特集

行政における パブリック・クラウド

英国や米国などの電子政府先進国では、2010年代よりクラウドサービスの活用を他の選択肢に優先して検討するクラウド・ファースト原則のもと、パブリック・クラウドの活用が積極的に推進されている。我が国でも2018年に「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」において、クラウドサービスの利用を第一候補として検討を行うクラウド・バイ・デフォルト原則が掲げられた。また、本年には政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録する「政府情報システムのためのセキュリティ評価制度（ISMAP）」が整備されるなど、パブリック・クラウドの活用に向けた制度整備が進められている。

本特集では、我が国及び英国政府におけるパブリック・クラウド活用に関する政策及び制度整備の内容を紹介するとともに、我が国行政機関が今後パブリック・クラウドを活用する上でのセキュリティや調達、契約・支払等の課題及び解決の方向性を解説する。本特集を通じて、パブリック・クラウドが既に行政機関にとって現実的な選択肢の一つとなっていることをお示ししたい。

特集

各国政府におけるクラウド導入に関する政策動向

諸外国	日本
・米国「クラウド・ファースト原則」策定（2010） ・カナダ「クラウド・コンピューティングロードマップ」策定（2010） ・米国「連邦クラウドコンピューティング戦略」策定（2011） ・英国「政府クラウド戦略」策定（2011） ・ニュージーランド「政府におけるクラウド活用に関する指令」発出（2012） ・英国「クラウド・ファースト原則」策定（2013） ・ニュージーランド「クラウド・ファースト原則」策定（2013） ・豪州「政府クラウド・コンピューティング原則」改訂（2014） ・カナダ「政府における適切なクラウドの導入に関する戦略」策定（2016） ・米国「連邦クラウドコンピューティング戦略」改訂（2018） ・カナダ「クラウド・ファースト戦略」策定（2018）	・「世界最先端 IT 国家創造宣言・官民データ活用推進基本計画」策定（2017） ▶クラウド・バイ・デフォルトの考え方に基づき国や自治体の情報システム改革・業務の見直し等の方針を国が定め、国と自治体が一体的に取組を推進 ・「デジタル・ガバメント推進方針」策定（2017） ▶情報システムに関して、民間クラウドや民間サービスを活用し、行政機関が全てを保有・管理する形態から必要なものを必要な期間利用する考え方へ転換 ・「デジタル・ガバメント実行計画」策定（2018） ▶各種クラウド利用に関する考え方や課題等を整理。特に、民間クラウドの技術的、管理的なレベルが政府情報システムの構築に十分か判断する材料を提供 ・「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」策定（2018） ▶クラウド・バイ・デフォルト原則を具体化するとともに、各府省のクラウドサービス利用検討フェーズに係る基本的な考え方を提示

（出典）一般社団法人 行政情報システム研究所作成

特集

行政におけるパブリック・クラウド

政府情報システムのためのセキュリティ評価制度（ISMAP）と今後の展望

政府機関における安全・安心なクラウドサービス利用へ向けた取組

総務省
情報流通行政局情報流通振興課
課長補佐
（前　サイバーセキュリティ統括官室　参事官補佐）
相川　航

総務省
サイバーセキュリティ統括官室
事務官
中村　公洋

1. はじめに

インターネット上に設けたリソースを提供するサービスであるクラウドサービスは、サービスアプリケーションから多様なIoTプラットフォームまで、様々なICTソリューションを支えており、データの利活用・管理における中核のサービスとなっている。クラウドサービスの多様化・高度化に伴い、効率性の向上、セキュリティ水準の向上などの目的から、官民ともに、クラウドサービスの導入が進み、情報管理や情報システムの舞台がクラウド上に移りつつあるといえる。

他方、クラウドサービスの導入においては、官民ともにセキュリティへの不安が挙げられており[1]、その導入を円滑化するためには、セキュリティに関する統一的な評価を実施することが有効だと考えられる。特にセキュリティの確保が求められる政府機関の情報システムについては、システムを構成するクラウドサービスのセキュリティを評価する制度の構築が急務となる。

その際、クラウドサービスの導入に係る様々な方針やガイドライン等に基づいて、各政府機関が独自に全てのセキュリティ要件を最初から確認するという従来の方法では非効率的であるため、クラウドサービスについて、統一的なセキュリティ基準を明確化し、実効性・効率性のあるセキュリティ評価制度が必要となる。

