CCMv4とISMAP2021とのマッピング解説

CCMワーキンググループ　2022年度・活動報告

目　次

1章　マッピングの背景

① 1999年、Salesforceが今で言うSaaS形態のCRMを開始し、2006年Googleが検索エンジン戦略で「クラウド・コンピューティング」を初めて提唱し、様々なクラウドサービスが始まった。

- ✓ その後、IBM/サン・マイクロ/シスコ/SAP/EMC/AT&T/Amazon/Google/Microsoft/Oracle等による市場開拓と共に、各社毎のクラウド要求事項が氾濫し、実装チェックや監査コストが増加し、課題解決が求められた。

② 2014年、米国CSA本部がクラウド固有の要求事項をチェックする対応表を纏め、クラウド利用者・事業者に提供した。また、CSA地域支部（Americas, EMEA, APAC）が、地域の法令・通信規制等に合わせた支部版の提供も開始された。

③ 2018年、CSA日本支部は、CCMワーキンググループを設立し、CSA_STAR認証とのマッピングやISOとのマッピング、及び日本独自のISMAPとのマッピングを追加したCSA日本支部版を提供している。

- 2016年、米CSA本部のCCMv3（Cloud Control Matrix）を翻訳し、公開。
- 2018年、CCMガイドラインを策定し、勉強会を実施。
- 2019年、ISO27017に対するSTAR認証のガイダンスを策定、勉強会を実施。
- 2022年、CCMv4.0.2（16ドメイン/133管理策）とISMAP2021とのマッピングを行い、公開。

1-1 CCMマッピングに出て来る3大名称の定義

① CCM（Cloud Control Matrix）by CSA

- 「クラウドコントロールマトリクス」と言う。
- 2014年に「クラウドに必要な管理策とアーキテクチャ及びサービスモデル」を対応させ、米国CSA本部が公開した報告書名。

② STAR（Security, Trust and Assurance Registry）by ISO

- 「STAR認証」または「クラウドセキュリティ認証」と言う。
- 「ISO27001のアドオン認証」としてクラウドセキュリティの成熟度を評価する認証名。
- 成熟度に応じて、Level1（セルフアセスメント）Level2（第三者評価）Level3（継続的モニタリング）

③ ISMAP（Information system Security Management and Assessment Program）by 日本政府

- 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」と言う。
- 2018年に「ガバメントクラウドに関する政府方針」に基づき定めた方針名。

（捕捉） CCMマッピングとCAIQ及びCAIQ-Liteとの関係

① CCM（Cloud Control Matrix）
- CSAが提供する、クラウドセキュリティ管理策マップ
- 17ドメイン、197の管理策（V4.0.5）
- CCM日本語版を公開

② CAIQ（Consensus Assessment Initiative Questionnaire）
- CSAが提供する、CCMの管理策マップをブレークダウン
- 17ドメイン、261の管理策（V4.0.5）
- CAIQ日本語版を公開

③ CAIQ-Lite
- CSAが提供する、CAIQの縮小版
- 16ドメイン、310の管理策（V3.0.1）　＞v4策定中
- CAIQ-Lite日本語版を公開

2章　公開したCCMv4/ISMAP2021版マッピングの解説

① 2022年度のCCMワーキンググループは、CCMとISMAPのクラウド固有の要求事項をマッピングし、チェックする対応表を策定した。

a. 大分類として、クラウドセキュリティに必要な管理策を14ドメインに纏めた。
b. 中分類として、管理策14ドメインにアーキテクチャ及びサービスモデルと紐付けした。
c. 小分類として、各管理策に実施対象者（利用者・テナント・事業者）を明示し、クラウドサービス実装時の要求事項を紐つけした。
d. また管理策v3以降として、ガバナンス・ドメインを追加した。

② その他の標準（SOC2, COBIT, FedRamp, HIPPA, ISMS, PCIDSS）などクラウド実装に言及している基準とも対比できるようにした。

2-1 CCM管理策とアーキテクチャ等とのマッピング

ドメイン

管理策の内容

サービスモデルとの対応

アーキテクチャとの適用

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 assuranc and policies	Shared	Shared	Shared	TRUE	TRUE	TRUE	TI		

