「クラウド監査人向けクラウドセキュリティ認定資格 CCAK(Certificate of Cloud Auditing Knowledge)解説」

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1月24日

CCAK(Certificate of Cloud Auditing Knowledge)　とは？

- 目的
  - CCAK is the first-ever, technical, vendor-neutral credential for cloud auditing. This certificate fills a gap in the industry for competent technical professionals who can help organizations mitigate risks and optimize ROI in the cloud.
    CCAKは、クラウド監査のための、技術的でベンダーニュートラルな初の資格です。この資格は、企業がクラウドにおけるリスクを軽減し、ROIを最適化することを支援できる有能な技術専門家を求めている業界のギャップを埋めるものです。

  - CCAK prepares IT professionals to address the unique challenges of auditing the cloud, ensuring the right controls for confidentiality, integrity and accessibility and mitigating risks and costs of audit management and non-compliance.
    CCAKは、クラウドの監査、機密性、完全性、アクセシビリティのための適切なコントロールの確保、監査管理やコンプライアンス違反のリスクとコストの軽減といった独自の課題に対処するためのITプロフェッショナルを育成します。

CCAK(Certificate of Cloud Auditing Knowledge)　とは？

- CCAKのポジション
  - ISACAが提供するCISA, CISM, CRISC, CGEITを補完
  - FedRAMP 3PAO Assessor, PCI-DSS Qualified Security Assessor, ISO 27001 Leader Auditor を補完
  - ISACAの監査の専門家とCSAのクラウド専門知識を強化
  - DevOps、CI/CDのような技術/配備フレームワークを含む
  - CSAのCCSKをベースにして、それを補完する内容
- 対象者
  - 内部・外部監査人
  - コンプライアンス管理者
  - 第三者監査人
  - ベンダー/パートナー・プログラムマネージャ
  - セキュリティ・アナリスト/アーキテクト
  - 調達部
  - サイバーセキュリティ・リーダー/アーキテクト
  - セキュリティ、プライバシー・コンサルタント

ベストマッチ

CCAK試験　概要

- 試験時間：　2時間
- 問題数：　76問
- 合格ライン：　70%
- 言語：　英語
- 試験費用：　$395：ISACA会員（$495：非会員）
  CSA本部の企業会員向けの割引もあるようです
- 試験方法：　オンライン
  PSIというサードパーティーの試験機関を使用
- CCAK向けテキスト
  - Certificate of Cloud Auditing Knowledge™ Study Guide：
    $59.00：ISACA会員（$70.00：非会員）
    CSA本部の企業会員向けの割引もあるようです

CCAK試験　必要な情報

- Certificate of Cloud Auditing Knowledge™ Study Guide
  - ISACAのウエブサイトより購入：$59（ISACA会員）、$70（非会員）
- Consensus Assessments Initiative Questionnaire (CAIQ) v3.1　（日本語）
  - https://cloudsecurityalliance.org/artifacts/caiq-translation-in-10-languages/
- Cloud Controls Matrix (CCM) v3.0.1　（日本語）
  - https://cloudsecurityalliance.org/artifacts/ccm-translation-in-10-languages/
- Top Threats to Cloud Computing Deep Dive (2018)　（日本語）
  - https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2020/11/Top-Threats-to-Cloud-Computing-Egregious-Eleven-Deep-Dive-J.pdf

注）CCM/CAIQは、一部V4.0の知識（V3との違い）も求められる。

CCAK活動状況

- ISACAとCSAのパートナーシップに基づいて展開
  - Study Guide, Exam
    - CSA:　コンテンツの開発
    - ISACA:　試験問題の開発
  - ISACAが、CCAKのトレーニング・試験の展開を担当

今後の日本での展開等についてはISACA次第か？？？

CSAジャパンとしては、以下のCSA本部側の担当を通じて対応可能

- Daniele Catteddu：　Chief Technology Officer
- Rick Blue:　Director, Training Partners