本稿では、上記の様な観点のもと、政府において検討を進めてきた「政府情報システムのためのセキュリティ評価制度（ISMAP）」について、その概要を説明するとともに、本制度の今後の展望について述べる。

[1] 民間企業に関する調査については、「ICT によるイノベーションと新たなエコノミー形成に関する調査研究」（2018年3月三菱総合研究所）などを参照。

2. ISMAP運用開始までの経緯

平成30年6月に、政府は「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日各府省情報化統括責任者（CIO）連絡会議決定。）を定め、クラウド・バイ・デフォルト原則を掲げる一方で、「未来投資戦略2018」（平成30年6月15日閣議決定。）、及び「サイバーセキュリティ戦略」（平成30年7月27日閣議決定。）において、クラウドサービスの安全性評価に関する検討の必要性が位置付けられた。

これを受け、平成30年8月から令和元年12月に

かけて、総務省と経済産業省が事務局となり、「クラウドサービスの安全性評価に関する検討会」（座長：大木　榮二郎　工学院大学　名誉教授）を開催し、令和2年1月にはパブリックコメントを経たとりまとめが行われた。

さらに、上記の閣議決定や検討会のとりまとめ等を踏まえ、「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」（令和2年1月30日サイバーセキュリティ戦略本部決定。）において、本制度の（1）基本的枠組み、（2）各政府機関等における利用の考え方、（3）所管と運用体制が決定された。

基本的枠組みを受け、令和2年5月25日に本制度の最高意思決定機関として有識者[2]と制度所管省庁（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）を構成員としたISMAP運営委員会が設置されるとともに、令和2年5月26日に第1回ISMAP運営委員会を開催し、委員会合において制度に関する各種規程等が決定され、ISMAPの運用が開始された。

併せて、今回の運用開始に先立ち、令和2年3月27日から同年4月26日までの間で実施していた「政府情報システムのためのセキュリティ評価制度（ISMAP）における各種基準（案）」に対する意見募集の結果についても令和2年6月3日に公表した。

[2] 有識者は①情報セキュリティ監査②クラウドコンピューティング③情報セキュリティの分野の専門家等を含む。

3. ISMAPの概要

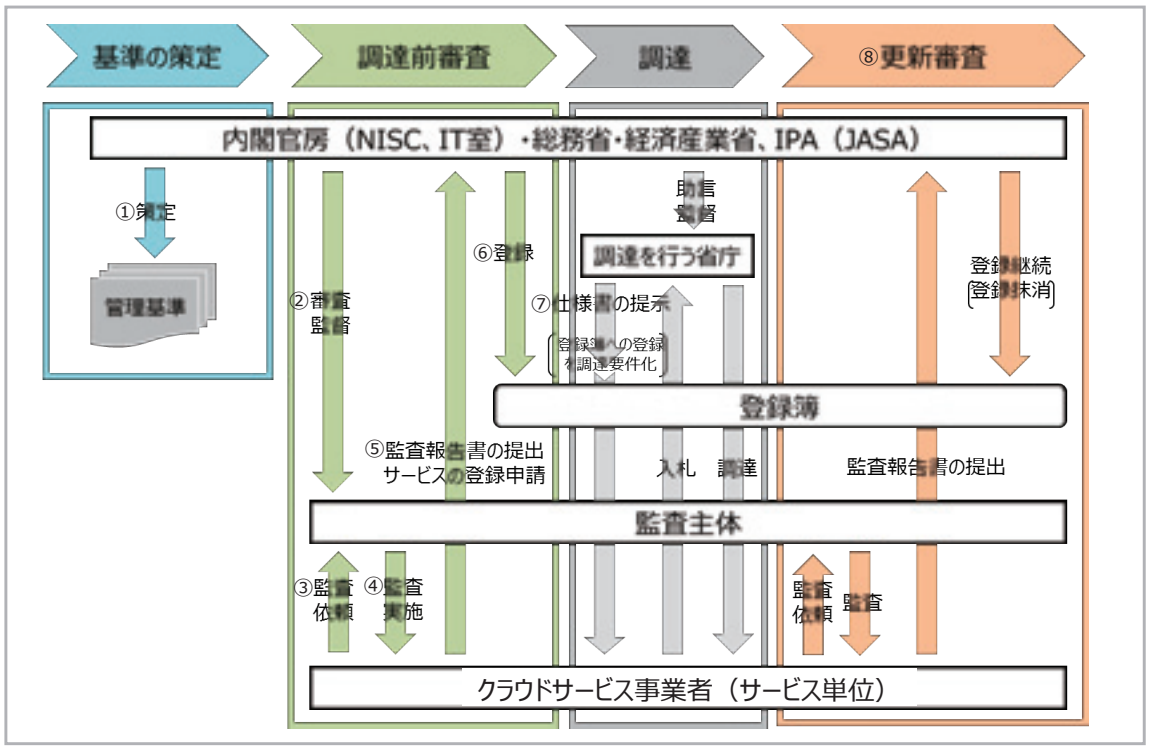
本制度は、情報セキュリティ監査の枠組みを活用した評価プロセスに基づき、本制度において定められた基準に基づいたセキュリティ対策を実施していることが確認されたクラウドサービスを、本制度が公表するクラウドサービスリストに登録するものである。また、本制度における監査を行うことができる監査機関についても、あらかじめ本制度で定める監査機関に対する要求事項を満たすことが確認され、本制度が公表する監査機関リストに登録とするものとしている。

