「ガバメントクラウドにおけるSaaS（公共SaaS）について（案）」に関する意見募集の結果について

令和７年４月１日
デジタル庁
省庁業務サービスグループ
ガバメントクラウド担当

「ガバメントクラウドにおけるSaaS（公共SaaS）について（案）」に関する意見募集を実施いたしました。お寄せいただいた御意見の概要とそれに対する考え方を、別添のとおり取りまとめましたのでお知らせいたします。

今回御意見をお寄せいただきました皆様に厚く御礼申し上げます。

１．実施期間等

（１）意見募集期間　令和７年３月７日（金）～令和７年３月21日（金）

（２）実施方法　電子政府の総合窓口「e-Gov」ホームページの掲載等により周知を図り、e-Govにより御意見を募集。

２．提出意見の総数等

（１）提出意見等　72件（このうち、意見募集対象とは直接関係しない御意見17件）

（２）提出意見の概要及びそれに対する考え方　別紙のとおり

３．本件に関するお問合せ先

デジタル庁省庁業務サービスグループ
TEL：03-4477-6775

別紙

No	御意見の概要	御意見に対する考え方
1	・総務省のセキュリティポリシーガイドラインの内容と明らかに乖離している記述があるが、そのギャップを説明する理由が十分でない。総務省のガイドラインでは、機密性3C以上の情報をクラウドサービスで扱う場合は、「そのクラウドサービス自体がISMAPに登録されていることが必要であり、単にISMAPに登録されたサービスで構成されているだけでは不十分」と整理されている。ガバメントクラウド上に構築されているクラウドサービスであることをもって、デジタル庁がセキュリティを担保したことにするというのは、国民の情報を預かる政府としてあまりに恣意的ではないか。 ・あるべき姿として、ガバメントクラウドは将来的に政府専用リージョン、ソブリンクラウドとして構築することを前提とすべきである。ガバメントクラウドをサービスとして提供が可能なクラウド事業者が現状外国企業に限られており、特に米国企業に偏っている。昨今の米国のトランプ政権をはじめとする不安定な世界情勢を考慮すると、米国企業に日本国民の住民情報がある状態はデータ主権の観点から許容されるべきではない。なお、ガバメントクラウドの技術要件になっているBYOKは利用者の鍵をクラウドに持ち込むものであって、CSP側から判読不能にする仕組みではないため、セキュリティ対策として不十分である。 ・ガバメントクラウドによるコスト最適化を謳っているが、全国市長会等がガバメントクラウド移行前より移行後の方が運用経費が増大することに対して財源的な措置を講じることを政府に申し入れしていることからもわかるとおり、大いに疑義がある。ガバメントクラウドに関連して、すでに莫大な税金・ベンダーの経営資源が投じられている。公共SaaSとして利用を拡大する構想を語る前に、これまでの政策の意思決定過程、費用対効果がしっかりと検証されるべきである。	・自治体のSaaS調達においてISMAPを取得しているものを条件としている団体は多くなく、ISMAPを取得していないSaaSであっても自治体がセキュリティ面の安全性を判断して採用されている現実があります。 ・また、自治体が調達したいSaaSにISMAPを取得してもらいたくとも事業者の資金力や人材不足によりISMAPを取得することが現実的でないケースがあります。 ・上記に鑑み、ガバメントクラウドの開発環境をそのような事業者に提供し、ガバメントクラウドの開発環境上で開発されたSaaSに関してデジタル庁で一定のセキュリティ面を担保することができれば、自治体はセキュリティ面の安全性判断の１つにデジタル庁が担保する部分を利用でき、事業者はボリュームディスカウントなどのあるガバメントクラウド環境で開発できることから、自治体と事業者双方にメリットがあるのではないかということで開発環境の提供を検討しています。 ・もっとも、このデジタル庁で検討しているセキュリティ面の担保はISMAPと同等のものを担保するものではなく、ISMAP取得を調達の要件としている自治体の調達要件をガバメントクラウドの開発環境で開発されたSaaSが満たすものではありません。
2	・価格表が詳細に公開されていることを公共SaaSの条件として記述しているが、一般論として価格表の類は企業秘密に相当する。価格表の公開を要求することは非現実的と言わざるを得ない。	・SaaSの提供価格を公表することは一般的に行われていることであり、価格の透明性を担保し同一SaaSを比較検討する意味でも必要と考えます。
3	・代理店を置いてもよいが、SaaS再販は原則NGとする理由が不明確である。新規参入が非常に厳しくなり、民間企業を不当に縛ることにならないか。競争性・公平性の観点から問題である。 ・ガバメントクラウドに構築されていればクラウドサービス自体がISMAPに登録されていなくてもよいという記述について、ISMAPは取得に時間・金がかかりすぎるという点を先に解決すべきではないか。デジタル庁が担保したことにするというのは、IaaS、PaaS、SaaS事業者に対して今まで時間と資金を投じてISMAP対応することを要求してきたこととの整合性がとれない。	・ガバメントクラウドという公共資産を再販することの是非やCSPの再販ルールを考慮して再販モデルを原則NGとしています。 ・公共SaaSはISMAPを取得した方が好ましいと考えています。その上で、ガバメントクラウドはISMAP登録済のクラウドサービスを採用しており、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境を提供することで、 ISMAP管理策の一部は対象外とすることが可能であり、公共SaaSの円滑なISMAP登録が推進され、行政機関等による公共SaaSの利用が促進されるものと考えています。当該案文もこのように訂正させていただきます。
4	この程度の内容の文書であれば、30日のパブコメ期間を確保できる時期に外に出せたはず。結局国民からの意見を出す機会を制限するつもりか。	本パブリックコメントは法令に基づくものではありません。しかしながら、公共SaaSを利用する機関、提供する機関等の皆様のご意見を広く聴取する目的で実施しているものです。
5	非公開文書の秘密性はどう担保されるのか。公務員以外のものには守秘義務がかからないのではないか。	公共SaaSで取り扱うデータの権利はSaaS利用者である国や地方公共団体等に帰属するものであり、公共SaaSの提供する機能を用いて暗号化やアクセス権の管理をSaaS利用者が行います。当該データへのアクセス制御、暗号化処理、守秘義務等の利用者が必要とする事項についてはSaaS事業者とSaaS利用者との間の契約により担保されていくものと考えます。
6	ガバメントクラウドにおける公共SaaSの整備方針を読みました。民間事業者の立場から以下コメントします。 セキュリティ面での懸念点があります。まず、ガバメントクラウド上に構築された公共SaaSについては「当該SaaSがISMAPを取得していなくともセキュリティ上のリスクが低いことをデジタル庁として担保する」という記述が9ページにあります。ISMAPは政府情報システムのセキュリティ確保のための重要な枠組みであり、これを簡易化する方針は危険です。 クラウド基盤がISMAP認証済みであっても、その上に構築されるSaaSアプリケーション自体のセキュリティリスクが低減されるわけではありません。アプリケーション層の脆弱性、アクセス制御の不備、APIセキュリティなどは依然として課題となります。 また、11ページの「閉域網に依存しない（インターネットからの利用を前提とした）セキュリティ対策」について当面は現行のガバメントクラウド接続方式でも可とする注釈がありますが、これはセキュリティモデルの一貫性を欠く可能性があります。 さらに、府省庁運営型と民間事業者運営型の2つの運営形態が示されていますが、セキュリティインシデント発生時の責任分界点が明確になっていません。特に12-13ページの契約・支払いスキーム図ではSaaS事業者と制度官庁間の監督関係は示されていますが、セキュリティ監査や脆弱性対応の責任体制については触れられていません。 公共SaaSの定義として共通環境（マルチテナント）を原則としている点も、テナント間のデータ分離不備によるリスクが考えられます。データの分離が技術的に確実に担保される仕組みや監査体制についても言及すべきでしょう。 民間事業者向けの公共SaaS選定および提供プロセスにおいても、セキュリティ監査や脆弱性対応の要件を明確にし、最低限満たすべきセキュリティ基準を設けるべきと考えます。	・公共SaaSはISMAPを取得した方が好ましいと考えています。その上で、ガバメントクラウドはISMAP登録済のクラウドサービスを採用しており、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境を提供することで、 ISMAP管理策の一部は対象外とすることが可能であり、公共SaaSの円滑なISMAP登録が推進され、行政機関等による公共SaaSの利用が促進されるものと考えています。当該案文もこのように訂正させていただきます。 ・閉域網に依存しないセキュリティ対策をとることは、ゼロトラストのみに依存するのではなく、また、境界型セキュリティとの組み合わせは過渡期における一般的なセキュリティ対策と考えます。 ・セキュリティインシデント発生時等の責任分界については、責任共有モデルを前提に、利用者（テナント）、SaaS事業者、ガバメントクラウド、各CSOが各々の責任範囲を中心に密に連携し、制度官庁等も含めて対策をとる前提です。今後、整備を進めてまいります。 ・テナント間のデータ分離については、論理分離、物理分離も含めて各SaaS事業者に広めの選択肢を提供して競争環境の醸成を図りつつ、利用者データの保護を含め、適切なセキュリティが担保されるような審査を実施することを想定しています。
7	1）インデントがおかしかったり、表に空行があったり、項番抜けがあったりします。公文書としてチェックしてないのでしょうか。 2）意見提出の期間が30日未満の理由に、「情報通信技術を活用した行政の推進等に関する法律の一部を改正する法律」（令和七年法律第四号）が令和７年３月８日に施行されることに伴い、令和７年４月より本文書を施行する必要があるため。」と記載がありますが、計画性がないのではないでしょうか。また令和7年4月に本文書を施行する理由を記載すべきではないでしょうか。夏休みの宿題みたいに間に合わせるために無理やりこなした感があるのはどうかと思います。 3）本文書の建て付けについて、教えてください。法令等ではない様に見えます。通達、告示等法的には、何に値するものなのでしょうか。	ご意見ありがとうございます。当該文書は、ガバメントクラウドにおけるGCAS（ガバメントクラウドアシスタントサービス）ガイドの一部になります。
8	この意見は、私が所属する組織とは関係のない、個人としての意見です。 8ページから9ページにかけての、「ガバメントクラウドの開発環境で整備された公共SaaS については当該 SaaS が ISMAP を取得していなくともセキュリティ上のリスクが低いことをデジタル庁として担保することで、行政機関等が当該公共 SaaS を採用しやすくできないかを検討中 。」という記載ですが、内閣サイバーセキュリティセンター（NISC）が「政府機関等のサイバーセキュリティ対策のための統一基準群」において、「クラウドサービスの選定基準については、ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト （以下「ISMAP 等クラウドサービスリスト」という。）から選定する」と記載されております。 そのため、デジタル庁が「行政機関等が当該公共 SaaS を採用しやすくできないかを検討」するとありますが、検討の主体はNISCが統一基準の改正を通して行うものであり、デジタル庁が行うものではありません。 また、NISCの見解は、サスの基盤であるクラウドサービスがISMAP 等クラウドサービスリストに掲載されていたとしても、サスそれ自体もISMAP 等クラウドサービスリストに掲載されるか、ISMAP管理基準を全て満たす必要があります。そのため、ガバメントクラウド上に整備することで、デジタル庁において統一的なセキュリティ統制がとられていることは、何ら意味を持ちません。 従いまして、「ガバメントクラウドの開発環境で整備された公共SaaS については当該 SaaS が ISMAP を取得していなくともセキュリティ上のリスクが低いことをデジタル庁として担保することで、行政機関等が当該公共 SaaS を採用しやすくできないか」をデジタル庁が検討することは、反対いたします。	公共SaaSはISMAPを取得した方が好ましいと考えています。その上で、ガバメントクラウドはISMAP登録済のクラウドサービスを採用しており、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境を提供することで、 ISMAP管理策の一部は対象外とすることが可能であり、公共SaaSの円滑なISMAP登録が推進され、行政機関等による公共SaaSの利用が促進されるものと考えています。当該案文もこのように訂正させていただきます。
9	＞令和６年度において、ガバメントクラウドとして利用できるクラウドサービスはアマゾン ウェブ サービスジャパン合同会社の Amazon Web Services（以下「AWS」という。）とグーグル・クラウド・ジャパン合同会社の Google Cloud、日本マイクロソフト株式会社の Microsoft Azure（以下「Azure」という。）、日本オラクル株式会社の Oracle Cloud Infrastructure（以下「OCI」という。）となる。このほか、さくらインターネット株式会社のさくらのクラウドについては、令和7 年度末までにガバメントクラウドとしての技術要件を満たすことができれば利用可能となる この部分であるが、何故他のクラウドサービスがガバメントクラウドとしての技術要件を満たしていないのか、一例をあげて詳述すべきと考える。 出来ているものだけとりあげるのは、ともすると利益相反とも解釈可能である。見解を詳述願う。	公共SaaSではなくガバメントクラウド全体へのご意見は本パブリックコメントの対象外となりますので、ご理解願います。

