【参考】ISMAP-LIU（イスマップ　エルアイユー）について（案）

令和４年６月15日（水）
NISC、デジタル庁、総務省、経済産業省

ISMAP-LIU策定の背景

政府情報システムのためのセキュリティ評価制度（以下「ISMAP」という。）は、政府機関等がクラウドサービスを調達する際、ISMAPクラウドサービスリストに登録されたサービスから調達することを原則とする制度として令和2年６月より開始。現在※25社34サービスが登録中　※令和４年６月１日時点

- ISMAPの対象となっている機密性２情報を扱う情報システムは IaaS、PaaS、SaaSと多岐にわたる。
- **中でもSaaSはサービスの幅が広く、用途や機能が極めて限定的なサービス**や、機密性２情報の中でも**比較的重要度が低い情報のみを取り扱うサービス等リスクが低いサービスもあり**、それらのサービスについて現行のISMAPと一律の取扱いとした場合、過剰なセキュリティ要求となり、それにより当該サービスの活用が進まない場合も考えられる。
- このため、**機密性２情報を扱うSaaSのうち、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ものに対する仕組みを創設**することとし、現行ISMAPの枠組みをベースとして、外部監査対象範囲の縮小を含め、想定される各論点について検討を行ったもの。
- あわせて、ISMAP-LIUの検討結果を踏まえ、新規の暫定措置期間のうち類型②について、クラウドサービスの登録申請の状況や各政府機関等におけるニーズを踏まえつつ、制度の利用推進の観点からの見直し要否の検討を行った。

ISMAP-LIUに関連する閣議決定等

デジタル社会の実現に向けた重点計画（令和４年６月７日 閣議決定）

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

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、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みを、令和４年（2022 年）中に策定し、当該仕組みを利用したクラウドサービスの申請受付を開始**するなど、クラウド・バイ・デフォルトの拡大を推進する。

成長戦略フォローアップ（令和４年６月７日 閣議決定）

４．GX（グリーン・トランスフォーメーション）及びDX（デジタル・トランスフォーメーション）への投資

（２）DXへの投資

（サイバーセキュリティ）

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、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みを2022年中に構築**する。

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（令和３年７月６日）

2 - ii　新規の暫定措置期間の枠組みについて

類型② 類型①- ⅰ ～ ⅲ 以外で、ISMAP への申請の予定があるSaaSであって、基盤となるIaaSの登録が必要等の理由により、暫定措置期間に間に合わない場合

代替のサービスがある場合、各政府機関等は、移行作業の準備や予算要求等の対応を進めることが望ましいが、IaaS 等の基盤サービスと比較し、相対的に小規模な SaaS サービスの場合、ISMAP における基盤サービスの先行登録が必要になるなど、ISMAP へ申請するまでに時間を要する可能性がある。そのため、CSP からの申請がなされる見込みであることを要件として、暫定措置期間に間に合わないSaaS サービスは、令和５年３月31 日までの間、暫定措置期間の延長を認めるものとする。

なお、**ISMAP においては、よりリスクの小さい情報システムが利用するクラウドサービスを対象として、簡素な仕組みの検討を予定**しており、その**検討結果を踏まえ、必要な場合は暫定措置期間の見直し**を行う。

ISMAPのうち、リスクの小さな業務・情報の処理に用いるSaaSサービスを対象とする仕組みの名称について

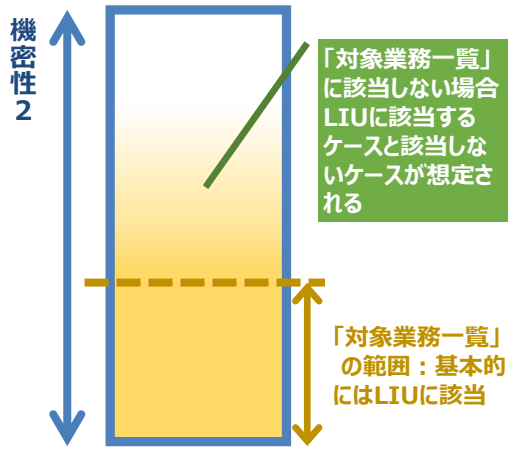
標記仕組みは、ISMAPが対象とするクラウドサービスのうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるSaaSサービスに対する仕組みであり、また情報システムの調達においては、業務・情報の影響度に応じたセキュリティを確保すべきとの考え方から、**影響度が低いと評価される業務、情報に用いられるSaaSを対象とする**制度として趣旨が広く理解されるよう、名称は、**ISMAP for Low-Impact Use（通称：ISMAP-LIU（イスマップ・エルアイユー））** とする方向で検討中。

