■「政府情報システムのためのセキュリティ評価制度(ISMAP)における各種基準(案)」に対する意見公募　御意見に対する考え方　別紙

項番	該当箇所	御意見	御意見に対する回答
政府情報システムのためのセキュリティ評価制度（ISMAP）基本規程（案）			
1	P1 L25	（CIO）連絡会議決定）の定義された　「の」⇒「に」または「において」	以下の通り修正します。 「（CIO）連絡会議決定）の定義された」 ⇒「（CIO）連絡会議決定）において定義された」
2	P2 L31	「運用している」⇒「運用されている」　または　全文を「クラウドサービス事業者が、ISMAP管理基準に準拠して統制目標及び詳細管理策を選択し整備した統制を、監査の対象期間にわたり有効に運用していることを評価することをいう。」	以下の通り修正します。 「運用している」⇒「運用されている」
3	P3 L13	「本規程」⇒「基本規程」　ではないか？	文意が通じるため、原案の通りとします。
4	P3 L15	「定めたもの」⇒「定めたもの。」	以下の通り修正します。 「定めたもの」⇒「定めたもの。」
5	P3 L18	「監査対象」⇒「監査の基準」とすべきではないか。 理由：監査対象は監査を受けるクラウドサービスであり、「ISMAP管理基準」はその監査における判断に際して基準となる基準である。「基準」が重なることを避けたいならば「監査において対照とすべき」または「監査において判断の拠り所となる」としてはどうか。	以下の通り修正します。 「監査対象となる基準」⇒「監査の対象となるもの」
6	P4 L16	「セキュリティ対策を実施状況」⇒「セキュリティ対策の実施状況」	以下の通り修正します。 「セキュリティ対策を実施状況」⇒「セキュリティ対策の実施状況」
7	P6 L4	「ISMAPクラウドサービスリストに速やかに掲載し公表するものとし」とあるが、公表のフォーマットまで明記してほしい。 理由：リストがPDFで公表されるのでは再利用性が低くなるため。たとえば、XMLなどのmachine-readableなフォーマットを期待する。	今後、本制度ホームページの構築を予定しており、その中でご要望につきましても、対応を検討して参ります。
8	P8 L8-L9	「ISMAP監査機関リストへ登録されたクラウドサービス又は監査機関」⇒「ISMAP監査機関リストへ登録された監査機関」	以下の通り修正します。 「ISMAP監査機関リストへ登録されたクラウドサービス又は監査機関」⇒「ISMAP監査機関リストへ登録された監査機関」
9	P10 L2	「正当な活動への対価」⇒「活動への正当な対価」の方が分りやすくないか？	ご指摘の箇所は他の意見も踏まえて修正いたしました。
10	P10 L4	「多くの」は不要ではないか？　また「過去に」等を補ってはどうか？	ご指摘の箇所は他の意見も踏まえて修正いたしました。
11	P10 L5	「情報を統合」⇒「情報の統合」	以下の通り修正します。 「情報を統合」⇒「情報の統合」
12	P10 L15	「及びその他」⇒「及び」または「その他」のどちらかが不要ではないか？	以下の通り修正します。 「及びその他」⇒「その他」
13	P10 L17, L20	「各府省情報化統括責任（CIO）連絡会議」⇒「各府省情報化統括責任者（CIO）連絡会議」	以下の通り修正します。 「各府省情報化統括責任（CIO）連絡会議」⇒「各府省情報化統括責任者（CIO）連絡会議」
14	P10 L20	「配慮事項」はどこでその情報を入手できるか、リファレンスを示すべきではないか？	現時点において、サイバーセキュリティ対策推進会議、各府省情報化統括責任（CIO）連絡会議での決定事項はなされておりませんが、御質問の件については、例えば、本制度の立ち上げに当たり、監査のキャパシティ等を勘案しつつ、必要に応じて、 各政府機関等の利用が見込まれるクラウドサービスが速やかに審査されるよう制度運営側において調達府省庁等を支援することが考えられます。
ISMAPクラウドサービス登録規則（案）			
15	P1 L18～L19	「報告書日」⇒「報告日」	以下の通り修正します。 「3ヶ月以内を報告書日とする」⇒「3ヶ月以内を作成日とする」
16	P1 L20	「申請者は、」を冒頭に加える。	「申請者は、」を冒頭に追加
17	P2 L10	「3.3において作成する改善計画書の有無」⇒「の有無」は不要では？	ISMAPクラウドサービスリストでは、改善計画書の有無のみを公開し、その詳細はまでは公開を行わないため、原案のとおりとします。
18	P3 L13	一般に公開する項目として「(1)クラウドサービスの名称」とあるが、利用者から見てもわかりやすい項目も追加してほしい。クラウドサービス利用者から見てわかりやすい項目としては、たとえばドメイン名やURLが考えられる。 理由：名称だけではクラウドサービス利用者から見て識別しづらい場合があるため。	ご指摘も参考に、以下のとおり追記致します。 7.5 (2) 当該クラウドサービスのホームページのURL
19	P2 L27	「サービス登録を更新」⇒「サービス登録の更新」	以下の通り修正します。 「サービス登録を更新」⇒「サービス登録の更新」
20	P2 L32	「提出する」は何を提出するのか、文章中に記述がない。または「登録申請する」という趣旨の述語に置き換える必要がある。	４．１に記載のとおり、「様式3 登録申請書」に４．１に規定する文書を添えて提出いただきます。文意がとおるため、原案のとおりとします。
21	P2 L40	「実施結果報告書」は基本規程及び本規程で定義用語でなく、本規程でここが初出であるが、何の「実施結果報告書」であるか、定義がない。定義を付するべきと思われる。なお、この後も数か所で使用されているので「以下同じ」という趣旨の記述を加えることが望ましい。	基本規程３．２において、監査機関が監査基準等に準拠して監査を行った結果として実施結果報告書を作成するものであることが明記されており、文意は明らかであるため、原案のとおりとします。
22	P2 L45	申請の受理の期限および5.2を行う期限を設けるべきではないか。	5.1について、いただいたご意見も参考に以下のとおり追記致します。 5.2 ISMAP運用支援機関は、随時、申請文書の受付を行う。 5.2について、いただいたご意見も参考に以下のとおり追記致します 5.3 ISMAP運用支援機関は、申請文書を受付した日から原則として２週間以内に申請文書の確認を実施する。
