「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のウェブ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：2018年６月７日（木）～６月28日（木）
- 意見総数：21者から66件 【内訳：14企業・団体から延べ58件、７個人から延べ８件】

・統一規範に０件、統一基準に61件、運用指針に２件、全般に対して３件の意見提出

（１）修正意見：全63件

・表現の適正化を求めるものについて、統一基準を修正（１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（62件）

☆主な意見

・未知の不正プログラムに係る被害の未然防止／拡大防止や、IT資産管理の自動化に係る将来像を見据えた対策に関する意見（14件）

・ウェブサイトや電子メールの暗号化による利用者側に立った対策に関する意見（４件）

・PDCAサイクルの効果的運用のための体制等の整備に関する意見（８件）

（２）その他の意見：全３件

※意見募集の対象外である「政府機関等の対策基準策定のためのガイドライン」に対しても延べ15件の意見提出

解説の充実や表現の適正化を求めるものについては、趣旨を踏まえてガイドラインを修正（８件）

（参考）提出者名：

株式会社 FFRI、CyberArk Software株式会社、スプランクサービスジャパン合同会社、株式会社テリロジー、トレンドマイクロ株式会社、日本マイクロソフト株式会社、マカフィー株式会社、一般社団法人 日本ネットワークインフォメーションセンター、特定非営利活動法人 日本セキュリティ監査協会、特定非営利活動法人 日本ネットワークセキュリティ協会、BSA | ザ・ソフトウェア・アライアンス、迷惑メール対策推進協議会、国立研究開発法人 国立国際医療研究センター、大学共同利用機関法人 情報・システム研究機構国立情報学研究所、個人（７）

「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一覧

通し 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	大学共同利用機関法人 国立情報学研究所	統一基準	p.1	1.1	(2)以降は全て「適用範囲」を「適用対象」と変更しているので、本標題も変更すべきではないか。	御指摘の統一基準1.1表題の「適用範囲」の字句は、1.1(2)「本統一基準の適用対象」のみに対応している訳ではありません。 1.1(5)「対策項目の記載事項」に記載のとおり、基本対策事項が遵守事項に対応するものであることから、ガイドラインに記載の基本対策事項も本統一基準の範囲としていることを示すため、「適用範囲」と記載しております。
2	特定非営利活動法人 日本セキュリティ監査協会	統一基準	p.6	1.3	「機関等」について下記を用語定義に追加 ● 「機関等」とは、府省庁及び独立行政法人及び指定法人の総称であり、「政府機関等」ともいう。 理由: 現行は「府省庁」なのでわかりやすいが、「機関等」だと具体的にどのような組織が含まれるのかあいまいなため。	御指摘の点に関して、統一規範第2条第2項において「国の行政機関、独立行政法人及び指定法人(以下「機関等」という。)」と記載しており、機関等にどの組織が含まれるかは明らかと考えられます。
3	特定非営利活動法人 日本セキュリティ監査協会	統一基準	p.7 p.57	1.3 7.3.2目的・趣旨	「ネットワーク」「通信ネットワーク」については、「通信回線」に変更 理由: 「ネットワーク」「通信ネットワーク」は「通信回線」と同義であり、統一すべき	御指摘については、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、これらの用語については遵守事項では全て「通信回線」で統一しています。他の箇所では文脈上わかりやすい表現を用いています。このため、原案のとおりとします。
4	大学共同利用機関法人 国立情報学研究所	統一基準	p.8	1.3	統一規範(案) の第ニ条2で定義されている「職員等」よりも範囲が広がっている印象を受ける。すべての組織において「職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている」を対象とすることが不適切な場合も考えられるため、「職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含めることが適切な場合も考えられる」のような記述のほうが、統一規範との整合性が高まるのではないか。	御指摘では、「すべての組織において『職員等には(中略)研修生等も含まれている』を対象とすることが不適切な場合が考えられる」とのことですが、派遣労働者、研修生等の機関等の指揮命令に服している者を職員等に含めることが不適切な場合とは、これらの者が機関等の管理対象である情報及び情報システムを取り扱わない場合に限られ、統一規範第2条第2項においては「次項に規定する情報を取り扱う者とする。」、統一基準1.3用語定義においては「機関等の管理対象である情報及び情報システムを取り扱う者をいう。」と定めているため、両文書の「職員等」の対象の範囲は一致していることから、原案のとおりとします。

