CCM (Cloud Control Matrix) 役割と使い方

一般社団法人　日本クラウドセキュリティアライアンス
CCMワーキンググループ

このセッションの内容

- CCM(Cloud Control Matrix)とは何かを理解する
  - CCMの位置づけと既存の規格・標準との関係
  - CCMとCSA Cloud Security Guidanceの関係
- CCMの構造を理解する
  - コントロールドメインの構成
  - マトリクス表の構成
- CCMとCAIQの使い方
  - 事業者の自己評価とユーザによる事業者評価
  - ユーザと事業者のコンセンサス
- CCMとSTAR
  - STARとそのロードマップ
  - OCF (Open Certificate Framework）
- CCM WGの活動予定
  - CCM及び関連ツールの日本語化（翻訳、レビュー）
  - 日本国内各種基準との比較、対照、補足
  - CCMピアレビューへの参加と日本からの意見フィードバック

CCMの位置づけ

クラウドユーザ・事業者のためのセキュリティガイダンス
１４の領域における、クラウドセキュリティの考え方についての解説

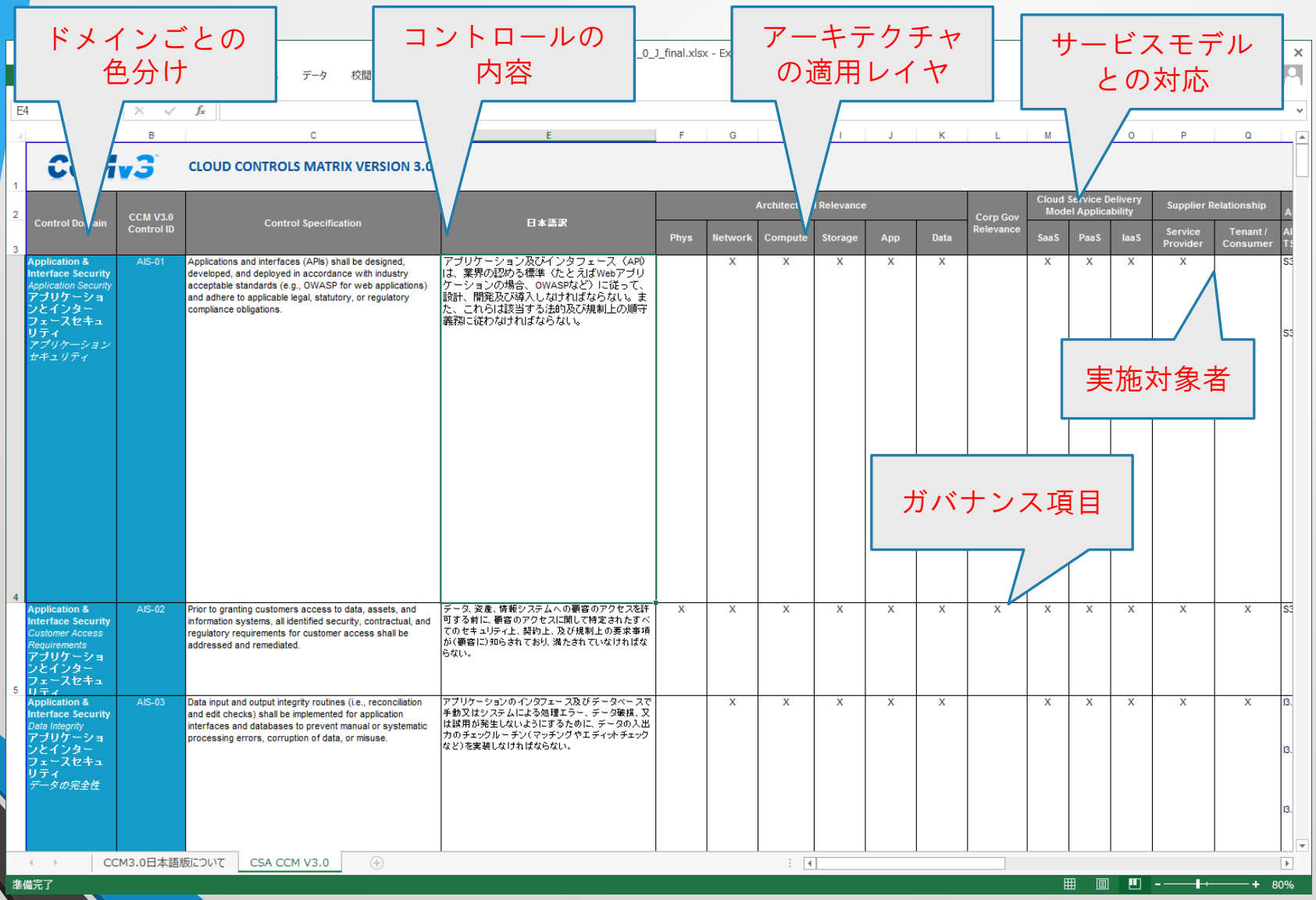
ガイダンスの14領域におけるセキュリティコントロールのフレームワーク
他の国際標準、業界標準などとの対応付けを含む
ガイダンスの実装基準的位置づけ

