National center of Incident readiness and Strategy for Cybersecurity

政府情報システムのためのセキュリティ評価制度（ISMAP）の概要

～ISMAPの基本的な枠組みとISMAP取得のメリット～

※　本資料は、トレンドマイクロ株式会社主催「基礎から分かるISMAP～クラウドサービス事業者・利用者にとってのメリットとは？～」（令和５年10月25日開催）において説明したものです。

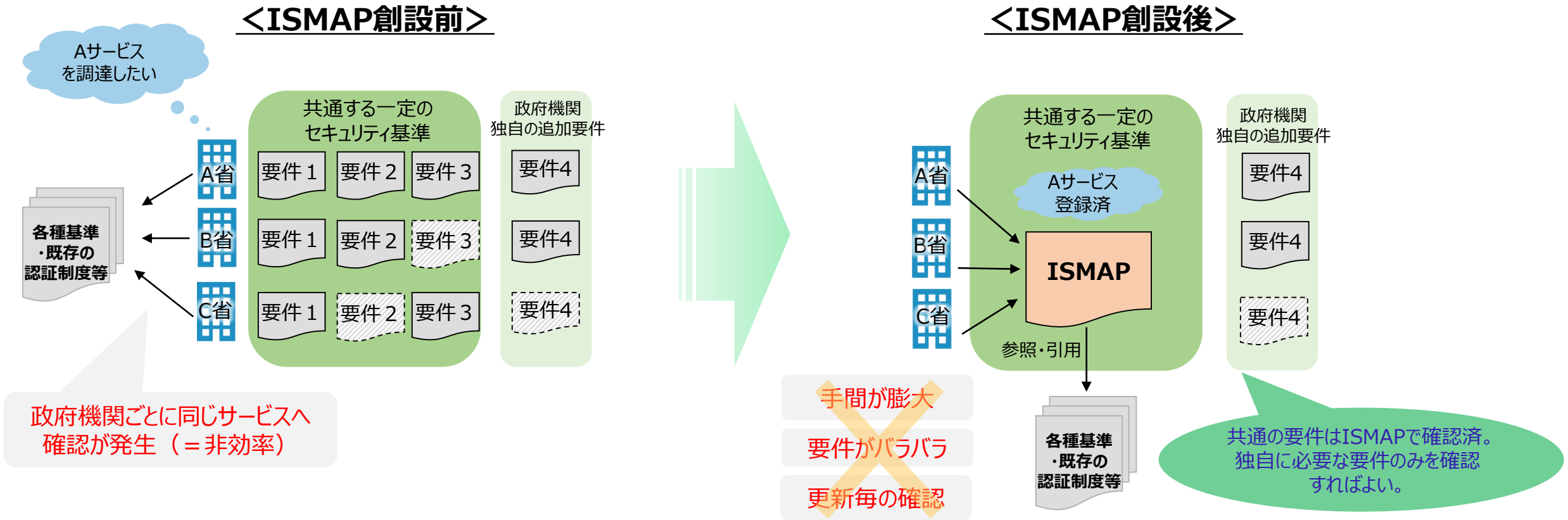
ISMAPの基本的な枠組み

1

ISMAP創設の目的

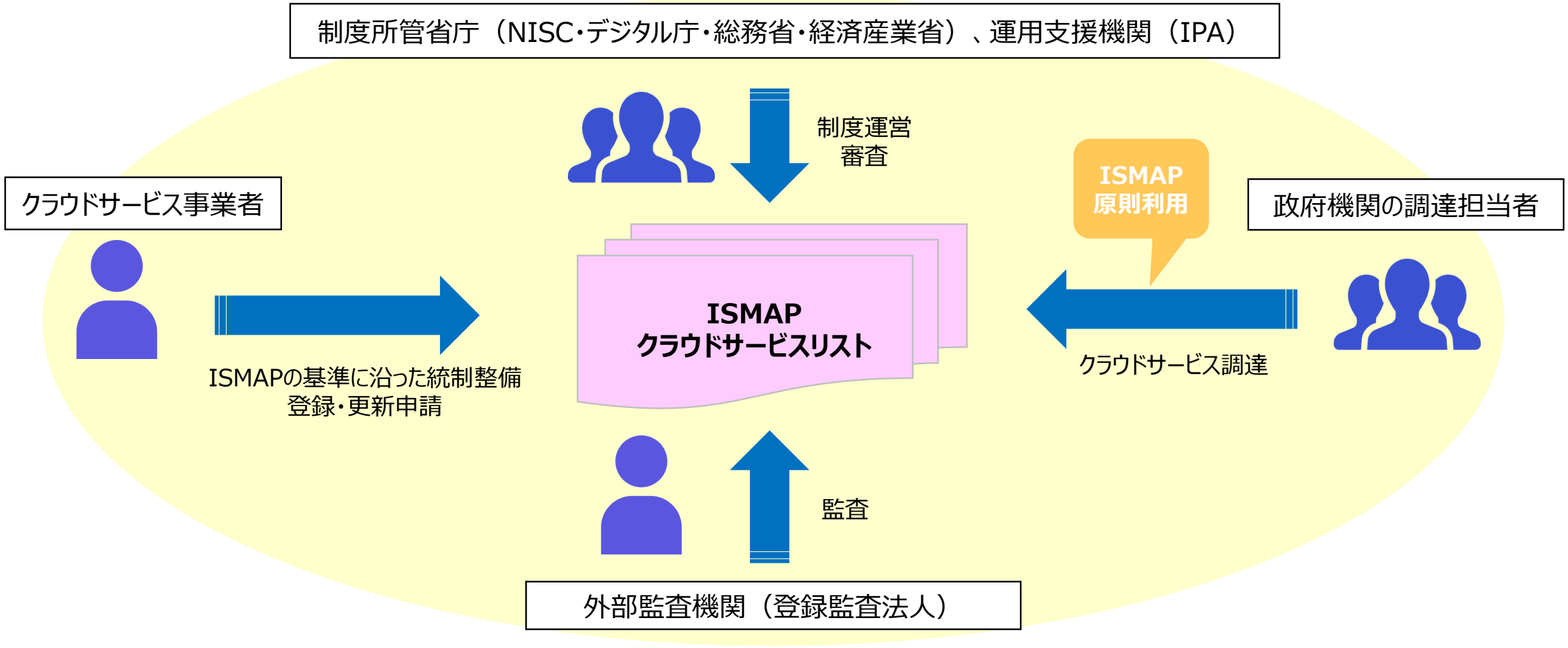
ISMAP（イスマップ）：Information system **S**ecurity **M**anagement and **A**ssessment **P**rogram

