「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５年３月２８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５年２月２３日（木）から３月８日（水）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、３４件（法人２４件、個人１０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５年３月２８日（火）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(改定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	ー	ー	本件の「意見提出が30日未満の場合その理由」は何ですか？	本件は、行政手続法上の意見公募手続の対象に該当せず、任意で意見募集を行うものであるため、意見募集期間を30日未満としております。
2	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	ii-19 ii-22	ii-19⑩情報資産の廃棄等（ア）、ii-22に記載にある、すべての情報資産の廃棄には復元できないように措置する必要があります。 その手段として、ii-49に記載の取り扱う情報の機密性保護のための暗号化を行っており、ii-56の機密性2以上のデータを取り扱う情報機器に対しては、「パージ（Purge）除去」レベルの消去を行うことを指定しております。それには、CISOが鍵管理方法を定めることと記載がございます。 しかし、NIST SP800-88 Rev.1では、「Purge」レベルのデータ消去は、利用開始時から適切な暗号化を実施し、暗号鍵を管理・消去することで実行されるとしております。 現在のように、暗号化消去についての記述が点在する場合、あたかも廃棄時に暗号鍵のみの消去を実行すれば「パージ（Purge）除去」レベルのデータ消去が実現されるような誤解が生じる可能性がありますので、暗号化消去について、より具体的な実施方法の記載のご検討をお願いします。 ※詳細は別途意見書に記載	クラウドサービスにおける暗号化消去については、ガバメントクラウドにおける暗号化消去の対応の方向性を踏まえて、具体的な記載内容を今後検討いたします。
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	ⅱ－ 24 ⅲ－ 100	第2章.情報セキュリティ対策基準（例文） 4.物理的セキュリティ 4.4.職員等の利用する端末や電磁的記録媒体等の管理の①において、「情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定（中略）等の物理的措置を講じなければならない」と記載がありますが、LGWAN接続のネットワークは令和2年の「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」の改定でWi-Fi接続やリモートワークが可能となり、それに伴いPC端末を移動する機会が多くなったため、この記載が効率的な業務の妨げや、頻繁な施錠・開錠作業による締め忘れ等のリスク増加の原因となると思われます。 また、テレワークにおける端末盗難に関する措置は、 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（例文） 6.技術的セキュリティ 6.2アクセス制御 (2)職員等による外部からのアクセス等の制限において「（注7）画面ののぞき見や盗聴を防止できるような環境を選定することで情報の漏えい対策につながる。また、テレワーク実施時の離席時の端末等の盗難に注意する。」と記載されており、「物理的措置を講じなければならない」との記載はありません。テレワークと同等の端末盗難に関する措置を講じていれば庁舎内のLGWAN端末においてもワイヤーで固定する必要はないと考えます。 しかしながら、端末の盗難時の対策は講じる必要があるため、『PC端末のログインに多要素認証方式を使用している事』、もしくは『PC端末本体にデータを保存しないシンクライアント端末である事』等を条件として追加することは必須と思われます。 そのため、 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改定案 第2編.地方公共団体における情報セキュリティポリシー（例文） 第2章.情報セキュリティ対策基準（例文） 4.物理的セキュリティ 4.4.職員等の利用する端末や電磁的記録媒体等の管理の①「執務室等で利用するパソコン」の記載を「執務室等で利用する、多要素認証方式を適用していない又はシンクライアント端末以外のパソコン」へ変更することを提案いたします。	地方公共団体の無線LANの利用の実態等を考慮して、今後検討いたします。
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		LGWAN接続のネットワークは令和2年の改正で無線LANの利用が緩和されましたが、今後の技術向上によって無線LANのセキュリティレベルが高くなった場合、実務効率化の観点からマイナンバー利用事務系においても無線LANの利用の緩和を検討することを提案いたします。	地方公共団体の無線LANの利用の実態等を考慮して、今後検討いたします。

