6th Grand Canvas ショートトーク

クラウドセキュリティアライアンスのAIセキュリティガバナンス

日本クラウドセキュリティアライアンス
運営委員　小川隆一

2025年9月17日

Disclaimer

- 本スライドの内容はCSAジャパン運営委員である小川が手を加えています（CSAジャパンの公式見解でない部分あり）

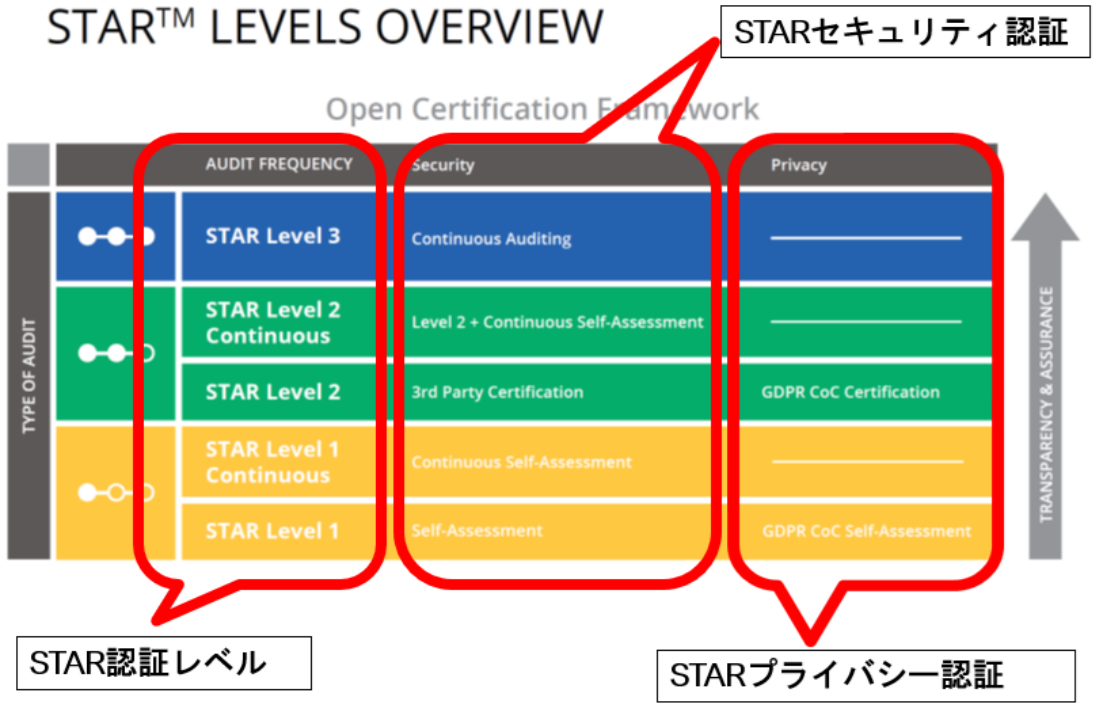
CSAジャパンのご紹介

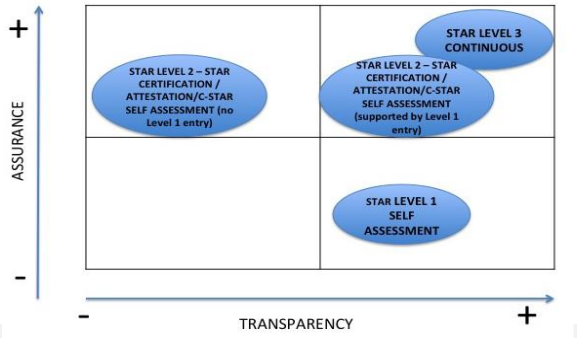
STAR（クラウドセキュリティ認証制度）

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
  - CSA STAR Attestation：　SOC2 + CCM
  - CSA STAR Certification：　ISO/IEC 27001 + CCM
  - CSA C-STAR：　GB/T + CCM
- 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
- 4000社以上のプロバイダーが登録

