「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
1	ii -12	個人	1．組織体制 ②CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。【推奨事項】 【変更】 ②CISO は、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーまたは最高情報セキュリティアドバイザーチームを置き、その業務内容を定めるものとする。 【理由】 近年高度化、巧妙化するセキュリティ侵害や個人情報の漏洩等の発生における、CISOまたは統括情報セキュリティ責任者等が担う必要かつ十分な措置を行うための、それを補佐する専門家または複数の専門家によるチームでの、判断、対応等の対するアドバイスが必要である。また、情報セキュリティ関する統一的な窓口(CSIRT)に係る情報セキュリティインシデントの取りまとめ、報道機関への公表等、専門家または複数の専門家によるチームでのサポート対応は今後益々必要性が高まっていくことから意見申し上げます。	CSIRTについては、第2編 第2章「1. 組織体制」(9)に記載しております。 すべての地方公共団体に最高情報セキュリティアドバイザーを設置することは困難であることから、推奨事項とし、必要に応じて地方公共団体で判断頂く旨の記述としております。 ご指摘につきましては、今後の参考とさせていただきます。
2	ii -26 iii -63	不明	第2章対策基準の5.3情報セキュリティインシデントの報告について、「情報セキュリティに関する統一的な窓口」の文言が修正されていない。 CSIRTの位置付けを明確化し、セキュリティインシデントが発生した際、現場での即応性を担保すると見受けるが、地方公共団体の実務上、セキュリティインシデントが頻発している状況なのだろうか。また、災害時のBCPとの整合性を確保するようにしているが、組織名称が違うだけで、現場では同じ体制になるのではないか。文書等で組織体制が複雑化すると現場が混乱するのではないか。セキュリティインシデントに限らず、BCPや地方公共団体内が1つの組織体制で動けるように包括的な組織体制にしておく必要があるのではないか。	第2編 第2章「1. 組織体制」（解説）図表11に記載の通り、CSIRTの一部として「情報セキュリティに対する統一的な窓口」を定義しております。 BCPとの組織体制については、今後の参考とさせていただきます。
3	ii -37	法人	（原文） 6.4不正プログラム対策 （1）統括情報セキュリティ責任者の措置事項 （追記） ⑧万が一、「5.3セキュリティインシデントの報告」が適用される事象が生じた場合において5.3(3)を迅速に行うための環境構築を行わなければならない。 （理由） インシデントレスポンスが必要となった事象において、迅速な原因と状況の把握が求められます。 また、影響範囲を最小限にとどめることを考え、CIRT組織がしっかりと調査を行える 環境構築が統括情報セキュリティ責任者の処置として求められると考えます。	情報セキュリティインシデントへの対応体制（CSIRT）については、第2編 第2章「1. 組織体制」(9)にて、CISOの役割として記載しています。 また、CSIRTの活動は、第2編 第2章「5.3. 情報セキュリティインシデントの報告」(3)に記載しています。
4	ii -12	法人	（原文） 1．組織体制 ②CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。【推奨事項】 （変更） ②CISO は、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーまたは最高情報セキュリティアドバイザーチームを置き、その業務内容を定めるものとする。 （理由） 近年高度化、巧妙化するセキュリティ侵害や個人情報の漏洩等の発生における、CISOまたは統括情報セキュリティ責任者等が担う必要かつ十分な措置を行うための、それを補佐する専門家または複数の専門家によるチームでの、判断、対応等の対するアドバイスが必要である。 また、情報セキュリティ関する統一的な窓口(CSIRT)に係る情報セキュリティインシデントの取りまとめ、報道機関への公表等、専門家または複数の専門家によるチームでのサポート対応は今後益々必要性が高まっていくことから意見申し上げます。	CSIRTについては、第2編 第2章「1. 組織体制」(9)に記載しております。 すべての地方公共団体に最高情報セキュリティアドバイザーを設置することは地方公共団体の規模、人材面、財政面など考慮して推奨事項とし、必要に応じて地方公共団体で判断頂く旨の記述としております。 ご指摘につきましては、今後の参考とさせていただきます。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
5	iii-36	地方公共団体	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－②情報のアクセス及び持ち出しにおける対策 －(ア)情報のアクセス対策　図表16「SIM9カード」とは、何か明示されたい。	「SIMカード」の誤記のため修正いたします。
6	iii-42	地方公共団体	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－⑥VPN接続による外部との通信 「遠隔での情報システム保守等」の「等」とは、具体的に何を指すか明示されたい。	情報システム保守を指しております。 ご指摘箇所につきまして修正いたします。
7	ii-19	地方公共団体	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－②情報のアクセス及び持ち出しにおける対策－(ア)情報のアクセス対策 「業務毎」の「業務」とは、具体的にどのような単位（例：個人番号利用事務）を指すか明示されたい。	付録2自治体情報セキュリティ強化対策事業実施要領（その1）（自治体情報システム強靭性向上事業）参考1．自治体情報システムに係るサーバ・端末別の接続ネットワークに業務システム名の記載欄にて、住民情報、戸籍、税、生活保護、国民年金といった単位で業務名を記していますので、参考にしてください。
8	ii-19	地方公共団体	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－①LGWAN接続系とインターネット接続系の分割 「LGWANへの不適切なアクセス等の監視等」における二つの「等」は、具体的に何を想定したものか明示されたい。	「LGWANへの不適切なアクセス等」の例として不正な通信元からのアクセス、許可されていないプロトコルを使用したアクセス等があります。 監視等については情報セキュリティ対策の例として解説に記載しております。
9	iii-34	地方公共団体	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の分離 「特定通信を行う際は、以下の点に留意しなければならない」の後に列挙されている箇条書きは、いずれかを満たせばよいのか、いずれも満たす必要があるのか明記されたい。	箇条書きはいずれも満たす必要があります。
10	iii-35	地方公共団体	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の分離　（注2） 「LGWAN-ASP等」の「等」とは、具体的に何を指すか明示されたい。	例外として認められた特定通信等が挙げられます。
11	iii-38	地方公共団体	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－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 「次の手段」として列挙されている箇条書きは、いずれかを満たせばよいのか、いずれも満たす必要があるのか明記されたい。	箇条書きはいずれも満たす必要があります。
12	iii-39	地方公共団体	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　（注5） 「マルウェア感染がないことを前提に、ファイル無害化機器、ソフトウェア、サービス等を利用し、無害化されていることを確認しなければならない」と記載されているが、この文意が不明。 無害化を求めているのではなく、無害化されていることの確認を求めているのか。だとすれば、その趣旨や理由のほか、具体的な手段・手法を例示されたい。 またまた、そもそもマルウェア感染がない前提であれば、無害化する必要も無害化されていることを確認する必要もないのではないかと思われるので、再検討いただきたい。	「マルウェア感染がないように、ファイル無害化機器、ソフトウェア、サービス等を利用し、無害化されていることを確認しなければならない」と修正します。
13	iii-39	地方公共団体	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－①－(ウ) 本文が見出しの説明として不十分である。「高水準なセキュリティ運用監視」と記載されているが、何をもって「高水準」と判断し、どのような作業が「セキュリティ運用監視」に該当するのか具体的に例示されたい。	期待すべき高水準なセキュリティレベルは「セキュリティ人材あるいは、専用の装置により自動化された常時監視、分析、対処」です。
14	iii-40	地方公共団体	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－②　（注8） (c)でどのような「監視の観点」を述べようとしているのか理解できない。「監視の観点」として、「削除が求められる」とはどういう意味か。それは、監視の結果として得られる効果ではないのか。明記されたい。	「通信元を確認し、不正なファイル共有アプリケーションの削除を指示する。」と修正します。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
15	iii-41	地方公共団体	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マイナンバー利用事務系とLGWAN接続系における無線LANの利用 「電波を遮蔽しきれない」ことが、どのような過程を経て、「完全に（インターネットと）分離している状態とは言えない」とする結論に至るのかを明示されたい。明示に当たっては、アクセス制御が適切に設定されているという前提のもと、有線LANとの違いを踏まえられたい。	無線LANの場合は近年脆弱性が指摘されており、完全に分離している状態とはいえません。
16	iii-41	地方公共団体	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－④修正プログラム及びパターンファイルの更新 「LGWAN-ASP等を利用して～が望ましい」とされているが、LGWAN-ASPが安全であるという根拠を示されたい。	地方公共団体情報システム機構から「総合行政ネットワークASPガイドライン 第5.0 版（平成30年3月30日改訂）」としてLGWAN-ASPに関するガイドを提供していますのでそちらを参照ください。
17	iii-41	地方公共団体	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－④修正プログラム及びパターンファイルの更新 「基本的にLGWAN-ASP等を利用して～取得し適用することが望ましい」とあるが、「基本」以外の例外として、どのようなものを想定されているのか明示されたい。	「LGWAN-ASP等を利用して～」に修正いたします。
18	iii-41	地方公共団体	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－④修正プログラム及びパターンファイルの更新 「LGWAN-ASP等」の「等」とは、具体的に何を指すか明示されたい。	LGWAN-ASP利用を推奨しますが、インターネット専用端末からパッチをダウンロードし、ウイルスチェック後団体の責任のもとでLGWAN接続系側で更新しするといった場合が考えられます。
