別紙4

「地方公共団体における情報セキュリティポリシーに関するガイドライン」（改定案）等に対する意見募集結果について

令和６年１０月２日
総務省自治行政局住民制度課
デジタル基盤推進室

令和６年９月１２日（木）から９月２０日（金）まで、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（改定案）等に対する意見募集を行ったところ、４３件の御意見が寄せられました。

提出された御意見及びその御意見に対する考え方を次のとおり公表します。

なお、「地方公共団体における情報セキュリティポリシーに関するガイドライン」及び「地方公共団体における情報セキュリティ監査に関するガイドライン」については、令和６年１０月２日（水）に改定・公表を行いましたので、お知らせいたします。

No.	提出者	該当資料	該当ページ（改訂版における該当ページを掲載）	御意見	御意見に対する考え方
1	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	―	選挙時の共通投票所や申告受付会場から個人番号系ネットワークへLTE回線等の優先でない閉域網で接続する際の留意事項や制約などの記載が以前からないが問題ないのでしょうか。	個別分野につきましては、制度所管部局がそれぞれ対策を示している場合があるため、地方公共団体から質問があった際に、制度所管部局との調整を踏まえ、個別に対応を行っています。
2	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	―	（１）令和５年度の「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、 「ウイルス」→「不正プログラム」、「証跡」→「ログ」と用語の整理がされたと理解しているが、 本ガイドライン案については、用語の統一が反映されておらず、一つの文書であるにも関わらず全体を通して一貫性がありません。 「パターンファイル」「ウイルス情報」「ウイルス定義体」「ウイスル定義ファイル」「アンチウイルス」「ウイルス対策」「不正プログラム対策」「コンピュータウイルス対策」などといった本文中にある用語のゆれらしきものは、統一基準群に準拠する形で整理されるべきではないでしょうか。 （２）不正プログラムに「感染」という表現は、「感染」という病理学上の用語を定義なしに流用しており、情報システムにおける「感染」とはどういった状態を指すのかインシデント対応の観点からも明示的に定義されるべきではないでしょうか。 仮に病理学的な定義を流用すれば、自己を複製する機能を持つ不正プログラムが実行されている状態を指すと思われるが、文脈上必ずしも自己を複製する機能を持った不正プログラムが実行されている状態のみを本文書は「感染」と想定している訳ではないはずです。「感染」について、適切な用語に置き換えた表現とするか、「感染」とは何か用語を定義されるべきではないでしょうか。 また「ウイルス」、「感染」という用語は特定の商用製品を想起させる用語であり、公平性の観点からも中立であるべき地方自治体に相応しい用語ではないのではないでしょうか。	(1)今後、用語の定義を明確にし、「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」などを参考に整理します。 (2)「ウイルス感染」は、特定の製品に用いられる用語ではなく、「コンピュータウイルス対策基準」（平成7年7月7日通商産業省告示第429号）で規定され、独立行政法人情報処理推進機構（IPA）HPの「コンピュータウイルス・不正アクセスに関する届出について」等において用いられており、現行の記載としております。 ・コンピュータウイルス対策基準（平成7年7月7日通商産業省告示第429号） https://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm ・IPA　「コンピュータウイルス・不正アクセスに関する届出について」 https://www.ipa.go.jp/security/todokede/crack-virus/about.html また、「地方公共団体における情報セキュリティポリシーに関するガイドライン」における「不正プログラムに感染」の用語は、「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」と同じ意味で使用しております。 ・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（令和５年度版） https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf
3	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-67	iii-67の「図表 41 情報の機密性に応じた機器の廃棄等の方法」において、 「（２）自治体機密性２以上に該当する情報を保存する記憶媒体（上記（１）に該当するものを除く。）」の 「OS 等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、」について、 「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」のP124において、HDDとSSDの違いにより取り扱いが異なることと「不良セクタ」に対しては有効ではない旨の記載があり、 同ガイドラインのP125以降の「機密性の高い情報の抹消方法の例」において、データ消去ソフトウェアによるものは、例示されておらず、消去方法の基準を同ガイドラインに準拠したものにするべきではないでしょうか。	ご指摘の通り、NAND型フラッシュメモリのSSDはウェアレベリングにより、データ抹消ソフトウェアによる上書きの１回では、消去すべき情報が残ってしまうことがあるため、磁気ディスクとは異なる注意点があります。SSDのデータ消去のあり方については、今後、地方公共団体の要望等を踏まえ検討いたします。
4	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	ii-29 ii-37	ii-29の「パスワードの管理」の7の「サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。 」について、 総務省の「国民のためのサイバーセキュリティサイト」では「パスワード管理ツール」の利用を推奨し「スマートフォンやWebブラウザ標準機能、あるいは専用のアプリケーションのパスワード保存機能を活用しましょう。」としており、総務省として考え方を統一すべきでないでしょうか。 （https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/06/） また同サイトにおいて「定期的な変更は不要」としているにも関わらず、 ii-37において「（カ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。 」 というように「パスワードの定期的な変更」を求める表現についても、最新の知見で定期的な変更が有効でないというものがあるのであれば、見直されるべきではないでしょうか。	