自治体DX時代の安全なクラウド活用
~ISMAPの在り方とAPPLICへの期待~

2021年6月15日
PwCあらた有限責任監査法人

pwc

講師紹介

加藤 俊直
Toshinao Kato

PwCあらた有限責任監査法人
システム・プロセス・アシュアランス部
パートナー
公認会計士 / システム監査技術者
公認会計士協会　情報セキュリティ等対応専門委員長

経歴等

- 製造業（自動車・ハイテク業界）、通信業、金融機関等を中心にサービスを提供し、米国上場企業に対するSOX 法監査、同法に基づくシステムアウトソーシング先監査・保証業務（SOC1、2）、プロジェクトの第三者評価などを数多く経験。
- 直近においては、大手の製造業や金融機関向けに、サイバーセキュリティ監査、ITガバナンス・マネジメントの評価及び高度化支援、自動車業界における外部委託先管理・評価に携わっている。
- 政府情報システムのためのセキュリティ評価制度（ISMAP）の監査ワーキンググループに参画し、中心的役割を果たす

川本 大亮
Daisuke Kawamoto

PwCあらた有限責任監査法人
システム・プロセス・アシュアランス部
パートナー
公認情報システム監査人 (CISA)

経歴等

- IT に関するアシュアランスおよびアドバイザリーサービスを日系・外資系企業に提供
- 内部監査、外部監査、US/J-SOXプロジェクト、セキュリティ評価、第三者に対する保証と意見表明サービスにおける、ITリスクの発見・評価の経験を豊富に有する
- 政府情報システムのためのセキュリティ評価制度（ISMAP）の監査ワーキンググループに参画
- 内閣府のデジタル市場競争会議に委員として参画

ISMAP制度設立の背景

政府情報システムのためのセキュリティ評価制度（ISMAP）は、以下の経緯で検討が開始されました。

2018 年 6 月より、政府調達においてクラウド・バイ・デフォルト原則を採用

- 政府情報システムは、**クラウドサービスの利用を第一候補**として、その検討を行う方針となった。

成長戦略、サイバーセキュリティ戦略等にて、安全性評価の検討を明記

- では、**官民双方**が一層安全・安心にクラウドサービスを採用し、継続的に利用していくため、**クラウドサービスの安全性評価について、諸外国の例も参考にしつつ、本年度から検討を開始** *1
- **政府全体としてクラウド化を推進**すること、クラウド化の推進に当たっては、**安全性評価など、適切なセキュリティ水準が確保された信頼できるクラウドの利用を促進**する方策について検討を進めることが明記 *2

*1 : 2018 年 6 月 15 日に閣議決定された「未来投資戦略 2018」
*2 : 2018 年 7 月 27 日に閣議決定された「サイバーセキュリティ戦略」

諸外国の政府調達におけるクラウド動向

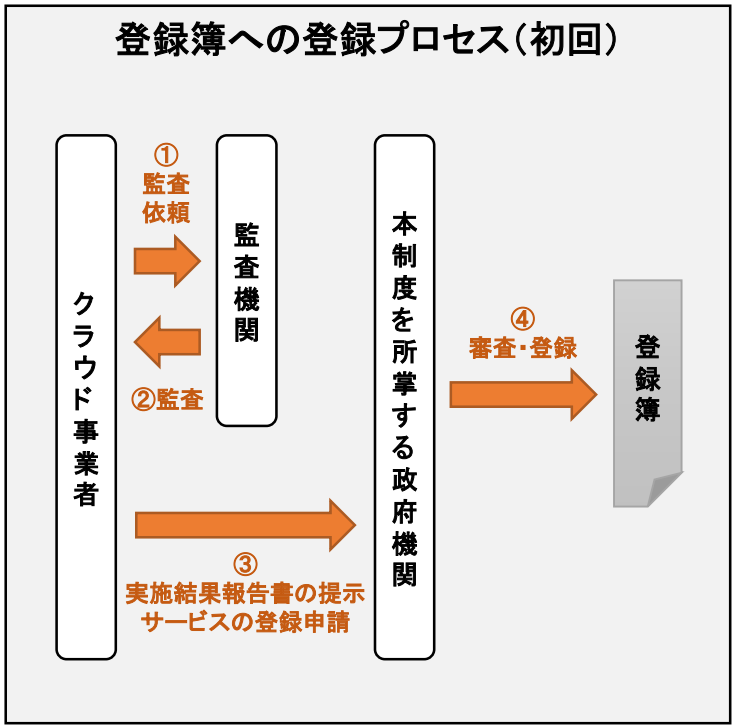
諸外国の政府調達では、多くが「①クラウド利用の方針」を定め、その後に「②政府クラウド安全性評価制度」を導入しています。

