「政府機関の情報セキュリティ対策のための統一基準群(案) 」に対する意見募集の結果の概要

資料 2-2

- 実 施 方 法： NISCのWebページ及び電子政府の総合窓口(e-gov)に掲載して公募
- 実 施 期 間： 2014年1月24日(金)～2月14日(金)
- 意見総数： 52件 【内訳：10企業・団体から延べ46件、4個人から延べ6件】

統一基準群全般に3件、統一規範に2件、運用指針に1件、統一基準に33件の意見提出。

その他、意見募集の対象外である府省庁対策基準策定のためのガイドラインに対しても13件の意見提出。

(1)修正意見 全44件

- 規定内容に係る表現の適正化に関する意見について、趣旨を踏まえて修正(全14件)。
- 他の箇所で規定しているなどの理由で原案どおりとする意見については、理由を付して回答(全30件)。

(2)政策展開に係る意見 全8件

- 今後の政策展開に係る意見については、当センターとしての考え方及び当該意見を今後の参考にする旨を回答(全8件)。

注)提出された意見は必ずしも明確にこれらに分類されるものではないが、事務局で理解した区分にて計上している。

（1）主な修正意見

● 4.1.1項「外部委託」に対する意見

クラウドコンピューティングの規制については、データの自由な移転の確保が非常に重要。

＜意見に対する考え方＞

国境を越えて情報が移転すると適用される法令が変わるため、そうした場合に機密情報が外国政府等に渡るリスクを政府機関は許容できない。

● 4.1.2項「約款による外部サービスの利用」に対する意見

要機密情報を取り扱う場合でもクラウドサービスを利用可能とすべき。

＜意見に対する考え方＞

今般の統一基準改定案において、要機密情報をクラウドサービスで取り扱うことは禁止していないため、誤解。

御意見を踏まえ、4.1.1項「外部委託」及び4.1.2項「約款による外部サービス」の適用範囲が明確になるように、4.1.1項及び4.1.2項の「目的・趣旨」の記載を修正する。（※）

（※）4.1.2項「約款による外部サービス」の「目的・趣旨」は、以下の様に修正（一部省略）。

「外部委託により行政事務を遂行する場合は、原則として4.1.1項「外部委託」にて規定する事項について、委託先と特約を締結するなどし、情報セキュリティ対策を適切に講ずる必要がある。しかしながら、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合には、民間事業者が約款に基づきインターネット上で無料で提供する情報処理サービス等、1.5節において「約款による外部サービス」として定義するものを利用することも考えられる。このような「約款による外部サービス」をやむを得ず利用する場合には、リスクを十分踏まえた上で利用を判断し、本項に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。」

（1）主な修正意見

● 6.3.1項「アプリケーション・コンテンツの作成時の対策」に対する意見

アクセス履歴等の利用に係る情報をcookieを用いて自動的に取得する機能のアプリケーション・コンテンツへの組み込みを、プライバシー侵害の例とすべきではない。

＜意見に対する考え方＞

当該規定は、利用者の意思に反して、アクセス履歴等の利用者等に係る情報が、サービス利用に当たって不必要であるにもかかわらず第三者に提供されることを問題視しているものである。
御意見を踏まえ、「プライバシーに係る情報が本人の意に反して第三者に提供」を、「サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意に反して第三者に提供」に修正する。

● 7.2.2項「ウェブ」（ウェブサーバー導入・運用時の対策に係る規定）に対する意見

「公開するウェブコンテンツを必要最小限にすること。」とあるが、政府が国民に対して情報を公開する重要な手段であり、「必要最小限」にしなければならないというのは修正すべき。

＜意見に対する考え方＞

当該規定は、公開を想定していないファイルや不要なものを削除するよう求めるものであり、本来公開すべき情報の範囲を限定する意図はない。
御意見を踏まえ、「公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。」に修正する。

（2）主な政策展開に係る意見

● 情報通信技術の活用による利便性と情報セキュリティリスクの回避は、どちらを取るかという問題ではなく、いかにリスクを定量化し、それに見合った対策をバランスよく取るかが重要な課題である。（統一基準群全般 リスク評価関連）

●現在の公務員の人事制度や官民連携も考慮に入れ、いかに専門性のある職務に必要な人材を教育し割り当てていくか、必要な人事制度の確立とそのロードマップも示すべき。（統一基準p13-14 教育関連）

● クラウドサービスの情報セキュリティ水準については、事業者が提供する情報セキュリティに関する情報、第三者による監査レポート、一定のセキュリティ認証等を取得したクラウドサービスであるかの確認、情報セキュリティに関連する国際的な規格への準拠及び実績等による判断を可能とすべき。（統一基準p23-26 外部委託関連）

