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(案)

令和元年12月

クラウドサービスの安全性評価に関する検討会

目次

本とりまとめと中間とりまとめの関係

クラウドサービスの安全性評価制度（以下、「本制度」という。）については、中間とりまとめ以降、制度の詳細設計や各種基準について検討会・WG双方で精力的に議論を重ねてきた。今回のとりまとめは、初年度に本制度を立ち上げる上で整理が必要な各種事項について、中間とりまとめ後の検討結果をまとめたものである。したがって、特に明記されていない限り、中間とりまとめの内容はそのまま踏襲していることから、本とりまとめを参照する際には、あわせて中間とりまとめも参照することが必要である。

1. 中間とりまとめ以降の制度枠組みに関する議論

1. 1. 本制度の位置づけ・使い方

本制度は、まず、制度として政府調達の候補となるクラウドサービスをセキュリティの観点から選定するため、政府機関等がクラウドサービスに対して要求するべき基本的な情報セキュリティ管理・運用の要求事項（管理基準）を定める。その上で、情報セキュリティ監査の枠組みを活用して、独立した第三者が政府の定める基準・手続に従って監査した結果に基づき、クラウドサービスが政府の要求する事項を満たしていると評価したクラウドサービスを登録する制度である。

従来は調達段階でのセキュリティ対策の確認と運用が個別に行われていたが、本制度は、クラウドサービスプロバイダ（以下、「CSP」という。）による情報セキュリティ対策の運用状況まで踏み込んで確認することによって、クラウドサービスは運用面の確認が重要であるという特性も踏まえた調達と運用一体でのセキュリティ対策の確保に資するものである。

本項では本制度におけるクラウドサービスの評価の位置付け並びに調達側の利用の在り方について、CSPが実際に自身のクラウドサービスの情報セキュリティ対策を実装・運用するまでの一連のプロセスの各段階において、本制度の評価の枠組みがどのように機能し、制度運営者・監査主体・制度利用者[1]の担う役割・責任がどのようなものであるのか、整理を行う。

＜CSPがセキュリティ対策を行うプロセス及び責任＞

本制度における登録を目指すCSPは、次のようなプロセスによって自身の行うべき情報セキュリティ対策の内容を決定し、実際に実施することとなる。

①登録を目指すクラウドサービスの範囲の確定
②当該クラウドサービスのセキュリティリスクの分析
③セキュリティリスクの分析結果に基づいた管理基準における3桁レベル[2]の統制目標の選択
④選択された統制目標を実現するための管理基準における4桁レベル[3]の詳細管理策の選択
⑤詳細管理策の選択に応じた個別管理策の設計
⑥個別管理策の実装・運用

CSPは、制度の登録を申請する以上、当然この一連のプロセスを適切に実施する責任及び実施していることを政府に説明する責任を、制度運営者との関係において有することとなる。

---

[1] 制度利用者とは、本制度における評価結果を利用する者をいう。
[2] 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。
[3] 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。

＜プロセスごとの評価の基本的考え方＞

安全性評価においては、一連の①～⑥までが妥当であることを第三者が完全に確認することが理想である。一方で、多種多様な形態があるクラウドサービスにおいて、個別サービスごとの①～④に該当する部分について、純粋に第三者が評価を行いその妥当性を完全に確認することを制度として位置づけることは非常に困難である[4]。

したがって、①～④については、CSPが適切に実施する蓋然性を高める枠組みを、純粋な監査の手続のみに依らず制度全体として確保しつつ、制度全体で要求した一連のプロセスにおいて不自然な点がない限りにおいて、CSPの判断が妥当であることを受容することとなる。

この蓋然性を高めるための枠組みとして、管理基準のうちガバナンス基準・マネジメント基準により、CSPが組織として適切なリスク分析とそれに基づく対策を実施する体制を築くことを求めるとともに、その体制の有無について監査において確認することが挙げられる。これに加えて、言明において4桁レベルの詳細管理策の中で選択しないものについて、その理由を明示させる[5]ことにより、CSPへの説明責任を求め、CSPの恣意的な判断を抑制することとする。

他方で⑤～⑥については、CSPが実際に自身のクラウドサービスにおいて行っていると言明している個別管理策自体が基準に位置づけられた4桁レベルの詳細管理策に妥当するものであるか、また実際にその個別管理策が実装・運用されているかを直接監査の手続によって確認することが可能である。このため、この部分については、制度として定めた標準的な監査手続に則って、監査主体が監査で実施状況を確認することになる。

また、CSPが自ら行う内部監査は、この一連のプロセスを適切に実施する上で必須となるプロセスであることから、制度において内部監査の詳細な基準や手続は定めないが、その実施は当然求められるものであり、監査主体向けの監査基準等を踏まえながら適切に実施されることが望ましい。[6]

その上で、本制度として登録されたクラウドサービスが、どのようなサービス範囲でありどのような対策を行っているのかについて、一連の評価プロセスの結果が、調達者/利用者[7]に対して情報提供されるものとなる。

＜制度運営者の担う制度上の役割＞

制度運営者は、CSPからの申請と添付された言明書や監査報告書を含む各文書を確認し、あらかじめ定められた基準に基づき、クラウドサービスの登録の可否を判断する。そして、クラウドサービスの登録の判断に関する最終的な全責任を負うことになる。登録の判断に関する責任とは、セキュリティリスクへの対応として、本制度において要求されている事項・プロセスが満たされていることを確認したというものであり、この確認の範囲において責任を負っているものである[8]。また、当然のことながら、本制度において要求さ

---

[4] 例えば、保証型監査であるSOC２であっても、①～④の全てを確認しているものではない。

[5] 裏返せば、①～③の分析・評価に基づく合理的な理由のもと、３桁レベルに対する４桁レベルの管理策が全て選択されないことは許容される

[6] 要求事項としての内部監査は、管理基準において位置づけられることとなる。

[7] 調達者/利用者とは、情報システムを調達する者又は当該システムを利用する者をいう。

[8] セキュリティリスクそのものが定性的な概念である以上、本制度における安全性評価の意味合いは、絶対的な安全やリスクゼロを保証するものではない点に留意が必要である。

れている事項・プロセスが適切に行われていれば、政府として利用するクラウドサービスとして十分にリスクが低減されることが確保されるよう、適切な制度設計と制度運用を行い、絶えず制度の見直しを行う責任を有する。

なお、登録されているクラウドサービスにおいてセキュリティインシデントが発生したとしても、その損害については、CSPが当該サービスに関する契約に基づく責任を負うものである。

＜監査主体の担う制度上の役割＞

監査主体は、あらかじめ定められる標準的な監査手続に基づいて、CSPが言明している管理策について監査を行い、その監査結果について監査報告書にまとめることとなる。監査主体はあくまでもCSPからの依頼に応じて、CSPとの契約の下で監査を行うことから、報告書に関する責任は一義的にはCSPとの関係において負うことになる。ただし、本制度に基づく監査の実施については、本制度において登録がなされた監査主体のみが実施することとなるため、本制度との関係では監査主体は監査基準・監査ガイドラインと標準的な監査手続に基づき誠実に監査を行う責任を有することとなる。

また、本制度における監査主体及び監査人の責任は、前述の⑤～⑥にあたる部分が中心となるが、①～④に該当する部分であっても、その不備が明らかであるにも関わらず監査人が指摘しなかった場合、監査基準に照らして不適切な点があれば、制度において監査主体及び監査人が注意義務違反に問われ、登録取消等の措置を受ける可能性がある点について留意が必要である。