具体的には、ISMAP運営委員会が決定したISMAP管理基準に対して、クラウドサービス事業者（CSP）が提供するサービスがそのサービスごとに基準を満たすか否かを監査機関が監査する。その上で、監査の実施結果報告書から基準を満たすサービスであると判断できるものについて政府が登録簿に登録することとする。システム調達を行う各政府機関等がクラウドサービスを利用する際には、原則として当該登録簿に登録のあるサービスから調達するものとする。上記枠組みをより詳細に時系列で並べると、以下のような流れとなる（図1）。

①ISMAP運営委員会が管理基準等を策定。
②基準に基づき、クラウドサービスを監査する監査機関をISMAP運営委員会が選定。
③CSPは選定された監査機関に対し、登録を目指すクラウドサービスの監査を依頼。
④依頼された監査機関は、一定の手続に従って監査を行い、監査の実施結果報告書等を作成。
⑤CSPは当該実施結果報告書等を添付の上、ISMAP運営委員会に対して登録を申請。
⑥ISMAP運営委員会は登録審査において問題がなければ登録簿へ登録。
⑦システムを調達する各政府機関等は、クラウドサービス利用に際し、登録簿からの選定を原則とする。
⑧CSPは登録継続のため、一定の期間ごとに監査を受け、登録の更新の申請を実施。

