別添３

「地方公共団体における情報セキュリティポリシーに関するガイドライン（案）」に対する意見及びそれに対する考え方

第２章　情報セキュリティ基本方針

番号	該当箇所	提出された意見の概要	意見に対する考え方
1	2.3.　2(2) （17 ページ）	「情報システム」の定義において「コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう」とあるが、例えば下記にある記述を考慮して、媒体の表記を統一していただきたい。 （第３章 3.4.物理的セキュリティ 3.4.1.サーバ等の管理 【例文】(5)　機器の定期保守および修理 「②　情報システム管理者は、記憶媒体を内蔵する機器を外部の事業者に修理させる場合」） 【理由】 「記憶媒体」「記録媒体」の使い分けに特別な意図がなければ、表現を統一するのが良いと考える。 【日本ユニシス(株)】	ご指摘の趣旨を踏まえ、「記録媒体」に表記を統一します。
2	2.3.　3(1) （18 ページ） 3.6.1. （56 ページ） 3.6.1.　(4)② 3.6.1.　(6)② （57 ページ） 3.6.1.　(4) （61 ページ）	「搾取」という用語について p.18　1 行目～2 行目および、p.56　【趣旨】の 2 行目 「重要情報の搾取」という表現がありますが、「搾取」よりも、「詐取」または「窃取」がふさわしいのではありませんか。他の箇所で「窃取」を使用されていますので、「重要情報の窃取」とされてはどうかと思います。 【個人】	ご指摘の趣旨及び「重要インフラの情報セキュリティに係る第 2 次行動計画」（平成 21 年 2 月 3 日　情報セキュリティ政策会議決定）の記述を踏まえ、「詐取」に修正します。

番号	該当箇所	提出された意見の概要	意見に対する考え方
3	2.3.　3(1) （18 ページ） 3.6.1. （56 ページ） 3.6.1.　(4)② 3.6.1.　(6)② （57 ページ） 3.6.1.　(4) （61 ページ）	「重要情報の搾取」という記述があるが、「搾取」という言葉の本来の意味と違う使われ方をしていると思われるので、言い換え（「重要情報の不正取得」など）が必要ではないかと考える。 【鹿児島県】	ご指摘の趣旨及び「重要インフラの情報セキュリティに係る第 2 次行動計画」（平成 21 年 2 月 3 日　情報セキュリティ政策会議決定）の記述を踏まえ、「詐取」に修正します。
4	2.3.　3(2) （18 ページ）	「無許可ソフトウェアの使用等の規定違反」とありますが、文書としての規程を示しているのであれば、下記同様、「規程」としていただきたい。 P45　3.5.1.職員等の遵守事項　【趣旨】 「職員等の故意又は過失による規程違反から生じており」 【理由】 ガイドライン全体を通して「規定」は行為そのものを示し、「規程」は規定された文書等を示しているように読みとれる。 【日本ユニシス(株)】	ご指摘の趣旨を踏まえ、下記のとおり修正します。 45 ページ 3.5.1.　職員等の遵守事項 …情報漏えい事案の多くが、職員等の故意又は過失による規定違反から生じており、職場の実態等を踏まえつつ、職員等の遵守事項を適正に定めるとともに、規定の実効性を高める環境を整備することが重要である。 49 ページ 3.5.2.　研修・訓練 …情報セキュリティに関する事故の多くが、職員等の規定違反に起因している。

