2023年 5月 18日

# CSA Japan Summit 2023

## 問題提起プレゼンテーション：
## **経済安全保障とメガクラウドの進化**
## ～ 日本のクラウドのあり方を問う ～

日本クラウドセキュリティアライアンス 監事 高橋郁夫 副会長 渥美俊英
コンサルタント 結城則尚

# 問題提起プレゼンテーション
# 経済安全保障とメガクラウドの進化

1 経過と問題提起
　　渥美俊英　CSAJ 副会長
2 (続) 新しい経済安全保障とクラウド
　　高橋郁夫　CSAJ 監事, 弁護士
3 テーマコメント
　　結城則尚　コンサルタント
4 ディスカッション
　　渥美、高橋、結城



日本クラウドセキュリティアライアンス
副会長　　渥美俊英
監事 弁護士　高橋郁夫
コンサルタント 結城則尚

# 問題提起　要旨

- 政府クラウドバイデフォルト、**「調達要件」が著しく高度化**
- ISMAP認定**＋200以上のクラウドネイティブ要件,米系4社だけ認定**
- 一方、**経済安全保障**の名の下で国産クラウドへの期待と支援策
- ロシアのウクライナ侵略、戦争技術の変化、国を守るメガクラウド

■ 国産＆プライベートクラウドなら安全なのか？

～ 障害時対応？　開発・運用・セキュリティ・統制自動化？

■ セキュリティクリアランス、ソブリンクラウド

**★ 日本の経済安全保障の動向、クラウドサービスはどうあるべき？**

# 公共クラウドバイデフォルトの「調達要件」が著しく高度化

## デジタル庁におけるガバメントクラウド整備のためのクラウドサービスの提供 -令和4年度募集-

### 公募公告

令和4年9月12日
支出負担行為担当官
デジタル庁会計担当参事官 奥田 直彦
本業務の実施可能な者を以下のとおり公募します。

### 1　公募件名

デジタル庁におけるガバメントクラウド整備のためのクラウドサービスの提供
-令和4年度募集-

- 調達仕様書（PDF／308KB）
- 基本事項(別紙1)（Excel／81.6KB）
- サービス内容(別紙2)（Excel／23.5KB）

### 2　目的等

本公告はクラウドサービスの適正かつ確実な提供を確保するため、公募参加者に対し、その確実なサービスの提供を証明する書類等の提出を求めるものであり、デジタル庁が当該提出された書類等の審査においてクラウドサービスの提供が可能と判断した者すべてと契約の締結を行うものである。

