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

- 実施方法：NISCのホーム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：2016年６月13日（月）～７月４日（月）
- 意見総数：13者から29件【内訳：８企業・団体から延べ20件、５個人から延べ９件】
  - ・統一規範に３件、運用指針に１件、統一基準に24件、全般に対して１件の意見提出。

（１）修正意見：全29件

- ・表現の明確化や適正化等を求めるものについては、必要に応じて趣旨を踏まえて、統一基準の解説書であるガイドラインを修正（4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（25件）

（２）主な意見

- ・クラウドサービス※の利用等の外部委託に対する意見（12件）
- ・標的型攻撃対策等の情報セキュリティの脅威への対策に対する意見（６件）
- ・情報セキュリティ対策の自己点検・監査に対する意見（３件）

※ 外部事業者が有する物理的又は仮想的なコンピュータ資源を利用者の需要に応じて柔軟に提供するサービス

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」に対しても延べ17件の意見提出。表現の明確化に関する意見について、趣旨を踏まえ修正（１件）

- （参考）提出者名：

特定非営利活動法人ＩＴプロ技術者機構、KPMGコンサルティング株式会社、（株）セールスフォース・ドットコム、日本オラクル株式会社、日本マイクロソフト株式会社、BSA｜ザ・ソフトウェア・アライアンス、秘密分散法コンソーシアム、ブルーコートシステムズ合同会社、個人（５）

政府機関等の情報セキュリティ対策のための統一基準群の改定（案）に関する意見募集の結果一覧

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
1	秘密分散法コンソーシアム	統一規範	P.2	第四条	政府機関の情報セキュリティ対策のための統一規範（案）の、P2、（府省庁情報セキュリティ文書）第4条3の、府省庁対策基準は、別に定める政府機関の情報セキュリティ対策のための統一基準（以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となるように定めなければならない。の記載末尾に、 尚、上記の、府省庁対策基準は、別に定める政府機関の情報セキュリティ対策のための統一基準（以下「統一基準」という。）と同等以上の情報セキュリティ対策を可能とする際には、既公開のNISC主要公表資料や公的組織の調査報告書、公的実証事業等の成果報告書等や調達可能な信頼できる民間等の最新セキュリティ技術標準化動向等の、公開資料等を参考とできる。 と、文章を追加すべきと考える。	統一規範では、府省庁が情報セキュリティ対策について行うべき基本的事項を規定しています。これを行うために参照するものとして、統一基準第1部総則1.1(5)において、府省庁対策基準の策定について定めており、御指摘の事項を含めて統一基準内で既に規定されています。
2	個人	統一規範	P.3	第十条	修文:「第十条　府省庁は、情報セキュリティ対策の自己点検を行わなければならない。」 →「第十条　府省庁は、情報セキュリティ対策の動的な情報セキュリティリスク管理に基づく自己点検を行わなければならない。」 （理由） APT攻撃のような高度サイバー攻撃に実効性のある対応をするためには、脅威および脆弱性を常時監視しリスクを可視化するための動的な情報セキュリティリスク管理が必要である。このような情報セキュリティリスク管理は、ISO/IEC 27005およびNIST SP 800-137で標準化されている。我が国においても、このような標準に基づく動的な情報セキュリティリスク管理に基づく自己点検の仕組みを導入すべきである。	統一規範第三条において、リスク評価の実施及びその結果に基づく情報セキュリティ対策を講ずる旨を規定しています。第十条の自己点検は、その対策の実施状況を点検する位置づけとして規定したものになります。以上より、御指摘の内容については統一規範全体において規定済みと考えます。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。
3	個人	統一規範	P.3 P.4	第十一条	（意見内容） 修文:「第十一条　府省庁は、府省庁対策基準が本規範及び統一基準に準拠し、かつ実際の運用が府省庁対策基準に準拠していることを確認するため、情報セキュリティ監査を行わなければならない。」 →「第十一条　府省庁は、APT攻撃のような高度サイバー攻撃に実効性のある対応をするために、府省庁対策基準が本規範及び統一基準に準拠し、かつ実際の運用が府省庁対策基準に準拠していることを確認するため、監査周期を短縮化した情報セキュリティ監査を行わなければならない。」 （理由） APT攻撃のような高度サイバー攻撃に実効性のある対応をするためには、動的な情報セキュリティリスク管理を行うためのセキュリティ常時監視を導入するとともに、情報セキュリティ監査の監査周期の短縮化が必要である。	統一規範は、政府機関のとるべき枠組みを定めており、情報セキュリティ監査を府省庁自らが行わなければならないことを明確化することが本項を規定する意図であり、原案どおりとさせていただきます。なお、監査の実施時期については、ガイドライン基本対策事項の2.3.2(1)e)に記載しております。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
4	秘密分散法コンソーシアム	運用指針	P.5	5	意見内容: 「政府機関等の情報セキュリティ対策のための統一基準群」の改定(案)についての、P4、監査に係る規定整備及び政府機関等の情報セキュリティ対策の強化下段の図中(運用指針に同内容の図あり)、NISCからサイバーセキュリティ戦略本部への上向き矢印中の文言で、 ・統一基準群(対策基準策定ガイドラインを除く。)の原案策定　等と記載されているが、 ・統一基準群(対策基準策定ガイドラインを含む。)の原案策定及び決定　等 と修正すべきと考える。 理由: 政府機関等の情報セキュリティ対策の運用等に関する指針(案)の、P1、2　統一基準群の策定において、～対策基準策定ガイドラインは、府省庁と協議の上、NISCにおいて決定する。と記載されており、パブコメ案の、対策基準策定ガイドラインを除く。では整合性が取れない為。	統一基準群のうち、統一規範、運用指針及び統一基準はNISCにおいて原案を作成し、サイバーセキュリティ戦略本部において決定するもので、対策基準策定ガイドラインはNISCにおいて決定するものであることから、このような記述としており、整合はとれています。
5	個人	統一基準	ー	全般	マイナンバーの取り扱いについて記載がないのに違和感がある。個人情報保護委員会のガイドラインはポリシーのみを記載されているものと考えられることから、政府におけるマイナンバーの取扱基準は統一基準として記載されるべきものと考える。 政府としてマイナンバーを一つも漏らさないような対策、万が一漏れてしまった場合における個人情報保護委員会との連携した対応などについてNISCが主体となって対応できるよう、本改正において必要かつ適切な事項を盛り込まなければならないと考える。 政府としてマイナンバーを取り扱うのであるから、そのセキュリティ基準は他でもないNISCが示すべきであって、他府省庁における対策に委ねることは許されない。 また、時期についても、本来であればマイナンバーの取り扱いが始まる前までに整備されるべきであり、既に手遅れと考えられることから、本改定に盛り込むべきと考えられる。	国が運営するマイナンバー関連の情報システムについても、統一基準群の対象範囲に含まれます。 ただし、統一基準群は、府省庁等の各組織がそれぞれ情報セキュリティポリシーを策定する際の情報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って、個別のシステムのセキュリティ要件を定める性質のものではございません。