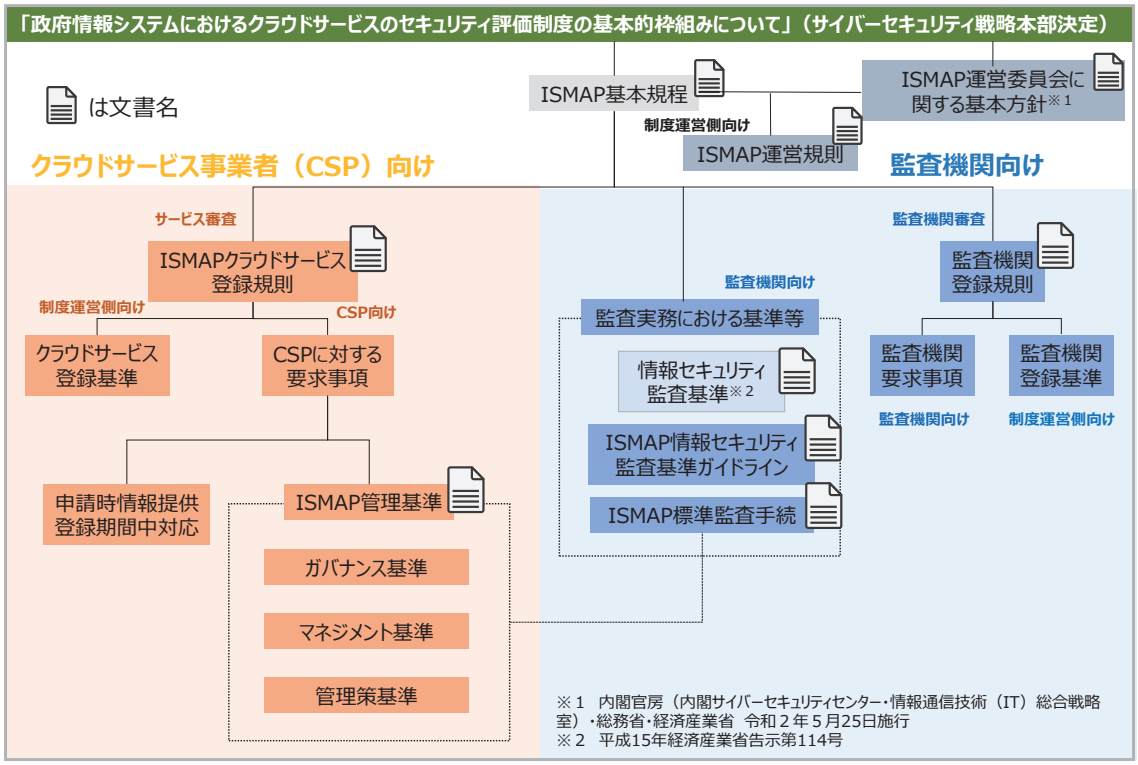
本制度に係る文書及び規程類については、制度全般に関する規程である「政府情報システムのためのセキュリティ評価制度（ISMAP）基本規程」（以下「ISMAP基本規程」という。）を除けば、①制度運営側[3]向け、②CSP向け、③監査機関向けの3種類に大別される。具体的には図2の通りである。今回は紙面が限られているため、文書としては「ISMAP基本規程」、「ISMAPクラウドサービス登録規則」、「ISMAP管理基準」、「ISMAP監査機関登録規則」の4点について説明をする。

図1　ISMAPの基本的な流れ



（出典）総務省作成

図2　ISMAPに関する規程等



（出典）総務省作成

（1）ISMAP基本規程

ISMAP基本規程とは、「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」（令和2年1月30日サイバーセキュリティ戦略本部決定。）に基づき、制度所管省庁が運営する「政府情報システムのためのセキュリティ評価制度」について定めるとともに、本制度に関して、クラウドサービス事業者、監査機関、制度所管省庁、ISMAP運営委員会、調達府省庁等が遵守しなければならない基本的事項を定めたものである。具体的には、制度全体に係る用語の定義、制度の体系、クラウドサービス・監査機関の登録、登録されたクラウドサービス事業者又は監査機関の権利、制度を構成する者の責任範囲等に関する事項が定められている。後述するISMAPクラウドサービス登録規則や監査機関登録規則等の個別具体的な規程類については、ISMAP基本規程に基づいて定められている。本制度の全体像を把握するためには、ISMAP基本規程を参照することが重要である。

（2）ISMAPクラウドサービス登録規則

ISMAPクラウドサービス登録規則とは、ISMAP運営委員会が定めるISMAP基本規程に基づき、クラウドサービスの登録に関する事項を定めた規則である。本規則において、申請者、すなわちCSPに対して大きく分けて3種類の要求事項を課している。

①管理基準

監査機関による監査の対象となる事項である管理基準（詳細は後述。）に関して、CSP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、言明した事項について監査機関の監査を受けなければいけない旨を規定している。

②申請時の情報提供

制度の信頼性確保、調達側での制度活用といった観点で、管理基準とは別に申請時においても要求事項を定めている。具体的には以下のようなものである。（※括弧内の数字はISMAPクラウドサービス登録規則の条項）

- 申請者の資本関係及び役員等の情報 （3.4（1））
- クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクについて、制度運営委員会及び当該省庁等がリスク評価を行うために必要な情報 （3.4（2））
- 契約に定める準拠法・裁判管轄に関する情報（3.4（3））
- ペネトレーションテストや脆弱性診断等の第三者による検査の実施状況と受入に関する情報（3.4（4）） 等

③登録期間中の対応

制度の信頼性確保、調達側での制度活用といった観点で、管理基準とは別に登録期間中の対応についてCSP宣誓事項及びその他の事項として定めている。具体的には以下のようなものである。

