クラウドサービスの安全性評価に関する検討会
中間とりまとめ

令和元年 7 月

クラウドサービスの安全性評価に関する検討会

目次

1. クラウドサービスの安全性評価に関する検討について

1. 1. クラウドサービスの利用に係る動向

データは「21世紀の石油」とも言われるように、その利活用と適切な管理の両立が国のあり方とその発展に大きな影響を与えることとなる。世界で生成され流通するデータの総量は毎年加速度的に増加しており、それにあわせるように、情報通信技術の発展も著しいものがある。こうしたインターネット技術や各種センサー・テクノロジーの進化等を背景に、パソコンやスマートフォンなど従来のインターネット接続端末に加え、家電や自動車、ビルや工場など、世界中の様々なモノがインターネットへつながるIoTデバイスが急速に普及している。

こうした中で、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[1]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・情報システムの舞台がクラウド上に移りつつあると言える。

政府においては、「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」（2018年６月７日CIO連絡会議決定）を定め、情報システム調達に際しては、コスト削減や柔軟なリソースの増減等の観点から、クラウドサービスの利用を第一候補として検討を行うこととしており、今後、そのさらなる利用拡大が見込まれている。

1. 2. クラウドサービスの安全性評価に関する検討の必要性

上述のとおり官民における更なるクラウドサービスの利用拡大が見込まれているところではあるが、足元の状況では、適切なセキュリティ管理への懸念等から、クラウドサービスの導入が円滑に進んでいない現状も散見される。

諸外国に目を転ずれば、2010年代に政府が情報システム調達においてクラウドファーストを掲げ、その後間もなく、政府が主導してクラウドサービスの安全性を評価する制度を構築・運用している事例がある。2018年にクラウド・バイ・デフォルト原則を採用した我が国においても、安全性評価の制度の検討が必要な段階に到達していると言える。

我が国においても、未来投資戦略2018（2018年６月15日閣議決定）では、「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。」とされている。また、サイバーセキュリティ戦略（2018年７月27日閣議決定）においても、「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し、対策を進める。」とされている。

このため、総務省及び経済産業省において、2018年８月より「クラウドサービスの安全性評価に関する検討会」（以下、「検討会」という。）を開催し、クラウドサービスに係る既存の各種ガイドライン、国内外の認証

[1] 「クラウドサービス」とは、「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）」（平成30年7月25日サイバーセキュリティ戦略本部）の定義を適用し、「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」を指す。

制度、監査制度等を整理した上で、適切なセキュリティを満たすクラウドサービスを導入するために必要な評価方法等について検討してきたところである。

今後、政府は検討会での議論を踏まえ、「政府機関等の情報セキュリティ対策のための統一基準群」や「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」に必要な反映を行う。

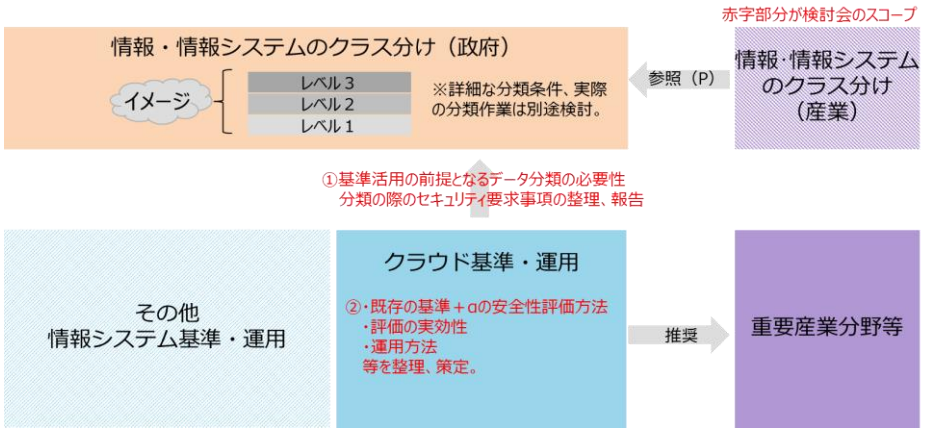
1. 3. 検討会のスコープ

制度設計に当たっては、検討会において大きく二つの観点から議論を行った。

一つは、情報[2]・情報システム[3]のクラス分けに関する議論、もう一つはクラウドサービスの安全性評価の制度そのものの議論である（参考図1）。これらの観点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整理を行うこととした。

なお、検討会において設計されることとなるクラウドサービスの安全性評価制度（以下、「本制度」という。）は政府調達における利用を第一に想定しているものの、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重要産業分野等において本制度の評価結果の活用を推奨[4]していくことを前提に、検討を進めている。

（参考図1）検討会のスコープ



---

[2] ここでいう「情報」とは、「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）」の定義を適用し、以下の情報を指す。

(ア) 職員等が職務上使用することを目的として機関等が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

(イ) その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、職員等が職務上取り扱う情報

(ウ) （ア）及び（イ）のほか、機関等が調達し、又は開発した情報システムの設計又は運用管理に関する情報

[3] ここでいう「情報システム」とは、「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）」の定義を適用し、ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、機関等が調達又は開発するもの（管理を外部委託しているシステムを含む。）を指す。

[4] 政府と民間企業では、セキュリティ対策により守るべき観点・対応すべきリスクが異なることから、クラウドサービスの調達において必要な安全性の評価も異なることは言うまでもない。民間企業において本制度の評価結果を活用する場合には、各自のリスク評価を踏まえて各々で判断を行う必要がある。

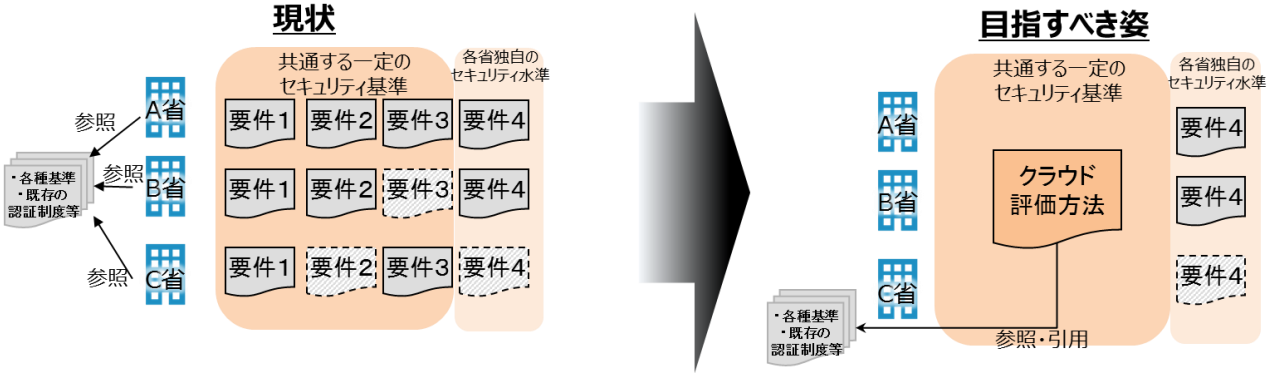
1. 4. 現状と目指すべき姿

前述の、検討会のスコープとして掲げた二つの観点について、議論の前提として認識している現状と、目指すべき姿は以下のとおりである。

現状において政府機関等の情報・情報システムのクラス分けをみると、「情報」については機密性、完全性及び可用性に基づく格付が行われているが、政府機関等の間でもその基準の運用や適用方法には差異が見られ、その結果として、クラウドサービス利用の利点の一つである政府機関内での情報連携やオープンデータ化が進まない一因となっていることが想定される。また、「情報システム」という単位での体系的な格付の考え方は示されておらず、求められるセキュリティ対策が調達側・クラウドサービスプロバイダ（以下、「CSP」という。）側双方にとって不明確であり、政府内で統一されていない。こうした状況から「情報システム」について、実効的な政府機関統一的な格付の考え方を整理し、それに応じた統一的なセキュリティ要件を示すことで、必要なセキュリティ対策の明確化につなげるとともに、クラウドサービスの利点を最大限活用できる環境が整うことが目指すべき姿である。

クラウドサービスの安全性評価については、現状、調達側では各政府機関等が様々な基準を参照しながらセキュリティ要件を設定しており、各政府機関等で共通の要件であっても各々で確認を行うこととなっているため、非効率である。CSP側から見ると、同じ要件であっても各政府機関等で別個に審査を受ける必要があり非効率であることに加え、CSP側が満たすべきセキュリティ要件のベースラインが不明確になる傾向がある。目指すべき姿としては、各政府機関が共通のクラウドサービスに係る要件について平準化・明確化し、一度その要件を満たしていることが示された場合に、結果の相互利用を可能とすることで、安全性評価の効率化を行うことである（参考図2）。