23	P3 L26	「違反歴」に関しては、ないことを必要条件とすると、対象となるサービス事業者の範囲をいたずらに狭める恐れがある。違反が過去にあっても、それが是正され、有効な再発防止策が実施され、かつ報告時点でも機能していることが確認できる場合には、登録から除外すべきではない。故にその趣旨の記述を加えていただきたい。	ここでの違反歴とは、ISMAPサービス登録規則14.2(4)に規定よって削除された場合を指しており、その旨が明らかとなるように、以下のとおり本文を修正致します。 (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(4)による登録の削除を受けていないこと。
24	P3 L35	「申請を受理した日」とあるが、だれがいつ、どのように「受理」するのか明記されていない。	いただいたご意見等も参考に、以下のとおり修正致します。 6.3 ISMAP運営委員会は、ISMAP運用支援機関が申請を受理した日から原則として6カ月以内に、ISMAP運用支援機関からの報告内容及び申合せの運用状況を踏まえて、総合的に登録の是非を判断する。
25	P4 L3	「Webサイトを通じて公開する」とあるが、公開のフォーマットまで明記してほしい。たとえば、XMLなどのmachine-readableなフォーマットを期待する。 理由：　リストがPDFで公表されるのでは再利用性が低くなるため。	今後、本制度ホームページの構築を予定しており、その中でご要望につきましても、対応を検討して参ります。
26	P4 L7	「様式3」⇒「様式5」	いただいたご意見等も参考に、以下のとおり修正致します。 「様式3　登録通知書」→「様式5　登録通知書」
27	P4 L11～L12	「判断を受けて、登録要求事項を満たしていないとした」⇒「判断において、登録要求事項を満たしていないとされた」 理由：　登録要求事項を満たしているかの判断はISMAP運営委員会であり、「満たしていないとする」（この場合の「する」は内容が不明確なので適当でないが）のはISMAP運用支援機関ではない。原文のままでは、ISMAP運用支援機関が決定するかのように読めるので、文脈の再整理と、それに対応した記述とすることが必要。	「本規則の6.3に規定するISMAP運営委員会の判断を受けて、」と規定しているとおり、登録要求事項を満たしているかの判断はISMAP運営委員会が行うものであることは文意から明らかであり、原案のとおりとします。

28	P4 L11～L12	「登録要求事項」は定義としては定義されていない。「要求事項」に関しては、第3章で「申請者に対する要求事項」として記述されており、ここにおいても「第3章に規定する要求事項」と表記するのが妥当と考えられる。	登録要求事項とは登録に係る申請者への要求事項であり、文意から明らかであるため原案のとおりとします。
29	P4 L13	「登録できない」はこの種の手続きおよびその文書の表現として論理性に欠ける。ここで行われる行為は登録申請の却下であり、「登録が不可である」もしくは「登録申請を却下する」といった表記とすることが望ましい。	文意から趣旨が明らかであるため原案のとおりとします。
30	P4 L16～	まず「登録の対象となった監査の対象期間の末日の翌日から1年4ヶ月後までに、更新の申請をしなければならない」と規定されるが、最初に書かれるべきなのは登録の有効期限ではないか。 そもそも、登録に関しては、 ①監査の対象期間 ②監査結果報告書を伴って登録申請する期限（監査結果報告書の日付から一定期間であって、監査の対象期間内であるべきはずの日） ③登録の有効期限 があると考えられる。　③は登録から一定の期間後であるのが普通であると考えられるが、①を超えて登録が有効であるとすると、監査の及ぶ範囲を超えてサービスの利用が可能であることになり、制度の趣旨に反するようにも思える。 この考察を元にすると、「監査の対象期間の末日の翌日から1年4ヶ月後」まで登録の有効期限があるのはあまりに長すぎるように感じられる。 また、利用者の理解を容易にし混乱を防ぐ意味で、①最初の登録の有効期限　②登録の更新申請の期限　の順に記述していただきたい。	登録の有効期限については、ISMAP基本規程3.5において規定するものとします。 その上で、監査の対象期間が１年間であり、その後の申請及び審査に要する期間を考慮すると、１年4ヶ月という期間は適切であると考えます。
31	P5 L30	「制度運営委員会」⇒「ISMAP運営委員会」	いただいたご意見等も参考に、以下のとおり修正致します。 「制度運営委員会」→「ISMAP運営委員会」
32	P6 L21	「制度所管官庁」は「ISMAP運用支援機関」または「ISMAP運用支援機関を通じてISMAP運営委員会」が本制度の流れからして妥当ではないか。 また、その下L29とも整合する。（そうでないと、制度所管省庁→ISMAP運用支援機関の取下届出の情報の流れの取り扱いを規定しなければならない。） なお、「制度所管官庁」は基本規程において「制度所管省庁」の語で定義されており、その誤りと思われる。	いただいたご意見等も参考に、以下のとおり修正致します。 「制度所管省庁」→「ISMAP運用支援機関を通じてISMAP運営委員会」
33	P7 L2	「郵送方法」とあるが、クラウドサービスを対象とする制度において、全てを紙で手続きするという発想はいかがなものか。「記録を確認」する方法は、ITおよびインターネットを経由する通信においてもいくらでも確保できるものであり、電子署名やタイムスタンプを活用することにより、紙の文書より確実に、真正性の確認や作成時点の特定が行えると考えられる。また、政府機関がクラウドを「バイデフォルト」で使うための手続きにおいて、紙の書類の郵送を必須とすることは、考え方・発想の面で矛盾をきたすことにならないか。従い、制度の運用手段としては、クラウドサービスの活用等も嫌に入れて、全てを電子的に実施できる仕組みを整えるべきと考える。	今後、本制度ホームページの構築を予定しており、その中でご要望のオンライン申請につきましても、対応を検討して参ります。