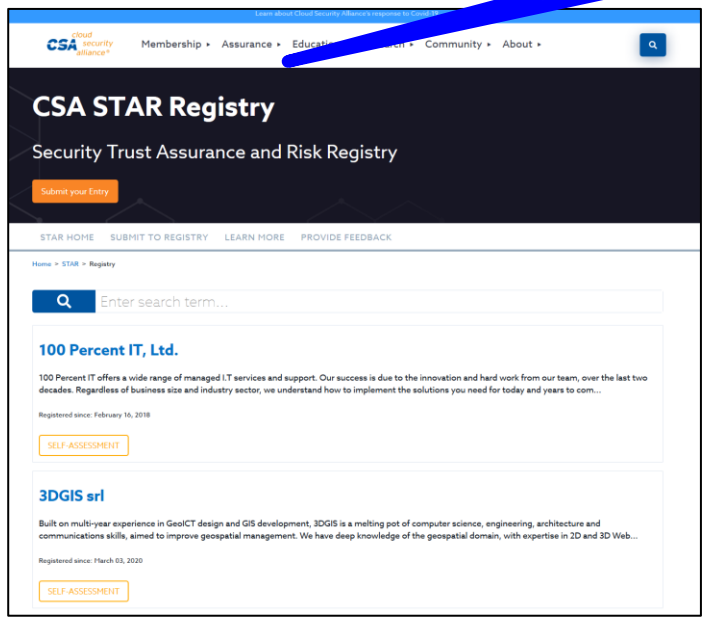




STARレベル1（セルフアセスメント）：透明性

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

CCM、CAIQ概要

国際的基準とマッピング済
- ISO/IEC 27001
- NIST SP800-53
- SOC 2
- PCI DSS
- FedRAMP

- **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
  - AIセキュリティに絡む主な特徴
    - Implementation Guidelines（CCMの実装者向けガイド）
    - Auditing Guidelines（CCMの監査者向けのガイド）
    - Scope Applicability（Mapping）（他の規格とのマッピング）
- **CAIQ（Consensus Assessment Initiative Questionnaire）**
  - 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
  - AIセキュリティに絡む特徴
    - CSP CAIQ Answer：　質問に対するCSPの評価結果（Yes/No）
    - 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（オプション）

CSAのAI関連活動

- Valid-AI-ted
- AI Controls Matrix (AICM)
- STAR for AI
- Compliance Automation Revolution (CAR)
- AI Safety Initiatives

Valid-AI-ted（2025年5月開始）

- LLMで、CAIQ評価レポートを分析
  - LLMによるCAIQ評価分析で自己評価の信頼性を向上
  - CAIQの「CSP Implementation Description」の内容をAIで評価
  - CCMの「 Implementation Guidelines 」を参照
  - 合格すると、Valid-AI-tedバッジが発行され、STAR Registryに表示

プレイヤー	Before：STAR Level1セルフアセスメント	After：Valid-AI-ted
CSP	• クラウド利用者とのチェックリストのやり取りが簡略化 • 透明性と信頼性の向上。顧客に対してセキュリティポスチャを明示 • マーケットでの競争優位性	• AIがCAIQセルフアセスメントを解析し、実装内容の適合性を自動スコア化。セルフアセスメントの質を高め、STAR Registryの信頼性を向上 • 監査前の自己チェックや改善点の特定が容易 • Valid-AI-tedバッジにより顧客への透明性・信頼性を示すことが可能
CSC	• CSPとのチェックリストのやり取りが簡略化 • CSPのセキュリティ、コンプライアンス状況を標準化されたフォーマットで比較可能 • 提供されるCAIQ情報を活用し、RFPやベンダーリスク評価の時間を短縮	• クラウドサービス選定の精度向上。AIによる解析により、従来より深いレベルでプロバイダのセキュリティ状況を可視化 • 複数プロバイダのセキュリティ強度を客観的に比較 • 実装内容の詳細が明確になり、利用者のセキュリティ検証負荷が低減
Auditor	• 評価基準の標準化。CCMとCAIQに基づく評価枠組みが明確であり、監査プロセスが効率化される • CSPが公開するセルフアセスメントや監査レポートを監査の補助資料として活用可能	• 監査の効率化。AIが事前にCAIQ記述を解析し、リスクや不備を指摘するため、監査の工数削減が可能。 • 一貫性・標準化AI評価により監査基準のばらつきが減少し、監査の客観性が向上

