cloud security alliance℠

ガイダンスドキュメント

Cloud Controls Matrix による監査

リリース 2:　2014 年 5 月 16 日

日本語版の提供について

本書「ガイダンスドキュメント　Cloud Controls Matrixによる監査　リリース2」は、CSAが公開している「Guidance Document Auditing the Cloud Controls Matrix Release2」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。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。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。

また、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
2015 年 4 月 17 日	日本語バージョン 1.0	

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有志により作成されています。

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。
http://cloudsecurityalliance.jp

2015 年 4 月 17 日

コンテンツ

1. はじめに

このドキュメントの目的は、認証機関および関連する組織に対するガイダンスを提供することです。これらの組織は、STAR 認証に関連する監査を行うか認証活動をサポートしています。

STAR 認証とそこに取り入れられているマネージメント能力モデル:

1. 認定されている組織の見込み客に対して、その組織がすでに持っている管理レベルに対するよりよい理解を与えます
2. 組織が改善したいと思っている領域を強調します
3. Cloud Controls Matrix(CCM)が必要最小限の要求になることだけでなく、このモデルを用いることで、各クラスで最も良いパフォーマンスの特性を示すことができます

したがって、マネージメント能力モデルを用いて監査をすることは、内部(ビジネスの改良)と外部(顧客への再保証と透明性)の両面で意味があることです。

このスキームの主な目的の 1 つは、クラウドサービスプロバイダの（監査）対象範囲が消費者のニーズを満たすものになっていて、サービスレベル合意書（SLA)に基づくものになっていることを保証することです。

2. このプロセスは、どのように認証された組織のクライアントに安心を提供しますか？

- ISO27001 は、組織が、顧客の要求事項、期待値および契約上の義務を理解することを要求します。 その結果、組織がその理解を達成するためのシステムを導入することを要求します。
- ISO27001 は、組織が、リスク分析を行い、顧客の期待に応える上でのリスクを特定することを要求します。
- CCM は、組織が、クラウドセキュリティのために重要な特定の問題に対応することを要求します。
- 成熟度モデルは、コントロールエリアにおける活動がどれくらい良く管理されているかを評価します。

認証がなければ、情報のセキュリティが 100%安全であることを保証できません。しかしながら、ISO27001 認証と STAR 認証は、組織が取り扱っている情報のタイプに適したシステムを持ち、それがよく管理されていて、クラウド特有の課題に対応していることを保証します。

3. 組織にスコアをつける

成熟度スコアは、組織内の改善の実施にあたっての手助けになりますが、認証書には書かれません。

組織は、コントロールに関するマネージメント能力の評価が行われる前に、すべてのコントロールが導入されており、有効に運用されていることを示さなければなりません。 組織が、コントロールエリアにおけるコントロールのどれかに重大な不適合がある場合には、そのコントロールエリアに与えられるスコアの最大値は 6 になります。

組織が監査されるとき、マネージメント能力スコアは、CCM の各コントロールエリア各々に与えられます。このスコアは、コントロールがこの領域で有効に機能していることを保証するためのマネージメント能力を示しています。CCM バージョン 3.X とバージョン 1.4 のコントロールエリアは以下になります。

コントロールエリア 3.0.1	コントロールエリア 1.4
1. アプリケーションとインターフェースセキュリティ	1. コンプライアンス
2. 監査保証とコンプライアンス	2. データガバナンス
3. 事業継続管理と運用耐障害性	3. 施設セキュリティ
4. 変更管理と構成管理	4. 人事
5. データセキュリティと情報ライフサイクル管理	5. 情報セキュリティ
6. データセンタセキュリティ	6. 法務関係
7. 暗号化と鍵管理	7. 運用管理
8. ガバナンスとリスク管理	8. リリース管理
9. 人事	9. 耐障害性
10. アイデンティティとアクセス管理	10. リスク管理
11. インフラと仮想化のセキュリティ	11. セキュリティ基盤
12. 相互運用性と移植容易性	
13. モバイルセキュリティ	
14. セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス	
15. サプライチェーンの管理、透明性、説明責任	
16. 脅威と脆弱性の管理	