No	御意見の概要	御意見に対する考え方
10	１）以下の記載があるが、何を言いたいのか理解できないので、いいたいことをきちんと書いた方がよいと思います。 Ｐ９　特定機能（粒度の大きいマイクロサービス）を提供する共通サービスも対象とする。 ２）以下ガバメントクラウド上に整備されたSaaSであるからセキュリティ上のリスクが低いとすることをデジタル庁が担保することが立証できてから、記載してはどうか。SaaS化したい熱い思いは伝わるが、現時点でできることとそうでないことを混ぜて書いてしまうのはミスリードを生みかねない。 P9-P10 ガバメントクラウドは ISMAP 取得済のクラウドサービス（IaaS、PaaS）であり、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境で整備された公共SaaS については当該 SaaS が ISMAP を取得していなくともセキュリティ上のリスクが低いことをデジタル庁として担保することで、行政機関等が当該公共 SaaS を採用しやすくできないかを検討中 。	１）共通サービス、共通機能として業務システムよりも規模の小さいもの（特定の認証機能や支払機能等）を想定しています。 ２）公共SaaSはISMAPを取得した方が好ましいと考えています。その上で、ガバメントクラウドはISMAP登録済のクラウドサービスを採用しており、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境を提供することで、 ISMAP管理策の一部は対象外とすることが可能であり、公共SaaSの円滑なISMAP登録が推進され、行政機関等による公共SaaSの利用が促進されるものと考えています。当該案文もこのように訂正させていただきます。
11	公共SaaSに存在する不確実性によるリスク及び利用権付与兼債務引受契約（仮称）の法的構成に関する要望（意見） 1.公共SaaSに存在する不確実性によるリスクについて 　公共SaaSにおいて省庁等と事業者はともに情報システム整備運用者として位置づけられるが、情報システム整備運用者としての責任分界が本文書では十分に定義されていない。このままであれば、サービス開始当初には予見しなかった運用業務を省庁等ではなく事業者が行うとデジタル庁において整理されるなど、事業者の責務が予見不可能な形で加重されるリスクがある。また、事業者はシステムの開発、構築または運用及びシステムに係る営業が本業であることから、情報システム整備運用者であれば行うべきシステム外の業務がなにか、どれが事業者の責務であるかを過去の業務経験からは判断できず、思わぬ負担が生じるリスクがある。そのため、デジタル庁においては、責任分界を明確にするガイドラインの作成等の対応を行うことを要望する。 なお、事業者によっては本文書の内容限りで受注可能と判断するところがあるかもしれないが、事後的に責務が発生するリスクを回避し、ガバメントクラウドを利用しないと判断する事業者が多くなる※と考えられる。 ※ガバメントクラウドを利用しない事業者が多い実例として、自治体窓口システムの母数に対してガバメントクラウドの利用が必須である自治体窓口DXSaaSのシステム数が少ないことがあげられる。 2. 利用権付与兼債務引受契約について ガバメントクラウド利用料の国に対する支払いは、利用権付与兼債務引受契約（仮称）に基づく債務の履行という法的構成から、事業者が適切に利益をのせられない恐れがある。すなわち、事業者から国へのガバメントクラウド利用料の支払い業務（以下「本業務」）は、法的構成にかかわらず本質的にはテナントに代行してガバメントクラウド利用料を国に納付する業務であるところ、営利企業が行う有償契約であるにもかかわらず、テナントの支払い代行という便宜供与を片務的に負うが、納付すべきガバメントクラウド利用料は決まっているため事業者には利益が出ないという位置づけになる懸念がある。そのため、デジタル庁においては、本業務において事業者が実費を超えて利益をのせてよいと位置づけるか、あるいはテナントによるガバメントクラウド利用料の支払いに関する契約を事業者とテナントとの間で行うことを許す（例えばテナントにより履行引受があることを排除しない）か、あるいは情報システム整備運用者の責務から本業務を外す選択ができることを要望する。	1　セキュリティインシデント発生時等の責任分界については、責任共有モデルを前提に、利用者（テナント）、SaaS事業者、ガバメントクラウド、各CSOが各々の責任範囲を中心に密に連携し、制度官庁等も含めて対策をとる前提です。今後、整備を進めていきます。 2　ガバメントクラウド利用料はSaaS事業者の経費の一つと位置づけており、アプリケーション開発やSaaS運用等で発生する人件費も含め、全体的な経費に健全な事業に必要な適切な利益を加えてSaaS利用料が構成されると考えています。
12	閉域網に依存しない（インターネットからの利用を前提とした）セキュリティ対策が取られること というのは、インターネット接続を認めるということでしょうか。インターネット接続は、現在の閉域網に多額のコストを払っている自治体の要望と合致する部分は大きいです。 ただ、インターネット接続を認めるのであればセキュリティリスク回避のため、NISTのゼロトラストアーキテクチャに基づいたインターネット接続の明記が必要ではないでしょうか。 接続に当たっては、ゼットスケーラー(株)の・Zscaler Private Accessのような、 従来のVPNのような攻撃表面が露出しないZTNA製品を選定することが重要でしょう。JAXAや各地の病院でもVPNインシデントが続出しています。 そもそも、現在従来型の3層分離を堅持することがコスト増・セキュリティリスク増大を招いているのではないかと考えます。	・ガバメントクラウドの各CSP環境にはインターネット接続が可能です。ガバメントクラウドにどのような接続環境を利用するかの判断は各利用者の遵守すべきルールによるものと考えます。 ・その上で、閉域網に依存しないセキュリティ対策をとることは、閉域網に強く依存したセキュリティ対策を強化するものであり、直ちに閉域網に閉じた運用を否定するものではありませんが、将来において、セキュアなクラウドに処理とデータを集約し、ゼロトラストを採用することで、閉域網に依存しないセキュリティ対策は可能と考えます。
13	（１）共通 SaaS（パターン A）の府省庁（国営）は無償以外は成立しない。原則とあるが、例外として有償でaaS利用者である地方公共団体から国がSaaS利用料を徴収することは出来ない。 　共通 SaaS（パターン A）の府省庁（国営）の資料に『有償の場合、請求支払の方法、利用契約の要否等は法整備も含めて主管府省庁が独自に設定・運用する』と記載がございますが、法整備も含めて主管府省庁が独自に設定しても、地方公共団体が国に歳出する費目はございません。そのため、地方公共団体から国がSaaS利用料を徴収することは出来ない。 　仮に、法整備も含めて主管府省庁が独自に設定・運用し、SaaS利用者である地方公共団体が日本政府の口座（日本銀行の口座）に入金（現行、地方公共団体の歳出の費目はない）したとしても、その金額が財務省によって、SaaS運営主体の主管府省庁に充当されることはない。その理由は、財源・予算の制度上、ミシン目の無い日本政府の口座に入金されたとしても、SaaS利用者である地方公共団体から徴収されたSaaS利用料の金額がいくらであっても、SaaS運営主体の主管府省庁は、共通 SaaS（パターン A）で整備したシステムの保守・運営費用の金額を財務省に対してデジタル庁一括計上予算にて予算要求することが必要となります。 　以上のことから、共通 SaaS（パターン A）の府省庁（国営）において、SaaS利用者である地方公共団体が主管府省庁に対してSaaS利用料を支払うことは、法整備も含めて主管府省庁が独自に設定・運用しても出来ない。共通 SaaS（パターン A）の府省庁（国営）の記載では、有償の場合は記載は不要と考えます。それとも、主管府省庁が作成する標準仕様書ごとに特別会計を行うということでしょうか？	公共SaaSは利用者（テナント）として地方公共団体だけでなく、府省庁、独立行政法人等も想定しております。
14	以下に、詳細な技術仕様は別途整理する。を参照されたいとあります。（日本語もおかしそうですが）どのような内容が、どのような粒度で、どのような立ち位置（リファレンスなのか、告示・基準等なのか）で示されるか教えてください。 また、「令和７年４月より本文書を施行する」との記載がありますが、詳細な技術仕様もなく、本文書は現実的に効力を発揮するのでしょうか。 P10 3.3公共SaaSにおける共通要件 公共SaaSにおける共通要件は、以下のとおりとする。なお、詳細な技術仕様は別途整理する。を参照されたい。	公共SaaSの要件については、詳細な技術仕様を別途、GCASガイドにおいて公開する予定です。審査に関する内容を主としてSaaS運営主体向けに記述する方針です。