34	P6 L37~L38 及び P7 L17	「様式14 異議申立書への回答」は、様式であるので、「様式14 異議申立書への回答書」の方が良いのではないか？	いただいたご意見も踏まえて以下のとおり修正致します。 「様式14 異議申立書への回答」→「様式14 異議申立書への回答書」
		ISMAP管理基準（案）	
35	P1 L43～L44	「注記これよりも広い定義が使われることもある。」「注記」は＜＞に入れる等の処理が必要ではないか。	以下の通り修正します。 「注記これよりも広い定義が使われることもある。」⇒「＜注記＞これよりも広い定義が使われることもある。」
36	P2 L14	「一部ついて」⇒「一部について」	以下の通り修正します。 「一部ついて」⇒「一部について」
37	P3 L35	「有す暗号」⇒「有する暗号」	以下の通り修正します。 「有す暗号」⇒「有する暗号」
38	P3 L21	「一時点」⇒「ある時点」の方が良いのではないか。 理由：「一時点」の含意は対象期間の中のあるどこかの時点であり、「ある時点」は任意の時点のように感じられる。評価はその評価時点の状態について評価を行うものであるが、評価の時点の選択において、ある程度の任意性を持つことにより、対象期間において概ね評価時点と同等の整備がなされていることが期待できる。「一時点」は時点が特定されるニュアンスが強く、それ以外の時点における整備の維持の期待を持ちにくくする感じがある。故に「ある時点」の方が望ましいと考える。	以下の通り修正します。 「一時点」⇒「ある時点」
39	P4 L11～L12	「クラウドサービス名称」⇒「クラウドサービスの名称」	以下の通り修正します。 「クラウドサービス名称」⇒「クラウドサービスの名称」
40	P4 L14	「一つのクラウドサービス名称」⇒「一つの名称のクラウドサービス」	以下の通り修正します。 「一つのクラウドサービス名称」⇒「一つのクラウドサービスの名称」
41	P4 L17	「提供している場合その」⇒「提供している場合、その」	以下の通り修正します。 「提供している場合その」⇒「提供している場合、その」
42	P5 L8	「一般に公開する」とあるが、公開のフォーマットまで明記してほしい。たとえば、XMLなどのmachine-readableなフォーマットを期待する。 理由：リストがPDFで公表されるのでは再利用性が低くなるため。	今後、本制度ホームページの構築を予定しており、その中でご要望につきましても、対応を検討して参ります。
43	P5 L21	「リージョン」はJIS Q27001, 27002, 27014, 27017において、定義がされていない用語と思われる。一般用語として定着しているものではないので、これら参照基準において定義がない場合には、本基準の1.3またはここにおいて定義-明記する必要があると考える。	とりまとめ「2.3 監査関連基準等の検討（４）リージョンとサンプリングの考え方」に記載のとおり、リージョンとは、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域を指すと考えています。この考えについてはFAQ等において示したいと考えています。
44	P5 L7及びL10	「選択性」⇒「選択制」　性質の問題でなく仕組みの問題であるので「性」でなく「制」であるべきではないか。	以下の通り修正します。 「選択性」⇒「選択制」
45	P5 L30～L34	「当該統制に係る監査の手続きを省略することができる」とあるが、手続きを省略したことを、エビデンスとして示してほしい。 理由：手続きを省略したことを、言明書の利用者が把握できるようにするため。	言明において明らかにされることから原案のとおりとします。
46	P8 L13	「意見が得られる」⇒「意見を得ることができる」　主語は「経営陣」であり、その行為の述語としては「が・・・られる」よりは「を・・・できる」の方が意味が明確になる。	JISQ27014では左記の文言が採用されているため、原案のとおりとします。

47	P8 L16～L17	「現在のプロセス及び予定している変更に基づくセキュリティ目的の現在及び予想される達成度を考慮し」⇒「セキュリティ目的の現在のプロセスによる達成度及び予定している変更に基づき予想される達成度を考慮し」 理由：文意の明確化	JISQ27014では左記の文言が採用されているため、原案のとおりとします。
48	P8 L24～L25	「必要な処置の優先順位を決めて開始する」⇒「必要な処置を優先順位をつけて実施する」	JISQ27014では左記の文言が採用されているため、原案のとおりとします。
49	P8 L27	「経営陣に付託するようにさせる」・・・「付託」の意味が不明。「報告」のことか？管理者が経営陣に何らかの行為を付託（してもらうように委託）することは、ガバナンス上おかしいので、「付託」は適切な用語と思われない。	JISQ27014では左記の文言が採用されているため、原案のとおりとします。
50	P8 L41	「"」はゴミと思われる。	「"」を削除
51	P8 L43	「文化」⇒「組織文化」　文化を実施する場が明確な方が理解しやすい。	JISQ27014では左記の文言が採用されているため、原案のとおりとします。
52	P9 L12～L13	「情報リスク及び情報セキュリティに影響する新規開発案件について、経営陣に対し注意を喚起させる」⇒「新規開発案件について、情報リスク及び情報セキュリティに与える影響について評価し報告させる」 理由：文意の趣旨からこう表記する方が理解しやすいと考える。	JISQ27014では左記の文言が採用されているため、原案のとおりとします。
53	P9 L29	「その」が何を指すか、文章の構造から特定が困難なので、具体的に書くべきである。	以下の通り修正します。 「そのとるべき」⇒「経営陣の方向性及び決定を支援するためにとるべき」
54	P9 L33～L35	この文章は全体として意味、意図するところが理解しにくい状態にある。言わんとするところを勝手に想定して文章を構成するとすれば次のようになる。このように書くことが分りやすくすることになると考える。 「保証は、経営陣が独立した客観的な監査、レビュー又は認証を外部の第三者に委託するガバナンスプロセスである。それにより、目標とするレベルの情報セキュリティを達成するためのガバナンス活動の目的及びその実行と運営のための処置を特定し、ガバナンス活動の妥当性を検証する。」	以下の通り修正します。 「これは、レベルの情報セキュリティ」⇒「これは、望ましいレベルの情報セキュリティ」
