

第 41 回 ISMAP 運営委員会 議事録

開催日時：令和 8 年 6 月 26 日（金）10:00～12:00

場 所：Web 会議

<出席者>

【委員】（五十音順、○は委員長※）

江崎 浩	東京大学大学院 情報理工学研究科 教授
○大木 榮二郎	工学院大学 名誉教授、特定非営利活動法人 日本セキュリティ監査協会 会長
後藤 厚宏	情報セキュリティ大学院大学 教授
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
根本 直樹	デジタル庁 統括官付 ガバナンス・マネージャー
間形 文彦	NTTドコモビジネス株式会社 情報セキュリティ部 担当部長
満塩 尚史	順天堂大学 健康データサイエンス学部 准教授
和貝 享介	公認会計士

【制度所管省庁】

中溝 和孝	内閣官房 国家サイバー統括室 審議官（制度・監督担当）
奥田 直彦	デジタル庁 省庁業務サービスグループ 統括官付審議官
赤阪 晋介	総務省 大臣官房 サイバーセキュリティ・情報化審議官
奥家 敏和	経済産業省 大臣官房 審議官（商務情報政策局担当）【欠席】

【説明者】

ISMAP運用支援機関（IPA） 議題 1、2、3、4、10
内閣官房国家サイバー統括室（NCO） 議題 9
経済産業省（METI） 議題 5、6
委員 議題 7
デジタル庁 議題 8

【事務局】

内閣官房国家サイバー統括室（NCO）

<議事次第>

1. ISMAP等クラウドサービスリストへの登録について
2. ISMAP監査機関リストへの登録について
3. 登録済みサービスの変更に関する届出について
4. 情報セキュリティインシデントについて
5. 監査機関の拡充について
6. 規程類の改正について

7. 委員発議の議題
8. 新たな申請類型について
9. ISMAP管理基準改定等について
10. 監査機関の品質モニタリング計画（2026年度）について

<議事>

【開会】

○事務局 第41回「ISMAP運営委員会」の開会を宣言。

1. ISMAP 等クラウドサービスリストへの登録について

○IPA説明者 ISMAPにおいて申請を受理したサービス（新規申請 5 件、更新申請 4 件の計 9 件）に関して、ISMAPクラウドサービス登録規則6.1に基づく技術的審査の結果をそれぞれ 7 つの観点（以降の(1)～(7)）から報告します。

なお、上記 4 件以外の 6 件については、審査において特段の懸念事項がない申請として、ISMAP運営規則2.4.2に基づく手続によりクラウドサービスリストへの登録を実施します。

○IPA説明者 新規申請 5 件及び、更新申請 4 件の計 9 件について、以下のとおり報告します。
IPAとしては、全てのサービスについて、ISMAP登録規則6.1に定める要件に適合しており、登録してもよいと考えます。

(1) 基本言明要件が満たされていること

いずれのサービスにおいても、提出された言明書と個別管理策の記載内容が、ISMAP管理基準2.2.4基本言明要件に記載の要件に適合していることを確認しました。

なお、対象外としている統制目標の項目について、対象外とする理由が合理的であることを確認しました。

また、非採用としている詳細管理策（末尾にB又はPBがあるもの）の項目について、非採用とする理由が合理的であることを確認しました。

(2) ガバナンス基準及びマネジメント基準の発見事項が存在しないこと

いずれのサービスにおいても、提出された実施結果報告書にて、発見事項が存在しないことを確認しました。

(3) 実施結果報告書における、管理策基準の発見事項の有無

提出された実施結果報告書にて、7 サービスにおいては選択された 4 桁管理策の発見事項が存在しないことを確認しました。

2 サービスについて、選択された 4 桁管理策の発見事項が存在したことを確認しました。

(4) 前項において発見事項が存在する場合、当該発見事項が軽微であること。軽微であることの要件の一つとして、当該発見事項に係る統制が実施結果報告書の日付から 2 ヶ月以内に改善することが示された改善計画書が存在すること

上記(3)において発見事項が存在しなかった 3 サービスについては、本項目は確認対象外となります。

上記(3)において発見事項が存在した1サービスについて、改善計画書が提出され、2ヶ月以内に改善することが示されていることを確認しました。

当該サービスにおける発見事項について、代替統制・補完統制が十分に機能しており、統制目標の達成に影響を与えるものではないこと、継続的あるいは反復的に発生しているものではないことを確認できたことから、発見事項は軽微であると判断しました。

(5) 3.4に規定する情報が適切かつ十分に開示されていること

いずれのサービスにおいても、3.4に規定する情報が適切かつ十分に開示されていることを確認しました。

(6) 3.5に規定する事項に関する宣誓事項が全て含まれていること

いずれのサービスにおいても、3.5に規定する事項に関する宣誓事項が全て含まれていることを確認しました。

(7) その他、本制度の規程類に照らして違反がない、もしくは過去に14.2(5)による登録の削除を受けていないこと。

いずれのサービスにおいても、規程の違反もしくは過去に登録削除を受けたものはないことを確認しました。

○IPA説明者 合わせて以下の内容について報告。

- ・「SPIRAL® ver.1」の発見事項・改善計画書の内容について
- ・「奉行iクラウド、奉行V ERPクラウド、奉行クラウドEdge」の発見事項・改善計画書の内容について
- ・「Google Workspace」のサービス変更について
- ・「AvePoint Online Services」のサービス変更について
- ・「Oracle Fusion Cloud:Enterprise Resource Planning (ERP),Enterprise Performance Management (EPM),Supply Chain & Manufacturing (SCM),Human Capital Management (HCM),Sales and Service」のクラウドサービスの名称およびサブサービスの名称の変更について

