業者もあれば、通知タイミングを明確に規定していない事業者もあるなど、ばらつきはあるが、サービス提供終了に関して事業者側より事前に通知するとの回答であった。

提供終了予定のない事業者については事業者の経営基盤等を確認し、裏付けを取ったうえで判断する。

2.1.7 ディザスタリカバリ(DR)

DR(Disaster Recovery)に対応するサービスメニューはありますか？ (Yes/No) サービスメニューがない場合は、DRを実現するための代替サービスはありますか？

(1) 本質問の趣旨

SI対象のシステムの情報資産を守るために、リスクとリターンに応じてポートフォリオを検討し、一つの事業者を利用するにしても複数拠点を活用したり、マルチクラウドを適用するなど、DR構成を保つ必要がある、DRに対する事業者の対応方針を確認する。

(2) アンケート回答と考察

各社のDRでは、具体的なサービスメニューは示されなかったが、データセンタの立地条件を利用したり、個別見積りするなど、なんらかの対応が可能との回答であった。

SI対象の情報資産のBCPに沿ったDR計画を立てることは可能であるが、コストへの影響を考慮し選定する。

2.2 バックアップデータ、保存

パブリッククラウドサービスでは、一般的にバックアップはクラウド事業者のサービス仕様に依存する。SIer はオンプレミスで容易にバックアップできていたことが、クラウドサービス上でも同様にできるかどうか確認する。

2.2.1 バックアップサービスの有無

仮想サーバおよび仮想ストレージに対するバックアップは、クラウドサービスとして提供されていますか？ 以下の中から最も当てはまるものを選択願います。

- 1)標準契約に含まれる
- 2)バックアップを含むサービスメニューがある（そのサービスに関して簡単にご説明ください）
- 3)バックアップサービスが単独のサービスとして存在する
- 4)標準サービスとしては存在しないが、個別対応が可能である
- 5)バックアップを含むサービスは提供していない
- 6)その他（具体的にご記載ください）

(1) 本質問の趣旨

オンプレミスにおけるデータのバックアップおよびデータ保全の方法としては、稼働系とは異なるディスクへのデータコピーや外部媒体へのバックアップ、DR を想定した遠隔地へのデータ回避や媒体の外部保管などが一般的である。しかし、クラウドサービスは、データの物理的ロケーションが利用者には通知されず、また可搬媒体等へのバックアップをサービスしていない場合がほとんどである。こうしたクラウド環境上のシステムでバックアップやデータ保全を講じる際に、どのような方法が可能であるか（サービスとして用意されているか）は、運用方式設計上の大きな課題であり、クラウドサービス選択のポイントの1つである。

(2) アンケート回答と考察

質問の意図が十分伝わらなかったためか、選択肢の 2)あるいは 3)と回答があったサービスは、仮想サーバのスナップショットやシステムバックアップの機能あり、という内容であった。また、顧客の「システム」をバックアップする「サービス」は無し、という回答もあった。そのほか、稼働系とは異なる媒体や、他データセンタ(Data Center:DC)へのバックアップオプションを有す

るという回答もあった。

クラウドサービス上のシステムは利用者からみると物理媒体が仮想化されており、ハードウェアの物理的な故障発生については稼働率の SLA に基づいて保障されている、と考えがちである。しかし、データ破壊はハードウェアの物理故障によるものだけではなく、プログラム障害や誤操作によっても発生し得る。

こうしたリスクを回避するためにも、データのバックアップや保全施策を講ずる必要があるが、クラウド「サービス」として特定の利用者データをバックアップするメニューは用意されておらず、サービスが提供する各種機能を組み合わせて実装しなければならない。その際、特定のディスクに回復不可能な障害が発生したり、クラウドサービス事業者の DC が機能不全に陥ったりする場合まで想定すると、それらを回避する手段が提供されているかどうかは、サービス事業者によって差異があるものと思われる。

2.2.2 仮想サーバのイメージコピー

稼働中の仮想サーバのイメージコピーを取得できるメニューはありますか？ (Yes/No)

(1) 本質問の趣旨

クラウドサービス上のシステムの多くは仮想基盤上の仮想サーバ上で動作しており、仮想サーバそのものをバックアップする、といった機能の利活用が可能であると想定される。こうした機能をバックアップやデータ保全の観点からどこまで利用可能かを確認する。

(2) アンケート回答と考察

ほとんどのクラウドサービス事業者は「なし」「Windows のみ可能」という回答であった。ただし「利用者から要望があり提供を検討中」「個別相談には応じる」という回答もあった。

この機能は仮想基盤では標準的に用意されているものであるが、利用権限をどこまで一般ユーザに開放するか、という点がネックになっているのかもしれない。

2.2.3 データの保証

クラウドサービスで提供される仮想サーバおよびストレージ上のデータは保証されていますか (Yes/No)

(1) 本質問の趣旨

2.2.1 の(2)でも触れたが、クラウドサービスの利用者は物理的なハードウェアの存在を意識しておらず、ハードウェア故障発生時にはライブマイグレーション機能によりサービスの継続性が(SLAの範囲内で)保障されるものと想定している。システムの稼働という意味では確かにそうかもしれないが、データの完全性が保証されるのか、という観点で確認する。

(2) アンケート回答と考察

回答のあったサービス事業者すべてが「保障しない」であった。また「利用者責任である」と付言する回答もあった。つまり、クラウドサービスを利用する場合も、オンプレミスと同様、データの完全性保証や保全是 **SIer** の役割となる。たとえば、データを保管するハードディスクの耐故障性が保障されていないとすると、DB(データベース)に書き出したつもりが実際には書き込まれていなかった場合にどうやってリカバリを行うか、**SIer** はオンプレミスの場合と同様の留意を払ってシステム設計を行う必要がある。

