「クラウドセキュリティの基本:
ベストプラクティスとポイント」

一般社団法人　日本クラウドセキュリティアライアンス

理事　諸角昌宏

CSAリサーチフェロー、 CCSP、CCSK、CCAK

2024年2月17日

プロフィール

- 一般社団法人日本クラウドセキュリティアライアンス　理事
- **Cloud Security Alliance リサーチフェロー**
- **CSA Authorized Instructor**
- **CCSK,CCSP,CCAK**　～クラウドセキュリティ・ファンのページ～フェースブックグループ
  https://www.facebook.com/groups/264458864908859/

本日のアジェンダ

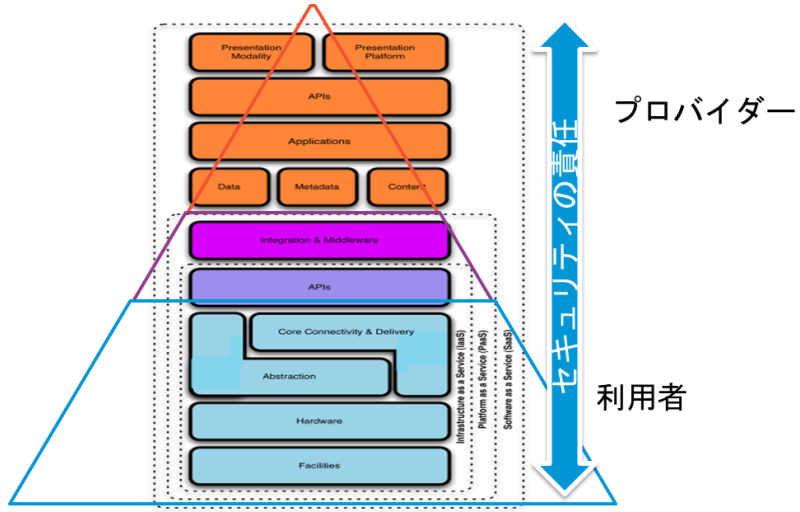
1. クラウドセキュリティの基本である責任共有モデル
2. クラウド利用者のセキュリティ対応における課題と対策
3. クラウド利用者がクラウドサービスのセキュリティを評価する際の課題と対策
4. CSA が提供する評価フレームワーク
5. クラウドサービスのセキュリティ評価方法
6. CCAK(Certificate of Cloud Auditing Knowledge)　概要
7. まとめ

1. クラウドセキュリティの基本である責任共有モデル

クラウドセキュリティの基本

責任共有モデル

- クラウド事業者は、一定のリスクに対する責任を負い、クラウド利用者はその先のすべてに責任を持つ
  - Security In the Cloud
  - Security Of the Cloud



（クラウドコンピューティングのためのセキュリティガイダンス　V3.0から引用）

- **クラウド利用者は、リスクを所管する最終的な責任（説明責任）を負っており、**クラウド事業者にリスク管理の一部を転嫁しているに過ぎない。
  - クラウド利用者の説明責任　＝　利用者の責任範囲のセキュリティ対策　＋　事業者の責任範囲のセキュリティ評価
  - クラウド事業者の説明責任　＝　利用者との契約の履行

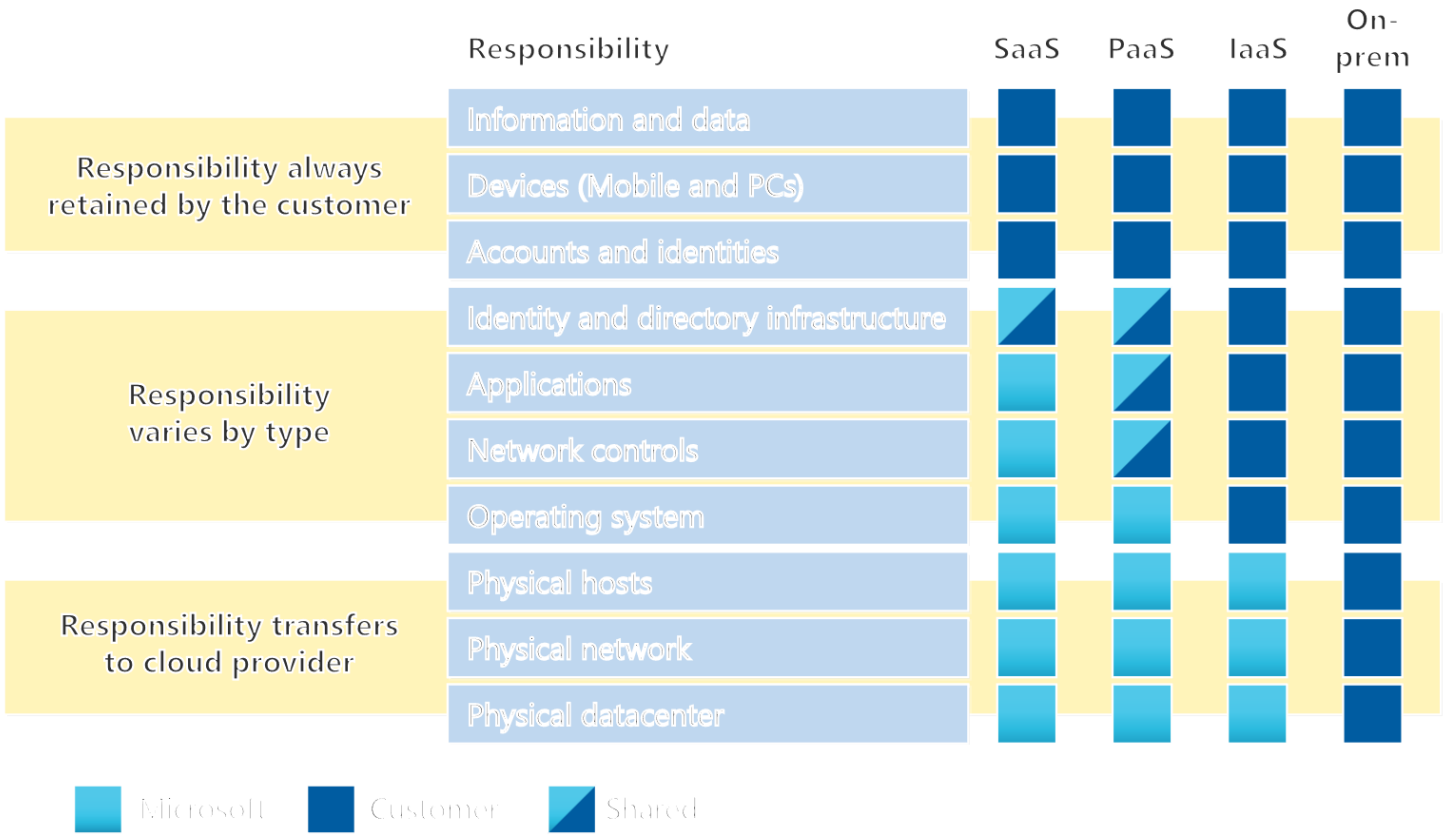
責任共有モデルにおける責任範囲

責任共有モデルの3つのカテゴリ

① すべてのサービスモデルにおいてクラウド利用者が責任を持つ

② クラウド利用者とクラウド事業者がサービスモデルによって責任範囲が決まる

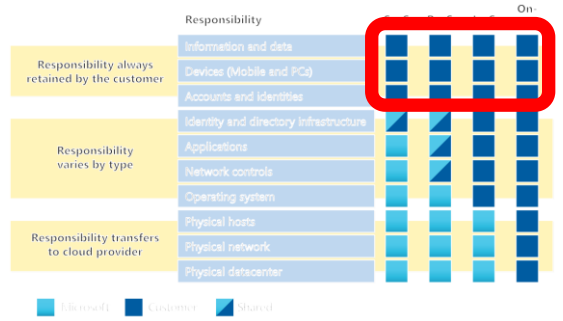
③ すべてのサービスモデルにおいてクラウド事業者が責任を持つ



引用：https://learn.microsoft.com/ja-jp/azure/security/fundamentals/shared-responsibility

責任共有モデルのカテゴリ　①

- すべてのサービスモデルにおいてクラウド利用者が責任を持つ



- カテゴリ①に含まれるもの
  - **データ、情報ガバナンス**
  - **アイデンティティ、アクセス管理（IAM)**
  - **クライアントセキュリティ**

- クラウドを利用するにあたって、
  クラウド利用者が設定、管理、監視等
  の責任を持つ。
  クラウド事業者は、環境を用意
  右図：Salesforceの例

Salesforce

- Salesforceのインフラストラクチャ、プラットフォーム、アプリケーションの安全な設計と実装を推進
- アウトバウンドおよびインバウンドのファイアウォールルールの管理
- Salesforce の機密資産に対する 2 要素認証（2FA）の実施
- テナントごとのデータ隔離の徹底
- プロアクティブなコードスキャンおよび侵入テストの実施
- サードパーティによるセキュリティ評価および監査実施
- 業界標準に準拠した管理の実施
- Salesforce 資産の継続的な監視とインシデント対応の実施