ISMAP-LIUの基本構成

- ISMAP-LIUの対象は、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もの。
- ISMAP-LIU該当性の判断に当たっては、**利用する各省庁における業務・情報の影響度※評価の提出を必須とし、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**。
  ※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。
- その際、CSP、各省庁による効率的な申請・業務・情報の影響度評価を促すため、**ISMAP-LIUにおける業務・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**することを想定。

「対象業務一覧」の考え方

- **「対象業務一覧」に該当する業務の場合：**
  CSPや利用省庁等が申請、業務・情報の影響度評価を行う際の参考として、ISMAP-LIUにおける業務・情報の影響度が低位である蓋然性が高い業務を例示したものであり、対象業務一覧に該当する業務に用いるSaaSに係る事前申請はLIU対象として扱う。
- **「対象業務一覧」に該当しない業務の扱い：**
  対象業務一覧に該当しない業務（要検討業務）に用いるSaaSについては、CSPからの事前申請を受け付けた上で当該業務に係わる業務・情報の影響度評価の結果が低位であることの妥当性を、複数の省庁(2省庁を想定)の結果から判断する。低位である妥当性が確認された業務については、順次、対象業務一覧に追加する。
  要検討業務の判断については、一定の処理期間を設ける。



対象業務一覧の取扱いについて

- 影響度が低位である蓋然性が高く、**ISMAP-LIUの対象となるSaaSが取り扱って差し支えないと考えられる業務（対象業務一覧）**を制度より例示として公表する。
- 制度開始当初においては、以下の８項目を対象業務とし、利用省庁や制度所管（特にISMAP運用支援機関（IPA））が、「当該業務が対象業務に該当するかどうか」及び「ある情報の影響度評価が低位であるかどうか」を形式的に判断できるよう、**影響度評価例を含む詳細を制度所管が定める「ガイダンス」として公表**する。
- その際、**対象業務としての該当性判断は赤字の記載部分に基づいて行う**。（黒字の記載部分は具体的な参考例であり、当該参考例に限定されない。）
- 要検討業務（もともと対象業務一覧に該当しない業務）のうち、業務・情報の影響度「低位」と判断された業務は順次対象業務一覧に追加し、一覧を拡充する。

