

**「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7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7年3月6日（木）から3月12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、166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」等の資料については、令和7年3月28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	提出者分類	該当資料	改定案該当箇所*	ページ数 又はNo.	質問/ 意見 分類	内容(原文)	回答
1	不明	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	第3編第2章 機密性分類	iii-27 iii-31	意見	機密性について「自治体機密性」という名称は住民や事業者が混乱するので「機密性」という名称に戻すべきです。国の基準と分けると言う理由は、住民目線ではありません。 また、国の基準で「3A」などというバカげた区分もないにもかかわらず、自治体だけ「3A、3B、3C」を設けるのも、国目線であり、廃止すべきです。セキュリティレベルを統一するためのガイドラインで表記が揺れてはなんのためのガイドラインなのでしょう。 果たしてこれらの機密性の区別をつけることができるのでしょうか？いくら優秀な職員であっても瞬時に区別できる人は少ないでしょう。ましてや住民や事業者が相手に応じて判断できるとお考えでしょうか。 セキュリティは共通理解があって始めて有効に機能するものです。その根幹となる機密性の表記が異なるなど、今後のどのように住民事業者に理解を求めるのでしょうか。 前回の自治体機密性への名称変更と「3A、3B、3C」への再分類の改悪を今回速やかに見直していただくよう要望します。	昨年10月の第9回検討会において「中央省庁（政府統一基準）と同じ表記だけでは混乱が起こると考えている。そのため、例えば「自治体」を「機密性3情報」の頭あるいは間に付ける等で、ラベリングを区別しやすくすればよいのではないか。」という意見があったことを踏まえ、「自治体機密性」としています。また、国（政府統一基準群）の分類との関係は図表22に示しています。
2	不明	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	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靱性の向上 (2) LGWAN接続系（注7）	iii-44	意見	隔離の仕組みは常に進化する。マルウェア等の感染を拡大しないことが重要である点が重要である。ついては、セキュアブラウザの仕組みを考慮し、以下のように文言を変更していただきたい。 クライアントPCに設けられた隔離領域（コンテナ、仮想マシン等）で動作し、無害化されていないファイルのダウンロードや端末内のデータの漏洩が不可能なよう設計されたブラウザと、そのブラウザからに限りインターネットへのアクセス要求を受け付けるゲートウェイ（プロキシサーバを含む）との組み合わせで構成されたシステムであるセキュアブラウザも、アプリケーション仮想化の一種と考えることができる。 なお、許可する通信は、画面転送用のプロトコル又はゲートウェイ通信のプロトコルのみとし、その他の通信はす (※意見は上記で途切れている。)	いただいたご意見について、途中で途切れているため回答が困難です。また、ご指摘のセキュリティ対策の変化の動向等も踏まえ、ガイドラインの内容については今後も引き続き検討いたします。
3	不明	不明	不明	不明	その他	反対。改正反対	本ガイドラインの改定は「国・地方ネットワークの将来像及び実現シナリオに関する検討会報告書」（令和6年5月）や、地方公共団体からの、令和6年地方分権改革に関する提案を踏まえて検討を行っているものです。また、地方公共団体に対して事前に意見照会を行い、改定を要望する意見を踏まえ実施するものとなります。
4	不明	不明	不明	不明	その他	反対。こんな読みきれないもの、改正反対	本ガイドラインは、地方公共団体の情報セキュリティポリシー策定・改定の参考にさせていただくために示しているものであるところ、昨今、サイバー攻撃による政府や企業の内部システムからの情報窃取等が大きな問題となり、重大なサイバー攻撃が、日常的に行われている状況であることから、実施すべき対策が増加している状況です。このような背景がある中、ガイドラインの内容を大幅に減らしてしまうと「セキュリティ対策を緩めてもよい」という誤った受け止められ方をする恐れがあると考えております。 (No.3も参照)
5	不明	不明	不明	不明	その他	反対。広く広報して、国民の声を聴いてください	本ガイドラインは、直接の対象となる地方公共団体に対し、事前に意見照会を実施し意見を反映した後、任意で意見を募集しているものとなります。 (No.3、21も参照)
6	不明	不明	不明	不明	その他	改正反対	(No.3参照)
7	不明	不明	不明	不明	その他	改正反対	(No.3参照)
8	不明	不明	不明	不明	その他	改正反対。こんな長い反対	(No.4参照)
9	不明	不明	不明	不明	その他	改正反対	(No.3参照)
10	不明	不明	不明	不明	その他	反対	(No.5参照)
11	不明	不明	不明	不明	その他	改正反対	(No.3参照)
12	不明	不明	不明	不明	その他	改正反対	(No.3参照)
13	不明	不明	不明	不明	その他	改正反対	(No.3参照)
14	不明	不明	不明	不明	その他	改正反対	(No.3参照)
15	不明	不明	不明	不明	その他	改正反対。わかりやすく短く書いてください	(No.4参照)
16	不明	不明	不明	不明	その他	反対。これだけ長いものに、一つずつ答えるのは、同じようなページ数の長い入力フォームがいるのではないですか。それは無理です	500文字を超え、長文となる場合は、メールでの意見を受け付けております。
17	不明	不明	不明	不明	その他	反対。マイナンバー反対。	本ガイドラインとは関係のない御意見に見受けられます。
18	不明	不明	不明	不明	その他	反対	(No.5参照)
19	不明	不明	不明	不明	その他	改正反対	(No.3参照)
20	不明	不明	不明	不明	その他	反対	(No.5参照)

