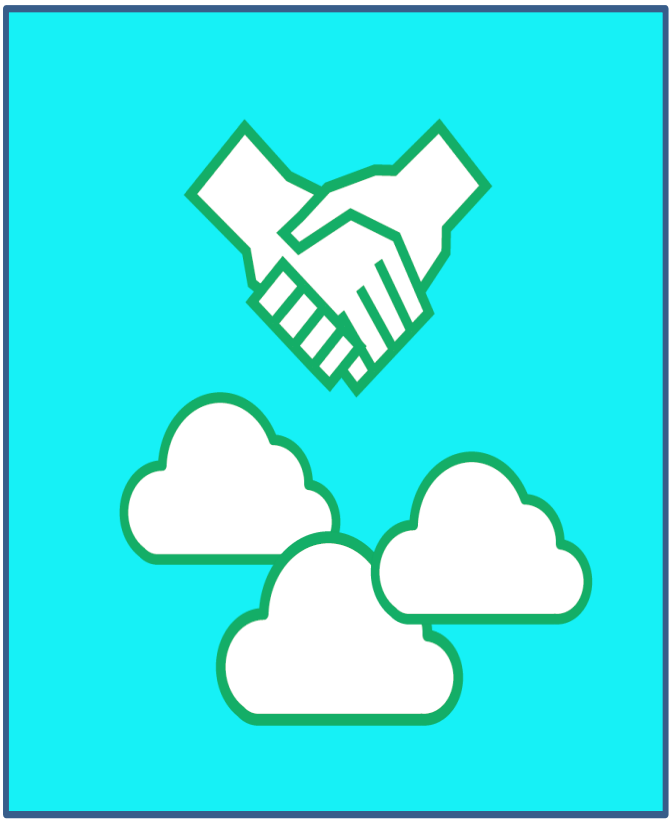


クラウドサービス利用者と SIer のための可用性確保ガイドライン

—IaaS を対象—

Ver1.0

概要

クラウドサービスの利用の拡大とともに、クラウドサービスの障害を原因としたシステム障害の報道・報告が増加している。

利用者側のクラウドサービス仕様や責任範囲への認識不足、障害発生に備えた可用性への対策不足が一因で、クラウドサービスの障害発生時に利用者業務への大きな影響につながっていると考える。

これを解決するため、３つの指標（サービス切替時間、稼働率、業務継続の要求度）を活用したクラウドサービス利用者と SIer のためのガイドラインを提案する。本ガイドラインは、２０１９年度　特定課題研究　「クラウドサービス利用における利用者視点での可用性確保の考察－ＩａａＳに関して－　」の内容に加筆したものである。

情報セキュリティ大学院大学　伊藤吉史

mgs194702 AT iisec.ac.jp　AT=@

変更履歴

２０２０．３．２１　初版発行

クラウドサービス利用者と SIer のための可用性確保ガイドライン

目次

1　ガイドラインのねらい

近年、クラウドサービスの利用が拡大しているが、クラウドサービスの障害を原因としたシステム障害の報道・報告が増加しつつある。クラウドサービス事業者に原因があるサービス障害の発生も要因ではあるが、利用者側のクラウドサービス仕様や責任範囲への認識不足、障害発生に備えた可用性への対策不足が一因で、クラウドサービスの障害発生時に利用者業務への大きな影響につながっていると考える。

この問題について、本ガイドラインでどのように解決できるかを以下に示す。

・クラウドサービス利用での可用性確保対策不足によって、どのようなシステム障害が起こっているかの事例とその背景を理解することにより、対策が必要であることが認識できる。
・クラウドサービス利用での可用性確保のため、３つの指標　①サービス切替時間、②稼働率、③業務継続の要求度　が重要であることが理解できる。
・可用性確保の３つの指標を使って、クラウドサービス利用者が可用性の要求を具体化し、ＳＩｅｒが可用性を確保したシステム構成を具体的に提示できる。

本ガイドラインは、クラウドサービスの内、ＩａａＳを対象とする。
利用者が具体化すべき可用性の要求の指標（メトリクス）を解説し、ＳＩｅｒが要求された指標に基づいて可用性対策が提案できることを目的としている。ガイドラインの主な読み手はＳＩｅｒを想定しているが、利用者自身がＳＩｅｒに対して可用性の要求を十分に検討して提案を行っているか検証するためにも活用できる。

適用範囲は以下のとおり
・ガイドラインの活用の工程は共通フレーム２０１３[1]の体系に当てはめると、2.2 要件定義プロセスと 3.1 運用プロセス が該当する。
・本ガイドラインでは、非機能要件のうち、可用性を対象としている。
　その他の非機能要件に関しては「非機能要求グレード」の可用性以外の要件の考え方や「高回復力システム 基盤導入ガイド」[2]の考え方がクラウドサービス利用に活用できる。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

2　システム障害の事例と背景

2.1　クラウドサービス利用における可用性確保不足によるシステム障害の事例

クラウドサービスはサービスの性質上、設備の増強、システム構成変更が日々発生し、各種変更でのシステムトラブルが起きやすい。またサイバー攻撃にも狙われやすい。これらの障害要因への利用者の認識不足から、利用者の業務に大きな影響のあるシステムトラブルが発生している。

2.1.1 クラウドサービスの障害による利用者システムでの業務影響の違い

２０１９年8月２３日、ＡＷＳ（アマゾンウェブサービス）の東京リージョンの４つのアベイラビリティーゾーン（以下ＡＺと省略して表記する。）の１つのＡＺで一定割合のサーバー（コンピューティングおよびストレージサービス等）が温度上昇のためシャットダウンまたはハードウェアの故障が発生した。このため、利用していた企業の公式発表などによると３０社超でシステム障害が発生した。[3]