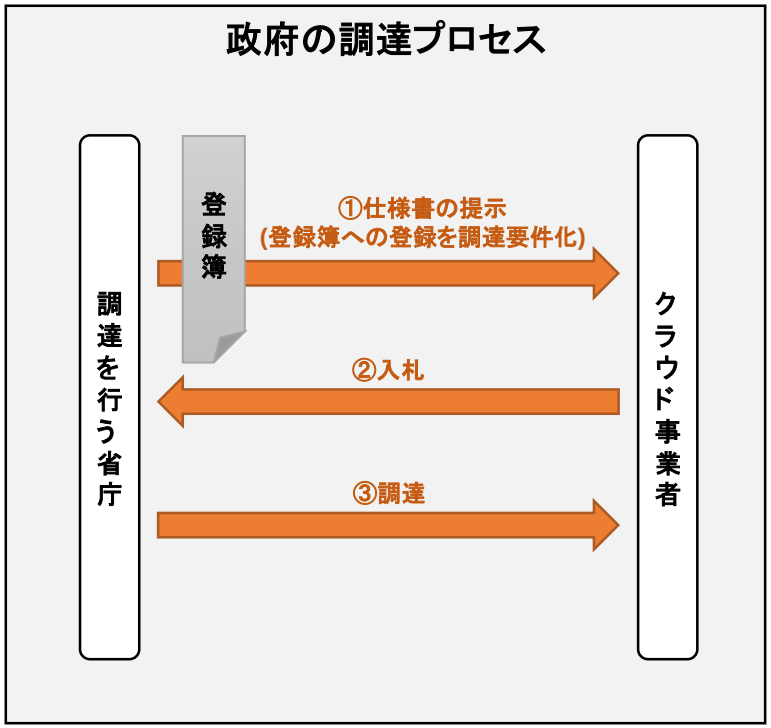
国	①クラウド利用の方針	②政府クラウド安全性評価制度	主な関連機関
アメリカ 	**2010 年** 「25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL INFORMATION TECHNOLOGY MANAGEMENT」 →クラウドファースト（**cloud first**）	**2011 年～** Federal Risk and Authorization Management Program	General Services Administration （※独立政府機関）
イギリス 	**2011 年** 「Government Cloud Strategy」 →クラウドファースト（**a public cloud solution first policy**）	**2013 年～** G-Cloud framework	Government Digital Services （※内閣府管轄）
オーストラリア 	**2014 年** 「Australian Government Cloud Computing Policy」 →クラウドファースト（**cloud first**）	**2014 年～** Information Security Registered Assessors Program	Australian Signals Directorate （※防衛大臣管轄）
シンガポール 	**2011 年** 「e-Government masterplan 2011-2015」 →政府プライベートラウドの構築、移行（**G-Cloud**）	**2013年～** Multi-Tier Cloud Security（MTCS:SS584）	Infocomm Media Development Authority （※情報通信省管轄）
日本 	**2018 年** 「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」 →クラウド・バイ・デフォルト	**2020 年～** **ISMAP制度開始**	

ISMAPの仕組み

ISMAPの制度が開始された2021年現在、クラウド・バイ・デフォルト原則により政府情報システムの調達はISMAP登録簿（クラウドサービスリスト）より行われます。