CCM、CAI自己評価による準拠事業者登録制度（英語版のみ）

CCMとは

- クラウドサービスに必要なコントロール（管理策・統制）とその実装方針の提示
  - 情報セキュリティ上の管理策
  - ITガバナンス上の統制項目（Ver 3から新たに導入）
- 適用対象の明示
  - 各コントロールとアーキテクチャレイヤの対応付け
  - 各コントロールと各サービスモデルの対応付け
  - 実施者（事業者、テナント、利用者）の明示
- 各種標準との対応付け
  - 既存の国際標準、業界標準、政府標準における同種コントロールとの対応付け
  - Ver3からSOC2にも対応

CCMの項目例（日本語訳版）



各種標準等との対応表

AICPA（SOC2）

COBIT（4.1）

FedRamp

HIPPA

ISMS

PCI/DSS

CSA ガイダンス

AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust Cloud Initiative	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZISM	PCI DSS v2.0
S3.10.0 S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.	I.4	G.16.3, I.3		SA-04	AI2.4		Domain 10	3.03.01. (c)	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-14	NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SC-2 NIST SP 800-53 R3 SC-4 NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18) NIST SP 800-53 R3 SC-8 NIST SP 800-53 R3 SC-8 (1) NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1) NIST SP 800-53 R3 SC-10 NIST SP 800-53 R3 SC-11 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-12 (2) -12 (5) -13 -13 (1) -14 -17 -18	1.2.6	45 CFR 164.312(e)(2)(i)	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.2 A.12.5.4 A.12.5.5 A.12.6.1 A.15.2.1	Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11	CIP-007-3 - R5.1	SC-2 SC-3 SC-4 SC-5 SC-6 SC-7 SC-8 SC-9 SC-10 SC-11 SC-12 SC-13 SC-14 SC-17 SC-18 SC-20 SC-21 SC-22 SC-23		6.5
S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.		C.2.1, C.2.3, C.2.4, C.2.6.1, H.1	10 (B) 11 (A+)	SA-01			Domain 10		NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6	-1 -2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6	1.2.2 1.2.6 6.2.1 6.2.2		A.6.2.1 A.6.2.2 A.11.1.1	Commandment #6 Commandment #7 Commandment #8		CA-1 CA-2 CA-5 CA-6		
I3.2.0 I3.3.0 I3.4.0 I3.5.0	(I3.2.0) The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies. (I3.3.0) The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. (I3.4.0) The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity	I.4	G.16.3, I.3		SA-05			Domain 10		NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-3	NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-3 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6) NIST SP 800-53 R3 SI-6 NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1) NIST SP 800-53 R3 SI-9 NIST SP 800-53 R3 SI-10 NIST SP 800-53 R3 SI-11	1.2.6	45 CFR 164.312 (c)(1) 45 CFR 164.312 (c)(2) 45 CFR 164.312(e)(2)(i)	A.10.9.2 A.10.9.3 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.6.1 A.15.2.1	Commandment #1 Commandment #9 Commandment #11	CIP-003-3 - R4.2	SI-10 SI-11 SI-2 SI-3 SI-4 SI-6 SI-7 SI-9		6.3.1 6.3.2
S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	B.1	G.8.2.0.2, G.8.2.0.3, G.12.1, G.12.4, G.12.9, G.12.10, G.16.2, G.19.2.1, G.19.3.2, G.9.4, G.17.2, G.17.3, G.17.4, G.20.1	6 (B) 26 (A+)	SA-03	DS5.11		Domain 10	3.02. (b) 3.04.03. (a)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-13	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-4 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-8	1.1.0 1.2.2 1.2.6 4.2.3 5.2.1 7.1.2 7.2.1 7.2.2 7.2.3 7.2.4 8.2.1 8.2.2 8.2.3 8.2.5		A.10.8.1 A.10.8.2 A.11.1.1 A.11.6.1 A.11.4.6 A.12.3.1 A.12.5.4 A.15.1.4	All		AC-1 AC-4 SC-1 SC-16		2.3 3.4.1 4.1 4.1.1 6.1 6.3.2a 6.5c 8.3 10.5.5 11.5

