「リスク管理アプローチに基づくSaaSクラウドサービスのセキュリティ評価」

Japan Security Summit 2023

一般社団法人　日本クラウドセキュリティアライアンス

理事　諸角昌宏

CSAリサーチフェロー、 CCSP、CCSK、CCAK

2023年10月

プロフィール

- 一般社団法人日本クラウドセキュリティアライアンス　理事
- **Cloud Security Alliance リサーチフェロー**
- **CSA Authorized Instructor**

- **CCSK,CCSP,CCAK**　～クラウドセキュリティ・ファンのページ～フェースブックグループ
  https://www.facebook.com/groups/264458864908859/

本日のアジェンダ

1. クラウドセキュリティの基本である責任共有モデル
2. クラウドのリスク管理とCSAツール
3. STAR Registryとは？
4. まとめ

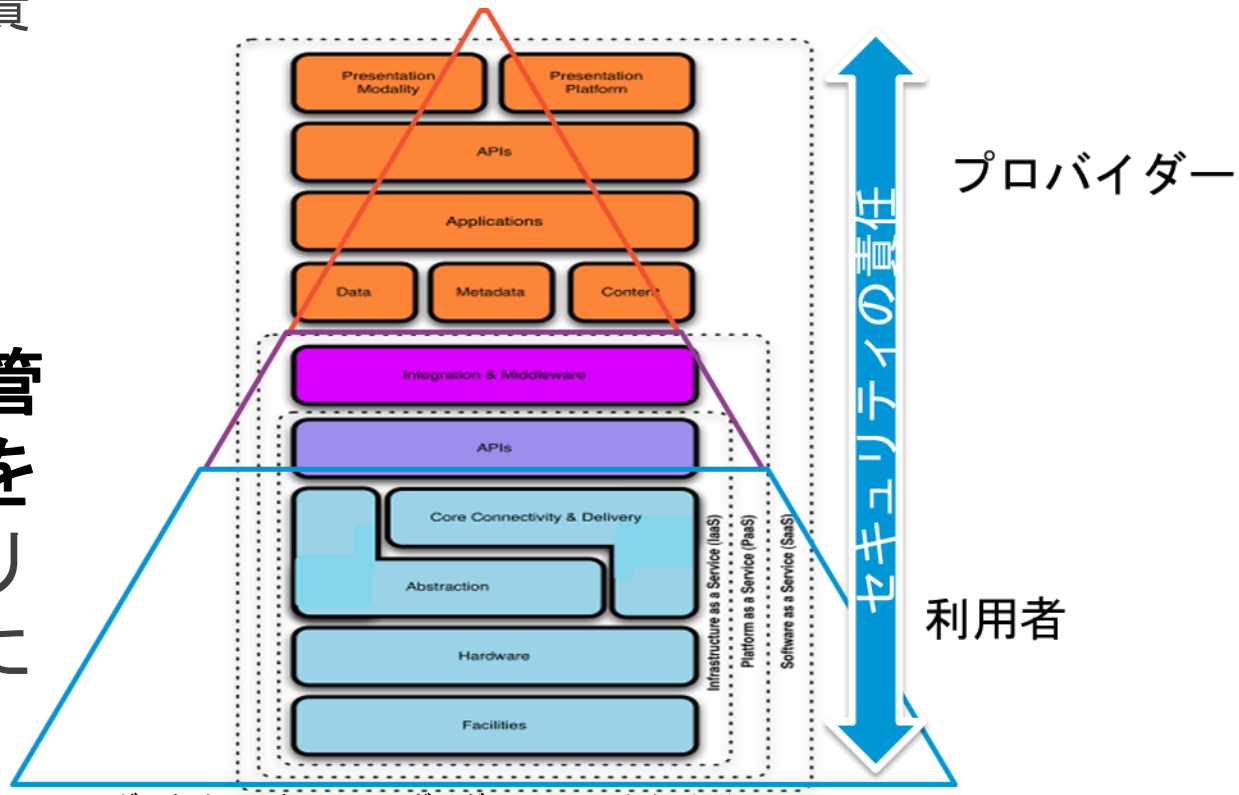
1. クラウドセキュリティの基本である責任共有モデル

クラウドセキュリティの基本

責任共有モデル

- クラウド事業者は、一定のリスクに対する責任を負い、クラウド利用者はその先のすべてに責任を持つ
  - Security In the Cloud
  - Security Of the Cloud