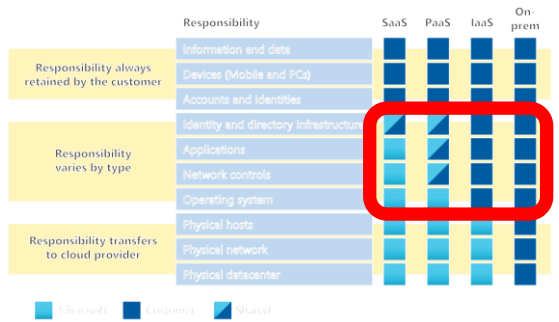
お客様

- HTTPS や SFTP などの安全な通信プロトコルの利用
- アプリケーションレベルのアクセス制御の徹底（例：IP 許可リストや ID 検証の使用）
- 顧客が管理する機密性の高いインターフェースへのMFAの導入
- 安全性の高いユーザープロビジョニングプロセスにそって、適切な役割と権限の付与
- タイムリーに監査ログの収集・分析
- カスタムコードの安全な設計と実装の徹底
- サードパーティとの統合および拡張機能の安全な調達、導入、および維持保守の徹底
- 関連するセキュリティ関連の基準および規制に準拠
- お客様およびカスタムサードパーティの統合資産を継続的に監視し、インシデントに対応
- 不正利用の防止、不正検知、防止策の導入

引用：https://help.salesforce.com/s/articleView?id=000389698&type=1

責任共有モデルのカテゴリ　②

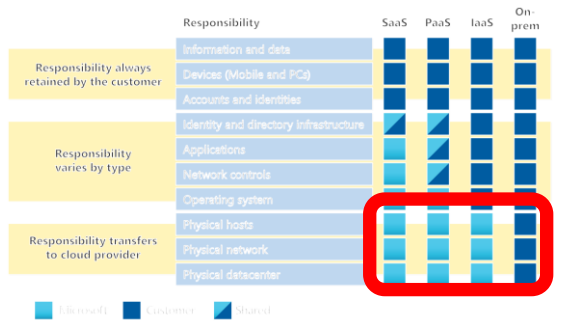
- クラウド利用者とクラウド事業者がサービスモデルによって責任範囲が決まる



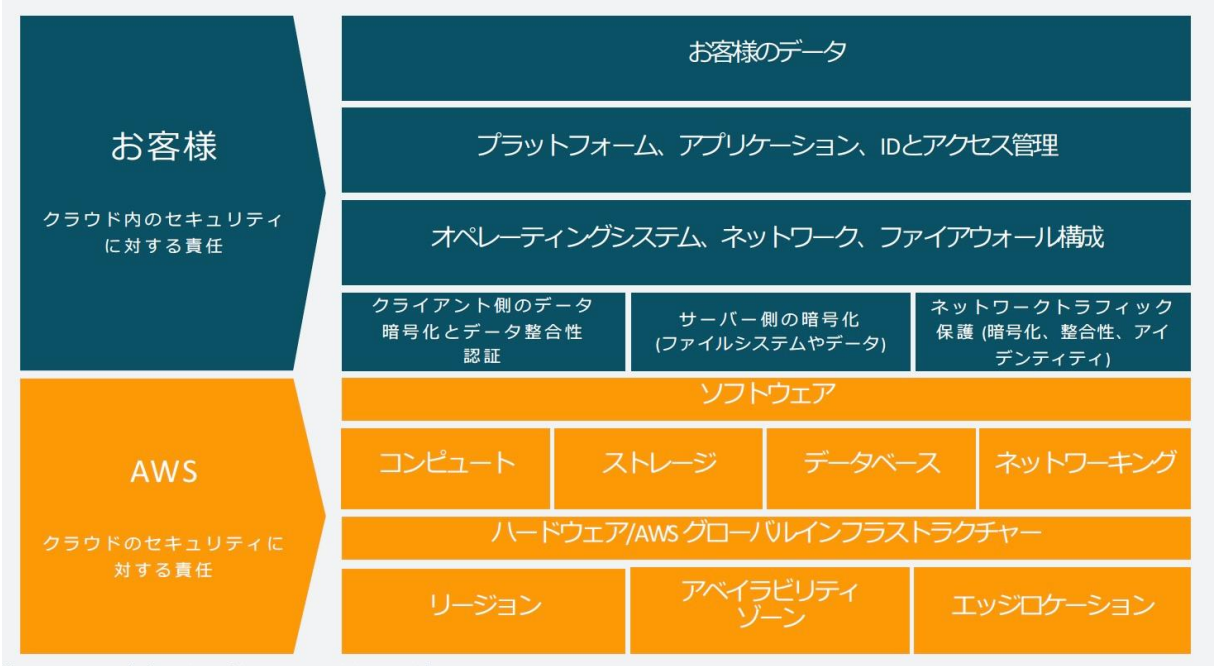
- IaaS/PaaS
  - クラウド利用者は、独自に**セキュリティを作り込む**必要がある境界防御で守られている環境から、クラウド環境に移行するにあたってのセキュリティの作り込みが必要
  - クラウド利用者は、クラウド事業者が提供する**クラウドサービスのセキュリティを評価**する必要がある
- SaaS
  - 基本的に、クラウド利用者は、クラウド事業者が提供する**クラウドサービスのセキュリティを評価**する必要がある

責任共有モデルのカテゴリ　③

- すべてのサービスモデルにおいてクラウド事業者が責任を持つ



- 基本的に、クラウド利用者は、クラウド事業者が提供するクラウドサービスのセキュリティを評価する必要がある
  - インフラストラクチャセキュリティ
    右図：AWSの責任範囲



引用：https://aws.amazon.com/jp/compliance/shared-responsibility-model/

責任共有モデルにおけるクラウド利用者の２つの課題

1. クラウド利用者のセキュリティ対応（実装）における課題

2. クラウド利用者がクラウドサービスのセキュリティを評価する際の課題

2. クラウド利用者のセキュリティ対応における課題と対策

クラウド利用者のセキュリティ対応の課題

- CSA Top Threat (重大脅威)レポートから振り返ってみる

- 2017年から2019年　動向
- 2019年から最新（2022年）動向

CSA Top Threatの歴史(1)

2010年（Top Threats）

1. Abuse and Nefarious Use of Cloud
   クラウドコンピューティングの不正および犯罪目的の利用
2. Insecure Interfaces and APIs
   安全ではないインターフェースおよびAPI
3. Malicious Insiders
   悪意ある内部者
4. Shared Technology Issues
   共有技術問題
5. Data Loss or Leakage
   データ喪失または漏えい
6. Account or Service Hijacking
   アカウントハイジャック、サービスハイジャック
7. Unknown Risk Profile
   未知のリスクのプロファイル

2013年（The Notorious Nine）

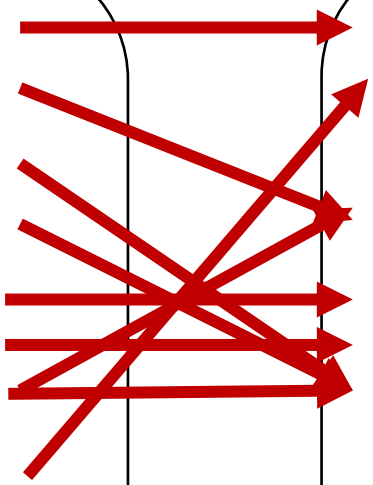
1. Data Breaches
   データ侵害
2. Data Loss
   データ喪失
3. Account Hijacking
   アカウントハイジャック
4. Insecure APIs
   安全ではないAPI
5. Denial of Service
   DoS攻撃
6. Malicious Insiders
   悪意ある内部者
7. Abuse of Cloud Services
   クラウドサービスの不正利用
8. Insufficient Due Diligence
   不十分なデューデリジェンス
9. Shared Technology Issues
   共有技術問題

注意：翻訳版の提供無し

CSA Top Threatの歴史(2)

2017年（Treacherous 12
危険な12 の落とし穴）

1. データ漏洩(Data Breaches)
2. 不十分なアイデンティティ・認証情報・アクセス管理
3. API のセキュリティ欠陥
4. システムとアプリケーションの脆弱性
5. アカウントの乗っ取り
6. 悪意ある内部者
7. 標的型攻撃の脅威（APT）
8. （CSP)データ喪失
9. 不適切なデューデリジェンス
10. クラウドサービスの誤用・悪用
11. DoS 攻撃
12. 共有技術の脆弱性



2019年（11の悪質な脅威）

1. データ侵害(Data Breaches)
2. 設定ミスと不適切な変更管理
3. クラウドセキュリティアーキテクチャと戦略の欠如
4. ID、資格情報、アクセス、鍵の不十分な管理
5. アカウントハイジャック
6. 内部者の脅威
7. 安全でないインターフェースとAPI
8. 弱い管理プレーン
9. メタストラクチャとアプリストラクチャの障害
10. クラウド利用の可視性の限界
11. クラウドサービスの悪用・乱用・不正利用