「国民のためのサイバーセキュリティサイト」のパスワードの保管では、利用する各サービスごとに異なるパスワードを管理するのは負担が大きいため、パスワード管理ツールを活用した認証等により、サービスへのアクセス時に認証を行うことを推奨しています。 一方、ガイドラインの「⑦サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。」は、 サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させることで、認証を回避することを禁止する規定です。 そのため、ガイドラインと「国民のためのサイバーセキュリティサイト」では趣旨が異なりますが、ガイドラインでは認証の回避という目的が判りづらいため、御指摘を踏まえ、下線部のとおり記載を修正します。 「⑦サーバ、ネットワーク機器及びパソコン等の端末に、パスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。」 また、ご指摘のあった（カ）につきましては、一般の利用者ではなく、特権IDが付与された利用者を対象としたものであり、御指摘を踏まえ、下線部について記載を修正いたします。 「（カ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID及びパスワードについて、人事異動の際のパスワードの変更、入力回数制限等のセキュリティ機能を強化しなければならない。 」
5	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	―	e-Govにて「難病の患者に対する医療等に関する法律」や「障害者の日常生活及び社会生活を総合的に支援するための法律」に関する厚生労働省などが所管する手続きに関しては、都道府県が受託事務しておりますが、そのようなことに関してもセキュリティ面を対応して手続きが行われればよいと思います。 また、自治体クラウドの併せて早急にご対応頂きますよう何卒よろしくお願いいたします。	ご意見は今後の施策検討の参考とさせていただきます。

No.	提出者	該当資料	該当ページ（改訂版における該当ページを掲載）	御意見	御意見に対する考え方
6	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-31 iii-32 iii-184	・iii-31 図表23について 機密性３Ｂについて、ISMAP登録サービスであれば利用可とあります。一方で情報資産の例としてはマイナンバー利用事務系の情報も含めて記載されていますが、条件として3.情報システム全体の強靭性の向上（例えばマイナンバー利用事務系の情報を扱うのであればマイナンバー利用事務系から接続し、接続先がインターネットに接続されていないこと等）を前提とすることを記載しなければならないと考えます。そうでないとインターネットに接続されているISMAP登録済のパブリッククラウドサービスにマイナンバー利用事務系の情報資産を登録して利用できると思われてしまうのではないかと考えます。 また、ISMAP登録サービスという点について、SaaSの場合、基盤がISMAPに登録されていればよいのか、基盤とその上に構築されているシステムの双方がISMAPに登録されている必要があるのか等、明確にすべきと考えます。 ただし、基盤とその上に構築されているシステムの双方がISMAPに登録されている必要があるとなった場合は、図表12にも記載されている通り、地方公共団体にとって利用可能なサービスはとても限られます。すでに導入済のサービスが使えなくなる等サービス低下につながるのではないでしょうか。 ・iii-32　図表24について 地方公共団体が管理する個人情報等はインターネット上に一時的にしか保管されていないのでしょうか。サイバー攻撃のリスクはもちろんありますが、一般企業ではインターネットでの取引は当たり前になっており、常にインターネット上に保管されている個人情報も多くあると思います。現に地方公共団体でもインターネット上に常に保管されている個人情報もあるように思われますが、あえて一時的に保管されると説明をしている意図があるのでしょうか。 ・iii-184　8.3(3)⑦について 推奨事項のままですが、図表23でISMAP登録サービスは利用可としていることと整合性が取れていないと考えます。本項から推奨事項を外すか、図表23を推奨事項にすべきと考えます。図表23に「参考にされたい」とありますが、元々必須ではなく推奨という意味がこめられているのでしょうか。	図表23について ISMAP制度の動向や地方公共団体が利用しているクラウドサービスの利用状況の実態等を踏まえ、今後検討いたします。 図表24について インターネットから申請を受け付ける場合は、インターネット領域でシステム処理が必要であり、一時的に申請データがインターネット上に存在する状態になります。業務システムの設計によりますが、インターネット接続系で一時的な保存を行うシステムをここでは扱っています。一つ一つのトランザクション処理が独立しており大量の情報資産を含む台帳とはなっておらず、あくまで一時的な保存であり恒常的な保存ではない点等を考慮し、自治体機密性３C以上の情報に求められる対策が必要としています。 8.3(3)７、図表23について 自治体機密性２について、ISMAP登録サービスの利用は推奨としております。
7	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	ー	本書におけるISMAPの立ち位置と必要性をもっとわかりやすく記載されたい。 長年メンテナンスされてきているので、どこかのタイミングでリファクタリングして、 わかりやすいガイドラインにされてはどうか。 過去の経緯は、末尾でも構わないですし、すべきことを端的に記載するようにしていただきたい。 詳細化はよいが、冗長な部分もありそうで、わかりづらい。	いただいたご意見は、今後の施策検討の参考とさせていただきます。
8	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	ii-16	今回の改定で自治体機密性という区分が作られましたが、住民が国の機密性と自治体の機密性を区分することは困難であり、自治体においても取り扱いが不明瞭になることが懸念されます。 そもそも国、自治体含む行政のセキュリティを統一化していくことを目的としてガイドラインを示している趣旨にも反すると考えます。 機密性の区分についてはこれまでどおり自治機密性ではなく機密性とし国と同じ表記にしていただきたい。	機密性分類については、「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」において、 ・地方公共団体が扱う住民の個人情報の量や種類、頻度が大きく重要であることを鑑み、国（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）のように、住民の個人情報を「機密性２」に分類するのではなく、引き続き「機密性３」に分類すべき ・このように国と中身が異なるにも関わらず、地方公共団体についても同じ「機密性」の用語を用いると混乱を招く懸念があるため、「自治体」の用語を機密性分類の名称に使用すべき との意見があったことを踏まえ、「自治体機密性」の用語を使用することとするものです。
