National center of Incident readiness and Strategy for Cybersecurity

# 政府機関等における クラウドサービスのさらなる活用について

## ～政府情報システムのためのセキュリティ評価制度（ISMAP）における取り組み～

※　本資料は、日本電気株式会社主催「NEC デジタル・ガバメント Day ～行政のさらなるクラウド活用へ～」（令和５年11月９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

# 政府機関等におけるクラウドサービスの活用について

## 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

（平成30年６月７日 CIO連絡会議決定）

２．１ クラウド・バイ・デフォルト原則

政府情報システムは、**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、その検討を行うものとする。

## 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

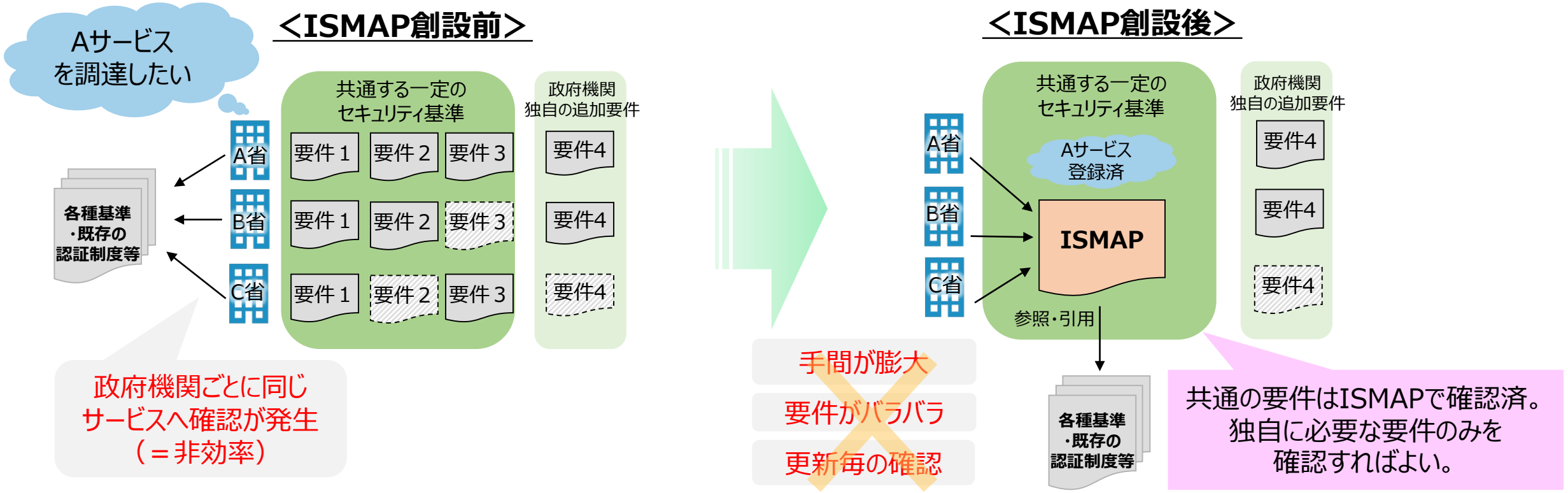
（１）サイバーセキュリティの確保

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**。

# ISMAP創設の目的

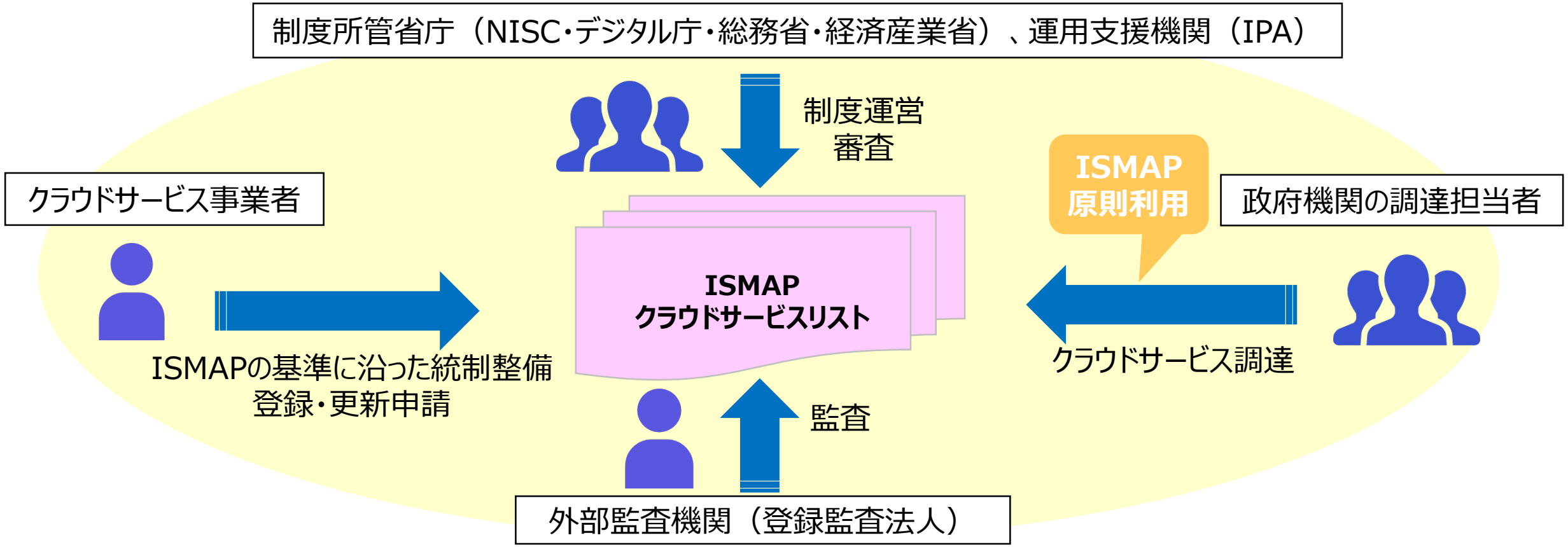
ISMAP（イスマップ）：Information system Security Management and Assessment Program

