イ ス マ ッ プ エルアイユー

ISMAP-LIUについて

令和４年１１月１日（火）
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※27社37サービスが登録中　※令和４年11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。

ISMAP-LIUの名称について

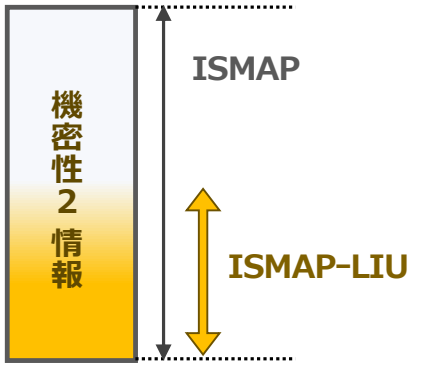
ISMAPが対象とするクラウドサービスのうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるSaaSサービスに対する仕組みであり、また情報システムの調達においては、業務・情報の影響度に応じたセキュリティを確保すべきとの考え方から、**影響度が低いと評価される業務、情報に用いられるSaaSを対象とする**制度として趣旨が広く理解されるよう、名称は、

ISMAP for Low-Impact Use（通称：ISMAP-LIU（イスマップ・エルアイユー）） とする。

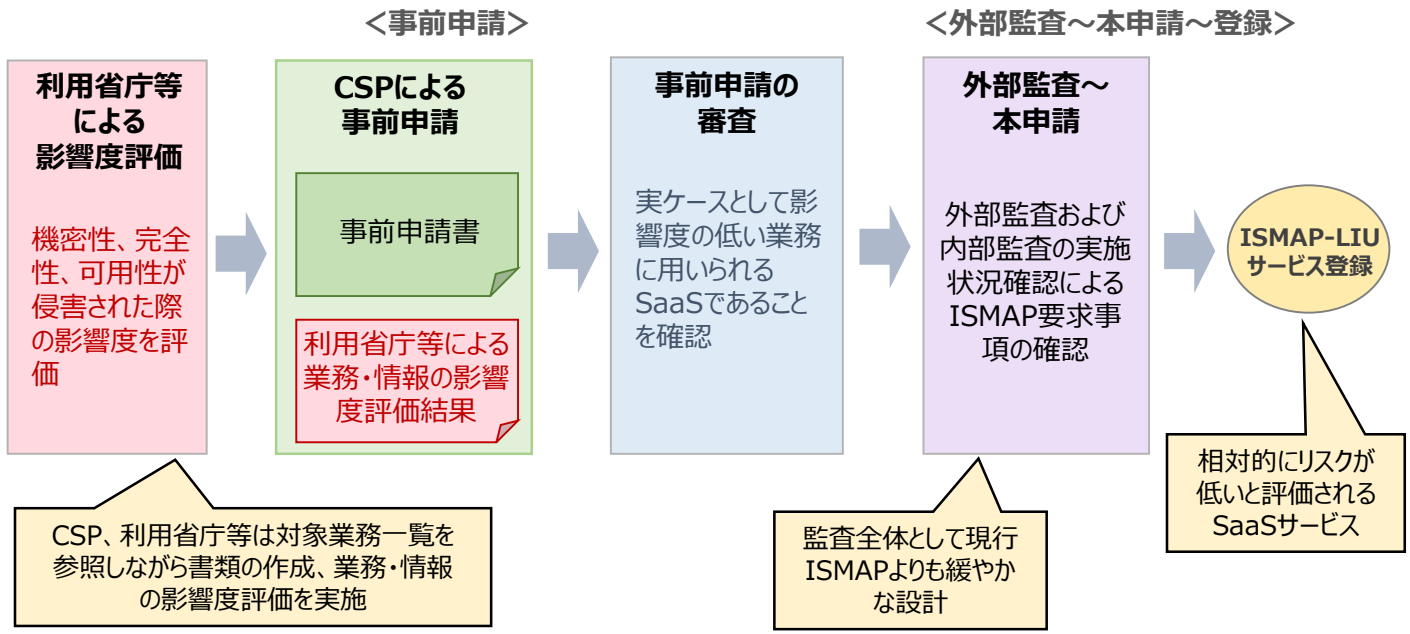
ISMAP-LIUの基本的な仕組み・登録までの流れ

- 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**。

【対象範囲のイメージ】



【ISMAP-LIUサービス登録の流れ】



ISMAP-LIUの該当性判断で求められる事項

- ISMAP-LIUの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**。

対象となるSaaSの該当性判断の仕組み

制度

- ISMAP-LIUの該当性審査のため、**事前申請プロセス**を設け、申請対象のSaaSに対する業務・情報の**影響度評価の結果が低位であることの審査を行う。**
- **各省庁の適正な影響度評価を促すため**、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**）**を例示**する。