「政府機関の情報セキュリティ対策のための統一基準群(案)」に対する意見募集の結果について

意見募集期間：平成26年1月24日(金)から同年2月14日(金)まで

14者　　52件

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
1	個人	統一規範	第十一条	3ページ	APT攻撃のような動的リスクに実効的に対応するために静的な情報セキュリティ監査に基づく情報セキュリティマネジメントの考え方からISO/IEC 27001:2005に準拠した情報セキュリティリスク常時監視（継続的監視）に基づく情報セキュリティリスクマネジメントの考え方に移行する必要がある。「ISO/IEC 27005:2011情報セキュリティリスクマネジメント」は、リスクマネジメントの共通国際標準ISO 31000／JIS Q 31000」に基づき標準化されているが、そのマネジメントプロセスは、動的なリスク対応のためにリスクアセスメント及び／またはリスク対応が反復的である。また、情報セキュリティリスクの監視及びレビューの対象もリスク要因とマネジメントプロセスの2つのレベルがあり、それぞれのレベルで継続的監視が要求されている。さらに、監視対象のリスク要因としては、資産の価値、影響、脅威、脆弱性及び起こりやすさが挙げられる。 したがって、本統一規範（案）の第十一条を次のとおり修文すべきである。 （監査） 第十一条　各府省庁は、――――確認するため、情報セキュリティリスクの常時監視（継続的監視）に基づく適時な情報セキュリティ監査を行わなければならない。	統一基準群の改定に際しては、国際規格の動向も参考としておりますが、頂きました御意見は今後の検討の参考とさせていただきます。
2	法人	統一規範	第二十条	5ページ	（暗号・電子署名） 第二十条に関連し、 システムのセキュリティは、採用する暗号アルゴリズムだけで守られるものではないことは、広く知られており、極論安全と評価されているような暗号アルゴリズムでも、暗号解読成功していても報告されていない可能性も否定できません。 代表的な暗号を用いたシステムで近年発生した世界的認証機関での不正証明書発行事件等を鑑みれば、自国の独立性維持の観点からも、可能であれば国内の敢えてアルゴリズム非公開の暗号やクリプトレックにリストアップされていないような新技術や新たな設計思想のシステム等も適宜選択できるような記載であるべきと考えます。 関連し、各ドキュメントの文中や章立てで、 　暗号 と記載されているところは、 　秘匿化（暗号等） 又は、 　暗号（秘匿化等） と記載すべきだと考えます。	御指摘の点については、今後の検討の参考とさせていただきます。 また、記載修正の御意見に関しましては、暗号化を含む秘匿性確保を求める場合、秘匿化の手段として暗号化を例示するなど規定を書き分けておりますので、原案どおりとさせていただきます。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
3	個人	運用指針	3	5-6ページ	APT攻撃のような動的リスクに対応するためには従来のPDCAサイクルベースの静的な情報セキュリティ監査に基づく情報セキュリティマネジメントの考え方から指揮統制分野で適用されているOODAサイクルベースの情報セキュリティリスク常時監視（継続的監視）に基づく情報セキュリティリスクマネジメントの考え方に移行すべきである。 したがって、「3　府省庁における情報セキュリティマネジメント」の章は、ISO/IEC 27005:2011国際標準等を参考にして「3　府省庁における情報セキュリティリスクマネジメント」として書き直すべきである。	統一基準群の改定に際しては、国際規格の動向も参考としておりますが、頂きました御意見は今後の検討の参考とさせていただきます。
4	法人	統一基準	全般	ー	【意見者】は、政府が、益々重要性を増している情報セキュリティの問題に関し、政府における情報セキュリティの統一基準をより良いものにするために改定をしていく努力について敬意を表する。サイバーセキュリティに関する政策においては、絶えず進化する脅威に直面するなか、デジタル経済の繁栄に欠かせない情報システムを保護するために市場の力を結集して、急速なイノベーションを活用して対応を進めていくことが求められている。 この点、「政府機関の情報セキュリティ対策のための統一基準」（案）（以下「本統一基準」）及び「府省庁対策基準策定のためのガイドライン」（案）（以下「本ガイドライン」）において、「外部委託」の一形態として、クラウドコンピューティングの利用について記載しているため、重要な論点であると考え、意見を述べる。 【意見者】は、クラウドコンピューティングが、引き続き情報技術分野の中で重要な技術の1つであり、世界におけるクラウドサービスに関する法令及び政策は、クラウドサービスの普及を支え加速させるものであるべきと考えている。クラウドコンピューティングの利点や特性を考えると、データの自由な移転の確保が非常に重要であり、そのため規制は国際的に出来る限り協調すべきであるというのが【意見者】の基本的な考えである。政府は、世界においてクラウドプロバイダーに課される義務の矛盾を最小限にすることに留意すべきである。 また、サイバーセキュリティに関しては、脅威が絶えず進化している以上、情報システムを保護する側にはそれ以上のイノベーションが必要であり、政府の政策においては、技術的中立性が重要となる。何らかの理由により技術を固定化させてしまったり、技術の進歩を遅らせるおそれのある政策を採用すべきではない。 さらに、【意見者】は、現在、世界中において情報セキュリティや個人情報保護の名の下に各国が保護主義に傾くことについて強い懸念を有している。本基準群は、中央省庁のポリシーとして適用され、また、調達の際の仕様にも関わるものであり、政府調達に影響を与えるものであるが、本基準群が、情報セキュリティの名の下に、政府調達に関して保護主義に傾いていないかについても十分考察し、問題があれば修正すべきである。	クラウドサービスの利用に関する規定は、国境の枠組みのもと行政活動を行っている政府がサービスを利用する場合に必要となる差別的ではない条件を列記しているものです。国境を越えて情報が移転すると適用される法令が変わるため、そうした場合に情報が外国政府等に渡るリスクを政府機関は許容できません。 これらの条件を満たすような質の高いサービスが提供されることを期待いたします。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
5	法人	統一基準	全般	ー	文書全体を通して 【意見者】は、内閣情報セキュリティセンターが中心となり、日本政府がより良き社会の実現に向けて情報通信技術を積極的に活用し、業務の効率化、課題の解決に取り組むことに全面的に賛成します。そのためには情報セキュリティ対策は必要不可欠な要素であり、世界規模のデジタル社会基盤(Global Digital Infrastructure)をいかに安全に活用するかは、政府の重要課題のひとつであり、民間にも共通した課題であることから、この文書で述べられている基準は民間への波及効果も大きく、世界から注目される基準であることを述べさせていただきます。情報通信技術の活用による利便性と情報セキュリティリスクの回避は、どちらを取るかという問題ではなく、いかにバランスを取るかが課題であり、危険だから利用しないではなく、いかにリスクを定量化し、それに見合った対策をバランスよく取るかが重要な課題である点も指摘させていただきます。	御指摘のとおり、ITの利便性と情報セキュリティリスクの対策のバランスを取ることは非常に重要であると認識しています。いただいた御意見については、今後の検討の参考とさせていただきます。
6	法人	統一基準	1.2	3-4ページ	1.2 情報の格付の区分・取得制限 （および全般） 従来の政府見解を踏まえて機密性1～3までとしていますが、機密性3は秘密文書にあたる情報であり、防衛省の「省秘」、外務省の「外交秘」などの 外国政府のC/S相当のものから、「特別管理秘密」、「特定秘密」、「特別防衛秘密」などのC/S/TSにまたがるもの、米国のインテリジェンス 情報などのTS/SCI以下と定義される特別なものなどのすべてを包含すると理解しています。 諸外国では日本での機密性3に相当する情報に応じて、システム要件を変えている場合が多く、GSOMIAやSOMIA等に基づき、交換する情報に よっては自国とセキュリティレベルが同様なシステムを要求する国もあると聞いております。 「機密性3」に関するシステム上の要件を、「一般に機密性3の情報を取扱う情報システムに必要な要件」と「機密性3のなかで特に高度で機微な情報 を取扱う情報システムに必要な要件」に区分する、もしくは府省庁共通のガイドライン等への考え方の記載をするのは、いかがでしょうか。	統一基準群は政府機関におけるセキュリティ対策のベースラインを定めているものであり、機密性3情報に関しても一般に必要な要件のみを定めていると御理解頂ければ幸いです。
7	法人	統一基準	1.3	6ページ	該当箇所 ： 用語の定義（「CSIRTとは・・・」） 意見 ： 「インシデント」という用語を分かりやすく定義していただきたい。 理由 ： インシデントが指す内容について、誤解をできるだけ回避する必要があると考えるため。	現時点でISO27000シリーズにおける定義が最も標準的なものであり、これを引用することが誤解が少ないと考えました。他方で、インシデントの定義については専門家の間でも議論が続けられており、NISCとしても動向を注視しているところです。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
8	法人	統一基準	2.1.1	9-10ページ	2.1.1組織・体制の整備 本節において、最高情報セキュリティ責任者の設置、情報セキュリティ委員会の設置、情報セキュリティ監査責任者の設置、統括情報セキュリティ責任者、情報セキュリティ責任者、最高情報セキュリティアドバイザーの設置が遵守事項として明記されています。これらの役務を設置することは大変重要な事で是非早急に実現しその役務、組織が十分に機能するような施策を取ることが重要と考えます。そのためには、それぞれの役務の権限と責任を更に明確化する必要があると考えます。また、現在の公務員の人事制度を考慮した場合、いかに専門性のある職務に必要な人材を教育し割り当てていくか、必要な人事制度の確立とそのロードマップも同時に示すべきかと考えます。必要な人材の育成、権限と責任の明確化がなければ、役職を作るだけの施策となりうる危険が存在します。	各役割の役務についてはガイドラインに記載しているため、原案どおりとさせていただきます。 なお、人材育成や人事制度の確立等については、内閣官房情報セキュリティセンターにおいて「新・情報セキュリティ人材育成プログラム」を策定しております。
9	法人	統一基準	2.1.1(3)	9ページ	2.1.1(3)情報セキュリティ監査責任者の設置 （原文）最高情報セキュリティ責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置くこと。 （修正案）最高情報セキュリティ責任者は、その指示に基づき実施する監査に関する事務を統括する者として、府省庁の情報セキュリティを推進する部局および統括情報セキュリティ責任者から独立した情報セキュリティ監査責任者１人を置くこと。 （理由）政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針（案）、３－３ 点検・見直しに、「なお、点検は客観的な視点から行なわれていると認められることが重要であり、このため点検対象の部門や者から独立した組織又は部門による監査を含めることが必要である。」と記述されている点を、基準において明確にすることが望ましい。 情報セキュリティを推進する部局および統括情報セキュリティ責任者は、情報セキュリティ対策を実施する立場であり、これらから独立した監査が行われるべきである。	御指摘いただいた点につきましては、統一基準「2.1.1(7) 兼務を禁止する役割」において関連規定を明記しているところではございますが、御意見は今後の検討の参考とさせていただきます。
10	法人	統一基準	2.2	12ページ	2.2 運用 情報セキュリティ対策は、攻撃側との技術、知識の競争ということもできます。そこで重要な対策の一つは、情報と知識の共有となります。その実現のために、運用、教育においては、プロセスの透明性の確保により情報、経験の組織間での共有をはかり、さらに民間への波及、すなわち官民連携も視野に入れた仕組みの確立が必要と考えます。縦割りの組織では、経験が活かされず、共有できる知識経験を活かすことができなくなるため、プロセス、意思決定の透明性を確保することが知識と経験を共有するためには重要と考えます。	御指摘いただいた点につきましては、今後の検討の参考とさせていただきます。