政府情報システムにクラウドサービスが選定されるためには、登録簿への登録が事実上必須となります。





ISMAPクラウドサービスリスト

2021年6月7日時点において、ISMAPクラウドサービスリスト（登録簿）には下記7社10サービスが登録されています。

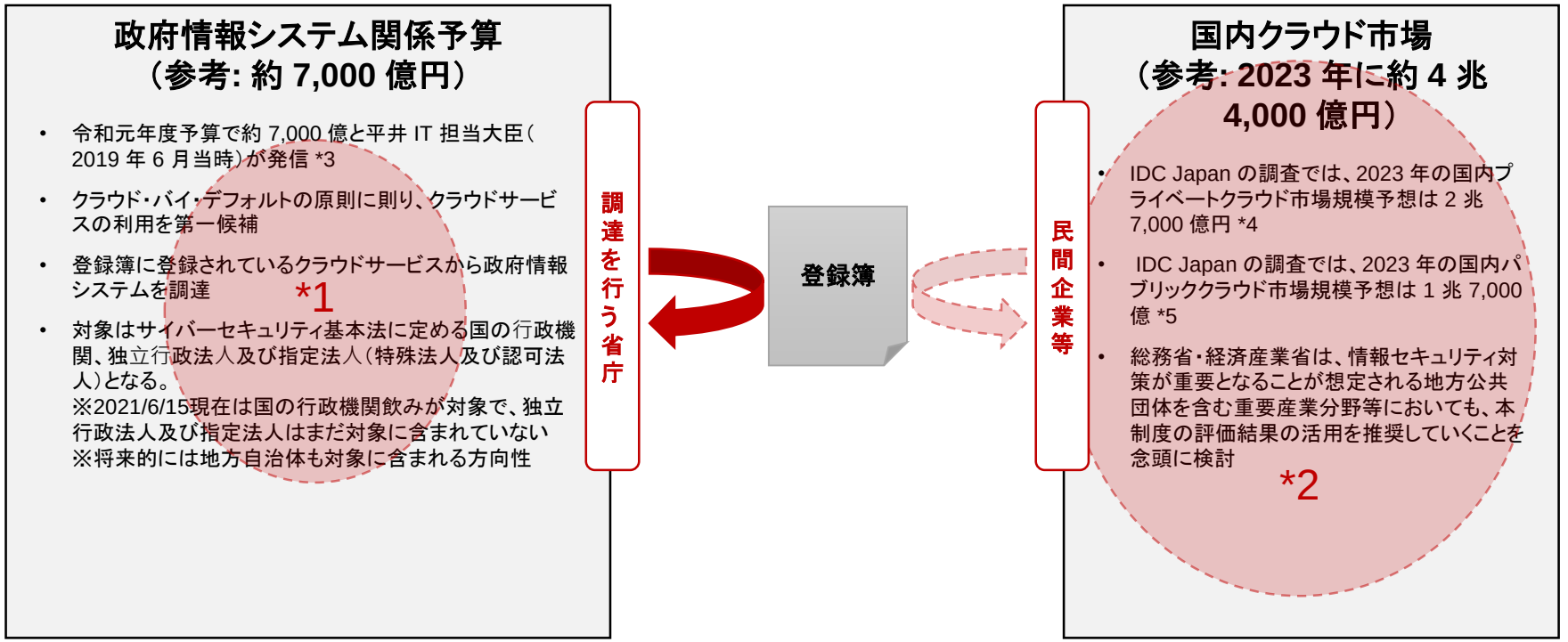
登録番号	登録日	サービス名	事業者名
C21-0001-2	2021/3/12	OpenCanvas(IaaS)	株式会社エヌ・ティ・ティ・データ （法人番号9010601021385）
C21-0002-2	2021/3/12	FUJITSU Hybrid IT Service FJcloud	富士通株式会社 （法人番号1020001071491）
C21-0003-2	2021/3/12	Apigee Edge	Google LLC （法人番号3700150072195）
C21-0004-2	2021/3/12	Google Cloud Platform	
C21-0005-2	2021/3/12	Google Workspace	
C21-0006-2	2021/3/12	Salesforce Services	株式会社セールスフォース・ドットコム （法人番号4010401076766）
C21-0007-2	2021/3/12	Heroku Services	
C21-0008-2	2021/3/12	Amazon Web Services	Amazon Web Services,Inc.
C21-0009-2	2021/3/12	NEC Cloud IaaS	日本電気株式会社 （法人番号7010401022916）
C21-0010-2	2021/3/12	KDDIクラウドプラットフォームサービス	KDDI株式会社 （法人番号9011101031552）