- 政府の情報システムは、**クラウド・バイ・デフォルト原則**、すなわちクラウドサービスの利用を第一候補として検討しています。
- 政府機関が同じクラウドサービスを利用するにもかかわらず、各機関それぞれが各種基準や既存の認証制度等を確認し、１からセキュリティ要件を確認することは非効率です。
- このため、政府機関が利用する際の統一的なセキュリティ基準を明確化し、安全性が評価されたクラウドサービスを効率的に利用できるようにするため、**「政府情報システムのためのセキュリティ評価制度（ISMAP）」を、2020年６月に創設**しました。



ISMAPの枠組み

- ISMAPでは、国際標準等を踏まえ策定したセキュリティ基準に基づき、各基準が適切に実施されているかを第三者が監査するプロセスを経て、**政府が求めるセキュリティ要求を満たしていると評価されたクラウドサービスを、「ISMAPクラウドサービスリスト」へ登録**します。
- 政府機関がクラウドサービスを調達する際は、**原則、「ISMAPクラウドサービスリスト」に掲載されたサービスから調達**します。



ISMAP登録までの流れ

※クラウドサービス事業者について、以下、CSP（Cloud Service Provider）といいます。

統制整備 運用	書類作成 監査準備	監査	登録申請	審査	登録
○ CSP（クラウドサービス事業者）は「ISMAP管理基準」に基づいた情報セキュリティ対策（統制の整備・運用）を実施します。* *CSPは、自身のサービス内容及びセキュリティリスク分析に基づいた統制目標の策定と管理策の整備・運用を行います。	○ CSPは「言明書」及び「経営者確認書」を作成し、自身のセキュリティ対策について基本言明要件に沿った言明を行い、それらを監査機関に提出します。 ○ 監査機関を「ISMAP監査機関リスト」から選定し、契約します。	○監査機関は、C整備状況評価及び運用状況評価を実施します。 ○CSPは、有効な証跡やサンプル等を監査機関に提出します。 ○監査機関は、監査実施後、「実施結果報告書」を作成し、CSPに提出します。	○ 監査において発見事項*が発見された場合、CSPは「改善計画書」を作成し、改善を実施します。 ○ CSPは言明書・実施結果報告書・改善計画書等文書を添えて、ISMAPポータルより申請します。 *外部監査において確認された不備事項	○ISMAP運用支援機関は、受理した申請文書について、技術的審査を行います。 ○ISMAP運用支援機関は、必要に応じてCSPに追加の情報提供を求めます。 ○「ISMAP運営委員会」が、最終的な登録の決定を行います。	○ クラウドサービスリストへ登録され、ISMAPポータルサイトにおいて公表されます。

ISMAP管理基準への言明について

〔ISMAP管理基準の言明〕

統制目標：CSPがリスクに対応するために達成するべき統制の目標とする項目
詳細管理策：CSPが統制目標を実現するために選択して満たすべき事項

第３章　ガバナンス基準	統制目標（3桁：x.x.x）	基本言明要件 原則として全て実施
	詳細管理策（4桁：x.x.x.x）	
第４章　マネジメント基準	統制目標（3桁：x.x.x）	
	詳細管理策（4桁：x.x.x.x）	
第５章～18章 管理策基準	統制目標（3桁：x.x.x）	
	詳細管理策（4桁：x.x.x.x.B,PB）	選択制
	詳細管理策（4桁：x.x.x.x）	

基本言明要件については、全てセキュリティ対策を実施する必要があります。ただし、「サービスの特性上、当統制目標は採用しえない」といった合理的な理由から、言明の対象外とすることは認められております。