9	法人	地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会(第12回)資料	ー	「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会(第12回)資料」において、α’モデルのリスクアセスメントについて記載されていますが、脅威レベルについての説明がありません。「最も高い3（脅威が発生しやすい）」と書かれていますが、何がどうなっていたら発生しやすいのかという説明がありません。すぐにでも発生する、あるいは数年に一度とされても何も裏付けがなく、数値に対する客観性を見出せません。逆に、発生しにくいと思われていたことが起こってしまっているのが現実なのではないでしょうか。最近のJNSAのドキュメントなどを参考に、リスクアセスメント方法自体を見直したほうがよいのではないでしょうか？（民間では、全てのリスクの発生可能性（脅威レベル）は同じ（すぐに発生する）としてリスクアセスメントを実施している例があります。）	リスクアセスメントについては、「制御システムのセキュリティリスク分析ガイド第２版～セキュリティ対策におけるリスクアセスメントの実施と活用～」（2023年３月IPA）に沿って、情報処理安全確保支援士が、その倫理綱領に従い、公正な立場で実施したものになります。
10	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-56	ガイドラインでは、「βモデル又はβ’モデルを採用する場合は、従来モデル（αモデル）と比較してインターネットからのリスクが増加し、より高度なセキュリティ対策の確実な実施が必要になることから、インターネット接続系とLGWAN接続系を完全に分離する場合を除き、その実施について事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出することとする。」とありますが、実際の監査項目は、無害化や画面転送の仕組みがきちんとできていることだけを確認するものとなっていて、そもそもの３層分離が適切に行われていることを確認する項目がありません。そういった確認は不要でしょうか？（ただし、何をもって適切に行われているのかが示されていることが必要です。監査人によって判断が分かれるようでは意味がありません。）	いただいたご意見は、今後の施策検討の参考とさせていただきます。
11	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-60	３層分離していても１台の複合機が２つのネットワークの両方に接続されているケースがあります。ガイドラインでは、「共有する場合には、１台のプリンタ・複合機にネットワーク毎に専用のLAN ポートを設け」とありますが、本当にそれで大丈夫でしょうか？実際に、複合機には、インターネット上の第三者に任意のコードを実行されるあるいは任意のファイルをインストールされる可能性があるといった脆弱性が発見されていますが、それでも複合機が侵害を受けるという懸念はないということが確認されていますでしょうか？それはできなくても、印刷やコピー時にメモリ上に読み込まれたデータが流出することがあるように思われます。もし、何らかの懸念があるのであれば、中途半端にせず禁止事項とするほうが良いのではないかと考えます。	いただいたご意見は、今後の施策検討の参考とさせていただきます。

No.	提出者	該当資料	該当ページ（改訂版における該当ページを掲載）	御意見	御意見に対する考え方
12	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	―	ネットワーク機器について脆弱性対策をきちんとというのが明記されるのは良いことですが、表現としては“ネットワークにつながっている全てのもの”という表現のほうが相応しいと考えます。例示でVPN装置とか無線AP等と一緒に、プリンタ、複合機、監視カメラなどのIoT機器も入れていただくのがいいと思います。また、どの団体でもNASが野放しであり非常に危険な状態です、それについても言及してもらいたいと考えます。ガイドラインには“サイバーハイジーン”という言葉が出てきませんが、どういう概念なのか、なぜ必要なのかをきちんと説明し、それが大前提であるということを指導していただければと思います。	いただいたご意見は、今後の施策検討の参考とさせていただきます。
13	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	―	α’/β/β’モデル採用団体に対する監査ですが、運用開始前に実施するのは、システムの確認という意味では必要かもしれませんが、運用の確認という意味ではかなり薄いと考えます。もちろん既存運用部分もありますが、モデル変更にともない新たな仕組みを構築する部分もあり、そこの運用状況の確認が全くできない（申請フォーマットだけを見ても意味が無い）監査となってしまいます。次に３年後となると、２年半ぐらいは危ういう運用がなされるかもしれず、かといってフォローアップ監査が義務付けられていない状況のため、監査をする側としては非常に後ろ髪を引かれる状況です。監査実施時期について再考をお願いします。加えて、このやり方は年度末のドタバタの時期に監査が集中することを示しています（実際にしています）。監査側は短納期での監査を強いられ、監査される団体側も繁忙の中での対応を強いられています（12/31深夜に監査証跡が提出された事例あり）。きちんと良い監査を実施するためにも、実際に監査の実施している業者の意見を確認する場を設けていただきたいと思います。	α’モデル、βモデル、β’モデルの各モデルについて、定期的な監査の実施を規定しております。 また、監査の周期や、監査の実施時期は、各地方公共団体が決めることであるため、現行の記載としております。
14	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	―	EDR（のようなもの）の導入が求められていますが、運用レベルに対する要求が記載されておらず、監査項目も入っていればOKという内容になっています。EDRと呼ばれている製品には、何らかの不審な動作を検知した場合に、即座にネットワークから切り離すことができるものとそうでないものがあることはご存じだと思います。即切断できない製品を導入している団体の運用設計において、検知→SOCで認識→職員に連絡→状況確認→判断→遮断といった流れとなっていますが、遮断されるまでの時間が設計されていないのがほとんどであり、翌営業日対応というのが多い状況です。昨今のラテラルムーブメントの状況を鑑みると、数時間程度が限界と思われますが、いかがでしょうか？なんのための仕組みなのか、何をしたいから入れるのかをきちんと伝え、そういった部分まで設計、運用するように指導をしていただきたいと思います。また、エンドポイント対策という言葉のせいか、クライアント端末だけに導入されるケースが非常に多い状況です。むしろまず保護すべきはADやファイルサーバ、DBサーバ、バックアップサーバなどのサーバだと思います。「地方公共団体向けβ’モデル移行に向けた手順書」の「移行時に検討すべき項目」としてそれらしき記載がありますが、ご参考となっており、それでは弱いと考えます。	いただいたご意見は、今後の施策検討の参考とさせていただきます。