CCM3.0日本語版について　CSA CCM V3.0

CSAガイダンスとCCM

- CCMドメインは、CSAガイダンスドメインをベースにしているが、細部で異なる点に注意
  - 全般的な考え方の理解→ガイダンス
  - 要求事項、管理策→CCM／CAIQ
- CCMの対応表にはガイダンスドメインへの対応が記載されているので、要求事項の詳細は、ガイダンスを参照するとよい
  - 但し、実装時の要求事項が他の基準（たとえばFedRAMPやPCI/DSSなど詳しい実装に言及している基準）から持ち込まれているケースもある

CCMのドメイン

- Audit Assurance & Compliance
- 監査・保証とコンプライアンス
- Business Continuity Management & Operational Resilience
- 事業継続管理と運用レジリエンス
- Change Control & Configuration Management
- 変更管理と構成管理
- Data Security & Information Lifecycle Management
- データセキュリティと情報ライフサイクル管理
- Datacenter Security
- データセンタセキュリティ
- Encryption & Key Management
- 暗号化と鍵管理
- Governance and Risk Management
- ガバナンスとリスク管理
- Human Resources
- 人事
- Identity & Access Management
- アイデンティティとアクセス管理
- Infrastructure & Virtualization Security
- インフラと仮想化のセキュリティ
- Interoperability & Portability
- 相互運用性と移植容易性
- Mobile Security
- モバイルセキュリティ
- Security Incident Management, E-Discovery & Cloud Forensics
- セキュリティインシデント管理、Eディスカバリ、クラウドフォレンジックス
- Supply Chain Management, Transparency and Accountability
- サプライチェーンの管理、透明性、説明責任
- Threat and Vulnerability Management
- 脅威と脆弱性の管理

CCMの使い方

- クラウド固有の要求事項をおおまかにチェックする
  - CCM／CAIQチェックリストによるチェック
- 既存の管理策でクラウド固有の問題がカバーされているかチェックする
  - 既存の標準コントロール　→対応するCCMコントロールのチェック（CAIQチェックリスト）
- 既存標準をもとにクラウド固有の実装レベルを決める
  - 既存の標準コントロール　→対応するCCMコントロール→対応する実装基準のコントロール（例えばFedRAMP,SP800-53など）