○委員長 (委員へご意見、ご質問等を確認)

○委員 1件目のSPIRALについて、1点だけ確認をさせてください。ライセンス数について、18.1.2.6の管理策、御確認いただいたという点で、それについては異存ございません。御報告のとおりかというふうに理解いたしました。

もう一つ教えていただきたい点は、共有IDの利用についての管理策です。9.2.1.2だったと思いますけれども、共有IDの利用について、必要な場合だけ許可して、承認し、記録をせよという管理策だったと思いますが、これについて、審査報告書を拝見しても言及されていなかったもので、問題なかったのかどうかだけ、念のため確認させていただければと思います。

○IPA説明者 クラウドサービスの安全性評価に関する検討会取りまとめの資料の中に、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ということと、もう一つ、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。こういう規定に基づきまして、その点についてさらに審査をすることはしておりません。

○委員 問題はなかったということですね。念のための確認です。

○IPA説明者 はい。

○委員 指摘がされなかったというふうに理解してよろしいのですね。

○IPA説明者 はい。結構です。

○委員 分かりました。

○委員長 他にご意見、ご質問等ございませんようですので、登録が適切と判断されたサービスにつきましては、ISMAPクラウドサービスリストへの登録についてIPAの原案のとおり決定の上、事務局にて資料を整えた上で、6月26日付でクラウドサービスリストを更新し、6月29日に公表したいと思いますが、よろしいでしょうか。

○委員一同 異議ございません。

2. ISMAP 監査機関リストへの登録について

○IPA 説明者 申請を受理した監査機関（新規申請1件）に関して、ISMAP 監査機関登録規則 6.1 に基づく技術的審査の結果を2つの観点（以降の(1)～(2)）から報告します。

○IPA 説明者 新規申請1件について、以下のとおり報告します。IPAとしては、ISMAP 監査機関登録規則 6.1 に定める要件に適合しており、登録してもよいと考えます。

(1) 3.1 から 3.8 に規定する要求事項を満たすことができること。

提出された申請文書及び申請文書に添付された資料等の記載内容が、ISMAP 監査機関登録規則 3.1 から 3.8 に規定する要件に適合していることを確認しました。

(2) その他、本制度の規程類に照らして違反がない、もしくは過去に 11.2(4)による登録の削除を受けていないこと。

規程の違反もしくは過去に登録削除を受けたものはないことを確認しました。

○委員長 （委員へご意見、ご質問等を確認）

○委員 私の知る限り、こちらの機構は比較的零細なところだというふうに認識しております。実態としてこういう体制があるかということはIPAさんのほうで確認されているのですけれども、ここのロケーションに行って確認をされているということでよろしいのでしょうか。ロケーションを見ている、確認しているということでよろしいのでしょうか。

それから、もう一つはお願いですけれども、監査法人以外で初めてということなので、今後、実績があったような場合には、品質管理のモニタリングの対象として、ぜひ確認の対象として選定していただいたほうがよろしいのではないかと思います。

○IPA 説明者 場所については、登記上、登録されているものではあるのですが、バーチャル上の貸しオフィスというふうに伺っております。ただ、今回の確認においては訪問調査という形で、ヒアリングを含めて拝見、確認をさせていただいております。

○委員 分かりました。実態をあまり明確に把握されていないのかなというのは若干懸念します。でも、それについては、先ほどお願いした、次の機会に品質管理のモニタリングをされるときに検討ということではよろしいのではないかと思います。

○委員長 監査をする組織としての脆弱性みたいなところが気になるという御指摘だったと思いますので、次のモニタリングのときにぜひよろしくお願ひしたいと思います。

○委員 私は、今の委員と同じく、懸念を1つ持ちました。一番、気になっているのは規模感でございまして、今回の ISMAP の監査業務というものは非常に重い業務でございしますので、それを全部賄い切れるかということが気になりました。

それについての質問をしたところ、内部のほうでやりますと。外部の業務委託等をする予定はないという回答がございましたが、やはり大事な業務でございしますので、法人の内部で、対応できる体制であるのか、フルタイムの担当の方が何人ぐらいいるのかというところが気になったところです。

ただ、この留意事項辺りは特に明記されていないことと、要件を満たしているということで、今回、登録自体はオーケーと思っておりますが、同じように、あとはモニタリングをしっかりとやっていただくということが必要だと思いました。

○IPA 説明者 従業員数については審査の形式要件ではないので確認してはおりませんが、今、おっしゃってくださったように、業務委託とかで法人外から募集したメンバーを使うということは想定していなくて、通常の本社にいらっしゃるメンバーで ISMAP の監査対応をされるという御回答をいただいております。

○委員長 いずれにしても、今、委員からもあったように、少しそういうところの懸念があるということでございますので、今後を見ていくということと思います。

○委員長 特にご質問、ご意見等ございませんようですので、登録が適切と判断された監査機関につきましては、ISMAP 監査機関リストへの登録・更新について IPA の原案のとおり決定の上、事務局にて資料を整えた上で、6月26日付で監査機関リストを更新し、6月29日に公表したいと考えますが、よろしいでしょうか。

