STAR継続型
技術文書

認証を取得するには

cloud security alliance®

CSA JC cloud security alliance℠ Japan Chapter

ACKNOWLEDGEMENTS

Alain Pannetrat
Christopher Niggel
Damir Savanovic
Daniele Catteddu
John DiMaria
Michael Roza

Ronald Tse
Tim Dafoe
Timo Alexander Gröf

日本語版提供に際しての告知及び注意事項

本書「STAR継続型技術文書　認証を取得するには」は、Cloud Security Alliance (CSA)が公開している「STAR Continuous Technical Document」の日本語訳です。本書は、CSAジャパンが、CSAの許可を得て翻訳し、公開するものです。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。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSAジャパンは何らの保証をするものではありません。
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。

変更履歴

日付	バージョン	変更内容
2019年6月26日	日本語版1.0	初版発行

日本語表記の注意点

本書の翻訳において、STAR Continuousに関して以下の2つの訳を使用しています：

- STAR継続型
  STAR　Level 3のSTAR Continuousは、STAR継続型と訳しています。
- STAR継続確認型
  STAR　Level 1およびSTAR Level 2のSTAR Continuousは、STAR継続確認型と訳しています。

これは、Level 1/2とLevel 3のContinuousの意味が異なることによります。Level1/2におけるContinuousは、クラウドプロバイダが1か月ごとに自己評価を更新するものであるのに対して、Level 3のContinuousは、管理策の検証を自動化することでより高い頻度の監査を可能にすることを意味します。

日本語版作成に際しての謝辞

「STAR継続型　信頼と一貫性の増進へ」の日本語訳は、CSAジャパンの「CCM/STARワーキンググループ」に参加するメンバーを中心とした、CSAジャパン会員の有志により行われました。
作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名および所属先（企業会員からの参加の場合のみ）を記します。
（氏名あいうえお順・敬称略）

伊賀　誠
勝見　勉
成川　達也
満田　淳

CSA STAR 継続型について

STAR 継続型は、クラウドサービスの継続的なコンプライアンス評価プログラムで、CSA STAR プログラムの不可欠な構成要素です。このプログラムにより、CSP は、そのセキュリティ検証機能を、クラウドセキュリティのコンプライアンスと認証に継続的に整合させることができます。

STAR 継続型は、指定された一連のセキュリティ要件に対応してクラウドサービスを継続的に監査するための必要な作業と条件を特定します。これにより、ガバナンスからインフラストラクチャまでの要素をカバ―し、クラウドサービスに、評価対象範囲における管理策の検証過程で実行する必要があるプロセスを定義することを要求します。

このプログラムは、継続的な監査を通じて、例えばセキュリティやプライバシー要件を運用に組み入れることによって、クラウドサービスにおいて必要な活動や条件が継続的に満たされるようにすることで、信頼を高めます。

CSA STAR 継続型の利点

STAR 継続型は、信頼性と透明性の両面で、従来の特定の時点での認証を改善します。

クラウドセキュリティの認証は、監査と監査の間のセキュリティ体制が維持されるという信頼に依拠することによって、クラウドサービスに対して付与されます。しかし、特定の時点での監査では、監査と監査の間にかなりの時間差があることしばしばです。これに対し、監査頻度を高めた継続的な監査を行うことで、セキュリティの状態が現実にそぐわなくなる可能性を小さくします。

これにより、ＣＳＰは継続的な監査プロセスの対象となるクラウドサービスについて、コンプライアンスの状況の細部にわたる報告ができ、「常に最新の」 コンプライアンス状況を達成できます。

CSA STAR 継続型の実現

STAR 継続型は、頻繁なテストを通じて、クラウドセキュリティ管理システムのプロセスの、より高いレベルの保証と透明性をもたらします。これにより、CSPは、利用者に対し、そのセキュリティプログラムの有効性をよりよく伝え透明性を高めるための、費用対効果の高い方法を得ることができます。