No	御意見の概要	御意見に対する考え方
15	ガバメントクラウドの施策方向性に関しては、以下の観点で取組むこと（今回及び今後も／環境変化ない限り）： １）サイバー空間は情報資源及び情報セキュリティの基盤となることから、サイバー空間とガバメントクラウドの安全性の確保と国家安全保障の観点から施策の立案とクラウド・情報技術開発を行うこと ２）地政学的・安全保障の観点から、ガバメントクラウドの国産化と外部依存率の低減を検討すること（海外に運営の重要部分のたづなを握られることなく主導権を確保し、生存及び安全保障優位性を確保すること） ３）サイバー空間とガバメントクラウドの利便性等についてはIT競争力上位に位置する国のIT競争力環境と対他比較を行い、施策立案及び情報技術開発を行うこと ４）国産のIT開発ベンダーの育成と国際的競争力向上を検討すること ５）情報技術の変化スピードは法制度整備よりも変化が速いので、環境変化に機敏に柔軟に対応できるようなガバメントクラウド等に関する法制度・社会システムを整備し前提とすること ６）ガバメントクラウド及び地方自治体との連携等については、利用者の視点からは行政縦割・たこつぼ化をできる限り排除するとともに、情報セキュリティの観点から情報アクセスできる範囲と取扱者は制約をかけ、利便性と情報セキュリティの両立を図ること ７）ＩＴ技術開発・デジタル技術に長けた人材の育成を強化すること、教師側・管理職側のＩＴスキルの向上施策も併せて検討実施すること ８）投入開発費を回収する視点及び何重にも及び下請け構造はできる限りシンプルにし、ガバメントクラウド・情報技術開発成果に対する投資対効果を図り投資回収を行うこと ９）ガバメントクラウドの利便性等は定期的にユーザー及びガバメント使用者のアンケート実施を行い、必要機能は定期的に見直すこと	公共SaaSではなくガバメントクラウド全体へのご意見は本パブリックコメントの対象外となりますので、ご理解願います。
16	【ISMAP,ISMAP-LIU取得済みのSaaSに基盤として特定のクラウドサービス利用を要件とすることの是非について】 ■指摘箇所 p.10 ＞１．基本要件 ＞・ガバメントクラウド上で稼働すること ■意見 対象のSaaSがISMAPやISMAP-LIUに登録されたクラウドサービスそのものである場合は、基盤も含めて安全性が評価されているのであるから、基盤にガバメントクラウドやISMAP登録のクラウドサービス（IaaS/PaaS）を利用するなどの基盤を制約する要件は必要ないのではないか。	本文書はガバメントクラウドを利用して提供される公共SaaSについて規定するものです。ガバメントクラウドを利用しないSaaSを制約するものではありません。
17	【ガバメントクラウド上に整備されたシステムのセキュリティについて】 ■指摘箇所 p.9-10 ＞ガバメントクラウドの開発環境で整備された公共SaaSについては当該SaaSがISMAPを取得していなくともセキュリティ上のリスクが低いことをデジタル庁として担保することで、行政機関が当該公共SaaSを採用しやすくできないかを検討中。 ■意見 ガバメントクラウドのCSPにより提供されるIaaS/PaaSは、責任共有モデルにおいてセキュリティの責任についてもCSPが提供し利用者によって利用されるIaaS/PaaSサービスの機能の範囲内に限定している。その上にSaaS事業者が構築するソフトウェアや設定についてはそのSaaS事業者が責任をもって担保するものであってガバメントクラウドのCSPの責任は及ばないため、「ガバメントクラウドの開発環境で整備された公共SaaSについては当該SaaSがISMAPを取得していなくともセキュリティ上のリスクが低い」とする理屈は成り立たない。 ISMAPのFAQでも「ISMAP管理基準では、ガバナンス基準、マネジメント基準をはじめとする多くの管理策への対応を、SaaSを提供する事業者自身が行う必要があることから、ISMAPに登録されているサービスと同等とみなすことはできません。」と説明されており、この考え方はISMAPではなくガバメントクラウドの置き換わったからといって変わるものではない。	公共SaaSはISMAPを取得した方が好ましいと考えています。その上で、ガバメントクラウドはISMAP登録済のクラウドサービスを採用しており、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境を提供することで、 ISMAP管理策の一部は対象外とすることが可能であり、公共SaaSの円滑なISMAP登録が推進され、行政機関等による公共SaaSの利用が促進されるものと考えています。当該案文もこのように訂正させていただきます。
18	【モダン化を要件としてSaaS運営主体が利用する技術を制約することの是非について】 モダン化をしているかどうかはSaaS事業者の競争領域とするべきであり、モダン化することで競争力が向上するのであれば淘汰的にそうなっていくものである。国が事業者が利用する技術を制限すれば、より革新的な技術の活用を阻害する恐れがある。マネージドサービスとして提供されていない技術を活用して高度なセキュリティや運用の自動化が行われることも十分に考えられるため、その利用を排除するべきではない。デジタル庁においては、クラウドサービス事業者の提供するマネージドサービスがモダン技術であると主張する情報発信が見受けられるものの、それではガバメントクラウドのCSPが提供するサービスしか利用できないという制約となり、また仕様やAPIが標準化され複数のサービスで実装されていないマネージドサービスの利用はクラウドロックインにも繋がる。採用技術についてデジタル庁の過度な干渉は控えるべきである。	ガバメントクラウドを通じて大規模災害時の円滑な対応、セキュリティレベルの均一的な向上、コスト最適化などを実現するためには、システムアーキテクチャのモダン化や運用のモダン化が必要と考えております。求められるモダン化の程度は利用者や業務特性等によっても変わり得るものであり、本文書の内容を満たした上でどの程度モダン化するかはご指摘のとおりSaaS事業者の競争領域と考えますので、技術における過干渉とならないよう留意しつつモダン化の具体的な技術方針を適宜更新していく所存です。