No	提出者分類	該当資料	改定案該当箇所*	ページ数 又はNo.	質問/ 意見 分類	内容(原文)	回答
21	不明	不明	不明	不明	その他	募集期間1週間ですか？間違いですか？ 意見求める為のパブリックコメントですが意見は求めている様に感じる。総務省さんそれで良いのですか？	本ガイドラインは、直接の対象となる地方公共団体に対し、事前に意見照会を実施し意見を反映した後に任意で意見を募集しているものになります。 また、本ガイドラインは地方自治法に基づく技術的助言で、法的拘束力を有しないものであり、行政手続法に基づく命令等に該当せず、同法第39条に基づく意見公募手続の対象外であるため、募集期間は前回同様とさせていただきます。 ※行政手続法 (定義) 第二条 この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。 八 命令等 内閣又は行政機関が定める次に掲げるものをいう。 イ 法律に基づく命令（処分の要件を定める告示を含む。次条第二項において単に「命令」という。）又は規則 ロ 審査基準（申請により求められた許認可等をするかどうかをその法令の定めに従って判断するために必要とされる基準をいう。以下同じ。） ハ 処分基準（不利益処分をするかどうか又はどのような不利益処分とするかについてその法令の定めに従って判断するために必要とされる基準をいう。以下同じ。） ニ 行政指導指針（同一の行政目的を実現するため一定の条件に該当する複数の者に対し行政指導をしようとするときにこれらの行政指導に共通してその内容となるべき事項をいう。以下同じ。） (意見公募手続) 第三十九条 命令等制定機関は、命令等を定めようとする場合には、当該命令等の案（命令等で定めようとする内容を示すものをいう。以下同じ。）及びこれに関連する資料をあらかじめ公示し、意見（情報を含む。以下同じ。）の提出先及び意見の提出のための期間（以下「意見提出期間」という。）を定めて広く一般の意見を求めなければならない。 2 (略) 3 第一項の規定により定める意見提出期間は、同項の公示の日から起算して三十日以上でなければならない。
22	不明	不明	不明	不明	その他	改正反対	(No.3参照)
23	不明	不明	不明	不明	その他	反対	(No.5参照)
24	不明	不明	不明	不明	その他	まずは募集期間を1ヶ月に訂正してください。	(No.21参照)
25	不明	不明	不明	不明	その他	改正反対	(No.3参照)
26	不明	不明	不明	不明	その他	改正反対	(No.3参照)
27	不明	不明	不明	不明	その他	「意見提出が30日未満の場合その理由」が白紙回答なのでやり直し！	(No.21参照)
28	不明	不明	不明	不明	その他	「意見提出が30日未満の場合その理由」が白紙回答なのでやり直し！	(No.21参照)
29	不明	不明	不明	不明	その他	提出期限30日未満は白紙回答なのでやり直し！	(No.21参照)
30	不明	不明	不明	不明	その他	提出期限30日未満は白紙回答なのでやり直し！	(No.21参照)
31	不明	不明	不明	不明	その他	説明案長すぎて読めずもっと簡素化してください	(No.4参照)
32	不明	不明	不明	不明	その他	提出期限30日未満でその理由が白紙なのでやり直し！	(No.21参照)
33	不明	不明	不明	不明	その他	改正反対	(No.3参照)
34	不明	不明	不明	不明	その他	改正反対	(No.3参照)
35	不明	不明	不明	不明	その他	反対	(No.5参照)
36	不明	不明	不明	不明	その他	改正反対	(No.3参照)
37	不明	不明	不明	不明	その他	反対	(No.5参照)
38	不明	不明	不明	不明	その他	改正反対	(No.3参照)
39	不明	不明	不明	不明	その他	内容云々の前にコメント募集期間短すぎ！ふざけるな！	(No.21参照)
40	不明	不明	不明	不明	その他	民間に委託するのではなく国や県で個人情報管理を管理して欲しい。民間に委託すると情報管理料金として、国民に負担が増えると思います。	民間事業者への業務委託は、専門的な知見を有する職員に限られていたり、そのような人材がいない場合に、民間事業者の知見や技術を活用し、情報システムの管理を安価にかつ安全に行うための方策の1つです。
41	不明	不明	不明	不明	その他	反対	(No.5参照)
42	不明	不明	不明	不明	その他	募集期間が短すぎる！そんなに急いで、何をたくらんでいるのか！	(No.21参照)
43	不明	不明	不明	不明	その他	募集期間が短すぎます。本案への不信感しかありません。改定をせず、改訂前ものを厳しくチェックしてください。	(No.21参照)
44	不明	不明	不明	不明	その他	コメントの募集期間が短すぎ。原則に反しています。そのおかげで、政府への不信感がさらに増しました。改定はもちろん反対。	(No.21参照)
45	不明	不明	不明	不明	その他	意見募集期間が30日未満です。それが7日となっている。しかも、正当な理由もありません。これは、パブコメとして無効ではないでしょうか？また、添付資料も難解の上、ページ数が多いため、嫌がらせとしか思えません。	(No.21参照)
46	不明	不明	不明	不明	その他	反対	(No.5参照)
47	不明	不明	不明	不明	その他	改正反対	(No.3参照)

No	提出者分類	該当資料	改定案該当箇所*	ページ数又はNo.	質問/意見分類	内容(原文)	回答
48	不明	不明	不明	不明	その他	任意の意見募集なら一般的な国民に直接影響のないものについてはこのように期間も短い中でやる意味がないのでは？ パブリックコメントに対して意義を成していないのでは？	いただいたご意見については、今後の施策の検討の参考とさせていただきます。
49	不明	不明	不明	不明	その他	反対	(No.5参照)
50	不明	不明	不明	不明	その他	改正反対	(No.3参照)
51	不明	不明	不明	不明	その他	改正反対	(No.3参照)
52	不明	不明	不明	不明	その他	改正反対	(No.3参照)
53	不明	不明	不明	不明	その他	改正反対	(No.3参照)
54	不明	不明	不明	不明	その他	反対	(No.5参照)
55	不明	不明	不明	不明	その他	改正反対	(No.3参照)
56	不明	不明	不明	不明	その他	提出期限30日未満でその理由が白紙なのでやり直し！	(No.21参照)
57	不明	不明	不明	不明	その他	反対	(No.5参照)
58	不明	不明	不明	不明	その他	反対	(No.5参照)
59	不明	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監査ガイドライン	不明	不明	意見	情報セキュリティ監査が文書確認のみで終わらず、実際の運用実態まで検証可能な監査手法を具体的に追加することを提案する。	運用実態については、ネットワークやシステムの設計書、システムの稼働記録や各種ログを確認することを規定しています。いただいたご意見につきましては、今後の検討の参考とさせていただきます。
60	不明	不明	不明	不明	意見	クラウドサービス利用時の自治体と提供事業者の責任範囲が曖昧である。特に海外データセンター利用時の法的リスクや情報の二次利用リスクへの具体的な対策基準を明記する必要がある。 情報セキュリティ監査が文書確認のみで終わらず、実際の運用実態まで検証可能な監査手法を具体的に追加することを提案する。	第1編「3.2. クラウドサービスの特性における留意事項」において、「機密性が高い情報は、国内のデータセンターに保存されることを確認する必要がある」ことを示しています。さらに政府機関等の対応に合わせ、第3編「8.3. 外部サービス（クラウドサービス）の利用（自治体機密性2以上の情報を取り扱う場合）」において、クラウドサービスの利用に当たっては、データセンターの存在地の国の法律の適用を受け、適正なかつ透明性のある手続(例：令状主義、透明性の確保、不利益処分に関する手続)に則らない形でクラウドサービス内の情報が外国の法執行機関の命令により強制的に開示されるといったリスクがあることを記載し、管轄裁判所について、国外の裁判所で裁判を行うこととならないよう、契約において日本国内の裁判所（必要に応じて地方公共団体の所在地を管轄する裁判所）を合意管轄裁判所として規定する必要があること等を規定しています。 (監査についてはNo.59参照)
61	不明	不明	不明	不明	その他	反対	(No.5参照)
62	不明	不明	不明	不明	意見	日本人の大切個人情報外国企業が請け負う事で、情報漏洩はしないのか。日本企業に管理をしてもらいたい。	地方公共団体における個人情報の取扱いについては、個人情報保護法令に基づき適切な措置が講じられるべきものと認識しております。 本ガイドラインにおいては、重要な情報資産を取り扱う業務を委託する場合について、第3編「8.1業務委託」において、個人情報漏えい防止のための技術的安全管理措置に関する取り決めや、業務上知りえた情報の守秘義務等を契約に盛り込むことを規定しています。
63	不明	不明	不明	不明	意見	情報は海外でも管理が可能なら海外で情報管理がされないか心配です。	(No.60、62参照)
64	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			意見	別紙1「情報セキュリティガイドライン」(P.300)には、次の改正を予定していることが記述されている。 要すれば、クラウドサービスを利用する場合の要件として、現行では、当該クラウドサービスの運用に使用されるデータセンターに適用される法令が、国内法であることを要件として規定しているところ、これを除外し、海外の法令のみが適用されるデータセンターを使用するクラウドサービスでも利用可能とするものである。 この改正は、日本人の個人情報、外国に搾取されることをも容認するものといえ、本件改正を断じて認めることはできない。 本件改正は、国民生活を脅かすものであり、国の安全保障の問題である。任意の募集とはいえ、このような重大な案件をわずか1週間の公募期間とするのは、国民に対する背信行為といえる。 まず、本案の廃止を求める。 加えて、30日以上の募集期間とすることを強く求める。	(意見募集期間についてはNo.21参照) (クラウドサービスについてはNo.60参照) ご指摘の「クラウドサービス利用時のデータセンターに適用される法令を国内法から除外し、海外法令のみが適用されるデータセンターの使用を認めること」旨の規定は存在せず、今回の改定においては、政府機関等における対応に合わせ、適正なかつ透明性のある手続(例：令状主義、透明性の確保、不利益処分に関する手続)に則らない形でクラウドサービス内の情報が外国の法執行機関の命令により強制的に開示されるといったリスクがあると判断される場合には留意が必要である旨を規定しています。
65	不明	不明	不明	不明	その他	反対	(No.5参照)
66	不明	不明	不明	不明	その他	民間企業へ管理をさせると、独占して同じ企業が請け負う事になり問題ではないか。県や市で管理が必要です。	本ガイドラインにおいて、同一の民間企業への業務委託を勧めるような方針を示しておりません。
67	不明	不明	不明	不明	その他	反対	(No.5参照)