6	日本オラクル株式会社	統一基準	P.6	1.3	【意見内容】 「クラウドサービス事業者」を「クラウドサービスを提供する事業者」と「クラウドサービスを用いて事業システムを開発・運用する事業者」に分けて定義する。 また(参考)「府省庁対策基準策定のためのガイドライン(案)」に該当箇所があるので、用語を再定義した上で記述内容を整理する。 【 理由 】 クラウドコンピューティングの参照アーキテクチャ国際規格(ISO/IEC 17789:2014)では、「クラウドサービスを提供する」ロール(Cloud Service Provider)と「クラウドサービスを用いて情報システムを開発・運用する」ロール(Cloud Service Developer)を完全に分け、責任分界点を明確にしています。しかし、該当文書ではそれらを分離せずに用語を定義しているため、責任分界点が不明になる恐れがあります。ちなみに、クラウドサービスのISMS国際規格(ISO/IEC 27017:2015)もISO/IEC 17789の責任分界点を前提に記述されています。	「4.1.1 外部委託」の「目的・趣旨」において、「…外部委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。」と明記しており、これはクラウドサービス事業者が「クラウドサービスを提供する事業者」又は「クラウドサービスを用いて事業システムを開発・運用する事業者」のいずれであろうと、それぞれの業務や責任の範囲を明らかにすることを意味しているため、特にクラウドサービス事業者の定義を変更する必要はないと考えます。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
7	個人	統一基準	P.14	2.2.4(1)	情報セキュリティインシデントへの対処 遵守事項 (1) 情報セキュリティインシデントに備えた事前準備に関して、 インシデントの予知・分析の対策も準備に含める。	御指摘の「インシデントの予知・分析の対策」が具体的にどのような対策を指すのか定かではありませんが、政府全体としては、政府横断的な監視によりサイバー攻撃やその準備動作等の脅威を検知するなどして情報収集を行い、関係機関に情報提供を行っています。 なお、御指摘を踏まえ、ガイドラインの解説を補足します。
8	個人	統一基準	P.15	2.2.4(3)	情報セキュリティインシデントへの対処 遵守事項 (3) 情報セキュリティインシデントの再発防止・教訓の共有に関して、 インシデント情報に関して、国内だけでなく、海外のトレンド・情報も含めた防止策・訓練・対応措置を検討していくことを追加。	統一基準群では、再発防止策等の検討に当たり情報収集を行う範囲について、国内、海外を限定しない記載としておりますが、御指摘を踏まえ、ガイドラインの解説を補足します。
9	KPMGコンサルティング株式会社	統一基準	P.18	2.3.2(2)	2.3.2(2)　監査の実施： 実施事項に、前年度の監査における指摘事項のうち未改善の事項を含むことが望ましいと考えます。	情報セキュリティ監査は、2.3.2(1)の監査実施計画及びその監査実施計画の基となる2.1.2(2)の対策推進計画に基づき実施するものです。対策推進計画は、府省庁の業務、取り扱う情報及び保有する情報システムに関するリスク評価に基づき策定されるもので、これを受ける監査実施計画、即ち御指摘対象の「何を監査実施対象とするか」についても、当該リスク評価に基づき策定されるものとなり、「前回監査結果の未改善事項」については、この当該年度リスク評価において引き続きリスク有りと評価された場合、対象に含まれることになります。 以上のとおり、御指摘の点については既に統一基準に記載のある当該プロセスに含まれており、それのみ特出しすることで、前述の正しいプロセスやリスク評価を経ずに当該項目のみ特別扱いするかのようなミスリードのおそれもありますので、原案どおりとさせていただきます。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
10	KPMGコンサルティング株式会社	統一基準	P.23	3.2.1(1)(b)	3.2.1(1)(b) 要管理対策区域における対策の基準の決定: 要管理対策区域ごとに立ち入りを許可する/許可しない者を判断するための基準を追加することが望ましいと考えます。	組織や区域の特性は、府省庁又は部局等ごとに異なると考えられます。したがって、各府省庁が組織や区域の特性に応じて対策の基準をポリシーに規定できるよう、統一基準及びガイドラインでは、各府省庁に共通した基準を定めています。
11	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.24 P.28	4.1.1 4.1.4	4.1.1では、「クラウドサービスの利用に係る外部委託については、クラウド特有のリスクがあることを理解した上で、4.1.4項「クラウドサービスの利用」についても本項に加えて遵守する必要がある。」と記述されています。クラウドが「特有の」リスクを有することは事実かもしれませんが、そのリスクが他の選択肢であるオンプレミスの情報システムなどのものよりも高いといった正しくない印象を与えることがない記載とすべきです。	御指摘の部分ですが、統一基準については、政府機関における判断材料とクラウドサービスへの要求事項を記しており、政府機関が求めるクラウドサービスの選定条件として意思表示することにより適合したクラウドサービスを市場から検索するという調達手続の方法について述べているものであって、クラウド特有のリスクが他の選択肢であるオンプレミスの情報システムなどのものよりも高いことを意図しているわけではありません。
12	(株)セールスフォース・ドットコム	統一基準	P.25	4.1.1(2)(c)	【原文】 委託先がその役務内容を一部再委託する場合には・・・ 【意見】 再委託先の管理については、再委託先のリスク管理のみならず、再委託先の選定に際し、委託元がリスク管理体制を鑑みた上で可否を申し出る権利、途中で再委託の中止の申し出の権限、適切な監査権限について、その代替案も含め記述されるべきと考えます。	御指摘の内容は、調達時の契約事項として取り扱われるものであり、統一基準においては、再委託の実施について、委託元の承認を受けることや再委託先のセキュリティ確保を委託先に担保させることなどを規定しています。
13	KPMGコンサルティング株式会社	統一基準	P.25	4.1.1(2)(c)	4.1.1(2)(c) 外部委託に係る契約: 当該規定は再委託に限定されているように見受けられますが、金融庁の監督指針を初め、世間の動向としては再委託先が更に業務を委託する(これを前述の指針では「二段階以上の委託」と表現)際にも、情報セキュリティの水準を十分に確保することが求められています。政府機関においては、その性質上大規模な情報システムも多数有することから、二段階以上の委託が発生する蓋然性が高いと思料します。このため、政府統一基準においても、再委託だけではなく二段階以上の委託先に対しても統制を可能と事項を含むことが望ましいと考えます。	契約における再々委託等の段階的な委託は様々な契約が想定されることから、統一基準においてそれらの詳細な規定はしていませんが、本規定における再委託の概念には、再々委託等の段階的な委託が含まれます。 なお、御指摘を踏まえ、誤解がないようガイドラインにて補足いたします。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