No	御意見の概要	御意見に対する考え方
19	【公共SaaSの利用規約・プライバシーポリシーについて】 民間事業者が運用する公共SaaSを自治体が調達し、そしてそれを住民が利用してその個人情報を預ける場合、住民は自治体が適切に個人情報を扱うことを期待する。すべての利用規約やプライバシーポリシーを読んで理解した上で同意する住民はほとんど存在しないと考えられる。また公共サービスを受ける上で公共SaaSの利用が必要であれば、利用規約に同意せざるを得ないことになる。しかし、実際に個人情報を管理するのは公共SaaSの運用主体となる民間事業者であり、営利目的のために個人情報を利活用しようとすることは容易に想像できる。 公共SaaSの利用規約やプライバシーポリシー、および住民の同意取得方法に規定を設けるなど、住民が想定しない形で民間事業者に個人情報が扱われることを防止するための仕組みが必要なのではないか。	公共SaaSは自治体の業務のみを対象にしたものではありませんので、住民情報を扱う自治体向け公共SaaSに特化したルールは、公共SaaS全体ではなく、業務標準を管理する制度官庁や個々のSaaS事業者、調達する自治体で設定されるものと想定しています。 また、ご指摘いただいた課題は公共SaaSに限定されるものではなく、従来型のシステムでも本質的には共通のものであり、公共SaaS化することでガバナンスを効かせやすくなる可能性が高まると考えています。
20	【アーキテクチャ要件として好ましい/好ましくないとされる基準について】 ■指摘箇所 p.11 ＞4．アーキテクチャ要件 ＞好ましくないシステム構成等はリファレンスアーキテクチャとしてお示しする予定である。 ■意見 好ましくないとするアーキテクチャについては公共SaaSとして認められないとするのであれば、好ましい/好ましくないの基準とその根拠を明確にして広く議論されるべきではないか。	好ましくないシステム構成としては、SaaSとしての管理機能（認証、テナント管理、利用量計測、ヘルスダッシュボード、課金管理等）を有さないものを現時点で想定しており、自治体システム関係者と広く意見交換を行っております。
21	【販売代理店のモデルに対する制約について】 ■指摘箇所 p.13 ＞・SaaS販売代理店を置くことは想定するが、再販モデルではなく販売手数料モデル（直接契約）を原則とする ■意見 再販モデルには、代理店が提供するサポート等によりSaaS利用者の負担を減らす、リソースに限りのあるSaaS事業者の負担を軽減しビジネスをスケールさせやすくなる、といったメリットがある。自治体相手のビジネスに不慣れなスタートアップ等の企業がSaaS事業者となる場合、自治体業務に詳しい販売代理店が挟まることで自治体の事情に合わせた顧客サポートができ、またSaaS事業者に対して適切なフィードバックが得られることも考えられる。これを認めないことはビジネスモデル上の工夫の余地をなくすことにも繋がるのであって、制限をかけるべきではないのではないか。	公共SaaSにおいても販売代理店の役割は重要と考えています。ガバメントクラウドという公共資産を再販することの是非やCSPの再販ルールを考慮して再販モデルを原則NGとしています。
22	【モダン化を要件とすることの是非について】 ■指摘箇所 p.12 ＞ガバメントクラウド（IaaS/PaaS）上で、ガバメントクラウドの要求するモダン化されたアプリケーションを開発し、公共SaaSの要件を満たす必要があることに留意されたい。 ■意見 デジタル庁においてはクラウドサービスが提供するマネージドサービスを多用する構成をモダン化した構成としてSaaSに求めると考えられるが、モダン化を進めるために必要なクラウド経験の豊富な技術者、高度なクラウド資格を持つ技術者のリソースが逼迫することでかえってコストが上昇する可能性もある。オンプレミスやプライベートクラウドで使われる仮想化技術も進化している中で、ガバメントクラウドのCSPが提供するマネージドサービスに拘泥することはむしろ足枷になり得る。 また、ガバメントクラウドとして最も採用されているCSPであるAWSによれば、モダナイゼーションはPeople, Process, Technologyの3つの柱から成り立っている。デジタル庁の説明するモダン化の用語定義においては、現場の課題理解やPeople（組織や文化含む）、Processの観点が抜け落ちており、その価値を享受することは難しいと理解すべきである。またTechnologyについても、AWSも最新技術の採用が正解とは限らないと説明している	ガバメントクラウドを通じて大規模災害時の円滑な対応、セキュリティレベルの均一的な向上、コスト最適化などを実現するためには、システムアーキテクチャのモダン化や運用のモダン化が必要と考えております。求められるモダン化の程度は利用者や業務特性等によっても変わり得るものであり、本文書の内容を満たした上でどの程度モダン化するか、またSaaSの価格設定をどうするかについてはSaaS事業者の競争領域と考えて対応することを考えております。
23	p.12,13 ＞契約・支払スキーム案 ■意見 ガバクラのアカウント払い出しはデジタル庁からSaaS運営主体あるいはSaaS事業者に対して行われることになっているが、SaaS上で扱われる個人情報の一元管理を避けるためには、デジタル庁がSaaSのテナントにアクセスできないことが保証されなければならない。プライバシーに配慮して運用されていることを広く国民に示すために、デジタル庁によるテナントへのアクセスを制限する技術的・制度的・運用的な対策について詳細な説明を公開するべきである。	公共SaaSで取り扱う業務データは利用者のものであり、デジタル庁がアクセスし利用することはありません。

No	御意見の概要	御意見に対する考え方
24	【モダン技術の定義に価格設定を含めることの是非について】 ■指摘箇所 p.6 ＞表1-1 用語の定義「モダン技術」 ＞十分に普及した（簡単に購入可能で、価格もアフォータブルな）新しい技術のこと。ただし、研究室レベルの最先端技術は含まない。 ■意見 モダン技術の用語定義にある「十分に普及した（簡単に購入可能で、価格もアフォーダブルな）新しい技術」について、価格設定はそのサービス・製品を販売する事業者によって決められるものであって、技術そのものの性質とは別の論理で決められるものであるため、価格設定をその定義に含むべきではない。 また、クラウドサービスとして提供される場合は従量課金になるので、利用量が多ければ高くなりそうでなければ安くなるということになり、利用の仕方によって高いかアフォーダブルかの判断も異なってくることになる。 上記のように価格がアフォーダブルであるとする基準が明確ではないため、この定義によってモダン技術を特定することは困難である。	研究室レベルの最先端技術ではないことを示すために、（簡単に購入可能で、価格もアフォーダブルな）という説明は有効と考えています。 なお、単に安ければよいという趣旨ではなく、「合理的な説明が可能な価格」という趣旨となります。 モダン化の詳細な説明については、GCASガイドで記載しています。 https://guide.gcas.cloud.go.jp/general/overview-explanation-chapter-06/
25	【ガバメントクラウドの要件の検討経緯の妥当性およびその要件が満たされていることの担保について】 ISMAP制度についてはその総務省やISMAP運営委員会の検討会において検討が重ねられて策定および見直しがされたものであり、その管理基準を満たしているかどうかについても第三者の監査機関によって監査している。一方でガバメントクラウドの要件については検討経緯が公開されておらず、その要件の根拠も示されていなければ、その要件が満たされているかどうかをどのように確認しているのかどうかも不明である。実際に各CSPがガバメントクラウドの一部の技術要件を満たせていない。 例えばガバメントクラウドの技術要件には「情報資産は国外に持ち出さない」という要件があるが、認証認可に用いられるIAMのサービスについてはそのデータ（ユーザやロール、ポリシーといったリソース）の原本がバージニア北部に格納され、コントロールプレーンとして運用されている、など。認証認可に係る情報は当然ながらセキュリティ上重要な情報資産である。 ガバメントクラウドとして提供されるクラウドサービスが、ガバメントクラウドの技術要件を満たしていることを定期的に確認する仕組みがなければ、ガバメントクラウドのセキュリティが高いということも担保できないのではないか。 デジタル庁として、どのようにしてガバメントクラウドの技術要件を策定したのかおよびその根拠、またガバメントクラウドとして調達されたクラウドサービスにおいてその要件が満たされていることをどのように確認しているのか、公表すべきではないか。	公共SaaSはISMAPを取得した方が好ましいと考えています。その上で、ガバメントクラウドはISMAP登録済のクラウドサービスを採用しており、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境を提供することで、 ISMAP管理策の一部は対象外とすることが可能であり、公共SaaSの円滑なISMAP登録が推進され、行政機関等による公共SaaSの利用が促進されるものと考えています。当該案文もこのように訂正させていただきます。 また、公共SaaSではなくガバメントクラウド全体へのご意見は本パブリックコメントの対象外となりますので、ご理解願います。
26	【クラウドサービスのオペレーターについての米国GovCloudとの違いについて】 米国のAWS GovCloudではそのオペレーターが米国内に居住する米国市民であることなどのスクリーニングが行われているが、日本のガバメントクラウドについてはオペレーターに対する要件が設けられていない。安全に公共サービスを実現する情報システムを運用するためには、ガバメントクラウドについてもセキュリティクリアランス制度を導入する必要があるのではないか。公共SaaSの基盤にガバメントクラウドを利用することを要件とするのであれば、米国GovCloudで設けられているオペレーターのスクリーニングが日本では設けられていなくても問題ないとする根拠や考え方を示していただきたい。	公共SaaSではなくガバメントクラウド全体へのご意見は本パブリックコメントの対象外となりますので、ご理解願います。
27	【公共サービスを実現するシステムのSaaS化を進めることの是非について】 ■指摘箇所 p.1 ＞約1,800の地方公共団体がそれぞれ個別にアプリケーションを整備していくことは必ずしも持続可能とは言えず、システムを所有から利用へと転換するSaaS利用を前提とし、その利点を最大限にいかすため、できる限りその利用規模を拡大していくことが求められる。 ■意見 民間の事業者がシステムを所有し提供するSaaSにおいては、事業者側の都合によりサービスの提供終了や提供価格・仕様の変更などが行われる恐れがあり、それらに対する利用者側のコントロールが困難になる。サービスを持続的・安定的に提供されることが求められる場合については、むしろ行政機関等が所有することも合理的な判断として認められるべきであり、「できる限りその利用範囲を拡大していく」ことは適切な方針とは言えない。 なお、約1800の地方公共団体がそれぞれ個別にアプリケーションを整備していくことは持続可能ではないとの記載があるが、実際には多くの自治体向けシステムはいくつかのパッケージに集約されるのであって、現状認識が正しくないのではないか。	自治体向けに必要と想定される内容はSaaS事業者の約款等で示され、自治体側の必要な要件は調達仕様で示されると考えています。ご指摘の課題は公共SaaSだけでなく従来型のパッケージシステムでも本質的には共通の課題と考えます。 また、自治体のシステムを公共SaaSのみとすべきとは考えておらず、様々な形態が併存するなかで、最適化されていくものと考えます。
28	【ガバメントクラウドのサービス提供が停止されることを想定した対策について】 米国企業の技術について米国政府が外交上の交渉材料として提供を停止する、あるいは米国企業の経営判断として日本から撤退するという可能性があるのではないか。公共SaaSにガバメントクラウドを基盤とすることを要求する場合、米国企業のクラウドサービスが上記のような理由で停止されることとなると、一斉に米国企業により提供されるクラウドサービスから国内のクラウドサービスに移行をしなければならなくなる。このような場合に、国や自治体でガバメントクラウド上に構築されたシステムも含めて、クラウド基盤の変更にどの程度の期間とリソースが必要になるのか試算し、対策を検討しておくべきではないか。 なお、「デジタル庁のガバメントクラウド整備のためのクラウドサービスの提供（令和5年度募集）」の調達仕様書によると、CSPは原則として1年前までにデジタル庁に通知をすればペナルティなくクラウドサービスの廃止や契約の終了をできることになっているようであるが、例えばAWSがサービス廃止や契約終了を申し出た場合、1年で公共SaaSや国や自治体のシステムをAWSから別の基盤に移行させるのは現実的ではないと思われる。	公共SaaSではなくガバメントクラウド全体へのご意見は本パブリックコメントの対象外となりますので、ご理解願います。