No	提出者分類	該当資料	改定案該当箇所*	ページ数又はNo.	質問/意見分類	内容(原文)	回答
68	不明	不明	不明	不明	その他	改正反対	(No.3参照)
69	不明	不明	不明	不明	その他	改正反対	(No.3参照)
70	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			意見	<p>1. クラウド・バイ・デフォルト原則が謳われており、クラウドを利活用する事が前提とされているが、国や地方公共団体がそれを行う大前提として、クラウドサービス(以下、CSと略す)事業者、CS販売者、CS構築者、及びCS運用事業者等は、外国人もしくは外国籍ではないこと、さらにはその法人の株式保有者における外国人または外国籍企業の影響を受ける個人または法人である実態の割合が10%未満であるなどの歯止めは絶対に必要である。根拠として、先のウクライナ紛争では、ウクライナ側の戦費として制裁によって凍結されたロシアの資産が流用された事例をあげる。あり得ない行為が国家間の紛争という背景では起こりうるということを示したものとする。つまり、如何に契約によってそのCS事業者等を縛っていても、国家間紛争という事態においては全てが棚上げされ、外国に有利に活用されてしまうという事実を示したものである。情報セキュリティで守られるべき情報は外国の関与から遠ざけられているべきである。言わずもがなであるが、それら純国内企業が選別されるべきというのは、純国内企業は日本の法律によって縛られるからである。</p>	<p>ご指摘は「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」(2023年(令和5)年9月29日)において「政府情報システムは、クラウド・バイ・デフォルト原則、すなわち、クラウドサービスの利用を第一候補として、その検討を行うものとする。」と規定されている「クラウド・バイ・デフォルト原則」についてのものと認識しており、本ガイドラインの対象である地方公共団体のセキュリティについては、政府機関等に対応に沿った形で、必要な対策を示してまいります。</p>
71	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			意見	<p>2. 経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業についても1.と同様の外国からの関与の排斥が必要である。</p> <p>3. p199の(3)クラウドサービスの選定2 では、前2項の懸念が記載されていたにもかかわらず、修正により削除されている。具体的には、「クラウド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」の部分は復活させるべきである。「留意が必要」の文言では意味をなさない。</p>	<p>ご指摘の箇所については、政府機関等における対応と整合性を合わせる観点で、「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)」の記載をもとに修正したものであり、また、第1編「3.2. クラウドサービスの特性における留意事項」において「機密性が高い情報は、国内のデータセンターに保存されることを確認する必要がある」ことを示しています。</p>
72	不明	不明	不明	不明	その他	改正反対	(No.3参照)
73	不明	不明	不明	不明	その他	改正反対	(No.3参照)
74	不明	不明	不明	不明	その他	改正反対	(No.3参照)
75	不明	不明	不明	不明	その他	反対	(No.5参照)
76	不明	不明	不明	不明	その他	反対	(No.5参照)
77	不明	不明	不明	不明	その他	改正反対	(No.3参照)
78	不明	不明	不明	不明	その他	改正反対	(No.3参照)
79	不明	不明	不明	不明	その他	改正反対	(No.3参照)
80	不明	不明	不明	不明	その他	反対	(No.5参照)
81	不明	不明	不明	不明	その他	反対	(No.5参照)
82	不明	不明	不明	不明	その他	反対	(No.5参照)
83	不明	不明	不明	不明	その他	改正反対	(No.3参照)
84	不明	不明	不明	不明	その他	改正反対	(No.3参照)
85	不明	不明	不明	不明	その他	反対	(No.5参照)
86	不明	不明	不明	不明	その他	反対	(No.5参照)
87	不明	不明	不明	不明	その他	反対	(No.5参照)
88	不明	不明	不明	不明	その他	反対	(No.5参照)
89	不明	不明	不明	不明	その他	改正反対	(No.3参照)
90	不明	不明	不明	不明	その他	反対	(No.5参照)
91	不明	不明	不明	不明	その他	反対	(No.5参照)
92	不明	不明	不明	不明	その他	提出期限30日未満でその理由が白紙なのでやり直します。	(No.21参照)
93	不明	不明	不明	不明	その他	改正反対	(No.3参照)
94	不明	不明	不明	不明	その他	改正反対	(No.3参照)
95	不明	不明	不明	不明	その他	改正反対	(No.3参照)
96	不明	不明	不明	不明	その他	改正反対	(No.3参照)
97	不明	不明	不明	不明	その他	反対	(No.5参照)
98	不明	不明	不明	不明	その他	改正反対	(No.3参照)
99	不明	不明	不明	不明	その他	改正反対	(No.3参照)
100	不明	不明	不明	不明	その他	改正反対	(No.3参照)
101	不明	不明	不明	不明	その他	反対	(No.5参照)
102	不明	不明	不明	不明	その他	改正反対	(No.3参照)

No	提出者分類	該当資料	改定案該当箇所*	ページ数 又はNo.	質問/ 意見 分類	内容(原文)	回答
103	不明	(別紙) マイナンバー利用事務系に係る画面転送の方式について	不明	不明	意見	「別紙3. マイナンバー利用事務系に係る画面転送方式について」は、Daaまで含めて検討した結果、分量が多いわりに理解できる人は少数であると感じます。 思い切ってオンプレの番号利用事務系からLGWAN接続系へ画面転送で利用するパターン1つに絞ってはいかがでしょうか。 それで困るケースはわずかであると感じます。	画面転送の導入を希望する団体が、自団体のネットワーク構成や予算等に見合う方針を選択できるよう、様々な方式を想定しリスク分析を実施しているものになります。
104	不明	不明	不明	不明	その他	改正反対	(No.3参照)
105	不明	不明	不明	不明	その他	改正反対	(No.3参照)
106	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
107	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
108	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
109	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
110	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
111	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
112	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
113	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
114	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
115	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
116	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
117	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
118	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
119	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
120	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
121	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
122	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
123	不明	不明	不明	不明	その他	こんごは、もう少しAIでも使って万人でも分かりやすい言葉を選んで意見募集して下さい。それから、こそつと一週間で締め切るなんてやめて下さい。もう、それだけでバブコメ無効です。30日間の期間を取れない、特別な理由が明記されていないから。ざまあみろ！	(No.21参照)
124	不明	不明	不明	不明	その他	改正反対	(No.3参照)
125	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	第3編第2章 6.技術的セキュリティ 6.1コンピュータ及びネットワークの管理 (13) 無線LANのセキュリティ対策及びネットワークの盗聴対策	iii-102	意見	【意見】 「(13)無線LANのセキュリティ対策及びネットワークの盗聴対策」冒頭の「無線LANを利用する場合は、解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続を防御する必要がある。」を削除すべき。 【理由】 その後の「①LGWAN接続系」以降に書かれている内容が、冒頭の一文の範囲に収まっていません。例えば表中の「端末の設定」や「電波調整・設定」は端末の保護や可用性に関するものであり、認証やAPへの不正接続とは異なる観点のものです。このため冒頭の一文はそれ以降に書かれていることを簡潔に要約したものとなっていません。 また必要なのは「①LGWAN接続系」以降に全て書かれており、冒頭の一文は無くても何ら支障のない冗長なものです。 本書は極めて長大なものとなり読解を困難にしています。無駄に文字数を増やすだけのものを無闇に記載すべきではありません。	「(13)無線LANのセキュリティ対策及びネットワークの盗聴対策」は、各地方公共団体の情報セキュリティポリシー策定・改定の際、例文として直接的に参考にさせていただく【例文】の中の小見出しであり【例文】において具体的な対策として規定されている 「①統括情報セキュリティ責任者は、無線LANの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。」(＝無線LANのセキュリティ対策)と 「②統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。」(＝ネットワーク盗聴対策)の内容を合わせたものとなっております。なお、ご指摘の「①LGWAN接続系」の項目は、【解説】の部分であり、【例文】の(13)の項目について特にLGWAN接続系における対策を詳細に示したもので、すべて意味のある規定となっております。

