「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４年３月25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４年１月12日（水）から１月25日（火）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、13件（法人８件、個人５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４年３月25日（金）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	該当ページ又は該当監査項目 （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	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-46	「8.2.外部サービスの利用」について、だれが何に責任を負うのかを明確にするという視点を加える必要があるのではないでしょうか。また、CSPとの契約またはSLAの段階において、役割とガバナンスを明確かつ十分に文書化することを明記しては如何でしょうか。 CSA_ver4.0※1 では、「いかなるクラウドプロジェクトであれ、最も重要なセキュリティ上の注意点は、だれが何に責任を負うのかを的確に把握することである。（※1_ 1.2.1 クラウドにおけるセキュリティとコンプライアンスの範囲と責任より）とあり、NIST SP800-61rev2※2 で定義しているインシデントレスポンスライフサイクルに関するCIRフレームワーク※３ では、CIRの場合は、従来のオンプレ型と違いCSPとCSCの責任と役割を明確に意識する必要がある。としている。 （参考）CIRフレームワーク※３ 「5.1 フェーズ 1：準備とそれにともなうレビュー」より 組織のインシデンスレスポンス機能を理解するためには、CSCとCSPの間に「責任共有モデル」が存在することを意識する必要がある。 オンプレ・・・システムを所有する組織がシステムに対して単独で責任を負います。 クラウド・・・CSCがすべてのシステムの所有者であるとは限りません。 採用されたサービスモデルとそれに対応する「責任共有モデル」に応じてCSCとCSP、サードパーティのIRプロバイダなどと連携し、インシデント発生時には、いち早く活性化できるよう、CSCはCSPのIR手順を理解し、SLAと契約を通じてそれらと整合をとる必要がある。 ※１　クラウドコンピューティングのためのセキュリティガイダンスver4.0 ※2018.7.24日本語訳V1.1 https://cloudsecurityalliance.jp/j-docs/CSA_Guidance_V4.0_J_V1.1_20180724.pdf ※２　NIST SP800-61Rev.2 https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final ※３　クラウドインシデントレスポンスフレームワーク ※2021.6.3日本語訳V1.0 https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2021/06/Cloud-Incident-Response-Framework-4_30_21_J.pdf	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。なお、情報セキュリティ確保のために外部サービス利用者自らが行うべきこと、外部サービス提供者に対して求めるべきこと等をまとめた様々な参考文書を「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」上に明記しております。
2	個人	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	342、364	「3.8.2外部サービスの利用（機密性２以上の情報を取り扱う場合）」及び「3.8.3外部サービスの利用（機密性２以上の情報を取り扱わない場合）」について、だれが何に責任を負うのかが文書化され、正式に承認されていることを確かめる必要があるのではないでしょうか。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。なお、情報セキュリティ確保のために外部サービス利用者自らが行うべきこと、外部サービス提供者に対して求めるべきこと等をまとめた様々な参考文書を「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」上に明記しております。
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	ⅰ-11	「第1章2.本ガイドラインの経緯」にも記載があるように、デジタル庁の設置により、地方公共団体のDX推進を国と一体となって進めていくにあたり、本ガイドラインの所管についてもデジタル庁若しくはNISCに移管することで、セキュリティ対策の一体化が図れるものと考えます。	引き続きデジタル庁及びNISC等関係機関と連携しながら、地方公共団体の情報セキュリティ対策の向上に努めてまいります。
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	ⅲ-139	「約款による外部サービス」を用いた機密性２以上の情報を取り扱う行政サービスについて、原則禁止で例外での取扱いではなく、一定の基準を示すべきと考えます。 ※ISMAPクラウドサービスリストのServiceNowやデジタル庁アイデアボックスのPoliPoliGovなどはどのような判断で機密性2以上を取扱えているのか。	「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」上、原則、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、機密性２以上の情報は取り扱わないこととしております。 ただし、約款等で記載されている内容が、自組織が求めるレベルのセキュリティ対策を保証するものである場合には、各地方公共団体の判断により、利用を認めるという運用も考えられます。
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	ⅱ-32	「CISOが定めた電子署名、暗号化」「CISOが定めた方法で暗号のための鍵を管理」「CISOは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供」とあるが、CISOが具体的にどのようなことを実施するべきか不明であり、CISOが個別に定めず「電子政府推奨暗号リストに定められた」とすることでセキュリティ水準を一定に保てると考えます。	御指摘の記載の解説において、「電子政府推奨暗号リスト」を参照することを求めております。
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	ⅱ-19	情報システム全体の強靭性の向上で、「α」「β」「β’」の3パターンが示されていますが、政府が自治体DX加速のため、いわゆる個人情報保護法制2000個問題の解決に着手しようとしているときに、情報セキュリティポリシーで新たな2000個問題が発生することを防ぐため、１つに絞る、若しくは目指すべきパターンを示すべきと考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
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	ⅲ-144	外部サービス利用判断基準として、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」などが参考として示されているが、自治体毎に判断基準のバラツキがでないよう、監査ガイドラインのように、統一的且つ具体的な雛形やサンプル等を提示する必要があると考えます。	地方公共団体が外部サービスを利用する際に参考となる情報を提供するよう努めてまいります。

No	提出者	該当資料	該当ページ又は該当監査項目 （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
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-45	国等が指定するクラウドサービスを利用する場合は、地方公共団体は情報システムを管理しているとはならない（8.外部委託の適用を受けない）という整理で良いでしょうか。（例　デジタル改革共創PF、HER-SYSなど）	個々のシステムにより取扱いは異なるものと考えます。
9	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-45	建築設計や測量委託において、委託先が情報共有のために用意するクラウドシステムについては、地方公共団体は情報システムを管理しているとはならない（8.外部委託の適用を受けない）という整理で良いでしょうか。（例 土木工事等の情報共有システム など）	委託先において外部サービスを利用する場合は、委託先においても外部サービス特有のリスクがあることから、「8.2.外部サービスの利用（機密性２以上の情報を取り扱う場合）」で規定する内容についても、委託先への要求事項に含める必要があります。
10	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-45	アンケート収集を事業者が直接実施し、集計結果が成果物であり、必要に応じて個別のアンケート内容を地方公共団体へ提供するような業務を委託した場合に、地方公共団体は情報システムを管理しているとはならない（8.外部委託の適用を受けない）という整理で良いでしょうか。	委託先において外部サービスを利用する場合は、委託先においても外部サービス特有のリスクがあることから、「8.2.外部サービスの利用（機密性２以上の情報を取り扱う場合）」で規定する内容についても、委託先への要求事項に含める必要があります。
