特定課題研究報告書・発表会

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

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についての考察
―ＩａａＳに関して―

２０２０年2月２２日

学籍番号　５５９４７０２
後藤研　博士前期課程　1年

伊藤　吉史

本特定課題研究の成果

3つの指標の活用により、クラウドサービス利用での
可用性確保ができることを示した

サービス切替時間

稼働率

業務継続の要求度

3つの指標を盛り込んだ可用性確保するためのガイドラインの作成

本ガイドラインが、クラウドサービス利用者とSIerの可用性確保
の認識あわせに役立ち、
利用者システムの安定稼働に寄与することを評価した

可用性確保不足に対する課題認識

クラウドサービスの利用拡大に伴い、システム障害の原因をクラウドサービスの障害が原因と報告・報道されることが多くなってきた。

2019年には、AWSの障害や日本電子計算（自治体向け）IaaSの障害等が発生。社会システムに大きな影響。

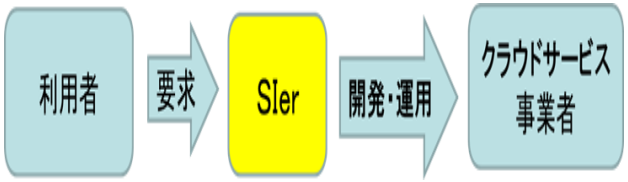
一方、クラウドサービスはサービスの性質上、設備の増強、システム構成変更によるサービスの障害は避けられない。

利用者のクラウドサービスへの認識不足、可用性への対策不足がシステム障害の一因と課題認識。

可用性確保不足に対する課題認識

課題の背景には、対策の拠り所になる、利用者視点での規格、ガイドラインの不足があると考えた

■ また、日本のクラウドサービスの利用は、ＳＩｅｒが事業者との間に入ることが特徴。(*1)



■ 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。

目指すこと

クラウドサービス利用者とSIerが具体的に可用性確保できるガイドラインを作成する

可用性の目標設定、対策検討、運用

(*1)ガートナーレポート：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

参考）「情報セキュリティ 10 大脅威 2020」

ＩＰＡより、2019 年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案をランキングが発表された。（2020 年 1 月 29 日）

６位　予期せぬ IT 基盤の障害に伴う業務停止

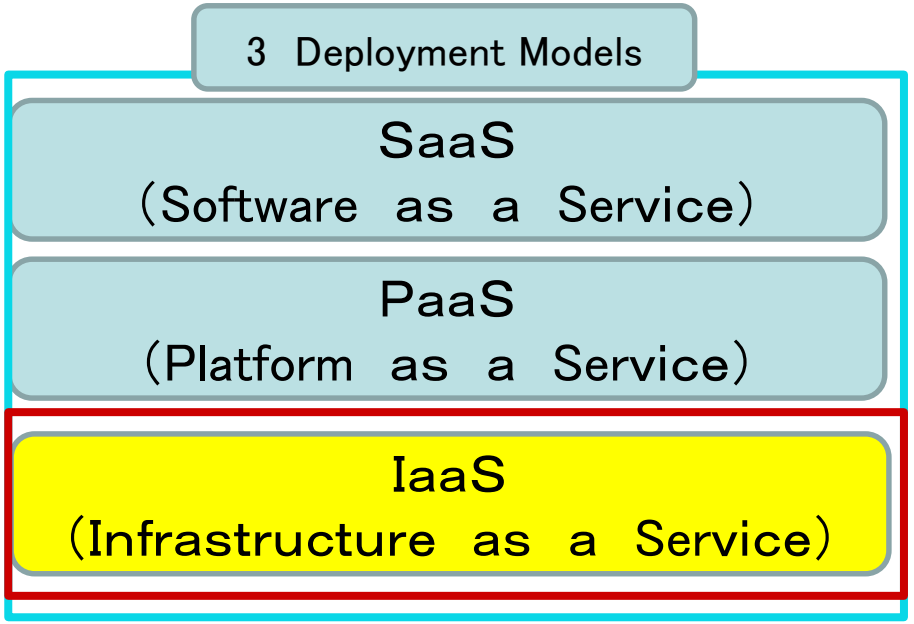
■「情報セキュリティ 10 大脅威 2020」　　NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
NEW	スマホ決済の不正利用	1 位	標的型攻撃による機密情報の窃取	1 位
2 位	フィッシングによる個人情報の詐取	2 位	内部不正による情報漏えい	5 位
1 位	クレジットカード情報の不正利用	3 位	ビジネスメール詐欺による金銭被害	2 位
7 位	インターネットバンキングの不正利用	4 位	サプライチェーンの弱点を悪用した攻撃	4 位
4 位	メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	5 位	ランサムウェアによる被害	3 位
3 位	不正アプリによるスマートフォン利用者への被害	6 位	予期せぬ IT 基盤の障害に伴う業務停止	16 位
5 位	ネット上の誹謗・中傷・デマ	7 位	不注意による情報漏えい（規則は遵守）	10 位