No	提出者	該当資料	該当ページ(改定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
5	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	i-33	i-33～i-34に記載の項目「責任分担／責任共有」の欄に、 「クラウドサービスを利用する前に、そのクラウドサービスが、クラウドサービス利用者の組織における情報 セキュリティの要求事項を満たすのか、評価を行い、クラウドサービスを利用する際のリスクの対応について、十分な検討が必要となる。」 との記載がありますが、情報セキュリティの要求事項を満たすのか評価を行う事に加えて、政府がクラウドサービスを調達する際の評価制度である「ISMAPに登録されているサービスであるかの確認を行うなど、十分な検討が必要である。」の記述の追加が望ましいと思われます。 【理由】 ISMAPでは「各政府機関は、クラウドサービスを調達する際は本制度において登録されたサービスから調達することを原則とし（※）」とあり、地方公共団体も行政機関であり広義の意味では政府機関の一部と考えられることから、政府機関の指針を反映した方が良いと思われます。 ※令和2年6月3日（水）内閣官房・総務省・経済産業省が連名で出した「政府情報システムのためのセキュリティ評価制度（ISMAP）について」の5ページ目に記載	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。
6	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	ｉ-33	図表11において、SaaSについては選択肢として否定しているようにも受け取れてしまうため、以下の記載に改めることができないでしょうか。 ・組織のセキュリティ要求事項に対する評価が、比較的難しい。（ISMAP におけるサービスリストの登録、第三者認証の取得や外部機関による監査報告書を開示可能な地方公共団体向けのアプリケーションサービスを提供しているクラウドサービス事業者を選定することが望ましいが、こうした事業者は少ないため、それ以外ののサービスの情報セキュリティ対策の実態を確認することが難しい。）	IaaS、PaaSと比較した内容を示しており、SaaSについて否定しているものではございません。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。
7	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	ｉ-34	3.2クラウドサービスの特性における留意事項の第三者認証 において、ISO22301を取得しているクラウドサービス事業者は少ないため、削除または他の確認手段も挙げるべきではないでしょうか。	ISO22301については、クラウドサービスを業務で利用する場合おいて参考となるものと考えています。
8	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	ⅱ-30	6.1コンピュータ及びネットワークの管理（6）ログの取得等の①において、ログ等を「一定の期間」保存するとありますが、最低1年以上や、3年以上が望ましいといった表記が必要ではないでしょうか。	第3編の解説に「ログは１年以上保管することが望ましい。」と記載しています。
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	ⅲ-31	（解説）（1）情報資産の分類 において、重要性分類の順番は、機密性、完全性及び可用性と逆になっているが、これを同じ順に合わせるように改定することはできないでしょうか。	重要性分類については、重要性分類における考え方の例を示したものとなります。
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-34	【例文】（1）マイナンバー事務系②情報のアクセス及び持ち出しにおける対策（イ）情報の持ち出し不可設定 において、USBメモリ等の電磁的記録媒体による情報持ち出しができないようにすること以外で、取り得る対策を例示していただけないか。	マイナンバー利用事務系は、他の領域と通信を分離することが原則であるため、情報の持ち出し不可設定として、USBメモリ等の電磁的記録媒体による情報持ち出しができないようにすることを記載しております。他の対策の記載の必要性については今後検討いたします。
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-45	（注10）において、クラウドサービスではIPアドレスを限定することが困難であることが多いため、ホスト名を指定したルーティングも併記していただけないでしょうか。	第2編及び第3編は、クラウドサービスの利用を前提としたものとではなく、幅広い情報システムの利用や運用形態を想定したものです。今後クラウドサービスの利用を想定した第4編特則と統合することを検討しております。