第３章　情報セキュリティ対策基準

番号	該当箇所	提出された意見の概要	意見に対する考え方
1	3.1. (2) （22 ページ）	ガイドライン案では「例文において、情報セキュリティポリシーの対象とする情報資産の範囲と情報資産の例は下表のとおりであるが、文書で対象としているのは、ネットワーク、情報システムで取り扱うデータを印刷した文書及びシステム関連文書である。これら以外の文書は、情報資産に含めていないが、文書管理規程等により適切に管理しなければならない。文書一般を情報資産に含めなかったのは、従来電子データ等の管理と文書の管理が、一般に異なる部署、制度によって行われてきた経緯、実態を踏まえたものである。しかしながら、情報資産の重要性自体は、電子データ等と文書の場合で異なるものでないことから、情報セキュリティ対策が進んだ段階では、すべての文書を情報セキュリティポリシーの対象範囲に含めることが望ましい。」とあります。 これについて、社団法人 日本画像情報マネジメント協会では、以下を提言申し上げます。 『全ての情報資産に当該ガイドラインを適用する際には、歴史的価値のある紙文書を除く、全ての紙文書（外部から入手した紙文書も含む）をスキャニングによって電子化文書とすることにより，全ての情報資産を電子化すべきである。 これにより、 (1) 紙文書と電子データの二重管理は不要となり、電子データのみでの情報セキュリティ管理が実施可能となる。 (2) 紙文書では難しい閲覧記録、修正記録に関するアクセスログなど、情報セキュリティ管理に必須な情報が自動的に、容易に管理できる. (3) 紙文書の電子化により、紙文書との二重管理に比べて、事務効率が大幅に向上し、管理コストが低減する。これにより、住民サービス向上の余裕が生まれる。 (4) 政府の ICT 政策目標にある「公務員も毎週 1 日は自宅でテレワーク」を実現するためにも、電子データのみによる情報セキュリティ管理の実施が基本前提となる。』 【(社)日本画像情報マネジメント協会】	情報セキュリティポリシーは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書であり、本ガイドラインはその考え方、内容について解説したものです。 従って、「全ての情報資産を電子化すべき」というご提言については、ご提言として承ります。

番号	該当箇所	提出された意見の概要	意見に対する考え方
2	3.5.1. (1) （48 ページ）	【意見】 「返却時の情報の消去を確実にしておかないと、万一当該パソコンを紛失した場合には、記録されている情報の特定が困難になる可能性が高い。」と記述されているが、記述の主旨が分りにくいので分り易く記述していただきたい。 【理由】 返却時の確実な情報の消去と、パソコン紛失時に記録されている情報の特定が困難な事の関連性を平易に記述するのが良いと考える。パソコン紛失に備えた情報の特定は、パソコンの返却時の情報の消去だけでなく、日常的に管理すべき旨を補足するのが良いと考える。 【日本ユニシス(株)】	ご指摘の趣旨を踏まえ、下記のとおり修正します。 (注 3) 持ち出し専用パソコンによる情報の持ち出しにおいては、万一当該パソコンを紛失した場合に、記録されている情報を容易に特定するため、日常においては当該パソコンに情報を記録をしないようにし、持ち出し時においては持ち出し情報が必要最小限であるかどうか確認を行った上で情報を記録し、返却時においては情報の完全削除をするといった運用を行う必要がある。
3	3.5.2. (2) （50 ページ）	【意見】 「研修計画を通じて職員等の中から将来の情報セキュリティ人材の育成や要員の管理や、メール等によって研修効果を向上させる等」とありますが、研修効果を向上させるための、メール等の具体的な利用方法に言及していただきたい。 【理由】 手段としてのメールの利用方法を例示すると、より実践的に研修効果を向上させる等の施策が講じやすいと考える。 【日本ユニシス(株)】	ご指摘の趣旨を踏まえ、下記のとおり修正します。 (2) 研修計画の立案及び実施 …また、最高情報統括責任者は、研修計画を通じて将来の情報セキュリティを担う人材の育成や要員の管理を行うとともに、地方公共団体の長によるメールでの周知等、研修効果を向上させる施策を講じることが望ましい。
4	3.5.3. (1) 3.5.3. (2) （52 ページ）	○事故、欠陥等の報告について 例文（(1)の②及び(2)の②）では、情報セキュリティ管理者から統括情報セキュリティ責任者に報告が必要なケースが、情報システム関連あるいはネットワーク関連に限られているが、実際には、統括情報セキュリティ責任者への報告の必要性は、これらのケースに限らないと思われる。（当県ではガイドラインの例文と同内容のセキュリティポリシーを定めているが、システム・ネットワークに関連しない事故の際、情報セキュリティ責任者（所属長）から統括情報セキュリティ責任者（当職）への報告を求めるに当たり、根拠付けに苦慮したケースがある。） このため、事故等の場合は必ず情報セキュリティ管理者から統括情報セキュリティ責任者へ報告するよう、例文を変更することが望ましいと考える。 【鹿児島県】	ご指摘の趣旨を踏まえ、下記のとおり修正します。 (1) 庁内からの事故等の報告 ②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。 (2) 住民等外部からの事故等の報告 ②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
5	3.5.4. (1) （54 ページ）	○IC カードの管理について IC カードの紛失時の対応に関する記述はあるが、そもそも、職員等は IC カードを紛失・毀損しないように取り扱うべき旨の規定を追加する必要があるものと考える。 【鹿児島県】	ご指摘の内容については、各地方公共団体において各団体の実情に応じて検討すべき事項と考えます。