省庁

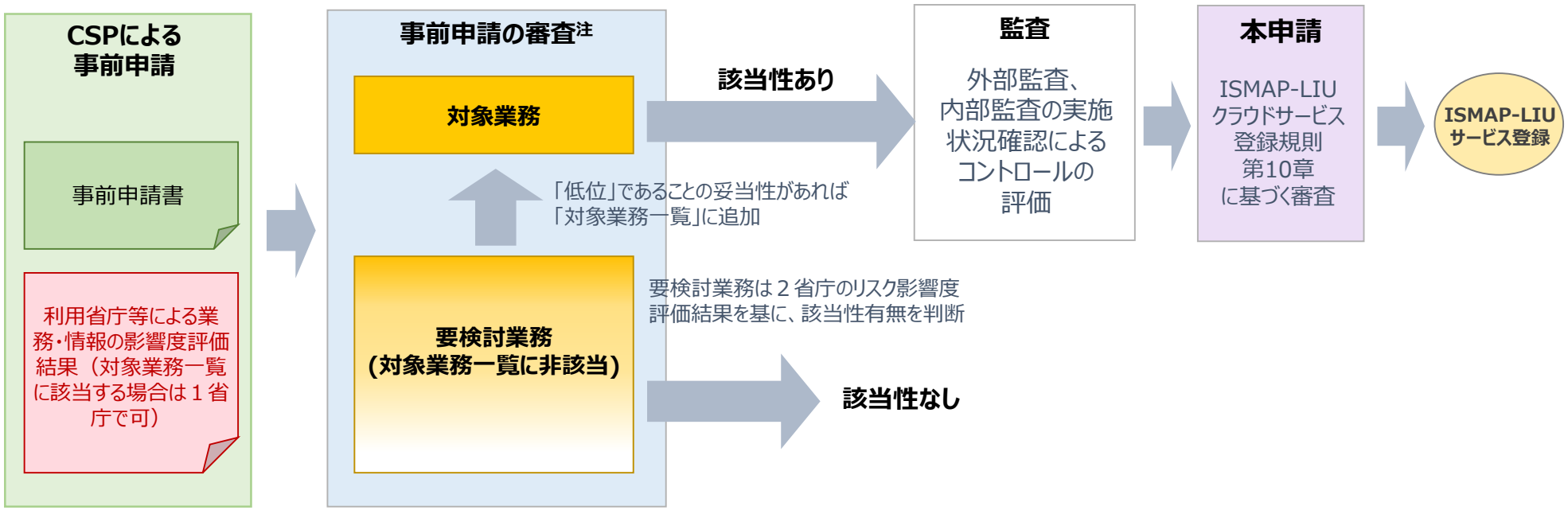
- **SaaSの利用に係わる業務・情報の影響度評価を行う。**
- 影響度評価においては、**評価対象業務がどの対象業務一覧の例示に該当するかも明記**する。

CSP

- CSPは**利用省庁による影響度評価結果を含む所定の書類**を準備の上、**事前申請プロセスにおいて提出**する。

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の該当性を判断。（ISMAPにはない審査プロセス）
- ISMAP-LIUの該当性として、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。

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。
- 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。

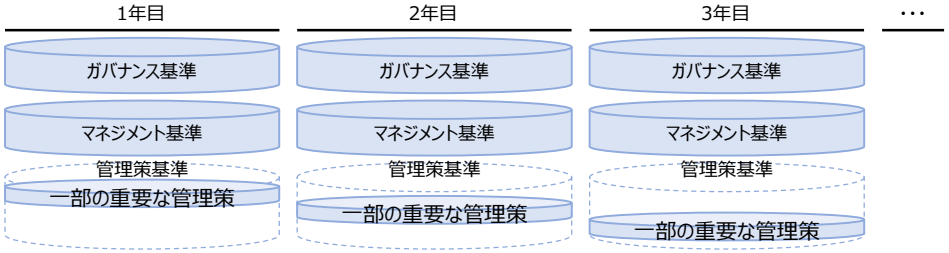
1. **公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務**
   有識者を招いた審議会等の運営を行うために、Web会議による会議運用や、ファイル共有による情報の保存・管理・共有を行う用途
2. **政府職員の業務上の役職・氏名情報を扱う業務**
   （業務の性質上、従事する職員の情報について厳格な秘匿が求められている場合を除く）
   政府職員の役職・氏名情報を用いて職員の人事管理やタレントマネジメントを行う用途
3. **名刺情報等の一般に広く提供する範囲の情報、公開情報の配信に伴う配信先等管理情報を扱う業務**
   企業、役職、氏名等の名刺情報を登録・管理を行う用途
   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情報の登録・管理を行う用途
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・一般公開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**
   定型的・日常的な業務連絡、日程表等／出版物や公表物を編集した文書
   ○○省の所掌事務に関する事実関係の問い合わせへの応答／意思決定の途中段階で作成したもので、当該意思決定に与える影響が極めて小さい文書

ISMAP-LIUにおける外部監査、内部監査、取消・公表制度について

- ISMAP-LIUの外部監査では、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、外部監査の対象範囲を縮小。
- 加えて、「取消・公表制度」や「内部監査の実施状況確認の仕組み」によってCSPの自発的な統制整備・運用を促す。

（参考）外部監査において対応すべき管理策数は現行ISMAPの概ね1/5程度になると想定され、監査の業務量としては相当の軽減が見込まれることから、相応のコストが軽減される見込み。