No	提出者分類	該当資料	改定案該当箇所*	ページ数又はNo.	質問/意見分類	内容(原文)	回答
126	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	第3編第2章 6.技術的セキュリティ 6.1コンピュータ及びネットワークの管理 (13) 無線LANのセキュリティ対策及びネットワークの盗聴対策	iii-102	意見	【意見】 無線LAN利用時に行うべき各種対策について、「①LGWAN接続系」と「②マイナンバー利用事務系」の2つのみに限定して記載されているが、「インターネット接続系」についても記載すべき。 なおインターネット接続系において記載すべき内容はLGWAN接続系と同一と考えられるため、「①LGWAN接続系」を「①LGWAN接続系及びインターネット接続系」に改めるだけで良い。 【理由】 現行の記載ではインターネット接続系での無線LAN利用時に何も対策しなくて良いかのように見えてしまい、不適切な設計・運用を助長するため。	今回の改定の対象は、第14回検討会において示したとおり、マイナンバー利用事務系における無線LAN利用です。番号法上の整理等を踏まえ、今回、マイナンバー利用事務系における無線LAN利用の要件を新しく示すとともに、その前提の、過去に地方公共団体あての通知の参考資料で示しているLGWAN接続系における無線LAN利用の要件を、明示したものです。したがって、インターネット接続系における無線LANの利用を仮に規定するとすれば新たな論点となります。
127	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	第3編第2章 6.技術的セキュリティ 6.1コンピュータ及びネットワークの管理 (13) 無線LANのセキュリティ対策及びネットワークの盗聴対策	iii-103	意見	【意見】 図表42と図表43を1つの表にまとめるか、または図表43について「図表42の要件に加え以下のものも必要」とすることにより、図表42で記載済の内容を省いて同一内容の繰り返し部分を削除すべき。 【理由】 図表43の内容の約半分が図表42と重複して冗長となっていることにより、ページ数の不要な増加を招くとともに、読み手の負担を増やしています。本書は極めて長大なものとなっており読解を困難にしています。追加する内容は最小限に留めるべきであり、冗長性を最小限に抑えるべきです。	図表42と図表43は、異なるネットワークセグメントにおける対策を示したもので、同一の表にするとかえって混乱を生むと考えております。
128	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	第3編第2章 6.技術的セキュリティ 6.1コンピュータ及びネットワークの管理 (13) 無線LANのセキュリティ対策及びネットワークの盗聴対策	iii-103	意見	図表42の分類「認証方式」の「正規利用者(認められた利用者)のみが無線LANに接続されるよう認証サーバを利用したWPA2/WPA3エンタープライズによる認証(IEEE802.1X認証)を行う。具体的には、無線LANに接続時、LGWAN接続系端末をIEEE802.1xのクライアント証明書により認証(ユーザID・パスワードを使わない、EAP-TLS等の機器認証を行うことで、正規の端末からの接続であることを担保)し、アクセスを認可」の部分について、例えば以下のように改めるべき。 「WPA2/WPA3エンタープライズモードを利用する。具体的は、当該ネットワークの正規の端末のみに配付したIEEE802.1Xのクライアント証明書により認証(ユーザID・パスワードを使わない、EAP-TLS等の機器認証)し、接続を許可する。」 【理由】 原案には以下2点の問題があるため。 ・1文目と2文目の内容に大差なく、ほぼ同じことを繰り返し記載するだけとなっている。 ・「802.1X」と「802.1x」で表記が揺れている。	認証の方式について、表記を「IEEE802.1X」とした上で、簡略化した記載にします。「正規利用者(認められた利用者)のみが無線LANに接続されるよう認証サーバを利用する方式である」という記載については、地方公共団体に対策の趣旨を理解していただくため、残す形にします。
129	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	第3編第2章 6.技術的セキュリティ 6.1コンピュータ及びネットワークの管理 (13) 無線LANのセキュリティ対策及びネットワークの盗聴対策	iii-103	意見	【意見】 図表42の分類「無線端末同士の通信の防止」を削除すべき。 【理由】 その要件は互いに信頼できない利用者同士が同居する公衆無線LANにおいて必要なものです。しかし本表はそもそも正規の業務端末しか接続できない業務用無線LANに関する要件を規定するものであり、公衆無線LANではありません。本書は極めて長大なものとなっており読解を困難にしています。追加する内容は真に必要なものを最小限とすべきであり、必要のない要件を無闇に記載すべきではありません。 なお、もしそれが真に必要なことと考えられる場合は、無線に限らず有線でも同様であるため、無線LANの対策項目ではなく有線・無線共通の項目として別途記載すべきものとなります。いずれにせよ無線LANの要件を定める本表からは削除すべきです。	ご指摘の箇所は、過去に地方公共団体あての通知の参考資料で示している要件であり、また、現行のガイドラインの第3編「6.1コンピュータ及びネットワークの管理」(13)(注11)においても、「無線端末間の通信が行われないよう適切な設定を行わなければならない」旨がすでに規定されているため、今回新規の対策を求めるものではありません。 また、LGWAN接続系において無線端末間の通信の制限が不要であると結論付けるには、無線端末間の通信を制限しなくてもセキュリティリスクが高くないエビデンスが必要と考えております。
130	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	第3編第2章 6.技術的セキュリティ 6.1コンピュータ及びネットワークの管理 (13) 無線LANのセキュリティ対策及びネットワークの盗聴対策	iii-103	意見	【意見】 図表42の分類「端末の設定」の「(インターネットへの接続は画面転送での接続に限る)」を削除すべき。 【理由】 この記載の意図として「有線LANでは画面転送以外(例えばセキュアブラウザ方式)も使ってよいが、無線LANでは画面転送に限る(例えばセキュアブラウザ方式は禁止)」という意図の可能性と、「有線・無線を問わず画面転送に限る」という意図の可能性のどちらなのかを判断しかねるため、両方について述べます。仮に前者とした場合、有線と無線でインターネットアクセス手法を変える必然性を見いだせません。したがって、削除すべきと考えます。仮に後者とした場合、無線LANの利用とは無関係なため削除すべきと考えます(無線LANの項目ではなく各接続系の項目に記載すべき内容です)。	当該記載は、LGWAN接続系の端末から、インターネット接続系への接続を画面転送に限定するものであるため、正確な記載になるよう修正いたします。 なお、有線LANについては、第3編「6.5.不正アクセス対策」(4)に規定しております。
131	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	第3編第2章 6.技術的セキュリティ 6.1システム開発、導入、保守 (注11)	iii-139	意見	【意見】 「[lg.jp]を含むドメイン名」を「[lg.jp]ドメイン名」に改めるべき 【理由】 「[lg.jp]を含むドメイン名」では「foolg.jpbar.example.com」というドメイン名でも良いという意味になってしまいます。 iii-108の「[lg.jp]ドメイン名を使用する」とも整合が取れていません。	「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」における「政府ドメイン名」の説明に沿った形で、「.lg.jp」で終わるドメイン名という形で修正します。