CSA Top Threatの歴史からわかること（2017~2019）

1. 「一般的な脅威」から「現実に即した脅威」への変化
   - 第3回（2017年）までのTop Threatは、クラウドに対する一般的な脅威、リスク、脆弱性に着目
   - 第4回（2019年）では、一般的な脅威等に関するものはあまりフォーカスされなくなってきている

2.クラウド利用者に起因する脅威の増加！

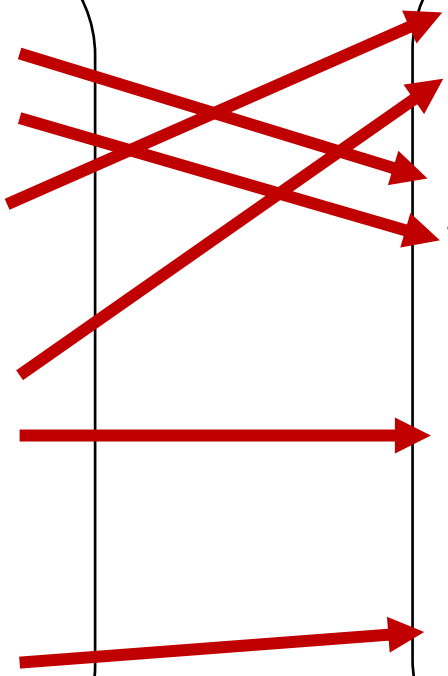
- クラウドに対する利用者の理解の成熟度の向上
- プロバイダ責任に対する脅威の順位の低下（**No worry to CSPの傾向**）
  （第3回（2017年）の図の青色項目）

	第3回（2017年）	第4回（2019年）
利用者	2, 6, 9	2, 3, 4, 6, 8
プロバイダ	8, 11, 12	
両方	1, 3, 4, 5, 7, 10	1, 5, 7, 9, 10, 11

CSA Top Threatの歴史(3)

2019年（11の悪質な脅威）

1. データ侵害(Data Breaches)
2. 設定ミスと不適切な変更管理
3. クラウドセキュリティアーキテクチャと戦略の欠如
4. ID、資格情報、アクセス、鍵の不十分な管理
5. アカウントハイジャック
6. 内部者の脅威
7. 安全でないインターフェースとAPI
8. 弱い管理プレーン
9. メタストラクチャとアプリストラクチャの障害
10. クラウド利用の可視性の限界
11. クラウドサービスの悪用・乱用・不正利用



2022年（パンデミック11）

1. 不十分なアイデンティティ、資格情報およびアクセスとキーの管理 (4)
2. セキュアでないインターフェースやAPI(7)
3. 設定ミスと不適切な変更管理(2)
4. クラウドセキュリティのアーキテクチャと戦略の欠如(3)
5. セキュアでないソフトウェア開発
6. セキュアでないサードパーティーリソース
7. システムの脆弱性 (8)
8. 予想外のクラウドデータ公開
9. サーバレスやコンテナワークロードの構成ミスや悪用
10. 組織的な犯罪、ハッカーとAPT(11)
11. クラウドストレージデータ流出

CSA Top Threatの歴史からわかること（2019~2022）

1. プロバイダ側のみに起因する脅威は引き続きゼロ
   - 利用者に起因する脅威はがセキュリティ責任を持つ項目は継続して増加

	第3回（2017年）	第4回（2019年）	第5回（2022年）
利用者	2, 6, 9	2, 3, 4, 6, 8	1, 4, 6
プロバイダ	8, 11, 12		
両方	1, 3, 4, 5, 7, 10	1, 5, 7, 9, 10, 11	2 3 5 7 8 9 10 11

2.「より具体的な脅威」に移行

- 2022年で新たに入ってきたもの
  - セキュアでないソフトウェア開発、セキュアでないサードパーティーリソース
  - 予想外のクラウドデータ公開、クラウドストレージデータ流出　← データ侵害

3.「クラウドネイティブの脅威」に着目

- 2022年で新たに入ったもの
  - サーバレスやコンテナワークロードの構成ミスや悪用

CSA Top Threatの歴史からわかること（まとめ）

1. プロバイダの管理下にあるクラウドセキュリティの課題は下がっている
   - 第3回（2017年）までのTop Threatは、クラウドに対する一般的な脅威、リスク、脆弱性に着目
   - 第4回（2019年）では、「一般的な脅威」から「現実に即した脅威」への変化
   - 第5回（2022年）では、「**より具体的な脅威**」に移行。新しいテクノロジーに絡む脅威に着目
2. 利用者がセキュリティ責任を持つ項目が継続して重大脅威としてリストアップ
   - **クラウド利用者が弱点であることを指摘**
   - 利用者が直接コントロールできる状況に焦点を当ててきている
   - 不十分なアイデンティティ管理、設定ミス等は引き続き上位にランク。
     - セールスフォースの設定問題(2011)
3. 新しいテクノロジーに基づく脅威
   - サーバレスやコンテナワークロードの構成ミスや悪用
   - アジャイル、DevOpsなどセキュアなソフトウエア開発
   - **プロバイダ管理責任が大部分となる**

クラウド利用者のセキュリティ対応における対策

- 例）Salesforce 設定問題
  - 利用者の設定の問題で決着。一時は、脆弱性とか互換性の問題という議論が行われた。
  - 日本ではNISC、金融庁などが注意喚起。でも、海外での注意喚起はあまり見られない。
  - 欧米では、ブログ等を使ったコミュニティで情報交換している。
  - 単純に利用者のリテラシーの問題で片づけるわけにはいかない。クラウドサービスの最新情報を常にキャッチして対応することが必要
  - 考えるべきは、今までのアプリケーション管理の考え方は通用しない。
    - 安定バージョン/最新バージョンという考え方はクラウドでは成り立たない。クラウドサービスは、最新かつ最高と考えられるもののみを提供する。これに、利用者は追従しなければいけない。そのためには、プロバイダからのリリース情報等をしっかり把握・理解し、必要な対策を取っていく必要がある。
  - **ただし、難しすぎる → 簡単化、自動化が必須 → CSPM、SSPM、CNAPPなどの利用。あるいは、プロバイダが提供するソリューションを利用（セキュリティはソフトウエアで解決する）**

3. クラウド利用者がクラウドサービスのセキュリティを評価する際の課題と対策

クラウドサービスのセキュリティ評価：５つの課題　(1)

1. チェックリスト作成の課題
   社内のセキュリティ基準に基づいてチェックシートを作成
   - クラウドサービスの評価として十分なのかが明確にできない
   - 企業で使うたくさんのクラウドサービスを1つ1つ評価していくのは非常に難しい
   - クラウドサービスごとに異なったセキュリティレベルやセキュリティの成熟度
   - ある程度統一した基準でクラウドサービスを評価できないものか

2. SaaSサービス評価の課題
   - クラウドサービスごとに異なったセキュリティレベルやセキュリティの成熟度
     - IaaS/PaaSは、クラウドサービスプロバイダが限定されるし、セキュリティレベルに大きな差はない
   - SaaSを利用する部門ごとに必要とされるセキュリティレベルもまちまちとなる

クラウドサービスのセキュリティ評価：５つの課題　(2)

3. クラウドセキュリティ認証の限界
   - 第三者認証の結果では、評価の信頼性は高いものの透明性は低い
   - 認証が取れているでは不十分。セキュリティの中味を知る必要がある

4. 契約内容の評価の課題
   - クラウドにおける契約は、基本的にクラウドプロバイダが出してくる契約事項に対してクラウド利用者側が許容できるかどうかを判断
   - 契約内容をしっかりと理解し、自らの要求事項を満たしているかどうかを評価

5. プロバイダの課題
   - 利用者からの問い合わせに1つ1つ回答していかなければならない
   - クラウドプロバイダが、セキュリティ情報を公開すれば、クラウド利用者はそれを見て評価することができるが、日本のプロバイダでセキュリティ情報を公開しているところが非常に少ない

クラウドサービスのセキュリティ評価方法　(1)

1. チェックリストを作成し、クラウドプロバイダに確認する方法
   - クラウド利用者側でチェックリストを作成し、クラウドプロバイダに回答を求める方法
     一般的には、標準として公開されている情報に基づいてチェックリストを作成：
     ISO/IEC 27001、SOC2、ISO/IEC 27017, クラウド情報セキュリティ管理基準、CCM、CAIQ、CAIQ-Lite

   - 利点
     - 利用者側が、独自の内容および形式で行うことができる。組織の要求事項に沿った形で処理が可能
     - クラウド利用者自らのリスク評価に基づいて詳細な評価が可能
   - 欠点
     - チェックリストを作成するために非常に大きな時間と工数が必要
     - オンプレをベースにしたチェックリストではあまり意味がない
     - クラウドセキュリティに精通した専門家が必要

クラウドサービスのセキュリティ評価方法　(2)

2. クラウドプロバイダが公開している情報を元に評価する方法
   - クラウドプロバイダが自社のホームページやホワイトペーパー等で公開しているセキュリティ情報を利用する方法

