WG活動報告1

「ISMAPタスクフォースに関するWG活動報告」

CSA運営委員、CCM/STARワークグループリーダ
笠松　隆幸

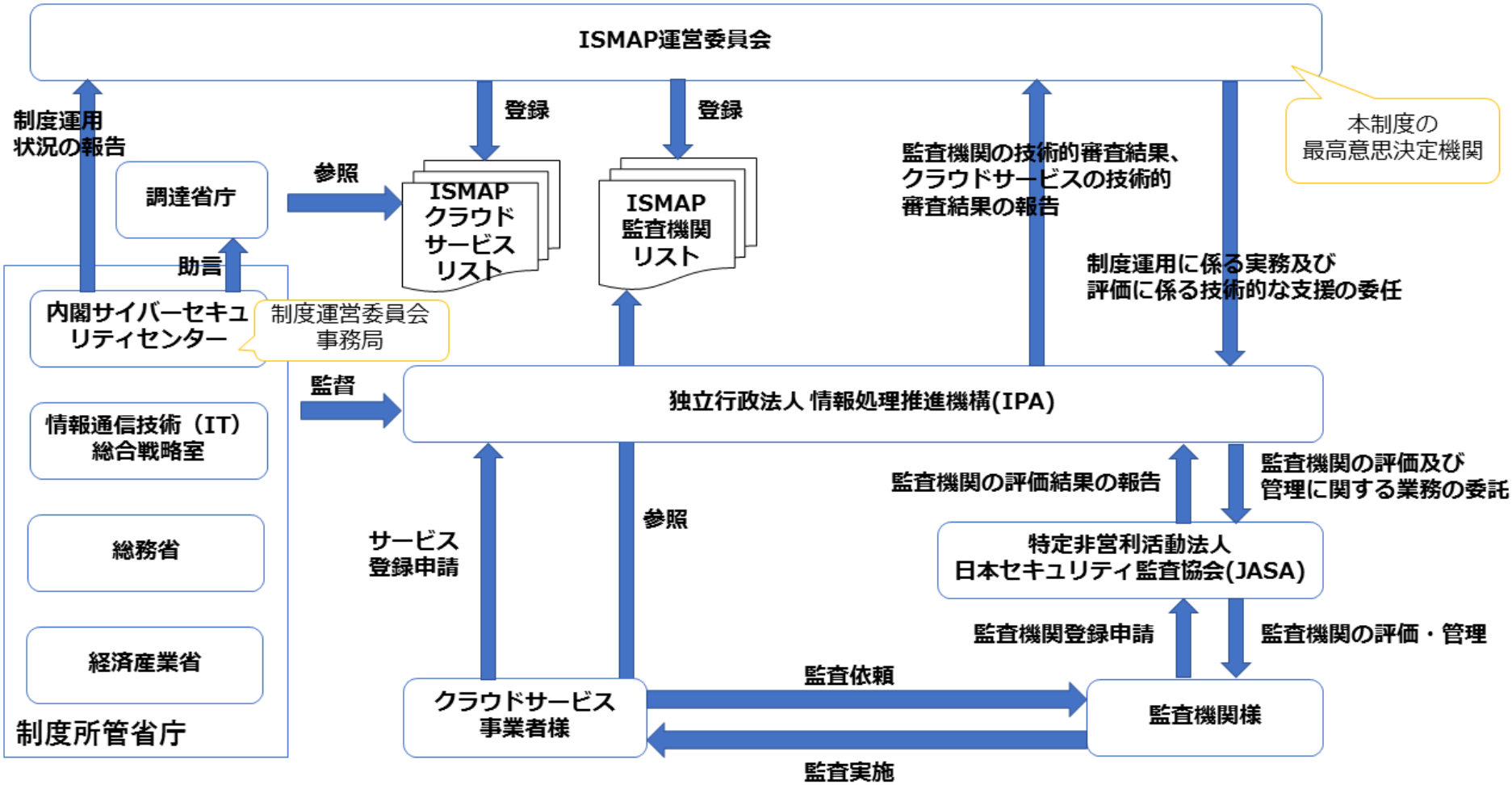
日本クラウドセキュリティアライアンス
（CSAジャパン）

ISMAPに関わる国側の経緯

- **設立**
  - 2019年6月、 2019年度に実証実験、2020年に利用開始と閣議決定。
  - 2020年6月、NISC・内閣官房情報通信技術（IT）総合戦略室・総務省・経済産業省は、「政府情報システムのためのセキュリティ評価制度：Information system Security Management and Assessment Program、以下ISMAPと言う。）を立上。
  - 2021年3月、初回となる「ISMAPクラウドサービスリスト」の登録・公開を行い、政府機関による本制度の利用を開始した。