（CSP宣誓事項の例）

- 調達交渉時に、調達機関の求めに応じ、言明書の詳細、申請するクラウドサービス従事者のうち、利用者の情報又は利用環境に影響を及ぼす可能性のある者の所属、専門性、実績、国籍に関する情報を提出すること。国籍については、個々人に紐付かない形で該当する国名を提出すること。（3.5（1））
- 登録されているサービスについて、登録期間中に利用者に重大な影響を及ぼしうる情報セキュリティインシデントが発生した場合に、遅滞なくISMAP運営委員会に報告すること。（3.5（2））
- 登録されているサービスについて、登録期間中に重大な統制の変更及び当該変更につながりうる事象が生じた場合又はリストに掲載されている情報に変更が生じた場合に、遅滞なくISMAP運営委員会に届け出ること。（3.5（3））等

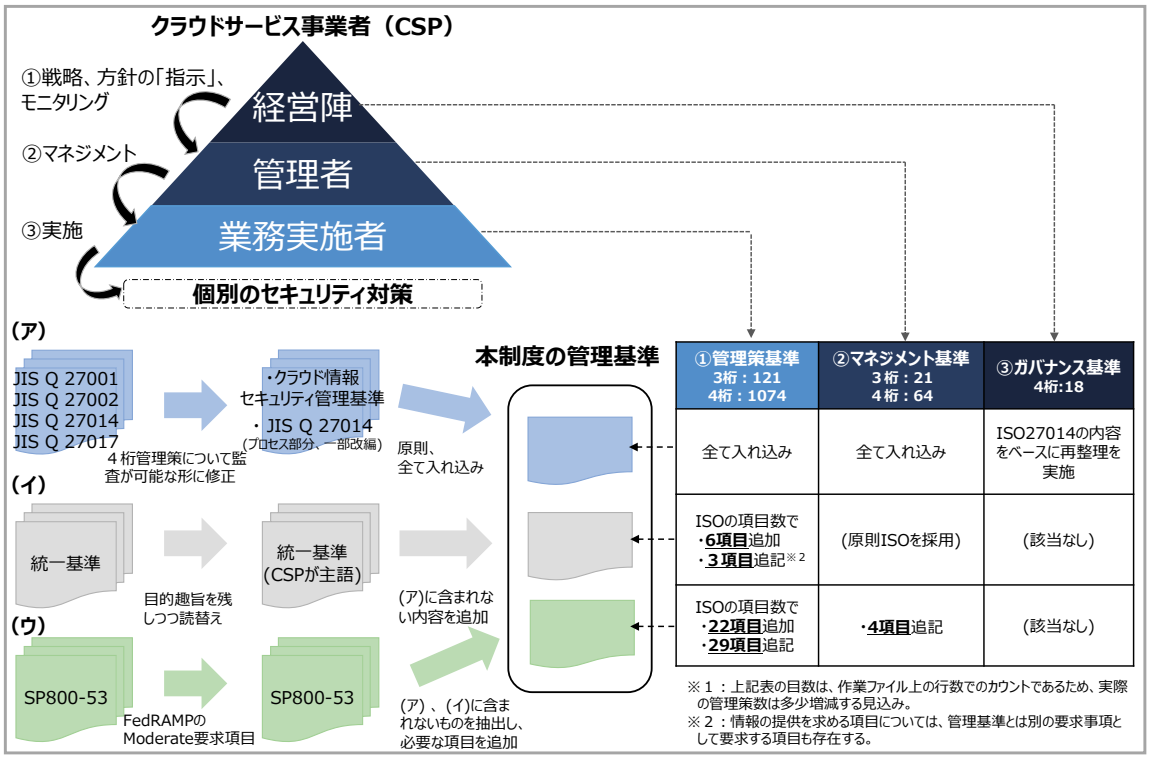
（CSP宣誓事項以外の例）

- 調達交渉時に、調達機関の求めに応じ、「IT調達に係る国の物品等又は役務調達方針及び調達手続に関する申合せ」の運用に協力すること（3.6） 等

（3）ISMAP管理基準

ISMAP管理基準とは、①CSPの「経営陣」が管理者層に対して、セキュリティに関する意思決定や

図3　ISMAP管理基準の構成



（出典）総務省作成

指示等を継続的に実施し、②これを受けたクラウドサービスの「管理者」が的確にマネジメントを実施し、③クラウドサービスの「業務実施者」が実際にセキュリティ対策を実施していることを確認するための基準である。上記①～③のそれぞれに対して基準を設け、確認するため、管理基準は①ガバナンス基準、②マネジメント基準、③管理策基準の3種類から構成される（図3）。