   - 利点
     - 情報をいつでも確認できるため、クラウドプロバイダからの返答待ちというようなことが起こらない
     - 標準に従って情報を公開しているので一元化した評価が可能（特にプロバイダには利点）
     - 最新の状況が利用可能
   - 欠点
     - プロバイダの公開情報を利用者の要求事項に適用させることが必要
     - クラウドセキュリティに精通した専門家が必要
     - 日本では、セキュリティ情報を公開しているクラウドプロバイダが非常に少ない

クラウドサービスのセキュリティ評価方法　(3)

3. CASBが提供しているスコアを使用する方法
   - CASBベンダーが提供しているスコアを用いて、利用者側で評価する方法である。スコアをそのまま使うという簡単な利用ができる。

   - 利点
     - 簡単
     - CASBベンダーが様々な角度から評価してスコア付けしているので信頼性が高い
   - 欠点
     - 一般的な評価によるスコア付け
       クラウド利用者のリスクアセスメントを考慮したスコアではない
     - 日本のクラウドサービスは評価されていないケースが多いようである
     - CASBの購入が必要（そもそもCASBの導入の要件になるのかどうか）。有料。

クラウドサービスのセキュリティ評価方法　(4)

4. VRM、TPRMを利用する方法
   - VRM（vendor risk management）、TPRM（third-party risk management）ベンダーのリスク管理をサービスとして評価してくれるもので、クラウドサービスの評価も行う

   - 利点
     - クラウド利用者が独自にチェックリストを作成する工数を大幅に削減
     - クラウドサービス導入後も継続的に評価できる
     - カスタマイズも可能であるので、クラウド利用者にあった評価が可能
   - 欠点
     - 比較的新しいサービスなので、ベンダーの選定を注意する必要がある
     - 日本のクラウドサービスに対するカバレッジは低い
     - 有料

4. CSA が提供する評価フレームワーク CCM、CAIQ、CAIQ-Lite、STAR認証とは？

CCM、CAIQ、CAIQ-Lite：　一言でいうと！

- **CCM（Cloud Control Matrix）**
  - CSAが提供するクラウドセキュリティ管理策集
  - 17ドメイン、197の管理策（V4.0.5）
- **CAIQ（Consensus Assessment Initiative Questionaire）**
  - CCMの各コントロールの内容をブレークダウンし、チェックリスト化
  - 質問数
    - 261個　(V4.0.2)
- **CAIQ-Lite**
  - CAIQの縮小版
  - 以下の方針に基づく厳選された内容
    1. CSA本部において、CAIQ-Liteのさまざまなバージョンを考案し、メンバー間で共有し内部研究を実施
    2. クラウドサービスを評価する利用者からのフィードバックを入手
    3. 600人以上のITセキュリティ専門家による統計分析を行い、クラウドサービスの評価を行う際にCAIQのどの質問が最も適切かの判断を実施

CCM、CAIQ、CAIQ-Liteの利点（4つのポイント）

1. タダ（無料）

- 商用利用でない場合、無料で利用可能
- CSAのウエブサイトから自由にダウンロード可能
- 日本語版はCSAジャパンのウエブサイトから自由にダウンロード可能

2. グローバル

- グローバルに通用する。グローバルに同じ内容で提供
  （CCM V3.0.1やCAIQ V3.0.1は10か国語に翻訳提供）
- グローバルに展開している企業は、統一したセキュリティ基準で評価した内容を各国で提供可能

3. クラウドセキュリティに特化

- 提供されている管理策などは、すべてクラウドサービスおよび関連する技術
- チェックリストを作成する際、チェックリストの網羅性を高めることが可能

4. 透明性

- 自己評価結果を公開するサイト（STAR Registry）を用意。STAR Registryも無償で利用可能

CCMの内容　(1)

ドメイン

管理策の内容

サービスモデルとの対応

アーキテクチャの適用レイヤ

CLOUD CONTROLS MATRIX VERSION 4.0.2

Control Domain	Control Title	Control ID	Control Specification	Typical Control Applicability and			Architectural Relevance - Cloud Stack Components					
				IaaS	PaaS	SaaS	Phys	Network	Compute	Storage	App	Data
Audit & Assurance - A&A												
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Shared	Shared	Shared	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
監査・保証	監査・保証のポリシーと手続き	A&A-01	監査・保証のポリシーと手順と基準について確立、文書化、承認、伝達、適用、評価、維持を少なくとも年1回レビューする。	Shared	Shared	Shared	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
監査・保証	独立した評価	A&A-02	少なくとも年1回、関連する基準に従って独立した監査および保証評価を実施する。	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE

CCMの内容　(2)

対応者/部門

言語選択

cs	Organizational Relevance									
Data	Cybersecurity	Internal Audit	Architecture Team	SW Development	Operations	Legal/Privacy	GRC Team	Supply Chain Management	HR	Language
TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	EN
TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	JP
TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	EN
TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	JP
TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	EN

注）「言語選択」のフィルターにより、「日本語」「英語」あるいは「両方」の選択が可能

CCMの内容　(3)

実装者向けのガイドライン

実装者向け
ガイドライン

CCM CLOUD CONTROLS MATRIX v4.0.10

Control Domain	Control Title	Control ID	Control Specification	Implementation Guidelines
Audit & Assurance - A&A				
Audit & Assurance	Audit and Assurance Policy and Procedures	**A&A-01**	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Both the cloud service provider (CSP) and cloud service customer (CSC) should develop a "customized integrated framework" of audit and assur This framework should incorporate/demonstrate compliance to leading industry standards and self-imposed business requirements while providi controls to assess the respective cloud environment and corresponding services. At a minimum, audit and assurance policies and procedures should include: a. Audit and assurance functions indicating purposes, responsibilities, authorities, and accountabilities to ensure organizational independence, professional care, audit objectivity, and proficiency, b. Audit and assurance plans, c. Audit development policies and procedures to determine criteria and assertions against which the subject matter will be assessed, quality assurance and supervision, sufficient and appropriate evidence, in accordance with commonly accepted frameworks and audit best practices, d. Audit reporting to communicate audit results and findings, e. Follow-up activities to monitor audit findings implementation progress
監査・保証	監査・保証のポリシーと手続き	**A&A-01**	監査・保証のポリシーと手順と基準について確立、文書化、承認、伝達、適用、評価、維持を少なくとも年1回レビューする。	クラウドサービスプロバイダ（CSP）とクラウドサービスカスタマ（CSC）両者は、監査と保証のポリシーと手順について「カスタマイズされた 発すべきである。 このフレームワークは、各クラウド環境と対応するサービスを評価するために、管理策の適切な範囲を提供しながら、主要な業界標準や自から を、組み込む／証明すべきである。 監査・保証のポリシー及び手続は、最小限、以下を含むべきである。 a. 組織としての独立性、専門的な配慮、監査の客観性、熟練度を確保するための、目的、責任、権限、説明責任などを示した監査や保証機能 b. 監査および保証計画、 c. 監査対象が評価される基準及び主張を決定するための監査展開方針及び手順、品質保証及び監督、一般的に公正妥当と認められたフレーム クティスに従った証拠

... | Introduction | CCM | Implementation Guidelines | Auditing Guidelines | ...

CCMの内容　(4)

監査者向けのガイドライン

監査者向け
ガイドライン

CCM CLOUD CONTROLS MATRIX v4.0.10

Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines
Audit & Assurance - A&A				
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update	1. Examine policy and procedures to confirm content adequacy in terms of purpose, authority and accountability, responsibilit communication, reporting, and follow-up. 2. Examine audit charter and determine if independence, impartiality, and objectivity are guaranteed. 3. Examine policy and procedures for evidence of review at least annually.
監査・保証	監査・保証のポリシーと手続き	A&A-01	監査・保証のポリシーと手順と基準について確立、文書化、承認、コミュニケーション、適用、評価、維持を少なくとも年1回レビューする。	1.ポリシーと手順を検証し、目的、権限と責任、責任、計画、コミュニケーション、報告、フォローアップの観点から、内容 する。 2. 監査基本方針を検証し、独立性、公平性、客観性が保証されているかどうかを判断する。 3. 方針と手続を検証し、少なくとも年1回、レビューの証拠を確認する。
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	1. Examine the process to determine standards and regulations applicable to the organization's systems and environments. 2. Determine if the organization maintains and reviews a list of such standards and regulations. 3. Determine if senior management exercises oversight over the independence of the assessment process. 4. Determine if the audit plan is informed by previous assessments, and is scheduled on an annual basis.
監査・保証	独立した評価	A&A-02	少なくとも年1回、関連する基準に従って独立した監査および保証評価を実施する。	1. 組織のシステムと環境に適用される標準と規則を決定するためのプロセスを検証する。 2. 組織がそのような規格や規則のリストを維持し、レビューしているかどうかを判断する。 3. 上級管理職が評価プロセスの独立性を監督しているかどうかを判断する。 4. 監査計画が、前回の評価から情報を得ており、年次ベースで計画されているかどうかを判断する。
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	1. Examine the process for determining the risks applicable to the organization's systems and environments. 2. Determine if a list of such risks is maintained and reviewed. 3. Determine if senior management exercises oversight over the applicable risks. 4. Determine if the audit plan is risk-based, and is scheduled on an annual basis.
監査・保証	リスクベースの計画評価	A&A-03	リスクベースの計画とポリシーに従って、独立した監査と保証評価を実施する。	1. 組織のシステムと環境に適用されるリスクを決定するプロセスを検証する。 2. そのようなリスクのリストが維持され、レビューされているかどうかを判断する。 3. 上級管理職が該当するリスクを監督しているかどうかを判断する。 4. 監査計画がリスクベースであり、年次ベースで計画されているかどうかを判断する。

Introduction | CCM | Implementation Guidelines | Auditing Guidelines | Scope ...

