資料３－１

クラウドサービスの安全性評価に関する検討会について

2019年4月11日
総務省、経済産業省

政府の決定文書とクラウドサービスの位置づけ

- 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。
- 成長戦略、サイバーセキュリティ戦略等において、安全性評価の検討を位置づけている。

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(2018 年6月7日 ＣＩＯ連絡会議決定)

２ 基本方針

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。

クラウドサービスの安全性評価の必要性

○ 適切なセキュリティ管理への懸念等から、政府におけるクラウドサービスの導入が円滑に進んでいない。
○ 民間においても、セキュリティをどのように確認をすればよいかわからず、導入に躊躇する場合がある。

という状況を鑑み、官民双方において、クラウドサービスを積極的に活用するために、何らかの安全性評価の仕組が必要。

未来投資戦略2018(2018 年6月15日 閣議決定　抜粋)

クラウドサービスの多様化・高度化に伴い、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、情報資産の重要性に応じ、信頼性の確保の観点から、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する。

サイバーセキュリティ戦略(2018年7月27日　閣議決定　抜粋)

各府省庁において情報の特性に応じて適切な情報システムの形態を選択するとともに、政府全体としてセキュリティ施策を効率的・効果的に実施できるよう、システムの構築と運用の集約及びセキュリティ水準向上の利点を活かすことができる、政府プライベートクラウドとしての政府共通プラットフォームへの移行を含むクラウド化を推進する。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。

→政府調達における利用を第一に想定しつつ、安全評価の制度運用が本格化した際には、特に情報セキュリティ対策が重要となることが想定される地方公共団体を含む重要産業分野等においても、本制度の評価結果の活用を推奨していくことを念頭に検討を進めている。

クラウドサービスに係る世界の潮流（海外の政府調達について）

- 海外の政府調達では、多くが①クラウドファーストを掲げ、②その直後にクラウドサービスの政府調達に係る認証制度を導入。
- 日本では、2018年6月にクラウド・バイ・デフォルト原則を採用したところ、安全性評価の仕組みの検討が必要。

	クラウド利用の方針	政府クラウド安全性評価制度	主な関連機関
	**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 FedRAMP	General Services Administration （※独立政府機関） GSA
	**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） GDS
	**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 irap	Australian Signals Directorate （※防衛大臣管轄） DEFENCE SIGNALS DIRECTORATE AUSTRALIA
	**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） IM
	**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**	本検討会において整備中	

出典：各制度HPより
※一部の国では、安全性評価制度の構想と並行してクラウド利用の方針を出している。

クラウドサービスの安全性評価に関する検討会のスコープ

- ①基準活用の前提となる情報・情報システムのクラス分けに関する議論と、②クラウド調達の基準等に関する議論を行う。
- 上記に加えて検討すべき事項については、継続的な検討事項として項目整理を行う。