管理基準は、統制目標とされる3桁管理策（A.x.x.x）と、それを達成するための手段となる詳細管理策である4桁管理策（A.x.x.x.x）で構成される。原則として3桁管理策を必須、4桁管理策は選択性とし、一部の重要な管理策を必須とする。基準の内容については、情報セキュリティに関するJIS Q（ISO/IEC）27001、27002と、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を基礎とし、「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7月25日、サイバーセキュリティ戦略本部決定。）の内容を、その趣旨を残したままCSP向けに書き換え（主語をCSP、対象をクラウドサービスとする）、（ア）に含まれない内容であり、かつCSPが実施しなければ政府において統一基準を満たすことが難しい内容を追加した。さらに、NISTのSP800-53の内容から、インシデントレスポンスに関連する内容を中心に、（ア）、（イ）に含まれない観点を追加した（図3）。

（4）ISMAP監査機関登録規則

監査機関登録規則とは、ISMAP 運営委員会が定めるISMAP基本規程に基づき、監査機関の登録に関する事項を定めたものである。監査機関に対する要求事項として、技術的・能力的な観点および信頼性の観点から、組織として以下の事項を満たす体制を構築可能であることをISMAP監査機関登録規則において要求する。ISMAP運営委員会が審査を実施し、その結果、登録が認められた監査機関はISMAP監査機関リストに登録され、2年ごとに登録更新を行う。（※括弧内の数字はISMAP監査機関登録規則の条項）

- 登録対象：わが国において情報セキュリティ監査を業務として行っている法人。（3.1）
- 準拠規程等：本制度に関してISMAP運営委員会が定める規程等に準拠すること。（3.2）

- 法人登録：国税庁から法人番号の登録を受けていること。(3.3)
- 業務品質：「情報セキュリティサービス基準適合サービスリスト」に「情報セキュリティ監査サービス」として登録を受けていること。(3.4)
- 問題事案対応：倫理審査機能を有する組織への所属、問題事案発生時の調査への協力。(※3.5)
- 業務執行責任者の要件：資格要件、実務経験、国籍等を要求。(3.6)
- 業務実施責任者の要件：資格要件、研修受講、国籍等を要求。(3.7)
- 業務チームの要件：業務執行責任者、業務執行責任者を含む最低3名以上で構成する。メンバーは原則日本人だが、やむをえない場合は、業務依頼者との契約締結前にISMAP運用支援機関に問い合わせを行う。(3.8) 等

[3] ここで制度運営側とは、ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関（独立行政法人情報処理推進機構）及びその委託を受けた者を指す。

4. 今後の展望

本制度の今後の展望については、紙面の都合上、以下3点に絞って述べる。

(1) 制度のスケジュール

制度のスケジュールについては、「デジタル・ガバメント実行計画」（令和元年12月20日 閣議決定。）において、2020年度内に政府機関における制度の利用を開始できるように検討を進めることとされている。令和2年7月時点では、制度運営側は、監査機関の申請・登録審査を踏まえ、監査機関の登録及びISMAP監査機関リストの8月中の公開に向けて準備を進めている。今後の制度の運用においては、COVID-19の感染拡大による監査手続の見直しの可能性等も含めて、監査等の実務の状況も踏まえながら柔軟に対応しつつ、2020年度中にはISMAPクラウドサービスリストが公開され、評価結果が利用可能となるよう取組を進めていく。

