Open Certification Framework

ビジョンステートメント

2012 年 8 月

日本語版の提供について

本書「Open Certification Framework　ビジョンステートメント」は、CSAが公開している「Open Certification Framework Vision Statement」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

背景

Cloud Security Alliance は、安全で信頼できるクラウドサービスの市場による採用を抑制している IT エコシステムに潜むギャップを特定しました。利用者には、プロバイダの障害耐性、データ保護能力、サービスの移植性を評価し比較するための簡単で費用対効果がよい方法がありません。この問題は、クラウドサービスの国際的な側面においてさらに深刻であり、国境をまたがるクラウドサービスの利用に大きな障壁となっています。

CSA は、ただ一つの認証、規制、あるいは、その他のコンプライアンスの形が、IT の未来を統治する際に他のものに取って代われるものではないことを認識しています。これは、既にオーバーロード状態にあるコンプライアンスのために、多額の費用と複雑さを追加することのリスクと同様です。しかしながら、グローバルに展開するコンピューティングユーティリティとしてのクラウドの登場は、コンプライアンスの懸念に対してより良い調和の実現を求めています。

ISO SC27 標準は、グローバルに受け入れられる可能性があります。しかしながら、27017/8 対 27001/2 の将来に関しては大きな疑問があります。 CSA は、それ自身の IP（私たちの Standards Incubator の役割として）を用いて、その成果に前向きな貢献ができるよう活動しています。

AICPA SAS70 とその後継の監査基準は、サービス会社のための監査基準書として重要な牽引役を果たしてきました。また、多くのクラウドプロバイダに人気があります。しかしながら、それはクラウドプロバイダの中で評価されるべきである一連の管理目標の標準としての基準に欠けています。

米国の連邦政府を含む政策立案者、欧州委員会、その他のものは、クラウドサービスの認証体系をサポートしています。

IT の保証、監査、認証に対する上記の伝統的なアプローチのすべてが、クラウドコンピューティングの急激な変化と動的性質の問題を抱えています。消費者とプロバイダのどちらも、すばやく活動する CSA に支持されたコンプライアンス活動が、グローバルな規制制度の中で広く適用されるという事実から利益を得ることになるでしょう。

ビジョンステートメント

CSA Open Certification Framework は、クラウドプロバイダのグローバルで、公認で、信用された認証を許容するための産業界の取り組みです。

CSA Open Certification Framework は、Cloud Security Alliance の産業界を主導するセキュリティガイダンスとコントロール目標に従った、柔軟で、成長性があり、多層構造を持つクラウドプロバイダ認証のためのプログラムです。

プログラムは、労力と費用の重複を避けるために、公認会計士のコミュニティの中で開発された一般的な第三者評価と認証ステートメントと統合していくでしょう。

CSA Open Certification Framework は、CSA GRC (Governance, Risk and Compliance) Stack 研究プロジェクトので定義されるコントロール目標と継続モニタリング構造に基づいています。

CSA Open Certification Framework は、プロバイダと消費者の様々な保証要件と成熟レベルに着目したいくつかの層をサポートしています。 これらは、CSA Security Trust and Assurance Registry (STAR)のセルフアセスメントから継続したモニタリングによる高保証の仕様までの範囲があります。

CSA Open Certification Framework は、以下の内容を提供します:

- コンプライアンス問題に取り組む地域に、信頼とグローバルなベストプラクティスにより道筋を提供すること。例えば、私たちは、政府が GRC Stack 上に独自の要求事項のレイヤーを作り、CSA Open Certification Framework の大きな採用者になることを期待しています。そして、公共部門クラウドの利用のための素早い認証を提供することを期待しています。
- 複数の認証の取り組みに対して、GRC Stack ツールをどのように使用するかというプロバイダのための明白なガイダンス。 例えば、ドキュメントの範囲は、プロバイダが CSA Cloud Controls Matrix (CCM)に組み込んでいる ISO/IEC27001 の証明経路にしたがっているかどうかがはっきりわかるようにすべきです。
- ISO、AICPA、およびその他の可能性のある組織をサポートできるような“認証体系（recognition scheme）”。これらは、認証/枠組みの内部に CSA の IP を組み込んでいます。