11	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-20～23、30	外部サービス利用時は「4.1.サーバ等の管理」「4.2.管理区域(情報システム室等）の管理」「4.3.通信回線及び通信回線装置の管理」「6.1.(10)外部ネットワークとの接続制限等」の適用範囲外でしょうか。	物理的対策として管理の対象となります。ただし、外部サービスの実態により自治体が直接管理が難しい場合は、外部監査報告書を確認するなどして対応することが考えられます。
12	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-18	境界型防御の禁止 ネットワーク内にあることを前提に防御しているので不便かつ危険。 ゼロトラスト以外を禁止してほしい。 1)パブリック・クラウド利用可能システムと利用不可システムの分離 2)システムのクラウド化徹底とネットワークセキュリティ依存の最小化 3)エンドポイント・セキュリティの強化 4)セキュリティ対策のクラウド化 5)認証と認可の動的管理の一元化 以上に逆行する行動をしても良い基準が定められてない。 https://cio.go.jp/sites/default/files/uploads/documents/dp2020_03.pdf クラウドでないサーバーを自前で調達しても良い基準が定められてない。 情報の送信 電子メール等により機密性２以上の情報を送信する者は、必要に応じ、パスワード等による暗号化又はパスワード設定を行わなければならない。 ストレージへのリンクで送信するべきで、閲覧権限を管理者から削除できるべきである。実体を相手に送信することはそれができないときにするべき。 クラウド前提の条文になっていないが、なぜこのような条文が出てきたのか不可解である。 情報資産の運搬 （ア）車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。 （イ）機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。 そもそもパスワードを使うな。 認証情報は個人のIDのみを利用するべきであり、パスワードを生成すればするほど漏れる可能性が高まるのでやってはいけない。なぜ禁止していないのか？禁止するべき理由は https://www.amazon.co.jp/%E3%82%BC%E3%83%AD%E3%83%88%E3%83%A9%E3%82%B9%E3%83%88%E3%83%8D%E3%83%83%E3%83%88%E3%83%AF%E3%83%BC%E3%82%AF-%E2%80%95%E5%A2%83%E7%95%8C%E9%98%B2%E5%BE%A1%E3%81%AE%E9%99%90%E7%95%8C%E3%82%92%E8%B6%85%E3%81%88%E3%82%8B%E3%81%9F%E3%82%81%E3%81%AE%E3%82%BB%E3%82%AD%E3%83%A5%E3%82%A2%E3%81%AA%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E8%A8%AD%E8%A8%88-Evan-Gilman/dp/4873118883/ref=asc_df_4873118883/?tag=jpgo-22&linkCode=df0&hvadid=342647643803&hvpos=&hvnetw=g&hvrand=14947104536272098350&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1009327&hvtargid=pla-836654098941&psc=1&th=1&psc=1 https://wowma.jp/item/478734379?aff_id=PLA_m_9601 前述したものも含めて上記に書いてある。この書籍が禁止していることをやるな。ゼロトラスト関係の書籍を一通り読んでから次回の会議をするべき。ゼロトラストと矛盾することが多すぎていちいち指摘するのが面倒なので、次回までに治すように。https://www.soumu.go.jp/main_content/000726081.pdf 89 でゼロトラストに関して参考にするようにと言われているが、上記書籍と政府CIOの意見は参考にしたのか？ 西村 毅、満塩 尚史、細川 努、楠 正憲、田丸 健三郎、梅谷 晃宏に聞くべきである。聞いていないのか？	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。

No	提出者	該当資料	該当ページ又は該当監査項目 （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
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	－	地方公共団体のサイバーセキュリティのレベルを統一的に向上させようとする貴省の不断の努力に感謝致します。会員企業は、クラウドコンピューティング、セキュリティソリューション、データアナリティクス、AI（人工知能）などの最先端の技術やサービスを世界に先駆けて提供し、政府や社会のデジタルトランスフォーメーションを支えています。サイバーセキュリティやデータ・ガバナンス政策の策定において、当法人は世界中の政府と緊密に協働してきました。そのことを通し、このような政策や法案が市民のプライバシーと自由を守りながら、サイバーセキュリティの脅威を効果的に抑止・管理するのを可能にするのを直に見てきました。 サイバーセキュリティ関連政策を成功させるための重要な要素として、国際的に認知された基準との整合性、リスクベース、成果志向、技術中立的アプローチの採用、イノベーション促進のために政策の順応性を高めることなどが挙げられます。そして、サイバーセキュリティ課題に対処するには、接続環境にあるデータ・エコシステムの完全性、機密性、回復力を防御するための革新的なツールと実践が必要であり、高度な暗号化など、最善のセキュリティソリューションを利用できることが不可欠です。したがって我々は、政府が民間部門と密接に協力し、セキュリティアプローチの最新の進歩の恩恵を受けられるように、セキュリティポリシーを策定することを奨めます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
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	－	デジタル社会の実現に向けた取り組みが加速する中、デジタル庁から発表された新たな「重点計画」を我々は高く評価しています。本計画では、地方公共団体の情報システムを刷新する政府の確固たるコミットメントが示され、デジタル変革のためには、安全なクラウドコンピューティングサービスを最大限に活用することが重要であることが認識されており、また、現在、ガバメントクラウドを検証する先行事業が一部の地方自治体で実施されています。市民サービス向上のために、パブリッククラウドの利用拡大を視野に入れながら、貴省がデジタル庁と共に、ガイドラインを継続的に見直されることを我々は強く推奨します。	引き続きデジタル庁及びNISC等関係機関と連携しながら、地方公共団体の情報セキュリティ対策の向上に努めてまいります。
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	－	マイナンバーのネットワーク保護のためのクラウド活用推進 今回のガイドラインは、先般、内閣サイバーセキュリティセンター（NISC）が改訂した「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」との整合性を図ることに重点が置いていると理解しています。クラウドサービスが「外部サービス」に含まれ、取り扱う情報の機密性に基づいたセキュリティ対策が推奨される等、ガイドラインにおいて明確化されたことを我々は支持します。また、クラウドサービスの選定において、国際的に認められたセキュリティ基準や第三者監査が認められていることも歓迎します。 本ガイドラインにおける上記の改善点を高く評価しつつも、我々は、場合によっては物理的なネットワーク分離を必要とするような、現在の「三層の対策」に依存しないセキュリティアプローチを継続的に検討されることを強く推奨します。会員企業のクラウドサービスは、インターネットを介した信頼性の高い安全なアクセスを可能にする世界で最も安全なインフラに支えられており、暗号化、ゼロトラストアーキテクチャ、高度アクセス管理などの国際的に認められた機能により、機密性の高い個人情報の安全な取り扱いを実現しています。機密性の高い個人情報やその他のデータを保護するための最も効果的なデータセキュリティソリューションは、これらのクラウドサービスによって提供されているのです。 このような視点から、現行のLGWANをインターネットに接続された情報システムから分離する現在のセキュリティ・アプローチを見直されることを求めます。この物理的な分離により、LGWANを使用する政府機関は、クラウドコンピューティングの高度なセキュリティと機能を十分に活用することができなくなってしまいます。貴省が有用であるとお考えであれば、この点に関する理解を深めるために、インターネット接続構成環境におけるセキュリティ確保に関する、会員による技術セッションを開催することも可能です。 我々は、地方公共団体がマイナンバーのデータ管理のための情報システムを保護する必要性を全面的に支持します。しかし、世界中の公共機関においては、情報セキュリティが最も必要とされる業務においてさえも、クラウドサービスが利用されています。信頼性、セキュリティ、拡張性、コスト削減、スピード、アクセスや利用のしやすさなど、高品質のクラウドコンピューティングサービスがもたらす多くの利点が認識されているのです。クラウドサービスは、AIやIoT（InternetofThings-モノのインターネット）、その他の先端技術を用いたイノベーションを可能にします。貴省が本ガイドラインをさらに更新し、日本における政府機関が上記のクラウドサービスの恩恵を享受できるようにすることを奨めます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