番号	該当箇所	提出された意見の概要	意見に対する考え方
6	3.5.4. (3) （54 ページ）	○ID 及びパスワード等の管理について パスワードを記載したメモの作成禁止の規定が削除されているが、これまでメモ作成の禁止を庁内で指導してきた立場としては、違和感がある。 仮に、パスワードの忘失を防ぐためにメモの作成を認める（想像しにくい十分な長さのパスワードであるほど忘失の危険性は高まるので、当県としても、メモの作成を完全に否定するものではない。）のであれば、そのメモの取扱に関する規定が、新たに必要となるものと思われる。 【鹿児島県】	「政府機関の情報セキュリティ対策のための統一基準(第 4 版)」等を参考に、削除したものです。 なお、ご指摘の趣旨を踏まえ、下記のとおり修正します。 3.5.4. ID 及びパスワード等の管理 【例文】 (3) パスワードの取扱い 「パスワードは、他者に知られないように管理しなければならない。」を新規に追加。 (解説) (3) パスワードの取扱い (注意 2) 複数のシステムを取扱う等により、複数の異なるパスワードが必要となる場合があるが、全てを覚えることの困難性から、安易なパスワードを数個使い回すといった運用が起こる可能性がある。 パスワードのメモを作成し、机上、キーボード、ディスプレイ周辺等にメモを置くことは禁止する必要はあるが、特定の場所に施錠して保存する等により他人が容易に見ることができないような措置をしていれば、メモの存在がパスワードの効果を削ぐものではないため、メモの作成を禁止するものではない。
7	3.5.4. (3) （54 ページ）	現在のガイドラインに記載のある「パスワードを記載したメモを作成してはならない。」という規定は、どのような理由で削除されたか。 【神奈川県】	上記 6 番に記載のとおりです。
8	3.6.1. （56 ページ）	○無線 LAN の盗聴対策について 地方公共団体においては、庁舎等における庁外者向けの無線 LAN 接続サービス（いわゆる「ホットスポット」）を提供する例が増加している（当県でも導入予定）ことから、その技術的セキュリティに関する記述を追加することが望ましいと考える。 【鹿児島県】	庁外者向けの無線ＬＡＮ接続サービスの提供に当たっては、ご指摘の技術的セキュリティだけでなく、物理的セキュリティ（無線 LAN アクセスポイントの設置場所、管理等）に関する規定も必要であること、無線 LAN アクセスポイントを踏み台にされた場合の対応等、留意すべき事項があることから、ご指摘の内容については、今後の検討事項とさせていただきます。