14	（株）セールスフォース・ドットコム	統一基準	P.26	4.1.2	【原文】　約款による外部サービスの利用 目的・趣旨 【意見】 省庁内での業務遂行において今後この約款による外部サービスは不可避のものとなると考えられます。この場合にこれらの検討を「やむを得ず」、「例外的に」と言った表現を使うことでその普及を根本から阻害する印象を与えかねません。積極的にこれらの検討も適正なリスク管理の元行っていくことを示し、選択肢の一つとすることを望みます。	本項では、政府機関において取り扱う情報の特性に鑑み、リスクを考慮の上、約款による外部サービスを利用してよい範囲等を定めて利用することを規定しており、約款による外部サービスの普及を阻害することは考えておりません。
15	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.26 P.28	4.1.2、4.1.4	①「約款による外部サービス」による取扱いを禁止される情報の範囲が過度に広くならないよう、該当する「要機密情報」の適用範囲を最も機微な情報に限定するよう狭めることを提言します。 ②本基準群中の記載により、クラウドサービスが「約款による外部サービス」ではないことを明示することを求めます。例えば、本ガイドラインの7頁に記載されている参考図を用いて、異なる外部委託サービスの関係についての説明を本基準群に含めることを提言します。 ③「約款による外部サービス」により「要機密情報」の取り扱いが禁止されるのは、当該サービスの約款の内容が要機密情報を扱う要件を満たしていない場合に限られる旨を明確にすべく、本基準群の記載を修正するよう提案します。 ④外部委託業者（特にクラウドサービスプロバイダー）が適切なセキュリティ対策を有するか否かを確認するために、政府機関は、利用可能な様々なセキュリティ対策に関する情報（例えば、第三者によるクラウドサービスプロバイダーの監査レポート、情報セキュリティに関する国際規格への準拠状況を活用すべきことを明確にしていただけるようお願いします。クラウドサービスプロバイダーが政府担当者による直接の現地調査を受け入れることを要件とすべきではありません。そのような要件は現実的でも効果的でもなく、間接的にデータやハードウェアを国内に置かせることを要求する結果を招くからです。	①要機密情報は、1.2節「情報の格付の区分」に規定するとおり、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であり、要機密情報を範囲とすることについては過度に広くないと判断しています。 ②「クラウドサービス」は「約款による外部サービス」とは異なるものであることを、1.3節「用語の定義」において、条件設定の余地の有無により規定しています。 ③上記①のとおりです。 ④統一基準において、具体的な認定・認証制度等は規定すべき性質のものではないことからその旨記述はしていませんが、ガイドラインの解説部分では、参考となる認証や報告書等について例示しております。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
16	日本マイクロソフト株式会社	統一基準	P.28	4.1.4	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 クラウドサービスの利用の目的・趣旨の小項目において、「クラウドサービスの委託先」との表現があるが、概念の受け止め方の違いによって理解に混乱が生じるおそれがある。 というのも、同遵守事項の小項目において、(1) クラウドサービスの利用における対策の(a) を見ると、「クラウドサービス（民間事業者が提供するものに限らず、政府が自ら提供するものを含む。以下同じ。）を利用するに当たり」という表現が出てくる。そうすると、同(b)(c)(e)で出てくる「クラウドサービス」の「委託先」という表現は、両者（前者であれば民間事業者が提供する場合のさらに委託先として下請け業者を指すこととなり、後者であれば政府が自ら提供する場合の委託先としてクラウドサービス提供事業者自身を指すことになろうか）を含む概念になってしまい分かりにくい。 そもそも、4.1.4は全体的に、政府機関がクラウドサービスの利用者であって、政府機関内部向けであろうと住民サービスであろうと一定の業務について、その一部をクラウドサービス提供事業者に委託するというシナリオを前提にしているように読める。そうであれば、「委託先」という表現は避けて「クラウドサービス提供事業者」とするなど、混乱が生じないように分かりやすく表現してほしい。	「4.1.1 外部委託」の「目的・趣旨」において「…外部委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。」と記述しており、混乱や誤解が生じることはないものと理解しています。
17	日本マイクロソフト株式会社	統一基準	P.28	4.1.4	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 クラウドサービスの利用の遵守事項の小項目において、(1) クラウドサービスの利用における対策の(e) を見ると、「各種の認定・認証制度の運用状況等から」との表記がある。これに対して、具体的な例示は、府省庁対策基準策定のためのガイドライン（案）P118で3つの例（ISO/IEC 27017、クラウド情報セキュリティ監査、SOC報告書）が出てくるが、その重要性からしても読み手の理解の容易性からしても、ガイドラインではなく統一基準の中で例示すべきである。また、その際には、ISO/IEC 27017をベースとしたクラウド情報セキュリティ監査に基づく我が国固有のクラウドセキュリティマーク制度がせっかく新設されて運用が開始されているのだから、それについてまず記載するべきである。次にそのベースとなったISO/IEC 27017について記載し、そのあとでSOC報告書について記載するのが妥当である。なおISO/IEC 27017について記載する際には、単に国際規格というだけでなく、認定機関による認証がなされていることを含め正確な記載をしていただきたい。	統一基準に例示すべきとの御意見についてですが、具体的な認定・認証制度の例示は統一基準に規定すべき性質のものではなく、ガイドラインに記載することとしています。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
18	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.28	4.1.4	4.1.4遵守事項(1)(b)は、「情報システムセキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること」を挙げています。BSAは準拠法、裁判管轄、適用される法令・規則を確認することの重要性について同意します。しかし、クラウドサービスプロバイダーが、準拠法に従いデータを安全・適切に扱うことを保証することができれば、データの保存場所を指定する必要はないはずです。クラウドサービスがもたらす優位性の多くは、国境を越えたデータ移動が可能であることによりもたらされます。よって、そのような移動を制限し、データが「特定の場所」にあることの説明を求めることは、データのセキュリティを何ら増すことがないのに、クラウドサービスやプロバイダーを制限することになってしまいます。データのセキュリティは物理的な保管場所に依存するのではなく、データを保護するための品質の高い機能、効果的な手段、制御の行き届いた管理によってもたらされます。	4.1.4(1)(b)の規定は、「必要に応じた」ものであり、委託事業の実施場所を常に指定するものではありません。また、クラウドサービス利用契約において準拠法が合意されている場合でも、例えば次のような国内法以外の法令が適用されるケースが想定されるため、実施場所も併せて指定することは有効な規定であると考えています。 委託事業者の法人としての国籍が外国籍であって、サーバが国外にある場合に、実態的に国内法以外の法令が適用されるようなケース