11	法人	統一基準	2.2.3	13-14ページ	2.2.3 教育 情報セキュリティ教育は、一般的な情報セキュリティに関する知識から、各組織が扱う情報に特化したものまでいくつかのレベルに分けられます。共通する知識については、組織を超えて基礎的な教育を施すことで省庁全体での基礎レベルを確保し、省毎の差異はその上で教育するなどの、政府機関全体での視野を持った教育を行うべきかと考えます。	共通する知識についての基礎的な研修等は既に実施中ではございますが、御指摘の点については、今後の検討の参考とさせていただきます。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
12	法人	統一基準	2.3.2	16-17ページ	2.3.2 情報セキュリティ監査 （修正案 (1)として追加。現行の(1)以下は繰り下げ） (1) 監査実施環境の整備 (a)最高情報セキュリティ責任者は、情報セキュリティ監査が独立した立場から、客観的かつ公正な監査が行われるように、情報セキュリティ監査責任者および監査実施者の権限を定めること。 (b)最高情報セキュリティ責任者は、情報セキュリティ監査が適正に行われるように、統括情報セキュリティ責任者および府省庁の情報セキュリティを推進する部局ならびに被監査部門に、客観的かつ公正な監査実施のための環境整備および監査への協力について、周知徹底すること。 （理由）政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針（案）、３－３ 点検・見直しに、「なお、点検は客観的な視点から行なわれていると認められることが重要であり、このため点検対象の部門や者から独立した組織又は部門による監査を含めることが必要である。」と記述されている点を、基準において明確にすることが望ましい。	御指摘いただいた点につきましては、統一基準「2.1.1(7) 兼務を禁止する役割」において関連規定を明記しているところではございますが、御意見は今後の検討の参考とさせていただきます。
13	法人	統一基準	3.1.1	19-21ページ	3.1.1 情報の取り扱い 情報の取り扱いに関しては、情報の格付けなどとともに、政府として保管しなければならない情報を誤って削除や紛失することがないように明確に保存期間、保存方法を記録するとともに、個人情報などは必要な期間後には廃棄ができるよう、保存期間を情報に対してそれぞれ明確にすべきと考えます。	御指摘の点については、参考3.1.1-1の完全性及び可用性についての取扱制限の例や遵守事項3.1.1(7)(a)においてお示ししておりますので、原案どおりとさせていただきます。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
14	法人	統一基準	3.1.1(1)	19ページ	3.1.1 情報の取扱い 遵守事項 (1) 情報の取扱いに係る規定の整備 (a) 統括情報セキュリティ責任者は、以下を含む情報の取扱いに関する規定を整備し、 行政事務従事者へ周知すること。 (エ)として、 これまでの統一基準群やその解説書等で記載されている技術等に問題が生じた為の改定ではないことになりますので少なくともそれらの対策や技術等のうち、明確にセキュリティリスクが増大したものは除外し、更に各省庁の実施した公費を用いたセキュリティ対策や新技術等の実証実験で効果を認められた対処 等を、選択の範囲として明確に記載することで実際の現場対処がシンプルにできるようになると考えます。 特に、新たな脅威は、守る側の手段を相手が熟知して行った結果ですので、標準化された技術や仕組み等を選択していれば良いわけではありません。 敢えて、一般化していないような技術や対策を積極的に取り入れることも、攻撃者に対して効果的な対策となります。それが、国産の技術であれば尚喜ばしいことだと考えます。	一般に、技術は多岐に渡り、また日々進歩しているため、採用時点で最良の選択がなされるよう、統一基準では主に性能規定の形で記述しており、また、2.4.1情報セキュリティ対策の見直しにおいて関連規定を明記しておりますので、原案どおりとさせていただきます。
15	法人	統一基準	4.1.1	23ページ	4.1.1 外部委託 目的・趣旨 調査業務や運用支援といった外部委託とパブリッククラウドのサービスはその提供内容が異なります。従って同じカテゴリの中で記載することはかえって混乱を招くため別記載とすべきです。パブリッククラウドサービスの大きな利点の一つに、省をまたがったサービスが低コスト、高セキュリティで提供可能なことがあげられます。 従ってパブリッククラウドについては米国政府の認定制度であるFedRampのようなクラウドを対象とした制度を別途検討すべきです。	4.1.1項の規定は、提供内容にかかわらず求められる要求事項を定めたものであることから、原案のとおりとさせていただきます。 御指摘の認定制度の点については、今後の検討の際の参考とさせていただきます。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
16	法人	統一基準	4.1.1 4.1.2	23、25ページ	4.1.1「外部委託」/4.1.2「約款による外部サービスの利用」の目的・趣旨の記載について 本統一基準4.1.1「外部委託」の目的・趣旨では、「なお、約款による外部サービスを利用し、行政事務を遂行する場合も外部委託の一つの形態と考えられるが、委託先と特約を締結することが難しく、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無いものについては、4.1.2項「約款による外部サービスの利用」を遵守する必要がある。」と記載している。また、本統一基準4.1.2「約款による外部サービスの利用」の目的・趣旨では、「約款による外部サービスを利用し行政事務を遂行する場合、4.1.1項「外部委託」にて規定する事項を特約として締結するなどし、情報セキュリティ対策に努めるべきである。しかしながら、約款による外部サービスでは特約の締結等ができず、必要とする情報セキュリティに関する十分な条件設定ができない場合が多く、サービスの継続性が保証されていない、データの保管場所やバックアップ方法が不明であるなど、利用に当たってのリスクが高いことから、要機密情報を取り扱う可能性がある場合においては利用すべきではない。」と記述している。これらの記述によれば、クラウドサービスでは、特約、即ち個別の約束が出来ないために、一般的に情報セキュリティリスクが高いように読めるが、これは、クラウドサービスの正当な評価とは言い難く、また要機密情報を取り扱う可能性がある場合に全て利用すべきでないと取れる書き方は行き過ぎであるから、修正すべきである。 即ち、約款の内容（情報セキュリティや個人情報保護に関する約束を含む）は、各クラウドサービスによって千差万別であるから、約款サービスであっても、約款及びサービスの内容を吟味のうえ、セキュリティに関する対策、サービス継続性、データ保管場所、バックアップ方法が明確になっていて十分であれば、要機密情報を取り扱う場合では利用可能と明記すべきである。 また、約款か個別契約かという契約手法の論点と情報セキュリティの水準の問題は全く別物であるため、両者を分けた精緻な議論が必要である。さらに、クラウドサービスのデータ保管やバックアップ方法に関する情報セキュリティ水準については、事業者が提供するクラウドサービスの情報セキュリティに関する情報、第三者による事業者の監査レポート、情報セキュリティに関連する国際的な規格への準拠及び実績等により判断が可能であるため、これらの情報によりメリットとデメリットを判断するような基準を記載すべきである。クラウドサービスの情報セキュリティ対策技術は日々進化している。もし、国際的に採用されていない日本特異な要求事項を盛り込んだ特約の締結を求める場合には、むしろ、日本におけるイノベーションを阻害し、また、サービス品質、技術水準の高さや機能に基づいて各省庁が合理的にサービスを選択することを妨げてしまうおそれがある。	要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合に限定して4.1.2項を規定しております。 御指摘の「約款サービスであっても、約款及びサービスの内容を吟味のうえ、セキュリティに関する対策、サービス継続性、データ保管場所、バックアップ方法が明確になっていて十分」なクラウドサービスであっても、要機密情報を取り扱う場合には、4.1.1項の遵守を求めております。 御指摘の点を踏まえて、4.1.1項及び4.1.2項の目的・趣旨について、適用範囲が明確になるよう修正いたします。
17	法人	統一基準	4.1.1 5.1.2	23-25ページ 27-28ページ	委託先、再委託先及びサプライチェーンに対する情報セキュリティ対策の着実な実施を要求することについては、今後、具体的な判断基準を示すとともに、調達仕様書・契約書のひな形等、実務レベルでの具体化をお願いしたい。 それらの検討の際は、有識者に加えて、委託先（受託者）である民間企業もぜひ参画させていただきたい。	御指摘の点については、今後の実施手順の整備等の際の参考とさせていただきます。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
18	法人	統一基準	4.1.1 5.1.2	24、28ページ	「意図せざる変更が加えられないための管理体制」(4.1.1)、「不正な変更が加えられない管理」(5.1.2)ガイドラインによると、これらの管理について確証の提出を要求しているが、委託先が既に取得している第三者認証（例えばISO/IEC27001等）で代用できる旨の追記を検討いただきたい。	情報システムのセキュリティ要件は、取り扱う情報の格付及び取扱制限、対象とする業務の特性等によって求める水準が異なるため、委託先が既に取得している第三者認証（例えばISO/IEC27001等）のみをもって代用可能とすることは不適切であるため、原案のとおりとさせていただきます。
19	法人	統一基準	4.1.1(2)	24ページ	4.1.1(2)(a)(エ)「委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供」について 統一基準(案)において、役員の情報や委託事情従事者の国籍に関する情報提供を委託先に求め、ガイドライン(案)ではその理由を「意図せざる変更が加えられないための管理体制」等を確認する際の参照情報として用いるためとしています。 しかしながら、役員の情報や委託従事者の国籍に関する情報は、「意図せざる変更が加えられないための管理体制」が確保されているか否かの判断には必要以上の情報であると思われます。 むしろ、成年被後見人等の欠格条項を明確にし、当該条項に該当しない旨の誓約を得ることで十分であり、適当と思われます。	サプライチェーン・リスクを担保する上で必要な管理体制を確保するために、企業情報や従業員の背景情報を確認することは、システムライフサイクル管理の国際規格ISO15288等でも用いられている標準的な手法であると考えます。
20	法人	統一基準	4.1.1(2)	24ページ	4.1.1(2)(a)(カ) 外部委託に係る契約「情報セキュリティ対策の履行状況の確認」 情報セキュリティ対策の履行状況の確認については、第三者による事業者の監査レポート、国際規格への準拠状況、クラウド事業者が提供する様々な資料の活用を推進していくべきである。クラウド事業者に個別のレポート提出・面談を求めるなど、クラウドサービスのコストメリットを減殺するような確認方法を仕様としないようお願いしたい。 例えば、Cloud Security Alliance’s Star Registryというプロジェクトでは、クラウド事業者が当該クラウドサービスで行われているセキュリティ管理に関する資料を提供することにより、全般的なクラウドのセキュリティ向上と、クラウド利用者がクラウドサービスのセキュリティについて知る機会の提供に取り組んでおり、このようなクラウド事業者と利用者の協働を促進していくべきである。	情報セキュリティ対策の履行状況の確認方法については、本規定を踏まえて調達者が必要な仕様を定めることになります。 なお、コストメリットのために情報セキュリティ確保について妥協を図ることは得策ではないと考えております。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
