cloud security alliance℠

STAR 実践認証を CSA に提供する米国公認会計士のためのガイドライン

2014 年 5 月

日本語版の提供について

本書「STAR実践認証をCSAに提供する米国公認会計士のためのガイドライン」は、CSAが公開している「Guidelines for CPAs Providing CSA STAR Attestation」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

序論

この文書は、STAR 実践認証（STAR Attestation）を行う際の米国公認会計士に対するガイダンスを提供します。この文書が、米国公認会計士協会（AICPA）の基準や AICPA Service Organization Control® (SOC) に関連したガイダンスを置き換えるものではありません。SOC についての情報および SOC に関連した基準とガイダンスを入手する方法については http://www.aicpa.org/soc を参照して下さい。

パート 1 – 専門家の要求事項

1 一般

1.1 Star 実践認証は SOC 2℠ 業務の 1 つの形態で、その規準には以下を含みます:

1.1.1 TSP セクション 100「セキュリティ・可用性・処理のインテグリティ・機密保持およびプライバシーに係る Trust サービス原則、規準および例示」（AICPA, Technical Practice Aids）（TSPC）のうち適用対象となる規準

1.1.2 Cloud Security Alliance(CSA)の Cloud Control Matrix（CCM)に含まれるコントロール仕様。（CCM コントロール仕様は、AT セクション 101「Attest Engagements [AICPA Professional Standards]」おける「適切な規準」に該当します。また、本書では CCM 規準と呼びます。AT セクション 101 はまた、AICPA 保証業務基準書の一部を構成し、一般に保証業務基準と呼ばれています)。

2 業務の遂行のための要件

2.1 SOC 2℠ 業務は、AT 101 と、SOC 2℠ Guide（受託会社のセキュリティ・可用性・処理のインテグリティ・機密保持およびプライバシーに係る内部統制の保証報告書)に従って、米国公認会計士が行います。

2.2 AT101 は、すべての保証業務を行い報告するための枠組みを提供します。SOC 2℠ ガイドは、AT101 をベースにした遂行と報告のガイダンスを提供しています。これは、クラウドサービス受託会社のシステムに関する記述書と、そのシステムにおけるセキュリティ・可用性・処理のインテグリティおよびシステムによって処理される情報の機密保持またはプライバシーに関連するであろう内部統制に関して、デザインの適切性、また、タイプ 2 保証業務においては、運

用状況の有効性評価に使われます。TSPC は、セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシーに関連する統制に関して、評価し報告するための規準を提供します。SOC2 報告書は一般的に、受託会社によって提供されるサービスの性質について知識のある特定の関係者のみを対象にした、使用が制限された報告書として提供されます。サービスの性質とは、つまり以下のようなものが含まれます：受託会社のシステムが、どのように委託会社、再受託会社、その他の関係者と関わるか；内部統制とその限界；適用対象となる、Trust サービス規準、これらの規準への適合を妨げるリスク、統制がどのようにリスクに対応するか；委託会社の相補的な内部統制と、それがどのように受託会社における関連した統制とともに、適用対象となる Trust サービス規準に適合するように働くか。

2.3 CCM は、TSPC におけるセキュリティ原則の規準と同等の規準を備え、さらにセキュリティに関して付け加えるべきいくつかの規準を含んでいます。

3 能力の要件

3.1 米国公認会計士のサービスは、米国公認会計士に固有の専門家基準に基づいて提供されます。これらの基準の遵守は、AICPA の規則とこれらの基準を採用した個々の州法の下で米国公認会計士の義務となります。

3.1.1 **州会計士法**。 米国公認会計士は、州によって免許を与えられます。米国公認会計士のサービスを提供するには、免許が必要であり、州政府は米国公認会計士の活動に対する監督権限を持っています。その結果、いくつかの米国公認会計士基準が、団体のみならず法の力により強制されます。会計士法の違反は、重篤な罰金と免許の停止か取消し処分につながります。

3.1.2 **倫理規範**。AICPA の専門家行動規範 （規範）は、すべての米国公認会計士サービスに適用されます。米国公認会計士は、提供されるサービスの形態や関わっている内容にかかわらず、規範を固く守らなければなりません。 AICPA の会員資格は、規範に示されている規則を受け入れていますし、AICPA 専門家倫理最高委員会が詳細なガイダンスを発行しながらそれを維持しています。規範は、行動基準を形成し、専門家基準の他の部分に記述された個々のサービスに対応する規則で補完されています。規則は、解釈と適用に関するガイダンスを提供する裁定で補完されています。 以下は、規範に含まれる一般的規則のまとめです。米国公認会計士に必要な 規則は、以下のようになります:

- 財務諸表サービス、あるいは、保証サービスを提供するときには、独立性を維持すること。
- 客観的であり、一貫性を保ち、利益相反を起こさず。そして、故意に誤った事実を伝えたり、自らの判断より他の判断を優先したりしてはならない。
- 専門家としてあるべき専門能力を持つこと。
- 専門家としての職業的注意義務を満たすこと。

