CSAジャパンのISMAPへの取り組みとSTAR認証の先進性

一般社団法人　日本クラウドセキュリティアライアンス
業務執行理事　諸角昌宏
CCSP, CCSK, CSAリサーチフェロー

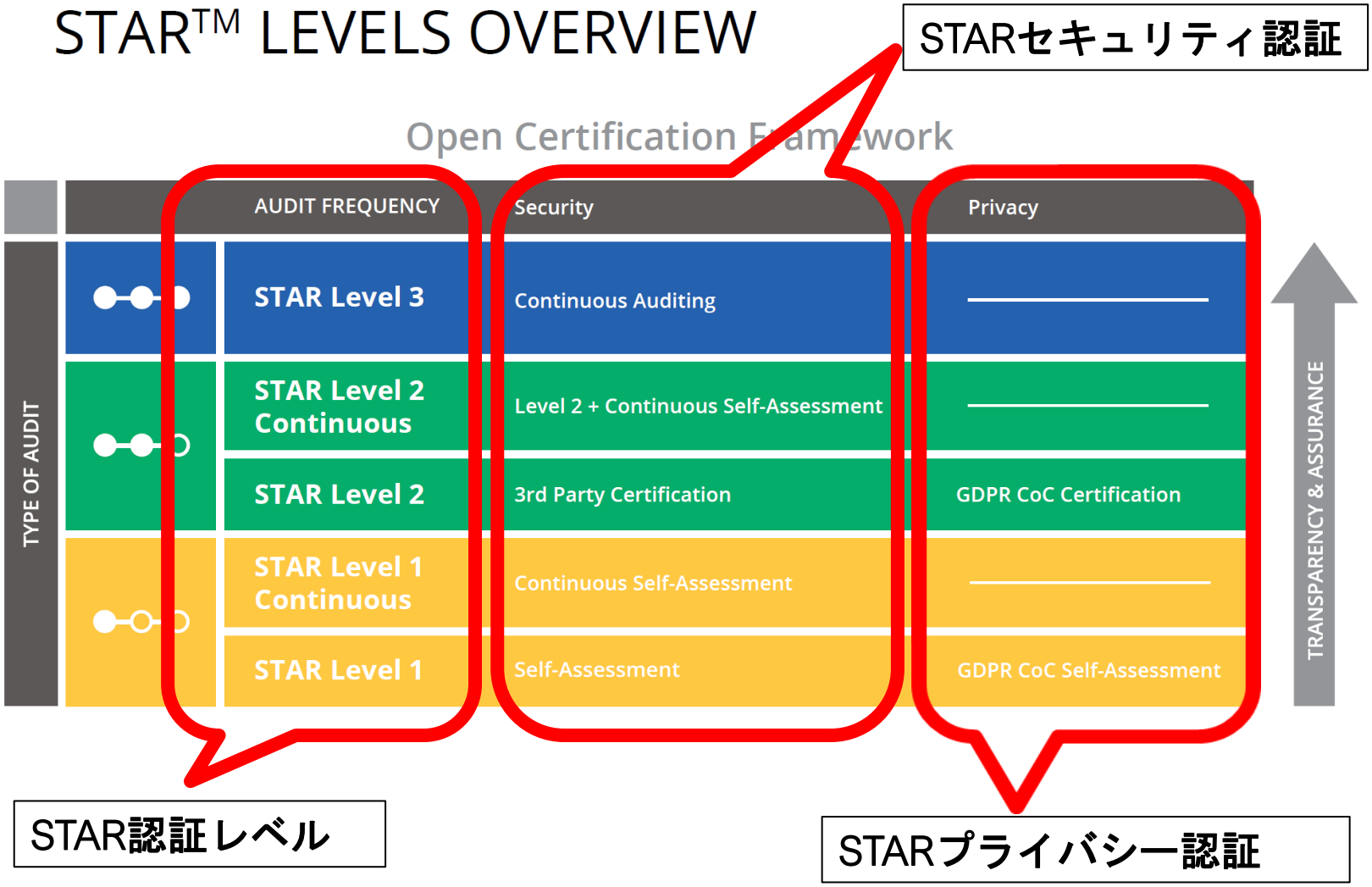
2020年11月18日

アジェンダ

1. STAR（Security, Trust & Assurance Registry）概要
2. STAR認証のビジョン
3. 相互認証とISMAP
4. 本日のまとめ

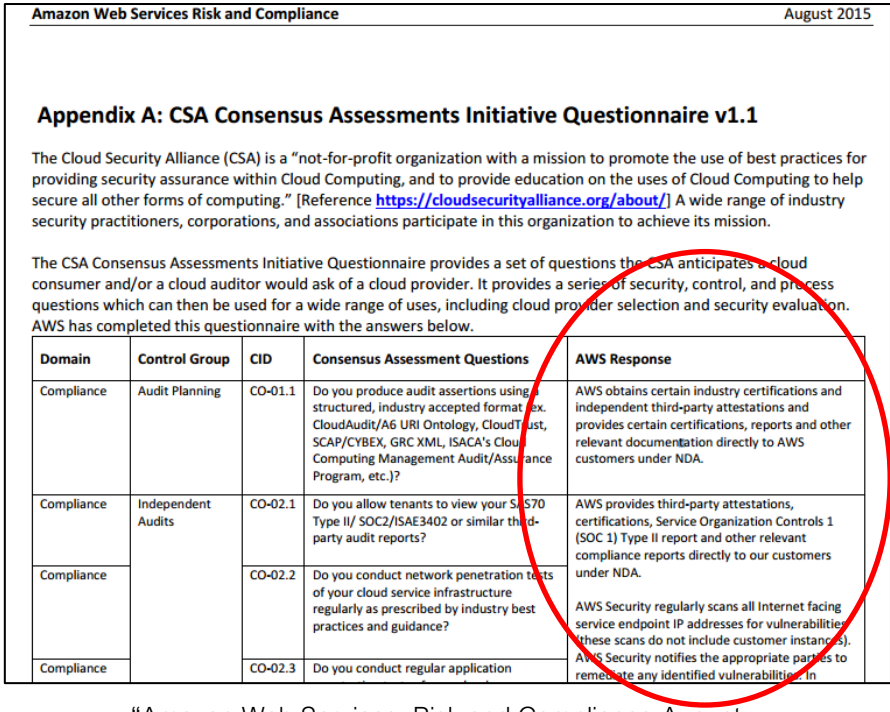
1. STAR（Security, Trust & Assurance Registry）概要

STARとは



STAR Level1 セルフアセスメント

- 概要
  - STARは、クラウドプロバイダのセキュリティレベルを公に公開し、ユーザがクラウドプロバイダを選定する際の判断に利用することができる環境を提供
  - STAR1 セルフアセスメントは、クラウドプロバイダが、CSAが提供しているCCMあるいはCAIQに基づいて独自に評価し、その内容をCSA STARのウエブサイトに公開
  - クラウド利用者がクラウドプロバイダを選択するに際して、セキュリティ管理について確認するための情報 として利用することが可能
  - 登録は以下のCSAのウエブサイトで公開：
    - https://cloudsecurityalliance.org/star/#_registr
- 日本語での登録支援を開始（2015年7月）
  - 今までは、登録に際して、英語で評価レポートを作成し、CSA米国のSTAR登録サイトに行き英語で手続きすることが必要
    - 日本のクラウドプロバイダにとって負担が大きく、かつ、クラウド利用者にとっても英語で内容を確認しなければならなかった
  - CSAジャパンがこの手続きを仲介することで、日本語での評価レポートを日本語のままで登録、かつ、手続きも日本で日本語で行うことが可能



Amazon Web Services Risk and Compliance — August 2015

Appendix A: CSA Consensus Assessments Initiative Questionnaire v1.1

The Cloud Security Alliance (CSA) is a "not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing." [Reference https://cloudsecurityalliance.org/about/] A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission.

The CSA Consensus Assessments Initiative Questionnaire provides a set of questions the CSA anticipates a cloud consumer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions which can then be used for a wide range of uses, including cloud provider selection and security evaluation. AWS has completed this questionnaire with the answers below.