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	iii-145	②場所でなく、データセキュリティ実践に基づくクラウドサービスプロバイダ（CSP）の選定 また、外部サービスの利用に関する本ガイドラインの説明が、日本国外のサーバにデータを保存・ 処理する可能性のあるCSPの利用を不必要に制限しているように読めることを、我々は引き続き懸念しております。データセキュリティの確保は、CSPが維持する技術的・物理的なセキュリティ管理に依存しており、データセンターの存在地は、CSPがどのように個人情報を保護するか又は利用者に適用される法律を遵守するかには、ほとんど関係がありません。実際、クラウドサービスの利点の多くは、国境を越えてデータが移転できることにあります。地理的に分散した複数のデータセンター間でデータを移転し、冗長的に保存することでレジリエンス（弾力性）が高まり、データのセキュリティは向上するのです。このアプローチは、日本政府が提唱する「データ・フリー・フロー・ウィズ・トラスト（DFFT）」と明確に合致しています。それゆえに、物理的な場所に焦点を当てた本ガイドラインは、そのような移転を制限することになり、実際には地方公共団体が扱うデータのセキュリティを損なう可能性があります。 以上を踏まえ、貴省に対し、外部サービスの選定の箇所について、以下のように修正することを求めます。 （iii-148頁） 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） 8. 業務委託と外部サービスの利用 8.2 外部サービスの利用（機密性2以上の情報を取り扱う場合） （２）外部サービスの選定 「② インターネットを介して提供される外部サービスの利用に当たっては、外部サービス提供者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、外部サービス提供者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、~~日本の法令の範囲内で運用できるデータセンターを選択する必要がある。~~日本の法令を遵守した場所・方法でデータが保管されることを保証できるサービスプロバイダが運用するデータセンターを選択する必要がある。」	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。

No	提出者	該当資料	該当ページ又は該当監査項目 （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
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	iii-146	②場所でなく、データセキュリティ実践に基づくクラウドサービスプロバイダ（CSP）の選定 さらに、ガイドラインの 8.2の（解説）（２）⑤では、地方公共団体が外部サービス提供者のセキュリティを保証するために、国際的に認められた様々な規格やその他のプログラムに基づく監査または監査報告書や認証に依拠するなど、一定の選択措置を推奨しています。この中には、ISO/IEC 27017や政府情報システムのためのセキュリティ評価制度（ISMAP）、日本セキュリティ監査協会のクラウド情報セキュリティ監査やSOC報告書（Service Organization Control Report）などが含まれています。地方公共団体が利用できるセキュリティ保証について、貴省が柔軟性を持たせていることを我々は高く評価します。地方公共団体がサービスや委託先の信頼性を判断する際に参考とする選択肢として、これらの認証・管理基準・監査要件が記載されており、すべてを満たす必要は無い、という点を明確化することを奨めます。 以上を踏まえ、貴省に対し、以下のように修正することを求めます。 （iii-149、150頁） 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） 8. 業務委託と外部サービスの利用 8.2 外部サービスの利用　（機密性2以上の情報を取り扱う場合） （２）外部サービスの選定 「⑤情報セキュリティ管理者は、外部サービスに対する情報セキュリティ監査による報告書 の内容、各種の認定・認証制度の適用状況等から、外部サービス及び当該 サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。…… このような評価に当たって、外部サービス提供者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用する必要がある。 なお、選定条件となる認証には、ISO/IEC 27017 によるクラウドサービス分野 における ISMS 認証の国際規格がある。また、ISMAP の管理基準を満たすことの確認や ISMAP クラウドサービスリスト等のほか、日本セキュリティ監査協会のクラウド情報セキュリティ監査や外部サービス提供者等のセキュリティに係る内部統制の保証報告書である SOC 報告書（Service Organization Control Report）を活用することを推奨する。上記の一つ又はそれ以上を参考とし、個別の案件に応じ、他の適切な認証やセキュリティ上の保証を利用することも可能とする。」 また、貴省の本改定ガイドラインの概要 で示されているように、外部サービス提供者が満たすべきセキュリティ保証要件についての柔軟なアプローチを、中央政府においても採用されることを奨めます。ISMAPは、NISC、デジタル庁、経済産業省、総務省による共同運用であることは認識しておりますが、中央省庁の情報セキュリティ認証に関しても、貴省が主導し、同様の柔軟な対応を実施することを推奨します。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
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	－	官民連携によるセキュリティ対策の刷新 テレワークが増加し、web会議サービス利用が急増したことによるセキュリティへの影響を考慮した対応を本ガイドラインが提示していることを支持します。 より効果的なガイドラインとするために、上記に加え、ますます深刻化するランサムウェアへの対策にも言及することを奨めます。対策に関しては、様々な機関や団体が取り組みを公表しています。 ガイドラインの中で本情報を参照・活用することを推奨します。 また、サイバーセキュリティ対策のコンセンサスを形成するために、政府と産業界が強固なパートナーシップを築くことを強く支持します。サイバーセキュリティの解決策は、官民連携を受け入れ、市場主導型の解決策を促進することで、最も効果的となります。当法人と会員企業は、貴省と協働し、セキュリティアプローチの最新の進歩に関する洞察を共有していけることを期待しています。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
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	－	本ガイドラインに対し意見する機会を頂けたことを感謝致します。提案された対策案に関し、利害関係者間で検討・議論をするための十分な時間を確保する上でも、今後は、少なくとも30日間の意見募集期間を設けることを強く希望します。今回の我々の意見が本ガイドラインを完成させる上で有益であることを願っております。日本のデジタルトランスフォーメーションの実現に向け、貴省を引き続き支援していきたいと我々は考えております。本意見について、ご質問、又、詳細について協議の機会を頂けるようでしたら、いつでもご連絡ください。	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日未満とさせていただいております。
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	ii-46	「8.2 外部サービスの利用」に係る以下の意見を提示させて頂きます。 ●全体に関して 外部サービス（クラウドサービス）については、主に約款により利用するパブリッククラウドとプライベートクラウドでは、利用者がコントロールできる範囲は異なるため、その選定及び調達に関する内容はそれぞれ分ける必要があると考えます。 パブリッククラウド（特にSaaSの場合）は、クラウドサービス事業者に対して要求を提示することは現実不可能であるため、相応の選定基準及び運用規程を定め、利用することになると考えます。	地方公共団体が外部サービスを利用する際に参考となる情報を提供するよう努めてまいります。
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	－	●小規模自治体への配慮 小規模自治体では、独自に外部サービスの利用に関する規程及び選定基準を定めることは難しいため、その雛形の提供を希望します。また、外部サービスの選定及び運用に関わる職員が限定されるため、自力でクラウドのサプライチェーンを含めたセキュリティ要件を定め、それが満たされているかを把握することは困難であります。従って、外部委託の活用又は最低限のベースライン等を提示することが必要かと考えます。	地方公共団体が外部サービスを利用する際に参考となる情報を提供するよう努めてまいります。