55	P9 L38	「意見を委託する」⇒「意見の提供を委託する」 理由：「意見」は行為ではないので委託できない。	JISQ27014では左記の文言が採用されているため、原案のとおりとします。
56	P10 L10	「サービス提供者」⇒「クラウドサービス事業者」 理由：クラウドサービスを提供するものは「クラウドサービス事業者」として定義されている。	以下の通り修正します。 「クラウドサービス提供者」⇒「クラウドサービス事業者」
57	P10 L18	「情報セキュリティマネジメント確立」⇒「情報セキュリティマネジメントの確立」	以下の通り修正します。 「情報セキュリティマネジメント確立」⇒「情報セキュリティマネジメントの確立」
58	P10 L22	「：」　ゴミ？	「：」は以下この構成で続くという表現のため、原案のとおりとします。
59	P10 L20及びL31	「トップマネジメント」は「経営陣」と同じ意味でしょうか。突然出て来る感じで、かつ日本語で何を意味するか、「経営陣」より、人により受け止め方が変わる可能性が高いと思われる。もしさして違いがないなら「経営陣」に統一すべきだし、区別して使うなら、どう使い分けているか、分るようにすべきだと考える。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
60	P11 L5～L6	誰の「責任及び権限」を誰に割り当て、誰に伝達するのか、明確でないので、明確にしてほしい。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
61	P11 L11	「責任・権限を割り当て」⇒「責任・権限を組織に割り当て」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
62	P11 L14～L15	「責任･権限を持つリスク所有者」⇒「リスク所有者の責任・権限」 理由：①他の項と形を揃える　②本文の記述との整合性をとる 関連意見：なお、「リスク所有者」は「リスクオウナー」の日本語化と思われるが、「リスクを所有する」という日本語は意味的になじまない。またownerは必ずしも所有者を意味しないことから、「リスク責任者」「リスク管理者」「リスク対応責任者」のような、日本語として意味が通じる言葉に置き換えることを提唱したい。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
63	P11 L20~L23	「管理層」⇒「管理者」 理由：両者は同じ意味で使われていると考えられるが、第3章では「管理者」が使われており、用語の統一が必要と考える。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
64	P11 L26～L27	「組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える」⇒「組織の目的に関連するとともに、情報セキュリティマネジメントが目指す成果の達成に向けた組織の能力に影響を与える」 理由：文章の意味をより捉えやすくするために。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
65	P11 L34	「を問わず」⇒「における」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
66	P11 L36	「原動力及び傾向」⇒「影響因子及びその傾向」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
67	P11 L41	「知識として見た場合の能力」⇒「知的財産」 理由：原文は違うかもしれないが、例示からすると意味としてはこのように解釈でき、日本語としてこなれる。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
68	P11 L37及びL44	「ステークホルダ」と「利害関係者」が場所により両方用いられているが、同じ意味、同じ用語と考えられる、全体を通じてどちらかに統一することが望ましい。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
69	P12 L4	「決定」⇒「定義」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
70	P12 L41	「を問わず」⇒「における」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
71	P12 L43	「原動力及び傾向」⇒「影響因子及びその傾向」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
72	P13 L2	「知識として見た場合の能力」⇒「知的財産」 理由：同上	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
73	P13 L19	「"」はゴミと思われる。　また、タブ位置がおかしい（他と違う）	「"」を削除
74	P13 L27	「更新するとともに」⇒「更新する。また」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
75	P13 L28	「決定」⇒「定義」　または「決定する」⇒「定める」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
76	P13 L39	「文書化され」⇒「文書化し」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。

77	P14 L14	「ことを確認するとともに、当該計画を作成する際、各対処計画が、情報セキュリテ」⇒「ことを確認する。また、当該計画を作成する際、各対処計画が情報セキュリテ」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