Domain	Control Group	CID	Consensus Assessment Questions	AWS Response
Compliance	Audit Planning	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	AWS obtains certain industry certifications and independent third-party attestations and provides certain certifications, reports and other relevant documentation directly to AWS customers under NDA.
Compliance	Independent Audits	CO-02.1	Do you allow tenants to view your SAS70 Type II/ SOC2/ISAE3402 or similar third-party audit reports?	AWS provides third-party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA.
Compliance		CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In
Compliance		CO-02.3	Do you conduct regular application	

"Amazon Web Services: Risk and Compliance August 2015" より引用

STAR Level2
第三者評価

- STAR認証（STAR Certification）
  - ISO/IEC 27001認証審査と同時に審査を実施
    - ISO/IEC 27001認証を取得していなければならない
  - クラウドコンピューティングのセキュリティにおける成熟度を評価
    - CSAが開発したCCMを用いて、クラウドサービスの成熟度を評価
  - クラウドサービスの成熟度のレベルに応じて、「ブロンズ」「シルバー」「ゴールド」のアワードを授与

注意：　STAR Attestation は　SOCベース。

ISO/IEC 27001 ＋ CCM ＋ 成熟度モデル ＝ STAR™ CERTIFICATION

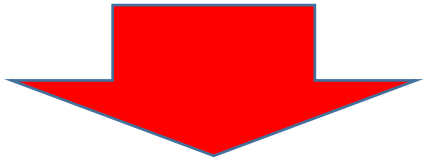
STAR Level3

- STAR Level3　（継続的モニタリング）
  - 認証取得後も、その対応状況を継続的にモニタリングし保証する制度。たとえば米国政府（FedRAMP）などでハイレベルの情報を扱う際に要求されており、現在、STARとしての枠組み検討が進んでいる

（準備中）

PLA(Privacy Level Agreement)行動規範のSTAR認証への取り込み

- 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
- PLAは **Code of Conduct for GDPR を使用**



