CSA STAR プログラムと
OPEN CERTIFICATION FRAMEWORK (OCF)
2016 年とその後の展望

Daniele Catteddu dcatteddu@cloudsecurityalliance.org

Jim Reavis jreavis@cloudsecurityalliance.org

Alain Pannetrat apannetrat@cloudsecurityalliance.org

日本語版の提供について

本書「**CSA STARプログラムとOPEN CERTIFICATION FRAMEWORK (OCF) 2016年とその後の展望**」は、CSAが公開している「**CSA STAR PROGRAM & OPEN CERTIFICATION FRAMEWORK IN 2016 AND BEYOND**」の日本語訳です。本書は、原文をそのまま翻訳したものです。また、本書内で参照されているURL等は、すべて英語版へのリンクとなっております。原文と日本語版の内容に相違があった場合には、原文が優先されます。また、この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。
本書は、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/STAR ワーキンググループの以下のメンバーにより作成されました。

変更履歴

日付	バージョン	変更内容
2016 年 11 月 04 日	日本語バージョン 1.0	

有田　仁
甲斐　賢
勝見　勉
最首　克也
羽田野　尚登
諸角　昌宏

なお、日本クラウドセキュリティアライアンスについては、以下の URL より参照してください。
https://cloudsecurityalliance.jp

2016 年 11 月 04 日

目次

1 はじめに

1.1 エグゼクティブサマリ

クラウドセキュリティアライアンス(CSA) のセキュリティ・信頼・保証の登録プログラム (SATR) は、クラウドセキュリティにとって業界トップの信頼指標である。CSA のオープン認証枠組み (OCF) は、CSA の業界トップのセキュリティガイダンスに従った、柔軟性のある、徐々に拡大する、マルチレイヤのクラウドサービスプロバイダ[1]認証のためのプログラムである。OCF/STAR プログラムは、ほかのセキュリティ監査や認証プログラムのリスクやコンプライアンス目標をはるかに超える、能力、実行力の柔軟性、ビジョンの完全さを備えた、グローバルなクラウドコンピューティングの保証枠組みとなっている。

OCF/STAR は以下を提供する：

信頼できるベストプラクティス – クラウドコントロールマトリクス (CCM) は、CSA による無料で自由に使ってよい、クラウドセキュリティ管理策の体系であり、世界でもっとも広く使われているクラウドセキュリティ標準である。

権威のあるリポジトリ – STAR リポジトリ[2]は、グローバルなリポジトリであり、クラウドサービスプロバイダがクラウドセキュリティのベストプラクティスの水準にあることを示すことができる。

第三者機関による評価– 評価機関に関する戦略により、各社個別の監査人の組み合わせによることなく、予め認定済みの監査機関をすぐに従事させることができる。

段階的保証レベル – エコシステムにより、自己評価とともに、成熟度評価を含む第三者評価を可能にし、様々な保証レベルを提供する。

枠組みの相互互換 – CCM とその他の標準とのマッピングや、相互認証協定やほかの取り組みを通じて、STAR/OCF は、独立して開発された数多くのセキュリティ標準や認証プログラムを組み入れることができる。

業界との結びつき – グローバルなソリューションプロバイダのコミュニティが、STAR を意識したソフトウェア製品やコンサルティングサービスを活発に開発している。

ツール – CSA のガバナンス・リスク・コンプライアンス (GRC) スタックや、CSA STAR Watch[3]アプリケーションといったツールが、クラウドに関する保証を向上させたり簡略にしたりしてくれる。

---

[1] 訳注：本書では、JIS に合わせて Cloud Service Provider をクラウドサービスプロバイダと訳すこととする。なお、今までの CSA ジャパンの文書ではクラウドサービス事業者と訳していた。

[2] https://cloudsecurityalliance.org/star/#_registry

本文書では、OCF/STAR を紹介する。クラウドセキュリティ認証に関連するいくつかの主要な問題を明らかにし、CSA が推進している直近および長期の活動を示す。

2 CSA STAR プログラムと OPEN CERTIFICATION FRAMEWORK(OCF)

2.1 背景

STAR は 2011 年に、より良い透明性と情報セキュリティ保証を提供することで、クラウド市場における信頼を改善することを目的として開始した。

STAR は、クラウドのステークホルダー -- クラウドサービスカスタマ (CSC)、クラウドサービスプロバイダ(CSP)、クラウド監査人、クラウドブローカなど -- に、クラウドサービスプロバイダが CSA の Cloud Controls Matrix (CCM)[4] や CSA の Consensus Assessment Initiative Questionnaire (CAIQ)[5] に基づいて自身のセキュリティ評価を行った情報を公表するための、公開のリポジトリを提供する。

CSA OCF ワーキンググループ (OCF WG) は、OCF/STAR をサポートする必要がある技術的な能力を開発することを目的として 2012 年に開始した。OCF WG のビジョン宣言[6] は次のとおり：

> *『CSA OCF WG は、クラウドサービスプロバイダに対するグローバルな、公認の、信頼された認証を与えるための業界としての取り組みである。OCF は、CSA の業界トップのセキュリティガイダンスとコントロール目標に従って、柔軟性のある、徐々に拡大する、マルチレイヤのクラウドサービスプロバイダを認証するためのプログラムである。本プログラムは、手間とコストの重複を避けるために、広く用いられている第三者評価および、公認会計士業界が開発した監査証明宣言と、組み合わせて使用する。*
>
> *CSA OCF が提供するものは：*
>
> *－すべての地域においてグローバルなベストプラクティスへのコンプライアンスに関する確認を行うための手段。例えば政府や産業別業界が、CSA OCF を本格的に採用することにより、GRC スタックの上にその独自の要件を付加することで、公的セクタのクラウド利用に対して手軽に素早く認証を提供できることが期待される。*

[3] https://cloudsecurityalliance.org/star/#_watch
[4] https://cloudsecurityalliance.org/group/cloud-controls-matrix/
[5] https://cloudsecurityalliance.org/group/consensus-assessments/
[6] https://cloudsecurityalliance.org/download/ocf-vision-statement/

－複数の認証の取得のためにプロバイダが GRC スタックツールを活用するための詳しいガイダンス。例えば、適用範囲定義書によって、プロバイダは CSA の Cloud Controls Matrix (CCM) を組み込んだ ISO/IEC 27001 認証のための道筋をたどることができる。

－「承認枠組み」。これにより、CSA が ISO、AICPA、その他の CSA の知財を取り入れた認証/枠組みをサポートすることが可能になる。CSA は可能な限り、一度認証されれば何度も使える (certify-once, use-often) ことをサポートする。