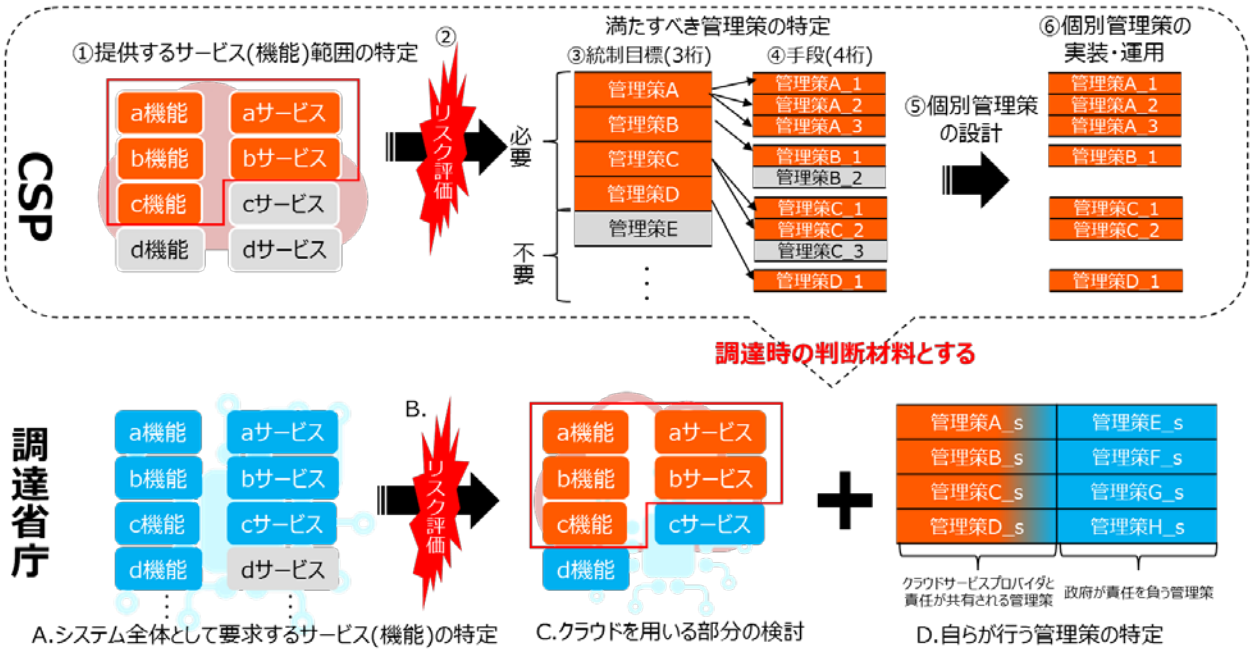
＜調達者の制度利用の考え方＞

情報システムを調達する政府機関等においては、調達にあたり通常以下のプロセスによって具体的な情報システムの内容とセキュリティ対策を決定・実施することが想定される。

A. 情報システム全体の機能の特定
B. 情報システム全体のセキュリティリスクの分析
C. 全体機能のうちクラウドサービスを利用する部分の特定
D. 利用するクラウドサービスのセキュリティ対策を踏まえた自ら行うべきシステム全体の対策の設計・実施

従来であれば、調達者はC及びDの段階で必要となるクラウドサービスの個別の情報について、自身で全てを確認する必要があったが、本制度においては、個々のサービスにおいてあらかじめ妥当性が評価された情報が提供されることになることから、調達者は個別に実施状況などの確認を省略して調達プロセスを進めることが可能となる。

（参考図1）CSP・調達省庁の役割



1．2．情報システムの調達者/利用者が留意すべき点

中間とりまとめでも指摘しているとおり、情報システムのセキュリティ確保の責任は、一義的に当該システムの調達者/利用者が負うものである。本制度において登録されたクラウドサービスを利用していたとしても、単にそのサービスを利用するだけでは情報システム全体のセキュリティが十分に確保されることにはならない。情報システムの調達者/利用者は、自身が利用するクラウドサービスについてユーザーとして適切な設定を行うことが当然に求められることに加えて、情報システム全体について、そのセキュリティリスクを分析し、適切な対策を行うことが求められる。本制度に登録されているクラウドサービスを利用するにあたっては、当該サービスが組み込まれる情報システムのセキュリティリスクを適切に把握した上で、当該サービスが提供するセキュリティ機能やセキュリティに係る提供情報を踏まえ、情報システム全体のセキュリティ対策を実施するとともに、セキュリティ確保についての最終的な責任を負わなければならない。[9]

他方で、本制度を運営する立場においても、政府機関等が適切な判断を行うことに資する情報を、適切に提供できるよう努めることが必要である。

1．3．制度運営に求められる体制

本制度は今後の政府調達において継続的に利用されることが想定されることから、安定的に制度を運営する体制が求められる。その際には、制度全体の実効性確保などの観点から、次のような機能を適切に保持することが重要である。

[9] 調達者側が適切な対応を行うためにも、調達者側において情報システムに係る専門的な人材を確保するなどの取組が、これまで以上に求められる。その一環として、専門的人材の確保にかかる待遇面での柔軟な検討も必要との意見が委員から提示されている。

①基準策定・更新[10]

②クラウドサービスの申請受付・審査・登録・モニタリング・変更管理等[11]

③監査主体の申請受付・審査・登録・モニタリング・変更管理等

これらの体制について、全てを制度所管機関が担うことが理想的ではあるが、その業務量や必要とされる知見・専門性などに鑑みれば、全てを制度所管機関で手当てすることは困難であることが想定される。このため、制度運用の実務については、制度運用によって収集される情報が政府の情報セキュリティにも密接に関わるという観点も踏まえると、高い公共性を有する適切な主体に委ねることが求められる。この点、改正情報処理の促進に関する法律が、先日の国会において成立し、独立行政法人情報処理推進機構（IPA）の業務としてクラウドサービスの安全性評価が位置づけられた。このため本制度の実務については、監査主体の管理等の実務部分を情報セキュリティ監査や監査主体の管理等に精通した民間団体からの協力を受けつつ、IPAが担うことが適切である。ただし、その場合であっても、制度の実効性確保のため、制度所管機関のもとで、クラウドサービスの登録等に係る最終的な意思決定等を行うことが必要であり、例えば、有識者と制度所管機関を構成員とした制度運営委員会を制度所管機関のもとに設置するといった体制を構築することが考えられる。

1．4．立ち上げ時の特例

中間とりまとめにおいて示された制度のフレームワークでは、制度として実現すべき最終的な全体像が位置づけられていた。一方で、政府としてクラウド・バイ・デフォルト原則が定められ1年以上が経過する中で、早急に制度の立ち上げが求められている。こうした中で、中間とりまとめで示された全ての内容を網羅した形で制度立ち上げを行うことは、時間的な制約などから困難であることは事実である。また、制度が立ち上げられて初めてCSPとして対応すべき事項が正式に明らかになることを踏まえれば、制度立ち上げ初期段階での監査において、一定期間におけるサンプリングに基づく運用評価を行うことも難しい。こうした観点から、立ち上げ時点で実施する内容等について、以下の整理とする。

（1）基準のレベル分け

中間とりまとめにおいては、政府の情報システムは情報システム上で取り扱う情報の性質等により、求められるセキュリティ水準が異なることから、管理策基準の項目数・統制の強度等に差異を設けることにより、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。

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（詳細は後述。）上述のとおり、時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する。

---

[10] 基準の更新業務については、毎年同じ作業が発生するとは限らず、参考としている国際規格等の改訂のタイミング等によって、作業量が膨大となる時期が存在する可能性に留意し、体制整備を行うことが必要である。

[11] 審査で処理すべき資料の量は膨大になることが想定されるため、効率的な審査が可能となる様式の整備や、ペーパーレスで審査を実施できるシステムの整備を行うことが必要である。

その他のレベルについては、制度立ち上げ後に遅滞なく検討を進め、検討が取りまとまり次第制度に追加することとする。

（2）監査範囲

本制度における情報セキュリティ監査は、クラウドサービスの運用状況まで確認するとの観点から、言明書の監査対象期間におけるサンプリングによる運用評価まで行うことが中間とりまとめで位置付けられた。他方で、制度が成立し、基準が明らかになったところで初めて、CSPはサンプル取得の準備を開始することができる。したがって、制度立ち上げ初期の時点ではCSPが必ずしも十分なサンプルの準備が可能とは限らない。このため、制度立ち上げ初期においては、一定期間のサンプリングによる運用評価までは求めず、CSPが言明する基準日における整備状況評価（時点評価）のみを行うこととし、例えば制度開始後一年などの一定期間が経過した後、監査対象期間に対する運用評価までを求めることとする。

なお、本制度における整備状況評価は、基準日における個別管理策の実装状況までを確認するものであり、単なる机上での個別管理策の設計の確認を超えたものであることから、整備状況評価のみを行った場合であっても、一時点の運用状況の確認に踏み込んだものとなると考えられる。

（3）関連文書の整備

本制度の円滑な運用にあたっては、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。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ることも事実である。また、ガイドラインの整備には一定の時間がかかる。

このため、制度立ち上げに際しては、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すこととし、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する。

1．5．監査の対象期間、申請期限等の考え方

本制度の評価の中核を占めるのが、監査のプロセスである。監査を行うに当たっては、監査の対象となる期間ないしは基準日の考え方を制度として整理する必要がある。また、監査の対象期間とその後の申請プロセスとの間に大きな期間が空いてしまうと、サービスが登録された時点では評価内容が陳腐化してしまうことになる。こうした観点から、監査の対象期間を軸にして、その後の監査報告書の日付や申請日の期限等を定める必要がある。

（1）言明書の監査対象期間・監査基準日

＜基本的考え方＞

言明書の監査対象期間は最大1年とする。その上で、翌年の監査対象期間は前年の監査対象期間の末日の翌日までを期首とすることとして、監査対象期間に隙間が生じないように設定するものとする。

なお、この期間はあくまでも監査の対象となる期間を示しているものであり、CSPが行う言明そのものの有効期間ではないことに留意する必要がある。CSPの言明の有効期間そのものは、CSPが言明の変

更を行わない限り継続するものである。

＜制度立ち上げ時の特例とその後の監査対象期間の整理＞

制度立ち上げ初期には、整備状況評価による時点評価のみが行われることとなる。監査対象は一定の期間ではなく、CSPが言明の基準とした一時点の基準日となる。次回以降の監査に当たっては運用評価も行うこととなるため、監査対象期間の設定が必要となる。このときの考え方は、基本的考え方と整合するよう、基準日の翌日を期首とした一年間となる。

＜CSP内での他の監査スケジュールとの調整＞

CSPの中にはすでに自身での内部監査を十分に行っている場合や、他の枠組による外部監査を受けている場合がある。この場合、CSPとしてはこれらの監査スケジュールと本制度における監査期間を整合させることで、本制度への追加的な対応コストを可能な限り効率化するというニーズがあると考えられる。