CCMの内容　(5)

他基準とのマッピング

他基準とのマッピング

CCM CLOUD CONTROLS MATRIX v4.0.5

				CIS v8.0				
Control Domain	Control Title	Control ID	Control Specification	Control Mapping	Gap Level	Addendum	Control Mapping	Gap
Audit & Assurance - A&A								
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	8.1	Partial Gap	Recommend the full V4 control specification to be used to close the gap. Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (8.1) 'Establish and maintain an audit log management process', 'Review and update documentation annually'.	12.1 12.1.1 12.11	Part
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	7.2	Partial Gap	Recommend the full V4 control specification to be used to close the gap. Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (7.2) 'Establish and maintain a risk-based remediation strategy'.	No Mapping	Ful
Audit & Assurance	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful
Audit & Assurance	Audit Management Process	A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful
Audit & Assurance	Remediation	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful

他基準： CIS, PCIDSS, ISO/IEC27001/02/17/18, NIST SP800-53 rev5, etc.

CAIQの内容　(1)

CCMのコントロールを必要に応じて複数の質問に分解している

CSPが自己評価した結果を記載

CAIQ CONSENSUS ASSESSMENTS IN[illegible]TIVE QUESTIONNAIRE VERSION 4[illegible]

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?					A&A-01
A&A-01.1	監査・保証のポリシー、手順、基準が確立され、文書化、承認、伝達、適用、評価、維持されているか？					A&A-01
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?					A&A-01
A&A-01.2	監査・保証のポリシー、手順、基準は少なくとも年1回見直され、更新されているか？					A&A-01
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?					A&A-02
A&A-02.1	独立した監査および保証の評価は、関連する基準に従って少なくとも年1回行われているか？					A&A-02
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?					A&A-03
A&A-03.1	独立した監査と保証の評価は、リスクベースでの計画とポリシーに基づいて行われている[illegible]					A&A-03

CAIQの内容　(2)

- CAIQのカラム
  - CSP CAIQ Answer：　質問に対するCSPの評価結果（Yes/No）
  - SSRM(Security Shared Responsibility Model) Control Ownership：責任共有モデルにおける説明責任と管理責任の所在
    - CSP Owned　：CSPが管理責任。CSPが説明責任
    - CSC Owned　：CSCが管理責任。CSCが説明責任
    - Shared CSP and CSC　：CSCとCSPが管理責任と説明責任を共有
    - 3rd-party outsourced：サードパーティが管理責任。CSPが説明責任
    - Shared CSP and 3rd Party：サードパーティとCSPが管理責任を共有。CSPが説明責任
  - CSP Implementation Description：　CSPからの補足情報（オプション）
  - CSC Responsibilities；CSCの管理責任の概要

CAIQの内容　(3)

CAIQの典型的な利用方法

1. **クラウド利用者**
   - プロバイダ/クラウドサービスのセキュリティを評価するためのチェックリスト
     - クラウド利用者が1からチェックリストを作成するのは厳しい
     - 幅広く利用されている1フレームワークであるCAIQをベースに作成するのが効果的
2. **クラウドプロバイダ**
   - クラウドサービスの透明性
     - プロバイダがセルフアセスメント（自己評価）した結果を公開: STAR Level1:セルフアセスメント（次頁以降説明）
     - クラウド利用者は、公開情報に基づいてプロバイダ/クラウドサービスのセキュリティを評価
     - セキュリティ情報の積極的な公開　＝　ビジネス上の差別化要因
     - クラウド利用者からの問い合わせを統一化可能

CAIQの内容　(4)

CAIQの典型的な利用方法（続き）

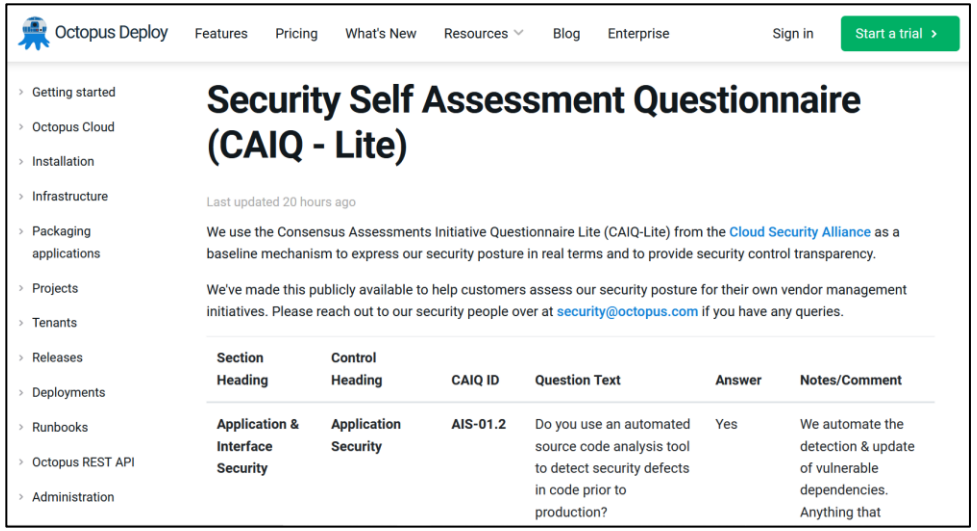
3. クラウド監査者

- 被監査者に対する的確な質問の作成
- 内部監査者
  - 内部評価のための質問のガイドとなる
- 外部監査者
  - クラウドプロバイダの監査における評価内容として使用
  - 認証/監査証明の補完（クラウド部分の評価）として使用

CAIQ-Liteの利用方法

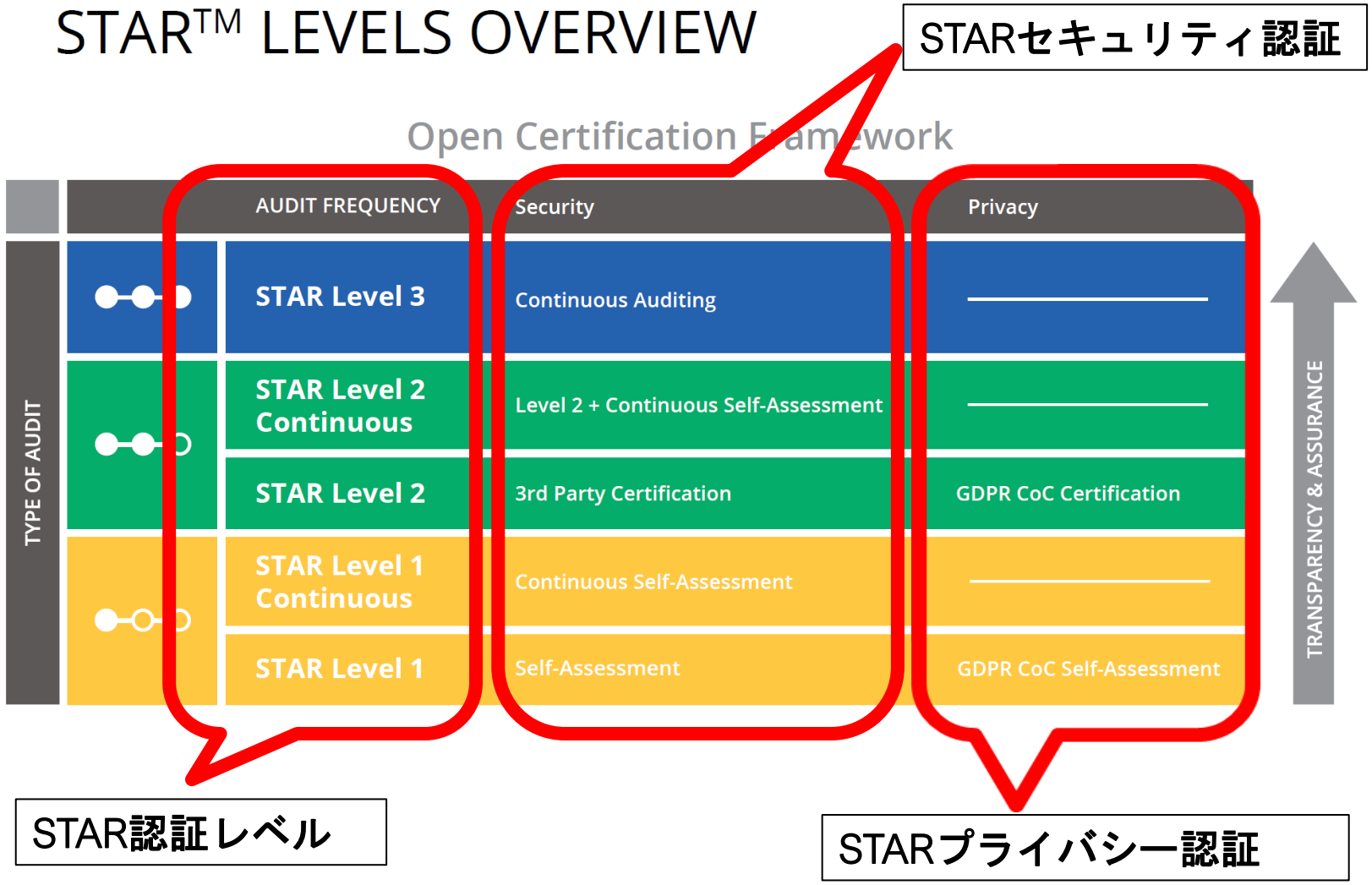
- クラウド利用者がプロバイダ/クラウドサービスのセキュリティを評価するためのチェックリスト
  - CAIQによる評価を行うのが厳しいケース（中小企業等）
  - 基本的なクラウドセキュリティの評価として利用