No	提出者	該当資料	該当ページ(改定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	iii-48	図表28において、インターネット接続系にもファイルサーバが必要ではないでしょうか。	図はイメージとして記載しております。
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	iii-50	図表30において、インターネット接続系にもファイルサーバが必要ではないでしょうか。	図はイメージとして記載しております。
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	iii- 113	（注5）において、「データのバックアップ」については、「端末の OS からアクセスできないディスクや媒体へ保管する」ことが記載されています。この記載ではThe No More Ransom Projectでも推奨されているクラウドサービスの活用が候補から抜けてしまうため、クラウドサービスに関する追記が必要では無いでしょうか。 参考）https://www.nomoreransom.org/ja/prevention-advice-for-users.html	御指摘を踏まえ、下線部について記載を修正いたします。 「なお、「データのバックアップ」については、バックアップの保存先が、ランサムウェアに感染した端末等からアクセスできる領域にある場合、バックアップを含め暗号化されてしまう可能性があるため、端末のOS からアクセスできないネットワークから切り離されたオフラインのディスクや媒体等へ保管することも検討が必要となる。また、可用性を担保する対策としては、対象となるデータだけではなく、システムのバックアップを取ることでシステムの迅速な復旧につなげることができる。その際、有事の際に早急に対応できるようバックアップから復旧可能なことや復旧手順を定期的に確認しておく。バックアップからの復元にあたってはランサムウェア感染前の復旧ポイントの特定手法や、復元したバックアップにマルウェアが残存していないかの確認を復旧手順に含めることが重要となる。」
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-153	（2）外部サービスの選定⑩外部サービスに係るアクセスログ等の証跡の保存 において、アクセスログ等の証跡に係る保存期間は1年間以上ではなく、もっと長期間を記載したほうが良いのではないでしょうか。	ログの保存期間は、ログの対象となる業務システムの性質より異なるため、１年以上と示しています。ログの保存期間は、地方公共団体の運用や取り扱う情報資産に応じて、具体的な期間を地方公共団体の情報セキュリティポリシー実施手順に定めていただくことを想定しています。
16	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	iv-7	第2章 本編におけるクラウドサービスの範囲について において、「β´モデルを活用して機密性の高い情報資産の運用」と記載がありますが、iv- 58の表記と差異があります。表記を統一して「β’モデルを活用して機密性の高い情報資産（住民情報等）の運用」とするべきでは無いでしょうか。	第４編特則第2章 本編におけるクラウドサービスの範囲は、クラウドサービス上で標準準拠システム等を利用することを想定し、対策基準の例文記載しています。そのため、ご指摘の箇所の例文は、標準準拠システム等を対象とした記載にしています。β’モデルにおいても活用可能であることをお示ししていますが、あくまでも参考として活用可能としているものです。
17	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	iv-15	【例文】（2）情報資産の管理①管理責任（ウ）において、クラウドサービスの環境に保存される情報資産についても（1）の分類に基づき管理することが望ましいに改めていただけないでしょうか。	情報資産の分類について、原則としてクラウドサービスを利用する場合とそれ以外の場合において異なることはないため現在の記載としております。

No	提出者	該当資料	該当ページ(改定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
18	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	iv-20	【例文】（2）LGWAN接続系②LGWAN接続系と接続されるクラウドサービス上での情報システムの扱い において、専用回線の定義を明確にするか具体例を挙げていただけないでしょうか。	ガバメントクラウドと庁内システムの接続方法は、現在検討中のため、今後の検討結果を踏まえて、記載の見直しを検討いたします。
19	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	iv- 24	（３．情報システム全体の強靭性の向上（２）LGWAN 接続系②LGWAN 接続系のクラウドサービス上での配置の扱いの解説 において、標準準拠システム等と同じくLGWAN 接続系の情報システムをガバメントクラウド上に構築する場合のみ記載されています。一方、iv- 7ではガバメントクラウド以外のクラウドサービス以外にも標準準拠システム等の利用・運用を行うことが想定されているため、LGWAN 接続系の情報システムでも記載を統一するべきでは無いでしょうか。 修正例）標準準拠システム等と同じくガバメントクラウドやISMAP 認証、クラウドサービスにおける第三者認証を取得したサービスに構築することが効率的であると～	第4編は標準準拠システム等のガバメントクラウド等への移行を踏まえて特則として記載しているものとなります。今後クラウドサービスの利用を想定した第4編特則と統合することを検討しております。