課題認識　～スコープ定義～

■ 研究対象

- クラウドサービスの内、ＩａａＳの利用を対象とする。
- 情報セキュリティのＣＩＡ（Ｃ：機密性、I:完全性）の内、Ａ：可用性を対象。



NIST cloud computing FORUM & WORKSHOP
“Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)“ の定義より筆者作成

■ 研究対象外

- ＩａａＳから上位のサービスである、ＰａａＳ、ＳａａＳ、他、ＤａａＳ、ＭａａＳ等は対象としない。
- サービス個別の要素が多く、他のサービスとの複数利用等の選択が難しく、可用性対策の一般解が導きにくい。

報告の内容

新たなガイドラインの必要性
なぜ、新たにガイドラインが必要か

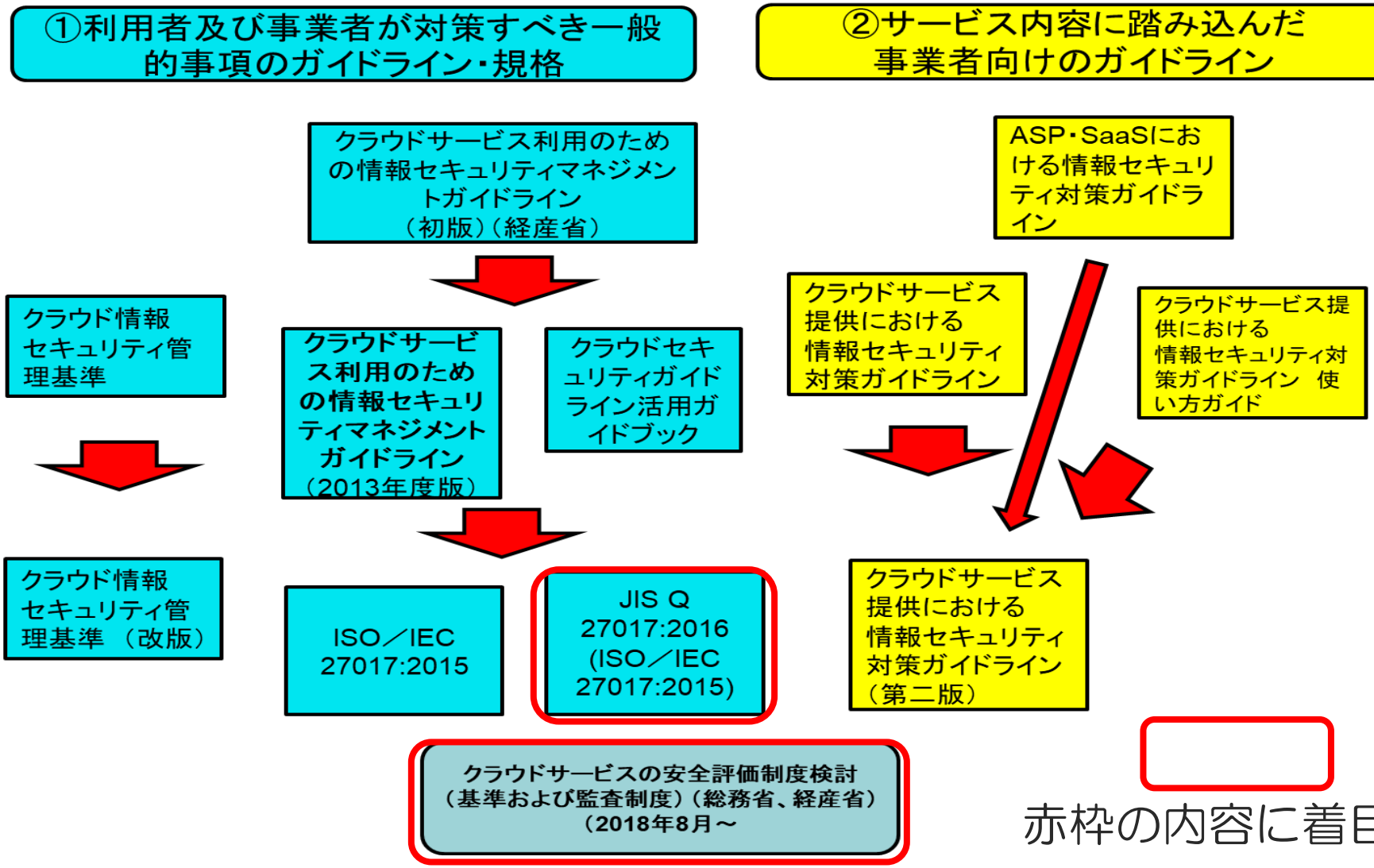
3つの指標で可用性を確保
どのような３つの指標なのか

ガイドラインの内容

ガイドラインの評価

新たなガイドラインの必要性

クラウドサービスに関するセキュリティガイドライン・規格の関連



新たなガイドラインの必要性

クラウドサービス利用の規格での定義・管理策

- JIS Q 27017 の可用性の定義、管理策を調査
- **定義**　可用性 (availability) ： 許可されたエンティティが要求したときに、アクセス及び使用が可能である特性
- **定義の抽象度が高い、**
  （可用性とは、情報を必要な人が必要な時に使える状態であること）
- 管理策について
  - 17.2.1 情報処理施設の可用性　（JIS Q 27002を適用）
  - 情報処理施設は，可用性の要求事項を満たすのに十分な冗長性をもって，導入することが望ましい。

