「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２年 12 月 28 日
総務省自治行政局
地域力創造グループ
地域情報政策室

令和２年 12 月９日（水）から 12 月 22 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、116 件の御意見が寄せられました。

提出された主な意見及びその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２年 12 月 28 日（月）に改定・公表を行いましたので、お知らせいたします。

■パブリックコメントで提出された主な意見及びその意見に対する総務省の考え方

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
1	個人	第1編	ｉ-18	「図表 4 のとおり、これを定期的に繰り返すことで、環境の変化に対応しつつ、情報セキュリティ対策の水準の向上を図らなければならない。」の部分について「図表 4 のとおり、これを定期的に繰り返すことで、環境の変化に対応しつつ、情報セキュリティ対策の水準の向上を図らなければならない。定期的に繰り返す頻度は、3年に1度程度等技術の進歩に応じて柔軟に検討する必要がある。」との変更を提案します。	今後の検討の参考にさせていただきます。
2	個人	第2編	ii -5	LGWAN接続系とインターネット接続系の分割の説明について、以下のように表記揺れが見られます。 ii-5～6 「安全が確保された通信だけを許可」 ii-20　「必要な通信だけを許可」 iii-6　「安全が確保された通信だけを許可」 iii-33　「必要な通信だけを許可」 iii-41　「必要な通信だけを許可」 「必要な通信」では「必要であれば必ずしも安全でなくても良い」と読めてしまうため、「安全が確保された通信だけを許可」の方に統一すべきと考えます。	インターネット接続系とLGWAN接続系の通信は、業務に必要でかつ無害化通信により安全が確保された通信だけを許可するものです。前後の文面から安全を確保することが読み取れる場合等は、必要な通信だけを許可すると記載しており、原案のとおりとさせていただきます。
3	個人	第2編	ii -5	第1章２（８）（９）において、マイナンバー利用事務およびＬＧＷＡＮ接続系の定義について 業務において、マイナンバーを含まない個人情報は多々あり、当該システムは必ずしもＬＧＷＡＮに接続しているとは限らないことから対策漏れが生じる可能性もある。 →　（案１）新たに個人情報利用事務（マイナンバー利用事務系を除く）を追加 　　（案２）マイナンバー利用事務系を個人情報利用事務系に改める。　各章にてマイナンバー利用に特化した対策は、その旨記載	今後の検討の参考にさせていただきます。
4	個人	第2編	ii -6	無害化通信について「インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信」と記載されていますが、この表現ではただアンチウイルスソフトでスキャンしただけでも無害化通信を名乗ることができてしまう状況です。アンチウイルスでは対応できない未知のウイルスへの対策であること、また万が一内部端末が感染しても遠隔操作や情報漏洩の経路にならないことも定義に記載すべきと考えます。 以上を踏まえ、例えば以下のように改めてはいかがでしょうか。 「インターネットメール本文のテキスト化や端末への画面転送等により、未知のコンピュータウイルスを確実に除去し、また万が一端末がコンピュータウイルスに乗っ取られたとしても遠隔操作や情報漏洩の経路となり得ないよう、安全が確保された通信をいう。」	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
5	法人	第2編	ii -7	情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策が必要なこと、記載のとおりと存じます。ただ、特に機密性において、必要以上に多くの情報資産が機密性レベル3とされていることがあり、利用しうる情報システムに制限が生じているともお聞きすることがあります。そのため、情報資産の機密性に関する分類に関しては、p. ii -16にて記載されておりますが、「秘密文書」について例示する等、機密性分類について指針が示されることが望まれます。	今後の検討の参考にさせていただきます。
6	法人	第2編	ii -7	情報管理システムの管理下におかれていない資産は守ることができないため、防御の対象に網羅性があることを検証する必要がある。また、内閣サイバーセキュリティセンターが公布した「サイバーセキュリティ戦略」に言及されている通り、サイバー空間の脅威から生じ得る被害やその拡大を防止するためには、平時からの取組が必要である。 「6. 情報セキュリティ対策　(3) 情報システム全体の強靭性の向上」に以下の文章を追加してはいかがでしょうか。 「対策を講じるにあたり、ネットワークに接続されたすべてのIT資産を把握し、パソコン等のすべての端末が情報管理システムの管理下におかれていることを確認した上で、平時からのサイバー空間における公衆衛生活動、具体的には不正プログラムからの防御や脆弱性の解消に取り組む。」	ソフトウェアにセキュリティホールが存在する場合、システムへの侵入、改ざん、損傷、漏えい等の被害を及ぼすおそれがあり、セキュリティホールをはじめとするセキュリティ情報の収集、共有及び対策を講じること等について規定しております。ご意見は今後の検討の参考にさせていただきます。
7	法人	第2編	ii -8	自己点検に際しては、最新の情報セキュリティおよび現在の情報セキュリティポリシーに照らし合わせた遵守状況を確認する必要があるため、特に数量が多いパソコン等の端末の遵守状況について、人間の判断を介さず、情報管理システムを用いて点検時点での遵守状況を確認できる手段を用いらなければならない。 「7. 情報セキュリティ監査及び自己点検の実施」に以下の文章を追加してはいかがでしょうか。 「自己点検に際し、特に数量が多いパソコン等の端末の管理状況については、網羅性と正確性を期すために、職員への聞き取りではなく、情報管理システムにて各端末のデータを取得し管理状況点検を行う。」	今後の検討の参考にさせていただきます。
8	個人	第2編	ii -12	CISOについては、責任の所在がある事が重要であるため、必ず1人置く、という様な形での記述を行われたい。	今後の検討の参考にさせていただきます。
9	個人	第2編	ii -19	第2章２（２）-10において、読み取れなくはないが、単に不要になった場合だと、リース満了後等のイメージが強いので、解釈に不具合等により交換した電磁的記録媒体も対象となる旨も記載した方がよいのではないか。	現行の記載でも読み取れるため、原案のとおりとさせていただきます。
10	個人	第2編	ii -19	「情報資産の廃棄を行う者は、情報を記録している電磁的記録媒体が不要になった場合…」について、以下のように改めてはいかがでしょうか。 「情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。」	4.1(７）において、ご指摘の内容については記載しておりますので、原案のとおりとさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
11	個人	第2編	ii -19	本ページ以降多数において、「暗号化又はパスワード(の)設定」という記述があり、「パスワードを設定すれば必ずしも暗号化しなくてもよい」という解釈が可能となってしまっています。 「パスワードのみ設定して暗号化しない」状態では目的を果たさないと考えられるため、「又はパスワード(の)設定」は一律削除すべきと考えます。 （「パスワードを設定しても暗号化しない」というファイルフォーマットはレアケースとして実在します。また PC における BIOS の起動パスワードや OS ログオンパスワードも、パスワードが判らない場合起動・ログオンできないだけで HDD は暗号化されないため第三者が読み出し可能です。） もし読者への解りやすさを考えて「パスワード」という単語を敢えて残すのであれば、「パスワード等により暗号化」と改めるべきと考えます。	今後の検討の参考にさせていただきます。
12	個人	第2編	ii -19	「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、暗号化又はパスワード設定を行わなければならない」とありますが、今回iii -32で電子メールでのパスワード伝送（いわゆるPPAP）を封じる記載が追加されたことにより、機密性2に該当する雑多な情報を無差別に暗号化することが非常に困難となり、「守れないルール」となる恐れが高くなります。 「必要に応じ」となっているので無差別に一律ということにはなっていませんが、「必要」の判断基準が不明なため、一般職員としては「判断つかないのでとりあえず暗号化する」と判断せざるを得なくなります。 このため「機密性2以上」を「機密性3」に改めるか、「機密性2以上」のままとする場合は「必要に応じ」の「必要」とはどのような場合かを整理し、無闇な暗号化を求めるものではないことを明記されることが望ましいと考えます。（例えば ISP が信用できない外国宛に送る場合は必要、庁内同士や LGWAN 経由では不要と記載する等）	今後の検討の参考にさせていただきます。
13	個人	第2編	ii -20	マイナンバー利用事務系で扱われるデータの秘匿性を鑑みると、インターネットから送信された情報の取り込みを行う端末はLGWAN系の環境に置き、基幹システム側の端末とその端末の通信を1対1の特定通信とする形にして、多層防御する必要があると思います。	今回の見直しにおいては、マイナンバー利用事務系にインターネット経由の申請等データを安全に取り込むために必要となるセキュリティ対策もあわせて提示しております。
14	個人	第2編	ii -22	（2）管理区域の入退室管理等において、当該情報システムに関連しない・・・通信回線装置、電磁的記録媒体を持ち込ませないようにしなければならないとあるが、運用する部屋においては、ベンダーによっては社内サーバーにある電子マニュアルを参照する必要があるため、管理区域全域にて持ち込ませないのは難しいことから、運用する部屋に限定した上で、セキュリティ対策や通信ログの提供などの対策を情報システム管理者が確認できた場合はこの限りではないが望ましい。	ベンダー等が必要となる機器の持ち込みについては、情報システムに関連するコンピュータ等に該当し禁止されているものではないので、原則問題ないと考えます。
15	個人	第2編	ii -24	「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。」とありますが、この「総合行政ネットワーク（LGWAN）に」は「LGWAN接続系に」の誤りではないでしょうか。	行政の様々なネットワークを原則LGWANに集約することを努めるという意図で記載しています。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
16	個人	第2編	ii -28	「CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。」部分について、「CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。多数のインシデントが発生することも想定し、一定の条件下における応急処置については、自動化されることが望ましい。」との変更を提案します。	今後の検討の参考にさせていただきます。
17	個人	第2編	ii -28	「CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。」の部分について、「CSIRT は、これらの情報セキュリティインシデント原因を究明し、疑義のログだけをフィルタリングせずに記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。」との変更を提案します。	今後の検討の参考にさせていただきます。
18	法人	第2編	ii -29	内閣サイバーセキュリティセンターが公布した「サイバーセキュリティ戦略」において言及されている通り、脆弱性への迅速な対応を可能とするために、情報システムの状態をリアルタイムに把握できる手段を用いらなければならない。 「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」に新たな項目として以下を追加してはいかがでしょうか。 「（21）パソコン等の端末の状態調査 セキュリティ侵害や特定の脆弱性に該当するパソコン等の端末の有無や影響範囲を調査する場合は、リアルタイムにシステムの状態を把握できる手段を用いらなければならない。」	今回の改定において、「IT資産を手作業で漏れなく正確に把握するには多大な労力が必要となる。そのため、自動でソフトウェアの種類及びバージョンを管理する機能を有するIT資産管理ソフトウェアを導入することが考えられる。」と追記しております。ご意見は今後の検討の参考にさせていただきます。
19	個人	第2編	ii -29	「サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。」とありますが、これはユーザーが強いパスワードを作成することを阻害する、現在では良くないとされているポリシーと思われます。 現在は、システム毎に異なる強いパスワードを作るかわりにパスワードマネージャー等を用いて端末に記憶させる方向が主流と考えます。（このことから、各モダンブラウザは入力フォームの autocomplete="off" をサポートしていません。） しかし、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。このため、このポリシーは「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、」という前提条件をつけて残す必要があると考えます。	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
20	個人	第2編	ii -31	「情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。」の部分について、「情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的もしくは論理的に遮断しなければならない。」との変更を提案します。	今後の検討の参考にさせていただきます。
21	個人	第2編	ii -32	「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」とありますが、大量のスパムが内部から送信されている場合は停止して調査すべきと思いますが、外部から着信している状況は日常茶飯事であり何ら問題ないためメールサーバの運用停止は不要と考えます。 また、大量スパム着信時の記載はii -40～41の「(2) 攻撃への対処」や「(6) サービス不能攻撃」とも重複するため、整合性を取る必要があります。 したがってこの項目の「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」は「大量のスパムメール等が団体内部から送信されていることを検知した場合は」に改めるか、この項目自体を削除すべきと考えます。	今後の検討の参考にさせていただきます。
22	個人	第2編	ii -33	第2章６　6.1（１５）-5　ウェブで利用できる電子メールだと全てが対象と見えるので、「ウェブサービスとして提供される電子メール」に変更した方がよいのではないか。ただし、Google等のAPIやツールなど、電子メールをIDとするものもあるため、使用を禁止するのが難しい場合もあります。	現行の記載でも特段の紛れが生じないため、原案のとおりとさせていただきます。
23	個人	第2編	ii -33	「職員等は、ウェブで利用できる電子メール、ネットワークストレージサービス等を使用してはならない」とありますが、これは「インターネット上の私用の」ということを前提として書かれたものだと思います。「業務用として割り当てられた」ものであれば何ら問題なく、また必要であるため、「情報システム管理者に定められたものを除き、」という文言を追加すべきと考えます。	今後の検討の参考にさせていただきます。
24	個人	第2編	ii -33	以下のような記載に修正してはいかがでしょうか。 「(19) 業務外ネットワークへの接続の禁止 職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者から定められたネットワークと異なるネットワークに接続してはならない。情報システム管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。」	ご指摘いただきました点は、「庁内無線LANのセキュリティ要件について」に記載しています。
25	個人	第2編	ii -35	⑦に「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」について、以下のようにしてはいかがでしょうか。 「統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし(以下略)」	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
26	個人	第2編	ii -35	「職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得てから接続しなければならない。」について、「職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って自動的に接続しなければならない。」との変更を提案します。	ご指摘を踏まえ、記載を修正いたします。
27	個人	第2編	ii -36	「(4) ログイン時の表示等」に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。「望ましい」や【推奨事項】とすべきと思われます。	今後の検討の参考にさせていただきます。
28	個人	第2編	ii -36	「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、以下のような例外条件を付け加えることが現実的と考えます。 「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。」	今後の検討の参考にさせていただきます。
29	個人	第2編	ii -39	ⅱ-39にて「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」との記述がありますが、調達時においても利用を予定している期間中にサポート終了しない製品を選定することが重要です。 したがって、7.3(1)②に以下のような内容を追加すべきと考えます。 「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。」	今後の検討の参考にさせていただきます。
30	個人	第2編	ii -40	「（ア）パソコン等の端末の場合　LAN ケーブルの即時取り外しを行わなければならない。（イ）モバイル端末の場合　直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。」について「（ア）パソコン等の端末の場合　LAN ケーブルの即時取り外し、もしくは論理的な切断を行わなければならない。（イ）モバイル端末の場合　直ちに利用を中止し、通信を行わない設定への変更を自動化等の仕組みを用いて行わなければならない。」との変更を提案します。	ご指摘を踏まえ、記載を修正いたします。
31	個人	第2編	ii -47	第2章 8.4　クラウドサービスの利用 において、サービスの中断や終了時は勿論のこと利用中における電磁的記録媒体の交換などに対するデータ消去についても要件として定めておく必要があるのではないか。	8.4④において、「クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めなければならない。」とされております。ご意見は、今後の検討の参考にさせていただきます。
32	個人	第2編	ii -47	「パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適正に管理する」とありますが、「望ましい」【推奨事項】レベルとすべきと考えます。	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
33	個人	第2編	ⅱ-47	政府統一基準で「機関等が自ら」となっている部分が「本市が自ら」と置き換えられていますが、 団体自身が提供するプライベートクラウドのほか都道府県の共同利用といったコミュニティクラウドのパターンもあることから、「本市または他団体が提供する」といった表記に改める必要があると思われます。	今後の検討の参考にさせていただきます。
34	個人	第3編	ⅲ-32	情報漏えいの観点から「あらかじめ受信者と合意した」「メール以外での伝達」は全く意味がないと考えます。 「パスワードと暗号化ファイル」セットで第三者に転送されたりする可能性を考慮し、「パスワードレス」の暗号方式を採用すべきです。	「メール以外での伝達」については、「テレワークセキュリティガイドライン第4版」(平成30年4月 総務省)や「庁舎内におけるクライアントＰＣ利用手順 電子メール編 雛型」（内閣サイバーセキュリティセンター）にも記載があることから、原案のとおりとさせていただきます。
35	個人	第3編	iii-32	電子メールのパスワード（鍵）の取扱いについて、別手段を用いて伝達することを「ことが望ましい」とされていますが、電子メールでは意味がないため「必要がある」と記載すべきと考えます。 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。	今後の検討の参考にさせていただきます。
36	個人	第3編	ⅲ-37	「十分な安全性が確保された外部接続先等」の定義を明確にすべきと考えます	今回の検討においては、eLTAXやぴったりサービスについて、リスク評価を行うとともに、有識者が参加した検討会において、安全性を確認しております。ご意見は、今後の検討の参考にさせていただきます。
37	個人	第3編	iii-37	注１（ア）にて通信は外部接続先から片方向通信のみと記載されているが、この場合、各種申請の入力補助についてマイナンバー利用事務系から情報を利用できない。電子申請についても住民が期待する利便性の水準に対し、著しく乖離したサービスしか提供できないことになると危惧する。	LGWAN接続系とマイナンバー利用事務系の間にDMZを設置し、外部接続先のLGWAN-ASPからのデータやファイルは、FW、連携サーバを介してマイナンバー利用事務系へ転送します。また、設置したFWにより、LGWAN-ASPと連携サーバの通信を制御することを想定しています。 プッシュ型の通知等の実現については、今後検討して参ります。
38	個人	第3編	iii-37	「マイナンバー利用事務系は、LGWAN 接続系やインターネット接続系と特定通信として接続してはならない。」について「行政のオンライン化、ワンストップ化等の目的を除いては、マイナンバー利用事務系は、LGWAN 接続系やインターネット接続系と特定通信として接続してはならない。」との変更を提案します。	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
39	個人	第3編	iii-37	注1でeLTAX、ぴったりサービス、自治体情報セキュリティプラットフォームとあるが、これのみ接続を許容するのか。 外部接続は基幹系システムに直接接続することを意味するのか。 国等の公的機関が構築したぴったりサービスのセキュリティ基準が他のLGWAN-ASPサービスとどれほど違うのかわからなく、もし他のLGWAN-ASPサービスを認めない場合は根拠を示していただきたい。 さらに、OSやウイルス対策の更新プログラムも自治体情報セキュリティプラットフォームだけの解釈になるのか。	現時点で想定しているシステム等は、（注1）に記載されたシステム等であり、これらを接続する場合は、連携サーバ等を介しての接続が必要としております。 今回の検討においては、eLTAXやぴったりサービスについて、リスク評価を行うとともに、有識者が参加した検討会において、安全性を確認しております。 OSの修正プログラムやウイルス対策ソフトの更新プログラムについては、自治体情報セキュリティ向上プラットフォームの利用の他、電磁的記録媒体の利用による適用も考えられます。
40	法人	第3編	iii -39	「知識」を利用する手段」の具体例として「パターン」の追加を提案いたします。	今後の検討の参考にさせていただきます。
41	個人	第3編	iii-41	「・インターネット接続系において内容を目視で確認するとともに、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等で危険因子が含まれていないことを確認」について「・インターネット接続系において内容を目視で確認するとともに、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等（ファイル無害化、サンドボックス、EDR 等）で危険因子が含まれていないことを確認」との変更を提案します。	今後の検討の参考にさせていただきます。
42	法人	第3編	iii-41 iii-42	仮想デスクトップについて、画面転送以外の実現方式(例えば、ローカルPCでの環境分離方式)も選択できる余地があってもよいと考えます。	今後の検討の参考にさせていただきます。
43	個人	第3編	iii-41 iii-42	ガイドライン内の画面転送において、仮想デスクトップ化という記述があります。こちらはSBCやVDIなどを想定しているかと思います。アプリケーション仮想方式ではWeb分離製品は対象となりますか。ブラウザを利用してWebアクセスを行うソリューションです。 Web分離製品例（SCVX、SecureBrowser、symantec WebIsoration、Ericom Shieldなど） また、画面転送の許可される方式について明記をお願い致します。	原則として、LGWAN接続系端末から仮想化したインターネット接続環境を画面転送で接続する方式（80/443ポートの遮断が可能な画面転送方式）を想定しております。
44	個人	第3編	iii-42	「（注６）仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。」の後に続けて例えば以下の内容を追記されると、画面転送型の莫大な経費負担に喘ぐ全国の自治体にとって非常に有益なものと考えます。 「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。」	今後の検討の参考にさせていただきます。
45	個人	第2編	iii-43	「・情報セキュリティ専門人材によるインシデントの早期発見と対処」について「・情報セキュリティ専門人材または情報セキュリティ人材と同等の能力を有するソフトウェアによるインシデントの早期発見と対処」との変更を提案します。	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
46	個人	第3編	iii -43	都道府県の調達するセキュリティクラウドに対して外部監査を義務付けるべきと考えます。	都道府県に対しては、標準要件を示し、適切に標準要件が遵守されるよう取り組んで参ります。
47	個人	第2編	iii-45	「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。」について「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、自動的に早期対処する仕組みを構築する必要がある。」との変更を提案します。	今後の検討の参考にさせていただきます。
48	法人	第3編	iii-45~iii-49	β/β'モデルにおけるセキュリティ対策について、端末内でのアプリケーション仮想化技術（ハイパーバイザ型あるいはコンテナ型）を活用することで、さらにセキュリティ、利便性、運用性の向上につながるといえます。	今後の検討の参考にさせていただきます。
49	個人	第3編	iii-46	図表にて「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、ファイアウォールでMACアドレスを用いた通信先限定はできません。一方中継サーバではFQDNによる制限が可能であるため、MACアドレスを削除しFQDNを追加すべきと考えます。	「中継サーバやファイアウォール等」となっているため、ファイアウォールで限定した記述ではございません。また、同様に、「通信ポート、IPアドレス、MACアドレス等」と記載しており、FQDNによる制限も含まれます。
50	個人	第3編	iii-46	図表にて「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」とありますが、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します。 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り、無差別なクリップボード禁止はただ正規のユーザーの業務効率を下げる効果しかありません。 コピー&ペーストのリスクは「テキスト以外のファイルを転送できてしまうと無害化されていないファイルが転送されてしまうこと」のみにあるため、ファイルとテキストを的確に区別し、テキストデータに限りコピー＆ペーストを認めるべきと考えます。	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
51	法人	第3編	iii-46 iii-48	β/β'モデルで、インターネット接続系からLGWAN接続系を利用する場合、情報セキュリティの観点では、 1.LGWAN接続系の情報をインターネット接続系へ持ち出さないこと 2.インターネット接続系のデータを無害化通信を除いて、LGWAN接続系へ転送しないこと が重要と認識しております。(αモデルのLGWAN接続系からインターネット接続系を利用するのと反対のケース) また、 β/β'モデルは、各端末でのセキュリティ対策等、インターネットからのリスク増加への対策も必須となっています。 このことから、上記の 1. に関して、LGWAN接続系の利用については、「画面転送」以外の方式も選択肢としてもよいのではないでしょうか。例えば、テレワークセキュリティガイドラインに記載されている「セキュアブラウザ方式」「アプリケーションラッピング方式(コンテナによる分離)」など。	今後の検討の参考にさせていただきます。
52	法人	第3編	iii-46 iii-48	図表20（P46）並びに図表22（P48）内の必須のセキュリティ対策には、マネージドサービスを前提とした記載がありますが、加えて必須要件として、上記（注10）の記載事項を記載するべきと考えます。	今後の検討の参考にさせていただきます。
53	法人	第3編	iii-49	P49の（注10）の記載事項の一部は、内閣官房サイバーセキュリティセンターより公布された、平成30年度版「政府機関等の対策基準策定の為のガイドライン」にも具体例として記載がありエンドポイント防御の観点から非常に有効であると考えます。 β´モデルだけでなく、βモデルにも適用するべきと考えます。	ご指摘については、図表中の「未知の不正プログラム対策（エンドポイント対策）」に対する注意事項のため、β'モデルだけでなくβモデルも想定した記載となっております。
54	個人	第3編	iii-49	「相互の通信でインターネット回線を利用している場合、VPN 通信等を用いて、通信元と通信先が特定されており、通信経路が限定されていなければならない。ただし、原則はインターネット回線ではなく閉域網を利用すること。」 は、ここだけ他と文体が異なるため、前後の順番を入れ替えて 「原則としてインターネット回線ではなく閉域網を利用すること。インターネット回線を利用する場合、VPN 通信等を用いて、通信元と通信先が特定されており、通信経路が限定されるようにすること。」 とすることが望ましいと考えます。	ご指摘を踏まえ、記載を修正いたします。
55	個人	第3編	iii-50	③において、マイナンバー利用事務系でもLGWAN接続系でも各種更新プログラムをインターネットから取得することを禁じていますが、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、「やむを得ずインターネットからファイルを取得する場合は、WSUS等の専用の中継サーバーを設け、その中継サーバー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ーは当該目的のサーバー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。」といった内容を記載すべきと考えます。	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
56	個人	第3編	iii-50	「マイナンバー利用事務系では、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。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からのインターネット接続は認められない。 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インターネットに接続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なった上で、修正プログラムおよびパターンファイルの提供元として十分に安全性が確保された外部接続先と接続を行う。または、インターネット接続系に設置したプロキシサーバ(中間サーバ)との特定通信によるデータの取り込みを行う。」との変更を提案します。	今後の検討の参考にさせていただきます。
57	法人	第3編	iii-53	境界の安全性確保に依存する従来のネットワーク・セキュリティ対策を見直すことを推奨します。地方公共団体が採用すべき具体的なセキュリティ対策を規定するのではなく、様々な利害関係者間で基準となるセキュリティ／プライバシーへの責任の在り方を推奨する、原則ベースのガイドライン策定に注力することを提案します。また、ガイドラインの中で、地方公共団体には、その管轄区域のニーズとリスクプロファイルに最適な情報セキュリティポリシーを企画・実施する自律性があることを明確にすることを推奨します。 さらに、「第3編　第2章　4.1（7）機器の破壊等」に記載されている、市民の個人情報を保存する機器の廃棄に関する詳細な対策の助言を改訂することを推奨します。記憶装置の物理的破壊や地方公共団体職員による現場監視の要件は、オンプレミスの IT システムを前提としています。地方公共団体によるクラウドコンピューティングの革新的活用に対応するために、本ガイドラインでは、詳細な媒体やデータの破棄方法を規定するのではなく、使用しなくなった場合にデータを復元できないようにすることに重点を置くべきです。したがって、暗号的消去（cryptographic erase）等のデータ消去方法を認め、データ復元を不可にする仕組みを明確にすることを推奨します。	「本ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したものである。したがって、本ガイドラインで記述した構成や例文は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げるものではない。」としております。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
58	法人	第3編	iii-56	マイナンバー利用事務系で利用していたシステム機器の廃棄について、規定的な措置をとらないよう求めます。マイナンバー利用事務系で利用していたシステム機器に関する「物理的な方法による破壊」「職員の立ち会いによる廃棄確認」といった要件は、オンプレミス利用を前提としたものと思われます。ガイドラインでは、具体的なデータ破壊の方法を書き下すのではなく、「データが復元不可能な状態」にするという原則の履行に重点を置くべきです。または、暗号化消去などの他のメディア廃棄の方法も列挙すべきです。加えて、職員の立ち会い要件については、暗号化消去を行ったことのログファイルの確認や第三者による廃棄確認証明など、職員の立ち合い以外による廃棄確認もガイドラインに盛り込むべきです。	情報システム機器の廃棄等については、「情報システム機器が不要になった場合やリース返却等を行う場合には、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。」といった原則を記載しています。 クラウドサービスを利用している場合は、暗号化消去（Cryptographic Erase）が可能なクラウドサービスの利用検討が考えられますが、クラウドサービスにおけるデータ消去の在り方ついては、政府でのクラウド活用に係る議論も踏まえ、今後検討していく予定です。 立ち会いによる確認を行う方法のほか、庁舎内において情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する方法についても記載しております。
59	地方公共団体	第3編	iii-56	分類の（１）、（２）、（３）のいずれにおいても「庁舎内において」とあるが、必要とされているのは場所ではなく、自治体の管理下から移動する前に、消去を行い、その消去を職員が確認することが求められていることと考えるため、「庁舎内おいて」という文言を削除いただきたい。	「庁舎内において」と記載しておりますが、確実に履行が担保されることが重要と考えており、各自治体において適切に判断することが必要と考えております。
60	地方公共団体	第3編	iii-56	分類の(2)にある、「一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である」とあり、具体例として①～⑤が例示されているが、この記載では、実際に委託事業者に委託する際の仕様書に記載しても、妥当かどうかが判断できないため、より具体的な記載いただきたい。 例えば、物理破壊とあるが、HDDであればプラッターに破損がなければ、磁気読み取りは可能とする話もあり、どこまで破壊すれば研究所で復元可能かが判断できない。	地方公共団体に対しては、「NIST SP800-88Rev.1」や「データ消去技術ガイドブック」、民間の消去ソフト、消去実施事業者認証等を紹介しており、自治体への情報提供を引き続き行って参ります。
61	地方公共団体	第3編	iii-56	調査や作業を委託するにあたり、事業者へ機密性の高い情報を貸与した場合については、事業者の消去報告や証明書によるものとし、機器の廃棄を求めないとする記述を新たに追記いただきたい。	ご指摘の記述は、自治体の管理する情報機器の廃棄等に関する記載となります。
62	法人	第3編	iii-56	4-1物理的セキュリティ（7）機器の廃棄等（※iii-56）における「職員の立ち合い」「庁舎内」に関して、実際の廃棄等の職員の立ち合いや廃棄等作業場所として庁舎内以外にも、遠隔監視等の仕組により同様のセキュリティが確保されると自治体が判断した場合、当該仕組を採用することは問題ないという理解でよろしいでしょうか。	確実に履行が担保されることが重要と考えております。遠隔監視等による履行の担保についても同様の考え方としており、各自治体において、適切に判断することが必要と考えております。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
63	個人	第3編	iii -56	マイナンバー利用事務系の領域において住民情報を保存する記憶媒体に関して、検討会の議事等も含め拝見しましたが、その物理的破壊を実施することとされた理由について明確に示されていないように感じます。2019年12月の神奈川県事案では、データ消去作業が実施されなかったことが要因であるところ、再発防止に物理破壊までを求める理由が示されるべきではないでしょうか。 コストのかかる対策項目であり、この点は各自治体においても十分な理解が必要であると考えます。	情報システム機器の廃棄等については、確実な履行を担保するための基本的な考え方として「ＯＳの初期化、および記憶装置の初期化（フォーマット等）による方法は、ＨＤＤの記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。」としています。 また、情報の機密性に応じた廃棄方法等の検討に当たっては、NIST等のガイドラインを参考にするとともに、有識者や自治体職員を交えた検討会において、整理を行ったものとなります。
64	個人	第3編	iii -56	個人情報保護の安全管理措置の規定が抽象的な場合など、整合性が不明確となり、情報廃棄の取扱いに混乱を生じることも想定されます。 今後、個人情報保護条例の2000個問題の解決を図る検討にあたっては考慮を要する点と思われます。	今後の検討の参考にさせていただきます。
65	個人	第3編	iii-85	「したがって、情報システムにおいては、仕様どおりにログ等が取得され、また、改ざんや消失等が起こらないよう、ログ等が適正に保存されなければならない。」について「したがって、情報システムにおいては、疑義に関連するログだけをフィルタリングせず仕様どおりにログが取得され、また、改ざんや消失等が起こらないよう、ログ等が適正に保存されなければならない。」との変更を提案します。	今後の検討の参考にさせていただきます。
66	個人	第3編	iii -86	特定用途機器のセキュリティ管理に関してIoT機器を含む記述として頂いた点は、自治体の理解も促進するものであり、また、昨今の対策必要性の高まりからも賛同します。 一方で、PC等と比して性能に劣る傾向やメンテナンス等管理の困難さといった特性を踏まるとともに、侵害時には実世界への誤ったフィードバックや重要な政策・意思決定をミスリードするなど、情報処理の範囲を超えた影響を及ぼす可能性がある、という観点から厚みを持たせた解説が必要ではないかと思います。	今後の検討の参考にさせていただきます。
67	個人	第3編	iii-88	「（注13）受信した電子メールをテキスト形式で～」の内容を記載する場所は、「(15)電子メールの利用制限」ではなく「(14)電子メールのセキュリティ管理」の方がより適切ではないでしょうか。	今後の検討の参考にさせていただきます。
68	個人	第3編	iii-88	「職員等が自由に暗号方法を利用」について、「暗号方法」の意味が解らないため、「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の「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。	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
69	個人	第3編	iii-104	「ウェブサイトを構築する場合は、「lg.jp」ドメインを含む属性型・地域型JPドメイン名の使用を調達仕様書に含める」とされていますが、以下のように修正してはいかがか。 「また、情報の提供、行政手続及び意見募集等の行政サービスのためにウェブサイト等を住民等向けに提供する場合は、そのサーバの設置場所が自庁内かクラウドかを問わず、提供するウェブサイト等が地方公共団体のものであることを利用者が容易に確認できるように、LG.JPドメイン名を利用すること。ただし、教育機関においてはED.JPドメイン名やAC.JP名ドメインを用いることが可能である。地域型JPドメイン名については当面利用しても良いものとするが、LG.JPドメイン名に移行することが望ましい。」	今後の検討の参考にさせていただきます。
70	個人	第3編	iii-104	「「lg.jp」ドメインの適用が困難なサービスを利用する場合は、そのドメインが団体のものとは異なることとその理由を団体のウェブサイトに掲示することが望ましい。」と記載いただきましたが、現在の記載内容は取り組み例の一つであるため、それにより達成する目標を併記することが望ましいと考えます。 例えば以下のような記載にすることが良いのではと考えます。 「「lg.jp」ドメインの適用が困難なサービスを利用する場合は、そのドメインが団体のものとは異なることとその理由を団体のウェブサイトに掲示する等により、ドメインは異なるが確かにその団体が提供するサービスであることを住民が確認できる状態とすることが望ましい。」	今後の検討の参考にさせていただきます。
71	法人	第3編	iii-106 iii-110 iii-115	次期自治体情報セキュリティクラウド要件において、EDR(Endpoint Detection and Response)監視/運用が要件概要・目的、詳細要件等に明記されています。 自治体における、EDRの導入は、自治体情報セキュリティクラウドと連携して行うことで、市町村から都道府県まで全体のセキュリティレベルを高めることが可能です。 今後5年間の自治体セキュリティを考える上で、重要な対策と考えられますので、EDR(Endpoint Detection and Response)監視/運用を明記することを提案いたします。 コロナ禍において、情報セキュリティ対策への予算配分の優先度が下がる傾向にあります。特に、過去に標的型攻撃を受けた可能性のある自治体を持つ都道府県は、サイバー攻撃の高度化により今後5年間、さらに厳しい標的型攻撃を受ける可能性が高いと予測しますので、注意喚起をしていただくことが重要と考えます。 「6.4. 不正プログラム対策」「6.5. 不正アクセス対策」「6.6. セキュリティ情報収集」の項に、「次期自治体情報セキュリティクラウドと連携してEDR監視/運用を行うことが必要である」という記述をご提案します。	次期自治体情報セキュリティクラウドの標準要件に記載しておりますので、原案のとおりとさせていただきます。ご意見は今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
72	個人	第3編	iii-109	「コンピュータウイルスに感染した兆候がある場合には、即座に LAN ケーブルを取り外す（パソコン等の端末の場合）又は通信を行わない設定への変更（モバイル端末の場合）を行い、被害の拡大を防がなければならない。」について。 自動化を取り入れない場合、全てを人的に対応することとなり多数のインシデントが発生した際に対処しきれません。その結果として、一時的に制限をかけるまでに時間を要し、情報漏えいにつながる恐れが極めて高くなります。自動化を検討すべき旨をガイドラインで明記し、周知する必要があると考えます。 当該部分について「コンピュータウイルスに感染した兆候がある場合には、即座に LAN ケーブルを取り外す、もしくは自動的に論理的なネットワーク隔離を行う（パソコン等の端末の場合）又は通信を行わない設定への変更、もしくは通信を行わない設定への自動的な変更（モバイル端末の場合）を行い、被害の拡大を防がなければならない。」との変更を提案します。	ご指摘を踏まえ、記載を修正いたします。
73	法人	第3編	iii-119	7.1. 情報システムの監視について、 ウェブサイトの常時TLS（SSL）化による暗号化された通信の脅威検知をおこなうため、当該通信データを復号し脅威の検査を行い再暗号化する機能を導入しなければならない。本要件は【推奨】となっておりますが、【必須】が望ましいと考えます。 ウェブサイトの常時暗号化（TLS（SSL）化）は、盗聴、改ざん、なりすましなどウェブサイトにアクセスする際のセキュリティ機能として急速に進展し、今日ではすでに96%の通信が常時TLS(SSL)化されている状況です。 常時TLS（SSL）化は、プライバシー保護やコンプライアンスに有効な一方、当該通信に潜む脅威の検知が困難となるという大きなリスクを抱えています。 攻撃者は常時TLS（SSL）化による脅威の検査ができない事実を悪用し、ユーザーの端末にマルウェアを送り込んだり、侵入したマルウェアがC&C（Command and Control）サーバーと通信を行いセキュリティ検査を回避する攻撃が可能となります。 そのため、ウェブサイトの常時TLS(SSL)化を可視化する対策として、SSL復号化機能を実装したセキュリティ機器の設置は【必須】が望ましいと考えます。 TLS（SSL）通信を可視化しセキュリティ検査を行うことにより、マルウェアの侵入や不正アクセス、データ漏洩などのセキュリティ対策を高めることが可能となります。	自治体からの意見を踏まえ、推奨とさせていただいております。今後の検討の参考にさせていただきます。
74	個人	第3編	iii-132	「・セキュリティインシデントへの対処方法」について「・セキュリティインシデントへの対処方法（脅威の除去及び環境の復旧代行）」との変更を提案します。	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
75	法人	第3編	iii-136	クラウドサービスにおいては、多数の利用者に対して同様のサービスを継続的に提供するものであるため、その構成する機器やシステムについての改善変更についても、ある利用者にとってはその契約期間中に改善変更がなされることがありうる。クラウドサービスは契約時の構成を一切変更するものではなく、このように継続的に改善変更を行っていくのが通常である。このクラウドサービスの性質に鑑みれば、一切の情報システムの変更についてクラウドサービス提供事業者に対して報告義務を課すのは現実的でないと考えます。そこで、クラウドサービス提供事業者はその情報システムを契約時に表明した基準（ISOやCSゴールドマーク等の基準、認証を参照して契約時に合意することを想定）を保持した上で変更できるとすべきと考えます。	本記載については、情報セキュリティ対策を実施するためには情報システムの状態を正確に把握する必要があることから、情報セキュリティ関連文書の内容を最新に保つために当該文書で管理している項目について報告を求めることが重要であることを踏まえ、「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」の記載を参考に追記を行ったものとなります。
76	法人	第3編	iii-141	第３編第2章の「5 人的セキュリティ」、「7 運用」のそれぞれの冒頭に、「クラウドサービスを利用する場合には、本項及び「8.4クラウドサービスの利用」を踏まえて確認・検討すること」といった文言を追加することを求めます。 同「4 物理的セキュリティ」及び「6 技術的セキュリティ」においては、「本項において、特にサーバ及び管理区域に関する部分の取扱いについては、主にオンプレミスの場合を想定している。クラウドサービスを利用する場合には、「8.4クラウドサービスの利用」を踏まえて確認・検討すること。」といった文言を追加することを求めます。 「第３編第2章 6 技術的セキュリティ」において、今回の見直しにより追加された「なお、近年のITの利活用拡大により、システムで使用しているソフトウェア等の種類も増加していることから、IT資産を手作業で漏れなく正確に把握するには多大な労力が必要となる。そのため、自動でソフトウェアの種類及びバージョンを管理する機能を有するIT資産管理ソフトウェアを導入することが考えられる。」と記す点については、クラウドサービスのマネージドサービスの活用も有効な解となりうる旨を併記すべきと考えます。	クラウドサービスの利用については、新設の「8.4 クラウドサービスの利用」を参照することが明らかであるため、原案のとおりとさせていただきます。
77	個人	第3編	iii-141	IaaS、PaaSに関する記述であること、明記すべきではないでしょうか。 SaaSは、基盤部分を含む流通経路を俯瞰することは困難のため、事業者の安全性が確保されていると判断できる場合は、この限りではないと考えるためです。	本記述は、「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」等を参考に記載しておりますが、SaaSについても総合的に対策を設計（構成）した上で、セキュリティを確保する必要があると考えます。
78	個人	第3編	iii-141	「クラウドサービス」はその多くが「約款による外部サービス」でもあると考えられますが、そうであることが一見解りにくいとともに、両社の違いが不明瞭であるという課題もあります。両者の関係性と違いを理解できるよう、本ページまたはiii-152において「クラウドサービス」の定義付けが必要と考えます。	ご指摘を踏まえ、記載を修正いたします。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
79	法人	第3編	iii-142	「クラウド・バイ・デフォルト」原則に基づくガイドラインの見直しを歓迎する一方、クラウド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 CSP の利用を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、データセンターの場所は、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、重複的に保存することでレジリエンス（回復力）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 G20 大阪トラックの主要な基本概念として提唱した「データ・フリー・フロー・ウィズ・トラスト（DFFT）」とはっきりと合致しています。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が損なわれる可能性があるのです。 以上を踏まえ、以下のように修正することを求めます。 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. 外部サービスの利用 8.4. クラウドサービスの利用 「② 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。また、データ保全、災害対策等の観点から、海外にバックアップ用のデータセンターを持つことも考慮する必要がある。」	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運用できるデータセンターを選択する必要があると考えております。ご意見については、今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
80	法人	第3編	iii-142	「日本の法令の範囲内で運用できる」という基準は、明確でない部分があり、また確認が困難な場合があると思料します。国外法が適用される可能性がない」と言い切ることはほとんどの大手クラウドサービス提供事業者にとっては難しいのではないかと懸念いたします。 そこで、不明確さのある、また保証することが困難なことも考えられる「日本の法令の範囲内で運用できる」という要件に代えて、明確な基準であるデータセンターの所在地要件と、「政府情報システムにおけるクラウド設置場所等に関する考え方」における要件を考慮し、「住民情報等の機密性の高い情報を蓄積する場合は、国内法・国外法が適用されるリスクについて検討の上、日本国内のデータセンターを選択する必要がある。ただし、海外に所在するデータセンターを利用する場合でも、データの保存性、災害対策等からバックアップ用のデータセンターが海外にあることが望ましい場合、又は争訟リスク等を踏まえ海外にあることが特に問題ないと認められる場合はこの限りではない。」とすることを提案いたします。	本記載については、改定以前のガイドラインにおいても8.1 外部委託（注7）に記載のあった内容であり、今回は原案のとおりとさせていただきますが、ご指摘も踏まえ、今後の検討の参考にさせていただきます。
81	法人	第3編	iii-142	原案ですと、支部含めて全国約250の裁判所に合意管轄が生じうることになりますが、全国の自治体に対してサービスを提供するクラウドサービス提供事業者にとっては、そのような対応は難しく、通常は契約において専属的合意管轄裁判所をひとつに定めていることが通常と思われます。重要なことは、万一の場合に裁判管轄が国外の裁判所とされることなく、日本の裁判所において裁判を受ける権利が保障されることであると存じます。 そこで、「管轄裁判所に関しては、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を合意管轄裁判所として規定する必要がある」とすることを提案いたします。	ご指摘を踏まえ、記載を修正いたします。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
82	個人	第3編	iii-142	クラウドサービスを利用するにあたっては、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運用できるデータセンターを選択する必要があることは記載の通りと考えます。一方、機密性が低い領域かつ国民の利便性の向上に寄与するサービスであれば、リスクや対策を考慮・加味した上でインターネットを介したクラウドサービスの積極的利活用を促すことで、地方自治体様におけるサービスの選択肢に幅をもたらすことが可能と考えます。 結果として、地方自治体様は様々なサービスを検討し、住民にとってより良い行政サービスを低コストで提供できる機会が増えると考えます。	「オープンデータ、環境計測値等の機密性の低い情報をクラウドサービスに蓄積する場合は、どの国の法令が適用されるのかを確認し、リスク等を考慮した上で選択することが望ましい。」としております。ご意見は今後の検討の参考にさせていただきます。
83	個人	監査ガイドライン	P.5、25	外部監査を義務付けるべきと考えます。 監査記録の公開を義務付けるべきと考えます。	ガイドライン上、「毎年度及び必要に応じて監査を行わせなければならない。」と記載しております。ご意見については、今後の検討の参考にさせていただきます。 「情報セキュリティ監査の結果については、行政の透明性確保、住民に対する説明責任遂行の観点からは積極的に公開することが望まれる。」「他方、情報セキュリティ監査の成果物には、情報資産やネットワーク及び情報システム等の脆弱性に関する情報が含まれており、情報セキュリティ確保の観点からは、全てを公開することは適当ではない場合もある。」「したがって、一律に公開、非公開とすることはいずれも適当ではなく、各地方公共団体の制定する情報公開条例の「不開示情報」の取扱いなどを踏まえ、適切な範囲で公開していく必要がある。」と考えております。ご意見については、今後の検討の参考にさせていただきます。
84	個人	その他	全般	ガイドラインは、自治体各々が判断可能な領域についての参考として示し、各自治体の自主性のもと、各々のセキュリティポリシーが策定されるものではないでしょうか。	「本ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したものである。したがって、本ガイドラインで記述した構成や例文は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げるものではない。」としております。
85	個人	その他	全般	クラウドサービスに関して、セキュリティ監査等の観点で求める参考の国際規格として、8.1項ではISO27001が示されているが、8.4項ではISO27017となっており、整合しないように読めます。	第8.1項ではセキュリティの汎用的な規格としてISO27001を参照としていますが、一方で第8.4項はクラウドサービスの利用に特化した規格としてISO27017を参照としています。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
86	地方公共団体	その他	全般	強靭化の見直しにおいて提示されたβモデル、β'モデルにおいてもパブリッククラウドの利用が提示されている。また、Web会議サービス、ソーシャルメディアサービスによる情報共有や研修など、多種多様なクラウドサービスが提供されている。 一般的に、パブリッククラウドで提供されるサービス利用する場合、必要となる情報資産（データやファイルなど）はパブリッククラウド上に保存（または一時的に保存）されるため、パブリッククラウド上のサービスを利用する場合は、情報資産（データやファイルなど）が、パブリッククラウド上に保存（一時保存含む）されるが、セキュリティ要件を担保する手段がない。 βモデル、β'モデル、Web会議などクラウドサービスや約款による外部サービス利用について、自治体が順守すべき一定の利用基準が必要と考えるため、ガイドラインにおいて提示いただきたい。	「8.4. クラウドサービスの利用」の項目を新設しております。ご意見については、今後の検討の参考にさせていただきます。
87	地方公共団体	その他	全般	地方公共団体がパブリッククラウド利用に当たり参考とできるように、ISMAPを地方公共団体が活用できるようにしていただきたい。	ISMAPの自治体への活用については、政府全体での検討も参考にしつつ、引き続き検討して参ります。
88	法人	その他	全般	各府省等を対象にしている「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 」に則り、地方公共団体版のクラウド・バイ・デフォルト原則を策定すべきだと考えます。マイナンバー利用事務系を含めてクラウド活用を原則とし、この考え方をもとに改めてガイドラインを見直すべきと考えます。また、総務省は、政府情報システムのためのセキュリティ評価制度（ISMAP）を、地方公共団体のクラウド調達の際の基準として採用すべきと考えます。地方公共団体におけるクラウド利用の前提として、LGWANをベースとしたITシステムと、クラウドベースのシステムとのコスト比較を行うべきです。 ガイドラインを内閣サイバーセキュリティセンター（NISC）やデジタル庁準備室などによる政府のデジタル化の取組と整合させていくべきと考えます。総務省は、国におけるクラウドを活用したデジタル基盤の整備に合わせて、ガイドラインを適時、継続的に見直し、改訂すべきです。	総務省では、これまでも「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」等を参考に、ガイドラインの見直しを行ってきたところですが、今後も政府全体の取組を踏まえ、適時適切に見直しをして参ります。
89	法人	その他	全般	総務省は、ゼロトラストなどの最新のセキュリティの考え方を地方公共団体における情報セキュリティ対策に活用するべきです。 地方公共団体がとるべきセキュリティ対策を具体的に規定するのではなく、情報セキュリティに関する原則を示したガイドラインとすることを求めます。また、総務省は、地方公共団体が地域のニーズに最も適した情報セキュリティポリシーを自ら計画・実行する権限を持つことをガイドラインの中で明確に記載し、実践すべきと考えます。 地方公共団体の情報セキュリティ対策を向上するため、国際的に認められた業界のセキュリティ基準や第三者監査の重要性を認識することを要望いたします。情報セキュリティを強化するためには、ISOやSOCなどの世界的なコンセンサスに基づいた業界標準やベストプラクティスに基づいたリスクベースのアプローチを活用していくことが重要と考えます。	総務省では、これまでも「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」等を参考に、ガイドラインの見直しを行ってきたところですが、今後も政府全体の取組を踏まえ、適時適切に見直しをして参ります。 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。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
90	法人	その他	全般	マイナンバー利用事務系とパブリッククラウドとを接続するためのセキュリティ要件をガイドラインにおいて明確化すべきだと考えています。 クラウドサービスにより、国際的に認められた暗号化や保存管理などの機能を活用し、最も安全なグローバルインフラの下でシステムを構築することで、機密性の高い個人情報を安全に取り扱うことが可能になります。進化し続けるクラウドサービスは、機密性の高い個人情報を保護するために最も効果的なデータセキュリティを提供することができます。	今回の改定では、「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」等を踏まえて、クラウドサービスの利用にあたってのセキュリティ確保に必要な事項等についても追記を行いました。ご意見については、今後の検討の参考にさせていただきます。
91	法人	その他	全般	新政権の主導の下でデジタルトランスフォーメーションが進められ、政府業務の高度化が図られる中、安全なクラウドサービスの取得と利用は、その実現に不可欠なものとなっています。この点において、本ガイドラインの見直しが「クラウド・バイ・デフォルト」原則に基づき、テレワークや行政職員の利便性向上を支援するために、以前よりもインターネット接続を可能とする新たな対策が示されたことを、我々は歓迎しています。また、地方公共団体において「クラウドネイティブ」アーキテクチャの方針を推進することで、各府省情報化統括責任者（CIO）連絡会議が中央政府向けに策定した方針 と、本ガイドラインとの整合性をより明確にできると考えております。つまり、地方公共団体がLGWANベースのシステムを実装するための総コストとクラウド導入の総コストをより適切に評価できるようにすることで、地方公共団体のクラウドアーキテクチャへの移行を促進することができるのです。	総務省では、これまでも「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」等を参考に、ガイドラインの見直しを行ってきたところですが、今後も政府全体の取組を踏まえ、適時適切に見直しをして参ります。
92	法人	その他	全般	マイナンバーを管理する情報システムの保護の必要性を十分認識しつつ、我々は、クラウドコンピューティング・ソリューションの導入を阻害したり、そのメリットを不必要に損なわずに、地方公共団体におけるセキュリティ対策や指針を貴省が継続して見直していくことを奨めます。クラウドサービスは、最も安全なグローバル・インフラの下でシステム構築をしながら、暗号化やストレージ管理など、国際的に認められた機能を活用することで、機密性の高い個人情報を安全に取り扱うことを可能にします。進化し続けるクラウドサービスの性質が、機密な個人情報を守るための最も効果的なデータセキュリティ提供を可能とするのです。 このような視点から、現行のLGWAN対策を修正し、クラウドのこうした特徴を活かして、LGWANとインターネット接続系の情報システムの分割をしないことを求めます。	今回の改定においては、セキュリティを確保しつつ、効率性・利便性の向上を図るようLGWAN接続系とインターネット接続系の分割の見直しを行うこととしておりますが、今後も政府全体の取組を踏まえ、適時適切に見直しをして参ります。
93	法人	その他	全般	セキュリティへの対応は、技術の進歩を反映して急速に進化しています。データ・セキュリティのベスト・プラクティスは、リスクベース、セキュリティ成果指向、多層防御、ゼロトラスト・セキュリティ・アーキテクチャといったアプローチを採用しています。これらは、高度なユーザーID管理や限定的なアクセス、常時安全な仮想プライベートネットワークやネットワーク・セグメンテーションのネットワーク制御、強力なデータ暗号化の実装により可能となります。我々は、貴省が今後も本ガイドラインの見直しを継続し、現在の技術により適合したセキュリティ・ソリューションを採用し、規定的な要件でなく、多層防御の原則に基づく、リスク管理されたコントロールとベスト・プラクティスを重視した、安全なクラウドサービスの取得と利用を通じて、政府の業務をより効果的に推進することを奨励します。	今後の検討の参考にさせていただきます。

No	提出者分類	該当箇所	該当ページ数	意見	意見に対する考え方
94	法人	その他	全般	昨今のサイバー攻撃は新型ランサムウェアやEmotetなどように、侵入と同時に実害が発生する攻撃が多く、攻撃の痕跡から被害個所の特定や対処を開始するまでには被害が拡大してしまう傾向にあります。 現在の検知技術には限界がある為、不正プログラムの活動を未然に防ぎ攻撃完遂を阻止する機構を防御方法に取り入れる事でセキュリティ対策の強化を行えると考えます。 副次的に、事故発生の抑制により有事対策に掛かるコストの低減を図る事が出来ると考えます。	今後の検討の参考にさせていただきます。
95	不明	その他	全般	危険因子という文言があるが、危険因子として認定できる要件はどのようなものか。	危険因子とは、マルウェア等を想定しており、網羅的に要件を示すことは困難ですが、下記のような挙動を示すものが危険因子の一例として考えられます。 ・ウイルス対策ソフトウェアの警告 ・予期しないダイアログボックスが表示され、なんらかの操作の許可を要求される 参考：NIST SP800-83(2005/11)「表 4-2. マルウェアと考えられる兆候」 なお、危険因子は様々な挙動を示すことから、サンドボックスや振る舞い検知などを利用し、不審なファイルを検知、除去することが重要と考えております。
96	不明	その他	全般	βモデル又はβ'モデルを採用する際に外部監査として必要な要件はどのようなものか。	「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」に記載しておりますので、ご参照ください。
97	不明	その他	全般	機器の廃棄において、マイナンバー利用事務系において、機密性2以上の対策を講じる必要性は妥当であるか。妥当であれば、機密性2以上の対策は十分であるのか疑問である。	今後の検討の参考にさせていただきます。
98	不明	その他	全般	リース満了後の機器の廃棄において、機密性2以上の場合でも場合によっては破壊の選択肢があるため、同様に契約に含める必要があるのではないか。	今後の検討の参考にさせていただきます。
99	個人	その他	全般	セキュリティ担保のためには、日本国籍所有者に管理や実務を限定することとソフトウエア等に中国製や韓国製のものを避けることも重要と考えています。	今後の検討の参考にさせていただきます。
100	不明	その他	全般	e-Govの「受付締切日時」欄の「23日0時」は誤記ではないのか？　意見募集要領の「4 意見募集期間」には「22日22時」と記載されているから。 e-Govの「意見提出が30日未満の場合その理由」欄に記載がないが、本件の意見募集期間を30日未満とした理由は何か？	本件は、行政手続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。

※とりまとめの都合上、類似の意見は整理した上で掲載しております。