CCAK　ドメイン構成

1. Cloud comAn overview of cloud governance, frameworks, and cloud governance tools: 18%
   クラウドガバナンスの概要、フレームワーク、クラウドガバナンスツールの紹介
2. pliance program: designing and building: 21%
   クラウドコンプライアンスプログラム：設計と構築
3. CCM and CAIQ Goals, Objectives, & Structure: 12%
   CCMとCAIQの目標、目的、構成
4. A Threat Analysis Methodology For Cloud using CCM: 5%
   CCMを用いたクラウドのための脅威分析手法
5. Evaluating a Cloud Compliance Program: 9%
   クラウドコンプライアンスプログラムの評価
6. Cloud Auditing: 15%
   クラウド監査
7. CCM: Auditing Controls: 8%
   CCM: コントロールの監査
8. Continuous Assurance and Compliance including DevSecOps: 7%
   DevSecOpsを含む継続的保証とコンプライアンス
9. STAR Program: 5%
   STARプログラム

各ドメインで求められる知識

1. クラウドガバナンスの概要、フレームワーク、クラウドガバナンスツールの紹介 (1)

- クラウドガバナンス概要
  - クラウドガバナンスと一般のガバナンスの違い
    - 直接管理できない、複数の地域にわたる法律の適用の問題、プロバイダごと異なる成熟度の問題等。
  - 責任共有モデル： サービスモデル（IaaS/PaaS/SaaS）のガバナンスの考え方
    - IaaS/PaaS: すべてのプロバイダに共通するポリシーの設定
    - SaaS: プロバイダごとに異なる成熟度に対する評価/契約/SLA
  - 責任共有モデル： 配備モデル（パブリック/プライベート等）のガバナンスの考え方
    - パブリッククラウド： マルチテナント環境を維持
    - プライベートクラウド： オンプレに近い環境、ただし、クラウド固有のリスクを考慮
    - そのほか
- 責任と説明責任
  - RACIマトリックスに基づく責任の所在の明確化
- クラウドにおけるトラストの考え方
  - Trust＝Accountability + Transparency + Assurance

1. クラウドガバナンスの概要、フレームワーク、クラウドガバナンスツールの紹介(2)

- クラウドガバナンスフレームワークの概要
  - CCM、NIST SP800-53、ISO/IEC27017、BSI C5、PCISSC Cloud Computing Guidelinesなど
- クラウドリスク管理
  - クラウド固有のリスクの考慮が必要
    - 隔離の失敗、インタフェース侵害、不十分なデータ削除、シャドーIT、サプライチェーンの問題、など
    - リスク管理フレームワーク
      - ISO/IEC 27005, NIST SP800-30　など
      - CSA提供フレームワークとして、CCM, CAIQ, Top Threat Deep Dive (別ドメインで詳細説明)
- クラウドコンプライアンス
  - コンプライアンスに対する責任範囲（プロバイダ、カスタマ、カスタマとしてのプロバイダ）の明確化
  - コンプライアンス継承

1. クラウドガバナンスの概要、フレームワーク、クラウドガバナンスツールの紹介(3)

- クラウドガバナンスツール
  - クラウドにおけるポリシー
    - 責任共有モデルにおける、ポリシー実施（PEP）
    - コントロール・オーナーとしての役割は、CSPのコントロールが十分か同課の評価
  - 契約
    - クラウド利用において最も重要なガバナンスツール
    - マスター契約、Terms&Condition、SLA、UAP、など

2. クラウドコンプライアンスプログラム：設計と構築(1)

- クラウドコンプライアンスプログラム
  - クラウドコンプライアンスプログラムの一般的な要素
    - Actor, Business/organization perspective, Governance perspective, Risk perspective
  - クラウド固有の要素としての考慮点
    - オンプレ：すべての要件に対して完全なコントロールと責任
    - クラウド：利用者とプロバイダの責任共有。ただし、説明責任は利用者に残る
- クラウドに関係する法律・規制要件の概要
  - HIPAA, GLBA, GDPR, SOX, CLOUD等
- クラウドに関係する標準の概要
  - ISO/IEC 17788,17789, 27017, 27018, 27701
  - NIST SP800-53, BSI C5, ENISA IAF, PCIDSS, PCI Cloud Computing Guideline, CIS, EU-SEC, など
  - CCM/CAIQ, PLA(CoC for GDPR) ：CSA