2.3 OS/ミドルウェアの動作保証、マイグレーション

クラウドサービスのリソースを、SIerはブラックボックスとして使用するが、稼働するOSやミドルウェアの動作保証は安定したシステムに重要である。

また、既存システムとクラウドサービス間の移植性も非常に重要であり、確認する必要がある。

2.3.1 ベンダ動作保証

ベンダーからの動作保証を得ているミドルウェアやソフトウェアがありますか？（Yes/No） 例：Oracle
--

(1) 本質問の趣旨

クラウド上へ持ち込むミドルウェアやソフトウェアが、オンプレミス同様に取扱いが可能か、またソフトウェアベンダから動作保証を得ているかを確認する。

(2) アンケート回答と考察

アンケートでは原則利用者責任であるとの回答であった。そのため、SIerは対象となるミドルウェアやソフトウェアのベンダに仮想サーバ上での稼働を保証またはサポートするかどうか、当該システムで性能を発揮するかどうか、十分に動作確認行うべきである。

しかしながら、例外として一部の事業者では主要なデータベース製品等において動作保証が得られているものがあるため、たとえば当該製品をベースとしたシステム構成を検討している場合、このような事業者を活用することでリスクを軽減することも可能である。

2.3.2 既存システムのマイグレーション

ミドルウェアを含む既存システムをクラウドサービス上にマイグレーションするサービスはありますか？（Yes/No）

(1) 本質問の趣旨

オンプレミス上の既存システムをパブリッククラウド上にマイグレーションするにあたり、既存で利用しているミドルウェアの動作確認ができているかどうかを確認する。

(2) アンケート回答と考察

クラウドサービス事業者のサービスとして対応していないが、個別見積りや移行支援の SIer を紹介するなどにより既存システムをクラウドサービス上へ P2V(Physical to Virtual)や V2V(Virtual to Virtual)でマイグレーションすることは対応可能であるとの回答であった。

SI 対象システムの規模やコスト等を考慮してマイグレーション実施計画を策定することが可能と思われる。

2.3.3 仮想サーバのインポート

利用者の構築した仮想サーバイメージを、クラウドサービス上にインポートすることは可能でしょうか？

(1) 本質問の趣旨

仮想サーバをプライベートクラウド上に仮想化しサーバ集約をすることが一般的になり、BCP 対策の一環で仮想サーバをクラウド事業者側へバックアップ、リストアするような SI のケースが考えられる。実現に際して仮想サーバイメージのインポートが可能かどうか確認する。

(2) アンケート回答と考察

仮想サーバのインポートは、各事業者ともサービスとして、または個別見積りで実現可能であるとの回答であった。本質問ではインポート後の動作保証にまで触れていないが、事業者によっては利用者責任とするならば「自由に」構築可能との回答もあった。本質問の内容と合わせて、追加で確認するとよい。

2.3.4 OS の ESOL

現在提供されている仮想サーバの、サポートサービスが ESOL(End Of Service Life)により提供停止となった場合、クラウド事業者としてどのように対応しますか。

(1) 本質問の趣旨

クラウド事業者が提供する仮想サーバ、または 2.3.3 のように SI 対象の仮想サーバをマイグレーションによりクラウドサービスへ持ち込んだ場合など、ケースは異なるが仮想サーバ OS の EOSL は発生する。これについてクラウド事業者側として、継続

利用が可能なのか、サポートポリシーを確認する。

(2) アンケート回答と考察

「新規受け付けを停止する」「サービス契約の変更を依頼する」「利用者責任での継続利用は可能」など、事業者ごとに回答は異なったものの、EOSLを迎えたOSのサポートは望めないと考える。

SI対象のシステムの改修頻度を考慮し、契約変更などにより新OSへ変更する、または継続利用を続けるなどの判断が必要となる。

2.4 性能保証

パブリッククラウドは、一つのリソースをマルチユーザで利用するため、高負荷を起因とした性能低下の可能性がある。ここでは性能保証に対してどのような対策を取っているかを確認する。

2.4.1 ハードウェアの選定基準

クラウドサービスの基盤に使う物理サーバやストレージなどハードウェアの選定基準はありますか？(Yes/No)

(1) 本質問の趣旨

SI対象のシステムをクラウド上で運用するにあたり、物理サーバやストレージなどハードウェアの選定基準がどのように作られていくのか。メーカー名やハードウェア型式名が判明することにより安心感を得られる。

(2) アンケート回答と考察

ほとんどのクラウド事業者は選定基準を持っているが公開しないと回答した。

クラウドサービスは、特定のメーカーや機種に依存したサービスではないので、機種の限定を要請できるようなものではないが、選定基準が公開されていれば、一定のハードウェア品質が担保されると考えられ、利用者としては安心できる。

2.4.2 拡張制限

仮想サーバや仮想ストレージスケールアップ、スケールアウトの制限は利用者へ明示されていますか？(Yes/No)
--

(1) 本質問の趣旨

システムをクラウド上で運用する場合、多くの利用者は初期コストをできるだけ下げたいと考える。ここではクラウドサービスがどの程度拡張性を持っているか、利用者のサイジングにあわせ、必要に応じて十分な拡張ができるか、またサービスがわかりやすく明示されているかを確認する。

(2) アンケート回答と考察

クラウドサービス事業者は明示していると回答した。クラウドサービスに応じた特色が出るポイントでもあり、利用者の使い方に合ったサービスを選定することが可能である。実際に始めたサ

ービスが拡張できずに、クラウドそのものを移行するケースにならないよう注意する。

2.4.3 時間帯による負荷対策

時間帯によって、仮想サーバや仮想ストレージのサービスの性能が落ちることがありますか？ 仮想サーバ、仮想ストレージ、内部ネットワークの一定以上の性能保証はされていますか？（Yes/No）
一部の利用者が CPU やディスク I/O などの共有リソースを占有しないように平準化する仕組みがありますか？