出展：ISMAPクラウドサービスリスト（https://www.ipa.go.jp/security/ISMAP/cslist.html）

ISMAP開始による影響

ISMAP の登録簿は、政府情報システムの調達のみならず、**地方公共団体や民間においても活用**の推進が念頭とされています。

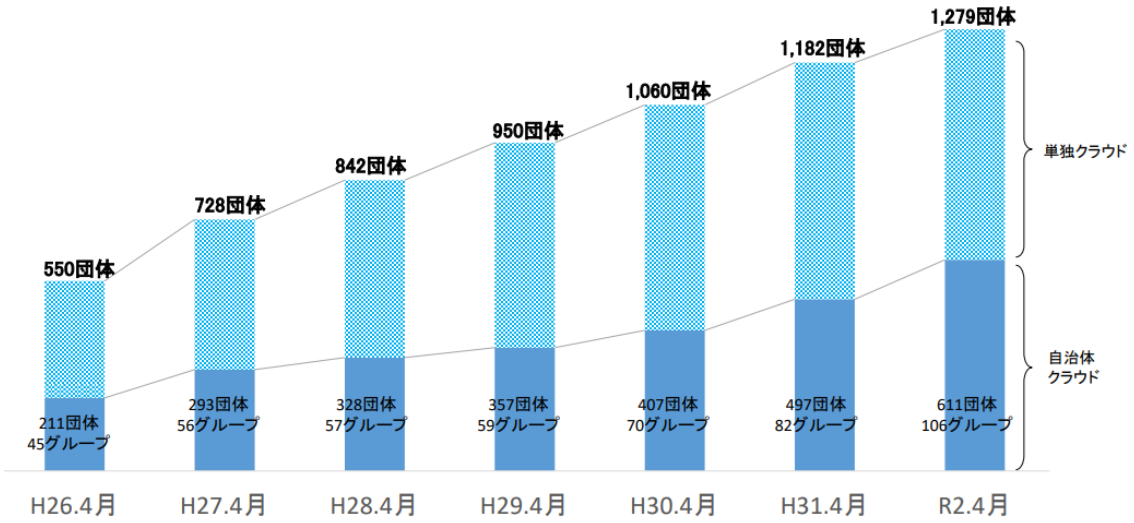
そのため、**登録簿にクラウドサービスが登録されることが、数兆円規模の市場に参入する前提条件**となる可能性が考えられます。



*1 : 政府情報システムの中でクラウドサービスを利用する範囲のイメージ
*2 : 国内クラウド市場の中で政府クラウドの登録簿を活用する範囲のイメージ
*3 : 平井卓也 衆議院議員のブログより出典（https://www.hirataku.com/blog/984/）
*4 : IDC Japanの国内パブリッククラウドサービス市場予測より出典（https://www.idc.com/getdoc.jsp?containerId=prJPJ44928319）
*5 : IDC Japanの国内プライベートクラウドサービス市場予測より出典（https://www.idc.com/getdoc.jsp?containerId=prJPJ45603419）

今後のISMAP対象範囲拡大について

地方自治体においてもクラウドの導入が進んでいますが、2021年6月7日時点では、ISMAPが調達要件となる対象は国の行政機関のみとなり、独立行政法人及び指定法人と地方自治体は対象に含まれていません。
ただし、近い将来に独立行政法人及び指定法人と地方自治体についてもISMAPが調達要件となる対象に含めれることが予想されるため、それらの組織にサービスを提供しているクラウド事業者は準備を進めておくことが推奨されます。