19	iii-41	地方公共団体	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－④修正プログラム及びパターンファイルの更新 LGWAN-ASPの一つとして、総務省が構築した「自治体情報セキュリティ向上プラットフォーム」が想定されるが、当該プラットフォームでは配信対象とされていない製品や、配信対象とされている製品であっても配信されない一部の更新ファイル、サポートされない方式（WSUSの高速インストール）等が存在する。修正プログラム等の適用を求める一方で、「インターネット接続は認められない」とするのであれば、これら当該プラットフォームでカバーしきれないものへの対応について、具体的に記述されたい。	LGWAN-ASPでのサービスでパッチ適用が難しい場合は、インターネット専用端末からパッチをダウンロードし、ウイルスチェック後団体の責任のもとでLGWAN接続系側で更新しするといった場合が考えられます。
20	iii-42	地方公共団体	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－⑦インターネット接続経由での各種業務システムの利用 「利用可能なネットワークをインターネット接続系に限定」とあるが、インターネット経由でインターネット接続系の機器に接続した後、仮想デスクトップによりLGWAN接続系のリソース（システム等）を利用することは差し支えないのか。差し支えないのであれば、記述をわかりやすく修正されたい。	情報セキュリティポリシーでは制限しておりませんが、地方公共団体にて実施することのリスクを検討し、適切な情報セキュリティ対策と運用ルールを策定した上での対応をお願い致します。
21	iii-42	地方公共団体	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－⑨インターネットメールによる障害通報 「特定サーバ間通信に限定し」とあるが、ここでいう「特定サーバ間」とは、何のサーバと何のサーバを指すのか、明記されたい。	該当の箇所については、具体的に何のサーバであるかを示しているのではなく、サーバ間で「特定通信」の方式を取ることを示しています。
22	iii-42	地方公共団体	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－⑨インターネットメールによる障害通報 「LGWAN-ASPを活用することが望ましい」とされているが、LGWAN-ASPが安全であるという根拠を示されたい。	地方公共団体情報システム機構（J-LIS）から「総合行政ネットワークASPガイドライン 第5.0 版（平成30年3月30日改訂）」としてLGWAN-ASPに関するガイドを提供していますのでそちらを参照ください。
23	ii -18 iii -32	個人	情報セキュリティ対策基準で追加された無害化通信について、実現方法の記述を削除若しくは見直ししていただきたい。理由は、既存の記述では、インターネットから受信した添付ファイル付きのメールについて、インターネット接続系で取り扱うことに誘導され、ネットワークを分離したにも関わらず、メールを起因とするインターネットとの不正通信が発生するリスクが低減されないためです。これは本来の目的であるインターネットからの脅威に対する業務環境の分離に逆行すると考えます。インターネットから受信したメールの添付ファイルをウイルスチェックやふるまい検知後に、LGWAN接続系の端末で操作したほうが、結果としてインターネットと不正通信するリスクはほぼ皆無となります。	「情報システム全体の強靭性の向上」において、インターネットとの接続には「LGWAN接続系」ではなく「インターネット接続系」を利用することが求められています。また、インターネット上のファイルをLGWAN接続系で使用する場合は、無害化を行うことが求められています。そのため、インターネット接続系とLGWAN接続系の通信は無害化通信とすることを求めています。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
24	iii-41	個人	「プリンタ・複合機は、必要に応じて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のネットワーク毎に設置されることが望ましい。共有する場合においてもマイナンバー利用事務系又は LGWAN接続系について、インターネット接続系と共有することは認められない。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、他の領域と分離された通信を 保証することが望ましい。それが困難である場合には、ネットワークの一方をLAN ポートに、もう一方はUSB ポートにプリンタサーバを繋ぐなどの方法を検討する必要がある。」とある。 上記から「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、他の領域と分離された通信を保証すればインターネット接続系とLGWAN接続系のプリンタを共有してもよい」と解釈してよいか。	インターネット接続系と共有することは認められないとの記述の通り、「インターネット接続系とLGWAN接続系のプリンタを共有」との解釈にはなりません。
25	iii-41	個人	”インターネット接続系を除き、無線LANの利用は避けることが望ましい。”とあるが、電子証明書の認証により強固なアクセス制御を実現できたり、高度な暗号化技術の採用により通信傍受を困難にさせたり、できるほか、端末同士での通信を制限する機能を利用することにより、不正プログラム感染時の拡大リスクを低下させることができるなど、むしろ有線LANよりもセキュリティを向上できる側面もあり、一概に避けることが望ましいとはいえないのではないか。	無線LANについては、電波の建物外への漏れを遮蔽しきれないなど、分離している状態とは言いきれないことから、インターネット接続系を除き、無線LANの利用は避けることが望ましいです。 ご指摘につきましては、今後の参考とさせていただきます。
26	ii-7 iii-10	法人	LGWANと接続する業務用システムとインターネット接続系の情報システムの通信ネットワークの物理的な分離に関する記述を削除することを求めます。これにより、本ガイドラインが、地方公共団体職員に対して、情報システムのセキュリティを確保するための最も効果的な方法はインターネットからの分離である、との誤解を生じさせてしまうことを防ぐことができます。 もし、この段階で物理的なネットワーク分離について言及する箇所を削除することが現実的ではない場合、少なくとも、情報システムがインターネットに接続されているか否かだけでリスクが決まるものではない旨明確に述べるよう、貴省に対し求めます。この点、基本方針5頁には、インターネットの接続の有無のみによって、情報システムの安全性を単純に判断するべきではなく、また、インターネットに接続されていることだけからクラウドサービスが危険だろうと思いこんではいけない、と記載されていますので、ご参照ください。私どもは、当該記載は理にかなった見解であると考え、これに同意します。	LGWAN接続系とインターネット接続系の分割とは、第3編 第2章「3. 情報システム全体の強靭性の向上」（解説）(2)に記載の通り、通信環境を分離したうえで、必要な通信のみを許可できるようにすることをいいます。 物理的なネットワーク分離のみを求めているわけではありません。
27	ii-31	法人	■ 行政機関におけるメールの添付ファイル使用全面禁止の提案 ページ ii-31 の (14)-⑥をはじめ各所に添付ファイルについての言及がありますが、昨今の標的型メールを例に出すまでもなく、情報漏えい事件や不正アクセス事故の多くがメールに添付されたファイルに端を発していることに着目する必要があります。なぜ、行政業務におけるメール利用で、ファイルを添付することを前提にする必要があるのでしょうか。メール添付を行わずとも情報の授受は行える筈ですから、セキュリティインシデントの根源となるメール添付ファイルの扱いは送受信の両方で全面禁止すべきと考えます。	ご指摘につきましては、今後の参考とさせていただきます。
28	iii-41	地方公共団体	第3編 第2章 3 （4） ③マイナンバー利用事務系とLGWAN接続系における無線LANの利用 無線LANは、災害に対する初動体制の確立や、働き方改革につながるフリーアドレス制度の導入に当たって、煩雑なネットワーク回線の敷設を最低限に抑えることができる点において非常に有用な技術である。また、接続の際に、端末やその利用者の認証を厳格に行うことで、有線での接続に準じたネットワーク分離を確保することができる。 したがって、「インターネット接続系を除き、無線LANの利用は避けることが望ましい」とあるのを、「無線LANを利用する場合には、端末やその利用者の厳格な認証などの措置をとらなければならない」とすべきである。	無線LANについては、電波の建物外への漏れを遮蔽しきれないなど、分離している状態とは言いきれないことから、インターネット接続系を除き、無線LANの利用は避けることが望ましいです。 ご指摘につきましては、今後の参考とさせていただきます。
29	iii-42	地方公共団体	第3編 第2章 3 （4） ⑥VPN接続による外部との通信 「IP－VPN等の閉域網」とあるが、これは「インターネットVPN」を含むのかが不明確である。 インターネットVPNでの接続が許容されていなければ、業務システムに重大な障害が発生した場合、特に地方部においては、保守を行う技術者が庁舎等から地理的に離れた場所に所在している為、迅速な対応ができない状況が懸念される。 したがって、「IP－VPN等の閉域網」とあるのを「IP－VPN、インターネットVPN等の閉域網」とされたい。	インターネットVPNも含みます。ただし、特定通信として適切に設定されており、閉域網であることが求められます。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
30	iii-42	地方公共団体	第3編 第2章 3（4） ⑦インターネット経由での各種業務システムの利用 列挙されている各項目は、全て実施することを必須とする趣旨か、あるいはいずれか一つまたは複数の項目を実施すれば可とする趣旨か、明確にされたい。 全て実施することを必須とするのであれば、 ①「仮想デスクトップ接続に限定」とあるが、同等のセキュリティを確保できるセキュアなブラウザの利用を許容されたい。 ②「利用可能なネットワークをインターネット接続系に限定」とあるが、多くの自治体ではLGWAN接続系のネットワークに業務システムを設置しており、テレワークの実施が事実上不可能になるため、この要件を削除されたい。	列挙している項目は対策の例示です。記載している項目のいずれかまたは複数の項目の実施を求めています。 また、本ガイドラインに記載の「テレワーク」は、インターネット接続系を対象とした記載です。
31	ii-19	法人	（原文） 1. LGWAN 接続系とインターネット接続系の分割 LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをLGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。 （原文に追記） なお、すべてのファイル形式に対して無害化が行えない現状を踏まえ端末側でふるまい検知等の次世代型の検知機能強化を行うことが望ましい。 （理由） 無害化処置がすべてのファイルに対応していない現状を踏まえ、感染リスクがゼロになったとは言い切れないと考えます。 そのため、端末上でのセキュリティ対策においてもふるまい検知などの次世代型のセキュリティ対策処置を講じる必要があると考えたため意見申し上げます。	LGWAN接続系にインターネットから取得したファイルを取り込む際には、インターネット接続系を経由することになります。 本ガイドライン第3編 第2章「3. 情報システム全体の強靭性の向上」【例文】(3)にて、インターネット接続系におけるふるまい検知について記載しています。
32	ii-18	地方公共団体	3.情報 システム全体の強靭性向上 端末が1台だけで完全に独立している場合（スタンドアロン端末）や、端末数台でのみ閉鎖的なネットワークを構成しているシステムの場合、実効性のある対策にも限界があると考えるが、どのように対策を講じるべきか、明確にしてほしい。	情報システム全体の強靭性向上の章につきましては、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に対する強靭化施策を受けての情報セキュリティ対策を記述しており、独自のスタンドアローン端末や閉鎖的なネットワークは本ガイドラインに準拠する情報セキュリティ対策を講じていただく必要があります。