複数のＡＺに冗長化していた場合は、システムの停止はなかったとの報道もあった。しかしながら、負荷分散装置の問題により、障害を回避できていなかった利用者のシステムがあると AWS からの報告があった。

冗長化の実装や生死監視による障害箇所の切り離し等、クラウドサービスの障害への利用者の認識と、障害対応の備えの違いによって、システム障害による利用者業務への影響に違いが出ている。

① 障害対策できていなかった利用者

障害対策ができていなかった利用者は以下のような状況になった。

・障害が発生したＡＺのみでシステムを構成していたので、ネットワークの輻輳が生じて利用者からリソースの制御ができない事象が発生しインスタンスの再起動ができなかった。

・マルチＡＺ構成としていたが、端末からの通信セッションの接続先ＶＭを固定化するアプリケーションプログラムの作りをしていて、障害 AZ から正常なＶＭへの通信セッションの切替ができなかった。(オンプレからクラウドに移行したケースに多い)

・2 つのＡＺを利用して、マルチＡＺの構成としていたが、障害 AZ を切り離せなかった。(ＡＷＳのサービス仕様では 3 AZ であれば切り離せた)仕様は理解していたが、対策をとっていなかった。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

② 障害対策ができていた利用者

障害対策ができていた利用者は以下のようにシステムの障害を回避できた。

・クラウドサービスの生死監視により障害になった負荷分散サービスやＷＡＦなどマネジメントサービスを切り離した

・端末からの通信セッションをＶM固定化をしないシステムの実装をしていたので、障害ＡＺから正常なＡＺへの通信セッションの切替ができ、業務を継続することが出来た。

・複数の AZ の利用方法を３重化していたので、障害 AZ を切り離しして障害を回避した。

2.1.2 クラウドサービス利用者がサービス仕様を具体的に認識していなかったことによるシステム障害

① ネットワーク通信断の認識違い

ある利用者は、オンプレミスで構築した、代理店との受発注システムをクラウドサービス上に移行した。その際、業務アプリケーションの見直しは特に行っていなかった。クラウドサービス事業者のネットワーク装置の保守作業時、３０秒の通信断が発生したところ、セッションタイムアウトが多発し、大きな業務影響が発生した。３０秒までの通信断については、クラウドサービスの仕様書に記載があったが、利用者は可用性の要求を具体化しクラウドサービスの仕様の確認をしてはいなかった。クラウドサービス事業者は、サービス仕様の範囲のため、保守作業による通信断について、利用者への事前連絡は行わなかった。利用者とクラウドサービス事業者の認識の相違がネットワーク装置の保守時に顕在化した。

② ＶM停止時間の認識違い

あるオンプレミスから移行した利用者では、クラウドサービスの一部の物理ハード障害により、ＶMの再起動が発生した。３分でＶMは再起動したが、サービス仕様にある、最大５分の停止が考慮されておらず、利用者のシステムが停止し、大きな利用者の業務影響が発生した。ＶM再起動の発生時に利用者とサービス事業者の認識の相違が顕在化した。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

2.2 クラウドサービス利用における利用者とＳＩｅｒの関係

このように、クラウドサービスは、様々な要因からサービス停止となる可能性があり、実際に、サービス停止が起きている。しかしながら、上記のシステムトラブル事例にあるように、利用者はクラウドサービスの可用性の実態についての理解が不足している。その背景には、日本におけるクラウドサービスの利用は、ＳＩｅｒがクラウドサービス事業者の間に入って、システム開発を行うことにある。[4] 利用者である企業はＩＴに関する専門技術の蓄積はないため、業務のシステム化要求はできたとしても、非機能である可用性に関しては、自ら主体的に関わってきていない利用者が多い。利用者のシステムの可用性の要求実現は、クラウドサービス仕様を前提に、利用者とＳＩｅｒが共同して行うべきものである。

図表１　クラウドサービス利用における関係

クラウドサービスを利用したシステムの可用性を確保し、システムトラブルの影響を受けない業務システムとするためには、利用者がシステム化する業務の可用性への要求を具体化し、ＳＩｅｒは、クラウドサービスの仕様で実現できるところ、できないところを明確にして、認識を共有する必要がある。

クラウドサービスの仕様で可用性を実現できないところを、システム開発・運用として対策していくか、要求を変更するかを、利用者とＳＩｅｒが認識あわせしていかなければならない。クラウドサービスの仕様は障害発生を前提としている。クラウドサービスの可用性に不確定要素が多いことを認識し、受容するか、回避するかを決めなければならない。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

3　システム構築時に検討すべき事項

3.1 非機能要求グレードの活用

利用者の要求にＳＩｅｒが認識を共有し、適切な対応をする目的で作られているガイドラインに、「非機能要求グレード」がある。「システム基盤の発注者要求を見える化する非機能要求グレード検討会」で２０１０年に公開され、活用されている。現在はＩＰＡにて公開されている。[5]

非機能要求の大項目には可用性があり、その中項目の継続性は、さらに、業務継続性、稼働率の小項目に分かれ、対象業務範囲毎に、サービス切替時間、業務継続の要求度、稼働率の指標（メトリクス）に細分化される。