- プロバイダがCAIQ-Liteを用いてセルフアセスメントし、その情報を自身のウエブサイト等から公開
  - STAR Registry への公開ではなく、独自に公開



引用：https://octopus.com/docs/security/caiq

STARプログラム　(1)

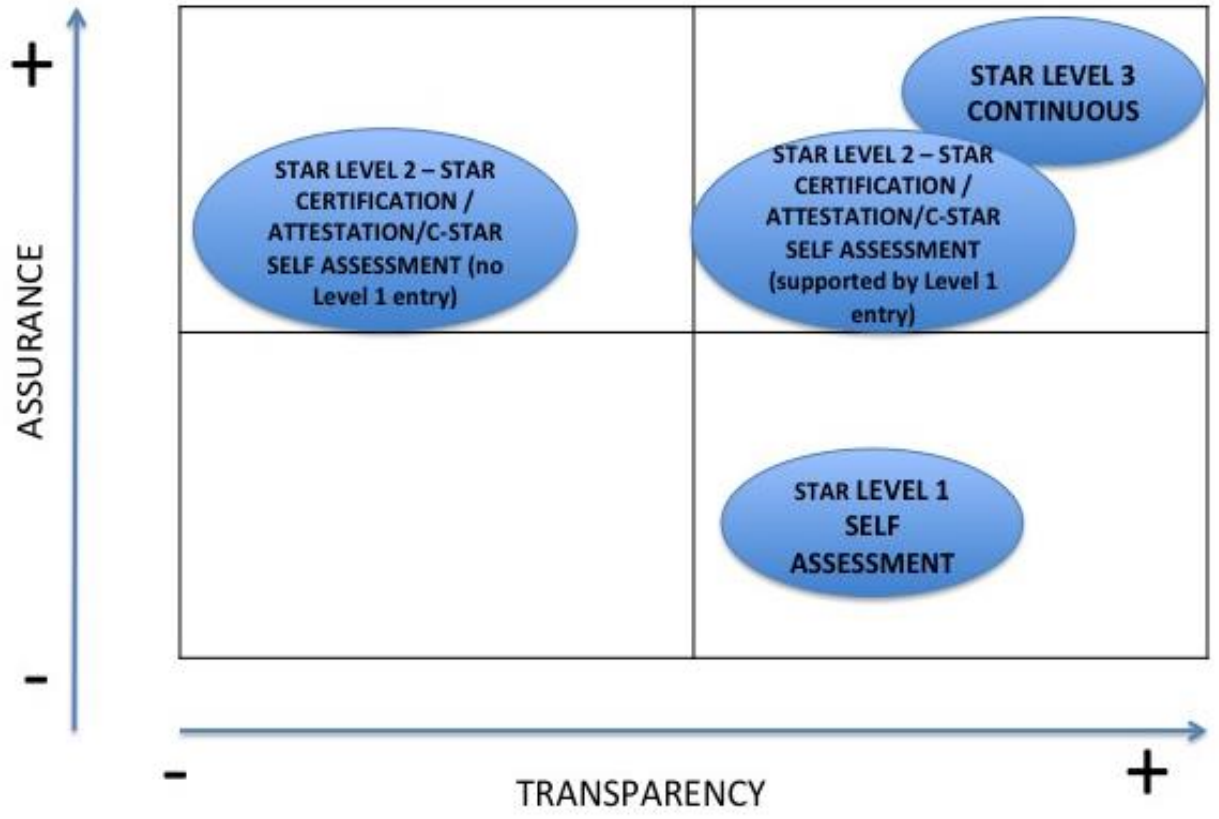


STARプログラム　(2)

STAR　透明性と高い保証

- レベル1
  - プロバイダ自己評価（セルフアセスメント）
- レベル2
  - 第三者認証/監査証明
- レベル3
  - 継続的モニタリング/継続的監査
  - Coming soon

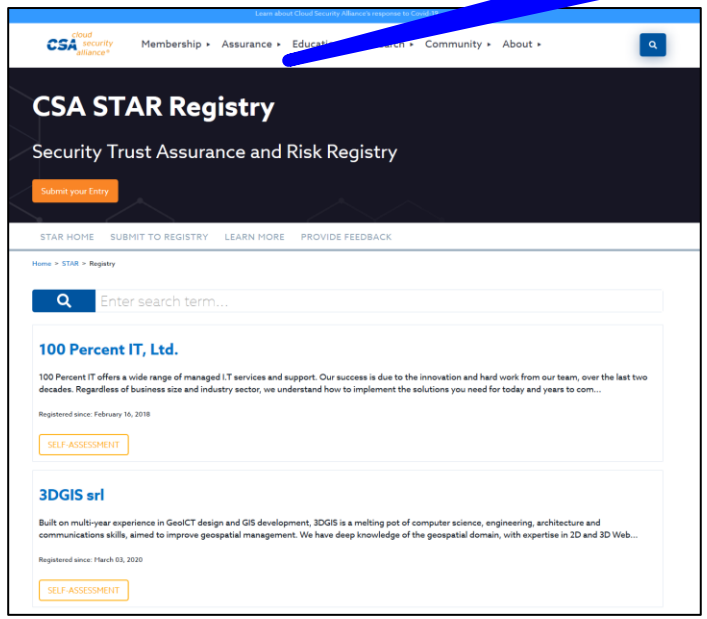
➢ 透明性と高い保証を実現
  ➢ レベル1　＋　レベル2



STARプログラム　(3)　：　STARレベル1

STAR Registry：　プロバイダのセルフアセスメントの結果を公開

公開サイト



プロバイダによるセルフアセスメント

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	Microsoft Azure has established baseline configuration standards and procedures are implemented to monitor for compliance against these	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	Microsoft Azure and Dynamics manage Security and Privacy key performance indicators (KPIs) to	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	Shared CSP and CSC	Microsoft Azure's software development practices are aligned with the Microsoft Security Development Lifecycle (SDL)	Customers are responsible for developing and following a secure software development program for the customer environment.
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	Shared CSP and CSC	Microsoft Azure has established software development and release management processes to control implementation of major changes. Security testing is performed in the	Customers are responsible for developing and following a secure software development program for the customer environment.
AIS-05.2	Is testing automated when applicable and possible?	Yes		Microsoft Azure perform security testing in the implementation, verification and release phases of the	Customers are responsible for developing and following a secure software development program for

引用：　Microsoft AzureのStar1

STARプログラム　(4)：　STARレベル2

- CSAが提供する第三者認証/監査証明
  - STAR Certification
    - ISMS + CCM
  - STAR Attestation
    - SOC2 + CCM
  - C-STAR
    - GB/T 22080-2008 + CCM

- 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
- 日本で展開している機関は少ない。But… クラウドセキュリティとして必要な考え方として理解することも大切
  https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2023/12/STAR-Attestation-Value-Proposition-20231002_J.pdf

5. クラウドサービスのセキュリティ評価方法

クラウドサービスのセキュリティ評価方法　概要

CSAのツールを使用

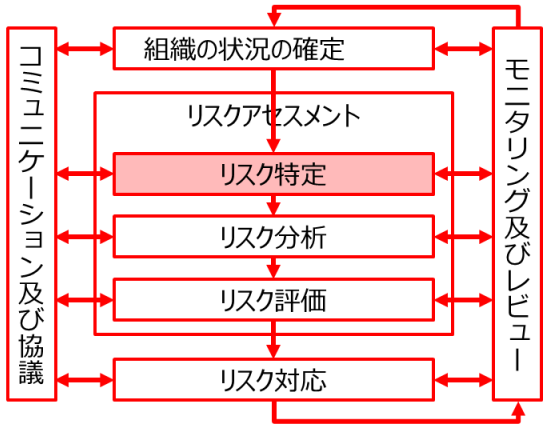
1. 網羅的アプローチ
   - 詳細リスク分析に基づく方法
   - IaaS/PaaSにおいては重要。SaaSにおいても可能であれば実施