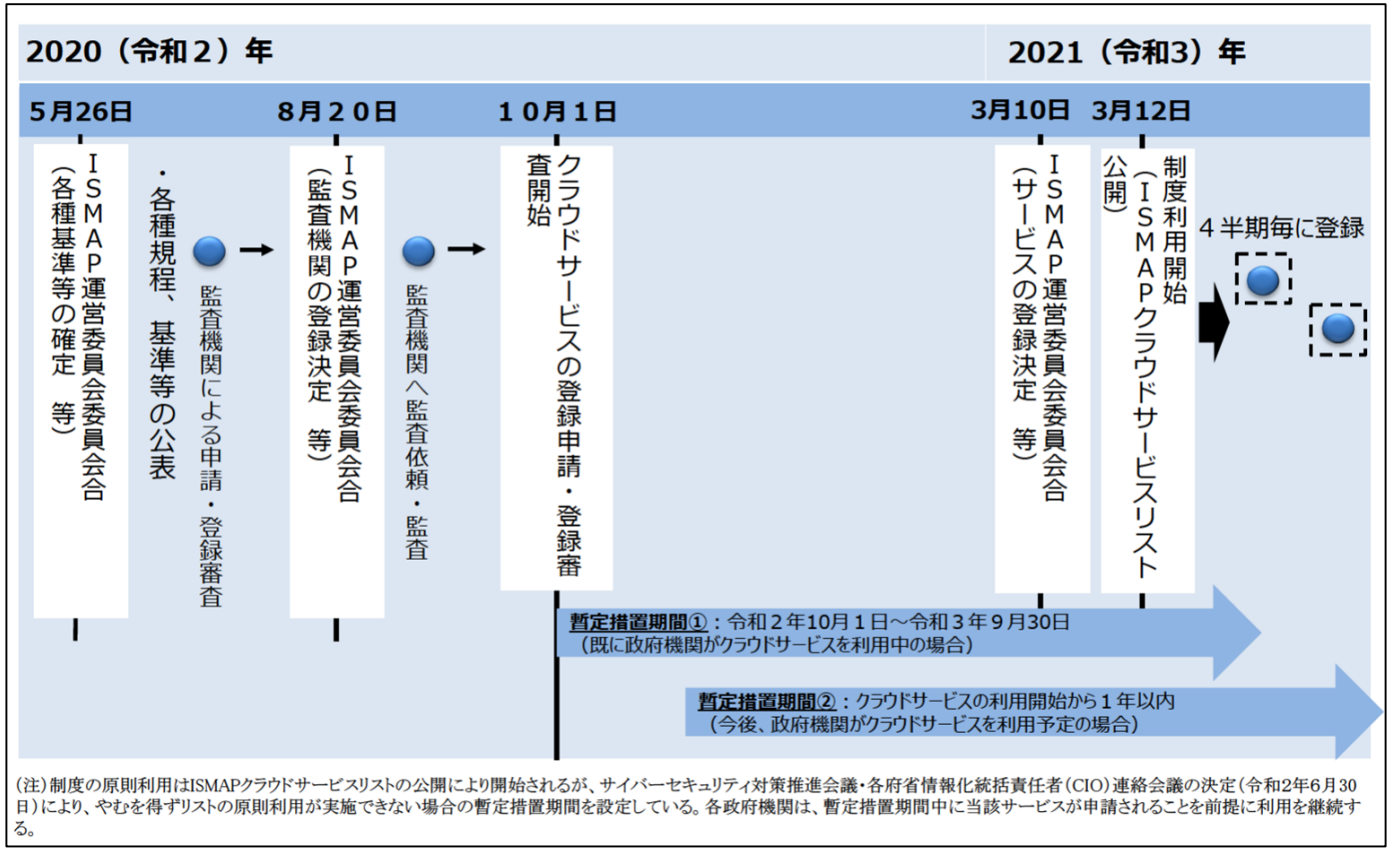


出典：クラウド導入状況(令和2年4月現在)：https://www.soumu.go.jp/main_content/000743575.pdf

暫定措置

既に政府機関がクラウドサービスを利用中の場合、2021年9月30日までに当該サービスがISMAP登録されることを前提に利用が継続される点に注意が必要です（暫定措置期間）。

また、今後政府機関がクラウドサービスを利用予定の場合、クラウドサービスの利用開始から1年以内にISMAP登録されることが前提となります。



（注）制度の原則利用はISMAPクラウドサービスリストの公開により開始されるが、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（CIO）連絡会議の決定（令和2年6月30日）により、やむを得ずリストの原則利用が実施できない場合の暫定措置期間を設定している。各政府機関は、暫定措置期間中に当該サービスが申請されることを前提に利用を継続する。