2. クラウドコンプライアンスプログラム：設計と構築(2)

- 管理策の実施
  - 一般的な管理策の内容、リスク対応等の知識
  - フレームワークとして ISC/IEC 27001, NIST SP800-53, CSA CCM等の構成
- クラウドセキュリティにおけるCertification, Attestation, Validation
  - Certification : ISO/IEC 27001 + CSA STAR Certification
  - Attestation: SOC + CSA STAR Attestation
    SOC1/2/3の概要
    BSI C5:
  - Validation: FedRAMP, MTCS, PCIDSS

3.　CCMとCAIQの目標、目的、構成(1)

- CCMの概要
  - CCMのリリース方針（full, dot release, minor releaseの意味）
  - ターゲット
    - カスタマ：主に要求事項の詳細リストの作成
    - プロバイダ：主にクラウド固有で業界で認知されているセキュリティに対する内部プログラム
    - 監査人/コンサルタント：　顧客に対するガイド
- CCMのドメイン構成
  - 業界標準とのマッピング、管理策のオーナーシップ、ガイダンスとの関係、など
  - 各ドメインの詳細
- CAIQの概要
  - CSPがセキュリティ仕様をに対していることを確認する質問集
  - CCMに対してCAIQに含まれる内容

3.　CCMとCAIQの目標、目的、構成(2)

- CCMと他の規格との関係，マッピング/ギャップ分析
  - マッピングの目的
  - マッピングされている標準、規格
  - ギャップ分析のアプローチ方法。ギャップで使用される定義（No gap, Partial Gap, Full Gap）
  - マッピングとリバースマッピングとは。
- CCM V3 から CCM V4への移行
  - CCM V3とCCM V4のドメイン構成の違い
  - 実装と監査用のガイダンス
  - V3からV4への移行ポリシー（STAR Certification, Attestationに適用）

- *CCM、CAIQの理解のための参考資料*
  - *2020年Japan Security Summit での講演資料（CCM、STAR認証、ISMAPとの関連について講演したもの）*
    https://www.slideshare.net/MasahiroMorozumi/ccmstarjapan-security-summit-2020

4.　CCMを用いたクラウドのための脅威分析手法(1)

- 脅威分析手法
  - クラウド脅威モデリング、ディープダイブの概要の理解
  - 分析
    - Attack Details, Technical Impacts, Business Impacts
  - 緩和策
    - 管理策、メトリックス
  - ユースケース
- 脅威分析ツール
  - CSA Top Threat and Survey
  - CSA Top Threat Deep Dive
  - CSA CCM
  - Mitre ATT&CK
  - NIST Valunerability Database
  - US National Cyber Awareness System

4.　CCMを用いたクラウドのための脅威分析手法(2)

- *脅威分析手法として以下の内容の理解が必要*
  - *クラウド脅威モデリング*
    https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2021/10/Cloud-Threat-Modeling_J.pdf
  - *クラウドの重大セキュリティ脅威　11の悪質な脅威*
    https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/10/top-threats-to-cloud-computing-egregious-eleven_J_20191031.pdf
  - *クラウドコンピューティングの重大脅威: 11の悪質な脅威 ディープダイブ*
    https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2020/11/Top-Threats-to-Cloud-Computing-Egregious-Eleven-Deep-Dive-J.pdf

5. クラウドコンプライアンスプログラムの評価(1)

- クラウドコンプライアンスプログラムの有効性評価の3つのポイント
  - 組織にとって、該当するクラウドサービスが目的と一致しているかどうかの評価
  - 管理策の有効性の評価
  - 継続的コンプライアンス（Continuous compliance）の実装
- ガバナンスの観点での評価
  - コーポレートポリシーとの整合性
  - ポリシー違反に対する対処
  - クラウドにおけるポリシー評価の自動化
- 法律、規制、標準の観点での評価
  - 適用される法律、規制、標準に対する評価
  - 契約関係の評価