○委員一同 異議ございません。

3. 登録済みサービスの変更に関する届出について

○IPA 説明者 前回のリスト更新時から次回の更新申請までに受領した変更届出について、再監査の必要性及び情報開示の内容案について報告します。

○IPA 説明者 Google LLC 社「AppSheet」の重大な統制変更等届出書及び登録取下届出書について、変更内容は「Google Workspace(C21-0005-2)への統合に伴う、AppSheet(C21-0028-2)の廃止」となります。ISMAP 登録規則第3章の要求事項の実施に疑義が生じるような変更には該当しないことから、再監査は不要と判断します。一方で、当該サービスに関する正しい情報を開示すべきであることから、「クラウドサービスリスト」から削除し、ISMAP ポータルの最新情報に「ISMAP クラウドサービスリスト上のサービス統合について」を公表する予定としております。

○IPA 説明者 Cisco Systems, Inc. 社「Webex」の重大な統制変更等届出書について、変更内容は「リージョンの誤記の訂正」となります。ISMAP 登録規則第3章の要求事項の実施に疑義が生じるような変更には該当しないことから、再監査は不要と判断します。一方で、当該サービスに関する正しい情報を開示すべきであることから、ISMAP クラウドサービスリストのクラウドサービスリスト詳細及び特記事項欄で開示を行う予定としております。

○IPA 説明者 Google LLC 社「Bare Metal Solution」の重大な統制変更等届出書につい

て、変更内容は「リージョンの削除」となります。ISMAP 登録規則第 3 章の要求事項の実施に疑義が生じるような変更には該当しないことから、再監査は不要と判断します。一方で、当該サービスに関する正しい情報を開示すべきであることから、ISMAP クラウドサービスリストのクラウドサービスリスト詳細及び特記事項欄で開示を行う予定としております。

○IPA 説明者 デジタルアーツ株式会社「「DigitalArts@Cloud」/「Desk」/「m-FILTER MailAdviser」（Microsoft 365 対応版）/「StartIn」/「f-FILTER」」の I S M A P クラウドサービスリスト掲載事項変更届出書について、変更内容は「サービス名称の変更、サブサービス名称の変更、当該クラウドサービスのホームページの URL の変更」となります。ISMAP 登録規則第 3 章の要求事項の実施に疑義が生じるような変更には該当しないことから、再監査は不要と判断します。一方で、当該サービスに関する正しい情報を開示すべきであることから、クラウドサービスリスト詳細のクラウドサービスの名称及び当該クラウドサービスのホームページの URL、特記事項で開示を行う予定としております。

○IPA 説明者 Google LLC 社「Google Cloud Platform」の重大な統制変更等届出書について、変更内容は「サブサービス名称の変更」となります。ISMAP 登録規則第 3 章の要求事項の実施に疑義が生じるような変更には該当しないことから、再監査は不要と判断します。一方で、当該サービスに関する正しい情報を開示すべきであることから、ISMAP クラウドサービスリストのクラウドサービスリスト詳細及び特記事項欄で開示を行う予定としております。

○IPA 説明者 ソフトバンク株式会社「ホワイトクラウド ASPIRE」の重大な統制変更等届出書について、変更内容は「サービスの事業移管、サービス名称の変更」となります。ISMAP 登録規則第 3 章の要求事項の実施に疑義が生じるような変更には該当しないことから、再監査は不要と判断します。一方で、当該サービスに関する正しい情報を開示すべきであることから、ISMAP クラウドサービスリストのクラウドサービスリスト詳細及び特記事項欄で開示を行う予定としております。

○委員長 （委員へご意見、ご質問等を確認）

○委員長 特にご質問、ご意見等ございませんようですので、本件につきましては、原案のとおり再監査は不要とし、クラウドサービスリスト詳細及び特記事項欄にて情報開示を行いたいと思います。よろしいでしょうか。

○委員一同 異議ございません。

4. 情報セキュリティインシデントについて

ISMAPクラウドサービスリストに登録済みサービスにおいて発生した情報セキュリティインシデントの報告 4 件について、ISMAP運用支援機関から ISMAPクラウドサービス登録規則に基づく直近の対応状況を報告。内容を討議の上、対応方針を決定した。

【詳細については非公開情報の保護やレピュテーションリスク等を考慮し、今回の議事においては公開可能な情報がないと委員において判断されたことを踏まえ、議事の公開は控えさせていただきます。】

5. 監査機関の拡充について

○METI説明者 監査機関の拡充について説明を行います。

○委員長 (委員へご意見、ご質問等を確認)

○委員 3点あります。一つは、9ページのところの誓約書の文言です。9ページだけでなく、ほかのページにも同様の文言があるのですが、この誓約書の枠内の8.の文言なのですけれども、真ん中のところを読みますと「業務執行責任者及び業務実施責任者を含む業務実施者が監査対象組織から独立していることを確実にしています」となっていますが、この「独立していること」というものは非常に表現が正しくないと思います。