番号	該当箇所	提出された意見の概要	意見に対する考え方
9	3.6.1. （59 ページ）	○オンラインストレージサービスに関する記述の追加について 　当県では、平成 22 年度から独自のオンラインストレージサービスを導入し、電子メールの添付ファイルの容量制限を超えるデータの庁内外とのやりとりに利用している。 　今後、他の地方公共団体でも利用の増加が予想されるほか、同様の民間のサービス（●●●●●●等）が既に広く利用されていることから、オンラインストレージサービスの利用に関する記述を追加することが望ましいと考える。 【鹿児島県】	ご指摘の民間のサービスの利用に関しては、意図しない者（オンラインストレージサービスを提供する者を含む。）によるファイルの閲覧等のリスクが存在することから、利用する場合には、3.7.5.に記載の「例外措置」として対応することが望ましいと考えます。
10	3.6.1. (13)⑤ （59 ページ）	国の一部の機関においては、地方公共団体とのファイルの受け渡しの際、民間事業者がインターネット上に提供するフリーのストレージサービスが指定されることがある。（具体例：●●●●●●） 　本ガイドラインでは、外部への不正な情報の持ち出し等を防止する観点から、これらのサービスの利用の禁止が明示されているにもかかわらず、国の一部の機関において利用を推進するような行為は、国・地方公共団体間、相互の情報セキュリティ水準を低下させることにつながるため、利用の禁止を徹底されたい。また、国・地方公共団体間では、LGWAN が整備されているため、この間で、容量の大きいファイルでも受け渡しが安全に行えるよう LGWAN の充実強化が望まれる。 【神奈川県】	国の行政機関については、「政府機関の情報セキュリティ対策のための統一基準(第 4 版)」(2010 年 5 月 11 日 情報セキュリティ政策会議決定）により、「府省庁支給以外の情報システムにより情報処理を行う場合に講ずる安全管理措置についての規定を整備すること。」（「1.4.1.2 府省庁支給以外の情報システムによる情報処理の制限」）とされており、例えば、総務省では「総務省支給以外の情報システムによる情報処理の手順書」を策定し、ファイル交換（保管）サービスに関する取扱いを規定しています。各府省庁においても同様の規定が整備され、当該規定を遵守した取扱いが行われているものと思われます。 　地方公共団体においては、自らが定めた情報セキュリティポリシー等を遵守することが重要であり、止むを得ない場合に限り、3.7.5.に記載の「例外措置」として対応することが望ましいと考えます。 　なお、LGWAN の充実強化に関しては、一義的には LGWAN 運営協議会の場で協議されるべきものと考えますが、今後の参考とさせていただきます。
11	3.6.1. (15)② （59 ページ）	【意見】 ライセンス管理において「導入する際は、ソフトウェアのライセンス管理を徹底しなければならない」とありますが、管理の主体者（主語）を明示いただきたい。 【理由】 組織としてライセンス管理を行うのか、職員個人としてライセンス管理を行えば良いのか、明示することで運用方針の検討が円滑に進むと考える。 組織的に管理を行うことが、法令遵守を、より効率良く推進できると考える。 【日本ユニシス(株)】	ご指摘の趣旨を踏まえ、下記のとおり修正します。 ②職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