コントロールのマネージメント能力は、1-15 のスケールでスコア付けされます。これらのスコアは、5 つの異なったカテゴリに分類されます。各カテゴリは、スコアのグループごとの取り組みの姿を示します。

スコア	記述
1-3	正式な取り組みなし
4-6	受身の取り組み
7-9	先を見越した取り組み
10-12	改良ベースの取り組み
13-15	最適化した取り組み

要約すると、CCM の複数のコントロールエリアに、1-15 の尺度でマネージメント能力スコアがそれぞれ与えられます。

4. 監査人用グリッド

監査人が一貫性を持ってスコアをコントロールエリアに適用することができるように、以下のグリッドには、組織が各スコアを達成するために要求されていることについて概説しています。

スコア	1 ～3	4 ～ 6	7 ～9	10 ～ 12	12 ～ 15
	正式な取り組み無し	リアクティブ	プロアクティブ	改善中	確信
証拠 / 定義	1. コントロールエリアを管理するためのシステムが設置されている証拠があります。	4. コントロールエリアの主要な運用をカバーするために実装されているシステムの証拠があります。必要に応じて、そのシステムは文書化されています。	7. コントロールエリアにおけるすべての日常的な運用をカバーする堅牢なシステムを実装しているという証拠があります。	10. コントロールエリアを管理するためのシステムが、日常的な活動と同様に緊急時の事象を管理することができるという証拠があります。	13. コントロールエリアでの経験に基づいて、コントロールエリアのオーナーは、積極的にベストプラクティスを共有し、組織の他のエリアへの展開をサポートします。
管理	2. 文書化されたシステム、あるいは、許可された作業方法のいずれかが存在するという証拠があります。	5. コントロールエリア全体の責任を理解しているコントロールエリアのオーナーが、明確に特定されています。	8. コントロールエリアが、積極的に監視され、測定され、行動が証拠に基づいて評価されているという証拠があります。	11. コントロールエリアのリスクをどのように管理するか、また、運用をどのように改善するかを決定するために、様々な情報源からの情報が検討されています。	14. コントロールエリアのオーナーは、業界や組織全体からのベストプラクティスを積極的にレビューし、コントロールエリアに適用していることを示すことができます。
追従 / 効果的	3. 幅広く認識されている受け入れ可能な作業方法の証拠があります。	6. システムが理解され、日常的に維持されているという証拠があります。	9. コントロールエリアの運用を行う重要な人が、コントロールエリアの日常的な運用を管理するために適切なトレーニングを受けていてスキルを持っているという証拠があります。	12. コントロールエリアの運用を改善する時、さまざまな利害関係者からの情報、監視、システムの測定が考慮されているという証拠があります。	15. コントロールエリアの変更は、組織の戦略的な目標に対して評価されます。

5. 監査人のためのグリッドの利用方法

このグリッドは、CCM のそれぞれのコントロールエリア(例えば、データガバナンスや施設のセキュリティ)に総合的なスコアを割り当てるのに使用しなければなりません。成熟度モデルは、コントロールに対して配置されるマネージメントプロセスの成熟度を評価することを目的としています。多くの場合、組織は、一つのコントロールエリアにあるすべてのコントロールに、共通のマネージメントアプローチを適用します。したがって、1 つの成熟度のスコアが 1 つのコントロールエリアの全体に適用されます。複数のマネージメントアプローチが取られる場合では、同じコントロールエリアにある異なったコントロールに対して異なったスコアが与えられます。このような状況では、最も低いスコアを取ります。1 つの成熟度スコアが 1 つのコントロールエリア全体に適用されると、成熟度レベルを説明することは簡単です。