- **6者の役割**
  - ① ISMAP委員会は、規定等の改廃決定、リスト登録の決定を行う。
  - ② NISCは、ISMAP委員会事務局を設置し、委員会の会合を開催する。
  - ③ クラウドサービス事業者は、ISMAP登録規則に基づいて、登録申請を行う。
  - ④ ISMAPの監査機関は、ISMAPのセキュリティ監査基準等に基づいて、審査する。
  - ⑤ IPAは、ISMAPクラウドサービスリストに追加登録などリスト運用管理を行う。
  - ⑥ システム調達者は、原則、「ISMAPクラウドサービスリスト」に登録されているクラウドサービス事業者から調達する。

ISMAP運営委員会と関連組織の役割



デジタル庁が関与する、クラウドシステムの例

大分類	小分類	A. 整備方針の策定	B. デジタル庁の統括・監理	C. 個別システムの整備・運用	D. 一括予算計上（注）	備考
(1)国のシステム	①デジタル庁システム	○	○	デジタル庁が整備・運用	○	国、独法、地方公共団体、準公共の民間事業者が相互に連携するためのシステムを含む
	②デジタル庁・各府省共同プロジェクト型システム	○	○	デジタル庁が整備、各府省が運用	○	
	③各府省システム	○	○	各府省が整備・運用	×（※）	※R４年度以降の取扱いは、一括計上の方向で検討
(2)独法のシステム	①国の交付金が交付されるシステム	○	○	各府省が交付金執行、独法が整備・運用	△（※）	※運営費交付金以外の交付金の場合は、一括計上可能か
	②上記以外のシステム	○	△（デジタル庁が指導・助言）	△（デジタル庁が指導・助言）	×	独法が整備・運用
(3)地方公共団体のシステム	①国の補助金が交付されるシステム	○（※）	○	各府省が補助金執行、地方が整備・運用	○	※標準化法の基本方針は、総務省と共同で策定
	②上記以外のシステム	○	×	×	×	地方が整備・運用
(4)準公共分野（重点計画で指定、国費が措置）の民間事業者のシステム	①緊急に整備を要する等のシステム	○（各府省と共同）	○	デジタル庁・各府省が共同で整備、事業者が運用	○	※整備の緊急性の度合い等に応じ、様々な整備のあり方を想定
	②上記以外のシステム	○（各府省と共同）	×	×	×	事業者が整備・運用
(5)(4)以外の民間事業者のシステム	①相互連携分野の民間事業者が利用するシステム	△（標準を策定）	△	×	×	事業者が整備・運用
	②上記以外のシステム	×	×	×	×	事業者が整備・運用

（注）(1)国のシステムの①②の「一括予算計上」に関して、R３年度は、デジタル庁に予算計上。ただし、特会で管理している経費など、現時点で各府省のシステムとは別に特定の事業と一体的に整備、運用されているシステムについては、各府省に予算計上。また、(2)独法、(3)地方公共団体、(4)準公共分野の「一括予算計上」については、R４年度以降の取扱いを検討。