15	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-48 iii-50 iii-52	α’モデルの場合、未知の不正プログラム対策（エンドポイント対策）は必須ではなく推奨の扱い（「以下の対策も有効である」との記載）となっています。本当にそれで大丈夫なのでしょうか？単純にリスクアセスメントの数字だけで考えているように思います。	リスクアクセスメントの結果を踏まえ、現行の記載としております。
16	法人	地方公共団体における情報セキュリティ監査に関するガイドライン	172	監査人資格を明確にという意見があり、情報処理安全確保支援士がガイドラインの本文には記載されていますが、情報セキュリティ監査業務委託仕様書（例）には記載されていません。一貫性を保つには、例にも記載いただくほうが良いと考えます。	「情報セキュリティ監査業務委託仕様書（例）」は例示です。また、監査ガイドラインの「2.3. 外部監査人の調達」に情報処理安全確保支援士は記載しており、外部監査人の調達にあたっては、各地方公共団体が決めることであるため、現行の記載としております。
17	法人	地方公共団体における情報セキュリティ監査に関するガイドライン	100	α’モデルの３パターンで監査項目を分けると想定していましたが、そうはなっていませんでした。パターン１でもパターン３相当の監査項目を確認し、例えば「ローカルブレイクアウトテナントアクセス制御」については“対象外”とした監査結果とすることでよいでしょうか？また、その場合、パターン２に移行する際には再監査が必要と考えますが、そういった考慮の記載は見受けられません。どのように考えられていますでしょうか？	α’モデルには３つのモデルを記載しておりますが、どのモデルにおいてもアクセス制御が適切に行われていることなどの監査は必要であると考え、現行の記載にしております。
18	法人	地方公共団体における情報セキュリティ監査に関するガイドライン	100	「ポリシーガイドライン」にてα’モデルのローカルブレイクアウトの記載で、「ログイン状況やアプリケーションの利用状況の監視を行う」ことが必要であるとの記載がありますが、監査項目にはその部分の記載がありません。追加が必要なのではないかと考えます（何をどのように監視するのかまで説明が必要と思います。）。	α’・β・β’モデルを採用する場合、「地方公共団体における情報セキュリティポリシーに関するガイドライン」の対策基準（例文）記載の組織的・人的対策を確実に実施する必要があるため、「地方公共団体における情報セキュリティ監査に関するガイドライン」p46の「5.人的セキュリティ」項番88に記載のとおり、情報システムやインターネットへのアクセス等について確認することを規定し、監査資料の例として、端末ログやファイアウォールのログを挙げております。
19	法人	地方公共団体における情報セキュリティ監査に関するガイドライン	―	自治体等によるセキュリティ監査の入札案件で、「○○県内に本店，支店又は営業所等を有する法人であること。」という限定があるケースを見受けます。地元産業の振興というのはわかりますが、そのことによりまともな競争が生まれず、質の低い高額な監査が実施されるという懸念があります。まずはきちんと監査品質を確保することが大前提のはずですので、そういう面での考慮をお願いしたいと考えます。	入札案件の条件は、各地方公共団体が決めることであることと、品質についても「地方公共団体における情報セキュリティポリシーに関するガイドライン」の第1編第3章　3. 評価・見直し　において独立かつ専門的知識を有する専門家による検証である情報セキュリティ監査であることや、第3編 第2章　9.1. 監査　において、監査を行う者は、十分な専門的知識を有するものでなければならないことを規定していることから、現行の記載としております。

No.	提出者	該当資料	該当ページ（改訂版における該当ページを掲載）	御意見	御意見に対する考え方
20	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	i-27	[対象箇所] i-27 図表8　情報セキュリティポリシーの見直しのプロセス 新たな脅威 （１３）無線LAN及びネットワークの盗聴対策 [意見] 盗撮、盗聴によるパスワードや技術情報の流出対策を講じていただけますよう、お願い申し上げます。 特に以下の対策につきまして、お手数をおかけしますが、お願い申し上げます。 （１）近赤外線カメラによる盗撮の対策 （２）ハイドロホンによる盗聴の対策 また、職員が、盗撮、盗聴の装置を職場に置く闇バイトで、収入を得られないよう、対策を講じていただけますよう、お願い申し上げます。 職場での活動で、公共団体以外からの不透明な収入を得ることが無いように、調査と対策をお願い申し上げます。 [理由] 近赤外線カメラとハイドロホンで、パスワードを盗み取れるからです。 パスワードを入力するときのディスプレイ画面を、近赤外線光をディスプレイにあてて反射する光を近赤外線カメラで盗撮できます。 また、入力するときに、口のなかで、パスワードをつぶやいているところをハイドロホンで盗聴できます。 MEMSの発達によって、近赤外線センサやハイドロホンが、小型高性能化できるからです[1][3]。 近赤外線は、以下の特性がございます。 非可視（目に見えない） プラスチックを透過する 白を反射して、黒を吸収する また、ハイドロホンは人体の内部の状態をも検知することができます[2]。 口のなかでつぶやく声でさえも聞き取ることが可能でございます。 なお、カメラやマイクにWiFiやBluetoothの無線通信の機能を持たせることは、容易でございます。 [参考資料] [1]ピエゾ技術の動向と海洋産業への応用（1） センサイト・プロジェクト [2]診断用超音波瞬時音圧の精密計測技術開発 千葉，吉岡（産総研） [3]赤外線カメラ基礎講座 株式会社ビジョンセンシング	いただいたご意見は、今後の施策検討の参考とさせていただきます。