- **クラウド利用者は、リスクを所管する最終的な責任（説明責任）を負っており、**クラウド事業者にリスク管理の一部を転嫁しているに過ぎない。



（クラウドコンピューティングのためのセキュリティガイダンス　V3.0から引用）

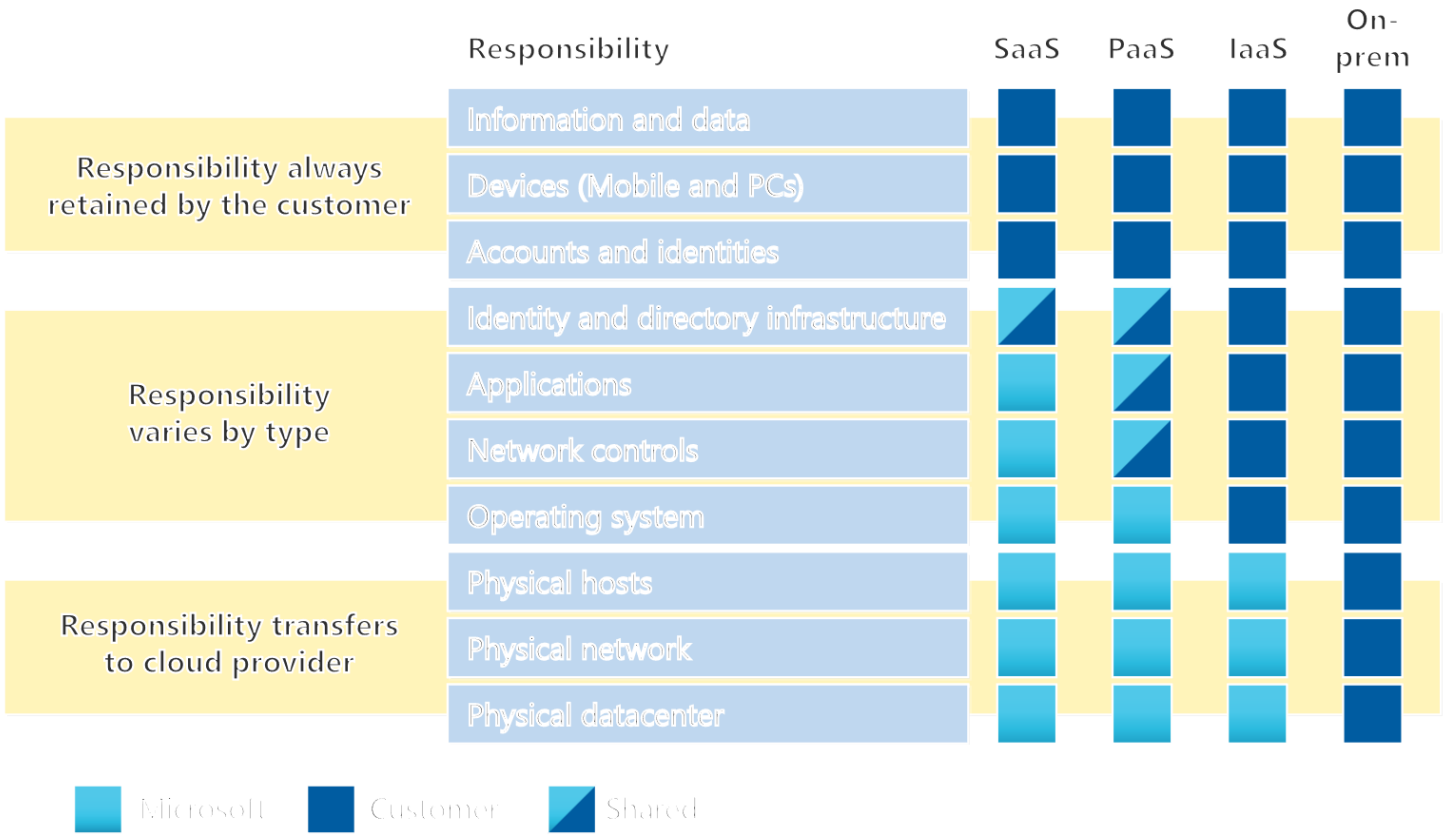
責任共有モデルにおける責任範囲

責任共有モデルの3つのカテゴリ

① すべてのサービスモデルにおいてクラウド利用者が責任を持つ

② クラウド利用者とクラウド事業者がサービスモデルによって責任範囲が決まる

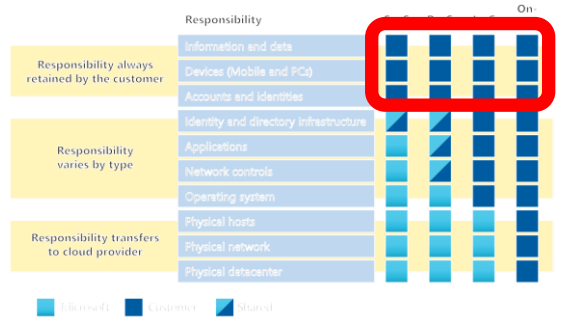
③ すべてのサービスモデルにおいてクラウド事業者が責任を持つ



引用：https://learn.microsoft.com/ja-jp/azure/security/fundamentals/shared-responsibility

責任共有モデルのカテゴリ　①

- すべてのサービスモデルにおいてクラウド利用者が責任を持つ



- カテゴリ①に含まれるもの
  - **データ、情報ガバナンス**
  - **アイデンティティ、アクセス管理（IAM)**
  - **クライアントセキュリティ**

- クラウドを利用するにあたって、
  クラウド利用者が設定、管理、監視等
  の責任を持つ。
  クラウド事業者は、環境を用意
  右図：Salesforceの例

Salesforce

- Salesforceのインフラストラクチャ、プラットフォーム、アプリケーションの安全な設計と実装を推進
- アウトバウンドおよびインバウンドのファイアウォールルールの管理
- Salesforce の機密資産に対する 2 要素認証（2FA）の実施
- テナントごとのデータ隔離の徹底
- プロアクティブなコードスキャンおよび侵入テストの実施
- サードパーティによるセキュリティ評価および監査実施
- 業界標準に準拠した管理の実施
- Salesforce 資産の継続的な監視とインシデント対応の実施

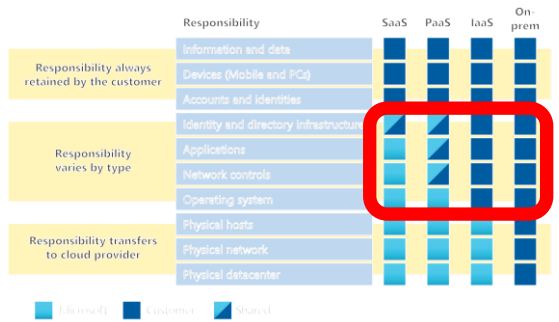
お客様

- HTTPS や SFTP などの安全な通信プロトコルの利用
- アプリケーションレベルのアクセス制御の徹底（例：IP 許可リストや ID 検証の使用）
- 顧客が管理する機密性の高いインターフェースへのMFAの導入
- 安全性の高いユーザープロビジョニングプロセスにそって、適切な役割と権限の付与
- タイムリーに監査ログの収集・分析
- カスタムコードの安全な設計と実装の徹底
- サードパーティとの統合および拡張機能の安全な調達、導入、および維持保守の徹底
- 関連するセキュリティ関連の基準および規制に準拠
- お客様およびカスタムサードパーティの統合資産を継続的に監視し、インシデントに対応
- 不正利用の防止、不正検知、防止策の導入