No	御意見の概要	御意見に対する考え方
29	【モダン化を強制することの是非について】 ■指摘箇所 p.6 ＞表1-1 用語の定義「モダン技術」 ＞十分に普及した（簡単に購入可能で、価格もアフォータブルな）新しい技術のこと。ただし、研究室レベルの最先端技術は含まない。 ■意見 ITの分野においては、ある程度登場してから年数が経った技術はいわゆる「枯れた技術」と呼ばれ、それを使用することはセキュリティ上好ましいとされる場合がある。長く使われることによってバグが修正されて品質が安定しており、また利用者側にも運用ノウハウが蓄積していることから、特に安定稼働や機密性といった高い信頼性やセキュリティが求められる公共システムにおいてはこういった「枯れた技術」を選択することは理にかなっている場合も多く、公共SaaSとしてモダン技術（新しい技術）でなければ認めないとするような要件は適さないのではないか。	適材適所で「枯れた技術」を利用することは当然と考えています。ソースコードレベルであれば、オープンソースでもマネージドサービスでも多用されていますし、モダン化を前提にアプリケーションを開発する際にも活用可能な場所は少なくないと考えます。しかしながらアーキテクチャレベルでの「枯れた技術」の採用には慎重であるべきと考えています。
30	【ガバメントクラウド上で稼働をすることを要件とすることの是非について】 ■指摘箇所 p.10 ＞１．基本要件 ＞・ガバメントクラウド上で稼働すること ■意見 民間向けに既にSaaSを提供している事業者からすると、それをCOTS(Commercial Off-The-Shelf)として公共SaaSに展開する場合、ガバメントクラウドに新たにシステムを構築して二重に運用する必要が出てくるため大きな負担となる。基盤としてISMAPに登録されたクラウドサービスを利用することを求めるだけであれば、元々ISMAP登録のクラウドサービスを利用しているスタートアップであれば二重の運用は必要ないため、運営事業者の負担も軽減され、サービスの提供や運用にかかるコストも低減できるのではないか。	民間向けに既に提供されているSaaSであれば、公共・準公共に特化したものではないので、公共SaaSの対象外と考えます。
31	【データの管理権について】 ■指摘箇所 p.10 ＞１．基本要件 ＞・データの管理権がテナントにあること ■意見 データの管理権がテナントに与えられたとしても、SaaSの運営主体もその権限を保有することになる。 （データを格納し取り出すだけのストレージサービス以外の）SaaSは原理的にエンドツーエンドの暗号化は実現し得ないことを考慮すると、ガバメントクラウドのCSPもまたデータを覗き見ることができることも理解すべきである。BYOKで暗号化しようとも、CSP施設内のネットワーク上のすべての経路あるいはメモリ上で暗号化されているわけではなく、またデータの暗号化/復号に使われる鍵もCSPがその気になればアクセスが可能である。 例えばAWSにおいてはデータ暗号化/復号のためのキーを暗号化/復号するCMK（カスタマーマスターキー）はFIPS 140-2セキュリティレベル3のHSMにて管理されているとされておりその運用についてISMAPの管理基準への対応状況が説明されているが、直接データの暗号化/復号に用いられるCDK（カスタマーデータキー）については平文の状態でHSMの外で扱われる。CDKは平文の状態で永続化されないとされているもののHSM外で扱われるためにAWSがそれを窃取できないことを保証できないし、その運用についてISMAPの管理基準への対応が説明されていない（AWS Artifactよりダウンロードできる ISMAP Customer Packageにて説明されていない）。CDKによって暗号化される前/復号後の平文の業務データもAWS施設内で扱われることになりそれに対する盗聴を防ぐこともできない。 また、暗号化の有無に関わらずCSPは自社クラウドサービス上に構成されたシステムやデータの削除が可能である。実際、昨年にはオーストラリアの年金基金であるUniSuperにおいてGoogle Cloudの過失によりアカウントごと、別リージョンのバックアップも含めてデータが削除されるというインシデントが発生している。 特に住民の個人情報を扱う公共SaaSにおいて、上記のようにSaaSの運営主体や外国企業であるCSPがデータの盗聴や削除が可能な状態で管理されることについて、広く議論するべきではないか。	公共SaaSではなくガバメントクラウド全体へのご意見は本パブリックコメントの対象外となりますので、ご理解願います。
32	【モダン技術の定義に技術の新しさを含めることの是非について】 ■指摘箇所 p.6 ＞表1-1 用語の定義「モダン技術」 ＞十分に普及した（簡単に購入可能で、価格もアフォータブルな）新しい技術のこと。ただし、研究室レベルの最先端技術は含まない。 ■意見 モダン技術の定義として「新しい技術」という表現があるが、新しい技術とするにあたっての基準がなく何がモダンなのかが不明確である。 例えばAWSで提供されている運用監視等に用いられるマネージドサービスであるAmazon OpenSearch ServiceはOSSであるApache Luceneをマネージドサービス化したものであるが、Apache Luceneは2000年に1.0版がリリースされており、AWSのようなクラウドサービスが世に出る前から存在する比較的歴史の長い技術であると言える。また、NoSQLの一種であるAmazon ElastiCacheの基になっているmemcachedは2003年から開発され実用されていた。Amazon RDSやAmazon Auroraの基になっているRDBMS（PostgreSQL等）は更に長い歴史を持っている。 この用語定義に従えば、新しくはないこれらの技術をマネージドサービスとしたAmazon OpenSearch ServiceやAmazon Autora等はモダン技術ではなく、GCASガイドのリファレンスアーキテクチャにあるようにそれらを使ってシステムを構成することはモダン化と言えないことになるのではないか。	各CSPの個々のサービスについて、どのサービスがモダンであるかという検討は特段行っておりません。リファレンスアーキテクチャとして推奨するシステム構成例を示していますが、ここでも、システム構成上での最適化を優先しています。 また、公共SaaSではなくガバメントクラウド全体へのご意見は本パブリックコメントの対象外となりますので、ご理解願います。