- 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。

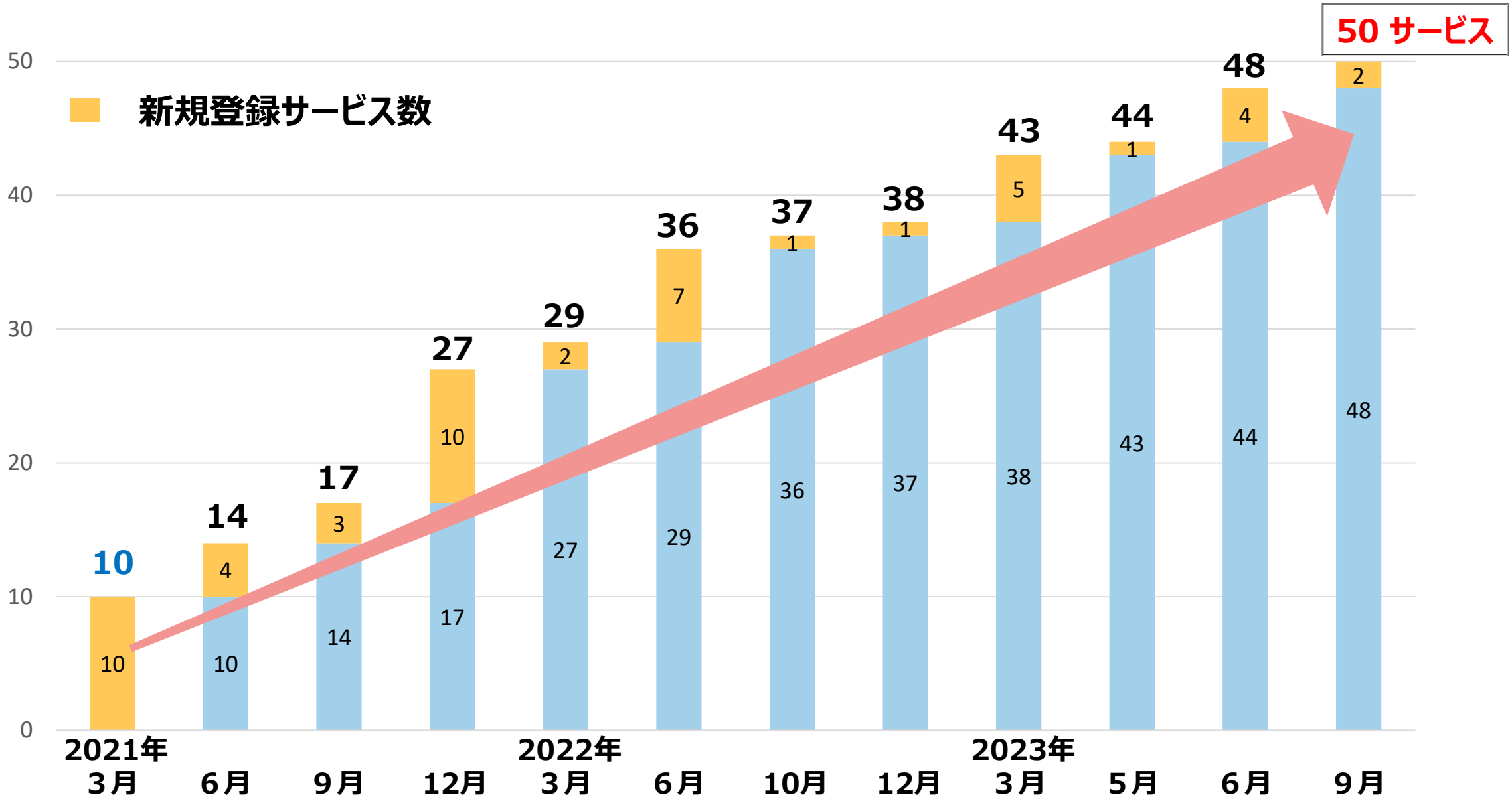


# ISMAP登録までの流れ

※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<br>運用 | 書類作成<br>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。*<br><br>*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。<br><br>○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、整備状況評価及び運用状況評価を実施します。<br><br>○CSPは、有効な証跡やサンプル等を監査機関に提出します。<br><br>○監査機関は、監査実施後「実施結果報告書」を作成し、CSPへ提出します。 | ○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。<br><br>○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。<br><br>*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。<br><br>○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。<br><br>○「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。 |