2. ベースラインアプローチ
   - 規格が定義している管理策を元に評価

3. クイックアプローチ
   - 評価レポートを使用して評価

網羅的アプローチ　(1)

CCMを使ったリスク特定



1. 利用するクラウドサービス（候補）に対するセキュリティ要求事項をCCMの管理策からリストアップする

① クラウドに移行する資産を特定

② 資産に対するセキュリティ要求事項を確認

③ セキュリティ要求事項に対して、該当するCCMの管理策をリストアップ

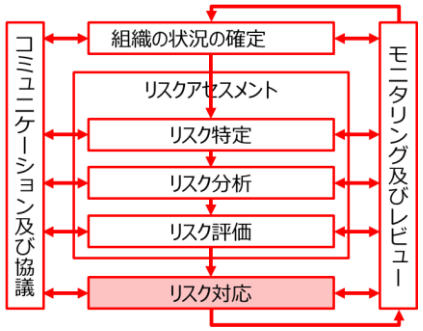
- その際、Implementation Guideline を参考にし、クラウドセキュリティとして必要となる実装・設定等を理解する

④ CCMでカバーされていないセキュリティ要求事項の明確化

- CCMでほぼ100%カバーされるが、業界/業種固有の要求事項がある場合にはこれを明確化しておく。

網羅的アプローチ　(2)

CAIQを使ったリスク対応
ー　クラウドサービスのセキュリティ評価

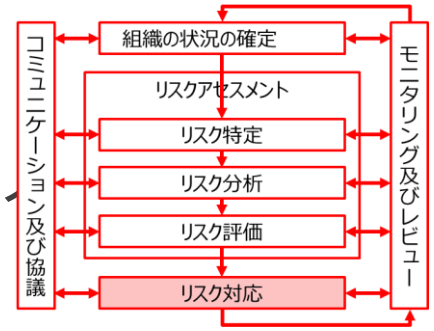


- CAIQ（Consensus Assessment Initiative Questionaire）の利用
  1. 利用しようとしているクラウドサービスのCAIQ評価レポートを以下のどちらかの方法で入手
     - STAR Registryのサイトよりダウンロード
       （STAR Registryについては後述）
     - CAIQをクラウドサービス事業者に送付し、評価結果を入手する
  2. リスク特定において要求事項として洗い出されたCCMの管理策に該当するCAIQの評価レポートを参照し、要求事項を満たしているかどうかを評価・判断
- CCMでカバーされていないセキュリティ要求事項については、クラウド事業者に質問し、明確化

網羅的アプローチ　(3)

CAIQを使ったリスク対応

　ー　CAIQ評価レポート等を用いてクラウドサービスのセキュリティ評価を行った後の対応



① クラウドサービスのセキュリティが要求事項をすべて満たしている場合
- ➔ そのクラウドサービスを利用

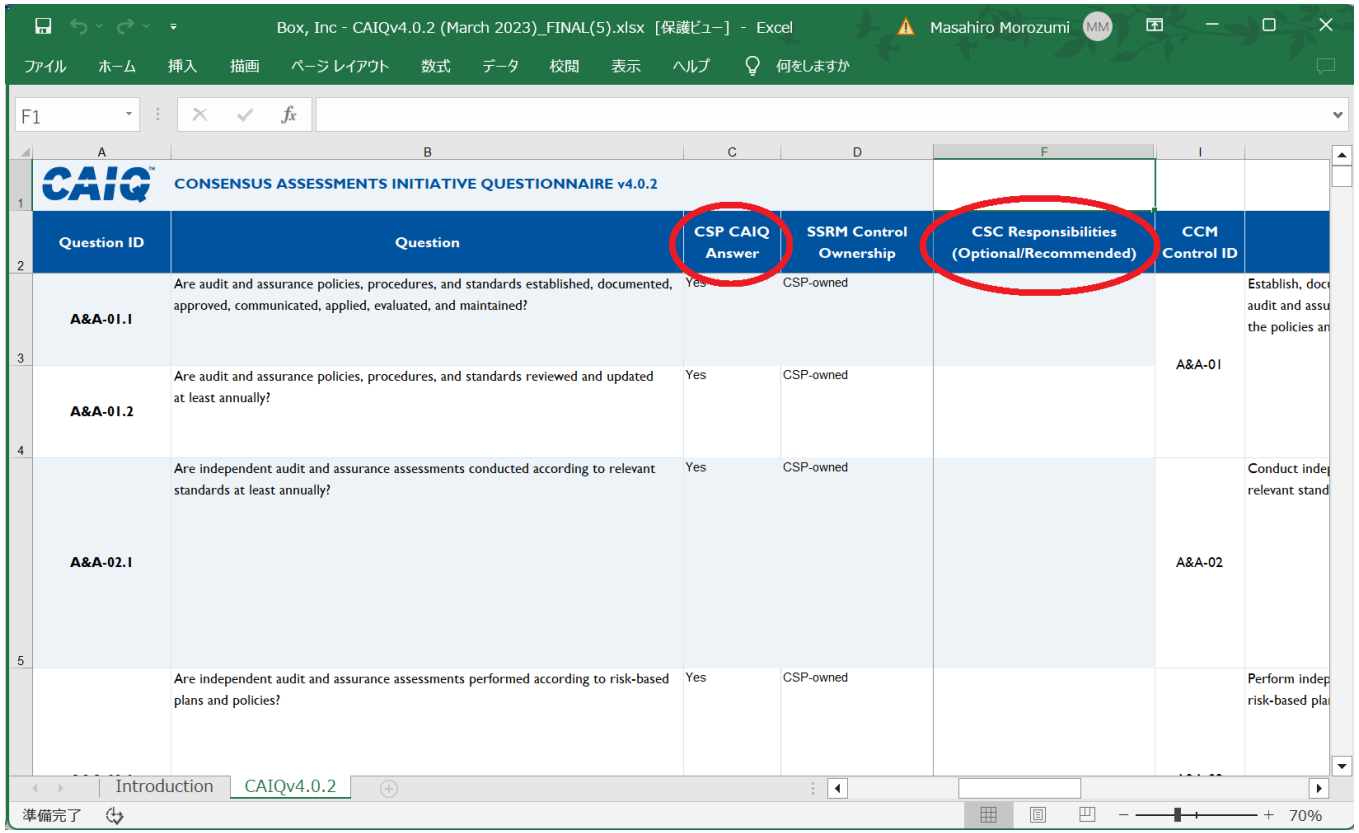
② クラウドサービスのセキュリティが要求事項を満たしていない場合
- ➔ リスク許容可能かどうかを判断。可能であればそのクラウドサービスを利用
- ➔ 許容可能でない場合
  - ➔ そのクラウドサービスは利用せず、別のクラウドサービスを評価する OR
  - ➔ 追加のセキュリティ対策を利用者として行い、要求事項を満たすようにして利用する

