「クラウド利用者の説明責任とプロバイダの透明性
~CSAが提供するCCM/CAIQ等の有効活用~」

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

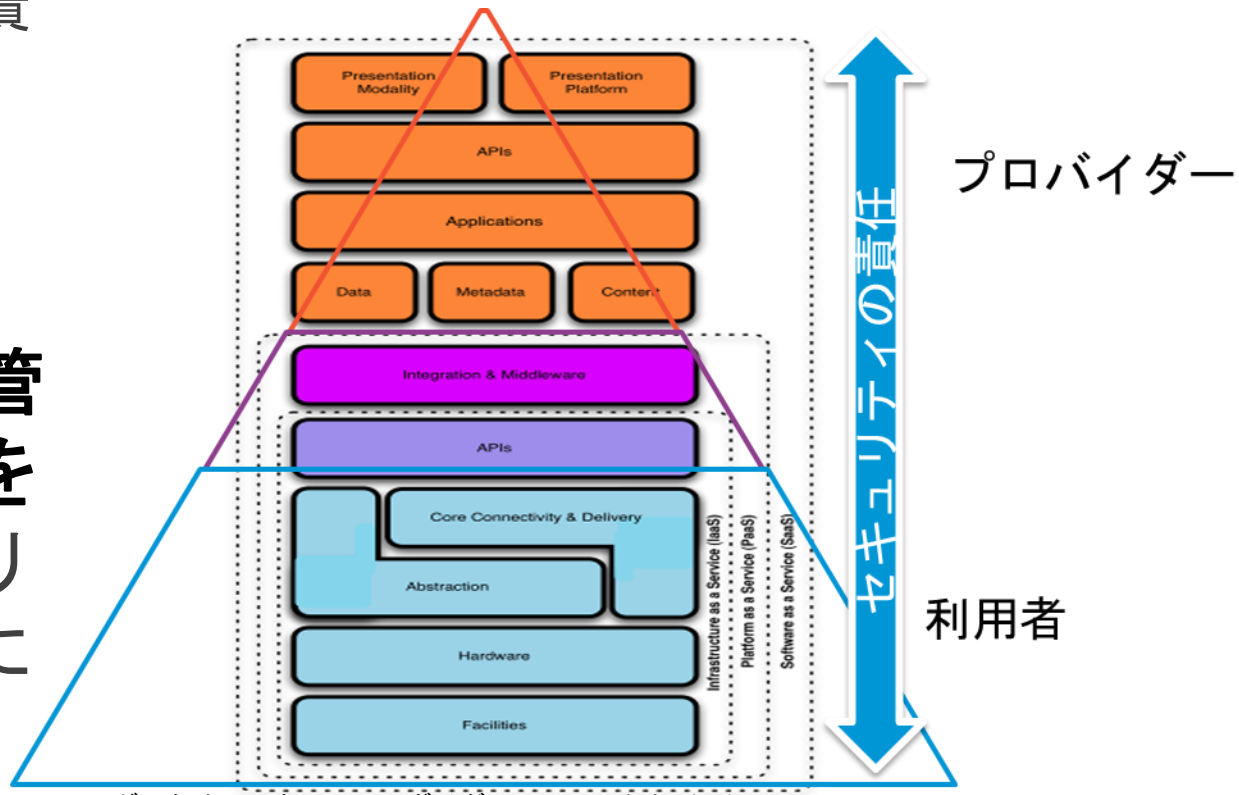
2022年5月26日

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。

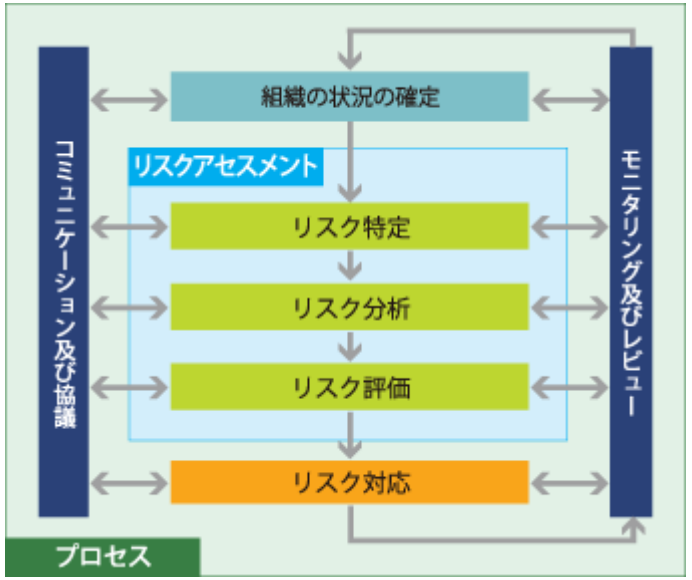


（クラウドコンピューティングのためのセキュリティガイダンス　V3.0から引用）

利用者側の説明責任　ー　何が違うのか

クラウドに限った話ではない！

- リスク管理**プロセス**はオンプレと全く変わらない！
  - 資産の特定　->　リスクの特定　->　リスク評価　->　リスク対応　・・・
  - クラウドでは、リスク管理の何が違うのか？
    - クラウド固有のリスクを特定すること
- **直接か間接かの違い！**
  - セキュリティ要求事項は、オンプレでもクラウドでも基本的に変わらない
  - 要求事項を満たしているかどうかの判断・対応
    - オンプレ：　自ら対策等を取っていく
    - クラウド：　プロバイダ/クラウドサービスが提供する機能・情報に基づいて判断



引用：情報誌 ISO NETWORK Vol.22、
https://www.jqa.jp/service_list/management/iso_info/iso_network/vol22/news/kikaku_3.html

利用者側の説明責任　ー　サービスモデルの考え方

説明責任に対するサービスモデルの考え方

- IaaS/PaaS
  - プロバイダが限定されている。セキュリティ要件の統一が可能
  - 利用形態として、オンプレからの移行、あるいは、新規システムの構築が主体
  - **利用者として、詳細リスク分析が必要**
- SaaS
  - 多種多様なクラウドサービス/プロバイダ
  - セキュリティレベルも様々。セキュリティに関する問い合わせに無回答の場合もあり
  - **利用者として、クラウドサービス/プロバイダごとのセキュリティ評価が必要**
    HOW？

利用者側の説明責任　ー　まとめ

やはり、説明責任を真剣に考えよう！

- まず組織としてのセキュリティ要求事項を明確化しよう！
  内部デューデリジェンス
  これは、クラウドに限らず組織としての要求事項
- 次に、クラウドプロバイダが要求事項を満たしているかを確認しよう！
  外部デューデリジェンス
  クラウドサービスが要求事項を満たしているがどうかを評価

でも１からやるのは大変、難しい！-> そこで、CCM, CAIQ, CAIQ-Liteの登場。フレームワークを使おう。

CCM、CAIQ、CAIQ-Liteとは？

CCM、CAIQ、CAIQ-Lite：　一言でいうと！

- **CCM（Cloud Control 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版は作成中

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

Control Domain	Control Title	Control ID	Control Specification	Typical Control Applicability and			Architectural Relevance - Cloud Stack Components					
				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

cs	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)

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 l
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：監査者向けのガイドラインはV4.0.5から提供。現在日本語版はV4.0.2

CCMの内容　(4)

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
Audit & Assurance	Remediation	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and	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

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

注：他基準とのマッピングはV4.0.5から提供。現在日本語版はV4.0.2

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
    - CSC Owned
    - 3rd-party outsourced
    - Shared CSP and CSC
    - Shared CSP and 3rd Party
  - CSP Implementation Description：　CSPからの補足情報（オプション）
  - CSC Responsibilities；CSCが管理責任を果たすための概要。