- 実行する専門サービスを、適切に計画し監督すること。
- 結論あるいは提言を支える十分なデータを入手すること。
- 関連する専門家基準に準拠すること。
- クライアント情報の機密性を維持すること。
- 特定のクライアントからの成功報酬を拒絶すること。
- 専門家としての信用を失う行為を行ってはならない。
- 事実に反する、誤解を招く、あるいは欺瞞的な広告に関わったり、強制的な、威圧的な、もしくは嫌がらせ的な勧誘・強要に関与してはならない。
- ある種の業務に対する手数料を辞退するか、受領が認められている場合には公開すること。
- 組織でのみ行動し、紛れの生じない法人名を使用すること。

3.1.3 **品質管理**。米国公認会計士は、財務諸表サービスと保証サービスに対して品質管理のポリシーと手続を適用しなければなりません。品質管理のシステムの目的は、監査法人に二つの合理的保証：その監査法人とその従業員が、適用対象となる専門家としての要件および法令ならびに規制要件を遵守していること、および、監査法人発行の報告書がその目的に照らして適正であること、を提供することです。品質管理のシステムには以下の 6 つの必要な要素があります:

- リーダシップの責任。すなわち、トップの姿勢
- 関連する倫理要件への準拠
- 米国公認会計士が有能で業務を行うことができ、関連する要件を遵守することができ、クライアントの誠実さを熟慮した場合のみ、クライアントとの関係と業務を受入れ、継続すること
- 必要な専門能力、職務能力、および遂行責任を担保する人的資質
- 一貫した品質、監督、レビュー、ならびに必要に応じてコンサルテーションに基づいた業務の遂行
- システムの継続的な有効性を保証するためのモニタリング

監査法人の品質管理は、定期的に独立した外部の専門家によって評価されます。評価は、品質管理が効果的であるかについて判断し、結果は正式な報告書としてまとめられます。報告書は通常一般に利用可能で、潜在的なクライアントや情報利用者に対して監査法人が品質管理基準を遵守しているかどうかを判断する機会を提供します。米国公認会計士協会相互審査委員会(AICPA Peer Review Board)は、最近、SOC 2℠業務を必須選択対象業務として承認しました。これは、監査法人が複数の SOC 2℠監査を実施する場合、少なくともその 1 つがピア・レビューの対象とされるべきであることを意味します。

3.1.4 **専門教育の継続**。 米国公認会計士は、米国公認会計士ライセンスを有する州の州政府会計委員会によって定められた継続した教育要件を守らなければなりません。州によって継続した専門教育のための要件は異なります。AICPA は、会員資格を維持するために CPE を必要とします。 また、会計検査院（GAO）に関連する仕事を行うための特別な CPE 要件があります。

4 実践認証の対象範囲

4.1 SOC 2℠報告書では、米国公認会計士は以下について意見を述べます:

- クラウドサービス受託会社のシステム記述書が、記述規準に基づいて適正に表示されているかどうか。
- コントロールが有効に運用されている場合、適用対象となる Trust サービス規準が満たされるという合理的な保証を提供するように、内部統制が適切にデザインされているかどうか。
- タイプ 2 報告書においては、適用対象となる Trust サービス規準と CCM の規準を満たすためにコントロールが有効に運用されてきたかどうか。
- プライバシー原則に関して報告する業務においては、受託会社がプライバシーの実践に関するステートメントにおける約束事項を遵守しているかどうか。

5 規準の制定と選択

5.1 AT101 は、適切な規準の属性を指定します。 SOC 2℠ガイドのパラグラフ 1.34-.35 は、クラウドサービス受託会社のシステム記述に関する規準を含んでいます。TSP セクション 100 は、内部統制のデザインと運用状況の有効性を評価するための規準を含んでいます。 CSA の CCM は、内部統制の仕様を提供しており、これはセキュリティに関連する追加の適切な規準となります。

パート 2　その他の CSA ガイドライン

1　CSA の資格

2015 年 3 月 15 日より、STAR 実践認証業務を行う人は、CSA の Certificate in Cloud Security Knowledge (CCSK)の資格を持っているか、あるいは、同等のトレーニングを受け試験をパスしていることが必要になります。これは、上記のパート 1、3.1.4 の要求事項の一部あるいは追加として、全米州政府会計委員会(State Boards of Accountancy)および IACPA により承認されました。

2　対象範囲

2.1 すべての場合において、提供されるクラウドサービスに関連する活動を含んでいることを保証するために、対象範囲を評価しなければなりません。

3　CSA への資料の提出

3.1 STAR 実践認証の受審完了に向けた情報の提出は、クラウドサービス受託会社の経営者によって決定されます。

透明性の精神から、CSA は、STAR 実践認証のエントリーに際して、審査業務が CCSK 認証を保持する米国公認会計士によって行われたかどうかを明示します。

STAR 実践認証はフォローアップ監査を必須としていないため、審査業務がカバーする「期間」はカバーされている対象範囲とともに STAR 登録に表示されます。

CSA STAR 実践認証の登録を受け付けると、CSA は登録者に CSA STAR ロゴとブランドの使用許可と用法のガイドラインを付与します。CSA STAR ロゴとブランドの使用は、CSA が明確に付与するまで認められません。STAR 実践認証についての CSA ガイドラインの詳細は、以下を参照してください。www.cloudsecurityalliance.org/star/attestation/.