CSA はプロバイダの認証を協調させ簡素化することを目的としており、複雑にすることは意図していない。』

2.2 OCF の階層構造

OCF WG は、枠組み自身を定義するとともに、枠組みの中に含まれる認証スキームを定義することに取り組んだ。本 WG は、OCF を 3 つの信頼レベル[7]（図 1 を参照）をもつように定義した。

レベル 1、自己評価：STAR 自己評価（提供中）
レベル 2、第三者評価：STAR 認証、STAR 監査証明、C-STAR 評価（提供中）
レベル 3、継続的モニタリング/監査：STAR 継続型（開発中）

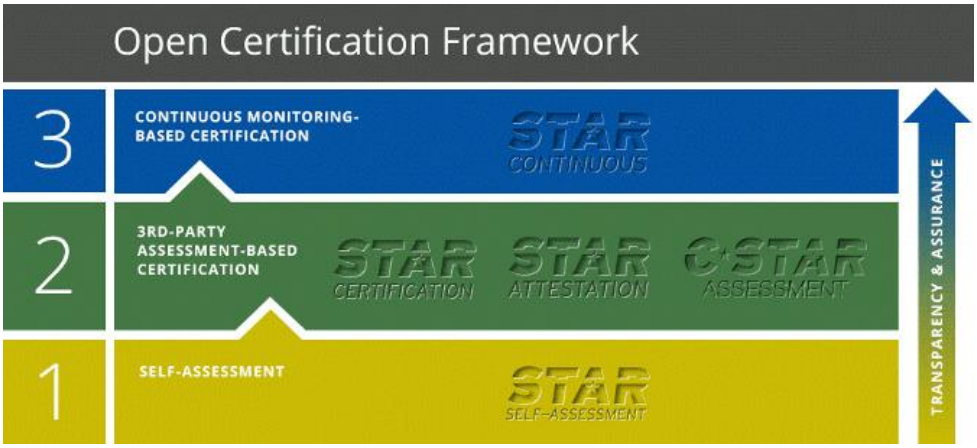

図 1[8]

2.3 OCF レベル間の関係

「保証」という観点からすると、OCF レベル 1 は低から中程度の保証を、OCF レベル 2 は高い保証を、OCF レベル 3 はとても高い保証を提供する。「透明性」という観点からすると、OCF レベル 1 は良い透明性を、OCF レベル 2 は低から高の透明性を、OCF レベル 3 はとても高い透明性を提供する（図 2 を参照）。

[7] https://cloudsecurityalliance.org/star/
[8] 訳注：OCF の 3 つの信頼レベル

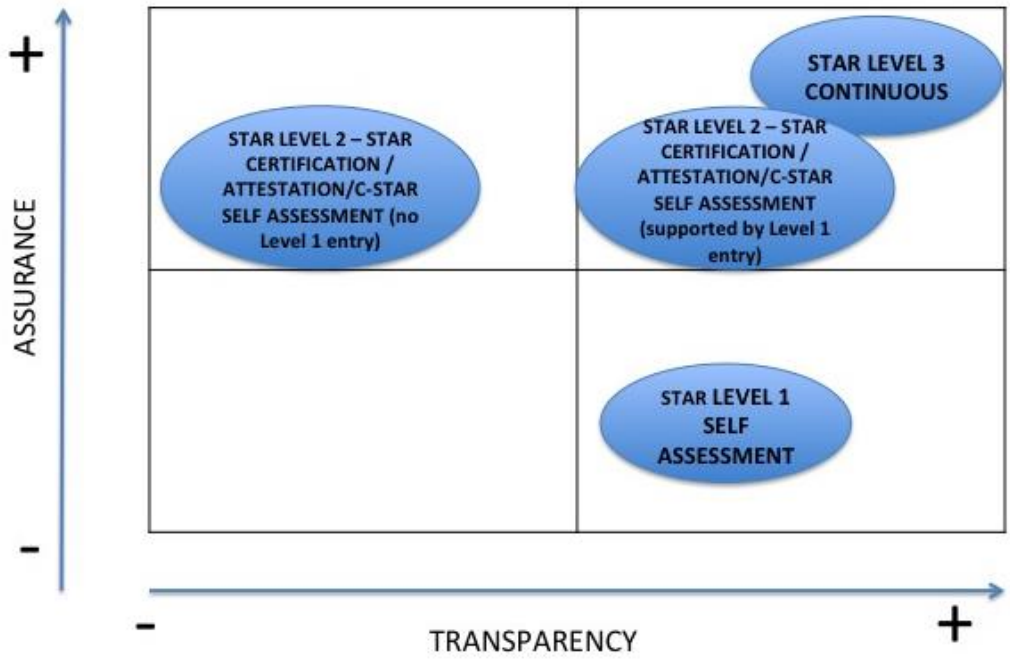

図 2[9]

3 つの OCF レベルによって提供される透明性の程度は、必ずしも 3 つの保証レベルと一致しないことに注意する必要がある。例えば、OCF レベル 1 は OCF レベル 2 よりも良い透明性を提供できる。なぜなら、STAR 認証スキームも STAR 監査証明スキームも、その組織がそのセキュリティ管理策を公開することを要求していないからである。

CSA は、OCF レベル 2 の認証を目指す組織に、最初に OCF レベル 1 の自己評価を行うことを推奨する。

3 クラウド認証：主な未達事項

3.1 枠組みの普及度合い

STAR が 2012 年に開始以来、クラウド市場は成長し成熟し、その分クラウド監査と認証の市場も成長し成熟した。

2012 年から 2015 年にかけて、数々の新しいクラウドに関連する認証枠組みが出現した。欧州ネットワーク情報セキュリティ庁 (ENISA) は、クラウド選抜産業グループ

[9] 訳注：OCF のレベル間の関係

(C-SIG) と協力し、*クラウド認証スキームリスト*[10] (CCSL) を作った。CCSL は、欧州のクラウド市場に適用できるセキュリティ認証スキームの一覧を提供する。

似た仕事が CSA もそのメンバーである CloudWATCH コンソーシアムによってなされた。*「クラウド認証のためのガイドラインと推奨事項*[11]*」*というタイトルの報告書には、クラウドコンピューティングのために現在利用可能なセキュリティ認証スキームが分析されている。15 個の事例が挙げられ、国家的、地域的あるいはグローバルな、業界特有の、クラウド特有の、および汎用的な認証スキームを含んでいる。

その間に ISO 27018:2014[12]と ISO 27017:2015[13]が公表された。本文書の執筆時点ではまだドラフト段階である[14]が、多くの早期導入者がこれらの実践規範にもとづくコンプライアンスを示すことに興味を持っている[15] [16]。