可用性の要求事項を構成する指標に言及がなく、かつ十分な冗長性とあり具体的な方法に踏み込めていない。

参考）品質の規格（JIS Q 25010)では、可用性は，システム，製品又は構成要素が作動状態でいる間の合計時間の割合。 指標があり具体的

新たなガイドラインの必要性

クラウドサービスの安全性評価に関する検討会（総務省、経済産業省）
中間とりまとめ（2019年7月）では、

■ 可用性の要件として何を求め、そのエビデンスをどのように考えるかを含めて十分検討を行うべきである。

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年12月）に対して、可用性の要件に関して、管理策として追加してはどうかとパブリックコメントを行ったが、

■ クラウド事業者と調達者／利用者の合意で取り決めることが適当とされ、「可用性や復旧についての要件を設定することを要件とする予定」、の回答にとどまっている。

新たなガイドラインの必要性

■ （先行研究）情報セキュリティの可用性に関する考察

- 黒川　信弘他　システム監査　Ｎｏｖ．２０１３

■ 東日本大震災における事業継続管理を課題認識し、情報セキュリティの可用性と事業継続管理が重視されない理由、ＩＳＭＳ取り組みの問題点と方策を考察。

■ 理由

- 日本の安全神話文化
- 高信頼システム利用による安心感の蔓延
- サプライチェーン高度化の落とし穴に対する認識不足

■ 可用性実現のための方策

- 経営・管理層のキーマンが可用性の現場の個々の要素の専門家をコントロール
- 事業継続管理に「情報資産そのもの可用性」「利用するための環境の可用性」を取り込む
- 他の枠組みの利用