21	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	i-35 i-36	1. ページ i-35「図表12」 多くのSaaSは内部アーキテクチャが不透明なため、暗にIaaSの利用を推奨しているようにも受け取れます。 「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」などによると、クラウドサービス検討時の優先順位はSaaSが優先であるので、矛盾しているようにも見えます。 ISMAPを取得したクラウドサービスの採用を必須とせず、内部が不透明なSaaSの利用を許可している方が問題となるため、「ISMAPを取得したサービスの採用を優先的に検討すべき」などの表現に変更すべきと考えます。 2. ページ i-36 「第三者認証クラウドサービスを評価する場合に、第三者認証を活用することが考えられる。第三者認証は、ISMS（ISO/IEC27001）に加え、ISMAP又はクラウドサービスにおける第三者認証（ISO/IEC2701710、ISO/IEC2701811等）12の取得を確認する必要がある。」 ISMAPは、第三者認証では政府機関が採用するにあたっては不足があるため、新設した政府機関向けクラウドサービス認証制度と認識しています。 また、地方公共団体を含め、普及を促進していく方針と聞いております。 現在の表現では、ISMAPと第三者認証が並列あるいは同列の表現になっており、ISMAP取得の動機が働かないため、ISMAP普及促進のためにも、1と同様に「ISMAPを取得したサービスの採用を優先的に検討すべき」などの表現に変更すべきだと考えます。	「地方公共団体における情報セキュリティポリシーに関するガイドライン」では、クラウドサービスのサービスモデルにより推奨/非推奨を定義しておらず、各サービスモデルの特徴や責任分界を把握し、第三者認証の活用等によりセキュリティを含めたサービスの信頼性やデータの保存場所を確認した上で、各団体規程に基づいて利用の判断を行っていただくことを規定しています。 また、ISMAPの利用については、住民の個人情報などの機密性の高い情報を扱う場合や、LGWAN接続系のローカルブレイクアウトによりクラウドサービスを使用する場合（α’モデル）等において規定しており、今後の方向性については、ISMAP制度の動向や地方公共団体が利用しているクラウドサービスの利用状況の実態等を踏まえ、検討いたします。
22	個人	―	―	地方公共団体に情報セキュリティ意識を高めてもらうという試みには賛成します。 しかし、丸投げにならないよう日本政府が地方公共団体に情報セキュリティの専門家を派遣する等して支援してください。	いただいたご意見は、今後の施策検討の参考とさせていただきます。

No.	提出者	該当資料	該当ページ（改訂版における該当ページを掲載）	御意見	御意見に対する考え方
23	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-210	別紙１　10．用語の定義　に於いての記載内容 ---------- ●「暗号化消去」 「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows のBitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。 ---------- この記載内容について； ◆以下は見解 ---------- 　暗号化消去が有効となるのは暗号化の開始時点において、ユーザが対象となるデータを記憶媒体に記録するより前であることと、暗号鍵がバックアップ等の複製も含めて確実に抹消されることが必要条件となっています。 　例えば、Windows10で使用しているPCをWindows11にグレードアップするために「PC正常性チェック」で診断すると、「このPCは現在、Windows11を実行するための最小システム要件を満たしていません」と表示されることが有ります。これはそのPCに暗号鍵を管理するTPM（Trusted Platform Module）モジュールが搭載されていないことを示しています。 　Windows に採用されている暗号化機能であるBitLockerは、TPMモジュールが存在しない場合でもデータを暗号化して保存することが可能です。しかし、暗号鍵はHDD等の媒体上のシステム領域等に書き込まれ、また外部（マイクロソフトアカウント等）にバックアップすることや、プリントアウトすることも可能であり、鍵の紛失時の対策を目的として、それらの手段を用いることも推奨されています。一方、暗号化消去が有効となるのはそれら全ての暗号鍵を漏れなく全て抹消されている場合であり、何処かに残存する場合には情報が漏洩する可能性を否定する事が出来ないので暗号化消去が成立したとする事は出来ません。 　(Windows11が要求する)TPMモジュールが搭載されている状態であれば、暗号鍵はTPMモジュール内に留まりますので、BitLockerを使用開始時から有効にすることにより、管理者権限を持つユーザが暗号鍵を更新・抹消することで暗号化消去が有効となる状態になります。 しかし、その様な状態であっても、PCの使用開始後に暗号化を有効にした場合（BitLockerの例）下記の様な結果となり、暗号化消去を成立させる条件を満たせなくなります。 １）「使用済み領域」に対する暗号化を選択・実行した場合 暗号化の対象が、現存する「ファイル」であるため、過去に削除され再使用されていないセクタに残るファイルの残骸やファイル・スラック領域に残るファイルの断片、「再割り当て済みセクタ」等のOSが認識不能な領域は、暗号化の対象外となります。よって、データ復旧ソフトを使用すると、暗号化開始以前のデータの断片などを読み出すことが可能なので、データが消去（Clear）されたと呼べるレベルに到達することありません。 ２）「メディア全体」に対する暗号化を選択・実行した場合 HDD等の記憶媒体が自動的に行う、バッドセクタ処理やペンディング処理により発生する「再割り当て済みセクタ」等のOSが認識しない領域は暗号化の対象に含まれないため、研究所レベルの特殊な手法を用いるとデータの断片などが読み出し可能な状態で残存します。本来の「暗号化消去」の結果である、機密性の高い情報に対するデータ抹消である「Purge」レベルではなく、通常のレベルである「Clear」レベルに留まります。 この様な状態であるにも関わらず、PCのデータ消去を生業としている一部事業者から、情報漏洩を防止する（データを抹消する）事を目的として、データの抹消ソフトを使用する代わりに、BitLockerを用いて暗号化を行い、その後暗号鍵を抹消することで暗号化消去（Purge）が成立するのではないか。との問い合わせを受けることがあります。 　上記の様な誤解を防止するためにも、暗号化消去の解説（補足）として： ■以下は追記文章案 ---------- １．記憶媒体に情報を書き込む以前に暗号化機能を有効としている場合。 ２．（復号に用いる）暗号鍵がバックアップ等を含む複製を含めて、確実に抹消された場合。 ---------- の2点を追記することが必要であると考えます。	いただいたご意見は、今後の施策検討の参考とさせていただきます。

No.	提出者	該当資料	該当ページ（改訂版における該当ページを掲載）	御意見	御意見に対する考え方