〔統制目標、詳細管理策の選択までのステップ〕

リスクの選定・分析

○　CSPは、言明の対象とするクラウドサービスに関するセキュリティリスク（実装構造、運用環境及びサービスの性質などに照らし想定されるリスク）を特定し、分析します。

統制目標の選択

○　リスク分析を踏まえ、提供するサービスに必要な統制目標（３桁管理策）を全て選択します。

○　統制目標は、適用不可能な理由を合理的に説明できる場合のみ、非選択とすることが可能になります。

詳細監理策の選択

○　選択した統制目標を実現するための手段としての詳細管理策（４桁管理策）を選択します。

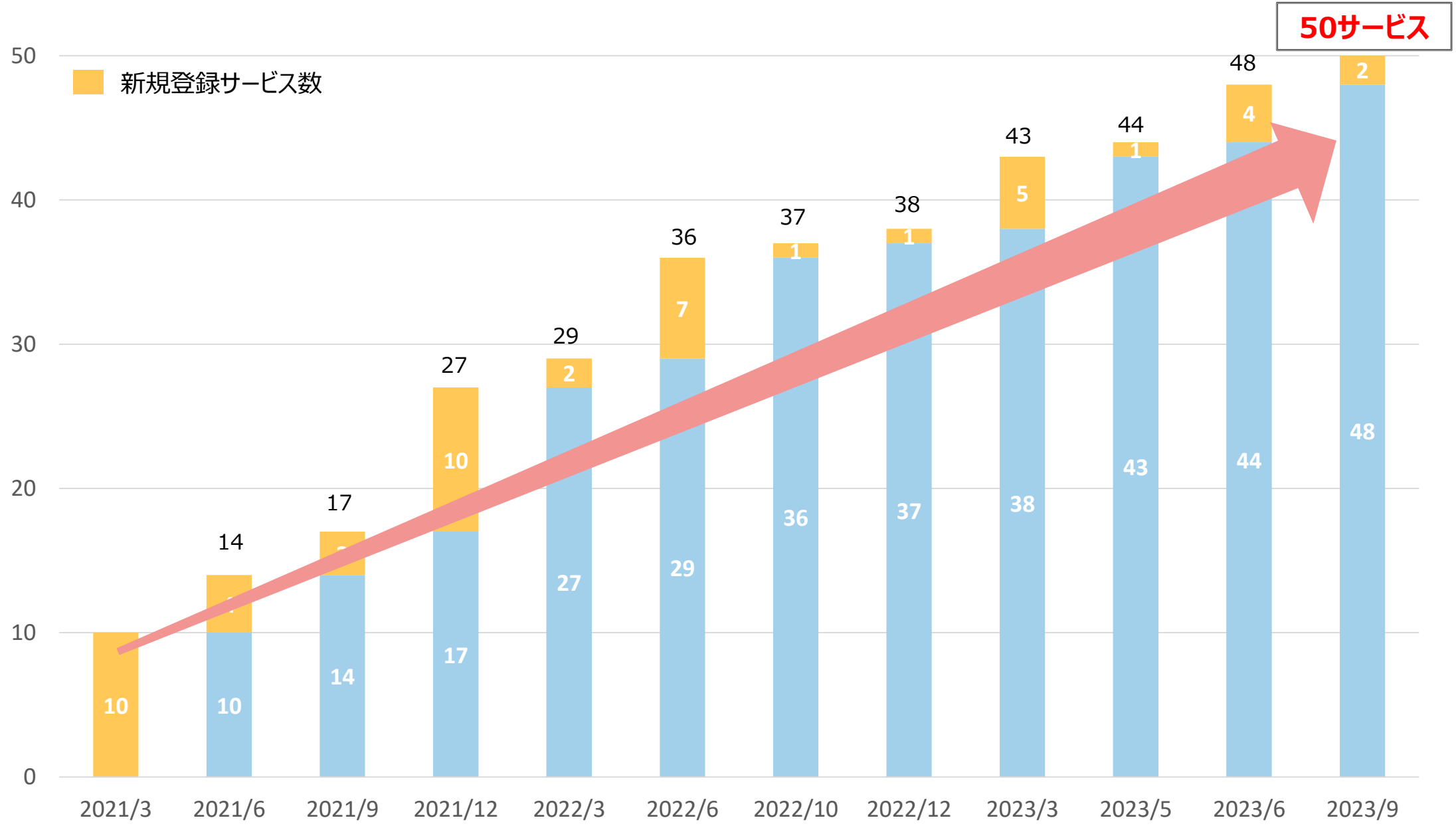
○　管理策基準のうち、末尾に「B」が付された詳細管理策は全て選択します。

個別管理策の策定

○　採用した詳細管理策の具体的対策としての個別管理策を策定します。

CSPが実際に実施しているセキュリティ対策は個別管理策の内容です。

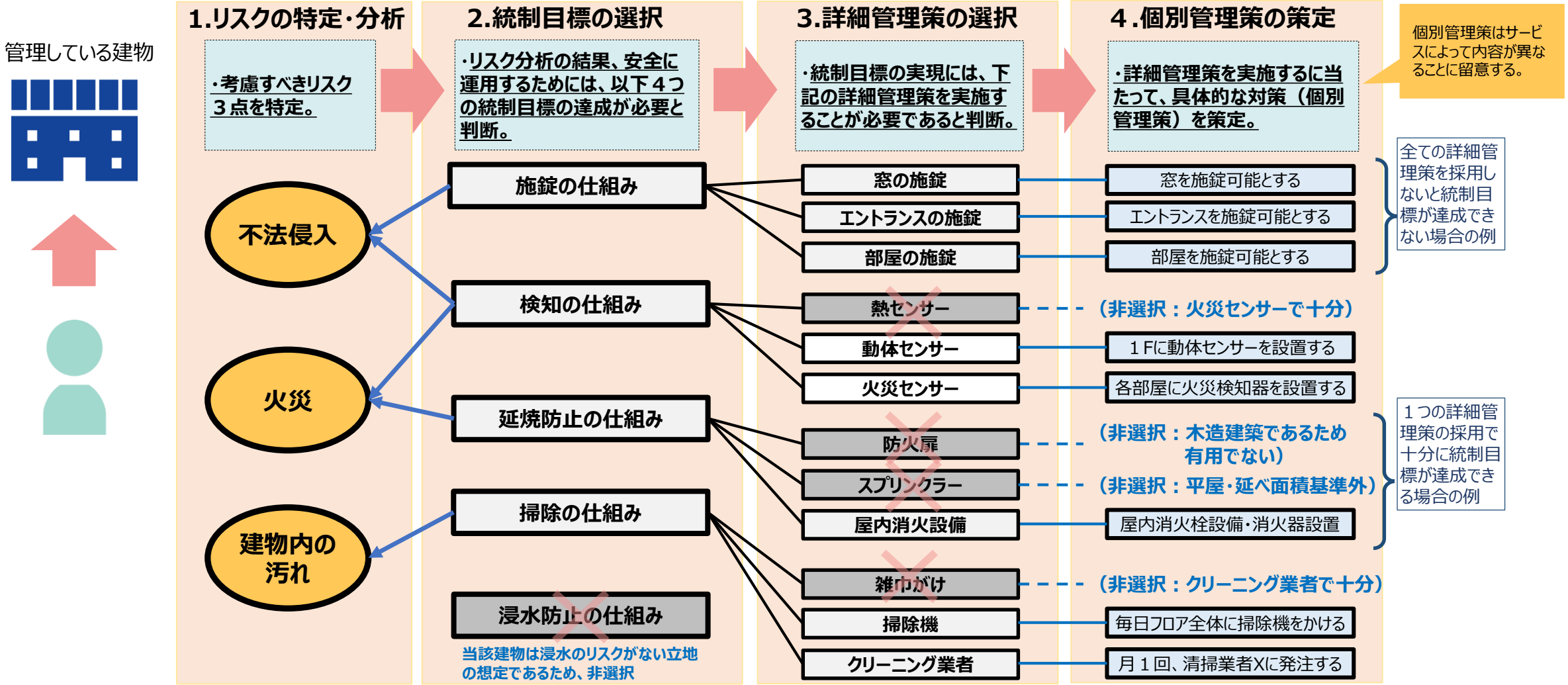
ISMAPクラウドサービスリストのサービス登録状況（2023年９月時点）



リスク分析と統制目標、詳細管理策の選択イメージについて

● リスク分析と統制目標、詳細管理策の選択について、建物を例に、選択プロセスをイメージしてみましょう！

（注）本事例は、クラウドサービスにおけるリスク特定・分析と、統制目標及び詳細管理策の関係を分かりやすく示すために作成したものであり、実際のISMAP管理基準や各種法令等に基づくものではありません。



ISMAP-LIUの仕組み

ISMAP-LIU（イスマップ・エル・アイ・ユー）：ISMAP for Low-Impact Use