19	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.28	4.1.4	委託先のクラウドサービスプロバイダーを選定する上で評価・判断するための要件として、関連する国際規格への準拠や認証を活用する旨、本ガイドラインにとどまらず、本基準群において明示するよう求めます。 また、米国政府が採用している、セキュリティ評価と認証における標準的手法の提供を目指すFederal Risk and Authorization Management Program（FedRAMP）のような、政府機関向けクラウドサービス認証制度の採用を推奨します。 これらを併せて用いることにより、情報システムセキュリティ責任者は、クラウドサービスプロバイダーを包括的に評価することができ、目的に対して、最も費用対効果が高く、安全で、機能に優れたクラウドサービスを選定する確率を高めることができます。また、結果として、公共部門にとどまらず、安全で効果的なクラウドサービスの導入の更なる普及を推進することになります。	統一基準に例示すべきとの御意見についてですが、具体的な認定・認証制度の例示は統一基準に規定すべき性質のものではなく、ガイドラインへ記載することとしています。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
20	ブルーコートシステムズ合同会社	統一基準	P.28	4.1.4	修正案） b）情報システムセキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令を適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄の指定、又はトークン化・暗号化等のデータ保護の方法を定めること。 d）情報システムセキュリティ責任者は、個別のクラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でサービス側、オンプレミス側共にセキュリティ要件を定めること。 f）情報システムセキュリティ責任者は、管理外の端末やクラウドのリスクを考慮してクラウドサービスの制御について検討し、クラウドの可視化やその監査、脅威やデータ漏洩からの保護について要件として対策を検討すること。 理由） b）既に国内法以外の法令が適用されるクラウドサービスに対し、国内法によるデータ保護が可能なソリューションが実用化されているため。 d）個別のクラウドサービス及び接続する方法によってセキュリティリスクは異なるため、共通のセキュリティ要件で網羅することは難しいため。 f）クラウドサービスのセキュリティとしてオンプレミス側で認められている技術であり、考慮が必要と考えられるため。	b）遵守事項(1)(b)において、国内法以外の法令が適用されるリスクを評価した上で、国内法以外の法令が適用されるクラウドサービスを選択した場合、遵守事項(1)(d)における「クラウドサービスの特性」に関する基本対策事項にて記される「f)クラウドサービス上で取り扱う情報の暗号化」をクラウドサービスに求め、契約内容に含められる旨が謳われているため、あえて遵守事項(1)(b)での「トークン化・暗号化等のデータ保護の方法を定めること」は内容的に重複となることから、現状のままといたします。 d）ご指摘のとおり、個別のクラウドサービス及び接続する方法によってセキュリティリスクは異なるため、ガイドラインの基本対策事項4.1.4(1)-2において、セキュリティ要件を例示しつつ、取捨選択等することにより、各々のリスクに対応できるよう自由度を持たせる構成にしてあるため、現状のままといたします。 f）については、どのような対策を指しているのか定かではありませんが、ガイドラインの基本対策事項4.1.4(1)-2において、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティ対策を構築するに当たっての要件を例示しており、オンプレミス側で認められている技術も包含しているとの認識であるため、現状のままといたします。
21	（株）セールスフォース・ドットコム	統一基準	P.28	4.1.4	【原文】クラウドサービスの利用 【意見】 日本政府として行政機関におけるクラウドサービス活用推進は世界最先端 IT 国家創造宣言や日本再興戦略においてもうたわれているところであり、今後積極的な利用を推進されることと推察いたします。しかし、ガイドラインも含め本章の表現にはその普及を根本から阻害するような危険性を煽る印象を与える可能性がある記述が散見されます。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。このため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が必要と考えます。利用促進を後押しできる表現を再考いただくことを望みます。 また、米国のFedRampをはじめとして諸外国では行政機関がクラウドサービスの利用促進ができるように認証制度を作っています。現にこの認証制度によりクラウド利用が進んでいます。日本でも同様の制度を作ることをご提案いたします。	御指摘の部分ですが、統一基準については、政府機関における判断材料とクラウドサービスへの要求事項を記しており、政府機関が求めるクラウドサービスの選定条件として意思表示することにより適合したクラウドサービスを市場から検索するという調達手続の方法について述べているものであって、普及を根本から阻害するような趣旨ではないと考えます。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
22	特定非営利活動法人　ITプロ技術者機構	統一基準	P.31	5.2.1	「インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離すること」の原則が、要否の判断の条件「情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等」と一体にして示されているため、訴求性が弱くなり明確になっていない。 これでは、インターネットに接点を有する情報システムから分離すること」の原則が、その組織の情報システムセキュリティ責任者の判断に明確に反映されず、実施が不十分となることが危惧され、政府機関の統一基準として不適切ではないかと考えられる。 つまり、だれにでもわかりやすく統一された判断基準の提示が必要と思われるので、例えば、(a)項を下記に変更する。 「(a)情報システムセキュリティ責任者は、重要な情報を扱う情報システム（情報の格付等に基づき判断する）については、インターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することとし、分離する情報システムについても、分離しない情報システムについても以下の事項を含む情報システムのセキュリティ要件を策定すること。」	「情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等」を、「分離すること」の要否の判断条件として規定しており、遵守事項は明確であると考えます。さらに、ガイドラインにおいて、特に重要な情報を取り扱うシステムは分離すべき旨を解説として記述しています。このようなことから、実施が不十分になるといった御懸念には及ばないものと考えます。