21	法人	統一基準	4.1.1(2)	24ページ	4.1.1(2)(b) 外部委託に係る契約「情報セキュリティ監査の受入れ」 本統一基準は、必要に応じて、情報セキュリティ監査の受入れを仕様に含めるべきであるとしている。しかしながら、以下の理由により、情報セキュリティ監査を契約当事者である政府担当者が行うことを政府調達の仕様に含めるべきではなく、当該規定は削除されるべきである。 まず、政府の担当者が、情報が保管・運用されているデータセンターにおいて実際に監査する実地監査を要求することは、実効性の観点からも適切でない。政府担当者の情報セキュリティ監査の手間と旅費等の別の制約要因によってデータセンターの日本国内設置義務を規定したのと同様の効果となるので、当該規定は削除すべきである。 政府担当者が単にデータセンターを見聞しただけで得られる情報は非常に限定的であり、そのメリットは少ない。安易に情報セキュリティ監査受入れの名目で、各契約当事者をデータセンターの中に立入りさせる運用自体、情報漏洩のリスクにつながってしまう。さらに、データセンターの日本国内設置義務につながる規定について合理的な根拠なくしてグローバルに展開されるクラウドサービスの利用を阻害することになる。 クラウド事業者が実際に情報セキュリティに関して信頼性の高いサービスを提供しているかどうかは、各契約当事者ではなく第三者による事業者の監査レポートや実績等により十分に確認可能であるため、各省庁は実地監査ではなく、多様なこれらの情報により確認するのが妥当である。また、複数の利用機関からの監査の受入れは、それ自体が重大なセキュリティ懸念を生じうることから、国際的な機関による代表代理監査を許容可能とすべきである。	4.1.1(2)(b)(ア)の情報セキュリティ監査の受け入れについては、データセンタに限らず外部委託全般を対象にしており、また、「取り扱う情報の格付等を勘案し、必要に応じて」仕様に含めることを求めているものであることから、削除することは不適当であり、原案のとおりとさせていただきます。 なお、一方通行ではなく相互信頼が醸成されてはじめて有効な契約が成立し、政府機関による外部サービスの利用が可能になるものと考えます。また、監査は信頼性確認のために行うものであり、手段は必ずしもデータセンターの物理的見聞に限られないと考えております。
22	法人	統一基準	4.1.2	25-26ページ	4.1.2 約款による外部サービスの利用 本節で記述されている内容は、いわゆるクラウドサービスの利用を含むものと読み取れます。現在の記述では、データの管理場所がわからない、バックアップの方法が不明などの理由からすべてのサービスを利用すべきでないという記述となっています。クラウドサービスを利用すべきではないと取られる文言は政府方針に反しており、さらに諸外国の方針からも大きく異なり誤解を生む記述となっています。クラウドサービスについて諸外国においては政府機関が積極的に利用する事ができるような認証制度の確立や評価制度が利用されていることを鑑みると、この記述は情報通信技術利活用の視点から逆行しているといわざるを得ません。以上より本節はクラウドサービスを安全に積極的に利用する視点から全面的に書き換えることが適切と考えます。 また、クラウドサービスを外部委託契約で利用する場合、4.1.1の遵守事項(2)(b)にある情報セキュリティ監査の受け入れを求めることは、参入障壁となる場合もあるため、他の手段により実現することを検討すべきと考えます。	4.1.2項はクラウドサービスの利用を禁止することを意図した規定ではありません。御指摘の点を踏まえて、4.1.1項及び4.1.2項の目的・趣旨について、適用範囲が明確になるよう修正いたします。 また、4.1.1(2)(b)(ア)の情報セキュリティ監査の受け入れについては、「取り扱う情報の格付等を勘案し、必要に応じて」仕様に含めることを求めているものであることから、原案のとおりとさせていただきます。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
23	法人	統一基準	4.1.2	25ページ	4.1.2 約款による外部サービスの利用の目的・趣旨について 統一基準(案)において、約款による外部サービスは、利用に当たってのリスクが高いことから、要機密情報を取り扱う可能性がある場合においては利用すべきではないとし、ガイドライン(案)で想定されるリスクが列挙されています。 しかしながら、約款による外部サービスの内容によっては、例えば、国内のデータセンターの利用の選択が可能であったり、何重にも情報のバックアップを図ることができたり、情報を確実に消去することができる等の機能を有するものもあります。つまり、本来は、約款であるが故にセキュリティリスクが高いという関係は成立しないものです。したがって、約款か個別の契約によるかという契約手法によって情報セキュリティの水準の高低を見積もることは本来手法として正しくないと思われます。 2021年度を目途に原則全ての政府情報システムをクラウド化するとの政府目標を達成するためには、要機密情報を約款による外部サービスにおいて一律に制限することなく、個別の約款の内容による外部サービスのリスク低減の内容や程度に応じて、取り扱うことができる情報の機密性を拡大するようなきめの細かい考え方をベースとして、統一基準（案）とガイドライン（案）に大幅に改定すべきと考えます。実際、ガイドライン(案)では、やむを得ず要機密情報を約款による外部サービスにおいて取り扱う場合、サービス提供者のサービス提供形態により回避可能なリスクもあることから、約款、利用規約等の詳細を確認するなどして例外措置の可否を判断することが重要であると記載されていますが、かかる考え方こそを政府基準（案）「4.1.2約款による外部サービスの利用」の目的・趣旨等に基本的考え方として記載することが望ましく、要機密情報を取り扱う可能性がある場合においては利用すべきでないとの一律の考え方を基本に置くべきではないと考えます。	本基準において、「約款による外部サービス」は、1.5節で「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く」ものとして定義しており、御指摘の「約款であるが故にセキュリティリスクが高いという関係」を一律にはお示ししておりません。 本規定では、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合に限定して「約款による外部サービス」を利用することを認める趣旨であり、約款サービスであっても、要機密情報を取り扱う場合等には、4.1.1項の遵守を求めております。 御指摘の点を踏まえて、4.1.1項及び4.1.2項の目的・趣旨について、適用範囲が明確になるよう修正いたします。
24	法人	統一基準	4.1.2	25ページ	4.1.2 約款による外部サービスの利用 目的・趣旨 「サービスの継続性が保証されていない、データの管理場所やバックアップ方法が不明であるなど、利用に当たってのリスクが高いことから、要機密情報を取り扱う可能性がある場合においては利用すべきではない。」とありますが、コストや国民の利便性を鑑みた場合、通常の情報システム以上の対策が実施されているクラウドサービスもあるため以下のような表現をご提案します。 ⇒「要機密情報を取り扱う可能性がある場合においては利用にあたってのリスクを押さえるため、サービスの継続性が保証され、データの管理場所やバックアップ方法を明らかにしている外部サービスあるいはSOC1,2など国際基準の認定やJASA(今年より開始予定)の認定などがあるなどの条件を付与して利用すべきである」	本規定は、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合に限定して「約款による外部サービス」を利用することを認める趣旨であり、約款サービスであっても、要機密情報を取り扱う場合等には、4.1.1項の遵守を求めております。 御指摘の点を踏まえて、4.1.1項及び4.1.2項の目的・趣旨について、適用範囲が明確になるよう修正いたします。 また、国際基準等の認定の利用については今後の参考とさせていただきます。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
25	法人	統一基準	4.1.2	25ページ	4.1.2 約款による外部サービスの利用 遵守事項 要機密情報が取り扱われないようにすること、とありますが、世界的には各国の規制こたえるためには、データが失われた時の暗号化は当然の措置と思われるようになっています。多くの場合，データが十分暗号化されているか「判読できないように処理」されており暗号化Keyがユーザの管理下にある場合，この規制では告知，法的責任からのセーフハーバー免責があると認識します。多くの規制（PCI を除く）は特に暗号化を求めていませんが，暗号化は解決策の一部であること，漏洩通知という最大のリスクを除去できるものとして推奨しています。従って暗号化を適用した場合の機密情報のレベルが下がることを前提として検討すべきです。すなわち、要機密情報のうち機密性2までは取り扱えると考えます。 例えば米国政府のFISMA規定ではパブリッククラウドでmoderate認定を受ければ機密性中程度(機密性2相当)まで扱えるようになっています。	本規定は、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合に限定して「約款による外部サービス」を利用することを認める趣旨であり、約款サービスであっても、要機密情報を取り扱う場合等には、4.1.1項の遵守を求めております。 御指摘の点を踏まえて、4.1.1項及び4.1.2項の目的・趣旨について、適用範囲が明確になるよう修正いたします。
26	法人	統一基準	4.1.2	25ページ	4.1.2 約款による外部サービスの利用　遵守事項 コストや国民の利便性を鑑みた場合、通常の情報システム以上の対策が実施されているクラウドサービスもあるため以下のような表現をご提案します。⇒「要機密情報を取り扱う可能性がある場合においては利用にあたってのリスクを押さえるため、サービスの継続性が保証され、データの管理場所やバックアップ方法を明らかにしている外部サービスあるいはSOC1,2など国際基準の認定やJASA(今年より開始予定)の認定などがあるなどの条件を付与して利用すべきである」	本規定は、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合に限定して「約款による外部サービス」を利用することを認める趣旨であり、約款サービスであっても、要機密情報を取り扱う場合等には、4.1.1項の遵守を求めております。 御指摘の点を踏まえて、4.1.1項及び4.1.2項の目的・趣旨について、適用範囲が明確になるよう修正いたします。 また、国際基準等の認定の利用については今後の参考とさせていただきます。
27	法人	統一基準	4.1.2(2)	25ページ	4.1.2(2) 約款による外部サービスの利用における対策の実施 「クラウドサービスでは要機密情報が取り扱われないように規定すること」「利用に当たってのリスクを認識した上で約款による外部サービスの利用を申請」と記載されており、これは、クラウドサービスは一般的にオンプレミスの情報システムに比べてよりリスクが高いと誤解を与えるうえ、クラウドにおいて特約が締結されない限り要機密情報を扱ってはならないという規定は設けるべきでなく、これらの記載は修正されるべきである。 約款という契約手法と情報セキュリティの水準に論理的関係性がないことは前記のとおりである。また、クラウドサービスにおいては、大規模なデータセンターを運用する中で日々得られるノウハウに基づきイノベーションが起こっており、最新の情報セキュリティ対策がなされていることから、個々の情報システム担当者や委託先のベンダーがオンプレミスで管理する個別の情報システムよりも高い情報セキュリティ対策がなされていることも多いというメリットがある。従って、クラウドサービスの利用にあたっては、情報セキュリティの観点も含めて、オンプレミスの情報システムとのメリット・デメリットを十分に比較衡量すべきであるが、一般的にクラウドサービスの方がリスクが高いとの記載は、クラウドサービスの正当な評価とは言い難いので修正すべきである。これにより、政府情報システムにおけるクラウドサービスの利用を遅らせ、TCO（Total Cost of Ownership）のメリットを十分に享受できないこととなれば、国民に過大な財政負担を強いることになり適切でない。	本基準において、「約款による外部サービス」は、1.5節で「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く」ものとして定義しており、一般的に、約款に基づき契約を行うサービスの情報セキュリティリスクが高いと一律にお示ししたものではございません。 本規定は、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合に限定して「約款による外部サービス」を利用することを認める趣旨であり、約款サービスであっても、要機密情報を取り扱う場合等には、4.1.1項の遵守を求めております。 御指摘の点を踏まえて、4.1.1項及び4.1.2項の目的・趣旨について、適用範囲が明確になるよう修正いたします。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