対応者/部門

言語選択フィルター

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

2-2 CCM管理策とISMAP管理策とのマッピング

ドメイン

ISMAP2021

CCM管理策とISMAP管理策とのGAP Identification
(Full Gap/Partial Gap/No Gap)

Control Domain	Control Title	Control ID		ISMAP Contoros Mapping	Gap Identification (Full, Partial or No Gap)	Gap Analysis CCMとISMAPのGapの内容、	Consideration ISO/200xx、FedRAMPとの違いについてのコメント	Language
Audit and Assurance -								
監査・保証	監査・保証の方針と手続き	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。	4.5.3 4.6.1 4.6.2 5.1.1 5.1.2	No Gap			JP
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。	3.1.6 4.6.2 18.2.1 18.2.3	No Gap			JP
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方針に従って、独立した監査と保証評価を実施する	3.1.6 4.4.6 4.4.7 4.6.2 18.2.1	No Gap			JP

2-3 CCM管理策とISO管理策及び海外管理策とのマッピング

ドメイン

CIS v8.0

AICPA TSC 2017

ISO27001/02/17/18

CLOUD CONTROLS MATRIX VERSION

			CIS v8.0			AICPA TSC 2017			ISO/IEC 27001/02/17/18		
Control Domain	Control Title	Control ID	Control Mapping	Gap Level	Addendum	Control Mapping	Gap Level	Addendum	Control Mapping	Gap Level	Addendum
Audit &											
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	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'.	CC2.2 CC2.3 CC3.2 CC5.3	Partial Gap	Missing specification(s) in TSC 2017: 'Review and update the policies and procedures at least annually'.	27001: 9.2	Partial Gap	Missing specification(s) in ISOs: Requirement of 'at least annually' in last sentence.
監査・保証	監査・保証の方針と手続き	A&A-01	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'.	CC2.2 CC2.3 CC3.2 CC5.3	Partial Gap	Missing specification(s) in TSC 2017: 'Review and update the policies and procedures at least annually'.	27001: 9.2	Partial Gap	Missing specification(s) in ISOs: Requirement of 'at least annually' in last sentence.