AI Controls Matrix (AICM)　(1)　(2025年6月開始)

- クラウドにおけるセキュアで信頼性の高いAIシステム構築のための管理策集
  - AI固有のリスクを評価し、管理
  - 信頼性の高いAIシステムを構築
  - 国際基準に準拠
- CCMと同じフレームワーク（CCMを拡張）
  - AICM固有に追加されたドメインがModel Security(MDS)
  - それ以外の17のドメインは、CCMのドメインにAICMとしての管理策が記述
  - 管理策を、AI向け（AI-Specific)、クラウド向け（Cloud-Specific)、AIとクラウド両方向け（Cloud&AI-Related）で明示

CCMのAIクラウド拡張

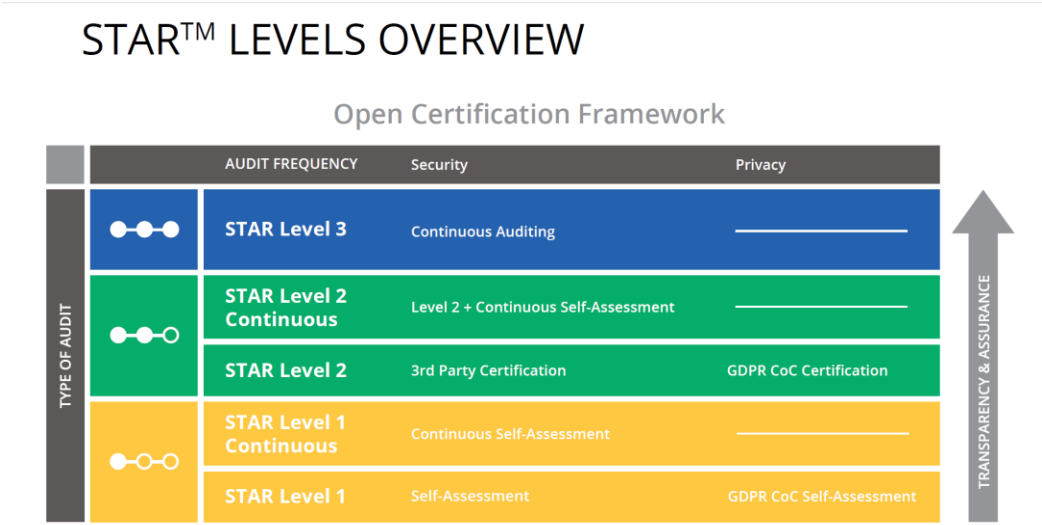
A&A	Audit & Assurance	IAM	Identity & Access Management
AIS	Application & Interface Security	IPY	Interoperability & Portability
BCR	Business Continuity Mgmt & Op Resilience	I&S	Infrastructure Security
CCC	Change Control & Configuration Management	LOG	Logging & Monitoring
CEK	Cryptography, Encryption & Key Management	MDS	Model Security
DCS	Datacenter Security	SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
DSP	Data Security & Privacy	STA	Supply Chain Mgmt, Transparency & Accountability
GRC	Governance, Risk Management & Compliance	TVM	Threat & Vulnerability Management
HRS	Human Resources Security	UEM	Universal EndPoint Management

AI Controls Matrix (AICM)　(2)

- AICMの現在の提供状況
  - 赤で囲った部分が現在提供されている部分（Mappingについては現時点でBSI AIC4とNIST AI 600-1 (2024)を提供）
  - 今後の予定
    - ISO42001とのマッピング（現在公開レビュー中）
    - Implementation Guidelines（現在公開レビュー中）
    - EU AI Actとのマッピング（作業中）
    - Auditing Guidelines（作業中）