33	ii-18	地方公共団体	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の分離 「他の領域」と「外部」のそれぞれの意味が例文中で明確に区別できるよう定義や補足を加えられたい（iii-33の(1)①から、「他の領域」は、LGWAN接続系及びインターネット接続系を指すものと思料）	「他の領域」は、LGWAN接続系及びインターネット接続系を指しています。
34	ii-18	地方公共団体	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の分離 「インターネット等」の「等」とは、具体的に何を指すか明示されたい。	インターネット以外の企業や団体等で設置されているネットワークを指しています。
35	ii-18	地方公共団体	2.情報資産の分離と管理 (2)情報資産の管理－⑦情報の送信 機密性2以上のものをメールで送信することは、危険性が高いことから、 ‘原則禁止とする。ただし、業務上やむを得ない場合には、情報セキュリティ管理者に許可を得た上で、暗号化及びパスワードを設定して送信しなければならない。’ としていただきたい。（都としても、今後、そのようにすべきかと検討中である。）	ご指摘につきましては、今後の参考とさせていただきます。
36	ii-19	地方公共団体	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 (ア)(イ)は、無害化通信の実現方法の例示という位置づけか。本文との関連性が明確になるよう修正されたい。	無害化通信の実現方法の例を示しております。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
37	ii -19	地方公共団体	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 本文中、「なおメールやデータをLGWAN接続系に取込む場合は、次の実現方法等により、無害化通信を図らなければならない」とあり、その際の無害化通信実現方法として、(ア)(イ)が例示されているものと思料するが、例示方法では「データ」をLGWAN接続系に持込むことにはならない。 本文と(ア)(イ)が対応するよう修正されたい。	データの取り込みについては、解説をしておりますので、そちらも併せてご確認ください。
38	ii -19	地方公共団体	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－①LGWAN接続系とインターネット接続系の分割 LGWANに接続できうる環境（LGWAN接続系）とインターネット接続系が分割されている環境下において、「LGWANへの不適切なアクセス等の監視等」を要する趣旨や理由、想定されるリスクを明示されたい。	地方公共団体内部からのLGWAN接続系への悪意を持った通信や、操作ミス等のリスクがあります。
39	ii -18	地方公共団体	3.情報 システム全体の強靭性向上 (1)マイナンバー利用事務系 マイナンバー利用事務系では、多要素認証の利用を義務付けている。この系に接続する端末において、当該端末にマイナンバーの表示機能や入出力機能がない場合においても、多要素認証は必須となるか、明確にしていただきたい。	多要素認証は必須です。
40	iii -33	地方公共団体	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の分離 「インターネット等」の「等」とは、具体的に何を指すか明示されたい。	インターネット以外の企業や団体等で設置されているネットワークを指しています。
41	iii -35	地方公共団体	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の分離 （注1） 「インターネット接続は認められないが、やむを得ずインターネットとデータをやりとりする場合は」とあるが、インターネット接続は「原則認められないが、例外はある」ということか。そうであれば、原則と例外があることがわかるよう明記されたい。	「原則認められないが、例外はある」との認識で構いません。
42	iii -38	地方公共団体	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－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 「限定を解除する」とは、どういう意味か。「持ち出し不可設定を解除する」という意味か、明記されたい。	「持ち出し不可設定を解除する」以外に、「電磁的記録媒体の利用を一時的に許可する」等が含まれます。
43	iii -38	地方公共団体	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－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 「管理者権限を持つ職員のみに許可する設定」の許可対象は何か。「管理者権限を持つ職員であれば持ち出しを許可する設定」という意味か、明確にしていただきたい。	「管理者権限を持つ職員であれば持ち出しを許可する設定」及び「電磁的記録媒体の利用を一時的に許可する」ことを含みます。
44	iii -38	地方公共団体	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 (ア)(イ)は、無害化通信の実現方法の例示という位置づけか。本文との関連性が明確になるよう修正されたい。	無害化通信の実現方法の例示です。
45	iii -38	地方公共団体	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 （注4） 「次の仕組み」として列挙されている箇条書きは、いずれかを満たせばよいのか、いずれも満たす必要があるのか明記されたい。	いずれかを満たす必要があります。
46	iii -39	地方公共団体	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－①－(ア) 「Webサーバ」とは、DMZ上で外部（インターネット）に公開しているものだけを指すのか。それとも、インターネット接続系の中で庁内向けに公開しているものも含むのか、明記されたい。	インターネット接続系に接続されているWebサーバすべてを指します。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所（ページ番号）	提出者	提出された意見	意見に対する考え方
47	iii－39	地方公共団体	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－①－(ア) 「LGWAN接続ファイアウォール」とは、「LGWAN接続ルータと対向する庁内ネットワーク側のファイアウォール」を指すのか。その意味を明確に定義されたい。	「LGWAN接続ルータと対向する庁内ネットワーク側のファイアウォール」を指します。
48	iii－40	地方公共団体	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－②　（注8） (c)で「ファイル交換ソフト」や「ファイル共有アプリケーション」を特に対象としている理由は何か。(a)、(b)、(d)の記載事項と比べると、粒度や現時点での脅威の度合いに差があると考えられる。その差をもってしても、記載しなければならない理由を示されたい。	読者に理解しやすいよう世間で話題となった例として示しております。
49	iii－40	地方公共団体	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－②　（注8） (c)で「ファイル交換ソフト」の例として、Winnyを挙げているが、世間を騒がせたのは10年以上前であり、いかにも古めかしい。適切に見直した上で記載されたものであれば、Winnyを例示された理由を示されたい。	読者に理解しやすいよう世間で話題となった例として示しております。
50	iii－41	地方公共団体	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－①プリンタ・複合機の情報セキュリティ対策 「マイナンバー利用事務系又はLGWAN接続系について、インターネット接続系と共有すること」は、例外なく認められないのか。だとすれば、「共有する場合には～」に該当するケースは、どういうものか。わかりやすく整理して記載されたい。	マイナンバー利用事務系とLGWAN接続系の共有のことを指しております。
51	iii－41	地方公共団体	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－②本庁・支所・出先機関間でのネットワーク通信 「相互の通信でインターネット回線を利用している場合」とあるが、「相互の通信」とは何か。本庁・支庁・出先機関間のことか、明示されたい。	本庁・支庁・出先機関間のことを指しております。
52	iii－41	地方公共団体	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マイナンバー利用事務系とLGWAN接続系における無線LANの利用 「電波を遮蔽しきれない等の理由で完全に分離している状態とは言えない」とあるが、ここでいう「分離」とはインターネットと当該系統（マイナンバー利用事務系又はLGWAN接続系）の分離のことか、明示されたい。	インターネットとの分離のことを指しております。
53	iii－41	地方公共団体	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－④修正プログラム及びパターンファイルの更新 前段（冒頭から「～望ましい」）は個々の機器による取得、後段（「WSUSの～」以下）は更新ファイルを配付する代表機器に関する記述という認識でよいか、提示いただきたい。	ご認識の通りです。
54	iii－42	地方公共団体	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－⑦インターネット接続経由での各種業務システムの利用 「以下のような情報セキュリティ対策を実施しなければならない」とあるが、他の箇所での記載と異なり「以下のような」とされていることから、あくまで例示という位置づけと考えてよいのか、明記されたい。	例示の位置づけです。
55	iii－42	地方公共団体	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－⑦インターネット接続経由での各種業務システムの利用 「以下のような情報セキュリティ対策」として列挙されている箇条書きは、いずれかを満たせばよいのか、いずれも満たす必要があるのか明記されたい。	あくまで例示であり、すべてを満たす必要があるわけではありませんが、対策の必要性を考慮していただき、必要な対策は実施していただく必要があります。
56	iii－42	地方公共団体	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－⑦インターネット接続経由での各種業務システムの利用 「データのダウンロード制限」とは、具体的に何をどう制限することを指すのか。また、ダウンロード元はインターネットに限らず制限するということか、明記されたい。	業務システムに含まれているデータのダウンロードを制限することを指しています。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
57	-	法人	1. 地方公共団体における情報セキュリティ確保の重要性は政府機関等における重要性と変わりないと考えます。 2. 平成30年6月7日付「政府機関等の対策基準策定のためのガイドライン（案）（平成30年度版）」6.2.2不正プログラム対策(p200)において、6.2.2(1)-1 下線部「既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること」とされ、同p201最終行からの記載に（例えば、シグネチャに依存せずに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、攻撃にスクリプト等と使用するファイルレスマルウェアの対策としても効果が期待できる。その他にも、サンドボックス、ふるまい検知等の技術があり、（中略）なお、不正プログラム対策ソフトウェア等の選定に当たっては、ソフトウェアの稼働によって端末及びサーバ装置への付加が増加し、業務に影響を与えるおそれがあること等も勘案したうえで判断する必要がある。）と記載されています。 3. 本「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（案）」には上記2と同趣旨の記載が見受けられません。サイバー攻撃への対策は官民一致して取り組むべき重要課題であり、本「ガイドライン案」においても、上記2と同様のご指導が考慮されるべきと考えます。	解説の参考として、不正プログラムの挙動を検知する方式について追記いたします。