通し 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		
5	独立行政法人 情報処理推進機構	ガイドライン	p.16	1.6	CRYPTRECに関する記述について、暗号モジュール評価基準については、現在、CRYPTRECの検討の対象になっていないため、CRYPTRECのWebページの記載にならい次のように更新すべきと考えます。 現行:「CRYPTREC(Cryptography Research and Evaluation Committees)」とは、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。 新 :「CRYPTREC(Cryptography Research and Evaluation Committees)」とは、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。	ガイドラインについては、パブリックコメントの対象ではなく、また、本改定における改定箇所ではありませんが、御意見を踏まえ修正します。
6	スプランク サービス ジャパン合同会社	統一基準		第2部 第6部	新規要件の追加:第2部に「システムの監視」を記載するとともに、第6部において「システムの監視と可視化」について要件化することを推奨します。 意見理由 第6部においては個々の対策については網羅されているが、それらを一元的に監視する可視化の仕組みを基準化することが必要と考えられます。個々の対策状況(認証、アクセス制御、不正プログラム対策等)を把握する具体的な手段を基準化しなければ、管理者によるセキュリティ上の問題の把握が難しく、政府ITシステム全体のセキュリティが確保されにくいと考えます。参考までに各国で謳われている検知や報告に関する統制状況を鑑みると(GDPR:72時間以内、CDM:72時間以内)、何らかの監視と可視化の義務化、報告までの目標期限が設定されています。我が国としても同等の基準が必要と考えています。	御指摘は、本改定における改定箇所ではないため、パブリックコメントの対象ではありませんが、御指摘の点について重要と考えており、今回のガイドラインの改定にあたり、IT資産のシステムによる管理について記載を追加しております。頂いた御指摘については、今後の検討の参考とさせていただきます。
7	個人	統一基準	p.11	2.1.1(5)(a)	(5) 最高情報セキュリティアドバイザーの設置 (a) 最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する者を最高情報セキュリティアドバイザーとして置き、自らへの助言を含む最高情報セキュリティアドバイザーの業務内容を定めること。 に関して、最高情報セキュリティアドバイザーの専門知識及び経験を担保するために情報処理安全確保支援士または同等以上の能力を有すると認められる者(CISSP等の国際資格)から最高情報セキュリティアドバイザーを専任することを要件とするべきと考えます。	御指摘については、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、最高情報セキュリティアドバイザーの業務内容は基本対策事項2.1.1(5)-1の例示のとおり多岐にわたることから、その能力を一定程度証明する資格の一つとして、情報処理安全確保支援士も考えられますが、これに限るものではないと考えられ、原案のとおりとします。
8	個人	統一基準	p.11	2.1.1(7)	「統一基準」中の2.1.1 (7)「情報セキュリティインシデントに備えた体制の整備」については、「NISCにおける『CYMAT』および政府機関等における『CSIRT』においては『情報処理安全確保支援士』の資格を有する職員等を必ず配置する」など、「情報処理安全確保支援士」を積極的に活用することを明示してはどうか。	CSIRT/CYMATに属する職員には、情報セキュリティ等に関する知識及び技能を有する者を充てることとしているが、それぞれCSIRT/CYMATに特化した知識及び技能に係る教育を提供しているところ、これら要員には特定の資格を求めていないため、原案のとおりとします。

通し 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		
9	個人	統一基準	p.11	2.1.1(5)(a) 2.1.1(7)(b)	「政府機関等の情報セキュリティ対策のための統一基準（案）」について意見を述べたい。 p10「組織・体制の整備」の項目内容において専門性を認定する具体的基準が欠けていると感じた。 特に、 ・p11.「(5) 最高情報セキュリティアドバイザーの設置」にて 『(a) 最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する者を最高情報セキュリティアドバイザーとして置き、自らへの助言を含む最高情報セキュリティアドバイザーの業務内容を定めること。』 と記載ある。また同様の表記として、 ・p11 「(7) 情報セキュリティインシデントに備えた体制の整備」にて 『(b) 最高情報セキュリティ責任者は、職員等のうちから CSIRT に属する職員等として専門的な知識又は適性を有すると認められる者を選任すること。』 との表記がある。 双方とも「専門的な知識」を求めているが、これを認定する具体的基準が欠けているため下記内容の追加を提案する。 経済産業省の「情報セキュリティサービス基準」を参照し、このp11「４．セキュリティ監視・運用サービスに関する附則 」に例示される「情報処理安全確保支援士」などの資格を専門的知識の認定要件とすることを提案する。 この資格は政府IT入札要件、内閣官房情報通信技術(IT)総合戦略室と総務省行政管理局の定める「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書（第3編第6章 調達）」のP44、P91、P92にも要件として示されている。	御指摘については、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、最高情報セキュリティアドバイザーの業務内容は基本対策事項2.1.1(5)-1の例示のとおり多岐にわたることから、その能力を一定程度証明する資格の一つとして、情報処理安全確保支援士も考えられますが、これに限るものではないと考えられ、原案のとおりとします。 また、CSIRTに属する職員には、情報セキュリティ等に関する知識及び技能を有する者を充てることとしているが、CSIRTに特化した知識及び技能に係る教育を提供しているところ、これら要員には特定の資格を求めていないため、原案のとおりとします。
10	東日本高速道路株式会社	ガイドライン	p.21 p.25	2.1.1(1)(b) 2.1.1(4)(a)	統一基準2.1.1(1)(b)最高情報セキュリティ副責任者と2.1.1(4)(a)統括情報セキュリティ責任者の違いについて。今回の改定で最高情報セキュリティ副責任者を必要に応じておくことができるように規定され、業務を見ると「最高情報セキュリティ責任者を助けて．．．」と記載されています。一方以前からある統括情報セキュリティ責任者は「最高情報セキュリティ責任者を補佐する者．．．」と記載されています。助けると補佐は同義語なので、この両者の業務の違いがはっきりと理解できません。最高情報セキュリティ副責任者と統括情報セキュリティ責任者の違いをガイドラインで業務の具体例を明示しながら明記していただけないでしょうか。	最高情報セキュリティ責任者の役割は、遵守事項2.1.1(1)(a)において「機関等における情報セキュリティに関する事務を統括する」ことと規定しており、ここで「事務を統括する」とは、ガイドラインの解説「遵守事項2.1.1(1)(a)『最高情報セキュリティ責任者』について」に記載のとおり、組織をふ瞰し、資源配分の方針決定を適切に行うなどリーダーシップを発揮することを意味しますが、これら最高情報セキュリティ責任者の所掌する事務を分掌することが、最高情報セキュリティ副責任者の役割となります。 一方、統括情報セキュリティ責任者の役割は、ガイドラインの解説「遵守事項2.1.1(4)(a)『統括情報セキュリティ責任者』について」に記載のとおり、「機関等の情報セキュリティ対策について総合調整する事務を担う」ことであり、ここで「総合調整する事務を担う」とは、機関等における具体的な情報セキュリティ対策を取りまとめることを意味します。 以上のことから、最高情報セキュリティ副責任者と統括情報セキュリティ責任者の役割は明確に異なることから、原案のとおりとします。