24	地方公共団体	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-43	LGWAN接続系とインターネット接続系の分割における、CADファイル等の特殊な拡張子を持つファイルの取り込み方法の追記について 「３．情報システム全体の強靭性の向上（2）LGWAN接続系①LGWAN接続系とインターネット接続系の分割（解説iii-43～）」において、インターネットからのファイル取り込みにおいては、以下の方法とされている。 ・テキストのみ抽出 ・PDFに変換 ・サニタイズ処理 ・目視及びソフトウェアでの危険因子の確認 ことに本意見書として提出したいのは、表題としたCADファイル等の特殊な拡張子を持つファイル（以下、CADファイル等という）の扱いであり、CADファイル等は上記のどれにも当てはまらない点が問題と考える。 これを利用場面から考察すると、自治体と相手先（官公庁及び一般企業等）とで双方編集を交えつつ送付し合いたい場合がある。テキスト及びPDF変換をしてしまうとそれ以降の編集が出来ず、サニタイズ処理はCADファイル等に対応している製品が少なく、あってもごく一部の拡張子に限るものばかりである。当市では、メール等で送付できる容量を超えるCADファイル等は原則CD等の媒体をもってやりとりを行っているが、クラウドバイデフォルトの原則に立ち返ってDX化を進めるにあたり当然オンラインストレージも検討している。今回の改定案も踏まえると、せっかくISMAP登録のサービスにまで範囲が拡充されても、肝心のファイルが受け取れないのであれば意味がない。また、仮に現状でオンラインストレージ等を導入しても、実際にファイルを無害化処理してみるまでは移動の可否が分からず、結局としてCDでの移動が一部発生するのであれば事務の効率が図れているとは言い難く、かつコストメリットも得られづらい。 目視及びソフトウェアでの危険因子の確認においては、いささか記述の具体性が無いようにも感じるが、以降に「アンチウイルスソフトウェアの最新化」等の文言が別途あることから、これはエンドポイント製品の導入のみをもって是とする意味ではないと解釈している。こちらにおいては、EDR製品の導入により是とできるのか等、線引きの記載は別途欲しい。 以上より、CADファイル等の業務利用を継続して行い、かつサニタイズ処理が難しいファイルの取り扱いにあたっては、記述が不足していると感じ、何らかの追記が欲しいと考える。	いただいたご意見は、今後の施策検討の参考とさせていただきます。
25	地方公共団体	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-45 iii-61	マイナンバー利用事務系及びLGWAN接続系からインターネットを通してパターン更新を行う是非に関する記載内容の修正について 「３．情報システム全体の強靭性の向上（2）LGWAN接続系③（解説iii-45～）」及び「３．情報システム全体の強靭性の向上（4）その他のセキュリティ対策③（解説iii-61）」において、（2）LGWAN接続系③ではα’モデルにおいてはセキュリティ関連サービスにおいてはISMAP以外でも利用を認めるとしているのに対して、（4）その他のセキュリティ対策③ではマイナンバー利用事務系及びLGWAN接続系からインターネットへのパターン更新は認められないとの記載になっており矛盾に感じる。私の解釈違いであれば良いが、文言の修正は求めたい。	ご指摘を踏まえ、「地方公共団体における情報セキュリティポリシーに関するガイドライン」の以下の部分について、 下線部のとおり追記いたします。 第3編　第2章 3. 情報システム全体の強靭性の向上 （４）その他のセキュリティ対策 ③修正プログラム及びパターンファイルの更新 マイナンバー利用事務系及びLGWAN 接続系では、OS・アプリケーションの修正プログラム及びウイルス対策ソフトの パターンファイルの更新等においても、インターネットに接続して利用してはならない(ただしLGWAN 接続系はα’モデルを除く)。
26	個人	ー	ー	見え消し版や新旧対照表がないのは不親切である。 少なくとも変更点概要くらいは提供しないのは、国民に広く意見を聞くという姿勢から外れている。 いま一度資料を提供したうえでパブリックコメントすべきである。	今回の意見募集についてはガイドライン改定案全体について実施しているものになります。いただいたご意見は、今後の施策検討の参考とさせていただきます。
27	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-59	・該当箇所 第3編 地方公共団体における情報セキュリティポリシー（解説） 第2章 情報セキュリティ対策基準（解説） 3.情報システム全体の強靭性の向上 （3）インターネット接続系 （イ）β’モデル　iii- 59 ・意見内容 情報漏えいに対する対策として有効な対策にIRM（Information Rights Management）の追記 ・理由 対策例として挙げられているファイルの暗号化は定義が広く、PCやシステムにログインできれば解読可能な暗号化やパスワードによる暗号化などでは、外部からの不正ログインや内部不正による持ち出しに対処できない。 IRM（Information Rights Management）はファイルの暗号化に加え、組織が定義したポリシーに従いファイルに対する操作権限を設定し、最小の権限でデータを活用させることができる。また、ファイル・アクセス毎にアクセス元の認証を行うことからゼロトラストの構成要素として挙げられている。 データ漏えい防止策として既に挙げられているDLPと比較し、各団体が自組織の運用に沿うものを選択できるよう、IRMの追記を希望する。	いただいたご意見は、今後の施策検討の参考とさせていただきます。
28	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-141	α’、β’等各モデルに求められるセキュリティ要件に対し内部対策要件の記載追加をお願いしたい (ア)　[6.5.不正アクセス対策 (7)標的型攻撃]において「内部対策」の記載があるものの、各モデルのセキュリティ要件の中に含まれていないため、各自治体の調達要件から考慮漏れしてしまうケースが散見される (イ)　具体的には内部に侵入することを前提として「検知・対処・復旧」に必要な情報を集約し使える状況にしておくことが求められる (ウ)　政府統一基準においてはp.425[リアルタイムでのログの調査・分析を行うための機能]、p.456[不正な通信を監視し、遮断]の箇所で令和5年度版より「NDR(Network Detection and Response)」の記載を追加しており、同様の記載の検討を行うことが考えられる	いただいたご意見は、今後の施策検討の参考とさせていただきます。
29	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-52	α’要件に記載されているIPS/IDSの要件が適用される目的・箇所が不明瞭なので明確にして欲しい (ア)　p.iii-52[図表33]に記載されているIDS/IPS要件がどのようなリスクに対してどのポイントで実装すべき対策なのか不明瞭と感じる (イ)　これまでの議論の過程からはLGWAN系に配置される各システムにおいて業務上迅速にパッチ等が当てられない事情を考慮し、内部に侵入した脅威が脆弱性を活用し内部拡散するリスクに対処する目的で、各システムが配置されるセグメントの手前にネットワーク型のIDS/IPS機能、もしくは各システムの各サーバ上に対しホスト型のIDS/IPS機能を付加する、と理解している	詳細な実装方法については、各団体の情報システムやネットワーク構成に応じて適切に実装していただくことが望ましいと考えているため、「地方公共団体における情報セキュリティポリシーに関するガイドライン」は現在の粒度としています。