6. 監査人は、コントロールエリアのスコア付けをどのようにするのでしょうか？

1. 監査人は、コントロールエリアにあるすべてのコントロールを調査し、組織が、リスクアセスメントに基づいて適切なコントロールを実装していることを確認するようにします。 コントロールを直接確認することができない場合には、クライアントは、リスクアセスメントでカバーされていない理由、適用宣言書に盛り込まれていない理由、あるいは代替コントロールを、明示する必要があります。
2. 監査人は、コントロールエリアを管理する組織の能力に関する証拠を探します。
    a. 類似の管理体制が、コントロールエリアの個々のコントロールのすべてにわたっていることが予想されます。しかしながら、かなり異なった複数の管理方法がある場合には、最も弱い管理方法に対するスコアがコントロールエリアに適用されます。
3. あるスコアを達成するためには、まず、より低いレベルにあるすべてのものから達成していかなければなりません。例えば、組織がモデルのうち低いレベルにおける不可欠の要素を達成しない限り、他により高い配点のものを持っていたとしても、低いスコアが与えられることになります。
4. クライアントがある領域で重大な NCR[1]を持っていると、可能なスコアの最大値は 6 になります。
5. そして、監査人は次のコントロールエリアに移行します。
6. 監査人が、すべてのコントロールエリアを評価すると、11 個のスコア（CCM v1.4 を使用して評価した場合）、あるいは、16 個のスコア（CCM V3.X を使用して評価した場合）になります。
7. 平均のスコアが、クライアントの総合的なレベルを割り当てるのに使用されます。

[1] NCR – Non-Conformance Report 不適合報告書

8. 組織のレポートは、システムが達成した成熟度のレベルを明示します。

注意 - コントロールの構成方法の関係で、コントロールエリアのすべてのコントロールを持っている組織は、コントロールマトリクス上かなり高いスコアになります。たとえば、リスク管理コントロールエリアでは、RI-01 は- 「組織は、リスクを受容可能なレベルにまで抑え込むために、事業のリスク管理の枠組みを構築し維持しなければならない。」と記述しています。 これは、成熟度モデルのほとんどの要素に対して評価することができ、洗練された実装として高いスコアが得られたり、不十分な管理を行うことで低いスコアに甘んじることも起こりえます。 しかしながら、コントロールエリアの他のコントロールを見ると、要求に対して、より明確であり、より詳細です。 例えば、「リスクは許容できるレベルまで軽減しなければならない。許容レベルは、リスク管理基準に基づき、妥当な解決時間枠の設定と役員による承認を経て確立し文書化しなければならない。」 について検討します。これは、モデルの上位の管理能力レベルになります。 したがって、クライアントが CCM コントロールのすべてを備えている場合、比較的よいスコアに達しないというのは難しいでしょう。
達成した能力レベルに応じて、以下のいずれかを取得します:

- アワードなし
- ブロンズアワード
- シルバーアワード
- ゴールドアワード

アワードは、コントロールエリアの平均スコアに基づいています。

- 組織の平均スコアが 3 未満の場合、アワードなしとして認証が与えられます。
- 組織の平均スコアが 3～6 の場合、ブロンズのアワードが与えられます。
- 組織の平均スコアが 6～9 の場合、シルバーのアワードが与えられます。
- 組織の平均スコアが 9 以上の場合、ゴールドのアワードが与えられます。

組織の平均スコアが 3 から 6 の場合、ブロンズレベルになります。組織の平均スコアが 6 から 9 の場合、シルバーレベルになります。組織の平均スコアが 9 以上の場合、ゴールドレベルになります。

ISO27001 は、マネージメントシステムの規格であり、定義上、組織を経営することへのシステム的な手法を要求します。したがって、組織が ISO27001 で認証されている場合、最低でもブロンズの認証を達成しないということはほとんどありません。

7. 認証の種類

評価に続いて、認証[2]をクライアントに与えます。しかしながら、認証書には成熟度レベルは記載されません。成熟度レベルは、レポートの中のみに詳細に書かれます。

8. 監査人によるコントロールエリアの監査の例

施設のセキュリティコントロールエリアを、ここでは例示として使用します。これは、比較的具体的な例になるからです（v1.4 では、このエリアに 8 つのコントロールがあります。最初の 4 つだけがここで例として上げられています）。