- クラウドサービスのうちSaaSは、サービスの幅が広く、用途や機能が限定的なサービスや重要度が低い情報のみを取り扱うサービスなど、リスクが低いサービスもあり、**現行のISMAPと同じ取扱いとした場合、過剰なセキュリティ要求となる**場合も考えられます。
- このため、主に**リスクの小さな業務・情報の処理に用いるSaaSサービスを対象**に、**新たに「ISMAP-LIU」の枠組みを設け**、令和4年11月1日から運用を開始しております。
- なお、ISMAP-LIUにおける外部監査対象となる管理策については、対象を重要な管理策に絞り、数年に平準化しつつ実施することにより、**外部監査の対象項目数を縮小**しています（現行ISMAPの概ね１／５程度になると想定）。

＜ISMAP-LIUにおける対象サービスの例＞・・・ISMAP-LIU対象業務一覧より

動画・音声、配信等

- Web会議サービス
- ファイル共有サービス
- 映像・コンテンツ等配信サービス
- Web アンケートサービス

人事・総務系管理

- 人事管理サービス
- タレントマネジメントサービス
- 採用管理サービス
- 名刺管理サービス
- e-ラーニングサービス
- 安否確認サービス

その他業務効率化

- ソースコード管理サービス
- CMS
  （Contents Management System）サービス
- 自動翻訳サービス
- チャットボットサービス

※重要度の低い行政文書等が対象

ISMAP-LIUの登録までの流れ

- ISMAP-LIUは、機密性２を取り扱うSaaSの中でも、**セキュリティ上のリスクの小さな業務・情報の処理に用いるサービスが対象です。**
- このため、対象となるSaaSサービスがISMAP-LIUに該当するかについて、**利用する政府機関等において、「業務・情報の影響度評価」を実施し、リスクの小さな業務に用いられるSaaSであることを事前に確認**します。