さらにいくつかの国では、自ら国家的な認証スキームを開発することを決定した。クラウドサービスを公的機関に提供するクラウドサービスプロバイダに対する認証の仕組みをつくることを目的とする。まず米国は「連邦政府によるリスクおよび認証管理プログラム [17] (FedRAMP) 」標準をつくり、つづいて英国は政府の G-Cloud[18]をつくり、さらにシンガポールは「多層クラウドセキュリティ [19] (MTCS)」 をつくった。最近ではドイツの情報セキュリティ連邦機関 [20] (BSI) とフランスのネットワーク情報セキュリティ機関 [21] (ANSSI) が、クラウドセキュリティのフランス・ドイツ共通ラベル (French-German Label) をつくることを目指すスキームを設置した。カナダ、香港、オーストラリア、イスラエル、トルコ、スロベニアを含むほかの国々は、自ら国家スキームに取り掛かっている。

これらの国家的な取り組みのすべては、国固有の要件を組み込むことで公的分野の調達プロセスを簡素化するという共通の目標を共有している。このことは理解できる一方、他方では多くの国で認証される余裕のないクラウドサービスプロバイダにとっての参入障壁をつくる。

この状況は、国家特有の認証スキームを開発するという国々の要求と、コンプライアンスコストを抑えたいクラウドサービスプロバイダの要求とを、どうやってうま

[10] https://resilience.enisa.europa.eu/cloud-computing-certification
[11]http://www.cloudwatchhub.eu/sites/default/files/CloudWATCH_Cloud_certification_guidelines_and_recommendations_March2015.pdf
[12] http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498
[13] http://www.iso.org/iso/catalogue_detail?csnumber=43757
[14] 訳注：ISO/IEC 27017:2015 は、2015 年 12 月に正式に発行されました。
[15] https://aws.amazon.com/blogs/aws/aws-certification-update-iso-27017/
[16] https://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27018
[17] http://www.fedramp.gov
[18] https://www.gov.uk/government/publications/g-cloud-security-accreditation-application
[19] https://www.ida.gov.sg/Tech-Scene-News/ICT-Standards-and-Framework/MTCS-Certification-Scheme
[20] http://www.pwc.de/de/pressemitteilungen/2015/cloud-computing-bsi-anforderungskatalog-fuer-cloud-anbieter-angekuendigt.html
[21] http://www.ssi.gouv.fr

くバランスをとるかという問題を提起する。両方とも間違いなく、顧客にとって良いことである。

3.2 より高いレベルの保証と透明性を提供する手段の不足

現在利用可能な認証スキームは、自己評価あるいは第三者評価のいずれかにもとづいている。それらは「ある時点 (point-in-time)」と「ある期間 (period-of-time)」を対象とするアプローチに依存する。前者のアプローチでは、監査人は、与えられたセキュリティコントロール目標が特定の時点（例えば今日）で満たされることを確認する。この例は、ISO 27001 や CSA STAR 認証である。後者のアプローチでは、監査人は、ある期間（たとえば過去 12 ヶ月）を通じてコントロールが効果的であることを観察する。この例は、SSAE16[22] SOC2 Type2 や CSA STAR 監査証明である。

いずれのアプローチも一般的に「十分に良い (good enough)」と見なされる一方、いずれのアプローチも、高リスクなプロファイルをもつクラウドのステークホルダー（例えば金融、医療、政府などの重要分野を運営する組織）が要求する高い保証や高い透明性を提供しない。例えば、金融分野では、CSA が ENISA のために作成した*「金融分野のクラウドコンピューティングの安全な利用*[23]*」*というレポートに書いてあるように、金融の規制には、クラウドサービスプロバイダが提供するセキュリティについての十分な証拠を提供するために透明性を改善すべきという相当の圧力がある。金融の監督当局は「ある時点」と「ある期間」の証明はコンプライアンスを示すための条件としては必要ではあるが不十分である、と考えている。そのため金融の監督当局は金融機関に対し、既存の認証を超えたガバナンス・リスク・コンプライアンス (GRC) ソリューションを採用することを求めている。

3.3 限定的な範囲：プライバシーは十分に考慮されていない

クラウドセキュリティの認証スキームにいろいろあるのと同様に、プライバシーのシール/認証も数多く提供されている。2014 年に欧州委員会が公表した、*「EU プライバシーシールプロジェクト：ポリシー選択肢の提案と評価*[24]*」*、という研究報告は、25 個のプライバシーに関連するシールスキームを調査し、一般データ保護規則 (GDPR) のプライバシー証明に関する必須要件を満たすかどうかを評価した。本報告は「プライバシー証明スキームは、複雑な振る舞いと標準に関する確定的な評価結果を出すことと、それらの結果を迅速に、透明性と利用可能性を確保して作成し、それらを保証された形で伝達する、という点で問題がある」と結論づけた。

---

[22] 訳注：米国保証業務基準

[23] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/cloud-in-finance

[24] https://ec.europa.eu/jrc/en/publication/eu-privacy-seals-project-proposals-and-evaluation-policy-options-final-report-study-deliverable-44

さらに本報告は「プライバシーとデータ保護に関する法の順守は、組織にとって課題である。一般データ保護規則 (GDPR) は、プライバシーとデータ保護に関して高度の法的基準を押し付ける。分析された EU 各国の認証スキームは提案された GDPR 要件にできるだけ近づこうとしている一方、それらのスキームがその標準や基準として GDPR 要件を具体的に組み込む方法について有効なガイドを提供できないならば、それらの認証スキームは機能不足に陥るかもしれない」と指摘している。

プライバシーを確保するための仕組みの必要性はまた、欧州のプロジェクト CIRRUS からの報告書*「クラウドセキュリティにおけるクラウド認証、国際化、標準化に関するグリーンペーパ」*[25]でも強調されている。

その記述によれば、2015 年 10 月に欧州司法裁判所は、欧州セーフハーバー協定が無効であり、十分な欧州市民のプライバシー保護を提供できないことを判示した。[26] セーフハーバーは、欧州と米国の間で 2000 年に締結された、本質的に自己認証のプログラムであって、米国の企業がプライバシーの 7 原則を遵守していることを自己認証する仕組みであった。[27]

1. **通知** – 組織は個人に、個人に関する情報を収集し利用する目的、もし質問や苦情があるときの組織への連絡方法、組織が情報を開示する第三者のタイプ、個人に関する情報の利用と開示を制限するために組織が個人に提供する選択肢と手段、を通知しなければならない。
2. **選択** – 組織は個人に、個人情報の(a)第三者への開示、(b) オリジナルに収集された目的またはその後本人が承認した目的以外の目的への使用についての選択(opt out)する機会を提供しなければならない。
3. **二次転送** – 第三者に情報を開示するために、組織は通知と選択の原則 (the Notice and Choice Principles) を適用しなければならない。
4. **セキュリティ** – 個人情報を作成し、維持し、使用し、広める組織は、個人情報を損失、誤使用および不正アクセス、開示、改ざん、破壊から保護するための合理的な予防措置を講じなければならない。
5. **データの完全性** –「原則」の一貫性：個人情報は、それが使われるための目的に関連したものでなければならない。
6. **アクセス** – 個人は、組織が保有する自身に関する個人情報にアクセスでき、情報が不正確な場合には訂正、修正、削除できるようにしなければならない。
7. **強制** –プライバシー保護が有効であるために、「原則」への遵守を保証する機構と、「原則」違反により影響を受けるデータ主体の個人に対する救済措置と、「原則」が守られない時の組織の責任を、含めなければならない。