# 【参考】ISMAPクラウドサービスリストのサービス登録状況



# 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

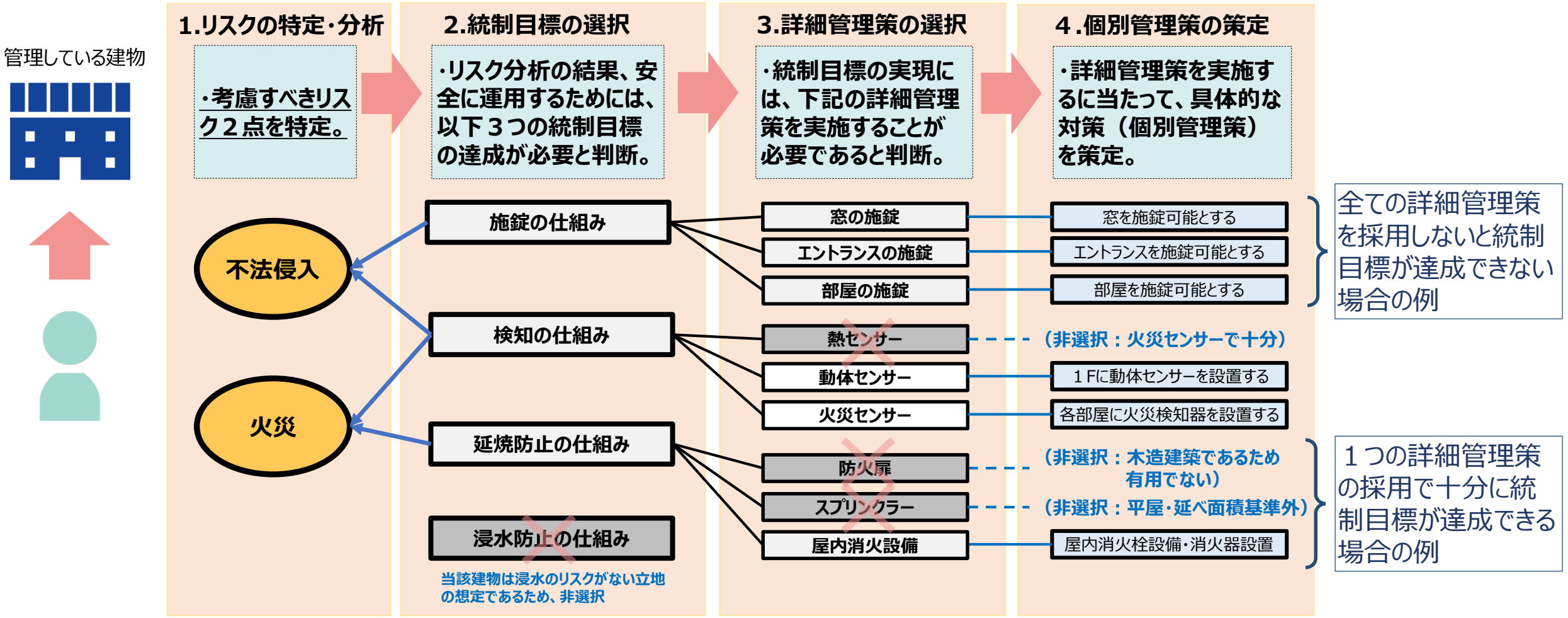
| | | |
|---|---|---|
| 第３章　ガバナンス基準 | 統制目標（3桁：x.x.x） | 基本言明要件<br>原則として全て実施 |
| | 詳細管理策（4桁：x.x.x.x） | |
| 第４章　マネジメント基準 | 統制目標（3桁：x.x.x） | |
| | 詳細管理策（4桁：x.x.x.x） | |
| 第５章～18章<br>管理策基準 | 統制目標（3桁：x.x.x） | |
| | 詳細管理策（4桁：x.x.x.x.B,PB） | |
| | 詳細管理策（4桁：x.x.x.x） | 選択制 |

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。

# 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

- 建物を例に、統制目標、詳細管理策の選択プロセス、考え方を示すと以下のとおりです。

（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。
- ISMAP-LIUにおける外部監査対象となる管理策は、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（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サービス
  （Contents Management System）
- 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