20	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- 114	iii- 113～114頁のランサムウェア対策について 「端末のOSからアクセスできないディスクや媒体へ保管する等の検討も必要となる。」 ランサムウェアからのデータ保護について、 内閣サイバーセキュリティセンターが定めている対策基準ガイドラインや、厚生労働省が示している安全管理ガイドラインの記載レベルとあわせて以下文言に見直し、 「バックアップデータを保存した媒体を端末及びサーバ装置やネットワークから切り離して保管することも考慮するとよい」 エアギャップによるデータプロテクションの要素を明記することを提案します。 ＜参考＞ ・内閣サイバーセキュリティセンター 政府機関総合対策グループ - NISC ⇒https://www.nisc.go.jp/pdf/policy/general/guider3_2.pdf →103～104頁 ⇒https://www.nisc.go.jp/pdf/policy/general/rev_pointr3.pdf →22頁 ・厚生労働省医療情報システムの安全管理に関するガイドライン 医療情報システムの安全管理に関するガイドライン　第5.2版（令和4年3月）｜厚生労働省（mhlw.go.jp） https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html ⇒Microsoft Word - 医療情報システムの安全管理に関するガイドライン第5.2版（本編） _訂正版（mhlw.go.jp） https://www.mhlw.go.jp/content/10808000/000936160.pdf →39頁	御指摘を踏まえ、下線部について記載を修正いたします。 「なお、「データのバックアップ」については、バックアップの保存先が、ランサムウェアに感染した端末等からアクセスできる領域にある場合、バックアップを含め暗号化されてしまう可能性があるため、端末のOS からアクセスできないネットワークから切り離されたオフラインのディスクや媒体等へ保管することも検討が必要となる。また、可用性を担保する対策としては、対象となるデータだけではなく、システムのバックアップを取ることでシステムの迅速な復旧につなげることができる。その際、有事の際に早急に対応できるようバックアップから復旧可能なことや復旧手順を定期的に確認しておく。バックアップからの復元にあたってはランサムウェア感染前の復旧ポイントの特定手法や、復元したバックアップにマルウェアが残存していないかの確認を復旧手順に含めることが重要となる。」
21	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	iv-7	クラウドサービスの利用はβ’モデルに限定されていると読み取れますが、現在かなりの割合の地方公共団体が、費用や人材などの課題からαモデルを採用しております。一方で、政府のクラウド利活用の方針や職員の働き方改革の推進にはクラウドサービスの利用拡大は必須と考えますので、「すべての地方公共団体をβ’モデルへの変更を推奨」あるいは「αモデルでのクラウド利用のガイドラインの策定」が急務と考えます。	地方公共団体の規模等によって対応可能なセキュリティレベルに差があることから、新たな技術や環境の変化を踏まえ、αモデル・βモデルそれぞれの採用団体への支援を進めてまいります。
22	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-42	・マイナンバー利用事務端末からの例外的な情報持ち出しにUSBメモリ等を利用する場合、紛失やデータ消去のし忘れ等の懸念がどうしても残る、と思われます。 セキュリティが担保されることを前提（例えば利用履歴の取得、通信の暗号化、一定期間経過後のデータ自動消去など）としたファイル授受装置を利用することにより厳密な管理が出来るので、選択肢の一つとして加えてもよいのではないでしょうか。	第3編解説に情報資産の運搬の手段としては、USBメモリに限らず、専用の運搬サービスや外部サービスといった手段も示しています。インターネットでの外部サービスを利用する場合は、マイナンバー利用事務系から媒体等でインターネット接続系に情報を移動し、外部サービスを介してファイルの授受を行うパターンとなります。いずれにおいても、情報資産が運搬された先での管理の徹底が重要となります。 ご意見は今後のマイナンバー利用事務系におけるクラウド利用の状況等を踏まえ、今後検討させていただきます。