No	提出者分類	該当資料	改定案該当箇所*	ページ数 又はNo.	質問/ 意見 分類	内容(原文)	回答
132	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	第3編第2章 3.情報システム全体の強靱性の向上 (1) マイナンバー利用事務系	ii -20 iii -46	意見	【意見】 ii -20、iii -35、iii -38、iv -19に「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」 iii -58、iii -59に「中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定」 とありますが、それぞれの接続先指定方法に「ドメイン名やFQDN」を追加すべきと考えます。あわせて「MACアドレス」は削除することが望ましいと考えます。 【理由】 通信先を限定する手段にMACアドレスは使えません。特に外部ネットワークとの通信においては、ドメイン名・FQDN・IPアドレスのいずれかで指定する必要がありますが、それに関する記載がありません。	ご指摘の箇所は、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の対策として、通信経路の限定を求める記載であり、接続先の限定だけでなくMACアドレスによる接続元の限定も必要であるため、現行の記載のままとさせていただきます。 ただ、ご指摘のとおりMACアドレスで接続先の限定はできないため、「MACアドレス等で通信先を限定する」と規定されている図表37及び39については修正いたします。 また、接続先の限定の方法につきましては、今後の検討の参考とさせていただきます。
133	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	第3編第2章 4.3通信回線及び通信回線装置の管理	ii -24 iii -72	意見	【意見】 「統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク(LGWAN)に集約するように努めなければならない。」について、「総合行政ネットワーク(LGWAN)」を「LGWAN接続系」にすべき。 【理由】 LGWANは団体の外部にあるものであり、集約しようがありません。「LGWAN接続系に」の誤記と思われます。	ご指摘の「総合行政ネットワーク(LGWAN)」は、LGWANに接続された情報システム及びその情報システムで取り扱うデータであるLGWAN接続系のことではなく、LGWANのネットワークを指すので、現行の記載のままとさせていただきます。
134	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	第3編第2章 5.4ID及びパスワード等の管理(3)パスワードの取扱い	ii -29 iii -90	意見	【意見】 「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。」の直前に「サーバ、端末環境を第三者が利用可能な状況にある場合は、」という前提条件を記載すべき。 【理由】 現在は、システム毎に異なる強いパスワードを作り、かわりにパスワードマネージャー等を用いて記憶させることがベストプラクティスとなっていると考えます。しかし現在の記載はそれに反したものとなっています。現在の記載は、弱いパスワードや使い回しを助長するものです。 また、スマートフォンのメールアプリ等、パスワードを端末に記憶させないこと自体ができず、実施不可能な場合もあります。 ただし、もし端末を第三者が利用できる状態にある場合には、パスワード保存機能はなりすましの要因となるため、その場合に限ってはこのポリシーは必要です。したがって、そのポリシーは残すものの、無条件にはなく必要条件を補記すべきと考えます。	パスワードが端末に記憶されており、当該端末の正規な利用者以外がパスワードの入力なしに端末が使用可能となる状態は、パスワードの入力による認証を経て端末が使用可能になる状態よりも、セキュリティリスクが大きいと考えられ、「サーバ、端末環境を第三者が利用可能な状況にある場合」に限定して良いかについては議論が必要と考えております。 また「弱いパスワードや使い回しを助長する」懸念について、パスワードは十分な長さとすることや、複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならないこと等を第3編「5.4. ID及びパスワード等の管理」で規定しております。
135	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	第3編第2章 2.情報資産の分類と管理(2)情報資産の管理(注8)	iii -33	意見	【意見】 「電子メール等により情報を送信する場合の暗号化に用いるパスワードについては、あらかじめ受信者と合意した文字列を用いるか、あるいは、電子メールで送信せずに電話などの別手段を用いて伝達することが望ましい。」について、「することが望ましい」を「しなければならない」に改めるべき。 また、これは共通鍵を前提とした記載になっていますが、より強度が高く安全な公開鍵暗号(PGPやS/MIME)も利用可能である旨を併記することが望ましいと考えます。 【理由】 現在の記載は、電子メールの添付ファイルのパスワードを電子メールで伝送するという非合理的慣習、いわゆる「PPAP」を助長するものであるため。	ご指摘のS/MIMEの利用については、電子メールのセキュリティ管理として、第3編「6.技術的セキュリティ 6.1コンピュータ及びネットワークの管理」(14)に規定しております。 いただいたご意見については、今後の検討の参考とさせていただきます。
136	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	第3編第2章 6.2アクセス制御(4)ログイン時の表示等	ii -37 iii -115	意見	【意見】 「(4) ログイン時の表示等」の内容は、「望ましい」や【推奨事項】とすべき。 【理由】 記載されているような機能を備えているパッケージシステムはかなり稀であり、守ることは非常に困難です。	ご指摘の箇所の趣旨は、「正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない」ようにすることであり、そのための対策が「等」の形で例示されているもので、言及されている対策の実装を必須とするものではありません。 また、当該部分の【解説】に、あくまでも「ソフトウェアに、ログイン試行回数の制限や、直近に使用された日時が表示される機能等がある場合」に限定し、「それらを有効に活用」するということを示しているため、この部分においても実装は必須でないことを規定しています。
137	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	第3編第2章 6.2アクセス制御(5)認証情報の管理	ii -38 iii -116	意見	【意見】 「統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。」について、「変更させなければならない」は「原則として」や「望ましい」といった一歩引いた表現に変更するとともに、以下のような例外条件を付け加えるべき。 「パスワードを変更させることが困難な場合は、初期パスワードを他者が推測できない十分な強度を持ったものとし、安全な伝達方法で職員等に知らせなければならない。」 【理由】 これは模範的ではあるものの、これを守るためには「あらゆる情報システムにパスワード変更機能を実装しなければならない」ということになり、守ることが極めて困難なケースがあります。	初期パスワード変更は、パスワードの管理の観点から従前より必要とされてきたものであり、現状の記載のままとさせていただきます。