引用：https://help.salesforce.com/s/articleView?id=000389698&type=1

責任共有モデルのカテゴリ　②

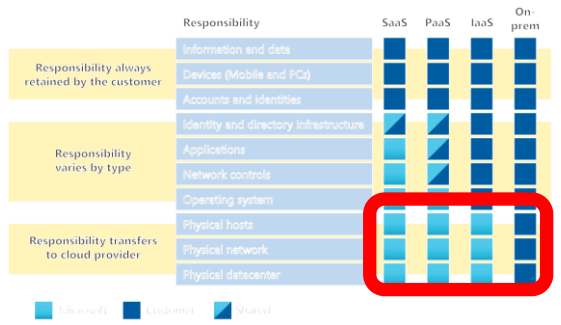
- クラウド利用者とクラウド事業者がサービスモデルによって責任範囲が決まる



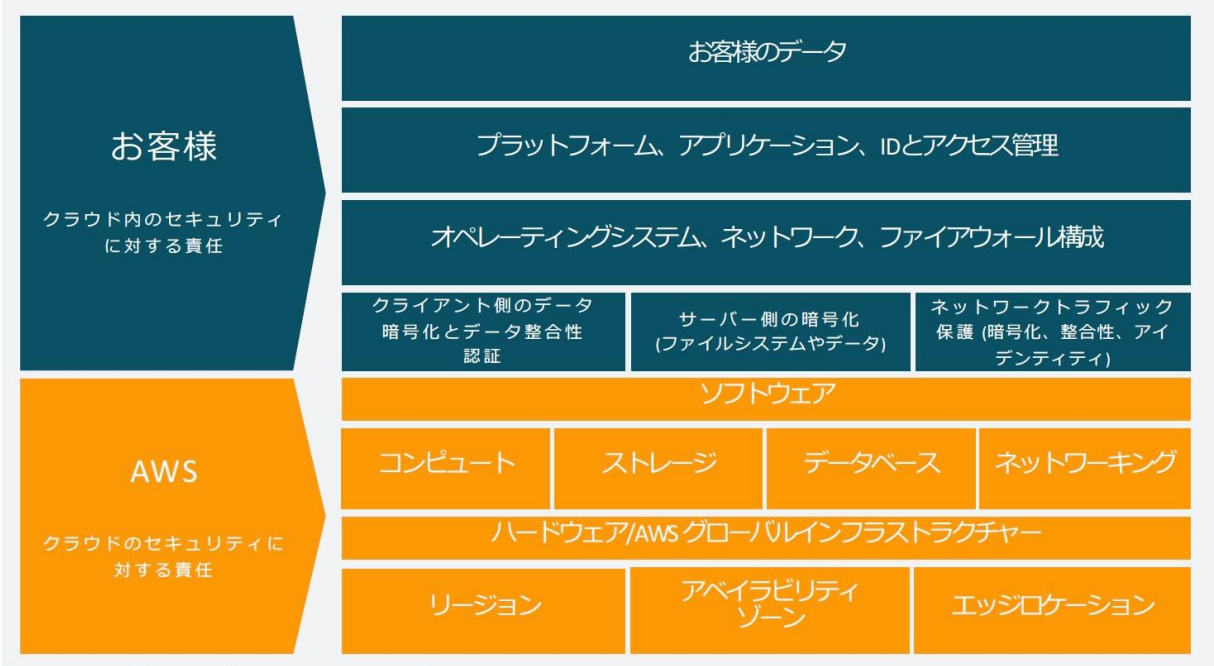
- IaaS/PaaS
  - クラウド利用者は、独自に**セキュリティを作り込む**必要がある境界防御で守られている環境から、クラウド環境に移行するにあたってのセキュリティの作り込みが必要
  - クラウド利用者は、クラウド事業者が提供する**クラウドサービスのセキュリティを評価**する必要がある
- SaaS
  - 基本的に、クラウド利用者は、クラウド事業者が提供する**クラウドサービスのセキュリティを評価**する必要がある

責任共有モデルのカテゴリ　③

- すべてのサービスモデルにおいてクラウド事業者が責任を持つ



- 基本的に、クラウド利用者は、クラウド事業者が提供するクラウドサービスのセキュリティを評価する必要がある
  - インフラストラクチャセキュリティ
    右図：AWSの責任範囲