No	提出者	該当資料	該当ページ(改定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-42	・αモデルにおいて、LGWAN接続系とインターネット接続系の分割は仮想デスクトップ方式等、画面転送による分割が想定されていますが、仮想デスクトップ方式はセキュリティの担保と引き換えに導入・維持コストが膨大になり、自治体によっては予算の捻出が難しいケースも想定されます。 そのためLGWAN端末内の隔離された独立空間で動作し、その他の端末内部領域へのアクセスが一切出来ないよう制御され、併せて、一切の情報ファイル等をLGWAN端末内に残すこともない仕組みを持つ仮想ブラウザ方式、仮想コンテナ方式であれば、導入コストも抑えられるため、選択肢の一つとして考えてもよいのではないでしょうか。	ご意見は今後の施策検討の参考とさせていただきます。
24	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	ローカルブレイクアウトに関して、図表26ではセキュリティクラウドから別経路としてインターネット回線が用意されるようになっていますが、汎用的なクラウドサービスの利用が進んだ場合にセキュリティクラウド内の通信量及びセッション数などが大幅に増え、各構成団体のクラウドサービス利用に影響を及ぼすことが想定されます。 そのため、各都道府県と各構成団体の協議に基づき、各構成団体のインターネット接続系からセキュリティを担保する前提で特定のクラウドサービスへの通信を許可することも検討する必要があるのではないでしょうか。	第3編解説に、各都道府県と各構成団体の協議の結果に基づき、各構成団体のインターネット接続系からセキュリティを担保する前提で特定のクラウドサービスへの通信接続することについて記載をしています。
25	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-45～46	ローカルブレイクアウトの説明と図が世間の「ローカルブレイクアウト」の定義とかけ離れているため修正すべき。 「回線の物理敷設場所」と「誰が管理するか」の要素に分けて整理すべき。 「ローカルブレイクアウト」は、一部の通信をセンターに集約することなく拠点から直接通信させることを指す旨の定義が複数の文献においてなされています。これを自治体にあてはめると、自治体の各庁舎から、または自治体の通信を集約するセンターから、一部の通信をセキュリティクラウドに集めることなく通信させることが該当すると考えられます。 しかしiii-45の(注10)において、「構成団体と１対１で紐づく通信元IP」との記載があり、この表現は暗黙に「市区町村の通信をいったん都道府県センターに集約してから別回線にルーティングする」という前提で書かれているように見えます。それは「SCの上流の回線を2本目に負荷分散すること」に過ぎず、「ローカルブレイクアウト」の定義に全く当てはまりません。 iii-46の図26においてもローカルブレイクアウト回線が「自治体情報セキュリティクラウド」のFWから分岐・引かれていますが、これも「2本目のセキュリティクラウド上流回線」であり「ローカルブレイクアウト」ではありません。冒頭にて「トラフィック増加に対応するため」という目的が記載されていますが、セキュリティクラウドに通信を集約してから分岐してはその目的を達成できません。「ローカル」ブレイクアウト回線は自治体側のFWにおいて分岐する図に改めるべきと考えます。 後段に「協議の結果、構成団体のインターネット接続系からローカルブレイクアウトする場合は」と、あたかも例外的であるかのような扱いで記載されていますが、それがそもそもローカルブレイクアウトであり、前段の「都道府県センターに束ねてから分岐すること」は、全く「ローカルブレイクアウト」ではありません。 本件は、「ローカルブレイクアウトの設計・構築・運用・管理を誰が行うか」と「ローカルブレイクアウト回線を物理的にどこに引き込むか」という本来異なる要素を同一視された結果おかしなことになったと推察します。 しかし、前段に記載されている「原則として、都道府県側の設定により、実施すること」と、「ローカルブレイクアウト回線を市区町村に敷設すること」とは別要素であり、矛盾なく成立します。 当方の県の次期セキュリティクラウドにおいても、ローカルブレイクアウト回線は市町村に敷設しており、その回線や分岐するUTMに関する管理は県の統括下にある構成となっています。 「管理の集約」と「設置場所の集約」は別の問題ですので、その点を分けて記載いただきたく思います。 なお、後段で「構成団体のインターネット接続系からローカルブレイクアウトする場合は、構成団体において、情報セキュリティに関する責任を負うこととなる」とありますが、こちらは「どこに回線を敷設するか」の話ではなく「ローカルブレイクアウトの設計・構築・運用・管理を誰が行うか」の話に変わっていると思われるため、同様に見直す必要があると思われます。	今回ガイドラインに追記した内容は、令和２年度に各都道府県、市区町村の代表の構成員とともに協議して決定した手順書に示された内容（総務省「次期自治体情報セキュリティクラウド導入手順書令和2年8月」）を改めて、ガイドラインに記載したものとなります。
