「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

番号	該当箇所	提出者	提出された意見	意見に対する考え方
1	3.8.1 （解説）(2)⑬(注7) （107ページ）	個人	情報セキュリティポリシーガイドラインの107ページにある「クラウドサービスの利用に関する考慮事項」で、「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」と記述されているが、特定の事業者を選択から排除するようにならないか。もっと選択の自由度が高くできるようにするか、「住民情報等の機密性の高い情報」に対する説明を設け、選択の幅を広げるような記述でも良いのではないか。	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ことを求めており、データセンターの所在地を制限するものではありません。 ご指摘につきましては、今後の参考とさせていただきます。
2	3.4.4【例文】 （45ページ）	個人	以下、情報セキュリティ対策基準の例文に以下追加して頂くようお願い致します。 3.4.4. 職員等の利用する端末や電磁的記録媒体等の管理 ブラウザの閲覧履歴や Cookieを保存しないようにする ブラウザのコンテンツをキャッシュに保存しないようにする Microsoft Officeアプリケーション（Word/Excel/PowerPoint等）の自動回復用ファイルの場所に保存されているファイルを定期的に削除する	取り扱う情報の管理については、「3.3 情報資産の分類と管理方法」並びに「3.4.4 職員等の利用する端末や電磁的記録媒体等の管理」に記載をしております。 個々の具体的な対策については、業務上の実施手順にて記載していただくことを想定しております。
3	3.6.2【例文】 （70ページ）	個人	3.6.2. アクセス制御 マイナンバーにアクセスする端末は、IP接続制限をし、海外サイトに接続できないようにする マイナンバー情報を格納しているサーバーは、海外からの接続させないように設定する	本ガイドラインは、マイナンバー制度等の個別制度に関する具体的なセキュリティ対策ではなく、地方公共団体における全般的なセキュリティ対策について記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
4	3.6.3【例文】 （75ページ）	個人	3.6.3. システム開発、導入、保守等 システム開発、導入、保守を行う業者とは別に、運用前に別の業者によって攻撃ツール等を使用し脆弱性確認を行わなければならない	地方公共団体における個別具体的な対策については、地方公共団体の地域の実情によって対応する必要があるため、ご指摘につきましては、今後の参考とさせていただきます。
5		個人	地方公共団体は、情報公開が基本原則であり、情報を守る（秘匿）というセキュリティーとは矛盾するテーマである。その矛盾に対して、どう折り合いを付けるべきかが書かれていなければ、セキュリティー・ポリシーのガイドラインとは言えないであろう。コンピュータに入っているデータ全てがセキュリティーの対象だなどとは、ありえない。セキュリティー・ポリシーとは方針であり、何をどこまでどのように守るのかの考え方を示すものである。そして、地方公共団体がバラバラにならないためにガイドラインがあるはずである。	ご指摘につきましては、参考とさせていただきます。
6	3.8.3 （111ページ）	地方公共団体	▼3.8.3. SMS（ソーシャルメディアサービス）の利用 今回新たに追加されているが、「SMS」というと携帯電話の（ショートメッセージサービス）の印象が強い。「SNS」（ソーシャルネットワークサービス）の方が一般的な認知度、理解度が高いのではないか。 また、職員個人のアカウントからの投稿による情報漏えいや、不適切な掲載による「炎上」も頻繁に起こっている。公式アカウントだけでなく、職員個人のアカウントへの業務上知りえた個人情報等の投稿の禁止を明示する必要がある。	ご指摘の趣旨を踏まえ、「SMS」は「ソーシャルメディアサービス」に修正いたします。 また、個人アカウントの利用に関するセキュリティについては、服務規程にて記載していただくことを想定しております。
7	3.5.1【例文】(1)④ （48ページ）	地方公共団体	▼3.5.1. 職員等の遵守事項 （1） 職員等の遵守事項④ 上記の点に鑑み、個人端末の業務目的での利用制限だけでなく、個人端末の職務室での利用禁止や、特に個人情報が多く扱われる部署（住基・税など指定するエリア）への持込禁止なども考慮するべきではないか。	個人端末の利用については、「3.5.1 職員等の遵守事項」（解説）(1)②にて、「支給以外のパソコンやモバイル端末等の業務利用」として記載をしております。