- 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

2. STAR認証のビジョン

STAR認証のビジョン

- クラウド認証の課題
  - **認証の継続型**
  - **認証の透明性**
  - **相互認証スキーム**

クラウド認証の課題

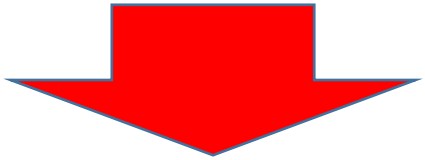
1. 認証の継続性
   - 「ある時点 (point-in-time)」と「ある期間 (period-of-time)」を対象とするアプローチに依存

2. 認証の透明性
   - 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

3. 相互認証スキーム
   - CSPは、40以上のフレームワークや規制に対応する必要がある
     - EU-SEC
     - FedRAMP
     - G-Cloud
     - C5
     - Etc…
   - 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

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

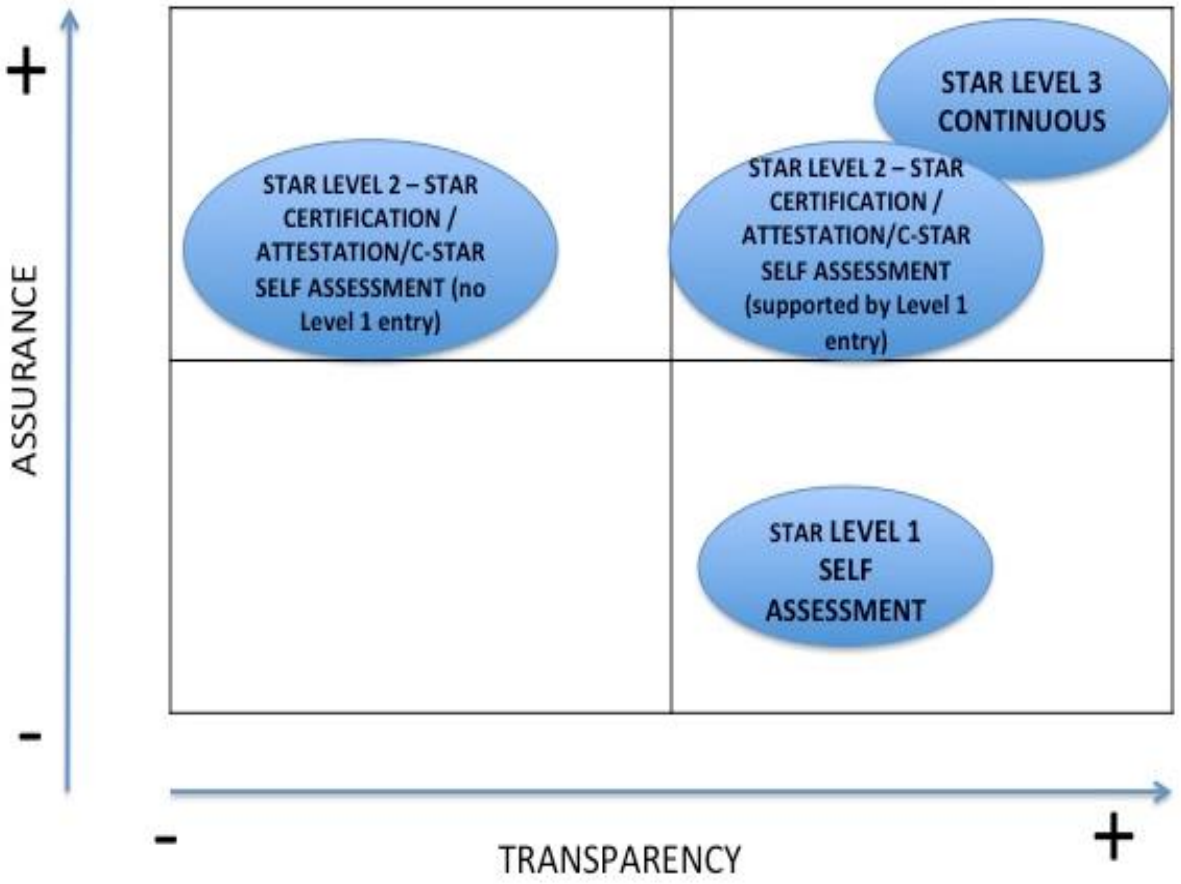


- クラウドサービスカスタマに対して、セキュリティ管理策の実施状況に関する十分に詳細な最新情報を提供

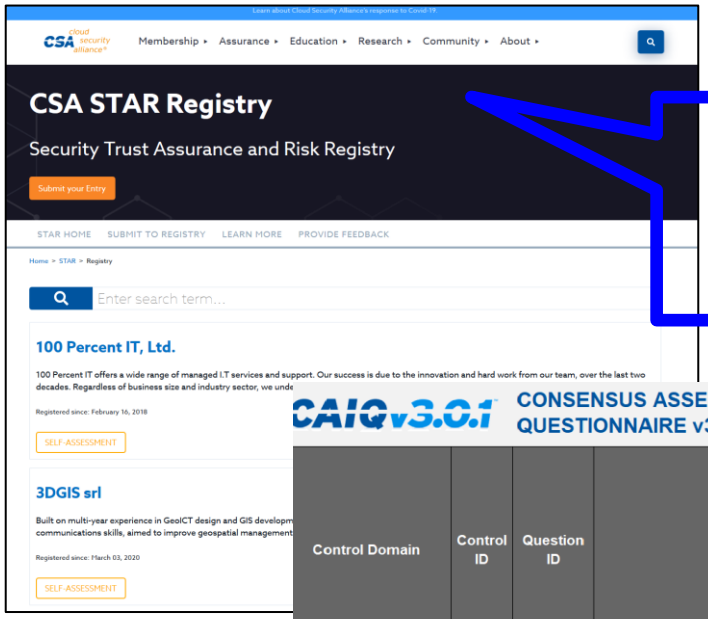
STAR　透明性と高い保証

- 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 Registry



公開サイト（Registry）

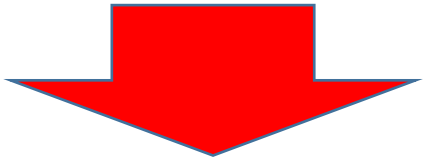
プロバイダによるセルフアセスメント

CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
