cloud security alliance℠

STAR 認証を提供する企業に対する要求事項

リリース 1：2013 年 7 月 16 日

日本語版の提供について

本書「STAR認証を提供する企業に対する要求事項」は、CSAが公開している「Requirements for Bodies Providing STAR Certification」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

コンテンツ

序論

国際規格と一致させるために、STAR 認証の体系は以下に適合するように設計されています:

- ISO/IEC17021: 2011、適合性評価 – マネジメントステムの審査及び認証を行う機関に対する要求事項
- ISO/IEC27006: 2011、情報技術–セキュリティ技術 –情報セキュリティマネジメントシステムの審査及び認証を行う機関に対する要求事項
- ISO19011、マネージメントシステム監査のための指針

このマニュアルは、ISO/IEC27001 認証プロセスを置き換えるものではありません。 むしろ、そのプロセスを補完あるいは拡張します。すべての認証機関は、組織の ISMS が適切に機能し、ISMS が継続的なコンプライアンスを達成できることを確認するために、内部で認証された ISO/IEC27001 計画マニュアルに従わなければなりません。

他の規格への参照が含まれているところには、比較する要求事項を見つけることができるように強調させています。

1. 一般

1.1 この文書は、ISO27001 審査の一部としてどのように Cloud Controls Matrix(CCM)の STAR 認証審査を行うかを概説します。

1.2 CCM で提示されたコントロールは、ISO27001 の追加コントロールと考えることができます。 *ISO/IEC27001:2006 の 4.2.1 g 節を参照。*

1.3　STAR 認証と同等あるいはそれ以上の範囲をカバーする ISO27001 認証を伴わない場合には、CCM 審査の認証証は有効ではありません。は。

1.4 CCM 審査を行う審査機関は、ISO27006 に従わなければなりません。

1.5 この文書は、ISO27006 の補足として考えられ、CCM の審査のための追加要求事項について概説するのに役立ちます。

1.6 審査機関は、この文書のパート 1 と 2 に従わなければなりません。 パート 2 は、認証計画がどのように運用されるかについての記述を提供しています。

1.7 STAR 認証審査を行うために、審査機関はこの文書に従い、Cloud Security Alliance(CSA)の要求を満たさなければなりません。

パート１ - 要求事項

2. 引用規格

2.1 以下の文書が、この文書の活用に必要です:

- BS ISO/IEC27001: 2005、情報技術–セキュリティ技術–情報セキュリティマネジメントシステム–要求事項
- ISO/IEC27006: 2011、情報技術-セキュリティ技術 -情報セキュリティマネジメントシステムの審査及び認証を行う機関に対する要求事項
- ISO19011、マネージメントシステム監査のための指針

2.1.1 他の文書の特定の節の参照は、文書間の対応関係を示すのに役立ちます。

3. 用語と定義

3.1 クラウドコンピューティング-コンピューティング資源をネットワーク越しに提供します

3.2 クラウドサービスプロバイダ-クラウドサービスを提供する組織

3.3 STAR データベース - CCM の審査の結果を格納する CSA が運営しているデータベース

4. 審査機関の要求事項

CCM 審査を行う審査機関は、ISO27001 審査の提供主体として、国際認定フォーラム(IAF)のメンバーとして認可された機関によって ISO27006 に基づき認可を受けていなければなりません。

4.1 審査機関は、ISO27006 のすべての要求事項に従うものとします。これは、CCM 審査を行うときにこの文書の要求事項に従うことと同様です。

4.2 この文書は、CCM を監査する特定の領域に対して明確にしていますが、審査機関が審査を行うときに ISO27006 に従う義務を軽減することはありません。

5. 能力要求事項

5.1 すべての審査者は、ISO27001 の公認の主任監査員コースに合格したという証拠を提示するか、ISO27001 審査機関に正式認可を受けた IAF メンバーのための資格のある経験豊富な ISO27001 審査者である証拠を提示できなければならない。 *ISO27006 の 7.2.1.3c.1 参照*。

5.2 すべての審査者は、BSI/CSA CCM コースを終了しなければならない。 *27006 の 7.2.1.3c.1 参照*。

5.3 すべての審査者は、情報セキュリティ分野で最低 2 年作業経験がなければならない。 *27006 7.2.1.3e.1 参照*。

5.4 審査者が、CSA の Cloud Security Knowledge(CCSK)認証を取っているか、クラウドコンピューティングや情報セキュリティアプリケーションで同じ水準の知識の代替のコースを終了している場合、5.3 節の要求事項は必要ない。