CSPが自身の監査スケジュールと本制度の監査期間の整合を図る場合には、上述の基本的な考え方と整合するよう、監査期間の期末と期首が連続するようにしつつ、監査期間自体を短縮することにより、次の監査期間において自身の監査スケジュールと整合を図ることとなる。

（2）監査報告書の日付

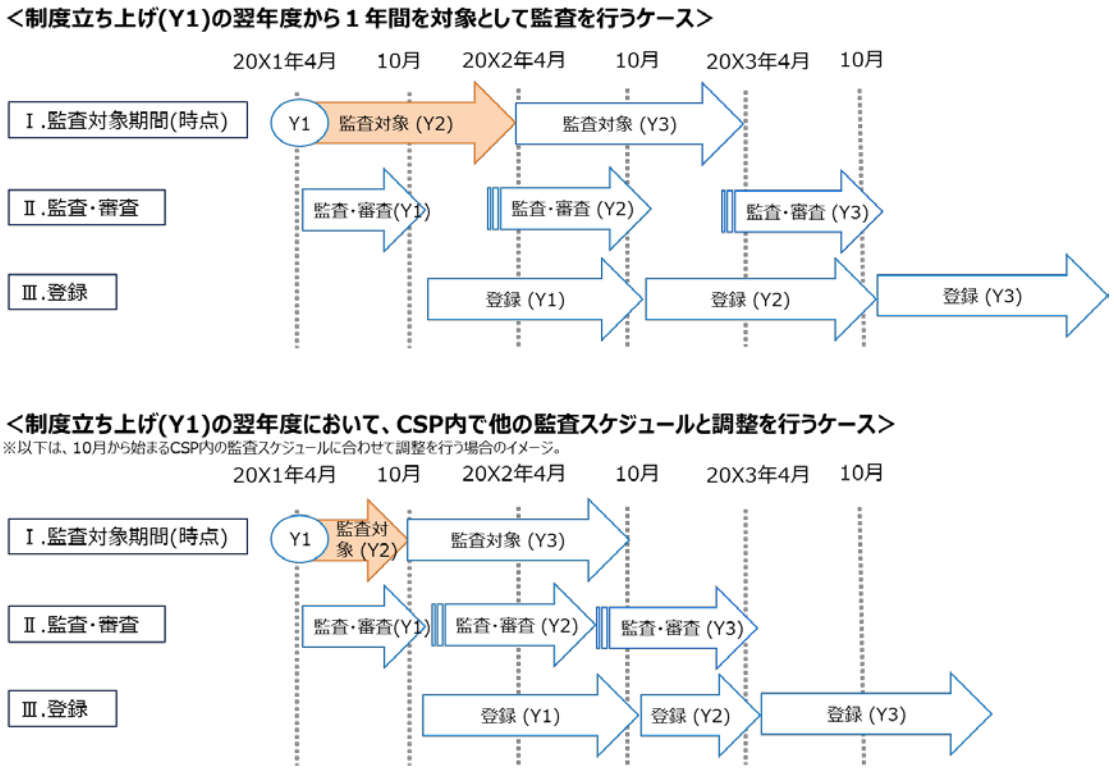
監査報告書の日付、すなわち監査人が監査報告書に署名する日付は、監査期間の末日若しくは監査基準日から最大で90日以内とする。これよりも監査報告書の日付が遅くなることを許容した場合、監査の対象期間と監査報告書の日時の乖離が大きくなり、その後の登録申請プロセスまで念頭におくと、監査対象期間が過去のものとなって監査報告の内容が陳腐化し、適切な登録判断に支障を生じる恐れがある。他方で、余りにも猶予期間が短い場合、監査人による監査対象期間の終盤部分についての監査報告の策定が実務上難しくなる可能性もある。この両面から判断した結果が、90日以内とすることが妥当との結論に至ったものである。

（3）申請期限

本制度においてCSPが登録申請を行うことができる日付についても、監査対象期間から大きく乖離すると監査結果が陳腐化するという観点から、一定の期限を定める必要がある。もともと本制度に基づく監査を受けるCSPは、本制度での申請を念頭においていると考えられることから、監査報告書が監査主体から提出される前から、申請書や必要書類の整理など、手続の準備を事務的に進めることが可能である。

このため、本制度における申請期限は、申請に添付する予定の監査の監査報告書の日付から30日以内とする。

（参考図2）監査の対象期間、申請期限等の考え方



1．6．言明書・監査報告書の主な記載事項と情報の扱い

言明書・監査報告書の主な記載事項と活用範囲は下記のとおり。今後、シミュレーション結果や調達側の要望等も踏まえて決定する。

＜言明書への主な記載事項＞

- クラウドサービスの名称
- 言明の対象範囲（対象となるロケーション、システム概要図）
- システムに関する記述（企業概要、クラウドサービス概要、詳細な内部統制の状況等）
- 対象管理策と統制内容（対象外となる管理策がある場合には、除外理由もあわせて記載）
- 監査対象期間

なお、記載対象となる管理策と統制の内容については、本制度が4桁レベルの詳細管理策に対する監査を行うものであることから、4桁レベルの詳細管理策単位まで記載を行うこととし、選択を行わない管理策については除外理由を記載することとする。

＜監査報告書への主な記載事項＞

- 監査依頼者の責任
- 監査実施者の責任
- 監査報告書の利用者の責任
- 監査手続内容（4桁レベルの詳細管理策単位で記載）

- 監査手続の実施結果（4桁レベルの詳細管理策単位で記載、発見事項の内容を含む）
- 監査報告書の配布及び利用制限について

＜情報の扱い＞

情報の扱いについては、「登録を行う上で利用する情報」と「調達をする上で利用する情報」の2つの観点で整理を行う必要がある。

前者には、本制度において求める情報の全てが該当し、制度所管機関への提出を求めるとともに、制度所管機関はこれら情報の取り扱いに十分注意する必要がある。

後者には、登録されたクラウドサービスから利用者が自らの求める機能、サービス、情報セキュリティ対策を満たした適切なクラウドサービスを選択する上で必要となる情報であり、必ずしも本制度で提出された情報の全てが該当するわけではない。係る観点から、登録簿における情報の公開の扱いや、個別の要求に応じた情報の開示の在り方については、利用者側が求める情報と、セキュリティ上開示が難しい情報のバランスを考慮し、監査シミュレーションの結果と調達側のニーズを勘案しながら決定することとする。

＜民間での活用について＞

本制度は政府が利用するクラウドサービスについて登録簿を作成するものであるが、公開される情報等について、1.2.の内容に十分留意しながら重要産業分野等をはじめとした民間においても参照[12]することで、クラウドサービスの適切な活用が推進されることを期待する。

1．7．発見事項と登録の基本的考え方

制度所管側においてサービス登録の審査を行う際、監査が適切に実施されていることを前提とした審査を行う。すなわち、監査のプロセスの適切性を確認する観点から、標準監査手続が適切に実施されたことを確認する必要があるが、監査報告書において発見事項が指摘されていない項目については、その内容の詳細を審査することはしない。仮に、監査報告書の全ての内容について制度所管側で詳細な審査を行った場合、監査主体が行ったプロセスを制度所管側において再度実施することとなり、非常に非効率である。

係る観点から、申請関連書類の記載漏れ、監査プロセスの適切性、発見事項の有無等の確認を行った上で、監査報告書に発見事項が存在しない場合、基本的には制度所管側は監査報告書の内容を受け入れることが妥当である。

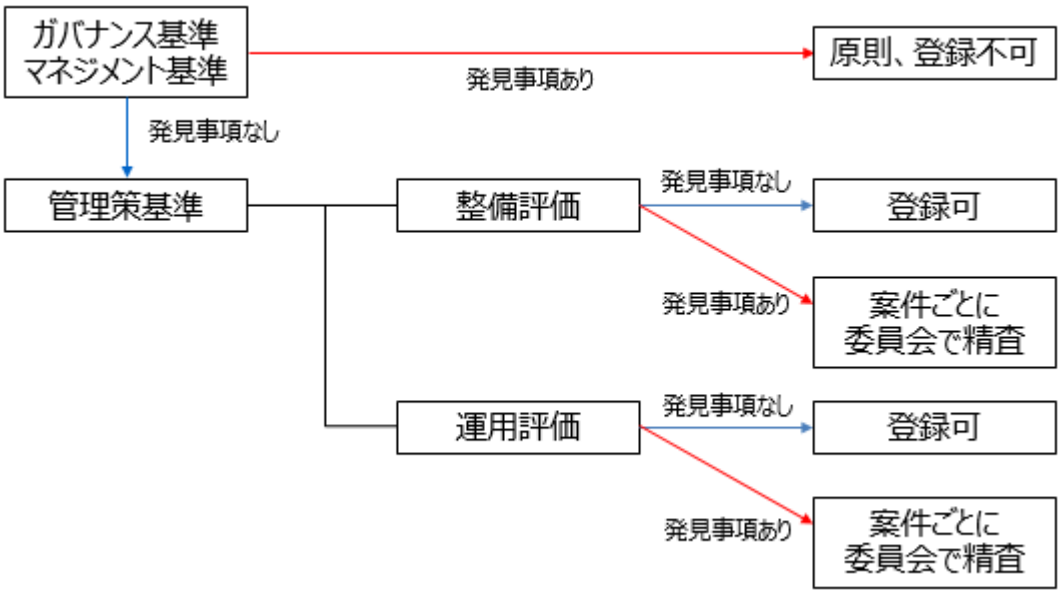
発見事項が存在しない状態を目指すべきことは言うまでもないことだが、一方で、実際の監査においては軽微な発見事項が報告されることが少なからず生じる。実際の運用を考えると、発見事項が一つでも存在する場合に例外なくサービス登録が行われない制度とした場合、セキュリティリスクに大きな影響を与えないにも関わらず登録が行われないことになる。したがって、発見事項が存在する場合においても、機械的にサービス登録を不可とするのではなく、その性質や個別の状況も踏まえて、以下の観点から登録の可否