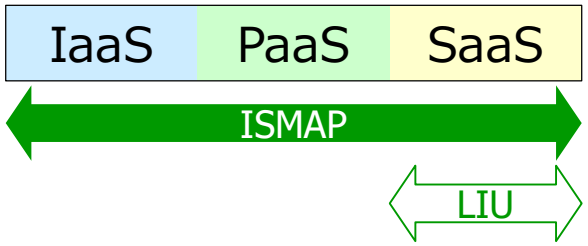
監査全体として現行ISMAPよりも緩やかな設計

**ISMAP-LIUサービス登録**

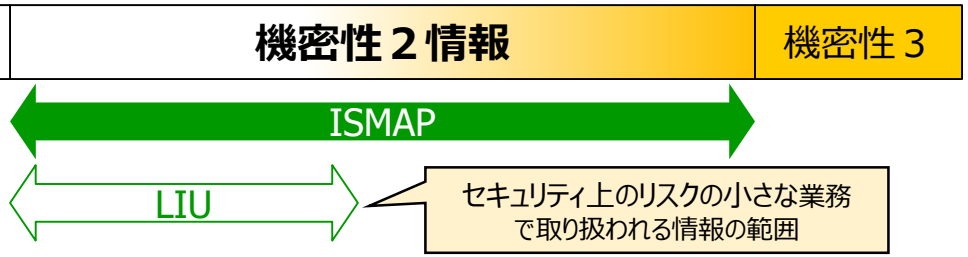
相対的にリスクが低いと評価されるSaaSサービスを登録

# 【参考】ISMAPとISMAP-LIUの比較

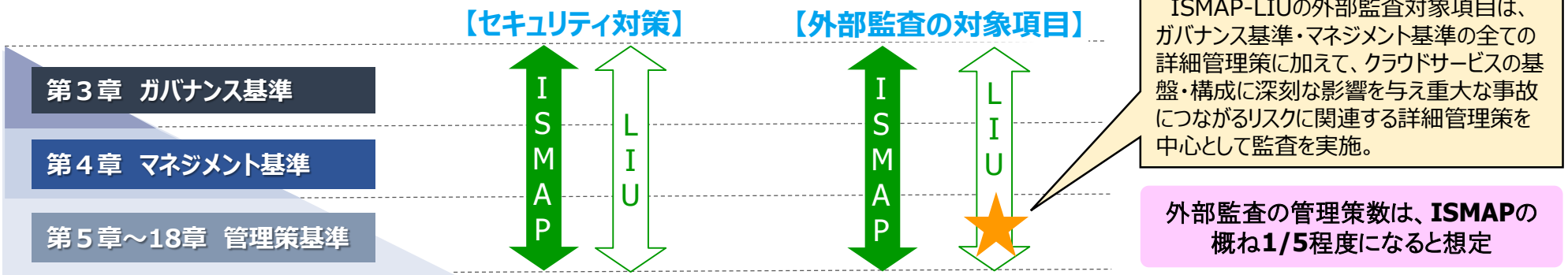
## 【対象となるサービス種別】



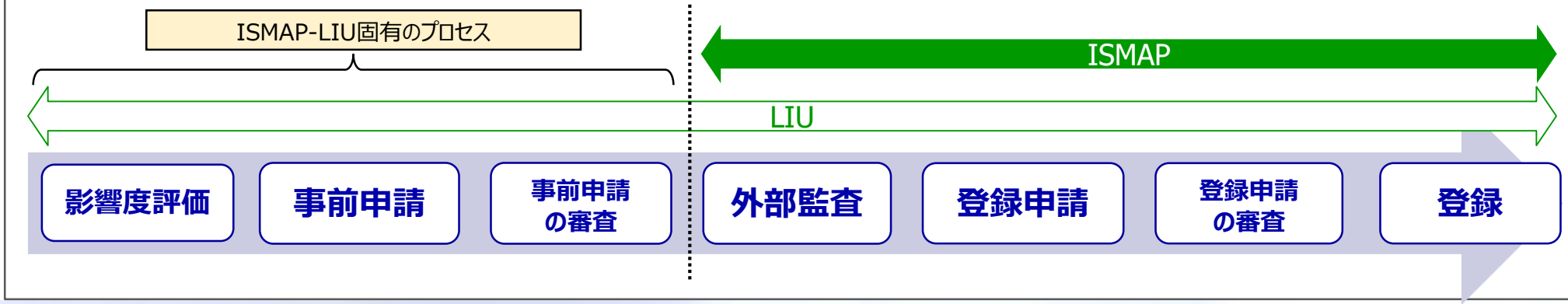

## 【対象となる取扱情報】




## 【ISMAP管理基準で求めるセキュリティ対策と外部監査の対象項目】




## 【サービス登録の流れ】



# 政府機関等におけるクラウドサービスのさらなる利活用について

2

# 政府機関等におけるISMAPの利用に関する決定

## 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４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。

# 政府機関等における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】ガバメントクラウドとISMAPの関係

● デジタル庁が構築するガバメントクラウドにおいても、ISMAPの取得が条件となっています。

**デジタル庁におけるガバメントクラウド整備のためのクラウドサービスの提供（令和5年度募集）　調達仕様書**

5　調達の範囲

（1）基本事項及びマネージドサービス

提供するクラウドサービスにおいては、外部からの不正アクセスや意図しない情報漏洩を未然に防止できるよう、**政府情報システムのためのセキュリティ評価制度である Information system Security Management and Assessment Program**（以下、「ISMAP」という。）**に登録されたクラウドサービスを条件**とする・・・（略）。

① 複数社のクラウドサービスなどを組み合わせてガバメントクラウドとして提供する共同提案の場合には・・・（略）。なお、この場合、**全ての事業者はISMAP取得を条件**とする。