2-4 CCMマッピングの日本語版/英語版の公開先

- CCMワーククキンググループが作成したマッピング表は、以下でダウンロードできます。

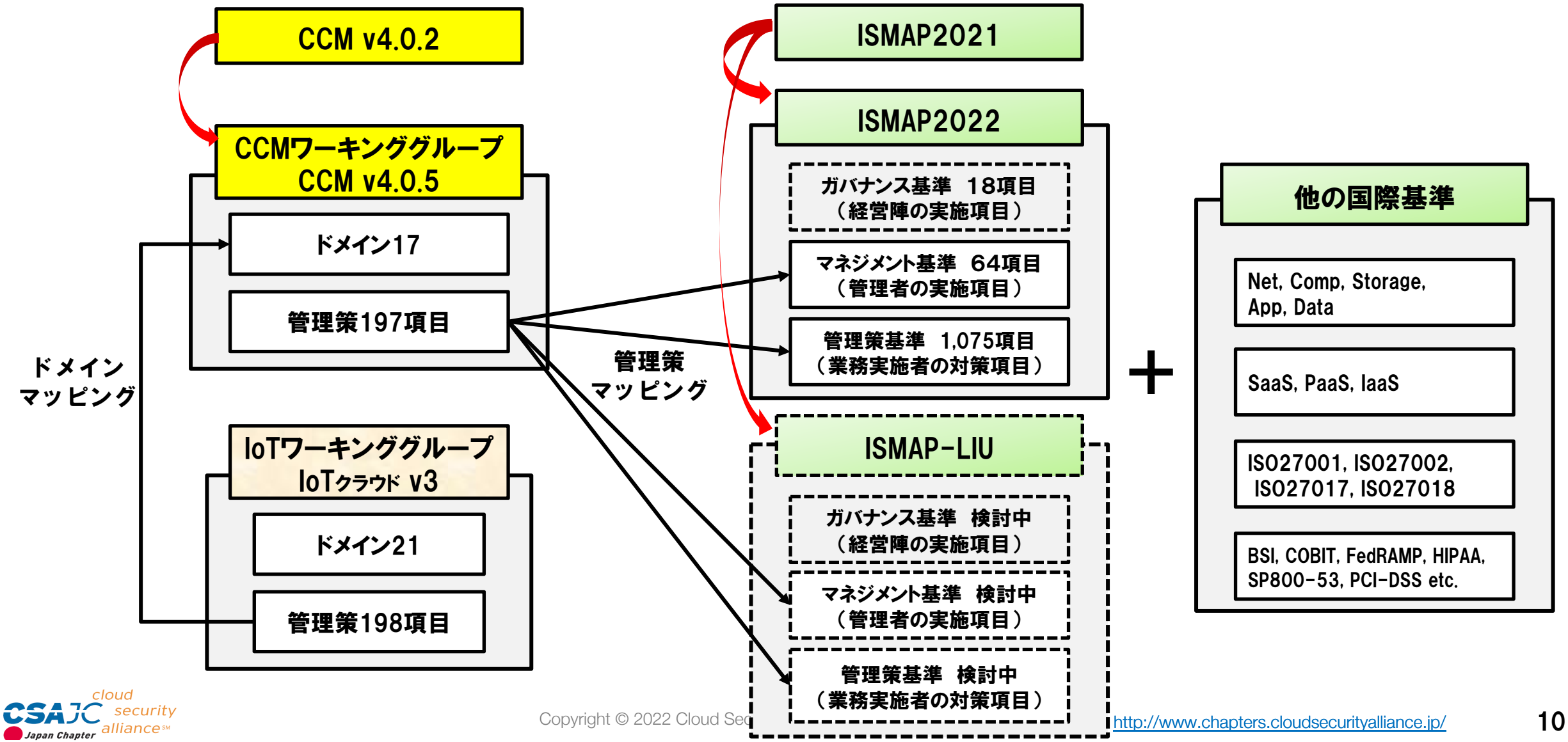
① 「日本語版；CCMv4とISMAP2021とのマッピング」は、CSA日本支部のWebサイトで公開しています。

- ダウンロード先
- https://www.cloudsecurityalliance.jp/site/?page_id=2048#ccm

② 「英語版；CCMv4とISMAP2021とのマッピング」は、米国CSA本部のWebサイトで公開しています。

- ダウンロード先
- https://cloudsecurityalliance.org/artifacts/csa-ccm-v4-0-addendum-ismap/