通し 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		
11	独立行政法人 情報処理推進機構	ガイドライン	p.40 p.42	2.1.2(1)(a)解説	JIS の用語に基づいて、JISについて、X章としている部分は、箇条Xと改めるべきと考えます。 現行：JIS Q 31000:2010, 5章 新　：JIS Q 31000:2010, 箇条5	ガイドラインについては、パブリックコメントの対象ではありませんが、御指摘を踏まえ修正します。
12	大学共同利用機関法人 国立情報学研究所	統一基準	p.10	2.1.1(1)(b)	最高情報セキュリティ副責任者は、最高情報セキュリティ責任者の命を受けてにしても、事務を「統括」すると定めるのは不適切ではないか。ガイドラインに示されている副責任者設置の趣旨を踏まえると、「統括を補佐する」「統括業務を分担する」程度の書き方が適切ではないか。また、最高情報セキュリティ副責任者の役割として、最高情報セキュリティ責任者に事故があった場合（緊急時にその役割を担うことが困難な場合を含む）に最高情報セキュリティ責任者の役割を代行することも定めるべきではないか。	最高情報セキュリティ副責任者の役割は、最高情報セキュリティ責任者の所掌する事務を分掌することであることから、最高情報セキュリティ責任者の規定（遵守事項2.1.1(1)(a)）と同様の「事務を統括する」という表現を用いております。 また、最高情報セキュリティ副責任者の役割は、各組織において、最高情報セキュリティ責任者が、最高情報セキュリティ副責任者へ命を与えることにより決まることから、統一基準に規定する必要はないと考えております。
13	大学共同利用機関法人 国立情報学研究所	統一基準	p.10	2.1.1(2)(a)	情報セキュリティ対策推進体制は、対策基準等の(審議)策定とも密接な関係を持つと考えられるため、(2)の情報セキュリティ委員会の役割と統合する規定として、次のように修正してはどうか。 「最高情報セキュリティ責任者は、機関等の情報セキュリティ対策推進体制の整備ならびに対策基準等の審議を行う組織として、部局の代表者を構成員とする情報セキュリティ委員会を置くこと。」	情報セキュリティ対策推進体制の役割は、機関等の情報セキュリティ対策の推進に係る事務を遂行することであり、一方、情報セキュリティ委員会の役割は、情報セキュリティに係る組織横断的な事項を審議することです。したがって、両者は役割が異なるため、原案のとおりとします。
14	大学共同利用機関法人 国立情報学研究所	統一基準	p.10	2.1.1(4)(a)	機関の実態等を鑑みて、統括情報セキュリティ責任者は最高情報セキュリティ副責任者と兼務できる規定にしてはどうか。	最高情報セキュリティ副責任者の役割は最高情報セキュリティ責任者の所掌する事務を分掌することであり、一方、統括情報セキュリティ責任者の役割は機関等における具体的な情報セキュリティ対策を取りまとめることであることから、両者は役割が異なります。また、遵守事項2.1.1(1)(b)において最高情報セキュリティ副責任者は必要に応じて置くことと規定しており、機関等において必ず設置される役職ではありません。これらを踏まえると、最高情報セキュリティ副責任者と統括情報セキュリティ責任者の兼務についてあらかじめ規定しておくことは適切とは考えられないため、原案のとおりとします。
15	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.10	2.1.1(1)(b)	「最高情報セキュリティ副責任者１名を必要に応じて置くこと」とされているが、組織の事情によっては副責任者を2名以上置くのが適切な可能性もあると思われるので、「最高情報セキュリティ副責任者１名以上を必要に応じて置くこと」とすべきではないか。	御指摘の点につきましては、各行政機関におけるサイバーセキュリティ担当の幹部職員の配置状況の実態に鑑み、これを統一基準に反映したものであるため、原案のとおりとします。