78	P14 L15	「実施されるよう、考慮するとともに、」⇒「実施されるよう考慮するとともに、」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
79	P15 L2	「リスク所有者」は「リスクオウナー」の日本語化と思われるが、「リスクを所有する」という日本語は意味的になじまない。またownerは必ずしも所有者を意味しないことから、「リスク責任者」「リスク管理者」「リスク対応責任者」のような、日本語として意味が通じる言葉に置き換えることを提唱したい。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
80	P15 L16	「"」はゴミと思われる。	「"」を削除
81	P16 L7	（）内「。」をトル。	（）内「。」を削除
82	P18 L3	「に基づいて」⇒「を提供して」または「の機会により」または「によって」 理由：「力量を備える」に対応する施策としては、これらを提供する必要があり、「に基づいて」はそぐわない。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
83	P18 L9	「"」はゴミと思われる。	「"」を削除
84	P18 L10及びL12	「つける」「着ける」　用字の統一を。	以下の通り修正します。 「つける」⇒「着ける」
85	P18 L17	「持てた」⇒「得られた」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
86	P19 L6	「。」は不要では？	「。」を削除
87	P19 L14及びL17	重複しています。	L17「情報セキュリティマネジメントを本管理基準の要求事項に適応させる権限者」を削除
88	P19 L28	「活動を実施するために必要な」⇒「活動の実施に必要な」 理由：「ため」の連続をされるため。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
89	P19 L32	「確信」は「確認」の方がそぐうのではないか。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
90	P19 L32	行末の「、」はトル。	行末の「、」を削除
91	P20 L5	「"」はゴミと思われる。	「"」を削除
92	P20 L24	「"」はゴミと思われる。	「"」を削除
93	P20 L23～L24	「継続的改善においては、これまで実施してきた管理策だけはなく、」までは継続的改善についての記述だが、「環境の変化に伴う新たな脅威やぜい弱性についても不適合を検出し処置する。」は新たな対処についての記述であり、継続的改善とは別の取り組みになる。一つの文章の中で二つのことを言っており、文意をわかりにくくしている。もし、後者も継続的改善の一環と位置付けているのであれば、例えば、「継続的改善においては、これまで実施してきた管理策だけはなく、環境の変化に伴う新たな脅威やぜい弱性に対する不適合の検出と処置による改善も含める。」などとしてはどうか。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
94	P21 L18	「"」はゴミと思われる。	「"」を削除
95	P20 L21	「維持する」⇒「維持を行う」 理由：「維持する」は、この用法においては、一語の動詞である。文意は計画、確立、実施に維持も含めた行為を行う、ということと理解できるが、「維持する」としてしまうと、「計画、確立、実施」を受ける動詞がなくなってしまう。故に助詞の「を」入れることで計画、確立、実施、維持の全てを受ける動詞（この場合「行う」）につなげる。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
96	P20 L24	「監査計画を実施する」⇒「監査を実施する」がより正確な表記ではないか。あるいは「監査計画を策定する」か？	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
97	P21 L44	「"」はゴミと思われる。	「"」を削除
98	P22 L9	「組織は」の前のスペースを削除	「組織は」の前のスペースを削除
99	P22 L13及びL14	「及び」と「と」はどちらかに揃えることが望ましい。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
100	P22 L15	「責任者」は監査の責任者であるか？明確にすることが望ましい。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
101	P22 L19～L20	「マネジメントレビューする」⇒「マネジメントレビューを行う」	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
102	P22 L26	「書」は不要？	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
103	P23 L4	「有効性の改善」⇒「有効性の検証」 理由：「有効性の改善」は活動の結果であって活動項目とは言えないので、この行を削除するか「有効性の検証」などに置き換えるべきではないか。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
104	P24 L41	「"」はゴミと思われる。	「"」を削除
105	P25 L24	「法律」⇒「法令」 理由：他の場所での用法に合わせる。	以下の通り修正します。 「法律」⇒「法令」 また、同様の記述として以下も修正する。 ・P14 L35 ・P15 L40 ・別表2　4.4.7.1内 ・別表2　4.4.7.4内 ・別表2　4.9.1.1内
106	P25 L39	「関連情報」は確実にする事項とはとらえにくい。（関連情報の）提供、共有、確認、等の行為を示す言葉を補うべきではないか。	以下の通り修正します。 「関連情報」⇒「関連情報の提供」
107	P28 L20	「遂行」⇒「履行」 理由：責任や義務は「遂行」より「履行」がなじむ。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