26	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-45	LGWAN接続系からのローカルブレイクアウトも考慮すべき iii-45の(注10)において、「構成団体のインターネット接続系からローカルブレイクアウトする」と、ローカルブレイクアウト元の想定がインターネット接続系のみとなっています。しかしiv-20において「LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合」も存在し得ることが示されています。このため、本項においてもLGWAN接続系からのローカルブレイクアウトも想定に含んだ記載とすべきと考えます。	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(改定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
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-45	ローカルブレイクアウトしない場合に構成団体がセキュリティに関する責任を負わないかのような記載を修正すべき (注10)において、「構成団体のインターネット接続系からローカルブレイクアウトする場合は、構成団体において、情報セキュリティに関する責任を負うこととなる」とありますが、これは裏返すと「構成団体のインターネット接続系からローカルブレイクアウトしない場合は、構成団体において情報セキュリティに関する責任を負わない」かのようにも見えます。しかし実際はそんなことはなく、ローカルブレイクアウトの有無にかかわらず、構成団体は自団体の情報セキュリティに関する責任を負うはずです。 ここで本来言いたかったことを推察すると、以下のようになるのではないでしょうか。 「構成団体のインターネット接続系からローカルブレイクアウトする場合は」 ↓ 「ローカルブレイクアウトの設計・管理を都道府県ではなく構成団体が行う場合は」 (「どこに回線を敷設するか」ではなく、「誰が管理するか」である) 「構成団体において、情報セキュリティに関する責任を負うこととなる」 ↓ 「構成団体単独でその回線利用に係るセキュリティ確保を行わなければならない」 (「誰が責任を負うか」ではなく、「適切に管理する負担を誰が負うか」である)	今回ガイドラインに追記した内容は、令和２年度に各都道府県、市区町村の代表の構成員とともに協議して決定した手順書に示された内容（総務省「次期自治体情報セキュリティクラウド導入手順書令和2年8月」）を改めて、ガイドラインに記載したものとなります。
28	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-45	「セキュリティクラウドと同等の情報セキュリティ対策機能を構成団体が自ら実装する必要がある」は非現実的 「セキュリティクラウドと同等の情報セキュリティ対策機能を構成団体が自ら実装する必要がある」とありますが、セキュリティクラウドの機能は多岐に渡り、その全てについて同等のものを市区町村が実装できるわけがありません。もしそれができるのであれば、当該団体はローカルブレイクアウト以前にセキュリティクラウドに参加する意味自体がないことになります。この文言は実質的に「禁止」と言っているに等しいものです。 前段において「都道府県と構成団体の協議」が前提となっているのですから、ここの記載は「セキュリティクラウドと同等の～機能を～実装がある」ではなく、「都道府県による管理と同等のセキュリティレベルを保つ必要がある」（そのための具体的な実施事項は前段の協議により様々異なる）のようにすべきと考えます。	令和２年度に各都道府県、市区町村の代表の構成員とともに次期セキュリティクラウドの機能等を検討した際に、インターネットの接続においては、セキュリティクラウドを利用する方向となりました。インターネット接続系において例外的に構成団体がローカルブレイクアウトする場合においても、セキュリティクラウドと同等なセキュリティ機能が必要となることを想定しております。ただし、ローカルブレイクアウトして利用する内容やサービスの範囲等で必要なセキュリティ機能は異なりますので、今後、ローカルブレイクアウトの定義を例外措置（一時的な利用）とするのか、恒久的な措置とするのか等様々な論点について整理した上で、記載内容の見直しを検討させていただきます。
29	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-45～46	通信元ポート番号による識別は一般的に不可能 iii-45の(注10)において、 「構成団体と１対１で紐づく通信元IP・ポート番号と通信先IP・ポート番号をもとに」とありますが、通信元のポート番号はごく稀な特殊ケースを除きランダムであり本件での通信識別に利用できないため、「通信元ポート番号」は削除すべきと思われます。 iii-46の図26も同様です。	今回ガイドラインに追記した内容は、令和２年度に各都道府県、市区町村の代表の構成員とともに協議して決定した手順書に示された内容（総務省「次期自治体情報セキュリティクラウド導入手順書令和2年8月」）を改めて、ガイドラインに記載したものとなります。あくまでも例示として挙げている内容のため、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(改定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	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-45～46	以上のまとめ 以上を踏まえた(注10)全体通しての修正案を以下に示します。 