[12] 関連して、本年５月２３日に『重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針』が改訂され、「事業環境の変化を捉え、インターネットを介したサービス（クラウドサービス等）を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する。」と位置付けられた。

を判断する必要がある。

- ガバナンス基準・マネジメント基準の内容において発見事項が存在した場合
  原則、登録を不可とするべきである。ガバナンス基準・マネジメント基準において発見事項が存在するということは、CSPが組織として適切なリスク分析とそれに基づく対策を実施する体制が築かれていないことを意味する。すなわち、1.1.のCSPがセキュリティ対策を行うプロセス①～⑥のうち、①～④が適切に実施されていない可能性が高いことを意味するからである。
- 管理策基準の内容において発見事項が存在した場合
  個別の事象ごとに登録の可否を判断すべきである。管理策基準の内容の不備は、ガバナンス基準・マネジメント基準とは性質が異なり、前述の①～④には影響を与えない。制度所管側において発見事項の内容を個別に精査し、「軽微」であると判断される場合には登録を認めることとし、この「軽微」のメルクマール[13]は例示を行うとともに、運用を行う中で事例を蓄積し、更新していくこととする。

（参考図3） 発見事項と登録の基本的考え方



1．8．登録されたサービスの変更時の扱い

（1）総論

中間とりまとめにおいて指摘しているとおり、制度運用を行う中で、クラウドサービスの動的な側面に柔軟に対応していくことが望ましい。

本制度はクラウドサービスの安全性に係る統制の有効性を確認することを目的としているものであること

[13] 例えば、形式的な不備（文書類の形式的な改訂漏れ、誤記等）については軽微と見なし、他方で、統制が機能していない場合のように実質的な不備（取得すべきログが抽出されない設定になっている等）については登録を認めない等

から、動的要素のうち、「統制の変更」[14]に着目して対応を行うものとする。統制の変更前後において統制の水準が維持されていることが求められるが、一般的にクラウドサービスにおいては細かな統制の変更が頻繁に生じる。したがって、制度の実効的な運用の観点から、その中でも特に重大な統制の変更と考えられるケースに該当する場合にのみ対応を求めるものとする。

（2）重大な統制の変更の考え方

重大な統制の変更とは、統制の整備前後のリスク評価に影響を及ぼす事象に関するものが該当する。CSPの統制の実装方法はサービスごとに異なり、重大な統制の変更に該当する事象を網羅的に示すことは困難であるため、重大な統制の変更につながりうる典型的な具体例[15]を示すものとする。

（3）重大な変更発生時の対応

CSPは統制変更を識別した場合、重大な統制の変更の考え方を参照するとともに、必要に応じて監査主体と相談を行った上で、当該変更が重大な統制変更に該当するかどうかの検討を行う。その上で、重大な統制変更に該当する場合には、制度運営事務局に届出を行い、変更箇所について再度監査を行うものとする。届出を受けた制度所管側では、必要に応じてCSPに対して照会を行いながら変更内容及び再監査結果を確認し、登録簿への登録継続の可否について検討を行う。なお、CSPは重大な統制変更に該当しないと判断した場合においても、統制の変更前後の運用記録を保管し、次回の更新監査の際に監査主体が確認を行えるようにする。その上で、更新監査において、統制の整備前後のリスク評価に影響を及ぼす事象の具体例として示された事象が発生していたにも関わらず、重大な統制変更を識別せず、届出及び再監査を実施していないことが判明した場合には、登録取消等の措置を含めて制度所管側において検討を行うものとする。

1．9．他のクラウドサービスを活用したクラウドサービスの登録の考え方

（1）総論

CSP がクラウドサービスを提供する上では、その機能の一部あるいは提供上不可欠なシステム基盤として、他のクラウドサービスを活用する場合が存在する。こうしたクラウドサービスを政府が活用する際には、政府が直接契約を行うクラウドサービスのサプライチェーン上に存在する他のクラウドサービスに対して、政府がセキュリティの状況を把握し、ガバナンスを働かせられるかどうかが重要な観点となってくる。

本項においては、便宜上、登録を目指すサービスを「クラウドサービス A」、その提供において利用している他のクラウドサービスを「クラウドサービス B」と呼ぶこととする。

---

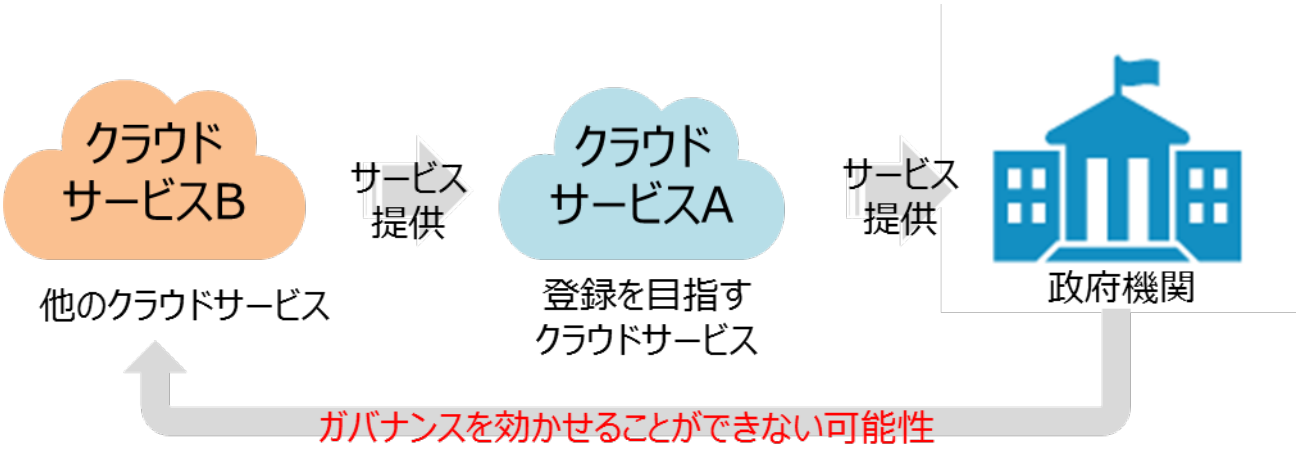
[14] 統制の変更には、３桁レベルの統制目標に対して選択する４桁レベルの詳細管理策を変更する場合や、同じ４桁レベルの詳細管理策であってもその実装方法や運用方法を変更する場合等がある。

[15] 例えば、リスクは以下に掲げる状況によって発生又は変化する可能性がある。事業環境の変化、新規担当者、新規の又は刷新された情報システム、急速な成長、新しい技術、新しいビジネスモデル・新製品又は新しい活動、会社の事業再構築、拡大する国外事業、新しい会計の意見書等。（国際監査基準３１５事業体とその環境の理解及び重要な虚偽表示リスクの評価（日本公認会計士協会）を参考とした。）

（2）登録の場合分け

本制度においては、（ア）クラウドサービス B が登録されている場合と、（イ）クラウドサービス B が登録されてない場合、のいずれの場合かで対応が異なる。

（参考図4）政府と機関とクラウドサービス A、B の関係



（ア）クラウドサービス B が登録されている場合

この場合、クラウドサービス B に対しても政府がセキュリティの状況を把握し、更新の監査等でガバナンスを働かせることができる。従って、クラウドサービス B が登録に際して選択した管理策の実施が確認されていることを前提に、当該管理策の内容を引き継ぎながら、クラウドサービス A 全体の監査を受ければよい。

なお、クラウドサービス B が登録されてからクラウドサービス A を申請することを前提とした場合、クラウドサービス A の登録が大きく遅れる可能性があることから、クラウドサービス B とクラウドサービス A が同時に申請されることは認めるべきである。

（例）既に登録されている他者の PaaS 上に構築した SaaS[16]を登録する場合

＜言明＞

① 全ての管理策の中で、サービス全体として満たすべき管理策を選択

② (a) 自身が満たすべき管理策と、(b)基盤部分の管理策を引き継ぐ部分を明示

③ (a)について、自身で個別管理策を設計し、実施。

16 本制度で言及しているSaaSとは、汎用的なクラウドアプリケーションを想定している。なお、SIerがIaaS/PaaS基盤を用いて提供するサービスについては、調達者/利用者が本来実施すべき情報セキュリティ対策を、一部、調達者/利用者に代わってSIerが実施しているという性格のものであり、利用者のニーズにあわせて特注でシステムを組み上げるものであるため、定型化して事前に本制度の登録を行うことが難しい。このため、後者のサービスの利用においては、基盤部分は登録簿に載っているIaaS/PaaSを用いつつ、SIerと調達者/利用者が協力してカスタマーが責任を持つべき対策を実施しなければならないことに留意が必要である。