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）

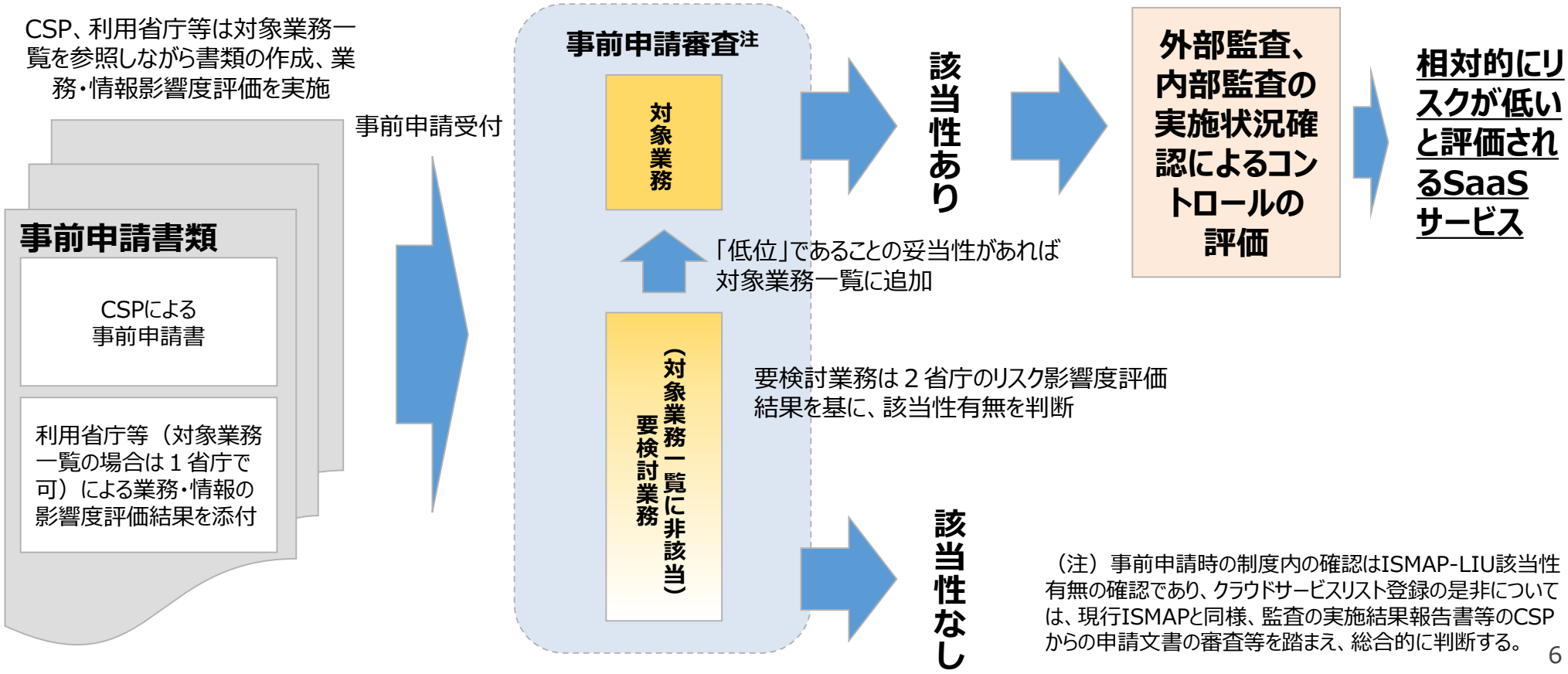
6. 災害時等に組織構成員の被災状況確認等を行う業務

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

事前申請から登録までの制度の全体像

- 事前申請において、**利用省庁等の業務・情報の影響度評価の提出を必須とするほか、対象業務一覧に当たるか確認の上**、ISMAP-LIU該当性を判断。（ISMAPにはない審査プロセス）
- ISMAP-LIU該当性として、影響度の低い業務に用いられるSaaSであることが確認された事前申請は、判断結果をCSPに通知した上で、外部監査等によるCSPのコントロールの確認等を通じて本申請の際に審査し、ISMAP-LIUとしての登録を判断。（この点はISMAPと同様。）



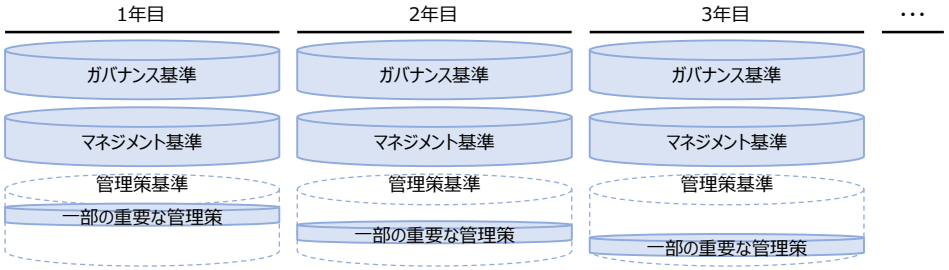
（注）事前申請時の制度内の確認はISMAP-LIU該当性有無の確認であり、クラウドサービスリスト登録の是非については、現行ISMAPと同様、監査の実施結果報告書等のCSPからの申請文書の審査等を踏まえ、総合的に判断する。