28	法人	統一基準	4部全般	23-26ページ	統一基準（案）及びガイドライン（案）では、パブリッククラウド等外部サービス利用による情報処理業務を外部委託の例の一つと位置づけ、従来型の情報システムの開発等と同列に取扱い、各省庁の統括情報セキュリティ責任者等に遵守させる事項を規定する内容となっています。加えて、約款によるサービスは特約の締結ができないものと一律に定義して、利用に当たってのリスクが高いことから、要機密情報を取り扱う可能性がある場合には利用すべきではないと規定しています。 しかしながら、パブリッククラウド等の外部サービスは、例えば、以下のように従来型の情報システムの開発等の外部委託とは本質的に異なるものであることを踏まえて、情報システムの開発等とは全く別建ての遵守事項の記載とするように全面的に規定し直すべきであると考えます。 －従来型の情報システムの外部委託は、個々の省庁によるニーズが異なるために、一定の遵守事項の下に個々の省庁によるセキュリティ対策が重視されるが、パブリッククラウド等の外部サービスは複数の省庁による利用のニーズが想定され、政府内での一貫性のあるセキュリティ対策を講じた方が、各省庁が個々にセキュリティ対策にリソースを割くよりも時間とコストを大幅に節約することができること。 －外部委託に当たっては、委託先が府省庁対策基準の該当項目を遵守し得る者であることが前提となっているが、サーバ装置や通信回線などハードウェアに伴うセキュリティ対策をパブリッククラウドのサービス提供者に個別に要求したり、委託先であるパブリッククラウドへの立入検査を要求したりすることは合理的ではない（立入検査の名目で契約当事者が立ち入ること自体、セキュリティ上のリスクを高めることになりかねない）。パブリッククラウドを利用する場合には、一定のセキュリティ認証等を取得したクラウドサービスなのかどうかを確認し、むしろ各省庁はコンテンツの暗号化対策などのセキュリティ対策に注力すべきであること。 －約款によるサービスを利用する場合であっても、例えば、サービス提供者が保存された情報を自由に利用できないサービスもあり、一部のサービスの特徴をもってして約款による外部サービス全体についてリスクを断ずることは適当ではなく、むしろ政府が統一されたリスク管理の考え方の下に外部委託可能なセキュリティ要件を定めることで、当該要件を満たす約款による外部サービスをサービス提供者が提供することが可能となること。 したがって、米国において統一されたリスク管理アプローチの下に構築されているFedRAMPのようなクラウドサービスのセキュリティ評価、認可、継続的なモニタリングの標準化されたアプローチを提供するプログラムを日本においても構築し、当該統一基準（案）及びガイドライン（案）に反映させるべきです。それは、2021年度を目途に原則全ての政府情報システムをクラウド化するとの基本方針が盛り込まれた「世界最先端IT国家創造宣言」を実現するためにも必要不可欠なことであると考えます。	本基準において、「約款による外部サービス」は、1.5節で「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く」ものとして定義しており、御指摘の「約款によるサービスは特約の締結ができないもの」と一律にお示ししたものではございません。 また、4.1.1項の規定は、外部委託の形態にかかわらず求められる要求事項を定めたものであることから、原案のとおりとさせていただきます。 本規定は、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合に限定して「約款による外部サービス」を利用することを認める趣旨であり、約款サービスであっても、要機密情報を取り扱う場合等には、4.1.1項の遵守を求めております。 御指摘の点を踏まえて、4.1.1項及び4.1.2項の目的・趣旨について、適用範囲が明確になるよう修正いたします。 なお、「パブリッククラウドを利用する場合には、一定のセキュリティ認証等を取得したクラウドサービスなのかどうかを確認」、「米国において統一されたリスク管理アプローチの下に構築されているFedRAMPのようなクラウドサービスのセキュリティ評価、認可、継続的なモニタリングの標準化されたアプローチを提供するプログラムを日本においても構築し、当該統一基準（案）及びガイドライン（案）に反映させるべき」等の御意見については、今後の検討の参考とさせていただきます。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
29	法人	統一基準	6.1.5	36ページ	6.1.5 暗号・電子署名，遵守事項(1)(a)(ア) 要機密事項は、機密性2以上の情報を指し、「漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報」となってい ます。昨今の情報漏えい事故を鑑み、また、暗号化処置のためのシステム整備費用も低下している状況かにおいては、要機密情報の暗号化は、「必要があるとみとめたとき」でなく、「原則として」等、より強い表現にすべきだと考えます。また、情報の暗号化に際しても、機器や媒体の窃盗に対しては（HDD等）ストレージの暗号化が有効ですが、rootのようなOS特権を得て、情報にアクセスした場合は、ストレージの暗号化は無力ですので、ファイルの暗号化やDBの暗号化を脅威に会わせて対策をとるべきと考えます。	要機密情報を扱う環境は府省庁によって異なっており、例えば通信回線がつながっていない端末について、限られた行政事務従事者しかアクセスが許されておらず、かつファイルの書き出しや用途等の管理が厳重にチェックされている環境下では、要機密情報であっても、暗号化を行う機能と同等の情報セキュリティ効果があると見做すことが出来るとの観点から、原案どおりとさせていただきます。 なお脅威に合わせたファイル及びDBの暗号化による対策については、今後の検討の参考とさせていただきます。
30	法人	統一基準	6.1.5	36-37ページ	6.1.5　暗号電子署名 暗号アルゴリズムの選定は国際的な動向、普及を考慮して行うべきと考えます。特に、安全性、相互運用性を考慮すると国際的に利用されているものを優先的に選定すべきであり、その選定においては十分透明性のある議論がなされるべきと考えます。	御指摘の点については、今後の検討の参考とさせていただきます。
31	法人	統一基準	6.1.5	36ページ	6.1.5 暗号・電子署名 目的・趣旨 世界的に各国の規制にこたえるためには、データが失われた時の暗号化は当然の措置と思われるようになっています。多くの場合，データが十分暗号化されているか「判読できないように処理」されており暗号化Keyがユーザの管理下にある場合，この規制では告知，法的責任からのセーフハーバー免責があると認識します。多くの規制（PCI を除く）は特に暗号化を求めていませんが，暗号化は解決策の一部であること，漏洩通知という最大のリスクを除去できるものとして推奨しています。従って暗号化を適用した場合の機密情報のレベルが下がることを前提として検討すべきです。すなわち、要機密情報のうち機密性2までは取り扱えると考えます。例えば米国政府のFISMA規定ではパブリッククラウドでmoderate認定を受ければ機密性中程度(機密性2相当)まで扱えるようになっています。	御指摘の「暗号化を適用した場合の機密情報のレベルが下がることを前提として検討すべき」とのご意見については、情報の暗号化を行ったとしても、情報に求められる機密性については変化しないと考えます。 パブリッククラウドの利用において、要機密情報を取り扱う場合は、4.1.1項の規定に従い適切な情報セキュリティ対策を行うことを求めており、暗号化による秘匿性確保の対策もその手段の一つと考えます。
32	個人	統一基準	6.2.4	40ページ	標的型攻撃対策として、「内部に侵入した攻撃を早期検知して対処する」等を含めた多重防御情報セキュリティ対策体系だけでは完全に検知及び防御できないため、実効性のある優先的対策として「内部の情報資産の脆弱性及びセキュリティ設定の脆弱性を早期検知して対処する」対策を追加されたい。本対策を実施しない限り、脆弱性を誘導システムとして使用するAPT攻撃を含む標的型攻撃に対する実効性のある根本的対策とはならないため、国家として最優先で本対策を実施すべきである。	標的型攻撃対策は政府としても重要な課題として認識しておりますので、いただいた御意見については、今後の検討の際の参考とさせて頂きます。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
33	法人	統一基準	6.3.1(2)	41ページ	6.3.1(2)(a)(カ)「府省庁外の利用者その他のプライバシーに係る情報が本人の意思に反して第三者に提供されるなどの機能」について ガイドライン（案）において、cookie機能につき、アクセス履歴等のプライバシー情報を本人の意思に反して取得する場合として記述されておりますが、これらの情報は 利用条件にもとづき取得され、セキュリティ対策によって保護されるものであります。総務省「パーソナルデータの利用・流通に関する研究会報告書」（平成25年6月）においても、IPアドレス及びクッキーについては、いかなる場合に保護されるデータに当たるかは、今後更なる検討が必要としています。したがって、保護の必要性には留意しつつも、当該機能をプライバシー侵害の例であると当然に決定すべきではないと考えます。また、ガイドライン（案）では、「例えば、利用者のキー入力の全てを当該利用者が意図しない形で送信するなどの機能」がプライバシー情報の本人の意思に反した第三者提供の例として挙げられています。しかし、世上、キー入力そのものが送信される場合と、キー入力数など統計情報が送信される場合との区別が十分につけられないまま、クラウドサービスのリスクだけが強調される場合もあることから、政府のクラウド化を進めるにあたっては、寧ろ十分な普及啓発に力点を置くべきであり、特定のクラウドサービスの利用を一律に困難にするガイドラインとすべきではないと考えます。	当該規定は、利用者の意思に反して、アクセス履歴等の利用者その他の者による情報が、サービス利用に当たって不必要に第三者に提供されることを問題視しているものです。 御指摘を踏まえ、「プライバシーに係る情報」の表現については、「サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報」に修正いたします。 なお、政府のサービスが唯一性を持つことに鑑みると、利用条件によってサービス提供に必須ではない本人に関係する情報が取得されることへの同意を、サービス利用の条件にするべきではないと考えます。
34	法人	統一基準	7.1.2(2)	45ページ	7.1.2 サーバ装置，遵守事項(2)(d) バックアップに関して言及していますが、バックアップ中もしくはバックアップした媒体の盗難、さらには万が一盗難された場合の対策として、バック アップ媒体の暗号化を行うことを考慮すべきと考えます。	本遵守事項は、可用性に特化して記載したものです。 バックアップも含めた情報の機密性確保については、3.1.1項(4)「情報の利用・保存」で求めているため、原案どおりとします。 なお、ガイドラインの7.1.2項(2)及び3.1.1項(8)の解説において、バックアップの手段や保管場所について示しています。
35	個人	統一基準	7.2.2(1)	47-48ページ	7.2.2(1)(a)(ウ)には、「公開するウェブコンテンツを必要最小限にすること。」とあります。 しかし、ウェブは、政府が国民に対して情報を公開する重要な手段です。それにもかかわらず、このコンテンツを「必要最小限」にしなければならないというのは、非民主的で不穏当だと思います。 したがって、「公開してはならない、又は無意味なウェブコンテンツを公開しないこと。」などとするべきだと思います。	当該規定は、公開を想定していないファイルや不要なものを削除するよう求めるものであり、本来公開すべき情報の範囲を限定する意図はございません。 御指摘を踏まえ、遵守事項7.2.2(1)(a)(ウ)について、以下のとおり修正致します。 (修正前) 「公開するウェブコンテンツを必要最小限にすること。」 (修正後) 「「公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。」