（参考図2）セキュリティ基準の平準化と明確化



それぞれの詳細については、「2.政府における情報・情報システムのクラス分けについて」、及び「3.クラウドサービスの安全性評価の制度について」で触れていく。なお、目指すべき姿については、クラウドサービスの利用に関わらず、政府の情報システム調達全体にも関わる部分が存在することに留意が必要である。また、クラウドサービスの活用により削減されるコストについては、セキュリティ確保やデータの連携・利活用に有効活用されることが望ましい。

1. 5. クラウドサービスの利用に係るセキュリティ確保の責任

クラウドサービス利用の有無に関わらず、情報システムの調達に当たっては、情報システムのユーザー

である政府機関等が、その調達する情報システム全体のセキュリティ確保に責任を負っている。その上で、クラウドサービスを利用する場合、クラウドサービスの提供者であるCSPとそのセキュリティ確保の責任を分担することになる。このため、安全性評価の仕組みにおいては、政府として許容できないリスクレベルに基づく要求事項を提示し、CSPに対してその要求事項を満たす対策の実施を求めることで、ユーザーたる政府機関等がCSPと責任を分担した部分についても、情報システム全体でのセキュリティ確保に対するユーザーとしての責任を果たすことが可能となるようにすることが原則的な考え方となる。

また、一般的にクラウドサービス自体に一定のセキュリティ確保が求められることは言うまでもなく、CSPが自身のクラウドサービスについて自らリスク分析を行い、対応策を実施するということが、政府の要求の有無とは関係なく求められている。したがって、政府として提示する要求事項は、CSPの提供する個別のクラウドサービスのリスク分析を行う性質のものではないという点に留意し、CSPが自らリスク分析を行い適切に対応することが、クラウドサービスの利用の前提となっている。

なお、こうした考え方に基づき安全性評価の仕組みを構築した場合であっても、その安全性評価の対象は個別のクラウドサービスにとどまるものであり、ユーザーたる政府機関等は、引き続き情報システム全体のセキュリティ確保に責任を負うことになる。また、CSPと責任を分担した部分についても、政府機関等はカスタマーとしての責任範囲について、必要な対策を講ずる責任を負っている。

2. 政府における情報・情報システムのクラス分け[5]について

2. 1. 政府における情報・情報システムのクラス分けの現状

情報セキュリティの基本は、機関等で取り扱う情報の重要度に応じた「機密性」・「完全性」・「可用性」を確保することであり、それぞれの機関等が自らの責任において情報セキュリティ対策を講じていくことが原則である。「政府機関等の情報セキュリティ対策のための統一基準」（以下、「統一基準」という。）においては、こうした前提のもと、情報の取扱い方のメルクマールとして、格付の区分を定義している。具体的には、「機密性」については3段階、「完全性」・「可用性」については2段階の区分を定義している。

現在、政府機関職員等は、こうした定義に基づき、情報を作成又は入手した段階で当該情報の取扱いについて認識をあわせるための措置として、情報の格付及び取扱制限の明示等を行うとともに、それに応じた対策を講ずることが求められている。一方で、「情報システム」という単位でのこうした考え方は示されていない。

2. 2. 情報システムのクラス分けの必要性

前述のとおり、現在、政府機関等の持つ「情報」に関しては、統一基準において格付の定義がなされているものの、それら「情報」が保存され、あるいは処理される「情報システム」という単位でのシステムの重要度に応じたセキュリティ水準の定義や考え方は示されていない。すなわち、セキュリティの観点から「情報システム」の取扱いについて認識をあわせるための措置は、体系的に整理がなされていない。

他方、本制度（制度の具体的な内容は後述）においては、その評価の結果、当該サービスが満たすセキュリティ水準が3段階にレベル分けされ、登録が行われることが想定されている。

こうした状況において、政府側で「情報システム」が確保すべきセキュリティ水準の考え方が体系的に整理されていないことにより、登録されたサービスのうち、どのセキュリティ水準のサービスを採用することが適切かを判断することが困難となり、本制度を最大限に活用できなくなることが予想される。

以上を踏まえ、政府機関等で取り扱う「情報システム」の重要度に応じて適切なセキュリティを確保するという観点から、「情報」の格付も参考としながら、「情報システム」についても「機密性」・「完全性」・「可用性」それぞれに関して格付と同様の概念を整理し、これらに基づいて必要な総合的なセキュリティ水準を定義する「クラス分け」の考え方を整理することが望ましいと考えられる。

なお、「情報システム」のクラス分けの方法論については、政府が自身の「情報システム」を整理し、具体例も想定しながら、それぞれのシステムの重要性を認識した上で検討を行うべきものである。本制度を活用する上で望ましい情報システムのクラス分けの考え方を以下のとおり示す。この考え方を踏まえて、政府において詳細の検討が行われることが求められる。

2. 3. 今後の望ましい情報システムのクラス分けの考え方

情報システムのクラス分けを行う際、そのシステムがどのような業務に用いられるのかを考えることが重要である。これは、同様の情報を取り扱うシステムであっても、その業務内容によって重要度が異なる場合が想定されるためである。例えば、国民へのサービス提供に直接使用されるシステムとサービス提供を管

[5] ここでいう「クラス分け」とは、「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）」における「格付」の考え方を準用し、情報・情報システムに対して重要度を格付けすることを意味する。

理・支援するシステム、緊急時対応に用いられるシステムとそうでないシステム等、業務単位でクラス分けを行うことで、実態に即した運用につながると考えられる。

こうした前提のもと、情報システムのクラス分けを行う際の整理として、「機密性」・「完全性」・「可用性」のそれぞれの観点については、以下のとおり整理することが望ましいのではないか（参考図3）。

○「機密性」について

原則、機密性については、情報システムで取り扱う情報のうち最も高い機密性の格付にあわせることが望ましいと考えられ、情報の格付と同様に3段階の格付を行う。また、情報によっては、単独では機密性が低くとも、集約することで機密性が高くなるものが存在し得ることに留意が必要である。

他方、前述の原則に基づいて、最も高い機密性に合わせて、機械的に情報システムの機密性を格付けした場合、要求水準の高止まりが引き起こされ得る。保守的になりすぎるが故に、必要以上の機密性水準を求めることは、セキュリティ対策費用の高止まりを招くのみならず、機密性と可用性の間に想定されるトレードオフの関係から、情報の活用・連携を阻害することにつながりかねない。こうした、情報システムの機密性格付の高止まりを防ぐためには、情報の機密性に応じて、構築するシステムの分離も検討するべきである。

○「完全性」について

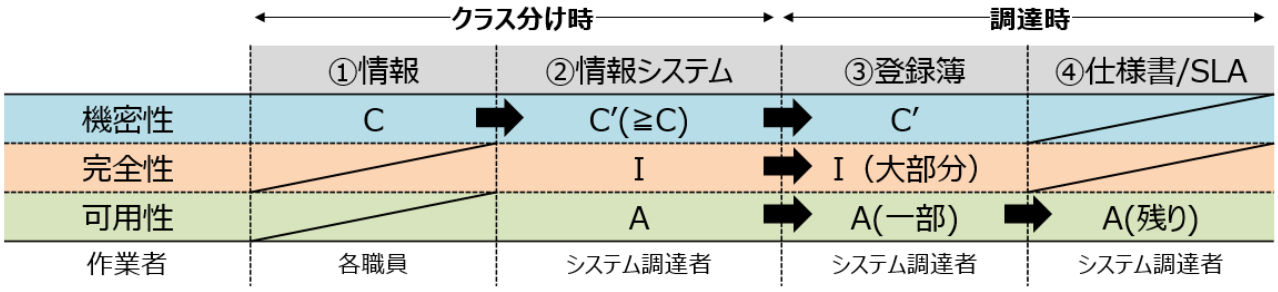
政府機関等の情報システムにおいては、全てのシステムで何らかの行政文書を取り扱うことが想定されることから、改ざん等が許容されるものは想定されず、ベースラインとして高いセキュリティ水準を求める必要がある。そのため、当面は1段階の高い完全性格付を求めることが妥当と考えられる。

その上で、公文書管理制度や、公文書管理委員会における議論も注視しながら、必要に応じて水準に段階を設けるなどの対応を適切に行っていく必要がある。例えば、将来的には、電子署名やタイムスタンプ等の活用により、改ざんの防止を図ることも追加的な手段として考慮され得る。

○「可用性」について

業務が低速化・停止した場合の政府機能・国民生活等への影響に注目して3段階で定義し、必要なバックアップの取り方・稼働率・復旧時間等に反映することが望ましい。

（参考図3）情報システムの「機密性」・「完全性」・「可用性」格付



※C、C’は機密性のレベル、Iは完全性のレベル、Aは可用性のレベルを指す。
※上記はイメージであり、機密性・完全性についてもSLA[6]で記載すべき内容が残る場合もある。

