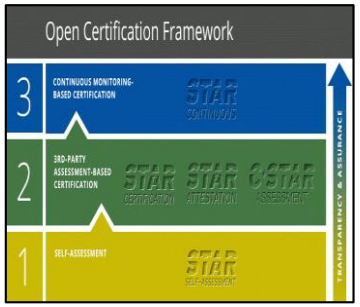
STAR認証のビジョン CCM/STAR　WGの活動

CSAジャパン　業務執行理事
CCM/STAR WG　リーダー
諸角　昌宏

Agenda



- クラウド認証の課題
- STAR認証の方向性
  - 相互認証スキーム
  - STAR　透明性と高い保証
  - STAR継続型
  - PLA行動規範の組み入れ
- ISOIEC27017との関係
- CCM/STAR WGの活動　まとめ

クラウド認証の課題

- 国ごとに固有の認証スキーム
  - ENISA：クラウド認証スキームリスト　(Cloud Certification Schemes List: CCSL)
  - ISO/IEC 27017:2015
  - 米国：連邦政府によるリスクおよび認証管理プログラム　(FedRAMP) 標準
  - 英国：政府のG-Cloud
  - シンガポール：多層クラウドセキュリティ　(Multi-Tier Cloud Security: MTCS)
  - そのほか…

  国固有の要件を組み込むことで公的分野の調達プロセスを簡素化
  多くの国で認証が必要。クラウドサービスプロバイダにとっての参入障壁
- より高いレベルの保証の要求
  - 「ある時点 (point-in-time)」と「ある期間 (period-of-time)」を対象とするアプローチに依存
  - 高リスクな重要分野を運営する組織が要求する高い保証を提供しない
- プライバシーが十分に考慮されていない
  - プライバシーとデータ保護の要件を具体的に組み込む方法について有効なガイドを提供できないならば、それらの認証スキームは機能不足になる可能性がある
- 透明性の限界
  - コンプライアンスの開示は、必ずしも透明性の提供に結びついていない
  - リスク評価の一環として、クラウドサービスプロバイダの運用の可視化を高いレベルで確保することが必要

STAR認証の方向性

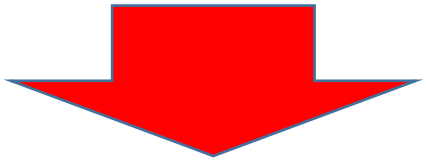
- 相互認証スキーム
- STAR　透明性と高い認証
- STAR継続型（STAR Continuous）
- PLA(Privacy Level Agreement)行動規範の組み入れ
- ISOIEC27017との関係

＊　本内容を記載した”CSA STAR PROGRAM & OPEN CERTIFICATION FRAMEWORK IN 2016 AND BEYOND”の日本語訳「CSA STARプログラムとOPEN CERTIFICATION FRAMEWORK (OCF) 2016年とその後の展望」を以下のURLから公開していますので参照してください。

http://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/11/CSA-STAR-PROGRAM-OPEN-CERTIFICATION-FRAMEWORK-IN_-2016-AND-BEYOND_J.pdf