2016年2月に欧州と米国は、欧州米国プライバシーシールド[28]と呼ばれる、大西洋をまたぐデータフローのための新たな枠組みに合意した。新しい取り決めは、本書執

[25] http://www.cirrus-project.eu/content/draft-version-cirrus-green-paper-cloud-security
[26] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf
[27] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML
[28] http://europa.eu/rapid/press-release_IP-16-216_en.htm

筆時点ではまだドラフト段階[29]だが、以下の新しい要素を盛り込むことになる：

- **欧州人の個人データを扱う企業が負う大きな義務と厳重な法的強制力**：欧州からの個人データを輸入したい米国企業は、いかにして個人データを処理し個人の権利を保証するかについての厳しい義務にコミットする必要があるだろう。企業がコミットメントを公表し、それを商務省が監視する。そのことにより、米国法のもとで米国連邦取引委員会（FTC）が執行（強制）できるようになる。加えて、欧州からの人材に関するデータを取り扱ういかなる企業も、欧州のDPA（Data Protection Authority）による決定に従うことを確約しなければならない。
- **米国政府によるアクセスに関する明確な保護策と透明性の責任**：米国は初めてEUに対して明文の保証を与え、法執行や国家安全保障のための公的機関によるアクセスに対して、明確な制限、保護、監督の仕組みの下に置かれることを認めた。これらの特例は、必要かつ適切な範囲でのみ使用されなければならない。米国は、新しい協定のもとで米国に転送される個人データに関して、無差別な、大規模の調査を行う規則を定めた。協定が機能していることを定期的に監視するために、国家安全保障のためのアクセスの問題も含め、年に1回の共同監査が行われることになる。欧州委員会と米国商務省が監査を指揮し、米国と欧州のデータ保護機関から、国家諜報活動の専門家も招聘される。
- **個別救済手段によるEU市民の権利の有効な保護**：新しい協定のもとでは、自分の個人データが誤使用されたと考えるすべての個人に対して、個別救済手段が提供される。企業は、苦情に対する応対の期限を切られる。欧州のDPAは、苦情を商務省や連邦取引委員会に提起することができる。加えて、裁判外紛争解決手段（ADR）は、無償で利用できる。国家情報機関によるアクセスが疑われる苦情については、新しいオンブズパーソン制度が導入される見込みである。

3.4 透明性の限界

クラウドサービスプロバイダの運用の透明性の欠如は、クラウド利用に際しての主たる障害として存続している。これは、クラウドサービスカスタマ[30]にとって、経済的利点と引き換えに、管理に多くを割く必要があることによる。

クラウド市場が成熟するのに伴い、クラウドサービスプロバイダはセキュリティコンプライアンスにより一層関心を払うようになってきている。にも拘らず、サービスの提供プロセスに関してのコンプライアンスの開示は、必ずしも透明性の提供に結びついていない。

クラウドサービスカスタマがプライバシーと金融関係の規制上の義務に対応した説明責任を負う状況では、そのような透明性の欠如は障害となる。上述のように、金

[29] 訳注：　欧州米国プライバシーシールドは、2016 年 2 月に正式に合意されました。
[30] 訳注：本書では、JIS に合わせて Cloud Service Customer をクラウドサービスカスタマと訳すこととする。なお、今までの CSA ジャパンの文書ではクラウドサービス利用者と訳していた。

融規制当局は金融機関に対して、適正なリスク評価の一環として、クラウドサービスプロバイダの運用の可視化を高いレベルで確保するよう要求している。STAR 認証や STAR 監査証明でさえ、必ずしも要求通りの透明性を提供できるとは限らない。先述の CloudWATCH コンソーシアムによるレポートは、以下のことを推奨している：

> *「購買手続きに、透明性に関する要求を加えること。クラウドサービスカスタマ、特に公的部門は、透明性をしっかりもたらすような認証・証明を持つことが有利になるようなクラウド選定手続きを採用することを推奨する。購買責任者にとって、認証における評価が拠り所とする技術基準の細部にわたって可視性を確保することが、とりわけ重要である。どのような技術的管理策が基準に含まれているか知っていることは、その技術的枠組みおよびその準拠する認証の仕組みが、その組織が必要とするコンプライアンスと技術的要求を満たすに足るかを判断する唯一の手段であるからである。さらに、評価・監査の品質に関して、重要性の尺度を適用すべきである。このことは特に公的部門の購買部署に推奨される。なぜならば、これら部署は特定の特性およびサービスを要求するに際して、交渉力の源泉が必要だからである。」*

また更に以下を推奨している:

> *「情報セキュリティを達成するに際して、適切な詳細レベルを設定するべきである。クラウドサービスプロバイダは、その情報セキュリティの実現に関して、より一層の透明性を実現することを推奨する。評価報告書には機密性のある情報が含まれることがあることを理解しているので、完全な開示を要求するわけではないが、それでも、クラウドサービスプロバイダは認証評価報告書の記載内容について、可能な限り開示するようにするべきである。」*

3.5 GRC を効率的に実現する手段の欠如

コンプライアンスがクラウドサービスプロバイダにとってコスト増要因となってきているのと同様に、クラウドサービスカスタマにとってもコスト増要因となってきている。その一つの要因は、国ごとの、また分野ごとの基準や認証が増えてきていることである。もう一つの要素は、実際の評価及び再評価のコストである。クラウドサービスプロバイダも、クラウドサービスカスタマも、そしてクラウド監査人も、皆簡素化の手段を望んでおり、できれば、監査に関連する情報の収集の自動化を期待している。

さらに、クラウドサービスカスタマは、（今や何千にも達する）クラウドサービスプロバイダからの様々なオファーを対照し比較する低コストのツールを必要としている。そのツールは、セキュリティ SLA、トラストレベル、透明性のレベル、その他の保証などについて、項目ごとに比較が可能なものでなければならない。クラウド

アクセスセキュリティブローカー(CASB)[31][32][33][34][35][36][37][38][39]の世界では比較ツールもあるが、どんなツールも実際の証拠に基づく比較は提供していない。

4 ソリューション： CSA の OCF/STAR プログラム

4.1 OCF のビジョン

CSA が持つ OCF のビジョンは、クラウドの関係者から寄せられる複雑な保証と透明性の要求に対して、クラウドのコミュニティ向けに GRC のソリューションを提供することである。