番号	該当箇所	提出された意見の概要	意見に対する考え方
12	3.6.3. (1)、(3) （70、71 ページ）	全体的に、大、中、小の項目表記が（1）①（ア）という規則で記述されているが、このページについては、（1）（ア）という表記となっている。（1）①というように修正していただきたい。 【日本ユニシス(株)】	ご指摘のとおり、修正します。
13	3.6.6. （79 ページ）	【意見】 新たなリスクに対する情報収集の項目として、「暗号の危殆化」、「IPv6 移行」、「SW サポートの終了」が記載されている。新たなリスクとしてこの 3 点を選択した理由、およびこの他に候補として挙がっていたリスクについて説明していただきたい。 【理由】 新たなリスクの検討段階で、幾つかの候補が列挙されたと思われるが、3 点が選ばれた背景と、それ以外の候補について補足することで、新たなリスクについての理解が深まると考える。 【日本ユニシス(株)】	本ガイドラインの改定の基となる「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針（第 3 版）」等を参考に、最近の重要な項目を掲載したものです。 なお、ご指摘の趣旨を踏まえ、下記のとおり修正します。 (注 5) 情報セキュリティに関する技術の変化による新たな脅威として、重要インフラ指針(第 3 版)では、下記の事項が挙げられている。
14	3.6.6. (3) （79 ページ）	「IPv6 への移行」などの情報セキュリティ技術の動向等の詳細について約 1 ページに渡り記述したのは、どのような主旨なのか。 【神奈川県】	ご指摘の内容については、上記 13 番に記載したとおり、「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針（第 3 版）」等を参考にしたものです。
15	3.6.6. (3) （79 ページ）	【意見】 「意図しない IPv6 通信の抑止と監視を考慮」という表現が、何を考慮すべきかがわかりにくいことの理由のひとつは、「監視」の対象が何なのかが不明確であることです。「監視」が次の何れを対象としているのかを含め、よりわかりやすい表現にしていただきたい。 1．意図しない IPv6 通信そのもの 2．意図しない通信の抑止（通信遮断） 「意図しない IPv6 通信の監視」の対象が上記の 1．であれば、「3.6.5.不正アクセス対策」でも言及することが可能であると考える。 【理由】 「意図しない IPv6 通信の抑止と監視を考慮」とあるが、何を考慮すべきかがわかりにくい。 【日本ユニシス(株)】	ご指摘の趣旨を踏まえ、下記のとおり修正します。 なお、「3.6.5.不正アクセス対策」への記述に関しては、地方公共団体における IPv6 移行状況が不明であること等から、現在においては必要ではないと考えます。 (注 7) IPv6 への移行については、IPv6 通信を導入する場合における他の情報システムへの影響や、IPv6 通信を想定していないネットワークに接続されるすべての情報システム及びネットワークに対する IPv6 通信を抑止するための措置、IPv6 通信を想定していないネットワークを監視し、IPv6 通信が検知された場合には通信している装置を特定し、IPv6 通信を遮断するための措置を考慮する必要がある。

番号	該当箇所	提出された意見の概要	意見に対する考え方
16	3.7.3. （83 ページ）	本ガイドライン、業務継続計画及びクラウド型サービス（ASP、SaaS 等）など、各種ガイドラインの規程体系（関連性）を明確に示されたい。 【神奈川県】	BCP はリスク発現時の業務継続を目的とした規定であり、BCP の策定時において、情報セキュリティポリシーとの整合性を検討し、必要に応じて情報セキュリティポリシーを見直すことが必要です。 また、ASP・SaaS サービス等の利用に当たり締結する SLA や契約の内容については、各地方公共団体が定めている情報セキュリティポリシーを遵守する内容であるべきと考えます。 なお、「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」（平成 20 年 8 月　総務省）との関連性については、「3.7.3. 侵害時の対応」に、「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）との関連性については、「3.7.4 外部委託」に記載しています。
17	3.7.3.　(2) （84 ページ）	先般、岡崎市において、ずさんな設計で作られた図書館蔵書検索システムが異常をきたし、図書館が当該業者の説明を鵜呑みにして警察に被害届を出し、無実の市民が逮捕されるという事件がありました。 「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」を改訂するにあたっては、このような事態を招来しないような配慮が求められます。 具体的には、異常、侵害を疑う事態においては警察だけでなく、第三者のセキュリティ専門業者や JPCERT コーディネーションセンターなどの機関と相談し、適切な対応をとることを定めるのが肝要かと存じます。 本件はまったく正当なアクセスだったのにプログラムがずさんだったために異常が起きたものですが、このような体制では実際に悪意のアクセスがあった場合に、適切に証拠を確保し対処することはできないことが予想され、不正アクセスにおいてもセキュリティの専門家に相談すること、少なくとも納入保守業者とは独立の業者と相談する体制を整えることが重要と思われます。 岡崎の事件については朝日新聞 http://www.asahi.com/digital/internet/NGY201008200021.html 等で報道されているほか、●●　●●さんが情報を整理公開しています。 http://www26.atwiki.jp/librahack/ 参考にしていただければ幸いです。 【個人】	本ガイドラインでは、情報セキュリティに関する事故、システム上の欠陥等を報告については 3.5.3.（52 ページ）に、不正アクセス等の侵害時については 3.7.3.（83 ページ）に記載しています。 また、この中で、情報セキュリティが侵害された場合等に備え、緊急時対応計画を策定することとしています。 ご指摘の事案のような「情報システム上の欠陥を発見した場合における対応」については、各地方公共団体において、情報セキュリティポリシー等を遵守することが重要であると考えます。 なお、ご指摘の趣旨を踏まえ、下記のとおり修正します。 ②発生した事案に係る報告すべき事項 (注２) 統括情報セキュリティ責任者が事案の詳細な調査を行うに当たっては、必要に応じて外部専門家のアドバイスを受ける、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）等に相談する等、事実確認を見誤らないように努める必要がある。