小項目	小項目説明	メトリクス	参考レベル	説明
業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。	対象業務範囲	内部向けバッチ系業務から全ての業務の５レベル	対象業務範囲とは、稼働率を算出する際の対象範囲を指す。
		サービス切替時間	２４時間未満から６０秒未満の５レベル	対策を施すこと（例えばクラスタ構成でのサーバの切替えなど）により、業務再開までに要する時間を指す。
		業務継続の要求度	障害時の業務停止を許容する、から二重障害時でもサービス切替時間の規定内で継続するの３レベル	発生する障害に対して、どこまで業務を継続させる必要があるかを示す考え方の尺度
稼働率	明示された利用条件の下で、システムが要求されたサービスを提供できる割合。	稼働率	９５％以下から、９９．９９９％までの５レベル	

図表２　業務継続性、稼働率の指標（メトリクス）

これらの３つの指標（メトリクス）①サービス切替時間、②稼働率、③業務継続の要求度を、クラウドサービス利用の可用性確保に適用する。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

3.2　3 つの指標の活用方法

3.2.1 サービス切替時間

クラウドサービスは、利用者からみると通常でも短時間の故障が発生している。ネットワークの通信断、VM の再起動、物理サーバーの障害様々あるが、クラウドサービス事業者はサービスの「障害」とは定義しておらず、利用者が対策すべきものとされている。クラウドサービスにおいて、サービス切替時間に影響を与えるＩａａＳの構成要素を以下にまとめる。

	A社	B社	C社
VM、物理サーバー	5分程度	5分未満	5分未満 (再起動) 15分(他サーバー)
ストレージ、 物理ディスク	3分程度	1～2分	未定義
ネットワーク	数秒	未定義	未定義

図表３　主なクラウドサービス事業者のＩａａＳ構成要素毎
のサービス切替時間

主なクラウドサービス事業者のサービス切替時間を見ると、５分程度のＶＭのサービス切替時間の考慮が必要である。

サービス切替時間の指標（メトリクス）を検討すると利用者の対象業務毎に、許容できるサービス切替時間を確認し、ＳＩｅｒは上記の切替時間を考慮した可用性のあるシステムを開発・運用する必要があることが導ける。具体的には、利用者からの通信（アプリケーションレベル)をどの VM でも処理可能な実装をしたり、ネットワーク切替に対応したリトライ通信の実装が必要であることが導ける。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

3.2.2　稼働率

クラウドサービス事業者は、「稼働率」をＳＬＡで設定している。利用しているインスタンスの稼働率ではなく、合意したサービスの範囲の稼働率である。例えば、二つ以上のＡＺの利用で同時に接続不可といった条件である。

また、ＳＬＡの稼働率を守れなかった場合は、業務損害の補償ではなく、サービスクレジットという、一定割合のサービス利用権の設定や、サービス料金の返金を行うとしている。例えば、利用者のシステムの稼働率の要求が９９．９９％である場合、クラウドサービス事業者のＳＬＡに記載されている稼働率が９９．９９％であっても、サービスクレジットが許容できなければ、利用者の要求を満たすことができない。

従って、本ガイドラインでの稼働率の指標の定義は、「非機能要求グレード」の考え方を拡張し、クラウドサービス事業者が提示する稼働率の数値だけではなく、クラウドサービス事業者が定義する稼働率の計算範囲やＳＬＡ違反の場合の補償も含めたものとする。

ＶＭ等のコンピューティングリソースについて主なクラウドサービス事業者の稼働率やサービスクレジットについて以下にまとめる。

	A社	B社	C社
対象リソース	VM	VM	VM
稼働率	月間稼働率 99．99% 3分以上障害が継続した時間の累計 メンテナンス、フェイルオーバー除外	月間稼働率 99．99% 2つ以上のAZの利用で同時に接続不可	月間稼働率 99．99% リージョン内の 2 つ以上の可用性ゾーンにまたがりデプロイした 2 つ以上のインスタンスがある場合
サービスクレジット	当月分料金10%減額	料金10%を将来の支払いに適用	10%料金返金

図表４　主なクラウドサービスのＳＬＡでの稼働率およびサービスクレジット

稼働率の指標を検討すると利用者とＳＩｅｒは、月間の稼働率の条件やＳＬＡ違反が生じた場合、サービスクレジットの補償で要求が満足できるか確認できる。満足できない場合は、サービスのＳＬＡ違反を前提に、複数のクラウドサービスを利用するマルチクラウドでの冗長化したシステムの開発・運用が必要であることを導くことができる。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

3.2.3　業務継続の要求度

可用性を確保するためにシステムを構成する要素の冗長化を行うが、その基本として単一障害点をなくす考え方がある。オンプレミスのシステムでは、物理サーバーの冗長化やストレージによるＤＢサーバーの冗長化により、単一障害点をなくす方法が一般的である。しかしながら、クラウドサービス事業者が障害発生を前提としていることから、一つのＡＺ内での冗長化では単一障害点をなくすことにはならない。

一つのＡＺを単一障害点（ＳＰＯＦ）ととらえると「非機能要求グレード」で示されているユーザ要求は、下記のように整理できる。

レベル	利用者要求（指標）	クラウドサービスの構成
レベル1	障害時の業務停止を許容する。	シングルAZ
レベル2	単一障害時は業務停止を許容しない。	マルチAZ
レベル3	二重障害時でもサービス切替時間の範囲内で継続する。	複数のクラウドサービスの利用（マルチクラウド）