OCF の複数レイヤーの認証スキームの背後にある想定は、低または中レベルのリスク状態にある組織は、自己評価ベースの認証を活用してセキュリティ保証要件を満たすことができる一方、高いリスクにさらされている組織は、第三者評価ベースの認証や継続的モニタリングベースの認証を要求できることにある。

ビジョンを示した文書である「GRC スタック研究スポンサーシップ[40]」では、CSA は「認定スキーム」「すべての地域で信頼できる世界水準の実践規範に基づくコンプライアンス問題解決の道筋」を提案し、「各国政府が、独自の要求を GRC スタックの上に重層することで、公的部門のクラウド利用のための柔軟な認証の仕組みを提供することを期待している。」

4.2 相互認証スキーム：CCM と OCF/STAR を参照標準に

CCM は最も広く利用されているクラウドセキュリティ管理策の枠組みである。世界中のクラウドサービスカスタマ、クラウドサービスプロバイダ、政府機関、規制当局、監査機関が利用している。

CCM はそのまま使うこともできるし、利用組織のニーズに合わせてカスタム化することもできる。組織のリスク状態によって、適用する管理策の数を簡素化・削減したり、拡大することでカスタム化可能である。

CCM はまた、上述したような国ごとのクラウドセキュリティ認証・認定に活用することもできる。

---

[31] https://www.skyhighnetworks.com/cloud-access-security-broker/
[32] https://www.netskope.com/only-netskope/
[33] https://www.cloudlock.com
[34] https://www.elastica.net
[35] http://www.ciphercloud.com
[36] https://palerra.com
[37] https://www.cloudpassage.com
[38] http://www.bitglass.com
[39] https://www.bitsighttech.com
[40] https://downloads.cloudsecurityalliance.org/membership/sponsorship/GRC-Stack_Sponsorship.pdf

認証スキームを広めるために、CSA は以下の二つのことを提案したい：

1. **CCM をセキュリティ管理策の標準化指標として活用する**： CCM は数多くの国単位、分野単位の基準へのマッピングを提供している。現状の CCM は、他の基準の要件の殆どに適合し、一部はそれを超えるものであることが示されている。今後も CCM は進化し、さらに多くの基準へのマッピングを提供していく。
2. **OCF/STAR を国際的相互認証枠組みとして活用する**： OCF/STAR は国ごと、地域ごと、分野ごとの認証を調整する経路を提供し、クラウドサービスプロバイダに、すでに実施した監査結果を活用する道を与えている。OCF レベル 2 が用いている認証・認定スキームはまさにその実例であり、企業は ISO27001[41]取得のためにつぎ込んだ労力を STAR 認証の取得に活かすことができる。同様に他の様々な枠組みにも応用できる。

4.3 STAR 継続型：継続的モニタリングに基づく認証枠組み

前述のように、高リスクを抱えるクラウド関係者は、高い保証と高い透明性を提供できる認証スキームを求めている。今日、それはまだ市場に存在していない。

このニーズに応える最善の道は、現状の仕組みの限界を打破する、継続的モニタリング・監査を通じてである。そのような継続型の仕組みは、以下のことが必要である：

- どんな時点においても、適切なセキュリティ管理策が実施されていることを保証すること
- 管理策が機能していることを自動的に確認できるようにすること
- 管理策の可視化を可能にすること

CSA が提供する STAR 継続型はこのニーズを満たし、さらにそれを超えるものである。それに加えて、全体像から見たときに不十分な現状の実施対策に追加で適用することができるものである。AWS[42]、マイクロソフト[43]、セールスフォース[44]、グーグル[45]は各社とも Web ポータルを開設し、クラウドサービスカスタマにサービスの指標に関するいくつかの情報を提供している。第三者のサービス（例：CloudScreener）もあり、独立のベンチマーキングと各社の比較のサービスを提供している。しかしこれらすべてが同じ悩みを抱えている。最も基本的な可用性や実行性能といった指標以上に可視化できるものが極めて限られていることである。

CSA は、セキュリティに関する継続的モニタリングの仕組みを実装するのに必要なコンポーネントの開発を開始した。

---

[41] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[42] http://status.aws.amazon.com/
[43] http://azure.microsoft.com/en-us/status/
[44] https://trust.salesforce.com/trust/status/
[45] https://cloud.google.com/monitoring/api

4.4 継続的モニタリング／監査の対象者

クラウドサービスプロバイダとプライベートクラウドサービスプロバイダは、以下の目的で継続的モニタリング／監査ベースの認証を用いるのが賢明である：

- GRC へのアプローチの支援
- クラウドサービスカスタマと監督機関（データ保護機関、国の金融監督機関等）に対する、クラウド環境における情報セキュリティへのアプローチの有効性および効率性に関する、独立の立場から評価した情報の提供
- クラウドサービスカスタマへの、適用すべきセキュリティ管理策の実施に関する詳細で標準化された最新情報の提供による支援

監督機関は多くの場合、第三者認証（例えば STAR 認証、STAR 監査証明、ISO 27001、SSAE16 SOC 2）を、適用される法規制上の要求条件への準拠性を保証するのに必要だが十分でないと考えている。監督機関は、とりわけ金融部門においては、クラウドサービスカスタマに対し、セキュリティ管理策の実施状況に関する十分に詳細な最新の情報と証拠について、クラウドサービスプロバイダから取得することを求める。

4.5 STAR プログラムへの PLA (Privacy Level Agreement)行動規範の組み入れ

プライバシーレベルの保証(PLA)は、クラウドサービスプロバイダが提供するデータ保護レベルを利用者および将来の利用者に伝達するための、透明で有効な方法である。サービスレベルの保証(SLA)がサービスの提供状態について測定基準とその他の情報を提供するのに対して、PLA は情報のプライバシーと個人データ保護への取り組みを対象とする。

PLA は、国境を越えるデータフローが問題になる際にとりわけ有用となる。それらはクラウドサービスプロバイダに対し、プライバシーの遵守を強力に主張する国々や EU などの加盟国の域内で行われる、個人データ保護法令に基づく義務の順守のための手引きを提供してくれる。

PLA に必要な共通の構造あるいは枠組みを用いることは、強力な国際標準の開発につながる。その支援のために、CSA は PLA の行動規範（PLA CoC）を開発中である。

4.6 PLA の行動規範（CoC）

CSA の PLA の行動規範（CoC）は、PLA の実施規範(Code of Practice)に基づく自発的な行動規範となる。それに忠実であることは、PLA に関係するサービスが関連するすべてのプライバシー法令に準拠するという、合理的な期待感を提供することになる。