3章　次のマッピング計画2023について



3-1 マッピング基準となる新CCM4.0.5について

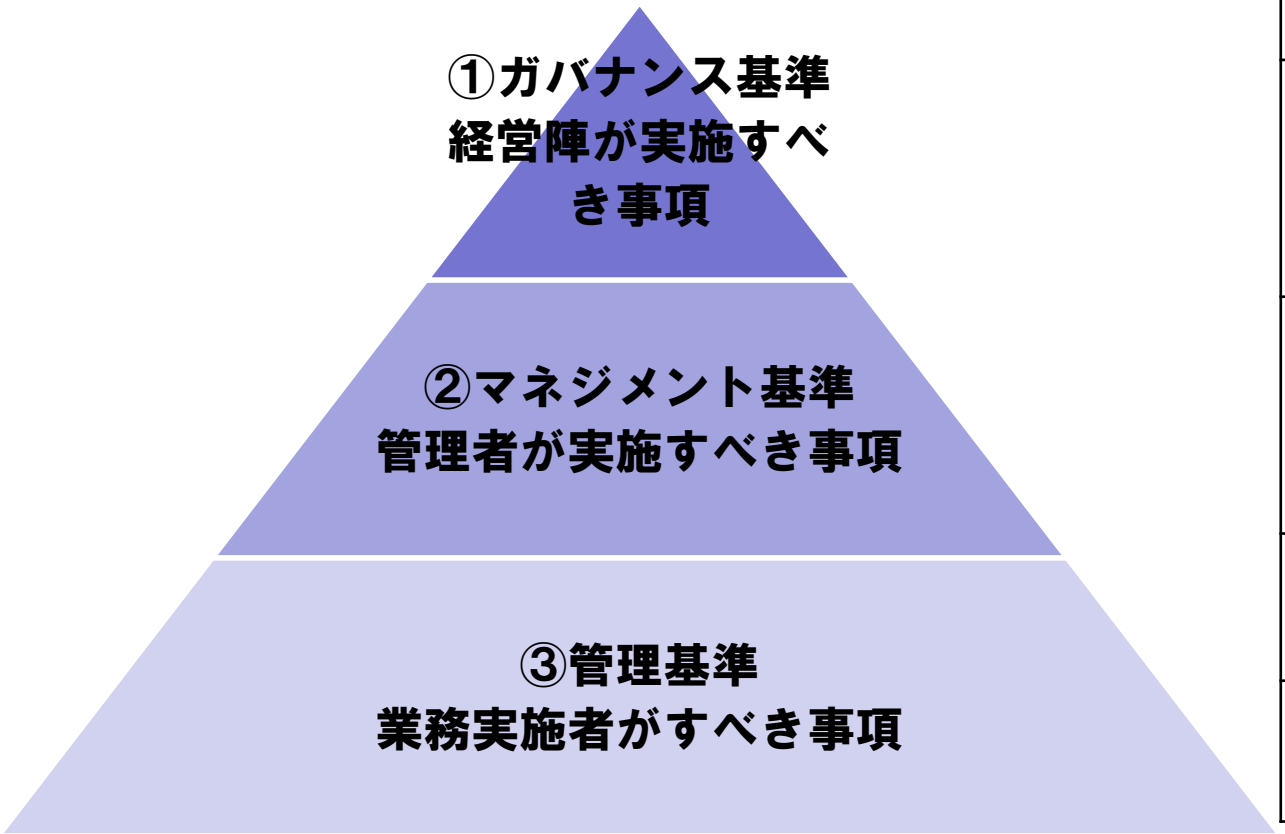
No	C-ID	Domain　4.0.5	ドメイン名
1	A&A	Audit & Assurance	監査と保証
2	AIS	Application & Interface Security	アプリケーションとインターフェースセキュリティ
3	BCR	Business Continuity Management & Operational Resilience	事業継続管理と運用レジリエンス
4	CCC	Change Control & Configuration Management	変更管理と構成管理
5	CEK	Cryptography, Encryption & Key Management	暗号、暗号化と鍵管理
6	DCS	Datacenter Security	データセンタセキュリティ
7	DSP	Data Security and Privacy Lifecycle Management	データセキュリティと プライバシーのライフサイクル管理（Privacy Guardと生産性）
8	GRC	Governance, Risk and Compliance	ガバナンス、リスクとコンプライアンス
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（エンドユーザ、エッジ端末、企業データ保護）
11	IPY	Interoperability & Portability	相互運用性と移植容易性
12	IVS	Infrastructure & Virtualization Security	インフラと仮想化のセキュリティ
13	LOG	Logging and Monitoring	ロギングとモニタリング
14	SEF	Security Incident Management, E-Discovery, & Cloud Forensics	セキュリティインシデント管理、Eディスカバリ及び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 & Vulnerability Management	脅威と脆弱性の管理 （自動化とセキュリティインサイト）
17	UEM	Universal Endpoint Management	統合エンドポイント管理（１つの管理コンソールで、PC・IoT・スマホを管理）

3-2 マッピング対象となるISMAPについて

- 2022年9月30日ISMAP改定基本方針では、
  - ① クラウドサービスの利用は、ガバメントクラウドを原則とする
    - ✓ 原則の優先度は、SaaSは優先高、IaaS/PaaSは優先中、オンプレは優先低
    - ✓ 自らサーバを構築せず、マネージドサービス利用又はコードにより自動生成し利用
    - ✓ 複数IaaS/PaaSのマルチクラウドは避ける
  - ② 「ガバメントクラウドを利用しない場合」は、ISMAP登録サービスを選択する
  - ③ 「ISMAP未登録である場合」は、 SaaSにおいて2021年７月６日サイバーセキュリティ対策推進会議・各府省情報化統括責任者連絡会議決定に係る暫定措置による対応に従い利用する
  - ④ 「暫定措置による対応も困難な場合」は、当該調達を行う政府機関等における最高情報セキュリティ責任者の責任において、管理基準を満たしていることを政府機関等で確認を行う
  - ⑤ 「ISMAP以外のクラウドセキュリティ認証」も検討する
    - ISMAP以外とは、以下の第三者による認証や監査フレームワークを示している。
      - 認証制　　ISO/27017 （STAR認証）、JASA CSマーク、米国 FedRAMP
      - 監査フレームワーク　　AICPA SOC2、AICPA SOC3、保証業務実務指針 3850