### 3　公募期間

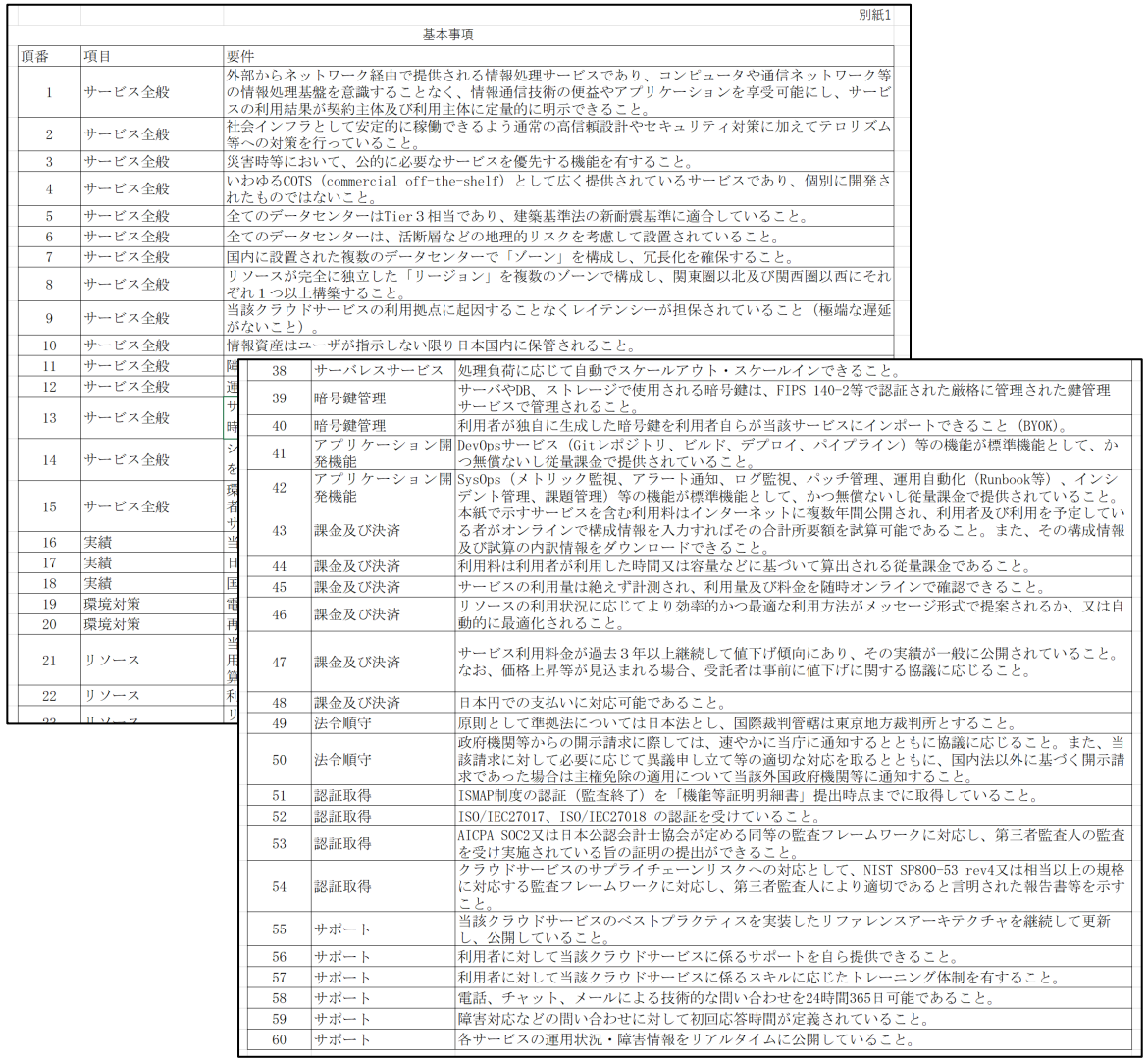
令和4年9月12日（月曜日）から令和4年9月26日（月曜日）17時までに下記提出先必着分に限る。

### 4　業務形態

クラウドサービスの提供

https://www.digital.go.jp/procurement/f7a497a7-1798-4690-abdf-79d3511d1752/

# 昨年9月のガバメントクラウド調達要件、延々200余



別紙1

基本事項

| 項番 | 項目 | 要件 |
|---|---|---|
| 1 | サービス全般 | 外部からネットワーク経由で提供される情報処理サービスであり、コンピュータや通信ネットワーク等の情報処理基盤を意識することなく、情報通信技術の便益やアプリケーションを享受可能にし、サービスの利用結果が契約主体及び利用主体に定量的に明示できること。 |
| 2 | サービス全般 | 社会インフラとして安定的に稼働できるよう通常の高信頼設計やセキュリティ対策に加えてテロリズム等への対策を行っていること。 |
| 3 | サービス全般 | 災害時等において、公的に必要なサービスを優先する機能を有すること。 |
| 4 | サービス全般 | いわゆるCOTS（commercial off-the-shelf）として広く提供されているサービスであり、個別に開発されたものではないこと。 |
| 5 | サービス全般 | 全てのデータセンターはTier３相当であり、建築基準法の新耐震基準に適合していること。 |
| 6 | サービス全般 | 全てのデータセンターは、活断層などの地理的リスクを考慮して設置されていること。 |
| 7 | サービス全般 | 国内に設置された複数のデータセンターで「ゾーン」を構成し、冗長化を確保すること。 |
| 8 | サービス全般 | リソースが完全に独立した「リージョン」を複数のゾーンで構成し、関東圏以北及び関西圏以西にそれぞれ１つ以上構築すること。 |
| 9 | サービス全般 | 当該クラウドサービスの利用拠点に起因することなくレイテンシーが担保されていること（極端な遅延がないこと）。 |
| 10 | サービス全般 | 情報資産はユーザが指示しない限り日本国内に保管されること。 |
| 11 | サービス全般 | 障 |
| 12 | サービス全般 | 連 |
| 13 | サービス全般 | サ 時 |
| 14 | サービス全般 | シ を |
| 15 | サービス全般 | 環 者 サ |
| 16 | 実績 | 当 |
| 17 | 実績 | 日 |
| 18 | 実績 | 国 |
| 19 | 環境対策 | 電 |
| 20 | 環境対策 | 再 |
| 21 | リソース | 当 用 算 |
| 22 | リソース | 利 |
| 23 | リソース | リ |