デジタル庁が関与する、マイナンバー事務の例

住民基本台帳・マイナンバー・公的個人認証関係事務の概要

		住民基本台帳（住民基本台帳法）	マイナンバー（番号法）	マイナンバーカード（番号法）	公的個人認証（公的個人認証法）
制度		●住民基本台帳の整備 ●住民基本台帳ネットワークを通じた個人情報の提供範囲の規定 ●住民票コードの指定・通知 ●情報提供ネットワークへの住民票コードの提供	●マイナンバーの生成・付番、通知（総） ●マイナンバーの利用範囲、特定個人情報の提供範囲の規定（内） ●情報提供ネットワークシステムの設置管理（総） ●マイナポータルの設置運用（内）	●マイナンバーカードの交付 ●マイナンバーカードの発行、失効管理 ●ICチップ空き領域の利活用	●電子証明書の交付 ●電子証明書の発行、失効管理 ●電子証明書の失効情報の提供
所管府省		●総務省（住民制度課）	●内閣府（番号制度担当室） 総務省（住民制度課、個人番号企画室）	●総務省（住民制度課）	●総務省（住民制度課）
組織	J-LIS業務内容	●住民基本台帳ネットワークシステムの管理 ●住民票コードの指定・通知 ●情報提供ネットワークシステムへの住民票コードの提供	●マイナンバーの生成 ●付番システムの管理 ●個人番号通知書の送付	●マイナンバーカードの発行・失効管理 ●カード管理システムの管理	●電子証明書の発行、失効管理 ●JPKIシステムの管理 ●電子証明書の失効情報の提供
組織	監督	●総務大臣への業務方法書、予算、事業計画等の届出、総務大臣による違法行為等の是正要求【組織法上の監督】 ●総務大臣による管理規程認可、監督命令、報告聴取、立ち入り検査等【作用法（住基法・番号法・公的個人認証法）上の監督】			
予算（R2当初）	内閣官房		●マイナポータル設置運用経費		
予算（R2当初）	総務省		●情報提供ネットワークシステム設置運用経費		
予算（R2当初）	J-LIS	（地方自治体の負担金） ※住基ネットシステムの管理経費	●個人番号通知書送付経費	●カード管理システム・JPKIシステム設置運用経費 ●マイナンバーカード等の作成・送付、申請受付経費等 （地方自治体の負担金、利用料） ※公的個人認証の運営経費	
予算（R2当初）	市区町村	●市区町村システム改修経費（マイナンバー制度導入時等）		●カード・電子証明書の交付に要する人件費、臨時窓口設置経費等	

デジタル庁が関与する、ベースレジストリの例

- ベース・レジストリとは、公的機関等で登録・公開され、様々な場面で参照される、人、法人、土地、建物、資格等の社会の基本データ。台帳等に相当する。
- 発信者や情報の真正性、完全性等を保証するための機能。

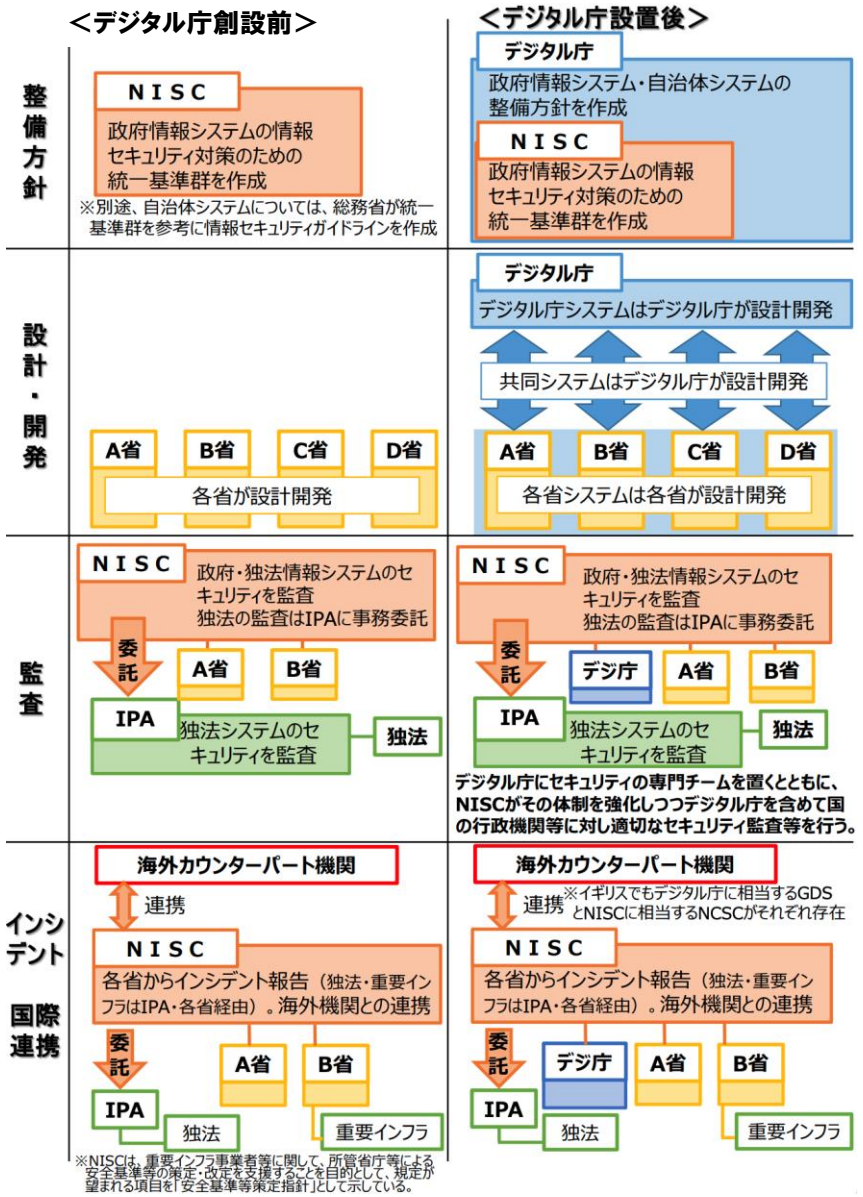
	ID	認証	電子署名等			
個人	○ マイナンバー法 （マイナンバー）	○ 公的個人認証法 （電子利用者証明）	○ 電子署名法 （電子署名） 公的個人認証法 （電子署名）	ー	○ 電子委任状法	ー （タイムスタンプ） ※文書作成時刻の署名
所管府省	総務省 ※ＪＬＩＳ	総務省 ※ＪＬＩＳ	総務省、 法務省、経産省 総務省 ※ＪＬＩＳ	－	総務省、経産省	－
法人	○ マイナンバー法 （法人番号）	○ （GビズＩＤ） ※法人以外に、個人事業主も含む	○ 商業登記法 （法人代表者の電子証明書）	ー （eシール） ※法人の電子証明書	○ 電子委任状法	ー （タイムスタンプ） ※文書作成時刻の署名
所管府省	国税庁	経産省	法務省	－	総務省、経産省	－