(1) 本質問の趣旨

クラウドが共有利用ということ为前提に、利用時の性能が他の利用者の影響を受けることがあるか、また契約した性能が保障されるかを確認する。

(2) アンケート回答と考察

多くのクラウド事業者は性能保証についてベストエフォートを謳いながらも一定以上の保証をしていると回答した。平準化の仕組みについては無回答が多かった。現時点で保障されるサービスはまだ少ないが、今後は差別化の上で新しいサービスとして性能保証を打ち出すサービスも考えられる。

2.4.4 大量データ移行サービス

大量データの移行に対応したサービスや特例措置はありますか？ （Yes/No） 例：利用者所有のディスク持込み、利用者環境とクラウドサービス間を接続する専用線の準備

(1) 本質問の趣旨

クラウドサービスを利用するにあたり、環境構築後に最初に発生する大きなイベントがデータ移行である。データ移行まで含めたサービスができるか否かは、利用者にとっては大きなポイントである。

(2) アンケート回答と考察

アンケート結果では、個別に対応すると回答したクラウド事業者があった。利用者にとってデータ移行ができるかできないかは、

事業停止時間を短くすることができるかどうかと関係するため、対応できるクラウド事業者の方が優位である。

2.4.5 禁止事項について

クラウドサービス利用に伴う、禁止事項はありますか？ (Yes/No)

(1) 本質問の趣旨

クラウド事業者が禁止している項目は利用者として最低限確認すべき項目である。同様にクラウド事業者特有の項目もあるので必ず確認する。違反した場合、サーバの隔離や停止、サービスの利用停止などの措置が発生する場合がある。

(2) アンケート回答と考察

ほとんどのクラウド事業者が禁止事項があると回答した。この内容に関しては利用者側が必ず確認すべき項目である。

2.5 運用関連

クラウドにおいても運用の高度化や効率化は重要な課題である。利用しているクラウドサービスによっては、システム運用の見直しやルールの改廃が必要になる場合がある。

SIer がクラウドサービス上に構築したシステムの安定稼働における関心事は、平常利用時の稼働状況の可視化と、障害発生時の利用者への通知内容やヘルプデスクの内容であるため、これらを確認する必要がある。

2.5.1 リソースの稼働状況監視と枯渇予知・通報

仮想サーバ及びリソースプールの稼働状況監視を行い、リソース枯渇の予知検知・通報機能を有していますか？（Yes/No）
--

(1) 本質問の趣旨

契約しているリソースプールの稼働状況を監視できることは当然であるが、異常値が検出された場合、どのような方法で通知されるかを確認する。リソースを消費していく、枯渇することが予測されるときに、その検知がいかに行えるか、どのようにしてその通報を受け取ることができるかは、枯渇してしまっても対応できずにシステムダウンを招く危険性を事前に回避するために必要な機能と考える。

(2) アンケート回答と考察

「運用管理サービスのオプションとして用意している」という回答もあったが、枯渇予知の通報ができるかという質問意図が伝わっていないためか「実施している」、「仮想サーバ、ハイパーバイザ、ストレージにて監視を行っている」という回答があった。

リソースプールの稼働状況が監視できる場合、どのような項目が監視できるか、例えば、契約している仮想サーバやストレージについて、CPU 使用率、メモリ使用率、トラフィック量、ストレージ I/O などの状態を監視できるかを確認する。監視項目について、リソース枯渇をどのように予知し、どのように通報するかは、サービス事業者によって差異があるので、サービス内容を確認する必要がある。

2.5.2 監視内容通知とヘルプデスク

利用者への監視内容を通知するサービスはありますか？ (Yes/No)
Yes の場合、どんな内容になりますか？
通知方法(メール)、通知レベル(info/Critical 等)、通知方法 (電話/メール)
ヘルプデスクサービスは提供されていますか？ (Yes/No)

(1) 本質問の趣旨

監視内容を通知する機能として、しきい値設定ができるか、メールによる通知が電話による通知か、利用者ポータルに表示されるのか、API が提供されているか、などを確認する。オプションで提供される場合もあるので、無償有償の範囲を確認し、利用するサービスを選定するための判断材料とする。

(2) アンケート回答と考察

すべてのサービス業者が、監視に関する通知機能を持っていて、メールで通知するという回答と、利用者が管理画面から確認するという回答があった。

メールでの通知では、「info レベル、Critical レベル」が設定でき、「プロセスの生死、ディスクやメモリ利用量のしきい値越えをメール通知する」という回答があった。

管理画面利用では、「契約品目や設定」「トラフィック量」「アクセスログ」等を利用者が管理画面で確認可能という回答があった。

ヘルプデスクについては、単に「有している」という回答のほか「有償サービスで提供」という回答もあった。

通常、通知機能は何らかの形で提供される。無償の範囲はどこまでか、オプションでどのようなレベルまで提供されるかを確認し、必要な機能を選択する必要がある。

2.5.3 顧客情報管理

顧客情報の管理方法は定義がありますか？

(1) 本質問の趣旨

ISMS、個人情報保護などについて、利用者情報の管理にポリシーがあるかを確認する。

(2) アンケート回答と考察

すべてのサービス業者から Yes との回答を得たが、補足説明にはバリエーションがある。「ISMS の監査を受けており、適切に

管理している」という回答や、「情報セキュリティ基本方針や個人情報保護ポリシーに沿って管理している」という回答があった。

「ポリシーがある」とだけ回答された場合には、どんな管理方法か、どんなポリシーに従っているかを追加確認し、具体的な内容を把握しておく必要がある。

2.5.4 問合せ時の本人確認

利用者からの問合せ時に本人確認はしますか？ (Yes/No)