8	3.4.2【例文】(2)③ （40ページ）	地方公共団体	▼3.4.2. 管理区域（情報システム室等）の管理 （2） 管理区域の入退室管理等③ 小規模規模自治体では複数のシステムが同一サーバー室内に設置されている例がほとんどであるが、サーバー室の入退室管理はできていても、室内のサーバーラックの施錠ができていない場合がある。システム別にサーバーラックの施錠管理が必要。	ご指摘の趣旨を踏まえ、「サーバラック」の施錠管理についても明確になるよう修正いたします。
9	1.6.1 図表5 （9ページ）	地方公共団体	▼誤字脱字 9Pプロセス図中の「ポリシー」長音記号の縦横	ご指摘箇所につきまして修正いたします。
10		法人	2014年に発生して社会問題になった 株式会社ベネッセホールディングスの情報漏洩対策の中で以下のような点が発表されています。 PCのローカル上に機密性の高いファイルがあったことを定期的にチェックしていなかったことで被害が拡大し大規模な事件に発展しています。 本ガイドラインの中で以下が明記されていないため 同様の事件、問題が発生するリスクが高いと不安視しています。 ・PCのローカル上に機密性の高いデータがあった場合に利用者の指導・監督 ・PCのローカル上に保存された機密性の高いデータの有無を監査する指針 ・PCのローカル上に機密性の高いデータがあった場合の完全削除する指針 ガイドラインに本項目を追加していただき情報漏洩リスクが減るよう指導していただきたいです。 個人情報漏えい事故調査委員会による調査結果のお知らせ http://blog.benesse.ne.jp/bh/ja/news/m/2014/09/25/docs/20140925%E3%83%AA%E3%83%AA%E3%83%BC%E3%82%B9.pdf P10 ---------- 2. 書出し制御設定 (2) 対応状況 今後は、社内 PC のローカルファイルに保存された業務データの有無を自動検索 するソフトを導入する方針である。	機密性に応じた情報の管理については「3.3 情報資産の分類と管理方法」【例文】⑤に記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
11		不明	地方自治体で、一人の職員のIDでログインしたまま他の職員が使っていた実例が明らかになった（ストーカー事件で報道された例）。IDを他人に使用させることを禁止しても、それだけでは物理的に防ぐことはできないし、監査でアンケートやインタビューを採り入れても、そのとき「していない」と答えれば違反を発見できない。 この問題のように、現時点で把握していても十分な対応策がない点について、ガイドラインのとおりにしても万全ではないことをはっきり認識するため、「未解決の課題」等として記載するべきである。	ご指摘の趣旨につきまして、「3.4 物理的セキュリティ」「3.5 人的セキュリティ」「3.6 技術的セキュリティ」に記載しております。 ご指摘につきましては、今後の参考とさせていただきます。

番号	該当箇所	提出者	提出された意見	意見に対する考え方
12	3.8.1（解説）(2)⑬(注7) (107ページ)	法人	意見:「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。」を「住民情報等の機密性の高い情報を蓄積する場合は、暗号化、トークン化等の保全策を講じること等を考慮することが望ましい。」に修正いただきたい。 理由:当該箇所については、本ガイドライン案の検討を行った「地方公共団体における情報セキュリティ対策の向上に関する研究会」において、「府省庁対策基準策定のためのガイドライン」（平成26年5月19日内閣官房情報セキュリティセンター）の「遵守事項4.1.1(1)(a)(ア)「委託先によるアクセスを認める情報及び情報システムの範囲」について」を参考にされたものと理解しております。内閣官房情報セキュリティセンターにおいて「府省庁対策基準策定のためのガイドライン」を改訂されるに当たっては、そのパブリックコメントの過程において、同センターは「海外法令に基づき外国政府等の第三者に情報が提供されるおそれのある場所に個人情報を置くことを不適切な管理の例として示しておりますが、設置場所を国内に限定することを条件とはしていません。」との見解を出されております。元来、機密性の高い情報の保全については、データセンターの設置場所によらず、暗号化、トークン化等の技術的な対策により講じることが望ましいと考えますので、日本国内のデータセンターでの保存を義務付ける原案は修正いただきたく存じます。	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ことを求めており、データセンターの所在地を制限するものではありません。 ご指摘につきましては、今後の参考とさせていただきます。