ベースラインアプローチ

CAIQのベースであるCCMの全管理策を元に、ベースラインアプローチで評価する。

1. CCMを要求事項リストとして使用。自組織として不要な部分を削除

2. CAIQ評価レポートの「CSP CAIQ Answer」を確認し、1のリストに対アして問題ないかどうかを判断



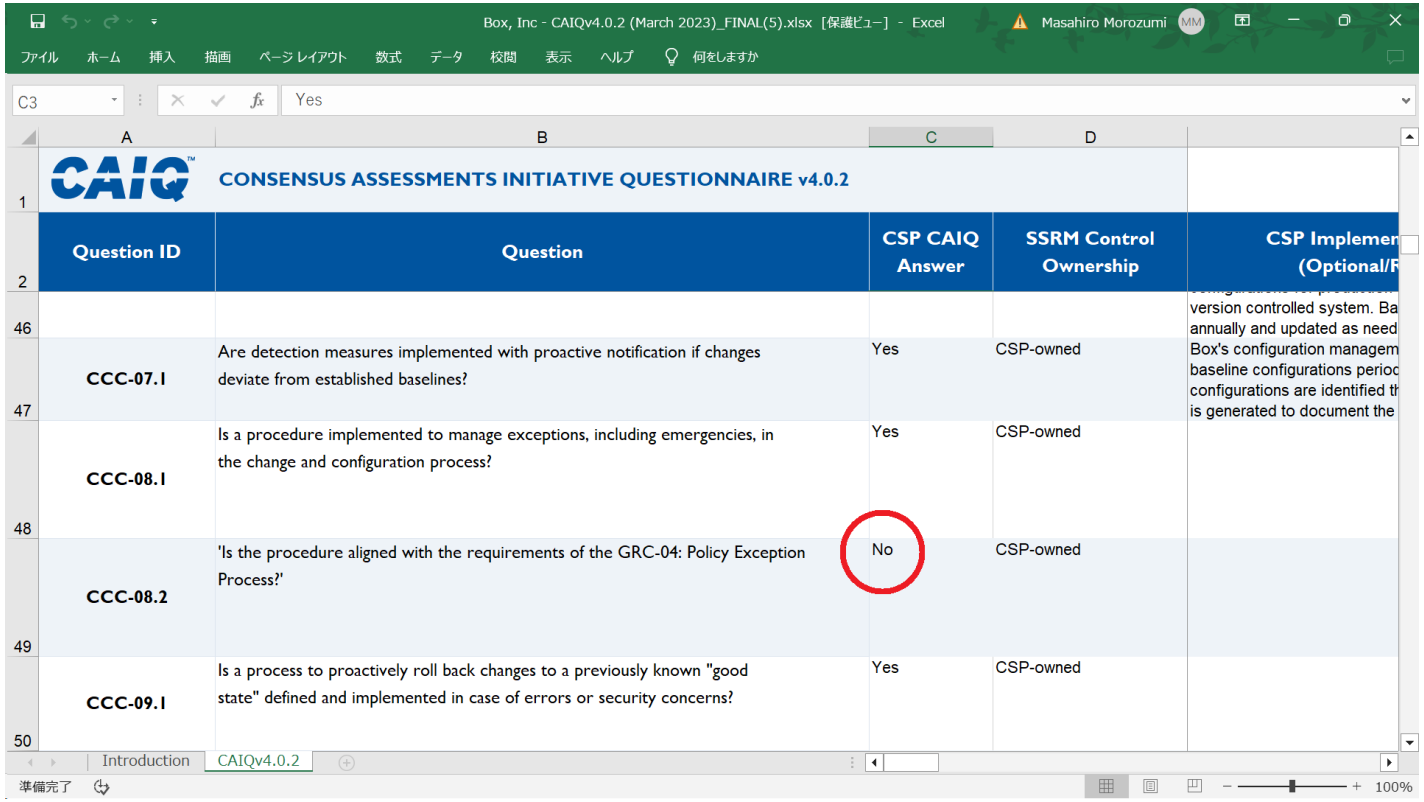
クイックアプローチ

CAIQ評価レポートの結果を評価する。

1. 利用しようとしているクラウドサービスのCAIQ評価レポートをダウンロード

2. 「CSP CAIQ Answer」で「No」の部分を抽出

3. 「No」の部分が自組織のセキュリティの観点で受容可能かどうかを判断



クラウドプロバイダへ、積極的な公開へのお願い！

CAIQを利用したセルフアセスメントを実施、STAR Registryに登録

CSAジャパンでは、 STAR Registryへの登録方法を支援

- STAR１日本語での登録方法
- 日本語での評価レポートの公開方法およびLevel1セルフアセスメントの重要性について　（ブログ）

現在、日本語CAIQを登録されているクラウド事業者

- 日本語CAIQ評価レポートを公開されている企業情報　（情報提供待ち）

6. CCAK(Certificate of Cloud Auditing Knowledge) 概要

CCAK(Certificate of Cloud Auditing Knowledge)　とは？

- 目的
  - CCAK is the first-ever, technical, vendor-neutral credential for cloud auditing. This certificate fills a gap in the industry for competent technical professionals who can help organizations mitigate risks and optimize ROI in the cloud.
    CCAKは、クラウド監査のための、技術的でベンダーニュートラルな初の資格です。この資格は、企業がクラウドにおけるリスクを軽減し、ROIを最適化することを支援できる有能な技術専門家を求めている業界のギャップを埋めるものです。

  - CCAK prepares IT professionals to address the unique challenges of auditing the cloud, ensuring the right controls for confidentiality, integrity and accessibility and mitigating risks and costs of audit management and non-compliance.
    CCAKは、クラウドの監査、機密性、完全性、アクセシビリティのための適切なコントロールの確保、監査管理やコンプライアンス違反のリスクとコストの軽減といった独自の課題に対処するためのITプロフェッショナルを育成します。

CCAK(Certificate of Cloud Auditing Knowledge)　とは？

- CCAKのポジション
  - ISACAが提供するCISA, CISM, CRISC, CGEITを補完
  - FedRAMP 3PAO Assessor, PCI-DSS Qualified Security Assessor, ISO 27001 Leader Auditor を補完
  - ISACAの監査の専門家とCSAのクラウド専門知識を強化
  - DevOps、CI/CDのような技術/配備フレームワークを含む
  - CSAのCCSKをベースにして、それを補完する内容
- 対象者
  - 内部・外部監査人
  - コンプライアンス管理者
  - 第三者監査人
  - ベンダー/パートナー・プログラムマネージャ
  - セキュリティ・アナリスト/アーキテクト
  - 調達部
  - サイバーセキュリティ・リーダー/アーキテクト
  - セキュリティ、プライバシー・コンサルタント

ベストマッチ

CCAK試験　概要

- 試験時間：　2時間
- 問題数：　76問
- 合格ライン：　70%
- 言語：　英語
- 試験費用：　$395：ISACA会員（$495：非会員）
  CSA本部の企業会員向けの割引もあるようです
- 試験方法：　オンライン
  PSIというサードパーティーの試験機関を使用
- CCAK向けテキスト
  - Certificate of Cloud Auditing Knowledge™ Study Guide：
    $59.00：ISACA会員（$70.00：非会員）
    CSA本部の企業会員向けの割引もあるようです

CCAK試験　必要な情報

- Certificate of Cloud Auditing Knowledge™ Study Guide
  - ISACAのウエブサイトより購入：$59（ISACA会員）、$70（非会員）
- Consensus Assessments Initiative Questionnaire (CAIQ) v3.1　（日本語）
  - https://cloudsecurityalliance.org/artifacts/caiq-translation-in-10-languages/
- Cloud Controls Matrix (CCM) v3.0.1　（日本語）
  - https://cloudsecurityalliance.org/artifacts/ccm-translation-in-10-languages/
- Top Threats to Cloud Computing Deep Dive (2018)　（日本語）
  - https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2020/11/Top-Threats-to-Cloud-Computing-Egregious-Eleven-Deep-Dive-J.pdf

注）CCM/CAIQは、一部V4.0の知識（V3との違い）も求められる。

CCAK活動状況

- ISACAとCSAのパートナーシップに基づいて展開
  - Study Guide, Exam
    - CSA:　コンテンツの開発
    - ISACA:　試験問題の開発
  - ISACAが、CCAKのトレーニング・試験の展開を担当

今後の日本での展開等についてはISACA次第か？？？
CSAジャパンとしては、CSA本部側の担当を通じて協力は可能

CCAKを利用したクラウドセキュリティ

CCAKの特徴

1. 対象者は、監査人だけではなく、幅広く利用できる知識
   - 特に、利用者が説明責任を果たすために必要となる評価の知識

2. CSAが提供している監査・評価ツールの知識
   - CCM/CAIQ, STAR認証、クラウド脅威分析手法、クラウド重大脅威ディープダイブなど

CCAKを利用したクラウドセキュリティ

クラウドサービス利用者にとってのCCAKのメリット

- クラウドセキュリティの一般的な知識だけでなく、評価に必要となる知識を取得
  - CCSKとかは、クラウドセキュリティの一般的な知識
- 評価に必要となる様々なツールの理解、実践が可能
- 利用者としてクラウドリテラシーを向上
- SIerに依存する体質からの脱却

CCAKは、監査人向けのクラウドセキュリティの知識というだけでなく、クラウドセキュリティ全般を理解するのに有効

7.　まとめ

まとめ

1. クラウドセキュリティにおける**責任共有モデル**の理解

2. **クラウド利用者のセキュリティ対応**における課題
   - クラウドセキュリティにおいて最も脅威となっているポイント
   - 効率的、効果的な対応　ー＞　簡単化、自動化
     CSPM, SSPM, プロバイダが提供するツール、サービス　など

3. クラウド利用者が**クラウドサービスのセキュリティを評価**する際の課題
   - 評価をどのようにしていくかというポイント
   - 効率的、効果的な評価方法　ー＞　簡単化、自動化
     - CSA STAR Registry、CASB, VRM/TPRM　など

4. **CCAK**への取り組み
   - CCAK資格の取得はともかく、CCAKを使用してクラウドセキュリティ監査を理解することは有効

さらに...

- CSA CEO, Jim Reavisによるクラウドの変遷
  - **CLOUD1.0**:　伝統的なITサービスをクラウド化するという新しいビジネスモデルの時代（2008-2016）
  - **CLOUD2.0**:　クラウドネイティブの時代。DevOps,コンテナ、サーバーレス、CNAPPなど（2016-2022中頃)
  - **CLOUD3.0**:　生成AIの登場と、生成AIとクラウドの統合の時代（2022中頃-現在）

本日の講演内容　＝　CLOUD1.0

CLOUD2.0, CLOUD3.0 のセキュリティ、それから先のセキュリティ！！！

CSAの活動　==　「場」の提供！

様々なワーキンググループ活動の「場」

自由な情報発信の「場」

https://cloudsecurityalliance.jp
mmorozumi@cloudsecurityalliance.jp

ありがとうございました