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	－	●要望 「利用に関する規程」及び「外部サービスの選定基準」の雛形が欲しい。	地方公共団体が外部サービスを利用する際に参考となる情報を提供するよう努めてまいります。

No	提出者	該当資料	該当ページ又は該当監査項目 （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-44	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（ⅲ-46）に関する意見： 三層対策において業務端末をインターネット接続系におくβモデルおよびβ’モデルが、クラウドサービスの活用やテレワーク業務環境の整備などパブリック・クラウドの利活用促進による業務効率化や利便性を高める上でメリットがある反面、サイバー攻撃などのリスクが高まるという懸念に対して、今回の改定では、「各端末（エンドポイント）でのセキュリティ対策や不正な挙動等を検知し、早期対処する仕組みを構築する必要がある」という表現だけに留まらず、より具体的な「エンドポイント対策」（EDR: Endpoint Detection and Responseの例）を加える内容の改定がなされており、パブリック・クラウドをより柔軟に活用できるβモデルやβ’モデルを安全に実装にする上で参考となるガイドラインとなっていると考えます。 各端末（エンドポイント）でのセキュリティの強靭化を高めることはパブリック・クラウドを活用していく上で今後益々重要になると考えますが、今回の改定で加えられた各端末への脅威を検知し遠隔で対処するEDRの様な仕組みを考慮するだけでなく、端末自体（ハードウェア）に根ざしたセキュリティを強化することも併せて重要です。 ハードウェアベースのセキュリティは、システム・パフォーマンスへの影響を最小限に抑えながら、ランサムウェア、クリプトジャッキング、システムメモリへの攻撃を発見するための技術であり、システムメモリのすべてを暗号化しOS以下のセキュリティポリシーを徹底することで、マルウェアの注入リスクを低減し、システム管理モードから仕掛けられる攻撃に対して安全なプラットフォームを提供します。 また、処理過程でのデータ保護対策では、データを暗号化したまま処理し機密データの公開を減らすことができる「コンフィデンシャル・コンピューティング（Confidential Computing）」という技術が開発され、対応するハードウェアが提供されています。 さらには、バックドアによるデータ漏洩を防ぐために端末を構成する部品およびシステムレベルのトレーサビリティと検証をおこない真正性を担保する仕組みも存在します。 今後、情報システム全体の更なる強靭性の向上を図るためには、このような「ハードウェアに根ざしたセキュリティ強化」の必要性を、具体的な実施方法とともにガイドラインとして示していくことが重要と考えます。	いただいた御意見は今後の施策の検討や実施に当たって、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-37	ⅲ-39（注1）について、マイナンバー利用事務系の「インターネットに接続されたシステム等で十分に安全性が確保された外部接続先との通信」先として、具体名は伏せますが、ほぼ全ての組織で利用されている文書・表計算等ソフトのオンライン認証（LGWAN-ASP等、ⅲ-40（注2）では認証できない）について、今回の追記内容に含まれていないものは、本ガイドラインにおいては接続を推奨しない認識でよろしいでしょうか。	ご認識のとおりです。
25	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-21	「(4)リスク分析の実施」において以下の追記を提案します。 「リスク分析とは、各地方公共団体が保有する情報資産を明らかにし、それらに対するリスクを評価することである。情報資産は、認識している資産だけでなく、外部視点（攻撃者視点）での調査・把握を行い、自組織で認識しているもの以外の資産がないかも含めて明確化すること。」 多くの部門で行政のデジタル活用が進む中で、部門・事業毎のホームページの開設など、保有・利用している全ての情報資産を正確に把握することは困難です。そのため、認識されている資産以外に、外部からの視点で自組織の資産として認識されているもの以外の資産がないかを検証することが、今後の安全なデジタル活用の促進には不可欠だと考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
26	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-28	「(2)IDの取扱い」について、以下の文章への修正を提案します。 「②原則、共用IDの利用は禁止とする。ただし、業務上止むを得ない場合に限り、その運用を認めるが、その場合は、過去に遡って共用IDの利用者が特定できるように記録・管理すること。」 先日閣議決定された「デジタル社会の実現に向けた重点計画」でもゼロトラストアーキテクチャは重視されており、ゼロトラストを実現するにあたりID管理は非常に重要な要素の一つです。過去の経緯からIDの共用を認めざるを得ないことは理解できますが、原則を設定し、適切な環境を周知すべきだと考えます。	御指摘を踏まえ、下線部のとおり記載を追加いたします。 5.人的セキュリティ 5.4ID及びパスワード等の管理【解説】 （2）IDの取扱い IDの利用は本人に限定することを規定する。 また、共用IDの利用は、業務上止むを得ない場合に限定する必要がある。その上で、止むを得ず共用IDを利用する場合には、過去に遡って共用IDの利用者を特定できるように記録・管理することが望ましい。
27	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-38、39	「(1)統括情報セキュリティ責任者の措置事項」、「(２)情報システム管理者の措置事項」において以下の追記を提案します。 「不正プログラム対策ソフトウェアはパターンファイルだけでなく振る舞い検知にて未知の不正プログラムに対しても対策を講じなければならない。」パターンファイルのみの対策では既知の不正プログラムには対策可能だが未知の不正プログラムへの対策ができず不十分であると考えます。	同様の趣旨の内容を記載済みのため、追記は不要と考えます。
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	ⅱ-38、39	6.4不正プログラム対策 (1)⑤、(2)②に共通して文言の修正を提案します。 「不正プログラム対策ソフトウェアが常にその最新の情報を利用し挙動する状態に保たれなければならない。」 「パターンファイルは、常に最新の状態に保つ」という表現は、振る舞い検知型などパターンファイルの更新が必要ない製品を意図せず排除すると考えられますので、表現を修正すべきと考えます。	いただいた御意見は今後の施策の検討や実施に当たって、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-44	③注１０について以下の追記を提案します。 修正案： 従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する（ふるまい検知）。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらに、インシデント発生要因の詳細な調査を実施することで、検知、復旧等の早期対処を可能とする。 「従来のパターンマッチング型の検知」と対比した検出機能を明示することで、読者が記載内容をより理解でき易くなると考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。

No	提出者	該当資料	該当ページ又は該当監査項目 （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	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- 44	「（３）インターネット接続系」について、以下の文章への修正を提案します。 「早期検知のための仕組みの構築には未知の不正プログラム対策（エンドポイント対策）の導入が有効である。エンドポイント対策は、従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらに、インシデント発生要因の詳細な調査を実施することで、検知、復旧等の早期対処を可能とする。 従来モデル（αモデル）を採用している場合でもLGWAN接続系から特定通信を利用したインターネット接続（外部サービスへの通信等）が発生する場合は、βモデル及びβ’モデルと同様にインターネットからのリスクが増加することから未知の不正プログラム対策の導入及びマネージドサービスの運用が有効である。」 αモデルにおいても特定通信としてインターネットに公開されたクラウドサービスに接続しているケースが散見される。これらの団体は従来のαモデルのように完全なインターネット接続との隔離ができていないことからβやβ’と同等の対策が必要と考えます。	いただいた御意見は今後の施策の検討や実施に当たって、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-47	注１１について、以下の通り変更を提案します。 原文： （前略）不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式が（後略） 修正案： （前略）不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、その実行ファイルないしは端末そのものを隔離する方式が（後略） 「これ」が指す単語は「不正プログラム」であると思われますが、実際の隔離はプログラムそのものではなくそれを実行するマルウェア、もしくは不審な挙動が行われている端末単位を対象にするため、変更することでより正確かつわかりやすい表現になると考えます。	御指摘を踏まえ、次のとおり記載を修正いたします。 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【解説】 （注11）未知の不正プログラムへの対策（エンドポイント対策） 【修正前】 　未知の不正プログラム対策として、OSのプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。（後略） 【修正後】 　未知の不正プログラム対策として、OSのプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、その実行ファイル又は端末を隔離する方式があり、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。（後略）