13	3.8.1（解説）(2)⑧ (106ページ)	個人	(2)契約事項 8再委託に関する制限事項の厳守 外部委託事業者と同等の水準であることを確認し、・・と記載されていますが、システム改修等の場合、再委託先が国内に限らず海外であることも想定されます。再委託先、すべてに対して現地に出向いてセキュリティ対策を確認後でなければ、再委託を認めてはならないとの解釈でしょうか。	再委託先のセキュリティの確実な確保については、外部委託事業者に担保させる旨を記載しております。 セキュリティ対策の手法は様々であり、担保の手法を制限するものではありませんが、外部委託事業者が全ての再委託先の責任を負うことを条件としております。
14	3.4.4（解説）⑥ (46ページ)	法人	地方自治体における近年の情報セキュリティ対策として、以下の3点につき考慮すべきと考えます。 1.個人のモバイル端末利用(BYOD)を考慮したセキュリティ対策 2.社会保障・税番号制度におけるセキュリテイ対策 3.近年の脅威へのセキュリティ対策 上記3点において求められる要件を情報セキュリティポリシーに反映することで、地方自治体のセキュリティレベルの向上に寄与できると考えております。 ＜意見詳細＞ 1. 個人のモバイル端末利用(BYOD)を考慮したセキュリティ対策について 該当項目:3.4.4. 職員等の利用する端末や電磁的記録媒体等の管理　⑥モバイル端末のセキュリティ 要件案:モバイル端末を業務利用する場合は、端末の紛失・盗難対策だけでなく、管理者での一元管理を可能にするモバイルデバイス管理機能や、各アプリケーションに対してポリシーを定義できるモバイルアプリケーション管理機能等を提供すること。 理由:モバイル端末が急激に普及している中、個人のモバイル端末を業務に活用する(BYOD)ことが民間企業を中心に増えてきている。今後地方自治体においても、BYODを活用する機会が増えていくと思われる為、モバイル端末におけるセキュリティ対策を要件として盛り込むべきと考える。特にBYOD環境においては、業務用のデータおよびアプリケーションと私用のデータおよびアプリケーションが混在した状態となるため、例えば本来共有されるべきでない業務用のデータが私用のクラウドストレージに保管されるといったことも発生しうる。こうしたBYOD環境特有のセキュリティリスクに対応するため、モバイルアプリケーション間でのデータの共有などについて制限をかけるような対策についても必要と考える。	BYODについては「3.5.1 職員等の遵守事項」（解説）(1)②に「支給以外のパソコンやモバイル端末等の業務利用」として記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
15	3.6 (60ページ)	法人	2.社会保障・税番号制度におけるセキュリテイ対策について 該当項目:3.6 技術的セキュリティ 3.6.1コンピュータ及びネットワークの管理 に新規追加 要件案:個人番号に関するシステムにおいて、そのデータの移動や複製などの行為が、常に監視され、ログとして保存されていること。 理由:社会保障・税番号制度において付番される12桁の番号が第三者に漏えいすることにより、個人番号を含む特定個人情報が悪用される危険性がある。そのリスクへの対応策として、個人番号を含むファイルに対する操作(作成・コピー・削除)、外部記録媒体への書き出し、外部ネットワークへの送信等に関する一連の行為を記録し、場合によっては不適切な行為をシステム的に禁止するなどして、情報漏えいの防止・抑止をする必要があると考える。また、退職などにより不要となった特定個人情報は削除しなければならないという規則への対応として、退職者の特定個人情報の削除漏れを検出する仕組みについても検討が必要と考える。	本ガイドラインは、社会保障・税番号制度等の個別制度に関する具体的なセキュリティ対策ではなく、地方公共団体における全般的なセキュリティ対策について記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