番号	該当箇所	提出された意見の概要	意見に対する考え方
18	3.7.3. (2)③(イ) （85 ページ）	【意見】 「次の事案が発生し、情報資産を保護のするために」は、「情報資産を保護するために」もしくは「情報資産の保護のために」の誤表記と思われる。 【日本ユニシス(株)】	ご指摘のとおり、「情報資産を保護するために」に修正します。
19	3.7.3. (2)③(ウ) （85 ページ）	【意見】 「情報システムの停止することがやむを得ない場合」は、「情報システムを停止することがやむを得ない場合」もしくは「情報システムの停止がやむを得ない場合」の誤表記と思われる。 【日本ユニシス(株)】	ご指摘のとおり、「情報システムを停止することがやむを得ない場合」に修正します。
20	3.7.4. （87 ページ）	ASP・SaaS など民間事業者が提供するいわゆるクラウド型の情報システムのサービスの利用にあたっては、本ガイドラインの注 6 に記載されている考慮事項のみならず、様々な情報セキュリティ上の課題が指摘されている。 これらのサービスの利用を個々の地方公共団体の判断のみで行うことは、行政機関全体としての情報セキュリティ水準にバラツキを生じさせる原因ともなりうる。 このため、地方公共団体がクラウド型のサービスを導入するにあたっての統一的な取り扱いをガイドライン等にまとめ提示したうえで、本ガイドラインの例文中に基本的な取り扱いに関する規定を明示することが望まれる。 【神奈川県】	クラウド型の情報システムのサービスの利用については、各地方公共団体においてリスク分析を行ったうえで、各団体の実情に応じて検討すべき事項と考えます。 なお、統一的な取り扱いをガイドライン等にまとめ提示することについては、「自治体クラウド推進本部　有識者懇談会」における議論等を踏まえる必要があり、今後の検討課題といたします。
21	3.7.4. (2)⑩ （89 ページ）	【意見】 「外部委託事業者が実施する情報システムの運用、保守等の状況を確認するため、当該委託事業者に監査、検査を行うことを明確に規定しておく」としていますが、下記理由のようなケースもあり、代替手段の選択肢についても言及していただきたい。 【理由】 P37-38 (6)(注 4)に、「地方公共団体職員によるデータセンター内部への立入りがデータセンターのセキュリティポリシーに違反する等、外部委託事業者を訪問できない場合は、訪問調査に代えて第三者による情報セキュリティ監査報告書、外部委託事業者の内部監査部門による情報セキュリティ監査報告書等によって確認する」とあり、物理的なセキュリティ状況を確認する代替手段が記述されている。当該個所との関連性を考慮するのが良いと考える。 【日本ユニシス(株)】	ご指摘の趣旨を踏まえ、下記のとおり修正します。 ⑩市による監査、検査 外部委託事業者が実施する情報システムの運用、保守等の状況を確認するため、当該委託事業者に監査、検査を行うことを明確に規定しておくことが必要である。 なお、地方公共団体において、当該委託事業者に監査、検査を行うことが困難な場合は、地方公共団体による監査、検査に代えて、第三者や第三者監査に類似する客観性が認められる外部委託事業者の内部監査部門による監査、検査によって確認する。