58	iv－29、30	法人	参考5．自治体情報システム強靭性向上モデル 要件シートの一例 NISCから平成30年6月に意見の募集が行われた「サイバーセキュリティ戦略（案）」には ″エンドポイント（端末等）においてマルウェアの挙動を検知することにより、被害の未然防止及び拡大防止に取り組む。″と記載があり、「政府機関等の情報セキュリティ対策のための統一基準群」の改定（案）には″①情報システムの内部（端末等）での挙動の検知による未知の不正プログラムに係る被害の未然防止／拡大防止（中略）の対策の導入を推奨。″とあり、エンドポイントにおける挙動検知での未知の不正プログラム対策が重要なポイントとなっている。 しかし、今回のガイドラインにはインターネット接続系の端末については″未知のマルウェア等に即時対応できる仕組みの導入を推奨する。″とあるが、その実現手法としては″ウイルス対策ソフトを導入する″、″一般的なウィルス対策を実施すること。″という記述にとどまっており充分と言えない。 また、個人番号利用事務系、LGWAN接続系については上記のような記述すら見受けられず、未知マルウェア対策が不要という誤解を与える可能性がある。 そこで、インターネット接続系、個人番号利用事務系、LGWAN接続系、それぞれに対し、例えば「端末での挙動の検知による未知のマルウェアに係る被害の未然防止および拡大防止を行うこと」と記載をより具体化することで、手段や目的を明確化し、「サイバーセキュリティ戦略」との整合性を取ることもできると考える。 また、エンドポイント型セキュリティ対策は他の対策と比較すると高い費用対効果を実現できるとの研究成果もあり、費用対効果の面でもエンドポイント対策を推進すべきと考える。	解説の参考として、不正プログラムの挙動を検知する方式について追記いたします。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
59	ii－37 iii－90	法人	－該当箇所 6.4 不正プログラム対策 （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 －意見内容 NISCから平成30年6月に意見の募集が行われた「サイバーセキュリティ戦略（案）」には　"エンドポイント（端末等）においてマルウェアの挙動を検知することにより、被害の未然防止及び拡大防止に取り組む。"と記載がある。加えて「政府機関等の対策基準策定のためのガイドライン（案）」の基本対策事項には"情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。"とあり、また解説には"未知の不正プログラムの検知及び感染防止への対応として(中略)シグネチャにより検知する方式以外の手法を用いる製品やサービスを導入することの重要性も高まっている。"や、"例えば、シグネチャに依存せずに 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、攻撃にスクリプト等を使用するファイルレスマルウェアの対策としても効果が期待できる。その他にも、サンドボックス、ふるまい検知等の技術があり、必要に応じこれら複数の検知方式の組み合わせにより、不正プログラムの検知精度を向上させることで、端末及びサーバ装置に対する不正プログラム感染リスクの低減を図ることも可能となる。"という記載があり、エンドポイントにおけるパターンファイルに依存しない挙動検知での未知の不正プログラム対策が重要なポイントとなっている。 しかし、今回のガイドライン上での記載を見ると「不正プログラム対策ソフトウェア」はパターン型のアンチウイルスソフトのみを指しているように思われる。これでは未知の不正プログラムへの対応ができないため、充分と言えない。 そこで、統括情報セキュリティ責任者の措置事項、情報システム管理者の措置事項のそれぞれに対し、例えば「その所掌するサーバ及びパソコン等の端末に、挙動検知での未知の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。」と追記することで、端末のセキュリティを向上させることができる。 また、挙動検知型不正プログラム対策ソフトウェアは日々のパターンファイルの更新やそれに伴うフルチェック（スキャン）も不要となり、運用に負荷を与えずに標的型攻撃などを含む未知の脅威対策ができ、「サイバーセキュリティ戦略」との整合性を取ることもできると考える。 また、エンドポイント型セキュリティ対策は他の対策と比較すると高い費用対効果を実現できるとの研究成果もあり、費用対効果の面でもエンドポイント対策を推進すべきと考える。	解説の参考として、不正プログラムの挙動を検知する方式について追記いたします。
60	iv－35	法人	セキュリティ対策のツール例 "マルウェアのような異常な動作をするプログラムを検知するもの"として"振る舞い検知機器"という記載があるが、機器に限らずソフトウェアも存在し、また上述したように振る舞い検知ソフトウェアの有効性や重要性が増していることから、例えば「振る舞い検知ソフト」などの表現に改めるべきと考える。	ご指摘の箇所は「自治体情報セキュリティクラウド事業」の内容を付録としてそのまま記載しております。 振る舞い検知の機能をもつ機器やソフトウェア等については、第3編 第2章「3. 情報システム全体の強靭性の向上」【例文】(3)に機能という意味合いで記載しております。
61	iii－114	不明	外部委託事業者の選定にあたり、事業者の情報セキュリティ水準を評価する基準として情報処理安全確保支援士（RISS）の保有者数を加えるべきと考えます。 情報処理安全確保支援士（RISS）はサイバーセキュリティに関する唯一の国家資格であり、資格保有者には高度で最新の知識の担保と、守秘義務違反等に関しては刑事罰を含む厳しい罰則課せられることから同資格の保有者数は事業者選定の選定の際の基準になると考えます。	情報セキュリティに関する資格の保有について、第3編 第2章「8.1. 外部委託」（解説）(1)に『・外部委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供』を記載しております。情報処理安全確保支援士（RISS）もこの中に含まれております。 ご指摘につきましては、今後の参考とさせていただきます。
62	iii－114	不明	委託業者選定基準に、RISS保持者を担当者に含められるか、を入れるべき。	情報セキュリティに関する資格の保有について、第3編 第2章「8.1. 外部委託」（解説）(1)に『・外部委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供』を記載しております。情報処理安全確保支援士（RISS）もこの中に含まれております。 ご指摘につきましては、今後の参考とさせていただきます。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
63	-	個人	・この重要インフラ指針の「4.1.4.「支援」の観点、（2）人材育成及び意識啓発の項目において『重要インフラ事業者等の従業員が情報セキュリティ方針及びセキュリティ管理策の個別方針に基づく義務と責任を果たせるようにするため、従業員に対して、情報セキュリティに関連する十分な教育・トレーニングを実施する（必要に応じて委託先においても実施）。 特に、情報セキュリティ対策の推進役となるセキュリティ人材の育成においては、政府機関の人材育成プログラムやセキュリティベンダーが提供するトレーニング等の活用や、関係主体等と連携した演習・訓練への参加、「情報処理安全確保支援士」等の資格取得等も期待される。 これらの取組は人材育成の達成状況を客観的に評価・確認する際にも有効となる。』 との記述がある。 「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」においても人材育成の重要性を追記することを提案する。 ・また、国民に対してマイナンバーの普及活用に際し、安全・安心の確保に取り組んでいる状況を客観的に示すためにも、情報処理安全確保支援士制度の活用も併せて提案します。	人材育成について、第2編 第2章「5.2. 研修・訓練」に記載をしております。 ご指摘につきましては、今後の参考とさせていただきます。今後の参考とさせていただきます。
64	iii-114	個人	外部委託事業者の選定基準に、情報処理安全確保支援士が従事することを推奨してはどうでしょうか。 情報処理安全確保支援士は定期講習が義務付けられているため、情報セキュリティに対する最新の知識、技術力を兼ね備えております。 また、法的に秘密保持義務があり、違反した場合は資格者個人が刑事罰の対象となるため、無資格者より不正を働く可能性が低いと考えられます。	情報セキュリティに関する資格の保有について、第3編 第2章「8.1. 外部委託」（解説）（1）に『・外部委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供』を記載しております。情報処理安全確保支援士（RISS）もこの中に含まれております。 ご指摘につきましては、今後の参考とさせていただきます。
65	iii-116	法人	（注7）クラウドサービスの利用に関する考慮事項 インターネットを介してサービスを提供するクラウドサービスの利用に当たっては、クラウドサービス事業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、クラウドサービス事業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、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で強固な法の支配の仕組みがある管轄区域内に所在し、日本の法令に従った方法でデータを保存することを保証できるサービスプロバイダーが運用できるデータセンターを選択する必要がある。	専門家で構成される有識者検討会議の議論の結果を踏まえ、セキュリティポリシーガイドライン第3編 第2章「8.1. 外部委託」（解説）（注7）を一部修正いたします。
66	-	法人	また、「政府機関等の情報セキュリティ対策のための統一基準」（「統一基準」）は、平成30年版においてクラウドサービスの利用について更に改善されることはなかったものの、平成28年版の段階において、クラウドサービスの定義を行い、クラウドサービスについて独立の項目立てとするなど、クラウドサービスの利用を正面から捉えている点において、技術やサービスの動向に合致していると考えます。従って、本ガイドラインについても、クラウドサービス利用に関しては、統一基準と同等レベルに重要なものとして正面から捉えていただき、これにより両者のクラウドサービスの取り扱いに関する差異が解消されることを希望します。	ご指摘につきましては今後の参考とさせていただきます。
67	iii-116	法人	本ガイドラインにおいて、「クラウドサービス等の新しい技術の導入や新たな脅威の発生等の情報セキュリティに関する環境変化により、情報資産や情報資産に対するリスクに大きな変化が生じた」（i-24）との記載や、クラウドサービスの利用に関する考慮事項として「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」（iii-117）との記載があります。これらは、本ガイドラインを読んだ者に対して、クラウドサービスの方がリスクが高いことを前提としていると誤解を与えかねません。クラウドサービスは合意した役割を利用者と事業者が共有し、それぞれの責任を果たすことで（責任共有モデル）安全に利用することができます。例えば、オンプレミスのシステムであっても、災害等によるサーバー類の消失や突発的なアクセス増加によって生じる可用性・拡張性・データの耐久性に対するリスクはクラウドに比べて高いと言えます。本来、地方公共団体が情報システムを導入する場合、クラウドサービスかオンプレミスかといった単純な分類ではなく、情報の収集、取扱い、処理および保管に伴うリスクはアプリケーション、プロセスおよび関連するシステムのセキュリティ設計およびアーキテクチャによって異なることに鑑み、具体的な事実関係に基づき客観的に検討して決定すべきです。	専門家で構成される有識者検討会議の議論の結果を踏まえ、セキュリティポリシーガイドライン第3編 第2章「8.1. 外部委託」（解説）（注7）を一部修正いたします。