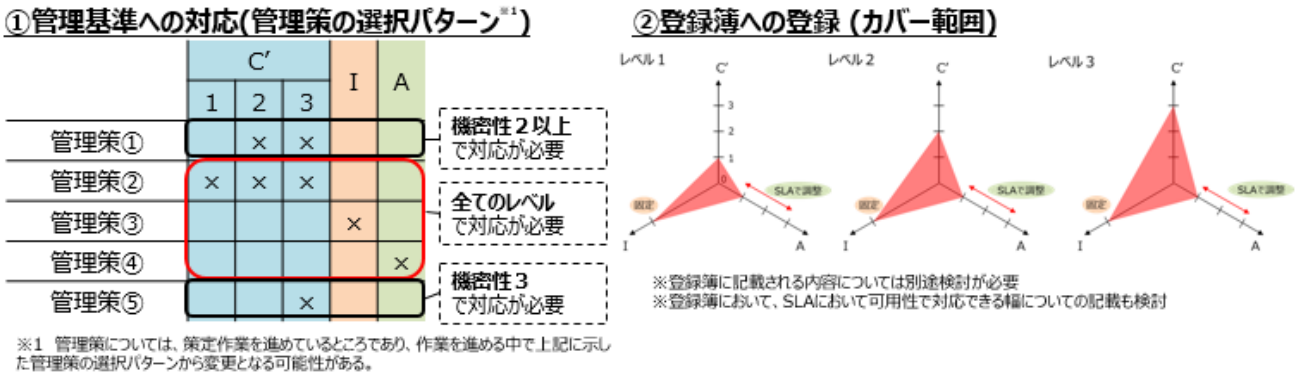
[6] SLA については必ずしも締結が必要なものではない。

以上の考え方に基づいて「機密性」・「完全性」・「可用性」のそれぞれの観点から情報システムを格付けし、それらの組合せにより、政府機関等が調達する「情報システム」に求めるセキュリティ水準をクラス分けすることで、適切なクラウドサービスの選択が可能になると考えられる。

セキュリティ水準を明確にした後、政府機関等は調達対象となるクラウドサービスが、その水準に適合していることを、然るべき段階で確認していくこととなる。この際、「機密性」・「完全性」については、検討会で議論している安全性評価の結果として登録簿に登録されているクラウドサービスのうち、適切なレベルのものを選択することで、然るべきセキュリティ水準を満たすことが可能となる設計とすることを目標としている。また、「可用性」については、登録簿からクラウドサービスを選択することで、一定の「可用性」に係る要件が達成されるものの、統一的に基準を設けることが必ずしも適当でない内容も含まれる。こうした内容については、その業務に照らして必要な「可用性」要件について、仕様書やサービスレベルアグリーメント（以下、「SLA」という。）に位置づけることによって調整する必要がある。この結果、登録簿から選定を行う際、登録簿上のレベルの数字は「機密性」格付に一致することとなる。

CSP側に視点を移すと、CSPは、登録簿への登録時と、調達時の2段階で政府の求める「機密性」・「完全性」・「可用性」の水準を満たしていくこととなる。登録簿への登録時には、政府の示す管理基準に対応することで、目標とするレベルに応じた「機密性」・「完全性」の大部分、及び「可用性」の一部の要件を満たした状態で登録簿に登録を行う（参考図4）。調達時には、仕様書・SLAへの対応を行うことにより、なお残る「可用性」の観点を中心とする要件を満たすことになる。すなわち、登録簿にクラウドサービスを登録されていることを以て、「機密性」・「完全性」に関するセキュリティ要件を満たしているという事実が全ての政府機関等で再利用されることとなり、効率性の向上に資する設計とすることが望ましい。

（参考図4）



※1 管理策については、策定作業を進めているところであり、作業を進める中で上記に示した管理策の選択パターンから変更となる可能性がある。

2. 4. 制度設計を行う上で整備することが望ましい文書・体制

各政府機関等の判断において差異が生じやすいのは、格付を行う部分とSLAを策定する部分である。格付に関しては、情報システムのクラス分けの手順やその視点について整理した文書を策定することが望ましい。その際、要求されるセキュリティ水準の必要以上の高止まりを防止するためにも、取り扱う情報の機密性水準が複数存在する場合の、その分離の検討方法や、通常時と緊急時における扱いの変化（特に、機密性と可用性の相互関係）についても検討がなされることが望ましい。また、業務に応じて情報システムのクラス分けをする際のメルクマールとして、事例集を作成することも望ましい。これにより、どのような業

務の場合に、どのようなセキュリティ水準を確保すべきであるかを判断する一助となると考えられる。SLAに関しては、情報システムの可用性の格付に応じて要求されるひな型を作成することが望ましいと考えられる。

こうした補助文書に加え、実効性を確保するためには、各政府機関等において情報システムの格付が適切に行われているか、また、SLAが適切に設定されているかを確認する仕組みの構築も重要となる。画餅とならないためにも、実効性ある運用を行えるような設計をする必要がある。

2. 5. 検討会で出されたその他意見

検討会においては、委員から上記のほかに、以下のような意見も出されているところであり、これらの点についても留意しつつ、検討を進めることが求められる。

- 情報の定義として、統一基準の定義を使用しているが、クラウドサービスの安全性評価における情報の定義として適切であるか検証が必要ではないか。すなわち、「記録された情報」となっているが、今後、政府機関等がクラウドサービス等を利用した場合に、例えばビデオ会議の内容はストリーミングで記録されない。しかし、それは情報の定義外の可能性もあるが、クラウドサービスを利用して行う業務に合わせて情報の定義を広げることも検討すべきではないか。
- 業務単位で格付を行うということであるが、業務という言葉の意味は幅が広いため、検討を進めていく中で、より粒度を明確にすべきではないか。
- 可用性の考え方について、従来のオンプレミスで求められていたものと意味合いが変わってきていることに留意が必要である。クラウドサービスでは、故障が起きた場合には古いシステムを破棄したり、バックアップはオンタイムで行っていたりするが、可用性の要件として何を求め、そのエビデンスをどのように考えるかを含めて十分検討を行うべきである。

3. クラウドサービスの安全性評価の制度について

3. 1. 制度設計の基本的視座

今回の制度の目的は、官民双方が一層安全・安心にクラウドサービスを採用し、継続的な利用を推進することにある。したがって、制度設計に当たっては、クラウドサービスの特性を踏まえ、クラウドサービスを利用することによるメリットを活かすことができるようなものにする必要がある。

かかる観点から、検討会においては、以下の基本的視座に基づいて、制度設計を行った。

- クラウドサービスはオンプレミスのシステムのように調達が終わった段階で完結するものではなく、運用そのものがサービス内容であることから、安全性評価の実効性確保の観点から、運用状況まで踏み込んだ制度とすること。
- クラウドサービスには拡張性や機能追加といった変化に価値があることや、クラウドサービス全体の技術変化のペースが非常に早いことを踏まえ、技術変化への柔軟性を確保すること。
- 各省が統一的に、一定のセキュリティ水準の確保を行えるような制度とすること。
- 制度運用の状況を踏まえ、重要産業分野等においてクラウドサービスを利用する際に、本制度の評価結果を活用することも視野に入れること。

3. 2. 制度のフレームワーク

（1）制度において必要な要件

制度のフレームワークを検討するに当たって、より具体的な要件を検討した結果、以下のような点を踏まえる必要があると考えられる。 基本的視座を前提としつつ、これらの要件を踏まえた形で、フレームワークを検討した。

- 同一主体のクラウドサービスであっても、サービスごとにセキュリティ水準は異なるため、評価の対象はCSP単位ではなく、サービス単位で行うこと。
- 情報・情報システムのクラス分けに応じたサービスの選択が可能となること。
- 既存の仕組みや認証制度等が最大限活用できるようすること。
- クラウドサービスの利用によって生じる経済性・効率性を損なわないこと。
- クラウドサービスの形態（IaaS、PaaS、SaaS）の差異を踏まえた制度とすること。
- クラウドサービスが複数の運用主体・要素で構成されることを考慮すること。
- 諸外国の制度、国際的な制度等に比して、過度に日本特異な制度とならないこと。

（2）制度のフレームワーク

制度の基本的な枠組みにおいて、具体的な安全性評価は、技術が日々進歩することを踏まえ、情報システムに専門的な知見を有する主体が実施することが重要である。既に民間において情報システムに関するセキュリティ監査が実施され、知見が集積していること、一定の評価水準を確保することが可能であること、また、運用後の継続的な確認が可能であることといった観点から、監査[7]の仕組みを活用した枠組みとする。