デジタル庁の動向と構想段階時の役割の例

2021年9月1日、デジタル庁が創設
- ✓ 10月22日、マイナンバー改善WGを開催
- ✓ 10月25日、データ戦略WGを開催
- ✓ 11月05日、新重点計画の意見募集
- ✓ 11月09日、デジタル臨時行政調査会を開催

ISMAP
発注業者選定基準

ISMAP
監査業者選定基準



ISMAPに関わるCSA側の経緯

- 2014年6月、クラウドのセキュリティ基準としてCCM (Cloud Control Matrix) を公開
- 2019年1月、CCM-ISO (27002,27017,28018) の日本語マッピングを公開
- 2021年8月、CCM–ISOマッピング表に、ISMAPの管理策を追加し公開
  - 課題1:ISMAPのセキュリティ基準は国際標準等を踏まえて策定と有るが、どの国際標準か、どの箇条か、クラウド事業者は具体的に把握し難い状況。
  - 課題2:ISMAP登録者は、海外クラウド事業者と、システム構築する事業者。

今回、CSA日本支部のISMAPワークグループで行ったマッピング

CCM3.0.1

16ドメイン	133コントロール
AIS	4
AAC	3
BCR	11
CCC	5
DSI	7
DCS	9
EKM	4
GRM	11
HRS	11
IAM	13
IVS	13
IPY	5
MOS	20
SEF	5
STA	9
TVM	3

×

国際標準等

- Net, Comp, Storage, App, Data
- SaaS, PaaS, IaaS
- ISO27001, ISO27002, ISO27017, ISO27018
- BSI, COBIT, FedRAMP, HIPAA, SP800-53, PCI-DSS etc.

×

ISMAP管理基準

- コントロール基準
- マネジメント基準
- ガバナンス基準

CCM (Cloud Control Matrix) とは

- CCMとは、
  - 米CSA本部が、CSAガイダンスで書き出した要求事項をもとに、クラウド固有の問題について、各種国際標準との対応をまとめた「マトリクス」である。
  - CCM1.0ではクラウドのセキュリティ基準を14の領ドメインに分け、その後、CCM3.0 では2項目を追加し16のドメインで対応付けを行っている。
    - 特に、CCM3.0において追加されたドメインには、 AICPA（米国公認会計士協会）が定めたSOC2（ITサービス企業における内部統制）の評価指標もあり、ITガバナンスとの関係付けも可能になった。
    - また継続して、各コントロールとアーキテクチャとの対応付けと、各コントロールと各サービスモデルとの対応付けも行っている。

- CCM-ISMAPマッピングとは、
  - CCM3.0.1とISO (27001, 27002,27017,28018) とのマッピングに、ISMAP管理基準の対応付けをしたものである。