23	個人	統一基準	P.36	6.1.1	遵守事項(1)(a)で「情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設ける」ことが求められ、6.1.3 権限の管理　遵守事項(1)(a)で、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずること。」が求められている。 この統一基準（案）に対応する府省庁対策基準策定のためのガイドライン（28 年度版）（案）の基本対策事項6.1.3(1)-1では、一般的な情報システムの特性を考慮に入れ「主体に対して管理者権限を付与する場合、主体の識別コード及び主体認証情報が、第三者等によって窃取された際の被害を最小化するための措置として、 a) 業務上必要な場合に限定する b) 必要最小限の権限のみ付与する c) 管理者権限を行使できる端末をシステム管理者等の専用の端末とする の3点が例示されている。 しかし、最近の脅威の動向および主体に対する認証技術の動向を考慮して、また、2010年8月に各府省情報化統括責任者（CIO）連絡会議で決定された「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」を参考に「複数要素認証」の導入を図り、アクセス制御技術の強化を図るべきではないかと考える。少なくとも、複数要素認証の導入を検討すべきだと考える。 特に、マイナンバーカードの導入に伴い、全ての担当者に対して身分証明書としての「マイナンバーカード」が発行される状況となったので、「知識」の認証要素としての「パスワード」と「所有」の認証要素として「マイナンバーカード」を用いた「二要素認証」を実現する素地は整ってきたと考える。	主体認証方式は、情報の格付等に応じて適当な方式が決定されることが求められるため、今般の改定においては一律に複数要素認証を遵守事項として位置づけておりません。 主体認証を行う情報システムにおいて、情報セキュリティ強度の更なる向上を図るために導入を検討するべき具体例として、多要素認証をガイドラインに掲載しておりますが、御指摘を踏まえ、ガイドラインの解説を補足します。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
24	KPMGコンサルティング株式会社	統一基準	P.40	6.2.1(1)(c)	6.2.1(1)(c) ソフトウェアに関する脆弱性対策の実施： ソフトウェアに関連する脆弱性情報を定期的に入手し、脆弱性対策計画を策定し、措置を講じることが望ましいと考えます。政府統一基準（案）では、ソフトウェアに関連する脆弱性情報を「入手した場合には」と限定されているため、意図的に入手しない場合に必要な対策が講じられない可能性があります。	脆弱性対策の状況を定期的に確認することは6.2.1(1)(d)で規定しており、御指摘の「意図的に入手しない」行為は統一基準に反する行為であり、当然入手する努力は求められます。
25	KPMGコンサルティング株式会社	統一基準	P.41	6.2.2(1)(b)	6.2.2(1)(b) 不正プログラム対策の実施： 想定される不正プログラムの感染経路を特定することを明確化することが望ましいと考えます。	具体的な対策は統一基準に規定すべき性格のものではなく、ガイドラインに記載することとしています。なお、御指摘の点については、ガイドラインの基本対策事項において規定しています。
26	個人	統一基準	P.42	6.2.4	（意見内容） 修文：目的・趣旨 「――――、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。」 →「――――、多重防御の情報セキュリティ対策体系並びにセキュリティ常時監視によって、標的型攻撃に備える必要がある。」 （理由） 実効性のある標的型攻撃（APT攻撃）対策は、検知された脅威に対する対策だけでは不十分であり、すり抜けた脅威に対しては、自己の動的な情報セキュリティリスク管理のためのセキュリティ常時監視対策を追加する必要がある。	御指摘の標的型攻撃対策の目的・趣旨に対する御意見については、本項の遵守事項6.2.4(1)(b)において、外部との不正通信を検知して対処する対策（内部対策）として規定しております。
27	個人	統一基準	P.42	6.2.4	標的型攻撃対策 遵守事項に関して、 標的型攻撃により、情報漏えいが起きた場合でも、その漏えい情報が制御可能な手段を多重防衛の対策の１つとして検討していくこと。	具体的な手段の例示は統一基準に規定すべき性質のものではなく、ガイドラインに記載することとしています。 なお、御指摘いただきました漏えい情報の制御可能な手段については、その有効性を見極めつつ、今後の取組の参考とさせていただきます。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
28	KPMGコンサルティング株式会社	統一基準	P.42	6.2.4(1)	6.2.4(1) 標的型攻撃対策の実施： 当該対策は、入口対策・内部対策・出口対策として整理することが望ましいと考えます。政府統一基準（案）では、内部対策にいわゆる出口対策の概念が入っているように見受けられますが、入口対策に対して内部対策という表現のみ用いた場合、表現が対になっておらず、出口対策の概念の理解が困難となり、本来政府統一基準が意図する対策が十分に施されないおそれがあると考えます。	内部対策には出口対策も含まれております。入口と出口を対にさせるよりも、外部からの侵入に対する入口対策だけではなく、侵入されることを前提に内部対策を講ずることが重要であることを強調するために現在の構成となっています。
29	個人	全般	P.228	7.2.2	行政機関全てのサイトにおいてhttpsアクセスの有効化とTLSv1.2の実装とPFS対応の暗号スイート利用の設定を行っていただきたい。 go.jpへのアクセスは全ての場合において狙われやすい事を各省庁に周知すべきであり、その前提で上記の措置を早急に行っていただきたい。	ガイドライン7.2.2(1)-5において、ウェブサーバの実装として、 1）TLS（SSL）機能を適切に用いる。 2)「SSL/TLS暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定する。 旨が記述されており、特に「SSL/TLS暗号設定ガイドライン」では暗号スイートとして、DHE、ECDHE方式の設定も含まれ、これらはPFSの特性を有しています。なお「行政機関全てのサイトにおいてhttpsアクセスの有効化」については、今後の検討の参考とさせていただきます。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