※　業務・情報の影響度は、クラウドサービスで取り扱われ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。

【ISMAP-LIUサービス登録の流れ】

＜事前申請（＝ISMAP-LIU固有のプロセス）＞

＜外部監査～本申請～登録（＝ISMAPと同じプロセス））＞

政府機関等による影響度評価

機密性、完全性、可用性が侵害された際の影響度を評価

「ISMAP-LIUにおける業務・情報の影響度評価ガイダンス」において、業務・情報の影響度が低位である蓋然性が高い業務（対象業務一覧）を提示。

CSPによる事前申請

事前申請書

利用省庁等による業務・情報の影響度評価結果

事前申請の審査

IPAにおいて、実ケースとして影響度の低い業務に用いられるSaaSであることを確認

外部監査～本申請

外部監査等によるISMAP要求事項の確認

監査全体として現行ISMAPよりも緩やかな設計

ISMAP-LIUサービス登録

相対的にリスクが低いと評価されるSaaSサービスを登録

ISMAP取得のメリット

①安心安全のセキュリティ確保
②政府機関等におけるISMAPの利用拡大
③地方公共団体及び基幹インフラ分野でのISMAPの活用
④利用者企業・組織で活用されるISMAP

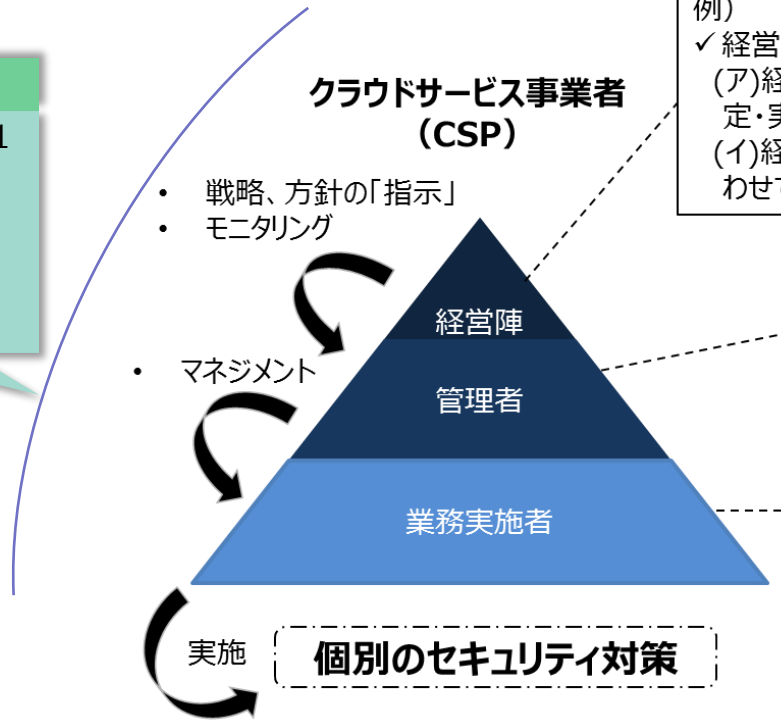
2

ISMAP取得のメリット～①安心安全のセキュリティ確保～

- ISMAPでは、クラウドサービスの情報セキュリティに関する**JIS Q（ISO/IEC）27017等を基礎**として、クラウドサービスに関する**統一的なセキュリティ基準（ISMAP管理基準）**を策定・公表しております。
- ISMAP管理基準では、情報セキュリティマネジメントに加えて、クラウドサービスのパフォーマンス、信頼性、データ、ネットワーク、ソフトウェア等に係る様々なセキュリティ対策の実装を要求しており、監査においてもこれらの実装状況を確認することとしております。
- さらに、クラウドサービス事業者が、ISMAP管理基準に基づく情報セキュリティ対策が適切に実施されているかについて、**毎年、サービスの更新申請時に外部監査を実施する**ことを通じて、**クラウドサービスの安全性を担保**しています。

＜ISMAP管理基準の構成＞

基礎となる基準等
- JIS Q（ISO/IEC)27001
- JIS Q27002
- JIS Q27014
- JIS Q27017
- 政府統一基準群
- NIST SP800-53



①ガバナンス基準
例）
- ✓経営陣は、情報セキュリティの戦略及び方針を承認する。
  (ア)経営陣は、管理者に、情報セキュリティの戦略及び方針を策定・実施させる。
  (イ)経営陣は、管理者に、情報セキュリティの目的を事業目的に合わせて調整させる。

②マネジメント基準
例）
- ✓情報セキュリティマネジメントの確立
- ✓情報セキュリティマネジメントの運用
- ✓情報セキュリティマネジメントの維持及び改善

③管理策基準
例）
- ✓アクセス制御に対する要求事項
- ✓媒体の取扱い
- ✓暗号による管理策
- ✓マルウェアからの保護
- ✓ログ取得及び監視
- ✓冗長性
- ✓パフォーマンス（運用のセキュリティ）
- ✓サービスの信頼性
- ✓データセキュリティ
- ✓ネットワークセキュリティ
- ✓ソフトウェア管理