具体的には、政府が設定した政府クラウド情報セキュリティ管理基準（仮称。以下、「管理基準」という。）

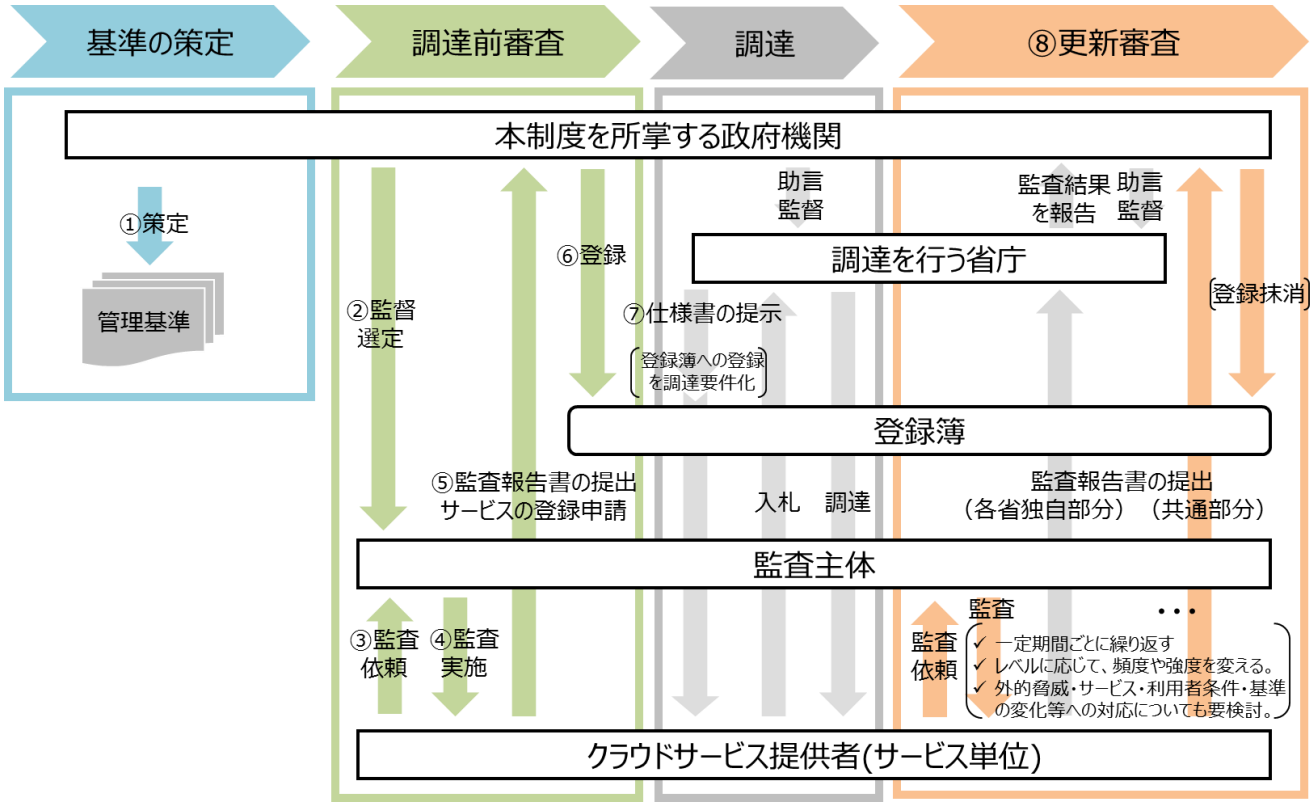
[7] 本文書における「監査」とは、情報セキュリティの監査を指し、財務書類の監査とは異なるものである。

に対して、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主体が監査する。その上で、監査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、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（参考図5）。

① 政府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主体を政府として選定。
③ CSPは選定された監査主体に対し、登録を目指すクラウドサービスの監査を依頼。
④ 依頼された監査主体は、一定の手続に従って監査を行い、監査報告書等を作成。
⑤ CSPは当該監査報告書等を添付の上、政府に対して登録を申請。
⑥ 政府は監査報告書等を確認の上、評価結果に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要件化。
⑧ CSPは登録継続のため、一定の期間ごとに監査を受け、更新手続を実施。

（参考図5）制度のフロー



また、上記フレームワークを実施するために、政府が示す基準として検討会で提示すべき基準等の一覧[8]を整理すると以下のとおりとなる。

① 管理基準： 調達に当たり政府がCSPに求めるセキュリティ基準

[8] これら基準等を利用する際の、各種フォーマット等の付属文書の作成も並行して行う。

② 監査主体の選定基準： 政府が監査主体を選定する際の基準
③ 監査基準： 監査主体が監査をする際の行為規範にあたるもの
④ 標準監査手続[9]： 具体的な監査手法及び監査手順を踏まえた標準的な監査の手続

(3)留意事項

このフレームワークの下で詳細な制度設計や制度運用を行う上では、以下の点について留意する必要がある。

- 本制度は、事実上、クラウドサービスを利用する政府機関等に代わって政府が選定した監査主体が監査を行うものであり、一定の手続に基づき認定機関や認証機関が定められる、JISやISOといった規格に対する第三者適合性評価制度(いわゆる認証制度)の枠組みとは性質が異なるものである。
- セキュリティに係る問題事案・疑義等が生じた場合には、政府機関等がその原因を確認し対応を行う仕組みのあり方を検討することが必要である。
- クラウドサービスを適切に利用することで、調達費用が低減されることが期待される。一方で、安全性確保のためには一定のコストがかかるものである。本制度の導入によって、CSPにとって例えば監査コストなどの追加的な費用[10]がかかることは事実であり、その費用は政府の調達費用に反映されるものとなるが、こうした費用は安全性確保のために必要な費用と考える必要がある。ただし、クラウドサービスの導入によるメリットを活かすためにも、システム調達全体としてクラウドサービス導入以前よりも費用が下がるよう、制度設計する必要がある。
- 監査を受けるに当たっては、監査主体に対して支払う監査費用が発生することになる。この費用については、登録を目指すCSPが負担することが必要である。
- 政府機関等はクラウドサービスを含む情報システムの利用に当たって、自らリスク分析を行う必要がある。特に、本制度において政府が統一的に定めたリスク受容水準を超えるリスク水準が必要な業務等がある政府機関等においては、リスク分析に基づき所要の追加的対策をCSPと個別に契約し、実装・運用する必要がある。この個別の契約に関する監査は当該政府機関等が実施する必要がある。

3. 3. 制度の詳細設計

上記のフレームワークを前提として、個別の要素についての詳細な考え方を、以下において整理する。

3. 3. 1. 管理基準及び監査基準

(1)基本的考え方

政府が要求する管理基準の内容は、組織に求められるガバナンス基準やマネジメント基準と、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付ける管理策基準によって構成される。

政府機関等が情報システムを調達するに当たっては、情報システム上で扱う情報の格付や実際に構築

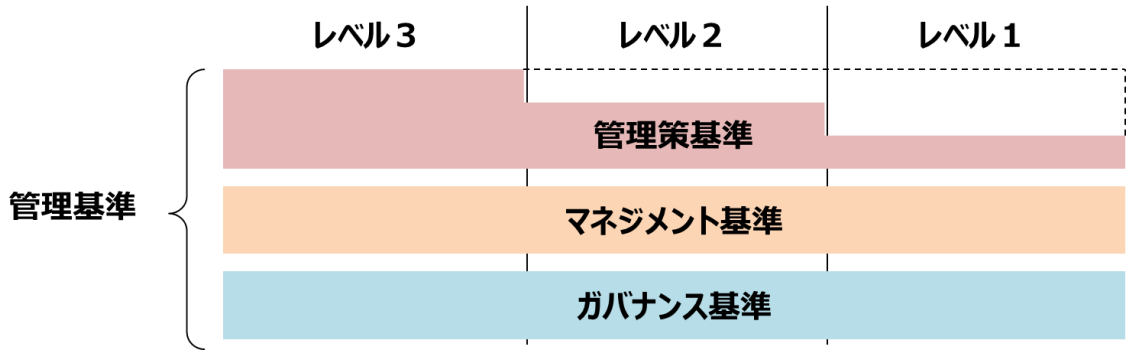
9 標準監査手続は、管理基準の内容に対応するものであるため、管理基準におけるレベルに応じて手続の内容も異なる部分がある。

10 本制度の導入の如何に関わらず、元来のセキュリティ対策において、一般的な水準に比して不足が存在していた場合、その不足分への対応は本来なされていて然るべきものであり、本制度による追加的な費用とは別の性質であることに留意が必要である。