| | | |
|---|---|---|
| 38 | サーバレスサービス | 処理負荷に応じて自動でスケールアウト・スケールインできること。 |
| 39 | 暗号鍵管理 | サーバやDB、ストレージで使用される暗号鍵は、FIPS 140-2等で認証された厳格に管理された鍵管理サービスで管理されること。 |
| 40 | 暗号鍵管理 | 利用者が独自に生成した暗号鍵を利用者自らが当該サービスにインポートできること（BYOK）。 |
| 41 | アプリケーション開発機能 | DevOpsサービス（Gitレポジトリ、ビルド、デプロイ、パイプライン）等の機能が標準機能として、かつ無償ないし従量課金で提供されていること。 |
| 42 | アプリケーション開発機能 | SysOps（メトリック監視、アラート通知、ログ監視、パッチ管理、運用自動化（Runbook等）、インシデント管理、課題管理）等の機能が標準機能として、かつ無償ないし従量課金で提供されていること。 |
| 43 | 課金及び決済 | 本紙で示すサービスを含む利用料はインターネットに複数年間公開され、利用者及び利用を予定している者がオンラインで構成情報を入力すればその合計所要額を試算可能であること。また、その構成情報及び試算の内訳情報をダウンロードできること。 |
| 44 | 課金及び決済 | 利用料は利用者が利用した時間又は容量などに基づいて算出される従量課金であること。 |
| 45 | 課金及び決済 | サービスの利用量は絶えず計測され、利用量及び料金を随時オンラインで確認できること。 |
| 46 | 課金及び決済 | リソースの利用状況に応じてより効率的かつ最適な利用方法がメッセージ形式で提案されるか、又は自動的に最適化されること。 |
| 47 | 課金及び決済 | サービス利用料金が過去３年以上継続して値下げ傾向にあり、その実績が一般に公開されていること。なお、価格上昇等が見込まれる場合、受託者は事前に値下げに関する協議に応じること。 |
| 48 | 課金及び決済 | 日本円での支払いに対応可能であること。 |
| 49 | 法令順守 | 原則として準拠法については日本法とし、国際裁判管轄は東京地方裁判所とすること。 |
| 50 | 法令順守 | 政府機関等からの開示請求に際しては、速やかに当庁に通知するとともに協議に応じること。また、当該請求に対して必要に応じて異議申し立て等の適切な対応を取るとともに、国内法以外に基づく開示請求であった場合は主権免除の適用について当該外国政府機関等に通知すること。 |
| 51 | 認証取得 | ISMAP制度の認証（監査終了）を「機能等証明明細書」提出時点までに取得していること。 |
| 52 | 認証取得 | ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 |
| 53 | 認証取得 | AICPA SOC2又は日本公認会計士協会が定める同等の監査フレームワークに対応し、第三者監査人の監査を受け実施されている旨の証明の提出ができること。 |
| 54 | 認証取得 | クラウドサービスのサプライチェーンリスクへの対応として、NIST SP800-53 rev4又は相当以上の規格に対応する監査フレームワークに対応し、第三者監査人により適切であると言明された報告書等を示すこと。 |
| 55 | サポート | 当該クラウドサービスのベストプラクティスを実装したリファレンスアーキテクチャを継続して更新し、公開していること。 |
| 56 | サポート | 利用者に対して当該クラウドサービスに係るサポートを自ら提供できること。 |
| 57 | サポート | 利用者に対して当該クラウドサービスに係るスキルに応じたトレーニング体制を有すること。 |
| 58 | サポート | 電話、チャット、メールによる技術的な問い合わせを24時間365日可能であること。 |
| 59 | サポート | 障害対応などの問い合わせに対して初回応答時間が定義されていること。 |
| 60 | サポート | 各サービスの運用状況・障害情報をリアルタイムに公開していること。 |