estriction		IAM-06.2	the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Access to tenant applications is controlled by the tenant
dentity & Access Management *hird Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you provide multi-failure disaster recovery capability?	X			
		IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	X			
		IAM-07.3		Do you have more than one provider for each service you depend on?	X			
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	X			Available internally
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?	X			
		IAM-07.6		Do you provide a tenant-triggered failover option?	X			Available on reque
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?	X			Available on reque
dentity & Access Management *ser Access Restriction / uthorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant and approve access to tenant data?	X			
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	X			

相互認証スキーム

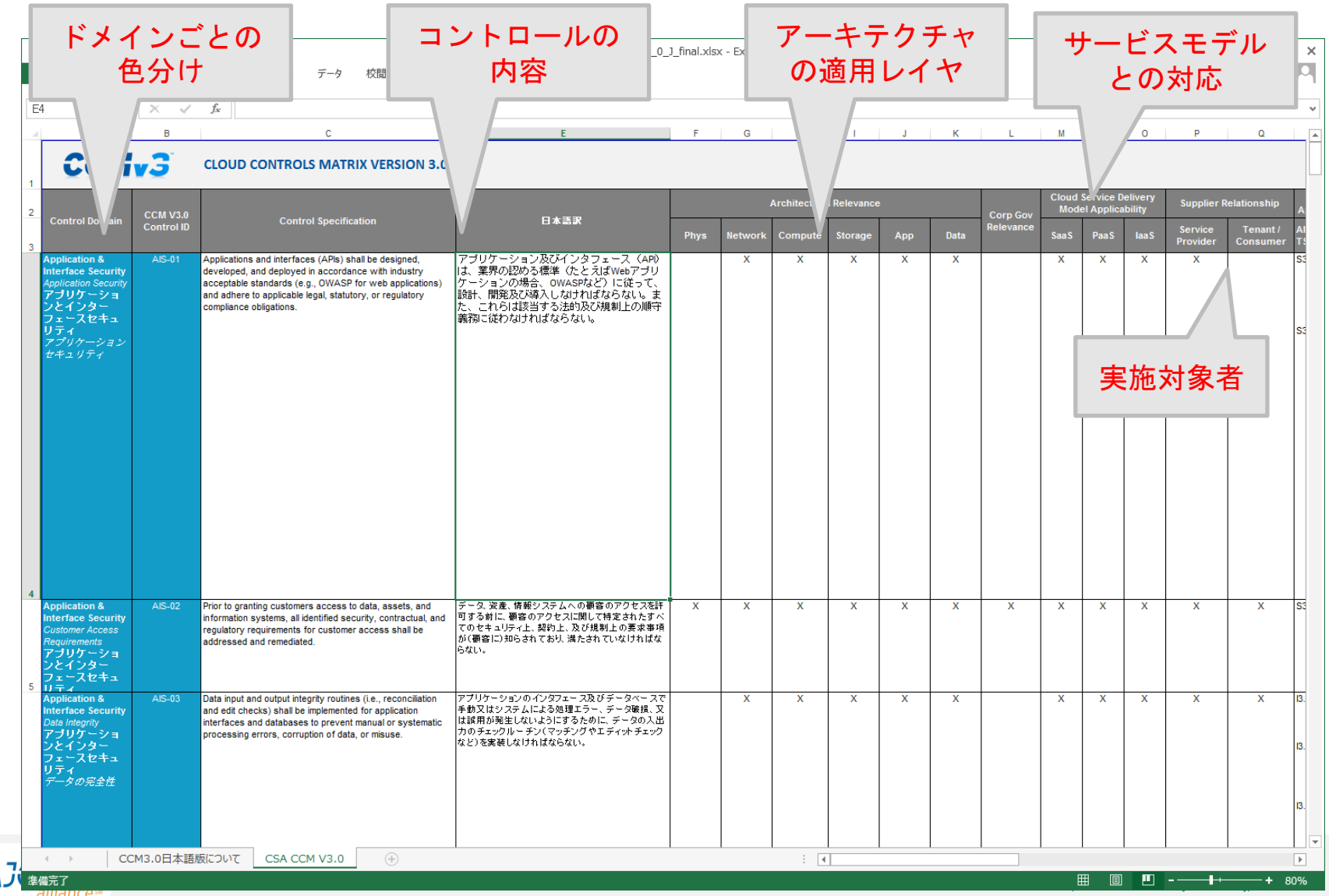
- CCMは、数多くの国単位、分野単位の基準へのマッピングを提供
- CCMは、ほかの基準の要件のほとんどに適合



