2024年 5月 22日

CSA Japan Summit 2024

テーマプレゼンテーション：
「クラウドセキュリティ、発見的統制の今」
～ クラウドの進化と活用、その先 ～

日本クラウドセキュリティアライアンス 会長 渥美俊英
デジタル庁 山本教仁様、PwC 保坂あずみ様

「クラウドセキュリティ、発見的統制の今」

1 テーマの趣旨

CSAJ 副会長　渥美俊英

2 デジタル庁ガバメントクラウドにおける予防的統制・発見的統制の考え方

～先進的利用現場から　デジタル庁　Chief Cloud Officer　山本教仁様

3 ISMAPと次世代のクラウドセキュリティ評価

～監査現場から　PwC　リスク・アシュアランス部 マネージャ 保坂あずみ様

4 パネルディスカッション

渥美モデレータ、山本様、保坂様

～ ミニプレゼンを深堀り

～ 意図、苦労、人材、課題など

CSAJ 渥美

デジタル庁 山本様

PwC 保坂様

「クラウドセキュリティ、発見的統制の今」

テーマの背景

- メガクラウドはこの10数年で、著しく規模拡大と機能拡大が進化
- この2-3年で予防的統制から発見的統制のサービスが著しく進化
- 更にベストプラクティスな設計ガイド、IoCテンプレートも無料公開
- この背景には、クラウド最大リスクである設定・設計ミス対策拡充

★本パネルでは、この先進的利活用の状況、
更に次世代の監査のあり方をテーマにします。

「クラウドセキュリティ、発見的統制の今」

問題提起：ミニプレゼンテーション

「クラウド最新動向と先進的活用、課題」

クラウドセキュリティアライアンスジャパン
副会長　渥美俊英

「クラウドセキュリティ、発見的統制の今」
テーマの背景の関心事

- クラウド利活用、日本は先進国で今なお遅れ
- 政府クラウド動向、調達要件高度化、世界初の直接調達、米系認定
- 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
- ウクライナ侵略、戦争IT技術の変化、国家を守るメガクラウド
- クラウドの著しい進化、予防的統制・発見的統制

■ クラウドの進化、適切な活用と組織、テクノロジー、人材育成
■ ISMAPのさらなる進化、次世代監査、クラウドサービスの活用

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/

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/

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

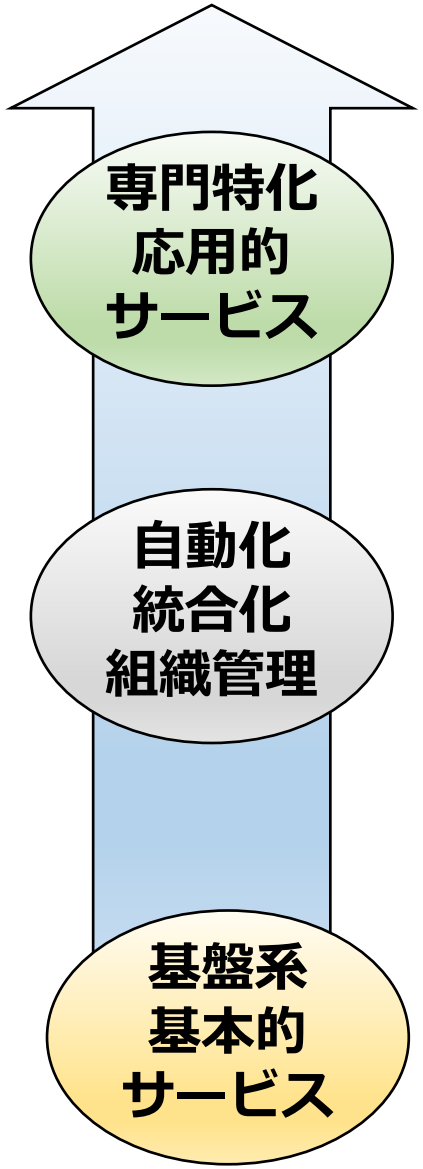
2022年10月03日 11時00分 公開

[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

グローバルクラウドの10年余りの進化と真価



セキュリティ、コンプライアンス特化

GuardDuty（継続的監視分析）
AWS Security Hub（アラート統合管理）
Amazon Detective（潜在イシュー検査）

AWS Inspector（セキュリティ評価）
Trusted Advisor（推奨設定確認）
Amazon Macie（機密データ保護）

AWS Organizations（アカウント管理）
Systems Manager（運用自動化）
Control Tower（設定自動化統制）

AWS KMS（暗号鍵管理）
AWS WAF（WAF）
AWS Shield（DDoS攻撃保護）

IAM（統合権限管理）
AWS CloudTrail（全てのイベントログ）
AWS Config（全ての変更管理）

クラウドならではのセキュリティ

責任共有モデル ～統制・監査にマネージドサービスを駆使

プリヴァト銀行
ウクライナ最大の銀行
270アプリケ、４PBデータ、
3500サーバをクラウド移行

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

「クラウドセキュリティ、発見的統制の今」
ミニプレゼンテーション１ への橋渡し

- ISMAPをテーマにした、過去のCSAJイベント
  ⇒ 登壇者のお立場もあり、、
- とあるメガクラウドご担当者の切実な声
  ⇒ 監査に「紙」の証跡が必須！？
- JASA20周年記念イベントで聞いたこれからの課題
  ⇒ お、これはようやくテーマにできる段階！

「クラウドセキュリティ、発見的統制の今」
ミニプレゼンテーション２ への橋渡し

- 前述のエピソードから　監査人の依然とした作業
  ⇒ 監査業務向けのクラウドサービス！？

- しかし監査人は、開発者利用者とは異なる役割、目線

- これだけ急速に進化するメガクラウドにどう取り組む

クラウドセキュリティ、発見的統制の今
パネルディスカッション　関心事

～ ミニプレゼンを深堀り

～ 意図、苦労、人材、課題など

◆クラウドの進化、適切な活用と組織、テクノロジー、人材育成

◆ ISMAPのさらなる進化、次世代監査、クラウドサービスの活用

◆政府がCSPから直接調達という決定の背景

～予防的統制・発見的統制の最上位を自らコントロール？

◆CSPMの「態勢」（X体制）の現状は

～最後には人が判断、対応、そのための練習

◆IaaS中心の国産CSPへの期待

～個人的には、是非とも頑張ってほしいです

◆ISMAPスキームに関わる監査サイドから

～ガバメントクラウドのIaaS向け管理策を超える考えに驚き

～まずは高度に進化したサービスを知ることから

◆ 次世代監査にクラウドサービスを活用

～クラウド利用者組織内の監査に役立つサービス群

◆ しかし、監査側は、クラウド利用側とは異なる

～仕組みの裏の理解、統制、SOC２のレベル以上？

◆利用者側も監査側も共通の悩み、人材

◆メガクラウドサービス、セキュリティ、統制が分かる人材

～メガクラウド外資によくあるカルチャー、会議、姿勢

◆クラウド最大のリスクは「設定のミス」ではない「設計の在り方」

～「責任共有の利用者側設定」からクラウドならではの仕組み

◆最後にひとこと、ご参加者につたえたいこと

◆私、渥美　クラウドで暮らしやすい豊かな日本の生活、社会

そのために、まだまだクラウドエバンジェリスト役やります