68	iii - 45	地方公共団体	③庁外への機器の設置について クラウド利用の場合もこの項目を遵守する必要はあるか。 サーバを庁外に設置する場合も、庁外に設置されたサーバを利用する場合も、状況は同じように思える。 我が部署では、文字通り解釈すべきか、意図から解釈すべきか、意見がわかれており、解説等でも明確にしていただきたい。	クラウドサービスの利用は、機器を設置しているわけではなく、サービスの利用となるため、本項目の対象外です。 ご指摘につきましては今後の参考とさせていただきます。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
69	iii-114 iii-116	法人	本ガイドライン中、外部委託の説明において、ISO/IEC 27001に対する言及がありますが(iii-114, 116)、ISO/IEC 27017やSOC報告書などに対する記載も追加して、国際的な認証や監査フレームワークへの対応について望ましいものであると積極的に言及し、地方公共団地に対してより客観的な判断材料を提供されることを提案します。 この点、政府機関等の情報セキュリティ対策のための統一基準群中の「政府機関等の対策基準策定のためのガイドライン」においては、「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、クラウド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すること」(129頁)が記載され、ISO/IEC 27017やSOC報告書の活用も例示されています（132頁）。また、基本方針においても、クラウドサービスの情報セキュリティ機能の実態を利用者が個別に詳細に調査することは困難であるため、パブリック・クラウドに関しては、第三者による認証や各クラウドサービスの提供している監査報告書を利用することが重要であり、ISO/IEC 27017等の認証取得やAICPA SOC2（日本公認会計士協会 IT7号）の監査フレームワークへの対応が推奨されています。本ガイドラインを修正する際、これらの国際的な認証等への言及が参考になるものと考えます	ご指摘につきましては、今後の参考とさせていただきます。
70	iii-116	法人	（注7）クラウドサービスの利用に関する考慮事項 中段に「クラウドサービスの利用に当たっては、契約の形態が従前の委託や請負と異なることが想定されることから、「地方公共団体におけるASP・SaaS導入活用ガイドライン」平成22年4月　総務省」を参照されたい。」との記載がありますが、クラウドサービスについては、非常に速いスピードでサービスの形態、提供内容、技術等々、進化している状況を鑑みると、2018 年（平成 30 年）6 月 7 日付で、各府省情報化統括責任者（CIO）連絡会議にて決定された「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等の最新の方針やガイドラインを参照するべきだと考えます。また、政府のクラウド方針に沿った形での地方公共団体におけるクラウド方針の早期の策定を期待します。	ご指摘につきましては、今後の参考とさせていただきます。
71	ii-44 iii-113	法人	【変更希望箇所】 8.外部サービスの利用 8.1.外部委託 （2）契約項目 ・外部委託事業者の責任者、委託内容、作業者、作業場所の特定 【希望内容】 「責任者」「作業者」の記載に対して、“ただし書き”又は“注釈”を記載お願いします。 【記載要望内容趣旨】 1. 請負契約において、作業者の氏名をあらかじめ外部委託先に提出させることができるのは、発注者の施設内に入場するなど施設の保安上の理由に限られる。 2. 請負契約において、外部委託先の作業者から発注者宛に「誓約書」を直接提出させことはできない。 3. 請負契約において、外部委託先の作業者に職務経歴書を求めたり、事前面談を行ったりしてはいけない。	ご指摘の箇所につきまして修正いたします。
72	-	個人	総務省は地方公共団体に対して自治体クラウドの導入を促しているが、自治体クラウドの対象システムにはマイナンバー利用事務系のシステムを含めることとなる。また、複数の地方公共団体による導入・運用が必要となる。このことについて述べている個所がないが、自治体クラウドの特徴を踏まえての記述が必要だと考える。	ご指摘につきましては、今後の参考とさせていただきます。
73	-	法人	特に最近、各府省情報化統括責任者（CIO）連絡会議で決定された「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（「基本方針」）が公表され、コスト削減や柔軟なリソースの増減等の観点から、クラウドサービスの採用をデフォルト（第一候補）として政府情報システムの検討を行う「クラウド・バイ・デフォルト原則」が打ち出されたことは意義ある進展であると考えます。この点、コスト削減や柔軟なリソースの増減等クラウドサービス利用によるメリットは、地方公共団体の情報システムの検討においても重要な考慮要素であると考えられるため、本ガイドラインにおいても同様に「クラウド・バイ・デフォルト原則」の方針を明示することに意義があると考えますので、そのような方針の追記を提案します。	ご指摘につきましては、今後の参考とさせていただきます。
74	-	法人	さらに、現在、官民データ活用推進基本法に基づき、各都道府県においては、「都道府県官民データ活用推進計画」を策定しているところです。今後、各地方公共団地において官民データの利用を促進していくためには、迅速に利用を開始し、柔軟にリソースを増減することができ、IaaS、PaaS、SaaSといった各レイヤーにおいて多様なサービスが提供されているクラウドサービスの利用を情報システムの第一候補として検討してすることが益々重要になっていくものと考えますので、当該視点も盛り込んでいただけるようお願いします。	ご指摘につきましては、今後の参考とさせていただきます。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
75	ii-7 iii-10	法人	本ガイドラインでは、情報セキュリティ対策として「通信経路の分割」に度々触れていますが（ii6, ii7, iii10）、基本方針5頁「コラム：クラウドサービスが危険だろうと思い込んではいけない」において「インターネットとの接続の有無のみによって、情報システムの安全性を単純に判断してはいけない。」「インターネットに接続されていることだけからクラウドサービスが危険だろうと思い込んではいけない。」と記載されるとおり、通信経路の分割を行うことが完全な情報セキュリティ対策というわけではありません。従って、そのような誤解を招かないよう、情報セキュリティ対策として責任共有モデルや多層防御の考えを示し、また、クラウドサービスが提供する情報セキュリティについても言及し、地方公共団体が最新の情報セキュリティ対策を取ることができるように修正すべきと考えます。	ご指摘につきましては、今後の参考とさせていただきます。
76	ii -44	法人	情報セキュリティ基本方針の例示として、8.1外部委託において「クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。」(ii-43)と記載しつつも、8.2約款による外部サービスの利用において、「機密性2以上の情報が取り扱われないように規定しなければならない」と記載しています（ii-44）。クラウドサービス等の外部サービスを利用する場合には、機密性に応じたセキュリティレベルを地方公共団体が検討すれば足りるものであり、前記のとおり情報システムによる情報の収集、取扱い、処理および保管に伴うリスクは、アプリケーション、プロセスおよび関連するシステムのセキュリティ設計およびアーキテクチャによって異なるものであり、その検討を客観的に行うべきであることから、一律に機密性2以上の情報を取り扱われないようにすべきとの規定は不要であると考えます。	ご指摘につきましては、今後の参考とさせていただきます。
77	ii -44	法人	（原文） ③情報セキュリティ管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。 （変更） 2. 情報セキュリティ管理者は、クラウドサービスを利用する場合は情報の機密性に応じてサービスを評価し利用の可否を検討すること。3. データ保護に関する責任を共有していることを理解し、自組織にて行うべき対策についても併せて検討すること。 （理由） クラウドサービスの利用は単純な外部委託とは異なります。自社の職員のパスワード運用の不備等による不正アクセス等が生じた場合は、クラウド事業者側に責任を求めることができません。そういった特性をよく理解し、不正アクセスへの検知対策やデータ保護に関する暗号化などの処置を講じる必要があると考えます。	ご指摘の趣旨は、本ガイドライン第3編 第2章「8.1. 外部委託」【例文】(2)及び(解説)(2)に記載していると考えます。 ご指摘につきましては、今後の参考とさせていただきます。
78	-	地方公共団体	パブリッククラウドサービスを利用することが当たり前になりつつある現状から、例外申請としてではなく、クラウドサービスを前提とした基準項目を追加すべき。	ご指摘につきましては、今後の参考とさせていただきます。
79	iii-88	地方公共団体	政府の基準として、‘インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じること’と示されていることからも、いずれかに明記すべき。	専門家で構成される有識者検討会議の議論の結果を踏まえ、ガイドライン第3編 第2章「6.3システム開発、導入、保守等」(解説)(注11)を修正いたします。
80	iii-37 図表 18 情報システムが正規の利用者かどうかを判断する認証手段」	法人	上記表内の「「知識」を利用する手段」の例として「パターン」の追加を提案いたします。「パターン」による認証が「知識」認証要素に含まれることは「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」の6.1.1(p157)においても言及されております。 「パターン」認証の具体例としては、Android端末における起動時の認証や、富士通社のネットワークサービスの認証オプションに採用されている認証 (http://www.fujitsu.com/jp/services/infrastructure/network/mobile/universal-connect/service/option/pattern-attestation/)が挙げられます。	ご指摘につきましては今後の参考にさせていただきます。
81	iii-36 図表17 認証の種類と手段	不明	iii-36 図表15 認証の種類と手段 「知識」と「所持」を併用する認証手段の具体例として「SIM9カ ード（携帯電話／スマートフォンの固有番号）とパスワードの併用」が挙げられておりますが、これがWebサービスへの二段階認証ログインのためのSMS認証あるいはTOTPアプリ等とパスワードの併用を指すのか、または携帯電話回線の不正利用を防止するためのSIMカードとPINコードを指すのか、明らかではありません。	ご指摘箇所の記述は、Webサービスへの二段階認証についての例として記載しています。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
82	iii-37 図表 18 情報システムが正規の利用者かどうかを判断する認証手段」	不明	SIMカードの換言説明として「携帯電話／スマートフォンの固有番号」との記述が2ヶ所ありますが、これが一体何を指すのか明らかではありません。SIMカードに記録されているのは契約者の固有番号であるIMSI、契約者の電話番号であるMSISDN、SIMカードの固有番号であるICCIDなどであり、一般に「携帯電話／スマートフォンの固有番号」であるIMEIとは性質を異にするものです。	ご指摘箇所の記述は、Webサービスへの二段階認証についての例として記載しています。