引用：https://aws.amazon.com/jp/compliance/shared-responsibility-model/

責任共有モデルにおけるクラウド利用者の２つの課題

1. クラウド利用者のセキュリティ対応における課題

2. クラウド利用者がクラウドサービスのセキュリティを評価する際の課題

➡ **今回はこちらに焦点を当てる。特にSaaSにおいては重要**

2. クラウドのリスク管理とCSAツール

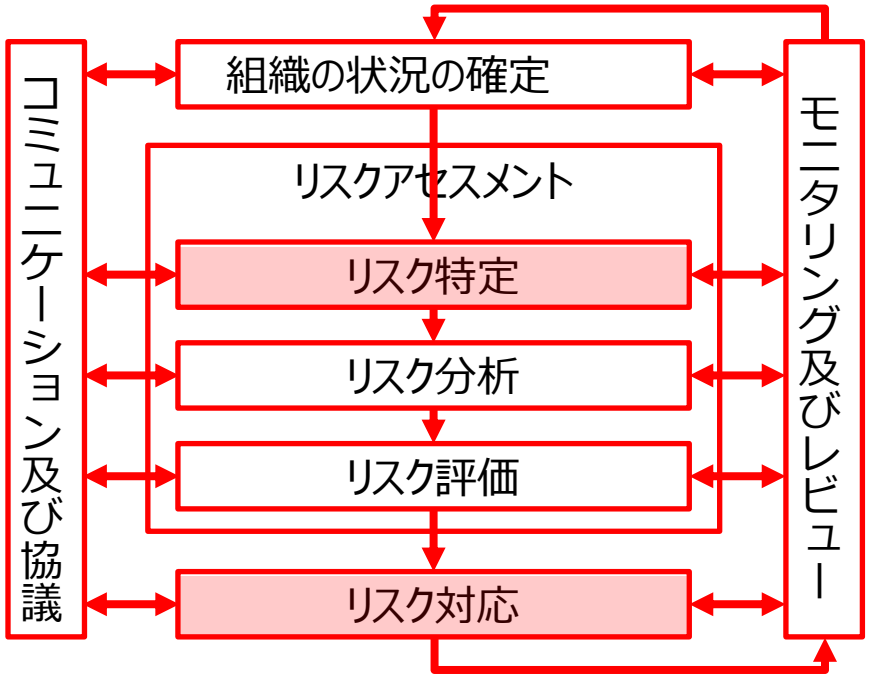
クラウドセキュリティのリスク管理方法

リスク管理における考慮点

1. リスク管理**プロセス**は同じ

2. リスク特定において、クラウド固有のリスクを特定

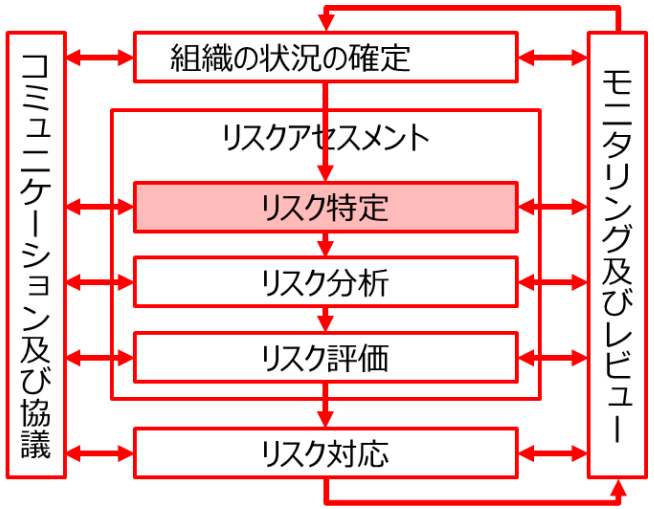
3. リスク対応において、クラウド固有のリスクへの対応を実施
   - ① クラウド利用者としてのセキュリティ対応
   - ② クラウド利用者として、利用するクラウドサービスのセキュリティを評価 ➔ ここではこちらを対象



出典 「ISO/IEC 31000:2010 リスクマネジメント―原則及び指針」

クラウドセキュリティのリスク特定　ー　CSAツール

クラウド固有のリスクを特定



- クラウド固有のリスクとは？
  - ENISAのリスクレポート
  - クラウドサービスにおけるリスクと管理策に関する有識者による検討結果
  - Etc.
  - ➔　なかなか理解するのが大変

- CCM（Cloud Controls Matrix）の利用
  - CCMがリストアップしているクラウド固有の管理策を利用し、クラウド固有のリスクを特定する。セキュリティ要求事項を明確化する。
  - CCMの管理策を理解することでクラウド固有のリスクを理解する。
    - CCMのImplementation Guidanceが参考になる。

CCM、CAIQ、CAIQ-Lite：　一言でいうと！

- **CCM（Cloud Controls Matrix）**
  - CSAが提供するクラウドセキュリティ管理策集
  - 17ドメイン、197の管理策（V4.0.5）
  - 16ドメイン、133の管理策（V3.0.1）
- **CAIQ（Consensus Assessment Initiative Questionaire）**
  - CCMの各コントロールの内容をブレークダウンし、チェックリスト化
  - 質問数
    - 261個　(V4.0.2)
    - 310個　(V3.1)
    - 295個　(V3.0.1)
- **CAIQ-Lite**
  - CAIQの縮小版で、310個を73個に削減（V3.0.1）
  - V4版は2023年9月公開。日本語版の作成中。

CCM、CAIQ、CAIQ-Liteの利点（4つのポイント）

1. タダ（無料）

- 商用利用でない場合、無料で利用可能
- CSAのウエブサイトから自由にダウンロード可能
- 日本語版はCSAジャパンのウエブサイトから自由にダウンロード可能

2. グローバル

- グローバルに通用する。グローバルに同じ内容で提供
  （CCM V3.0.1やCAIQ V3.0.1は10か国語に翻訳提供）
- グローバルに展開している企業は、統一したセキュリティ基準で評価した内容を各国で提供可能

3. クラウドセキュリティに特化

- 提供されている管理策などは、すべてクラウドサービスおよび関連する技術
- チェックリストを作成する際、チェックリストの網羅性を高めることが可能

4. 透明性

- 自己評価結果を公開するサイト（STAR Registry）を用意。STAR Registryも無償で利用可能

CCMの内容　(1)

ドメイン

管理策の内容

サービスモデルとの対応

アーキテクチャの適用レイヤ

CLOUD CONTROLS MATRIX VERSION 4.0.2

				Typical Control Applicability and			Architectural Relevance - Cloud Stack Components					
Control Domain	Control Title	Control ID	Control Specification	IaaS	PaaS	SaaS	Phys	Network	Compute	Storage	App	Data
Audit & Assurance - A&A												
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Shared	Shared	Shared	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
監査・保証	監査・保証のポリシーと手続き	A&A-01	監査・保証のポリシーと手順と基準について確立、文書化、承認、伝達、適用、評価、維持を少なくとも年1回レビューする。	Shared	Shared	Shared	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
監査・保証	独立した評価	A&A-02	少なくとも年1回、関連する基準に従って独立した監査および保証評価を実施する。	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE

CCMの内容　(2)

対応者/部門

言語選択

	Organizational Relevance									
Data	Cybersecurity	Internal Audit	Architecture Team	SW Development	Operations	Legal/Privacy	GRC Team	Supply Chain Management	HR	Language
TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	EN
TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	JP
TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	EN
TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	JP
TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	EN

注）「言語選択」のフィルターにより、「日本語」「英語」あるいは「両方」の選択が可能

CCMの内容　(3)