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-48	「（４）その他のセキュリティ対策」⑤について、以下の文章への修正を提案します。 「⑤VPN接続による外部との通信遠隔での情報システム保守により、マイナンバー利用事務系及びLGWAN接続系についてVPN接続による通信を許可する場合は、特定通信としての設定がされており、かつIP－VPN等の閉域網や適切なセキュリティ設定を施されたインターネットVPN、又はLGWANに接続されなければならない。」 LGWAN接続系に配置されるPCでも特定通信としてMicrosoftのM365等を利用してTeamsやOfficeを利用する他にも利便性が高い外部サービスを利用するケースが考えられます。その場合にはIP-VPNや閉域接続以外にも適切なネットワーク設定を施した上でインターネットVPNを利用して低コストで接続させることも考慮されるべきと考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
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-48	「③修正プログラム及びパターンファイルの更新」についてクラウド型のセキュリティ対策製品についてはプロキシサーバを利用する構成において特定ポート通信を許可する変更を提案します。 最新の脅威に対応していくためにはクラウド型のセキュリティ対策が必要となってくるため、条件の緩和が必要だと考えております。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
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-144	シャドーIT対策として以下の追記を提案いたします。 原文：所属する組織の承認を得ずに職員等が外部サービスを利用することは“シャドーIT”と呼ばれるが、シャドーITは監視が不十分になりやすく、セキュリティリスクが高まる等の問題がある。そのため、シャドーITの対策としては、職員等が外部サービスを利用する場合に必ず申請を行い自組織が承認を行う運用が考えられる。 案：所属する組織の承認を得ずに職員等が外部サービスを利用することは“シャドーIT”と呼ばれるが、シャドーITは監視が不十分になりやすく、セキュリティリスクが高まる等の問題がある。そのため、シャドーITの対策としては、職員等が外部サービスを利用する場合に必ず申請を行い自組織が承認を行う運用が考えられる。より有効な対策として、CASB等、外部サービス利用状況を可視化するシステム導入あるいはサービス利用がある。 外部サービスに関わるシャドーIT対策としては、CASB導入等、サービス利用状況を可視化することが非常に有効です。 実質的には、シャドーITの対策としては、申請/承認、職員教育だけでは難しい現実があると考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
35	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	－	8.2. 業務委託と外部サービスの利用について (4)外部サービスの利用承認についての具体的な解説文章がありませんでした。記載が必要と考えます。	御指摘の記載については解説する事項がないため、原案のとおりとさせていただきます。

No	提出者	該当資料	該当ページ又は該当監査項目 （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
36	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-149	8.2. 業務委託と外部サービスの利用について (4)外部サービスを利用した情報システムの導入・構築時の対策内にある①(オ)外部サービス上に保存する情報や外部サービスの機能に対してアクセス制御できることの確認が必要と記載があります。クラウドストレージサービスなど外部サービス上にファイルを保存、管理するものを利用する場合、端末内に存在する一時ファイルや同期ファイルの保護やアクセス制御も考慮が必要と考えます。	今後の検討の参考とさせていただきます。 なお、端末に対する対策については、「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」の解説に記載しております。
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	i-21	「(4)リスク分析の実施」において以下の追記を提案します。 「リスク分析とは、各地方公共団体が保有する情報資産を明らかにし、それらに対するリスクを評価することである。情報資産は、認識している資産だけでなく、外部視点（攻撃者視点）での調査・把握を行い、自組織で認識しているもの以外の資産がないかも含めて明確化すること。」 多くの部門で行政のデジタル活用が進む中で、部門・事業毎のホームページの開設など、保有・利用しているすべての情報資産を正確に把握することは困難です。そのため、認識されている資産以外に、外部からの視点で自組織の資産として認識されているもの以外の資産がないかを検証することが、今度の安全なデジタル活用の促進には不可欠だと思います。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
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	ii-47	(3)③に「また、外部サービス利用時にはサービス事業者のセキュリティ体制を確認・定期確認を行うこと」を追加することを提案します。 iii-136の8業務委託と外部サービスの利用に詳細記載があるが、今後の外部サービス利用増加を予想しiiの項目でも明示的にするべきだと考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
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	ii-18	3.情報システム全体の強靭性の向上 (1)マイナンバー利用事務系 ①マイナンバー利用事務系と他の領域との分離 「マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（MACアドレス、IPアドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。」下線部の「プロトコル（ポート番号）」の削除を提案します。 MACアドレス、IPアドレス、ポート番号の詐称は現在では容易であり、アプリケーション単位でのアクセス制御が必要と考えます。本機能はすでに一般的であり、多くのセキュリティベンダーが提供可能です。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
40	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	(1)マイナンバー利用事務系に「③ガバメントクラウドにおけるセキュリティ対策」項目を追加を提案します。 文章案：③ガバメントクラウドにおけるセキュリティ対策（ア）CWPP、CSPMの導入　ガバメントクラウドにはワークロード保護とセキュリティ管理体制を整えること（イ）通信接続方式　ガバメントクラウドと接続には閉域通信もしくはLGWAN経由での通信を行いセキュリティ対策を行う。 ガバメントクラウドの利用時の注意事項の記載がないため、パブリッククラウドを利用する際の一般的なセキュリティ対策を施すことを促す必要があると考えます。	ガバメントクラウドの活用を前提とした地方公共団体の情報セキュリティ対策の在り方については今後検討してまいります。
41	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-21	3.情報システム全体の強靭化の項目に「④外部サービスの利用」を追加。 文章案：（4）外部サービス（ア）前述のインターネット接続系のセキュリティ対策を踏まえた上で、クラウド事業者の責任共有モデルを前提としたクラウドワークロード保護とクラウドセキュリティ管理体制を整え、パブリッククラウドのセキュリティ対策を実施すること。 パブリッククラウドを代表とする外部サービス利用時の注意事項の記載がないため、パブリッククラウドを利用する際の一般的なセキュリティ対策を施すことを促す必要があると考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
