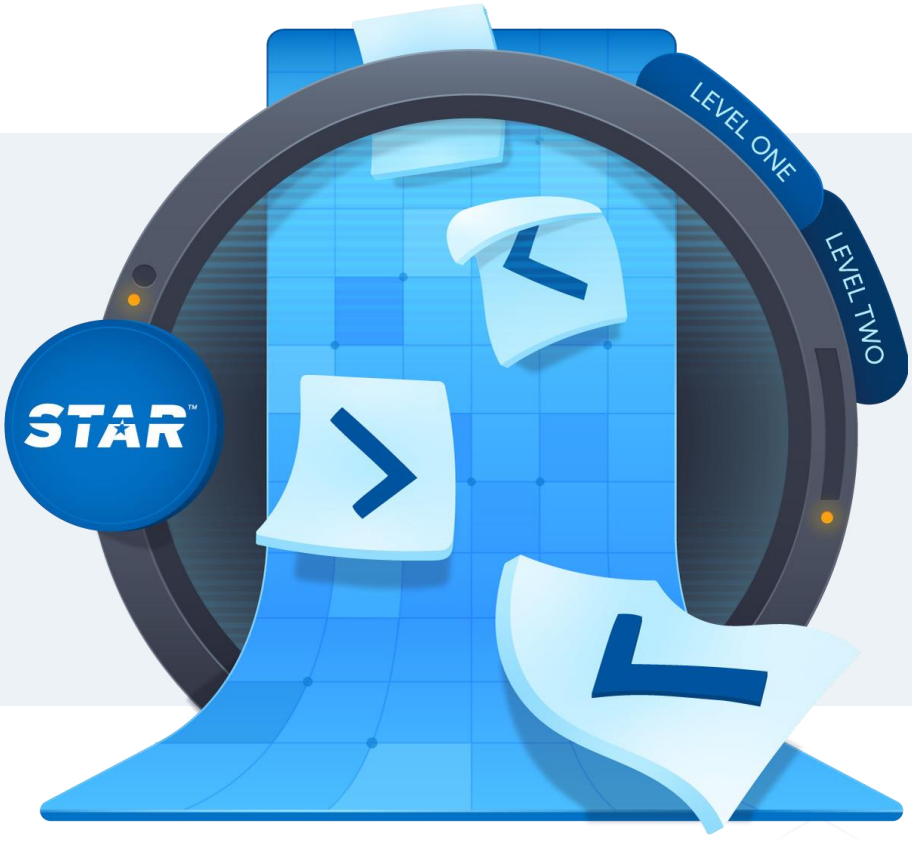
STAR Attestationのバリュープロポジション

2023年10月



日本語版提供に際しての告知及び注意事項

本書「STAR Attestationのバリュープロポジション」は、Cloud Security Alliance (CSA)が公開している「STAR Attestation Value
Proposition」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
2023年12月24日	日本語版1.0	初版発行

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス(CSAジャパン)は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1.　責任の限定
CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。
(1)　本書の内容の真正性、正確性、無誤謬性
(2)　本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3)　本書の内容に基づいて行われた判断や行為がもたらす結果
(4)　本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2.　二次譲渡の制限
本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。
ただし、以下の場合は本項の例外とします。
(1)　本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2)　本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3)　CSAジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4)　転載、再掲、複製の作成と配布等について、CSAジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3.　本書の適切な管理

(1)　本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。

(2)　本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する(組織内の利用者に順守させることを含む)ようにしなければなりません。

(3)　本書をダウンロードした者は、CSAジャパンからの文書(電子メールを含む)による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。

(4)　本書を印刷した者は、CSAジャパンからの文書(電子メールを含む)による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4.　原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

5.　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「STAR Attestationのバリュープロポジション」は、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を記します。（氏名あいうえお順・敬称略）

諸角　昌宏

Acknowledgments

Lead Authors

Doug Egan
Stephen Germain

CSA Global Staff

John DiMaria
Stephen Lumpe

目次

はじめに

概要

企業がより機密性の高い重要なデータを処理するためにクラウドサービスを利用するようになるにつれ、セキュリティおよびリスク管理チームは、クラウドサービスプロバイダが適用しているセキュリティ管理の種類と厳格さを迅速に評価し、理解するためのツールを必要としています。CSA STAR Attestationは、このようなニーズに対応するために設計されたクラウドに特化した認証プログラムです。CSA STAR Attestationは、CSAとAICPAの協力により、AICPAの基準（Trust Service Principles, AT 101）とCSA Cloud Controls Matrixを使用して、公認会計士がSOC 2業務を実施するためのガイドラインを提供するものです。

問題提起

クラウドに対する要件は、非クラウド環境とはかなり異なる可能性があり、セキュリティコンプライアンスの一般的なアプローチは、クラウドにおける保証の証拠を提供するための実行可能なソリューションにはなりません。

以下の独自の考慮が必要になります。

- クラウドコンピューティング環境の範囲の理解
- クラウド環境特有の側面をカバーするセキュリティ管理
- リスクを正しく捉えたリスクアセスメント
- 有効性を証明する監査証跡

背景

企業がより機密性の高い重要なデータを処理するためにクラウドサービスを利用するようになるにつれ、セキュリティおよびリスク管理チームは、クラウドサービスプロバイダが適用しているセキュリティ管理の種類と厳格さを迅速に評価し、理解するためのツールを