図表５　ユーザ要求とクラウドサービスの構成の対応

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

3.2.4 指標からクラウドサービスの構成を選択する方法

稼働率と業務継続の要求度の指標からクラウドサービスの構成を選択する方法を以下に示す。

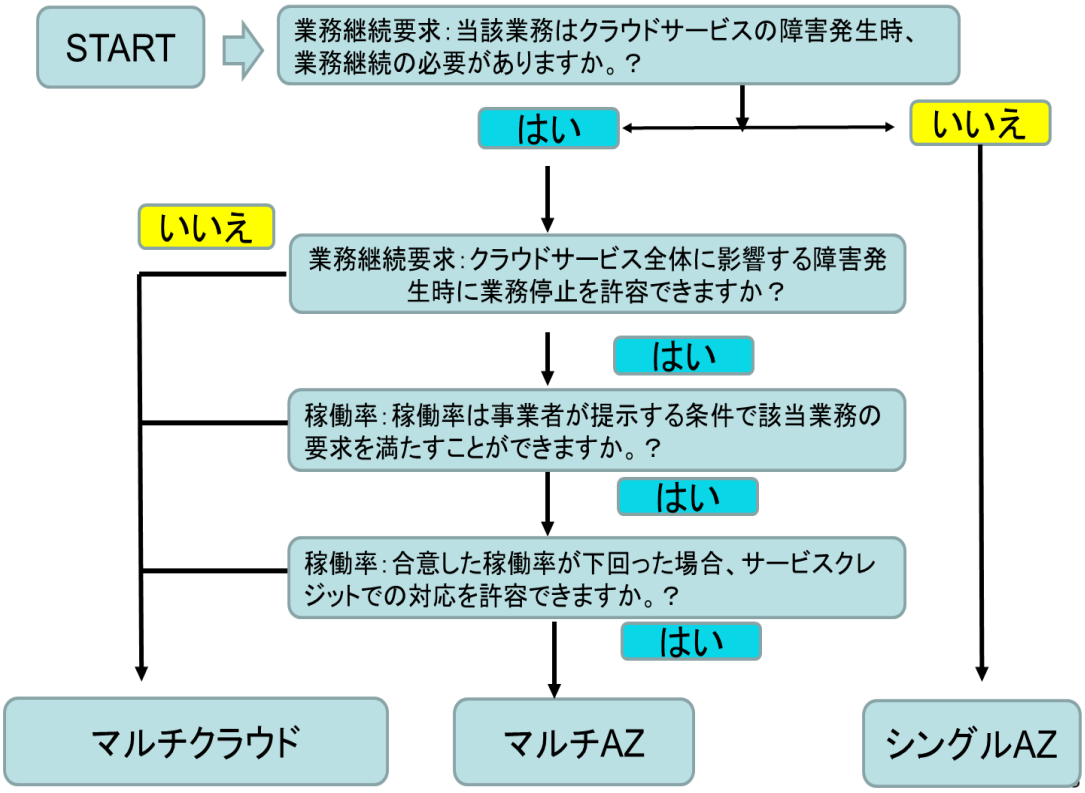
まず、業務継続の要求度に着目し、クラウドサービスの障害時発生時に業務継続が必要か確認する。障害時に業務停止が許容できる場合は、シングル AZ を選択する。

クラウドサービスの障害時発生時に業務継続が必要な場合は、障害の許容範囲を確認する。サービス全体に障害の影響が及ぶ場合を許容できる場合は、稼働率の許容範囲を確認する。

クラウドサービス事業者が提示した稼働率で、稼働率違反があった場合に、サービスクレジットでの対応で許容できる場合は、マルチ AZ 構成を選択する。

サービス全体に障害の影響が及ぶ場合でも業務を継続したい、クラウドサービス事業者が提示する稼働率では許容できない、稼働率がＳＬＡを下回った場合にサービスクレジットの補償では許容できない場合は、複数の業者を利用するマルチクラウドを選択する。

以上の選択方法をまとめると、以下のフローになる。



図表 6　システム構成の検討フロー

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

3.3　利用者の要求に対応した可用性確保の提示方法

①　利用者の業務範囲毎の可用性の要求をメトリクス毎に表で整理する。
以下に例を示す。

対象業務	利用者要求（指標）		
	サービス切替時間	業務継続の要求度	稼働率
業務A	10分以上 許容	障害時停止許容する	95% （サービスクレジット許容）
業務B	10分未満	単一障害時は業務停止を許容しない。	99．9% （サービスクレジット許容）
業務C	5分未満	二重障害時でもサービス切替時間の範囲内で継続する。	99．99%

図表７　業務範囲毎の可用性の要求の整理例

システム全体ではなく、業務範囲毎にユーザ要求を確認することが重要である。また、一旦決めた可用性を業務範囲の重要度を棚卸して、変更することも必要である。情報資産の棚卸という観点でも必要である。

②　利用するクラウドサービスの候補の選択と整理

利用するクラウドサービスの候補をいくつか選択し、サービス仕様や、ＳＬＡを参照し、サービス切替時間、稼働率について、図表３、４のように整理を行う。

③　対象業務毎の可用性確保案の検討

対象業務毎に、以下のように検討する。以下の例では、選択したクラウドサービスの整理したサービス仕様や、ＳＬＡの前提を図表３、４とする。

・業務Ａ

サービス切替時間は、１０分以上を許容するので、５分程度の、ネットワークや、ＶＭの再起動時間は許容できることになるので、切替時間対策は「なし」となる。
業務継続の要求度は、クラウドサービスの障害時停止を許容するので、「シングルＡＺ」となる。

稼働率は、９５％が要求であるが、達成できなかった場合について、利用するクラウドサービス事業者のサービスクレジットを許容できることを利用者に確認することによって、「９５％　サービスクレジット許容」となる。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