No.	提出者	該当資料	該当ページ（改訂版における該当ページを掲載）	御意見	御意見に対する考え方
30	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-46	パブリッククラウド利用時の主なインシデントとして意図しない設定不備が多いため、CSPMの記載追加をお願いしたい (ア)　p.iii-46においてクラウドサービスにおける設定不備の脅威について触れているが、対策として政府統一基準のp.194[設定の誤りを防止するための対策]としてCSPM（Cloud Security Posture Management）が挙げられている (イ)　さらに貴省にて発出されている「クラウドサービス利用・提供における適切な設定のためのガイドライン」p.42にもCSPMの記載が見られる <https://www.soumu.go.jp/main_content/000843318.pdf>	いただいたご意見は、今後の施策検討の参考とさせていただきます。
31	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-39	マイナンバー系のWAFの必要性について (ア)　p.iii-39[マイナンバー利用事務系のサーバのOS等への修正プログラムの常時適用が困難な場合]について、WAFの利用が挙げられているが、インターネットにさらされない前提のサーバに対してWAFが求められる理由があればご教示願いたい。もし必要ないのであれば混乱を招くので記載の削除をご検討いただきたい。	サーバのOS 等への修正プログラムの常時適用が困難な場合における、脆弱性を悪用した攻撃を防ぐための手法の例としてWAFを挙げております。
32	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	―	インシデント報告ルートの一元化の検討を要望 (ア)　能動的サイバー防御の議論でも産業界から要望が出ているが、今後より一層の政府とのリスクコミュニケーションを活発化させることを目指し、報告窓口の一元化について他産業と同様に議論をお願いしたい (イ)　参考ＵＲＬ：https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai2/siryou1.pdf	地方公共団体は、サイバーセキュリティ基本法（平成26年法律第104号）第12条第２項第３号に規定される重要社会基盤事業者等（重要インフラ事業者等）であり、「重要インフラのサイバーセキュリティに係る行動計画（2024年３月８日サイバーセキュリティ戦略本部改定）」に基づき、大規模なサービス障害が生じた際には重要インフラ所管省庁（総務省）に連絡することとされています。
33	法人	―	―	システムの重要度に応じたセキュリティ対策の強化 (ア)　政府統一基準の令和５年度版で取り入れられたシステムの重要度に沿った対策基準の強化について、地方公共団体の事情を加味して同様の考え方を取り入れられるよう検討をお願いしたい (イ)　その場合、現在データの重要度、ネットワークの重要度が存在し、さらにシステムの重要度が追加されるとその整合性が複雑になるため地方公共団体において真に守るべき対象が何であるのかを明確にする必要があると考える	地方公共団体が住民の個人情報を扱うことを鑑み、住民の個人情報の流出を防止することを目的とした各種対策を規定しております。また、情報資産の取扱いについては、その団体の実情を踏まえて定められることが重要であるため、情報資産を保有している各団体において、機密性、完全性及び可用性を踏まえ、被害を受けた場合に想定される影響の大きさをもとに分類を行い、必要に応じ取扱制限を定める必要がある旨規定しております。
34	法人	―	―	任務保証の概念の取り込み (ア)　地方公共団体も含まれる重要インフラが参照すべき「重要インフラのサイバーセキュリティに係る行動計画」に示されている任務保証の概念について地方公共団体の事情を考慮したガイドラインへの取り込みの検討をお願いしたい	いただいたご意見は、今後の施策検討の参考とさせていただきます。
35	法人	―	―	環境寄生型攻撃への対応を考慮したログの取得方法等の提示 (ア)　能動的サイバー防御の議論で発生している環境寄生型攻撃への対応について、地方公共団体の事情を考慮したログの取得方法等の提示の検討をお願いしたい (イ)　NISCよりこのような形でベストプラクティスが示されているのでご参考までに共有する <https://www.nisc.go.jp/pdf/policy/kokusai/Provisional_Translation_JP_ASD_LOTL_Guidance.pdf> (ウ)　今後能動的サイバー防御の仕組みが導入されることを考慮し、日本政府より提供されるIOCや攻撃手法、攻撃傾向に関する情報を受け取り、自庁の環境で該当する攻撃が発生していないか確認する仕組みの整備に係る記載の検討をお願いしたい	能動的サイバー防御の議論も踏まえつつ、関係省庁と連携して取り組んでまいります。
36	法人	―	―	経済安全保障への対応を見据えた調達方法に関する検討 (ア)　政府統一基準の一部改訂(令和６年７月)において記載が強化されている「サプライチェーン・リスク対策」の観点で、地方公共団体の事情を鑑みた記載の検討 (イ)　2024年度中に開始予定の「IoT製品に対するセキュリティ適合性評価制度」を活用した選定・調達についての記載の方向性の検討 (ウ)　その他経済安全保障の観点で地方公共団体の抱えるリスクの分析ならびに対応策の検討	サプライチェーン・リスクへの対応については、関係省庁と連携して取り組んでまいります。

No.	提出者	該当資料	該当ページ（改訂版における該当ページを掲載）	御意見	御意見に対する考え方
37	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-31	■意見内容(要旨) 自治体機密性３Ｂにおけるパブリッククラウドサービスの利用について、「ソブリンクラウドの利用が望ましい」としていただきたくお願いいたします。 ■意見理由 自治体機密性３Ｂの分類基準について、「行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産」と定義されていますが、ここでは「住民の個人情報」の内容として、例えば特定個人情報と要配慮個人情報の分類定義に触れられておらず、同一の扱いと見受けられます。 また、自治体機密性３Ｂと自治体機密性３Cについて、機密性の分類基準が異なるにも関わらずパブリッククラウドサービスの範囲としては、同様の取り扱いとなっています。 上記2点により、例えば特定個人情報と要配慮個人情報が同等の扱いとなることが懸念されます。 個人情報の保護に関する法律においても、この2つの情報の取扱いには明確な差があると認識しています。要配慮個人情報は、プライバシーの侵害リスクが特に高いため、収集時や第三者提供時に本人による明示的な同意が必要であることから、管理も一層厳格に行う必要があると考えます。 （※） ※令和7年6月1日施行　個人情報の保護に関する法律　第2条（定義） ※令和7年6月1日施行　個人情報の保護に関する法律　第20条（適正な取得） ※令和7年6月1日施行　個人情報の保護に関する法律　第27条（第三者提供の制限） そのため、特定個人情報と要配慮個人情報を同様の機密性分類「自治体機密性３Ｂ」とするのであれば、その高い機密性とプライバシー保護の重要性から、取り扱いにおいては「自治体機密性３C」に対してより高度な管理が必要と考えます。 例えば、欧州連合（EU）やEU各国では、GDPR（General Data Protection Regulation）でデータの取り扱いに厳しい基準が課されるため、個人情報の取扱いについてはソブリンクラウドを活用しています。 ソブリンクラウドは、クラウドインフラを提供するデータセンターやサービスプロバイダーが国内事業者としデータを自国内に留め、自国の法律に基づいて運用管理することを目的としています。さらに信頼性と透明性確保の観点から、物理的にもパブリックサービスとは異なるインフラ領域にて管理し、データの処理方法や保管場所について明確な情報を提供します。 ソブリンクラウドであれば、データの管理、セキュリティ、法的リスクの軽減、監査容易性、そしてデータ主権の確保という観点から、要配慮個人情報を含めた個人情報を取り扱うのに最適な選択肢と考えます。 これにより、データが適切に保護され、規制を遵守しながら、自治体は個人情報の適切な管理を行うことが可能です。	ご指摘の点については、他省庁の動向も踏まえ検討してまいります。
38	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-31	機密性3Cに「職員の属性に基づく個人情報」とあるが、検討過程の資料を拝見すると住民記録と同等かという議論と解釈しています。そのため、住基データ相当である、家族情報や人事情報等が該当するのではないかと考えておりますが、職員の属性に基づく個人情報の定義を明記いただければ幸いです。 ※システムのログインアカウントとして使われることが多い職員名やメールアドレス、所属組織までもが3Cとして扱われるかを懸念しております。	職員の属性に基づく個人情報と住民の個人情報を分けた理由は、人事給与システムなどで使用する職員の情報よりも、住民の個人情報の方が、機密性が高い情報として扱うべきとの有識者の意見があったことを踏まえたものになります。なお、「地方公共団体における情報セキュリティポリシーに関するガイドライン」は技術的助言であるため、情報資産を有する各地方公共団体は、それぞれが策定する情報セキュリティポリシー等の規程類を遵守することになるため、各団体の規程類の中で、定義されていくものとなります。
39	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	―	解説の中でISMAPが複数回登場します。スタートアップや中小ベンチャーが事業を加速させるフェーズにおいてISMAPの取得は成長の阻害となる（リソース、コスト双方の観点で）可能性が高く、政府の推し進めるスタートアップ推進の流れにもそぐわないように感じられます。 また次年度に向けた予算要求が進む中、スタートアップ活用を想定した数多の事業があります。直近ISMAPは審査プロセスが高速化されたとはいえ、内部準備も含めると最低でも1.5年はかかりますゆえ、この適用タイミングですと事業取りやめを含む混乱が起きると考えます。 代替となる認証資格の検討（ISMSに加えISO27018等）や、取得の緩和、段階的な改訂案の適用（移行期間を設ける）等の考慮、もしくはガバメントクラウド参画プロセスを、抜本的に柔軟性を上げていただく等を併せて検討いただけますと幸いです。	政府機関等の対策レベルと整合性を担保する考え方から、自治体機密性３B及び３Cの情報については、ISMAP登録サービスで取り扱うものとしております。また、ISMAP制度については、政府情報システムのためのセキュリティ評価を実施する目的から、内閣サイバーセキュリティセンター（NISC）を含む関係省庁において検討がなされているものになります。
40	法人	―	―	同様に、ISMAPの取得並びに継続的な監査はスタートアップや中小ベンチャーの資金繰りを圧迫する恐れがあるため、政府による支援策の検討を期待いたします。	ISMAP制度については、政府情報システムのためのセキュリティ評価を実施する目的から、内閣サイバーセキュリティセンター（NISC）を含む関係省庁において検討がなされているものになります。
41	個人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-7	iii-7について 教育委員会や病院等の他のセキュリティポリシーのガイドラインが適用される部分について、本ガイドラインの自治体機密性という分類の適用された文書の場合、相互の文書の送付に支障が出る可能性があるため、相手先ガイドライン上ののでの機密性の互換性についてどのように考えるべきなのか解説を追加していただきたい。 また都道府県警察など例示されていないが別の規程があるようなものについても本ガイドラインで想定されている取り扱いについて例示及び解説を加えていただきたい。	個別分野の所管省庁が求めているセキュリティ対策と、「地方公共団体における情報セキュリティポリシーに関するガイドライン」の規定の対象が重複するケースは、各地方公共団体の情報システムやネットワークの状況による場合があるため、各所管省庁と調整の上、対応しております。
42	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	iii-45	〔アルファ ダッシュ〕モデルにおいて利用可能なクラウドサービスの要件について 【箇所】このため、本モデルにおいて利用可能なクラウドサービスは、ISMAP管理基準を満たし、ISMAPクラウドサービスリストに登録されているサービスとする。（iii- 45） 【意見】指摘箇所等では、文理上「ISMAP-LIUクラウドサービスリストに登録されているサービス」では要件を満たさないように読めるところ、本文中いくつかの箇所で「ISMAP」とあるのは「ISMAP-LIU」を明示的に排除しているか、あるいは含むものであるのか、明らかになるよう整理して記述していただきたい。	ISMAP-LIUは、ISMAPの枠組みのうち、リスクの小さな業務・情報の処理に用いるSaaSサービスを対象とした仕組みであることを踏まえ、LGWANをローカルブレイクアウトし接続するリスクに対応するための要件としてはISMAPクラウドサービスの利用を規定しております。
43	法人	地方公共団体における情報セキュリティポリシーに関するガイドライン	―	「LGWAN外部契約サービス」及び「LGWAN外部閉域利用サービス」の位置付けについて 【箇所】〔なし〕 【意見】令和5年5月より導入された「LGWAN外部電子契約サービス」及び「LGWAN外部閉域利用サービス」について全く記述がなく、それらのサービスを利用する場合と、例えば〔アルファ ダッシュ〕モデルを採用する場合のそれぞれの準則の適用関係、優先劣後関係がこのガイドラインからは不明である。この点の解説を注記していただきたい。	各地方公共団体において、どのようなサービスを利用するかについてご判断いただくことになります。