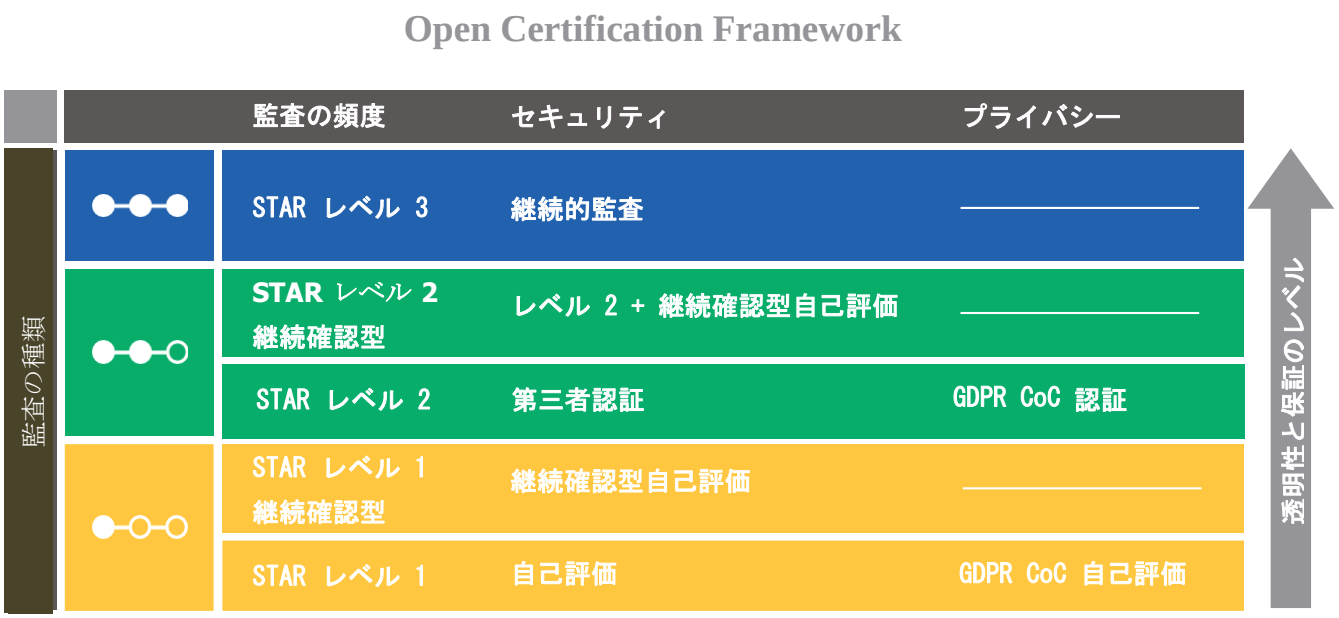

表 1: STAR 監査の頻度

STAR 継続型は、CSP の現在の STAR のレベルの上に構築することで実現できます。

- 自己評価（特定時点の評価）の実施のために CAIQ を使用する STAR レベル1 のCSP は、継続確認型自己評価を使用して一定期間にわたる管理策の有効性を実証し、STAR レベル 1 継続確認型を実現します。
- 第三者認証を取得している STAR レベル2の CSP は、継続確認型自己評価を追加することで STAR レベル2 継続確認型を実現できます。これにより、通常の STAR レベル2の次の監査時点で利用者に通知するのではなく、迅速にセキュリティプログラムの変更を利用者に知らせることができます。
- STARレベル3 のCSP は、セキュリティ管理策が常に監視・検証されていることを保証する継続的で自動化されたプロセスによって、最も高い透明性を実現します。

図 2: STAR 監査の保証

図２は各STAR レベルが提供する保証と透明性のレベルの比較を示します。クラウド利用者は、図２の示すところにより、必要な保証と透明性に関して適切な判断を下すことができます。

継続的監査について

継続的監査は、「事前に定義された一連の目標が達成されていることを確認するために情報システムを評価する継続的なプロセス」[1]です。

STAR継続型では、継続的監査のこれらの一連の目標はCSA CCMに基づいています。その個々の目標はすべて、組織の事業目標および組織の状況に関連付けられています。

目標達成度の測定は、CSA CCMの組織への実装方法に依存します-- CCMは要件を示しますが、詳細な実装方法は示しません。セキュリティ目標の達成度は、ISO 19086-1に規定されている概念であるサービス品質目標（SQO）[2]およびサービスレベル目標（SLO）[3]を定義することによって、定量的または定性的な方法で測定でき、事前に定義した頻度で評価されます。

[1] European Security Certification Framework “Continuous Auditing Certification Scheme”
[2] サービス定性目標（SQO）：「クラウドサービスの特定の定量的な特性についての，クラウドサービスプロバイダによるコミットメント」[ISO 19086-1]
[3] サービスレベル目標（SLO）：「クラウドサービスの特定の品質に関する特性についての，クラウドサービスプロバイダによるコミットメント」[ISO 19086-1]

継続的監査を受けているCSPは、最初に認証目標を設定する必要があります。それはCSA CCMに従って定義された一連のSQOとSLOで構成されており、それぞれの目標ごとに評価頻度が設定されています。クラウドサービスのセキュリティにとって重要な管理策は、頻繁な評価を伴う強力なSLO / SQOにによって表現されます。逆に、より低いリスクに関する管理策は、より弱いSLO / SQOで、より少ない頻度の評価でも許容されます。