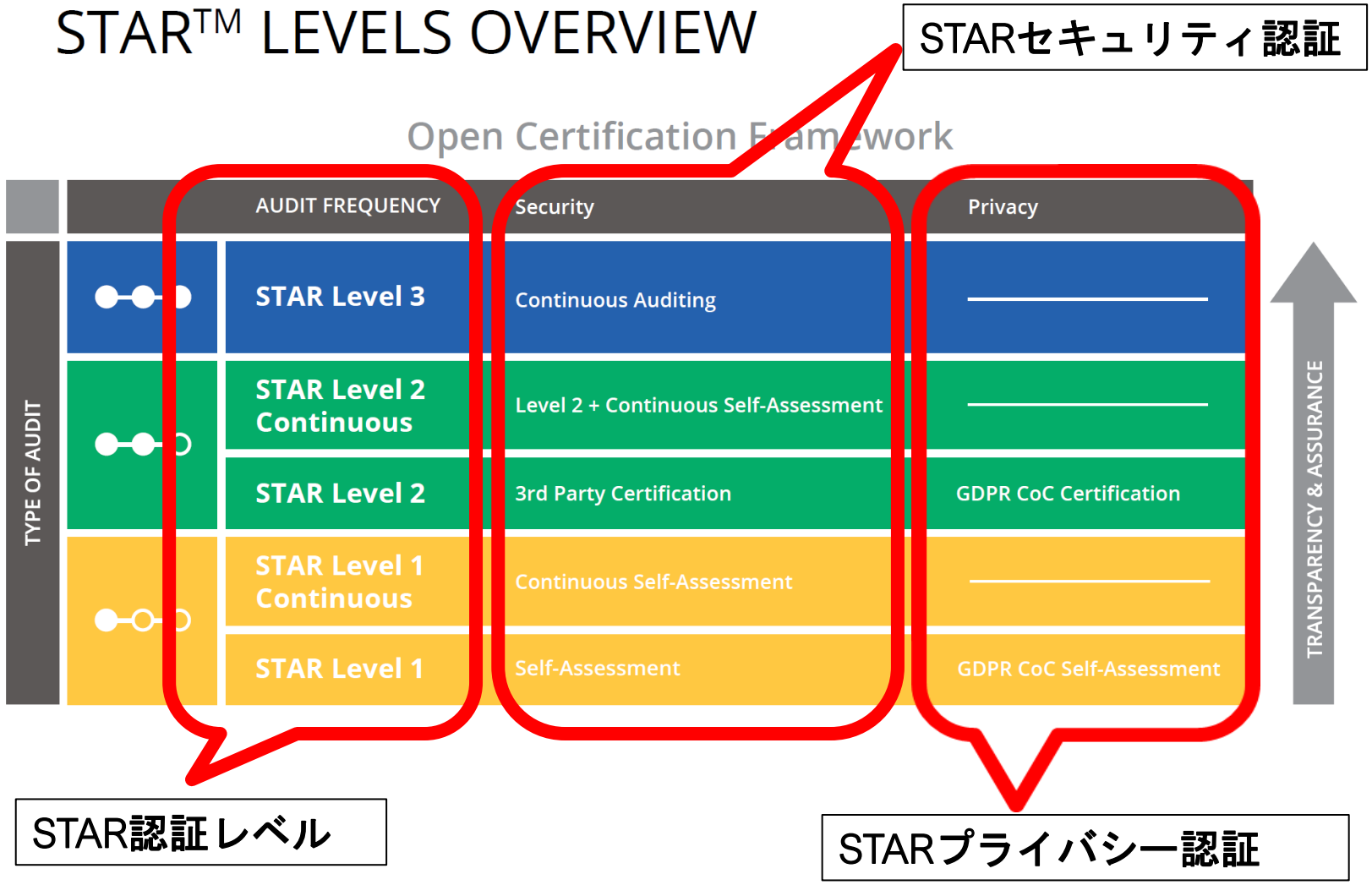
CAIQの内容　(3)

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**
   - 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をベースに作成のが効果的

2. **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

STARプログラム　(1)