外部監査の仕組み



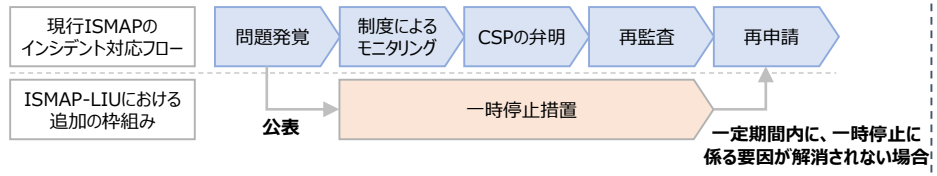
- ✓ 外部監査は**毎年の頻度**で実施する。
- ✓ **ガバナンス基準・マネジメント基準については、全管理策を対象**とする。
- ✓ **管理策基準については、「サービス基盤やサービス構成に直接的な影響を及ぼし得る管理策」を主な対象**とする。

内部監査の実施状況確認の仕組み



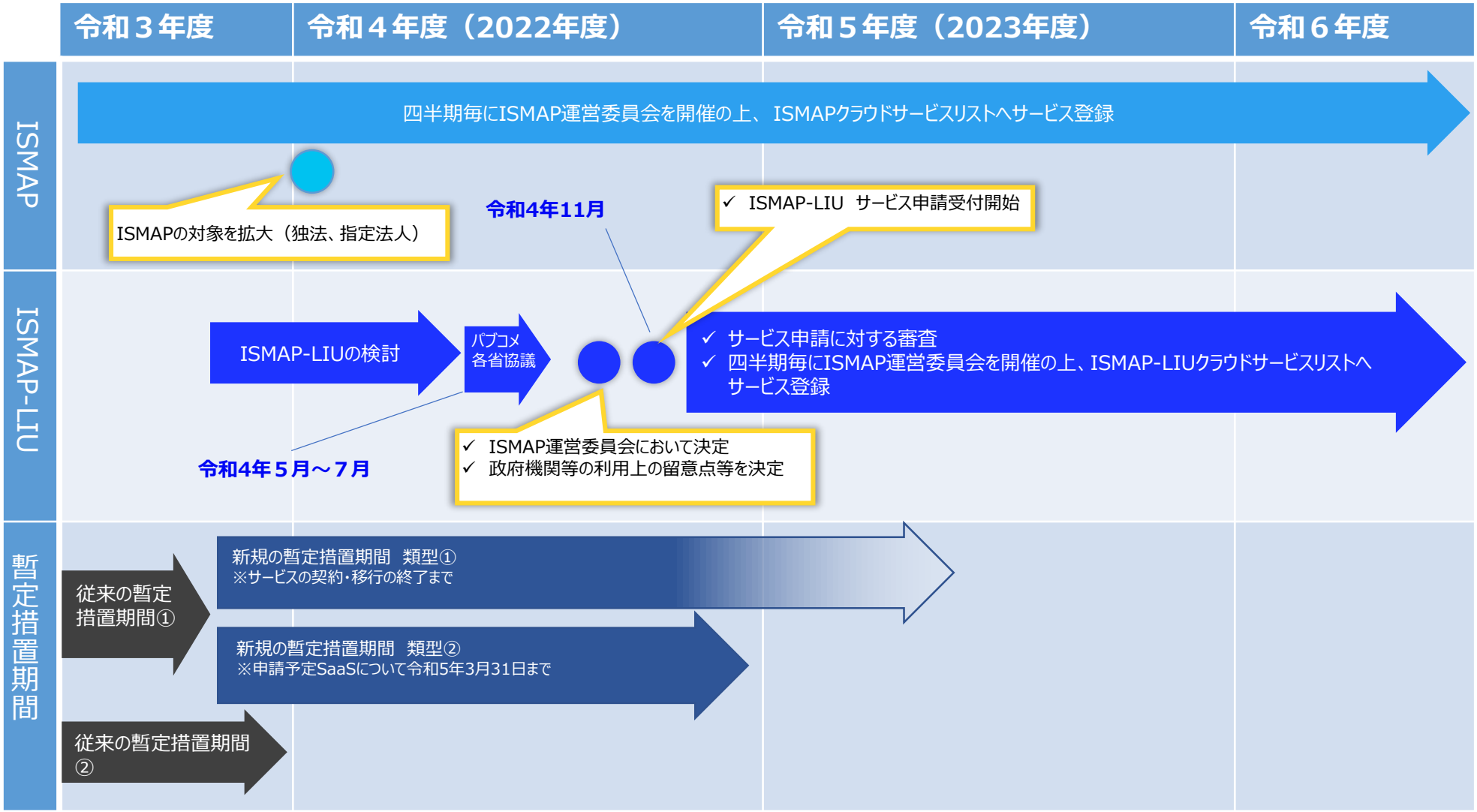
- ✓ CSPの自発的な統制整備・運用を促すことを目的に、CSPが自ら実施する**内部監査の内容についてを報告を求める**。
- ✓ **全統制目標について少なくとも3年に一度は内部監査の実施を求める**。

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。

ISMAP-LIU及び暫定措置期間のスケジュール



ISMAPおよびISMAP-LIUの規程類全体像