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[11]を行うこととする（参考図6）。

（参考図6）管理基準の体系



また、監査を活用した制度とするに当たって、監査人や監査人の所属する組織が遵守すべき事項を定めた監査基準等も策定する必要がある。なお、監査基準については、原則レベル分けに依らず同一の基準となる事が想定される。

このほか、検討会での議論を踏まえ、管理基準や監査基準等の策定に当たっては、以下の点を踏まえながら、具体的な作業を進めることとした。

- 既存の国際規格等に基づく認証制度等を最大限活用できるよう、国内外の制度との比較・分析を行い、既存制度との対応関係が分かるものとすること。
- クラウドサービスに係る様々な指針等が既に策定されている一方、実効性が不十分であると言える状況にあることから、クラウドサービスの調達を行う際には、本制度で策定する基準のみを参照すれば必要十分なものとすること。
- サイバー空間上の基準に留まらず、クラウドサービスを運用するデータセンター等の物理的な基準も位置付けること。
- クラウドサービスの形態（IaaS、PaaS、SaaS）によってCSPの責任範囲が異なる[12]ことを念頭に、まずはIaaS、PaaSに該当する基準を先行して検討すること。
- 実際の作業については、検討会の下にワーキンググループを設置し、検討を進めること。
- 管理基準のうち、ガバナンス基準およびマネジメント基準についても、今後、詳細の検討を行うこと。
- 本文1.5に記載したとおり、CSPは自身のサービスのセキュリティに責任を負っており、本制度に限らず一般論として、自ら個別管理策の有効性を確認することが求められていることから、例えばSOC2

[11] 上位レベルに登録されているサービスは、下位レベルのセキュリティ水準も満たすものと見なされることとなる。他方、利用者側として不必要に高いレベルのクラウドサービスを利用することで、それに伴いコストが不必要に高いものとならないよう費用対効果に留意する必要がある。

[12] 一般に、CSPがサービス提供において負う責任範囲の大きさはSaaS＞PaaS＞IaaSとなる。

のような外部監査人による評価や、組織内において独立した立場で評価を行う内部監査[13]を活用している。これを踏まえ、本制度ではガバナンス基準もしくはマネジメント基準において、CSPに対し自らの個別管理策の有効性をモニタリングおよび評価するプロセスの構築・実施を求めること。

- 内部監査の実施にあたり、内部監査人や内部監査結果の品質を確保するため、監査基準や標準監査手続において独立性要件や内部監査手続を位置付けること。

(2)現在の検討状況

① 管理基準について

現在、検討会の下に設置したワーキンググループにおいて、管理基準の策定作業を進めている。具体的には、以下の手順に従って実施している。

I. 管理基準の参考とする国内外の基準等は次の八つとする。
   - JIS Q 27001 (ISO/IEC 27001)
   - JIS Q 27002 (ISO/IEC 27002)
   - 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)

II. JIS Q 27001 (ISO/IEC 27001)、JIS Q 27017 (ISO/IEC 27017)を軸として、これらの管理策にその他の基準等がどのように紐付くのか、マッピングを行う。

III. マッピングを基に、必要な項目を選定する。

IV. 統一基準でなされている整理に合わせて、必要な項目を再構成する。

また、参考としているものの多くは、情報セキュリティ全般に対する基準等であることから、具体的な記述内容が必ずしもクラウドサービス向けとなっていない。このため、実際の管理基準の記述においては、CSPとクラウドサービスカスタマを対策の実施主体とした記載にすることで、管理策の具体的な解釈が容易になるように検討を進める。

加えて、データセンターの物理的な基準等、上記基準には含まれていない要素についても、引き続き検討していく。

[13] 内部監査のメリットとしては、様々な認証制度や評価制度に一元的に対応できるようなプロセスを自身で組むことが可能であることや、外部監査人による評価に比べてコストメリットを得られる場合が多いこと、また、組織の内部の者であるため、クラウドサービスの内容や管理策等の詳細について精通していることが挙げられる。

② 監査基準について

並行して、監査基準についても、基本的には管理基準と同様のプロセスによって策定作業を進めている。監査基準の策定にあたり参考としている国内外の基準等は以下のとおりである。

なお、検討会において、監査の枠組みについては、予め定められた標準監査手続に則って、対象サービスがセキュリティ管理基準を満たしているか否かの評価を行うもの（詳細は本文3.3.3を参照）とされたことを踏まえ、日本公認会計士協会専門業務実務指針4400「合意された手続業務に関する実務指針」を参考とし、策定作業を進めていく。

- JIS Q 17020（ISO/IEC 17020）
- JIS Q 17021-1（ISO/IEC 17021-1）
- JIS Q 17065（ISO/IEC 17065）
- JIS Q 27006（ISO/IEC 27006）
- 企業会計審議会　監査基準の改訂に関する意見書
- 日本公認会計士協会　保証業務実務指針3000「監査及びレビュー業務以外の保証業務に関する実務指針」
- 日本公認会計士協会　専門業務実務指針4400「合意された手続業務に関する実務指針」
- 経済産業省　情報セキュリティ監査基準（Ver1.0）

（3）留意事項

管理基準については、現在詳細な内容を検討中であるが、最終的な策定に向けて、以下の点に留意しつつ引き続き検討を進める。また、監査基準については、監査報告書の品質管理の基準も含むこととし、引き続き検討を行うこととする。

- 個別の項目が過度に具体的・詳細に及ぶ場合、管理策の具体的な実施におけるCSPの選択の幅が狭まりコスト増要因となるほか、技術変化に応じた基準の変更が頻繁に発生するといったデメリットがある。一方で、抽象的すぎる場合、実効性が欠如する可能性がある。このため、自由度を持たせるべき項目と詳細に設定すべき項目の設定や、遵守事項と推奨事項の区別といった観点も含め、適切なバランスを考えること。
- 策定の過程で、政府システムへの納入実績等の観点から代表的なCSPに直接意見照会を行うなど、基準の実効性や実行可能性について十分に配慮すること。

3. 3. 2. 監査主体の選定

（1）基本的視座

フレームワークにおいて提示したとおり、クラウドサービスの評価を行うのは民間の監査主体である。一方で、今回の安全性評価の制度は、政府機関等が利用するクラウドサービスの安全性を確保することが大きな目的の一つである。このため、事実上政府に代わって監査を行う主体に対しては、政府として主体的に関与する必要がある。したがって、政府が本制度における監査を行うことができる監査主体を、予め定めた基準に基づき選定することとし、選定された監査主体による監査を受けていない場合には、当該サービスについての登録は認めないものとする。なお、ここでいう選定とは、個別の監査案件に対して監査する主体を指定するものではなく、監査主体が基準を満たしているか否かを確認するものであり、CSPが自身のサ

ービスの監査を受ける際に、確認を受けた監査主体の中から依頼先を選択できるようにするものである。

監査主体の選定においては、当該監査主体について以下の二つの基本的視座を踏まえ、具体的な選定の枠組みを構築する必要がある。

- 評価を行う技術的/専門的能力を有しているか
- 主体自体が信用に値するか

（2）監査主体の選定の全体像

監査主体の選定のプロセスを概観すると、通常の選定プロセスと問題事案発生時の対応の二つの流れが想定される。その上でプロセスにおける論点として、以下の点が挙げられる。

① 監査主体の選定基準の具体的要件

選定基準の具体的な要求事項については、実際に監査を行う監査人に対して求められる要件と、監査人が所属する組織に対して求められる要件が存在する。これらの対象について、基本的視座で示した技術的/専門的知見と主体の信頼性の２点を確保することが必要となる。これらを踏まえると、具体的な要求事項の例としては、以下のような内容が考えられる。

＜監査人[14]に対する要求事項の例＞

・資格要件：情報セキュリティや監査制度への知見を担保する観点から、例えばCISSPやCISAといった国際資格や、情報処理安全確保支援士や公認情報セキュリティ主任監査人といった資格を要求。
・実務経験：監査実務の円滑な実施や品質の確保の観点から、前述の資格が必要とされる業務における、一定期間の実務経験を要求。
・国籍要件：事実上政府に代わって評価をする観点から、監査人の日本国籍を要求。

＜法人に対する要求事項の例＞

・組織体制：監査報告書の品質を確保するための基準を遵守することが可能な体制を要求。
・法人登録：国内に法人登録があることを要求。

② 問題事案発生時の対応

監査主体が適切な体制構築や定められた監査手続の実施を怠るなどの事態が生じた場合、最終的には選定の撤回など何らかのペナルティが課される必要がある。他方で、こうした不利益を監査主体に課す場合には、ペナルティの受容性を高める観点からも、十分な事実検証が必要であることから、問題事案を検証し対応を審議する体制を構築する必要がある。