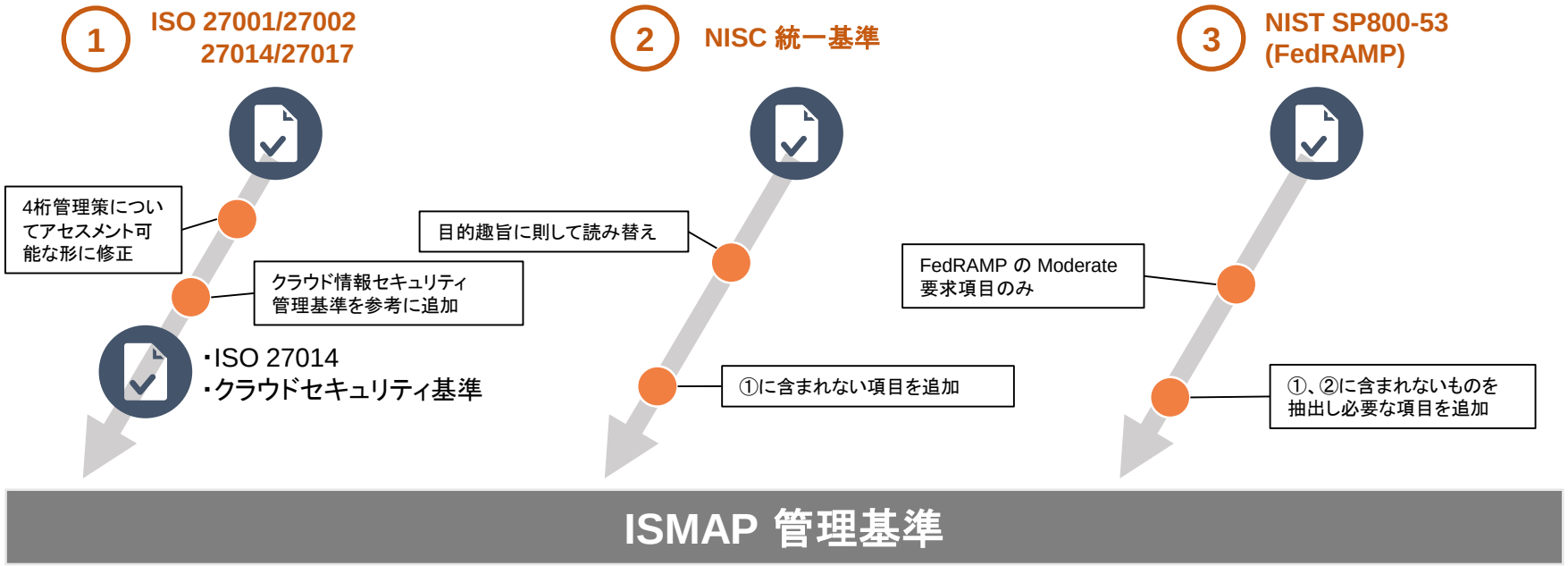
出展：スケジュールhttps://www.ipa.go.jp/files/000082875.pdf