(1) 本質問の趣旨

ヘルプデスクへの問い合わせで、どのように本人確認するのかを確認する。なりすましによるハッキングの可能性がないかを懸念している。

(2) アンケート回答と考察

本人確認するという回答が多いが、一部では本人確認しない、という回答もあった。本人確認する方法として、サービス ID を利用するという回答もあった。

本人確認しない、という場合はヘルプデスクで一般的な質問も受け付けている場合が考えられるが、契約者が契約範囲内の質問をする場合にも確認しないようなら、なりすましによる問い合わせも可能かもしれない。利便性と安全性とのトレードオフに留意する。

2.6 契約関連

クラウドサービスの利用のしやすさは、迅速にサービス提供を開始するのに、有力な決め手となる。

柔軟な手続きであればあるほど、サービス提供を早めることができる。

2.6.1 契約申込手段

新規契約時の利用申し込み手続きは、どのような手段で行えますか？

(1) 本質問の趣旨

企業(法人)が各種サービスを利用する際、(a)クラウド事業者の営業担当へ連絡し、(b)サービス規約と申込書(書面)を受け取り、(c)社内での決裁手続きを経て、(d)購買(調達)部門からの発注する、といった流れを取ることが一般的である。しかし、セルフサービス化によるコストダウンを競争力の源泉の1つとしている多くのクラウドサービス事業者において、実態がどうかを確認する。

(2) アンケート回答と考察

広く知られているように、Webやメールといったオンラインでの申し込みのみ可能というサービスもあるが、「Webも書面も可」という回答もあった。また基本的に「営業経由での手配」という回答もあり、わが国の商習慣を意識していることも垣間見ることができた。ただし、サービスの利用者を法人に限っているか、一般消費者まで広げているか(どこに重点を置いているか)でも対応は異なってくるものと想定される。

2.6.2 契約者の制限の有無

クラウドサービスを利用する契約者に制限はありますか？(Yes/No)

(1) 本質問の趣旨

サービスの対象者が法人のみか、一般利用者を含むかで、契約関連の内容が大きく異なることが想定されるため確認する。

(2) アンケート回答と考察

今回の回答はすべて「法人のみ」との回答であった。また「与信をパスした法人のみ」との回答もあった。一般に契約行為にあたっては与信審査を行うが、アンケート回答企業のうち、決済手

段がクレジットカードのみ、と回答した事業者は、クレジットカード会社を通じて、利用者の支払い能力の与信を行っている、と考えることができる。

2.6.3 損害賠償規定の有無

損害賠償の規程はありますか？ (Yes/No)

(1) 本質問の趣旨

SLA を遵守できなかった場合の損害賠償規程はあるのかを確認する。

(2) アンケート回答と考察

多くは「あり」と回答。「なし」と回答したサービス事業者も「検討中」という付言があった。損害賠償の範囲、程度、免責規程などについては、個々のサービスによって千差万別であるため、その比較は行っていないが、サービス規約が提示された事業者の損害賠償保障規程を見る限り、基本的にはサービス料以上の保障は得られないようである。

SIer にとっても、クラウドサービスの不具合を起因とするシステムダウン等の障害に対しては、その保証範囲は限定的にならざるを得ない。

2.6.4 最小契約の単位、期間

最小契約単位はありますか？ 例：1 仮想サーバ、1 カ月～
最小契約単位を下回り、一時的なりソース変更による課金の扱いはどうなりますか？ 例：最小契約期間が 1 か月の中、テストにより、1 日だけ仮想サーバを大量に作り、完了後削除した等

(1) 本質問の趣旨

提供サービスの内容に関する質問で、どれだけ手軽に使えるか、スモールスタートが可能かを確認する。

(2) アンケート回答と考察

最小契約単位（機能）は、1 仮想サーバからという回答が大半であった。最小契約単位（期間）は 1 ヶ月というのが一般的であったが、付加的なサービスの場合は 1 日単位というケースもあつ

た。一方で、最小契約単位は2ヶ月という回答もあったが、その理由までは聞き取れていない。

最小契約単位内での利用リソースの変更や途中での解約の際、日割計算されるかどうかはサービス事業者によって異なる回答となったが、従量制課金の場合は日割精算可、というのが一般的な傾向である。

興味深かったのは「サーバ使用料は日割可能であるが、OSは月単位」という回答である。ソフトウェアについてはライセンス料の規定の関係で柔軟な利用が難しいと考えられる。

2.6.5 初期費用と有無と課金体系

初期費用は発生しますか？（Yes/No）
利用料は完全固定確認、従量課金、固定＋従量課金のいずれかになりますか？（Yes/No）

(1) 本質問の趣旨

どれだけ手軽に使えるか、スモールスタートが可能かを確認する。

(2) アンケート回答と考察

初期費用は不要という回答が多かったが、法人限定でサービスを提供している事業者は初期費が必要という回答であった。

利用料については、「固定のみ」「固定または従量選択可能」「固定＋従量」と千差万別であった。従って、コスト比較を行う際は、システムの拡張計画も加味して行う必要がある。

一方、SIerがデータセンタ事業も取り扱っている場合、長期間の大規模なクラウド利用がハウジングやホスティングと比べてコスト高になるようであれば、プライベートクラウド提案やハイブリッド提案に結びつける戦略も考えられる。

2.6.6 決済手段

クラウドサービスにおける利用料の支払いはどんな方法がありますか？ 例：クレジットカード、口座振替など

(1) 本質問の趣旨

わが国では企業間の取引決済にクレジットを使うことは一般化していないものの、有名なクラウドサービスの決済手段がクレジ

ットカードのみである、ということに対し、各事業者がどのように応じているかを確認する。

(2) アンケート回答と考察

請求書の発行による指定口座への振込、引き落としとの回答が大半で、クレジットカード決済は不可と明示する回答もあった。わが国でのクラウドサービスは、わが国の商習慣を強く意識した決済手段で応じていると考えられる。