83	ii -35	個人	（2）3 「本人確認を行う方法」とありますが、「多要素認証等」の文言としたほうが良いかと思います。	ご指摘につきましては、今後の参考とさせていただきます。
84	ii -33 iii-78	個人	1.パスワードの定期変更について 前回公表した平成27年度のポリシーの「情報セキュリティ対策基準（例文）」部分から、5.4　ID及びパスワード等の管理（3）パスワードの取扱いの部分で「定期的な変更」を除かれたとお見受けします。 こちらは、昨今の常識にもなりつつあるため理解できます。 一方で、6.2　アクセス制御　③特権を付与されたIDの管理等の項では「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」となっております。 この「定期変更」が特権IDだけに残っているのはどういったお考えでしょうか。 定期変更＝セキュリティ機能を強化　であるならば、前述の5.4　ID及びパスワード等の管理にも残すべきかと思います。 ただ、前者のパスワードの定期変更はパターン化を引き起こし、パスワード強度が下がるため不要となったと認識しております。 この齟齬についてはどちらかにそろえるべきと考えますが、いかがでしょうか。	特権IDのパスワードについては、一般ユーザのパスワードとは取り扱いが異なり、定期的に変更するべきものと位置付けております。
85	ii -27、28	地方公共団体	共有IDに対するパスワードの取扱いについて 5.人的セキュリティ　5.4. ID及びパスワード等の管理（2）IDの取扱いにおいては、「②共有IDを利用する場合は共有IDの利用者以外に利用させてはならない。」と規定されていますが、（3）パスワードの取扱いにおいては、「⑧職員等間でパスワードを共有してはならない。」と規定されています。 この場合、共有IDとパスワードの取扱いに矛盾があります。ついては「⑧職員等間でパスワードを共有してはならない。」に「ただし共有IDは除く。」の追記が必要と考えます。	ご指摘の箇所につきまして修正いたします。
86	ii -28	地方公共団体	⑦パスワードの記憶について 「ID 及びパスワード等の管理」で、「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。」とあるが、端末に限った話ではない（サーバも同様）。	ご指摘の箇所につきまして修正いたします。
87	ii -33 iii-78	地方公共団体	⑫パスワードの定期的変更について 今回の改正により、パスワードの定期的変更の項目が削除されたが、「特権を付与されたIDの管理等」の項目において、「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。」とあるが、修正漏れではないか。	特権IDのパスワードについては、一般ユーザのパスワードとは取り扱いが異なり、定期的に変更するべきものと位置付けております。
88	ii -34	地方公共団体	6.技術的セキュリティ 6.2.アクセス制御 （5)認証情報の管理－② ‘ログイン後、直ちに’ではなく、‘初回ログイン後、直ちに’と明確にしていただきたい。	ご指摘の箇所につきまして修正いたします。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所（ページ番号）	提出者	提出された意見	意見に対する考え方
89	iii-80	地方公共団体	⑨パスワードの使いまわしについて1 平成29年3月、政府において、パスワードの流出が報道されたが、これは、業務システムで使用しているパスワードを、インターネット上のWebサービスでも使っていたものが流出したものであった。 これを受けて、NISCから各省庁にセキュリティにかかる注意喚起があり、それを受けて総務省（J-LIS）から都道府県にセキュリティポリシーの状況について確認の依頼があった。 それによると、ガイドラインの「パスワードは、他者に知られないように管理しなければならない。」が該当するとのことであったが、これをもって禁止の根拠とするのは、ちょっと弱い気がする。 「認証情報の管理」の解説には、「パスワードの使いまわしを行ってはならない」と書かれているが、別に以下の内容について、例文に明記すべきではないか。 ・パスワードの設定に当たっては、業務目的外で使用しているものを使用しないこと。 ・業務システムを利用するために利用しているパスワードを、業務目的外で利用しないこと。	ご指摘につきましては、今後の参考とさせていただきます。
90	iii-80	地方公共団体	⑩パスワードの使いまわしについて2 「認証情報の管理」の解説に、「パスワードの使いまわしを行ってはならない」と書かれているが、この項目は、システム管理者が守るべき項目であり、システム管理者は使いまわしを把握することは難しいので、この項目の解説としてあるべきではない。	本項目は、利用規約等でパスワードの使いまわしが行われないような措置を講じることを指しております。 ご指摘につきましては、今後の参考とさせていただきます。
91	-	法人	本ガイドラインにおいて、「庁内ネットワーク」という用語が頻出しております（例えば、ii-30, 34, iii-40,58,70,74,75,79,81,92,96, iv-11,30など）。しかしながら、「庁内ネットワーク」自体については、本ガイドラインにおいて、定義や説明が行われていません。実際の自治体のネットワークは、外部委託データセンターを使用するなど多様な形態がとられており、例えば、閉域接続により外部サービスを利用しているケースもあるものと理解しております。従って、このような形態も含めて、本ガイドラインにおいて「庁内ネットワーク」と言う場合には、実際にどのような使用形態があるかを例示頂き、分かり易いガイドラインにしていただくことを希望します。	ご指摘の箇所につきまして修正いたします。
92	i-13	個人	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」が平成30年4月4日に第5版に改訂されている。P11の記述および「図表 1 情報セキュリティポリシー等に関する取り組みの推移」の表記が古いため修正願いたい。	ご指摘の箇所につきまして修正いたします。
93	ii-33	個人	3（オ） 「定期変更」という文言は不要ではないでしょうか。	ご指摘の箇所につきまして修正いたします。
94	ii-31	地方公共団体	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 (15)電子メールの利用制限－⑤ ‘ウェブで利用できるフリーメール、ネットワークストレージサービス等’というと、フリー＝無料と捉えられてしまう。 他の言い方で明確に説明していただきたい。	ご指摘の箇所につきまして修正いたします。
95	iii-48	地方公共団体	⑤モバイル端末について 「管理区域（情報システム室等）の管理」の項目では、「機密性2以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。」とある。 しかし、「モバイル端末」は、用語の定義として「端末のうち、業務上の必要に応じて移動させて使用することを目的としたもの」とある。 また、「端末」は、用語の定義として「情報システムの構成要素である機器」とあるため、情報システムを使うための機器、具体的には、モバイルワーク用のタブレット端末やスマートフォンなどを指していると思われる。 つまり、個人所有の携帯電話、スマートフォン、タブレット等は、上記の用語の定義では「モバイル端末」に該当しないこととなるが、規定の趣旨としてそれで良いか。	ご指摘の箇所につきまして修正いたします。
96	iii-52	地方公共団体	⑥施錠保管について 「職員等の利用する端末や電磁的記録媒体等の管理」として、「モバイル端末の使用時以外の施錠保管等の物理的措置を講じなければならない。」とあるが、電磁的記録媒体についても同様であると考えられるので、電磁的記録媒体についても触れるべきではないか。	ご指摘の箇所につきまして修正いたします。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
97	iii-10	個人	「 ②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット 接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する 場合には、無害化通信を行う。」とあるが、総務省をはじめ他の省庁が開発運用しているインターネット上のシステムに地方公共団体はアクセスする必要がある。 国のシステムからダウンロードするファイルについても無害化が必要である現状である。 国の責任において省庁が運用開発し地方公共団体がアクセスしうるシステムはすべてLGWANからアクセスできるよう整備する必要がある。	ご指摘につきましては、今後の参考とさせていただきます。
98	iii-42	個人	「⑦インターネット経由での各種業務システムの利用 テレワーク等のインターネット経由で各種業務システムにアクセスする場合は、 以下のような情報セキュリティ対策を実施しなければならない。・仮想デスクトップ接続に限定 ・利用可能なネットワークをインターネット接続系に限定 ・専用端末化（電子証明書、MAC アドレスによるフィルタリングなど） ・通信の暗号化（WPA2 方式など） ・データのダウンロード制限 上記の他、多要素認証で端末の正規の利用者を確実に認証することが望ましい。」とあるが、テレワークはインターネット接続系システムのみ利用できるという解釈でよいのか？総務省でもテレワークを行っていると想像するがインターネット接続系のみのテレワークか？ 団体によるが地方公共団体で利用する主たるシステムはLGWAN接続系・マイナンバー利用事務系上にある。よって、テレワークを実現させるためには最低でも地方公共団体のLGWAN接続系に接続する必要がある。 よって「⑥VPN 接続による外部との通信 遠隔での情報システム保守等により、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 等の閉域網または LGWANで接続されなければならない。」をテレワークにもちいてもよいと考えてよいか。	本ガイドラインに記載の「テレワーク」は、インターネット接続系を対象とした記載です。 ご指摘につきましては、今後の改定の参考とさせていただきます。
99	iii-88	不明	iii-88「以前利用していたドメイン（旧ドメイン）を運用停止する場合は、第三者に不正に取得されないようドメインを一定期間保持する。詳細は「ドメイン管理ガイド(2.0版)」（平成28年12月1日内閣官房情報通信技術（IT）総合戦略室）を参照されたい。」とありますが、当該ガイドラインには運用停止や一定時間保持に関する詳細は記載されていません。 「ドメイン管理ガイド(2.0版)」の後継文書となる「Webサイト等の整備及び廃止に係るドメイン管理ガイドライン（初版）」（2018（平成30）年3月30日各府省情報化統括責任者（CIO）連絡会議決定）には詳細が記載されていますが、goドメインの場合と非goドメインの場合とで廃止フローが異なっており、これを地方自治体に準用する際にどのように読み替えるのかが明らかではありません。	ご指摘の内容については、「ドメイン管理ガイド(2.0版)」（平成28年12月1日内閣官房情報通信技術（IT）総合戦略室）の「2 具体的なドメイン管理方法」(3)b)に記載されております。 ご指摘につきましては、今後の参考とさせていただきます。
100	-	不明	著名なセキュリティカンファレンス「Black Hat USA 2016」にて「badWPAD」と名付けられた脆弱性の調査結果が発表され、pad.tokyo」ドメインを利用することで東京都庁のネットワークが乗っ取り可能であったことが示されました。これに関連してJPCERT/CC及びIPAより「JVNTA#91048063 WPAD と名前衝突の問題」が公表されており、ここで挙げられた対策方法のいずれか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に盛り込む必要があると考えます。社内ネットワークで使用するシステムのホスト名や独自TLDに関するクエリの名前解決についてはWAPDという個別の機能に留まらない潜在的なセキュリティリスクとなることから、セキュリティポリシーとして記載するに値するものです。	ドメイン認証のセキュリティ管理については第3編 第2章「6.3. システム開発、導入、保守等」（解説）（注11）（注12）に記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