通し 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	BSA｜ザ・ソフトウェア・アライアンス	統一基準	p.29	4.1.4	我々は特にクラウドサービスの利用に関する箇所（第 4 部「外部委託」 4.1.4「クラウドサービスの利用」）において、クラウドサービスを利用する場合にはセキュリティリスクが高くなると解釈されかねないことを懸念します。当該箇所の記述は、オンプレミスのITシステムと比較してクラウドコンピューティングのリスクが高くなるのではないかという印象を与え、誤解を招きかねません。また、プライベートクラウド、パブリッククラウド、ハイブリッドクラウドなど様々なクラウドサービスモデルを考慮に入れることも重要であり、オンプレミスシステム同様、具体的なリスクは、どのような状況で使用されるかに基づいて評価されなければなりません。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、クラウドサービスの利用において、検討しなければならないことや契約に定める要件等を定めており、セキュリティリスクについてクラウドサービスをオンプレミスの情報システムと比較して論じているわけではありません。
17	BSA｜ザ・ソフトウェア・アライアンス	統一基準	p.29	4.1.4(1)(b)	4.1.4「 遵守事項(1)(b)」において、委託業務の実施場所に関する記述も修正した方が良いと考えます。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足り、本基準群において委託事業の実施場所の指定を求める必要はないと考えます。日本政府はクラウドコンピューティング利用を促進しようとされていますが、その一方で、このような記載をすれば、クラウドコンピューティング技術やサービスの導入が阻まれてしまうことになります。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、クラウドサービスの利用契約において準拠法が合意されている場合でも、サーバが国外にある場合に、国外法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おり、原案のとおりとします。
18	マカフィー株式会社	統一基準	p.29	4.1.4(1)(a)	変更案: (a)情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、機関等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、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すると共に委ねた情報に対して適切な取扱制限を実施すること。 理由: 重要な情報を委ねることの可否に加えて、委ねると判断した後にクラウドサービスへ保存される情報に対して適切な対策を実施していくことが重要であると考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、クラウドの利用におけるセキュリティ対策は、遵守事項4.1.4(1)(d)に規定し、具体的な対策は、基本対策事項4.1.4(1)-2に記載しているため、原案のとおりとします。
19	マカフィー株式会社	統一基準	p.29	4.1.4(1)(b)	変更案: (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が望ましい。 理由: 「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」という記載により、クラウドサービス事業者選定の幅が狭まるため、表現の緩和が必要と考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、4.1.4「クラウドサービスの利用」は、クラウドサービスのセキュリティを確保するため、利用における対策を規定しているものであり、ご指摘の「クラウドサービス事業者選定の幅が狭まるため、表現の緩和」については、統一基準の本旨にそぐわないため、原案のとおりとします。
20	マカフィー株式会社	統一基準	p.29	4.1.4(1)(b)	変更案: (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が適用されるリスクを評価して委託先を選定すること。 理由: 「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」という記載により、クラウドサービス事業者選定の幅が狭まることが想定されます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、クラウドサービスの利用に当たっては、その委託先で機関等の情報が適切に取り扱われることが重要であるため遵守事項4.1.4(1)(b)「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。」が必要と考えており、原案のとおりとします。

通し 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		
21	マカフィー株式会社	統一基準	p.29	4.1.4(1)(c)	変更案: (c) 情報システムセキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、利用するサービスを選定する際の要件とすること。 理由: クラウドサービスの活用を考えていく上で、「委託」という考えが適合し難いと考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、利用するサービスを含めた委託先を選定する際の要件として記載しているため、原案のとおりとします。
22	マカフィー株式会社	統一基準	p.29	4.1.4(1)(d)	変更案: (d) 情報システムセキュリティ責任者は、クラウドサービスの特性である「共同責任モデル（責任共有モデル）」を理解し、4.1.4(1)(a)基づく情報の格付けに応じて、利用者側が実施できるセキュリティ対策について検討し要件を定めること。また、自機関が認可したクラウドサービス以外が利用されていないかを監視する仕組みもその要件に含むこと。 理由: クラウドという環境において、情報の流通経路全般を見渡しセキュリティ設計を行うことは、クラウドサービス利用者においてはほぼ不可能に近いと考えます。4.1.4の目的・趣旨の8行目以降の記載にある「また、クラウドサービスでは、～困難である」と本項目は乖離があるように思われます。クラウドサービス利用の特性を理解する上では、一般的には「共同責任モデル（責任共有モデル）」という考え方を述べた方が適切と考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、クラウドサービスとオンプレミスでは異なる特性があることから、情報の流通経路全般を俯瞰してセキュリティ対策を講ずる必要があり、4.1.4(1)(d)にこれを記載しております。また、「自機関が認可したクラウドサービス以外が利用されていないかを監視する仕組み」については、遵守事項7.3.1(1)(h)において、「情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間で送受信される通信内容を監視するための措置を講ずること。」と定めており、さらに基本対策事項8.1.1(2)(a)においてウェブサイトフィルタリング機能を例とした「職員等が閲覧できる範囲を制限する機能を情報システムに導入すること」を求めているため、原案のとおりとします。
23	マカフィー株式会社	統一基準	p.29	4.1.4(1)(e)	変更案: (e) 情報システムセキュリティ責任者は、クラウドサービス利用検討時の及び、利用後において各クラウドサービスに関する安全性の格付け情報を収集すること。利用するサービスの信頼性が十分であるかを第三者機関の評価に基づき定期的にスクリーニングし利用の検討や、利用の継続を判断すること。 理由: クラウドサービスにおいては、個々の利用者が個別にクラウド事業者の安全性を確保するために監査等を行よりも、信頼できる第三者機関の評価を定期的に入手し確認することが重要と考えます。CSA（Cloud Security Alliance）などが求めるセキュリティ基準を満たしているかなど標準化された指標での評価を入手できることが必要と考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、ご指摘の第三者機関の評価については、ガイドラインの解説4.1.4(1)(e)「クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること」について」において、既に第三者による監査／認証等を活用することとしており、原案のとおりとします。
24	マカフィー株式会社	統一基準	p.29	4.1.4(1)(f)	追加案: (f) 情報システムセキュリティ責任者は、クラウドサービス利用する場合は、自機関の利用者に起因して起きるセキュリティインシデントにも留意しセキュリティ対策を講じること。 理由: 4.1.1には、事業者がセキュリティインシデントを起こした場合、もしくはその危険性については備えるように言及しているが、自機関における利用者に起因した事案（アカウント情報の漏洩）への言及がされていません。クラウドサービス利用においては、この点に備えるように言及すべきであると考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、御指摘の利用者に起因するセキュリティインシデント（アカウント情報の漏えい）の対策として、遵守事項8.1.1(5)にて識別コード・主体認証情報の取扱いに係る対策を記載しているため、原案のとおりとします。