## おそらく世界で最もクラウドネイティブ

- 個別に開発されたものではないこと
- 情報資産はユーザが指示しない限り**日本国内に保管**
- 国内の利用企業ユーザ数及び**公開事例が100以上**
- **データベースや運用管理**等、オンデマンドで利用
- 全てのマネージドサービスを**数回のクリック**で利用

## テンプレート

- 自動的に**サービス間連携が構成**され、稼働環境を構築できる機能を**無償で利用可能**
- ベストプラクティスに基づくアーキテクチャを実装するテンプレートを**インターネットに無償で公開**

https://www.digital.go.jp/procurement/f7a497a7-1798-4690-abdf-79d3511d1752/

# 今年9月、ガバメントクラウド調達第2ラウンド

## 日本政府の共通クラウド基盤に「Azure」「Oracle Cloud」追加　またも国産サービス入らず

2022年10月03日 11時00分 公開

[ITmedia]

デジタル庁は10月3日、日本政府の共通クラウド基盤「ガバメントクラウド」（政府クラウド）として、米Microsoftの「Microsoft Azure」と米Oracleの「Oracle Cloud Infrastructure」を新たに選定したと発表した。過去に採択した「Amazon Web Services」と「Google Cloud Platform」も引き続き採用する。

| クラウドサービス名 |
| --- |
| Amazon Web Services |
| Google Cloud Platform |
| Microsoft Azure |
| Oracle Cloud Infrastructure |

# メガクラウド(AWS) この2年余り変化


## 急進化しているサービス分野

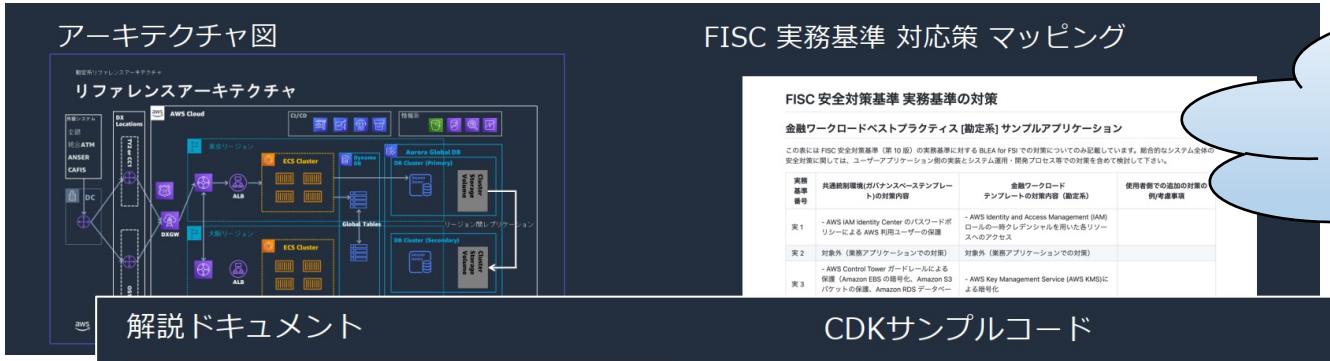
| | | | | | |
|---|---|---|---|---|---|
| コンピューティング | 9(+4) | 機械学習 | 25(+12) | アプリケーション統合 | 8(+2) |
| コンテナ | 4(+1) | 分析 | 14(+4) | カスタマーエンゲージメント | 4 |
| ストレージ | 6(+1) | 移行と転送 | 9(+2) | ビジネスアプリケーション | 8(+5) |
| データベース | 9(+2) | コスト管理 | 4(+1) | メディアサービス | 11(+2) |
| ネットワーキング | 9(+1) | モバイル | 4 | Customer Enablement | 4(+4) |
| 開発者用ツール | 10(+3) | ロボット工学 | 1 | エンドユーザーコンピューティング | 3 |
| セキュリティ | 20(+6) | ブロックチェーン | 1 | ゲーム開発 | 1 |
| 管理とガバナンス | 24(+8) | 量子テクノロジー | 1(+1) | AR/VR | 1 |
| IoT | 13(+3) | 衛星 | 1 | | |