# 地方公共団体における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。

**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（令和５年３月版）**

第1編 総則

第4章 本ガイドラインの構成と対策レベルの設定及びクラウドサービスに関する留意点

・第三者認証

クラウドサービスを評価する場合に、第三者認証を活用することが考えられる。第三者認証は、ISMS（ISO/IEC27001）に加え、**ISMAP**又はクラウドサービスにおける第三者認証（ISO/IEC2701710、ISO/IEC2701811等）**の取得を確認する必要がある**。

第3編 地方公共団体における情報セキュリティポリシー（解説）

第2章 情報セキュリティ対策基準（解説）

8.業務委託と外部サービスの利用

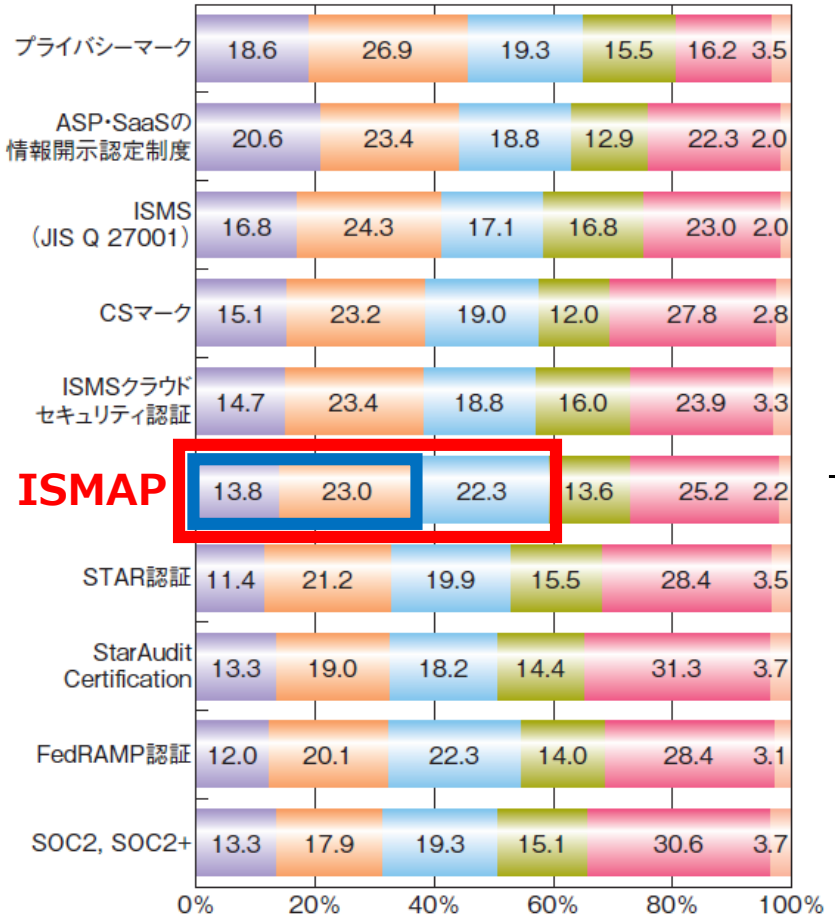
なお、選定条件となる認証には、ISO/IEC 27017によるクラウドサービス分野におけるISMS 認証の国際規格がある。また、**ISMAPの管理基準を満たすことの確認やISMAPクラウドサービスリスト等**のほか、日本セキュリティ監査協会のクラウド情報セキュリティ監査や外部サービス提供者等のセキュリティに係る内部統制の保証報告書であるSOC報告書（Service Organization Control Report）**を活用することを推奨する**。

（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/

# 民間企業で活用されるISMAP

● 民間企業において、クラウドサービスの選定に携わった者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、**ISMAPはクラウド関連の認証・認定制度として一定の認知度があり、その活用が進んでいます**。

**〔SaaS に関連する認定・認証制度の参照度合い（利用者n=457）〕**




「選定条件」+「選定時参考」と回答した利用者

**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

**59.1%**

（出典）
独立行政法人 情報処理推進機構（IPA）情報セキュリティ白書2023
https://www.ipa.go.jp/publish/wp-security/2023.html