通し 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		
25	マカフィー株式会社	統一基準	p.29	4.1.4(1)(f)	追加案: (f)情報システムセキュリティ責任者は、自身が認知・許可していないクラウドサービスが使用されていないことを定期的に確認し、使用されている場合には適切な対策を実施すること。 理由: 情報システム担当が許可しているクラウドサービスでは無いもの(シャドーIT)が使用されていることが大きな課題になっており、遵守事項として明記する必要があると考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、遵守事項7.3.1(1)(h)において、「情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間で送受信される通信内容を監視するための措置を講ずること。」と定めており、さらに基本対策事項8.1.1(2)-1においてウェブサイトフィルタリング機能を例とした「職員等が閲覧できる範囲を制限する機能を情報システムに導入すること」を求めているため、原案のとおりとします。
26	日本マイクロソフト株式会社	統一基準	p.25	4.1.1(2)(b)	クラウドサービスの提供において、左記に関する規格や認証の取得の証明により、上記にかかる情報提供は不要として頂きたい。 理由: 専門機関による第三者の監査結果によって、クラウドサービス提供上、十分なセキュリティ対策が講じられているか確認しうると考えるため。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、遵守事項4.1.1(2)(b)において定めている事項は、情報セキュリティ責任者が情報システムの運用等を外部委託する際に、情報システムの特性も踏まえ実施すべき情報セキュリティ対策について規定しているものであり、クラウドサービス事業者が自ら取得する第三者の認証により確認される事項とは必ずしも合致するものではないため、原案のとおりとします。
27	日本マイクロソフト株式会社	統一基準	p.26	4.1.1(2)(c)(ア)	クラウドサービスの利用においては、信頼に足る第3者監査機関によるクラウドサービスに対する監査結果をもって、代替できることとして頂きたい。 理由: 専門機関による第三者の監査結果によって、クラウドサービス提供上、十分なセキュリティ対策が講じられているか確認しうると考えるため。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、遵守事項4.1.1(2)(c)(ア)の規定は、外部委託において、平常時だけではなくインシデント発生時などの必要性が生じた時に機関等自らが監査する場合も含まれることから、必ずしも第三者監査機関による監査結果によって代替できるものではないため、原案のとおりとします。
28	国立研究開発法人 国立国際医療研究センター	統一基準	p.26	4.1.1(2)(c)	情報セキュリティ監査の受け入れについて 独立行政法人の業態は多岐にわたるため、各独立行政法人に対して、外部委託している業者全てに対して情報セキュリティ監査を行うことは技術的にも人的にも困難である。また受け入れる業者側も、多くの顧客から監査を受け、内部の情報や体制を晒すこととなり、却って業者自身のセキュリティを下げることや、監査対応で著しく業務効率を下げることが予想される。 情報セキュリティ監査を受けた実績の報告で代替する等の対応を検討いただき、業態によっては(特に病院等の業務が多岐にわたり多数の外部委託を実施している法人など)この方法で許可する旨の文言を追加いただきたい。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、遵守事項4.1.1(2)(c)(ア)の規定は、「必要に応じた」ものであり、全ての外部委託先の情報セキュリティ監査を必ず実施しなければならないとするものではないため、原案のとおりとします。

通し 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		
29	個人	統一基準	p.29	4.1.4	クラウドシステム等の提供場所（提供ホスト所在国）についても注意するよう周知を行っていただきたい。（金融庁、財務省、国税庁等の各種ホストが香港やシンガポールにあるものによって提供されているのであるが、国民による個人情報や他機密ともすべき様な内容を含む意見提出や通報等をこれらに提出させるのか、という話である（フィンテック？聞いて呆れる。）。政府として止められたい。） また、名前解決のエリアスにより、*.go.jpとなっているホスト名を海外のサーバによって提供しないようにしていただきたい。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、クラウドサービスの利用に当たっては、その委託先で政府機関の情報が適切に取り扱われることが重要であり、遵守事項4.1.4(1)(b)「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。」と定めております。
30	特定非営利活動法人 日本セキュリティ監査協会	統一基準	p.30	5.1.1(1)	「統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備すること。」は文として不自然である。下記に修正すべき。 「統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項をとりまとめた情報システム台帳を整備すること。」	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、当該情報システムのセキュリティ要件に係る事項を情報システム台帳として整備する趣旨としており、誤解が生じるものではないと認識していることから、原案のとおりとします。
31	BSA｜ザ・ソフトウェア・アライアンス	統一基準	p.32	5.2.1(2)(a)	5.2.1 の「情報システムの企画・要件定義」における「遵守事項(2)(a)」において、セキュリティ対策として「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」することが提案されていることに懸念があります。インターネットから分離すれば、リアルタイムでセキュリティ・アップデイトを受けられるという利点が阻まれ、却ってリスクが増大しかねません。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、ガイドラインの解説「遵守事項5.2.1(2)(a)『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』について」に記載のとおり、特に重要な情報を取り扱う情報システムについてインターネットからの分離が求められる旨の考え方を示したものであり、情報システム全般について一律に分離を求めるものではなく、分離によるメリット、デメリットを総合的に判断した上で、分離の要否を判断することを求めています。したがって、御懸念の点も判断の要素に含まれております。