CSA は、できる限り、一度の認証で何度でも使える、ということをサポートします。

CSA は、プロバイダへの認証が複雑にならないように、調和をとり、簡素化したいと考えています。

信頼されたクラウドサービスのための認証スキーム

政府、民間、公共部門は、IaaS、PaaS、SaaS または(X)aaS が提供しているセキュリティやプライバシーのレベルを評価し認証するための標準を要求しています。

セキュリティとプライバシーのそのようなグローバルに認知された標準は、現在クラウドコンピューティングサービスの中で受け止められている信頼のギャップを満たすことで、クラウドコンピューティングの大規模なグローバルな採用を伸ばしくものと期待されます。

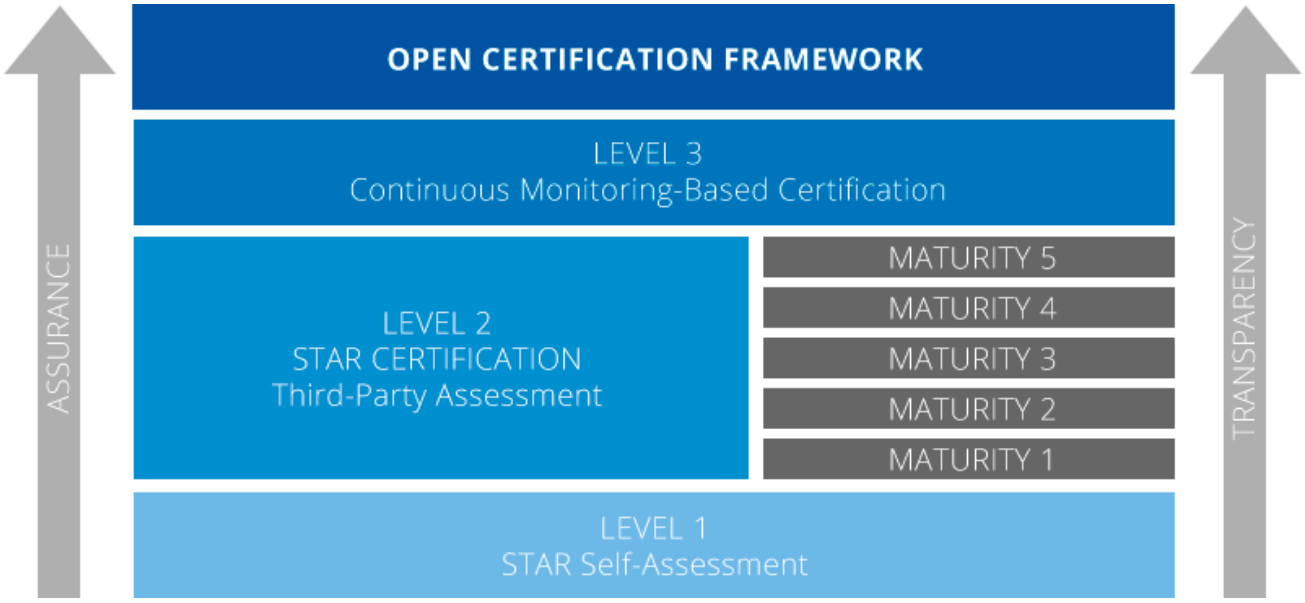
この信頼のギャップは、主に、クラウドプロバイダに対する基本的な保証の問題に直面しているクラウドユーザに苦労を強いています。たとえば、以下のようなことです:

- 法令遵守と契約責任の理解
- 責任の定義と所在の明確化
- 説明責任の履行要求
- 要求を、クラウドの言語/コントロール/チェックに置き換えること
- クラウドサービスの事前分析評価、および、クラウドサービス契約の実行状況の継続的な監視のための手段を示すこと

これらは、対象範囲とプロセスが目的と SLA にかなっているかどうかを確実にする以下の 8 つの経営原則によってサポートされます:

- 顧客中心
- リーダーシップ
- 人とのかかわり
- プロセスアプローチ
- マネージメントへのシステムアプローチ
- 継続的な改善
- 意志決定へのエビデンス・ベースド・アプローチ
- 互いに有益なサプライヤー関係

Open Certification Framework の構造



open certification framework は、信頼に対する３つのレベルで構成されています。それぞれのレベルは、クラウドサービスプロバイダの運用における可視性と透明性のレベルを提供し、クラウド利用者に対するより高いレベルの保証を提供しています。

レベル 1: STAR セルフアセスメント
クラウドプロバイダは、CSA のベストプラクティスに対するコンプライアンスを示すために、以下の 2 つの異なったタイプのレポートを提出できます:

The Consensus Assessments Initiative Questionnaire (CAIQ),
Cloud Controls Matrix (CCM)

レベル 2: STAR 認証(第三者評価)
この枠組みのコンセプトは、CSA Cloud Control Matrix(CCM)と組み合わされた ISO/IEC 27001:2005 管理システム規格の要求条件と、組織自身の内部の要求条件または仕様を使用することです。これらは、システムがどれくらい成熟しているかを評価します。回答が記録され、後でそれらの成熟度のレベルのために分析されます。 この成熟度には、スコアが与えられます。 そして、すべてのスコアが集められ、異なったドメインの管理システムのスコアや全体のシステムのスコアが算出されます。

上記に加えて、評価者によって確認されスコアが与えられるプロセスを含んだ内部パフォーマンス評価基準がクライアントに与えられます。

レベル 3: 継続したモニタリングに基づいた認証。これは現在開発中です。この概念は、利用者要件の実施をほぼリアルタイムでモニターします。これは、監査証拠の連続した収集に基づいています。

STAR 認証(レベル 2)

「クラウド」には、固有の情報リスクがあります。一方、エンドユーザは彼らの情報のセキュリティに懸念があり、クラウドサービスプロバイダ (CSP)を信じることができるか否かの懸念があります。

リスクが扱われていて、範囲が SLA で規定されていることを保障する追加の厳しさが必要です。

STAR 認証は、組織の情報管理システムの効率を評価し、範囲、プロセス、および目標が「目的に適っている」ことを保証します。 成熟度レベルを使用して、組織が改良の必要な領域の優先付けを行い、合格・不合格モデルではなくビジネスを良い方向に導いていくことを手助けします。また、該当するセクターの他の組織を効果的に比較することができます。

この強化された評価サービスは、効果的なパートナーシップと同様に、戦略上、および、操作上のビジネス利益というものにフォーカスするアプローチです。Plan、Do、Check、Act(PDCA)アプローチと Cloud Controls Matrix (CCM)で概説された基準に基づき、このサービスは、査定人が長期に渡っての持続性とリスクについて、会社のパフォーマンスを定量的にスコア化することができます。また、SLA をベースに進められることに加えて、役員が毎年の改善状況を定量化し測定できるようにしています。

経営原則と管理の適用を通して、CCM に概説されているように、評価者は主たる経営指標の改善を果たすということにフォーカスすることができます。これにより、組織は既存のビジネス管理システムを前進させ、ビジネスのベストプラクティスを具体化することに注力できるようになります。

CCM は、クラウドベンダへのガイドとなり、将来のクラウド利用者がクラウドプロバイダの総合的なセキュリティリスクを評価するのを助けるために、基本的なセキュリティ原則を提供するように明確に設計されています。フレームワークとして、CCM は、クラウド産業に適合した情報セキュリティに関連する、必要な構造、詳細、および明快さを組織に提供します。CCM は、企業情報セキュリティコントロール要件を強調することによって既存の情報セキュリティコントロール環境を強化し、クラウドにおける執拗なセキュリティの脅威を削減し、脆弱性を特定し、標準化されたセキュリティと運用上のリスク管理を提供し、セキュリティへの期待値、クラウドの体系づけと用語の整理、およびクラウドに実装されたセキュリティ対策を常態化することを希求しています。

Cloud Controls Matrix は、評価者による評価と統合され、マトリックスの相互参照を使用することで関連する ISO27001 コントロールに対して該当する CCM のコントロールが参照できるようになっています。認証範囲の中で、組織の総合的なパフォーマンスの結果が作成されます。