3-3 フル版ISMAP2022の留意点

①2021年7月にゼロトラストが追加



②監査頻度の基準

No	主たる監査対象	実施頻度の例
1	規定等	最低年１回
2	設計書、仕様書、手順書等 （根拠となる文書・記録等サンプルテストを実施しないもの）	最低年１回、 変更が発生した都度
3	申請書、承認記録、システムログ、台帳等） （根拠となる文書・記録 サンプルテストを実施するもの）	随時 （統制の性質に応じて、日次・週次・月次・四半期等に一度）
4	パラメータ、ステータス、コマンド等 （根拠となる設定等）	最低年１回、 変更が発生した都度
5	設備、建物等	最低年１回 （施設へのアクセスログ等は上記No.3に同じ）

3-4 簡易版ISMAP-LIUの留意点

① ISMAP-LIU（ISMAP for Low-Impact Use）とは、機密性2の情報でも比較的リスクが小さい業務・情報の処理を行うSaaS対象とする新たなセキュリティ要求の仕組みです。

- 一律にフルISMAPで扱った場合、過剰なセキュリティ要求となる
- 情報システムは、業務・情報の影響度に応じたセキュリティを確保すべきである
- 現在、パブコメと検討が行われ、2022年度に制度立ち上げ、申請受付開始する計画
- 当初10月公開予定としていたが、遅れている

② ISMAP-LIUの適用判断は、利用する業務・情報の影響度評価の提出を必須とし、2省庁により影響度評価が「低位」であることの妥当性有無を持って判断する。

- 影響度評価は、処理される各種情報において、機密性・完全性・可用性が損なわれた場合の影響度を示す。
- 業務・情報の影響度が低位である蓋然性が高い業務を「対象業務一覧」として制度より例示（制度開始当初は８項目）し、公開する。