通し 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	一般社団法人 日本ネットワークインフォメーションセンター	統一基準	新規	5.2	ドメイン名の活用におけるライフサイクルの考慮について 情報システムのライフサイクルを考慮する際、ドメイン名のライフサイクルについても考慮が必要です。既存システムについても、日本の政府機関や各省庁所管の研究所、特殊法人、独立行政法人のみが登録可能なgo.jpドメイン名への移行により、ドロップキャッチを防止することができます。加えてこれまで利用した過去のgo.jpドメイン名以外のドメイン名の利用停止の際には、そのドメイン名を直ちに登録解除するのではなく、問題のなくなる期間までドメイン名を保持することで、ドロップキャッチを防止できます。 第5部 情報システムのライフサイクル、5.2 情報システムのライフサイクルの各段階における対策、において、次の通り提案します。 イ.「go.jpドメイン名ではないドメイン名を使用する政府機関等のシステムはgo.jpドメイン名への移行を推奨すること。go.jpドメイン名への移行後の旧ドメイン名については一定期間登録を維持するなど第三者による再登録への対策を採ること。」を追記する。 ロ.「go.jpドメイン名の使用ができず他のドメイン名を使用する場合は、使用後も一定期間登録を維持するなど第三者による再登録への対策を採ること。」を追記する。	御指摘については、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、御指摘の点については、政府部内においては、「Webサイト等の整備及び廃止に係るドメイン管理ガイドライン（2018年3月30日 各府省情報化統括責任者（CIO）連絡会議決定）」に規定されております。また、統一基準においても、遵守事項 6.3.2(1)(a) にて、政府ドメイン名の使用に関する規定を設けており、さらに、ガイドラインの解説「遵守事項6.3.2(1)(a)『政府ドメイン名を情報システムにおいて使用する』について」において、「仮に政府ドメイン名以外を使用した場合には、そのサイトの使用を終了した後も、当該ドメイン名を不正に利用されないように登録管理を一定期間維持しなければならない」ことを示しています。
33	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.33	5.2.1(2)(a)(イ)	「監視するデータが暗号化されている場合は、必要に応じて復号すること」とされているが、暗号化されている情報を監視環境において復号することが困難な場合も多いので、「監視するデータが暗号化されている場合は、可能な範囲で必要に応じて復号すること」としてはどうか。	復号の必要性を判断するに当たっては、暗号化されたデータを復号できるか否かについても踏まえることを想定しており、原案のとおりとします。
34	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.33	5.2.1(4)(b)	「当該対策による情報システムの変更内容について、速やかに報告させること」との記述内容がやや理解しにくいので、「当該対策による情報システムの変更内容について、変更が発生次第速やかに報告させること」としてはどうか。	御指摘の記載については、変更が発生した場合は、遅滞なく報告させるものとして記載しているものであり、誤解が生じるものではないと認識していることから、原案のとおりとします。
35	スプランクサービスジャパン合同会社	統一基準	p.40	6.1.4(1)(a)	6.1.4(1) (a)に「サーバ、ネットワーク及びクライアントに関する必要なログを取得すること」と明記の検討を推奨します。 意見理由 ガイドラインにはサーバー・ネットワーク等のログ取得の記載はあるが、クライアントについての記載は見受けられません。また、どのログを取得すべきかはガイドラインではなく、統一基準として明確に定めることを推奨します。特にクライアントログは重要であると考えており、今日のセキュリティ・インシデントの発生源は、70%以上がクライアントからというデータも存在します。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、端末のログを取得することも重要と考えており、6.1.4(1) (a)の情報システムには端末も含まれているため、原案のとおりとします。