16	3.6.1【例文】(6) (61ページ)	法人	3.近年の脅威へのセキュリティ対策について (1) 該当項目:3.6 技術的セキュリティ 3.6.1コンピュータ及びネットワークの管理 (6)ログの取得等 要件案:取得した各種ログを定期的に点検又は分析する機能を設け、第三者等からの不正侵入・不正操作等の有無について点検、および分析・監視を実施しなければならない。 理由:外部からの脅威による情報漏えいを防止する為には、ログを取得するだけでなく、複数のログの相関を取る、既知の攻撃元IPアドレスなどとの照合を行うといった分析を行い、リアルタイムでインシデントを検出する仕組みを整備する必要があると考える。	ログの取得、分析、監視については「3.6.1 コンピュータ及びネットワークの管理」に記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
17	3.6.2【例文】(2) (71ページ)	法人	(2) 該当項目:3.6.2　アクセス制御 (2)職員等による外部からのアクセス等の制限 要件案:外部からのアクセスを認める場合、ID・パスワードによる認証だけでなく、ワンタイムパスワード等のその他の認証要素も利用した多要素認証を提供すること。 理由:近年の脅威として、個人が別サービスで利用しているID・パスワードが盗まれ、第三者が不正にアクセスするインシデントが起こっている。このようなインシデントを防止する為に、ID・パスワード以外の別の認証方式を提供することが必要となっている。	外部からのアクセスを認める場合の本人確認については「3.6.2 アクセス制御」に記載しております。 個々の具体的な対策については、業務上の実施手順にて記載していただくことを想定しております。
18	3.4.2【例文】(3)② (41ページ)	法人	該当箇所:P41 3.4.2【例文】(3) ② 意見:②の文章の後にP38 3.4.1(解説)(6)(注4)を入れていただきたい。 理由:外部委託を選択した場合は機器等の搬入出について職員が立ち会うことが出来ない場合があるため、その場合は(注4)に従ってしかるべき対応をすることが適切と考えます。	ご指摘の該当箇所では、庁舎内の管理区域における搬入出について記載しております。 データセンター等、立ち入りができない場所における搬入出については、「3.4.1 サーバ等の管理」(解説)(6)(注4)に記載しております。
19	3.8.1（解説）(2)⑬(注7) (107ページ)	法人	該当箇所:P108 3.8.1(解説)(注7)6行目 意見:「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。」を「住民情報等の機密性の高い情報を蓄積する場合は、当該情報の暗号化、トークン化等の安全策を講じること等を考慮する必要がある。」に修正いただきたい。 理由:当該箇所については、「府省庁対策基準策定のためのガイドライン」（平成26年5月19日内閣官房情報セキュリティセンター）の「遵守事項4.1.1(1)(a)(ア)「委託先によるアクセスを認める情報及び情報システムの範囲」について」に準拠されたと拝察しております。しかし「府省庁対策基準策定のためのガイドライン」の改訂の過程で出されたパブリックコメントの回答において、同センターは「海外法令に基づき外国政府等の第三者に情報が提供されるおそれのある場所に個人情報を置くことを不適切な管理の例として示しておりますが、設置場所を国内に限定することを条件とはしていません。」との見解を出されております。本来、機密性の高い情報の保全については、データセンターの設置場所によらず、暗号化、トークン化等の技術的な対策を講じることがデータを守る上ではより重要と考えます。	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ことを求めており、データセンターの所在地を制限するものではありません。 ご指摘につきましては、今後の参考とさせていただきます。

番号	該当箇所	提出者	提出された意見	意見に対する考え方
20	3.5.4 （解説）(3)（注2） （59ページ）	法人	【意見箇所】 p59：（解説）（3）パスワードの取扱い（注2） 【内容・背景】 原案では、メモは許容するとしていますが、昨今ではパスワードを管理するソフトウェアや管理専用装置などが広く展開されており、昨今の動向を鑑みた許容があっても良いと思います。 【変更案】 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。またパスワード管理ソフトウェアや管理専用装置の利用によって、安易なパスワードの使い回しを行わないようにすること。	ご指摘につきましては、今後の参考とさせていただきます。