**合計 205サービス (+62　43%増)**

# IaC(Infrastructure as Code)の進化、現実解

**AWS 金融リファレンスアーキテクチャ 無料公開** (2022/10)

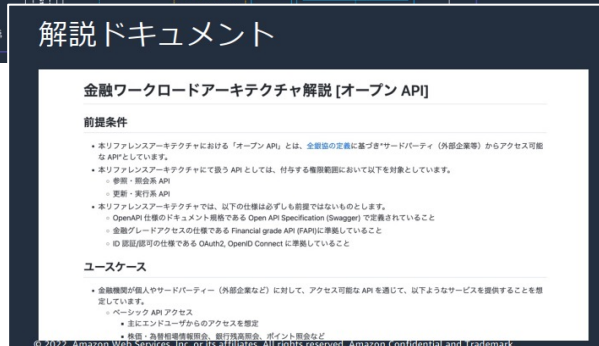
- Open API、勘定系、顧客チャネル(CC)、マーケットデータ配信
- アーキテクチャ図、設計解説書、**自動構築サンプルコード**
- FISC安全対策基準要件との対応策、システム実装とのマッピング



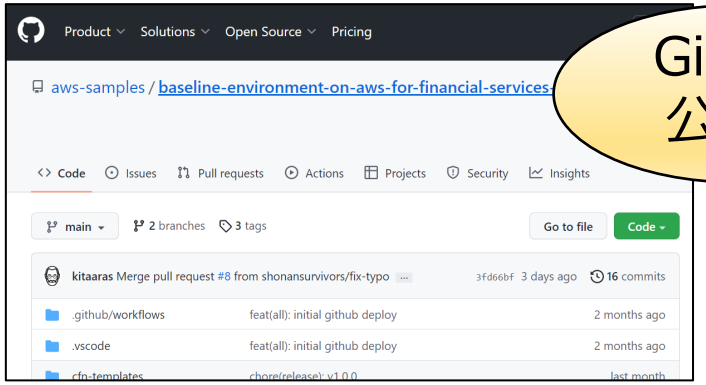




IT民主化、SIerも変化
人ができることは？








Github
公開!!

https://aws.amazon.com/jp/compliance/fintech/

https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute

# メガクラウドへの「反動」

2022年5月7日　日本経済新聞

**クラウド国産化を推進　経済安保で「重要物資」指定、サイバー攻撃に迅速対処**

政府は経済安全保障上、安定供給が必要な「特定重要物資」にクラウドサービスを指定する調整に入った。サイバー攻撃に備えるため半導体や医薬品と同じ扱いにする。トラブルに国内人員が常時対応できることなどを要件に**日本企業「国産クラウド」の競争力強化をめざす**。

**記事に書かれている事：**

- 機微な情報を外資のクラウドサービスで扱うことには漏洩など安保上のリスク
- 日本がサイバー攻撃を受けた際に迅速に対応してもらえない恐れ
- 政府は国内企業によるクラウドサービスの育成が急務と判断
- 経済安保推進法案は重要物資に「プログラムを含む」と明記
- 指定された物資を取り扱う事業者は**政府から財政支援**や金利負担の軽減