ISMAPワークグループの成果物の紹介1

■ CCM3.0では、16のドメインでセキュリティ基準の対応付けを行った。

No	C-ID	Domain	ドメイン名
1	AIS	Application & Interface Security	アプリケーションとインターフェースセキュリティ
2	AAC	Audit Assurance & Compliance	監査保証とコンプライアンス
3	BCR	Business Continuity Management & Operational Resilience	事業継続管理と運用レジリエンス
4	CCC	Change Control & Configuration Management	変更管理と構成管理
5	DSI	Data Security & Information Lifecycle Management	データセキュリティと情報ライフサイクル管理
6	DCS	Datacenter Security	データセンタセキュリティ
7	EKM	Encryption & Key Management	暗号化と鍵管理
8	GRM	Governance and Risk Management	ガバナンスとリスク管理
9	HRS	Human Resources	人事
10	IAM	Identity & Access Management	アイデンティティとアクセス管理
11	IVS	Infrastructure & Virtualization Security	インフラと仮想化のセキュリティ
12	IPY	Interoperability & Portability	相互運用性と移植容易性
13	MOS	Mobile Security	モバイルセキュリティ
14	SEF	Security Incident Management, E-Discovery, & Cloud Forensics	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	STA	Supply Chain Management, Transparency, and Accountability	サプライチェーンの管理、透明性、説明責任
16	TVM	Threat and Vulnerability Management	脅威と脆弱性の管理

ISMAPワークグループの成果物の紹介2

■ CCMのマッピング項目例1

ドメイン区分

コントロールの内容

アーキテクチャとの対応付け

ガバナンスとの対応付け

サービスモデルとの対応付け

実施対象者との対応付け

Control Domain	CCM V3.0 Control ID	Updated Control Specification	日本語訳	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	AICPA 2009 TSC Map
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 programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	アプリケーションプログラミングインタフェース（API）は、業界の認める標準（例えばWebアプリケーションの場合、OWASPなど）に従って、設計、開発、導入及びテストしなければならない。また、APIは該当する法令上及び規制上の遵守義務に従わなければならない。			X	X	X	X		X	X	X	X		S3.10.0 S3.10.0
Application & Interface Security	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and	データ、資産、情報システムへの顧客のアクセ	X	X	X	X	X	X	X	X	X	X	X	X	S3.2.a

ISMAPワークグループの成果物の紹介3

- CCMのマッピング項目例2

AICPA（SOC2）

BSIとの対応付け

CCM1.0との対応付け

COBITとの対応つけ

FedRAMPとの対応付け

HIPPAとの対応付け

ISOとの対応付け

Scope Applicability										
AICPA 2009 TSC Map	AICPA Trust Service Criteria (SOC 2SM Report)	AICPA 2014 TSC	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	Canada PIPEDA	CCM V1.X	CIS-AWS-Foundation v1.1		
S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	CC7.1	I.4	G.16.3, I.3		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	SA-04			
S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined p lated security policies.									

CIS-AWS-Foundation v1.1	COBIT 4.1	COBIT 5.0	CSA Guidance V3.0	FedRAMP Security Controls (Final Release, Jan 2012)	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	FERPA	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001:2013	ISO/IEC 27002:2013	ISO/IEC 27017:2015	ISO/IEC 270018:2015
	AI2.4	APO09.03 APO13.01 BAI03.01 BAI03.02 BAI03.03 BAI03.05 MEA03.01 MEA03.02	Domain 10	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-14	NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SC-2 NIST SP 800-53 R3 SC-4 NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18)		1.2.6	45 CFR 164.312(e)(2)(i)	A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2	9.4.2 9.4.1 12.6.1 14.2.1 14.2.3 14.2.7 18.2.2	9.4.1 12.6.1 14.2.1	
		APO09.01 APO09.02 APO09.03	Domain 10	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1)	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1)		1.2.2 1.2.6 6.2.1		A9.1.1.	9.1.1		