PLA の実施規範（以下、「PLA」という）は、クラウド環境におけるデータ保護法令の遵守に必要な要件一式を定義するという目的を持つ。それは CSA の「*Privacy Level Agreement Outline Version 2*」に基づくものとなる。[46]

PLA の行動規範の遵守のためのポリシー、仕組み、及び手順は、PLA CoC 認証スキームにより定義される。同スキームは以下を含む：

- 認証の範囲と対象
- 監査の規則と仕組み
- 監査人の資格付与手続き
- 認証取消と異議取り扱いの仕組みのための条件
- 認証費用

4.7 PLA CoC の認証スキーム：OCF／STAR プログラムへの統合

PLA CoC 認証は、PLA CoC への準拠を認証するための対象、範囲、規則、要件及び手順を定義するスキームである。

PLA CoC の認証は 2 つのレベルの保証、すなわち自己評価及び第三者評価により構成される。

PLA の自己評価では、PLA に対して独立した第三者による評価を受けるものではない。当該組織はプライバシー管理策に関する独自の内部評価に誠実に取り組み、しかるのちに STAR Registry への登録のため CSA に提出することになる。

PLA 認証では、認定を受けた第三者機関によるところの、当該組織のプライバシー管理策に関する評価に基づくことになる。

4.8 OCF レベル間の関係性の変更の可能性

OCF WG は、OCF Level 1 が OCF Level 2 の必要前提条件となること、また OCF Level 2 が OCF Level 3 の必要前提条件となることを、組織に対して要求する可能性を検討している。

CSA は、少なくとも STAR Registry を用いて、Level 1 と Level 2 を両方達成した組織を明示できるようにし、できれば特別のシールを導入することを考えている。

4.9 CSA STARWATCH の機能

CSA STARWatch は、ビジネスと技術のギャップを橋渡しするウェブベースのクラウド GRC 管理ツールである。組織が全社的なクラウドセキュリティポリシーの策定と

[46] https://cloudsecurityalliance.org/download/privacy-level-agreement-version-2/

実施を管理するのに役立つように開発されている。STARWatch は CSA の国際的に認知された CCM/CAIQ の取り組みに基づいている。CCM/CAIQ は有用な内容とマッピングを提供することで、いかなる組織でもそのセキュリティポリシーと手順をモニタリングするだけでなく、さらにカスタマイズすることも可能にする。組織のクラウドセキュリティへの取り組みに関して、クラウドの専門家と監査人を強く結びつけるのを手助けするナレッジ管理ポータルとして、STARWatch を使うことができる。

CSA STARWatch ツールは、CAIQ 及び CCM の各項目に対する監査情報の収集を整合化する方法を提供する。以下の機能が追加されると想定される：

- クラウドサービスカスタマの要求事項の収集の自動化
- 監査情報の収集を効率化し頻度を高めるための CloudAudit[47]の導入
- クラウドサービスカスタマのリスクプロファイルの作成
- クラウドサービスカスタマの要求事項とリスクプロファイルの、適合するクラウドサービスへのマッピング
- SLA の測定に役立つ測定基準の提供
- CCM 管理策と PLA の要件の、SLO やプロパティに対するマッピング
- 設定された要求事項とリスクプロファイルに基づくサービスの比較
- Cloud for Europe プロジェクトが開発した Federated Certified Brokerage Platform の活用[48]

[47] http:/cloudaudit.org/
[48] http://www.cloudforeurope.eu

5 附属書１：継続的モニタリングと継続的監査

継続的モニタリングとは

継続的モニタリングというコンセプトは、情報セキュリティ評価や監査の領域においては決して新しいものではない。例えば、NIST Special Publication 800-137[49]は「情報セキュリティの継続的モニタリング(ISCM)」を「組織のリスクマネジメントにおける意思決定を支援する、情報セキュリティ、脆弱性及び脅威に対する継続的意識を維持すること」と定義している。FedRAMP や PCI-DSS にも、継続的モニタリングへの言及がある。

NIST SP 800-37 Rev 1[50] では以下のように説明している：

> *「効果的な組織全体にわたる継続的モニタリングプログラムは以下を含む:*
>
> - *組織の情報システムの構成管理とコントロールプロセス*
> - *組織の情報システムと運用環境において予定された、あるいは実施された変更によるセキュリティ上の影響分析*
> - *組織的に定義された継続的なモニタリングの戦略に基づいて選択されたセキュリティ管理策（システム固有の、共有の、またはハイブリッドのものを含む）の評価*
> - *適切な組織職員に対するセキュリティ状態の報告*
> - *情報システムに関連するセキュリティリスクの継続的管理への権限ある職員の積極的関与*

CSA は、継続的モニタリングに「情報セキュリティやプライバシー保護に関連する、コンピュータによって読み取り可能な検証済みかつ最新の情報の、自動化された収集」というさらなる定義を与えることを提案している。

「検証済の情報」というのは、人間（例：評価や監査）によって、あるいはコンピュータ（例：監査証跡やイベントレポート）によって収集されたデータが有効であると確認されていることを指している。

「自動化された収集」という意味は、自動化された手段によってデータが収集されていることを指している。収集は、人間の活動（例：結論の導出）やコンピュータによる検知（例：センサー出力の検知）などによって得られる。

---

[49] http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf
[50] http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

「最新の」という意味は、データが適切な時間間隔で収集されていることを指している。時間間隔は、時間、日、週など、適時にアクションを取ることが可能な時間である。収集はリアルタイムである場合もありえる。

継続的監査とは

継続的モニタリングと同様に、「継続的監査」も、情報セキュリティの領域では新しくも特別でもないコンセプトである。

例えば、金融セクタにおいては、継続的監査は、管理策とリスクの評価のような監査作業を頻繁に実施するための自動化された方法として、広く使われている。

CSA は、継続的監査を、情報セキュリティとプライバシーの保護に関連した、コンピュータや人間によって読み取り可能な最新化された情報の自動化された収集である、と定義する。

「継続的監査」と「継続的モニタリング」の違いには注意が必要である。前者は、監査上の事実判定の（可能であれば証拠も）収集を行うが、後者はその事実判定が正しいという継続的な検証を提供している。

モニタリングと監査の対象とは

理論的には、継続的モニタリングや継続的監査は単純であるが、実務的にはそれは課題である（データが、サーバの可用性や通信のスループットのような複雑でない事項にのみ関連しているのでない限り）。セキュリティやプライバシーの領域では、継続的モニタリングの概念は、高レベルの統制目標や低レベルの対象（例：SLO やパフォーマンス指標、セキュリティ状態）に適用される。

STAR 継続型の文脈では、SLO に関連する統制目標（例：CCM の管理策）やセキュリティ指標の双方をモニタリングすることが必要である。異なるアプローチが、モニタリングと監査のそれぞれの目的に応じて検討されることになる。