実装者向けのガイドライン

実装者向け
ガイドライン

CCM CLOUD CONTROLS MATRIX v4.0.5

Control Domain	Control Title	Control ID	Control Specification	Implementation Guidelines
Audit & Assurance - A&A				
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Both the cloud service provider (CSP) and cloud service customer (CSC) should develop a "customized integrated framework" of audit and assurance policies and procedures. This framework should incorporate/demonstrate compliance to leading industry standards and self-imposed business requirements while providing appropriate coverage of controls to assess the respective cloud environment and corresponding services. At a minimum, audit and assurance policies and procedures should include: a. Audit and assurance functions indicating purposes, responsibilities, authorities, and accountabilities to ensure organizational independence, professional care, audit objectivity, and proficiency, b. Audit and assurance plans, c. Audit development policies and procedures to determine criteria and assertions against which the subject matter will be assessed, quality assurance and supervision, sufficient and appropriate evidence, in accordance with commonly accepted frameworks and audit best practices, d. Audit reporting to communicate audit results and findings, e. Follow-up activities to monitor audit findings implementation progress
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent audit and assurance should be free from conflict of interest and undue influence in all matters related to audit and assurance engagements. The frequency of audit and assurance evaluations should comply with applicable standards, regulations, legal/contractual obligations, and statutory requirements. The audit and assurance process should assess all applicable CCM domains.
			Perform independent audit and assurance assessments according to risk-based plans and policies.	Independent audit and assurance assessments should be based on risk-based plans that define audit objectives, scope, resources, timeline and deliverables, documentation and reporting requirements, use of

注：日本語V4.0.6で日本語訳を提供

CCMの内容　(4)

監査者向けのガイドライン

監査者向け
ガイドライン

CCM CLOUD CONTROLS MATRIX v4.0.5

Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines
Audit & Assurance - A&A				
Audit & Assurance	Audit and Assurance Policy and Procedures	**A&A-01**	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	1. Examine policy and procedures to confirm content adequacy in terms of purpose, authority and accountability, responsibilities, planning, communication, reporting, and follow-up. 2. Examine audit charter and determine if independence, impartiality, and objectivity are guarantee 3. Examine policy and procedures for evidence of review at least annually.
Audit & Assurance	Independent Assessments	**A&A-02**	Conduct independent audit and assurance assessments according to relevant standards at least annually.	1. Examine the process to determine standards and regulations applicable to the organization's sys and environments. 2. Determine if the organization maintains and reviews a list of such standards and regulations. 3. Determine if senior management exercises oversight over the independence of the assessment p 4. Determine if the audit plan is informed by previous assessments, and is scheduled on an annual
Audit & Assurance	Risk Based Planning Assessment	**A&A-03**	Perform independent audit and assurance assessments according to risk-based plans and policies.	1. Examine the process for determining the risks applicable to the organization's systems and environments. 2. Determine if a list of such risks is maintained and reviewed. 3. Determine if senior management exercises oversight over the applicable risks

注：日本語V4.0.6で日本語訳を提供予定

CCMの内容　(5)

他基準とのマッピング

他基準とのマッピング

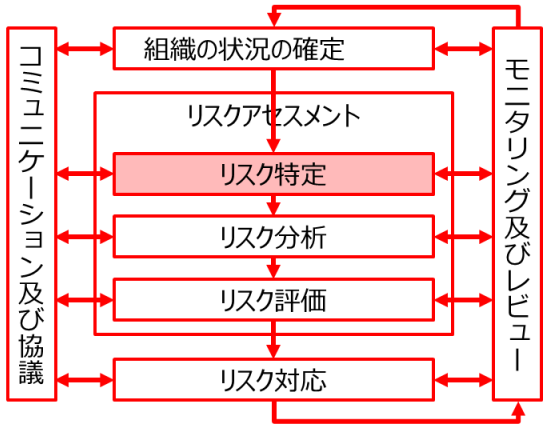
CCM CLOUD CONTROLS MATRIX v4.0.5

				CIS v8.0				
Control Domain	Control Title	Control ID	Control Specification	Control Mapping	Gap Level	Addendum	Control Mapping	Gap
Audit & Assurance - A&A								
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	8.1	Partial Gap	Recommend the full V4 control specification to be used to close the gap. Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (8.1) 'Establish and maintain an audit log management process', 'Review and update documentation annually'.	12.1 12.1.1 12.11	Part
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	7.2	Partial Gap	Recommend the full V4 control specification to be used to close the gap. Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (7.2) 'Establish and maintain a risk-based remediation strategy'.	No Mapping	Ful
Audit & Assurance	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful
Audit & Assurance	Audit Management Process	A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful
[illegible]	[illegible]	[illegible]	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and	[illegible]	[illegible]	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	[illegible]	[illegible]

他基準：　CIS, PCIDSS, ISO/IEC27001/02/17/18, NIST SP800-53 rev5, etc.

クラウドセキュリティのリスク特定　ー　CSAツール

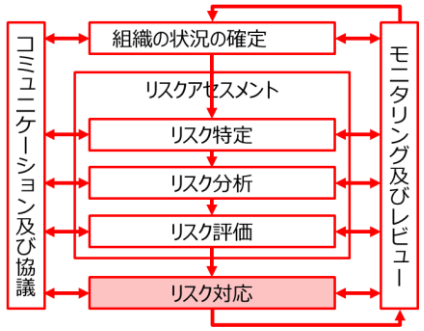
CCMを使ったリスク特定方法



1. 利用するクラウドサービス（候補）に対するセキュリティ要求事項をCCMの管理策からリストアップする
   - ① クラウドに移行する資産を特定
   - ② 資産に対するセキュリティ要求事項を確認
   - ③ セキュリティ要求事項に対して、該当するCCMの管理策をリストアップ
     - その際、Implementation Guideline を参考にし、クラウドセキュリティとして必要となる実装・設定等を理解する
   - ④ CCMでカバーされていないセキュリティ要求事項の明確化
     - CCMでほぼ100%カバーされるが、業界/業種固有の要求事項がある場合にはこれを明確化しておく。

クラウドセキュリティのリスク対応　ー　CSAツール

クラウドサービスのセキュリティ評価



- CAIQ（Consensus Assessment Initiative Questionaire）の利用
  1. 利用しようとしているクラウドサービスのCAIQ評価レポートを以下のどちらかの方法で入手
     - STAR Registryのサイトよりダウンロード
       （STAR Registryについては後述）
     - CAIQをクラウドサービス事業者に送付し、評価結果を入手する
  2. リスク特定において要求事項として洗い出されたCCMの管理策に該当するCAIQの評価レポートを参照し、要求事項を満たしているかどうかを評価・判断
- CCMでカバーされていないセキュリティ要求事項については、クラウド事業者に質問し、明確化