組織から独立しているというのは法人と別個にあるということを表すと思うのですけれども、ここで正しくは「組織から独立性を保持している」「組織から独立性を確実にしていく」という、独立性というふうにしないと、単に組織的に、法人的に独立していても、サービスの観点で独立性に抵触するという場合もありますから、ほかの規程の箇所と同様に、独立性という言葉で全体を統一すべきで、ここを改定をお願いしたいと思います。

2番目は、誓約書の15ページに誓約書Bがありますけれども、これは先ほどおっしゃったように、業務実施者がその所属法人のところに出すということで、例えば担当者が3人、実施責任者、品質管理責任者、そのほかのことで3人しかいない場合に、この法人宛てに私はこの組織でやりますという誓約書を出しても非常に形式的で、法人内でクローズした形で誓約しているだけというふうに思われます。

この「【所属法人名】御中」と書いてあるところは、例えばやはり様式Aと同じような形のIPAですとか、これは規則上あまり意味がない、そういうことができないのかもしれませんが、IPAとか、それから、運営委員会のほうに相手に出すべきではないかというふうに思います。

そこで疑問が生じるのは、この記述と、9ページに戻りますと、運営委員会に出している監査機関登録申請書のほうの「記」と書いてある誓約書には独立性のことがうたってありますから、この監査登録機関申請書のほうでは運営委員会に向けて独立性を宣言しているようにも思えるのですが、この辺りの関係が少し分からないので、教えていただきたいということが2番目です。

独立性については、主にこの目的とか趣旨は監査法人以外のところについて規定することになるのだろうと思いますから、ガイドラインやFAQでいろいろ触れてあるのですけれども、できるだけ具体例を示したものをこういう場合と、あくまで例示列挙ではありますが、そのほかもあるのですけれども、例示を具体的に示すということが重要かなと思っていますので、今後、その辺りの御検討をお願いしたいと思います。

○委員長 それでは、以上の3点について、経済産業省、どういうふうにお考えか、お願いいたします。

○METI 説明者 まず、1点目です。「独立していることを確実にしています」というところの修正については承りました。修正をさせていただいて、後ほど展開をさせていただきますので、御承諾いただければと思っております。

2点目、法人宛てではなく運営委員会に宛てて誓約書Bを提出すべきではないかという点については、監査検討委員会の皆様にもお伺いを立てていたところではあるのですが、まず、監査検討委員の皆様からは、個人名で ISMAP 運営委員会御中という形で出すのは非常に難しいであろうという形の御指摘をいただいております。したがって、まず、個人名で出していただくという場合においては、所属監査機関内にとどめる形にさせていただきたいという形で御指摘をいただいておりますので、そのような形にしております。

法人名として出していただくのは、この誓約書Aという形にしておりまして、様式1または様式5の拡張したものにしておりますので、まず、この誓約書Bのところで個人名にしているのは、組織内で保持をして、きちんと組織内で業務執行責任者、業務実施責任者の独立性を担保しているということを組織内で確認をしていただく。その結果を誓約書Aという形で、様式1の形で我々、ISMAP 運営委員会御中という形で出していただくという形の整理をしておりますので、現状の整理のままにしたいと考えているのがお答えになろうかなと思っています。

3点目、独立性に関する例示というところは、監査実施マニュアルのほうに幾つか記載をさせていただいております、こちらの例示に関しても監査検討委員会の皆様に御承諾をいただいている形となっております。

○委員 今の誓約書の件は、Bで個人で宣言した後、法人として誓約書Aを使うということなのですね。

○METI 説明者 おっしゃるとおりです。誓約書Aは必ず出していただきます。誓約書Bは組織内で保持をしていく形になります。

○委員 承知しました。

○委員長 それでは「独立している」の表現のところは変更するということをお願いします。

○委員 直前の委員の発言の3点目に若干関係するのですが、スライド5のところで誓約書Bに関しては括弧つきで条件が書かれているというふうに思っております。ただ、先ほどFAQでという話もありましたが、これはFAQで書くのかなと思っています。そうすると、この誓約書Bというものはひな形だということなので、そもそも、これは規程として書くべきなのか。要はサンプルとして書くのは別に構わないと思いますが、その整理がどうなっているのかなと思っております、今のお話からいくと、例えば誓約書Aはルールとしてちゃんと規程類に書くべきだというふうに思っていますが、誓約書Bに関しては誓約書Bという形で誓約書Aと並ぶものではないと思っており、内部で構築する内容を規程として書くべきではないかと思っております、その辺の経産省の御見解を伺えればと思います。

○METI 説明者 まず、この誓約書Bと置かせていただいているものについては規程化はしない想定です。様式化せず、あくまでひな形のままにしたいと思っています。監査法人とセキュリティーベンダーで独立性の担保の仕組みのやり方が変わってきますので、それを様式化してしまうと、監査法人にもこの様式Bというものの提出を確実に求める形になってしまいますので、そこは明確に分けておきたいと思っています次第です。

ただし、先ほど説明があったとおり、様式Bはあくまでひな形ですので、これを使っ
ていただいてもいいですし、各セキュリティーベンダー等の中で別個の、例えば様式等
を各会社の中で持っているのであれば、誓約書Bの内容が盛り込まれているのであれば、
それで代替することもできるという形にしていきたいと思っています。