対象規格・基準の一覧

- "AICPA TS Map"
- "AICPA Trust Service Criteria (SOC 2SM Report)"
- "BITS Shared AssessmentsAUP v5.0"
- "BITS Shared AssessmentsSIG v6.0"
- CCM V1.X
- COBIT 4.1
- CSA Enterprise Architecture / Trust Cloud Initiative
- **CSA Guidance V3.0**
- ENISA IAF
- **"FedRAMP Security Controls(Final Release, Jan 2012)--LOW IMPACT LEVEL--"**
- **"FedRAMP Security Controls(Final Release, Jan 2012)--MODERATE IMPACT LEVEL--"**
- GAPP (Aug 2009)
- HIPAA / HITECH Act
- **ISO/IEC 27001-2005**
- Jericho Forum
- NERC CIP
- **NIST SP800-53 R3**
- NZISM
- **PCI DSS v2.0**

赤字は主要な国際、業界、政府標準
下線はCCMをより詳細に実装する際
参考にできる規格（実装レベル記載）

マトリクスに記載された標準コントロールを実装する場合には、より抽象的な標準→CCM→実装基準の順に参照するといい

例：　ISO/IEC27001 → CCM → SP800-53

CAI・CAIQとは

- CCMの各コントロールの内容をブレークダウンし、チェックリスト化したものがCAIQ
- CAI(Consensus Assessment Initiative)は、CAIQを使用してユーザと事業者が相互の対応状況を確認するもの
- STAR Level1（後述）はCAIQをもとに、事業者が自己チェックを行った内容を公開する制度

CAIQ（チェック項目例）

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

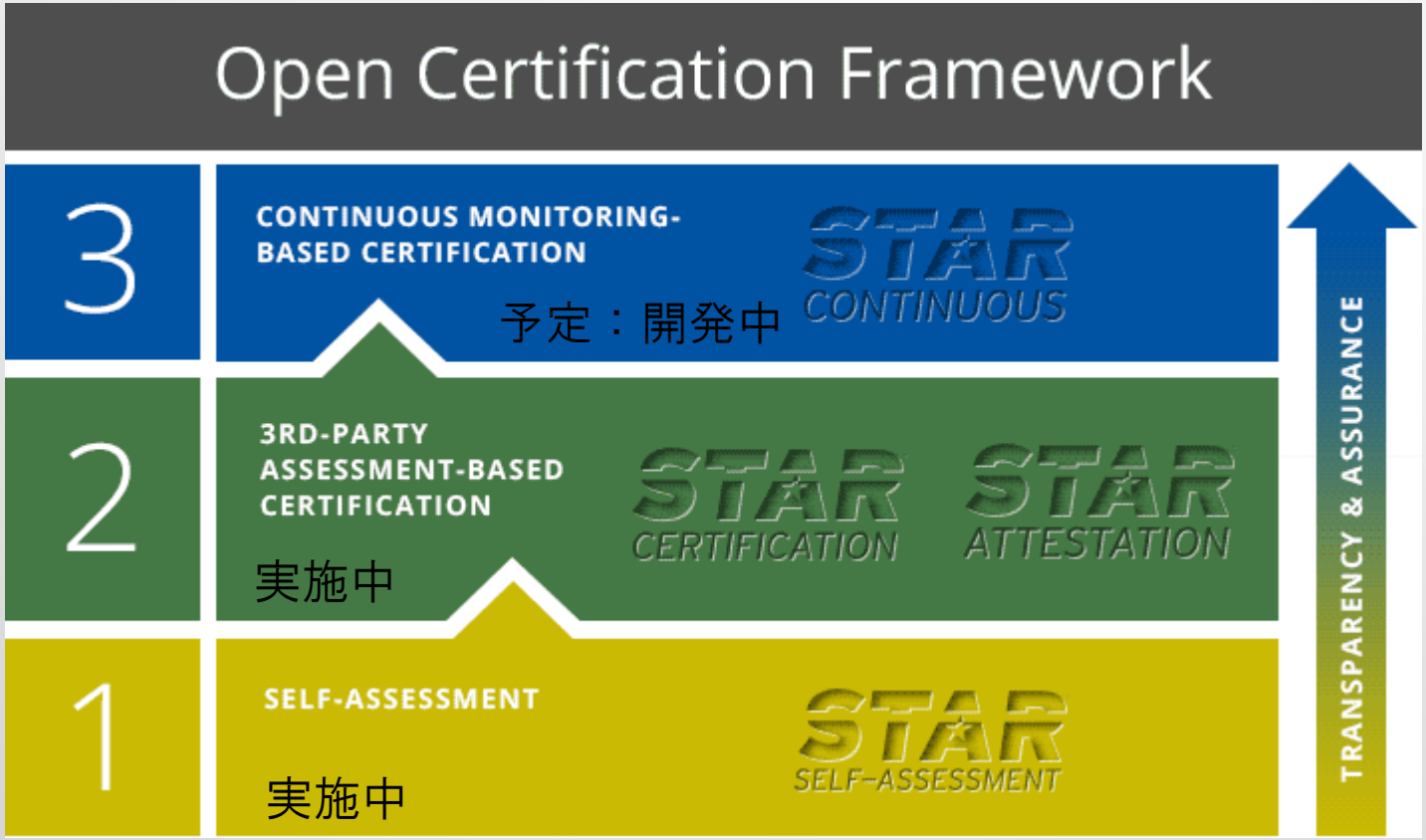
CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Proposed
Application Security	AIS-01	AIS-01.1	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you utilize industry standards (Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider	
		AIS-01.2		Do you utilize an automated source-code analysis tool to detect code	
		AIS-01.3		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development	
		AIS-01.4		Do you review your applications for security vulnerabilities and address any issues prior to deployment to	
Customer Access Requirements	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, all identified security, contractual, and regulatory requirements for customer access shall be addressed and remediated.	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	
Data Integrity	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be	Are data input and output integrity routines (i.e., reconciliation and edit	