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
36	法人	統一基準	7.3.2(1)	52ページ	7.3.2 (1)(a)「IPv6通信を行う情報システムに係る対策」について IPv6技術を利用する通信を行う情報システムを構築する場合は、IPv6 Ready Logo Programに基づくPhase-2準拠製品を選択することとありますが、特定のプログラムの準拠製品に限定する合理的根拠が見当たりません。むしろ、IPsecやIKEといったプロトコルについても許容できるように、特定のプログラムについて触れることなく、調達する機器が備えるべき機能について記載すべきと考えます。	IPv6 Ready Logo Programは、IPsecやIKEといったプロトコルについても許容するプログラムであると理解しております。他方で御指摘を踏まえて、記述の限定性を緩和するよう、修正いたします。
37	法人	全般	全般	ー	1、震災等からの教訓 パブコメドキュメント全般に関連し、 ・有名になったStuxnetや東日本大震災以降、想定外という事態が発生しないような工夫が国民の生命と財産を守るべき行政組織のセキュリティ対策としては必要ということは衆目の一致する改定の方向性に加わるべきとと考えます。	御意見ありがとうございます。今後の検討の参考とさせていただきます。
38	個人	全般	全般	ー	先日も東京都の情報が漏えいしたとの事。 金融関係も、さわやかな顔をして、やりたい放題です。 メディアも危ない人が、居ますし。 沖縄では、爆音訴訟の現場は、小鳥が鳴いて、とてもほのぼのしていました。 アフガニスタンの復興支援は、そろそろ終わるそうですね。12年凍結していたのに。子供の死亡率が世界一高いです。 最高のサービスとは。 セキュリティーは大切な信頼です。 国民から、世界からの信頼を頂けるようにお願いします。 他国と繋がりには重要です。 都庁で落し物を拾って渡した、アメリカのお母さんの、サンキュウー。ベリーマチッチ。は声が出ないほど鳴き声でした。 集団的自衛権の行使は、必要なのでしょうか。	御意見ありがとうございます。
39	個人	全般	全般	ー	情報は保存し　勝手に破棄しないこと　さらに公的な文書については公開するという情報の保管　情報公開の原則をはじめに明示すべきである。	情報の公開については、「公文書等の管理に関する法律」や「行政機関の保有する情報の公開に関する法律」といった別の制度に基づくものであり、今回の統一基準群の改定が影響を及ぼすものではありません。
40	法人	ガイドライン	全般	ー	該当箇所　：　文書中への追記（原文に該当箇所はありません） 意見　：　各府省でインシデントが発生した際の対応について、各組織・体制の役割とともに時系列で付録等に図や表で記載いただきたい 理由　：　現実にインシデントが発生した際、かかる記述があればより適切な対応ができると考えるため。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、各府省でインシデントが発生した際の対応については、各府省で定めるものであり、原案どおりといたします。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
41	法人	ガイドライン	3.1.1(6)	73-74ページ	3.1.1 情報の取扱い ＜3.1.1(6)(b)(c)関連＞ 3.1.1(6)-2 要機密情報である電磁的記録を要管理対策区域外に運搬又は府省庁外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずること。 b) 運搬又は送信を複数の情報に分割してそれぞれ異なる経路及び手段を用いる。 と記載されていますが、この記述であるとどのような割り方であっても分割したとみなされることとなりますし、実際にどのような分割手法を用いればよいのか現場が判りません。 ここの記述は、これまでの統一管理基準解説書では、秘密分散技術と具体的な技術名が記載されていた部分と考えますので、技術名を明記することで現場対処が迅速になると考えます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、御指摘を踏まえ、秘密分散技術については従前の統一基準群と同様、ガイドラインに記載をいたします。
42	法人	ガイドライン	4.1.1(1)	89-90ページ	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 ガイドライン（案）において、委託業務に使用される情報システムが海外のデータセンターに設置されている場合には、国内であれば不適切と判断されるアクセスをされる可能性があることに注意を払い、特に「行政機関の保有する個人情報の保護に関する法律」上の個人情報を取り扱う委託業務においては、保存された情報等において国内法令が適用されること等を外部委託の際の判断条件とすることを求めています。 しかしながら、同法上、行政機関が保有する個人情報を国内法が適用される場所に制限するとの規定はありません。 従って、「行政機関の保有する個人情報の保護に関する法律」で定義する個人情報について、国内法が適用される場所に制限することを外部委託の際の条件にすべきではないと考えます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方を示します。 行政機関の保有する個人情報の保護に関する法律第六条において、「行政機関の長は、保有個人情報の漏えい、滅失又はき損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならない。」と定められています。 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。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
43	法人	ガイドライン	4.1.1(1)	90ページ	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」 「特に、委託業務において使用される情報システムが海外のデータセンターに設置されている場合等においては、保存している情報に対して現地の法令等が適用されるため、国内であれば不適切と判断されるアクセスをされる可能性があることに注意が必要である。『行政機関の保有する個人情報の保護に関する法律』で定義する個人情報については、国内法が適用される場所に制限する必要があると考えるため、個人情報を取り扱う委託業務においては、保存された情報等において国内法令が適用されること等を外部委託の際の判断条件としておくべきである。」と規定し、事実上、グローバルクラウドを排除し、個人情報が関係する場合には、国内データセンター設置要件を課している。 しかしながら、本来、クラウド事業者の国籍やデータセンターの場所が、利用者に適用される法律に適切に対応できるかどうかを決する一番重要なものではない。実際、クラウドサービスは世界的に展開されることが多く、他国でサービスを提供しつつも特定国内の法律も十分に遵守することができる場合が多くある。同時に、国内のクラウド事業者であっても、開発力や資金力の不足、情報収集の不十分さ等様々な理由に起因して、単に日本に存在するというだけでは直ちに十分な法律（改正を含む）対応ができない場合がある。従って、海外に設置されたデータセンターについて殊更リスクを強調することは誤解を招くものであって、かかる理由で利用を禁止することは適切でなく、削除すべきである。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方を示します。 「行政機関の保有する個人情報の保護に関する法律」第六条において、行政機関の長は、保有個人情報の漏えい、滅失又はき損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならない。と定められています。 海外法令に基づき外国政府等の第三者に供出されるおそれのある場所に個人情報を置くことを適切でない管理の例として示していますが、設置場所を国内に限定する意図はありません。
44	法人	ガイドライン	4.1.1(1)	90ページ	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 通常の情報システムよりも強固なセキュリティを確保しているパブリッククラウドサービスもあります。従って、海外にデータセンターがあることのみを理由に利用を制限するのはコスト低減や国民の利便性を損なう可能性が高いと考えます。 従って下記のような記述を追加することをご提案します。 ⇒「海外データセンターに個人情報が保存される場合においても、機密情報箇所が暗号化されかつ暗号化キーがユーザ側で管理されている状態で保存されている場合においては問題が無いものとする」	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方を示します。 海外にデータセンターがあることにより、情報が外国法令の適用下に置かれ、外国政府の要求により供出されることは特に機密情報の管理上、好ましくないと考えます。なお参考までに、米国の政府調達においても、CONUS(CONtinental United States)条項など、情報の所在地に条件を付す例は一般的であると考えます。
45	法人	ガイドライン	4.1.1(1)	90-91ページ	4.1.1(1)(a)(イ)「委託先の選定基準」について ガイドライン（案）において、委託先の選定基準策定に当たっては、例えば、ISO/IEC 27001等に基づく認証制度の活用や、国際規格を踏まえとありますが、国際規格については、委託先の選定が容易となるように、具体的に「SOC 1,2,3等の国際規格」と明確化すべきです。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、御指摘の点については、以下のとおり修正いたします。 （修正前） 「例えば、ISO/IEC 27001等に基づく認証制度の活用や、国際規格を踏まえ、情報セキュリティガバナンスの～」 （修正後） 「例えば、ISO/IEC 27001等の国際規格とそれに基づく認証制度の活用、情報セキュリティガバナンスの～」