5. クラウドコンプライアンスプログラムの評価(2)

- リスクの観点での評価
  - 一般的なリスク管理としてのコンプライアンス評価をクラウドにも適用
    - リスク対応としての管理策のコンプライアンス状況の評価
    - コンプライアンス目的とリスク選好の整合性
    - 管理策の有効性のモニタリング
- 継続的コンプライアンス
    - Continuous Auditing: 継続した評価プロセス。管理策の評価
    - Continuous Monitoring: 継続した情報セキュリティを維持するため
    - Continuous Assurance: Continuous MonitoringとContinuous Auditingの結果
    - Continuous Compliance: Continuous Assuranceとほぼ同義
  - Continuous Auditingの指標（SLO, SQO）の理解

6. クラウド監査

- 一般的な監査の知識
  - Scope, 基本原理（independence, Integrity and objectivity, Due Professional care, Confidentiality, etc.）, Internal/External auditing, Audit/Assessment など
  - 監査の標準
    - ISO/IEC 17021, ISC/IEC 27006, ISO/IEC 19011
    - SOC
- オンプレの監査とクラウド監査の違い
  - 技術的な考慮点
    - オーナーシップ、ITリソースの場所、災害復旧（DR)、コンプライアンス要件
  - 責任共有のインパクト
    - サービスモデルごとの監査範囲、監査計画
    - コンプライアンス継承
- 継続監査(Continuous Auditing)の必要性

7.　CCM: コントロールの監査（監査のガイドライン）

- CCM Auditing Guidelineの理解
  以下の資料が公開されているが、こちらはCCM V4ベース。V3のものを探したが見つからなかった。
  試験としては、以下の資料の内容を理解すれば大丈夫そう。
  https://cloudsecurityalliance.org/artifacts/ccm-v4-0-auditing-guidelines/
- 監査のスコープ
  - クラウドサービスモデル、クラウド配備モデルを考慮
  - CCMに基づくリスク評価
  - CCM Audit Workbook の利用
    - Control audit frequency, Test Plan, Test result, Reference to supporting documentation
    - これらに基づいて監査の準備、実施、評価を行う