108	P29 L5	このサービス機能については「提供し」の行為も指定すべきではないか。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
109	P29 L10	この「手順」については「策定し」または「確立し」も入れるべきではないか。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
110	P29 L26	この「プロセス」については「策定し」または「確立し」も入れるべきではないか。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
111	P29 L33	この「プロセス」については「策定し」または「確立し」も入れるべきではないか。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
112	P30 L28～L31	管理策として「9.5.2.2.PB クラウドサービス事業者は、要塞化するにあたって参考にした基準を明記する。」を追加してほしい。 理由：　要塞化のベースラインを、言明書の利用者が把握できるようにするため。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。

113	P31 L4	「用いる」は「実施する」の方が良いのではないか？	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
114	P32 L2	「システム資源の使用を満たすことを確実に」において、「使用を満たす」は日本語としてなじまないので「満たす」は「担保する」または「保障する」に置き換えるか、または単に「システム資源の使用を確実に」としてはどうか。 なお、別表3にある詳細管理策の文脈からは「システム資源の利用が組織の目的を満たすことを」とする変更も有効ではないかと考えられる。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
115	P32 L40	この「手順」については「策定し」または「確立し」も入れるべきではないか。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
116	P33 L6	「運用」は「情報」ではないか？	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
117	P33 L21	管理策として「13.1.5.P インターネットからアクセスする場合に、クラウドサービス事業者のドメインが正しいことを確認する手段を提供する。」を追加してほしい。 理由：政府機関が利用するクラウドサービスでは、ドメインの乗っ取りのリスクが高いため。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
118	P33 L25～L26	「合意」が何を指すか、明確でないと感じる。原語がagreementであるとすると、この文意の日本語表記としては「組織と外部関係者との間の業務情報のセキュリティを保った転送について、契約に明記する。」といった形とするのが適当ではないか。	経済産業省が策定する情報セキュリティ管理基準において左記の文言が採用されているため、原案のとおりとします。
119	P33 L38～L40	ここに列挙される箇条項目は、他の部分での表記法に合わせるなら、箇条ごとに改行されるべきではないか。	箇条ごとに改行を追加しました。
120	P35 L25	「adversesituation」⇒「adverse situation」	以下の通り修正します。 「adversesituation」⇒「adverse situation」
121	P36 L6	PIIはいきなり出てくる単語であり、日本の基準の中でそのまま使うには定着しているとは言えない。「個人識別情報」に置き換えるか、それを補う必要がある。	以下の通り修正します。 「PII」⇒「個人識別情報」
122	P36 L11	「記載」⇒「情報」ではないか？	以下の通り修正します。 「実装した暗号化機能の記載を」⇒「実装した暗号による管理策の記載を」
ISMAP管理基準　別表３			
123	6.1.1.4	「この責任」　対象となる責任を具体的に記述するか、「6.1.1.3に規定する責任」のように特定する語を補うべきである。 理由：　6.1.1.4は管理策として独立した箇条であるので、別の箇条を受けて「この」としても、「どの」が特定されない。	別表３に関していただいている意見については、意見公募対象外であるため、個別のご意見ごとの回答は差し控えます。なお、ご意見については、文言の修正について基本的には情報セキュリティ管理基準等の内容に即して判断しており、そのほか必要に応じてご意見を踏まえた修正を行うこととしております。
124	6.1.1.5	「局所的(local)」は具体的に何を指すかイメージしにくいので、例示等により具体的イメージが分るようにしていただきたい。	－
125	6.1.1.6	「責任は依然としてその個人にあり、」は主語に対応しない記述であるので、「責任は依然としてその個人にあることを認識し、」など、主語である「個人」の行為となる記述に改めるべきである。	－
126	6.1.1.11	「個人が責任をもつ領域を規定するために、情報セキュリティ分野における責任を果たせるよう」は・・・ために、とその後の行為の対応関係がない。「個人が責任をもつ領域において」等に変更するべきである。	－
127	6.1.1.11	「任命された個人が当該分野の力量をもつこと」はそれを受ける述語がない。「持つことを確認し」または「持つことを確実にし」などの述語を補うべきである。なお、その場合、続く「及び」は不要となると考える。	－
128	6.1.2.1	「ように注意する」は表現として弱く、抑止力にならないので「管理策を適用する」または「手順を整備する」等の具体的対策を指定すべきではないか。	－
129	6.1.3.3.PB	「国々を通知する」⇒「国々及びその法管轄を通知する」 理由：　国名だけでは、当該施設の立地やクラウドサービス事業者における当該施設に関する契約等の関係において、法管轄が特定されない恐れがある。利用者にとってのリスクは法管轄がとこ化による面が大きいので、法管轄も合わせて通知するようにすべきである。	－