番号	該当箇所	提出された意見の概要	意見に対する考え方
22	3.7.4. (2)⑫ （90 ページ）	【意見】 「ASP・SaaS サービスの利用に関する考慮事項」において言及されている、情報管理の越境問題や国内法の適用問題に加え、P88 の(解説)から続く個々の内容についても、必要に応じて考慮すべき旨、記述を追加していただきたい。 【理由】 平成 22 年 5 月 総務省「スマート・クラウド研究会報告書」において指摘されている「クラウドサービスの課題」を踏まえると、現在は従来の外部委託の考えを、そのまま適用するための合意形成の途中段階と考える。 「スマート・クラウド研究会報告書」では、例えば、個人情報保護法第 22 条の個人データの取扱いの全部又は一部の委託時の監督（P24～P25）や、クラウドサービスの監査との関係（P27）についての検討の必要性の記述があることから、当ガイドライン（案）でも、このような見方があることに言及するのが良いと考える。 【日本ユニシス(株)】	ご指摘の趣旨を踏まえ、下記のとおり修正します。 (注 6) …解析が行われる可能性があることに留意が必要である。 なお、ASP・SaaS サービスの利用に当たっては、契約の形態が従前の委託や請負と異なることが想定されることから、「地方公共団体における ASP・SaaS 導入活用ガイドライン」（平成 22 年 4 月 総務省）を参照されたい。
23	3.8.1. (8) （96 ページ）	【意見】 「総務省が平成 15 年 12 月に策定した『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』及び」とあるのは、今回パブリックコメントを募集している「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」が公表される平成 22 年の公表日を記載するのが望ましい。 【理由】 今回のパブリックコメント反映時には、最新の『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』を参考にする必要があると考える。 【日本ユニシス(株)】	ご指摘の箇所については、策定した年月を記載しているものであるため、原案のとおりとします。
24	3.8.3. （99 ページ）	情報セキュリティポリシーの見直しについて，「毎年度見直しを行い、必要があると認めた場合、改善を行う」との記述があるが、「見直し」という言葉にはもともと「改善」の意味が含まれている（広辞苑：もう一度見て誤りを正す）ので、言い換え（「毎年度実態との照合を行い、必要があると認めた場合、改善を行う」など）が必要ではないかと考える。 【鹿児島県】	ご指摘の趣旨を踏まえ、下記のとおり修正します。 情報セキュリティ委員会は、情報セキュリティポリシーについて情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、毎年度評価を行い、必要があると認めた場合、改善を行うものとする。

その他

番号	該当箇所	提出された意見の概要	意見に対する考え方
1		平成 18 年に分かりやすい表現にしたとなっていますが、そもそも、情報セキュリティの定義がとても分かりにくいと思います。 ポリシーはすべての社員、職員に守ってもらう必要があるため、すべての社員が理解できる分かりやすい表現にする必要あります。 ・機密性…一般の人にもわかる言葉だと思います。 ・完全性…少しわかりにくいと思います。 ・可用性…ほとんどの人が聞いたことがない言葉だと思います。 サーバ等の管理にはクラウドについて触れなくていいのでしょうか。 今後、自らの所有・管理はへっていく流れにあると思いますが。 【個人】	ご指摘の内容については、2.3.（17 ページ）に記載しています。 また、本ガイドラインは、地方公共団体が保有する情報資産の情報セキュリティ確保方針等を定めたものであるので、自ら所有・管理をしていないサーバ等については記載していません。
2		変更の狙いについて 今回追記、削除あるいは変更された理由や狙いを、差し支えない範囲で簡単に説明していただけないでしょうか。今後、当ガイドラインを参考にして自組織の規程を見直すときに、理解の促進につながります。（誤字の訂正、表現の改良など、理由が明らかであったり、些細なものは除く） 【個人】	今回の改定の理由については、1.2.本ガイドラインの経緯（3 ページ）に記載しています。