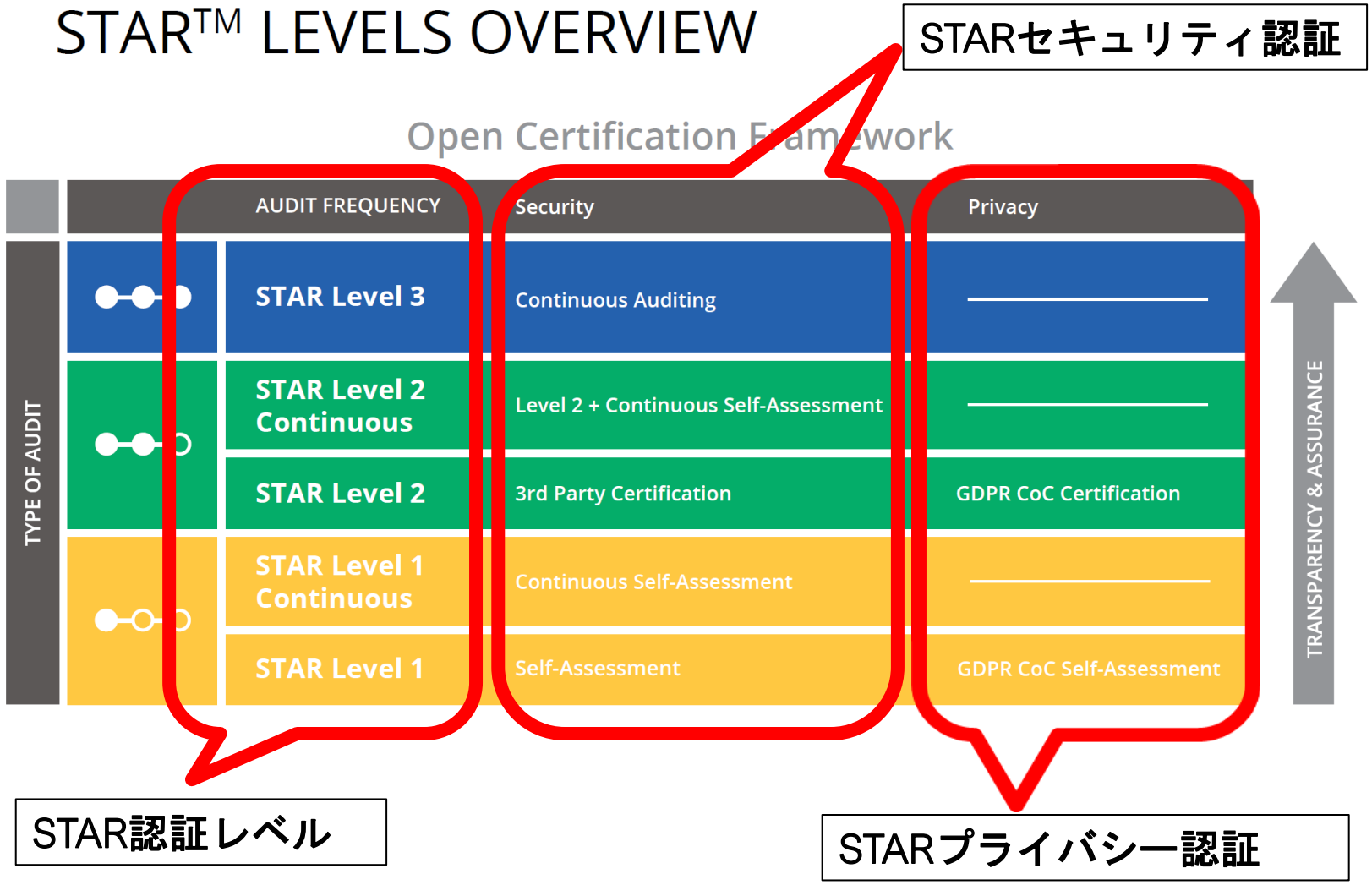
8.　DevSecOpsを含む継続的保証とコンプライアンス

- 継続的保証とコンプライアンスとして、自動化（Automation）とオーケストレーション（統合管理？　orchestration）にフォーカス
  - DevOps, DevSecOps　のフレームワークの理解
  - CI/CDに基づく全体的な流れ
  - 監査人としては、このフレームワーク、プロセスを監査する
    - きちんと構成されているCI/CDであれば完全な監査が可能
  - セキュリティテストのCI/CDプロセスへの統合の理解
    - テストの種類（SAST, DAST等）
    - チェックポイントとしての Security gate　の考え方
  - コンテナ、FaaS/サーバレスについての理解

9. STARプログラム(1)

- STARレベル1,2,3の概要
  - OCF（Open Certification Framework) の概要
- STARにおけるセキュリティとプライバシー
  - セキュリティはCCM
  - プライバシーはCode of Conduct (CoC) for GDPR Compliance
- STAR Registry
- STAR認証における成熟度モデル
- STAR関連の評価として C-Star
- STAR Continuous (レベル3)

9. STARプログラム(2)



9. STARプログラム(3)

- *参考資料*
  - *ブログ：https://cloudsecurityalliance.jp/newblog/2021/10/07/csa%e3%81%ae%e8%aa%8d%e8%a8%bc%e5%88%b6%e5%ba%a6%e3%81%ab%e3%81%a4%e3%81%84%e3%81%a6/*
  - *2020 Japan Security Summitのスライドの資料 https://www.slideshare.net/MasahiroMorozumi/ccmstarjapan-security-summit-2020*

CCAK 試験TIPs

CCAK　試験TIPs　(1)