- 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
  （注：　枠組みであり、相互認証を可能にするものではない）

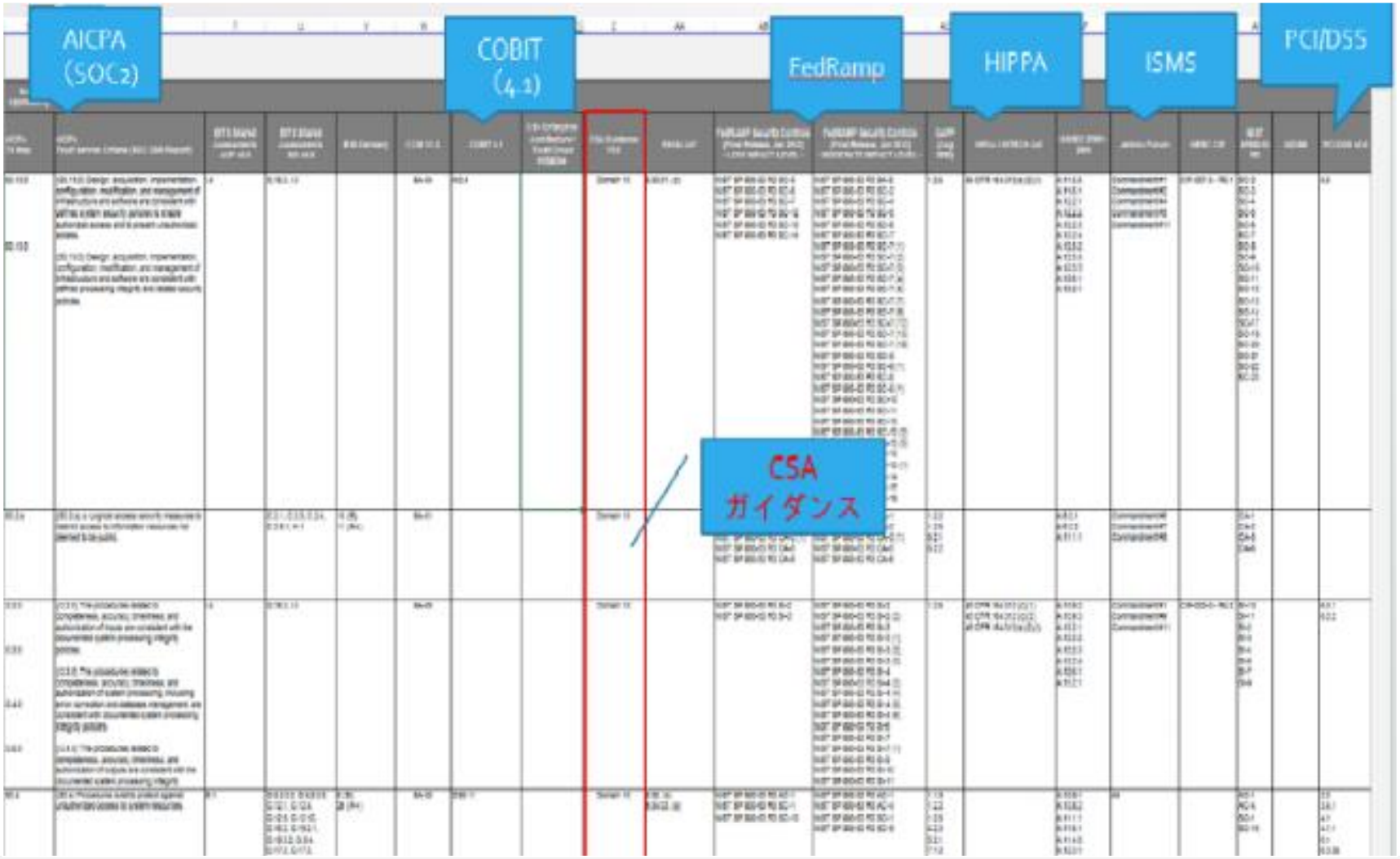
取組み
1. CCMと各規格とのマッピング及びリバースマッピング
2. CCMと各規格とのギャップ（GAP)分析
3. ギャップ分析ドキュメントとして公開
   1つの認証の取得から別の認証の取得までの労力を最小化する

CCMの項目例（日本語訳版）



Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		A
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	
Application & Interface Security *Application Security* アプリケーションとインターフェースセキュリティ *アプリケーションセキュリティ*	AIS-01	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	アプリケーション及びインタフェース（API）は、業界の認める標準（たとえばWebアプリケーションの場合、OWASPなど）に従って、設計、開発及び導入しなければならない。また、これらは該当する法的及び規制上の順守義務に従わなければならない。		X	X	X	X	X		X	X	X	X		S3 S3
Application & Interface Security *Customer Access Requirements* アプリケーションとインターフェースセキュリティ	AIS-02	Prior to granting customers access to data, assets, and information systems, all identified security, contractual, and regulatory requirements for customer access shall be addressed and remediated.	データ、資産、情報システムへの顧客のアクセスを許可する前に、顧客のアクセスに関して特定されたすべてのセキュリティ上、契約上、及び規制上の要求事項が(顧客に)知らされており、満たされていなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S3
Application & Interface Security *Data Integrity* アプリケーションとインターフェースセキュリティ *データの完全性*	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	アプリケーションのインタフェース及びデータベースで手動又はシステムによる処理エラー、データ破損、又は誤用が発生しないようにするために、データの入出力のチェックルーチン(マッチングやエディットチェックなど)を実装しなければならない。		X	X	X	X	X		X	X	X	X	X	I3. I3. I3.