④ (b)について、基盤部分が管理策に対応していることを示す。

＜監査＞

① (a)について、通常の手続に則って監査を実施。

② (b)について、基盤部分が該当項目について対策を実施しているということを確認。但し、詳細な実施の内容までは確認しない。

＜登録審査＞

① (a)について、通常の登録の審査手順に従って確認。

② (b)について、基盤部分が登録されているということを確認。

＜留意点＞

現時点において、レベル2の要保護情報が含まれるシステムを想定して検討を行っている。したがって、同レベルの中で、SaaS であるからといって、他のサービス形態と比してセキュリティ対策が簡素でよいということにはならない。すなわち、ファシリティからアプリケーションまでの総体として満たさなければいけない項目が変化するものではないということに留意が必要である。SaaS の登録においては登録プロセスの効率化が行われることが望ましいが、ここでの「効率化」の意味は、既に基盤部分で行われている対策について、SaaS 事業者が二重で行う必要がなくなるためには、どのような制度設計ができるか、という観点である。この点において、基盤の登録が行われていれば管理策を引き継ぐことを前提に監査を受けることが可能であり、全てを自身で構築している場合に比べて監査工数が低減されることが期待される。

（イ）クラウドサービス B が登録されてない場合

この場合、クラウドサービス B について、政府側が詳細なセキュリティ実施状況を確認することが困難となる。そのため、クラウドサービス A からクラウドサービス B を切り分けて、クラウドサービス B をサービスの対象範囲から除いてクラウドサービス A の登録を目指すことが基本的な考え方となる。

他方、クラウドサービス A を提供する上で、クラウドサービス B がセキュリティ上のリスクに与える影響が小さい場合には、登録者が供給者管理等の対策を実施することで、クラウドサービス B を切分けることなく登録することを認めるべきである。これは、細かなサービスの一つ一つについて逐一登録を求めた場合、いわば細切れ的にクラウドサービスの断片が登録されることになりかねず、利用者の視点から非常に使い勝手の悪い登録簿となる懸念があるためである。この場合には、クラウドサービス A の CSP はクラウドサービス B が登録の範囲外であることを明示した上で、その供給者管理等によってクラウドサービス B の安全性について確認を行った上で、自身の責任のもとでクラウドサービス B の利用を行うことを言明することとなる。

ただし、前述の例のように、クラウドサービス B を基盤としているなど、それが存在しない場合にクラウドサービスとして成立しない場合には、基盤部分が別途登録されていることが不可欠である。

（3）責任の在り方

1.1の考え方に従い、クラウドサービス A の CSP は言明の時点において、クラウドサービス A のうち自身が運用する範囲を明確にする必要がある。これは裏を返せば、他のクラウドサービス B の利用の有無とその範囲を明確にする必要があるということである。そして、クラウドサービス B の部分も含めたクラウドサービス A 全体の管理策の選択、実装を行う責任を有するのは登録を行う CSP である。

すなわち、政府と契約を行うのはクラウドサービス A を提供する CSP であることから、クラウドサービス B で何らかのセキュリティトラブルが発生した場合であっても、政府との関係ではクラウドサービス A の CSP が一義的に責任を負い、クラウドサービス A を提供する事業者の責任で解決を図る。その上で、クラウドサービス B の CSP の責任については、クラウドサービス A の CSP とクラウドサービス B の CSP 間の契約等に基づいて CSP 間で解決を図る。

2. 各種基準等の検討

2. 1. 基準等の検討体制

2019年度には、検討会の下部会議体として「管理基準WG」と「監査WG」の2つのWGを開催し、議論を行った。具体的な各種基準等を検討する上で、実効性の確保の観点から、より広く民間からの意見を取り入れるため、「管理基準WG」にはCSPに所属する有識者を議決権のない専門委員として、また、「監査WG」には監査法人等に所属する有識者を委員として加え、議論を深めた。

「管理基準WG」においては、技術的な実現可能性の観点も踏まえながら、管理基準に含まれるガバナンス基準・マネジメント基準・管理策基準の素案作成を進めてきた。

「監査WG」においては、監査基準、制度における監査の位置づけ、証跡の扱い、監査期間の考え方等、制度の中で監査に深く関わる内容について議論を進めてきた。

なお、中間とりまとめで指摘されたことを踏まえ、主に9～10月に監査シミュレーションを実施した。シミュレーションの目的は、主に管理基準案で監査が可能であるかの確認及び標準監査手続のひな形の作成であった。シミュレーションにおいては、管理基準への対応が可能であること、標準監査手続の作成が可能であることは確認され、制度の枠組みに大きな変更は必要ないとの結論に至った。その上で、制度の詳細に関しては、特に運用評価に関する意見が提示された。この点については、対応方針を後述する。

2. 2. 管理基準の検討

（1）管理基準の構成について

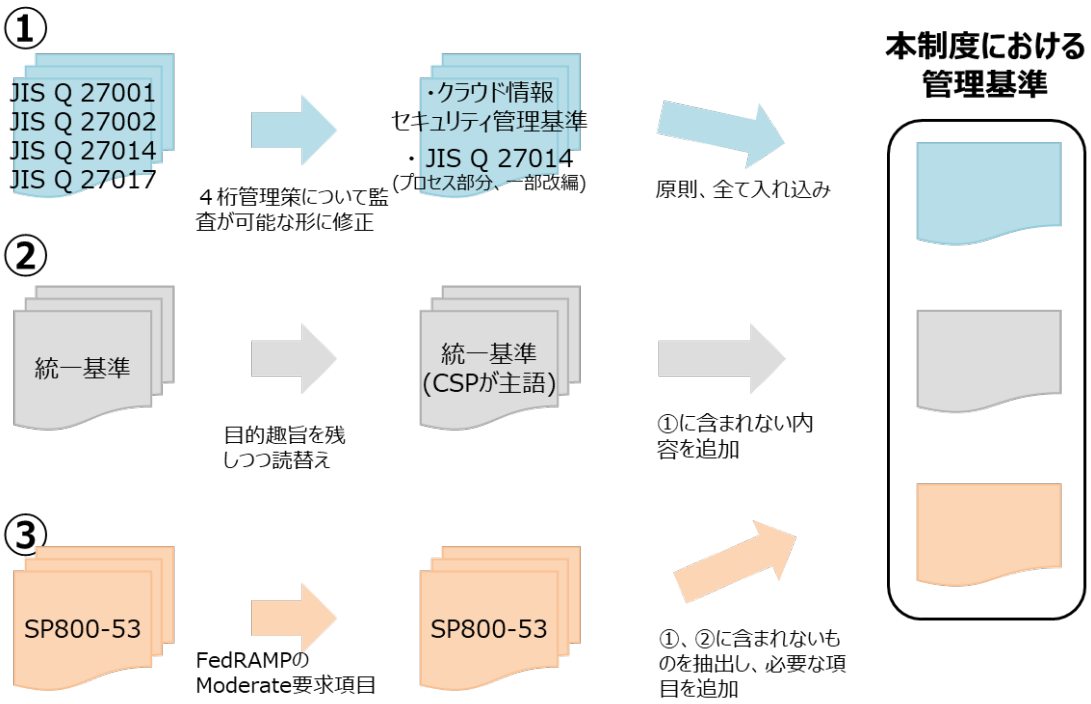
管理基準は、中間とりまとめで示したとおり、ガバナンス基準・マネジメント基準・管理策基準の3種類から成る。中間とりまとめにおいて、管理基準を「Ⅳ.統一基準でなされている整理に合わせて、必要な項目を再構成する」としていたところ、CSP への意見照会[17]を経て、統一基準の整理に再構成するのではなく、CSP による対応の容易さも鑑み、広く浸透している国際規格の整理に合わせることとした。

---

[17] 「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」の3.3.1（3）において、「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。」とされていたことから、意見照会を実施した。

すなわち、(参考図5)のように、国際規格をベースとしながら、統一基準及び SP800-53 から国際規格に不足していると考えられる項目のうち、政府として必要と考えられる項目を追加する形で管理基準作成した。なお、管理基準は1.4.(1)に記載のとおりレベル2を対象として設定した。

(参考図5)管理基準の構成と考え方



① 国際規格について

本制度の枠組みに関連する国際規格[18]には、情報セキュリティに関する JIS Q 27001 (ISO/IEC 27001)、JIS Q 27002 (ISO/IEC 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 27017 (ISO/IEC 27017)が存在する。1.1.に記載のとおり、本制度は情報セキュリティ監査の枠組みに基づくものであることから、監査人が監査上の判断の尺度として用いるべき基準として、これら国際規格に準拠して編成された「クラウド情報セキュリティ管理基準(平成28年度版)」を参考とすることとした。なお、当該基準にはガバナンス基準・マネジメント基準・管理策基準が含まれるが、ガバナンス基準については、当該基準策定以降に発行された JIS Q 27014(ISO/IEC 27014)を参考として、主に監査の実施可能性の観点を踏まえ検討を行っている。