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	ii-28	「(2)IDの取扱い」について、以下の文章への修正を提案します。 ②原則、共有IDの利用は禁止とする。ただし、業務上止むを得ない場合に限り、その運用を認めるが、その場合は、過去に遡って共有IDの利用者が特定できるように記録・管理すること。 先日閣議決定された「デジタル社会の実現に向けた重点計画」でもゼロトラストアーキテクチャは重視されており、ゼロトラストを実現するにあたりID管理は非常に重要な要素の一つです。過去の経緯からIDの共用を認めざるを得ないことは理解できますが、原則を定義し、適切な環境を周知すべきと考えます。	御指摘を踏まえ、下線部のとおり記載を追加いたします。 5.人的セキュリティ 5.4ID及びパスワード等の管理【解説】 （2） IDの取扱い IDの利用は本人に限定することを規定する。 また、共用IDの利用は、業務上止むを得ない場合に限定する必要がある。その上で、止むを得ず共用IDを利用する場合には、過去に遡って共用IDの利用者を特定できるように記録・管理することが望ましい。
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	ii-29	「(6)ログの取得等」について、以下の文言追記を提案します。 (6)ログの取得・活用等 ③統括情報セキュリティ責任者及び…実施しなければならない。特にインターネット接続系においては、取得したログは常に活用され、事後対応だけでなく、事前対応に活用することで安全性の確保に努めなければならない。 インターネット接続系の利活用が今後増加する中で、ログを事後的にしか活用しないというのは問題があると感じます。 全てのセグメントではなく、特にインターネット接続系においてログの常時活用を明示することで、安全性を確保すると共に、ログ保管の重要性の認識を高めることにつながると考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。

No	提出者	該当資料	該当ページ又は該当監査項目 （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
44	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-38、39	6.4不正プログラム対策 (1)⑤、(2)②に共通して文言の修正を提案します。 不正プログラム対策ソフトウェアが常にその最新の情報を利用し挙動する状態に保たれなければならない。 「パターンファイルは、常に最新の状態に保つ」という表現は、振る舞い検知型などパターンファイルの更新が必要ない製品を意図せず排除すると考えられますので、表現を修正すべきであると考えます。	同様の趣旨の内容を記載済みのため、追記は不要と考えます。
45	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-48	(5)外部サービスを利用した情報システムの導入・構築時の対策 「(エ)設計・設定時の誤りの防止」を「(エ)設計・設定時の誤り検知とシステム的な防止」への変更を提案します。 クラウドサービスの浸透に伴い、作業者および利用者の人為的なミスにより、意図せず情報が公開され漏洩につながるケースが非常に多く発生しています。これを防止するには作業者および利用者が注意するなどの人的対策だけでは不十分であり、システム的に設定不備、脆弱性の検知と防止する手段の導入が不可欠と考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
46	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-48	(6)外部サービスを利用した情報システムの運用・保守時の対策 「(キ)設計・設定時の誤りの防止」を「(キ)設定変更・運用時の誤り検知とシステム的な防止」への変更を提案します。 No.45同様に、柔軟に利用方法の変更や機能追加されるクラウドサービスでは、常時監視をし安全な状態を維持し続けることが非常に重要と考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
47	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-36	(1)マイナンバー利用事務系の①のアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。下線部の「プロトコル（ポート番号）」の削除を提案します。 MACアドレス、IPアドレス、ポート番号の詐称は現在では容易であり、アプリケーション単位でのアクセス制御が必要と考えます。本機能はすでに一般的であり、多くのセキュリティベンダーが提供可能です。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
48	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	―	(3)（イ）「暗号通信の復号化（自治体情報セキュリティクラウドで提供していない場合）」の追記を提案します。 ファイアウォール、IPSなど高度なセキュリティ製品を導入しても暗号化された攻撃は発見・遮断をすることができません。あえて暗号通信の復号化という言葉を明示することにより自治体側で検討を促す必要があると考えてます。ⅲ-124の解説にも記載されていることも明示的にした方がいいと考える理由です。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
49	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-46	政府統一基準では、「8.2(2)外部サービスの選定」についてクラウドサービスとクラウドサービス以外に分けていましたが、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分けていただきたい。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
50	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-46～48	外部サービスの例に記載したサービスのうち、以下の項目について、遵守できない（情報開示されていない、設定ができない等）場合は、各自治体でサービスの利用可否を判断することになるのか。利用可否を判断するに当たっての一定の基準を教えていただきたい。 （２）外部サービスの選定 （３）外部サービスの利用に係る調達・契約 （５）外部サービスを利用した情報システムの導入・構築時の対策 （６）外部サービスを利用した情報システムの運用・保守時の対策	ご認識のとおりです。 また、地方公共団体が外部サービスを利用する際に参考となる情報を提供するよう努めてまいります。
51	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	マイナンバー利用事務系について、通信要件が緩和され、インターネットとの通信を許し、その条件が示された。LGWAN接続系についても通信要件が緩和され、クラウド等の直接インターネット上のサービスとの通信が許される条件を明示していただきたい。	今回の「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」の改定においても、マイナンバー利用事務系及びLGWAN接続系がインターネット環境とは分離・分割を行うという方針に変更はございません。
52	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	―	文書管理システムではマイナンバー利用事務系、LGWAN接続系、インターネット接続系で扱う様々な事業の意思決定を行うことから、自ずと他の層のデータを扱い、保存することが想定されます。このような例に限らず、三層の構えを踏まえ他の層のデータを扱わなければならないシステムの在り方や他の層からのデータの移動、他の層のデータを保存することについて記載が必要と考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。

No	提出者	該当資料	該当ページ又は該当監査項目 （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
53	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-87	＞「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- 89において、推奨的な記述があるのではあるが、義務化すべきであると思われるので述べておく。 地方公共団体が、正規に、その使用する電子メールサーバで、外部と送信及び受信を行う電子メールについては、当該正規の電子メールサーバにおいて、必ずTLSによる暗号化（SMTPoverTLS、STARTTLSの利用による）の利用を行うように（行えるように）されたい。 TLSによる暗号化は、一般的（ただし日本国内の電気通信事業者における電子メールでの利用可能化についてはかなり遅滞している（あまりに無責任で国民・国内事業者・行政の安全を重んじない総務省のせいで、であるが。）。）であるがそれなりに有用性があり、また特筆すべき特徴として、他の暗号化と併用が可能であるという利点がある。 TLSによる暗号化処理を地方公共団体が正規に管理する電子メールサーバで行う場合は、その内容について地方公共団体が確認出来るので問題ある暗号化された秘密のやり取りについての危険性は特に無く、単に望ましいだけであるので、これは（特に、電子メールの行政における利用が進められようとしている昨今においては）必ず行うべき事である。 それを行わずして、行政や各種事業者等が、サイバーセキュリティや個人情報保護等の評価で自らの評価を高く行っている場合などについては、ICT関係者ならずとも市民皆が、鳥滸がましさというよりもその虚偽性と不誠実さについて、当該組織に疑念を持たざるを得ないものになるのであるが、電気通信でやり取りがなされるコンテンツというのは、各所において危険に晒されるものであるので、電子メールについてのTLSでのその送信及び受信両方の保護については、ちゃんと行われるようにされたい。 電子メールについてのTLSでの保護については、今よりももっと強い、義務的な記述で行うようにされたい。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