各種標準等との対応表



対象規格・基準の一覧 (CCM V3.0.1)

- "AICPA TS Map"
- "AICPA 2014 Trust Service Criteria (SOC 2SM Report)"
- "BITS Shared AssessmentsAUP v5.0"
- "BITS Shared AssessmentsSIG v6.0"
- CCM V1.X
- COBIT 5.0
- COPPA(Children's Online Privacy Protection Act)
- CSA Enterprise Architecture / Trust Cloud Initiative
- CSA Guidance V3.0
- ENISA IAF
- European Union data Protection Direction 95/36/EC
- "FedRAMP Security Controls(Final Release, Jan 2012)--LOW IMPACT LEVEL--"
- "FedRAMP Security Controls(Final Release, Jan 2012)--MODERATE IMPACT LEVEL--"
- FEPRA (Family Education and Rights Privacy Act)
- GAPP (Aug 2009)
- HIPAA / HITECH Act and the Omnibus Rule
- ISO/IEC 27001-2005, 2013
- ITAR (Information Traffic in Arms Regulation)
- Jericho Forum
- Mexico – Federal Law on Protection of Personal Data Held by Private Parties
- NERC CIP
- NIST SP800-53 R3 Rev 3 Appendix J
- NZISM (New Zealand information Security Manual)
- ODCA (Open Data Center Alliance) Usage Model: PAAS Inter Interoperability Rev 2.0
- PCI DSS v3