③ 監査主体の選定の有効期間（更新期間）と有効期間中における監視・報告のあり方

監査主体の選定に当たっては、確認を行う政府と確認される監査主体の双方に相応のコストがかかることとなる。このため、選定の有効期間は複数年とする。他方で、複数年にわたり監査主体の状況が確認されないことは、監査主体の水準の維持の観点から適切とは言えないことから、有効期間中において、

[14] ここでの「監査人」とは、署名する権限を持つ者を指す。

監査主体に基準に則した状況を報告させるなど、一定の監視機能を有する必要がある。

④ 監査主体の選定プロセス全体の運用体制

一連の監査主体の選定プロセスについて、全ての体制を政府機関内に築くことは困難であることが考えられる。このため、選定プロセスの実務について、外部機関に委託する等の対応を認める必要がある。

以上のような論点への対応を踏まえ、今後政府において、選定基準や選定プロセスの体制構築について検討を進めることし、実際の制度立ち上げ前に、検討会において報告を求めることとする。

(3)留意事項

監査主体の選定については、以下の点に留意しつつ引き続き検討を進める。

- 政府は内部監査人の選定は行わないが、内部監査結果の品質を確保するために、内部監査人の独立性や技術的/専門的能力を担保するための仕組みについても検討が必要である。
- 監査人に対する国籍要件を、監査チームに対しても適用していくべきかについて検討が必要である。
- 監査主体による監査業務の第三者への委託についても選定基準において検討する必要がある。
- 制度開始時において、十分な監査主体を確保するための経過措置も検討する必要がある。

3. 3. 3. 監査の枠組みと具体的プロセス

(1)監査の役割

監査の枠組みを検討する前提として、改めて本制度における監査の役割を確認する必要がある。本制度の目的は、政府が調達するクラウドサービスの安全性を確保することにあり、①クラウドサービスを利用する政府、②クラウドサービスを提供するCSP、③クラウドサービスの監査を行う監査主体という3つの主体が存在する。その中で、政府は受容できないリスクの範囲に基づいて、自身が要求するセキュリティ水準に基づく管理基準を提示する必要があり、CSPはその要求された管理基準を満たすべく、自身のサービスに応じて個別管理策を設計・運用することでセキュリティを確保する責任を負う。監査主体の役割は、CSPの個別管理策が適切に管理基準を満たしているか確認することとなる。

したがって、監査という行為そのものは、リスクに対するセキュリティ水準の高さを直接的に左右するものではない。また、事故が将来にわたって発生しないことを確認するものではなく、万が一、事故が起きた場合の対応についても別途検討する必要がある。また、監査では、あくまでも過去の一時点あるいは過去の一定期間においてCSPのサービスが管理基準を満たしていることを確認[15]するものであることに留意する必要がある。

(2)具体的な監査プロセス

監査人が監査を行う際には、予め定められた標準監査手続に則って、対象サービスが管理基準を満たしているか否かの評価を行う。監査のプロセスについては、大きく三つのフェーズに分かれる。

[15] 個別管理策の運用状況評価を継続的に監査する制度とすることで、監査対象期間以降の将来の期間において個別管理策の有効性が直ちに損なわれることを抑止する事が期待される。また、マネジメント基準やガバナンス基準の評価においては、体制の維持等の継続性についても一定の確認が行われる。

① 適正表示

適正表示では、CSPがガバナンス基準とマネジメント基準に対する実施状況を示すとともに、自身のサービスの内容に対応する管理策を選択し、言明書において明らかにする。なお、言明書の根拠は内部監査等において確認された内容に基づくものとする。監査人は、サービス範囲に照らして必要十分な管理策が言明書において表示されているかを確認することとなる。ここでは、以下の点に留意して標準監査手続をはじめとした詳細な制度設計を行うこととする。

- 選択しない管理策がある場合には、CSPは言明書において除外理由の記載を行うこと。
- 言明書において、サービス内容に照らして必要十分な管理策が表示されていることを、内部監査で確認し、その結果を本制度の監査において利用することを可能とすること。
- 適正表示の段階で、情報セキュリティガバナンス[16]等の観点から、CSPによる自らのガバナンス活動の有効性評価も含むガバナンス基準に関する評価を行うこと。

② 個別管理策[17]の整備

個別管理策の整備では、CSPは、自身が必要と判断し選択した管理策を達成するための個別管理策を策定し、監査人は、当該個別管理策が適切に設計されているかを確認する。ここでは、以下の点に留意して、標準監査手続をはじめとした詳細な制度設計を行うこととする。

- 管理策そのものに実装すべき技術まで詳細に位置付けるのではなく、実装された技術が管理策の水準を満たしているかの判断は監査人が行うこととすること。
- その上で、何らの技術的メルクマールもないままに監査人が判断を行うことは困難であるため、基準とは別に実装され得る技術の例を示すこと。
- 技術例に含まれていない技術を利用する場合には、CSPが監査人に対して、例示と同程度のセキュリティ水準を実現していることを説明し、監査人が妥当であるか否かを判断する。その上で、監査人は判断根拠を記録として残し、必要に応じて政府が事後的に確認できるようにする。
- ただし、監査人による判断が難しい場合に、専門家による助言を仰ぐ仕組みを検討することも必要である。

③ 個別管理策の運用

個別管理策の運用では、CSPが自身の個別管理策を実際に運用し、その証跡を監査人に提示する。監査人は、監査の対象期間を通じて、個別管理策が適切に運用されたかを証跡に基づいて確認する。ここでは、以下の点に留意して標準監査手続をはじめとした詳細な制度設計を行うこととする。

- 証跡については基本的にサンプルチェックで状況を確認すべきところであるが、サンプルの標本

[16] 情報セキュリティガバナンスについては、「情報セキュリティガバナンス導入ガイダンス（平成21年6月）」（経済産業省）等における定義を参考に検討を行う。なお、情報セキュリティガバナンス導入ガイダンスを受けて、ISO/IEC 27014において標準化が行われている。

[17] 「個別管理策」とは、CSP自身が個別に管理策基準を満たすために整備する管理策を指しており、個々の特定の管理策を指しているわけではない。

数などを予め定めたサンプルテーブル[18]も必要となること。

- サンプルチェックの有効性をどのように判断するかも予め明確にしておくこと。

（3）証跡等の活用方法

監査において、個別管理策等の有効性を評価するために監査人が入手・評価する資料が証跡である。監査人は、標準監査手続に定められた証跡収集の手法（質問・閲覧・観察・再実施等）に則り証跡を入手し、評価を行うこととなるが、監査対象から直接証跡を入手することが原則となる。ただし、監査の目的に照らして十分かつ適切な証跡を入手できると判断できる場合には、既存の認証制度・監査制度[19]や内部監査において収集された資料等を利用することが監査の効率化や精緻化の観点から有効であることから、これを認めることが妥当である。これらの利用のあり方については、監査基準等において一定のルールが設けられるべきである[20]。

なお、登録簿におけるレベル1に該当するようなクラウドサービスの監査においては、本制度の監査人による内部監査結果の有効性評価[21]にとどめることも検討すべきである[22]。

また、監査手続については、一定の監査品質を確保する観点から、あらかじめ定められた標準監査手続に即して手続を実施することとする。個別管理策の運用状況の評価等においてサンプリングによる手続を実施する場合にも、標準監査手続において示された件数、抽出方法等に基づきサンプルを抽出するものとする。

ただし、本制度の監査人が直接クラウドサービスを評価する場合の監査手続と、本制度の監査人が内部監査結果や他の監査・認証制度における手続実施結果の有効性を評価する場合の監査手続とでは実施すべき手続が異なるため、個別に標準監査手続を定めることも継続的に検討していく必要がある。

（4）登録簿への登録の判断

一連の監査プロセス終了後には、CSPが監査報告書を政府に提出し、登録簿への登録を申請することとなる。登録に際しては、政府が監査報告書の内容を確認し、登録の可否を判断する必要がある。諸外国においては、評価終了後の政府における確認のプロセスに時間がかかり、クラウドサービスの登録が進まないという事例も見受けられる。また、監査報告書の内容を事細かに政府側で確認することは、政府側での

---

18 「監査・保証実務委員会報告第82号 財務報告に係る内部統制の監査に関する実務上の取扱い（最終改正平成24年6月15日）」（日本公認会計士協会）において示されている統計的サンプル数を参考に、コストと有効性のバランスを考えながら検討を行う。

19 認証制度の例として、ISO/IEC 27017によるISMSクラウドセキュリティ認証や、米国FedRAMPなどがあり、監査制度としてJASA-クラウドセキュリティ推進協議会CSマーク、AICPA SOC2（日本公認会計士協会 IT委員会実務指針第７号）AICPA SOC3（SysTrust/WebTrsut）（日本公認会計士協会 IT委員会実務指針第２号）がある。