通し 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	独立行政法人 情報処理推進機構	ガイドライン	p.191	6.1.5(1)(b)(エ)解説	遵守事項6.1.5(1)(b)(エ)「管理手順を定めること」について 情報システムとしての鍵の管理手順を1から全て情報システムセキュリティ管理者が作成することは、非常に負荷が高く複雑な作業です。現実には、鍵管理を担う製品や、鍵管理を半自動化・支援する製品が存在し、そういった製品を組み合わせて現実的で実行可能な鍵の管理手順を実施するべきと考えます。 そのため、「暗号化された情報の復号又は電子署名の～適切に管理する必要がある。」の後に、次のような記述を追加すべきと考えます。 情報システムとしての鍵の管理手順の一部であって、製品が提供する暗号鍵管理機能によって実現可能な管理手順については、これによって代替しても良い。「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については、(「公開セキュリティポリシ」(non-proprietary security policy)と呼ばれる、)製品が実現する鍵の管理方針が公開されており、情報システムとしての鍵の管理手順の作成にあたってそれを参照してもよい。	ガイドラインについては、パブリックコメントの対象ではなく、また、本改定における改定箇所ではありませんが、「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ことについては、基本対策事項6.1.5(1)-1c)に記載があり、また、御指摘いただいた解説については、鍵の管理手順を策定するに考慮する視点を記載しているため、原案のとおりとします。
37	独立行政法人 情報処理推進機構	ガイドライン	p.191	6.1.5(1)(b)(エ)解説	「鍵の廃棄」部分について 「廃棄」という単語によって、単に捨てるといったニュアンスが強くなってしまいますが、鍵のライフサイクルの中で求められていることは、暗号鍵が復元できないように「消去」「破壊」することです。 そのため、用語としては「鍵の消去」又は「鍵の破壊」が適切な表現と考えます。 (なお、JIS X 19790では「鍵のゼロ化」という表現を用いています。) その上で、説明として「確実に消去される仕組みが必要である」と述べていますが、仕組みがあるだけで実行されなければ問題です。 鍵を消去する状況では、何らかの情報機器に格納された状態で鍵の消去を行うわけですが、そこで想定される情報機器としてはUSBメモリ、SSD、HDD、HSMなどが考えられます。 例えば、SSD、USBメモリなどのウェアレベリングを用いたフラッシュメモリにおいては、HDDと同様の方法で情報を消去しようとしても、確実に消去されたかについては、ほとんど確認できないのが現実です。 また、HDDやSSDの媒体の不良のリスクだけでなく、コントローラが故障して、最終的に消去できなくなるリスクも考慮に入れるべきと考えます。PCをリース、レンタルしている場合、コントローラが故障して代替手段として磁気的に消去しようとしても、契約によって禁止されている場合もあります。 以上から、説明文に次のような記述を追加すべきと考えます。 鍵を格納する機器を廃棄又は返却する場合に備えて、鍵を確実に消去する機能が備わっている機器を選定・調達し、その機能を実行する運用が必要である。「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は、鍵を確実に消去する機能が備わっている。 鍵を確実に消去する機能が備わっていない機器に鍵を格納している場合には、代替となる消去方法を検討し実行する必要がある。	ガイドラインについては、パブリックコメントの対象ではなく、また、本改定における改定箇所ではありませんが、「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ことについては、基本対策事項6.1.5(1)-1c)に記載があり、また、御指摘いただいた解説については、鍵の管理手順を策定するに考慮する視点を記載しているため、原案のとおりとします。
38	独立行政法人 情報処理推進機構	ガイドライン	p.192	6.1.5(1)-1c)解説	基本対策事項6.1.5(1)-1 c)「「暗号モジュール試験及び認証制度」に基づく認証」について P.191で、既に「擬似乱数」という用語を用いているため、整合性をとるために、次のように修正すべきものと考えます。 現行:疑似乱数 新　:擬似乱数	ガイドラインについては、パブリックコメントの対象ではなく、また、本改定における改定箇所ではありませんが、御指摘を踏まえ、ガイドラインを修正させていただきます。

通し 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		
39	独立行政法人 情報処理推進機構	ガイドライン	p.192	6.1.5(1)-1d)解説	JIS X 19790が改正されたことを受けて、JIS X 19790の用語定義と整合するよう次のように修正すべきと考えます。 現行:タンパ検出 新　:タンパー検出 現行:タンパ証跡 新　:タンパー証跡 現行:暗号モジュールのセキュリティを危殆化する試みがなされたことを示す、外観上の表示 新　:暗号モジュールのセキュリティを危殆化する試みがなされたことを示す、観察可能な表示 現行:タンパ応答 新　:タンパー応答 現行:暗号モジュールがタンパを検出したときにとる自動的な動作 新　:暗号モジュールがタンパーを検出したときに取る自動的な動作	ガイドラインについては、パブリックコメントの対象ではなく、また、本改定における改定箇所ではありませんが、御指摘を踏まえ、「外観上の」を「観察可能な」に修正させていただきます。 また、御指摘の部分は、JIS X 19790 の文脈に係る部分ですが、「タンパ」の用語については、ほかの箇所でも使用しており、また、統一基準全体の用語については、 JIS X 19790 の記載のみに依拠している訳ではありません。ついては、「タンパ」の用語は、統一基準上の用語の平仄の観点などから、原案のとおりとします。
40	マカフィー株式会社	統一基準	p.40	6.1.4(c)	変更案: (c) 情報システムセキュリティ責任者は、情報システムにおいて、様々な機器から取得したログを相関的かつ継続的に分析する機能を設けること。また、不正侵入や不正操作等が判明した場合には、原因調査のための分析を実施すること。 理由: 「政府機関等の情報セキュリティ対策のための統一基準(平成30年度版)(案)」において、CSIRTは、被害の拡大防止等を図るための応急措置の実施及び復旧や情報セキュリティインシデントに関する関係機関との情報共有を行うことを求められています。 しかしながら、現実にこれらを可能とするためには、情報セキュリティインシデントの原因調査を迅速かつ正確に行える仕組みが必要となり、サイバー攻撃が高度化・巧妙化を鑑みると、ログ分析の重要性は年々増していると考えております。 また、「サイバーセキュリティ戦略(案)」において、情報システムのセキュリティ対策の高度化・可視化に向けた具体策として、様々な機器で発生する事象やアカウント管理情報を組み合わせた脅威分析検知と、その分析作業の自動化の有効性がうたわれているところです。 つきましては、統一基準におきましても、6.1.4(1)(c)に記載されていた「定期的に点検又は分析する機能」に加えて、インシデント発生時の原因調査を迅速に実施するために様々な機器から発生するログを相関的に分析する機能を備えるべきと考えますので、遵守事項に左記を追加することを提言いたします。 さらに、ガイドラインにおいては、機関の規模、情報システムから送出されるログ量、対象となる行政事務の機密性等に応じて、「自動化」を基本対策事項に加えていただくことについても、合わせてご検討ください。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、今後、3年間のサイバーセキュリティに関する施策の基本的方針である「サイバーセキュリティ戦略(案)」を引用していただいているように、御指摘の内容は今後の課題であると認識しています。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。
41	国立研究開発法人 国立国際医療研究センター	統一基準	p.41	6.1.5(1)(c)	電子証明書の使用について 規程自体が証明書をGPKIに限定しているわけではないのは承知しているが、技術的な制限を記載するべきと考える。 例えば自己証明書を使用しない、企業認証型SSL以上の強度とする、電子政府の暗号リストから漏れた技術を使用しない、などが考えられる。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、御指摘の電子証明書に関わる必要技術面の事項については、遵守事項6.1.5(1)(b)及びガイドラインに記載していますので、原案のとおりとします。