2.6.7 サービスの再販可否

クラウドサービスを契約した利用者がカスタマイズをして再販売や OEM 提供をできますか？
--

(1) 本質問の趣旨

この質問は、近年注目を浴びている「ホステッド・プライベート・クラウド」への活用が可能であるかどうかを確認するためである。クラウドサービスの SLA が顧客あるいは SIer の要求に十分応えるものとなっていない場合、パブリッククラウドの高度な機能やコストメリットを活用しつつ、不足する部分を補うのが、パブリッククラウドサービス(の一部)を特定企業が専有利用する「ホステッド・プライベート・クラウド」である。

(2) アンケート回答と考察

回答があったすべてのクラウドサービス事業者から「可能」との回答を得た。ただし、それが「ホステッド・プライベート・クラウド」としてのサービス提供を想定していたかどうかは不明であり、初期投資回収につながる大口需要については問題なしとしているのかもしれない。

2.6.8 個別対応の可否

大口契約の場合、サービスの個別対応など可能でしょうか？

(1) 本質問の趣旨

質問趣旨は質問 2.6.7 に同じであるが、小さな個別カスタマイズにも応じてしまうと維持コストが増大するため、海外のサービス事業者は一切受け付けない、というところが多いため確認する。

(2) アンケート回答と考察

一定の制限や要件にもよるが、少なくとも相談には応じる、と

いう回答が多かった。いかにもわが国の営業慣習を反映しているように思われるが「サービスビジネス」のあり方として正しいかどうかは議論の余地がある。

2.7 拡張性

クラウドサービスは、基本的にはインターネット接続で共有されたリソースを利用する形態となるが、多くの SI においては、既存システムと専用線で接続したり、リソースを占有できる専用サーバが必要となったり、利用者の機器を持ち込むというニーズが多い。そのため、共用リソースだけではない利用形態が可能なかを確認する必要がある。

2.7.1 機器持ち込み、ネットワーク接続形態

(a)	クラウドサービスがあるデータセンター内に利用者の機器持ち込みは可能でしょうか？ (Yes/No)
(b)	クラウドサービスのネットワークの接続はどんな接続形態がありますか？ 利用者が使っているネットワークアドレスの持ち込みはできますか？ (Yes/No)

質問 1-(a)

(1) 本質問の趣旨

標準に提供される機器だけでは実現できず、特殊な機器を利用せざるを得ない場合は、その機器をデータセンタに持ち込んで、パブリッククラウドサービスのリソースとネットワーク接続して利用しなければならない。その場合は、データセンタに機器を持ち込めるかがポイントとなる。

(2) アンケート回答と考察

機器持ち込みが可能という回答と持ち込み不可という回答が半々だった。

機器持ち込みができるかどうかはサービス業者のポリシー次第である。システム実現に機器持ち込みが必須かどうかを、まず検討すべきである。

持ち込みが可能な場合は、さらに、どんな機器が持ち込み可能か、どんな条件で持ち込み可能かを確認する。また、持ち込み条件を記載したドキュメントを要求し、実現可能性も確認する。

質問 1-(b)

(3) 本質問の趣旨

インターネットと安全に接続することが必須である。場合によ

っては、顧客の LAN と閉域網で接続することが求められる場合もある。インターネット接続でファイアウォール、パケットキャプチャ装置などを利用する場合や、専用線による接続、VPN による接続が、クラウドサービス事業者のデータセンタに機器設置できるか、あるいは、特別の機器の持ち込みが可能かどうか、そのデータセンタが使えるかどうかの判断基準となる場合がある。

クラウドサービス事業者のデータセンタで、既存に利用しているネットワークアドレスを持ち込みたい場合もあるが、利用者が指定するネットワークセグメントを利用できるか利用できないか確認する。

(4) アンケート回答と考察

クラウドサービスなのでインターネット接続ができることは前提である。それ以外に専用線接続できるという回答が多い。インターネット VPN、閉域網いずれも接続できるという回答も見られた。

専用線、VPN の接続については、接続方法、接続条件がそれぞれ異なるので、確認する必要がある。

ネットワークアドレスの持ち込みについては「可能なアドレスと不可能なアドレスがある」という回答や「原則できないが、PI アドレスの場合、サービスによっては可能」という回答があった。

持ち込み可能な場合でも、持ち込み可能なアドレスに制限がある場合が多いので、制約条件を確認する必要がある。

2.7.2 専用サーバ、専用ネットワーク

利用者がクラウドサービス上のリソースを占有できる専用サーバ、専用ネットワーク等のサービスはありますか？ (Yes/No)
--

(1) 本質問の趣旨

専用線、インターネット VPN などで、占有して接続できる手段が提供されているか、また、利用者が物理的にリソースを専有できるサーバがあるかを確認する。パブリッククラウドは、リソースを共有するので、セキュリティ上問題と考えたり、性能上の問題で占有したい、とする場合がある。

(2) アンケート回答と考察

ほとんどのクラウドサービス事業者で対応可能との回答であっ

た。個別見積りにて対応という業者もあり、メニュー化されておらず必要に応じて個別対応するというクラウドサービス業者もある。

専用サーバはハウジングと類似していて、利用者がコントロールできる分、データセンタの SLA 適用外の可能性もあるので、提供条件を確認する必要がある。

2.8 セキュリティ

多くのクラウドサービスは、基本的なセキュリティ要件は満たしていると考えるが、ここでは差異化要素として「クラウドサービスそのもののセキュリティ対策」について確認する。

「パブリック」なサービスであるがゆえに、ユーザ別の情報分離のためにどのような対策が取られているのかを確認する。

なお、セキュリティに関するガイドラインは、総務省、経済産業省、ASP・SaaS・クラウドコンソーシアムといった多くの機関から発刊されているので本書巻末のリストを参考にさせていただきたい。

2.8.1 センターファシリティのセキュリティレベル

センターファシリティのセキュリティレベルの公開はしていますか？ (Yes/No)