セキュリティ SLO と CCM による統制には、強い相互関係がある。ISO 19086-1[51]や ISO19086-4[52]、EC C-SIG SLA 標準化ガイドライン[53]に含まれる、CSA によって提唱されたセキュリティ SLO は、CCM の管理策から直接に導かれたものである。

統制目標のモニタリング対セキュリティ指標のモニタリング

[51] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67545
[52] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68242
[53] https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

本来、CCM や ISO27002 のような管理のフレームワークにおいて提唱されている統制目標とは、コンプライアンス、ガバナンス、技術の要素の組み合わせである。従って、幾つかの統制目標は、継続的手法はもちろん、短期時間軸における自動化された手段によっては評価できない要素を含んでいる。例えば、CCM の統制目的は「文書化された手続」や「適用される法的義務」、あるいは「フォレンジック調査機能のサポート」のような包括的な機能的要件を含んでいる。これらの要素は、人間による評価を必要とし、自動化されたプロセスでは、その最新の実装をモニタリングすることはできない。

統制目標を詳細な仕組みとポリシーとして具体化したものである管理策は、継続的モニタリングにおいてうまく利用することができる。しかし、多くのコントロールは、人間による評価を必要とする要素を含む。

高度に自動化されたモニタリングや監査においては、モニタリングや監査し得るものは、しばしば、ある統制の個別ばらばらの特性であったり、統制が失敗したことを示す特性であったりする。

特定のケースでは、ある管理策の存在や有効性が、他の類似の管理策やセキュリティ指標によって推測される場合がある。例えば、文書化されたバックアップポリシーを要求する管理策を設定して、目標復旧時点(RPO)に沿った復旧の月次テストを定めることもある。ポリシーを記載した文書が最新であることや技術的バックアップの仕組みがポリシーに添っていることは、自動化された手段によってはモニタリングできないが、復旧頻度や成功率、シミュレーションで実際に復旧できた復帰点(RPA)を自動化された方法でモニタリングし、それを RPO と比較することで、管理策を支援する技術的仕組みが正確に導入され機能していると判断することができる。

継続的モニタリングは、それが対象とする領域の性格上、セキュリティ指標の考え方により良く当てはまる。セキュリティ指標には、例えば、月次の稼働時間、転送・保存データの暗号化、キー長、インシデント対応時間、データ消去品質、国レベルのアンカリング（データ保存場所）などがある。

すべてのセキュリティ指標が、測定標準に副った値によって示されるわけではない。ある指標は、記述的（例：場所）であり、あるものは計算的（例：稼働時間）であり、あるものは予測的（例：エントロピー）であり、また他のものは説明的（例：月次稼働時間は、月次の可用性と相関する）になる。

継続的モニタリングは、常に管理策に直接的に適用されるわけではなく、統制目標についてはさらに適用される可能性が低い。むしろ、継続的モニタリングは、私たちが指標として参照するよりシンプルな属性に適用される。継続的モニタリングの業務範囲においては、セキュリティ指標をモニタリングするが、モニタリングそのものはパフォーマンスのような他の指標にも適用できることは明らかである。セキュリティ指標のモニタリングは、管理策や要求事項の状態について間接的ながら有効な指標を提供する。

継続的監査は、管理策や統制目標、セキュリティ指標に対してより良く適用できるものであると言える。

6 附属書 2：CLOUDAUDIT 及び CLOUD TRUST PROTOCOL

CloudAudit 及び Cloud Trust Protocol（CTP）は、CSA GRC スタック特に OCF/STAR における重要コンポーネントである。それらは、組織（クラウドサービスカスタマ、クラウドサービスプロバイダ、又はクラウドブローカ）の情報セキュリティリスクマネジメント及びガバナンスプログラムにおいて多くの役割を果たすことを意図している。それらには次のものが含まれている：

- 伝統的な評価、監査及び認証の補完
- セキュリティ運用センター（SOC）の運用の支援
- インシデント対応及びインシデント管理の実践の支援

CloudAudit

CloudAudit のゴールは、共通なインタフェース及びネームスペースを提供することで、監査プロセスを合理化することに関心がある企業及びクラウドサービスプロバイダに、オープンで、拡張可能で、かつセキュアなインタフェース及び方法を用いることにより、それを可能にすることである。CloudAudit は、監査において自動化され得るものを自動化することを目的としている。

CloudAudit は、インターネット上の草案[54]として記述されており、今では CSA GRC スタックの一部である。

CloudAudit がどのように働くかを理解するために、まず、STAR 認証を進めているあるクラウドサービスプロバイダを想定する。適用される管理策は、適用宣言書（SoA）に含まれている。監査人は、利用可能な証拠に基づいて、管理策が実施され、管理策のためのプロセスが十分に成熟していることを検証して、その結果を報告書にまとめる。監査により多くの可視性を得たいと望むクラウドサービスカスタマは、リスク分析ツールに手作業で結果を入力することができる。

CloudAudit は、REST （Representational State Transfer）[55]のインタフェースを通じて、監査情報を表現することにより、この手作業のプロセスを改善する。例えば、あるクラウドサービスカスタマが、クラウドサービスプロバイダ による cloudhosting.org の管理目標 AIS-01（CCM V3.0.1 ドメイン 1 アプリケーション及びインタフェースセキュリティ）について、より多くのことを知りたい場合、クラウドサービスカスタマはある特定の URL（例えば、http://cloudhosting.org/.well known/cloudaudit/org/CSA/CCM/v3.0.1/AIS/01/manifest.xml）に問い合わせすることができ

[54] https://tools.ietf.org/html/draft-hoff-cloudaudit-00
[55] https://en.wikipedia.org/wiki/Representational_state_transfer

る。その問い合わせ（クエリー）は、証拠となる文書（例えば、PDF、スプレッドシート）の URL を返す。

Cloud Trust Protocol

CTP は、クラウドサービスカスタマがクラウドで使用するサービスについて非常に特定されたセキュリティ関連の情報を得ることができる仕組みである。CTP は、透明性と信頼性を高める。

CTP は、継続的モニタリングにより従来型の監査を補完する。CTP は、１つの監視技術を定義しているのではなく、継続的モニタリング技術の１つの重要な側面に関する仕様であることに気を付ける必要がある。

図３で示すように、CSA は、 クラウドサービスプロバイダ が必要な時間の間、精緻に定義された計測値を継続的に示すことができる標準インタフェースとして、 CTP を構築することを提案している。その計測値をどのように利用するかは、CTP によっては定義されない。