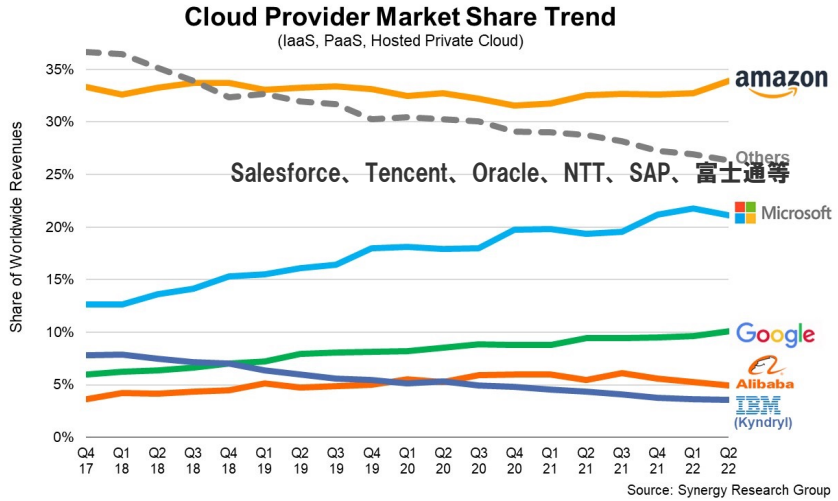
（補足） ISMAP-LIU制度開始当初の８項目とは

1. **公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務**
   有識者を招いた審議会等の運営を行うために、Web会議による会議運用や、ファイル共有による情報の保存・管理・共有を行う用途
2. **政府機関等職員の業務上の役職・氏名等情報を扱う業務**
   （業務の性質上、従事する職員の情報について厳格な秘匿が求められている場合を除く）
   政府職員の役職・氏名情報を用いて職員の人事管理やタレントマネジメントを行う用途
3. **名刺情報等の一般に広く提供する範囲の情報、及びユーザ名・パスワード・メールアドレス等の情報を扱う業務**
   企業名、役職、氏名等の名刺情報を登録・管理する業務
   政府機関等の顧客に対する映像・コンテンツ等の配信に伴う配信先の特定を目的としたユーザ登録・管理業務
4. **民間から提供される情報であり、当該情報提供者が低リスクだと判断している情報を処理する業務**
   民間企業・民間団体が利用しているWeb会議やファイル共有のためのSaaSを用いて、当該情報提供元企業が提供する情報の保存・管理を行う用途
5. **オープンソース・公知の事実・一般情報を扱う業務だが例外的に要機密扱いとする必要がある場合**
   Webサイトの公開前情報など、公開が予定されている情報であり、当該情報の公開が意思決定されている情報を扱う用途
   機械翻訳を用いて他国の政策情報や技術情報等を翻訳し調査を行う用途（政府の特定情報に対する調査傾向が要機密となる場合）
6. **災害時等に組織構成員の被災状況確認等を行う業務**
7. **組織構成員に対する組織ルールやビジネススキル等の教育を行う業務**
8. **「行政文書の管理に関するガイドライン」において保存期間１年未満に該当するもののうち、定型的・日常的な業務連絡等を扱う業務**
   政府機関等の掌握事務に対する事実関係の問合せへの応答業務

4章　マッピングに関わる動向

① デジタル庁は、 2022年10月03日「ガバメントクラウド」の応募選考の結果、海外企業4社を決定。

1. 「Amazon Web Services」　アマゾンウェブ ジャパン
2. 「Google Cloud Platform」　グーグル　クラウド　ジャパン
3. 「Microsoft Azure」　日本マイクロソフト
4. 「Oracle Cloud Infrastructure」　日本オラクル



② 応募要件は「ISMAP（政府情報システムのためのセキュリティ評価制度）の登録企業で、ISMAP調達仕様書（基本事項およびマネージドサービスの技術要件詳細）を満たすクラウドサービスを運営する事業者」となっていた。しかし2021年と2022年の募集に、国内企業の応募が無かったもよう。

4-1 デジタル庁が、アナログ規制の見直し方針を確定

① デジタル庁は、2022年末に、２年間で見直す工程表を策定し、公表

- 目視、実施検査　2,927条項の方針確定　（河川法、都市公園法等の見直し）
  河川やダム及び公園等に対し、ドローンや水中ロボットの巡視、防犯カメラの画像解析
- 定期検査・点検　1,036条項の方針確定　（建築物衛生法、ビル管理法、消防法等の見直し）
  建築物物内の衛生や消防設備に対し、IoTを活用した自動測定や常時監視
- 常駐・専任　1,058条項の方針確定　（労働安全衛生法、指定距宅サービス基準の見直し）
  作業主任者や介護サービスに対し、複数事業所の兼務可、テレワークやICT技術で代替
- 対面講習・立札　217条項の方針確定　（道路交通法、河川法施行令等の見直し）
  免許取得・更新や河川立札掲示に対し、ネット申込やネット動画講習や、Webサイト掲示
- その他、書面掲示768条項と往訪閲覧1,421条項の方針確定

② デジタル手続法の見直しとして、ＦＤ等記録媒体の政令省令1,602条項の方針確定
（税記録、裁判録等）

	個別の記録媒体の名称を含む規定							（参考）一般名称を用いる規定	
	合計	光ディスク	シー・ディー・ロム/シーディー・ロム	磁気ディスク	光磁気ディスク	フレキシブルディスク	磁気テープ	記録媒体	記録用の媒体
法律	**157**	23	0	110	0	0	24	241	12
政令	148	30	1	84	2	9	22	52	0
府省令	1,589	211	206	920	2	215	35	241	17
合計	**1,894**	264	207	1,114	4	224	81	534	29

4-2 中央省庁や地方自治体が、クラウド/SaaSへ移行事例

① 中央省庁の動き；文科省は、ITインフラの一部をクラウドSaaSへ移行した。

- MS Office から MS 365 へ移行。理由の1つに、職員が同時に共同編集できる機能があったこと。
- Skype から Slack へ移行。理由の1つに、上司や他部署に気軽にチャットで相談できる匿名Slack機能があったこと。
- オンプレのファイルサーバから box へ移行。理由の1つに、前年度に予算化してないと保存容量が増えても追加できなかったことの解消。