以下の記述は、監査人がどのようにコントロールを監査するかの簡略化した例です。監査人が行うことを詳細に記述しているわけではありません。監査方法は、監査される組織のタイプによって大幅に異なります。監査方法の枠組みは、ISO27001 による組織の顧客の期待値と契約上の義務に対する分析、および、ISO27001 による組織の総合的な情報セキュリティリスク分析によって形成されます。

コントロール	ID	記述
施設のセキュリティ-- ユーザアクセス	FS-01	オフィス、部屋、施設、セキュリティエリア内での安全でセキュリティが確保された労働環境を維持するために、ポリシー及び手順を確立しなければならない。
施設のセキュリティ-- ユーザアクセス	FS-02	利用者及び保守要員による情報資産及び情報処理機能への物理的アクセスは制限しなければならない。
施設のセキュリティ―管理されたアクセスポイント	FS-03	機微なデータ及び情報システムを保護するために、物理的なセキュリティ境界（フェンス、壁、柵、警備員、ゲート、電子的監視、物理的認証メカニズム、受付デスク、安全パトロール）を実装しなければならない。
施設のセキュリティ-- 安全なエリアの承認	FS-04	許可された者だけが立入りできるようにするために、物理的な立入り制御の仕組みによってセキュリティエリアへの入退出を制限し監視しなければならない。

1. 監査人は、同じ管理体制がコントロールエリアの中のすべてのコントロールをカバーしているかどうかを定めます。もし、たった 1 つの管理体制がコントロールエリアをカバーしている場

[2] 追加の証書発行が制度上難しい場合は、STAR 認証書は ISO27001 認証書のスコープに含めることができ、適宜に裏書きすることができる。

合には、コントロールエリアの１つ１つのコントロールすべてに対して１つの成熟度スコアのみが必要になります。

2. 次に、監査人は、すべてのコントロールが実施されているか、リスク分析と妥当性の報告書を通して正当と認められる理由により除外されているか、補完コントロールによってカバーされているかを定めます。これは、ISO27001 アセスメントで評価されるのと同じ方法で行われます。
3. 次に、監査人は、マトリックスに対してコントロールをカバーしている管理機能を見ます。最初の 3 つの要素は以下になります:
   1) コントロールエリアを管理するためのシステムが設置されている証拠がありません。
      a. 監査人は、コントロールを管理するためのなんらかの形のシステムを特定することのみを必要とします。これは、認識されているプロセスを見つけるだけです。
   2) 文書化されたシステム、あるいは、許可された作業方法のいずれかが存在するという証拠があります。
      a. 2 を達成するためには、コントロールエリアのオーナーは、プロセス、手続き、システムのいずれかが実施されていることを示す文書を提供できるか、文書化されていなくても従っているプロセス、手続き、システムの証拠を提供できるはずです。
   3) 幅広く認識されている受け入れ可能な作業方法の証拠があります。
      a. 3 を達成するためには、監査人は、システムが主要なスタッフの間でどのように運用されているか、また、それが一般的に理解されているかという幅広認知させることを定めることができます。

注意 –ISO27001 に準拠したシステムを持っているクライアントが、上記の 3 つを達成できない可能性は低いです。

   4) コントロールエリアの主要な運用をカバーするために実装されているシステムの証拠があります。必要に応じて、そのシステムは文書化されています。
      a. 4 を達成するために、監査人は、コントロールエリアのすべての重要な側面をカバーしているシステムを見ようとします。クライアントは、主要なプロセスを特定し、システムの中でそれがどのようにコントロールされているかを説明できることが必要になります。
   5) コントロールエリア全体の責任を理解しているコントロールエリアのオーナーが、明確に特定されています。
      a. 5 を達成するための鍵は、実装されているシステムを理解している人によって明確にコントロールエリアの所有と説明責任が示されることができることです。
   6) システムが理解され、日常的に維持されているという証拠があります。
      a. 6 を達成するために、監査人は、コントロールシステムが毎日の運用を行っている人に理解されているという証拠を見つけることができるべきです。