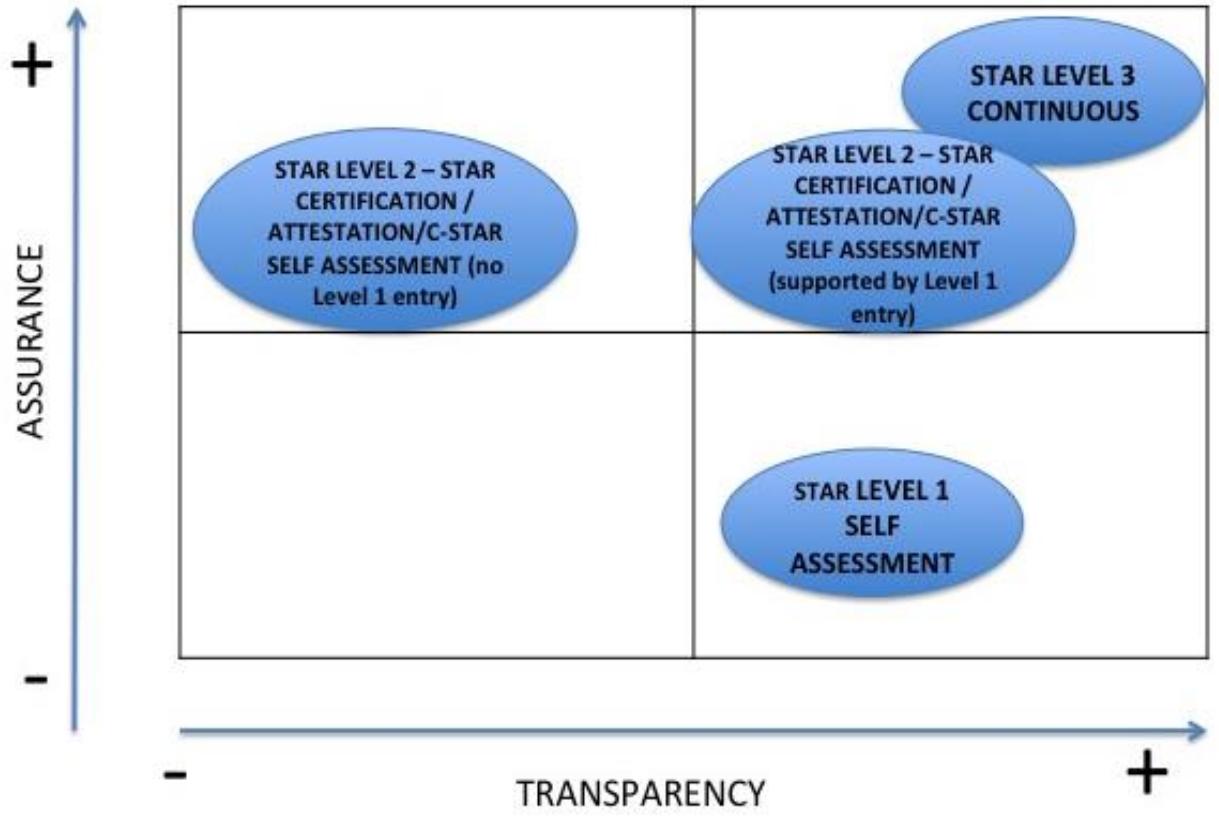


STARプログラム　(2)

STAR　透明性と高い保証

- レベル1
  - プロバイダ自己評価
- レベル2
  - 第三者認証
- レベル3
  - 継続的モニタリング/監査

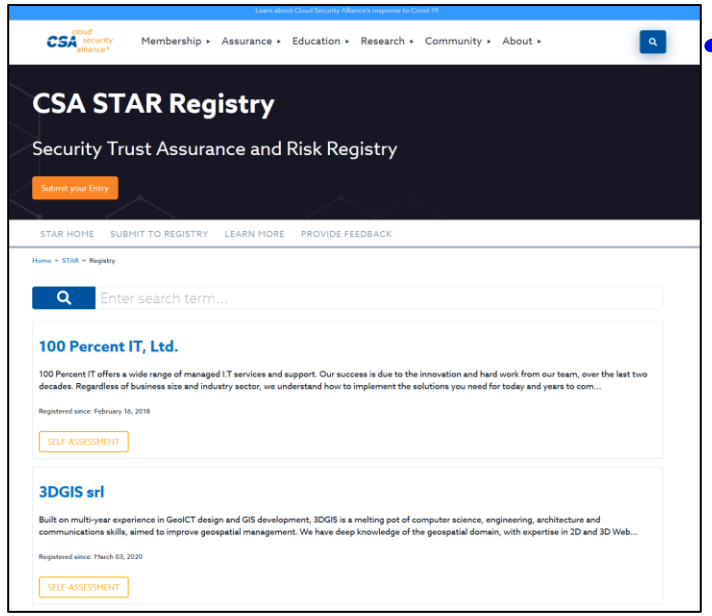
透明性と高い保証を実現



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
（Registry）



プロバイダに
よるセルフア
セスメント

CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
estriction		IAM-06.2	the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Access to tenant applications is controlled by the tenant
dentity & Access Management *hird Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you provide multi-failure disaster recovery capability?	X			
		IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	X			
		IAM-07.3		Do you have more than one provider for each service you depend on?	X			
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	X			Available internally
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?	X			
		IAM-07.6		Do you provide a tenant-triggered failover option?	X			Available on reque
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?	X			Available on reque
dentity & Access Management *ser Access Restriction / uthorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant and approve access to tenant data?	X			
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	X			

CAIQ-Liteとは？

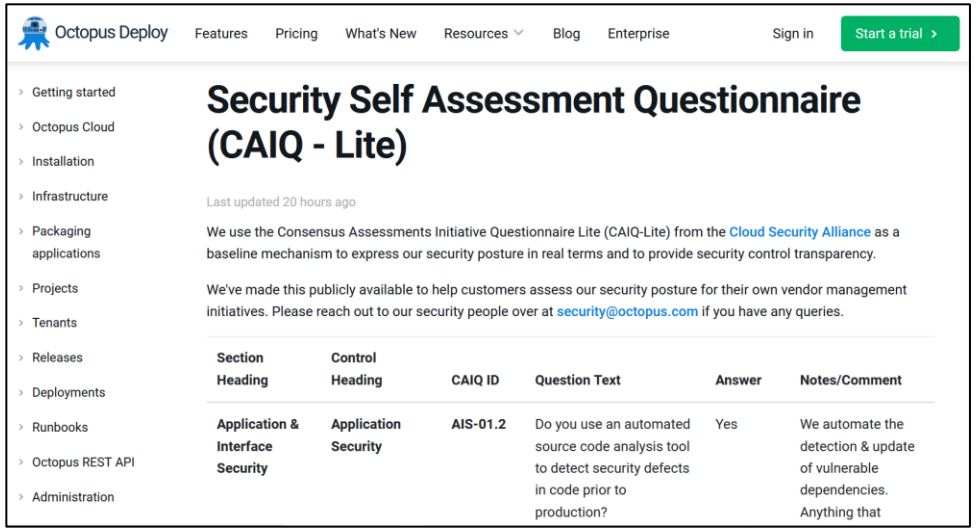
- CAIQの縮小版
  - 質問数を295個から73個に削減
  - 現在提供されているのはV3.0.1。V4.0は計画中