付録Aに示されている自動測定方法や推奨監査頻度のガイドラインを使用することで、継続的監査フレームワークは、保証のレベルを実現する労力と、それを実証する労力のバランスをとります。

STAR継続型の取得方法

STAR継続型認証を取得するには3つの方法があります。

- Level 1 継続確認型：継続確認型自己評価
- Level 2 継続確認型：継続確認型評価を伴う認証/評価証明
- Level 3 継続型：継続的認証/評価証明

それぞれについて以下に詳述します。

継続確認型自己評価（レベル1）

STAR継続確認型自己評価はSTAR自己評価プログラムを拡張したものです。それは自己評価アプローチの上に作られており、CAIQ / CCMに基づく自己評価文書をより高い頻度で提出することで、被監査者がより高いレベルの保証を証明出来るようになります。

一般的なSTARレベル1自己評価は、CSPがその評価範囲（通常はクラウドサービス）を決定することから始まります。その後、CSPはCAIQまたはCCMを使用して、このクラウドサービスがセキュリティ管理策の目標をどのように実装するかを記述した自己評価文書を作成して提出します。この自己評価文書は検証のためにクラウドセキュリティアライアンスに提出され、一般公開のためにCSA STARレジストリに登録されます。

STARレベル1の自己評価の有効期間は12ヶ月です。その後、自己評価文書を再提出しなければなりません。自己評価文書の提出はすべてSTARレジストリに表示され、現行の文書以外は「廃止（deprecated）」としてマークされます。

STARレベル1継続確認型自己評価は、同じアプローチに基づいていますが、追加の要件があります。

- 提出された自己評価文書の有効期間は12ヶ月ではなく1ヶ月です。
- 提出文書は、CAIQの質問またはCCM管理策に対する「はい」、「いいえ」、または「該当なし」の回答で構成されます。より高いレベルの透明性を提供するために、組織が運用プロセスの変更を文書化することをお勧めしますが、必須ではありません。

上記の有効性要件を満たさないSTARレベル1継続確認型自己評価は、STARレベル1自己評価に格下げされます。

継続確認型評価を伴う拡張認証/拡張評価証明（レベル2継続確認型）

STARレベル2継続確認型は、第三者評価を要件とするSTARレベル2に「継続型自己評価」を追加し、CSPのより高いレベルの保証と透明性を示します。

STARレベル2では、CSPは、決定された適切な範囲に対して、CSAのレベル2プログラムの何れかにより第三者に評価されます。STAR認証、STAR評価証明、C-STARを含むレベル2プログラムは、CSA CCM、ISO/IEC 27001、AICPA トラスト・サービス基準 (TSC) の、それぞれの厳しい要求のクラウドセキュリティ基準に基づいており、CSP の評価範囲に適用されます。

STARレベル2継続確認型は、STARレベル2を達成したCSPに、第三者による監査から次の監査までの間の継続的な信頼を示すために、追加のSTAR継続確認型自己評価を提供することを要求します。自己評価プロセスが適切に実施され、かつ要求されるレベルの透明性を提供していることを確実にするために、STARレベル2の評価をする第三者認証機関は、CSPの自己評価文書を検証する責

CSPは、レベル2プログラムの達成をSTARレジストリに登録できます。

STARレベル2継続確認型の継続確認型自己評価がSTARレベル1の継続確認型自己評価で具体的に示されている有効性要件を満たさなければ、STARレベル2に格下げされます。

継続型認証/継続型評価証明（レベル3）

レベル 3 継続型認証は、ISO / IEC 27001の認証サイクル、AICPA SOC 2 Type IIレポートの監査期間による信頼を超えてクラウドサービスの保証レベルを拡張する、選び抜かれたクラウドセキュリティ評価プログラムです。

STARレベル3継続型では、すべての継続型評価が第三者である監査人の監督下で実施されることを求めます。これは、レベル2継続確認型がレベル2への追加として、CSP自身による高い頻度での自己評価提示を求めていることとは異なります。

レベル3継続型認証では、2つの段階（フェーズ）を満たすことが求められます。第一段階では、認定された第三者の評価者が、CSPの環境で管理策がどのように実行され、目標が達成されているかについての最初の監査を実行します。第一段階が正常に完了すると、CSPは継続的な評価プログラムである第二段階を開始できます。

第二段階では、求められる頻度で実行される管理策の自動および手動テストの開発のため、CSPは第三者の監査人と協力する必要があります。これらの高頻度で継続的なテストの結果は、検証と承認のために、CSPによって監査人に提供されます。

検証済みの継続的監査結果の概要は、一般公開のためにCSPのSTARレジストリに登録されます。CSAは、CSPが直接生成したいかなる証拠も受け付けません。