ISMAPワークグループの成果物の紹介4

■ CCMのマッピング項目例3

ISOとの対応つけ

SP800-53との対応付け

PCI-DSSとの対応付け

ISMAPとの対応付け

ISO/IEC 27001:2013	ISO/IEC 27002:2013	ISO/IEC 27017:2015	ISO/IEC 270018:2015	NIST SP800-53 R3	NIST SP800-53 R4 App J	PCI DSS v2.0	PCI DSS v3.0	PCI DSS v3.2	NIST 800-53 R4 Moderate	AICPA TSC 2017	FedRAMP R4 Moderate	ISMAP	Scope applicability Gap between ISMAP and ISO
A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2	9.4.2 9.4.1 12.6.1 14.2.1 14.2.3 14.2.7 18.2.2	9.4.1 12.6.1 14.2.1		SC-2 SC-3 SC-4 SC-5 SC-6 SC-7 SC-8 SC-9 SC-10 SC-11 SC-12 SC-13 SC-14 SC-17 SC-18 SC-20 SC-21 SC-22 SC-23	AR-7 The organization designs information systems to support privacy by automating privacy controls.	6.5	6, 6.5	6; 6.5	RA-5 SA-3 SI-2 SI-10	CC8.1 CC7.1 CC3.1	RA-5 SA-3 SI-2 SI-10	<Control> 14.2.1 14.2.3 14.2.7 <Management> 4.5.4.4 4.5.4.5 4.5.5.1	<Control> 推奨：ISMAPとして削除と判断した 9.4.1 9.4.2 12.6.1 18.2.2 <Mangement> 推奨：ISMAPとして削除と判断した 4.5.4 4.5.4.1 4.5.4.2 4.5.4.3 4.5.5.2 推奨：ISMAPとして追加と判断した 4.5.5.1
A9.1.1.	9.1.1			CA-1 CA-2 CA-5	AP-1 The organization determines and		4.1.1, 4.2, 4.3	4.1.1; 4.2; 4.3		CC6.1 CC6.2 CC6.3		<Control> 9.1.1 18.1.1	<Control> 推奨：ISMAPとして追加と判断した 18.1.1

CCM-ISMAPマッピングの使い方

- ISMAP登録申請を希望する場合、以下の視点でチェックすると良い。

① クラウド固有の要求事項をチェックする
  - CCM／CAIQチェックリストによるチェック

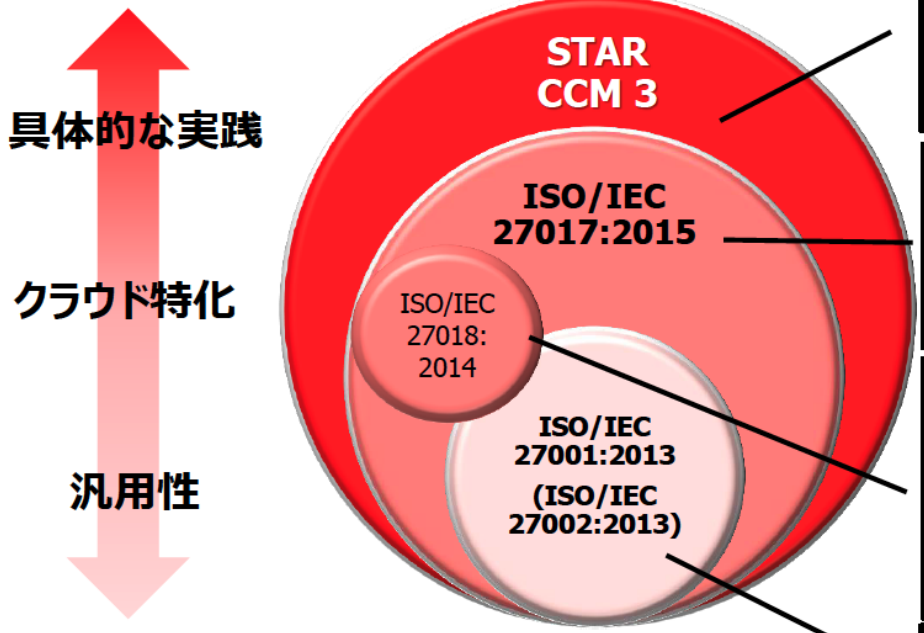
② 既存の管理策でクラウド固有の問題がカバーされているかチェックする
  - 既存の標準コントロール →対応するCCMコントロールのチェック（CAIQチェックリスト）

③ 国際標準等を基にクラウド固有の実装レベルを決める
  - 既存の標準コントロール →対応するCCMコントロール→対応する実装基準のコントロール（例えば、FedRAMP, SP800-53など）

対応付けの国際標準等の例

- マトリクスに記載された標準コントロールを実装する場合には、より抽象的な標準→CCM→実装基準の順に参照するといい
  - 例: ISO/IEC27001 → CCM → SP800-53
    - “AICPA TS Map”
    - “AICPA Trust Service Criteria (SOC2 SM Report)”
    - ”BITS Shared AssessmentsSIG v6.0”
    - CCM V1.X
    - COBIT 4.1
    - CSA Enterprise Architecture / Trust Cloud Initiative
    - CSA Guidance V3.0
    - ENISA IAF
    - ”FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--”
    - ”FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--”
    - GAPP
    - HIPAA / HITECH Act
    - ISO/IEC 27001
    - Jericho Forum
    - NERC CIP
    - NIST SP800-53 R3
    - NZISM
    - PCI DSS v2.0