# 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、関係者の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。

# 【参考】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。

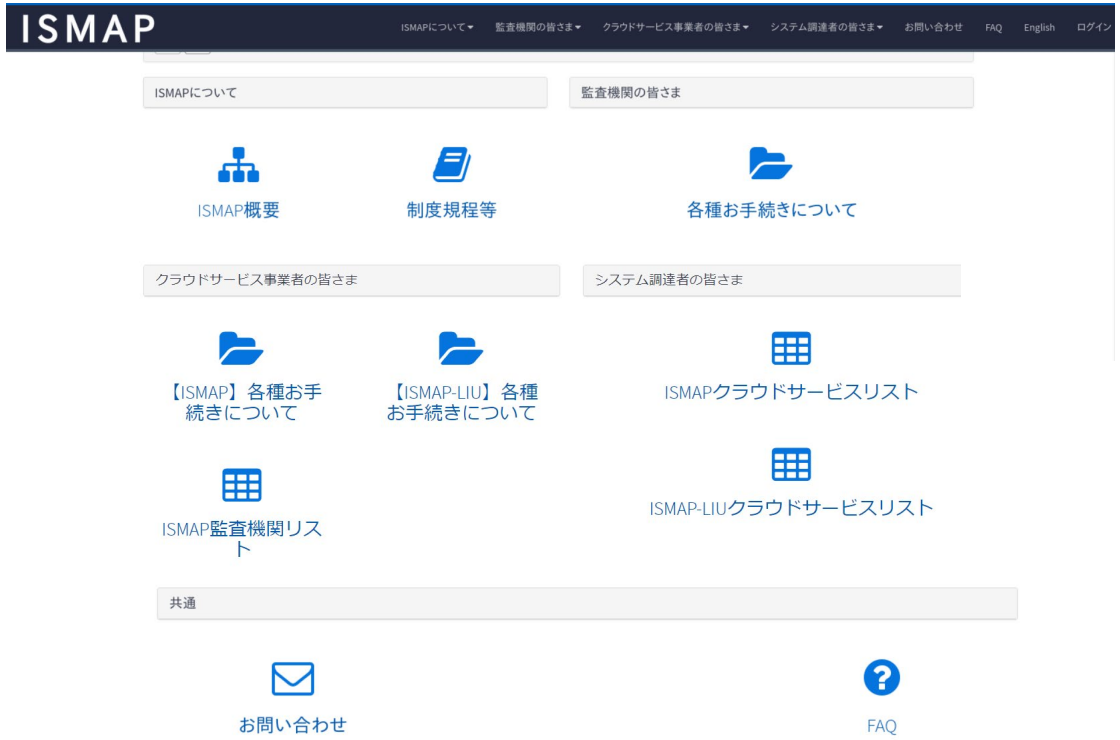
https://www.nisc.go.jp/policy/group/general/ismap.html


## ○ ISMAPポータルサイト

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



# 【参考】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

### 相談窓口

ISMAP-LIU登録に関する質問や相談を受け付ける相談窓口を次のとおり開設しております。お気軽にご連絡ください。
デジタル庁の担当者から折り返しご連絡いたします。

### 連絡先

次のリンク先にアクセスいただき、必要事項をご記入の上、ご連絡ください。
フォームリンク

### 質問・相談例

- 自身が提供するSaaSサービスがISMAP-LIUクラウドサービスリストに登録できるかどうか教えて欲しい
- ISMAP-LIUクラウドサービスリスト登録を申請したいが、必要になる条件を教えて欲しい
- ISMAP-LIUクラウドサービスリスト登録を目指しているが、「業務・情報の影響度評価」を実施してくれるパートナー省庁が見つからないので支援して欲しい

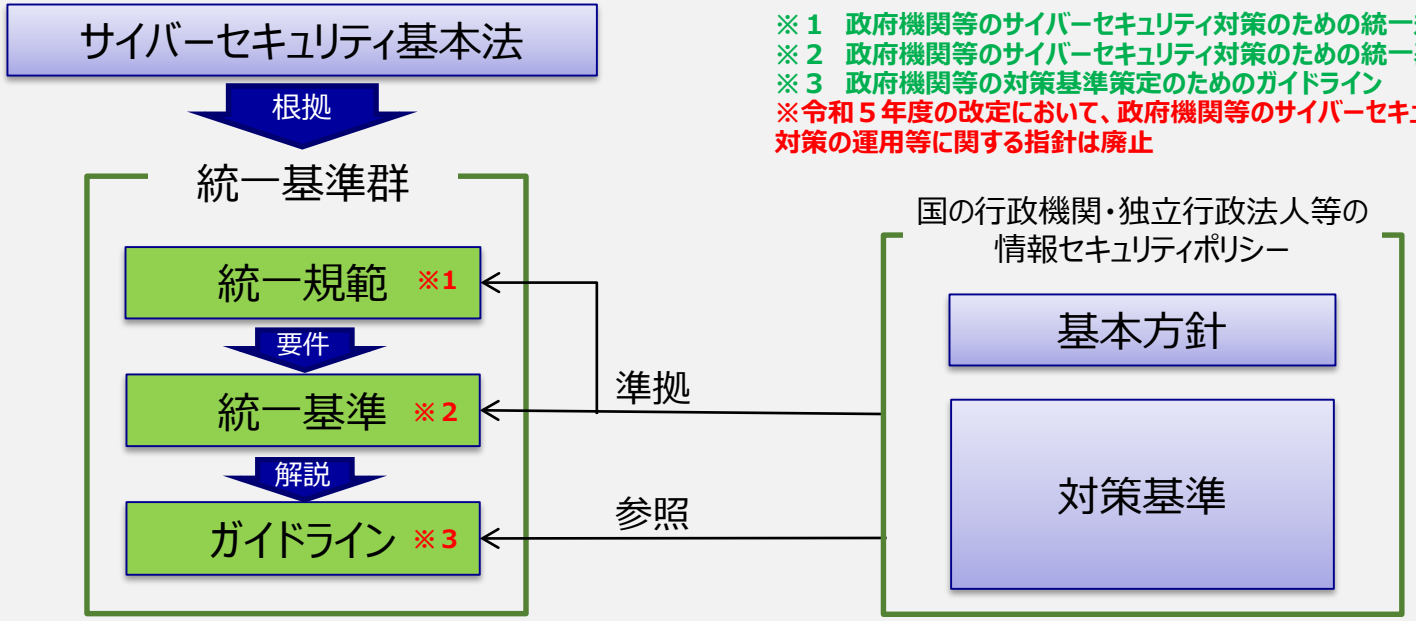
# 【参考】
# 政府機関等のサイバーセキュリティ対策のための統一基準群について