必要としています。CSA STAR Attestationは、このニーズに応えるために設計された初のクラウド専用のAttestationプログラムです。CSAのCloud Controls Matrix（CCM）に基づくSTARは、主要な標準にマッピングされたクラウド固有のセキュリティ管理策として唯一のメタフレームワークで、第三者による監査レビューを可能にすることで、セキュリティチームがクラウドへの移行を可能にするために必要なサポートと信頼を提供します。
SOC2 attestationまたは国際的な同等基準（ISAE3000など）に基づく厳格なプログラムとして、STAR Attestationは、サービス監査人による管理策のテストの説明を含む、クラウドサービスプロバイダのシステムと管理策の説明に関する強固なレポートを提供します。この報告書は、セキュリティ及びCCMの基準に関連するクラウドサービスプロバイダのクラウド特有の管理策を理解する必要がある幅広いユーザーのニーズを満たすことを意図しています。従来のSOC 2 attestationと同様に、以下の2種類の報告書があります。

- Type 1, クラウドサービスプロバイダのシステムに関する経営者の説明と、管理策の設計の適切性に関する報告書（「ある時点」の評価）。
- Type 2, クラウドサービスプロバイダのシステム、管理策の設計及び運用の有効性の適切性に関する経営者の説明についての報告書（「一定期間」の評価）

Type 1 監査は、より厳格なType 2 監査への足がかりとして使用されます。CSA STAR Attestation Type 1のステータスは、データの機密性、完全性、可用性を保護するためのポリシーと手順の徹底的な評価を通じて、クラウドセキュリティへのコミットメントを顧客に示すものです。すなわち、SOC 2 Type 1報告書に基づいてSTAR Attestationを取得した組織は、STAR Attestationのステータスを維持するためにSOC 2 Type 2報告書を提出する必要があります。STAR Attestationの有効期間は、報告書作成および提出のための基本的な有効期間に加えて、3ヶ月の猶予期間（「最大有効期間」）延長されます。

バリュープロポジション

CSA STARは、組織が情報を保護し、サイバー脅威から身を守り、リスクを低減し、情報ガバナンスとプライバシープラットフォームを強化することを可能にする一方で、複雑性を低減し、保証と透明性を向上させる統合された費用対効果の高いソリューションを提供することにより、クラウドプロバイダ、ユーザー、およびその関係者への信頼を導くことをリードする国際的に調和のとれたソリューションとして認められています。

STAR Attestationに投資している組織は、プロバイダ選定プロセスにおいて、ユーザーに対してより簡単に正当性を示すことができます。STAR Attestationを導入しているプロバイダは、RFPプロセスにおいて業界のリーダーとみなされます。
STAR Attestationは、以下のような方法で複雑さとコストの削減を促進します。

- 監査の廃止または削減
  - STAR Attestationは、SOC2とCCMに基づいています。CCMは、40以上の主要な標準、ベストプラクティス、および規制にマッピングされた、クラウド固有のセキュリティ管理に関する唯一のメタフレームワークです。CCMは現在、クラウドセキュリティの保証とコンプライアンスのデファクトスタンダードと考えられており、顧客や見込み客が監査を行ったり、長時間のアンケートを要求したりする必要性を大幅に減らしています。
  - CSPがサードパーティのインフラ（AWS/Azure/IBM/GCP/データセンター）を使用してクラウドサービスを提供し、これらのサードパーティがSTAR attestationを取得している場合、利害関係者に十分な保証を提供するだけでなく、監査やセキュリティ質問票の送付の必要性をなくすか、大幅に減らすことができます。
- サプライチェーンの評価時間の短縮
  - STAR Attestationは、クラウドプロバイダを監視・評価するための継続的で一貫した手法を提供します。
  - STAR Registryを通じて完全な可視性と透明性を提供し、クリーンで標準化されたデータを通じて実際の状況を客観的に把握することで、サプライチェーン全体のベンチマーキングに利用できます。
- RFP獲得の増加
  - STAR AttestationはSOC2+CCMに基づいており、CCMにはCAIQと呼ばれる拡張質問セットがあります。組織は、CAIQの情報を用いてRFPを作成することで、さらなる保護を得ることがよくあります。そして、RFPのインタビュー時にベンダーの回答の妥当性を検証することができます。これは、STAR Attestationレポートとともに、RFPプロセスの強力なツールとなります。
- CCMの管理策の内容は、Attestation Standard（「CCMクライテリア」）として定義された適切な基準で構成されており、TSCのセキュリティ原則の基準と同等の基準に加え、セキュリティに関連する一定の追加基準を含みます。

- SOC 2®レポートにおいて、公認会計士は、適用されるTrustサービス原則及びCCM基準に基づき、サービス組織のサービスコミットメント及びシステム要求事項が達成される合理的な保証を提供するために、管理策が効果的に運用されていたかどうかについて意見を表明します。
- STARは、時間、コスト、信頼、透明性の面で複雑さを軽減することを促進します。

結論

CSA STAR Attestationは、すべてのあらゆる規模の企業に大きなメリットをもたらします。CSA STAR Attestationを取得することで、より多くの顧客がこれらの対策の証明を求めるようになり、信頼、評判、そして新たなビジネスが生まれる可能性があります。さらに、クラウドサービスプロバイダとして以下のようなメリットもあります。

- 経営トップに可視性を提供し、クラウドセキュリティ業界および SOC2 の期待に照らして、自社のセキュリティシステムの有効性を評価できるようにします。
- クラウドサービスを最適化するために、組織の目的をどのように反映させるかを考えた監査を実施します。
- 外部のAICPA事務所が独立的に検証した判定を行い、進捗およびパフォーマンスレベルを証明します。
- 同業他社とのパフォーマンスを比較します。

さらに、クラウドサービスプロバイダの顧客にとって、CSA STAR Attestationは、実施されている管理レベルの理解を深めるものとなります。

詳細についてはこちらを参照してください
https://cloudsecurityalliance.org/star/levels/
あるいは、こちらにコンタクトしてください
info@cloudsecurityalliance.org