・業務Ｂ

サービス切替時間は、１０分未満であるので、５分程度の、ネットワークや、ＶＭの再起動時間でのシステム停止とならないように、切替時間対策は「あり」となる。

業務継続の要求度は、単一障害時は業務停止を許容しないので、マルチＡＺまたはマルチクラウドを選択する。稼働率は、９９．９％が要求であるが、達成できなかった場合について、利用するクラウドサービス事業者のサービスクレジットを許容できることを利用者に確認することによって、「９９．９％　サービスクレジット許容」となる。

サービスクレジット容認であると、マルチＡＺを選択することが可能であるので、業務継続の要求度および稼働率の要求の両方を満足するシステム構成として、マルチＡＺを選択する。

・業務Ｃ

サービス切替時間は、５分未満であるので、５分程度の、ネットワークや、ＶＭの再起動時間でのシステム停止とならないように、切替時間対策は「あり」となる。

業務継続の要求度は、二重障害時でサービス切替時間の範囲内で継続することであるので、マルチＡＺでは要求を満たせないので、マルチクラウドを選択する。

稼働率は、９９．９９％が要求であり、サービスクレジットでは達成できなかった場合を許容できないので、業務継続の要求度および稼働率の要求の両方を満足するシステム構成として、マルチクラウドを選択する。

以上をまとめると下記の表となる。

	利用者要求（指標）			SIer提案例		
対象業務	サービス切替時間	業務継続の要求度	稼働率	切替時間対策	業務継続システム構成	稼働率
業務A	10分以上許容	障害時停止許容する	95%（サービスクレジット許容）	なし	シングルAZ	95%（サービスクレジット許容）
業務B	10分未満	単一障害時は業務停止を許容しない。	99．9%（サービスクレジット許容）	あり	マルチAZ	99．9%（サービスクレジット許容）
業務C	5分未満	二重障害時でサービス切替時間の範囲内で継続する。	99．99%	あり	マルチクラウド	99．99%

図表８　業務範囲毎の可用性の要求の整理例

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

4　可用性確保の運用

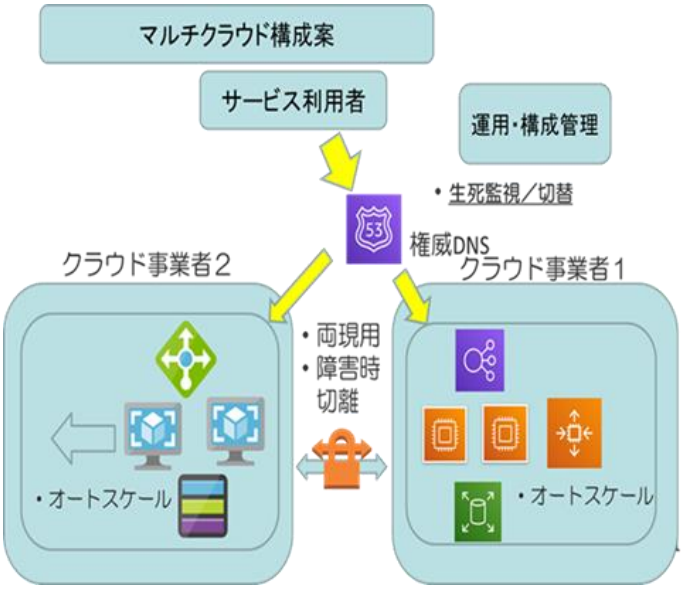
4.1　可用性の要求を保つ運用方法

クラウドサービス上のどのリソースを利用者に割り当てるかは、クラウドサービス事業者が判断するので、利用者が選ぶことはできない。ＳＬＡで提示されている稼働率に調整するため、マイグレーションによって、リソースが移動されることも考えられる。

マルチＡＺまたはマルチクラウドでシステムを構成する場合、可用性を確保するためには、稼働率の要求を保つように、一定の割合で、ＡＺまたは事業者のサービスの利用配分を調整する。

２０１９年８月のＡＷＳのトラブル事例では、一つのＡＺが間欠障害になった場合、複数のＡＺで冗長構成にしていても、クラウドサービス事業者が用意していた機能では障害が発生したＡＺを切り離しすることができず、利用者のシステムが障害になることがあった。ＡＺの可用性が低下した場合に切り離しを行えることが利用者のシステムの可用性確保に重要である。

例として、以下のようなクラウド事業者１、クラウド事業者２のクラウドサービスを利用したマルチクラウドでのシステム構成を考える。



図表９　マルチクラウドでのシステム構成例

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

① ２つのクラウド事業者の IaaS を利用し、同一 OS、ミドルウェア、 アプリケーションのシステムを構築する。
② １つの事業者の DNS サービスを利用してドメイン登録を行い、２つの事業者のサービス上で構築したシステムの IP アドレスを登録。
③ ＤＮＳサービスで、クラウド事業者の二つのサービスに負荷分散する。
④ 業務範囲毎に、ＶＭ、ストレージ、ネットワーク等の生死監視やトラヒック監視、切替時間の分析を行い、目標とする可用性の値との差を日々監視し、サービスの利用配分を調整する。
② 一つのクラウドサービスが障害になった場合は、もう一方に通信を片寄する。

このように運用することにより、どちらかのクラウドサービス事業者の稼働率が、利用者の要求を下回ると、他方のクラウドサービス事業者のサービスを多く利用するように調整できるので、要求した稼働率を確保することができる。