- Study Guideを理解すれば合格できる（あくまで経験上）
  - Study Guide をすべて読みこむのは大変。以下のCCAK Questions and Answers Collectionをやりながら、Study Guide の該当箇所を理解していくのが良いと思われる。

    https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KpGiEAK
    （$99：ISACA会員、$125：非会員）

- CCM/CAIQ/STAR認証については、以下を理解しておくことが必要。
  - CCMの各ドメインの内容。最低限、各ドメインの概要。
  - CCMの構成（EXCELのカラム）
  - CAIQの概要及びCCMとの違い。
  - STAR認証の特徴（レベル1/2/3）
  - CCM V3 と CCM V4の違い
    - 変更されたドメイン名および内容
    - ガイダンスとの違い（CCMに含まれていて、ガイダンスに含まれていないもの）

CCAK　試験TIPs　(2)

- クラウド重大脅威の構成・概要を理解しておくことが必要
  - 脅威モデリングとしてCSAが用いている手法
- 継続的モニタリング、継続的監査の理解。Study Guideの内容を理解しておく
  - STAR認証の Continuous
  - DevSecOps等、自動化との絡み
- その他、一般的なセキュリティ知識の理解
  - リスク管理
  - ガバナンス、コンプライアンス

CCAKとクラウドセキュリティ

CCAKを利用したクラウドセキュリティ

CCAKの特徴

1. 対象者は、監査人だけではなく、幅広く利用できる知識
   - 特に、利用者が説明責任を果たすために必要となる評価の知識

2. CSAが提供している監査・評価ツールの知識
   - CCM/CAIQ, STAR認証、クラウド脅威分析手法、クラウド重大脅威ディープダイブなど

CCAKを利用したクラウドセキュリティ

1. 対象者は、監査人だけではなく、幅広く利用できる知識
   - クラウドセキュリティの課題
     責任共有モデル　＝　管理責任の分担　＋　**利用者説明責任**

   - 利用者が説明責任を果たすには？
     - プロバイダ、クラウドサービスの評価（デューデリジェンス）
     - 必要なこと！
       - 利用者としてクラウドリテラシーを向上
       - SIerに依存する体質からの脱却

CCAKの内容を理解することで：

- クラウドセキュリティの一般的な知識だけでなく、評価に必要となる知識を取得
  - CCSKとかは、クラウドセキュリティの一般的な知識
- 評価に必要となる様々なツールの理解、実践が可能