② 統一基準について

統一基準は政府機関等が遵守すべき事項を規定している。これらの事項は、CSP が実施すべき対策に加えて利用者が追加的な対策を施して初めて達成されるものであり、統一基準の項目

[18] JIS Q 27017 (ISO/IEC 27017) 及びJIS Q 27014 (ISO/IEC 27014)は、我が国が主導して策定した国際規格である。

をそのまま CSP に求めることは適切でない。このため、政府統一基準の目的趣旨に則して、CSP が主体として行うべき内容を勘案し、基準項目としての読み替えを行った。

こうして読み替えた基準について、①で含まれず、かつ「CSP が実施しなければ、調達者/利用者側が統一基準を満たすことに支障を来す内容か否か」の観点から CSP に求めるべき内容であると判断されるものについて、追加を行うこととする。

③ SP800-53[19]について

クラウドサービスに関する基準を検討する上では、基準の網羅性・検討の効率性の観点から、既存の基準を参考として追加項目の有無を精査した。中間とりまとめにおいて参考にするとされた海外の基準の中で、運用実績が長く、複数回の基準更新が行われてきたものとして NIST の SP800-53 が挙げられる。当該基準について分析を行い、追加すべき項目の精査を行った。

この際、クラウドサービスを対象としていること、レベル2を対象としていること、国際規格との対応関係という観点から、FedRAMP において Moderate の要求事項とされている項目であって、NIST が行っている ISO/IEC 27001 との比較において、ISO/IEC 27001 では対応がとれないとされている項目に検討の対象を絞り込んだ。

上記の絞り込み作業の結果残った項目の一つ一つについて、「クラウド情報セキュリティ管理基準(平成28年度版)」の内容と比較対照作業を行い、管理策として新たに追加すべき内容と、①の内容に追記することで趣旨を入れ込むべき内容を精査した。この作業において、(参考図6)における傾向の差異を踏まえ、以下を念頭に検討を行った。

- 記載方法が異なっても、目的が同じと考えられる内容については、①を優先する。
- 同趣旨の管理策においてより踏み込んだ内容が記載されているものについては、追記を行う。(管理策数を増やさない)
- ①に観点として不足していると思われる項目は、管理策としての追加を検討。

[19] 現在、SP800-53 rev 4 の改訂作業が進められているところであるが、本検討においては基準の網羅性・検討の効率性の観点から、その一例としてSP800-53を参考としているものであり、SP800-53の遵守を目指すものではない。従って、当該改訂による変更について、直ちに本制度に影響が与えられるものではなく、国内外の各種制度や、最新の技術動向を踏まえての見直しを行う際の参考の一つとなるにとどまる。

(参考図6)国際規格と SP800-53 の主な観点の差異

JIS Q 27001、27002、27017 (ISO/IEC27001、27002、27017)	SP800-53
「セキュリティリスク管理」に注目	「情報の保護」に注目
「マネジメント」を重視 ※PDCAを前提とするため、更新等に明確な言及がない箇所が存在	「対策」を重視 ※レビュー、変更、更新、頻度まで明確に記載
手段まで詳細に規程していない	詳細を規程し、自動化を追求
事業継続計画に言及	緊急時に言及
構成管理は限定的	構成管理に詳細に言及

※全ての管理策について上記が当てはまるわけではない。

(2)CSP を主語とした管理策への読み替えについて

本制度における管理基準の特徴として、CSP を主体とした管理基準となっていることが挙げられる。統一基準をはじめ参考としている基準の多くはオンプレミスの情報システムの利用者が実施主体であり、CSP を実施主体として策定されたものではない。係る観点から、以下の3つの定型管理策への読み替え作業を行った。

- 定型管理策1:CSPが、自ら当該管理策を実施すべきもの
- 定型管理策2:CSPが、政府機関が当該管理策を実施するための機能を提供すべきもの
- 定型管理策3:CSPが、政府機関が当該管理策を実施できるように情報を開示すべきもの

なお、定型管理策2が求められている場合、「機能」を提供することとなるが、この場合、定型管理策3が位置づけられていなくても、提供する「機能」の使い方等に関する情報の提供についても求められることとなる。

(3)管理基準の種別ごとの考え方と検討状況について

① ガバナンス基準・マネジメント基準について

ガバナンス基準については、情報セキュリティガバナンスに関する国際規格である JIS Q 27014 (ISO/IEC 27014)に基づき検討を行うこととした。JIS Q 27014 は、大きく「一般」「概要」「原則」「プロセス」から構成される。ガバナンス基準については、経営陣によるコミットメントに主眼が置かれているため、監査の対象範囲とするか否かも含めて、管理基準においてどのように位置づけるかの検討を行っている。

また、マネジメント基準については、「クラウド情報セキュリティ管理基準(平成28年度版)」のマネジメント基準項目について、SP800-53 の内容を一部入れ込む形で整理を行っている。

② 管理策基準について

管理策基準については、「クラウド情報セキュリティ管理基準(平成28年度版)」の管理策基準項目について、前述の SP800-53 の項目を追加、及び内容を一部追記する形[20]で整理を行っている。

[20] 例えば、クラウド情報セキュリティ管理基準において「Aをレビューする。」という管理策が存在し、SP800-53において「A'をレビューし、更新する。」という管理策が存在し、AとA'が同趣旨と考えられる場合、本制度の管理策としては「Aをレビューし、更新する。」という一つの管理策として追記を行うことで吸収を行った。

（4）統一基準由来の管理策の扱いについて

統一基準由来の管理策については、政府内において「CSP が実施しなければ、政府側が統一基準を満たすことに支障を来す内容か否か」という観点で項目の精査を行う必要がある。係る観点から、原則として、定型管理策2と定型管理策3に相当する内容については必須項目と位置づける必要がある。他方、定型管理策1は、限定的なものとなることが想定される。その理由は、政府が統一基準を満たす上で必ずしも必須となる内容ではなく、政府から見ると委託先管理に含まれる内容と考えられるものが多く含まれ、その方法を統一基準の内容をベースに細かに規定して必須項目とすることは、CSP やその提供するクラウドクラウドサービスによって異なるはずの内容までも規定することとなり、技術の発展等を阻害する恐れがあることである。

（5）その他

CSP は管理基準に基づき様々な情報の提出が求められるが、その中には例えば、データセンター等の場所や準拠法令、裁判管轄権等についての情報などがある。こうした情報は登録審査において登録可否を総合的に判断する際の材料となりうる。[21]加えて、こうした情報が政府に提供されることにより、政府機関が個別の情報システムを調達する際にリスクを勘案し、データセンターの設置場所も考慮しながら適切なクラウドサービスを選択できるように促していく。

2．3．監査関連基準等の検討

（1）標準監査手続の考え方

中間とりまとめにおいて提示したとおり、本制度において、監査主体はあらかじめ定められた標準監査手続に基づいて監査する。標準監査手続の策定にあたっては、以下のような整理の下で、作成作業を進めている。

- 標準手続は4桁レベルの詳細管理策管理策に紐付ける形で作成。
- 手続の内容は4桁レベルの詳細管理策ごとに、監査対象を原則「ヒト」「モノ」の2つに区分し、それぞれについて「整備」「運用」の2つの観点から整理。
- その上で「整備」「運用」それぞれについて、「閲覧」「質問」「観察」といった監査技法を位置付け。
- 監査技法ごとに、より詳細な確認方法を記載。

なお、監査シミュレーションにおける指摘において、運用評価を全ての管理策で実施することによって、監査工数が大幅に増加し、それにかかる費用も上昇する懸念が示された。このため、運用評価を行う対象の管理策について重点化・効率化を検討し、その結果を踏まえ監査手続に反映する方向で、引き続き監査WGにおいて検討を行うこととする。

（2）監査主体登録基準の考え方

① 基本的な考え方

中間とりまとめにおいて提示したとおり、本制度において、政府は予め定めた基準に基づき監査主体の

[21] 本制度のレベル２の基準に基づく登録においてデータセンターの国内設置が一律に求められるということではない。

選定を行い、監査主体リストに登録される。選定対象となる主体は、我が国において情報セキュリティ監査[22]を業務として行っている法人とする。

② 監査主体登録基準の具体的な要件

中間とりまとめにおいて、監査主体の選定においては、評価を行う技術的/専門的能力を有しているか、主体自身が信用に値するか、という二つの基本的視座を踏まえて選定の枠組みを構築するものとしていたところ、これを受けて、法人としての監査主体とそこに所属する個人という観点から選定の具体的要件について検討を行った。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。

＜法人に対する要求事項の例＞

- 法人登録: 国内に法人登録があることを要求。
- 監査サービスの品質: 情報セキュリティサービス基準適合サービスリスト(サービス分野:情報セキュリティ監査サービス)[23]に登録されていることを要求。それに加えて、本制度で求められる水準の品質管理体制に関する要求事項を追加。
- 準拠規則等: 本制度の規程類に準拠すること。
- 監査報告等: 本制度が定める様式に従って監査報告書を作成するとともに、監査が適正に行われたことを示す記録を作成し、適正に保存すること。また、制度所管機関からの問い合わせ等に適切に対応すること。
- 問題事案発生時の検証体制を有する組織への所属: 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行わなかった場合等、最終的には選定の取り消し等の措置がとられる必要がある。こうした措置を行う場合には、十分な事実検証が必要であるが、制度立ち上げ時点において政府内にこのような機能を備えた組織を構築することは困難であるため、当面の間は、そのような体制を有する組織に所属していることを要求する。