**「プライベートクラウド」は日本企業も同等のサービスを提供することが可能**

**IaaS中心のプライベートクラウドにクラウドの真価はあるのか？**

**??!!**

https://www.nikkei.com/article/DGKKZO60560200W2A500C2EA3000/

# 「重要インフラのサイバーセキュリティに係る行動計画」の概要

## 官民連携による重要インフラ防護の推進

- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

NISCによる総合調整

### 重要インフラ所管省庁

- 金融庁
  [金融]
- 総務省
  [情報通信、行政]
- 厚生労働省
  [医療、水道]
- 経済産業省
  [電力、ガス、化学、クレジット、石油]
- 国土交通省
  [航空、空港、鉄道、物流]

### 重要インフラ(全14分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油


### 関係機関等

- サイバーセキュリティ関係省庁
  [総務省、経済産業省等]
- 事案対処省庁
  [警察庁、防衛省等]
- 防災関係府省庁
  [内閣府、各省庁等]
- サイバーセキュリティ関係機関
  [NICT、IPA、JPCERT/CC等]
- サイバー空間関連事業者
  [サプライチェーン等に関わるベンダー等]

## 「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

### 障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

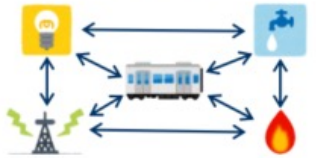
### 安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

### 情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

### リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

### 防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

# セキュリティクリアランス

- 政府や軍隊で指定された機密情報を扱う職員に対して、その人物に信頼性があるかどうかを政府が確認する手続き

- 総務省「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（第3版）」

  クラウドサービス提供事業者は、セキュリティクリアランスを取得した職員のみが、機密情報を取り扱うこと

- 自民党「経済安全保障上の重要政策に関する提言」

・本人同意を前提としたバックグラウンドチェックなど

- 総合政策委員会　主査ヒアリング

・NTTデータ、KDDIから、「不可欠」「実効性のある制度の検討を期待」

# ロシア侵略に見る戦争技術の変化とクラウド

- 2022年2月侵攻当日、AWSはウクライナ政府とクラウド移行開始
- この2週間前に、ウクライナ議会はデータ国内保管のIT法を変更
- ロシアの2/24ミサイル攻撃の前、Microsoftがまずサイバー攻撃を検知
- AWS、Microsoftは、政府、企業のシステムを一気にクラウド移行
- 移行支援(数百億円)は両社共無償　戦争に直面した多大なノウハウを得た
- 厳しい戦禍の下、行政、戸籍、経済、決済、教育はクラウドで維持


**クラウドサービスは、私たちの国の戸籍や経済活動の救世主。**

**クラウドをミサイルで破壊することはできない。**

フェドロフ副首相兼デジタル変革大臣 Twitter

# ソブリンクラウド　～基調講演から

- 基調講演を聞いてクラウド黎明期にシアトルで思ったこと
  - ・米国政府、連邦、州は、メガクラウドで支えられている
  - ・だから、世界中の大企業、金融業や製造業のシステムもクラウドでできる

- ソブリンクラウド
  - ・特定の法域、データ所在、データ主権
  - ・現実的にGlobal Cloudsのマルチクラウドとなる
  - ・難点(Drawbacks)　技術革新とレジリエンスが一部低減
  - ・Aligning Sovereign with Global Clouds　管理分散、一層の自動化
  - ・責任共有モデルの深い理解と実践

# 経済安全保障、論点と国産クラウドへの期待、未来

- 広域障害時に、米系ベンダのサポートは日本ユーザが後回し？
- プライベートクラウドならば国産ベンダーも同等なのか？
- 本来の論点

  技術：　Confidential Computing、耐量子コンピュータ暗号、暗号チップ 他
  方式：　安全で高度な自動化サービスを組合わせる、人ができることに集中
  統制：　データ主権、セキュリティ自動化、セキュリティクリアランス
  　　同盟国のクラウドサービスのセキュリティ、統制レベルのベース
  言葉：　ソブリンクラウド、クオリティクラウド

- 国産クラウドへの期待

  IaaSからの進化、安全で高度なクラウドサービスと運用提供