# 統一基準群の位置づけ

● 国の行政機関及び独立行政法人等は、統一規範及びその実施のための要件である統一基準に準拠するとともに、ガイドラインを参照しつつ、組織及び取り扱う情報の特性等を踏まえて情報セキュリティポリシーを策定。

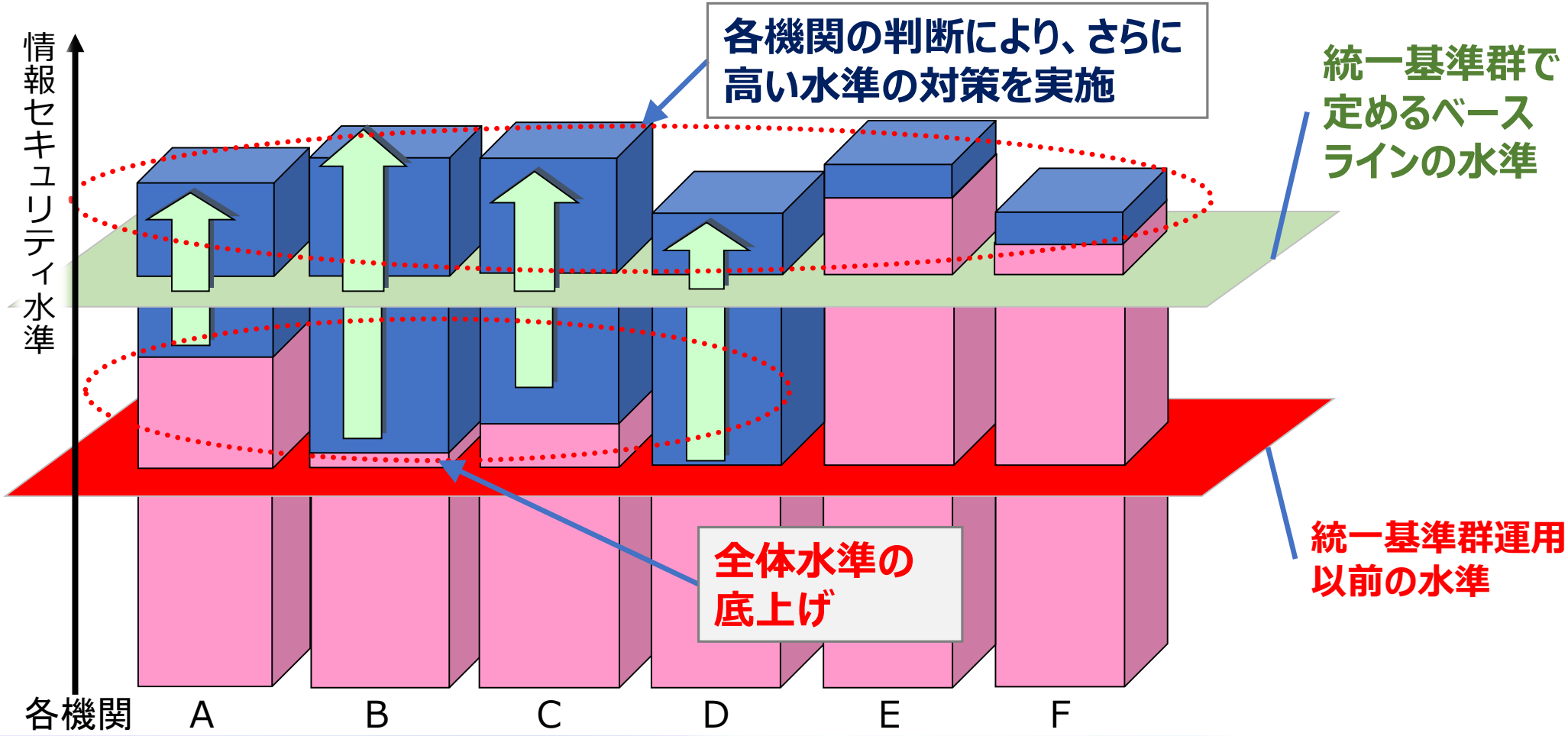
サイバーセキュリティ基本法（平成26年法律第104号）（抜粋）
第二十六条　サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる。
（略）
二　**国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成**及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

政府機関等のサイバーセキュリティ対策のための統一規範（抜粋）
第四条　機関等は、自組織の特性を踏まえ、**基本方針**及び**対策基準**を定めなければならない。
（略）
3　対策基準は、別に定める政府機関等のサイバーセキュリティ対策のための**統一基準と同等以上の情報セキュリティ対策が可能となるように**定めなければならない。