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
46	法人	ガイドライン	4.1.1(1)	90-91ページ	4.1.1(1)(a)(イ)「委託先の選定基準」について パブリッククラウド利用に対する選定基準については米国のFedRampのような基準を政府で統一して制定すべきと考えます。また、以下のような特定した記述はさけるべきと考えます。 →これら機関がマネジメントシステム認証の信頼性向上を目的とした取組である「MS認証信頼性向上イニシアティブ」に参画し・・・	ガイドラインについては今回のパブリックコメントの対象ではございませんが、御指摘の点については、今後の検討の参考とさせていただきます。 御指摘の「これら機関がマネジメントシステム認証の信頼性向上を目的とした取組である「MS認証信頼性向上イニシアティブ」に参画し・・・」の内容については、あくまで例示であり、原案どおりとさせていただきます。
47	法人	ガイドライン	4.1.1(2)	94ページ	4.1.1(2)(a)(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」 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として、個別の報告や実地監査の受入れを要求事項とするのは不適切であり削除すべきである。それらの確認は、第三者による事業者の監査レポート、情報セキュリティに関する国際規格への準拠状況、クラウド事業者が提供する様々な資料の活用によるべきであることは、前記各論2及び3のとおりである。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、御指摘の点については、あくまで一例として示しているものであり、原案どおりとします。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
48	法人	ガイドライン	4.1.2(1)	99-100ページ	4.1.2(1)(a)(ア)「約款による外部サービスを利用してよい業務の範囲」について 本内容はパブリッククラウドサービスを利用する場合の危険性について列挙してありますが、通常の情報システムサービスでも同様のこと、またはそれ以上の危険性が伴う場合もあります。むやみに列挙することは各省庁への無駄な危機感をあおるだけとなり、クラウドサービスによるメリットがいかにあったとしても、それを採用することに躊躇する可能性があります。危険性を記述するのであれば、通常の情報システムについても同様に記述し、客観的にメリット・デメリットを比較できるようにするべきです。 また、「約款による外部サービスで要機密情報を取り扱うことを禁止している」とありますが、コストや国民の利便性を鑑みた場合、通常の情報システム以上の対策が実施されているクラウドサービスもあるため、「要機密情報を取り扱う可能性がある場合においては利用にあたってのリスクを押さえるため、サービスの継続性が保証され、データの管理場所やバックアップ方法を明らかにしている外部サービスあるいはSOC1,2など国際基準の認定やJASA(今年より開始予定)の認定などがあるなどの条件を付与して利用すべきである」などといった表現にすることをご提案します。また米国政府が行っているFedRampプログラムのような認定制度を政府統一で制定するべきと考えます。 なお、世界的に各国の規制こたえるためには、データが失われた時の暗号化は当然の措置と思われるようになっています。多くの場合，データが十分暗号化されているか「判読できないように処理」されており暗号化Keyがユーザの管理下にある場合，この規制では告知，法的責任からのセーフハーバー免責があると認識します。多くの規制（PCI を除く）は特に暗号化を求めていませんが，暗号化は解決策の一部であること，漏洩通知という最大のリスクを除去できるものとして推奨しています。従って暗号化を適用した場合の機密情報のレベルが下がることを前提として検討すべきです。すなわち、要機密情報のうち機密性2までは取り扱えると考えます。例えば米国政府のFISMA規定ではパブリッククラウドでmoderate認定を受ければ機密性中程度(機密性2相当)まで扱えるようになっています。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方を示します。 本解説は、クラウドサービスの利用に当たってのリスクを一律に記載したものではなく、1.5節において定義する「約款による外部サービス」の利用にあたって生じうるリスクを例示したものであり、ガイドラインの記載については、原案どおりといたします。その他の御意見につきましては、統一基準への御意見への回答をご参照ください。
49	法人	ガイドライン	6.1.2(1)	143ページ	6.1.2(1)-1 以下を例とするアクセス制御機能の要件を定めること。 d)の要件は、一人のユーザーがPC＋モバイル端末といった複数のアクセス環境を利用するシーンでは成り立たないのでこの記述は不適当と考えます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、御指摘の点については、政府機関における情報システムの使い方を踏まえた不正防止の観点で規定したものであり、対策の一例であることから原案どおりといたします。
50	法人	ガイドライン	6.1.3(1)	145ページ	6.1.3(1)-1 a)について 最小限の特権機能を「与える」ことが記述されています。一般的にUnix系システムのrootやDB管理者は管理下すべての権限を持つことが標準とされることが多いです。管理者特権であっても、例えばある特定の領域（たとえば人事データ）にはアクセスできないよう、権限を剥奪する機能も検討すべきと考えます。従って、当該頁最終行は「特権を付与したり剥奪する方式がある」等の表現がより好ましいと考えます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、御指摘の点については、今後の検討の参考とさせていただきます。