それで、この誓約書Bの運用等についても監査実施マニュアルのほうに具体的に明記
をさせていただいておりますので、その中で監査機関の皆様には御確認をいただきた
いと思っています。

併せて、これはFAQとして外部に公開すべきではというお話もあろうかと思ってい
ますが、監査実施マニュアルはあくまで監査機関に限って公開をしているマニュアル
になりますので、その中で監査機関向けに公開をしていく、御確認をいただくという形
のほうよろしいのではないかとということで、FAQではなく、マニュアルのほうに記載
をさせていただいています。

○委員 内容としては了解しました。AとBというようなことで、Bもルールに見えてしま
ったので懸念を申し上げたところですので、その辺りは表現を御検討いただければと
思います。

○委員長 この質疑については以上とさせていただきたいと思います。

6. 規定類の改正について

○METI説明者 監査機関の拡充に伴い、監査機関登録規則・様式について、議題5での説明
のとおりISMAP監査機関登録規則・様式1・様式1別紙・様式2・様式4・様式5・様式
7の改正を行います。

○委員長 (委員へご意見、ご質問等を確認)

○委員長 それで、これは規則としてということですが、先ほど討議の中で、この監査機関
が独立しているという表現を、独立性を確立しているとかという表現に変えるべきだ
ということで、経済産業省もそうするというような答弁だったと思うのですが、それにつ
いてはどうしますか。

○METI説明者 そこは独立性を保持するという形で修文をした上で、様式1については御
決定いただきたいというふうに思っているところです。経産省が修正をしますというこ
とです。

○委員長 幾つか関連する記載もあるかと思いますが、これはいつまでに決定しないとまず
いですか。

○METI説明者 次回の運営委員会だと考えております。

○委員長 関連する表現のところも少し見直していただいて、それに合わせて、見直すべき
ことは訂正した上で、この規則を変えるということにしたいと思うのですが、事務局、
これは後でメールで皆さんに確認いただくというようなことでもよろしいでしょうか。

○IPA説明員 問題ございません。

○委員長 それでは、先ほどの表現を見直したものをつくっていただいて、それでメールで
皆さんに確認した上で、運営委員会での決定としたいと思いますが、よろしいですか。

○METI説明者 経産省は問題ございません。

○委員長 委員の皆様、そういう運営でよろしいでしょうか。

○委員一同 異議ございません。

○委員長 パブコメの実施について、委員の皆様、御意見等ございましたらお願いします。

○METI 説明員 パブコメは、御提案のとおり、不要というふうに考えております。

○委員長 ありがとうございます。では、経済産業省の案のとおり、パブコメは実施せずということにしたいと思いますが、よろしいでしょうか。

○委員一同 異議ございません。

○委員長 それでは、皆さん、後ほどメールで確認をいただきたいと思います。

7. 委員発議の議題について

○委員 「公開RFCs等からみるFedRAMP制度の現状」について、報告を行います。

この後にも新たな申請類型のお話もあるかと思いますが、現状のFedRAMPについて、皆さんも御承知かと思いますが、僭越ながら、私のほうで少しまとめたものをお話しさせていただきますと思っています。

現在、FedRAMPでは従来型の登録がされていますし、加えて、約30の20Xと呼ばれるものが登録されています。

まずここで報告すべきと思ったところの一つでございますが、コミュニケーションがかなり頻繁に行われております。RFCが約30本、昨年度YouTubeの動画が約6か月で、私が確認する限り、40本プラスα登録されています。そこで、いろいろな情報が公開されているところでございます。

このYouTubeの中を見ていて、エピソード的なお話をすると、FedRAMPが米国の中ではFedWALLと言われていた。要は障壁だと言われていたこともあり、改革をしたいのだというお話もございますので、そういった意気込みで彼らがやっているということをご承知いただければと思います。

20Xの改革ですが、FedRAMPでは従来のSP 800-53のモデレートが約300を超える項目がございます。これを直接監査するのではなく、KSIというKey Security Indicatorということで、抽象化レイヤーにしたもので、モニタリング可能なもの、測定可能なものということで、そこを評価するということになってます。これによって継続的な評価ができるということになります。

そうすると、評価機関、従来、Auditorと言っていたものが、FedRAMPでは、Third-Party Assessment Organization(3PAO)となります。こちらの役割も、証拠のレビュー、実際の個別の文書をレビューというよりはモニタリングの検証ということに変わってきています。つまり、手作業の証拠レビューを3PAOがやっているのではなく、自動評価のスキームが動いているかということを検証しているということになります。

次に、米国でもお墨つきになっていることをやはり問題視しています。そのため、Authorizationという「認可」だという誤解があるということで、名称のほうをFedRAMP Authorizedではなくて、FedRAMP Certifiedと名称が変更しています。

また、DoDのHigh、Moderate、Lowと同じ定義ではない、Equivalentではないということで、カテゴリーの名称もClass A、Class B、Class C、Class Dと変えています。特にClass

Aは、従来、FedRAMP Readyと言っていたカテゴリについては、低リスクのもので既に実績のあるもので、正式なFedRAMPの評価を行う代わりに、外部の評価枠組みであるSOC2レポート等を活用するということを想定しています。ただし、こちらのClass Aについては、早期にClass B、Class C、Class Dに移行しなければならないとされています。