30	秘密分散法コンソーシアム	ガイドライン	P.80	3.1.1(6)(a)(b)	府省庁対策基準策定のためのガイドライン（案）のうち、データ送受信や移送が発生する箇所と、そうしたデータ送受信や移送に必要な機器、回線やメディア、関係する業者等に関しては、電子情報の移送（モバイルPCやUSBメモリー等も含む）に関しては、これまでのNISC公表の、統一管理基準やその解説書、府省庁対策基準策定のためのガイドライン等を参考とし、 遵守事項(6) 情報の運搬・送信 ＜3.1.1(6)(a)(b)関連＞3.1.1(6)-2 b) 要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬又は送信する。 （解説） 例えば、1個の電子情報について、分割された一方のデータからは情報が復元できないよう情報量的に解読不能となるように、秘密分散技術を適切に用いて分割して移送を行うこと。 なお、暗号と併用する場合には、分割前であっても分割後の複数生成ファイルに行っても良いが、分割前に暗号化を行うことで、管理すべき暗号鍵の管理数を抑制することができる。 分割後に暗号化する手法としては、要機密情報を秘密分散技術を用いて2個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方をDVD、USB メモリ等の外部電磁的記録媒体で郵送する方法が考えられる。 と修正し、各該当箇所に 遵守事項(6) 情報の運搬・送信 ＜3.1.1(6)(a)(b)関連＞3.1.1(6)-2 b) 要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬又は送信する。 を参照するよう追記する。 また、電子情報の保管（BCPも含め）に関しては、これまでのNISC公表の、統一記述基準解説書の記載事項を参考として、各該当箇所に、セキュリティを確保する措置の例としては、暗号や秘密分散技術を利用して情報の漏えいや改ざんを防止することが挙げられる。 と、下記理由記載の、既公表主要文書の、政府機関の情報セキュリティ対策のための 統一技術基準（平成 24 年度版）解説書の記載事項を参考とし、暗号と併記するなどして、例示すると良いと考える。	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お示しします。 秘密分散技術以外にもデータを分割してセキュアに送信等行う方法が存在する可能性があることから、特定の技術を指定しないよう記載を見直しています。 御指摘の内容については、今後の検討の参考とさせていただきます。
31	秘密分散法コンソーシアム	ガイドライン	P.80 P.81	3.1.1(6)-2 b)	該当箇所記載部分の、例えば、1個の電子情報について、分割された一方のデータからは情報が復元できない方法でファイルを2個に分割し、～ の部分は、これまで継続して主要公開資料等で同一部分の記載内容を参考とし、 例えば、1個の電子情報について、分割された一方のデータからは情報が復元できないよう情報量的に解読不能となるように、秘密分散技術を適切に用いて分割して移送を行うこと。 なお、暗号と併用する場合には、分割前であっても分割後の複数生成ファイルに行っても良いが、分割前に暗号化を行うことで、管理すべき暗号鍵の管理数を抑制することができる。 分割後に暗号化する手法としては、要機密情報を秘密分散技術を用いて2個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方をDVD、USB メモリ等の外部電磁的記録媒体で郵送する方法が考えられる。 とすべきと考える。	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お示しします。 秘密分散技術以外にもデータを分割してセキュアに送信等行う方法が存在する可能性があることから、特定の技術を指定しないよう記載を見直しています。 御指摘の内容については、今後の検討の参考とさせていただきます。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
32	秘密分散法コンソーシアム	ガイドライン	P.82	3.1.1(7)(b)	これまでNISC主要公表資料の中で記載されてきている、「秘密分散技術」を適切に用いることで実現できる為、府省庁対策基準策定のためのガイドライン（案）の、P82～83、 （解説） 遵守事項3.1.1(7)(b)「抹消する」についての、最後尾（P83上部）には、 更に、要機密情報である書面を電磁的記録媒体に記録する際に、当初から「秘密分散技術」を適切に用いて、分割された一方のデータからは情報が復元できないよう情報量的に解読不能となるような処理を行ったものだけを記録する方法もある。 と追加し、P83中段の、遵守事項3.1.1(7)(c)「復元が困難な状態にする」については、その最後尾に、更に、秘密分散技術を適切に用いて、電子情報として事実上の廃棄処理を行い、生成された複数の割符ファイルを個別に適切に管理することにより、「復元が困難な状態にする」手法があり、こうした情報運用管理を日常的に行っていれば、不正アクセス等によって、組織内から完全な情報が一度に漏えいすることは発生しにくくなるメリットが期待できる。 と記載すると良いと考えられる。	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、御指摘の内容については、今後の技術の進展を見つつ、検討の参考とさせていただきます。
33	日本マイクロソフト株式会社	ガイドライン	P.115	4.1.4	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 クラウドサービスの利用の目的・趣旨の小項目において、「クラウドサービスの委託先」との表現があるが、概念の受け止め方の違いによって理解に混乱が生じるおそれがある。 というのも、同遵守事項の小項目において、(1) クラウドサービスの利用における対策の(a) を見ると、「クラウドサービス（民間事業者が提供するものに限らず、政府が自ら提供するものを含む。以下同じ。）を利用するに当たり」という表現が出てくる。そうすると、同(b)(c)(e)で出てくる「クラウドサービス」の「委託先」という表現は、両者（前者であれば民間事業者が提供する場合のさらに委託先として下請け業者を指すこととなり、後者であれば政府が自ら提供する場合の委託先としてクラウドサービス提供事業者自身を指すことになろうか）を含む概念になってしまい分かりにくい。 そもそも、4.1.4は全体的に、政府機関がクラウドサービスの利用者であって、政府機関内部向けであろうと住民サービスであろうと一定の業務について、その一部をクラウドサービス提供事業者に委託するというシナリオを前提にしているように読める。そうであれば、「委託先」という表現は避けて「クラウドサービス提供事業者」とするなど、混乱が生じないように分かりやすく表現してほしい。	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お示しします。 「4.1.1 外部委託」の「目的・趣旨」において「…外部委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。」と記述しており、混乱や誤解が生じることはないものと理解しています。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
34	日本マイクロソフト株式会社	ガイドライン	P.118	4.1.4	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 P118で3つの例（ISO/IEC 27017、クラウド情報セキュリティ監査、SOC報告書）が出てくるが、その重要性からしても読み手の理解の容易性からしても、ガイドラインではなく統一基準の中で例示すべきである。また、その際には、ISO/IEC 27017をベースとしたクラウド情報セキュリティ監査に基づく我が国固有のクラウドセキュリティマーク制度がせっかく新設されて運用が開始されているのだから、それについてまず記載するべきである。次にそのベースとなったISO/IEC 27017について記載し、そのあとでSOC報告書について記載するのが妥当である。 なおISO/IEC 27017について記載する際には、単に国際規格というだけでなく、認定機関による認証がなされていることを含め正確な記載をしていただきたい。	統一基準に例示すべきとの御意見についてですが、具体的な認定・認証制度の例示は統一基準に規定すべき性質のものではなく、ガイドラインに記載することとしています。 JASAのCSマーク制度の記載提案について、ガイドラインの解説において「その他、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…を活用することも考えられる。」として紹介しております。