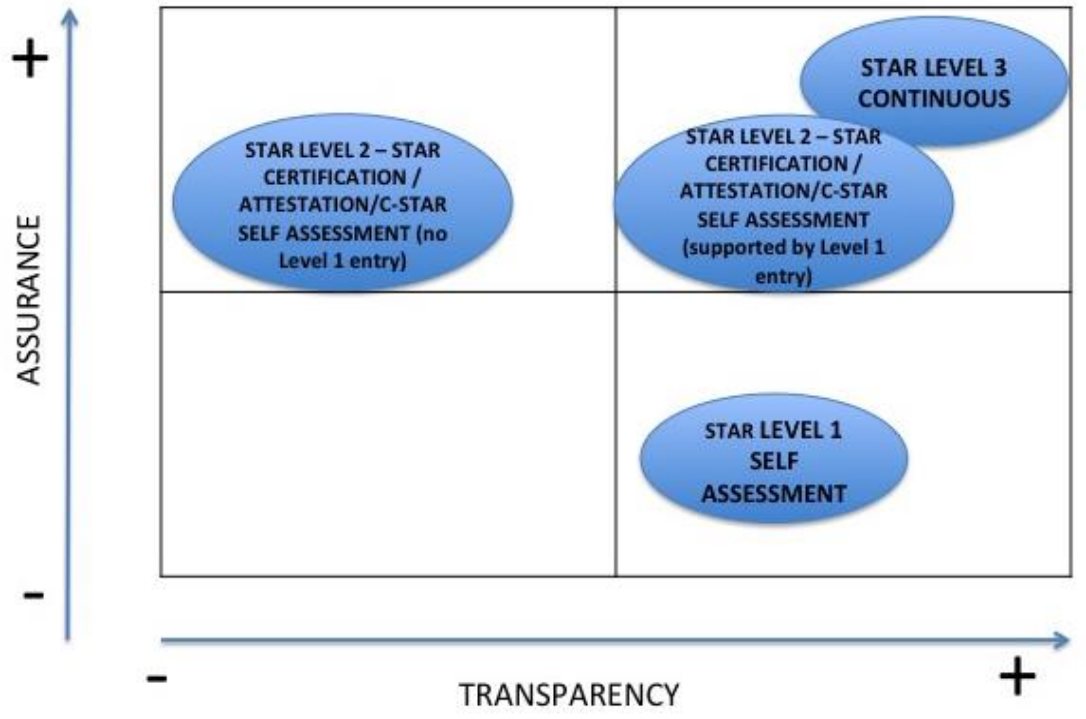
CCAKを利用したクラウドセキュリティ

2. CSAが提供している監査・評価ツールの知識
（ここではSTAR認証にフォーカス）

- 様々な標準の限界：　ISO/IEC27017、SOC2監査レポート、CSマーク、ISMAP

- 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



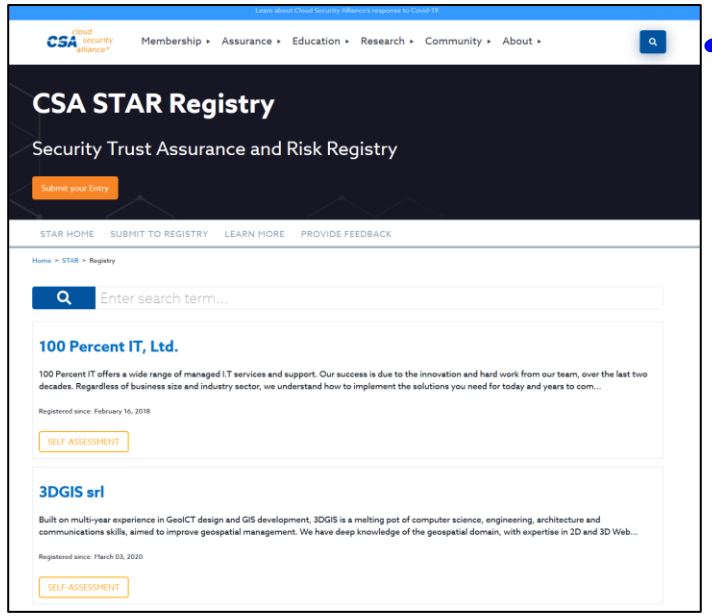
CCAKを利用したクラウドセキュリティ

2. CSAが提供している主な監査・評価ツールの知識(つづき)

- STAR Registry

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			

まとめ(1)

- CCAKは、監査人向けのクラウドセキュリティの知識というだけでなく、クラウドセキュリティ全般を理解するのに有効
- CSAが提供しているツールを、うまく活用した内容
  - CCM/CAIQ:　クラウドセキュリティの評価、要求事項の明確化
  - STAR
    - 透明性（レベル1）と信頼性（レベル2）の組み合わせ
    - 継続モニタリング、継続監査へのアプローチ（レベル3）
    - STAR Registry の有効活用
  - クラウド脅威モデリング、クラウド重大脅威、クラウド重大脅威ディープダイブ
    - クラウド脅威分析の手法として有効
- クラウドに関連する新しい分野をアドレス
  - DevSecOps, コンテナ、サーバレス等のセキュリティ

まとめ(2)

- CCAKの試験、Study Guideの日本語化の予定は未定
  - 英語でのスタディー、テストに積極的に取り組みましょう！
- CCAKのプロモーション
  - ISACA, CSAがどのようにプロモーションしていくのかを引き続き追跡中。
- 今後に向けて
  - クラウドセキュリティの推進の観点から、CCAKを広めていくことは重要と考える
    - 資格というだけではなく、クラウドセキュリティを推進していくうえでも有効

勉強会、輪講、などなど。アイデア、企画等ありましたらぜひご連絡ください！

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