更には、今回、FedRAMP制度がCertificationであるとしており、最終的な運用認可は各省庁が行うということを明確化しており、FedRAMP制度と各省庁の役割分担が明確化していると言えるかと思います。

また、機械可読の義務化ということで、前の会議でもお話ししたかと思いますが、OSCALを導入しコントロール構造化する対応ということで、今後のCSPのコントロールは機械可読であることを要求しており、本格的に2026年9月30日から運用を開始される予定です。

ただし、Class D、高いレベルで必須ということで進められていくようです。もちろん、A～Cに関しても、現状は従来どおりですが、今後、OSCALに移行するのではないかと思います。機械可読なコントロールの導入により、人が手で書いた説明文であるセキュリティ計画のコピペ運用から脱却すると言われています。

運用の標準化も進んでおり、例えば、脆弱性管理、重大な変更通知、インシデント発生対応等が標準化されようとしています。具体的には、例えばインターネットからの到達＋悪用可能な脆弱性については3日以内の対応をするとか、重要な変更通知に関しましては、Adaptiveであれば10営業日以内に報告してください。ただし、事前承認というよりは事後通知という形に変わるということですし、インシデントの発生については、各Classによって規定された時間で連携できるようになります。こういう形で、かなり標準化の具体的なオペレーションの連携が進んでいるようです。

情報公開に関してですが、先ほど申し上げたOSCAL等を想定し、これまではFedRAMPで共有することとしていましたが、今後は、各CSPでトラストセンターという形で、データを共有する形に変えています。これは著作権とかオーナーシップが各CSPにあることを明示的にしています。CSPから共有される文書のテンプレートでは、従来、CUI、つまり、政府の非機密情報と書かれていたのですが、こちらも外されています。機密性に関しても各CSPが決めるということになり、政府としてのCUI表示は外されています。今後、公開できる情報はCSPが整理するようになっていくかなと思っています。

今までは認証制度のお話でございましたが、1点、セキュリティー・インボックスということで、FedRAMPの制度側から各CSPに直接連絡がオンタイムで連絡する窓口として専用メールの仕組みをつくっています。これにより、政府全体で対応すべき脆弱性対応等が発生した場合これを活用し連絡をしているという今までにない取組も御紹介します。

私のご紹介はこちらまでですが、従来のSaaSの認証に関して今後進めていくことは重要ですが、今後、AIとかLLMだけではなくて、Agentic AIの仕組みに関しても考えていかなければいけないのだろうと思っており、今回紹介したFedRAMPの対応は、その対応までを見据えた状況だと思っており、皆さんに御紹介した次第です。

私からは以上でございます。

○委員長 （委員へご意見、ご質問等を確認）

○委員 今回の委員の報告へのコメントですけれども、これを伺って、従来のあるバッチでた

めておいたものを過去のデータとして手作業でサンプリング、試査でやるという手続から、継続監査、リアルタイムで継続的に、しかも自動検証で精査、全ての取引を全部見るという方式になったということで、私も AI などの検討についてはそういう方向を目指すべきだと思っていますが、非常に参考になりました。

8. 新たな申請類型について

○デジタル庁説明者 新たな申請類型について、説明を行います。

○委員長 （委員へご意見、ご質問等を確認）

○委員 新しい制度の御提案ありがとうございます。ただ、どういうクラウドサービスの用途を念頭に置かれているのかということの御説明がありませんでしたので、正直申し上げますと、判断ができませんでした。具体的にどういう用途、どういうリスクを抱えるであろうサービスなのかということと併せて、どういうコントロールで、あるいはどういう制度の枠組みの中で監査をしていくのかということとセットで考えていただけるとよかったかなというふうに思います。参考になるのは、恐らく、先ほど委員から御提示いただいた資料の4ページにもあったとおり、Class A、Class B、Class C、Class DのClass分けがあって、Class Aだったら活用できる外部枠組みという御説明があったかと思いますので、そんなものを御参考いただきながら、用途と併せて議論できるとよいかなと思いますので、次回、御提案を持ってきていただくときには用途を、特にどういうリスクを抱えているであろう情報を取り扱うのかということに注力した御説明をいただけるとうれしいなと思いました。

○デジタル庁説明者 用途に関しましては、申し上げたとおり、現状、野良で既に使われているSaaSが全て対象と考えてございます。それについては、以前の利用実態調査の御説明をしたと思いますけれども、様々あるということで把握してございまして、それらは各省庁が、自分たちでは野良であっても利用するというリスクを、ある種、自己判断して使っているという現状だと思ってございますので、仮にこの制度に巻き取ったとしても、それを使う使わないはやはり利用省庁の判断で調達するかしないかが決まるというふうに考えてございます。

繰り返しとなりますが、情報というものをきちんと正しく、これがIaaS/PaaSで、ISMAPであるということで、セルフアセスメントでこのSaaSについてはここまでちゃんとCSPが説明しているといったこと。それを基に、では、省庁として自分の業務で使っているのか悪いか。やはりどこまでいっても責任主体というものは利用省庁になりますので、当然、これですごく重要なシステムを扱う省庁がいるということも否定はできないのですけれども、ただ、繰り返しますけれども、今、既に野良SaaSについて、こういった制度が全くない中で使っている省庁がある。そういったところが、この利用の範疇に入るというふうに考えてございます。