35	日本マイクロソフト株式会社	ガイドライン	P.116 P.120	4.1.4	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 遵守事項4.1.4(1)(a)「情報の取扱いを委ねることの可否」について、の解説で、「クラウドサービスの利用に当たっては、情報の管理や処理をクラウドサービス事業者に委ねるため・・・」との表記がある。 しかし、当該情報の中身に関与しないクラウドサービスにおいては、当該情報の管理責任はあくまで利用者の側に留保される。 例えば、4.1.4(1)-2c)「クラウドサービスの委託先による情報の管理・保管」について、の解説で、「当該情報の責任は利用者である情報オーナーが負うことになる」と言っているのはそのような趣旨であろう。情報オーナー（Data Subject）、情報管理者（Data Controller）、情報処理者（Data Processor）という違いを意識すべきであり、クラウドサービス事業者が常に情報管理主体となることを前提とするように読める冒頭のような記述は削除すべきであり、責任分界点はクラウドサービス内容によって異なることが分かるように記載いただきたい。	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お示しします。 御指摘の遵守事項4.1.4(1)(a)及びその解説において、クラウドサービスの委託先による情報の管理や処理をもって当該情報の管理責任がクラウドサービス事業者側にあるとは規定していません。ガイドラインの基本対策事項4.1.4(1)-2c)の解説に、「当該情報の責任は利用者である情報オーナーが負う」と明確に記載することで誤解は生じないものと考えます。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
36	日本マイクロソフト株式会社	ガイドライン	P.116	4.1.4(1)(a)	情報セキュリティ強化の観点から統一基準群の改定（案）が策定され、年金機構事案等を踏まえた対策強化が行われることについて賛同します。さらに改善して欲しい点について、意見を述べます。 遵守事項4.1.4(1)(a)「情報の取扱いを委ねることの可否」について、の解説で、リスクとして挙げられている項目の「不特定多数の利用者の情報やプログラムを一つのクラウド基盤で共用することとなるため、情報が漏えいするリスクが存在する」との表記がある。 しかし、共用すること自体から情報が漏えいするリスクが導かれるような表現は誤解を生じる。 例えば、一戸建てなら安全だがマンションは建物を共用しているので盗難にあうリスクがある、というと論理飛躍で違和感があるのと同様である。この部分は削除とするか、「・・・共用することとなるため、個々のユーザーごとの環境の分離が適切に行われていることの確認を行うこと」といった方向での内容にすべきである（ISO/IEC 27017の13.1.3 Segregation in Networkを参照する等）。	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お示しします。 この解説の目的は、2～4行目で「そこで、適切なクラウドサービス事業者を選定することにより以下のようなリスクを低減することが考えられる。」のとおり、『適切なサービス事業者の存在を強調すること』です。よって、御指摘の表現は、政府機関側の読者にとっては留意すべきリスクとして理解しやすい例示であり、上記の適切なサービス事業者を強調するとの事項と併せ、バランスを取った表現としたものです。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
37	日本オラクル株式会社	ガイドライン	P.127 P.128	5.1.2(1)(a)	以下の「ISO/IEC 15408に基づく認証」に関する記述を「参考事項」に変更する。 · 基本対策事項　＜5.1.2(1)(a)関連＞ [現案] 5.1.2(1)-2・・・ISO/IEC 15408に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準と して定めること。 [提案] 5.1.2(1)-2・・・ISO/IEC 15408に基づく認証を取得しているか否かを、調達時の参考事項として機器等の選定基準に加えるこ と。 · （解説）基本対策事項5.1.2(1)-2「ISO/IEC 15408に基づく認証」について [現案] 機器等の調達においては、ISO/IEC 15408に基づく認証を取得している製品の優遇を選定基準の一つとすることで、第三者による情報セキュリティ機能の客観的な評価を受けた製品を活用でき、信頼度の高い情報システムが構築できる。 [提案] 機器等の調達においては、ISO/IEC 15408に基づく認証を取得している製品を参考事項に加えることで、第三者による情報セキュリティ機能の客観的な評価を受けた製品を活用でき、信頼度の高い情報システムが構築できる。但し、どの時点の保証を得ている認証製品であるかを調達時に確認することが必要となることと、認証の取得には一定期間が必要なため、選定対象を認証製品に限定すると最新の製品や技術の恩恵を受けられない制約になることを理解する必要がある。 【理由】 ISO/IEC15408に基づく認証は国際的な極めて重要な枠組みと考えます。しかしその認証取得には長期の審査と多大な経費が必要となります。実際問題として、新製品のリリースから認証取得まで長い期間を必要とするため、当該認証取得を評価項目に加えると、古い製品又はセキュリティ対策能力の低い製品が選定され、結果として情報システム全体のセキュリティ強度が低下するなど、セキュリティ対策が後手に回ります。 現在、セキュリティ対策はリスクマネジメントフレームワークを活用したリスクベースの対策へ軸足を移しつつあると認識していますので、典型的なチェックベースのポリシーであるISO/IEC15408認証取得を参考事項として位置付けることが良いと考えます。	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お示しします。 ガイドライン基本対策事項5.1.2(1)-2では、ISO/IEC15408に基づく認証の取得を調達時の評価項目とすることを定めていますが、第三者による客観的な評価を必要と判断する場合に限るものであり、一律の基準ではないため、御指摘の御懸念には及ばないと考えます。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
38	BSA｜ザ・ソフトウェア・アライアンス	ガイドライン	P.133	5.2.1(2)(a)	5.2.1の遵守事項(2)(a)及び府省庁対策基準策定のためのガイドライン（28年度版）（以下「本ガイドライン」）（133頁）における「インターネットやインターネットに接点を有する情報システム（クラウドサービスを含む。）から分離」に関する記述を削除することを求めます。これにより、本基準群が政府職員に対して情報システムのセキュリティを確保するための最も効果的な方法がインターネットからの分離であるとの誤解を生じさせてしまうことを防ぐことができます。	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お示しします。 インターネットに接点を有する情報システムにおいては、メール等の標的型攻撃による不正プログラム感染は避けられないものになっており、既に政府機関において様々な取組を進めているところ、本規定は、その一つを情報システムを構築する際の重要な要件として規定したものです。「インターネットに接点を有する情報システムから分離すれば他の対策は不要」といった趣旨ではなく、あくまで対策事項の一つとして位置づけられるものです。