既にあったクラウドセキュリティの評価制度



Cloud Controls Matrix (CCM)
CSAガイダンスの16のドメインに則したクラウドサービスにおける133の情報セキュリティ仕様（CSPが利用）
CSAに認可された認証機関によるSTAR**成熟度**審査

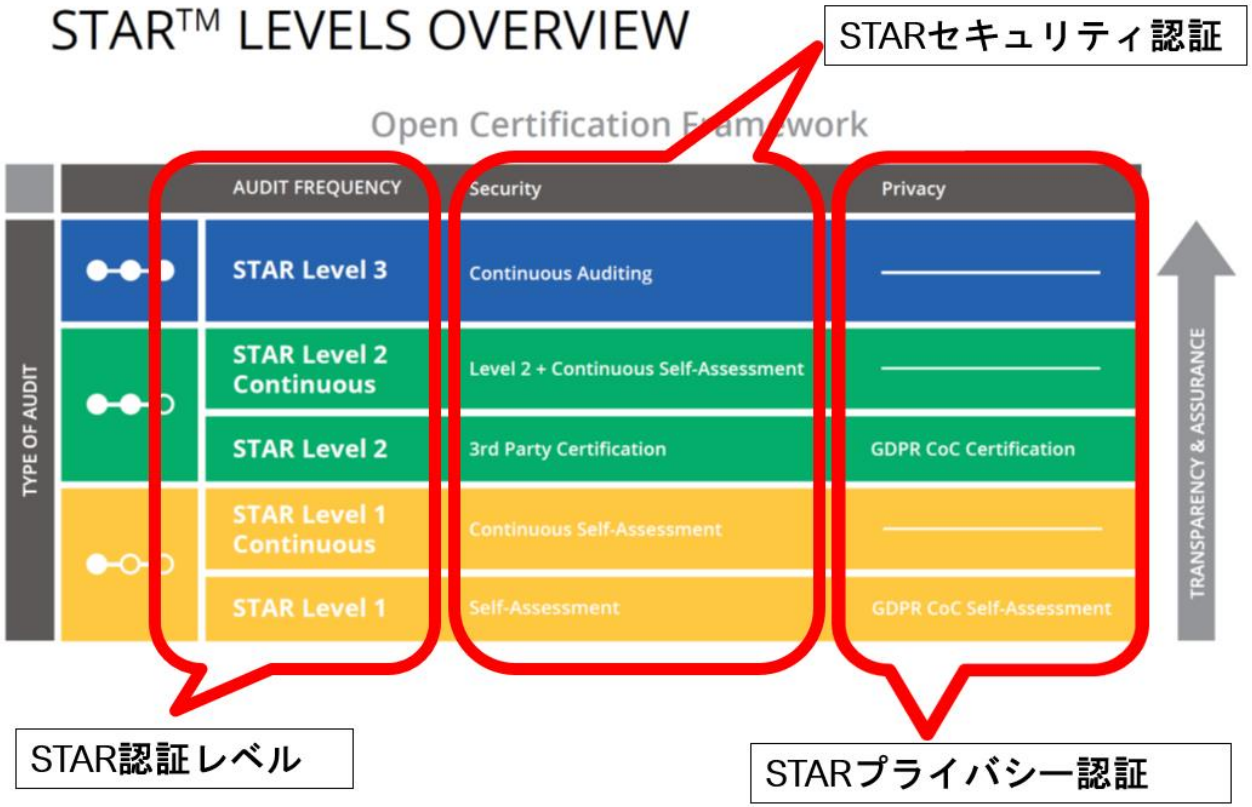
クラウドサービスにおける情報セキュリティリスクの管理ガイドライン
ISO/IEC 27001の管理策に対応した37の管理策と7の拡張管理策（CSC及びCSPが利用）
認定された認証機関による適合性審査

パブリッククラウドのPII保護における情報セキュリティリスクの管理ガイドライン
ISO/IEC 27001の管理策に対応した16の管理策とISO/IEC 29100のプライバシー原則に対応した25の拡張管理策（パブリッククラウドでPIIを処理するCSPが利用）
認証機関の非認定による適合性審査