130	6.1.4.4 及び 6.1.4.5	これらの管理策の手段としては、商用サービスの購入や利用も考えられるので、そうした対策を手段として補っていただきたい。	－
131	6.2.1.22	エンドユーザ合意書の内容には、個人所有のモバイル機器の譲渡・売却・買い替え等に際しての事前承認やデータ消去に関する義務等も盛り込むべきではないか。	－
132	7.1.2.2	「契約には、・・・署名を行う。」は論理的対応関係が整合しないので「署名を含める」等の述語に変更すべきではないか。	－
133	7.2.2.17	「沿っている」は状態を指す言葉で行為を示さないので「沿って定める」「沿ったものとする」等の述語に置き換えるべきではないか。	－
134	8.1.1.3	「文書」「既存の目録」等の言葉が意味するところが理解できない。この管理策の意図する意味はむしろ「目録は、専用の文書または既存の文書として維持する。」ではないか。ただし、「既存の」の意味する所は依然として理解が困難である。「存続すべき」といった意図か？	－
135	8.1.2.3	「目録を作成する仕組み」⇒「目録を作成し維持する仕組み」 理由：目録は作成するだけでなく最新のものに維持することが重要で、その仕組みも用意すべきである。なお「維持する」だけでは厳密には最新のものとして、という意味は含まれないが、本管理基準全体を通して「維持」は最新のものへの更新を含む用語として用いられていると解釈されるので、とりあえず「維持する」とした。そうでない場合は「最新のものに」を補っていただきたい。	－
136	8.1.4.4	「複製」だけでなく「削除」も含めるべきではないか。 理由：解雇の通告を受けた従業員は、組織に対して否定的な感情を持つ可能性があり、その発露として重要な情報を破壊することが考えられる。その防止策も講じるべきである。	－
137	8.1.5.P 及び 8.1.5.2.P	「時期」⇒「時機」ではないか？	－
138	8.2.1.3 乃至 8.2.1.10	「分類体系」または「分類」の前に「情報の」を補うべきではないか。 理由：各管理策は独立した箇条であり、「分類」は何の分類であるか特定しないと意味が分かりにくい恐れがある。	－

139	8.2.1.6	「それぞれのレベル」⇒「情報の分類体系におけるそれぞれの保護レベル」 理由：独立した箇条として意味がつかめるように。	—
140	8.2.2.2, 8.2.2.3, 8.2.2.5	「ラベル」⇒「情報のラベル」 理由：独立した箇条として意味がつかめるように。	—
141	8.2.3.4	「複製は」⇒「複製を」　助詞の選択の是正	—
142	8.2.3.5	「IT資産は、」⇒「IT資産を、」　助詞の選択の是正	—
143	8.2.3.6	「複製には、」⇒「複製に、」　助詞の選択の是正	—
144	8.2.3.7	「他組織から又は他組織への分類ラベル及びアクセス制限を解釈する」⇒「他組織からの又は他組織への分類ラベル及びアクセス制限の解釈を伝達する」	—
145	8.3.1.5 乃至 8.3.1.8	「媒体の管理のために」⇒「媒体の管理において」 理由：「ために」の重複により論理の組み立てが分りにくくなることを避けるため。	—
146	9.1.1.2	「アクセス制御」は「アクセス制御方針」ではないか？	—
147	9.1.1.3	「サービス提供者」⇒「クラウドサービス事業者」 理由：クラウドサービスを提供するものは「クラウドサービス事業者」として定義されている。	—
148	9.2.2.1	（）内末尾に「。」を付す。	—
149	9.2.2.4	「サービス提供者」⇒「クラウドサービス事業者」 理由：クラウドサービスを提供するものは「クラウドサービス事業者」として定義されている。	—
150	9.2.3.10	（）内末尾に「。」を付す。	—
151	9.2.4.8	「業者」は定義されていない用語であり、具体的に指定することが望ましい。	—
152	9.3.1.1	「助言」は「要求」「支持」または少なくとも「通知」の方が強制力を伴うので良いのではないか。 以下9.3.1の詳細管理策において、基本的に同じ。	—
153	9.4.4.8	「不要な」がどこまでかかるかわかりにくいため、「システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムで不要なものは、」と語順を入れ替えて明確化する。	—
154	9.4.4.11.P	「プログラムは」⇒「プログラムの利用は」または「プログラムの使用は」または「プログラムへのアクセスは」等に変更する。 理由：制限の対象は行為であり、「プログラムを制限する」は論理的対応性に欠けるから。	—
155	9.5.1.1.P	「クラウドサービス利用者の使用する資源からのクラウドサービス事業者の内部管理を分離するため」において「資源からの」の「の」は取るべきであるが、文意をより明確かつ分かりやすくするため、「クラウドサービス事業者の内部管理からクラウドサービス利用者の使用する資源を分離するため」としてはどうか。	—
156	10.1.1.4	「鍵が紛失、危険又は損傷した場合」のうち「危険」は文脈的にも論理的にもそぐわないので、意図された文意に沿った他の用語と置き換えるか、削除する。	—
157	10.1.1.8	「組織の方針を実施するときには・・・規制及び国内の制約を含める。」は何に「含める」のか不分明である。「含める」べきは「規制及び国内の制約」への対応または対処であると考えられ、含める対象は「実施」ではなく「方針」そのものまたは「策定」もしくは「検討」等の行為であろうと推察される。この推察に基づく変更案としては「暗号に関わる組織の方針の決定に際しては、・・・規制及び国内の制約への対処を含める。」等が考えられる。	—
158	11.1.1.2, 11.1.1.5, 11.1.1.6	1.～4.または1.2.の箇条の文末に「。」を付す。	—
159	11.1.2.7	「維持及び監視する」⇒「記録し維持する」 理由：日誌や監査証跡は「監視」対象としてなじまない。むしろ維持もしくは保存が重要である。	—
160	11.1.5.1	「要員は、」は不要ではないか。	—