(1) 本質問の趣旨

ISO などの認証取得や自社セキュリティポリシーの観点から、クラウドサービス運営データセンタのセキュリティレベルの公開が必要になる場合がある。

(2) アンケート回答と考察

提供サービスが自社データセンタでの運営でないケースも多くあり、非公開との回答もあった。しかしながら、クラウドサービスとして ISMS 監査を受けているとの回答も得られた。

2.8.2 クラウドサービスに対するセキュリティ対策

クラウドサービスとしてのセキュリティ対策は明示されていますか？ (Yes/No) (特に、他利用者への情報漏えい対策)

(1) 本質問の趣旨

クラウドサービス事業者としてサービスに対する具体的なセキュリティ対策について公開されているか確認する。

(2) アンケート回答と考察

一般的には、約款や Web 上でホワイトペーパー等で情報公開されているが、保安上の理由から公開しないケースもあるので、情報を見つけれない場合は、事業者個別に確認する。

2.8.3 利用者が遵守すべきセキュリティ要件

利用者が遵守すべきセキュリティ要件はありますか？ あるとすれば、それが遵守されていることをどのような手段で確認していますか？

(1) 本質問の趣旨

クラウドサービス事業者として、サービスをより安全に提供する目的から利用者に対し遵守すべきセキュリティ要件を出しているか、出しているとすればどのような手段で遵守しているかを確認する。

(2) アンケート回答と考察

本件を明示しているケースは少ない。業者によっては、サービス契約時にサービス利用者は、ウィルス等の有害なコンピュータプログラムに対する適切な対策など、セキュリティ対策を実施する責任を負うと明示していたり、事業者が必要と判断した場合には報告を求めることができる旨の同意書をとるケースがあるので注意が必要である。

2.8.4 利用者の監査法人に対する対応

利用者の監査法人への対応のために、要件や構成変更を求められることがありますか？（Yes/No）

(1) 本質問の趣旨

サービス利用者が監査法人から、クラウドサービスに関する情報開示を要求された場合、対応可能かどうかを確認する。

(2) アンケート回答と考察

多くのサービスが監査法人からの情報開示に対応していないことを前提に監査法人への対応を検討するべきである。

2.8.5 セキュリティ攻撃に対する対応

国内・海外からの攻撃に対しての対応はどうしていますか？ PRとして特出するセキュリティ対策がありますか？

(1) 本質問の趣旨

クラウドサービスは、海外からの攻撃対象とされやすいが、特

筆すべき対策があるかどうかを確認する。

(2) アンケート回答と考察

本件に対する対応は、保安上の関係から公開されないケースが多い。一般的にアクセス検知を行い攻撃と判断された場合、当該経路の遮断を行っていると思われる。

2.8.6 ペネトレーションテストの実施

クラウドサービス上のセキュリティを確認するために、定期的にペネトレーションテストは実施していますか？ (Yes/No)

(1) 本質問の趣旨

既知の攻撃方法や侵入方法などをシステムに対して実際に行うことで、セキュリティ上の弱点を発見するテストを、クラウドサービス事業者として取り組んでいるかを確認する。

(2) アンケート回答と考察

サービス業者により取り組みは異なる。また、本件に関する情報は Web 等の公開情報からは知ることは困難であるのでサービス業者に個別に確認する必要がある。ただし、ペネトレーションテストの実施詳細についての情報開示は困難と思われる。

2.8.7 サービス基盤内ネットワーク分離について

クラウドサービスの基盤内で、サービス環境のネットワークと管理系ネットワークは物理的に分離されていますか？ (Yes/No)

(1) 本質問の趣旨

利用者の通信経路とサービス事業者の経路が分離されていない場合、サービス事業者内からのセキュリティ事故が起こる可能性が高くなる。そのリスクがあるかどうかを確認する。

(2) アンケート回答と考察

本件を明示している業者は少ない。一般的には、分離されていると考えるが、サービス業者によっては回答を差し控えるケースがある。確認のしやすい質問でありリスクを認知するうえでも質問することをお勧めする。

第3章 新たな観点

3 新たな観点

今回の調査では4章に示した「クラウド事業者へのアンケート票」を用いたが、調査後、さらに押さえておくべき観点があるとの指摘を頂戴した。アンケート票の追加項目として加えていただきたい。

3.1 サービス継続性

- **トラブル発生時の目標復旧時間(RTO:Recovery Time Objective)**
トラブル発生時の対処方法は質問しているが、復旧時間を問う質問項目は本票にはなかった。トラブルによる停止時間は、顧客へのサービス停止時間でもある。SIerとしては「時間」管理することは重要である。