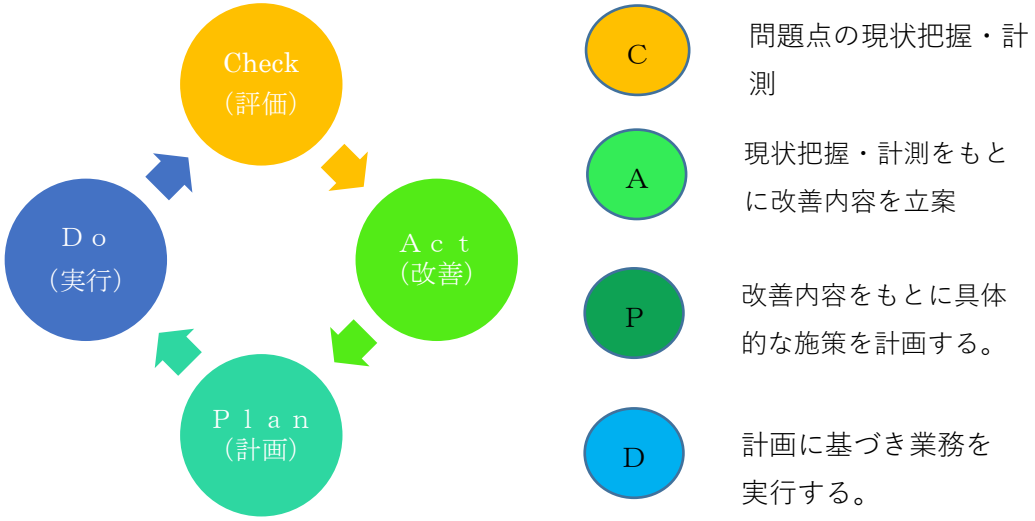
また、どちらかのクラウドサービス事業者が障害となった場合には、他方のクラウドサービス事業者のサービスのみを利用して、業務影響を少なくできる。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

4.2 可用性監視の運用方法（ＣＡＰＤｏ）

4.1 項の方法を継続することによって可用性の要求を保つためには、可用性を監視し、値のレビューを行い、対策を実施し、結果の監視を行うサイクルを継続することになる。この一連のサイクルの方法として、まず監視から始める、ＣＡＰＤｏの考え方を適用する。

ＣＡＰＤｏは PDCA の順番を変えて「C（=Check)」を最初にもってきた改善サイクル手法である。具体的な運用方法を付録―１０に示す。



図表１０　ＣＡＰＤｏの考え方

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

フェーズ	実施概要	実施詳細
Ｃｈｅｃｋ	目標とする可用性の値との差を日々監視する	ＶＭ、ストレージ、ネットワーク等のＭＴＢＦ、性能情報の収集と分析のツールを用いて、目標とする可用性の値との差を日々監視する。
Ａｃｔ	目標とする可用性の値との差のレビューを行う。	月次で、目標とする可用性の値との差のレビューを行い、傾向を確認する。目標とする可用性と実際の値が上回っている場合はよいが、差が少なくなる傾向が見えてきた場合は、クラウドプロバイダーに契約に基づきレビューを申し入れる。
Ｐｌａｎ	可用性を維持する対策を立案する。	目標とする可用性以下になる傾向が見えてきた場合は、ＡＺやクラウドサービスの利用割合の変更を計画する。
Ｄｏ	対策を実施する	計画を実行し、可用性が目標以下になることを予防する。 マルチＡＺまたはマルチクラウドでシステムを構成している場合、障害発生時は、正常なＡＺまたはクラウドサービスのみ利用するように利用割合の調整を行い、業務影響を最小限にする。

図表１１　ＣＡＰＤｏの考え方を活用した運用方法

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

5　ガイドラインの評価

以下の二つの観点でガイドラインの評価を行う。

① 障害事例や、障害シナリオに対して、有効な提案ができること

② 具体的な業種を挙げて、有効な提案ができること

5.1　障害事例や、障害シナリオに対する評価

可用性確保が不足するポイントとして、以下の４つを評価する。

①　クラウドサービス仕様の確認不足

第二章で論じたように、クラウドサービスが障害とは定義しない、短い時間でのＶＭ切替や、ネットワークの通信断への対策の不足が洗い出せるようになっているかを評価する。

２章３項で示した、クラウドサービス利用者がサービス仕様を具体的に認識していなかったことによるシステム障害では、クラウドサービスのＶＭやネットワークの切替時間に対する考慮ができていなかった。サービス切替時間の指標を使うことによって、利用者の業務システムのサービス切替時間の許容時間を設定することによって、対策が必要かどうか確認できるので、障害発生を防ぐことが出来る。

③ 稼働率に対する認識違い

オンプレミスのシステムでの稼働率と違い、クラウドサービスでは、稼働率に対して計算する範囲等の前提条件が存在する。クラウドサービスを利用した利用者のシステムの稼働率とクラウドサービスの稼働率の違いが洗い出せるようになっているかを評価する。

業務システムの稼働率目標を９９．９５％と設定したので、あるクラウドサービス事業者のＳＬＡを確認して、稼働率９９．９９％のマルチＡＺ構成とした。ところがＡＺの一部障害で、障害のＡＺを利用者のシステムから切り離すことができず、４時間の業務停止が発生した。４時間の停止によって、利用者のシステムは月間稼働率は、９９．４５％となるが、しかしながらＡＺの一部障害のため、クラウドサービスのＳＬＡ違反とはならない。本研究での稼働率の指標を使うことによって、稼働率の計算範囲の定義やサービスクレジットで稼働率目標が達成できるか確認ができ、対策が必要かどうか確認できるので、障害発生を防ぐことが出来る。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

