Security, Trust and Assurance Registry (STAR)の概要

CSA Security, Trust and Assurance Registry (STAR)プログラムは、クラウドプロバイダの信頼と保証を包括的に提供します。CSA STAR プログラムは、プロバイダと利用者による、さまざまな保証要件および成熟度レベルを把握できるように設計された一般からアクセス可能な形での登録簿であり、世界中の利用者、プロバイダ、業界、政府によって使用されています。STAR は、3 つのレベルの保証から構成されており、現在、4 つの異なった形態で提供しています。すべての提供形態が、Cloud Controls Matrix(CCM)におけるクラウドを対象としたコントロール目標の、簡潔かつ包括的なリストに基づいています。CCM は、クラウド特有のセキュリティコントロールの唯一のメタフレームワークで、主な規格、ベストプラクティス、および規制にマッピングされています。 以下は、STAR が提供する内容の全体図になります。

日本語版の提供について

本書「Security, Trust and Assurance Registry (STAR)の概要」は、CSAが公開している「Security, Trust and Assurance Registry (STAR) Overview」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。従って、日本独自の法令や基準に関する記述は含まれておりません。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。

なお、本書は、予告なく変更される場合があります。

日本クラウドセキュリティアライアンスに関する情報は、以下の URL より参照可能ですのでご覧ください。
http://cloudsecurityalliance.jp

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の以下の有志により作成されています。
（敬称略、順不同）

勝見　勉
山浦　広大
二木　真明
笹原　英司
小川　隆一
諸角　昌宏

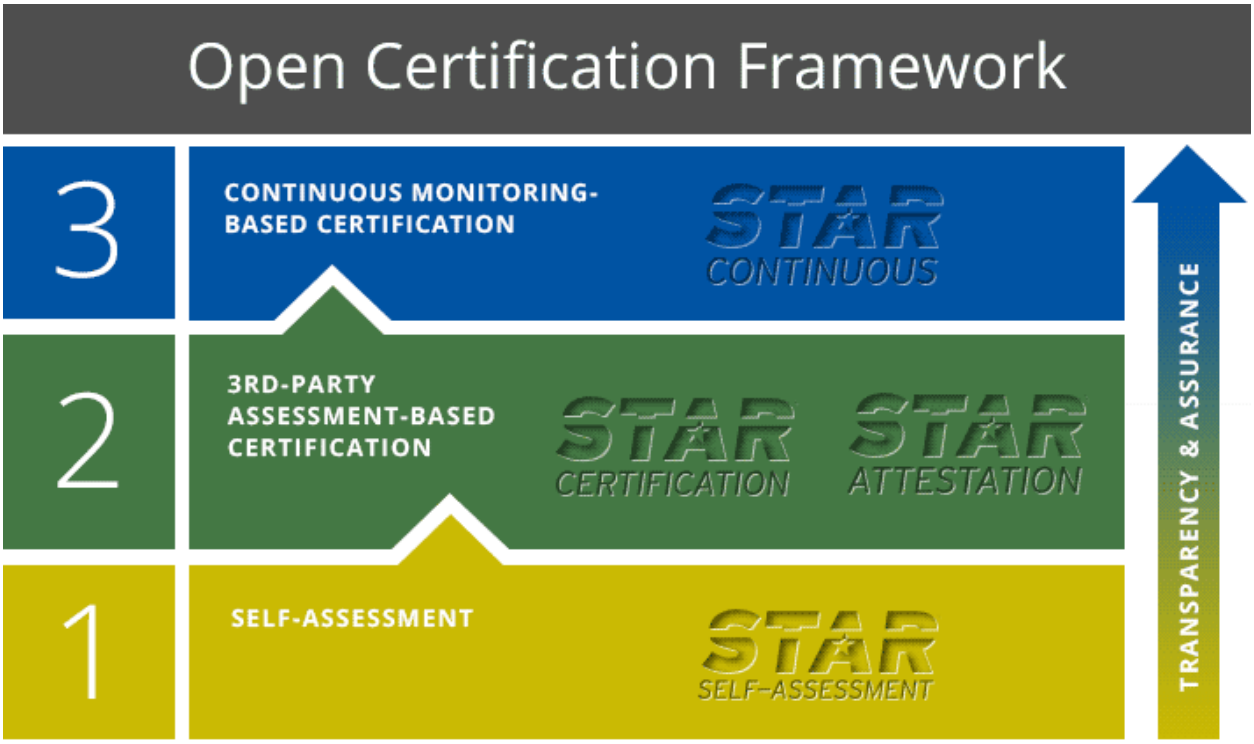
2014 年 9 月 24 日

CSA STAR プログラムの提供

CSA STAR は、CSA GRC スタックの 2 つの主要な研究コンポーネントに基づいています：

Cloud Controls Matrix (CCM) - 管理策の体系である CSA CCM は、クラウドコンピューティングに適応させた情報セキュリティに関して、必要な構造、詳細、および、明瞭さを組織に対して提供します。

Consensus Assessments Initiative Questionnaire (CAIQ) - これは、クラウド利用者とクラウド監査員が、クラウドプロバイダに対して聞きたいと思われる一連の質問です。 それは、一連の”yes”, “no” 形式のコントロールの保障に関する質問を提供しており、質問はそれぞれのクラウド利用者に固有な証拠要件に沿って調整することができます。