第4章

参考文献ほか

4 参考文献ほか

4.1 クラウド事業者へのアンケート票

今回の調査で使用したアンケート帳票を紹介する。

クラウド事業者へのアンケート票

分類	通番	質問内容	回答内容	参考資料 (URL など)
サービスの継続性	1.1	<ul style="list-style-type: none"> クラウドサービスにおける稼働率(SLA)の定義はありますか？ (Yes/No) SLA の定義は一般公開されていますか？ (Yes/No) 		
	1.2	<ul style="list-style-type: none"> クラウドサービスで提供される仮想サーバ上で動作するアプリケーションの動作保証は、行われますか？ (Yes/No) 		
	1.3	<ul style="list-style-type: none"> 物理サーバやストレージにウィルスやバグなどの不具合を検知した場合の対処方針はありますか？ (Yes/No) サービス停止を伴うメンテナンス作業を行う場合、利用者との調整を行う際の方針はありますか？ 		
	1.4	<ul style="list-style-type: none"> 定期メンテナンスや緊急メンテナンスの実施はありますか？ (Yes/No) 利用者へのメンテナンスの通知方法は具体的にどのような方法がありますか？ 		
	1.5	<ul style="list-style-type: none"> クラウドサービスのシステム基盤上で、EOSL(end of service life)対応の作業を行う場合、利用者に連絡を行っていますか？ (Yes/No) 		
	1.6	<ul style="list-style-type: none"> クラウドサービス事業者の都合により、クラウドサービスの提供が終了する場合、利用者へサービス停止の何カ月前に通知されますか？ 		
	1.7	<ul style="list-style-type: none"> DR(Disaster Recovery)に対応するサービスメニューはありますか？ (Yes/No) サービスメニューがない場合は、DR を実現するための代替サービスはありますか？ 		
バックアップデータ 保全	2.1	仮想サーバおよび仮想ストレージに対するバックアップは、クラウドサービスとして提供されていますか？ 以下の中から最も当てはまるものを選択願います。 1)標準契約に含まれる 2)バックアップを含むサービスメニューがある（そのサービスに関して簡単にご説明ください） 3)バックアップサービスが単独のサービスとして存在する 4)標準サービスとしては存在しないが、個別対応が可能である 5)バックアップを含むサービスは提供していない 6)その他（具体的にご記載ください）		
	2.2	<ul style="list-style-type: none"> 稼働中の仮想サーバのイメージコピーを取得できるメニューはありますか？ (Yes/No) 		
	2.3	<ul style="list-style-type: none"> クラウドサービスで提供される仮想サーバおよびストレージ上のデータは保証されていますか (Yes/No) 		
OS/ミドルウェアの動作保証マイグレーション	3.1	<ul style="list-style-type: none"> ベンダーからの動作保証を得ているミドルウェアやソフトウェアがありますか？ (Yes/No) 例：Oracle 		
	3.2	<ul style="list-style-type: none"> ミドルウェアを含む既存システムをクラウドサービス上にマイグレーションするサービスはありますか？ (Yes/No) 		
	3.3	<ul style="list-style-type: none"> 利用者の構築した仮想サーバイメージを、クラウドサービス上にインポートすることは可能でしょうか？ 		
	3.4	<ul style="list-style-type: none"> 現在提供されている仮想サーバの、サポートサービスが ESOL(End Of Service Life)により提供停止となった場合、クラウド事業者としてどのように対応しますか。 		
性能保証	4.1	<ul style="list-style-type: none"> クラウドサービスの基盤に使う物理サーバやストレージなどハードウェアの選定基準はありますか？ (Yes/No) 		
	4.2	<ul style="list-style-type: none"> 仮想サーバや仮想ストレージスケールアップ、スケールアウトの制限は利用者へ明示されていますか？ (Yes/No) 		
	4.3	<ul style="list-style-type: none"> 時間帯によって、仮想サーバや仮想ストレージのサービスの性能が落ちることがありますか？ 仮想サーバ、仮想ストレージ、内部ネットワークの一定以上の性能保証はされていますか？ (Yes/No) 一部の利用者がcpu やディスク I/O などの共有リソースを占有しないように平準化する仕組みがありますか？ 		
	4.4	<ul style="list-style-type: none"> 大量データの移行に対応したサービスや特例措置はありますか？ (Yes/No) 例：利用者所有のディスク持込み、利用者環境とクラウドサービス間を接続する専用線の準備 		
	4.5	<ul style="list-style-type: none"> クラウドサービス利用に伴う、禁止事項はありますか？ (Yes/No) 		

分類	通番	質問内容	回答内容	参考資料 (URL など)
運用関連	5.1	・仮想サーバ及びリソースプールの稼働状況監視を行い、リソース枯渇の予知検知・通報機能を有していますか？ (Yes/No)		
	5.2	・利用者への監視内容を通知するサービスはありますか？ (Yes/No) ・Yes の場合、どんな内容になりますか？ 通知方法(メール)、通知レベル(info/Critical 等)、通知方法 (電話/メール) ・ヘルプデスクサービスは提供されていますか？ (Yes/No)		
	5.3	・顧客情報の管理方法は定義がありますか？		
	5.4	・利用者からの問合せ時に本人確認はしますか？ (Yes/No)		
契約関連	6.1	・新規契約時の利用申し込み手続きは、どのような手段で行えますか？		
	6.2	・クラウドサービスを利用する契約者に制限はありますか？ (Yes/No)		
	6.3	・損害賠償の規程はありますか？ (Yes/No)		
	6.4	・最小契約単位はありますか？ 例：1 仮想サーバ、1 カ月～ ・最小契約単位を下回り、一時的なリソース変更による課金の扱いはどうなりますか？ 例：最小契約期間が 1 か月の中、テストにより、1 日だけ仮想サーバを大量に作り、完了後削除した等		
	6.5	・初期費用は発生しますか？ (Yes/No) ・利用料は完全固定確認、従量課金、固定+従量課金のいずれかになりますか？ (Yes/No)		
	6.6	・クラウドサービスにおける利用料の支払いはどんな方法がありますか？ 例：クレジットカード、口座振替など		
	6.7	・クラウドサービスを契約した利用者がカスタマイズをして再販売や OEM 提供をできますか？		
	6.8	・大口契約の場合、サービスの個別対応など可能でしょうか？		
拡張性	7.1	・クラウドサービスがあるデータセンター内に利用者の機器持ち込みは可能でしょうか？ (Yes/No) ・クラウドサービスのネットワークの接続はどんな接続形態がありますか？ 利用者が使っているネットワークアドレスの持ち込みはできますか？ (Yes/No)		
	7.2	・利用者がクラウドサービス上のリソースを占有できる専用サーバ、専用ネットワーク等のサービスはありますか？ (Yes/No)		
セキュリティ	8.1	・センターファシリティのセキュリティレベルの公開はしていますか？ (Yes/No)		
	8.2	・クラウドサービスとしてのセキュリティ対策は明示されていますか？ (Yes/No) (特に、他利用者への情報漏えい対策)		
	8.3	・利用者が遵守すべきセキュリティ要件はありますか？ あるとすれば、それが遵守されていることをどのような手段で確認していますか？		
	8.4	・利用者の監査法人への対応のために、要件や構成変更を求められることがありますか？ (Yes/No)		
	8.5	・国内・海外からの攻撃に対する対処はどうしていますか？ PR として特出するセキュリティ対策がありますか？		
	8.6	・クラウドサービス上のセキュリティを確認するために、定期的にペネトレーションテストは実施していますか？ (Yes/No)		
	8.7	・クラウドサービスの基盤内で、サービス環境のネットワークと管理系ネットワークは物理的に分離されていますか？ (Yes/No)		