CAIQの内容　(1)

CCMのコントロールを必要に応じて複数の質問に分解している

CSPが自己評価した結果を記載

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?					A&A-01
A&A-01.1	監査・保証のポリシー、手順、基準が確立され、文書化、承認、伝達、適用、評価、維持されているか？					A&A-01
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?					A&A-01
A&A-01.2	監査・保証のポリシー、手順、基準は少なくとも年1回見直され、更新されているか？					A&A-01
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?					A&A-02
A&A-02.1	独立した監査および保証の評価は、関連する基準に従って少なくとも年1回行われているか？					A&A-02
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?					A&A-03
A&A-03.1	独立した監査と保証の評価は、リスクベースでの計画とポリシーに基づいて行われている					A&A-03

CAIQの内容　(2)

- CAIQのカラム
  - CSP CAIQ Answer：　質問に対するCSPの評価結果（Yes/No）
  - SSRM(Security Shared Responsibility Model) Control Ownership：責任共有モデルにおける説明責任と管理責任の所在
    - CSP Owned　：CSPが管理責任。CSPが説明責任
    - CSC Owned　：CSCが管理責任。CSCが説明責任
    - Shared CSP and CSC　：CSCとCSPが管理責任と説明責任を共有
    - 3rd-party outsourced：サードパーティが管理責任。CSPが説明責任
    - Shared CSP and 3rd Party：サードパーティとCSPが管理責任を共有。CSPが説明責任
  - CSP Implementation Description：　CSPからの補足情報（オプション）
  - CSC Responsibilities；CSCの管理責任の概要

CAIQの内容　(3)

CAIQの典型的な利用方法

1. **クラウド利用者**
   - プロバイダ/クラウドサービスのセキュリティを評価するためのチェックリスト
     - クラウド利用者が1からチェックリストを作成するのは厳しい
     - 幅広く利用されている1フレームワークであるCAIQをベースに作成するのが効果的
2. **クラウドプロバイダ**
   - クラウドサービスの透明性
     - プロバイダがセルフアセスメント（自己評価）した結果を公開: STAR Level1:セルフアセスメント（次頁以降説明）
     - クラウド利用者は、公開情報に基づいてプロバイダ/クラウドサービスのセキュリティを評価
     - セキュリティ情報の積極的な公開　＝　ビジネス上の差別化要因
     - クラウド利用者からの問い合わせを統一化可能

CAIQの内容　(4)

CAIQの典型的な利用方法（続き）

3. クラウド監査者

- 被監査者に対する的確な質問の作成
- 内部監査者
  - 内部評価のための質問のガイドとなる
- 外部監査者
  - クラウドプロバイダの監査における評価内容として使用
  - 認証/監査証明の補完（クラウド部分の評価）として使用

CAIQ-Liteとは？

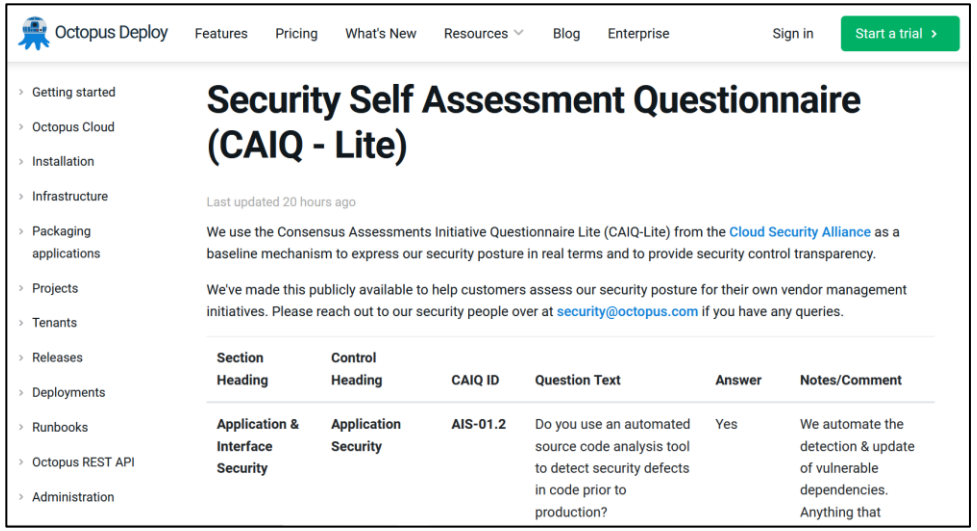
- CAIQの縮小版
  - 質問数を295個から73個に削減
  - 現在提供されているのはV3.0.1。V4.0は開発中

- 以下の方針に基づく厳選された内容
  1. CSA本部において、CAIQ-Liteのさまざまなバージョンを考案し、メンバー間で共有し内部研究を実施
  2. クラウドサービスを評価する利用者からのフィードバックを入手
  3. 600人以上のITセキュリティ専門家による統計分析を行い、クラウドサービスの評価を行う際にCAIQのどの質問が最も適切かの判断を実施

CAIQ-Liteの利用方法

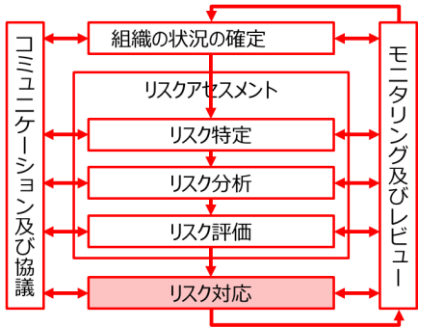
- クラウド利用者がプロバイダ/クラウドサービスのセキュリティを評価するためのチェックリスト
  - CAIQによる評価を行うのが厳しいケース（中小企業等）
  - 基本的なクラウドセキュリティの評価として利用