毎年実施する外部監査により、クラウドサービスの安全性を担保

ISMAP取得のメリット～②政府機関におけるISMAPの利用拡大～

● 政府機関等（各府省庁等＋独立行政法人等）における**ISMAP登録済みサービスの利用率は全体で約60%**で、うち、IaaS＋PaaSでの利用率は約90%となっております。また、前年度と比較し利用率が全体的に上昇しており、**着実にISMAP登録サービスからの調達が進んでいます**。

＜政府機関等におけるクラウドサービスの利用状況（令和４年10月末時点）＞

利用形態	区分	ISMAP登録		対前年比	ISMAP未登録		利用件数計
		利用件数	利用率		利用件数	利用率	
IaaS	各府省庁等	133	**88%**	＋21%	18	12%	151
	独法等	173	**92%**		16	8%	189
	政府機関等	306	**90%**		34	10%	340
PaaS	各府省庁等	74	**89%**	▲7%	9	11%	83
	独法等	30	**88%**		4	12%	34
	政府機関等	104	**89%**		13	11%	117
IaaS＋PaaS 計	各府省庁等	207	**88%**	＋16%	27	12%	234
	独法等	203	**91%**		20	9%	223
	政府機関等	410	**90%**		47	10%	457
SaaS	各府省庁等	105	**50%**	＋11%	105	50%	210
	独法等	145	**33%**		288	67%	433
	政府機関等	250	**39%**		393	61%	643
合計	各府省庁等	312	**70%**	＋16%	132	30%	444
	独法等	348	**53%**		308	47%	656
	政府機関等	660	**60%**		440	40%	1100

政府機関等における
クラウドサービスの利用
60%
対前年比
+16%

政府機関等における
IaaS+PaaSの利用
90%
対前年比
+16%

各府省庁等における
SaaSの利用
50%
対前年比
+11%

（出典）ISMAP制度所管省庁「利用実態調査」。
※ 調査対象のクラウドサービスは、機密性２情報を取り扱うもの。
※ 「利用件数」は、各政府機関等で利用している件数（２省庁で同じサービスを利用している場合は利用件数を２件とカウント）

（参考）ISMAPの利用に関する決定等

＜デジタル社会の実現に向けた重点計画＞（令和5年6月9日　閣議決定）

第３ デジタル社会の実現に向けた戦略・施策

第３-１ 戦略として取り組む政策群　４． サイバーセキュリティ等の安全・安心の確保

（１）サイバーセキュリティの確保

また、**政府情報システムのためのセキュリティ評価制度（以下「ISMAP」という。）においては、統一的なセキュリティ要求基準に基づき安全性が評価されたクラウドサービスをISMAPクラウドサービスリストに登録し、政府機関等における本制度の利用を促進する**とともに、制度運用の合理化に向けた検討及び改善を継続的に実施するなど、クラウド・バイ・デフォルトの拡大を推進する。

＜政府機関等のサイバーセキュリティ対策のための統一基準＞（令和5年7月3日　サイバーセキュリティ戦略本部決定）

4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）

遵守事項

(2) クラウドサービスの選定

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、クラウドサービスの選定基準に従い、前項で定めたセキュリティ要件を踏まえて、原則として**ISMAP等クラウドサービスリストからクラウドサービスを選定**すること。

＜政府情報システムのためのセキュリティ評価制度（ISMAP）の利用について＞

（令和2年6月30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（CIO）連絡会議決定）

１ 原則利用の考え方について

各政府機関等は、クラウドサービスの調達を行う際は「政府情報システムのためのセキュリティ評価制度（ISMAP）」において登録されたサービスから調達することを原則とする。

ISMAP取得のメリット～③地方公共団体及び基幹インフラ分野でのISMAPの活用～

- 地方公共団体におけるクラウドサービスの調達については、**総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」**において、**活用すべき認証の１つとしてISMAPが推奨**されています。
- また、特定社会基盤役務の安定的な提供の確保に関する制度において、特定重要設備にクラウドサービスを利用する場合、届出を省略することを可能とする方向で、ISMAPの活用を検討中です。

＜地方公共団体における情報セキュリティポリシーに関するガイドライン（抜粋）＞

- 外部サービス提供者及び当該サービスの信頼性が十分であることを総合的に判断するためには、外部サービスで取り扱う情報の機密性・完全性・可用性が確保されるように、外部サービス提供者のセキュリティ対策を含めた経営が安定していること、サービスを提供する基盤環境やアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。
- このような評価に当たって、外部サービス提供者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用する必要がある。
- なお、選定条件となる認証には、ISO/IEC 27017 によるクラウドサービス分野におけるISMS 認証の国際規格がある。また、**ISMAPの管理基準を満たすことの確認やISMAPクラウドサービスリスト**等のほか、日本セキュリティ監査協会のクラウド情報セキュリティ監査や外部サービス提供者等のセキュリティに係る内部統制の保証報告書であるSOC 報告書（Service Organization Control Report）**を活用することを推奨する。**