＜監査人に対する要求事項の例＞

I. 業務執行責任者[24]に対する要求事項の例

- 資格要件: クラウドコンピューティングや情報セキュリティ、監査に関する知見を担保する観点から、これらの領域における資格を要求。

---

[22] 「情報セキュリティ監査の目的は、情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、情報セキュリティマネジメントの体制及びコントロールの整備、運用状況を、独立かつ専門的な立場から、一定の基準に従って検証又は評価し、もって保証を与えあるいは助言を行うことにある。」(経済産業省『情報セキュリティ監査基準Ver.1.0』)

[23] 情報セキュリティサービス基準適合サービスリストは、経済産業省が策定した「情報セキュリティサービス基準」への適合性を審査登録機関によって審査され、同基準に適合すると認められた事業者の情報セキュリティサービスを掲載するものである。そのうち、情報セキュリティ監査サービスとは、情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備・運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与え又は助言を行うサービスをいう。(経済産業省『情報セキュリティサービス基準』を参照。)

[24] 業務執行責任者とは、監査主体に所属する者であって、情報セキュリティ監査業務及びその結果報告書に対する責任を負う者を指す。

- 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、業務執行責任者に日本国籍を要求。

II. 業務実施者[25]に対する要求事項の例

- 技術要件： すべての業務実施者は、次に掲げる知識及び技能を備えていなければならない。
  - 情報システムの企画、開発、運用、保守に関する知識及び技能
  - 情報セキュリティのマネジメント及びコントロールに関する知識及び技能
  - 情報セキュリティ技術及びクラウドコンピューティングに関する知識及び技能
  - 情報セキュリティ監査の実施（監査計画の立案、監査手続の選択適用、監査証拠の入手と評価、監査調書の作成、監査報告書の作成）に関する知識及び技能
  - その他の関連知識
- 研修受講： 監査実務の円滑な実施や品質確保の観点から、情報セキュリティ監査サービスの品質確保に資する教育又は研修の受講を要求[26]。
- 国籍要件： 業務実施者に対しても国籍要件を適用していくべきかについては引き続き検討を行う。

③ 監査主体リストへの登録・変更・取消

制度運営委員会によって監査主体登録基準を満たすことが確認された監査主体は、監査主体リストへ登録される。リストへの登録有効期間は2年間とし、更新を行う場合には、監査主体は所定の様式に従い申請を行うものとする。他方で、監査主体の水準の維持の観点から、有効期間中において、監査主体に基準に則した状況を報告させるなど、一定のモニタリング機能を設けるものとする。モニタリングの結果、基準に定める要件を満たさないと認められた監査主体は、監査主体リストからの登録が取り消される。

（3）証跡等の活用について

本制度における監査において、監査人は、原則、監査対象から直接入手した証跡を本制度で定める標準監査手続に従って評価を行うものとする。そのため、監査人の直接評価に代えて既存の認証制度・監査制度・内部監査等の報告書の結果をそのまま利用することは認められず、また、本制度で定められた標準監査手続以外の手続によって評価を行うことも認められない。ただし、監査人が標準監査手続を実施する際に適切とみなす場合には、既存の認証制度・監査制度・内部監査等において収集された証跡を監査証跡として採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。

（4）リージョン[27]とサンプリングの考え方

---

[25] 業務実施者とは、監査主体に所属する者であって、情報セキュリティ監査業務に携わる、業務執行責任者以外の者を指す。

[26] 監査品質の確保の観点から、制度運用を行う中で監査手続を実施する際のガイドラインの作成等も検討するものとする。

[27] クラウドサービスを提供する情報処理設備を収容するデータセンターが設置されている独立した地

CSPは、言明書においてサービスを提供するリージョンを明らかにする。本制度における監査は、言明書の範囲を対象とすることから、監査証跡として用いられる資料は、言明書に明記されたリージョンの中から収集されたものであることが必要である。したがって、複数のリージョンを跨いで同一の統制下にある場合であっても、言明書において明記されたリージョンのものでない資料を本制度の証跡として採用することは認められない。他方で、言明書に明記したリージョンの範囲内であって、かつ、統制が同質である場合[28]には、監査証跡として用いられる資料が複数のリージョンを跨いでいる場合であっても、監査対象となる母集団を単一と見なし、この母集団の中からサンプル抽出を行うことを認めるものとする。

3. 今後の進め方と課題

3. 1. 制度立ち上げまでの今後の検討の進め方とスケジュール

本とりまとめにおいて制度の枠組みはまとめられることとなる。他方で、2. に記載のとおり、各種基準については現時点において大枠は固まっているものの、詳細部分についてはなお検討中である。したがって、各種基準は今後WGにおいて議論した上で、WGとしての案をとりまとめると共に、制度所管機関において最終的な決定を行うものとする。その際、CSPへの要求事項となる管理基準を中心とした主要な基準については、事前にパブリックコメントを行う。

制度のスケジュールについては、これまでの各種政府決定文書において、2020年秋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。他方で、制度に対してCSPや監査主体が適切に対応するためには、事前の準備期間を適切に取る必要がある。したがって、各種基準については、できる限り早急に検討を進め、本年度内にはパブリックコメントを実施する[29]とともに、速やかな制度の立ち上げを行う。その後の制度の運用においては、監査等の実務の状況も踏まえながら柔軟に対応しつつ、遅くとも2020年度中には評価結果が利用可能となるように、制度の立ち上げに向けて全力を挙げて取り組むべきである。

3. 2. その他の論点

①調達者/利用者が構築を行う上で重要な視点の整理

1.2.で述べたとおり、本制度で登録されたクラウドサービスを活用する際にも、登録簿に載っていることを以てリスクゼロとはならないため、調達者/利用者側においても情報セキュリティ対策を行う必要がある。このように調達者/利用者が留意すべき点等について、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル[30]」（以下、「SBDマニュアル」という。）の内容を参考としながら、クラウドサービス特有の代表的な留意点について、中間とりまとめの後に調査を行ってきた。その結果を踏まえれば、例えば、（参考図7）の点に留意しながらクラウドサービスの調達と情報システム全体の構築を行うことが望ましい[31]。

域。

[28] 例えば、統一された手続があり、同一の管理者によって査閲される等

[29] 標準監査手続については、質・量両面から丁寧な作業が必要であり、迅速な作業をすることは前提としつつも、拙速は避けるべきであるとの指摘が委員からなされた。

[30] https://www.nisc.go.jp/active/general/pdf/SBD_manual.pdf

[31] (参考図７)に示された対策は、調達者/利用者側で行うべき対策が網羅されているわけではなく、あく

ただし、SBDマニュアルは、クラウドサービスを前提として策定されたものではないため、（参考図7）において「主なセキュリティ留意点」としてまとめた内容は、従来の対策方針をCSPで書き直したものである。クラウド・バイ・デフォルトを推進する上で、セキュリティの留意点をまとめるためには、（参考図7）の内容に加えて、SaaSの活用、クラウドネイティブアーキテクチャの採用、横断的なアーキテクチャの活用、従来の境界型セキュリティアーキテクチャの後継となるセキュリティアーキテクチャ、DevOps等の継続的な運用・開発を考慮する必要がある。

（参考図7）クラウド利用時のセキュリティ上の留意点

	対策区分(※)	対策方針(※)	主なセキュリティ上の留意点	調達者/利用者側における対応策の一例
1	侵害対策	• 通信回線対策 • 不正プログラム対策 • 脆弱性対策	✓ ネットワーク上のアクセス制御や経路上の通信の閉域性の確保は利用者側での設計が必要 ✓ マネージドサービス上での脆弱性対応が必要	✓ FW機能等の活用による外部アクセスの制御 ✓ 接続サービスの活用によるNW経路閉域化 ✓ CSP提供のパッチ適用機能の活用、等
2	不正監視・追跡	• ログ管理 • 不正監視	✓ CSPが提供する各種サービスに対する操作ログの収集及び不正操作の検知の仕組みの実装が必要	✓ ログ収集・不正検知サービスの活用 ✓ CSP提供範囲外における監査・管理の仕組みの実装(パケットキャプチャ、画面録画)、等
3	アクセス・利用制限	• 主体認証 • アカウント管理	✓ 管理コンソールの操作におけるアカウント自体のアクセス制御に加え、インターネットからのアクセス制限の考慮が必要	✓ 多要素認証機能（MFA）の利用 ✓ 必要最小権限の付与 ✓ 拠点IPや踏み台等による接続元の制限、等
4	データ保護	• 機密性・完全性の確保	✓ データ保護に際しては暗号化の実施に加え、選択した暗号化方式にもとづいた暗号鍵の管理を利用者責任のもと実施する必要がある	✓ 機密性や規制に応じた暗号化方式の選択 ✓ 暗号鍵サービス利用時のライフサイクル管理 ✓ データライフサイクル管理(データ廃棄)、等
5	物理対策	• 情報窃取・侵入対策	✓ CSPの管理範囲である物理環境（データセンタ環境等）に対し、通常利用者側はCSPが実施するセキュリティ対策に依存する必要がある	✓ 物理環境におけるセキュリティ対策を要求する第三者認証の取得状況の確認、及び監査レポートによる詳細確認、等
6	障害対策 (事業継続対応)	• 構成管理 • 可用性確保	✓ CSPが定める復旧条件（SLA等）や復旧プロセス（通知等）に従い、利用するサービスの仕様を把握し利用者側で冗長化の対応が必要	✓ CSPサービスを活用した冗長構成の構築 ✓ 復旧の仕様に従ってのサービス採否の判断 ✓ CSP提供の障害通知機能の活用、等
7	サプライチェーン・リスク対策	• 情報システムの構築等の外部委託における対策 • 機器等の調達における対策	✓ CSP側における委託先や機器調達の契約やプロセスに対し、通常利用者側はCSPが実施するセキュリティ対策に依存する必要がある	✓ 委託上のセキュリティ対策を要求する第三者認証の取得状況の確認、及び監査レポートによる詳細確認、等
8	利用者保護	• 情報セキュリティ水準低下の防止 • プライバシー保護	✓ オンプレミス環境同様、システム利用者のセキュリティ水準を低下させないようアプリケーションを設計・構築する必要がある	✓ オンプレミス環境と同様の対策を実施(アプリケーションの最新ブラウザ上での動作対応、等)