54	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-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） 頁ii- 40中「（７）業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。」との記載部分） ・意見内容 当該部分について「（７）業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。（８）不正プログラム対策ソフトウェアはパターンファイルによる既知の不正プログラムに対する対策だけでなく、振る舞い検知にて未知の不正プログラムに対しても対策を講じなければならない。」との変更を提案します。 （理由） 同じガイドライン内である頁iii-113（注3）に「インターネットからの不正プログラム感染、侵入を防御するための方式として、パターンファイルでは未知の不正プログラムの検知が難しいことから、不正プログラムの挙動を検知する方式等によって既知及び未知の不正プログラムの検知並びにその実行を防止する機能を有するソフトウェアを導入することも有益である。」との記載があり、パターンファイルによる対策では既知の不正プログラムは対策可能であるが、未知の不正プログラムへの対策が難しい旨の言及があり、未知の不正プログラムの検知並びにその実行を防止する機能を有するソフトウェアを導入が有益である旨の記載がある為、関連する本項目に対してもその旨を明記し周知する必要があると考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
55	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-39	（「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） 頁ii- 40中「（５）不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。」との記載部分） ・意見内容 当該部分について「（５）不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。（６）不正プログラム対策ソフトウェアはパターンファイルによる既知の不正プログラムに対する対策だけでなく、振る舞い検知にて未知の不正プログラムに対しても対策を講じなければならない。」との変更を提案します。 （理由） 同じガイドライン内である頁iii-113（注3）に「インターネットからの不正プログラム感染、侵入を防御するための方式として、パターンファイルでは未知の不正プログラムの検知が難しいことから、不正プログラムの挙動を検知する方式等によって既知及び未知の不正プログラムの検知並びにその実行を防止する機能を有するソフトウェアを導入することも有益である。」との記載があり、パターンファイルによる対策では既知の不正プログラムは対策可能であるが、未知の不正プログラムへの対策が難しい旨の言及があり、未知の不正プログラムの検知並びにその実行を防止する機能を有するソフトウェアを導入が有益である旨の記載がある為、関連する本項目に対してもその旨を明記し周知する必要があると考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
56	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-40	（「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） 頁ii- 41中「（５）統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。」との記載部分） ・意見内容 当該部分について「（５）不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。（６）外部ネットワークからの異常な通信を検知し、不正侵入を検知及び防止しなければならない。」との変更を提案します。 （理由） 「6.5. 不正アクセス対策」に関連する当該部分において、不正アクセス対策として不正アクセスの検知方法に関して言及されておらず、外部ネットワークからの異常な通信をゲートウェイで検知及び防止する旨の広義の追加を行い、その必要性を周知することが必要と考えます。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。

No	提出者	該当資料	該当ページ又は該当監査項目 （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
57	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-41	（「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）頁ⅱ- 42中「また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、」との記載部分） ・意見内容 当該部分について「また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、内部侵入後の同一セグメント内での探索などの不正通信及びセグメント間の不正通信を監視する、侵入範囲の拡大の困難度を上げる、」との変更を提案します。 （理由） 昨今のサイバー攻撃では攻撃者が内部に侵入した後に、ラテラルムーブメントとよばれる同一セグメント内での攻撃の拡散がおこなわれるため「（７）標的型攻撃」の項においてそれを防止する具体的内容を明記し、周知する必要があります。併せて、同一システム内に複数のセグメントが存在する場合はセグメント間の不正通信を検知して対策する旨を明記する必要があります。 上記に関し、関連する『スマートシティセキュリティガイドライン（第2.0版）』(https://www.soumu.go.jp/main_content/000757799.pdf）において内部対策として下記の言及があります。 「外部からの通信に限らず、システム内の他セグメントからの通信や同一セグメント内の通信においても適切なアクセス制御の実装は必要である点に注意する。」 「ネットワークにおけるセキュリティ監視としては、インターネットとシステムの境界にIDS（不正侵入検知システム）やIPS（不正侵入防止システム）を設置し、それを監視することによって、不正なコマンドが含まれた通信等を検知、遮断することが可能となる。同一システム内に複数のセグメントが存在する場合は、セグメント間の通信においてもIDS/IPSによる監視が有効な場合がある。」	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
58	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-44	（「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）頁ⅲ- 47中「詳細な調査を実施することで、検知、復旧等の早期対処を可能とする。」との記載部分） ・意見内容 当該部分について「詳細な調査を実施することで、検知、復旧等の早期対処を可能とする。なお、従来モデル（αモデル）においても、LGWAN接続系から特定通信を利用したインターネット接続（外部サービスへの通信等）を行う場合は、βモデル、β’モデルと同様にインターネットからのリスクが増加することから未知の不正プログラム対策の導入及びマネージドサービスの運用を行う。」との変更を提案します。 （理由） αモデルにおいても特定通信としてインターネットに公開されたクラウドサービスに接続しておりβやβ’モデルと同様の対策が必要であるため、その旨を周知する必要があります。	「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」上、LGWAN接続系からインターネット上の外部サービスを利用する際には、自治体情報セキュリティクラウドを経由して接続することとしております。
59	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	（「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）頁ⅱ- 49表中「OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃時のソフトウェアの脆弱性を狙った攻撃に迅速に対応する。」との記載部分） ・意見内容 当該部分について「OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃時のソフトウェアの脆弱性を狙った攻撃に迅速に対応する。なお、管理（収集）されたOSやソフトウェアのバージョンに該当する脆弱性情報を、CVSSなどの一般的な脆弱性リスク基準（スコア）と自動的に照合・一覧表示し、リスクレベルに応じて適切に対応可能な仕組みを用意すること。」との変更を提案します。 （理由） 脆弱性管理として、管理されているバージョンと、脆弱性情報（リスク）との照合を人の手で実施していた場合、緊急度の高い脆弱性情報の発見やその対応にタイムラグが発生する可能性と、脆弱性の確認漏れが発生する可能性があるため、OSやソフトウェアのバージョン管理だけでなく、管理（収集）されたバージョンに該当する脆弱性情報をCVSSなどの一般的な脆弱性リスク基準（スコア）と自動的に照合・一覧表示し、リスクレベルに応じて適切に対応する仕組みが必ず必要であり、それを明示する必要があります。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