受付番号	提出者	対象文書	該当箇所	該当ページ	概要	御意見に対する考え方
51	法人	ガイドライン	6.1.5(1)	154ページ	該当箇所 ： 6.1.5(1)-1「…ISO/IEC19790等に基づく認証…」 意見 ： 該当箇所を「…ISO/IEC19790等に基づく認証等…」としていただきたい 理由 ： 方式を限定せず、同等の認証方式も認めるべきと考えます。 ISO/IEC19790 に規定されている暗号アルゴリズムの範囲であれば、現在、海外で継続して評価手続きを行っている FIPS 140-2 認証でも同等に取り扱えると認識しています。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、御指摘の点については、以下のとおり修正いたします。 （修正前） ISO/IEC19790に基づく認証を取得している製品を選択する。 （修正後） 「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。
52	法人	ガイドライン	7.1.2(1)	194-195ページ	7.1.2(1)(d) について 暗号化に関しては言及がありますが、すべてのデータの暗号化が業務遂行もしくはシステム上難しい場合は、権限に応じたデータの一部秘匿（データマ スキング）も対策として考えられます。	ガイドラインについては今回のパブリックコメントの対象ではございませんが、次のとおり考え方を示します。 遵守事項としては、保守作業における情報の漏えいの防止するための対策を求めており、解説の内容（暗号化）は例示であるため、御意見の内容を妨げるものではありませんが、今後の検討の参考といたします。