6. 認証の範囲

6.1 組織の範囲を区切り、認証の対象範囲にどのような機能を含むかを明確に定義しなければならない。

6.2 クライアントに誤解を招く恐れのある範囲や、（認証の）利用者が登録範囲にカバーされていると想定するであろう組織の部分を含んでいない範囲は、許容されない。 ISO27006 の 9.1.2 節参照。

6.3 ISO27001 認証の範囲は、STAR 認証の範囲より小さくてはならない。

6.4 範囲は、クライアントのデータあるいはクライアントが受けているサービスに関わりのある重要な活動の完全なつながりにできるかぎり密接に反映して書かれていると期待される。組織がクライアントと結んでいるサービス内容合意書（SLA）の主要部分をカバーしていると期待される。

7. 監査時間

7.1 CCM 審査を伴う ISO27001 審査を行うための監査期間は、ISO27006 の定義に基づき ISO27001 審査に必要な期間の、最低 1.5 倍にと見積もられる。 *ISO27006 の 9.1.3/9.1.4 Annex C を参照*。

7.2 ISO27001 に従って、サンプリングは許可されます。

8. ISO27001 と CCM を一緒に評価

8.1 ISO27001 と CCM の審査を一緒に行ったとしても、ISO27001 の審査に割り当てられる時間は通常減少することはありません。しかしながら、ISO27001 と CCM に関する監査要求事項にはオーバラップするところがあるので、労力の重複は避けられます。潜在的に重複する領域を簡単に特定するために、ISO27001 の一致する領域が CCM の中で指定されています。

9. 監査と認証

9.1 審査サイクルは、ISO27001 の審査サイクルに従います。*ISO27006 の 9.2 /9.3 /9.4 節を参照。*

9.2 初めて同時に ISO27001 と STAR 認証の両方を取得する組織のために、SO27001 と CCM のすべての要求事項をカバーする、2 部からなる初期審査があります。その後、訪問調査が行われる。3 年間にわたって、訪問調査は ISO27001 と CCM のすべての範囲をカバーします。証明の更新審査は、サイクルの終わりに行われます。

9.3 既存の ISO27001 認証に STAR 認証を加える組織では、すべての適用できるコントロールセットは最初の訪問のときに監査されます。 CCM を監査するために割り当てられた時間が、証明更新のための訪問（調査）を行うのに必要である時間の追加 50%であれば、どのような種類の訪問（調査）でも構いません。

10. コントロールの設定

10.1 コントロールが実施され有効であるという合理的な証拠がなければなりません。通常、これは、何らかの記述のコントロールが 3 カ月実施されたことを意味します。しかしながら、コントロールがより短い期間で有効であることを示す証拠を集めることができた場合、これが考慮されます。

11. コントロールの選択

11.1 場合によっては、コントロールは適用できないかもしれません。 ISO27001 で説明されているように、コントロール領域の除外は適切に正当化されなければなりません。 ISO27001 の 4.2 1.g 節を参照。

11.2 補完的コントロールは、CCM における 1 つのコントロールが他のコントロール領域で実施される対策によって冗長となる場合に許容されます。

パート 2 - CSA にデータを提出

12. 能力モデル

12.1 CCM は、管理能力モデルに対して監査されます。このモデルをどのように監査するかというガイダンスは、CSA の‘Auditing the Cloud Controls Matrix’の文書に示されています。

12.2 ‘Auditing the Cloud Controls Matrix’の文書にあるガイドラインに従って、すべての STAR 認証審査が監査されなければならない。

13. スコアの提出

13.1 審査に続いて、組織は、その認証を STAR レジスタ上に公開することを選択できます。以下のオプションの 1 つを選ぶことができます:

- CCM に対して評価されたものを公開しますが、スコアは公開しないを選択
- スコアの要約は公開しますが、CCM の個別のコントロール領域のスコアは公開しない
- 各コントロール領域ごとのスコアをすべて公開

13.2 組織がどのレベルの公開を行うように準備するかを確かめるのは認証機関の責任になります。

13.3 クライアントの同意に続いて、認証機関は、相互に合意したデータ交換プログラムに則って CSA の STAR データベースに記載するために CSA にスコアを提出します。

14. 認証を発行

14.1 STAR 認証証明書は、組織が ISO27001 の審査を通過していない場合、発行されません。