101	iii-95	法人	自治体様を営業させていただいている中で昨今の自然災害に伴う突発的なウェブサイトへのアクセス増加により防災情報の配信に課題があられるケースを伺います。そのため、現状のガイドライン案に記載ありましたサービス不能攻撃部分について、 自然災害などに伴う突発的な正常アクセスの増加時にも情報システムの可用性を確保するような対策が含まれることがより自治体様にとって望ましいと思い、意見提出させていただきます。	自然災害への対策については、第2編 第1章「3. 対象とする脅威」(3)及び第3編 第2章「7.3. 侵害時の対応」（解説）(3)に記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
102	ii -31	個人	統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。	スパムメール受信時の対応については、ご指摘の文言にて第2編 第2章「6.1. コンピュータ及びネットワークの管理」(14)②に記載しております。
103	iii-39	個人	通信パケットの監視及び破棄、通信ポートの制御、不正なプログラムの検知、不審なメールの検知及び遮断、不審なURLへのアクセス遮断、ログ監視、コンテンツの改ざん検知等の機能を持った、高度な情報セキュリティ機器を導入する。 => 自組織のドメインを騙ったなりすましメール（不審メール）を防止する対策は、自社社員や取引先への標的型攻撃を未然に防止するために必要です。なりすましメール対策の一つである DMARC レコードによるメール流通のモニタリング・監視や SPF及び DKIMへの対応を記述した方がよいです。	DMARC、SPF及びDKIMについては、第3編 第2章「6.1. コンピュータ及びネットワークの管理」（解説）(14)に記載しております。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
104	iv－33	個人	Webサーバ、メールリレーサーバ（メールサーバを含む場合もある。以下同じ。）、プロキシサーバ、外部DNSサーバ、LGWAN接続ファイアウォール（機器は集約せず、セキュリティクラウド上のログ分析システムにログを転送するように設定を変更）である。 => DMARC では、なりすまし防止の技術だけではなく、自組織ドメインで送信されたメールの流通状況をモニタリングする仕組みも備わっています。これらのデータを監視する必要性も合わせて記載した方がよいです。	DMARCについては、第3編 第2章「6.1. コンピュータ及びネットワークの管理」（解説）(14)に記載しております。
105	全般	個人	情報セキュリティ対策基準で追加された情報システム全体の強靭性の向上について及び特定個人情報の適正な取扱いに関するガイドラインによる物理的、人的、技術的セキュリティ対策について、対策基準の物理的、人的、技術的セキュリティ対策の各項目へ記載していただきたい。理由としては、地方公共団体が取り扱う情報資産の分類による物理的、人的、技術的セキュリティの対策について、一覧性を高めることによる実施漏れや相互関係の不備が低減され、情報セキュリティ対策の向上が図れると考えます。	本ガイドラインは、地方公共団体において情報セキュリティ対策基準全体を参照したうえで対応いただくことを想定しています。そのため、強靭性の向上及び特定個人情報の適正な取扱い等について物理的、人的、技術的セキュリティ対策の各項目に記載はしておりません。 ご指摘につきましては、今後の参考とさせていただきます。
106	―	個人	意見募集期間が１１日間と短期間である。適切な募集期間が必要であると考える	ご指摘につきましては、今後の参考とさせていただきます。
107	全般	個人	ガイドラインの「推奨事項」以外の記載については遵守すべきと地方公共団体は認識する必要があるのか。セキュリティ整備にはコストはかかるが、遵守すべきとするのではあれば総務省から地方公共団体への財政措置が必要であると考える。また、セキュリティ確保・向上のための投資判断や財政とのバランスやポートフォリオについての記述をガイドラインに設けることはできないか。	本ガイドラインの「推奨事項」以外の記載については遵守すべき事項です。ただし、本ガイドラインは地方公共団体にて策定する情報セキュリティポリシーの参考としていただく位置づけの文書です。 ご指摘につきましては、今後の参考とさせていただきます。
108	iii－73	個人	「(3) 他団体との情報システムに関する情報等の交換他団体との間で情報システムに関する情報及びソフトウェアを交換する場合は、その用途等を明確にして目的外利用や紛失、改ざん等が起こらないようにしなけれ ばならない。（注3）これを担保するため、相手方の団体との間で当該内容を明記した合意文書を取り交わす等の対策を取ることが望ましい 」という記述があるが、ソフトウェアの交換等どのような状況を想定しているか不明なため解説が欲しい。	他団体等の外部と、情報（紙文書、データ等）を様々な手段（メール、紙文書の配布等）でやり取りする場合の情報の取扱いを想定しております。 ご指摘につきましては、今後の改定の参考とさせていただきます。
109	―	法人	もっとも、本ガイドライン案の公表と意見提出期限の間はわずか10日間であり、これは非常に短い期間であり、今後は意見募集期間を少なくとも30日間以上設けるよう希望します。	ご指摘につきましては、今後の参考とさせていただきます。
110	ii －24	個人	4（イ） 「情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない」とありますが、具体的な措置を記載した方がよいかと思います。	具体的な措置につきましては、第3編 第2章「5.1. 職員等の遵守事項」（解説）(1)①に記載しております。
111	ii －26 iii－63	個人	(2)４ 「報告を受けるための窓口を設置し、当該窓口への連絡手段を公表」とありますがが、当該窓口が攻撃を受ける可能性があるので、「問合せ窓口」を公表とう文言の方かよいかと思います。	ご指摘につきましては、今後の参考とさせていただきます。
112	ii －34	個人	(2)６ 「接続する前に、コンピューターウイルスに感染していないことを確認しなければならない」とありますが、具体的な措置を記載した方がよいかと思います。	具体的な措置につきましては、第3編 第2章「6.2. アクセス制御」（解説）(2)に記載しております。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
113	iii－42	地方公共団体	「第2章　情報セキュリティ対策基準（解説）」のインターネット経由での各業務システムの利用（iii－41ページ）について、多くの自治体で各業務システムがLGWAN接続系に構築されていることを踏まえて、情報セキュリティの確保に配慮しつつ、自治体におけるテレワーク等を普及していくため、テレワーク等のインターネット経由で各業務システムにアクセスする場合におけるセキュリティ対策の内容等を明確化していただきたい。 1　LGWAN接続系にある業務システムへのアクセスできることを明確化すること 　〇項目名の「⑦インターネット経由での各業務システムの利用」を「⑦インターネット経由での各業務システム（LGWAN接続系に設置されているシステムを含む。）の利用」に改めること。 2 「・利用可能なネットワークをインターネット接続系に限定」については、インターネット接続系にある業務システムしかアクセスできないと解釈可能なため、「・テレワーク等の端末からアクセスするネットワークをインターネット接続系に限定すること」に改めること。 ※なお、上記1、2について、そもそもの意図が、「インターネット接続系にある業務システムしかアクセスを認めない」ということであれば、多くの自治体で各業務システムがLGWAN接続系に構築されている現状では、テレワークの普及は困難な状況であると考えています。 ※この場合、「インターネット経由での各業務システムの利用」とは違った考え方（LGWAN接続系にモバイル閉域網で接続するなど）でテレワークを考えなければならず、インターネット利用とのコスト比較等を考えると、テレワークの普及が難しくなると考えています。 3 「・仮想デスクトップ接続に限定」「・データのダウンロード制限」の2つについて、「・テレワーク等の端末との通信は、仮想デスクトップ接続など画面転送を行う接続方法に限定し、テレワーク等の端末にデータをダウンロードできない措置を講じること」とし、セキュリティ対策内容を明確化すること 4 「・専用端末化（電子証明書、MACアドレスによるフィルタリングなど）」について、「・テレワーク等の端末は、セキュリティ管理者又はネットワーク管理者から貸し出された端末又は許可を受けた端末とし、電子証明書、MACアドレスによるフィルタリングなどによりアクセスできる端末を特定すること」とし、セキュリティ対策内容を明確化すること	本ガイドラインに記載の「テレワーク」は、インターネット接続系を対象とした記載です。 ご指摘につきましては、今後の改定の参考とさせていただきます。
114	－	不明	本ガイドラインの提示から〆切までが10日である。 意見提出が30日未満であり、適切な理由は明記されていないが、 早期に改定する理由があるのか。	ご指摘につきましては、今後の参考とさせていただきます。
115	ii －29	法人	（原文） ③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、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。 （原文に追記） なお、取得したログについては各システムログを複合的に分析し高度なセキュリティ侵害についても分析を実施しなければならない。 （理由） セキュリティ侵害は日々高度化しており、システム個々のログを確認するだけではなく複合的にシステムログを確認しなければ発見できないものも多く存在するため、この文言が必要後考えます。	ご指摘につきましては、今後の参考とさせていただきます。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
116	ii -39	法人	（原文） （5）職員等による不正アクセス 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、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。 （変更） 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、職員等による不正アクセスを防止するために、システムログ分析等を強化し通常とは異なる状況を発見できるような環境を準備すること。 職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。 （理由） 職員等による不正アクセスはあってはならないことですが、より起きにくい環境を構築するために強靭化等で導入したシステムのログを有効活用し抑止力を強化すべきと考えます。	ログの確認につきましては、第3編 第2章「7.2. 情報セキュリティポリシーの遵守状況の確認」（解説）（1）にて記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
117	iii -21	個人	②CIOに関する記述について このたびのポリシーでは、解説の部分に一言CIOの説明はありますが、例文を中心にCIOとCISOの差異について説明が薄い（例文には「CIO」が一言も出てこない）という印象を受けました。 例文にもCIOとCISOの相関について追記すべきと考えますがいかがでしょうか。	ご指摘につきましては、今後の参考とさせていただきます。
118	-	法人	○インターネットの定義について インターネット上の脅威から特定個人情報およびLGWANを隔離するという方針を継続することには、賛成です。一方で、本ガイドラインにおけるインターネットの定義があまりに広く、パブリッククラウド等を活用することによるコスト削減、業務効率向上、セキュリティ向上の可能性を逸してるいる側面があるとも、指摘せざるを得ません。従って、インターネットからの隔離を徹底してセキュリティの脅威の排除は推進する一方で、一定の要件を満たすクラウド事業者やインターネットサービスについては積極的に利用していく事も、今後検討していくべきと考えます。	ご指摘につきましては、今後の参考とさせていただきます。
119	-	法人	○End To Endの暗号化と回線の評価について セキュリティの向上の為には、End To Endで信用できる暗号化方式で暗号化されるように規定することが重要であると考えます。公開鍵暗号化方式を採用した暗号化技術は、技術的に具体的な脆弱性は現在指摘されていません。このようなことから、End To Endの暗号化こそがいかなる盗聴にも対応できる手法であると、一般的には認識されています。 一方で、インターネットか閉域網か専用線かなどの経路の規定がセキュリティの観点で論じられることもありますが、End To Endの暗号化が施されていない通信はいかなる通信経路で通信したとしても、セキュリティリスクをはらんでいるとも言えます。	暗号化については、第3編 第2章「6.1. コンピュータ及びネットワークの管理」【例文】（16）及び（解説）（16）に記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
120	-	法人	○災害対策について 九州の震災、西日本の豪雨の際に、被災した自治体において情報システムが機能しなくなり、緊急対応が必要な状況下、パブリッククラウド技術を利用して業務を遂行するという事例が多くみられました。可用性もセキュリティの重要な要素なので、災害発生時におけるパブリッククラウド利用も想定しつつ、バランスの取れた気密性と完全性の定義することが肝要であると考えます。	ご指摘につきましては、今後の参考とさせていただきます。
121	iii -74	法人	解説）（9）外部の者が利用できるシステムの分離等 「電子申請受付システム等、外部の人々が利用できるシステムは、必要に応じ、ほかのシステムのネットワークと切り離すなどの措置が必要である。」との記載だけがありますが、これらのシステムにおいても個人情報等を扱うことを鑑み、これらについても、このセキュリティポリシーできちんと取り扱うべきだと考えます。また、切り離すことを前提とするのではなく、セキュリティを担保したうえでシステム間の連携により業務の効率化、住民サービスの向上を目指すべきだと考えます。	ご指摘につきましては、今後の参考とさせていただきます。
122	ii-6 iii-7	地方公共団体	■基本方針 4.適用範囲 （2）情報資産の範囲 「個人情報」についても、明記していただきたい。	概念としては②のネットワーク及び情報システムで取り扱う情報に含んでおります。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所 （ページ番号）	提出者	提出された意見	意見に対する考え方
123	ii -31 ii -44	地方公共団体	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 (15)電子メールの利用制限 (15)「ウェブで利用できるフリーメール、ネットワークストレージサービス」と、8.1.(1)③外部委託の「クラウドサービス」及び8.2.の「約款による外部サービス」との違いが明確でなく、混乱が生じる可能性がある。そのため、それぞれの定義を明確にしていただきたい。	6.1(15)は、個人で利用できてしまうプロバイダー等が提供するメールやオンラインストレージを指しており、8.1は契約行為を伴った業務委託の中で利用するクラウドサービスを指しております。また、8.2は約款への承認によるサービス利用という位置づけの中でのクラウドサービスについて説明しております。
124	ii -34	地方公共団体	6.2.アクセス制御 (2)職員等による外部からのアクセス制限－⑦ 「⑦統括情報セキュリティ責任者は、公衆通信回線（公衆無線LAN等）の庁外通信回線を庁内ネットワークに接続することは原則して禁止しなければならない。」とあるが、テレワークにより職員が公衆通信回線からアクセスすることが一般化する中で、書き方として工夫していただきたい。	ご指摘につきましては、今後の参考とさせていただきます。
125	ii -34	地方公共団体	6.2.アクセス制御 (2)職員等による外部からのアクセス制限－⑦ 「⑦統括情報セキュリティ責任者は、公衆通信回線（公衆無線LAN等）の庁外通信回線を庁内ネットワークに接続することは原則して禁止しなければならない。」とあるが、より正確に、「…一般電話回線や公衆無線LAN等の公衆通信回線を庁外通信回線として使用し、庁内ネットワークに…。」と表記していただきたい。	ご指摘につきましては、今後の参考とさせていただきます。
126	ii -44	地方公共団体	8.2.約款による外部サービスの利用 当該サービスの利用において機密性2以上の情報が取り扱われないように規定しなければならないとのことだが、業務上使用する情報の大部分は機密性2であると考えられる。そのため、「機密性2以上」を「機密性3」に限定しないと、実用に耐えられないのではないため、再検討していただきたい。	ご指摘につきましては、今後の参考とさせていただきます。
127	iii -7～9	地方公共団体	④ネットワークに接続しないスタンドアロンパソコンについて スタンドアロンパソコン（プレゼン等を目的とした持ち出し用パソコンも含む）は、セキュリティポリシーの対象となっているか。 まず、「端末」は、用語の定義として「情報システムの構成要素である機器」とあり、「情報システム」は、「コンピュータ、ネットワーク及び電磁的記録媒体で構成され」とある。 そこから考えると、スタンドアロンパソコンは「端末」には該当しないと考えられる。 また、ポリシーが対象とする「情報資産の範囲」は、「①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体」と規定されており、前述のとおり、スタンドアロンパソコンは情報システムに含まれないとすると、「電磁的記録媒体」に含まれることになるかとも考えられるが、図表10によると、「電磁的記録媒体」の例として、「サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体」とあり、そこから考えると、スタンドアロンパソコンは対象にならないと考えられる。 スタンドアロンパソコンにも、場合によっては重要な情報が入っている場合もあり、セキュリティポリシーの対象とするべきである。 対象であると考えられているなら、明示的に表現していただきたい。 対象外であると考えられているなら、解説等でも明確にしていただきたい。	独自のスタンドアローン端末や閉鎖的なネットワークは本ガイドラインに準拠する情報セキュリティ対策を講じていただく必要があります。
128	ii -23	地方公共団体	⑧公用メールアドレスの目的外利用について 平成29年3月、政府における公用個人メールアドレスの流出が報道されたが、これは、公用個人メールアドレスを、インターネット上のWebサービスで私用で使っていたものが流出した事案であった。 これを受けて、NISCから各省庁にセキュリティにかかる注意喚起があり、それを受けて総務省（J-LIS）から都道府県にセキュリティポリシーの状況について確認の依頼があった。 それによると、ガイドラインの「業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。」が該当するとのことであったが、これをもってメールアドレスの私的利用禁止の根拠とするのは、ちょっと弱い気がする。 別に以下の内容について、明記すべきではないか。 ・公用のメールアドレス（個人用も含む）を業務目的以外の目的で利用してはならない。	ご指摘につきましては今後の参考とさせていただきます。

「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（案）」に対する意見及びそれに対する考え方

No.	該当箇所（ページ番号）	提出者	提出された意見	意見に対する考え方
129	iii-80	地方公共団体	⑪管理者権限の管理について 「アクセス制御」の「特権を付与されたID の管理等」について、「管理者権限」が、「サーバの全ての機能を利用できる権限」と説明されているが、厳重に管理すべき管理者権限はサーバに限らないので、「サーバ等」としてはどうか。	ご指摘につきましては、今後の参考とさせていただきます。
130	iii-37	不明	「SIM9カ ード（携帯電話／スマートフォンの固有番号）とパスワードの併用」は 「SIMカ ード（携帯電話／スマートフォンの固有番号）とパスワードの併用」の誤植と思われます。	ご指摘の箇所につきまして修正いたします。
131	ii -19	地方公共団体	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 「インターネット業務端末」とは、「インターネット接続系の端末（インターネット接続系に接続された端末」と同義か。同義であれば、後段の「LGWAN接続系の端末」と表現を統一されたい。異義であれば、その意味を明確に定義されたい。	ご指摘の箇所につきまして修正いたします。
132	iii-38	地方公共団体	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 「インターネット業務端末」とは、「インターネット接続系の端末（インターネット接続系に接続された端末」と同義か。同義であれば、後段の「LGWAN接続系の端末」と表現を統一されたい。異義であれば、その意味を明確に定義されたい。	ご指摘の箇所につきまして修正いたします。
133	iii-39	地方公共団体	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 （注4） 「インターネット接続系の端末」と「インターネット接続系端末」という用語が混在しているが、同義か。同義であれば表記を統一されたい。異義であれば、それぞれの意味を明確に定義されたい。 また、同ページの「インターネット業務端末」との差異についても、同様に明確にされたい。	ご指摘の箇所につきまして修正いたします。
134	iii-42	地方公共団体	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－② （注8） (c)で「ファイル交換ソフト」と「ファイル共有アプリケーション」は同義か。同義であれば、表現を統一されたい。異義であれば、その意味を明確に定義されたい。	ご指摘の箇所につきまして修正いたします。
135	-	地方公共団体	①アルファベットの表現の統一（全角・半角） 「DNS」「LGWAN」等全角と半角が入り乱れているので、半角なら半角で統一した方がよい。	ご指摘の箇所につきまして修正いたします。
136	-	地方公共団体	②用語の統一 「外部の者」と「外部の人々」が混在している。意味は同じと思われるので、統一した方がよい。	ご指摘の箇所につきまして修正いたします。
137	iii-32	地方公共団体	⑭その他 「情報システム全体の強靭性の向上」で、解説付きの例文で、「（ア）情報のアクセス対策」の項目に、「なお、外部接続先もインターネット等と接続してはならない。」とあるが、第2編の例文には記載がないので、誤りである。	ご指摘の箇所につきまして修正いたします。
138	-	地方公共団体	⑬「措置」「対策」について、 「措置を講じる」「措置を実施する」「措置をとる」「措置を検討する」 「対策を講じる」「対策を実施する」「対策を行う」「対策を施す」 というように用語が使われているが、「実施する」「とる」「施す」は同じ意味ではないか（表記ゆれ）。 「講じる」と「実施する」等は、使い分けがされているか。その場合、「講じる」と規定されている項目は実施するところまでは求めていないのか。 「侵害時の対応等」の解説で、 「(キ) 事案に係る証拠保全の実施を完了するとともに、暫定措置を検討する。 (ク) 暫定措置を講じた後、復旧する。」とあるが、どう解釈すればよいか。 「情報セキュリティインシデントの報告」の解説では、「被害の拡大防止等を図るため応急措置の実施及び復旧に係る指示」とある。	「とる」、「施す」、「行う」を「講じる」、「検討する」、「実施する」のいずれかの表現に該当するか検討し、修正いたします。 「暫定措置」「応急措置」は、表現を「応急措置」に統一いたします。