相互認証スキーム

- CCMは、数多くの国単位、分野単位の基準へのマッピングを提供
- CCMは、ほかの基準の要件のほとんどに適合

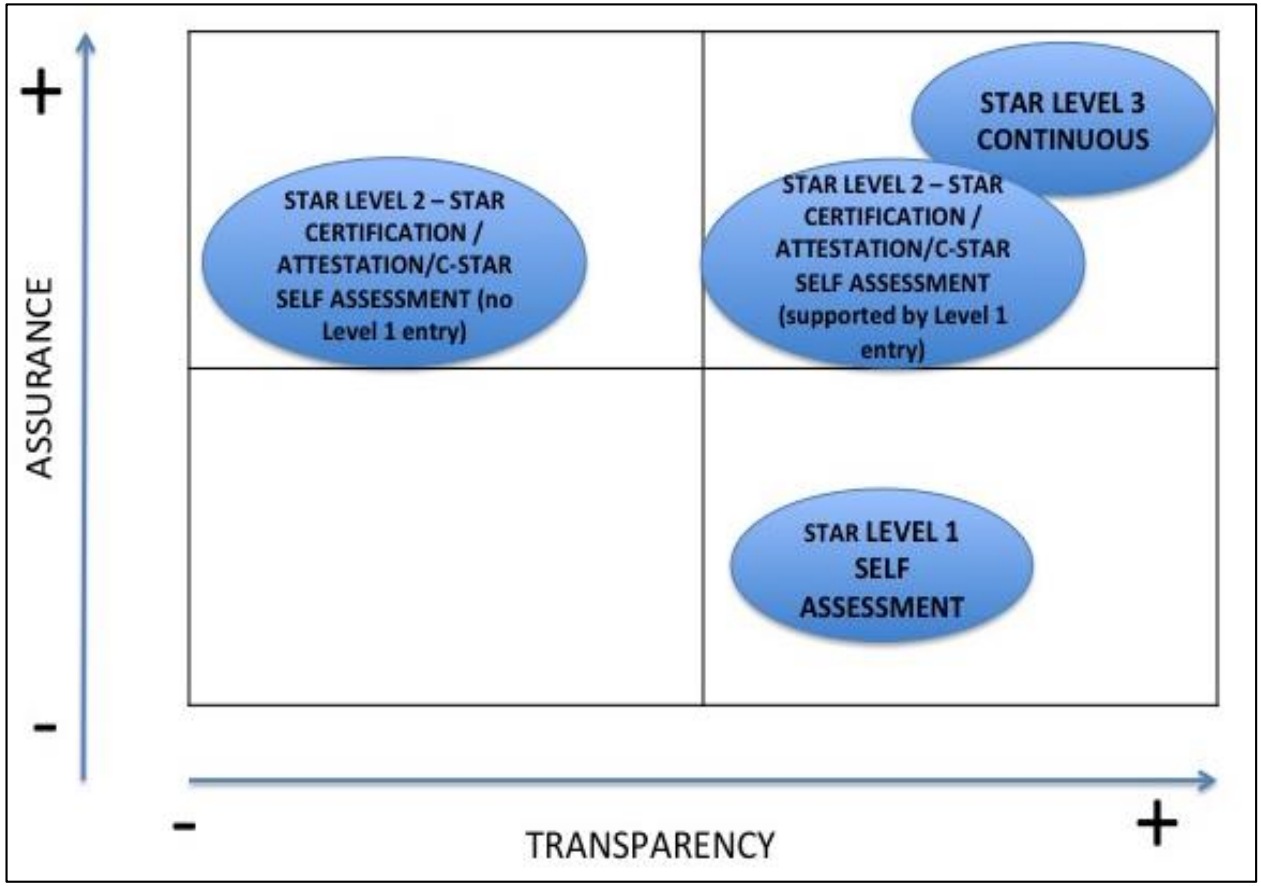


- CCMを、セキュリティ管理策の標準化指標として活用
- STARを、国際的相互認証枠組みとして活用

STAR　透明性と高い保証

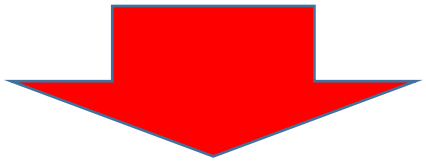
- レベル1
  - 自己評価
- レベル2
  - 第三者認証
- レベル3
  - 継続的モニタリング/監査

透明性と高い保証を実現



STAR継続型（STAR Continuous）

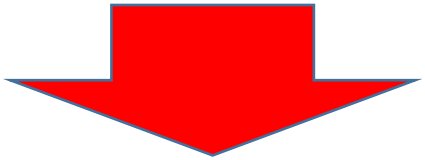
- 継続的監視・監査を実現
  - どの時点においても、適切なセキュリティ管理策が実装されていることを保証
  - 管理策が機能していることを自動的に確認可能
  - 管理策の可視性が可能



- クラウドサービスカスタマに対して、セキュリティ管理策の実施状況に関する十分に詳細な最新情報を提供

PLA(Privacy Level Agreement) 行動規範の組み入れ

- クラウド環境におけるデータ保護法令遵守に必要な要件一式を定義
- 組織のプライバシー管理策に関するアセスメント
- STARプログラムへのPLAの組み込み



- 国境を越えるデータフローが問題になる際にとりわけ有用
- 個人データ保護法令に基づく義務の順守のための手引きを提供

STAR認証、ISO/IEC27017との関係(1)

- CCM/STAR WGで検討した対応方針
  1. STAR認証と27017クラウドセキュリティ認証のポジショニング
     - CCMと27017の管理策が乖離しないようにする
     - 認証を取得する人にとって、ダブルエフォートにならないようにする
  2. STAR認証と27017クラウドセキュリティ認証の認証スキームの明確化
     - どちらも27001をベースにした認証スキーム
     - STAR認証は、管理策に加えて成熟度モデルを提供している

- CCM/STAR WGの取り組み
  1. CCMに27017のマッピングを実装
     - CCMと27017の管理策の乖離を防ぐ
     - CCMが27017を包含できるようにする
  2. STAR認証の監査工数の検討、CSA本部へのアプローチ
     - 27017とSTARを同時取得する場合、STAR認証に掛かる監査工数を削減する。可能であれば、成熟度モデルに対する監査工数の追加のみとする提案
     - 27017とSTARを同時取得する場合、 STAR取得費用をディスカウントする提案
     - STARを27017に対して追加取得する場合も上記に準ずる

STAR認証、ISO/IEC27017との関係(2)

- CSAグローバルの状況
  - 国ごとにいくつものクラウドセキュリティ認証スキームがあり、STAR認証を国際的相互認証枠組みとして活用していく
    - 27017クラウドセキュリティ認証は、One-of-themという考え方
    - 27017クラウドセキュリティ認証に対して、各国および認証機関の対応待ち

- CCM/STAR WGの今後の取り組み
  - CCMおよびSTAR認証の情報発信、普及活動
    - CCMの解説ガイドの作成を予定
      「IPA 中小企業のためのクラウドサービス安全利用の手引き」とCCMのマッピングの実施、および、解説ガイドの作成
  - 認証の課題に対する取り組み
    - STAR継続性のスタディ、普及
      - CSA本部よりリリースされ次第、できるだけ速やかに日本でも公開、普及を実施予定
    - 透明性、PLA等の普及活動

CCM/STAR WGの活動　まとめ

- 活動報告
  - CCMへのISC/IEC27017のマッピング
    - 2016年3月リリースのCCMよりマッピングを公開
    - CSAジャパン主導で実現
  - 「CSA STARプログラムとOPEN CERTIFICATION FRAMEWORK (OCF) 2016年とその後の展望」の公開
    - 「CSA STAR PROGRAM & OPEN CERTIFICATION FRAMEWORK IN 2016 AND BEYOND」の日本語訳
    - STARのビジョンおよびポジションを解説
    - 2016年11月4日公開

- 今後の活動
  - CCMの解説ガイドの作成予定
    - 「IPA 中小企業のためのクラウドサービス安全利用の手引き」とCCMのマッピングの実施、および、解説ガイドの作成
  - STAR継続性のスタディ、普及
    - CSA本部よりリリースされ次第、できるだけ速やかに日本でも公開、普及を実施予定

ありがとうございました！