レベル 1: CSA STAR セルフアセスメント

CSA STAR セルフアセスメントは、様々なクラウドコンピューティング環境によって提供されたセキュリティコントロールを文書化したもので、無償で提供されています。それによって、利用者が、現在利用している、あるいは、契約しようと考えているクラウドプロバイダのセキュリティについての評価を助けます。クラウドプロバイダは、完成した Consensus Assessments Initiative Questionnaire(CAIQ)を提出するか、Cloud Controls Matrix(CCM)に対するコンプライアンスを文書化したレポートを提出します。この情報は、一般に利用可能になり、業界における透明性を促進し、特定のプロバイダのセキュリティプラクティスに対して、利用者に目に見える形で提供するようになります。

レベル 2: CSA STAR 実践認証

CSA STAR 実践認証は、CSA と AICPA との共同作業によるもので、米国公認会計士が AICPA の基準(Trust Service Principles, AT 101)と CSA の Cloud Controls Matrix を使用することで SOC2 業務が行えるように、ガイドラインを提供します。STAR 実践認証は、クラウドプロバイダに対する独立した第三者による厳格な評価を提供します。

レベル 2: CSA STAR 認証

CSA STAR 認証 は、クラウドサービスプロバイダのセキュリティに対する独立した第三者による厳格な評価です。技術に中立な形の認証は、CSA Cloud Controls Matrix と共に ISO/IEC 27001:2005 マネージメントシステム標準の要件を利用します。

レベル 3: CSA STAR 連続監視

現在開発中で、2015 年にリリース予定です。

CSA STAR 連続監視は、クラウドプロバイダの現在のセキュリティ実践を自動化することができます。プロバイダは、CSA の様式と仕様に基づいてセキュリティ実践を公開し、顧客とツールベンダは、この情報を検索して、さまざまな目的に沿って提示できます。

CSA STAR への参加

クラウドサービスのユーザ

クラウドサービスのユーザは、プロバイダとの話し合いにおいて CSA STAR への参加を求めるべきです。これは、クラウドサービスの調達や RFP(Requests for Proposals)を行っている間、頻繁に行います。STAR によるセキュリティプラクティスの公開は、ベンダーの選定を簡素化し加速します。さらに、世界的規模でクラウドプロバイダ側の、より一貫したレベルのセキュリティプラクティスを保証します。

あなたのクラウドプロバイダが CSA STAR に参加することを拒否した場合には、あなたには、Consensus Assessments Initiative Questionnaire(CAIQ)あるいは Cloud Controls Matrix(CCM)を非公開で作成し、そのコ

ピーを送っていただくことをプロバイダにお願いすると選択肢があります。しかしながら、プロバイダが STAR に参加することを求めていただくことを、強く推奨します。1 つの非公開の CAIQ フォームはあなたを助けますが、プロバイダの透明性はクラウドユーザ全体のコミュニティを助けます。

クラウドサービスプロバイダ

クラウドサービスプロバイダは、CSA STAR に参加することによって多くの利益を得ることができます。突き詰めていくと、販売している製品の最も重要な機能は信頼(Trust)です。そして、CSA STAR は、あなたのクラウドサービスが信頼できるということを最も包括的に保証しています。

- グローバルな STAR 登録の中での開示
- CSA STAR ロゴとブランドの使用
- 顧客の要求に基づいた革新的なコンプライアンス
- 顧客の内部調査とセキュリティ評価に応じることにおける規模の経済

IT 監査員と審査機関

もし、あなたが、監査、実践認証、あるいは、認証サービスを提供するビジネスを行っている場合、CSA STAR レベル 2 に参加することを検討するように推奨します。IT システムの多くがクラウドコンピューティングに移行しているように、クラウド特有のセキュリティ保証のために主要な国際標準を提供することによって、あなたの IT 保証を提供するビジネスは成長するでしょう。あなたの特定のビジネス、場所、および、着目点によって、CSA STAR 実践認証か CSA STAR 認証のどちらか、あるいは、両方を提供してください。

セキュリティソリューションプロバイダとコンサルタント

あなたがプロフェッショナルサービスを提供する場合、CSA は、CSA STAR に基づくプラクティスを開発することを推奨します。これは、プロバイダと利用者の両方に対して、安全なクラウドの採用—これは、共同責任になりますーのために支援します。あなたが、セキュリティ製品と SaaS ソリューションを開発している場合、CSA STAR に関連するデータとベストプラクティスをどのようにして直接統合できるかについて検討してください。私たちの知的財産の多くを、著作権使用料無料で利用することができます。

CSA STAR: クラウド信頼と保証の未来

CSA STAR は、クラウドにおける保証のための業界における最も強力なプログラムです。STAR は、透明性、厳しい監査、規格の調和、および、継続したモニタリングという主要な原則を包含しています。ベストプラクティスと初期レベルを、無償で達成することができます。また、クラウドコンピューティングにおける信頼を可能にするために、プロバイダと利用者が STAR を採用することを推奨します。

詳細な情報

一般的な問合せ: star-help@cloudsecurityalliance.org

CSA STAR 認証監査員: https://cloudsecurityalliance.org/star/certification/#_auditors

CSA STAR 実践認証監査員: https://cloudsecurityalliance.org/star/attestation/#_auditors