20 ここでの評価は、システム監査におけるチェックリスト法（チェックリスト法については「システム監査基準」（平成30年４月20日経済産業省）の定義を参照）のように、監査人があらかじめ作成したチェックリスト形式の質問書に対して被監査主体が回答する方法とは異なり、適切な証跡収集の手法に則って関連する資料等を入手し、管理策への適合状況を評価するものであることに留意する必要がある。

21 サービスを直接評価するのではなく、内部監査が適切に実施されていることを、外部監査人が標準手続に則って確認すること。当該評価を制度として取り入れている事例として、JCISPAが運営しているCSゴールドマークがある。

22 この手法の適切な活用が、規模の小さいCSPの制度対応負担の軽減にもつながり得る。

確認に多くの体制を割く必要が生じるとともに、一定のコストをかけて行った監査に対して二重のコストをかけることにもつながりかねない。一方で、監査報告書の内容の確認が不十分となることは、登録プロセスの信頼性を毀損し、制度全体の信頼性を損なうことにもなる。

このため、政府が登録の可否を判断するに当たっては、監査報告書の記載内容を明確化するとともに、政府の登録の判断基準を一定程度定型化する必要がある。制度の趣旨を踏まえれば、政府が登録を認めるクラウドサービスについては、少なくとも政府として許容できないリスクへの対応が、CSPにより全て実施されている必要がある。ここで、政府が管理基準において要求している内容は、当該リスク低減を実現するための統制目標[23]として定められるものである。したがって、CSPの実施している管理策が、その統制目標に照らして有効であるかが重要となる。かかる観点から、報告書の記載内容と政府の判断については、以下のような考え方に基づいて詳細な手続を位置付けるものとする。

- 政府は監査結果の外形的な不備（例えば適切な監査主体が監査を行っていない 等）がないかを確認する。
- 加えて、管理策の有効性については、統制目標の管理策及び遵守事項とされている一部のいわゆる4桁レベルの管理策[24]については遵守を必須とし、言明書で選択した全ての管理策の範囲でこれらが全て満たされている場合のみ登録を認めることとする[25]。
- 政府が上記の確認を行うことを念頭に、監査人は監査報告書に管理策への適合の是非とその判断理由等を記載する。
- 特に、4桁レベルの管理策で満たしていないものがある場合であって、統制目標にあたる管理策が有効であると監査人が判断する場合、政府が必要に応じて監査人に合理的な説明を求めることができるようにする。

（5）留意事項

監査の実効性や品質の確保の観点から、以下の点について留意する必要がある。

- 監査人が統制目標の遵守状況を判断する上で、リスクと管理策の対応関係を明確に示す必要があることから、この対応表の策定についても検討が必要である。
- 監査品質を維持するためにも、例えば監査調書をサンプリングして確認する仕組みを設けるなど、監査人に対する牽制機能を設けることを検討する必要がある。
- 加えて、監査人に対する定期的な研修や知見を共有する仕組みを設ける必要がある。
- なお、制度立ち上げ期は毎年監査を実施することとし、制度運用を進める中で効率化した方法も検討することとする。

3. 3. 4. 登録簿への登録情報

（1）基本的考え方

[23] 例えばクラウド情報セキュリティ管理基準において6.1.1のように3桁で表現される管理策を指す。
[24] 統制目標の管理策を実現するためにより具体的に記載された6.1.1.1のように4桁で表現される管理策を指す。
[25] 現在管理基準が策定中であることを鑑み、詳細な設計については、管理基準の内容も踏まえながら実効性に留意する形で検討することとする。

監査結果や手続に不備がなく登録が認められたクラウドサービスについては、そのサービスが満たすセキュリティ水準に応じた3段階のレベル表示とともに、登録簿に掲載されることとなる。登録簿上にどのような形で情報を記載するかという観点から、以下の論点について検討を行った。

① 登録簿に載せるクラウドサービスの粒度

登録簿に載せるクラウドサービスの単位・粒度については、制度運用側が予め定義をするという考え方もあり得るが、CSPごとに様々な要素を組み合わせた多様なサービスが提供されることに鑑み、登録されるサービスの単位・粒度は各CSPが自身で定義することとする。

ただし、監査を受けたサービス範囲と、登録されているサービス範囲が一致していなければならないことは言うまでもない。

② 登録簿で示すべき参考情報

登録されるクラウドサービスは、そのサービス内容が多岐に亘ることから、それぞれのセキュリティ確保の責任範囲も異なることとなる。このため、CSPは登録されるクラウドサービスの責任範囲を明示することが必要である。これは、監査プロセスにおける言明書において、CSPが対応する管理策の範囲を明確することとも整合的である。

これに加え、CSPは調達する側への情報提供として、提供形態（IaaS、PaaS、SaaSのいずれか若しくはその組合せ）及び実装可能形態（パブリッククラウド、プライベートクラウド、コミュニティクラウド、ハイブリッドクラウド等）についても、自身の判断に基づき示すこととする。

③ 2種類以上の形態でサービスを登録するケースの考え方

クラウドサービスによっては、例えばPaaSとして提供されるサービスであって、一部機能を除くことでIaaSとしても利用できるサービスなども想定される。このようなケースについて、それぞれを異なるサービスと見なして別々に監査・登録プロセスを求めることは、いたずらにCSPの負担を増加することとなる。このため、このようなケースについては、提供形態を「PaaS及びIaaS」として一つのサービスとして登録することを認めることが適当[26]である。

ただし、PaaSとして利用する場合とIaaSとして利用する場合では、セキュリティ確保の責任範囲が異なることから、それぞれの提供形態ごとに責任範囲が示される必要がある。

④ 複数のサービスで構築されるサービスの登録の考え方

クラウドサービスによっては、他社のクラウドサービス基盤の上にサービスを構築するケースが想定される。このような場合、登録を目指すクラウドサービスは、他社基盤部分も含めたクラウドサービス全体としての責任範囲と、自社が負うべき責任範囲の両方を示す必要がある。その上で、自社が構築する部分についての評価を受けるとともに、原則、他社のクラウドサービス基盤が本制度において登録されていることが登録の条件となる。したがって、仮に基盤となる他社のクラウドサービスが登録抹消となった場合には、自社のサービスも登録抹消となる。なお、例外的なケースであると考えられるが、基盤となる

[26] サービス範囲の拡大、アーキテクチャの更新、ガバナンス体制の変更などが含まれる場合においては、別のサービスとして改めて監査を受ける必要がある。

他社のクラウドサービスの評価まで自社で行い、それが妥当だと監査において認められる場合には、登録することは可能である。

　なお、サービスの基盤となるPaaSやIaaSが登録されていることが、多くのSaaSの登録の前提となることが予想されるため、経過措置についても検討することが必要である。

4. 今後の進め方と課題

4. 1. シミュレーションの実施

（1）基本的考え方

本制度をより実効的なものとするためには、現在策定作業を行っている各種基準を用いて試行的な運用を行うことで、対応コストや課題を抽出し、実際の運用で問題が生じるリスクを低減しておくことが重要である。他方で、実際に政府機関等がこれから調達を行うシステムを対象として試行運用を行った場合、業務に直結する調達の進捗に影響を与え、業務の遂行に支障を来す可能性がある。こうした状況を踏まえれば、実調達に影響のないシミュレーションという形で、実効性の評価を行うことが現実的である。本制度のフローに鑑み、登録簿に載せるまでの段階である「監査・構築」のシミュレーションと、登録簿に載った後に政府機関等が行う「調達」のシミュレーションという、2種類のシミュレーションを行うことが必要である。

（2）現在の検討状況

「監査・構築」のシミュレーションの目的は、CSP視点からの管理基準及び監査への対応コスト・期間の試算や、監査主体視点からの監査コスト・期間の試算、また両者共通して、各種フォーマットの改定やクラウドサービス特有のリスクの更新を行うことである。こうした目的から、実施主体はCSP及び監査主体とし、登録が想定される既存のクラウドサービスを対象とすることで、効率的に課題を抽出できるものと考えられる。

「調達」のシミュレーションの目的は、本制度が政府における調達プロセスに与える影響を調査することである。具体的には、仕様書やSLAがどのように変化し、また、それに対応する提案書がどのように変化するのかを調査すると同時に、調達期間や費用への影響と、その課題についても評価する。調達プロセスにおける変化を評価するという目的に照らして、既に仕様書が存在しているシステムを対象とすることが望ましいと考えられる。こうした観点から、実施主体は政府のシステム調達関係者と、システムインテグレーターあるいはCSPとし、対象を既存のシステムとすることが妥当と考えられる。