No	御意見の概要	御意見に対する考え方
33	我々は通常のSaaSを運営しており、デジタル庁様や官公庁等でも我々のSaaSを利用していただくために、ISMAP取得を目指しプロジェクトを進めています。DMP（行政自治体と企業をつなぐプラットフォーム）に掲載する予定です。 民間企業で通常のSaaSを運営している視点から見て、大きく2点にに対して疑問・意見があります。 1点目は「公共SaaS」とは何なのか？ドキュメントを見てもよくわかりませんでした。このドキュメントでは下記のような定義されています。 > 国又は地方公共団体等が利用する SaaS（以下「公共 SaaS」という。） > ガバメントクラウドを利用環境として、GCASガイド「ガバメントクラウド利用検討の基本的な考え方」3.2 に規定する「重点計画に記載の公共・準公共分野に該当し、制度官庁が標準仕様を定める情報システム」を SaaSとして構築されたもの。 > 我々は通常のSaaSであり、ガバメントクラウド環境を利用して制度官庁が標準仕様を定める情報システムではありません。通常のSaaSは公共SaaSに当てはまらない理解であっていますでしょうか？その場合、通常のSaaSは官公庁様には利用していただけなくなるのでしょうか？通常のSaaSと公共SaaSの具体的な事例や違いを知りたいです。 また、官公庁利用専用のSaaSを作るのであれば、それはSaaSの活用なのではなく、専用ソフトウェアの開発なのだと思います。今まで状況が変わるのでしょうか？ 2点目は、セキュリティに関する考え方です。 このドキュメントでは公共SaaSのセキュリティについて下記のように書かれています。 > ガバメントクラウドは ISMAP 取得済のクラウドサービス（IaaS、PaaS）であり、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメ	１点目について。 通常のSaaSと公共SaaSは異なるものと考えております。 通常のSaaSを官公庁が利用できなくなるとは全く考えていません。汎用的なSaaSを官公庁が直接利用する場合もあるほか、システムの機能の一部としてSaaSを利用する場合もあると考えます。 また、汎用的な既存SaaSのシステムを流用し公共SaaSの要件にミートさせる形で公共SaaSとして新たに構築されることも可能です。公共SaaS向けに専用ソフトが必要か否かはわかりませんが、公共・準公共に特化していて制度官庁等の業務標準に準拠することが求められます。 2点目について。 公共SaaSはISMAPを取得した方が好ましいと考えています。その上で、ガバメントクラウドはISMAP登録済のクラウドサービスを採用しており、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境を提供することで、 ISMAP管理策の一部は対象外とすることが可能であり、公共SaaSの円滑なISMAP登録が推進され、行政機関等による公共SaaSの利用が促進されるものと考えています。当該案文もこのように訂正させていただきます。
34	さくらインターネット株式会社等の日本企業のクラウドサービスを積極的に採用してください。外資系企業のクラウドサービスばかりでは、外資系企業(外国で)の個人情報関連の規約、法律に則って個人情報が扱われてしまいます。 デジタル赤字を減らす為にも宜しくお願いします。 P.9を参照 令和 6 年度において、ガバメントクラウドとして利用できるクラウドサービスはアマゾン ウェブ サービスジャパン合同会社の Amazon Web　Services（以下「AWS」という。）とグーグル・クラウド・ジャパン合同会社の Google Cloud、日本マイクロソフト株式会社の Microsoft Azure（以下「Azure」という。）、日本オラクル株式会社の Oracle Cloud Infrastructure（以下「OCI」という。）となる。このほか、さくらインターネット株式会社のさくらのクラウドについては、令和 7 年度末までにガバメントクラウドとしての技術要件を満たすことができれば利用可能となる。	公共SaaSではなくガバメントクラウド全体へのご意見は本パブリックコメントの対象外となりますので、ご理解願います。
35	【公共SaaSとしてガバメントクラウドを利用することにより海外の会社にシステム管理のためのIdPを委ねることの是非について】 2025年3月18日に、自民党デジタル社会推進本部長長であり初代デジタル大臣でもある平井卓也氏がSNSで以下の投稿をしている。 「自宅の鍵を海外の会社に作ってもらい、その会社が合鍵を持っているとしたらどうでしょうか？ その会社が信用できるとしても、もし悪意を持った第三者に鍵の情報が渡ったら、自分の家に勝手に侵入されるリスクがあります。これは、サイバーセキュリティの分野でも同様です。今朝のデジタル本部では、中小企業のサイバーセキュリティ対策、人材育成、技術・産業振興について有識者ヒアリングを実施しました。今回指摘されたサイバーセキュリティの国産化は、国家の安全保障や経済の安定にも不可欠です。持続可能なサイバー防衛体制を構築するためにも、人材、技術、産業振興を国産化していくことが重要です。 #平井卓也 #サイバーセキュリティ」 「ガバメントクラウド概要解説」によるとガバメントクラウドへのシングルサインオンにはGCASが使われるが、GCASの内部ではCloud IdentityというGoogle Cloudのサービスが使われており、Google CloudがIDプロバイダー（IdP/IDaaS）として機能する。このIdPで管理されシングルサインオンに使われる資格情報も鍵と表現するに相応しい情報だが、それをGoogle Cloudという海外の会社に預けることになる。たとえガバメントクラウドとしてさくらインターネットを採用したとしても、その環境にログインするためには海外の会社のクラウド上で管理されるユーザーと資格情報を使う必要があるということになる。 そして、IdPを管理する組織（デジタル庁やGoogle Cloud）は、ユーザーを削除/無効化したり、ユーザーを追加したり、ユーザーの資格情報を上書きしてしまうといったことが技術的に可能である。 上記のことから、公共・準公共分野のサービスを実現するシステムにおいて海外企業がクラウドサービスの認証に使うユーザーやその資格情報を管理するガバメントクラウドを採用することは、自民党の考えるサイバーセキュリティの方針に反する恐れがある。	公共SaaSではなくガバメントクラウド全体へのご意見は本パブリックコメントの対象外となりますので、ご理解願います。

No	御意見の概要	御意見に対する考え方
36	【公共SaaSとしてガバメントクラウドを利用することにより海外の会社にデータと鍵を預けることの是非について】 ガバメントクラウドで実際に採用されているCSPとしては海外の会社がほぼ100%であり、国内企業のさくらインターネットは仮認定かつ2025年度末までに全ての要件を満たすことができなければ認定取り消しの恐れがあることを考慮すれば、公共SaaSでガバメントクラウドを基盤として利用することを要件とする場合、実質海外の会社に公共サービスに関するデータを預けることが強制されることになる。 このように海外の会社に公共・準公共分野のサービス、特に国民のデータを預けることは、サイバーセキュリティ上問題になるのではないか。 2025年3月18日に、自民党デジタル社会推進本部長長であり初代デジタル大臣でもある平井卓也氏がSNSで以下の投稿をしている。 「自宅の鍵を海外の会社に作ってもらい、その会社が合鍵を持っているとしたらどうでしょうか？ その会社が信用できるとしても、もし悪意を持った第三者に鍵の情報が渡ったら、自分の家に勝手に侵入されるリスクがあります。これは、サイバーセキュリティの分野でも同様です。今朝のデジタル本部では、中小企業のサイバーセキュリティ対策、人材育成、技術・産業振興について有識者ヒアリングを実施しました。今回指摘されたサイバーセキュリティの国産化は、国家の安全保障や経済の安定にも不可欠です。持続可能なサイバー防衛体制を構築するためにも、人材、技術、産業振興を国産化していくことが重要です。 #平井卓也 #サイバーセキュリティ」 上記の内容はまさにガバメントクラウドに当てはまる内容である。ガバメントクラウドを公共SaaSの基盤として利用する場合、海外の会社が構築したクラウドサービスを利用し、暗号化/復号に用いる鍵は海外CSPが作成した鍵、あるいはBYOK（Bring Your Own Key）という形で海外の会社に預けた合鍵を、海外の会社であるCSPのクラウドサービス上で使用することになる。 公共・準公共分野のサービスを実現するシステムにおいて海外企業のシェアがほぼ100%を占めるガバメントクラウドを採用することは、自民党の考えるサイバーセキュリティの方針に反する恐れがある。	公共SaaSではなくガバメントクラウド全体へのご意見は本パブリックコメントの対象外となりますので、ご理解願います。
37	3.3 公共SaaSの共通条件　の　1.基本要件の二つ目の丸ポチ 民営の場合は業務仕様が制度官庁等の業務標準に準拠していること （業務標準が存在しない場合や共通サービスについては別途、整理を行う ） ＜コメント＞ 内閣官房の「国・地方デジタル共通基盤推進連絡協議会」で検討されている「共通SaaS」との関係を記載いただきたい。	公共SaaSの運営主体が府省庁（国営）の場合は、「国・地方デジタル共通基盤推進連絡協議会」で検討されている「共通SaaS」のパターンAに相当します。 公共SaaSの運営主体が民間（民営）の場合は、同じくパターンBに相当します。
38	9ページあたりで以下のことが述べられている。 「ガバメントクラウドは ISMAP 取得済のクラウドサービス（IaaS、PaaS）であり、デジタル庁において 統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境で整備された公共 SaaS については当該 SaaS が ISMAP を取得していなくともセキュリティ上のリスクが低いことをデジタル庁として担保することで、行政機関等が当該公共 SaaS を採用しやすくできないかを検討中 。」 クラウドはインフラにしか過ぎずその上位層のアプリ制御まで担保することは困難と思慮。審査方法や有限のリソース(職員数など)制限などどのように考えているのか知りたい。	公共SaaSはISMAPを取得した方が好ましいと考えています。その上で、ISMAPに未登録のサービスであってもISMAPの例外規定で利用者がリスクを評価する際に有用な情報を提供することで支援したいと考えています。
39	3.2 公共SaaSの定義の２の３つ目のポチ 自治体共同利用方式における「アプリケーション分離」に概ね分類されるが、システムのモダン化を前提としており、従来の共同利用とは大きく異なる。 ＜コメント＞ 不要な偏見が入っているので最後の一言は削除すべき。 自治体共同利用方式における「アプリケーション分離」に概ね分類されるが、システムのモダン化を前提としている。	従来の共同利用におけるアプリケーション分離との関係性と相違を明記する趣旨の記載となります。