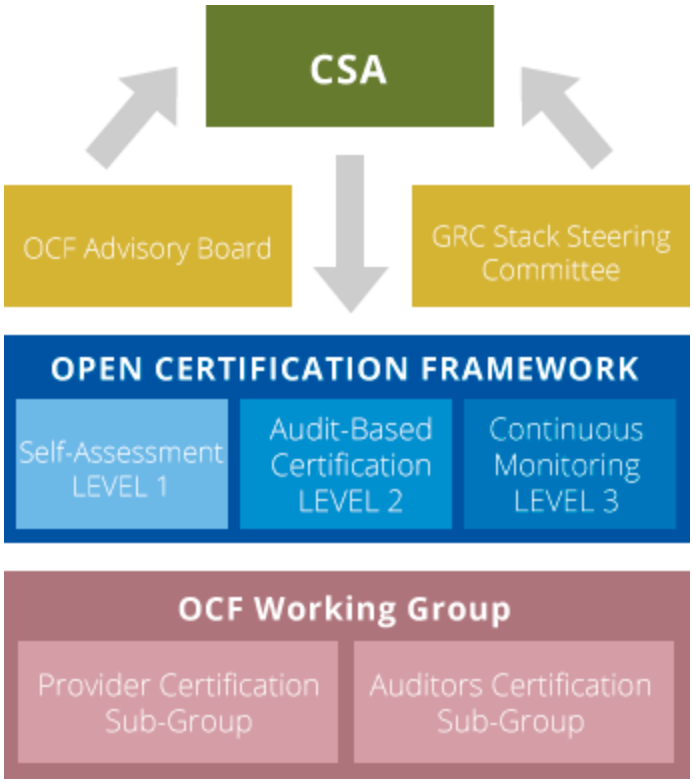
STAR 認証のための公認審査員(監査人)

監査人の認証委員会は、監査人要件と監査人の認証プロセスを定義します。
監査人の認証プロセスは、英国規格協会 (BSI)によって管理されます。

OCF タイムライン

- LEVEL1 は、現在、STAR を通して利用可能です。
- Open Certification Framework は、2013 年 Q1 に利用可能になる予定です。
- 監査人認証体系は、2013 年 Q1 に利用可能になる予定です。
- プロバイダのための STAR 認証は、2013 年 Q2 に利用可能になる予定です。
- LEVEL3 継続モニタリングは、2015 年以降に利用可能になる予定です。

ガバナンス構造



OCF は、CSA の直接の管理下にあります。これは、OCF 運営委員会(SC)と GRC Stack 運営委員会によってサポートされています。OCF SC と GRC Stack SC は、OCF の開発と実装において CSA マネージメントに対する戦略的アドバイスを提供します。

GRC Stack SC は、以下のようなアドバイスを提供し、技術的な方向を示します:

- 概念的な GRC Stack フレームワークの改良
- GRC Stack の既存のコンポーネントの改良
- GRC Stack フレームワーク(完全な継続モニタリングソリューションが出されるまでの CCM の利用)の実装。

また、GRC Stack SC メンバーは、コミュニティにおける GRC Stack の大使として活動します。

OCF SC は、以下のようなアドバイスと戦略的方向性を提供します:

- OCF 概念フレームワークの改良
  (LEVEL2 認証スキームを定義、改良します)
  (LEVEL3 認証スキームを定義、改良します)
- 透明性要件の定義（認証と評価/監査の範囲に関する最小限の開示要件を定義します)
- 法律、規定のコンプライアンス要件　(国家の法律と規定のコンプライアンス、および、セクター固有のコントロール層の GRC SC と協力しての定義）の取り扱い
- STAR の改良
- GRC Stack の既存のコンポーネントの改良
- OCF の実装

また、OCF SC メンバーは、コミュニティにおける OCF の大使として活動します。

OCF 作業部会は、プロバイダ認証 サブ作業部会と監査役認証サブグループによって構成され、Level STAR 認証スキームと監査人の認証スキームを定義します(OCF 作業部会 group Charter を参照してください)。