（出典）
総務省HP ＞ 地方公共団体における情報セキュリティポリシーに関するガイドライン
https://www.soumu.go.jp/denshijiti/jyouhou_policy/

＜（参考）クラウドサービスを利用した特定重要設備に関する考え方（抜粋）＞

クラウドサービスを利用した特定重要設備に関する考え方

クラウドサービスを利用する場合の基本的な考え方　※省略できる届出事項と要件を主務省令(様式)で定め、必要に応じ技術的な解説で補足等を行うことを想定。

- ✓ 特定重要設備は、他の事業者が提供するクラウドサービスを利用して構築されることも想定される。
- ✓ クラウドサービスについては、政府が求めるセキュリティ要求を満たしたサービスを予め評価・登録する制度（ISMAP）が既に整備されているところ、**事業者負担の軽減の観点から、ISMAPを取得しているものについては、当該制度において確認している事項等に係る情報の届出を省略することを可能とすることが適切であると考えられる**。

（出典）
内閣官房HP トップページ ＞ 各種本部・会議等の活動情報 ＞ 経済安全保障法制に関する有識者会議（令和４年度～）
第７回　令和５年　６月１２日
資料1　特定社会基盤役務の安定的な提供の確保に関する制度の運用開始に向けた検討状況について
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/4index.html

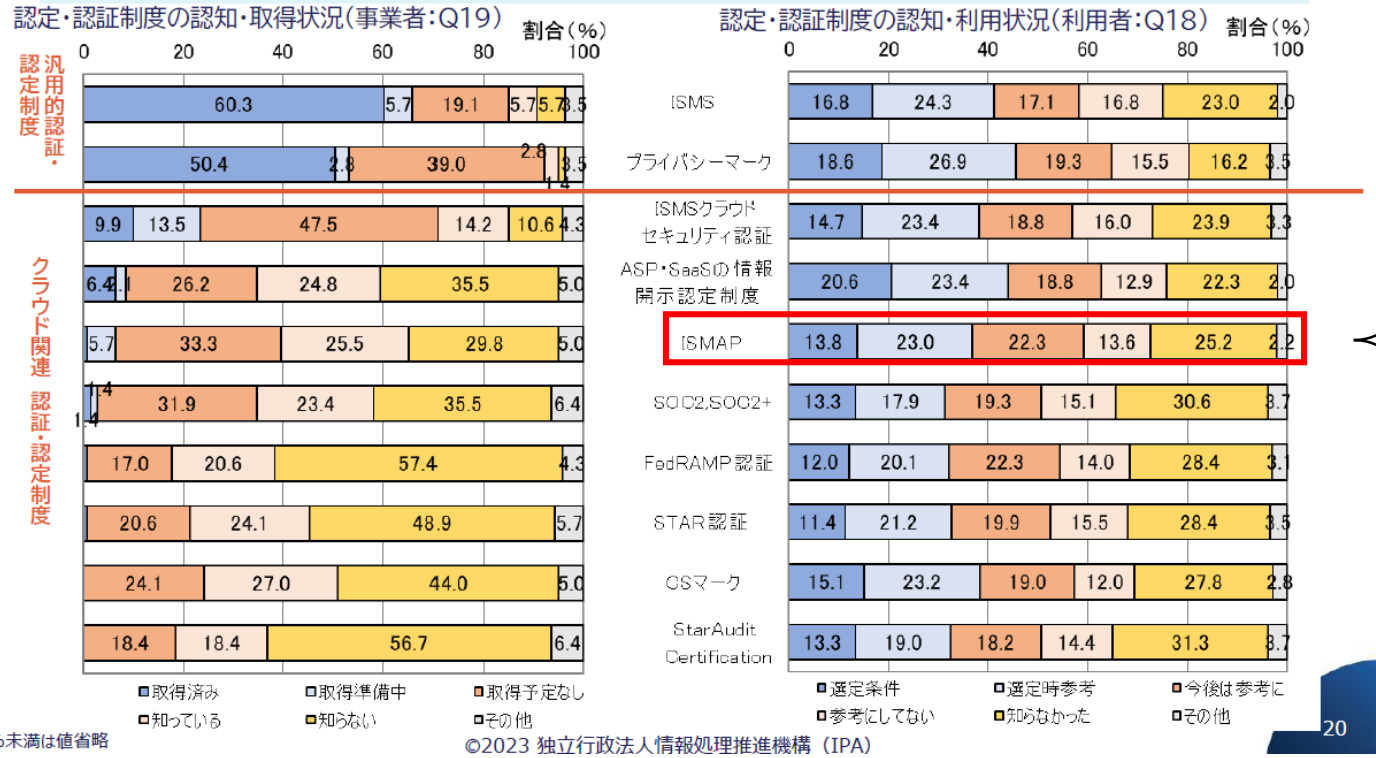
ISMAP取得のメリット～④利用者企業・組織で活用されるISMAP～

● 利用者企業・組織内の利用者（政府機関等外）を対象にしたアンケート結果では、３～４割の利用者がなんらかの認証・認定制度の取得を選定の条件や参考にすると回答しており、**クラウド関連の認証・認定制度として、ISMAPも一定の認知度があります**。