No	御意見の概要	御意見に対する考え方
40	＜対象＞ 1.5 用語の定義 3.1 ガバメントクラウドにおけるSaaS ＜コメント＞ 自治体システム標準化の共同利用型との区別が分かりづらいため、次のように「「標準準拠SaaS（仮称）」など「公共SaaS」の一段上のグループを追加するのはいかがでしょうか。 １．「公共情報システム」の定義 デジタル行政推進法第十八条第一項に規定する 「国又は地方公共団体の事務の実施に関連する 情報システム」のこと ２．「標準準拠SaaS（仮称）」の定義 ・「公共情報システム」のSaaSのうち、 ・制度官庁等が定める標準仕様に準拠（適合確認） するもの ※運営主体は国営、又は民営（独立行政法人等含む） ３．「公共SaaS」の定義 ・「標準準拠SaaS（仮称）」のうち、 ・「デジタル庁が定める公共SaaSの要件」を満たし、 ・ガバメントクラウド上で提供することをデジタル 庁より承認されたもの	ご提案ありがとうございます。共同利用は特定の複数利用者による利用を想定するものであり、SaaSは不特定多数の利用を想定して広く利用者を募るものです。より分かりやすい表現については継続的に検討させて頂きます。
41	1.5 用語の定義 3.1 ガバメントクラウドにおけるSaaS ＜コメント＞ 「 国・地方デジタル共通基盤の整備・運用に関する基本方針 」に記載されている「共通SaaS」との関係について記載願いたい。	公共SaaSの運営主体が府省庁（国営）の場合は、「国・地方デジタル共通基盤推進連絡協議会」で検討されている「共通SaaS」のパターンAに相当します。 公共SaaSの運営主体が民間（民営）の場合は、同じくパターンBに相当します。
42	医療機関向けにクラウド電子カルテを提供する一企業を代表して意見いたします。 本件の対象は、資料P1？2によれば、国又は地方公共団体の事務の実施に関連する情報システムとして、国又は地方公共団体の情報システムのほか、準公共分野で制度官庁等が業務仕様を定めて民間事業者が整備運用する情報システムも対象にすることとしています。 この場合、例えば、民間医療法人が経営する医療機関に提供するために、民間企業が開発運営したクラウド型電子カルテについては、準公共分野である医療分野のシステムであり、厚生労働省等において様々な業務仕様が定められているため、利用するクラウドはガバメントクラウドでなければならないのかが分かりません。また、仮にガバメントクラウドを提供するCSP（P5,P9）を利用する場合にはガバメントクラウドの利用が求められるというルールなのかもわかりません。あるいは、公共SaaSの定義が、「ガバメントクラウド上で、業務アプリケーションを開発し、SaaSの形態でサービスを提供する類型」（P9）としていることから、民間事業者の自主的な選択によりガバメントクラウドを利用する場合に本件のようなデジタル庁を介した契約等のルールの順守が求められるのか分かりません。募集要領の方では、「準公共分野であって制度官庁等が標準仕様を定めて民間事業者が SaaS 形式で整備運用する情報システム（以下「公共 SaaS」という。）等もガバメントクラウドを利用できる」と言及しており、民間企業にとっては任意であるならば、本ルール上もその旨が分かるようにすべきと考えます。 また、仮にガバメントクラウドの利用が任意でない場合、これらの点については、上記のような、準公共分野においてガバクラと同一のCSPを利用しサービスを提供する民間SaaSが、デジタル行政推進法に定める「国又は地方公共団体の事務の実施に関連する情報システム」であると拡大解釈するのは不適当と考えます。 また、上記の事例の派生として、民間企業が提供するクラウド型電子カルテを公立病院に提供する場合も、公立病院における医療提供は、行政権に基づく公権的な地方公共団体の事務ではないため、同じく本ルールの対象外と考えます。 以上のような考え方で差し支えないか、電子カルテに限らず、準公共分野の民間ベンダーに誤解が生じないよう、ルールを明確化すべきと考えます。	公共情報システムの整備・運用をガバメントクラウドを利用して行うかどうかは公共情報システムの管理者が検討の上判断されるものと考えます。 その上で本文書は、ガバメントクラウドで公共情報システムをSaaSとして提供する場合の考え方や規範を示すものです。 例えば、制度所管官庁たるA省があるシステムに必要な要件（以下「標準仕様」という。）を定め、その要件等を満たしたSaaSをガバメントクラウドで提供することは公共SaaSとして可能であると考えております。また、ガバメントクラウドで標準仕様をみたした公共SaaSを提供される場合には、本文書の考え方に沿って規範を遵守することが求められるものです。 なお、ガバメントクラウド以外で提供されるSaaSについては本文書の射程外です。
43	意見番号：1 該当箇所：9ページ / 項番3.1 / ガバメントクラウドにおけるSaaS 意見： 原案に記載の「ガバメントクラウドはISMAP取得済のクラウドサービス（IaaS、PaaS）であり、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境で整備された公共SaaSについては当該SaaSがISMAPを取得していなくともセキュリティ上のリスクが低いことをデジタル庁として担保することで、行政機関等が当該公共SaaSを採用しやすくできないかを検討中」という方針に賛同いたします。 また、この方針を踏まえ、ガバメントクラウド上でデジタル庁様が提示するガイドラインに従って開発・提供される公共SaaSについては、ISMAPを取得していなくても自治体の機密性3B/3Cを扱えることを明記することが適切であると考えます。 理由： 本方針は、ガバメントクラウドの統一的なセキュリティ統制を活用することで、スタートアップや中小企業の参入を促進し、公共SaaSの普及および行政機関のデジタル化を加速する合理的な措置であると考えます。	公共SaaSはISMAPを取得した方が好ましいと考えています。その上で、ガバメントクラウドはISMAP登録済のクラウドサービスであり、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境を提供することで、 ISMAP管理策の一部は対象外とすることが可能であり、公共SaaSの円滑なISMAP登録が推進され、行政機関等による公共SaaSの利用が促進されるものと考えています。当該案文もこのように訂正させていただきます。

No	御意見の概要	御意見に対する考え方
44	意見番号：2 該当箇所：2ページ / 項番1.2 / 本文書の位置づけ 意見： 公共SaaSの適用範囲を「重点計画に記載の公共・準公共分野に該当し、制度官庁等が標準仕様を定める情報システム」に限定することは、対象範囲が狭すぎるため、新たな技術領域や行政機関・自治体ごとの独自のニーズに対応できない可能性があります。したがって、標準仕様が未整備の分野や個別の業務要件に対応するための、柔軟な適用枠を設けていただくことを提案いたします。 理由： 新規の技術領域（生成AI、データ統合・分析など）や標準仕様が存在しない業務が公共SaaSの適用対象外となることで、革新的なSaaSの導入が遅れ、行政のデジタル化を阻害する懸念があります。柔軟な枠組みの整備が不可欠です。	ご指摘のとおり、標準業務については適切なガバナンスを担保しつつ、積極的なSaaS利用の拡大に資するように柔軟な運用が必要と考えています。
45	意見番号：3 該当箇所：10ページ / 項番3.2 / 公共SaaSの定義 意見： 「マルチテナントを原則とする」という基本方針に賛同いたします。一方で、取り扱うデータや業務の特性によっては、マルチテナントでの運用が適さない場合もあります。特に、サービス利用停止時のデータ消去要件に準拠するため、マルチテナント構成では実現が難しいケースが存在し得ます。そのため、シングルテナントの選択が適切となるケースを例外規定として明示いただくことを要望します。 理由： 公共SaaSにおける運用実態に応じた柔軟な設計が求められるためです。セキュリティ要件、カスタマイズ要件、パフォーマンス要件などにより、シングルテナントを必要とするケースもあると考えます。	ご指摘のとおり、SaaSのコンピュータ層とデータ層についてはマルチテナントを前提としつつ、柔軟なシステム構成が選択可能とされるべきと考えています。管理層（コントロールプレーン）については一元的な実装が必要ですが、コンピュータ層とデータ層については一元的な実装からテナント毎の論理分離や物理分離等も含め、SaaS運営主体が自由にシステム構成を選択可能とすべきと考えています。
46	意見番号：4 該当箇所：10ページ / 項番3.2 / 公共SaaSの定義 意見： 「業務アプリケーションのソース、バージョンは全テナント共通を原則とする」とありますが、SaaSの開発・運用にあたってはステージング環境でのテストが必須です。ガバメントクラウド上におけるステージング環境の構成可否について、言及を加えていただくことを要望します。 理由： ステージング環境の確保は、品質保証・リスク回避の観点から不可欠であり、実際の運用設計を行う上での明確な指針が求められます。	ソースやバージョンの共通は原則であり、ステージングや新バージョンの適用タイミングにおいて一時的な相違（新旧の混在）が発生することは想定しています。
47	意見番号：5 該当箇所：10ページ / 項番3.3 / 公共SaaSの共通要件 意見： 「民営の場合は業務仕様が制度官庁等の業務標準に準拠していること（業務標準が存在しない場合や共通サービスについては別途整理を行う）」という要件に賛同いたします。 理由： 標準準拠は業務の効率化とコスト最適化に資するだけでなく、民営SaaSの参入を促すものです。特に、「別途整理を行う」という記載は、柔軟な対応の余地を示すものであり、重要な記述と考えます。	ご意見ありがとうございます。
48	意見番号：6 該当箇所：10ページ / 項番3.3 / 公共SaaSの共通要件 意見： 「ガバメントクラウドの不適切な利用（目的外利用）を防ぐ内部統制の仕組みを有すること」に関して、当該要件がSaaS事業者を対象とするものか、利用組織側の統制を指すのかが不明瞭であるため、明確に記載いただきたいです。 理由： 目的外利用の防止は両者に関係する事項であり、どちらが担うのか、あるいは双方の責務を明確に分けて記載いただくことが望まれます。	本記述は公共SaaSの要件であり公共SaaS事業者に求めるものとなります。
49	意見番号：7 該当箇所：10ページ / 項番3.3 / 公共SaaSの共通要件 意見： 「データの管理権がテナントにあること」との記載について、「管理権」の定義が不明確です。「データの所有権および管理の権限はテナントにあること」など、より明確な表現とすることを提案いたします。 理由： データの取扱責任を明確にすることで、意図しないデータ利用の防止や監査体制の構築がしやすくなります。ISO/NISTなどの用語とも整合性を取ることが望ましいと考えます。	ご提案ありがとうございます。ご意見のとおり修正させていただきました。
50	意見番号：8 該当箇所：11ページ / 項番3.3 / 公共SaaSの共通要件 意見： 「テナント毎の利用状況がダッシュボードやAPIで取得可能でありGCASと連携可能なこと」に賛同いたします。加えて、サービス提供における責任分界点（SaaS事業者／GCAS／利用組織）についても明示いただけると、導入検討がしやすくなります。 理由： 役割分担が明確になることで、システムの導入・運用に関する判断がスムーズになります。	ご意見ありがとうございます。責任分界については今後、明確にしてまいります。