外部監査の仕組み・制度運用の仕組みの全体像

- 外部監査では、ガバナンス・マネジメント基準は全量を対象としつつ、管理策基準はサービス基盤・構成に直接的な影響を及ぼし得る管理策（一部の重要な管理策）を主な対象に数年に平準化しつつ実施することで、全体として外部監査対象範囲を縮小[注]。その上で、取消・公表制度や内部監査に係る報告書の提出を求める。
- 上記のとおり、外部監査対象範囲を縮小し、内部監査の実施状況報告を3年で一巡することによって、監査全体としては現行ISMAPよりも緩やかな制度設計となる。したがって、取消・公表制度においてCSPの自発的な統制整備・運用を促す。

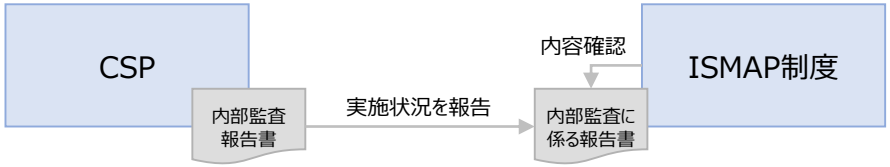
（注）事前申請を通過後、監査機関と民・民における監査契約締結前において、実際の外部監査対象管理策数等を踏まえた上で契約を結ぶことを監査機関に周知しており、CSPにおいてはその際に、コストメリット等を享受できるものと想定。

①：外部監査の仕組み



- ✓ 外部監査は**毎年の頻度**で実施する。
- ✓ **ガバナンス基準・マネジメント基準については、全管理策を対象**とする。
- ✓ **管理策基準については、「サービス基盤やサービス構成に直接的な影響を及ぼし得る管理策」を主な対象**とする。