情報セキュリティマネジメントシステム
35の管理目的及び114管理策（汎用的）
認定された認証機関による適合性審査

CCMに関わる CAI、CAIQ、 STAR とは

- CAI (Consensus Assessment Initiative) は、CAIQを使用してユーザと事業者が相互の対応状況を確認するもの
- CAIQ は、CCMの各コントロールの内容をブレークダウンし、チェックリスト化したもの
- STAR Level1は、CAIQをもとに、事業者が自己チェックを行った内容を公開する制度



CSA STAR Level1セルフアセスメントの公開サイトの紹介

- STAR Level1セルフアセスメントの重要性および日本語での評価レポートの公開方法について、ブログしています。
- CSAは、STAR Level1セルフアセスメントとしてプロバイダが自己評価した結果を、CSAが提供しているCAIQ(Consensus Assessment Initiative Questionnaire)に、を記述し、
  - それを公開するウエブサイト(CSA STAR Registry: https://cloudsecurityalliance.org/star/registry/)を提供しています。
- またCSAジャパンでは、日本のプロバイダが積極的にセキュリティ情報を公開できるように以下の2つの支援をしています。
  - 日本語CAIQ評価レポートの登録手順を日本語で提供
    STAR Level1 セルフアセスメントの登録手続きは、英語で行う必要がありますが、一連の手順を日本語で紹介しているウエブサイトを参照してください。
    https://www.cloudsecurityalliance.jp/site/?page_id=1005
  - 日本語 CAIQ評価レポートを公開されているプロバイダとクラウドサービスの情報を公開
    CSA STAR Registryには、すべてのクラウドサービスの情報がアルファベット順にリストされていますが、日本語で探すことは難しく、以下のウエブサイトにを参照。
    https://www.cloudsecurityalliance.jp/site/?page_id=19811

お知らせ：8月からCCM4.0.2で、新たなマッピングを開始しました

WG名	CCM/STAR
WG開設年月	2021年8月から2022年3月
WGリーダ名	笠松　隆幸 （tkasamatsug@gmail.com）
WG目的	CSA日本支部として独自の検討を加え、CCM4.0.2/ISMAPのマッピングを作成し、リリースする
WG概要	「政府情報システムのためのセキュリティ評価制度（ISMAP）」は、「日本版FedRAMP」とも呼ばれ、日本政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、クラウドサービス調達におけるセキュリティ水準の確保を図り、円滑な導入を目的とした制度です。 WGでは、米国CSA本部が作成した「CCMにおける国際規格ISO27000シリーズの管理策とISMAP管理策のマッピング表（CCM4.0.2）」について、CSA日本支部が独自に13分野/133管理策のマッピングを見直し、国内CCM準拠のクラウド事業者へ分かり易いマッピングを提供していくことを目標とし、Gap分析を行います。
WG実施形態	月1回をベースに、対面会議またはオンライン会議で実施する。
WG参加条件（アプリ/メルアド等）	オンライン会議Teams、会議案内Slack、会員チャットSlack、フォルダー共有OneDrive、成果物Office365のアプリを使用。 （注1）WG用ツールは、無料のWeb版と有料のデスクトップ版、どちらも可能です。 （注2）WG用IDは、CSA会員登録したメルアドを利用すること。個人ID、会社ID、客先IDなど複数の使い分けに注意！ （注3）WG用PCは、個人PCと会社貸与PC、どちらも可能ですが、貸与PCはツールのインストール制限に注意！ （注4）WG用回線は、有線1Gの回線を推奨、無線LTE・4G・5G等は電波状況により切れる事に注意！
参照規格等	ISO27001、ISO2702、ISO27014、ISO27017、ISMAP
スケジュール予定	月1回開催し、各1時間30分を予定。 MAX10回で終了し、成果物をCSA日本支部としてリリース予定。 スケジュールは、2021年8月に第1回キックオフ、その後1次レビュー、2次レビュー、成果物の修正方針を決定、成果物の文書校正、2月クロージング、3月「CCM4.0.2/ISMAP」版のリリースの予定。
WG参加のメリット	①リリース版に、協力者の本人名と会社名を記名できる。＞法人会員の方、会社貢献しましょう。 ②他の学会での論文発表に利用したり、教育機関や社会的施設等で講演・講義の資料として利用できる。 ③最新のCCMv4（翻訳）を公開前に読める。 ④クラウドサービス事業者に対してCCM/ISMAP管理基準の導入支援ができるように成る。

質疑応答