※：「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル 2019年9月24日版」より

（出典：アクセンチュア　クラウドサービスの安全性評価に関する検討会　調達・構築関連調査）

また、2.2.の方針で検討を行っている管理基準について、上記視点と管理策との対応関係を整理しているところであり、調達者/利用者が本制度の登録に関する情報を利用する際に、どの管理策を確認することで上記留意点に関する情報を得られるのかを一定程度示すことが重要である。[32]また、この情報を得た上で、調達者/利用者側の対応としては、「監査レポートの内容を確認するもの[33]」と、「監査レポートの内容を確認した上で、必要な設計・設計等を利用者側の責任にて実施する必要があるもの[34]」のどちらに該当するのかを把握し、調達者/利用者側における誤った設定等に起因するセキュリティインシデントを防ぐことができるよう、促していくことが重要である。本制度の運用を行う中で、登録に関する情報について調達者/利用者が確認し、適切に活用できるようになる必要がある。こうした目的を達成するためのガイダンス、ベストプ

まで対策策の一例を示しているものである。最新の技術動向も踏まえながら、自身の利用する機能やサービスに応じた対策を講ずることが必要である。

[32] JIS Q 27017(ISO/IEC 27017)においてはCSPだけではなくクラウドサービスカスタマが実施すべき項目も記載されているため、こうした情報も活用するとよい。

[33] 例えば、「物理対策」の対策区分について、データセンターにおける対策等は調達者/利用者側が対策を実施するものではなく、CSP側が適切なセキュリティ対策を行っていることを確認することが重要。

[34] 例えば、「アクセス・利用制限」の対策事項について、調達者/利用者側は、CSPから提供される情報や機能を用いて、サービスへのアクセス制限や多要素認証機能を適切に設定することが重要。

ラクティス等についても検討を行っていく必要がある。

②クラウド・バイ・デフォルトを推進する上で重要な論点

クラウド・バイ・デフォルトを推進していくためには、（参考図7）の1～6について検討・整理することが重要であるが、今回行った調査においては1の内容に焦点を当てていた。その他の観点は必ずしも本検討会のスコープに収まるものではないが、クラウドサービスをとりまくトレンドに遅れることなく、引き続き、2～6の内容についても調査・検討を行い、政府におけるクラウド・バイ・デフォルトを推進する環境整備を行っていく必要がある。なお、①の視点を整理した上で、それを調達者/利用者側が理解できなければ、クラウドサービスの活用は進まない。（参考図8）の2として挙げた、利用者側のクラウドサービスに関する知識、能力の強化を行うことにより、クラウドサービスのメリットを最大限活用できる体制を整備していくことが喫緊の課題である。[35]

（参考図8）クラウド・バイ・デフォルト原則を推進するために必要な検討事項

1	• 安全性評価制度の整備が進む中、仕組みの実行性を向上させるため現状の政府情報システムの実態を踏まえた利用者側の観点における監査レポート(言明書や監査報告書を含む各文書)の活用に係る検討が必要
2	• クラウドサービスの利用者側における、利活用に際して必要な体制やプロセス（CI/CDやDevOps等の開発運用手法に対応した人材及びプロセス）の整備に向けた検討が必要
3	• AIやIoTといった特定技術領域の活用にあたっては、提供されるサービス内容や技術仕様がCSPによって大きく異なる点を踏まえたクラウドサービスの活用検討が必要
4	• システム単体のみならず、複数システムを横断的に対象とした、組織・団体を跨っての費用対効果を追求したクラウド化方針及び全体アーキテクチャの検討（統一的な利用のための判断基準の策定及び共通化対象機能や採用技術の選定等）が必要
5	• 新たなサイバー攻撃やセキュリティ上の脅威に対抗するための既存の枠組みとの整合性を踏まえた次世代のセキュリティアーキテクチャ(セキュリティ境界内におけるトラフィックの評価やユーザ挙動の検証の仕組み等)の検討が必要
6	• システム固有の業務やアプリケーション領域における、採用可能性のあるアーキテクチャや技術製品が多岐に渡ること踏まえたクラウドの効果をより大きくするための利用策（SaaS活用やクラウドネイティブアーキテクチャの採用等）の検討が必要

（出典：アクセンチュア　クラウドサービスの安全性評価に関する検討会　調達・構築関連調査）

③競争政策

必ずしも本制度の範疇ではないが、本制度におけるサプライチェーンの扱いなどの考え方から、本制度の登録をSaaS等のクラウドサービスは、様々な機能を提供する大手のCSPによる登録されたサービスに、その基盤を依存する度合いが高まる可能性がある。これに対し、大手CSPが例えば自社のSaaSサービスを自社で提供する基盤サービス上で構築する場合と、同じサービスを利用してSaaSサービスを提供しよう

[35] その一環として、外部からの専門人材の確保も必要であり、専門的人材の確保にかかる待遇面での柔軟な検討も必要との意見が委員から提示されている。

とするサードパーティとの間で、大手CSPが不当な取り扱いの差異を設ける可能性も否定できない。このような場合、適切なサービスの競争環境が歪められることになりかねない。このため、政府として引き続き、こうした問題にどのように対処すべきなのか検討を進めるべきである。

④見直しの体制

中間とりまとめでも度々指摘されているとおり、クラウドサービスの世界は非常に技術進歩が早く、制度立ち上げ後に立ち上げ時に策定した基準にしたがって運用を行うだけでは、早晩クラウドサービスの実態から制度が乖離してしまうことになりかねない。加えて、実務運用の中で、審査プロセスや制度への対応コストの面で課題が明らかになった場合、適切な対応を行わなければ結果としてクラウドサービスの利用に支障が生じる恐れもある。したがって、本制度においては、技術動向や国際的なクラウドサービスの利用動向などを絶えずフォローし、また、②の2～6で示した内容を踏まえ、基準やガイドラインへの柔軟な反映や運用状況を踏まえた制度全体のフォローアップを行うことが不可欠である。このため、（ア）政府は柔軟な見直しが可能となる場を設けること、（イ）IPAにおいてこうした動向の継続的な調査を行う体制を築くこと、の2点を検討会として求めたい。

⑤経過措置

政府の情報システムの調達は数年のスパンで考えられるものがほとんどであり、制度立ち上げ時点ですでに利用を開始しているクラウドサービスについて、登録がないことをもって即座に利用停止とすることは非現実的である。これは調達プロセスのうちシステム開発のフェーズまで進んでいる場合等においても同様である。したがって、本制度の立ち上げに当たっては、情報システムの調達/利用の実務に、不合理な支障を生じさせることがないよう、例えば既存システムについてはシステム更新のタイミングで本制度への準拠を求めるなど、適切な経過措置を設ける必要がある。他方、政府機関等においては、自身の使っているクラウドサービスを提供するCSPに対して、サービスの登録がない場合に本制度への登録を促すことが望ましい。

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　エグゼクティブフェロー
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　参与
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	AI・サイバーセキュリティ推進室
防衛装備庁	長官官房総務官

【事務局】

総務省	サイバーセキュリティ統括官室
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、五十音順）

＜管理基準 WG＞

【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
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
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

【専門委員】

久保田　朋秀	日本マイクロソフト株式会社
坂田　昭彦	NTT コミュニケーションズ株式会社
鈴木　拓也	富士通株式会社
瀧澤　与一	アマゾンウェブサービスジャパン株式会社

＜監査 WG＞

【座長】

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　エグゼクティブフェロー

【委員】

遊馬　正美	EY 新日本有限責任監査法人　シニアパートナー
加藤　俊直	PwC あらた有限責任監査法人　パートナー
辻村　啓	有限責任監査法人トーマツ　ディレクター
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
山口　達也	有限責任あずさ監査法人　パートナー
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、事務局は検討会に同じ）