4.2 主な SLA ガイドラインリスト(2014 年 3 月現在)

ウェブ等で公開されている SLA ガイドラインをリストアップした。クラウド SLA 以外も含んでいる

主なSLAガイドラインリスト

	書名	出典	発行日	入手先
1	クラウドサービス総覧 2014 年春版 IaaS/PaaS 編	日経 BP	不明	http://itpro.nikkeibp.co.jp/article/Active/20140219/537647/?bpnet
2	クラウドサービス提供における情報セキュリティ対策ガイドライン～利用者との接点と事業者間連携における実務のポイント～	総務省	2014 年 4 月	http://www.soumu.go.jp/main_content/000283647.pdf
3	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	経済産業省	2014 年 3 月	http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf
4	クラウドセキュリティガイドライン活用ガイドブック	経済産業省	2014 年 3 月	http://www.meti.go.jp/press/2013/03/20140314004/20140314004-3.pdf
5	ASPIC が取組んできたガイドライン・指針等	ASP・SaaS・クラウドコンソーシアム	2014 年 3 月	http://aspicjapan.org/information/guideline/index.html
6	クラウド情報セキュリティ管理基準	日本セキュリティ監査協会	2013 年 8 月	http://www.jasa.jp/information/result/pdf2011/2011_cloud_doc02.pdf
7	自治体クラウドの情報セキュリティ対策等に関する調査研究 報告書	総務省	2013 年 5 月	http://www.soumu.go.jp/main_content/000224718.pdf
8	民間向け IT システムの SLA ガイドライン 第四版	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, SLA/SLM 専門委員会	2012 年 3 月	http://www.amazon.co.jp/dp/4822262642
9	SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0	Cloud Security Alliance	2011 年 11 月	https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
10	クラウド ASP・SaaS 利用者の必要知識と関連ガイドライン等について	ASP・SaaS・クラウドコンソーシアム	2011 年 10 月	http://www.jtp.co.jp/service/ict/minutes/20111003/ict20111013_2_2.pdf
11	クラウドサービス利用者の保護とコンプライアンス確保のためのガイド	ASP・SaaS・クラウドコンソーシアム	2011 年 7 月	http://www.aspicjapan.org/information/guideline/pdf/jp_ver1.0.pdf
12	「中小企業のためのクラウドサービス安全利用の手引き」対応 クラウド事業者による情報開示の参照ガイド	独立行政法人情報処理推進機構	2011 年 4 月	http://www.ipa.go.jp/files/000011596.pdf

	書名	出典	発行日	入手先
13	中小企業のためのクラウドサービス安全利用の手引き	独立行政法人情報処理推進機構	2011年 4月	http://www.ipa.go.jp/files/000011595.pdf
14	クラウド時代の法制度と情報セキュリティ	情報セキュリティ大学院大学	2011年 2月	http://lab.iisec.ac.jp/~hayashi/FRI2.pdf
15	クラウドサービスレベルのチェックリスト	経済産業省	2010年 8月	http://www.meti.go.jp/press/20100816001/20100816001-4.pdf
16	スマート・クラウド研究会報告書 スマート・クラウド戦略	総務省? スマート・クラウド研究会	2010年 5月	http://www.soumu.go.jp/main_content/000066036.pdf
17	地方公共団体におけるASP・SaaS 導入活用ガイドライン	総務省	2010年 4月	http://www.soumu.go.jp/main_content/000061022.pdf
18	SLA 適用領域の拡大に関する調査報告書－エグゼクティブサマリー	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	2010年 3月	http://home.jeita.or.jp/is/publica/2009/is-09-jyousi-5/index.html
19	SaaS 向け SLA ガイドライン	経済産業省	2008年 1月	http://www.meti.go.jp/committee/materials/download/files/g80207c05j.pdf
20	民間向け IT システムの SLA ガイドライン ー追補版：SaaS 対応編	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、SLA/SLM 専門委員会	2008年 1月	http://home.jeita.or.jp/is/committee/solution/guideline/080131/080131SaaS_a.pdf
21	<付録1 / 付録2：SaaS 対応サービスレベル項目一覧表(Excel 版)>	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、SLA/SLM 専門委員会	2008年 1月	http://home.jeita.or.jp/is/committee/solution/guideline/080131/100224_SaaS080122.xls
22	ASP サービスモデル利用規約と解説	情報サービス産業協会	2005年 3月	http://www.jisa.or.jp//tabid/272/pdid/16-J004/Default.aspx
23	情報システムに係る政府調達への SLA 導入ガイドライン	独立行政法人 情報処理推進機構	2004年 3月	http://www.meti.go.jp/policy/it_policy/tyoutatu/tyoutatuSLAGuideline.pdf

—禁無断転載—

26-J002

クラウドインテグレーションにおける SLA の検討ポイント

平成 26 年 11 月発行

発行：一般社団法人情報サービス産業協会

〒104-0028 東京都中央区八重洲 2-8-1 日東紡ビル 9 階

TEL 03-6214-1121

URL <http://www.jisa.or.jp/>

©Copyright, Japan Information Services Industry Association, 2014