- プロバイダがCAIQ-Liteを用いてセルフアセスメントし、その情報を自身のウエブサイト等から公開
  - STAR Registry への公開ではなく、独自に公開



引用：https://octopus.com/docs/security/caiq

クラウドセキュリティのリスク対応　ー　CSAツール



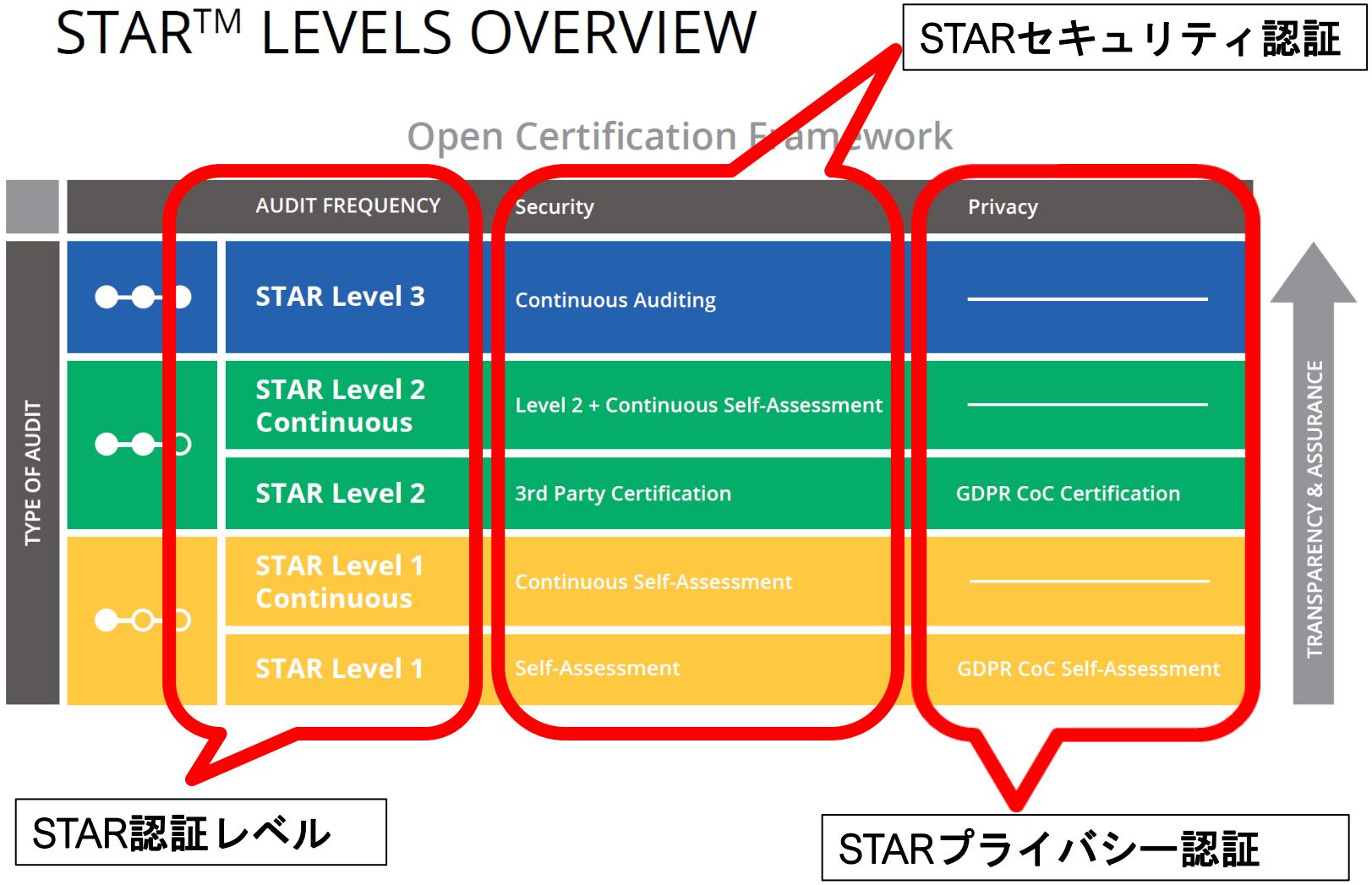
CAIQ評価レポート等を用いてクラウドサービスのセキュリティ評価を行った後の対応

① クラウドサービスのセキュリティが要求事項をすべて満たしている場合
- ➔ そのクラウドサービスを利用

② クラウドサービスのセキュリティが要求事項を満たしていない場合
- ➔ リスク許容可能かどうかを判断。可能であればそのクラウドサービスを利用
- ➔ 許容可能でない場合
  - ➔ そのクラウドサービスは利用せず、別のクラウドサービスを評価する OR
  - ➔ 追加のセキュリティ対策を利用者として行い、要求事項を満たすようにして利用する

4. STAR Registryとは？

STARプログラム　(1)