No	提出者分類	該当資料	改定案該当箇所*	ページ数又はNo.	質問/意見分類	内容(原文)	回答
138	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	第3編第2章 3.情報システム全体の強靱性の向上 (3) インターネット接続系	iii -58 iii -59	意見	<p>【意見】 図表37及び38における「LGWAN接続系からインターネット接続系へのデータ転送（クリップボードのコピー＆ペースト等）は禁止」とについて、「LGWAN接続系とインターネット接続系間のデータ転送(テキスト形式以外のデータやファイルのコピー＆ペースト)は禁止」と改めるべき。</p> <p>【理由】 現在は以下2つの問題があるため。 ①コピー＆ペーストができない場合、URLやメールアドレス、パスワード等の記憶困難な文字列を1文字1文字転記することになり、著しい業務効率低下と事務処理ミスリスク向上というデメリットが発生する。 しかし万が一仮想デスクトップクライアント側が乗っ取られた場合、攻撃者はクリップボード利用可否に関わらず画面操作を介した PowerShell 実行等により任意のデータ転送が可能である。このように無差別なクリップボード禁止はマルウェアに対しては実効性が希薄であり、ただ正規のユーザーの業務効率を下げる効果しかない。 正規ユーザーによるコピー＆ペーストにより生じるリスクは、その操作によりファイルの送受信も可能となった場合に、別途定めているサンドボックスや無害化等を通らないファイル転送が行われてしまうことのみにあると思われるため、ここではテキストと非テキストを区別する必要がある。 ②現在は「LGWAN接続系からインターネット接続系へのデータ転送」についてしか禁じておらず、「インターネット接続系からLGWAN接続系へのデータ転送」は無制限となっている。これにより、インターネット接続系に存在し得るマルウェアをLGWAN接続系に持ち込んでしまうことを容認するものとなっている。</p>	<p>ご指摘の箇所は、βモデル、β'モデルの対策になり、リスク分析結果を踏まえ過年度に規定したものであり、修正するのであれば、過年度と同様定量的なリスクを評価する等、エビデンスが必要と考えております。 なお、「インターネット接続系からLGWAN接続系へのデータ転送」は無制限にはなっており、図表37及び39のとおり、無害化処理を規定しています。</p>
139	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	第3編第2章 3.情報システム全体の強靱性の向上 (4) その他セキュリティ	iii -62	意見	<p>【意見】 ③の「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(略)LGWAN-ASP等を利用して修正プログラム等を取得し適用することが望ましい。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。」について、最初の文の「利用してはならない」の前に「原則として」を追加し、最後の「WSUSの～認められない。」の一文は削除し、「LGWAN-ASPが存在しないアプリケーション等、インターネットからファイルを取得する手段しか存在しない場合は、専用の中継サーバを設け、その中継サーバのみがインターネットからファイルを取得するよう構成しなければならない。またその中継サーバは当該目的のサーバから取得したファイルのみを中継するよう構成しなければならない。」という内容を記載すべき。</p> <p>【理由】 現在の記載事項は、LGWAN-ASPIに配信サービスがないアプリケーション（例えばAdobe AcrobatやJUST Office等）についてはセキュリティパッチを適用せずに放置することを求めるものであり、マイナンバー利用事務系及びLGWAN接続系のセキュリティレベルを低下させる本末転倒な要件となっているため。</p>	<p>第3編「6.4 不正プログラム対策」に「ソフトウェアのパッチの適用等を確実に実施することが基本」と規定しており、第3編「7.1. 情報システムの監視」においても「インターネットとの境界にある機器におけるセキュリティパッチの適用は特に重要である」と規定しているため、「セキュリティパッチを適用せずに放置することを求めるもの」ではありません。 ご指摘の箇所である「マイナンバー利用事務系及びLGWAN接続系では（略）インターネットに接続して利用してはならない」という部分に関し、インターネットに接続していないシステムへのセキュリティパッチの適用については、第3編「6.4 不正プログラム対策」（2）に「電磁的記録媒体の使用は組織内で管理しているものに限るとともに、不正プログラム対策ソフトウェアを開発元等から定期的に取り寄せ、パターンファイルの更新やパッチの適用を確実に実施することが必要」と規定しています。 なお、LGWAN接続系については、αモデルの(ア)のパターンによりセキュリティパッチ適用が可能です。</p>
140	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	第3編第2章 6.技術的セキュリティ 6.1システム開発、導入、保守 (16) 電子署名・暗号化	iii -108	意見	<p>【意見】 「職員等が自由に暗号方法を利用すると～」の一文を意味の通る文に修正すべき。</p> <p>【理由】 「暗号方法」が意味不明なため、「暗号化アルゴリズムの選定」や「暗号の運用方法」等、本来の意図に則した用語の置き換えが必要と思われます。 また後続の「暗号鍵を紛失した場合に、復号が困難になり」という問題はその後「暗号方法は組織として特定の方法を定める」ことによって解決されないため、背景となる課題を整理する必要があると考えます。</p>	<p>「暗号方法」の意味については、ご指摘の「暗号方法は組織として特定の方法を定める必要がある。」の部分の後で、「その方法について情報システム管理者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された『電子政府推奨暗号リスト』を参照した上で、情報システム及び電子署名のアルゴリズム並びにそれを使用した安全なプロトコル及びその運用方法について、定めなければならない。」のように方法の詳細について説明がなされております。</p>
141	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	第3編第2章 3.情報システム全体の強靱性の向上 (1) マイナンバー利用事務系	iii - 37	意見	<p>【意見】 DaaSの場合は、管理系の通信がインターネットと接続することが想定される（例：ID認証の通信等）がマイナンバー利用事務系として閉域性をどのように確保することができるのかお示しいただきたい</p> <p>【理由】 DaaSについては、完全に閉域性が担保できないと考えられる。マイナンバー利用事務系においては、外部（インターネット）から閉域性を確保することが必須であることから、DaaSの安全性をどのように担保すべきかが非常に難しい。プライベートなIaaS基盤に仮想デスクトップ（VDI）を閉域ネットワーク上に構築することと、パブリッククラウド上のDaaSとは異なると考える。</p>	<p>DaaSの利用について規定しているのは、今回の意見募集の対象で、本ガイドラインの別紙である「別紙 マイナンバー利用事務系に係る画面転送の方式について（案）」であり、ここに規定しているDaaSを利用した画面転送の方式については、すべてリスク分析の結果を踏まえ規定したことになります。</p>
142	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	第3編第2章 3.情報システム全体の強靱性の向上 (2) LGWAN接続系	iii - 43	意見	<p>【意見】 「安全性が確保された通信の定義」をお示しいただきたい</p> <p>【理由】 「安全が確保された通信とは、同ページ（ア）から（ウ）までのすべてを実施されたものである」と考えられるが、一方で、（ウ）については、βモデル・β'モデルを考慮して、EDR（Endpoint Detection and Response）による目視確認と未知の不正プログラム検知及び防止が記載されているが、外部からの攻撃リスクを防ぐにあたり、EDRの種別がNGAVやAIによるシグネチャベースの製品をも含むのか検討が必要と考える（EPPでは未知の攻撃の検知や対応ができないため）</p>	<p>今回「必要な通信だけを許可できるようにする」を「安全が確保された通信を必要最低限許可」に修正した趣旨は、地方公共団体から、必要な通信という認識であればどのような通信を通して良いと誤解されてしまう懸念から、上記のとおり修正するよう意見があったためであり、具体的に安全を確保する方法は、（ア）から（ウ）に規定されている「分割」の実施となります。</p>

No	提出者分類	該当資料	改定案該当箇所*	ページ数又はNo.	質問/意見分類	内容(原文)	回答
143	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	第3編第2章 3.情報システム全体の強靱性の向上 (3) インターネット接続系	iii - 58 iii - 60	意見	<p>【意見】 EDRの製品は、EPPに機能を拡張した製品も出てきており、EDRの定義が曖昧となってきたため、どのような機能が必要とされるか記載をいただきたい ※IoCとIoAに対応した機能を有したものをEDRと定義</p> <p>【理由】 IoC (Indicators of Compromise) のみに対応したEDRでは、事後対応を目的としており、侵入が発生した後の痕跡を検出し、攻撃が成功した後に識別することとなるが、IoCと合わせて、IoA (Indicators of Attack) に対応しているEDRでは、事前予防を目的としており、侵入が発生し攻撃が進行中であることをリアルタイムに検出できるため、未知の攻撃や新たな脅威に対処することができる。EDRは、IoCとIoAの両方を活用しないと、未知の攻撃検知は不可能と考える。</p>	<p>未知の不正プログラム対策（エンドポイント対策）については、検討会や地方公共団体の意見を踏まえ、以下のとおり定義しております。</p> <p>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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。</p> <ul style="list-style-type: none"> ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策
144	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	第3編第2章 6.技術的セキュリティ 6.1コンピュータ及びネットワークの管理 (13) 無線LANのセキュリティ対策及びネットワークの盗聴対策	iii - 106	意見	<p>【意見】 本改訂より、「マイナンバー利用事務系に係る画面転送の方式」について追記されているが、画面転送方式でマイナンバー利用事務系のシステムやデータを取り扱うための、特定個人情報などを取り扱う区域の管理についても記載いただきたい。 LGWAN接続系端末から、画面転送方式によりマイナンバー利用事務系システムやデータを取り扱う場合については、LGWAN接続系端末の管理区域外持出も制限されると考えてよいか。</p> <p>【理由】 ゼロトラストアーキテクチャの実装では、一人一台端末で業務を行うことを前提として、テレワーク環境での業務が検討されることとなるが、画面転送方式でもゼロトラスト構成においても、特定個人情報を取る扱う事務取扱担当者が、管理区域外から情報を取り扱うことはあってはならないと考える。</p>	<p>特定個人情報等を取り扱う区域の管理については、番号法に基づく「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」（平成26年12月 18 日個人情報保護委員会）の、物理的安全管理措置の中で規定されています。 物理的安全管理措置の中で、以下のとおり規定されています。</p> <ul style="list-style-type: none"> ・ 事務取扱担当者等以外の者が特定個人情報等を容易に閲覧できないよう留意する必要がある。 ・ 取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。 <p>端末を取扱区域から持ち出した場合、事務取扱担当者等以外の者が住民の特定個人情報等を閲覧できる可能性や、盗難又は紛失等を防止する物理的な安全管理措置（施錠、セキュリティワイヤー等による固定）が区域外で徹底されないリスクが生じることや、組織的安全管理措置（取扱状況の把握及び安全管理措置の見直し）の実施のために、端末や関連機器等の取扱状況を客観的に評価することが困難になるため、端末の取扱区域外への持ち出しについては、現時点において庁内であっても原則禁止としています。</p> <p>ただ、このような特定個人情報を扱う政府機関等や個人情報保護委員会の施策の動向を踏まえ、今後検討する余地があると考えております。</p>
145	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	第3編第2章 6.5不正アクセス対策 (4) 内部からの攻撃	iii - 152	意見	<p>【意見】 「有線については、IP アドレスなどでフィルタリングを行い、端末間の通信を防止することが望ましい」とあるが、具体的な手法についてお示しいただきたい。</p> <p>【理由】 具体的にはNDR（Network Detection and Response）により、ネットワーク上のログを収集し、脅威を検知・検出・対応することも考えられるが、IPアドレスのフィルタリングではHUB（島HUB）で折り返す同一セグメントの通信を制御することは不可能と考える。</p>	<p>一例として、LANスイッチにおける、端末セグメントに割り振ったIPアドレスのネットワーク部を指定した通信制限が考えられます。</p>
146	不明	不明	不明	不明	意見	<p>意見募集期間が約 1 週間(3/6 9:00～3/12 17:00)と短いのはなぜですか？ 30日を切る場合は、特別な理由の明記が必要だと思いますが、パブコメ理由欄が空白で明示されていません。もう、これだけでこの案件は無効とを考えます。</p> <p>更に付け加えるが、難読でページ数の多いpdfファイルが添付されているがとても不親切。わざと煙に巻いているのではないかと推察してしまいます。AIでも使ってもらってわかりやすい言葉で、要点を絞った添付資料を希望いたします。意見提出は中高生の教材にも使用可能なようにもっと簡潔をお願いします。一般の企業であれば常識レベルが役所には通じないと言われる所以です。</p> <p>以上のことから、募集期間の見直しと説明文の改訂を求めます。</p>	(No.21参照)
147	不明	不明	不明	不明	その他	反対	(No.5参照)
148	不明	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-49 iii- 53 iii- 98 iii- 119 iii- 120	意見	マルウェアについては、不正プログラムと統一した方が良い。	いただいたご意見につきましては、今後の検討の参考とさせていただきます。
149	不明	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- 58 iii- 60	意見	脆弱性管理についてSBOMの作成について言及した方が良い。	SBOMの脆弱性管理への活用については政府機関等における対策の動向を踏まえ、今後、記載を検討します。