登録簿掲載のハードル

ISMAP の登録簿への掲載はISOなどの認証取得に比べてハードルの高いレベルとなっています。

下図のように、ISMAP の管理基準は ISO や NISC 統一基準、FedRAMP などの管理基準を組合わせて作成されています。

また、既に取得しているその他の認証があっても、ISMAP において該当する管理基準の外部評価が免除されるわけではありません。



ISMAPの管理策の構成

ISMAPの管理策は①ガバナンス基準②マネジメント基準③管理策基準の三つから構成されています。

ガバナンス基準 — 18 項目 ※1

・ISO27014をベースに作成されています。

＋

マネジメント基準 — 64 項目 ※1

- ISO27001とNIST SP800-53をベースに作成されています。

＋

管理策基準 — 1075 項目 ※2

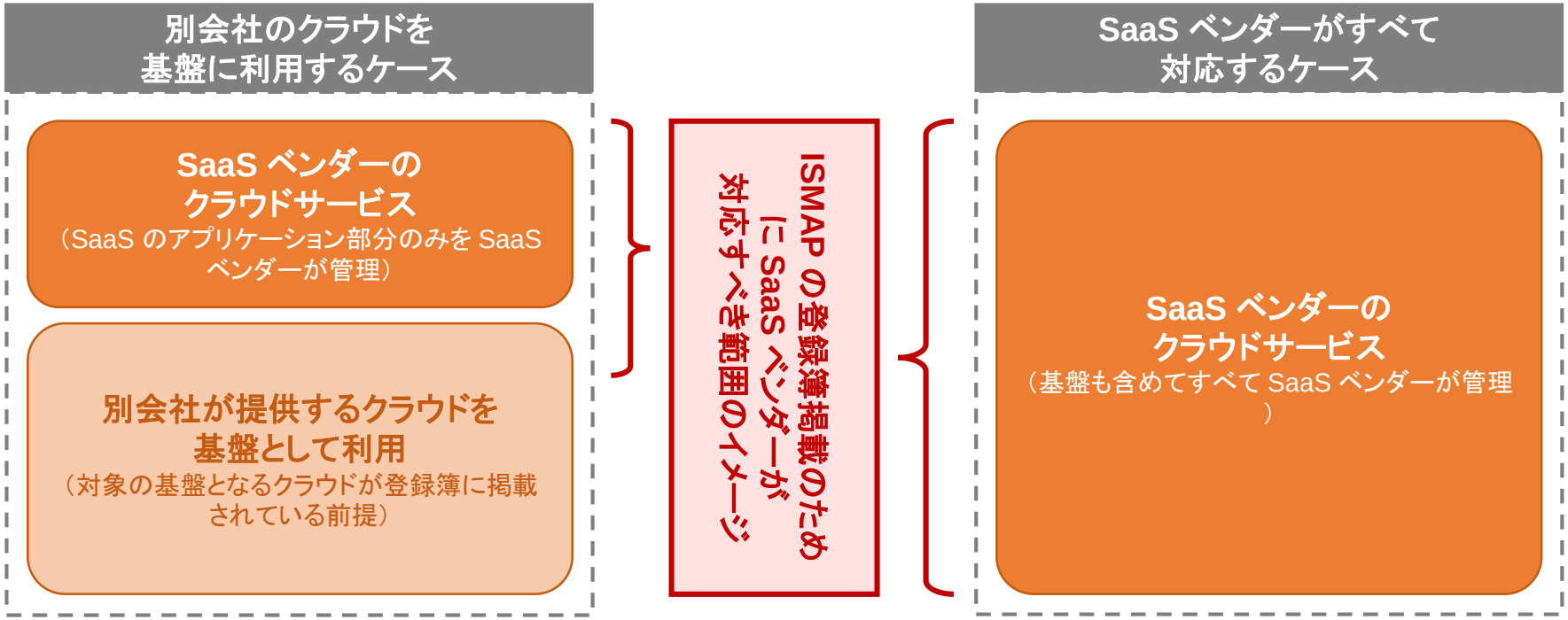
- ISO27002, 27017, 統一基準，NIST SP800-53をベースに作成されています。

※1: ガバナンス基準、マネジメント基準に対応する管理策は全て選択する必要がある。
※2: 管理策基準に対応する管理策は選択式だが、選択しなかった理由が合理的であるかは審査会で判断される。（監査機関は判断しない。）