60	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-47	（「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）頁ⅲ- 50中「不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。なお、製品の導入だけでは未知の不正プログラムへの対策とはならない。」との記載部分） ・意見内容 当該部分について「不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。また、従来のセキュリティ対策ソフトと同様、偽装や隠蔽、セキュリティソフトの停止や削除などにより検出を回避するような攻撃者の挙動に対して、対策を行う必要がある。なお、製品の導入だけでは未知の不正プログラムへの対策とはならない。」との変更を提案します。 （理由） 昨今のサイバー攻撃は巧妙化されており、侵入後にアンチウィルス等のセキュリティ対策製品のエージェント（センサー）自体を停止する攻撃手法も増えています。さらに、ランサムウェアでも同様な攻撃手法で被害を拡大させる事例が確認されています。 このような攻撃に対して、既知の不正プログラム対策である従来型のパターンマッチングによるアンチウィルスソフトウェアは、カーネルモードで動作させることで、自らが排除されることを回避していますが、対象のセキュリティ対策製品がカーネル上で動作していない場合は停止・排除させられてしまい、エンドポイント対策が無意味となってしまいます。 そのため、当該「（注１１）未知の不正プログラムへの対策（エンドポイント対策）」の項において、偽装や隠蔽、セキュリティソフトの停止や削除などにより検出を回避するような攻撃者の挙動に対して、対策を行う必要性を明示し周知する必要があります。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。

No	提出者	該当資料	該当ページ又は該当監査項目 （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
61	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	（「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）頁iii- 51中「WSUSのファイル更新サーバ及びウイルス対策ソフトのパターンファイル更新サーバ等についても、マイナンバー利用事務系及びLGWAN接続系からのインターネット接続は認められない。」との記載部分） ・意見内容 当該部分について「WSUSのファイル更新サーバ及びウイルス対策ソフトのパターンファイル更新サーバ等についても、マイナンバー利用事務系及びLGWAN接続系からのインターネット接続は認められない。不正プログラム対策ソフトウェアとしてクラウドサービスを利用する場合は、LGWAN接続系及びマイナンバー利用事務系から、プロキシサーバ等を利用して、一部のサーバのみがクラウド上のセキュリティ対策ソフトウェア製品へ特定ポート通信をとる構成においてクラウドへ接続する。」との変更を提案します。 （理由） 同じガイドライン内である頁iii- 39に「マイナンバー利用事務系のサーバ、端末については、ウイルス対策ソフトを導入し、最新の定義ファイルを常時更新する。また、OSの修正プログラムについても最新の修正プログラムを常時更新する運用や対策を行わなければならない」との記載があり「ウイルス対策ソフトを導入し、最新の定義ファイルを常時更新」し「OSの修正プログラムについても最新の修正プログラムを常時更新する運用や対策を行」う旨の記載と整合性をとるためには、何らかの常時更新手段を明示し周知する必要があり、またLGWAN接続系、マイナンバー利用事務系のセグメントにおいてもランサムウェアのような情報漏えいが目的でないタイプのマルウェアについては、攻撃対象がインターネットに接続していることは必要なく内部に侵入した脅威の対策のために当該頁iii- 39記載の最新の脅威対策を適用するには、クラウド上から最新の脅威情報を取得する必要があるため、LGWAN接続系及びマイナンバー利用事務系から脅威及びその対策の情報を取得するための特定通信を明示する必要があります。その手段として特定ポート通信による接続を明示する必要があります。	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
62	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	（「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）頁iii- 51中「遠隔での情報システム保守により、マイナンバー利用事務系及びLGWAN接続系についてVPN接続による通信を許可する場合は、特定通信としての設定がされており、かつIP-VPN等の閉域網又はLGWANで接続されなければならない。」との記載部分） ・意見内容 当該部分について「遠隔での情報システム保守により、マイナンバー利用事務系及びLGWAN接続系についてVPN接続による通信を許可する場合は、特定通信としての設定がされており、かつIP-VPN等の閉域網又はLGWANで接続されなければならない。保守用の外部通信であっても、マイナンバー利用事務系及びLGWAN接続系と保守用ネットワークの分離を実施した上で、無害化通信により安全が確保された通信を実現すること。」との変更を提案します。 （理由） VPN接続は接続元と接続先の間の直接通信を許可してしまう仕組みであるため、遠隔での保守回線を閉域網で構成した場合であっても、最近の事例にあるように保守用端末を経由し、VPN装置の脆弱性などを利用して、外部から庁内アクセスが行われるリスクがあります。 そのリスクを回避するには直接接続を回避することが有効であり、保守用の外部通信であっても、マイナンバー利用事務系及びLGWAN接続系と保守用ネットワークの分離を実施した上で、無害化通信によって安全が確保された通信を実現する必要があることを周知する必要があります。 直近では以下の事例も発生しています。これは保守回線から侵入した可能性があるとされています。 https://xtech.nikkei.com/atcl/nxt/news/18/11561/	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。
63	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-110	（「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）頁iii- 113中「(注３)インターネットからの不正プログラム感染、侵入を防御するための方式として、パターンファイルでは未知の不正プログラムの検知が難しいことから、不正プログラムの挙動を検知する方式等によって既知及び未知の不正プログラムの検知並びにその実行を防止する機能を有するソフトウェアを導入することも有益である。」との記載部分） ・意見内容 当該部分について「(注３)インターネットからの不正プログラム感染、侵入を防御するための方式として、パターンファイルでは未知の不正プログラムの検知が難しいことから、 不正プログラムの挙動を検知する方式等によって既知及び未知の不正プログラムの検知並びにその実行を防止する機能を有するソフトウェアを導入することも有益である。当該ソフトウェアの導入とあわせて下記の対応に留意すること。 ・マルウェアに感染しないように、脆弱性・設定ミスを統制・可視化するようにして予防フェーズを徹底する。 ・既知ツールを使った既に判明済みの振る舞いを検知して自動的に排除する方策(NGAV (Next Generation Anti Virus) 等)を導入することで、職員によるインシデント対処数を低減させる。 ・端末の統制管理に、段階的な自動化の仕組みを導入して、利用者と管理者の負荷を下げる。 ・検知から最終的な対処までの間に、一時的な対処を自動的に行う仕組みを導入する。」との変更を提案します。 （理由） 未知の不正プログラムへの対策を定義するだけでは、膨大な数のインシデント対応に職員が忙殺され、真に緊急度が高いインシデントに対して正確で迅速な対処ができず、セキュリティ事故が発生する可能性が上がります。また、多くの不正プログラムはパターンマッチングでは排除できない既知のツールを使ったものが多く、攻撃手順などから脅威を個別に判別する必要があります。 その対応にはソフトウェアの導入だけではなく、緊急度が高いインシデントに対して正確で迅速な対処をするための職員の運用負荷低減が必要であり、そのための未知の不正プログラム対策（エンドポイント対策）に関する細目の例示が必要です。 （補足） 以下のURLは、侵入から数十分から数時間で情報漏えいまで至った事例です。いかに職員の運用負荷を減らし、緊急度の高いインシデントに集中するかが重要です。 https://news.mynavi.jp/article/20190822-881410/ https://www.fujitsu.com/downloads/JP/group/fri/businesstopics/cybersecurity/dl/trendreport201906.pdf https://ascii.jp/elem/000/001/816/1816709/	いただいた御意見は今後の施策の検討や実施に当たって、参考とさせていただきます。