No	御意見の概要	御意見に対する考え方
51	意見番号：9 該当箇所：13ページ / 項番3.5 / 公共SaaSの利用申請等 意見： 「ガバメントクラウド利用開始時期から適切なリードタイムを考慮し、各種申請を行うこと」との記載について、利用開始時期から逆算した具体的な申請スケジュールの目安を追記いただくことを希望します。 理由： 実務においては、通常のガバメントクラウド利用で2年度前からの調査票提出が必要とされています。公共SaaS導入においても、類似のスケジュール感が必要か判断する参考になります。	ご意見ありがとうございます。目安となる期限については、具体的な審査方法等を踏まえて設定することを考えています。
52	さくらインターネット株式会社　ガバメント推進室として、以下の意見を提出いたします。（意見提出にあたっての住所、氏名についてはさくらインターネット株式会社として記載しております） 以下の意見本文 ーーー 要旨 ・本意見書は、ガバメントクラウドを活用した公共SaaSの整備において、既存のLGWAN-ASPサービスとガバメントクラウドの効率的な連携方法について、提案するものです。特にガバメントマルチクラウドネットワーク（以下、「GMCN」）を活用したLGWAN-ASPのサービス提供方法の検討を要望します。 1　背景と目的 ・意見を求められている当該文書は、ガバメントクラウド（以下、「ガバクラ」）を利用して新たに整備する公共SaaSの共通技術要件等を整理することで、その企画・構築を効率的かつ効果的にする目的で作成されたものと考えております。 ・新たに構築されるサービスのための技術要件整理も重要ですが、既存の枠組みもあわせて整理することで更なる利用促進が図られるものと考えます。 ・公共情報システムとして民間事業者が整備し、主に地方公共団体が共同して利用しているサービスとしては既に「LGWAN-ASP」が存在しております。 2　現状と課題 ・今後LGWAN-ASPをガバクラと連携していくことを考えた時には、経路の問題を初めとしたいくつかの課題が存在することがすでにわかっております。 ・「システムを所有から利用への転換するSaaS利用」を促進するという観点を考えた時に、LGWAN-ASPの取り扱いについても今回の文書とあわせて検討されるべきであり、その一助とするために以下に提案いたします。 3　具体的提案 3.1 LGWAN-ASPのGMCNサービス化による効率化の提案 ・現在、ガバクラとLGWAN-ASPを連携させる場合、データの流れとして「ガバクラ ー 地方公共団体 ー LGWAN-ASP」という経路を経る必要があり、システム運用の負担増加や遅延の要因となっています。この構造は、ガバクラの利便性を十分に活用しきれない要因の一つとなっていると考えます。 ・この課題を解決するため、LGWAN-ASPとして提供している事業者が直接ガバクラ上でサービス（アプリケーションを含む）を提供できる仕組みを整備することを	ガバメントクラウド以外でサービスを提供されているものは本文書の射程外です。いただいたご意見は参考にさせていただきます。
53	意見1 3.2「公共SaaS」の定義において、「「重点計画に記載の公共・準公共分野に該当し、制度官庁等が標準仕様を定める情報システム」を SaaS として構築したもの」とあり、また 「SaaS の運営主体が業務システム等の機能をサービスとして提供し、SaaS利用者は原則としてシステム開発・運用を行わずにサービスを利用する。」とありますが、公共SaaSは、ローコードで設定を行うような公共むけSaaSも対象として考えてよろしいでしょうか。 意見2 3.3 1.基本要件（必須要件）に「ガバメントクラウド上で稼働すること」とあります。私どもも現存のガバメントクラウド上で稼働するように環境の整備を進めたいと考えていますが、それによってコスト高になってしまう可能性があり、ガバメントクラウドとして要求される設定を当社現行環境（AWS）で実装する方がコストを抑えられ、公共・準公共分野の皆様にご利用いただきやすくなると考えております。どこまで実装出来るかや、費用などの諸条件如何かとは思いますが、そういったご検討も行なっていただけるものでしょうか。	公共SaaSはガバメントクラウド上で提供されるすべてのSaaSです。ガバメントクラウド上で提供されないものは本文書の射程外となります。ガバメントクラウド上で公共SaaSを提供するか、ガバメントクラウド以外でSaaSを提供するかの検討は各SaaS事業者において行われるものと考えます。
54	1 標準化法の対象となる業務に関しては明確な指針がありますが、それ以外の自治体業務についても、民間企業が提供する既存のSaaS等の活用を前向きに検討することが重要だと考えております。 また、業務や分野によっては、公共"専用"のSaaSではなく、民間でも使われるSaaS(チャットツールやファイル共有サービス、電子契約、名刺管理サービスなど)もあり、それらを積極的に活用することで、公共分野だけでSaaSの費用負担をせず、官民で使えるSaaSが広がることで経済合理性がより生まれると考えています。 「3.3 公共SaaSの共通要件」において、（業務標準が存在 ない場合や共通サービスについては別途、整理を行う ）とありますが、共通サービスの対象となる業務等については、早期に明確化されることを希望します。 現在すでに進んでいる自治体のデジタル化推進や検討が止まらぬように、幅広い民間事業者や、自治体を含めた双方向のオープンな議論の場を設けることをご検討ください。 2 [3.1ガバメントクラウドにおけるSaaS]で、「ガバメントクラウドは ISMAP 取得済のクラウドサービス（IaaS、PaaS）であり、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境で整備された公共 SaaS については当該 SaaS が ISMAP を取得していなくともセキュリティ上のリスクが低いことをデジタル庁として担保することで、行政機関等が当該公共 SaaS を採用しやすくできないかを検討中」とあります。AWSやAzure自体、IaaSとしてISMAPを取得済みですが、ガバメントクラウドではない、ISMAP取得済みのIaaS(AWSやAzure等)上に構築されたアプリケーション(=SaaS)でもISMAP取得していなくとも行政機関等が当該SaaS(公共SaaS、外部SaaS問わず)を採用しやすくできないかの検討はしていますでしょうか？ ガバメントクラウドではないISMAP取得済みのIaaS(AWSやAzure等)上に構築されたアプリケーション(=SaaS)では検討できない、セキュリティ等の差分などがございましたらご教示ください。	1 共通サービスの対象となる業務等の明確化については、引き続き検討を進めます。 2 ガバメントクラウド上で提供されないものは本文書の射程外となります。

No	御意見の概要	御意見に対する考え方
55	P.9 ＞ ガバメントクラウドは ISMAP 取得済のクラウドサービス（IaaS、PaaS）であり、デジタル庁において統一的なセキュリティ統制がとられていることから、 ＞ ガバメントクラウドの開発環境で整備された公共SaaS については当該 SaaS が ISMAP を取得していなくともセキュリティ上のリスクが低いことをデジタ庁として担保することで、行政機関等が当該公共 SaaS を採用しやすくできないかを検討中 。 ■意見１ ガバメントクラウド上に構築されたSaaS部分のリスクが低い事をどのようにデジタル庁が担保する事をお考えなのでしょうか。 1. ガバメントクラウド上に構築されているからSaaS部分の評価は不要という整理を行う。 → 脆弱性満載のアプリケーションの場合でもガバメントクラウド上に構築されているからという理由でデジタル庁がお墨付きを与える事になると思いますので悪手に思います。 2. ガバメントクラウド上に構築されているSaaS部分をデジタル庁側で別途設定したセキュリティ要件で監査して安全を保証する（ISMAP/ISMAP-LIUの要件から一部要件を抜粋 / ガバメントクラウドで担保されるIaaS部分の評価を除く等） → ISMAP/ISMAP-LIUで評価し、IaaS部分を確認不要にすればいいだけなので、わざわざ別の枠組みを設ける意味は無いように思えます。（普通にISMAP/ISMAP-LIUを取得すれば良いように思えます） 3. ガバメントクラウド上に構築されているSaaS部分をデジタル庁側で別途設定したセキュリティ要件で監査して安全を保証する（ISMAP/ISMAP-LIUの要件に無い（異なる）別のセキュリティ要件を設ける） → 同じ情報を取り扱っているサービスでもガバメントクラウド上に構築されているかどうかで要件が異なるという、要件のダブルスタンダードになるので悪手に思えます。 ■意見２ こちらの方針はISMAPの運営組織と方針の認識は合っていますでしょうか。	公共SaaSはISMAPを取得した方が好ましいと考えています。その上で、ガバメントクラウドはISMAP登録済のクラウドサービスであり、デジタル庁において統一的なセキュリティ統制がとられていることから、ガバメントクラウドの開発環境を提供することで、 ISMAP管理策の一部は対象外とすることが可能であり、公共SaaSの円滑なISMAP登録が推進され、行政機関等による公共SaaSの利用が促進されるものと考えています。当該案文もこのように訂正させていただきます。