利用者はSaaSに関する認定・認証取得を選定条件・参考にしたい

IPA

- 約３～４割の利用者がなんらかの認証・認定制度の取得を選定の条件や参考にすると回答
- 事業者側のクラウド関連の認証・認定制度の取得状況は1割以下



1%未満は値省略

「選定条件」+「選定時参考」と回答した利用者は

36.8%

「選定条件」+「選定時参考」+「今後は参考に」と回答した利用者は

59.1%

（出典）
独立行政法人 情報処理推進機構　セキュリティセンター / 「クラウドサービス（SaaS）のサプライチェーンリスクマネジメント実態調査概要説明資料」
https://www.ipa.go.jp/security/reports/economics/scrm/t6hhco000000hg8a-att/ResearchSummary.pdf

おわりに

- ISMAPは、制度の運用開始から３年が経過し、政府機関等がクラウドサービスを調達する際のセキュリティ・信頼性を確認する制度として定着してきております。

- 引き続き、CSPの皆さまをはじめ様々なご意見をうかがいながら、ISMAP制度が担保している安全性・信頼性を保持しつつ、変化の速いクラウド分野に対応できる制度であるよう、常に変革してまいります。

ISMAP関連のコンテンツについて

- ISMAPに関する詳しい情報は、以下のHPをご確認ください。

○ NISC　HP

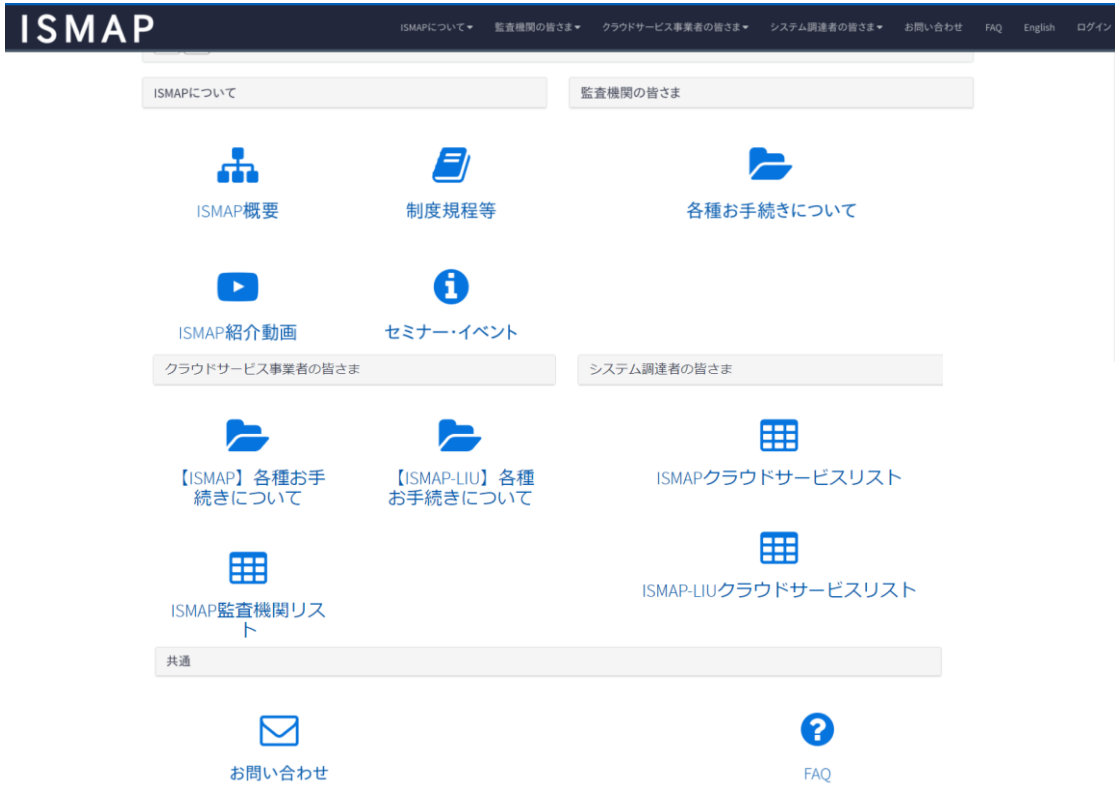
制度の枠組みや関連資料等を紹介しております。

https://www.nisc.go.jp/policy/group/general/ismap.html

○ ISMAPポータルサイト

クラウドサービスリストとともに制度規定やFAQ等など、制度全般のポータルサイトとしての機能を設けております。

https://www.ismap.go.jp/csm



お問い合わせ

● ISMAPに関連するご質問等については、こちらへお問い合わせください。

○ ISMAP全般について

ISMAPポータルサイト内部にお問い合わせ欄を設けております。

https://www.ismap.go.jp/csm?id=sc_cat_item&sys_id=c8586a16dbdfa010eeab7845f39619f7

○ ISMAP-LIU 相談窓口について

ISMAP-LIU登録に向けた相談等を受け付ける総合窓口として、デジタル庁に「ISMAP-LIU相談窓口」を設けております。

https://www.digital.go.jp/policies/security/ismap-liu#help_desk