No	提出者分類	該当資料	改定案該当箇所*	ページ数又はNo.	質問/意見分類	内容(原文)	回答
150	不明	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- 103 iii- 105	意見	<p>・無線端末同士の通信の防止 無線端末同士の通信の制限は、ランサムウェアなどのリスクを考慮してであるかと思われるが、有線端末でも同様のリスクがあり無線端末のみ制限する理由の説明が必要ではないでしょうか。 また、プリンタなどの通信に際しても不都合が存在する可能性があり、一律で制限することには、ネットワーク設計や機器選定を含めて課題が多いのではないのでしょうか。 ・端末の設定 許可されたSSIDのみを表示することの要件はOSの仕様依存するものであり、許可されたSSIDのみ接続可能とすることで足りるのではないのでしょうか</p>	(端末間通信については、No.129参照) ご指摘の「許可されたSSIDのみを表示することの要件」について、端末の仕様やOSの種類によっては、SSIDの非表示設定ができないことがあり実効性がない場合もあることを鑑み、推奨としています。
151	不明	不明	不明	不明	その他	改正反対	(No.3参照)
152	法人	(別紙) マイナンバー利用事務系に係る画面転送の方式について	P38通信経路	38	意見	<p>・回線について マイナンバー利用事務系 DaaS からガバメントクラウド上の標準化対象業務にアクセスする際の通信も、画面転送の通信と同様にインターネット回線を経由する想定でしょうか？</p> <p>・経路について 上記の理解で合っている場合、マイナンバー利用事務系 DaaS をホストするCSPと標準化業務をホストするCSPとの間の通信はお認め頂いてもよいのでは考えます。 何故なら、マイナンバー利用事務系 DaaS からガバメントクラウド上の標準化対象業務にアクセスする際の通信は、異なるCPSを採用している場合もCSP間で通信する経路とする方が、庁内を経由する場合と比較して、経済面、安全面の両面で効果的と考えられるからです。</p> <p>異なるCPSを採用している場合であってもCSP間で通信をする方が、経路がシンプルで導入費用を大きく抑えられる可能性が高く、また、お示し頂いている追加のセキュリティ対策も容易であり、既存の庁内のセキュリティに影響を与えないことから、技術的にもより安全に接続が実現出来ると考えます。 一方で、マイナンバー利用事務系 DaaS から庁内を経由してガバメントクラウド上の標準化対象業務に辿り着くためには、庁外からマイナンバー利用事務系への経路の確立、マイナンバー利用事務系のIPアドレス体系の広報等が必要となります。 これらの点は現行のセキュリティポリシーとは大きく異なる為、各自治体においてセキュリティポリシーの見直しを図った上で、既存環境の大幅な変更が必要になることが想定されます。 え三層分離の環境への影響が極めて大きいと考えます。</p> <p>従いまして、異なるCPSを採用している場合もCSP間で通信する経路とする方が、庁内を経由する場合と比較して、経済面、安全面の両面で効果的であり、より迅速な自治体IT環境の発展が期待できると考えております。</p>	今回の画面転送のリスク分析では、リソースの問題から、すべてのパターンを想定し実施することは困難であるため、現行のガイドラインの規定や製品の動向を踏まえ、考えられるパターンについて分析を実施しているものです。 なお、当該団体が、ガイドラインや今回の別紙に規定していない構成をとっているということであれば、当該構成について団体として慎重かつ徹底したリスク分析を実施した上で、その結果を踏まえ必要な対策を検討し、自団体幹部にもリスク等を十分に説明し、了解を得て当該構成を実装することや、仮にインシデントが発生した際に住民に対して説明責任を果たせるように対応することが重要です。
153	不明	不明	不明	不明	意見	改正案は、アルファダッシュモデルの対策を実施することが前提としているので、アルファダッシュモデルが利用できない場合は、LGWAN接続系でも利用できないと思慮される。 アルファダッシュモデルのインターネット接続系のマイナンバー系接続を禁止する具体的根拠を示してください。	(No.152参照) 別紙 マイナンバー利用事務系に係る画面転送の方式について(案)に示している各種方式は、リスク分析の結果を踏まえて定義したものになります。LGWAN接続系からDaaSの方式を利用して画面転送を行う場合(通信経路(1)(2))は、αモデルの対策を行うことを前提としておりますが、通信経路(5)のように、LGWAN接続系からオンプレミスの画面転送(VDI)を利用するパターンも示しています。
154	不明	不明	不明	不明	その他	改正反対	(No.3参照)
155	不明	不明	不明	不明	その他	改正反対	(No.3参照)
156	不明	不明	不明	不明	その他	各市町村の情報管理方法にヒアリングはしたのですか。 外資に日本の個人情報を管理させるのでしょうか。 それとも、日本にある外資系企業に依頼するのですか。 日本の個人情報は日本にある日本企業に依頼をして欲しい。	(No.60、62参照)
157	個人	(別紙) マイナンバー利用事務系に係る画面転送の方式について	セキュアブラウザの技術的対策	90 97	意見	<p>【別紙3 マイナンバー利用事務系に係る画面転送の方式について(案)】 P90、P97にセキュアブラウザの技術的対策で画面転送機能と記載がございます。 セキュアブラウザには1.ゲートウェイやサーバーで隔離領域を展開して、その領域に展開されたコンテンツをクライアントに画面転送する方式と2.クライアントに隔離領域を展開して、その領域でブラウザを起動、コンテンツを表示する方式があると認識しております。</p> <p>対策の定義として端末とブラウザ実行環境の分離対策により、ブラウザ実行環境上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないとあります。対策の定義が満たせれば、方式は限定されない認識でよろしいでしょうか。</p>	セキュアブラウザについては、第3編「3.情報システム全体の強靱性の向上」(2)(注7)において「クライアントPCに設けられた隔離領域(コンテナ、仮想マシン等)で動作し、無害化されていないファイルのダウンロードや端末内のデータの漏洩が不可能なよう設計されたブラウザと、そのブラウザからに限りインターネットへのアクセス要求を受け付けるゲートウェイとの組み合わせで構成されたシステムであるセキュアブラウザ」と規定しております。
158	不明	(参考資料)「マイナンバー利用事務系に係る画面転送の方式」監査項目			意見	<p><対象> 別紙4_ (参考資料)「マイナンバー利用事務系に係る画面転送の方式」監査項目(案)</p> <p><コメント> 全パターン共通の監査項目のNo.3は削除漏れではないでしょうか。 監査項目の内容はNo.2と同一です。</p>	ご確認いただきありがとうございます。誤記のため、修正いたします。
159	不明	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監査ガイドライン			意見	<対象> 別紙2_情報セキュリティ監査に関するガイドライン(見え消し) <コメント> 目次の"3,14"は、"3.14."の誤りではないでしょうか。以下、引用です。3,14 マイナンバー利用事務系で無線LANを利用する場合の監査項目 ... 134	ご確認いただきありがとうございます。誤記のため、修正いたします。

