cloud security alliance℠

STAR 認証を公開するには

リリース 1: 2013 年 8 月 8 日

日本語版の提供について

本書「STAR認証を公開するには」は、CSAが公開している「Publicizing Your 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

本書の目的

STAR 認証の取得という成果を得たら、それを世の中に広めましょう。このガイドラインでは、認証について、関係者、つまり従業員、顧客、ビジネスパートナー、そのほか一般に公表し、告知し、宣伝するための方法を記述します。

このガイドラインは、プレスリリース、広告、マーケティング資料、ビデオ、社内向けアナウンス、ロゴ[1]、スローガン、キャッチコピーのような販促宣伝や広報の資料を作成するのに有用ですし、出版物や放送からインターネットやマルチメディア向けアプリケーション、広告やバナーにいたるメディアへの展開のためのキャッチフレーズに利用できます。

ガイドラインの利用者

このガイドラインは、以下のような幅広い潜在的な利用者を対象にします:

- 経営層
- 管理職
- 社内あるいは外部のエージェントと仕事を行っている広報、マーケティング、宣伝部門
- グラフィックデザイナ
- 出版社、ジャーナリスト
- 認定機関、認証機関、管理システム・コンサルタント（このガイドラインを顧客に伝えることを進める人）
- 認証された組織の顧客
- 認証された組織によるベストプラクティスを監視する消費者団体
- 公の知識人

STAR 認証が意味すること

[1] 必要に応じて、CSA あるいは認証機関(CB)にコンタクトしてください

製品やサービスの適合性を達成するためには、組織が ISO/IEC 27001 に従った管理システムを持っていることを保証する認証プロセスが必要です。また、CSA の CCM コントロールが取り組んでいて、STAR 能力成熟度モデルによる評価を受けていることが必要です。特に、組織に対して以下のことを期待しています:

A. 製品、サービス、プロセスに適した、また、認証の範囲に適合した管理システムを構築していること。
B. 製品に対する顧客のニーズや期待値と同時に、関連する法令および規制による要求や遵守事項、を分析し理解すること。
C. 製品やサービスの特性が、顧客および法令/規制の要求に合うように設定されていることを確実にすること。
D. 期待された結果を出す(すなわち、製品/サービスの適合性を達成し顧客満足度を確保するように、管理プロセスを確立させ、マネジメントすること。
E. 運用とプロセスの監視をサポートするのに必要なリソースが利用可能であることを保証すること。
F. 製品/サービスの定義された特性を監視し制御すること。
G. 不適合[2]を防ぐことを目標とすること、また、以下のような体系立てられた改善プロセスを持つこと:
    1. 発生した不適合を修正する（提供後に発生した不適合を含む）
    2. 不適合の原因を解析し、再発を防止するための対策を取る
    3. 顧客の不満に対応する
H. 効果的な内部監査および経営陣によるレビュープロセスを導入すること
I. マネジメントシステムの有効性を監視し、計測し、継続的に改善すること

STAR 認証が意味しないこと

1) STAR 認証が、製品/サービスではなく、組織の情報セキュリティーマネジメントシステム(ISMS)のための要件を定義していることを理解することは重要です。それは、「一貫して顧客、社内、適切な法律および規定要件に合う製品/サービスを提供する」ための組織の能力に信頼を与えるものです。

2) STAR 認証は、組織が優れた製品/サービスを提供しているか、または製品/サービス自体が ISO（または、その他の）規格か仕様の要求を満たしていることを意味するものではありません。認証されるのは管理システムです。

3) 成熟度モデルは、組織の ISMS の一部を構成する様々な要素とプロセスの成熟度を示しています。成熟度の値(ゴールド、シルバー、ブロンズ)は、セキュリティのレベルを示しているわけではなく、また、

[2] Nonconformance – Failure to fulfil specified requirements

より高い数値の組織が低い数値の組織より安全性が高いということを言っているわけではありません。組織に対して、認証結果を公表するように薦めていますが、認証に関するマーケティングの発信は間違って誘導しないようにすべきです。つまり、組織は高い成熟度の値を取ったからと言って、組織が保有する情報が低い成熟度の値の組織が保有する情報よりも本質的に安全であることを伝えるべきではありません。

すべての認証と同様に、認証が意味していることについての誤った主張を行うことは、不適合となることがあり、最終的に認証が保留されることになります。

認証の範囲

認証機関によって出されている標準に対する適合性証明書は、認証が対象とする企業活動の範囲を特定しています。

それゆえ、STAR 認証をプレスリリースする場合、マーケティングあるいは製品資料のような媒体で参照する場合、ウエブサイトに公表する場合に、認証でカバーされている組織活動の対象範囲を示すべきです。

もし、組織のプロセスの一部のみが認証によってカバーされていたり、事業部や事業所の一部のみがカバーされている場合には、すべての組織がすべての活動とプロセスを認証していたりすべての地理的な場所が認証されているというような印象を与えてミスリードすることは許されません。

このガイドラインに関して何か説明が必要なら、認証機関に問い合わせていただくか、あるいは、Cloud Security Alliance の次のメールアドレスに連絡してください。info@cloudsecurityalliance.org.