② 地方自治体の動き；自治体の基幹業務17を特定し、システムのクラウド移行を開始した。

- 最初に選択した基幹業務は、住民基本台帳システム、今年度からクラウドへ移行開始。
- その他16の基幹業務は、原則2025年度末までにクラウドへ移行終了。
  - ✓ 基幹業務システムは、国が仕様を定め各自治体に導入義務化。かつ導入後のカスタマイズ禁止も義務化としている。
  - ✓ 基幹業務17とは、住民基本台帳、選挙人名簿管理、固定資産税、個人住民税、法人住民税、軽自動車税、国民健康保険、国民年金、障害者福祉、後期高齢者医療、介護保険、児童手当、生活保護、健康管理、就学、児童扶養手当、子ども子育て支援。

4-3 自民党が、機密情報の国産クラウド採用を提言

① 機密情報に限って「プライベートクラウドも採用」

- 22年5月16日、自民党の政策提言「デジタル・ニッポン 2022」をデジタル庁に検討申入をした。
  - ✓ 提言は、機密情報に限ってガバメントクラウド原則を崩すとの考えを示している。
  - ✓ 行政の機密情報を扱う専用クラウド基盤の構築は、国産のクラウドサービスを採用するほか、データセンター内に政府専用区画を設けるプライベートクラウド技術なども採用としている。
  - ✓ 政府調達では機密情報を扱うプライベートクラウドとその他の行政情報を扱うパブリッククラウドを組み合わせることを想定。国産に限るのは、プライベートクラウドや、パブリッククラウドとの接続回線などとしている。

② 政府による機密性の格付

格付	基準	例
機密性3	行政事務で扱う情報資産の内、秘密文書に相当する機密性を要する情報	外交文書 防衛関連文書
機密性2	行政事務で扱う情報資産の内、秘密文書に相当する機密性は要しないが、漏洩により国民の権利が侵害され又は行政事務の遂行に支障を及ぼす恐れがある情報	マイナンバー
機密性1	機密性3、又は機密性3以外の情報	公表される行政情報 オープンデータ

（捕捉） 次期CCMワーキンググループの活動計画

WG名	CCMワーキンググループ（過去の会議体名：CCMwg, CCM/STARwg, CCM/ISMAPwg）
WG開設年月	2023年1月から2023年7月予定
WG目的	CSA日本支部として独自のマッピング項目を加え、CCM4.0.5と、ISMAP2022及びISO27001等の他基準も含めたマッピングを作成し、公開する。 ※ISMAP-LIUとのマッピングは、正規版公開時点で再検討
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4.0.5について、CSA日本支部が独自に17分野/197管理策とのマッピングを見直し、ISO27001/02/17/18の管理基準準拠及び国内CCM準拠のクラウド事業者へ、分かり易いマッピングの対応表を提供する。またCCMとISMAPとのGap分析を行う。
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、各1時間30分を予定。
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、共同編集Microsoft365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	CCM4.0.5、ISMAP2022、ISO27001、ISO2702、ISO27014、ISO27017、SOC、FedRampなど
スケジュール予定	月1回開催し、6回から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、2023年1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、7月クロージング、9月「CCM4.0.5/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。

ご清聴ありがとうございました

（紹介）Congress2022　CCMwgスピーカ

① 講演者名　　CSA日本支部・運営委員、CCMwgリーダ
笠松　隆幸（カサマツ　タカユキ）

② 講演の題名　CCMv4とISMAP2021とのマッピング解説（30分）

③ 講演の概要

- ✓ CCMワーキンググループは、2018年から活動し、国内外にあるクラウドセキュリティ管理策の比較を行い、マッピング（対応表）を策定してきました。
- ✓ 2021年は、CCMv3である16分野/133管理策と、ISO27002/27017/27018の管理策および日本国内法令等についてマッピングし、勉強会や公開を通して普及を行いました。
- ✓ 2022年は、CCMv4である17分野/197管理策と、政府情報システムのセキュリティ評価制度ISMAP2021ともマッピングし、本年10月に公開しました。
- ✓ 本日は、その概要をご紹介致します。