情報セキュリティの規格、ガイドラインでは限界と指摘

結論

可用性の要件への具体的な対策は、利用者にゆだねられている。
具体的な管理策を提示する、利用者視点の規格やガイドラインはない。

３つの指標で可用性を確保

非機能要求グレードのメトリクス（指標）活用

「非機能要求グレード」は、「非機能要求」についてのユーザとベンダとの認識の行き違いや、互いの意図とは異なる理解を防止することを目的に

「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年公開。現在は、ＩＰＡにて維持、公開。

引用先：「非機能要求グレード」実践セミナー
～システム基盤の非機能要件定義を講義と演習で身につける～2017年11月21日　より筆者作成

機能要求

- ビジネスに直結
- イメージしやすい
- 利用者が自らの言葉で語れる

営業情報をクラウドで共有したい

非機能要求

- ビジネスに直結しない
- イメージしにくい
- 具体化が進まないと利用者が語りにくい

システムが使えない時間は極力少なくしてほしい

システム基盤に関する非機能要求を６項目に分類

大項目	要求例	確認結果に基づき、実施する対策例
可用性	・運用スケジュール（稼働時間・停止予定など） ・障害、災害時における稼働目標	・機器の冗長化やバックアップセンターの設置 ・復旧・回復方法及び体制の確立
性能・拡張性	・業務量および今後の増加見 もり ・システム化対象業務の （ピーク時、	性能目標値を意識したサイジング 来へ向けた機器・ネットワークなどのサイズ
運用・保守性	・運用中に求 働レベル ・問題発生時	
移行性	・新システム び移行方法 ・移行対象資産の種類および移行量	・移行体制の確立、移行リハーサルの実施
セキュリティ	・利用制限 ・不正アクセスの防止	・アクセス制限、データの秘匿 ・不正の追跡、監視、検知
システム環境エコロジー	・耐震/免振,重量/空間,温度/湿度,騒音など、システム環境に関する事項 ・CO2排出量や消費エネルギーなど、エコロジーに関する事項	・規格や電気設備に合った機器の選別 ・環境負荷を低減させる構成

可用性の目標をメトリクス（指標）で定義

対象業務範囲毎に、可用性の指標（メトリクス）である、サービス切替時間、稼働率、業務継続の要求度、の活用を考察する

３つの指標で可用性確保

可用性を確保するための指標の考察

サービス切替時間

稼働率

業務継続の要求度

サービス切替時間に関する指標

クラウドサービスは、ネットワークの短時間の通信断、VMの再起動、物理サーバーの障害様々発生するが、サービスの「障害」とは定義されておらず、利用者が対策すべきものとされている。

サービス切替時間の関連事項に着目することができる。
SIerは、利用者が許容できるサービス切替時間を確認し、
下記の条件で満足できるか確認することができる。

	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

主なクラウドサービス事業者のＩａａＳ切替時間

稼働率に関する指標

クラウドサービス事業者は、「稼働率」をＳＬＡで、設定している。
合意したサービス範囲の稼働率であって、利用者が割り当てられているインスタンスの稼働率ではない。

稼働率の関連事項に着目することができる。
利用者の要求を満足できるように、SIerは、稼働率および、対象範囲やサービスクレジットでの補償等の考慮ができる。

	A社	B社	C社
対象リソース	コンピューティング	コンピューティング	コンピューティング
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%未満 99．0%以上 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%サービスの将来の支払いに適用	10%サービス料金返金