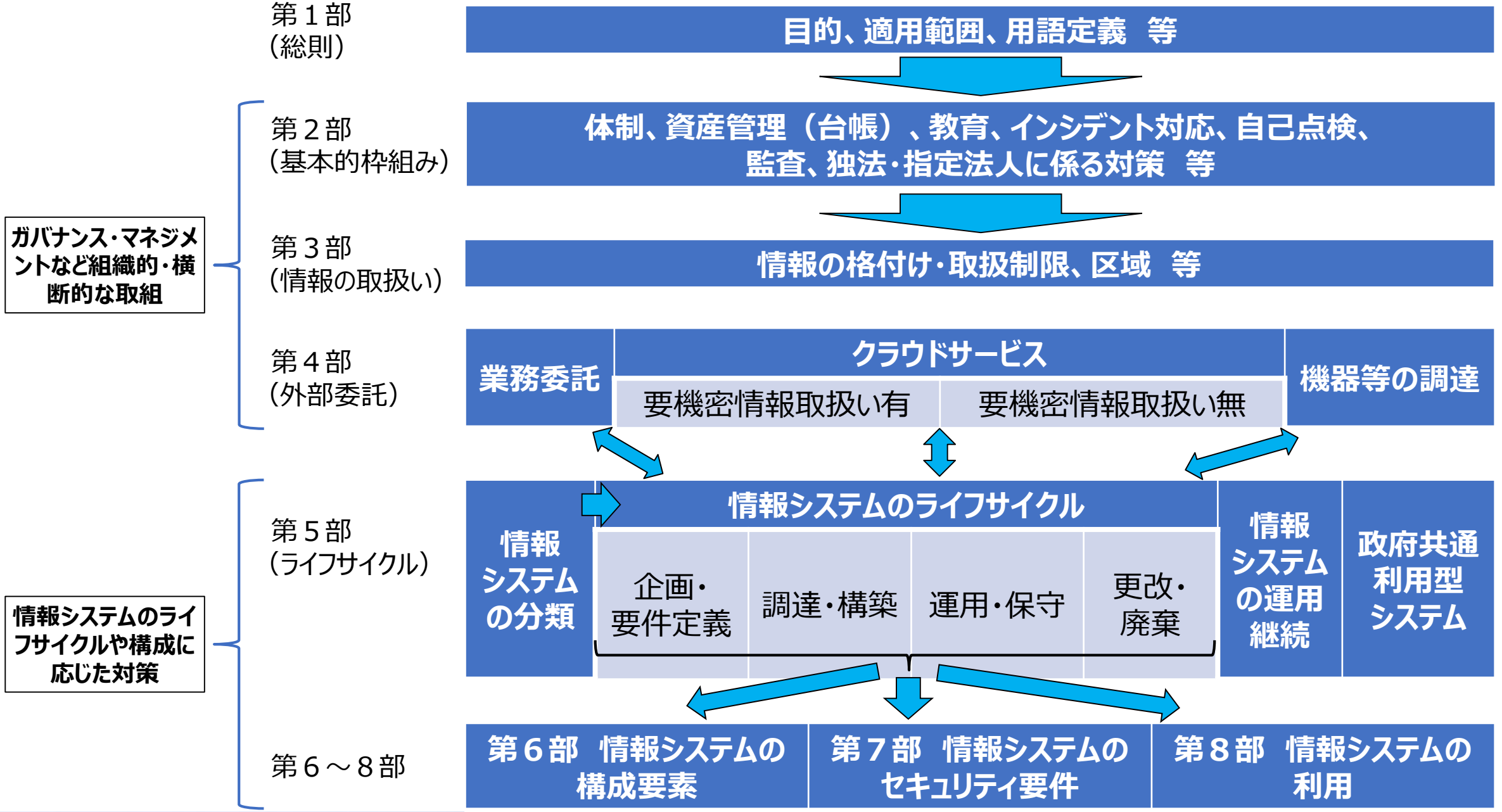


# 統一基準群の役割

- 統一基準群は、政府機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組み。
- 政府機関及び独立行政法人等の情報セキュリティのベースラインを示しており、各機関の判断により、さらに高い水準の対策も可能。



# 統一基準の目次構成（概要図）



# 4.2 クラウドサービス

**用語定義**

「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、**利用者によって自由にリソースの設定・管理が可能なサービス**であって、**情報セキュリティに関する十分な条件設定の余地があるもの**をいう。

クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。

なお、統一基準におけるクラウドサービスは、**機関等外の一般の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービス**であって、**当該サービスにおいて機関等の情報が取り扱われる場合に限るもの**とする。



クラウドサービスを利用する場合は、そのクラウドサービスで要機密情報（機密性２情報・機密性３情報）を取り扱うかどうかによってセキュリティ対策が異なるよ！

要機密情報を取り扱うよ!

4.2.1、4.2.2へ

要機密情報を取り扱わないよ!

4.2.3へ

**＜クラウドサービスの例＞**

- 仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）
- データベースや開発フレームワーク等のミドルウェア等提供サービス（PaaS）
- Web会議サービス
- ソーシャルメディア
- 検索サービス、翻訳サービス、地図サービス

# 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）

- 要機密情報を取り扱う場合は、原則、ISMAP／ISMAP-LIUサービスリスト（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。また、セキュリティ要件は、ISMAP管理基準の管理策基準が求める対策と同等以上の水準を求めること。



## クラウドサービスの選定（要機密情報を取り扱う場合）のイメージ