21	3.6.1【例文】(6) （61ページ）	法人	【意見箇所】 p61：（6）ログの取得 【内容・背景】 「悪意ある第三者等」の「等」の部分含まれるかもしれませんが、悪意がない場合でも不正操作（本来は権限がないはずの人がアクセスできてしまっている等）が発生する場合があります。 【変更案】 必要に応じて悪意の有無に関わらず第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。	ご指摘の通り、「悪意のある第三者等」の「等」に、誤操作等を含めております。
22	3.6.1【例文】(14) （63ページ）	法人	【意見箇所】 p63：（14）電子メールのセキュリティ管理 【内容・背景】 昨今の攻撃においても、いまだに実行ファイルをそのまま添付するような手法も一定量存在しております。そのため添付データの種類についても、送受信の禁止を示唆しておくと良いと思います。 【変更案】 統括情報セキュリティ責任者は、電子メールに実行ファイルが添付されている電子メールの送受信を配慮しなければならない。	電子メールのセキュリティ管理については「3.6.1 アクセス制御」【例文】（14）（15）、（解説）（14）（15）に記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
23	3.6.1【例文】(17) （64ページ）	法人	【意見箇所】 p64：（17）無許可ソフトウェアの導入等の禁止 【内容・背景】 不正にコピーしたソフトウェアに限らず、昨今では不正に製品を有効にするためのシリアル等を入手して、製品を利用していることがあります。 【変更案】 ③職員等は、不正にコピーしたソフトウェアや不正に入手したシリアル等を利用してソフトウェアを利用してはならない。	不正なシリアルを利用したソフトウェアの利用については、不正にコピーしたソフトウェアの利用の１形態と考えております。 ご指摘につきましては、今後の参考とさせていただきます。
24	3.6.1 （解説）(10) （67ページ）	法人	【意見箇所】 p67：（10）の説明解説 【内容・背景】 某大学での事案にもあった通り、公開が必要なサービスの管理者アカウントやパスワードが適切に管理されているかについて言及すると良いと思います。 【変更案】 エラーメッセージの簡略化(攻撃者に対して、システムの技術情報を過度に表示し、与えない対策)、管理者アカウントやパスワードの適切な管理を実施することによって、防御能力を高めることができる。	管理者アカウントやパスワードの管理については「3.6.2 アクセス制御」【例文】（1）③に記載しております。 ご指摘につきましては、今後の参考とさせていただきます。
25	3.6.1 （解説）(17) （68ページ）	法人	【意見箇所】 p68：（17）無許可ソフトウェアの導入等の禁止 【内容・背景】 昨今ではサイト改ざんの事案も絶えず発生しており、「提供元のサイトの信頼性」自体の理解が難しいのが脅威の現状です。 【変更案】 提供元のサイト等の信頼性が確保できることを確認した上で入手する必要がある。	ご指摘の趣旨を踏まえ、ガイドラインを修正いたします。
26	3.6.2【例文】(5)② （72ページ）	法人	【意見箇所】 p72：仮のパスワード 【内容・背景】 組織によっては、仮発行のパスワードが「12345」のような固定値の場合があります。そのため、仮パスワードにも配慮が必要です。 【変更案】 パスワードポリシーに基づく仮のパスワードを発行し、	パスワードの管理については「3.5.4 ID及びパスワード等の管理」に記載しております。 個々の具体的な対策については、業務上の実施手順にて記載していただくことを想定しております。
27	3.6.5 （解説）(1)（注2） （87ページ）	法人	【意見箇所】 p87：（1）の解説（注2） 【内容・背景】 CSIRT連携が「地方公共団体における庁内のCSIRTと連携」と限定的な連携になっています。CSIRTとは外部連携を担う役割が必要です。必要に応じた外部CSIRTとの連携についても言及する方が良いと思います。 【変更案】 地方公共団体情報システム機構（自治体CEPTOAR）等の関係機関や他の地方公共団体における庁内のCSIRT、また民間企業のCSIRT等の外部CSIRTと連携して情報共有を行うことが望ましい。	ご指摘の趣旨を踏まえ、外部との連携についてガイドラインを修正いたします。