○委員長 A～Dみたいな分類は考えていないという御意見ですか。

○デジタル庁説明者 考えていないと言うと語弊がありますが、繰り返しますけれども、既に使われてしまっている現状があって、当然、それらはある意味で各省庁としては低リスクと考えた上で使っているだろうというのが実態でありますので、当然、それ

以外の、現状の ISMAP に登録されているような SaaS というものは既に省庁としても多分、それは重要だということで考えて利用しているわけであって、一方で全く登録されていなくても、業務上、自分たちとして問題ないと考えて利用しているという実態なので、その辺りはまさにこの低リスクというふうに評価できると思っていまして、これは精緻にというよりも、繰り返しになりますけれども、既にある野良 SaaS が少なくとも全部の対象であるということが考えてございます。

その上で、新規に来る場合であれば、それは当然、一定程度、最初から機密上の必須要件を加えるということも考えますけれども、取りあえず、今、既に使っている野良 SaaS をこれは全て巻き取るというのが、繰り返しになりますけれども、課題になっていまして、では今後、新規になる場合は一旦、セルフだけではなくて、追加の必須要件を加えた上で、繰り返しますけれども、それでもやはり利用省庁が自らの判断で、自分の業務上、問題ないかというのは判断いただく。これが大前提となっていると考えてございます。

○委員 このスライド 3 ページにある、四角に囲まれているセルフアセスメント、それから、継続的な品質評価。これはどこも実施すべきであるので、これについて、全ての SaaS 運用主体に規定するというのは必要なのだろーと思います。それに加えて、この類型の中では段階的な追加の必須要件の例として書かれておりますが、制度化するとき、それほど厳しい中で緩やかな制度化、緩和されるという方向を考えると、①～⑤のようなことを後々、申請の条件にするということはなかなか難しいのではないかと、省かれてしまうのではないかとというふうに一つ懸念があります。

それから、前の 2 ページの現状の課題というところで挙がっております。私は、この制度よりもむしろ、LIU を充実すべきだというふうに考えます。LIU ができないという条件の中で、②のところでコストがかかり過ぎるということを言われていますけれども、ここの例示で挙げさせていただいたことですが、例えば約 4000 万円とか約 1600 万円、例えば約 4000 万円というものはプライム市場上場会社の会計監査で中規模のところはこのぐらいかかります。会計監査です。保証型といいますか、アシュアランス型でそのぐらいかかると思います。それから、LIU の約 1600 万円というものは、これは会社法の中小規模の会計監査、保証する会計監査でこのぐらいかかると思います。

今の ISMAP、それから、LIU が、コストがかかり過ぎているというふうに思います。監査法人は、監査意見を述べずにこの評価をやっていますから、監査法人には責任がなく工数を任意にかけられるということで、監査法人として、この ISMAP はある意味で裁量により自由に報酬を設定できる業務です。それで、幾らでもコストをかけることも可能だというふうにも考えておりますので、ぜひ今後、批判的にコスト管理といいますか、監査法人の報酬についても批判的な目を入れる形で ISMAP の制度を検討し、特に明細なところについては ISMAP-LIU をもう少し安価な形といいますか、コストを減らした形で実現をするという方向を目指していただければと思います。

○委員 直前の委員のコメントにも関係すると思いますが、先ほど御説明した中でやはり大きいと思っているのは、米国の場合、Authorization から Certification だというように改めて整理したところは大きいと思っております。そういう意味では、利用組織が最終的にはどの業務に使うかを確認するということは、Authorization だと思います。一

方、制度としては委員がおっしゃったとおり、確認をしているだけだという言い方になりますが、Certification ということだと思っていますので、その認識は我々としても整理していくべきかなというふうに思っています。

○委員長 そういったところがコストの問題であったり、適用するアプリケーションの問題であったりとかというものに関係すると思うので、その辺りはまたデジタル庁のほうできちんと整理をしていただければと思います。

○委員 これらの話は随分前にもやっていますし、JC-STAR も近い運用なのですから、ある意味、こういう非常に軽いテストを、検査環境というものを提供して、最近は自動ツールみたいな話が先ほど FedRAMP の紹介をしてくれましたけれども、そういうツールをしっかりと業界もしくは政府で提供して、次のステップのちゃんとした LIU を取るときのフィルターの役割にするというような方法は検証の中でできる。それから、調達の中にこのフィルターで、調達側としては無駄になってと言ったら怒られますけれども、たくさんの数多いものをフィルターするという、最初のフィルターでこれをやるというようなことは非常に効果的であるということは過去の経験から分かっていますので、これが Certified としてという形はいろいろな議論があると思いますが、少なくとも、このツールとして非常に最初にフィルタリングする、そういう環境をちゃんと提供するというのは極めて有効なことになるかと思っています。

○委員長 そちら辺を含めて、デジタル庁のほうで整理をしていただければと思います。

9. ISMAP 管理基準改定等について

○NCO説明者 ISMAP管理基準改定等について説明を行います。

○委員長 （委員へご意見、ご質問等を確認）

○委員 改定までのスケジュール案ですが、私は3番目の改定日の延長がよろしいかと思います。理由は、御説明にもありましたけれども、フィージビリティスタディーはしっかりやっていただくべきだと思います。特に新しい制度ですので、この時間を削ってほしくないなと思います。