②：内部監査の実施状況確認の仕組み

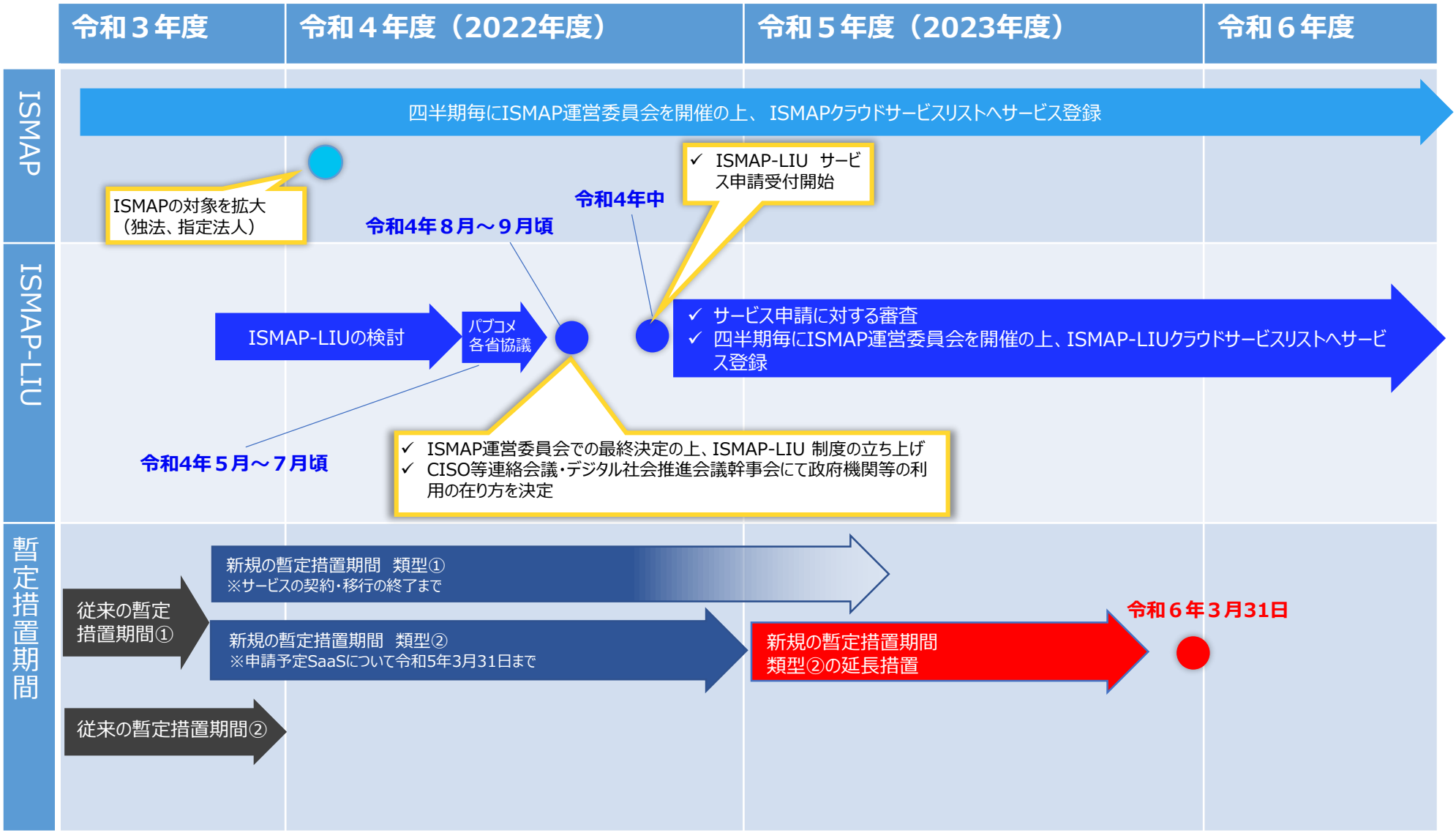


- ✓ CSPの自発的な統制整備・運用を促すことを目的に、CSPが自ら実施する**内部監査の内容についてを報告を求める**。
- ✓ **全統制目標について少なくとも3年に一度は内部監査の実施を求める**。

③：取消・公表制度

- ✓ ISMAP-LIUにおける取消公表の流れは、ISMAP本体における再監査、再申請のプロセスを基本的には踏襲する。
- ✓ ただし、**特に重大な影響を及ぼしうるインシデントが発生した際には、追加の枠組みとして、制度側で当該サービスの登録を即座に一時停止**する。
- ✓ 当該仕組みにより、CSPの**自発的な統制整備・運用を促す**ような制度設計を目指す。

ISMAP-LIU及び暫定措置期間のスケジュール（案）



ISMAP-LIUの全体像

「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（サイバーセキュリティ戦略本部決定）

制度運営側向け

- 運営委員会 基本方針※1
- 運営規則
- ★基本規程

政府機関等向け

ISMAPの利用について（CISO等連絡会議・デジタル社会推進会議幹事会決定）

- 別紙１　ISMAPの暫定措置の見直しについて【一部改正】
- **別紙２　ISMAP-LIUの制度及び利用について【新規】**

クラウドサービス事業者（CSP）向け

サービス審査

★クラウドサービス登録規則

- クラウドサービス登録基準（制度運営側向け）
- CSPに対する要求事項（CSP向け）
  - 申請時情報提供 登録期間中対応
  - ★管理基準
    - ガバナンス基準
    - マネジメント基準
    - 管理策基準

サービス審査

LIUクラウドサービス登録規則【新規】

政府機関等向け
- **【別紙】影響度評価基準【新規】**

政府機関等向け

影響度評価ガイダンス【新規】

監査機関向け

監査機関向け

監査実務における基準等

- 情報セキュリティ監査基準※2
- ★監査ガイドライン
- ★標準監査手続

監査機関審査

監査機関登録規則

- 監査機関登録基準（制度運営側向け）
- 監査機関要求事項（監査機関向け）

は文書名

※1　内閣官房（内閣サイバーセキュリティセンター・情報通信技術（IT）総合戦略室）・総務省・経済産業省　令和2年5月25日施行

※2　平成15年経済産業省告示第114号

※★は、ISMAP-LIU策定に合わせて一部改正を行うもの