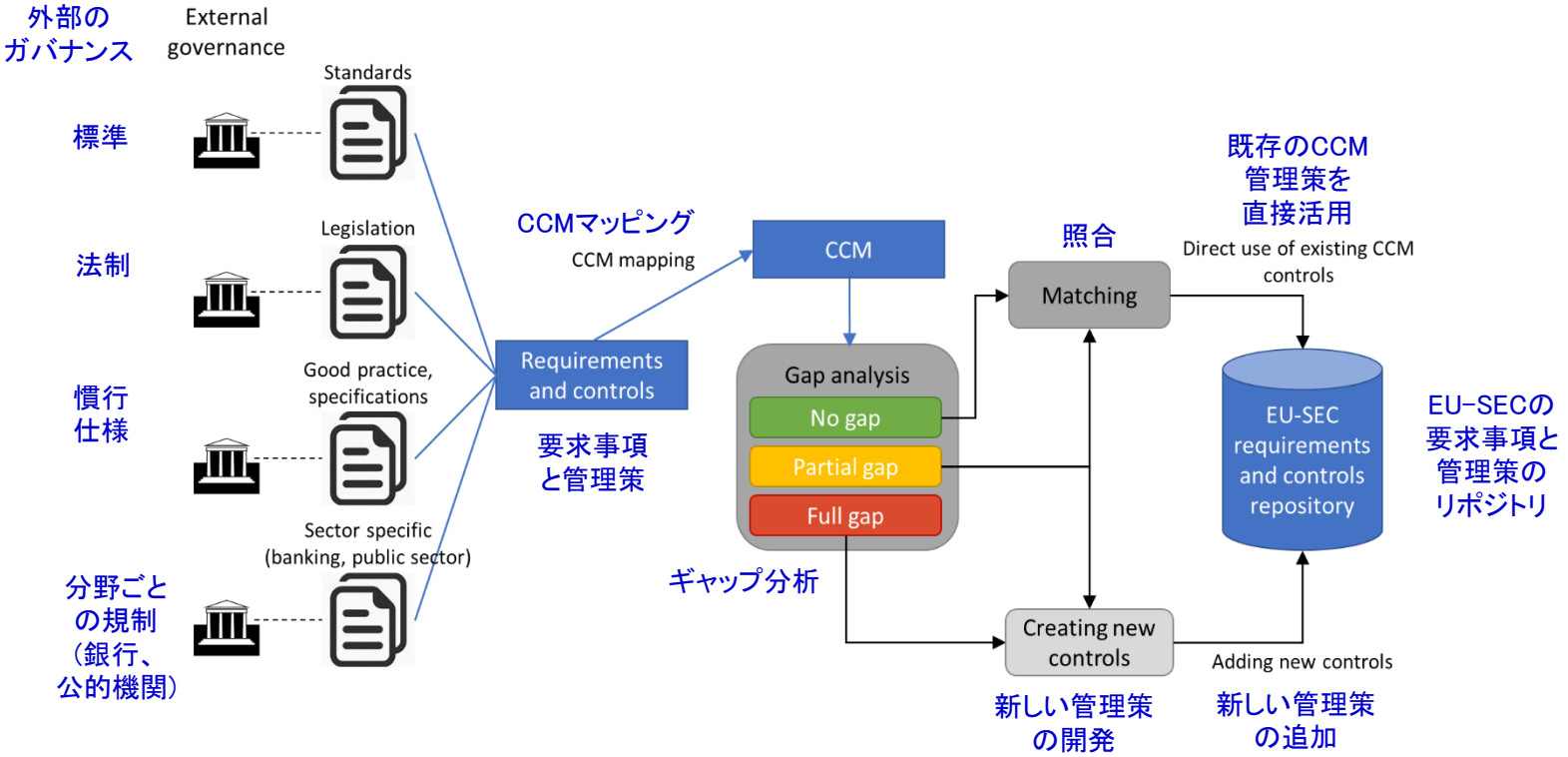
例： ISO/IEC27001 → CCM → SP800-53

3.　相互認証とISMAP

相互認証スキーム　EU-SEC

クラウドコンピューティングを信頼に基づき、かつ基準に準拠して活用するために、クラウドセキュリティの複数主体による認証の枠組みを開発中

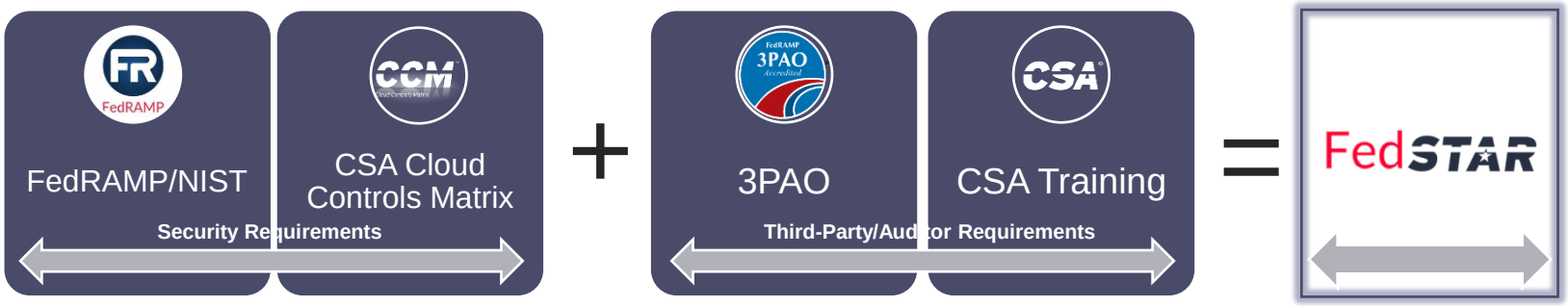
・（例）CCMを利用した要求事項の収集・分析



引用：　EU-SEC, “EU-SEC Awareness Workshop” (September 10, 2018)

相互認証スキーム　FedSTAR

FedRAMP + CSA STAR = FedSTAR



- FedRAMPとの相互認証プログラム（FedSTAR）：
- GSA (General Services Administration,米国共通役務庁)と調整中
- 継続的監査(Continuous auditing)の枠組みを開発中

引用：　https://www.afcea.org/site/sites/default/files/files/Offset%20Symposium%20PFC%20Final%20v2.pdf

そのほかの相互認証スキーム

- シンガポール：　Multi-Tier Cloud Security (MTCS)
  - クラウドサービスを公的機関に提供するクラウドサービスプロバイダに対する認証の仕組み
  - CSA STARとMTCS間の相互認証仕様（Cross certification specifications）を2015年に公開
- ドイツ：　C5 と CCM とのギャップ分析資料を2019年に公開
  - 管理策の双方向マッピング（マッピング、リバースマッピング）
  - ギャップ分析
- そのほか…

相互認証スキーム　日本での取り組み

- ISMAP（政府情報システムのためのセキュリティ評価制度）とCCMとの双方向マッピングの作業中
  - ISMAP->CCM マッピング
  - CCM->ISMAPマッピング
  - ギャップ分析
- ゴール
  - グローバル企業がISMAP対応にかかる労力の最小化に貢献
  - CSAグローバルにおけるISMAPの認知度向上に貢献

- ISMAPとの双方向マッピングは、CSA本部から公開予定
  - 他のフレームワーク、規格と同様にグローバルで認識されるマッピングとしていく

CCM、ISMAP　マッピング戦略　(1)

- ISMAPの３つの構成：　CCMとのマッピング対象
  - ガバナンス基準（別表１）
    - JIS Q27014をベースにしたガバナンス基準
  - マネジメント基準（別表２）
    - 情報セキュリティ管理基準の項番4.x（4.4.1.1～4.8.2.2）の内容
    - 27001の本文（項番4~10）に対応
    - 注）項番4.9は、情報セキュリティ管理基準にはない。プロバイダと利用者の情報交換がクラウドにおいて重要ということで、クラウドサービスにおいて特に考慮すべき事項を規程

CCM、ISMAP　マッピング戦略　(2)