39	（株）セールスフォース・ドットコム	ガイドライン	P.133	5.2.1(2)(a)	【原文】情報システムのセキュリティ要件の策定 【意見】 本項のガイドラインの解説には、「特に重要な情報を取り扱う情報システムについては、インターネットからの直接的なサイバー攻撃を受けないよう、インターネット回線や、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することが求められる」とありますが、昨今の標的型攻撃による情報漏えい事件はインターネットに繋がった情報システムから漏洩する事案だけでなく、インターネットからはアクセス出来ない情報システムからの漏洩も多く存在しております。インターネットに繋がっているから危険なのではなく、利用する者のリテラシーおよびネットワーク構成、インターネットに繋がっていない情報システムのあり方にも依存するので、限定的に「インターネットに接点を有する情報システムからを分離することを求める」事が対策にはならないのではと考えます。記載について再考いただくことを望みます。	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お示しします。 インターネットに接点を有する情報システムにおいては、メール等の標的型攻撃による不正プログラム感染は避けられないものになっており、既に政府機関において様々な取組を進めているところ、本規定は、その一つを情報システムを構築する際の重要な要件として規定したものです。「インターネットに接点を有する情報システムから分離すれば他の対策は不要」といった趣旨ではなく、あくまで対策事項の一つとして位置づけられるものです。
40	（株）セールスフォース・ドットコム	ガイドライン	P.133	5.2.1(2)(a)	【原文】情報システムのセキュリティ要件の策定 【質問】 本項のガイドラインの解説には、「特に重要な情報を取り扱う情報システムについては、インターネットからの直接的なサイバー攻撃を受けないよう、インターネット回線や、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することが求められる」とありますが、この「特に重要な情報」とは機密性3の情報という理解でよろしいでしょうか？	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お示しします。 政府機関が特に重要な情報と考える情報であり、機密性3情報と規定していません。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
41	KPMGコンサルティング株式会社	ガイドライン	P.163	6.1.2(1)-1 d)	解説　基本対策事項6.1.2(1)-1 d)「ネットワークセグメントの分割によるアクセス制御」について セグメンテーションの分割による分離を実施した場合、そのセグメンテーションが有効であることを定期的に検証する観点を取り入れることが望ましいと考えます。当該有効性の確認手段の例として、ペネトレーションテスト等が考えられます。	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お示しします。 御指摘の内容については、遵守事項5.2.3(1)(a)及び基本対策事項5.2.3(1)-2において、セキュリティ機能の適切な運用を求める規定に含まれております。
42	KPMGコンサルティング株式会社	ガイドライン	P.165	6.1.3(1)-1 b)	解説　基本対策事項6.1.3(1)-1 b)「必要最小限の権限のみ付与」について 標準で組み込まれた識別コード（例　WindowsにおけるAdministrator等）を無効化する観点も取り入れることが望ましいと考えます。この観点は基本対策事項として定義することも考えられます。	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お示しします。 不要な管理者権限アカウントの削除については、ガイドラインの基本対策事項6.2.4(1)-4a)において規定しています。
43	KPMGコンサルティング株式会社	ガイドライン	P.168	6.1.4(1)(b)	解説　遵守事項6.1.4(1)(b)「保存期間」について 世間の動向に鑑みると、不正アクセス発生等から1年以上経過したのちに情報漏えい等が検知される事例も多数あるため、ログの推奨保存期間が1年で十分か否かを、再度検討することが望ましいと考えます。（当然に設備投資の費用対効果の観点もあるため、それらを踏まえた検討が必要と思料します）	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お示しします。 御指摘の点については承知しており、解説において「過去の事例を踏まえ、ログは1年以上保存することが望ましい」としております。

No.	提出者	対象文書	該当箇所		概要	御意見に対する考え方
			ページ	章節項		
44	KPMGコンサルティング株式会社	ガイドライン	P.181	6.2.2(1)(c)	基本対策事項 ＜6.2.2(1)(c)関連＞について 6.2.2(1)-5 情報システムセキュリティ責任者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。 a) 不正プログラム対策ソフトウェア等の導入状況 b) 不正プログラム対策ソフトウェア等の定義ファイルの更新状況 上記例示として、電子メールに添付されている実行形式ファイルの不用意な実行防止や最近のランサムウェアによる被害の増加を勘案し、 c) 外部から入手した実行形式ファイルの実行を不可能となるように設定 d) 添付ファイルとして実行形式ファイルを付した電子メールの送受信遮断 e) 不正プログラム対策に係る適時のデータバックアップの徹底 を追記することが望ましいと考えます。	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、次のとおり考え方をお示しします。 御指摘の実行プログラム形式ファイルの取扱いについては、基本対策事項8.1.1(2)-2、データバックアップについては、遵守事項3.1.1(8)(a)において規定を設けています。
45	KPMGコンサルティング株式会社	ガイドライン	P.188	6.2.4(1)(a)	解説　遵守事項6.2.4(1)(a)「標的型攻撃」について 標的型攻撃への対策として、以下の事項も有効であると考えます。 ・6.1.1項　主体認証機能 ・6.1.2項　アクセス制御機能 ・6.1.3項　権限管理機能 ・6.1.4項　ログの取得・管理 ・6.1.5項　暗号・電子署名	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、解説を補足します。
46	KPMGコンサルティング株式会社	ガイドライン	P.187	6.2.4(1)-2 e)	基本対策事項　6.2.4(1)-2 e) USBポートの無効化のみならず、CD/DVDドライブの原則無効化も例示することが望ましいと考えます。	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、次のとおり考え方をお示しします。 最も危険性が高いUSBメモリの対策について例示していますが、本項の規定で、「USBメモリ等の外部電磁的記録媒体」が対象であることを明記しており、御指摘のCD/DVDドライブについても含まれるため、原案どおりとさせていただきます。