赤字部分が検討会のスコープ

情報・情報システムのクラス分け（政府）

イメージ

レベル３
レベル２
レベル１

※詳細な分類条件、実際の分類作業は別途検討。

参照（P）

情報・情報システムのクラス分け（産業）

①基準活用の前提となるデータ分類の必要性
分類の際のセキュリティ要求事項の整理、報告

その他
情報システム基準・運用

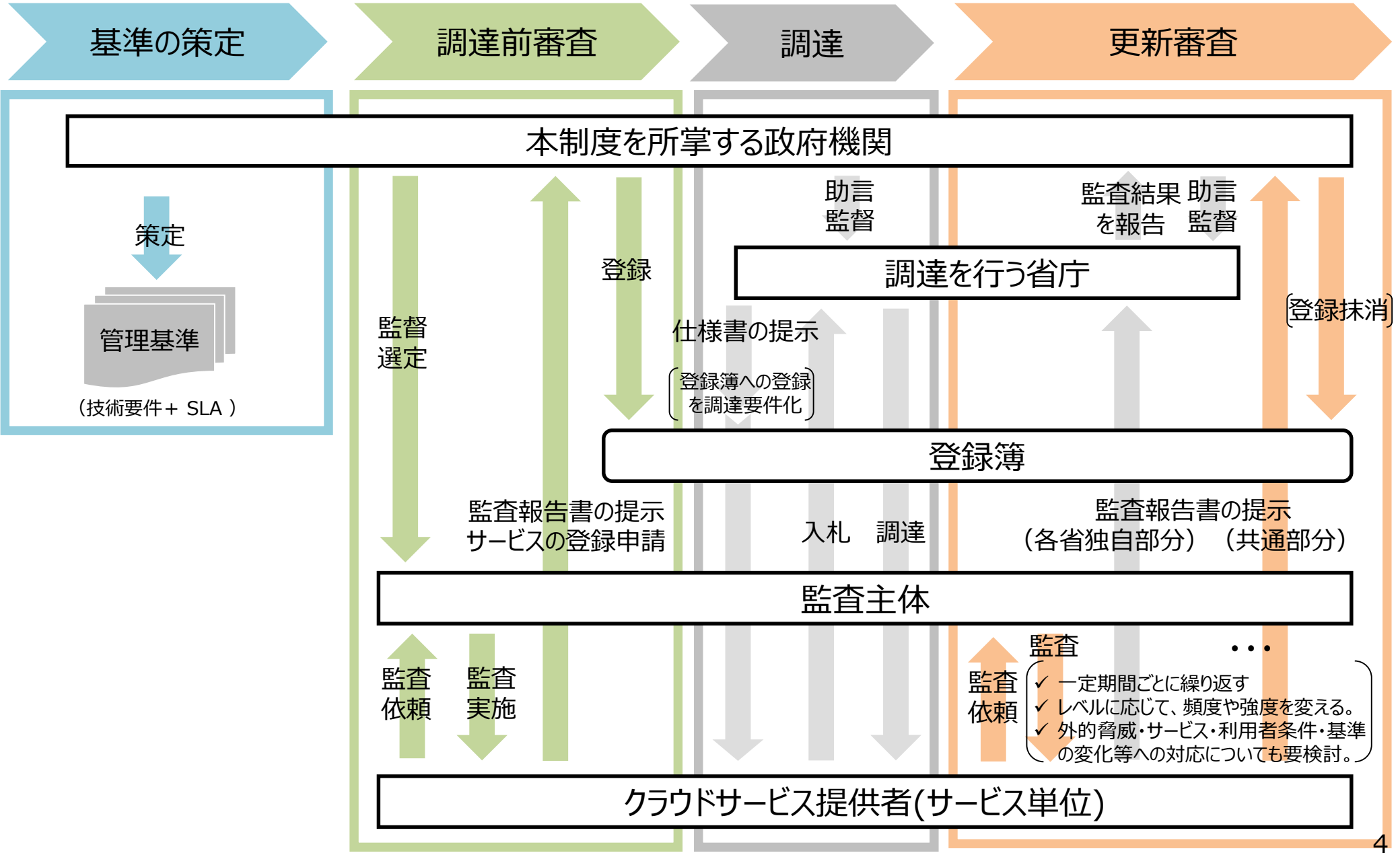
クラウド基準・運用

②・既存の基準＋αの安全性評価方法
・評価の実効性
・運用方法
等を整理、策定。

推奨

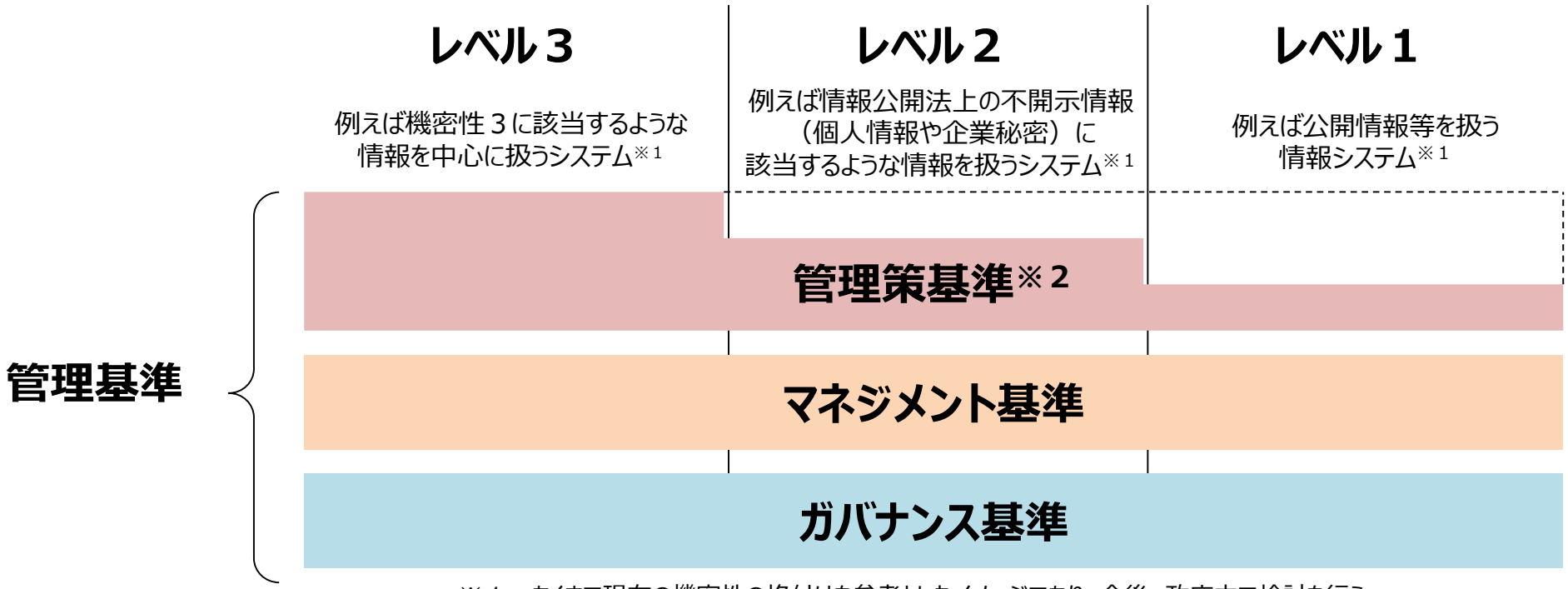
重要産業分野等

クラウド安全性評価のフロー



管理基準項目のイメージ

- ガバナンス基準、マネジメント基準、管理策基準からなる管理基準を策定する。管理策基準を中心に、レベルに応じて項目数・強度・内部監査の活用等に差異を設ける。



※１：あくまで現在の機密性の格付けを参考としたイメージであり、今後、政府内で検討を行う。
※２：個別のサービス単位で具体的なリスクを低減するために必要な管理策を位置づけたもの。

＜参考となる基準等(例)＞

- JIS Q 27001 (ISO/IEC 27001)
- JIS Q 27002 (ISO/IEC 2700 2)
- JIS Q 27017 (ISO/IEC 27017)
- NIST SP800-53 rev.4
- Australian Government Information Security Manual (ISM)
- サイバーセキュリティ戦略本部　政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）
- 日本セキュリティ監査協会　クラウド情報セキュリティ管理基準（平成28年改正版）(経済産業省　情報セキュリティ管理基準（平成28年度版））
- 総務省　クラウドサービス提供における情報セキュリティ対策ガイドライン（第2版）

この他に、データセンターの物理的な基準等も検討する必要がある。

今後のスケジュール(案)

＜2019年＞

夏　　各種基準の素案策定、基準の意見募集（パブリックコメント）

年内　　検討会最終とりまとめ。制度の立ち上げ

＜2020年＞

秋　　全政府機関等での制度活用開始