注意 –基本的な ISO27001 システムを実装している（改善の機会がある）クライアントは、4 から 6 のどれかになるべきです。

7) コントロールエリアにおけるすべての日常的な運用をカバーする堅牢なシステムを実装しているという証拠があります。
    a. 7 を達成するために、監査人は、システムが「堅牢」であり、コントロールエリアのすべての日常的な運用をカバーしているように定めることができるようにすべきです。クライアントは、システムの弱点を評価し可能な限り除去し、コントロールエリアで要求されるかもしれないプロセスと手続きの範囲を考えているという証拠を示すことが期待されます。
8) コントロールエリアが、積極的に監視され、測定され、行動が証拠に基づいて評価されているという証拠があります。
    a. 8 のために、監査人は、コントロールエリアの監視と測定が存在し、情報がレビューされ評価されていて、問題が見直される場合には行動が取られることを明確に特定できなければなりません。
9) コントロールエリアの運用を行う重要な人が、コントロールエリアの日常的な運用を管理するために適切なトレーニングを受けていてスキルを持っているという証拠があります。
    a. 組織が 9 を達成するために、監査人は、コントロールエリアの運用を行う人が、日常的な運用を効果的に行うためのシステムを理解するために必要となるスキルを持っているという証拠を見つけることができなければなりません。

注意 –.強固な ISO27701 に準拠した管理システムを持っている組織は、おそらくこのカテゴリにいるでしょう。

10) コントロールエリアを管理するためのシステムが、日常的な活動と同様に緊急時の事象を管理することができるという証拠があります。
    a. 10 を達成するために、監査人は、主要な緊急事態を特定するための分析が行われ、システムがこのような緊急事態を管理できるように実装されているという証拠を見つけなければなりません。
11) コントロールエリアのリスクをどのように管理するか、また、運用をどのように改善するかを決定するために、様々な情報源からの情報が検討されています。
    a. 11 を達成するために、監査人は、組織がコントロールエリアにおけるリスクに対して幅広くアプローチし、PESTLE 分析のようなアプローチを検討し、リスクの管理方法を理解するためにすぐそばのコントロールエリアに目も向けているという証拠を見つけなければなりません。
12) コントロールエリアの運用を改善する時、さまざまな利害関係者からの情報、監視、システムの測定が考慮されているという証拠があります。
    a. 12 を達成するために、監査人は、信頼できる利害関係者の分析が行われ、その利害関係者が適切に参画し、コントロールエリアの改善が行われていることを見つけなければなりません。また、情報の監視や測定が、弱点を特定することの手助けを行うだけでなく、改善点を伝えるのに用いられているという証拠がなければなりません。

注意 –この括りで得点のある組織は、強固なシステムを実装しているだけでなく、継続的にシステムを前向きに進めています。このカテゴリの組織は、ISO27001 のコンプライアンス要件以上のことを行っています。

13) コントロールエリアでの経験に基づいて、コントロールエリアのオーナーは、積極的にベストプラクティスを共有し、組織の他のエリアへの展開をサポートします。
    a. 13 を達成するために、監査人は、組織がコントロールエリアからの見解を集め、他のエリアの組織のパフォーマンスの改善に適用できるかどうかを検討しているという証拠を見つけることができなければなりません。
14) コントロールエリアのオーナーは、業界や組織全体からのベストプラクティスを積極的にレビューし、コントロールエリアに適用していることを示すことができます。
    a. 監査人にとって 14 を達成する鍵は、業界全体からのベストプラクティスを具体化するために積極的に組織に目を向けているという証拠を見つけることです。これは、業界全体のイニシアチブやベンチマークを行うイニシアチブに積極的に参加することを含むかもしれません。
15) コントロールエリアの変更は、組織の戦略的な目標に対して評価されます。
    a. 15 を達成するために、組織は、組織全体の戦略がコントロールエリアの運用と継続的な改善をどのように形成しているかを表明できなければならない。これは、コントロールエリアにおける運用によって理解されなければならない。

注意 –13 から 15 に得点のある組織は、組織の文化の中に情報セキュリティ管理システムを完全に組み込んでいることが期待されます。そして、業界において指導的な役割を果たすことが期待されます。