自治体情報セキュリティクラウド構成団体からのクラウドサービスの利用増加等に伴うトラフィック増加に対応するため、ローカルブレイクアウトを行う場合には、その実施可否について、セキュリティ上のリスクを勘案し、都道府県、市区町村で協議の上、慎重に判断する必要がある。 ローカルブレイクアウトを行う場合、自治体情報セキュリティクラウド内で構成される機能が適用できなくなることや、当該ルートを狙った攻撃等のリスクの増加を十分に理解した上で、セキュリティリスクの増加を最小限に止める必要がある。例えば、信頼できる事業者が提供する特定のクラウドサービスのみローカルブレイクアウトを認める、構成団体の通信元IPと通信先IP・ポート番号をもとにポリシーベースルーティングで通信を振り分ける、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などといった適切なセキュリティ対策を講じるとともに、セキュリティインシデント発生時の対応手順をあらかじめ用意する必要がある。 ローカルブレイクアウトを行う場合、原則として構成団体のインターネット接続系から行うものとする。通信先のクラウドサービスがLGWAN接続系である場合は、構成団体のLGWAN接続系からローカルブレイクアウトすることもあり得るが、構成団体内における分割と同様に、通信先のクラウドサービスもその通信経路もインターネット接続系から分割された構成としなければならないことに留意する。 ローカルブレイクアウトを行う場合、原則として、都道府県の設定により実施することとする。構成団体による設定を行う構成とする場合、その接続構成・設定状況を構成団体が都道府県に報告する等により、都道府県による設定と同等のセキュリティレベルを保つ必要がある。また、自治体情報セキュリティクラウドと同様に、接続構成が十分に安全な状態で運用されているか、定期的に外部監査を受けなければならない。	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	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	iv-20	LGWAN接続系からパブリッククラウドを利用するための通信中継を行うLGWAN-ASPサービスを禁止する意図があるのか。その必要はないのではないか。 iv-20において 「LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合…専用回線を用いて接続しなければならない 」とありますが、ここでの「専用回線」とは、イーサ型専用線やIP-VPNのような閉域網のことを指しているのでしょうか? また、現存するLGWAN-ASPの中には、LGWAN接続系からパブリッククラウドを利用するための通信中継を行うものが複数存在しており、またその中継経路は必ずしも閉域網とは限らずインターネットの場合もあります。今後はそのようなサービスの提供・利用を禁止する意図があるのでしょうか? 私の意見として、その通信経路の設計・アクセス制御が適切であれば、中継経路が閉域網であることは必須ではなく、閉域網はそれを達成する手段の一つに過ぎないものと考えます。	ご意見は今後の施策検討の参考とさせていただきます。
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	iii-38	(「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」iii-38中「・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は、IPS(ホスト型・ネットワーク型侵入検知システム)や WAF(Web Application Firewall) 等を用いて、脆弱性を悪用した攻撃を防ぐといった対処も考えられる。」との記載部分) ・意見内容 当該部分について「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をおこなうとともに、Firewallや IPS/IDS(ホスト型・ネットワーク型侵入検知システム)や WAF(Web Application Firewall) 等を用いて、境界防護および境界内防護に関する環境を整備し脆弱性を悪用した攻撃を防ぐといった対処も考えられる。」との変更を提案します。 (理由) 近年、キュリティ上の驚異が増え、単一のセキュリティ対策では対応が十分ではなくなっています。そのため、より実効性のあるガイドラインとするため、修正プログラムの常時適用と合わせて、ネットワーク関連のセキュリティ対策による境界防護および境界内防護を明記する事を提案します。また、セキュリティ対策機能として記載されているIPSおよびWAF以外に、Firewallも一般的に利用される機能であるため追記を提案します。 (補足) 『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』(総務省:2022年10月) におきましてもP48［ 図表III. ３. １－１ クラウドにおけるセキュリティ設定項目の類型と対策 ］ネットワークの項目に下記の記載があり、マイナンバー利用事務系においても有効な対策と考えられます。 -------- クラウド利用は、インターネット経由となるため、外部ネットワークとのアクセスに関する基本的なセキュリティ設定、仮想プライベートクラウドのセキュリティ設定、Firewall/IPS/IDS や WAF などによる境界防護および境界内防護等に関する設定を確実に行う必要がある。 ------- https://www.soumu.go.jp/main_content/000843318.pdf	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(改定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
33	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-38	（「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」iii-38中「マイナンバー利用事務系においては、インターネットとの接続が出来ないため、シグネチャの更新方法(自治体情報セキュリティ向上プラットフォームの活用や媒体による手動更新等)を確認する必要がある。」との記載部分) ・意見内容 　当該部分について「マイナンバー利用事務系においては、原則としてインターネットとの接続が出来ないため、シグネチャの更新方法(自治体情報セキュリティ向上プラットフォームの活用や媒体による手動更新、例外的なインターネット接続が可能であるか等)を確認する必要がある。」との変更を提案します。 （理由） iv-7において下記の記載がありますので、本項における記載に関しても同様な内容への修正を提案します。 ------- ガバメントクラウド以外のクラウドサービスについては、ISMAP認証やクラウド サービスにおける第三者認証1を取得したサービスにおいて、標準準拠システム等の利用・ 運用が想定される。この場合、修正プログラムの更新や管理コンソールのアクセス等の運用 保守を行うにあたり、デジタル庁より示されたリスクアセスメントの結果等を参考とし、ガバメントクラウドと同等の情報セキュリティ対策が実施されていることを評価(内部監査・ 外部監査等)することを条件に、例外的にインターネット接続を可能とする。 ------	第４編は、標準準拠システム等を想定して、ISMAP・第三者認証やリスクアセスメントの実施を条件のもと、例外的なインターネット接続を可能としています。ご指摘の第3編に関しては、クラウドサービスの利用を前提としたものとではなく、幅広い情報システムの利用や運用形態を想定したものとなっています。マイナンバー利用事務系全般に関して、例外的なインターネット接続を拡大する意図ではないため、現行の記載としております。
34	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-114	（「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」iii-114中「また、可用性を担保する対策としては、対象となるデータだけではなく、システムのバックアップを取ることでシステムの迅速な復旧につなげることができる。その際、有事の際に早急に対応できるようバックアップから復旧可能なことや復旧手順を定期的に確認しておくことも重要となる。」との記載部分) ・意見内容 　当該部分について「また、可用性を担保する対策としては、対象となるデータだけではなく、システムのバックアップを取ることでシステムの迅速な復旧につなげることができる。その際、有事の際に早急に対応できるようバックアップから復旧可能なことや復旧手順を定期的に確認しておくこと、及び、バックアップからの復元にあたってはランサムウェア感染前の復旧ポイントの特定手法や、復元したバックアップにマルウェアが残存していないかの確認を復旧手順に含める事が重要となる。」との変更を提案します。 （理由） ランサムウェア被害によるバックアップからの復旧においては、通常のバックアップからの復旧だけではなく、復旧ポイントの特定に時間を要する事が多いため特定方法を事前に確立しておくことが重要となります。また、復元したバックアップデータからの再感染を防止するために復元データの安全性の確認も重要な作業となります。	御指摘を踏まえ、下線部について記載を修正いたします。 「なお、「データのバックアップ」については、バックアップの保存先が、ランサムウェアに感染した端末等からアクセスできる領域にある場合、バックアップを含め暗号化されてしまう可能性があるため、端末のOS からアクセスできないネットワークから切り離されたオフラインのディスクや媒体等へ保管することも検討が必要となる。また、可用性を担保する対策としては、対象となるデータだけではなく、システムのバックアップを取ることでシステムの迅速な復旧につなげることができる。その際、有事の際に早急に対応できるようバックアップから復旧可能なことや復旧手順を定期的に確認しておく。バックアップからの復元にあたってはランサムウェア感染前の復旧ポイントの特定手法や、復元したバックアップにマルウェアが残存していないかの確認を復旧手順に含めることが重要となる。」