161	11.1.5.4	「記録装置（例えば、携帯端末に付いたカメラ）は、」⇒「記録装置（例えば、携帯端末に付いたカメラ）の持ち込み及び利用は、」 理由：不許可の対象となる行為を特定する。	—
162	11.1.6.1	「識別及び認可された要員に制限する」は論理矛盾ではないか？	—
163	11.2.1.4	「それ以外の装置を分離」⇒「それ以外の装置から分離」	—
164	11.12.1.5	脅威には静電気も含めるべきではないか。	—
165	11.2.3.3	1.～4.の箇条の文末に「。」を付す。	—
166	11.2.3.3	小動物の行為による短絡、食害、排泄物等による化学的損傷に対する防護を加えるべきではないか。	—
167	11.2.4	保守を、装置の供給者又は供給者の指定する第三者に委託する場合の管理策も必要ではないか。11.2.4.2及び11.2.4.4に規定する保守要員が組織の外部の者である場合には、これら管理策の内容では不十分で、委託先組織の契約上の責任、保守要員のセキュリティ上の管理や技術・スキル等に対する要求条件の保障等の要件を明示することが望ましい。	—
168	11.2.5.2	「資産の持出し期限を設定し、また、返却がそのとおりであったか検証する。」⇒「資産の持出し及び返却の期限を設定し、また、返却が設定された期限であったか検証する。」 理由：意図する管理策の明確化。	—
169	11.2.5.3	「記録は定期的及び必要な時にレビューする。」を追加する。	—
170	11.2.9	（脚注）以下は、全く同じ内容が11.2.9.1に規定されているので不要ではないか？	—
171	11.2.9.2	「電子記憶媒体」⇒「可搬型電子記憶媒体」 理由：可搬型以外の電子記憶媒体はこの管理策による保護の適用は不可能もしくは著しく困難である。	—
172	11.2.9.5	コピー機、スキャナ等の内部記憶装置に残留するデータの管理についても規定すべきではないか。	—
173	12.1.2.9	「備える」⇒「整える」	—

174	12.1.3.7	「上記の」⇒「12.1.3.5及び12.1.3.6による」 理由：箇条外の個所を指して「上記の」とすることは、独立した箇条としては不適当なので、どの管理策によるか特定できるよう管理策番号で指示する必要がある。	－
175	12.2.1.7	「レビューの実施。」⇒「レビューを実施する。」	－
176	12.2.1.7	「調査する」⇒「調査して原因を解明する」	－
177	12.2.1.8	1.及び3.の箇条の文末に「。」を付す。	－
178	12.2.1.12	「情報を収集」⇒「マルウェアに関する情報を収集」	－
179	12.2.1.13	1.及び2.の箇条の文末に「。」を付す。	－
180	12.3.1.17.P 乃至 12.3.1.23.P	各管理策の行頭に「クラウドサービス事業者がクラウドサービス利用者に提供する」を加える。 理由：各管理策の目的を、個別管理策ごとに正確に表記するため。	－
181	12.4.2.1	冒頭に「ログ情報は」を補う。 理由：対象を特定するため。	－
182	12.4.3.2	文末に「。」を付す。	－
183	12.4.5.2.P, 12.4.5.3.P, 12.4.5.5.P	冒頭に「12.4.5.1.Pによる」を補う。 理由：単独で見た場合に何の監視機能かわからないため。	－
184	12.5.1.8	何の変更か具体的に明記する。	－
185	12.6.1.11	1.～4.の箇条の文末に「。」を付す。	－
186	12.6.2.2	行頭に「組織は、利用者がインストールしてもよいソフトウェアの」を補う。 理由：何の特権かわかるようにするため。	－
ISMAP監査機関登録規則（案）			
187	P1 L30	申請者に対する要求事項には、申請者の組織としての業務執行能力を確認するための指標や情報が必要ではないか。具体的には財務の健全性とコーポレートガバナンスが機能していることを確認する情報を要求すべきと考える。財務の健全性の最低ラインとしては、例えば、債務超過でないことが考えられる。コーポレートガバナンスについては、経済産業省によるCGSガイドラインが求めるガバナンスのための施策を実施していることを具体的に示す組織図や議事録または報告書等の提出等を求めることが考えられる。 なお、政府機関の調達手続きに関しては、各府省が登録審査の精度を有しているところ、そのような制度を適用することも考えられる。 また、ISMAP監査ガイドラインが示す監査機関に要求される義務を履行できる能力を有すること、といった要件定義も考えられる。	法人としての業務遂行能力に関しては、3.2準拠規程等において、基本規程やISMAP情報セキュリティ監査ガイドライン等の本制度の規程等に準拠して業務を遂行することを要求しており、また、3.4業務品質において、情報セキュリティサービス規準審査登録制度において情報セキュリティ監査サービスに登録されていることを要求することで、本制度における監査業務を適切に遂行するために必要となる品質管理体制を備えた組織であることを担保することが可能と考えます。よって、原案のとおりとします。
188	P2 L5	別表2に示す組織が、「・・・を行う機能を有する」との判断は、どのような公的基準に基づき、公的にまたは一般に妥当と判断されるどのような評価手法及び手続によって行われたのか、脚注等によって示していただきたい。	3.5.1に規定しているとおり、情報セキュリティ監査の実施状況等について審査を行い、必要に応じて倫理審査に諮り、処分を行う機能を有することが確認できた組織を別表２にお示ししております。
189	P2 L17	以下の各箇条の末尾に「。」を付す。	各箇条の末尾に「。」を追加
190	P2 L23及びL37	クラウドコンピューティングに関する知見の例として、一般に知られている資格等、例えばCCSK (Certification of Cloud Security Knowledge) を示してほしい。 理由：具体的な知見およびそのレベルを示すため。	クラウドコンピューティングに関する知見は、特定の資格の取得状況に限らず、過去の実務経験等も踏まえて総合的に判断を行うものとします。
191	P3 L12	「制度規定」とは具体的に何か、説明または例示する用語を補うか、脚注等で示すことが望ましい。	文中の「制度規定」とは、ISMAP基本規程を指すため、以下の通り修正します。 「制度規定」⇒「基本規定」