以上の考え方を踏まえ、実施主体と詳細を調整し、本格的な運用を行う前にシミュレーションを実施することが望ましい。

4. 2. 動的な要素への対応について

本制度の運用を行う中で、クラウドサービスに係る様々な動的要素に対して柔軟に対応していくことが望ましい。具体的な動的要素としては、クラウドサービス側の変更と制度側の変更に大別される。前者については、CSP側において運用中のサービス変更やガバナンス体制の変更が行われることで、言明書として選択した管理策等に変更が加わることなどが考えられる。後者については、既存の制度設計において想定していない技術の登場により、それに伴う新たなリスクの発生や、新たなセキュリティ対策の必要性が生じることが考えられる。あるいは、クラウドサービス自体のみならず、監査手法についても自動化等による効率化が可能となり、制度の部分的な見直しが必要となる可能性がある。

こうした動的な要素への対応を制度に組み込むことが必要であるという認識を共有しつつも、実際に本制度を運用していく中で生じる変化も予想されることから、制度立ち上げ時点において全てを取り込むのではなく、本文3.3.3（5）でも言及したとおり、当面は、毎年本制度に則ってクラウドサービスの監査を実施することで適切な対応方法を見極め、継続的に検討を続けていくこととする。

4. 3. 技術の検証・評価等について

既に言及したとおり、クラウドサービスに含まれる技術は急速に変化していくものである。こうした、クラウドサービスの利点であるダイナミズムを最大限活かし、イノベーションを阻害しないためにも、制度が技術変化に柔軟に対応していくことが重要である。

新たな技術への対応は、政府機関等に限らず、民間企業一般においても期待されることである一方で、その有効性やセキュリティについて、各政府機関等、あるいは民間事業者が個別に検証・評価を行うことは非効率である。こうした状況を踏まえれば、本制度における活用を想定しながら、今後、第三者の立場から、新たな技術について何らかの検証・評価を行う仕組みを検討することが望ましい。

また、監査手法の自動化などの検討も行うことで、安全性評価の水準を維持しながらコスト低廉化・効率化を行うことが望ましい。

4. 4. システム全体のアーキテクチャについて

検討会で議論している制度によって安全性が評価されるのは、あくまでシステム全体の中の構成要素としての、個々のクラウドサービスであることに留意することが必要である。言い換えれば、これらクラウドサービスの組合せ、及び利用者側で構築する部分を含めたシステム全体の安全性については、議論の対象となっていない点に留意が必要である。したがって、政府機関等がシステム全体の安全性を評価するためには、オンプレミス等の従来のシステムを含めたシステム全体の構築の方法、いわば、アーキテクチャ設計を行うことが重要である。こうした論点は、本文2.3で触れた、機密性の異なる情報・情報システムの分離あるいは連携をいかに行うのかという視点にも直結するものである。このように、クラウドサービスを有効に活用するためにも、システム全体の設計について考える必要が残ることを肝に銘じ、政府内において、今後、整理がなされることが望ましい。

4. 5. 政府内の体制構築・制度利用の実効性確保について

本制度を継続的に運用するためには、政府内において責任ある体制構築が不可欠である。具体的に想定される業務として、制度の恒常的運用に関しては、①監査主体の選定・モニタリング業務並びに監査人に対する研修の実施、②クラウドサービスの登録に係る監査報告書の確認・登録・更新並びに登録簿の管理業務を担う体制が必要であることに加え、③各種基準の更新・整備業務が必要となる。特に、変化の激しいクラウドサービスの性質を踏まえれば、基準の更新・整備に関して、恒常的にクラウドサービス分野の動向をフォローすることが必要である。これに加え、本文4.2や本文4.3に必要な体制についても検討が求められる。

全ての体制を政府内で構築維持することには、一定の限界があることも考えられることから、例えば実務部分について外部機関に委託することなども含め、本制度が実効的に継続運用されるよう、体制構築を行うよう、検討会として強く求める。

加えて、本制度を実効性のあるものとするために、調達する側の政府機関等の調達状況について、適切なフォローアップを行う事が重要である。

また、特にSaaSを中心として、登録簿上にクラウドサービスが充実するまでには一定程度の期間を要することも想定される。こうした期間において、登録簿に載っていないサービスを利用したい場合においても、検討会の議論と同等の安全性評価がなされる必要があるが、その経過期間の設定については、今後整理

が必要である。

4. 6. スケジュール

検討会に係る今後のスケジュールは、以下を想定している。

2019年　年内　検討会とりまとめ。
とりまとめ後　基準のパブリックコメント。
2020年　夏　クラウドサービスの監査・登録作業等。
2020年　秋　全政府機関等での制度活用開始。

5. まとめ

クラウドサービスとは常に変化し続けるものであり、運用を行うことが本質である。変化が急速に起こり続ける中で、セキュリティ対策としても、オンプレミスに代表される従来のシステムでは一定程度有効であった、定期的なチェックのみでは限界が存在することに留意すべきである。

クラウドサービスを利用する全ての政府機関等は、情報システムの調達及び利用に当たって、クラウドネイティブの考え方に従った、前例のない取り組みをしなければならないということを再確認し、変化に合わせて柔軟に対応していくことが求められる。こうした観点からは、本制度において対象となる個別のクラウドサービスの利用に留まらない、情報システム全体の構築・調達のあり方が問われることになることを認識し、対応していくことも必要である。一方、CSPにおいては、本制度への対応の過程において、内部監査の実施等を通して、より一層のセキュリティ確保体制の構築や、セキュリティ意識の向上が実施されることが期待される。

監査という枠組みを活用することによって、政府とCSPの双方が、変化に柔軟に対応しながらセキュリティを向上することで、安全・安心なクラウドサービス活用につながることを期待するとともに、本検討会の議論が、ひいては政府全体として時代に即したより良い情報システムの調達のあり方の検討を深めることにつながれば幸いである。

クラウドサービスの安全性評価に関する検討会
検討会委員名簿
（敬称略）

【座長】

大木　榮二郎	工学院大学　名誉教授

【委員】（五十音順）

江口　純一	独立行政法人情報処理推進機構　理事
江崎　浩	東京大学大学院　情報理工学研究科　教授
加藤　雅彦	長崎県立大学　情報セキュリティ学科　教授
河合　輝欣	特定非営利法人　ASP・SaaS・IoTクラウドコンソーシアム　会長
岸　　泰弘	PwCあらた有限責任監査法人　パートナー
後藤　厚宏	情報セキュリティ大学院大学　学長
中尾　康二	国立研究開発法人　情報通信研究機構　主管研究員
永宮　直史	特定非営利活動法人　日本セキュリティ監査協会　事務局長
間形　文彦	NTTセキュアプラットフォーム研究所　主幹研究員
満塩　尚史	内閣官房　IT総合戦略室　政府CIO補佐官
宮下　清	一般社団法人　日本情報システム・ユーザー協会　常務理事
山内　徹	一般財団法人　日本情報経済社会推進協会　常務理事

【オブザーバー】

内閣官房	情報通信技術（IT）総合戦略室
内閣官房	内閣サイバーセキュリティセンター
総務省	サイバーセキュリティ統括官室
総務省	行政管理局
総務省	自治行政局地域力創造グループ
経済産業省	サイバーセキュリティ課
防衛省	サイバーセキュリティ政策室
防衛装備庁	長官官房総務官

【事務局】

総務省	情報通信政策課
経済産業省	情報経済課

クラウドサービスの安全性評価に関する検討会
WG委員名簿
（敬称略）

【座長】

間形　文彦	NTTセキュアプラットフォーム研究所　主幹研究員

【委員】（五十音順）

小川　隆一	独立行政法人情報処理推進機構　セキュリティセンター分析G　ラボ室長
加藤　俊直	PwCあらた有限監査法人　パートナー
駒瀬　彰彦	株式会社アズジェント　セキュリティセンターフェロー
小山　覚	一般社団法人ICT-ISAC　事務局長・副運営委員長
菅谷　光啓	NRIセキュアテクノロジーズ株式会社　フェロー
成田　康正	一般財団法人　日本情報経済社会推進協会　セキュリティマネジメント推進室長
三笠　武則	特定非営利活動法人　ASP・SaaS・クラウドコンソーシアム　執行役員
山田　英史	株式会社ディアイティ　セキュリティ事業部担当部長

【オブザーバー】

内閣官房	情報通信技術（IT）総合戦略室
内閣官房	内閣サイバーセキュリティセンター
総務省	サイバーセキュリティ統括官室
総務省	行政管理局
総務省	自治行政局地域力創造グループ
経済産業省	サイバーセキュリティ課
防衛省	サイバーセキュリティ政策室
防衛装備庁	長官官房総務官

【事務局】

総務省	情報通信政策課
経済産業省	情報経済課