SaaSベンダーにおけるISMAP

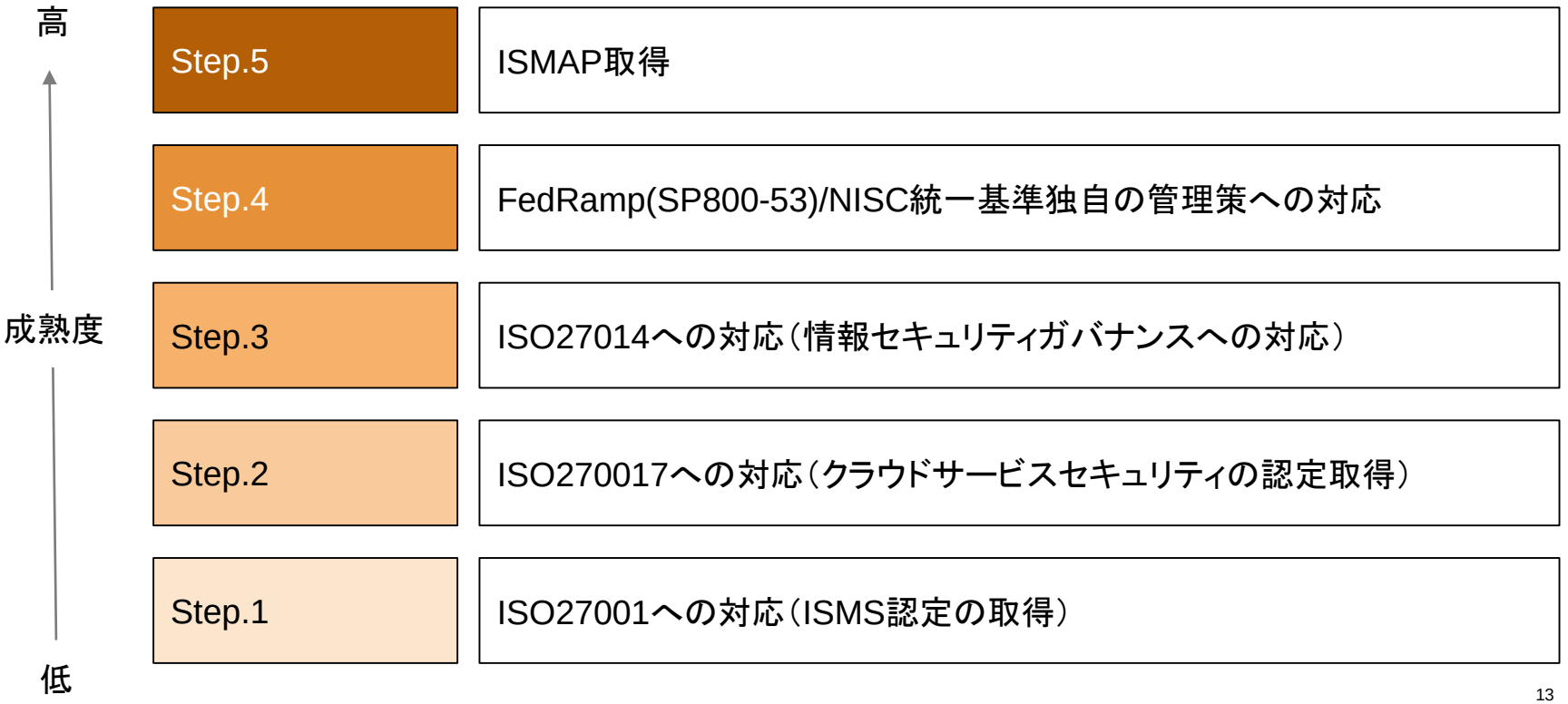
前述の通り、ISMAP では高レベルの管理基準への対応が求められ、特に**国内の中小規模のクラウドベンダーが自力で登録簿に自社のクラウドサービスを掲載することは少々高いハードルがある**と考えられます。

SaaS を提供するベンダーの場合、**登録簿に掲載済みのクラウドサービスを SaaS の基盤として利用することで、登録簿へ掲載するために対応すべき範囲を縮小でき得る仕組み**になっています。



ISMAP取得までのステップ

ISMAPの登録簿への掲載はISOなどの認証取得に比べてハードルが高く、ISMAPを構成する要素を持つ各規格（ISO27001、ISO27017、ISO27014、FedRamp、統一基準等）に段階的に対応していくことが、結果的にISMAP取得に向けた近道となります。
また、自社のみでの対応が困難である場合には、共通基盤の仕組みや、管理策の共通化等が有効な施策となることも考えられます。



コンタクト先

ISMAPに関するお問い合わせは以下の担当者宛にご連絡いただきますようお願いいたします。

PwCあらた有限責任監査法人

システム・プロセス・アシュアランス部

パートナー　加藤俊直
E-mail: toshinao.kato@pwc.com/ Tel:080-3270-8795

パートナー　川本大亮
E-mail: daisuke.kawamoto@pwc.com / Tel: 080-3158-7438

Thank you

pwc.com