業務継続の要求度に関する指標

可用性を確保するためにはシステムを構成する要素の冗長化を行うが、単一障害点（ＳＰＯＦ）をなくす考え方がある。

一つのＡＺを単一障害点ととらえると「非機能要求グレード」で示されている利用者の要求は、下記の表のように整理できる。

SIerは、利用者がどの範囲のシステム障害を許容できるのか確認し、システム構成を設計することができる。

レベル	利用者要求	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）

ガイドラインの内容

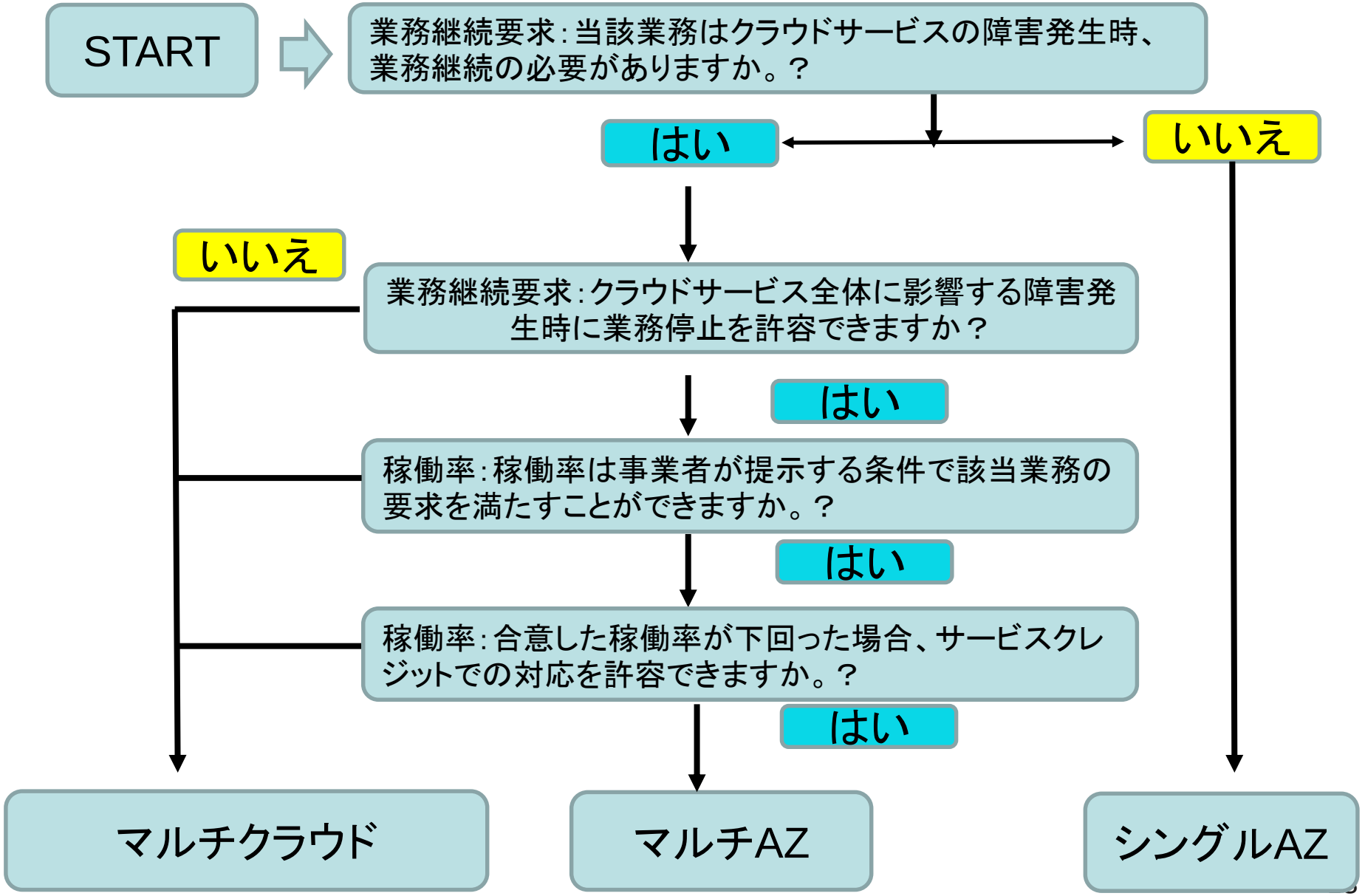
ガイドラインの構成は以下のとおり
内容の一部を説明する

利用者の要求に対応した可用性確保の提示方法

SIerは、利用者要求を業務システム毎に確認・整理
→効率的にクラウドサービスを利用

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%
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%
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%