STAR for AI
（AIを実装したクラウドのためのSTAR認証拡張）

- CSA STARの拡張によるAIとクラウド企業およびエンタープライズユーザー向け認証プログラム
- AI Controls Matrix (AICM)を使用
- 対象
  - AI企業、クラウドプロバイダ、SaaSプロバイダ、AIエンタープライズユーザー
- STARプログラムの上に、AIのためのSTARを構築
  - STARのフレームワークを活用
    - STAR for AIレベル1 – Self Assessment & Valid-AI-ted
    - STAR for AIレベル2 – 3rd Party Audit
  - 現状からのシームレスな移行
    - 4,000社以上のクラウドプロバイダーの登録実績
    - 政府、業界、企業で幅広く採用



STAR for AI

プレイヤー	メリット	課題
CSP	• AICMに基づくAI特化のSTAR認証を取得し、信頼性と透明性を顧客へ示すことが可能 • AIを安全に運用できるプロバイダとして差別化が可能 • STAR for AIのフレームワークにより、複数規制（ISO 42001、EU AI Actなど）に効率的に対応可能	• 新たなAICM準拠や第三者監査にかかるコストやリソース負担が増加か？ • 技術的成熟度不足により、AI特有のリスク管理策（モデル攻撃対策、データ品質保証など）の実装負荷が高くなるか？
CSC	• AIを活用したクラウドサービスのセキュリティレベルをSTAR for AIで確認可能 • AICM準拠したSTAR認証を比較することで、プロバイダー選定の負荷が減少 • 導入時のリスク低減が可能	• STAR for AI未登録プロバイダとの比較が困難 • AICMの技術的・専門的な内容を正しく理解するための知識が必要
Auditor	• AICMを活用することで、AIシステム監査の統一基準として利用可能 • STAR for AI認証情報を参照することで、監査の事前準備や検証作業が削減 • グローバル基準と整合が取れているため、複数規格に対応しやすい	• AICMのガイドラインやベストプラクティスが発展途上のため、評価基準の安定性に課題 • AIモデルやMLOps特有のリスクを理解するため、高度なAIセキュリティ知識が必要

Compliance Automation Revolution(CAR)

- 背景
  - コンプライアンスマネジメントがクラウドセキュリティの大きな負荷
  - 沢山のコンプライアンス要件に対して、本当の意味でのセキュリティ向上につながっていない
  - GRCユーザーの60%がいまだにスプレッドシートですべてを管理（参照：Coalfire Compliance Report 2023）
- HOW
  - AIによるコンプライアンスの自動化
    - 継続的なモニタリングアーキテクチャにより、問題をリアルタイムで検出
  - 規制・規格の取り込みと正規化された管理フレームワークのために生成AIを利用
    - AIを活用した規制の分析により、複雑な要件を理解
  - 監査分析のための生成AI
    - 自動化された管理策のテストにより、手動によるオーバーヘッドを排除
    - マシン・ツー・マシンのコンプライアンス通信を可能にする標準（OSCAL)の利用

AI関連活動のまとめ

1. 既存ガバナンスフレームワークとの連携
   - CCMを基盤とし、AI向け管理策を追加した拡張版（AICM）を展開
   - ISO 42001、NIST AI RMF、EU AI Act などの規格・法規制とのマッピング

2. STAR for AI の認証拡張
   - 従来の CSA STARプログラムをAI領域に拡張。AIサービス提供者・SaaSベンダー・エンタープライズAIユーザーの信頼性を可視化
   - AICMを活用して、AI関連サービスのセキュリティ成熟度を評価・認証

3. AIによるコンプライアンス自動化
   - Valid-AI-ted プログラム
     - AI（LLM）でCAIQ評価レポートを自動解析し、評価の精度と効率化を実現
   - Compliance Automation Revolution（CAR）
     - 生成AIを用いて、規制要件の分析・監査・テストを自動化する取り組み

最後に

ご興味の方は小川まで
CSAジャパン参加絶賛募集中
企業会員
個人会員