- 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

クラウドの評価方法
CAIQ、CAIQ-Liteの利用方法

クラウドの評価方法

1. クラウド利用者自ら1からチェックリストを作成し評価を実施
   - 利点：　クラウドのリスクに基づいた詳細な評価が可能
   - 課題：　クラウドセキュリティに精通した専門家が必要
2. CASBが提供するクラウドサービスリスク評価を利用
   - 利点：　精度が高い。スコア付けに基づき評価が容易
   - 課題：　CASBの導入が必要。利用要件に関わらず一様の評価
3. VRM（vendor risk management）、TPRM（third-party risk management）ソリューションを利用
   - 利点：　精度が高い。手間がかからない
   - 課題：　ソリューションあるいはサービスの購入が必要。新しい領域なので、有効性等の評価が必要

クラウドの評価方法

4. プロバイダ公開情報を利用
   - プロバイダ公開情報（ウエブページ等）、STAR Registry
   - 利点：　いつでも参照可能。管理策に関する網羅性が高い
   - 課題：　情報を公開していないプロバイダは評価できない

5. フレームワークを利用し、利用者独自にチェックリストを作成、評価
   - 標準：　ISO/IEC 27017, クラウド情報セキュリティ管理基準
   - CSA：　CAIQ、CAIQ-Lite
   - 利点：　管理策に関する網羅性が高い
   - 課題：　クラウドセキュリティの知識が必要。やり易さはフレームワークに依存

CAIQ、CAIQ-Liteの利用方法：クラウド利用者　(1)

IaaS/PaaS　利用者

詳細リスク分析による評価

1. 内部デューデリジェンスの実施
   - 組織としてのセキュリティ要求事項を明確化
2. 外部デューデリジェンスの実施
   - CAIQを用いてセキュリティ要求事項のチェックリストを作成
     - STAR Registryにプロバイダが公開している情報に基づく
     - STAR Registryに公開していないプロバイダの場合は直接回答を求める
   - CAIQでカバーされていないセキュリティ要求事項のチェックリストを作成
     - プロバイダに回答を求める

CAIQ、CAIQ-Liteの利用方法：クラウド利用者　(2)

SaaS　利用者

1. CASBが提供するクラウドサービスリスク評価に基づいて評価
2. CAIQ-Liteを用いたベースラインアプローチによる評価
   - プロバイダ公開情報（ウエブページ等）に基づいて評価を実施
   - VRM、TPRMの利用も考慮
   - プロバイダが情報公開していない場合、CAIQ-Liteを直接プロバイダに送付し回答を求める
3. 詳細リスク分析による評価
   - CAIQを用いて詳細にクラウドサービスを評価

クラウドプロバイダの対応

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、あるいは、自社ウエブサイトに公開
     - 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　（情報提供待ち）
- 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）

まとめ　ー　CCM,CAIQ,CAIQ-Lite,STARに関連するCSAジャパンの活動

- **CCM/STAR WG**
  - CCM,CAIQ,CAIQ-Lite,STAR 資料/情報の翻訳/公開、プロモーション
  - ISMAPとCCMのマッピング
- **CASB WG**
  - SaaS をよりセキュアに利用・運用するためのベストプラクティスの調査・研究
- **クラウドプライバシーWG**
  - STARプライバシー認証のベースになる “CODE OF CONDUCT FOR GDPR COMPLIANCE”（日本語名：GDPR 準拠の為の行動規範）の翻訳/公開
  - 「個人情報の保護に関する法律準拠の為の行動規範」の作成/公開
- **IoT WG**
  - IoT Control Matrixの翻訳/公開（現在、V3の作業中）
- **クラウドセキュリティWG**
  - AWS/Azure/GCPのセキュリティのアーキテクチャレビュー（CCMの技術面を支援）

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

info@cloudsecurityalliance.jp

ありがとうございました