加えて、パブリックコメントの意見募集も、改定案②ですと、さすがに2週間というのは短過ぎるのではないかと思います。よって、通常のパブコメと同様に、30日は設けていただきたい。世の中とのコミュニケーションをしっかり取っていただいた上で、公表用の資料の作成も、拙速な資料づくりではなくて、しっかり吟味していただきたいと思いますので、ここはしっかりと時間を取って、完成度の高い資料づくりをしていただければと思います。したがって、スケジュール案③に賛成です。

○委員 改定までのスケジュール案ですが、私も同じ意見です。いわゆる、案③がいいのではないかと。理由も、基本的にはもちろん、意見募集の期間とか、いただいているようなスケジュールでやるほうが、ある意味では安定した移行ができる、スケジュールができるのではないかと、設定ができると思っています。

○委員 スケジュールに関しましてはお二人と私も同意見でございますが、1点だけ、パブリックコメントを取るところは、このとおりで結構かと思いますが、先ほどの FedRAMP の話ではないですが、やはりコミュニケーションを十分取っていただきたいと思っています。

ますので、何か発信できること、フィードバックをどこまでもらうかというのはありますが、そういった、もう少しパブコメ以外のコミュニケーション手段も考えていただければというふうに思っていますというのが一点でございます。

2点目でございますが、説明書の対象理由のところですが、こちらは対象外パターンに関する質問です。こちらの対象外パターンに記載された理由は表に出るのですでしたか。一般には出ないのかなと思っておりますが、まず、その辺りの確認をさせてください。

あとは、実際に説明書を私も幾つか見ておりますが、説明書の内容を各省庁の担当者も理解することが難しいかと思っておりますので、これを機にコメントですが、できれば説明書そのものの全体のフォーマットをスタンダード化するといったことも検討することが必要なと思っております。説明書に関しての質問とコメントになってしまいましたが、以上です。

○NCO 説明者 今、おっしゃっていただきました理由というものは、この対象外パターン1～6のところの、これでしょうか。

○委員 そうです。その理由というものは表には出ないのですね。

○NCO 説明者 これは説明書の別添2ですか。1個前のスライドにございますけれども、現行で非採用理由のパターン、プルダウン式になっておりまして、こちらを先ほどのパターンに置き換えたいと思っております。

○委員 外に出る説明書という理解でよろしいですか。

○NCO 説明者 説明書自体は外には出ません。今、整理したのはこちらのプルダウンのところです。

○委員 分かりました。これは内部の申請ということですね。私が申し上げたのは外に出る説明書ということでございます。そこが行き違っているかもしれませんが、そういうことで、出ないということですが、そこは分かりました。

ただ、私が申し上げたかったのは、どちらかというところ、出る説明書、外に出ている説明書をちゃんと理解しやすいように整理していただければというふうに、これはコメントでございます。

最初のスケジュール案は③ということで皆さん一致しておりますので、そちらで検討いただければと思います。そのほか、4項目までありましたけれども、今までの検討の経緯を踏まえて、さらに検討をお進めいただけたらと思います。

10. 監査機関の品質モニタリング計画（2026年度）について

○IPA 説明者 ISMAP 監査機関登録規則に基づき実施した監査機関の品質モニタリング計画について、ISMAP 運用支援機関から説明します。

○委員長 （委員へご意見、ご質問等を確認）

○委員 今後のこととして検討いただきたいのですけれども、品質モニタリングの中に経済的観点、つまり、監査効率化。無駄がないか、多過ぎた手続をやり過ぎていないかというような観点をぜひ入れていただいて、専門家が必要であれば専門家も入れていただいて、ぜひ検討項目として実施いただきたいと思います。

○IPA 説明者 どういった確認方法ができるかは分かりませんが、検討していきたいと思

ます。

○委員長 他にご意見、ご質問ございましたら、よろしいでしょうか。

○委員一同 異議ございません。

11. その他について

○委員長 参考資料5として、第40回の「ISMAP運営委員会」の公開議事録が送付されています。こちらの内容で公開をしたいと思いますが、よろしいでしょうか。

○委員一同 異議ございません。

【閉会】

○委員長 （委員、制度所管省庁から発言がないため）。事務局にお返しします。

○事務局 第41回「ISMAP運営委員会」閉会及び次回開催について連絡。

以上

《議事録に関する補足等》

- 本議事録は、ISMAP運営委員会事務局である国家サイバー統括室が作成、公開しております。
- 本議事録においては、非公開情報の保護やレピュテーションリスク等を考慮し、審査に関する詳細情報（事業者による統制に関わる情報、発見事項の内容等）、ISMAPポータルサイト（<https://www.ismap.go.jp/csm>）に公表されない情報、情報セキュリティインシデントに関する情報等については、記載しないようにしています。
- 特に、情報セキュリティインシデントに関する情報については、原則、非公開情報として取り扱っております。
- それぞれの議題・議事において、ISMAP運営委員会委員により、議事の公開/非公開可否について確認しております。
- また、委員による自由闊達な意見交換を促すこと及びISMAP運営規則「2.4委員会における意思決定」を踏まえ、発言者した委員を特定しない形としております。ただし、討議及び議決に加わっていないこと等の記載について、委員の申し出により、対象となる委員名及びサービス名等を記載する場合があります。