No	提出者分類	該当資料	改定案該当箇所*	ページ数又はNo.	質問/意見分類	内容(原文)	回答
160	不明	(別紙)マイナンバー利用事務系に係る画面転送の方式について			意見	<p><対象> 別紙3_(別紙)マイナンバー利用事務系に係る画面転送の方式について(案)</p> <p><コメント> ページ番号が図表の後ろに隠れています。以下ページ番号です。 18,32,38,50,70</p>	ご確認いただきありがとうございます。図表の大きさ(見やすさ)を考慮しつつ、修正いたします。
161	不明	不明	不明	不明	意見	通常より募集期間が短すぎるのではないか。	(No.21参照)
162	不明	不明	不明	不明	意見	持ち出し端末のUSBを物理的に塞ぐとの案があるがナンセンスではないか。マウスも使えないのか。	ご指摘の部分については、政府機関等における対策に合わせて「第三者が端末に物理的にアクセスしやすく、情報が持ち出される可能性が高い環境下」という限定された条件の中で、「例えば、使用する端末のUSBポート等を物理的にロック(塞ぐ)して封印、システム設定で端末のUSBポート等を無効にするといった対策を施した持ち出し専用パソコンで業務を行うことが根本的な対策として考えられる」という形で、根本的な対策の例を示したものであり、マウスの使用禁止を規定しているものではありません。
163	不明	不明	不明	不明	意見	<p>総務省自治行政局住民制度課デジタル基盤推進室 各位</p> <p>パブコメ案件番号145210465の意見期間、他について質問させて下さい。</p> <p>案件番号145210465の意見期間についてお尋ねします。意見募集期間が約1週間(3/6 9:00から3/12 17:00)と短いのはなぜですか?30日を切る場合は、特別な理由の明記が必要だと思いますが、パブコメ理由欄が空白で明示されていません。もう、これだけでこの案件は無効と考えます。</p>	(No.21参照)
164	不明	不明	不明	不明	意見	<p>総務省自治行政局住民制度課デジタル基盤推進室 各位</p> <p>パブコメ案件番号145210465の意見期間、他について質問させて下さい。</p> <p>案件番号145210465の意見期間についてお尋ねします。意見募集期間が約1週間(3/6 9:00から3/12 17:00)と短いのはなぜですか?30日を切る場合は、特別な理由の明記が必要だと思いますが、パブコメ理由欄が空白で明示されていません。もう、これだけでこの案件は無効と考えます。</p> <p>更に付け加えるが、難読でページ数の多いpdfファイルが添付されているがとても不親切。わざと煙に巻いているのではないかと推察してしまいます。AIでも使いもつとわかりやすい言葉で、要点を絞った添付資料を希望いたします。意見提出は中高生の教材にも使用可能なようにもつと簡潔にお願いします。一般の企業であれば常識レベルが役所には通じないと言われる所以です。</p> <p>以上のことから、募集期間の見直しと説明文の改訂を求めます。</p>	(No.4、21参照)
165	不明	不明	不明	不明	意見	<p>総務省自治行政局住民制度課デジタル基盤推進室 各位</p> <p>パブコメ案件番号145210465の意見期間、他について質問させて下さい。</p> <p>案件番号145210465の意見期間についてお尋ねします。意見募集期間が約1週間(3/6 9:00から3/12 17:00)と短いのはなぜですか?30日を切る場合は、特別な理由の明記が必要だと思いますが、パブコメ理由欄が空白で明示されていません。もう、これだけでこの案件は無効と考えます。</p> <p>更に付け加えるが、難読でページ数の多いpdfファイルが添付されているがとても不親切。わざと煙に巻いているのではないかと推察してしまいます。AIでも使いもつとわかりやすい言葉で、要点を絞った添付資料を希望いたします。意見提出は中高生の教材にも使用可能なようにもつと簡潔にお願いします。一般の企業であれば常識レベルが役所には通じないと言われる所以です。</p> <p>以上のことから、募集期間の見直しと説明文の改訂を求めます。</p>	(No.4、21参照)
166	不明	不明	不明	不明	その他	改正反対	(No.3参照)

■パブリックコメント開始時からの修正箇所

項番	資料	該当ページ	修正内容
1	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 -103	<p>図表42 <修正前> 正規利用者(認められた利用者)のみが無線LANに接続されるよう認証サーバを利用したWPA2/WPA3エンタープライズによる認証(IEEE802.1X認証)を行う。具体的には、無線LANに接続時、LGWAN接続系端末をIEEE802.1xのクライアント証明書により認証(ユーザID・パスワードを使わない、EAP-TLS等の機器認証を行うことで、正規の端末からの接続であることを担保)し、アクセスを認可</p> <p><修正後> 正規利用者(認められた利用者)のみが無線LANに接続されるよう認証サーバを利用したWPA2/WPA3エンタープライズモードを利用する。具体的は、当該ネットワークの正規の端末のみに配付したIEEE802.1Xのクライアント証明書により認証(ユーザID・パスワードを使わない、EAP-TLS等の機器認証)し、接続を許可する。</p>
2	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 -103	<p>図表42 <修正前> (インターネットへの接続は画面転送での接続に限る)</p> <p><修正後> (インターネット接続系への接続は画面転送での接続に限る)</p>
3	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	<p>第3章 6.3. システム開発、導入、保守等【解説】(8)(注11) <修正前> 「lg.jp」を含むドメイン名の使用を調達仕様書に含める必要がある。</p> <p><修正後> 「.lg.jp」で終わるドメイン名(以下「『lg.jp』ドメイン」という。)の使用を調達仕様書に含める必要がある。</p>
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	iii -58 iii -60	<p>図表37及び39の「LGWAN接続系の画面転送」の「概要」欄 <修正前> (略) 通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。</p> <p><修正後> (略) 通信ポート、IPアドレス、MACアドレス等で通信経路を限定することで可能とする。</p>

■パブリックコメント開始時からの修正箇所

項番	資料	該当ページ	修正内容
5	(参考資料)「マイナンバー利用事務系に係る画面転送の方式」監査項目	5	No.3の項目削除
6	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	ii	目次 <修正前> 3,14 マイナンバー利用事務系で無線LAN を利用する場合の監査項目 <修正後> 3.14. マイナンバー利用事務系で無線LAN を利用する場合の監査項目
7	(別紙) マイナンバー利用事務系に係る画面転送の方式について	18 32 38 50 70	図表の大きさ（見やすさ）を考慮しつつ、修正する。