システム構成　検討フロー



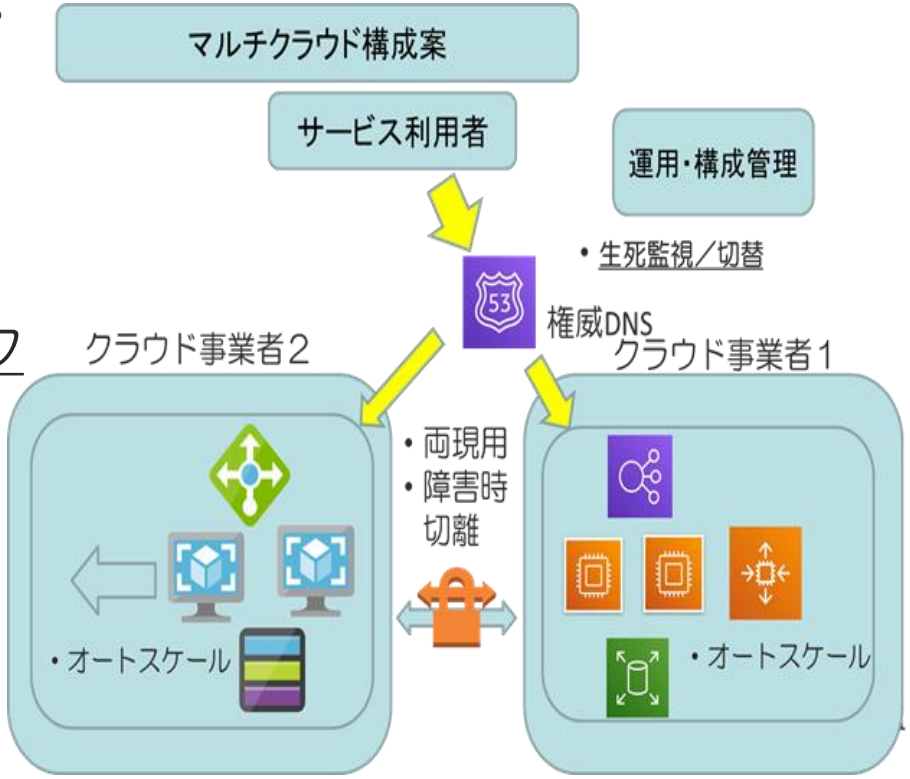
ＳＩｅｒ提案例

	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%以下（サービスクレジット容認）	なし	シングルAZ	95%以下（サービスクレジット容認）
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容認）	あり	マルチAZ	99．9%（サービスクレジット容認）
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%

可用性を確保する運用実施例

マルチクラウドでシステムを構成し、可用性を確保する場合。

- 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。
- 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つの事業者の構築したシステムのIPアドレスを登録。
- 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。
- 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。
- 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



ガイドラインの評価　業種を対象にした評価

自治体システム

可用性要求の指標を参照して設定する。

「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」地方公共団体情報システム機構
平成26年3月

	利用者要求（指標）		
対象業務	**サービス切替時間**	**業務継続の要求度**	**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%
（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%**

ガイドラインの評価　自治体システムへの適用

	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					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 満	業務停止を許容せず			マルチAZ	99%

現状、自治体のシステムは単一のAZ(データセンター)でクラウドサービス利用されているものが多い。

２０１９年１２月　日本電子計算のＩａａＳ（単一AZ）で47自治体などのシステムが停止。復旧長期化。

本ガイドラインを用いることにより、単一障害点をAZ単位とする対策が可能となり、利用者システムへの影響を小さくできる。

ガイドラインの評価　　障害シナリオ

クラウドサービス仕様の確認不足

物理ハード障害で、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。

サービス仕様には記載あり

ガイドラインを使って

サービス切替時間の指標
・サービス切替時間の明確化
・切替時間要求の明確化
・VM切替対策の検討

稼働率に対する認識違い

稼働率を99．95%と設定し、マルチAZ構成をとっていたが、AZの一部障害で4時間の業務停止が発生

稼働率はサービス全体での定義

ガイドラインを使って

稼働率の指標
・稼働率定義範囲の明確化
・サービスの限界を確認
・マルチクラウドを選択肢

本ガイドラインを用いることにより、サービス仕様との認識相違が明らかになる。障害対策実施により、利用者システムへの影響を小さくできる。

まとめ

本特定課題研究の成果

3つの指標の活用により、クラウドサービス利用での
可用性確保ができることを示した

- サービス切替時間
- 稼働率
- 業務継続の要求度

3つの指標を盛り込んだ可用性確保するためのガイドラインを作成

本ガイドラインが、クラウドサービス利用者とSIerの可用性確保
の認識あわせに役立ち、
利用者システムの安定稼働に寄与することを評価した

今後の課題

クラウドサービス利用での可用性の確保は、一方でデータを複数
のリソース（AZ、複数事業者）に分散することにつながる。
機密性との関係について考えていきたい。

ご清聴ありがとうございました


情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY