参考資料

「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」改定に対する地方公共団体への意見照会結果

総務省

2021年12月20日

地方公共団体の情報セキュリティポリシーに関するガイドラインの改定等に係る検討会

「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」改定に対する地方公共団体への照会結果

意見照会の概要

【照会対象】全ての都道府県及び市区町村（1,788団体）

【照会期間】令和３年11月22日（月）～令和３年12月6日（月）

分類（改定のポイント）	意見	質問	合計
1-①.外部サービスの再定義	18	16	34
1-②.外部サービス利用時のセキュリティ要件	24	31	55
1-③.クラウドサービス選定の指標・基準等	21	11	32
2.情報セキュリティ対策の動向を踏まえた記載の充実	13	9	22
3-①.テレワーク実施時のセキュリティ対策	4	2	6
3-②.BYOD利用時のセキュリティ対策	4	0	4
3-③.Web会議サービス利用時のセキュリティ対策	11	8	19
4.マイナンバー利用事務系から外部接続先へのデータのアップロード	19	17	36
今回改定範囲外	33	6	39
その他	11	5	16
合計	158	105	263

「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」改定に対する地方公共団体への意見照会結果（意見）

項番	対象資料	対象ページ	意見分類	御意見
1	ガイドライン改定案	iii - 142	１-①.外部サービスの再定義	ガイドライン改定に伴い、各自治体で整備が必要となる「外部サービス利用判断基準」の雛形やサンプル等をご提示いただけると幸いです。
2	ガイドライン改定案	iii - 141	１-①.外部サービスの再定義	改定案では、「民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、（中略）原則として機密性２以上の情報を取り扱うことはできない」と記載されている。（iii - 141） だが、すでにいくつかの自治体では「約款による外部サービス」を用いた機密性２以上の情報を取り扱う行政サービスを導入していると聞くため、例外事例を例示することにより、例外事例に対する一定の基準を示してほしい。
3	ガイドライン改定案	iii -46	１-①.外部サービスの再定義	セキュリティ対策の中でエンドポイント対策（EDR）について言及した記述があるが、EDRという名前を名乗れば何でもOKの状態になっているため、そのあたりの条件を明確化してほしい。
4	ガイドライン改定案	iii - 141	１-①.外部サービスの再定義	【趣旨】には「画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、・・・原則として機密性２以上の情報を取り扱うことはできない。」とあるが、本文中ではこの記述が全くないため、本文のみ見た場合には機密性２以上の情報が扱えるものと読めてしまう。本来、このような重要なことを趣旨のみに書くことに違和感を覚える。また、「原則として・・・できない」となっているが、Googleやマイクロソフトといった世界規模でサービスを展開している企業と個別に利用に係る契約を締結することは非常に困難であると思われるため、約款による外部サービスにおいても一定の条件を満たせば機密性２以上の情報を扱えることとし、どのような条件を満たせば例外として機密性２以上の情報が扱えるか具体的に示していただきたい。
5	ガイドライン改定案	Ⅲ-141	１-①.外部サービスの再定義	基幹システム等で利用が想定されるクラウドサービス及びホスティングサービスとWeb会議サービス、ＳＮＳ及び検査サービスでは、サービス提供事業者との契約における自由度に相当程度差異があり、同等に取り扱うことは無理があるのではないか。
6	ガイドライン改定案	iii-141	１-①.外部サービスの再定義	約款による外部サービスにおいて、機密性２以上の情報を取り扱うことはできないとする記載について、約款による外部サービスに該当するサービスは無料のオンラインストレージやLINE、Youtube、Web会議など多岐に渡り、既に業務に組み込まれているサービスも多く、一律に禁止とすると業務への支障が懸念される。そのため、「機密性２に該当する情報のうち、行政機関の保有する情報の公開に関する法律第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報」以外は取り扱ってもよいとする等、一定の条件の下で機密性２に該当する情報の一部についての取り扱いを認める基準を示してほしい。
7	ガイドライン改定案	iii - 141	１-①.外部サービスの再定義	「外部サービスの利用に係る規定の整備」において、様々な要件が規定されているが、具体な要件を策定することは専門的な知識のない自治体職員には困難である。そのため具体的な要件を示していただきたい。
8	ガイドライン改定案	ⅰ -3、ⅱ -46、iii -135	１-①.外部サービスの再定義	8.節の表題が「外部委託」とされているが、クラウドサービスなどの利用において、予算上及び契約上では運用・保守も含めて「委託」ではなく「サービス利用」としていることが多い。項目の立て方として「8.　外部委託」の下に「8.2　外部サービスの利用」を位置づけるのは混乱を招くと考えられるため、8.節の表題を例えば「8.　業務委託と外部サービスの利用」などとしてはどうか。

項番	対象資料	対象ページ	意見分類	御意見
9	ガイドライン改定案	iii -147	1 -①.外部サービスの再定義	「SLAを締結する必要がある」との一文があるが、「SLA」とは何のことかが文中にも巻末の用語の定義にも説明が無いため、「SLA＝サービス品質保証（Servive Lebel Agreement）」であることの説明がどこかに欲しい。
10	改定のポイント	7	1 -①.外部サービスの再定義	機密性２以上の情報を取り扱う場合、利用部門ではなく、統括部門に利用申請するのか。この場合、同じサービスの利用であっても機密性２以上の情報の取り扱い有無により申請先が変わり運用が難しい。利用申請先は利用部門に統一してほしい。
11	改定のポイント	3	1 -①.外部サービスの再定義	外部サービスの利用について、「機密性２以上を取り扱う場合」と「機密性２以上の情報を取り扱わない場合」で分類されていますが、「機密性２以上を取り扱う場合」として記載されている内容は非常に厳格な基準となっており、取り扱う情報が機密性２以下のみである場合にも適用することは実務上困難であることから、分類の基準を「機密性３を取り扱う場合」と「機密性３の情報を取り扱わない場合」にしてほしい。 （補足） ・現行のガイドラインの機密性の定義に照らし合わせた場合、行政で取り扱うほぼ全ての情報が機密性２以上に該当するため、今後外部サービスの利用が更に拡大していくことを踏まえると、一律的に「機密性２以上」に適用すると実際の運用との乖離が発生してしまうことを懸念しています。 ・セキュリティマネジメントの観点からも、市民の個人情報や入札予定価格等のような「機密性３（秘密文書に相当する情報資産）」と、その他の一般的な文書等の「機密性２（秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産）」の間には、取扱いに差を設けることが望ましいと考えます。
12	改定のポイント	P4	1 -①.外部サービスの再定義	「外部サービス」の具体例に情報流出で問題となった「情報共有ツール」や、「大容量ファイル交換サービス」が無いため追加してはどうか。
13	ガイドライン改定案	iii-141	1 -①.外部サービスの再定義	＜外部サービスの例＞に情報流出で問題となった「情報共有ツール」や、「大容量ファイル交換サービス」が無いため追加してはどうか。
14	ガイドライン改定案	ii -46	1 -①.外部サービスの再定義	昨今の委託先事業者におけるランサムウェア感染事案は「情報システムの開発、構築及び運用業務」の業務委託ではなかったため、業務委託には「業務運用支援務業務、プロジェクト管理支援業務、調査・研究業務」等を含むことを、業務委託の定義として記載してほしい。
15	ガイドライン改定案	ii -46	1 -①.外部サービスの再定義	8.1(１) 外部委託事業者の選定基準については，以下の文言（下線部分）を追加して記載してほしい。 ①情報セキュリティ管理者は、外部委託事業者の選定にあたり、委託事業者からの住民の個人情報等の流出を防止するため、委託内容及び取り扱う情報の重要性に応じた情報セキュリティ対策が確保されることを確認しなければならない。

項番	対象資料	対象ページ	意見分類	御意見
16	ガイドライン改定案	ii -46	１-①.外部サービスの再定義	8.1(２) については，以下のとおり，文言（下線部分）を追加・修正して記載してほしい。 8.1(２) ~~契約項目~~外部委託先における情報セキュリティ要件 情報システム管理者は，~~情報システムの運用、保守等を~~業務委託する場合には、委託内容及び取り扱う情報の重要性を踏まえ，外部委託事業者との間で必要に応じて次の情報セキュリティ要件を調達仕様書又は契約書に明記~~した契約を締結~~しなければならない。 ・情報セキュリティポリシー及び情報セキュリティ実施手順のうち委託業務に関連する事項の遵守 ・外部委託事業者の責任者、委託内容、作業者の所属、作業場所の特定 ~~・提供されるサービスレベルの保証~~ （理由） ・情報セキュリティ要件は，契約書よりも調達仕様書に記載するケースが多いため。 ・業務委託は，「情報システムの運用，保守」に限定されないため。 ・情報セキュリティポリシー及び情報セキュリティ実施手順の「全て」を，外部委託事業者に遵守させることはできないため。 ・サービスレベルの保証は，外部サービスの利用の章で規定されているため。
17	改定のポイント	3	１-①.外部サービスの再定義	「…（従来の「約款による外部サービス」）については、…要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として機密性２以上の情報を取り扱うことはできない」旨の記載があるが、この部分の記載について再検討を行う必要があるのではないか。（仮に画一的な約款や規約等であっても、当該規約等がポリシーで定める要件を満たしていることを確認できるのであれば、取扱が可能となるケースはあり得るものと思われる。また、これまでの原則（個別契約要）の考え方を維持することが実態と整合しているのか否かといった点を含め、検討が必要と思われる。）
18	ガイドライン改定案	iii -141	１-①.外部サービスの再定義	「原則として機密性２以上の情報を取り扱うことはできない」旨の記載があるが、この部分の記載について再検討を行う必要があるのではないか。（仮に画一的な約款や規約等であっても、当該規約等がポリシーで定める要件を満たしているのであれば、取扱が可能となるケースはあり得るものと考えられるため。）
19	ガイドライン改定案	iii -143	１-②.外部サービス利用時のセキュリティ要件	「②情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。」の記載について、AWSやMicrosoft365等のような利用形態が約款によるものについては、外部サービス提供者と自治体間で個別に契約書を交わすことが現実的には困難と思われるため、「②情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認すること。また、調達仕様の内容を契約に含めること（ただし、約款や規約等への同意により利用可能な外部サービスであり、個別に契約書等に行うことが困難な場合については、この限りではない。）。」といった記載内容に変更してほしい。
20	ガイドライン改定案	iii - 153	１-②.外部サービス利用時のセキュリティ要件	（６）外部サービスを利用した情報システムの更改・廃棄時の対策　について、別項目の情報廃棄の基準を参照する記載となっているが、「 2. 情報資産の分類と管理（２）情報資産の管理 ⑩情報資産の廃棄」や「 4.1. サーバ等の管理（７）機器等の廃棄」については、従来よりオンプレミス方式やデータセンター利用の形態においてはハウジング方式といった、システム利用側が機器を占有している方式が想定のものと理解しています。 現在のクラウドサービスでは、仮想サーバのリソースを払い出して利用する方式(IaaS)や、開発プラットフォームとしての形態（PaaS）、業務機能自体のサービス提供（SaaS）といった、利用側ではハードウェアを意識しない形態が想定され、近い将来、自治体システムが移行を進めて行くガバメントクラウドにおいてもそうした機能が要件となっている認識です。 こうしたクラウドサービスを利用するにあたっては、各利用団体が利用終了するタイミングでの物理破壊は困難であり（PaaS/SaaSにおいては論理消去も困難な可能性）、また、たとえ占有機器を利用する方式においても立ち会い等まで行えない可能性があります。 このため、現在の案でセキュリティポリシーガイドラインとして盛り込んだとて、従来方式のみでのクラウド活用に留まるどころか、立ち会い等で現実的ではない規定とならないか危惧されます。今後、ガバメントクラウド上でシステムを提供する事業者側での検討要素にもなってくるため、この点の早期の明確化をお願いします。

項番	対象資料	対象ページ	意見分類	御意見
21	改定のポイント	6～9	１-②.外部サービス利用時のセキュリティ要件	CISOが「外部サービス（機密性２上の情報取り扱う場合）利用に関する規定を整備」することとあるが、各自治体で一から作成すると事務負担やガイドライン準拠まで相当の時間がかかることが予想されるため、ガイドライン改正にあわせて参考となる例文等を提示いただきたい。 下記についても同様 ・外部サービス利用して情報システム運用する際のセキュリティ対策 ・外部サービス利用して情報システム構築する際のセキュリティ対策 ・利用を終了する際のセキュリティ対策 ・外部サー ビスに係るシャドーIT 対策
22	ガイドライン改定案	iii-142	１-②.外部サービス利用時のセキュリティ要件	8.2 (2) 外部サービスの選定 ②(エ)外部サービス提供者の資本関係・役員等の情報、外部サービスの提供が行われる施設等の場所、外部サービス提供に従事する者の所属・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外部サービスの提供が行われる施設等の場所については、セキュリティの観点から公表されていない場合が多く、情報提供を求めることは難しいと考えます。「調達仕様にてリージョンを指定する」等に置き換えてはいかがでしょうか。 また、サービス提供において従事者の情報を求めることは困難と思われます。 いずれも、ほとんどのサービス提供事業者が調達仕様を満たせないことが予想されることから、記載の見直しが必要と考えます。
23	ガイドライン改定案	iii -49	１-②.外部サービス利用時のセキュリティ要件	「（注１０）未知の不正プログラムへの対策（エンドポイント対策） 未知の不正プログラム対策として、OS のプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、不審な挙動を示す端末のホスト名や IP アドレスなどの情報 をログとして取得し、管理者へ通知する必要がある。」はセキュリティ対策が不十分なため、この一文に「また、従来のセキュリティ対策ソフトと同様、偽装や隠蔽、セキュリティソフトの停止や削除などにより検出を回避するような攻撃者の挙動に対しても、十分に対策を行う必要がある。」を追加して欲しい。
24	ガイドライン改定案	iii -49	１-②.外部サービス利用時のセキュリティ要件	ガイドライン案では、セキュリティ対策が不十分であるため、「単純な未知の不正プログラムへの対策を定義するだけでは、職員が対処切れない数のインシデントを常に対応することになり、忙殺されてしまい、本来の緊急度が高いインシデントに対して、正確で迅速な対処ができず、セキュリティ事故が発生する可能性を上げてしまいます。多くの不正プログラムはパターンマッチングでは排除できない、既知のツールを使ったものが多いため、攻撃手順などから脅威と判断する必要がある。以下のような未知の不正プログラムへの対策（エンドポイント対策）の在り方を定義して、セキュリティ自体の質と職員の運用負荷の低減を実現すべきだと考えます。 ・マルウェアに感染しないように、脆弱性・設定ミスを統制・可視化するようにして予防フェーズを徹底する。 ・既知ツールを使った既に判明済みの振る舞いを検知して自動的に排除(NGAV Next Generation Anti Virus 等)することで、インシデント対処数を低減する。 ・端末の統制管理に、段階的な自動化の仕組みを導入して、利用者と管理者の負荷を下げるようにする。 ・検知から最終的な対処までの間に、一時的対処を自動的におこなうような仕組みの奨励。」 を追加してほしい。

項番	対象資料	対象ページ	意見分類	御意見
25	ガイドライン改定案	iii -49	1 -②.外部サービス利用時のセキュリティ要件	インターネット接続の手法は、定義しなければ、各自治体の独自の判断でリスクのある接続方法が取られてしまう可能性がある。 ランサムウェアのような情報漏えいが目的でないタイプのマルウェアについては、インターネットに接続していることは必要ない。つまり、LGWAN接続系のセグメントにおいても、このような脅威は無視できない。 これらに対して最新の脅威対策をするには、インターネット上から最新の脅威情報を取得する必要がある。そのため、LGWAN接続系から脅威情報・対策の情報を取得するためのインターネット通信を特定通信と許可する必要があると考えます。
26	ガイドライン改定案	iii - 141 ～iii - 154	1 -②.外部サービス利用時のセキュリティ要件	「外部サービスの利用に係る規定の整備」のための、規定例（ひな形）を参考として提示してほしい。併せて、外部サービス利用判断基準・選定条件の観点やチェックリストも提供していただきたい。解説に「以下を含む内容を規定すること」といった文言はあるが運用における具体的な文章に落とすには確認観点が抽象的という印象を受ける。 団体の規模やセキュリティポリシー、扱う情報によって規定や判断基準が異なってくることは致し方ないと考えるが、あまりにも団体ごとに選定条件や判断基準がバラバラだと一定水準の情報セキュリティの維持が難しくなるため、確認観点や確認結果に対する考え方（何を確認し、どの場合許可・不許可とする等）は有識者の意見も取り入れ共通のものを示してほしい。
27	ガイドライン改定案	iii - 141 ～iii - 154	1 -②.外部サービス利用時のセキュリティ要件	本ガイドラインに今回判断基準や選定条件に関する項目が追加されたが、世の外部サービスの多くが提示いただいた条件を満たすことは難しいのではないか。実運用を想定したものなのか疑問がある。（特に利用希望の多いSaaS型のクラウドサービスは、団体の定めるセキュリティ要件を契約として外部サービス提供事業者と取り交わすことは難しいと考えており、利用可能な外部サービスが少ないのではないかと危惧している。） 「十分なセキュリティ要件を示せない」、「契約の仕様として入れられない」サービスが多いと思うが、国としてまず外部サービス提供事業者へ必要な情報開示、自治体向けの特別な契約を可能とする等の要請を行い、環境を整えることを積極的にしてほしい。
28	ガイドライン改定案	iii - 142	1 -②.外部サービス利用時のセキュリティ要件	「外部サービス提供者の資本関係・役員等の情報、外部サービスの提供が行われる施設等の場所、外部サービス提供に従事する者の所属・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」とあり、外部サービス提供事業者が情報提供するか疑問がある。また、情報提供を受けるだけでよいのか、情報提供を受けて選定可否を判断するのか。選定可否の判断に利用するのであれば、１自治体が国籍を指定するにはハードルが高く、またICT関係の企業において外国人労働者を採用していることも多いため、実現性を考えた内容に修正してほしい。他の意見でも記載したが、実運用することが難しい記載もあるので、外部サービスの利用規定や選定に係る要件の確認内容と確認結果に対する考え方を具体的に示してほしい。
29	ガイドライン改定案	ii-48 iii-143 iii-147	1 -②.外部サービス利用時のセキュリティ要件	前回の改正時にも意見したが、今回の改正箇所でも「⑧情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する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、～」と記載されている。しかし、「情報の流通経路全般を見渡した形でセキュリティ設計」の内容がよくわからない。 また、解説には「システムの重要度に応じて求められる可用性のレベル等（稼働率、目標復旧時間、バックアップの保管方法など）を十分に検討し、調達の際に、検討した結果を調達仕様書に具体的に盛り込まなければならない。」とか、「サービスレベルを保証させるための SLA を締結する必要がある。」とか、「バックアップについては、契約において、各業務システムの重要度を勘案した適切なバックアップレベルを設定し、別途のバックアップの取得など、レベルに応じた適切な対策を実施することが重要である。」と、可用性の説明があるが、例えば通信の暗号化といったような、「経路」に関するセキュリティの説明がない。可用性について述べたいのであれば、例文の記述をそのような内容にするべきである。
30	改定のポイント	3・4	1 -②.外部サービス利用時のセキュリティ要件	リモート保守に関してのセキュリティ対策の基準等の記載がある方が良い。

項番	対象資料	対象ページ	意見分類	御意見
31	ガイドライン改定案	ii -47及びiii -147	1 -②.外部サービス利用時のセキュリティ要件	8.2 約款による外部サービスの利用(機密性2以上の情報を取り扱う場合)－(2)外部サービスの選定－(カ)情報セキュリティ対策その他の契約の履行状況の確認方法について、具体的な履行状況の確認方法が記載されていない。政府機関等の対策基準策定のガイドライン(令和3年度版、NISC)P120-121では、委託元の具体的な確認方法が記載されており、これに倣う必要があると思うがどうか。
32	改定のポイント	P6,7	1 -②.外部サービス利用時のセキュリティ要件	外部サービスの利用部門が、外部サービスの選定、調達及び契約が終わったのち、利用申請を統括部門に提出する流れになっておりますが、契約後に審査してもあまり意味がないのではないかと思います。 契約後に何を審査するのか、何をもって可否を決定するのか教えていただけないでしょうか。また、現実的に審査結果を否とすることは難しいと思うのですが、いかがでしょうか。 外部サービスの選定時に外部サービスや調達仕様書の審査を行うべきではないでしょうか。
33	改定のポイント	P6,P7	1 -②.外部サービス利用時のセキュリティ要件	外部サービス利用の流れで、利用部門で調達・契約後に統括部門に利用申請となっているが、契約後に否決はしにくいため、契約前に申請または仮申請が必要な流れとして欲しい。
34	ガイドライン改定案	ii-48	1 -②.外部サービス利用時のセキュリティ要件	外部サービス利用の流れで、利用部門で調達・契約後に統括部門に利用申請となっているが、契約後に否決はしにくいため、契約前に申請または仮申請が必要な流れとして欲しい。
35	改定のポイント	P3	1 -②.外部サービス利用時のセキュリティ要件	約款による外部サービスは機密性2以上の情報を原則取り扱えないとしているが、ISMAP等によりセキュリティ要件を満たすことが確認できれば、原則禁止ではなく地方団体の責任において利用検討できることとしてほしい。
36	ガイドライン改定案	iii-141	1 -②.外部サービス利用時のセキュリティ要件	約款による外部サービスは機密性2以上の情報を原則取り扱えないとしているが、ISMAP等によりセキュリティ要件を満たすことが確認できれば、原則禁止ではなく地方団体の責任において利用検討できることとしてほしい。
37	ガイドライン改定案	ii -47	1 -②.外部サービス利用時のセキュリティ要件	外部サービスの利用に関する規定を整備することとあるが、各自治体で同様のレベルが担保される必要があるため、目安となるものを明示してほしい。 明示の際は、これまでの様々なガイドラインについて、「外部サービス」として整理してほしい。
38	ガイドライン改定案	ii -47	1 -②.外部サービス利用時のセキュリティ要件	（１）と（２）の関係性について重複が多く、相違がわかりづらいため、整理してほしい。
39	改定のポイント	7~8	1 -②.外部サービス利用時のセキュリティ要件	(3)調達・契約⇒(4)利用承認後に、セキュリティ対策の規定についての流れ（(5)~(7）)が記載される流れとなっているが、セキュリティ対策の規定の部分は、一般的な流れとして(1)規定の整備の部分に記載した方がわかりやすいのではないか。（セキュリティ対策の規定を整備したのち、選定、調達・契約といった流れが一般的と思われるため。）
40	ガイドライン改定案	ii -34	1 -②.外部サービス利用時のセキュリティ要件	(22)②は、資料①p3の記述にあるとおり、「原則」をつけるのが現実的と思われます。

項番	対象資料	対象ページ	意見分類	御意見
41	ガイドライン改定案	ii -49	1-②.外部サービス利用時のセキュリティ要件	8．2（7）イ項では「外部サービスで取り扱った情報の廃棄」と書かれてiるが、p. iii - 55の図表24では気密性２以上のデータを保存する記憶媒体の処理として具体的に物理的破壊などの方法が示されている。外部サービス、特にクラウド等の利用においては、記憶媒体の物理的破壊等は困難と想定されることから、外部サービス利用における記憶媒体の廃棄方法について具体的に示していただきたい。
42	ガイドライン改定案	ii -34	1-②.外部サービス利用時のセキュリティ要件	ソーシャルメディアの利用に関して「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、この「IC カード等」とは IC カードを利用した二要素認証のことを指しているのでしょうか? もしそうだとした場合、まずそう読み解ける記載とすべきと考えます。しかしソーシャルメディアにおける二要素認証の手段として IC カードを利用できるケースはレアであり SMS 等によるものが一般的であること、また IC カードによる二要素認証は特に LGWAN 接続系では困難であるため、IC カードによる二要素認証を前提とした表現は改めるべきと考えます。また SMS や認証アプリ等も通常業務環境では利用困難なケースが多いため、「望ましい」【推奨事項】レベルとすべきと考えます。 または、もし「IC カード等」を単なるパスワードの記録媒体として記載したに過ぎないのであれば、そのようなケースは現実に想定し得ないため、媒体の例示としては「ハードディスク、USB メモリ、紙等」に改めるか、括弧書きを削除すべきと考えます。
43	ガイドライン改定案	ii -47	1-③.クラウドサービス選定の指標・基準等	本編に対する指摘ではありませんが、今回の改定で様々な規定、基準の整備が必要となっております。（「外部サービスの利用に関する規定」「外部サービス利用判断基準」「外部サービス提供者の選定基準」等々） これらの規定において、国からサンプルのご提供をお願いしたい。各自治体でセキュリティに対する対策、利用するシステム等が異なることから、各自治体での作成が必要なことは理解はするところだが、一定の基準等をガイドライン等でお示しいただけると各自治体も作成の負担がへるのではないかと思います。
44	改定のポイント	10	1-③.クラウドサービス選定の指標・基準等	「ISMAP については、自治体の規模等を考慮し、一律に基準を設けることはせずに参考とすべき第三者認証の一つとして追加する。」とあるが、国（関係省庁）から、「ISMAPの〇〇（クラウドサービス）を使用して資料共有する」という主旨の通知が発出されるケースもあるため、自治体のポリシー上対応ができないサービスに対しては代替手段を用意していただけるという認識でよいか。もし代替手段を提供する等対応が難しいのであれば、国・地方公共団体共通の方針を示すべきではないか。
45	ガイドライン改定案	iii - 148	1-③.クラウドサービス選定の指標・基準等	判断基準、選定条件が複数提示されているが、ＩＳＭＡＰであれば資料②に提示されている内容（選定条件、セキュリティ要件等）を全て満たしているという解釈はできないと思われるため、必要な情報を収集する外部サービス利用所属の職員の負担、判断を行うセキュリティ部門の職員の負担が増大すると考えるので、「ガイドラインの規定の●●、△△・・・■■は〇〇という認証規格を取得していれば担保できることを示す」等負担を軽減する方法を検討し、具体的な確認項目を表やリストといった見やすい形式で提示してほしい。
46	ガイドライン改定案	iii-148	1-③.クラウドサービス選定の指標・基準等	外部サービスの信頼性が十分であることの参考情報として ISMAPを活用することは、各自治体の外部サービス選定に係る審査作業を軽減するものではないため、 ISMAPクラウドサービスリストにある外部サービスであれば選定基準を満たすものとしてほしい。
47	ガイドライン改定案	iii-154	1-③.クラウドサービス選定の指標・基準等	外部サービスにおける情報資産の破棄について、業者のクラウドサーバで復元できないよう処置をし、その処理を記録するなどの手続きを講じることは不可能であるため、ISMAP等信頼性を満たす外部サービスに限りこれら破棄に係る手続きが不要であることとしてほしい。
48	ガイドライン改定案	iii-141	1-③.クラウドサービス選定の指標・基準等	画一的な約款や規約等への同意のみで利用可能となる外部サービスにおいて、機密性２以上の情報の取り扱いを原則禁止としているが、ISMAP等で信頼性を一定担保できるサービスについては、取扱いを認めてほしい。
49	ガイドライン改定案	ii - 33	1-③.クラウドサービス選定の指標・基準等	「（１５）⑤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。」は、今回改定案の「8.外部委託」のサービス利用再定義内容との整合性が取れないので、内容を見直してほしい。

項番	対象資料	対象ページ	意見分類	御意見
50	ガイドライン改定案	iii - 141	1 -③.クラウドサービス選定の指標・基準等	【趣旨】に記載された、「なお、民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは・・・（中略）・・・原則として機密性２以上の情報を取り扱うことはできない。」については、通信回線サービス等の約款利用ができないように受け取れるので、「電気通信サービスや郵便、運送サービス等」が除外されることを明記してほしい。また、クラウドサービスを約款利用することも原則不可と受け取れるので、「利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除き」（現行総務省ガイドラインの「10.用語の定義」の記載事項）を追記してほしい。
51	ガイドライン改定案	iii - 142	1 -③.クラウドサービス選定の指標・基準等	「(1)外部サービスの利用に係る規定の整備」の「②外部サービス提供者の選定基準」「③ 外部サービスの利用申請の許可権限者と利用手続」「④ 外部サービス管理者の指名と外部サービスの利用状況の管理」については、整備に必要な情報が（解説）に記載されていないので、追記してほしい。（記載イメージは、政府機関ガイドライン126～129頁の基本対策事項及び解説）
52	ガイドライン改定案	iii - 142	1 -③.クラウドサービス選定の指標・基準等	「（２）サービスの選定」は、選定作業に必要な確認事項が①～⑨まで記載されているが、高度な専門知識を要する内容であることから、全ての自治体が同一水準で選定作業を行うことは困難と感じる。一方で、政府機関ガイドラインでは、「サービスの選定」を、クラウドサービスとそれ以外に分けた上で、クラウドサービスについては、「ISMAP管理基準の管理策基準が求める対策と同等以上の水準を求めること」とした上で、簡素な記述とされている。 ISMAPは、各政府機関等が独自に 全てのセキュリティ要件を最初から確認する非効率な作業を不要とすることを目的とする制度であると理解している。地方自治体においてもクラウドサービス利用の統一的なセキュリティ基準を明確化するために、機密性２以上の情報を取扱う場合のクラウドサービス利用においてはISMAP登録サービスからの選定を原則化することとして、政府機関ガイドラインに記載ぶりに合わせて欲しい。 また、ISMAPは政府機関で主に扱われる機密性２のレベルを想定した基準を定めていることから、自治体で機密性３の情報を扱うために必要となる、ISMAPプラスアルファの選定条件を明確化して（解説）に記載してほしい。 具体的には、政府ガイドライン140頁の「・ 遵守事項4.2.1(5)(b)「利用申請を審査」について」に記載された「クラウドサービスがISMAPクラウドサービスリストに登録されている場合には、ISMAP管理基準に加えて個別に求めた外部サービス提供者の選定条件及び外部サービスのセキュリティ要件の範囲を確認すれば良い。」 との考え方を取り込んでほしい。
53	ガイドライン改定案	iii - 145～154	1 -③.クラウドサービス選定の指標・基準等	「8.2. 外部サービスの利用 （機密性２以上の情報を取り扱う場合）」は高度な専門知識を要する内容であることから、十分な解説が無いと、自治体によって独自の解釈が生じ、その結果セキュリティ対策の平準化を損なうことが危惧される。そこで、政府機関ガイドライン「4.2.1 要機密情報を取り扱う場合」の「基本対策事項」「解説」の記載事項で、改定案の（解説）に反映していない箇所を、改定案の（解説）に積極的に取り込むことで（解説）内容を充実させてほしい。
54	ガイドライン改定案	iii - 146～147	1 -③.クラウドサービス選定の指標・基準等	「（２）外部サービスの選定」に①～⑫の解説が記載されているが、例文①～⑨の記載順と一致しておらず、例文と解説を対比させて読むことが困難であるため、記載順を整理して欲しい。

項番	対象資料	対象ページ	意見分類	御意見
55	ガイドライン改定案	iii-154	1 -③.クラウドサービス選定の指標・基準等	「(6)外部サービスを利用した情報システムの更改・廃棄時の対策」の②に、「情報資産の廃棄は「 2. 情報資産の分類と管理 （２） 情報資産の管理 ⑩情報資産の廃棄」、「4.1. サーバ等の管理 （７） 機器等の廃棄」を参照すること。」との記載が有るが、この参照先はオンプレミスの機器を主に想定したものであることから、クラウドサービス等を利用する場合は、その特性に応じた廃棄方法を具体的に記載をしてほしい。 ※特定個人情報を取扱う「ガバメントクラウド」の調達仕様書や個人情報方後評価書記載例では、「NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。」との表現となっている。 ※政府機関ガイドラインでは、「基本対策事項4.2.1(8)-2 a)「情報の廃棄方法」について」とその （解説） において、外部サービス利用時を想定した廃棄方法が記載されている。
56	ガイドライン改定案	iii-157～158	1 -③.クラウドサービス選定の指標・基準等	「8.3. 外部サービスの利用 （機密性２以上の情報を取り扱わない場合） 」の （解説） は、政府機関ガイドラインの「4.2.2 要機密情報を取り扱わない場合」を反映させた内容となっているが、政府機関ガイドラインの （解説） の記載内容が反映していない。例えば、「遵守事項4.2.2(1)(a) （ア） 利用可能な業務の範囲について」や「・ 遵守事項4.2.2(2)(a)利用に当たってのリスクについて」の （解説） に箇条書きされたリスクは、約款によるサービス利用の実施判断を行う際に有用な情報なので、総務省ガイドラインの解説に記載してほしい。
57	ガイドライン改定案	ii-47	1 -③.クラウドサービス選定の指標・基準等	外部サービス提供に従事する者の国籍に関する情報提供を選定の指標とするのは国籍差別等に繋がる懸念があり不適切と思われる。事業者の所在地、本社の所在地等の情報提供とするべきではないか。
58	ガイドライン改定案	ii -47	1 -③.クラウドサービス選定の指標・基準等	8.2外部サービスの利用 （機密性２以上の情報を取り扱う場合） 利用基準～調達・導入～運用保守・廃棄までに渡り、求められる順守事項が示されされ、システムの業務委託レベルの順守対応管理が求めれれる状況となり、外部サービスを活用する利点 （技術の進展やサービスの進化への対応、ユーザニーズへの柔軟な対応など） がそがれる懸念を感じます。 又、対応事務への支援として、外部サービスの利用規定などの雛型を提供いただく事も考慮いただきたい。
59	ガイドライン改定案	iii -142～145	1 -③.クラウドサービス選定の指標・基準等	例文8.2 外部サービスの利用 （機密性2以上の情報を取り扱う場合） (1)～(3)において「外部サービス提供者の選定基準」「外部サービス提供者の選定条件」という用語が出てくるが、両者の違いが不明なので、明らかにしてほしい。
60	ガイドライン改定案	ii -47	1 -③.クラウドサービス選定の指標・基準等	各自治体において、独自で「外部サービス （機密性２以上の情報を取り扱う場合） の利用に関する規定」を整備することは非常に困難な作業であると考えます。情報セキュリティレベルの標準化 （業務の標準化・共通化） の観点からも、規定の具体例や政府で策定した規定を提示していただきたい。 （「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） や総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン （第３版） 」 （2021年9月） は情報量が多く、これらを参考にして規定を整備することは難しいと考えます。）
61	改定のポイント	3	1 -③.クラウドサービス選定の指標・基準等	No1の質問に関して、ISMAPに登録されているサービスでも同様の場合、当市は将来的にMicrosoft365上でアクセス権、接続元IPや端末等で制御したうえで機密性２以上の情報を扱いたいと考えているため、この部分の緩和をお願いしたい。
62	改定のポイント	6~7	1 -③.クラウドサービス選定の指標・基準等	外部サービスの利用の流れとして、(1)規定の整備⇒(2)選定⇒(3)調達・契約⇒(4)利用承認となるが、(3)と(4) は逆の順序が適当なのではないか。 （実務上、一般的な流れなのではないか。）
63	ガイドライン改定案	ii -47~ ii -48	1 -③.クラウドサービス選定の指標・基準等	外部サービスの利用の流れとして、(1)規定の整備⇒(2)選定⇒(3)調達・契約⇒(4)利用承認となるが、(3)と(4) は逆の順序が適当なのではないか。 （実務上、一般的な流れなのではないか。）

項番	対象資料	対象ページ	意見分類	御意見
64	ガイドライン改定案	Ⅱ-33	2.情報セキュリティ対策の動向を踏まえた記載の充実	「CISOが定めた電子署名、暗号化」「CISOが定めた方法で暗号のための鍵を管理」「CISOは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供」とあるが、CISOが具体的にどのようなことを実施るべきか不明であり、CISOが個別に定めず「電子政府推奨暗号リストに定められた」とすることでセキュリティ水準を一定に保てると考えます。
65	ガイドライン改定案	ii-6	2.情報セキュリティ対策の動向を踏まえた記載の充実	適用範囲に「地方公営企業」が含まれるが、医療、水道など重要インフラ事業は事業者としてのガイドラインがあり、業務の特性を考慮すると本対策基準の適用範囲とすることは公営企業のDXを阻害することになるため、公営企業としての事業は、適用範囲外とすべきと考えます。 ・医療情報システムの安全管理に関するガイドライン ・水道分野における情報セキュリティガイドライン
66	ガイドライン改定案	ii-40	2.情報セキュリティ対策の動向を踏まえた記載の充実	6.4.(2)情報システム管理者の措置事項に「業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。」を追加するべきと考えます。
67	ガイドライン改定案	ii-40	2.情報セキュリティ対策の動向を踏まえた記載の充実	【6.4.(3)職員等の遵守事項】は技術的対策ではなく人的対策によるものであるため、5.1.職員等の遵守事項にまとめることにより、自己点検時などに漏れが無くなるものものと考えます。
68	ガイドライン改定案	ii-32	2.情報セキュリティ対策の動向を踏まえた記載の充実	「6.1.(14)②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。」とあるが、大量のスパムメール等は日常的に受信し検知しており、それをもって運用を停止することはありえないため、「スパムメール等が内部から送信されていること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。」とするか、そもそも項目を削除するのが適正と考えます。
69	ガイドライン改定案	ii-33	2.情報セキュリティ対策の動向を踏まえた記載の充実	「⑤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。」が、いわゆる約款による外部サービスなどを想定していたとしても、クラウドファーストを推進していく上で勘違いしやすい記述であるため、削除することが良いと考えます。
70	ガイドライン改定案	iii-46～iii49	2.情報セキュリティ対策の動向を踏まえた記載の充実	解説の本文及び図表において『不正プログラム対策』『不正プログラムの対策』『不正プログラムへの対策』が混在しているので統一してはどうか。
71	改定のポイント	12	2.情報セキュリティ対策の動向を踏まえた記載の充実	LGWAN系、インターネット接続系ともに仮想化し、シンクライアント（若しくはそれと同等の制限をかけた）端末で双方を閲覧・操作することも技術的に可能だと思われるが、αモデルでもβモデルでもない、そのような場合を想定したセキュリティルールの規定はないのか。

項番	対象資料	対象ページ	意見分類	御意見
72	ガイドライン改定案	iii-117	２.情報セキュリティ対策の動向を踏まえた記載の充実	標的型攻撃メール対策として、「・不自然なメールが着信した際は、 電話等の別の手段で差出人にメール送信の事実を確認する。」との記載がありますが、電話であったとしてもメール中の電話番号に折り返し連絡した場合、相手にヒントとなる情報を与えるほか、詐欺などの被害に合う可能性があるため、「不審メールには返信しない」としてほしい。
73	ガイドライン改定案	iii -43～iii -44	２.情報セキュリティ対策の動向を踏まえた記載の充実	LGWAN 接続系とインターネット接続系の分割について、インターネット環境の画面データをLGWAN 環境にて閲覧する際、現在は画面転送方式のみが想定され、許可する通信は画面転送用のプロトコルのみが記載されている。 近年、画面転送以外にも端末内分離方式（インターネット環境からデータを取得し、LGWAN環境でWeb閲覧するような方式）等の様々な方式があるので、そういった現在の新技術を反映した記載を充実してほしい。
74	ガイドライン改定案	iii -117	２.情報セキュリティ対策の動向を踏まえた記載の充実	6.5 不正アクセス対策－(7)標的型攻撃－①人的対策例(標的型攻撃メール対策)中、『不自然なメールが着信した際は、電話等の別の手段で差出人にメール送信の事実を確認する。』について、文意の解釈のままメールに記載された電話番号を信用して問い合わせを行ってしまうと、なりすましを助長・見破ることができない場合があり入り口対策としては不十分である。【公式に存在する電話番号かどうか別の手段で確認の上、電話等により差出人にメール送信の事実を確認する】にすべき。 参考:IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」 https://ipa.gp.jp/security/technicalwatch/20150109.html
75	ガイドライン改定案	ii - 20	２.情報セキュリティ対策の動向を踏まえた記載の充実	「LGWAN接続系とインターネット接続系の分割」の技術的要件として、「イ） インターネット接続系の端末から、LGWAN接続系の端末へ画面を転送する」ことが求められているが、情報セキュリティ対策技術に向上に伴い、必ずしも画面転送方式だけがセキュアな方式とは限らない。総務省の定める「テレワークセキュリティガイドライン」で定義される「セキュアブラウザ方式」や「アプリケーションラッピング方式」も許容されるよう、記載内容を改めていただきたい。
76	ガイドライン改定案	ii -19 iii -34	２.情報セキュリティ対策の動向を踏まえた記載の充実	電子メールを用いたファイルの送信においては、民間企業では暗号化ファイルが添付された電子メールを破棄する対策をとるものが出てきており、対応に苦慮していることから、p. ii -19の（２）⑦「情報の送信」、p. iii -34の（２）③注６において、PPAP対応の記述を補足して頂けないか。
77	ガイドライン改定案	Ⅱ-25、	３-①.テレワーク実施時のセキュリティ対策	「（ア） CISO は、機密性２以上、可用性２、完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。」とあるが、テレワークを推進していく上で、基本的な事項について別に定めるのではなく「対策基準２(２) 情報資産の管理」にの以下の記載を追加することにより、取り扱いが明確になると考えます。 （１１）外部での情報処理 ア 外部で情報処理を行う者は、取扱う情報資産について、移動中は常に携行し、紛失、盗難等を防止しなければならない。 イ 外部で情報処理を行う者は、機密性２以上の情報資産を取扱う場合は、業務に関係の無い者からの覗き見等を防止するための措置を講じなければならない。

項番	対象資料	対象ページ	意見分類	御意見
78	ガイドライン改定案	iii -67	３-①.テレワーク実施時のセキュリティ対策	本県においては、全職員がテレワークをするに十分な貸出用端末の準備がなく、在宅勤務の場合は、職員が自前のPC等を利用することを見込んでいるため、支給以外の利用申請内容について、（注５）に記載の内容を都度求めることは現実的ではない。類似申請がどうしても必要ならば、セキュリティ上、どうしても外せない情報を厳選してほしい。特に契約者名義と通信回線サービス名称はいらないのではないか。
79	ガイドライン改定案	iii-100	３-①.テレワーク実施時のセキュリティ対策	β又はβ'モデル採用自治体においては、テレワーク実施時に、庁内ネットワークに接続せずMicrosoft365などのクラウドサービスを使用して業務を遂行することが考えられるが、この様なサービス利用時におけるセキュリティインシデントに対応するため、SIEMやSOCの利用などのセキュリティ対策を積極的に導入すべき旨を追記してほしい。
80	ガイドライン改定案	iii-99	３-①.テレワーク実施時のセキュリティ対策	インターネット接続系を経由してLGWAN 接続系の端末に接続するモデルについては、「新型コロナウィルスへの対応等を踏まえたLGWAN接続系のテレワークセキュリティ要件について（令和2年8月18日総行情第111号総務省自治行政局地域情報政策室長通知）」において、セキュリティクラウドを経由する通信経路の図が記載されている。大規模な自治体のリモートアクセスをセキュリティクラウドで収容するのは通信負荷が非常に大きく現実的ではないため、こういった記載をする際には十分考慮いただきたい。 ※上記の通知にあたって、事前に都道府県に意見照会等はなかった
81	ガイドライン改定案	iii-67	３-②.BYOD利用時のセキュリティ対策	BYOD使用申請内容は一律とするのではなく、取り扱う情報資産やセキュリティ対策の条件（BYODで利用する端末へのデータ保存可否やMDMの導入等）に応じた申請内容となるようにガイドラインを整理いただきたい。
82	ガイドライン改定案	iii-67	３-②.BYOD利用時のセキュリティ対策	β又はβ'モデル採用自治体においては、BYOD利用時に、庁内ネットワークに接続せずMicrosoft365などのクラウドサービスを使用して業務を遂行することが考えられるが、この様なサービス利用時におけるセキュリティインシデントに対応するため、SIEMやSOCの利用などのセキュリティ対策を積極的に導入すべき旨を追記してほしい。
83	ガイドライン改定案	iii - 67～68	３-②.BYOD利用時のセキュリティ対策	「(1)職員等の遵守事項」の（注６）に記載された「支給以外の端末の業務利用」に必要な6項目の対策の内、１～５は「いずれかの対策を実施する必要がある」と解釈できるが、6番目の項（遠隔消去）は、 ・１～５のどの対策を実施した場合でも、セットで必要なのか ・１～５の内、特定の対策を実施した場合に、セットで必要なのか ・１～５の全ての対策を実施できない場合に必要なのか が読み取りにくいので、明確な表現に改善してほしい。
84	ガイドライン改定案	iii - 90	３-②.BYOD利用時のセキュリティ対策	「(19)無許可でのネットワーク接続の禁止」の（注１６）に記載された「支給以外の端末を庁内回線に接続することの許可手続」は、リモートワーク時の庁内回線接続も含まれるが、iii-67の5.人的セキュリティの5.1.(1)④（注５）（注６）に規定された支給以外の端末の利用申請の手続きとは、別の場所に記載されていることから、支給以外の端末を利用したリモートワーク実施時に必要な手続きの全体像を読み取るのが困難である。iii-90の（注１６）は、iii-67（注５）（注６）と併せて記載してほしい。
85	ガイドライン改定案	ii -34	３-③.Web会議サービス利用時のセキュリティ対策	【6.1.コンピュータ及びネットワークの管理】で例文において新設された6.1.(２１) Web会議サービスの利用時の対策、(２２) ソーシャルメディアサービスの利用も含め、「職員等は、」で始まるものは技術的対策ではなく人的対策によるものであるため、5.1.職員等の遵守事項にまとめるめることにより、自己点検時などに漏れが無くなるものものと考えます。

項番	対象資料	対象ページ	意見分類	御意見
86	ガイドライン改定案	iii-141	３-③.Web会議サービス利用時のセキュリティ対策	外部サービスの具体例として、「Web会議サービス」が挙げられています。 講じるべき対策からみて、庁内（組織内）の閉域ネットワーク内で完結するテレビ会議システムを含める主旨ではないと解されますので、「Web会議サービス（インターネットを使用せず、組織内の閉域ネットワークで通信が完結するテレビ会議システムは含まない）」とするなど定義を明確にしてほしい。
87	ガイドライン改定案	ii -34	３-③.Web会議サービス利用時のセキュリティ対策	「Web 会議を適切に利用するための利用手順」について、サンプル等のご提示をお願いしたい。
88	ガイドライン改定案	iii -91	３-③.Web会議サービス利用時のセキュリティ対策	（２１）Web会議サービス利用時の対策について、上記の通り、本県では自前の端末の利用をあらかじめ想定しているため、記載を外してほしい。
89	ガイドライン改定案	iii -91	３-③.Web会議サービス利用時のセキュリティ対策	（２１）Web会議の機密性２以上の情報を取り扱う場合について、現状、Web会議の運用管理をやまがた幸せデジタル推進課で一括して行っており、月700件ほどの利用申請がある。E2Eではできない録画記録やライブ配信の需要は増加しており、デフォルトではそういった機能も使えるよう、E2Eは外している。使用課の機密性情報の有無によって、都度E2E機能を具備したり外したりすることは、不可能である。
90	ガイドライン改定案	iii -91	３-③.Web会議サービス利用時のセキュリティ対策	注19に「原則として、許可されたWeb会議サービスを利用」とあるが、利用可能なWeb会議サービスとして許可の判断を行うための参考資料があれば文中に記載いただきたい。
91	ガイドライン改定案	iii - 91	３-③.Web会議サービス利用時のセキュリティ対策	「原則として、自組織で許可されたWeb 会議サービスを利 用すること。」とあるが、セキュリティを考慮すると、どのＷＥＢ会議サービスを利用するのが適当か判断が難しい。国が推奨しているＷＥＢ会議サービスの紹介や、主なＷＥＢ会議サービスのセキュリティの比較評価を示してほしい。
92	ガイドライン改定案	iii - 91	３-③.Web会議サービス利用時のセキュリティ対策	Web会議において機密性２以上の情報を取扱う場合に必要なセキュリティ対策が明記された点は非常にありがたい。その一方で、Web会議は約款による外部サービスとして提供される場合が大半であることから、「8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）」に記載されたサービス選定条件を遵守できるかの確認は難易度が高いと思われる。そこで、自治体によって（利用可能なサービス選定の）判断が分かれることが無いように、Web会議サービスの具体的な選定方法に踏み込んだ記載をしてほしい。
93	ガイドライン改定案	ii -34	３-③.Web会議サービス利用時のセキュリティ対策	(２１) Web 会議サービスの利用時の対策 コロナ禍により、Web会議はNewNormalなビジネススタイルとなる中で、「外部からWeb 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。」までを求めるについては、過剰の感があると考えますので、推奨事項でお願いしたい。

項番	対象資料	対象ページ	意見分類	御意見
94	ガイドライン改定案	ii -34	３-③.Web会議サービス利用時のセキュリティ対策	（２１）④について、利用申請で承認を受けるべき内容はどのようなものになるか。 また、承認の権限者が不明のため、「情報セキュリティ管理者」など明示してほしい。
95	ガイドライン改定案	ii -34	３-③.Web会議サービス利用時のセキュリティ対策	（２２）（ア)前段と、（２２）⑤の関係性について、重複又は相違がわかりづらいため、整理してほしい。
96	ガイドライン改定案	ii -20	４.マイナンバー利用事務系から外部接続先	情報システム全体の強靭性の向上で、「α」「β」「β'」の3パターンが示されているが、１つのパターンに絞る、若しくは目指すべきパターンを示すべきと考えます。現状を考慮し、各自治体の状況に配慮した3パターンの提示と思われるが、政府が自治体DX加速のため、いわゆる個人情報保護法制2000個問題の解決に着手しようとしているときに、情報セキュリティポリシーで新たな2000個問題が発生することは防ぐべきであるためです。
97	ガイドライン改定案	iii-39	４.マイナンバー利用事務系から外部接続先	国等の公的機関が構築したインターネットに接続されたシステム等で十分に安全性が確保された外部接続先としてeLTAXやマイナポータル等が挙げられているが、”十分に安全性が確保された”状態は具体的にどのような対策が施されたシステムのことを指すのかをお示しいただきたい。 例えばLGWAN-ASPであれば、国等の公的機関以外が構築したシステムであっても、総合行政ネットワークASPガイドライン等によって十分に安全性が確認されているシステムのみが提供されているという認識である。よって、マイナンバー利用事務系からLGWAN-ASPへの接続であればeLTAX等への接続と同等の取り扱いとしていただきたい。
98	ガイドライン改定案	iii - 39	４.マイナンバー利用事務系から外部接続先	双方向でのデータ移送を行うにあたっての前提となる追加的なセキュリティ対策として、マイナンバー利用事務系の端末におけるOS修正プログラムの常時適用といった内容が盛り込まれている認識です。 この点について、住民窓口で利用する業務システム群では、サービスの可用性を求められるものとなっており、外部のリスクとの徹底的な分離を行ってきたこととも相まって、常時の修正プログラム適用を行うことは困難な団体も多いのではないかと考えられます。実際にその運用を開始するにあたっては、マイナンバー利用事務系での更新プログラム配信に関する環境整備、各業務システムの保守契約見直し等、対応に係る経費・運用コストがかさんでしまうことも想定されます。 また、本件の対応の必要性が、自治体側からの情報アップロードの実現にあたってのものであるならば、マイナポータルやLGWAN全体の健全性のための必須要件とするなどについて、各自治体での策定を行う情報セキュリティポリシーのガイドラインとしての位置付けではなく、明確な示し方をして頂きたいと考えます。
99	改定のポイント	p16	４.マイナンバー利用事務系から外部接続先	改正のポイント４は、従来の片方向通信から双方向通信（アップロード含む）まで認めるという将来を見据えた重要な論点である。一方、双方向通信を認めるには、リスク分析の結果を踏まえた追加のセキュリティ対策をセキュリティポリシーに明記したうえで講じることが必要となるため、資料②においてもう少し詳細な例示をお示しいただきたい。
100	ガイドライン改定案	iii - 39	４.マイナンバー利用事務系から外部接続先	「マイナンバー利用事務系から外部接続」するシステムに限らず、国の各省庁に対しても「地方公共団体における情報セキュリティポリシーに関するガイドライン」の浸透や、セキュリティ対策の指導・監督を十分に行ってほしい。
101	ガイドライン改定案	ii -20	４.マイナンバー利用事務系から外部接続先	3.情報システム全体の強靭性の向上－(1)マイナンバー利用事務系－①マイナンバー利用事務系と他の領域との分離 『インターネット等からマイナンバー利用事務系との双方向でのデータの移送を可能とする。』について、【双方向でのデータの移送】では間接的な表現であるため、シンプルに【データ通信】でいいのではないか。
102	ガイドライン改定案	iii - 39	４.マイナンバー利用事務系から外部接続先	「双方向でデータを移送する」という表現について、「移送」の意味が不明確であるため、できることできないことを明確化するような表現に見直してほしい。 ※現状の改定案では以下のような点が不明である。 例①　「双方向通信が可能」と受け取って良いのか？ 例②　市民（庁外側）からの申請をトリガーとした自動処理が可能なのか？

項番	対象資料	対象ページ	意見分類	御意見
103	ガイドライン改定案	iii - 39	４.マイナンバー利用事務系から外部接続先	本市では、市民への証明書等交付事務を自動化する電子交付を早期に実現したいと考えている。そのためには、市民からの電子交付の請求（本市ではグラファー社の電子申請システム利用を想定）を受けて、マイナンバー利用事務系の業務システムで交付物を生成し、市民に電子交付する仕組みが必要であり、総務省ガイドラインのR2年12月改定版で追記された片方向通信に加えて、新たなセキュリティ対策が必要と認識している。R3年度の同ガイドライン改定において、このような電子交付に必要なセキュリティ要件を具体的に記載してほしい。
104	ガイドライン改定案	iii - 39	４.マイナンバー利用事務系から外部接続先	「マイナンバー利用事務系のサーバ、端末については、・・・ OS の修正プログラムについても最新の修正プログラムを常時更新する運用や対策を行わなければならない」については、サーバに最新の修正プログラムを常時更新するのは（工数を要する動作確認作業が毎月必要になるという意味で）現実的ではないので、現行規定に戻すか、対象を外部接続先とのやり取りを行う機器に限定してほしい。

項番	対象資料	対象ページ	意見分類	御意見
105	ガイドライン改定案	iii - 40	４.マイナンバー利用事務系から外部接続先	「(1)マイナンバー利用事務系」の（注3）に記載された金融機関との口座振替（口座振込）データのやり取りのように、自治体における様々な部署で日々発生している業務において「外部媒体の利用を必須化する規定」の存在は、事務効率化を阻害する要因となっており、更に媒体利用そのものがセキュリティリスクを伴うものであることを考慮し、今回の「双方向でデータ」を実現する改定に合わせて、現場の実務を踏まえた見直し（マイナンバー利用事務系端末機からの、LGWAN-ASP（例：金融機関への口座振替業務）の直接利用を認める。それができない場合は、LGWAN接続系とマイナンバー利用事務系間の特定通信を認める。）を行ってほしい。
106	ガイドライン改定案	iii -39	４.マイナンバー利用事務系から外部接続先	「（注１）現在、国等の公的機関が構築したインターネットに接続されたシステム等で十分に安全性が確保された外部接続先の通信としてeLTAX、マイナポータル、自治体情報セキュリティ向上プラットフォーム等が考えられる。」としてほしい。 理由：システムの標準化により、これまで市町村から紙で提供されていたものがデータでの提供となるなど、eLTAX・マイナポータル・自治体情報セキュリティ向上プラットフォーム以外との連携が想定されるため。
107	ガイドライン改定案	iii -39	４.マイナンバー利用事務系から外部接続先	「OSの修正プログラムについても、マイナンバー利用事務系のシステムへの影響の大きさを踏まえ、最新の修正プログラムを常時更新する運用や対策を行わなければならない。」としてほしい。 理由：修正プログラムの内容やシステムへの影響を考慮しながら適用時期や対策を決める必要があるため、現在の記載を残してほしい。
108	ガイドライン改定案	iii-35	４.マイナンバー利用事務系から外部接続先	「国等の公的機関が構築したシステム等、十分に安全が確保された外部接続先」について、「公的機関の範囲の明示」と、「十分に安全が確保された」をどのように判断すればよいか、解釈を具体的に定めてほしい。
109	ガイドライン改定案	iii-39	４.マイナンバー利用事務系から外部接続先	「OSの修正プログラムについても最新の修正プログラムを常時更新する運用」とされているが、常時更新するためには、マイナンバー利用事務系とインターネット系の特定通信等修正プログラムを取得する通信が必要となるため、通信手法について具体的に明示するか、見直しを検討してほしい。
110	ガイドライン改定案	ii -20	４.マイナンバー利用事務系から外部接続先	国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先とは双方向通信を可能とあるが、自治体の裁量で様々なシステムと特定通信できてしまうことになりかねない。十分に安全性が確保されたとする具体的な基準をお示しいただきたい。
111	ガイドライン改定案	ii -20	４.マイナンバー利用事務系から外部接続先	ワクチン接種記録システム「ＶＲＳ」は、ＬＧＷＡＮ環境に構築されており、インターネット環境からは国配布のタブレットのみアクセスできるよう制限をかけている。データの流れだけではなく、システムへのアクセスに関する事項もガイドライン化が必要と考える。
112	ガイドライン改定案	iii - 39	４.マイナンバー利用事務系から外部接続先	修正後は「マイナンバー利用事務系のサーバ、端末については、ウイルス対策ソフトを導入し、最新の定義ファイルを常時更新する。また、OSの修正プログラムについても最新の修正プログラムを常時更新する運用や対策を行わなければならない」とされているが、OSの修正プログラムを常時更新することは、既存システムの安定稼働に影響を及ぼし運用経費も増額される可能性がある。十分に安全性が確保された接続のみのため、ガバメントクラウドの検証が十分になされ、既存のシステムへの影響も考慮したうえで速やかに適用することとしてほしい。

項番	対象資料	対象ページ	意見分類	御意見
113	ガイドライン改定案	ii -20	４.マイナンバー利用事務系から外部接続先	３．（１）①項のインターネット等とマイナンバー利用事務系とのデータの移送において、「LGWAN−ASPを経由して」が削除されているが、LGWANを経由することを前提としていると思われることから、「LGWAN経由」は残してほしい。LGWAN経由以外もありうるならば、その旨を記述してほしい。また、双方向でのデータの移送なので、「インターネット等から」ではなく、「インターネット等と」ではないか。
114	ガイドライン改定案	ii -20	４.マイナンバー利用事務系から外部接続先	県では、インターネットからLGWAN接続系へのファイル取り込み時に資料②p. ii -20の（２）①（ウ）項に示す「危険因子をファイルから除去」するサニタイズを行っている。セキュリティレベルを落とすことがないように、３（１）①項の「安全性が確保された外部接続先」がインターネットからのファイル取り込み等において「危険因子をファイルから除去」する処理を行っていることを担保する記述を追加してほしい。
115	ガイドライン改定案	ii -49	今回改定範囲外	リースや購入した機器の廃棄時の情報抹消については記載があるが、クラウドサービス利用後のデータの抹消方法について記載がないため、具体的な方法を示していただきたい。
116	ガイドライン改定案	ii-35	今回改定範囲外	「特権を付与されたID及びパスワードについて、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。」との記載があるが、IDの定期変更は必要ないのではないか。また、職員等の端末等のパスワードの定期変更はなくなっているので、職員等の端末等のパスワードと比較しての定期変更の機能強化は意味がない。 そこで、「特権を付与されたIDのパスワードについては、定期的に変更することとし、職員等の端末等のパスワードよりも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。」と修正してはどうか。
117	ガイドライン改定案	ii-43 iii-123	今回改定範囲外	例文に、「④暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。【推奨事項】」とあるが、「再暗号化」は必要な場合だけに限定する必要はないのではないか。
118	ガイドライン改定案	iii-46	今回改定範囲外	前回の改正時にも意見したが、「インターネット接続系とLGWAN接続系を完全に分離する場合を除き」とあるが、完全に分離の定義を明確化してほしい。 例）「特定通信（Jアラート等のインターネット系とLGWAN系の両方に通信が発生するものを除く）が存在している場合は完全に分離とはいえない」等。
119	ガイドライン改定案	ii - 24	今回改定範囲外	4.4.④の「情報システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。」と、ii-20の3.（１）マイナンバー利用事務系②アの「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のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。」とは、重複した内容が異なる表現で記載されているため、ii-20の3.（１）マイナンバー利用事務系②アにまとめて記載してほしい。
120	ガイドライン改定案	iii - 68	今回改定範囲外	「セキュアブラウザ」という言葉が定義なしで使われているため、「10. 用語の定義」で定義してほしい。

項番	対象資料	対象ページ	意見分類	御意見
121	ガイドライン改定案	ii -20	今回改定範囲外	LGWAN 接続系とインターネット接続系の分割については、インターネット接続系の端末からLGWAN 接続系の端末へ画面を転送する方式（画面転送方式）のほか、LGWAN接続系のクライアントＰＣ内に設けられた隔離領域（セキュアコンテナ、ローカルコンテナ等）内でインターネットを閲覧する方式についても言及していただきたい。
122	改定のポイント		今回改定範囲外	改定のポイントが、ガイドラインのどのページを指しているのかが、すぐわかるようにページ数を記載してほしい。
123	ガイドライン改定案	ii -16	今回改定範囲外	機密性の定義について、改めて整理を行うことが必要となるのではないか。（「機密性２」に該当する内容は広範であり、また、その性質も多様であるが、現状における機密性区分においては、公表を前提とした「機密性１」以外の情報を取り扱う場合は、原則的に一律厳格な制約が求められる建付けとならざるを得ない状況のため。）
124	ガイドライン改定案	ii -6	今回改定範囲外	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-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-35 「必要な通信だけを許可」 iii-43 「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、またより正確には「安全が確保された通信を必要最低限許可」とすべきと考えます。
125	ガイドライン改定案	ii -6	今回改定範囲外	(11) 通信経路の分割について「～安全が確保された通信だけを許可できるようにすることをいう」とされていますが、この「安全が確保された通信」とは何を指すのかが不明瞭です。 「安全が確保された通信」を満たすための重要なポイントは、外→内の通信については「インターネット接続系から LGWAN 接続系へのマルウェア侵入を確実に防ぐこと」、内→外の通信については「万が一 LGWAN 接続系端末がマルウェアに乗っ取られたとしても C2 サーバーとの通信や情報漏洩が可能な経路となり得ないこと」の二要素に大きく整理できると思われますが、前者については次の「無害化通信」やⅲ-43で定義されている一方、後者について記載された箇所を見つけられません。後者の規定がないため、例えば LGWAN 接続系からインターネットの任意のメールアドレスに対して電子メールを送り放題である状態を、本ガイドラインは容認することになってしまっています。後者の内容を明文化すべきと思われます。
126	ガイドライン改定案	ii -6	今回改定範囲外	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、無害化の最も重要なポイントである「未知のウイルスが送られてきても100%防げるものである」ことが十分に表現されていないように思われます。 そこで、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の影響を確実に排除した通信をいう。」

項番	対象資料	対象ページ	意見分類	御意見
127	ガイドライン改定案	ii -19	今回改定範囲外	「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、 ①情報資産が所有者の管理下から離れるケースは「廃棄」以外に「返却」「譲渡」「売却」等があります。ii -22やiii -52では「機器を廃棄、リース返却等をする場合」、iii -54では「不要になった場合やリース返却等を行う場合」と、廃棄以外のケースを想定された記載となっていますので、それらと記載を合わせるべきと考えます。 ②「情報を記録している電磁的記録媒体が不要」なことは、廃棄（等）する時点で自明です。 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。 「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。」 続く(イ)や(ウ)も同様です。
128	ガイドライン改定案	ii -19	今回改定範囲外	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あり記憶媒体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。
129	ガイドライン改定案	ii -19	今回改定範囲外	○「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、前回iii -34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、「ほぼ守れないルール」となってしまいました。 「必要に応じ」と補記されているため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）
130	ガイドライン改定案	ii -24	今回改定範囲外	「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」の誤記と思われます。 なお昨年度は「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」との回答をいただきましたが、LGWANは団体の外にあるネットワークであり、庁内ネットワークを庁外に集約するというのは意味が通らない状況と考えます。

項番	対象資料	対象ページ	意見分類	御意見
131	ガイドライン改定案	ii -29	今回改定範囲外	「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、現在はパスワードの定期的変更と同様に良くないとされているポリシーと思われます。 現在は、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、このポリシーは残存させるものの、「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るべきと考えます。
132	ガイドライン改定案	ii -32	今回改定範囲外	「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」について、もし大量のスパムが「内部から送信されている」場合は重大なインシデントであり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。 このルールに愚直に則るとメールサーバは1年中止めっぱなしにせざるを得なくなるため、この項目は削除すべきと考えます。 （または、「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」に改めることで存在意義が残りますが、内部端末が乗っ取られているインシデント対応について「電子メールのセキュリティ管理」項目で記載するのはやや不自然です。）
133	ガイドライン改定案	ii -33	今回改定範囲外	「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」ということを暗黙の前提として書かれたものだと思います。しかし「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、またクラウドファースト時代には当たり前のものとなっていくため、「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。
134	ガイドライン改定案	ii -33	今回改定範囲外	業務端末に無線 LAN 機能が搭載されると、「無線 LAN 搭載端末を、職員の故意または過失により業務無線 LAN 以外のネットワーク（例えば来庁者用公衆 Wi-Fi や私有のスマホテザリング）に接続してしまい、この業務外ネットワークで脅威に晒される」リスクが大きく高まると考えられます。このため、OS のポリシー設定により、端末が接続可能な SSID を業務用のものに限定することを当方では行っており、同様の内容を本ガイドラインにも記載すべきと考えます。 なお、この「業務端末の業務外ネットワークへの接続」リスクについては、有線についても少ないながら同様に存在します。ii -33の(19)にそれを防げそうな内容が書かれてはいますが、業務用とそれ以外を区別しておらず、そのような意味を汲み取ることが困難です。また技術的対策への言及がありません。 そこで、例えば以下のように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によって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。」 なおこの意見について、昨年度は「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」との回答をいただきましたが、当該資料には上記のリスクのみが記載されており、その対策である上記の OS ポリシー等による措置については記載されていません。また有線に関する同リスクについても記載されていません。 このため、上記対策を少なくとも「庁内無線LANのセキュリティ要件について」に記載すべきと思いますが、リスクそのものは有線・無線を問わないため、本ガイドラインにも記載することが望ましいと考えます。

項番	対象資料	対象ページ	意見分類	御意見
135	ガイドライン改定案	ii -36	今回改定範囲外	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」と記載があり、文字通り読むと一見「公衆通信回線（要するにインターネット）と庁内ネットワークの2つのネットワーク間の相互接続」の話のように見えますが、後段では利用者の認証の話が書かれており、何に関する話なのか意図の読解が非常に困難でした。 おそらく元々ここで言いたかったのは「ネットワーク同士の相互接続」ではなく「インターネットから庁内ネットワーク又は情報システムにリモートアクセスすること」だったと思われますが、一見そう見えない状況です。 また、インターネットも公衆通信回線ですが、現在の（公衆無線LAN 等）の括弧書きによって、「公衆無線LANでない、自宅のインターネット回線や私有モバイルWi-Fiルーターから庁内へのリモートアクセス時は適用対象外」であるかのように読めます。しかし「ただし」以降に書かれている内容は、自宅の回線であっても同様に必要なはずです。 以上を踏まえ、例えば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)」
136	ガイドライン改定案	ii -36	今回改定範囲外	「(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。
137	ガイドライン改定案	ii -37	今回改定範囲外	「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、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。 したがって、「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、できない場合の次善の策とし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。」 また、この変更とともにii -29及びiii -78にある職員等の責務「仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。」も同様に修正が必要と思われます。
138	ガイドライン改定案	ii -39	今回改定範囲外	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。」
139	ガイドライン改定案	iii-34	今回改定範囲外	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「望ましい」とされていますが、電子メールで伝達することは全く意味がないため、「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。

項番	対象資料	対象ページ	意見分類	御意見
140	ガイドライン改定案	iii-43	今回改定範囲外	当方では LGWAN 接続系のクライアント PC 上の隔離領域で動作するタイプのセキュアブラウザ（Soliton SecureBrowser）をこの4年間利用しており、セキュリティ事故を一切起こしていない実績があります。この方式は、画面転送型である VDI や SBC と異なり、サーバーリソース・ライセンス費ともに劇的に低減できるメリットがあります。現在は同種のブラウザとして RevoWorks Browser 等も登場しています。 この方式の採用にあたって、本市は2016年当時総務省に説明に伺い個別了承をいただきました。また神奈川県では今年度末から県全体で導入することとなりました。しかしそれが問題ないことが他団体に公知のものとなっておりません。 そこで、「（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。」
141	ガイドライン改定案	iii-47	今回改定範囲外	図表20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、中継サーバや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。
142	ガイドライン改定案	iii-47	今回改定範囲外	図表20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。 正規ユーザーによるコピー&ペーストのリスクは、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、ここではファイルとテキストを的確に区別し、禁止する対象を「テキスト以外の形式のデータやファイルのコピー&ペースト」とすべきと考えます。 また、この項目では「LGWAN接続系からインターネット接続系へのデータ転送」についてしか規定していませんが、「インターネット接続系からLGWAN接続系へのデータ転送」についても同様とすべきではないでしょうか。 その規定がない現状は、無害化していないファイルをコピペ機能を通じてインターネット接続系から LGWAN 接続系に転送しても問題ないかのように見えてしまっています。

項番	対象資料	対象ページ	意見分類	御意見
143	ガイドライン改定案	iii-50	今回改定範囲外	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、前々回のガイドライン改定の説明会の場において、各セキュリティクラウドがLGWAN-ASPと同等の機能を独自実装していることを認める発言がありました。実際神奈川県でもそのような中継サーバーが配置され、各市町村はそれを利用しています。自治体が行っていけないことはセキュリティクラウドも当然行ってはいけないはずであり、発言内容やセキュリティクラウドでの実装状況とこの記載は矛盾しています。 また、LGWAN-ASPの各種更新ファイル中継システムについて、ただのファイル中継だけでなく全ファイルをサンドボックスにかけて振る舞い検知をかけたり人力で検査する等特別な処理を行っているのかと事業者にヒアリングしたところ、そのようなことは行っておらずただのファイル中継に過ぎないことも確認しました。同等のことを各団体やセキュリティクラウドが行うことで何らセキュリティリスクは上がらないと考えられるため、禁止する必要はないと考えます。 また、LGWAN-ASP にはあらゆるソフトウェアの更新プログラム配信サービスがあるわけではありません。例えば WSUS を利用できない Microsoft Office 2019 以降や Adobe Acrobat、Adobe CC、Google Chrome、Mozilla Thunderbird、JUST Office、一太郎、AutoCAD 等々は LGWAN からパッチを取得することができず、さらにこの条項でインターネットからの取得も封じられているため、この条項に従うと LGWAN 接続系のセキュリティレベルが大きく低下します。 以上を踏まえ、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更新プログラムやパターンファイルの配信サーバーから取得したファイルのみを中継するよう、接続先URLのFQDN等により厳密にホワイトリスト管理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。
144	ガイドライン改定案	iii-88	今回改定範囲外	「（注14）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。
145	ガイドライン改定案	iii-89	今回改定範囲外	「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。

項番	対象資料	対象ページ	意見分類	御意見
146	ガイドライン改定案	iii-108	今回改定範囲外	「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、 同様の内容が政府統一基準では「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（略）機関等外向けに提供するウェブサイト等が実際の機関等提供のものであることを利用者が確認できるように、政府ドメイン名を情報システムにおいて使用すること。ただし、次に掲げる場合を除く。（略）」と記載されています。この2つを比較すると、本ガイドラインには以下3点の課題があります。 ①統一基準では、「情報提供」に限らず「行政手続き」や「意見募集等」の「システム・アプリケーション」も含めた「ウェブサイト等」についてGO.JPドメインを利用しなければならないと読めるよう明記されているのに対し、本ガイドラインでは「ウェブシステム」や「ウェブアプリケーション」を含まない（情報提供目的の）「ウェブサイト」のみに対象範囲を限定しているかのように解釈できる表現となっています。 これについて昨年度、実際そのように範囲を絞る意図があるのか、例えば電子申請システムはLG.JPでなくて良いという考えなのかを総務省に問い合わせたところ、そのような意図はないとの回答をいただきました。しかし現状の文面ではそう読み取れないため、誤読されないよう、政府統一基準に表現を合わせるべきと考えます。 ②ドメイン種別について、「「lg.jp」ドメインを含む属性型・地域型JPドメイン名」とされており、LG.JPと地域型との間に優先度の差が設けられてないうえ、属性型であればLG.JPに限らずOR.JPやNE.JP等でも構わないと読めるようになっています。属性型はおそらく教育機関におけるED.JPやAC.JPの利用を想定したものと思われますが、読者からは必ずしもそう読み取れない状況であるため、政府統一基準に倣い、「原則LG.JPだが、教育機関においてはED.JPやAC.JPを用いても良い」と明記すべきと考えます。 また地域型JPドメイン名は、2001年の汎用JPドメインの創設、2012年の都道府県型JPドメインの創設により、地域型JPドメインとよく似た紛らわしい名称のドメインを誰もが取得可能となっていることを踏まえ長期的には廃絶していくべきところですが、未だ多数の自治体が利用し続けている実態を鑑み、「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に移行することが望ましい。」旨を記載すべきと考えます。 ③「構築」と書かれていることから、「オンプレでの構築」のみを意図しているのか、SaaS 等の「クラウドサービスの利用」も含んでいるのかが不明瞭になっています。これについて昨年度、クラウド利用時は対象外と考えているのかと総務省に問い合わせたところ、そのような意図はないとの回答をいただきました。しかし現状の文面では必ずしもそう読み取れないため、誰もがそう読み取れるような表記にすべきと考えます。 以上3点の課題を踏まえた修正例を以下に示します。 「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外部サービスかを問わず、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、システム更改等機会を捉えLG.JPドメイン名に移行することが望ましい。」

項番	対象資料	対象ページ	意見分類	御意見
147	ガイドライン改定案	iii-108	今回改定範囲外	昨年度の改定の際に、「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。」
148	ガイドライン改定案	ii-34	その他	ii-34では本市と表現されているが、iii-75では本市から自組織へ改訂され、iii-91でも自組織の表現となっている。本市と自組織の表現により違いがあるのでしょうか。もし違いがないようであれば、他ページにも本市と自組織の表記が散見されるため、全ページにおいて、どちらかへ表記を統一してほしい。
149	－	－	その他	意見照会の期間が大変短く、適切な検討が出来ないため、今後は最低１ヶ月間は確保していただきたい。（意見が出ないように、わざと短くしているとしか考えられない。）
150	ガイドライン改定案		その他	外部サービスに係る変更が多岐にわたり、複雑でわかりにくい。理想のガイドラインを策定しても、自治体職員が理解できなければ意味がないため、要点を整理し、分かりやすいものにしていただきたい。
151	ガイドライン改定案	iii -174	その他	「10. 用語の定義」の「約款による外部サービス」は削除漏れではないでしょうか。
152	ガイドライン改定案		その他	「外部委託業者の選定基準」や「外部サービス提供者の選定基準」、「外部サービスに係る規定」等について、盛込む項目については記載されているが、具体策については明記されていないため自治体ごとにばらつきが出るのではないかと懸念されるため，基準等の雛型などがあるといいのではないか。
153	ガイドライン改定案	iii - 135	その他	外部委託には、業務委託と外部サービスの利用が含まれるという認識で合っていますでしょうか。 上記認識があっている場合、以下について確認させてください。 ・「8.1 業務委託」の例文に「外部委託事業者の選定基準」や「外部委託事業者の選定にあたり」といった文言が出てきます。ここに記載の外部委託事業者は業務委託事業者と外部サービス事業者の両方を指しているのでしょうか。 両方を指している場合、「8.1 業務委託」の中に記載されていると誤って認識する可能性があります。業務委託の事業者のみの場合、用語を修正してはいかがでしょうか。

項番	対象資料	対象ページ	意見分類	御意見
154	ガイドライン改定案	iii - 142	その他	「外部サービス利用」時の対策として、以下の例文が追記されています。一方で、「業務委託」では同様の内容が例文ではなく、解説に記載されています。これらの違いについて教えてください。 「8.2 外部サービスの利用（機密性２以上の情報を取り扱う場合）」 （２） 外部サービスの選定 ②情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。 （ア）～（キ）
155	ガイドライン改定案	iii - 174	その他	用語の定義として、「約款による外部サービス」が残っていますが、今回の改定により出現しなくなっているため、不要ではないでしょうか。
156	ガイドライン改定案	-	その他	政府統一基準では、「8.1.3」に新規項目としてテレワークが追加されセキュリティ対策が記載されていましたが、地方公共団体における情報セキュリティポリシーに関するガイドラインには含めないのでしょうか。
157	ガイドライン改定案	iii - 47	その他	政府統一基準では、「8.2(2)外部サービスの選定」についてクラウドサービスとクラウドサービス以外に分けていましたが、地方公共団体における情報セキュリティポリシーに関するガイドラインでは分けないのでしょうか。
158	ガイドライン改定案		その他	このタイミングで発出するガイドラインとしては、ガバメントクラウドを想定した環境についての考え方を明示してほしい。
159	ガイドライン改定案	iii -49	その他	昨今のサイバー攻撃は巧妙化されており、侵入後にアンチウィルス等のセキュリティ対策製品エージェントが排除されることも増えている。さらに、ランサムウェアでもそのような形で被害を拡大させることが目立ってきており、従来のアンチウィルスソフトウェアは、カーネルモードで動作させることで、自らが排除されることを回避していることから、OSカーネルの中で動作していないアプリケーションは停止・排除させられてしまい、エンドポイント対策が無意味になってしまう懸案があるため、以下の下線部分の追記を意見します。 ---------- （注１０）未知の不正プログラムへの対策（エンドポイント対策） 未知の不正プログラム対策として、OS のプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、不審な挙動を示す端末のホスト名や IP アドレスなどの情報 をログとして取得し、管理者へ通知する必要がある。<u>また、従来のセキュリティ対策ソフトと同様、偽装や隠蔽、セキュリティソフトの停止や削除などにより検出を回避するような攻撃者の挙動に対しても、十分に対策を行う必要がある。</u> なお、製品の導入だけでは未知の不正プログラムの対策とはならない。監視体制やCSIRTとの連携等、組織的な対策と合わせて検討が必要となることに留意する必要がある。

「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」改定に対する地方公共団体への意見照会結果（質問）

項番	対象資料	対象ページ	質問分類	御質問
1	ガイドライン改定案	ii -21他	1 -①.外部サービスの再定義	外部サービス利用時は「4.1.サーバ等の管理」「4.2.管理区域(情報システム室等）の管理」「4.3.通信回線及び通信回線装置の管理」「6.1.(10)外部ネットワークとの接続制限等」の適用範囲外でしょうか。
2	ガイドライン改定案	iii -135	1 -①.外部サービスの再定義	国等が指定するクラウドサービスを利用する場合は、地方公共団体は情報システムを管理しているとはならない（8.外部委託の適用を受けない）という整理で良いでしょうか。（例 デジタル改革共創PF、HER-SYSなど）
3	ガイドライン改定案	iii -135	1 -①.外部サービスの再定義	建築設計や測量委託において、委託先が情報共有のために用意するクラウドシステムについては、地方公共団体は情報システムを管理しているとはならない（8.外部委託の適用を受けない）という整理で良いでしょうか。（例 土木工事等の情報共有システム など）
4	ガイドライン改定案	iii -83	1 -①.外部サービスの再定義	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の「⑤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。」とあるが、一方で8.2. 外部サービスの利用 （機密性２以上の情報を取り扱う場合と8.3. 外部サービスの利用 （機密性２以上の情報を取り扱わない場合） では、セキュリティ対策を行った上での外部サービスの利用は認められています。”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”も外部サービスでのクラウドサービスのひとつかとも思われますが、利用できるサービス、できないサービスの判断できるような例示等を示した上でお教えいただきたい。
5	ガイドライン改定案	iii -141	1 -①.外部サービスの再定義	具体例にある「クラウドサービス」に、LGWAN-ASPは含まれますか。含まれる場合、オンプレミス以外はすべて対象となるとの認識でよろしいでしょうか。 LGWAN-ASPは、地方公共団体情報システム機構のセキュリティ要件を満たしていると認識していますので、地方自治体で選定基準等を設ける必要はないのではないかと考えます。
6	ガイドライン改定案	iii -174	1 -①.外部サービスの再定義	巻末の用語の定義にある「約款による外部サービス」の語句についての説明が残ったままだが、ガイドライン本編の改正で「約款による外部サービス」の規定が削られる今回の改正において、用語の定義から「約款による外部サービス」の語句の定義は削らなくて良いのか。
7	ガイドライン改定案	iii -84,iii-92,iii142～iii144,iii156	1 -①.外部サービスの再定義	外部サービスについて必要な規定等は次のとおりでよいか。 また、Web会議サービス及びソーシャルメディアサービスについては、外部サービスの中でも利用頻度が高いため個別に記載しているという理解でよいか。 ①Web会議サービス利用手順（統括情報セキュリティ責任者）iii-84 ②ソーシャルメディアサービス運用手順（情報セキュリティ管理者）iii-84,iii-92 ③アカウント運用ポリシー（ソーシャルメディアポリシー）（情報セキュリティ管理者）iii-92 ④外部サービス（機密性２以上の情報を扱う場合）の利用に関する規定（統括情報セキュリティ責任者）iii-142 ⑤外部サービス（機密性２以上の情報を扱う場合）を利用して情報サービスを構築する際のセキュリティ対策（統括情報セキュリティ責任者）iii-144 ⑥外部サービス（機密性２以上の情報を扱う場合）を利用して情報サービスを運用する際のセキュリティ対策（統括情報セキュリティ責任者）iii-144 ⑦外部サービス（機密性２以上の情報を扱う場合）の利用を終了する際のセキュリティ対策（統括情報セキュリティ責任者）iii-144 ⑧外部サービス（機密性２以上の情報を扱う場合）で発生したインシデントを認知した際の対処手順（情報セキュリティ管理者）iii-144 ⑨外部サービス（機密性２以上の情報を扱わない場合）の利用に関する規定（統括情報セキュリティ責任者）iii-156
8	ガイドライン改定案	iii -84	1 -①.外部サービスの再定義	Web会議サービス利用手順は統括情報セキュリティ責任者が定め、ソーシャルメディアサービス運用手順は情報セキュリティ管理者が定めるとあるが、この違いは何か。ソーシャルメディアサービス運用手順もWeb会議サービス利用手順と同様、統括情報セキュリティ責任者が定めてもよいか
9	ガイドライン改定案	ii-141	1 -①.外部サービスの再定義	「不特定多数の利用者に対して提供される外部サービスは、原則として機密性２以上の情報を取り扱うことはできない。」と明記されたが、例えば、SNSサービスを利用した相談業務などは原則認められないということでしょうか。
10	ガイドライン改定案	ii -34	1 -①.外部サービスの再定義	(２２)ソーシャルメディアサービスの利用 ②機密性２以上の情報は発信してはならない LINE公式アカウントの機能であるLINEチャットを利用して、特定の市民の方と相談対応などを行う場合も、この要件に該当してしまいますか？それとも外部サービス利用の機密情報を取り扱う場合でのセキュリティ対策/順守での対応となりますか？

項番	対象資料	対象ページ	質問分類	御質問
11	ガイドライン改定案	ii -47	1 -①.外部サービスの再定義	8.2外部サービスの利用（機密性２以上の情報を取り扱う場合） 以下の外部サービス利用について、カテゴリを教授ください。 １．LINE公式アカウントツールのシステムを利用した、特定市民の方への情報配信（セグメント配信）やチャットによる電子申請の手続き ２．Logoフォームサービスを利用した、行政手続きの電子申請や手数料の電子決済 ３．民間のキャッシュレス決済サービスを利用した、市民の方の支払い決済～行政への収納連携までのプロセス ４．マイナポータルサービスは本規定の外部サービスの対象外と認識していますが・・
12	ガイドライン改定案	iii -84	1 -①.外部サービスの再定義	例文6.1(22)ソーシャルメディアサービスの利用①(ア)において「当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。」と記載がある。この対策がなりすまし対策に有効である理由を教えてほしい。偽装アカウントにおいても運用組織を偽って記載することは可能と認識している。
13	改定のポイント	3	1 -①.外部サービスの再定義	Sier等の受注者と運用委託契約をし、その契約内で受注者と外部サービス間で約款による契約をしている場合、「改定後の分類」の「１ 業務委託」と「２ 外部サービス」扱いのどちらに該当するかご教示頂きたい。 また、上記１， ２のどちらに該当する場合においても、機密性２以上の情報を取り扱うことが可能な認識で良いか。 ※ISMAP取得有無に応じて機密性２以上の取り扱い可否が異なる場合、そちらについてもご教示頂きたい。
14	改定のポイント	3	1 -①.外部サービスの再定義	LGWAN-ASPは、外部サービスに含まれますか？
15	改定のポイント	3	1 -①.外部サービスの再定義	LGWAN-ASPは、外部サービスに含まれない場合、LGWAN-ASPの選定基準については、何がありますか？
16	改定のポイント	3	1 -①.外部サービスの再定義	「民間事業者等が不特定多数の利用者に対して提供するSNS等の画一的な約款や規約等への同意のみで利用可能となる外部サービス（従来の「約款による外部サービス」）については、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として機密性２以上の情報を取り扱うことはできない点は、従前より変更なし。」の記載について、以下の点についてご教示ください。 ・約款等への同意により利用可能な外部サービスであっても、必要十分なセキュリティ要件を満たしている場合には、機密性２以上の情報資産を取り扱うことが認められるという理解でよろしいでしょうか。 （補足） AWSやMicrosoft365等については、利用形態としては、約款等への同意により利用可能なサービスに該当すると思われますが、ISMAPクラウドサービスリストに登録されていることからも、実質的には、機密性２以上の情報資産を取り扱うことが可能なサービスに位置付けられていると理解しております。一方で、ISMAPクラウドサービスリストに登録されていない外部サービス（約款利用のもの）であっても、SOC2報告書やFedRAMP等を取得しており、一定以上のセキュリティ要件を満たしていることが客観的に評価されている外部サービスについては、機密性２以上の利用を許容していいのかどうか、その取り扱いについて苦慮しています。 約款等への同意により利用可能なサービスについて、機密性２以上の情報を取り扱いを認める場合の条件が不明確であるため、その点に関する解釈について御教示いただけますと幸いです。
17	ガイドライン改定案	iii -148	1 -②.外部サービス利用時のセキュリティ要件	「なお、選定条件となる認証には、ISO/IEC 27017 によるクラウドサービス分野におけるISMS 認証の国際規格がある。また、ISMAP の管理基準を満たすことの確認やISMAP クラウドサービスリスト等のほか、日本セキュリティ監査協会のクラウド情報セキュリティ監査や外部サービス提供者等のセキュリティに係る内部統制の保証報告書であるSOC 報告書（Service Organization Control Report）を活用することを推奨する。」の記載について、以下の点についてご教示ください。 ・ISO27017認証を取得している外部サービスやISMAPクラウドサービスリストに登録されている外部サービス、SOC報告書を取得している外部サービス等については、本ガイドラインにおいて、機密性２以上の情報を取り扱う場合に外部サービス及び外部サービス提供者に対して求めているセキュリティ要件を、一般的には十分に満たしていることが、客観的に評価されていると判断できるという理解でよろしいでしょうか。 （補足） 自治体が独自に外部サービスのセキュリティ対策の実施状況等を確認することは実際には困難であるため、上記の認証等をもって評価し選定することが現実的な対応になるかと考えております。

項番	対象資料	対象ページ	質問分類	御質問
18	ガイドライン改定案	iii -150	1 -②.外部サービス利用時のセキュリティ要件	「（注４）外部サービスには様々なサービスがある。それぞれの外部サービス利用においては、以下に留意する。」について、具体的な内容として、SNS サービス、検索サービス、翻訳サービス、地図サービス、SNSサービスを介したキャッシュレスサービスについて留意事項が記載されていますが、これらについては、外部サービスがISMS認証やSOC報告書等を取得しているかどうかに関わらず、サービスの性質上、一律的に適用される留意事項なのでしょうか。
19	改定のポイント	3	1 -②.外部サービス利用時のセキュリティ要件	「画一的な約款や規約等への同意のみで利用可能となる外部サービスは～（略）～原則として機密性２以上の情報を取り扱うことはできない」とありますが、同意のみのサービスであっても、必要十分なセキュリティ要件を満たすことが確認できれば、機密性２以上の情報を取り扱うことができるという認識でよいでしょうか？
20	改定のポイント	3	1 -②.外部サービス利用時のセキュリティ要件	「画一的な約款や規約等への同意のみで利用可能となる外部サービスは～（略）～原則として機密性２以上の情報を取り扱うことはできない」とありますが、同意のみのサービスであっても、必要十分なセキュリティ要件を満たすことが確認したうえで、同意のほかに何らかの情報にかかる取り交わしをすれば、利用可能という認識でよいでしょうか？
21	ガイドライン改定案	ii -48	1 -②.外部サービス利用時のセキュリティ要件	【8.2.（３）外部サービスの利用に係る調達・契約】クラウドサービスの利用時において、サービス提供者が示す条件への申込によるものではなく地方公共団体が仕様等契約条件を示して入札し契約することを想定しているのでしょうか。
22	ガイドライン改定案	iii - 154	1 -②.外部サービス利用時のセキュリティ要件	(6)外部サービスを利用した情報システムの更改・廃棄時の対策にて、 ②統括情報セキュリティ責任者は、更改・廃棄時における情報の廃棄に係る規定を策定する場合、以下を含む内容を規定すること。なお、情報資産の廃棄は「２．情報資産の分類と管理（2）情報資産の管理⑩情報資産の廃棄」、「4.1.サーバ等の管理（7）機器等の廃棄」を参照すること。 とあるが、令和2年5月22日総行情第77号「情報システム機器の廃棄等時におけるセキュリティの確保について」で通知された機器の廃棄等の方法（物理破壊、磁気破壊、データ抹消等）や確実な履行を担保する方法等について、外部サービスを利用した情報システムの更改・廃棄時では具体的にどこまで求められるのか伺いたい。 ⇒特に「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」について、通知との整合性は確保されるのか？
23	ガイドライン改定案	iii -92	1 -②.外部サービス利用時のセキュリティ要件	（22）（イ）本県ではSNSでの情報配信時に短縮URLを掲載し、URLクリック数を測定して情報への反応率をデータ取得している。このツールでは、URL短縮は必須ではないが、短縮化しないと測定ができない仕組みであり、クリック数計測できないと、そのツールを使用している意味がなくなる。この場合、使用が避けられない場合に該当するか。
24	ガイドライン改定案	iii-91	1 -②.外部サービス利用時のセキュリティ要件	6.1. コンピュータ及びネ ットワークの管理 解説 (21) Web 会議サービスの利用時の対策 ・機密性２以上の情報を取り扱う場合は、可能な限りエンドツーエンド（E2E ）の暗号化を行うこと。 ・機密性２以上の情報を取り扱う場合は、Web 会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、 E2E の暗号化を利用できなくなる機能を可能な限り使用しないこと。 iii-141【趣旨】にて、「画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、（中略）原則として機密性２以上の情報を取り扱うことはできない。」とありますが、冒頭の引用においてWeb会議サービスの機密性２以上の情報の取り扱いが許容されているように見えます。 Web会議サービスは約款や規約により利用するものと認識していますが、機密性２以上の情報の取り扱いが許容されるのか否か、またその整理内容についてご教示いただけますでしょうか。

項番	対象資料	対象ページ	質問分類	御質問
25	ガイドライン改定案	iii-141	1 -②.外部サービス利用時のセキュリティ要件	【趣旨】なお、民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、セキュリティ対策やデータの取扱いなどについて 自組織 への特別な扱い を求めることができない場合が多く、機密性２以上の情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として機密性２以上の情報を取り扱うことはできない。 ほとんどの外部サービスが約款や規約によって利用するものと認識しており、実質的に機密性２以上の情報においては外部サービスでの取り扱いができないことになると考えます。 クラウド・バイ・デフォルト原則が提唱される中、次のようなサービスにおいても、約款・規約によるものは機密性２以上の情報は取り扱えないということでしょうか。具体的に整理された内容をお聞かせください。 ・ISMAP認定されたサービス（kintoneやCisco Webex、Box等） ・LGWAN-ASP クラウド・バイ・デフォルト原則が全ての情報システムをクラウド化するものでないことは承知していますが、上記趣旨の前提により、クラウドサービスの利用が進まないことを危惧しての質問です。複数ユーザに同じサービスを提供することがクラウドサービスの特徴の一つであり、その実現のために約款・規約による利用方法が採用されている状況を鑑みると、約款・規約であることを理由に取り扱いを制限すべきでないと考えます。
26	ガイドライン改定案	iii-143	1 -②.外部サービス利用時のセキュリティ要件	8.2 (2) 外部サービスの選定 ⑥情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。 セキュリティや戦略の観点から、外部サービス提供事業者の委託先事業者の情報提供を求めることは難しいと考えます。具体的に、どの程度の情報の提供を求める想定でしょうか。
27	ガイドライン改定案	iii-154	1 -②.外部サービス利用時のセキュリティ要件	②統括情報セキュリティ責任者は、更改・廃棄時における情報の廃棄に係る規定を策定する場合、以下を含む内容を規定すること。なお、情報資産の廃棄は「 2. 情報資産の分類と管理（２）情報資産の管理 ⑩情報資産の廃棄」、「 4.1. サーバ等の管理（７）機器等の廃棄」を参照すること。 外部サービスにおいては、HDD・SSD等の記録媒体の取り扱いを利用者側で制御できないことから、 iii-53「4.1. サーバ等の管理（７）機器の廃棄等 図表24 情報の機密性に応じた機器の廃棄等の方法」に記載の方法での廃棄が困難です。どのような方法での廃棄が想定されますでしょうか。
28	ガイドライン改定案	iii - 141～144	1 -②.外部サービス利用時のセキュリティ要件	外部サービスの例に記載したサービスのうち、以下の項目について、遵守できない（情報開示されていない、設定ができない等）場合は、各自治体でサービスの利用可否を判断することになるのでしょうか。一定の基準があればご教示いただけないでしょうか。 （２）外部サービス選定 （３）外部サービスの利用に係る調達・契約 （５）外部サービスを利用した情報システムの導入・構築時の対策 （６）外部サービスを利用した情報システムの運用・保守時の対策
29	ガイドライン改定案	Ⅲ-154	1 -②.外部サービス利用時のセキュリティ要件	「②統括情報セキュリティ責任者は、更改・廃棄時における情報の廃棄に係る規定を策定する場合、以下を含む内容を規定すること。なお、情報資産の廃棄は、以下を含む内容を規定すること。なお、情報資産の廃棄は「 2. 情報資産の分類と管理（２）情報資産の管理 ⑩情報資産の廃棄」、「 4.1. サーバ等の管理（７）機器等の廃棄」を参照すること」という記載されているが、オンプレミスと同等の要件を定めるべきということでしょうか。そうだとすれば、実現性の乏しく現実的ではない。
30	改定のポイント	10	1 -②.外部サービス利用時のセキュリティ要件	本改定により，クラウドサービス選定の指標・基準等をお示しいただきましたが，マイナンバー利用事務系及びLGWAN接続系と物理的に分離した閉鎖ネットワーク上で，機密性2以上の情報を取り扱うクラウドサービスのみと外部通信する場合，行政施設とデータセンター間を繋ぐ通信は，次の「VPN 接続による外部との通信」に準拠すればよいのか。 【資料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」（改定案）の第3篇-第2章-3-(4)-⑤「VPN接続による外部との通信」(iii -50ページ)】 ー以下，抜粋ー ⑤VPN 接続による外部との通信 遠隔での情報システム保守により、マイナンバー利用事務系及びLGWAN 接続系についてVPN 接続による通信を許可する場合は、特定通信としての設定がされており、かつIP－VPN 等の閉域網又はLGWAN で接続されなければならない。

項番	対象資料	対象ページ	質問分類	御質問
31	ガイドライン改定案	ⅱ-47、48	1-②.外部サービス利用時のセキュリティ要件	「外部サービス利用判断基準」、「外部サービス提供者の選定基準」は例示される予定はありますか。
32	ガイドライン改定案	ⅲ-144	1-②.外部サービス利用時のセキュリティ要件	約款による外部サービス利用に係る規定の整備は情報セキュリティ管理者が行うこととされていたが、統括情報セキュリティ責任者により統括的に整備する形に変更となるのか（利用者側での規定の整備は不要となるという認識で良いか）。
33	ガイドライン改定案	ⅲ-172ほか	1-②.外部サービス利用時のセキュリティ要件	以前からソーシャルメディアサービスでの機密性2以上の発信は禁止されているが、例えば、関係者間チャットによるコミュニケーション利用は、ソーシャルメディアサービスの範囲か？
34	ガイドライン改定案	ⅲ-55、ⅲ-144ほか	1-②.外部サービス利用時のセキュリティ要件	外部サービスを利用した情報システムの更改・廃棄時の対策で、オンプレミスの機器廃棄との作業の整合性を確認したい。特に、マイナンバー系の業務を外部サービスで運用する場合、機器や情報の廃棄についてはどのように考えているのか？
35	ガイドライン改定案	ⅱ-47～48	1-②.外部サービス利用時のセキュリティ要件	データセンターの設置場所は国内・国外問わずの取扱いとして問題はないか。
36	ガイドライン改定案	ⅱ-47	1-②.外部サービス利用時のセキュリティ要件	インターネット上に個人情報を預けることについて問題はないか。
37	ガイドライン改定案	ⅱ-47	1-②.外部サービス利用時のセキュリティ要件	外国籍の人間が関与することに保安上の問題はないか。
38	ガイドライン改定案	ⅱ-49～50	1-②.外部サービス利用時のセキュリティ要件	「廃棄」はどこまでの処理を指すか ・データセンター内機器の物理廃棄まで求めるのか ・職員の立会いを求めるのか
39	ガイドライン改定案	ⅱ- 47	1-②.外部サービス利用時のセキュリティ要件	改定案に対する意見ではありませんが、改定案8.2及び8.3に追加された「外部サービスの利用に係る規定の整備」に関し、規定の内容は各自治体の考えで異なるものになるかと思いますが、どの自治体においても最低限規定すべき規定例を示していただけるとありがたい（外部サービス利用判断基準や外部サービス提供者の選定基準）。
40	ガイドライン改定案	ⅲ- 93	1-②.外部サービス利用時のセキュリティ要件	「（イ）アカウント乗っ取りを確認した場合には、被害を最小限にするため、（後略）」とありますが、ソーシャルメディアサービスの監視等はどのようにすべきでしょうか。定期的な確認は不要でしょうか。
41	改定のポイント	6	1-②.外部サービス利用時のセキュリティ要件	利用に関する規定の整備について、準則が出る予定についてご教示ください。
42	改定のポイント	5	1-②.外部サービス利用時のセキュリティ要件	シャドーITの具体的な例示などあれば、ご教示ください。
43	改定のポイント	7	1-②.外部サービス利用時のセキュリティ要件	セキュリティ対策の規定の整備について、準則が出る予定についてご教示ください。
44	ガイドライン改定案	ⅱ-47	1-②.外部サービス利用時のセキュリティ要件	(1)④「外部サービス管理者」とは、利用者側の県職員等のことですか。「利用状況の管理」とは、利用実績等を把握しておくようにという趣旨でしょうか。
45	ガイドライン改定案	ⅱ-49	1-②.外部サービス利用時のセキュリティ要件	(5)(イ)導入・構築時においても、扱う「情報の暗号化」が必須ということですか。
46	ガイドライン改定案	ⅱ-92	1-②.外部サービス利用時のセキュリティ要件	(22)「･･･による情報発信」とありますが、ⅱ-34には「･･･の利用」とあり、「･･･の利用」の誤記でしょうか。
47	ガイドライン改定案	ⅱ-154	1-②.外部サービス利用時のセキュリティ要件	②(イ)基盤となる物理機器の廃棄とあるが、機密2以上情報のいわゆる物理的破戒等を、ｸﾗｳﾄﾞｻｰﾋﾞｽ事業者に求めることは困難と思いますが、どのような規程を作れば良いでしょうか。
48	ガイドライン改定案	ⅲ-148	1-③.クラウドサービス選定の指標・基準等	「ISMAPの管理基準を満たすことの確認」とありますが、ISMAP管理基準のすべての資料を確認するにはJIS規格の購入が条件であり、管理基準の内容を自治体ですべてを把握するのは難しいと思われます。「ISMAPの管理基準を満たすことの確認」は事業者に満たしているかを聞取り、確認すればよいという認識でしょうか。

項番	対象資料	対象ページ	質問分類	御質問
49	ガイドライン改定案	iii-148	１-③.クラウドサービス選定の指標・基準等	ISMAPクラウドサービスリストの利用について記載されていますが、このリストに記載されていれば、対象サービスは問題なく利用して良いと考えてよろしいでしょうか。リストに記載されていても注意するべき点や条件があればお教えください。
50	ガイドライン改定案	ii -48	１-③.クラウドサービス選定の指標・基準等	【8.2.（３）外部サービスの利用に係る調達・契約】Web会議やチャットなど、サービス提供者が示す条件への申込みにより外部サービスを利用する場合に、機密性2以上の情報を取り扱う場合は例外措置としての取扱いが適正なのでしょうか。
51	ガイドライン改定案	ii -47	１-③.クラウドサービス選定の指標・基準等	「統括情報セキュリティ責任者は、以下を含む外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規程を整備すること。」また「情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。」とありますが、取り扱う情報の整理や規程を整備することで、各市町村単位でクラウド環境利用についての方針を定めることができる、という認識で良いでしょうか。 また、αモデルを採用している場合は、上記で整理された通信については、特定通信として認められるべきもの、という扱いとなる認識でよろしいでしょうか。
52	改定のポイント	10	１-③.クラウドサービス選定の指標・基準等	自治体で保有する記憶領域についてはデータ消去の基準が設けれ羅れているが、ハウジング以外のクラウドサービス利用について、データ消去はどのような対応をとるべきか。
53	ガイドライン改定案	iii -11・iii -135	１-③.クラウドサービス選定の指標・基準等	外部委託と業務委託が混在しているように思いますが、いかがでしょうか。
54	ガイドライン改定案	iii - 146～147	１-③.クラウドサービス選定の指標・基準等	iii-147の６行目からの「管轄裁判所に関しては、・・・」の段落の、「また、・・・」以降の文章が、直前の説明との関連が分かり難い。「また、」の直後に、「準拠法及び裁判管轄を指定した場合であっても」を挿入するような意味で捉えればよいのでしょうか？
55	改定のポイント	p11	１-③.クラウドサービス選定の指標・基準等	ISMAPの管理基準を満たすことの確認やISMAPクラウドサービスリスト等～を活用することを推奨するとあるが、ISMAPクラウドサービスリストに掲載されていないサービスの場合、 ISMAPの管理基準を満たすことの確認はどのように行うことを想定しているか。
56	ガイドライン改定案	iii -142～145	１-③.クラウドサービス選定の指標・基準等	例文8.2 外部サービスの利用（機密性2以上の情報を取り扱う場合）(1)～(3)における「外部サービス提供者の選定基準」「外部サービス提供者の選定条件」の内容は、あくまでも調達時に考慮しなければならない事項であり、必ず満たす必要があるわけでは無いという解釈でよいか。 例えば「例文8.2.(2)②(エ)」における「外部サービス提供に従事する者の所属・専門性・実績及び国籍に関する情報提供」は、グローバルに展開するクラウド事業者では実現不可能と認識している。
57	改定のポイント	3	１-③.クラウドサービス選定の指標・基準等	米印で記載の約款による外部サービスは機密性２以上の情報を取り扱うことはできないと記載があるが、同資料10ページに記載のISMAPに登録されているサービスであっても同様な認識でしょうか？
58	ガイドライン改定案	iii - 146	１-③.クラウドサービス選定の指標・基準等	「（２）外部サービスの選定」において、「②インターネットを介して提供される外部サービスの利用に当たっては（後略）」とありますので、今後、インターネットを経由した機密性２以上の情報を取り扱うことが可能であると考えて良いのでしょうか。 その場合、機密性２以上の情報を取り扱う場合インターネットVPN、SSL/TLS通信（TLS1.2以上）などでも適切に運用されていることが確認できれば、利用可能と判断しても良いのでしょうか。 また、マイナンバー利用事務系の端末からインターネットを経由した利用も認められると考えて良いのでしょうか。
59	ガイドライン改定案	iii -115	２.情報セキュリティ対策の動向を踏まえた記載の充実	標的型攻撃対策として「入口対策」「内部対策」「出口対策」と明記されましたが、従前の解説よりも具体的な対策方法が想定されているのでしょうか。想定されている場合は、ご教授いただけると幸いです。

項番	対象資料	対象ページ	質問分類	御質問
60	ガイドライン改定案	iii-46～	２.情報セキュリティ対策の動向を踏まえた記載の充実	β、β´モデルを採用する場合、「未知の不正プログラム対策（エンドポイント対策）の導入が有効」とあります。また、各モデルの図のなかに「高度なセキュリティ対策(24時間365日)」「エンドポイント対策」とあります。これらから、「未知の不正プログラム対策（エンドポイント対策）の導入」は、24時間365日の人的監視を伴うEDRの導入を意味しているという認識でよいでしょうか？ 24時間365日の人的監視を伴うEDRの運用コストについて、インターネット接続系1,300台で1,000万円/月との参考見積があります。地方自治体にとっては非常に高額であり、対応に苦慮しております。 人的監視の時間緩和や代替策をご検討いただくことは可能でしょうか？
61	ガイドライン改定案	iii-46～	２.情報セキュリティ対策の動向を踏まえた記載の充実	「インターネット接続系とLGWAN接続系を完全に分離する場合」とは、具体的にどのような状態であれば、完全に分離していると言えるのでしょうか（例えば、①両ネットワークの端末は完全に分離している場合、②両ネットワークがファイアウォールで接続されており特定通信（一部の通信）のみやりとりを許可している場合、など）
62	ガイドライン改定案	ii -27、ii -40	２.情報セキュリティ対策の動向を踏まえた記載の充実	不審メールを受信した場合のインシデント対応における最初に取る行動はどれが正しいのでしょうか 「5.3.(1)①職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。」 「6.4.(3)③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない」 「6.4.(3)⑦⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において LAN ケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。」
63	ガイドライン改定案	ii -5、ii -20	２.情報セキュリティ対策の動向を踏まえた記載の充実	表記ゆれと思われますが意図的に使い分けているのでしょうか。 2.(11)安全が確保された通信だけを許可 3.(2)①必要な通信だけを許可
64	ガイドライン改定案	ii -20、ii -24	２.情報セキュリティ対策の動向を踏まえた記載の充実	3.(3)のβモデル、β´モデルよるインターネット接続系への業務端末の配置と4.3.③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。」との整合が取れていないと思われるが、意図的に使い分けているのでしょうか。
65	改定のポイント	12 （複合機：iii -49，50）	２.情報セキュリティ対策の動向を踏まえた記載の充実	複数のネットワーク系統を1つの機器で管理できるという製品の紹介を受けるが、利用の検討の際に考慮すべき事項は何か。 また、複合機の付属機器については、「インターネット接続系と他系統を共用することはできない」とされているが、その機器を利用して共用することは問題ないか。 例①：RICOH－複合機付属機器（外付け増設インターフェースボックス「タイプM19」） 例②：ハミングヘッズ－資産管理ツールのオプション機能による端末切替機能（「SeP」セパレートオプション） 例③：ストレージ装置について、LGWAN系とインターネット接続系のファイルデータを、論理的な分離を行っている同一ストレージに保存すること
66	改定のポイント	7	２.情報セキュリティ対策の動向を踏まえた記載の充実	オンラインストレージサービスについても適用されるという認識でよいか。また、自治体間で行うファイル等受け渡しについて、一定量を超えた場合の望ましい手法は何か。
67	ガイドライン改定案	iii -43	２.情報セキュリティ対策の動向を踏まえた記載の充実	３．（２）イ項では、（イ）インターネット接続系の 端末からLGWAN 接続系の端末へ画面を転送する方式が記載されているが、仮想コンテナを用いるWeb無害化方式も無害化の手段として認められるでしょうか。
68	ガイドライン改定案	iii -67	３-①.テレワーク実施時のセキュリティ対策	「やむを得ず支給以外の端末を使用する場合は、以下のような対策を実施することが必要である。」との記載があり、具体例として、「支給以外の端末のコンピュータウイルスチェックが実施されていることやファイル共有ソフトウェアの導入がされていないことを情報セキュリティ管理者が確認する」等があげられているが、情報セキュリティ管理者はどのようにして職員のパソコンを確認すればよいのか。特に新型コロナ等で急遽在宅勤務になった場合等は自宅へ行き確認をする必要があるのか。
69	ガイドライン改定案	iii-67、68	３-①.テレワーク実施時のセキュリティ対策	シンクライアント、セキュアブラウザ等の機能により、支給以外の端末に情報を残さない仕組みとする場合であっても遠隔からの命令等により暗号化消去する機能を設ける必要があるのか。

項番	対象資料	対象ページ	質問分類	御質問
70	ガイドライン改定案	ii-34	３-③.Web会議サービス利用時のセキュリティ対策	(21)④～承認を得なければならない。 とあるが、誰からの承認を想定しているか。
71	ガイドライン改定案	ii-34	３-③.Web会議サービス利用時のセキュリティ対策	Web会議サービス利用時の対策③にかかれている会議を主催する場合の対策は理解できるが、外部から招待される場合として、想定されるものには、業者等との打合せも含まれると思われるため、その都度利用申請、承諾を行うというのは個別のメール送受信をすべて管理することに等しく実運用上支障をきたす。ここでいう「必要に応じて」というのはどのあたりを想定しているのか？
72	ガイドライン改定案	iii - 91	３-③.Web会議サービス利用時のセキュリティ対策	インターネット接続系にαモデルを採用している自治体において、インターネット接続系端末にて「機密性２以上の情報を取扱うWeb会議」を開催することは、三層分離の原則を踏まえた総務省ガイドラインの規定上可能でしょうか？ ※政府機関や他自治体等とのWeb会議は基本的にインターネット経由でのアクセスが必要であるが、会議の性質上、機密性２以上の情報（アップロードする会議資料含む）を扱わざるを得ない場合が多いが、αモデルを採用している自治体においては、インターネット接続系端末から参加することにほかない状況にある。
73	ガイドライン改定案	ii-34	３-③.Web会議サービス利用時のセキュリティ対策	外部からのWeb会議招待について、利用申請を必要とするのはなぜか。
74	ガイドライン改定案	ii -34	３-③.Web会議サービス利用時のセキュリティ対策	④外部からWeb会議に招待され利用申請が必要な場合について、具体的にどのような場合に必要か想定があればお示しいただきたい。
75	ガイドライン改定案	iii-91	３-③.Web会議サービス利用時のセキュリティ対策	「(２１)Web会議サービスの利用時の対策」について、ネットワークの負荷やセキュリティ対策の要因で庁内ネットワークの利用が難しいため、別途、モバイル回線やインターネット回線を導入していますが、そうした場合の対策はどのように判断すれば良いのでしょうか。 また、Web会議サービス利用端末でメール、検索やダウンロード等も行うことができますが、どのような対策が必要になるのでしょうか。
76	ガイドライン改定案	ii -91	３-③.Web会議サービス利用時のセキュリティ対策	(21)四つ目のポツ「エンドツーエンドの暗号化を行う」とは、具体的には例えば、どういう対応をすればよいでしょうか。
77	ガイドライン改定案	ii -34、ii -91	３-③.Web会議サービス利用時のセキュリティ対策	(21)②「取り扱う情報に応じ」、四つ目、六つ目のポツ「可能な限り」とありますが、ｺﾛﾅ禍で対面協議が行えない中では、機密2以上の情報をＷＥＢ会議で取り扱うことも許容されるということですか。
78	ガイドライン改定案	iii -38	４.マイナンバー利用事務系から外部接続先	特定通信（片方向）については、LGWAN-ASPサービスも認められるものの、データ移送が認められるのは、現状ではeLTAX、マイナポータル、自治体情報セキュリティ向上プラットフォームのみという認識でよいでしょうか。また、データ移送が認められる外部接続先が増える可能性はありますか。
79	改定のポイント	16	４.マイナンバー利用事務系から外部接続先	図の特定通信の説明に、「「eLTAX」、「ぴったりサービス」、等の十分に安全性が確保…」と記載されていますが、「等」は何を指しますか。 汎用電子申請システムについては、自治体DX推進手順書に関する説明会における質問への回答（令和３年９月８日時点）の質問回答５番で、「各自治体の判断でその他のシステムとの特定通信を行うことを否定するものではない」とありますが、汎用電子申請システム以外で想定されているもの、あるいは逆に明示的に特定通信が認められないものがあればご教示ください。
80	改定のポイント	p16	４.マイナンバー利用事務系から外部接続先	リスク分析について「…地方公共団体の協力のもと…」、また第3会検討会が12月下旬開催とあるが、具体的にどのような分析方法を取られるのか。
81	改定のポイント	16	４.マイナンバー利用事務系から外部接続先	行政手続きのオンライン化に対し、考慮すべきセキュリティ事項はあるか。
82	ガイドライン改定案	iii -39	４.マイナンバー利用事務系から外部接続先	改定案では、マイナンバー系と安全性が確保された外部接続先との双方向通信を行う場合は、「OSの修正プログラムを常時更新する運用や対策を行わなければならない」と記載されていますが、双方向通信は行わず、一方向通信（データの取り込みだけ）を行う場合は、OSの修正プログラムは従来通り適時の適用として良いのでしょうか？

項番	対象資料	対象ページ	質問分類	御質問
83	ガイドライン改定案	iii -39	４.マイナンバー利用事務系から外部接続先	「国等の公的機関が構築したシステム等十分に安全性が確保された外部接続先については、インターネット等からマイナンバー利用事務系との双方向でのデータの移送を可能とする。」とありますが、十分に安全性が確保された外部接続先についてはインターネット経由でのアクセスとなり、今後構築されるガバメントネットワーク経由でのアクセスの対象外となる、という認識でよろしいでしょうか。
84	ガイドライン改定案	iii -39	４.マイナンバー利用事務系から外部接続先	「国等の公的機関が構築したシステム等十分に安全性が確保された外部接続先については、インターネット等からマイナンバー利用事務系との双方向でのデータの移送を可能とする。」とあり、具体的な外部接続先として「自治体情報セキュリティ向上プラットフォーム」が挙がっていますが、LGWAN接続系からも同様に接続可能という認識で良いでしょうか。 接続可能な場合、現在はLGWAN-ASPでのサービス提供ですが、LGWAN側のサービスは今後廃止になるという認識でよいでしょうか。また、LGWAN接続系からの接続において具備すべきセキュリティ要件をご教示ください。
85	ガイドライン改定案	iii -39	４.マイナンバー利用事務系から外部接続先	「マイナンバー利用事務系のサーバ、端末については、ウィルス対策ソフトを導入し、最新の定義ファイルを常時更新する。また、ＯＳの修正プログラムについても最新の修正プログラムを常時更新する運用や対策を行わなければならない。」とありますが、この対象となる端末には、外部接続先との通信が許可されていないマイナンバー利用事務系の端末も含まれている、という認識で良いでしょうか。
86	ガイドライン改定案	iii -39	４.マイナンバー利用事務系から外部接続先	記載のある連携サーバとは申請管理システムを構築する際、DMZ内に構築する連携サーバを指しているのでしょうか。
87	ガイドライン改定案	iii -39	４.マイナンバー利用事務系から外部接続先	連携サーバが申請管理システムの連携サーバを指しているのであれば、申請管理システム等を必ず構築する必要がありますか。 申請管理システム等を構築せず、現在利用しているぴったりサービスのFパターン（JLISのASPサービス利用）を継続利用することも検討しておりますが、セキュリティポリシーガイドラインの改定案上、引き続き利用することは問題ないのでしょうか。
88	ガイドライン改定案	iii -39	４.マイナンバー利用事務系から外部接続先	マイナンバー利用事務系が双方向にデータを移送する場合とは、どんなデータをマイナンバー利用事務系から外部接続先に移送することを想定していますか。
89	改定のポイント	16	４.マイナンバー利用事務系から外部接続先	「ユーザーからの要望等を踏まえ、（略）リスク分析の結果を踏まえて、追加で必要となるセキュリティ対策を記載することで双方向通信を認めるかの判断を行う。※リスク分析については、地方公共団体の協力のもと「制御システムのセキュリティリスク分析ガイド第２版」（ＩＰＡ）を参考に、実際のネットワーク構成、サーバ構成等について事業被害ベースのリスク分析を実施し、分析結果を第３回検討会で報告予定」とあり、決定していないようなニュアンスであるが、双方向は認められたということか。「追加で必要となるセキュリティ対策」は何か。
90	ガイドライン改定案	iii - 39	４.マイナンバー利用事務系から外部接続先	「LGWAN ASP を経由して」という文言を削除した意図は何か。どのような通信経路・システムを想定した判断か。
91	ガイドライン改定案	ii -20	４.マイナンバー利用事務系から外部接続先	①「LGWAN-ASPを経由して」という文言が削除されているが、十分に安全性が確保されたインターネット上のシステム等であれば、マイナンバー利用事務系のシステムとの間で、LGWAN-ASPを介すことなく、直接データの移送を双方向で行ってよいという理解で問題ないか。また、その場合、安全性が確保されたシステム等については国から示されるのか、各自治体で判断することになるのか。
92	ガイドライン改定案	ii -20ほか	４.マイナンバー利用事務系から外部接続先	国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先に向けたアップロードが一部許可された認識である。外部接続先は今後どのように見直し（追加し）ていく方針か？（ガイドライン改定のタイミング？、都度？）また、国等の公的機関が構築したシステム等とそれ以外のシステムの安全性に対する明確な違いはどこなのか？
93	ガイドライン改定案	iii -38～39	４.マイナンバー利用事務系から外部接続先	eLtax端末は強靭性の向上対策のため多要素認証が必要か。必要であればその内容はどのようなものか。
94	ガイドライン改定案	ii -20	４.マイナンバー利用事務系から外部接続先	「ＬＧＷＡＮ-ＡＳＰを経由して～」の文言が削除されているが、ＬＧＷＡＮ-ＡＳＰは経由しなくてもよいということなのか。 （一方資料①Ｐ16の図にある、「今回検討するデータの流れ」だとＬＧＷＡＮ-ＡＳＰを経由しているように見える。）
95	ガイドライン改定案	ii -6	今回改定範囲外	会計年度任用職員及び再任用職員は、非常勤職員に分類されるのか臨時職員に分類されるのか。ご教示願います。
96	ガイドライン改定案	ii -26	今回改定範囲外	非常勤職員及び臨時職員への対応は、職員以上に必要となるか。ご教示願います。

項番	対象資料	対象ページ	質問分類	御質問
97	ガイドライン改定案	iii -88	今回改定範囲外	（13）無線LAN及びネットワーク盗聴対策の「庁内無線LANのセキュリティ要件について」とはどのような文献か。参考にしたいのでご教示願います。
98	ガイドライン改定案		今回改定範囲外	情報セキュリティ実施手順について、市で規定している内容が問題ないか確認するため、最低限記しておくべき事項を教示いただきたい。
99	ガイドライン改定案	ii -20	今回改定範囲外	マイナンバー利用事務系について、通信要件が緩和され、インターネットとの通信を許し、その条件が示されました。LGWAN接続系についても通信要件が緩和され、クラウド等の直接インターネット上のサービスとの通信が許される条件が明確に示されないのはなぜでしょうか？ （クラウドサービス利用拡大が推進される中、マイナンバー利用事務系で直接インターネットとの通信が許されるケースが示されるとなると、庁内でLGWAN接続系でクラウド等のインターネット上のサービスを利用したいという要望に対して、適切な対応が求められます。）
100	ガイドライン改定案	i -3ほか	今回改定範囲外	大項目として「外部サービス」が「外部委託」に変更されているが、委託契約を締結しないサービス利用の形態も包含することに違和感を感じる。なぜ「外部サービス」の記述から変更したのか？
101	ガイドライン改定案	iii -121	その他	以前J-LISから実施されていたように、脆弱性セルフ診断ツール等をご提供いただくことは可能でしょうか。もしくは、J-LISへ提供を提案頂くことは可能でしょうか。
102	ガイドライン改定案	ii-20	その他	現在弊市では、現地調査や訪問相談等の庁外での業務の効率化のためにモバイル端末の導入を検討する部署が増えており、国のガイドラインや弊市のセキュリティポリシーに基づき以下の観点で導入可否の判断を行っているが、モバイル端末を導入する場合の判断基準について御見解をいただきたい。 多要素認証の導入や庁外での外部通信禁止等、十分な安全管理措置を講じられていること、特にマイナンバー利用事務系の情報を取り扱う場合には、個人を特定できないようマスキング加工を施すなど個人情報を端末内に保持しないことを基本的な判断基準としている。 また、現地調査用として導入するモバイル端末はそれ以外の用途では利用しないこととし、庁内でマイナンバー利用事務系のシステムにアクセスして業務用PCとして併用することは、以下の観点から不可としている。 ・ブラウザベースでのシステムであり、マイナンバー利用事務系のネットワークに接続していない状態ではシステムを利用することができないという前提があったとしても、個人情報を含むページがキャッシュとして保持される危険性がある。 ・マイナンバー利用事務系の情報のアクセス対策として、業務毎に専用端末を設置することが望ましいとされている。
103	ガイドライン改定案	ii -10	その他	「8.1 外部委託」は「8.1 業務委託」への修正漏れでしょうか。
104	ガイドライン改定案	iii - 124 iii - 128 iii - 163	その他	外部委託事業者と外部事業者について、違いはありますでしょうか。 既存の文言は外部委託事業者となっていますが、今回追加した文言が外部事業者になっております。
105	改定のポイント	12	その他	追記される「製品の導入だけでは～留意する必要がある。」について、導入する製品は必ずしもＥＤＲである必要は無いのか。