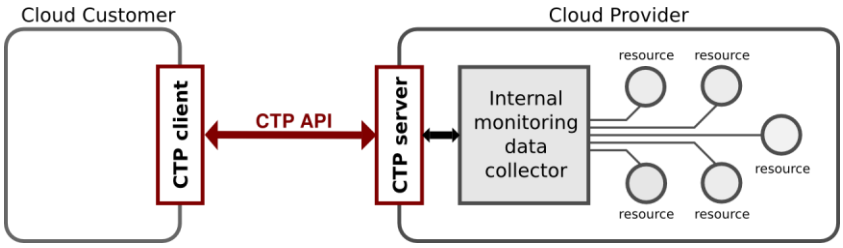

図 3[56]

CTP の構成要素は、遵守状態の結果を対象にしてはいない。むしろ、クラウドサービスの部分である特定の資源（例えば、サービス、API、データベース等）にリンクされているセキュリティ指標が対象となる。

CTP は、「サービス X が、ドメイン B における、フレームワーク C の統制目標 A1 に対して実装している監査事象及び証拠は何か？」、あるいは「最近 1 ヶ月の間のサービス Y のサービスを提供している仮想マシン上のインシデントに対する平均インシデント対応時間は何か？」といった質問に答えることができる。

CloudAudit と同様、CTP は REST のパラダイムを使用する。これは、SSL / TLS その他のウェブサービスのセキュリティ標準により提供されている機密性及び認証の仕組みの利点を利用することができることを意味する。

[56] 訳注：CTP API の標準インタフェースと構築イメージ

CTP と CloudAudit は、共に REST インタフェースを持っており、同じゴールをもった類似ツールのように見えるかもしれない。実際は、全く別物である。CTP は、セキュリティ指標の定常的な監視を可能にする。一方、CloudAudit は、監査結果の標準化された表示を可能にする。

CTP は進行中のプロジェクトである。CSA は、*「Cloud Trust Protocol データモデル及び API*[57]*」* をリリースし、その API を実装するオープンソースのプロトタイプサーバを開発した。しかしながら、CTP は現時点では、標準化されたセキュリティ評価指標のカタログの策定に至っていない。研究されている 1 つの手段は、ISO 19086-2[58]に記述されたモデルである。

[57] https://cloudsecurityalliance.org/group/cloudtrust-protocol//#_downloads
[58] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67546

7 附属書 3：STAR 継続型

STAR 継続型は、クラウドサービスプロバイダに対する監査、評価、モニタリング及び認証の自動化を可能にする。CSA は、クラウドのセキュリティ、監査、監視及びマネジメントの製品を開発しているクラウドサービスプロバイダの業界と密接に連携して STAR 継続型の仕様を開発する。

STAR 継続型は、次のような CSA の成果物の上に構築することになる：

- クラウドコントロールマトリクス（CCM）
- Cloud Trust Protocol（CTP）
- CloudAudit（A6）
- Cloud Trust ワーキンググループ（CTWG）
- Privacy Level Agreement（PLA）

この附属書では、当面の STAR 継続型の姿と、将来の継続的監査の実装可能性について述べる。

短期的な実装：STAR 継続的監査ベース自己認証（SCAS）

附属書２で説明したように、CloudAudit のゴールは、セキュリティ監査表明に対するインタフェース及びネームスペースを提供することである。情報は、標準化されたディレクトリ構造で表現され、REST インタフェースを介して利用できるようにすべきである。

STAR 継続的監査ベース自己認証（SCAS）は、CCM 管理策に関して継続的な監査を提供することを意図している。それを適用することは、OCF レベル１又は２の監査に取り組んでいるクラウドサービスプロバイダにとって自然な次のステップである。

SCAS は、クラウドサービスプロバイダにセキュリティ管理策の変更を動的に報告することを可能にする。例えば、既に STAR 認証を得ているクラウドサービスプロバイダが、２つの時点の STAR 継続的監査の間で特定の管理策の実装がどう変化したか報告することができる。

CSA は、次の２つの SCAS の実装を視野に入れている：

- SCAS1 は、STAR 自己評価（OCF レベル１）の静的なアプローチと、動的アプローチである STAR 継続型（OCF レベル３）の組み合わせである。
- SCAS2 は、第三者認証／監査証明（OCF レベル２）と、動的アプローチである STAR 継続型（OCF レベル３）の組み合わせである。

SCAS の完全に開発された版は、STAR 登録制度を改善する。そして、STARWatch と CloudAudit によって CSA が既に達成した成果をより高める。つまり、STAR 認証の監査における証拠の収集を劇的に改善するのである。

CSA は、SCAS の実装によって、あるクラウドサービスプロバイダが、STAR 継続型の監査表明を発信する自身の WEB サイトを持つことができると予測している。クラウドサービスプロバイダは、その発信を CSA を介して行うこともできる。

SCAS は、数年後には OCF/STAR の中に組み込まれると考えられる。

将来の実装が見込まれるもの：STAR 継続的モニタリングベース認証（SCMC）

STAR 継続的モニタリングベース認証（SCMC）は、現在利用可能なセキュリティ認証スキームの 1 つの発展形を表している。SCMC は「時点」と「期間」の監査から離れて、継続的な監査のアプローチを取り入れることを意図している。Cloud Trust Protocol は、SCMC に不可欠になる。

CSA は SCMC に関して、以下のことを視野に入れている：

- クラウドサービスに対するセキュリティ指標を定義すること
- 対象となる指標に対しての測定手法を定義すること
- SLO を定義すること
- ISO 19086-3 の要求事項に基づく認証[59]
- 監視結果を 提示するためのインタフェースとしての CTP
- 関係者（即ち、CSA、クラウドサービスカスタマ、クラウドサービスプロバイダ、監査人、クラウドブローカ）のいずれかによってホストされたモニタリング結果のリポジトリ

SCAS と同様に、SCMC は数年後には OCF/STAR にその方法が組み込まれる見込みである。

CSA STAR 継続型の課題

STAR 継続型の定義と実装における初期の課題のいくつかは、CTP の設計とそれを通じて収集されるデータの完全性に関連している。以下のようなニーズが課題となっている：

- セキュリティの測定手法と互換で、表面から見えない形で、かつ相互運用性があるモニタリングツール
- セキュリティ指標を技術的メカニズムにリンクさせ、逆に技術的メカニズムをセキュリティ管理策にリンクさせるための方法
- セキュリティ指標についての最新の情報をモニタリングする手段。例えば、資源内の「暗号化されたデータのパーセンテージ」と名付けられたセキュリティ指標がある場合、そのような測定結果の証拠を提供する方法がなければならない。
- CTP の API と CTP のデータモデルは、IaaS、PaaS、SaaS に対応するのに十分な汎用性を有することが望ましい。

[59] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67547

- 監査ログと監査証拠の完全性及び真正性を保証する手段
- セキュリティ指標の信頼性（例えば、情報源の真正性）を保証する手段
- STAR 継続型によって得られるデータに基づき、クラウドサービスプロバイダ間の有意な比較を得るためのメカニズムの組み込み