現在、CCM WGにてVer 3.0 翻訳作業中：ボランティア募集！！

STARとは

クラウド事業者のセキュリティとガバナンスを可視化する取り組み



OCF: CSAが提唱している複数認証制度の組み合わせ、相互乗り入れを可能にするオープンな認証フレームワーク。これにより事業者は複数認証取得時の重複作業を軽減できる

STARのレベル

- STAR Level1　（自己チェック）
  - CCM/CAIQを用いた自己チェック状況を事業者が自主的に登録することで、クラウド事業者としてのセキュリティ対応状況を公開する制度　（開始済み）
- STAR Level2　（第三者による認証・監査制度）
  - ISO27001-2005 もしくはAICPA SOC2 取得事業者に対し、CCM*1等に基づく第三者評価を実施、クラウド事業者としてのセキュリティを追加認証する制度。（OCFの考え方に準拠）
- STAR Level3　（継続的モニタリング）
  - 認証取得後も、その対応状況を継続的にモニタリング*2し保証する制度。たとえば米国政府（FedRAMP）などでハイレベルの情報を扱う際に要求されており、現在、STARとしての枠組み検討が進んでいる。　（準備中）

＊1:2014/5現在、CCM v1.4 または CCM v3 のいずれか＋ISO/IEC27001-2005 または AICPA SOC2 で認証。2015/3 にCCMの部分は v3に完全移行の予定

*2:現在開発中のCTP（Cloud Trust Protocol）を使用し常時モニタリングする。 CTPは、クラウド事業者がユーザに対して準拠状況を常時開示するための プロトコル

CCMワーキンググループの活動

CSAジャパンでは、CCM ワーキンググループ（CCM WG)を行い、広く日本におけるCCMの展開を推進していくことを目的として以下の活動を行っています。

1. CCM/CAIQの日本語化、および、日本語版の監修
   - CCM3.0日本語版：　　一般公開済み
   - CAIQ3.0.1(draft)日本語版：　会員公開済み
2. CCMの日本の法令、標準、基準へのマッピング
3. CCMのガイドラインの作成
4. CCMの日本における啓発活動の実施
5. CSAグローバルのCCMに対する日本の視点に立ったピアレビューの実施およびフィードバックの提供

また、本WGの活動に参加していただける方を募集しています。募集要項等につきましては、以下のURLを参照してください。

http://www.cloudsecurityalliance.jp/ccm_wg.html