(2) 本制度固有のガイドライン等の整備

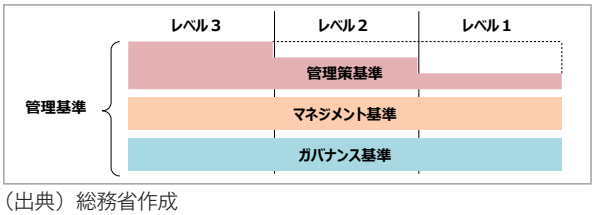
中長期的には、本制度の円滑な運用にあたり、管理基準や標準監査手続等の基準類の整備に加え、これらの基準類の解釈や具体的な実装例を示したガイドラインの整備が望ましいと考えられる。一方でこれらの解釈や実装例については、実際の運用の中で知見が蓄積されていく側面があり、ガイドラインの整備には一定の時間がかかるため、管理基準の解釈等については、管理基準の参照元となった基準におけるガイドライン等を補足文書として示しつつ、制度固有のガイドラインについては運用を行う中でその知見も踏まえながら、必要に応じて策定することとしている[4]。現在、制度運営側において、本制度の円滑な運用に向け、制度固有のガイドライン等について整備を鋭意進めている。

(3) レベル分けされた基準への対応

政府機関等が情報システムを調達するにあたっては、情報システム上で扱う情報の格付や実際に構築するサービスに求められる機能に応じて、求められる情報システム自体のセキュリティ水準が定められる。例えば、情報システム上で扱う情報が公開情報等に限られる場合と機密性が高い情報も扱う場合で、求められるセキュリティ水準も自ら異なるものとなる。このため、管理策基準の項目数・強度・内部監査の活用等に差異を設けることで、登録されるクラウドサービスのレベル分けを行うこととした（図4）。

これまでの基準の検討においては、まず、クラウドサービスの利用ニーズが高く、かつ一定以上のセキュリティ水準が求められるという観点から、レベル2の水準を念頭に管理基準の内容を検討してきた。時

図4 管理基準のレベル分けイメージ



（出典）総務省作成

間的制約もある中で、全てのレベルの基準を整備した上で全てのレベルを対象に制度を立ち上げることは困難であることから、制度立ち上げ時においては、まずレベル2の水準のみ整備する形で、制度を立ち上げることとしている。その他のレベルについても、随時検討を進め、遅滞なく制度に追加する予定である。

[4]「クラウドサービスの安全性評価に関する検討会　とりまとめ」（令和2年1月30日公表）https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00096.html
※本制度の枠組みや運用に係る制度運営側の基本的な考え方については当該とりまとめに詳しい。

5. おわりに

本制度は、国の行政機関のみならず、独立行政法人及び指定法人まで対象範囲を広げる[5]ことを視野に入れて検討を進めている。さらに、本制度の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重要産業分野等をはじめとした民間において、クラウドサービス登録簿及びその他公開される情報等が参照されることで、クラウドサービスの適切な活用が推進されることも期待される。本制度が安全・安心なクラウドサービス利用に向けて実効性・効率性をもって幅広く参照されるために、制度運営側は実務の状況等も踏まえながら、柔軟に制度の整備を進めていく。

[5] ISMAP基本規程の制度立ち上げ時の特例として、「本制度の施行から当面の間は、調達府省庁等に独立行政法人及び指定法人は含まないものとする。」としている。

参考
▼「政府情報システムのためのセキュリティ評価制度（ISMAP）」の運用開始
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00071.html
▼「政府情報システムのためのセキュリティ評価制度（ISMAP）」HP
https://www.ipa.go.jp/security/ismap/index.html
▼「政府情報システムのためのセキュリティ評価制度（ISMAP）運営委員会の基本方針」
https://www.nisc.go.jp/active/general/pdf/ismap_houshin.pdf

相川　航（あいかわ　わたる）
総務省情報流通行政局情報流通振興課　課長補佐
（前　サイバーセキュリティ統括官室　参事官補佐）
平成20年総務省入省。情報通信国際戦略局情報通信政策課、大臣官房秘書課、総合通信基盤局電気通信事業部事業政策課、米国留学（ペンシルベニア大学、コロンビア大学にて修士号を取得）、国土交通省総合政策局国際物流課、総務省サイバーセキュリティ統括官室等を経て令和2年7月より現職。

中村　公洋（なかむら　きみひろ）
総務省サイバーセキュリティ統括官室　事務官
平成31年東京大学大学院工学系研究科修士課程修了。修士（工学）。平成31年総務省入省。平成31年4月より現職。