④ クラウドサービス大規模障害時の復旧対策不足

クラウドサービスの障害が大規模に発生した場合は、短い時間でのＶＭ切替や、ネットワークの通信断への対策では対応ができない。可用性の要求に対して、大規模障害時の復旧対策が洗い出せるようになっているかを評価する。

業務システムの稼働率目標を９９．９５％と設定したので、あるクラウドサービス事業者のＳＬＡを確認して、稼働率９９．９９％のマルチＡＺ構成とした。ところがＡＺの一部障害で、クラウドサービスのコンソールへのアクセス障害、ＡＰＩコール異常が発生し、ＶＭの再起動ができなくなり、4 時間の業務停止が発生した。クラウドサービス事業者としては、一つのＡＺ障害ではあるが、利用者からするとサービス制御が不能になった状態は、二重障害と同等である。業務継続の指標を使うことによって、ＡＺが二重障害の場合でもサービス切替時間以内に復旧することを確認し、対策が必要かどうか確認できるので、障害発生を防ぐことが出来る。

⑤ ＤＤｏＳ攻撃への対策

自らのシステム以外のＤＤｏＳ攻撃の場合にも、クラウドサービスを利用している場合は、リソースの影響が発生する。可用性の要求に対して、他システムのＤＤｏＳ攻撃時の対策が洗い出せるようになっているかを評価する。

他の利用者のシステムへのＤＤｏＳ攻撃があっても、自らのシステムの可用性を確保したい場合には、業務継続の指標によって二重障害の場合でもサービス切替時間以内に復旧すると設定することによって、マルチクラウドを選択することができ障害発生を防ぐことが出来る。

以上の考察を図表１２にまとめる。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

項番	可用性確保不足のポイント	障害のシナリオ 例	該当指標（メトリクス）		
			切替時間	稼働率	業務継続
1	クラウドサービス仕様の確認	事業者の物理ハード障害により、利用者のVMの切り替えが発生。3分後にVMの再起動完了したが、該当VMで稼働していた業務システムが停止。	○切替時間への要求明確化		
2	稼働率の計算範囲に対する認識 （稼働率は利用者インスタンスではなくリージョン全体での値）	稼働率目標を99．95%と設定し、マルチAZ構成をとっていた（99．99%の稼働率とSLAに記載）が、AZの一部障害で4時間の業務停止が発生。		○ 稼働率の範囲の明確化	
3	クラウドサービス大規模障害時の復旧対策不足	VMが停止し、再起動を行うおうとしたが、コンソールへのアクセス障害、APIコール異常が発生。VM再起動できず。			○サービス制御不能時対策
4	DDoS攻撃への対策	他の利用者へのDDoS攻撃の影響で、自社のシステムがスローダウンの影響を受けた。			○サービス全体影響時対策

図表１２　ガイドラインの評価

４つの障害シナリオに対して、３つの指標のいずれかが該当し、利用者の可用性への要求への対策をガイドラインによって洗い出すことができるので有効性を評価できた。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

5.2　業種事例での評価

5.2.1　電子商取引システム

電子商取引システムに対して、可用性の要求指標（メトリクス）を設定し、有効な提案例が検討できるかを評価する。

電子商取引システムは、社会的には代替できるサービスがあるため、「非機能要求グレード」では社会的影響が限定されるシステムに分類されている。しかしながら、非機能要求グレード」の標準で設定されるサービス切替時間６０分は、ビジネス損失が大きい。このため、クラウドサービス仕様では障害とされない５分未満も対処する設定とする。

以上の検討から、利用者要求（指標）とそれに対応した、ガイドラインから導かれる提案例は以下のようになる。

	利用者要求（指標）			SIer提案例		
対象業務	サービス切替時間	業務継続の要求度	稼働率	切替時間対策	業務継続システム構成	稼働率
電子商取引	*60分未満* ⇓ 5分未満	二重障害時でもサービス切替時間の範囲内で継続する。	99．99%	セッション保持対策	マルチクラウド	99．99%

図表１３　電子商取引システムの可用性要求の具体化と提案例

２章で示した、２０１９年８月のＡＷＳ障害では、以下の電子商取引関連のシステムが停止し、午後１時ごろから午後４時ごろまで、約３時間ビジネスができなくなった。

	企業名	サービス
1	チケットスター	チケット販売サイト「楽天チケット」
2	東急ハンズ	ECサイト
3	ピクスタ	画像販売サイト「PIXTA」
4	フィスコ仮想通貨取引所	仮想通貨交換所「Zaif」
5	ユニクロ	UNIQLOオンラインサイト
6	楽天	フリーマーケットアプリ「ラクマ」
7	PayPay	スマホ決済サービス「PayPay」

図表１４　２０１９年８月のＡＷＳ障害で影響を受けた電子商取引関連システム

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

複数のＡＺで冗長化したアプリケーションの一部で障害が起こっていたり、負荷分散サービス（ＡＬＢ）がエラーの返信を多発したり、ＡＷＳ内部のネットワーク通信が加速度的に増加してネットワークリソースを逼迫させ、ＡＷＳのマネジメントコンソールへのアクセス障害やＡＰＩコール異常が発生した。[6]

クラウドサービスの二重障害が発生した場合に備え、本ガイドラインの考え方を使って、マルチクラウドを選択（サービスクレジット許容なら、マルチＡＺを選択）することによって、利用者のシステムへの影響を小さくできる。