- ISMAPの３つの構成：　CCMとのマッピング対象 (前頁からの続き)
  - 管理策基準（別表３）
    - 管理策： 3桁
      - 27001/27002および27017（拡張管理策）の分類、管理目的、管理策に対応
    - 詳細管理策：4桁
      - 27002の「実施の手引き」を細分化したものと同等
    - 5桁（P,B､PB）は、27017の実施の手引き。P,B,PBの意味付けは以下
      - P:　クラウドで事業者が特に考慮すべき管理策
      - B:　管理策自体が基本言明要件である管理策
      - PB:　PとBの両方
    - 4. 追加された実施の手引き
      - 情報セキュリティ管理基準（27002,27017どちらにも）に含まれていないもので、ISMAPが独自に追加した実施の手引き

CCM、ISMAP　マッピング戦略　(3)

- マッピング方針
  - 管理策基準（別表３）
    - 27001,27002,27017の管理策をベースにCCMにマップ
    - 管理策基準の修正分・追加分を考慮する
  - マネジメント基準(別表2)
    - マネジメント基準は27001の情報セキュリティ管理プロセスをカバーしている
    - 別表2と27001の管理プロセスのマッピングを行い、それをベースにCCMにマッピングする
  - ガバナンス基準(別表1)
    - 別表 はガバナンスの基準でありCCMの管理策とは異なる
    - ISMAPで記述しているNIST SP-800 53 とのマッピングにおいても別表１は考慮されていない
    - したがって、別表１とCCMとのマッピングは行わない
- リバースマッピング方針
  - マッピング情報をもとに作業

CCM、ISMAP　リバースマッピング方針　(1)

- CSA本部のリバースマッピング方針
  - リバースマッピングの3ステップ
    1. ターゲットの規格の管理策にCCMをマップ
    2. 双方の規格の間のギャップを分析
    3. 補完する管理策の検討

  したがって、単純に逆方向へのマッピングを行うだけでなく、双方の管理策間のギャップ（CCMではカバーできていないところ）を明確にし、今後の検討に活かす：

  - ギャップの種類
    - No Gap：　ギャップ無し。CCMの管理策で当該規格の管理策を完全カバー
    - Partial Gap：　一部ギャップあり、CCMの管理策では不足部分がある
    - Full Gap：　完全ギャップ。CCMの管理策ではカバーされていない

  - リバースマッピングの例
    - ISO/IEC 27002,27017,27018 -> CCM

CCM、ISMAP　リバースマッピング方針　(2)

ギャップ分析

CCM管理策へのリバースマッピング

ギャップ説明

補完考慮点

	ISO 27002, 27017, 27018						
	Standard	ID	Control	Gap Identification (Full, Partial or No Gap)	Controls Mapping	Gap Analysis	Compensating Controls
3	27002	5.1.1	Policies for information security	No Gap	GRM-06	The controls proposed fully cover the security objective of 5.1.1.	
4	27002	5.1.2	Review of the policies for information security	No Gap	GRM-08 GRM-09	The controls proposed fully cover the security objective of 5.1.2.	
1	27002	6.2.2	Teleworking	Full Gap		No equivalent control(s) exists in CCM. EU-SEC mapping to HRS-05 does not match any of the requirements of 6.2.2.	
6	27002	7.2.3	Disciplinary process	No Gap	GRM-07	The control proposed fully cover the security objective of 7.2.3.	
7	27002	7.3.1	Termination or change of employment responsibilities	Partial Gap	HRS-04	HRS-04 control has currently vague and confusing content, it is neither clear to whom this control applies to (is it human resources personnel "for performing" the termination? is it all employees?), nor to the time period it concerns,	The following portion is proposed to be added to the addendum: "Information security responsibilities and duties that remain valid after termination
	27002	8.1.1	Inventory of assets	No Gap	DCS-01 GRM-04	The controls proposed fully cover the security objective of 8.1.1.	

CCM、ISMAP　リバースマッピング方針　(3)

- CCM、ISMAP　リバースマッピング方針
  - CSA本部のリバースマッピング方針に従って以下の3ステップで実施
    1. ターゲットの規格の管理策にCCMをマップ
    2. 双方の規格の間のギャップを分析
    3. 補完する管理策の検討

CCM、ISMAP　作業現状

CCM V3.0.1へのISMAPマッピング作業の問題

- 既存のCCMとISO/IEC 270xxのマッピングをISMAPのマッピングに適用した場合の違和感

  - 既存のCCMのマッピングを踏襲した場合の説明
    ISMAPのマッピングとして適当なのかどうか？

  - ISMAPの管理策を独自にCCMにマッピングした場合の整合性
    ISMAP の観点でISO/IEC 270xxとのマッピングを見直し、既存のCCMのマッピングと整合性をとれるようにすべきか？

WGとして上記の壁が解決できず、マッピング作業を諦める方向

4.　本日のまとめ

本日のまとめ

- 大きく、以下の2点をとらていただきたい

1. STAR認証のビジョン
   - 認証の継続型
   - 認証における透明性と高い保証
   - 相互認証スキーム
2. 相互認証性の取り組みとISMAP
   - グローバル視点の対応
   - 包括的な認証に向けての取り組み

ありがとうございました！

https://cloudsecurityalliance.jp
info@cloudsecurityalliance.jp