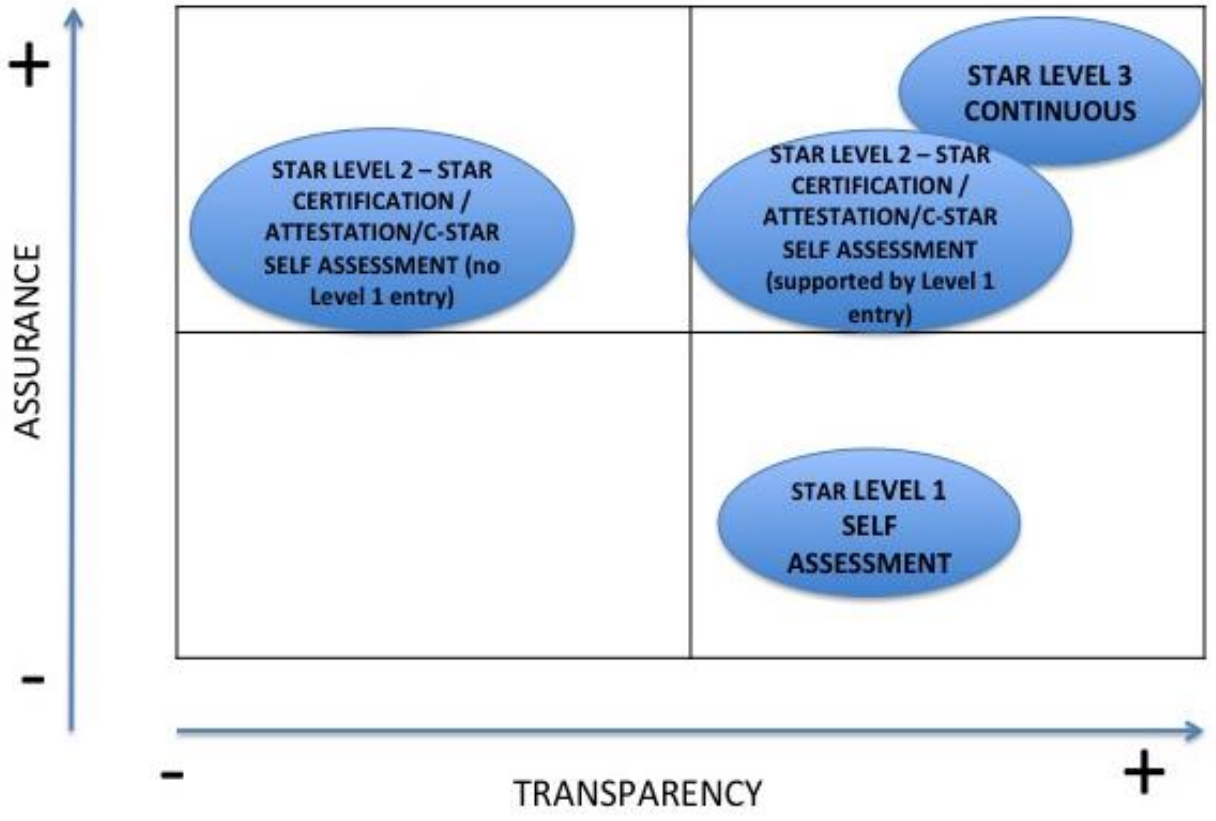


STARプログラム　(2)

STAR　透明性と高い保証

- レベル1
  - プロバイダ自己評価（セルフアセスメント）
- レベル2
  - 第三者認証/監査証明
- レベル3
  - 継続的モニタリング/継続的監査

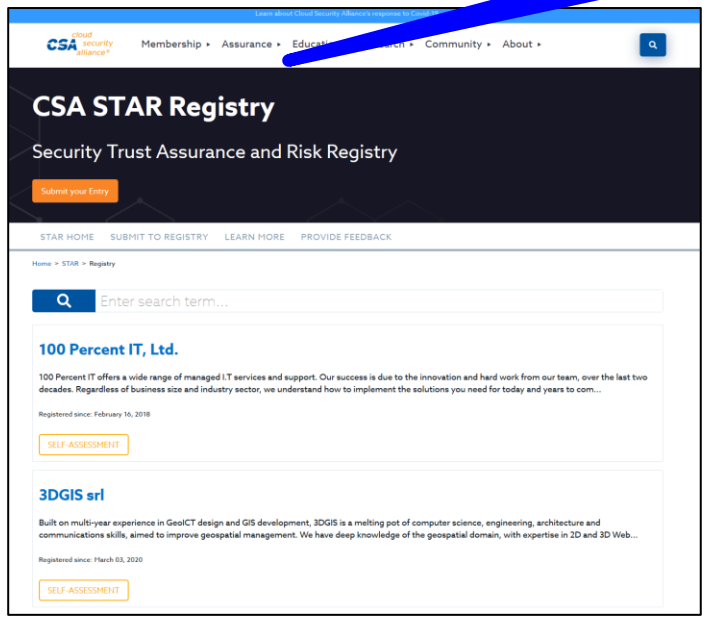
➢ 透明性と高い保証を実現
  ➢ レベル1　＋　レベル2



STARプログラム　(3)

STAR Registry：　プロバイダのセルフアセスメントの結果を公開

公開サイト



プロバイダによるセルフアセスメント

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	Microsoft Azure has established baseline configuration standards and procedures are implemented to monitor for compliance against these	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	Microsoft Azure and Dynamics manage Security and Privacy key performance indicators (KPIs) to	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	Shared CSP and CSC	Microsoft Azure's software development practices are aligned with the Microsoft Security Development Lifecycle (SDL)	Customers are responsible for developing and following a secure software development program for the customer environment.
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	Shared CSP and CSC	Microsoft Azure has established software development and release management processes to control implementation of major changes. Security testing is performed in the	Customers are responsible for developing and following a secure software development program for the customer environment.
AIS-05.2	Is testing automated when applicable and possible?	Yes		Microsoft Azure perform security testing in the implementation, verification and release phases of the	Customers are responsible for developing and following a secure software development program for

引用：　Microsoft AzureのStar1

クラウドプロバイダへ、積極的な公開へのお願い！

1. CAIQ-Liteを利用し、セルフアセスメントを実施、公開
   - 自社ウエブサイトに公開
     - クラウドセキュリティの基本要件の評価結果を公表

2. CAIQを利用し、セルフアセスメントを実施、公開
   - **STAR Registry**に登録
     - クラウドセキュリティの詳細要件の評価結果を公表
     - プロバイダには、CAIQ-LiteよりCAIQによる評価を推奨

CSAジャパンでは、 STAR Registryへの登録方法を支援

- STAR１日本語での登録方法
- 日本語CAIQ評価レポートを公開されている企業情報
- 日本語での評価レポートの公開方法およびLevel1セルフアセスメントの重要性について　（ブログ）

5.　まとめ

まとめ

1. クラウドセキュリティの中核はクラウドサービスのセキュリティ評価
2. クラウドのリスク管理におけるCSAツールの有効性
3. STAR RegistryへのCAIQ評価レポートの公開の重要性

CSAの活動　==　「場」の提供！

様々なワーキンググループ活動の「場」

自由な情報発信の「場」

https://cloudsecurityalliance.jp
mmorozumi@cloudsecurityalliance.jp

ありがとうございました