5.2.2　自治体システム

自治体システムに対して、可用性の要求指標（メトリクス）を設定し、有効な提案が検討できるかをみていく。

利用者の可用性要求（指標）は、「電子自治体の取組みを加速するための 10 の指針」フォローアップ検討会報告書[7]にて、非機能要件に関して、「地方公共団体の情報システム調達仕様書における非機能要件の標準化に関する調査研究」[8]を活用するとされている。

この中で、「非機能要求グレード」を参照して社会的影響が限定されるシステム（可用性２）と社会的影響が殆ど無いシステム（可用性１）の二つに分類されている。

利用者の可用性要求（指標）とそれに対応した、ガイドラインから導かれる提案例は以下のようになる。

	利用者要求（指標）			SIer提案例		
対象業務	サービス切替時間	業務継続の要求度	稼働率	切替時間対策	業務継続システム構成	稼働率
（可用性2）住民情報、福祉、税、学校教育、他	60分未満	二重障害時でもサービス切替時間の範囲内で継続する。	99．99%	セッション保持対策	マルチクラウド（サービスクレジット許容ならマルチAZ）	99．99%
（可用性1）内部情報、統計	24時間未満	単一障害は業務停止を許容せず	99%	対策不要	マルチAZ	99%

図表１５　自治体システムの可用性要求の具体化と提案例

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

２０１９年１２月には、日本電子計算のＩａａＳ（Jip-Base）において、自治体システムに障害が発生した。利用者業務への影響が出たシステムでは、二重障害の対策がデータセンター内に閉じており、障害時に代替策が取れず復旧が長期化した。（データ消失も一部あり）

単一障害点をデータセンター単位とする、本ガイドラインの考え方によって対策すれば、マルチクラウドを選択（サービスクレジット許容なら、マルチＡＺを選択）することによって利用者のシステムへの影響を小さくできる。

5.3　評価のまとめ

障害事例や、障害シナリオに対して、３つの指標のいずれかを活用し、利用者の可用性への要求への対策を網羅的に洗い出すことができることを示した。また、業種の事例として、電子商取引システム、自治体システムを挙げて、利用者の可用性の要求を指標で表し、システム構成を提案し、過去の発生した障害への対策に有効であることを示すことができた。

以上のことから、ガイドラインの有効性を示すことができた。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

6　まとめ

クラウドサービス利用でのシステム障害は、利用者が可用性の要求を三つの指標で具体化し、ＳＩｅｒがそれに応じたシステム構成の実現案を提案し、両者でリスクを共有することにより防ぐことができる。

本ガイドラインが活用されることによって、クラウドサービス利用者とＳＩｅｒの可用性確保の共通認識に役立ち、システムの安定稼働に貢献できると幸いである。

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

引用文献

[1] 共通フレーム 2013　～経営者、業務部門とともに取組む「使える」システムの実現～ IPA,2013 年 3 月
[2] 高回復力システム基盤導入ガイド　IPA,2018 年 4 月
[3] 動かないコンピュータ NIKKEI COMPUTER 2019.12.26
[4] 日本におけるクラウド IaaS のマジック・クアドラント Published 20 August 2019 ｶﾞｰﾄﾅｰ https://www.gartner.com/technology/media-products/reprints/google/1-OEUH29V-JPN.html
[5] 非機能要求グレード２０１８　利用ガイド　IPA,2018 4 月
[6] 万が一の障害にも耐えられるようにするためのＡＷＳ利用ガイド　2019.9 サーバーワークス
[7]「電子自治体の取組みを加速するための 10 の指針」フォローアップ検討会報告書 平成 27 年 3 月 26 日　総務省 自治行政局 地域情報政策室
[8]「地方公共団体の情報システム調達仕様書における非機能要件の標準化に関する調査研究」平成 26 年 3 月（財）地方自治情報センター

参考資料

[9] 総務省,令和元年版情報通信白書
[10] 動かないコンピュータ NIKKEI COMPUTER 2019.9.5
[11] NETSCOUT, NETSCOUT's 14th Annual Worldwide Infrastructure Security Report 2019
[12] ユーザのための要件定義ガイド　第２版　ＩＰＡ
[13] NIST, cloud computing FORUM & WORKSHOP " Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)
[14] 経産省,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（２０１３年度版）
[15] JIS Q 27017:2016 セキュリティ技術－JISQ27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範
[16] 総務省,経産省,　クラウドサービスの安全性評価に関する検討会　中間とりまとめ 2019.7
[17] JIS Q 20000-1:2013 サービスマネジメント－第 1 部：サービスマネジメントシステム要求事項
[18] JIS Q 27001:2014 セキュリティ技術－情報セキュリティマネジメントシステム要求事項
[19] 黒川信弘他,情報セキュリティの可用性に関する考察（システム監査　Nov.2013）

© Yoshifumi Itou 2020　mgs194702ATiisec.ac.jp

[20] Mohammad Shahrad, David Wentzlaff, Availability Knob: Flexible User-Defined Availability in the Cloud SoCC '16 Proceedings of the Seventh ACM Symposium on Cloud Computing Pages 42-56

[21] 総務省,経産省, クラウドサービスの安全性評価に関する検討会 とりまとめ案 2019.12

[22] Merve Unuvar, Selecting Optimum Cloud Availability Zones by Learning User Satisfaction Levels IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 8, NO. 2, MARCH/APRIL 2015

[23] ISO/IEC 19086-2:2018(E) Cloud computing — Service levelagreement (SLA) framework — Part 2:Metric model

[24]「クラウドサービスの安全性評価に関する検討会 とりまとめ（案)」に対する意見公募の結果について 御意見に対する考え方
https://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000197497

© Yoshifumi Itou 2020 mgs194702ATiisec.ac.jp