通し 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		
42	CyberArk Software 株式会社	統一基準	p.39	6.1.3(a)	情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を適切に設定し、それらが適切に利用されていることを常時監視し対応するための措置を講ずること。 理由： 組織全体で膨大な数に及ぶ管理者権限（の認証情報）を適切に管理するには、初期段階でアクセス権限を適切に設定するだけなく、その設定が当初のルールに則った形で適正に利用されていることを常時確認することが必要です。適正な利用を人手で常時確認することは膨大な工数がかかりますが、最新の管理者権限ソリューションなどのツールを利用することで、24時間365日適正な利用を監視することが可能です。また、不正が疑われる利用あった場合は予め設定した対処を自動で実施することができます。実際、米国の国土安全保障省が主導するCDM(https://www.dhs.gov/cdm)Phase2では、政府機関全体の管理者権限を一元管理できる統合基盤を導入し、管理者権限の適切な設定と、その後適正な利用を常時監視する仕組みを実現しています。シンガポール政府も、同様の目的で特権アカウント統合管理基盤の導入を急ピッチで進めています。日本におきましても、国の機密情報や国民の個人情報を取り扱う機関においては、同様の取り組みを実施すべきと考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、情報システムの状態のリアルタイムでの把握は重要と考えており、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。御指摘の点については原案のとおりとします。
43	CyberArk Software 株式会社	統一基準	p.40	6.1.4	(c)情報システム責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある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すること。国の機密情報や国民の個人情報を取り扱う機関においては、重大セキュリティ事故に直結する可能性が極めて高い管理者権限を持つアカウントのアクセスログ、操作ログについて、その影響の大きさから鑑み、リアルタイムに点検または分析を実施し、悪意ある第三者等からの不正侵入・不正操作への対策を講じること。 理由： 米調査会社のForrester社が実施した調査によると、サイバー攻撃の80%において管理者権限を有するアカウント情報が窃取・悪用されています。攻撃者は、高権限を持つ管理者アカウントを搾取した上で、情報の搾取、改ざん、システム停止などの目的を遂行することが常套手段となっており、管理者権限を有するアカウントのログインログや操作履歴などは、他のログに比べ不正侵入や不正操作の発見に対し大きく寄与するものと考えます。また、サイバー攻撃による被害の防止・最小化の観点より、いかに早くその兆候・事実を検知し、対策を行うことが非常に重要です。そのため、管理者権限に関わるログの点検・分析の頻度を、定期的ではなくリアルタイムで実施可能な仕組みを構築することが望ましいと考えます。	御指摘の内容は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、ログの点検及び分析の作業の自動化についてガイドライン 基本対策事項 6.1.4.(1)-5に記載されています。よって原案のとおりとします。
44	CyberArk Software 株式会社	ガイドライン	p.185	6.1.4(1)-5	加筆 b)ログ情報をソフトウェア等により集計し、下記を例とする不正侵入や不正操作、誤操作等の情報セキュリティインデント及びその予兆の検知と通知の自動化 ・リアルタイムに事前に定義された手順以外での管理者権限利用(ログイン)を検知し通知する ・リアルタイムに未知の特権アカウントからのアクセス(ログイン)を検知し通知する ・リアルタイムにブラックリストコマンドの実行を検知し、ブロックする ・リアルタイムに、通常と大きく異なる時間帯・IPからの管理者権限利用(ログイン)を検知し通知する 理由： 悪意のある第三者等による不正侵入や不正操作、誤操作等の被害を最小化するためには、怪しい挙動をリアルタイムに検知した上で、迅速に対応策を講ずることが重要です。 最新の技術動向を踏まえると、事前に想定された操作手順やアクセス形態、または通常の振舞いと異なる形で管理者権限が利用されていると思われる操作などを、リアルタイムに捕捉することは十分可能です。国の機密情報や国民の個人情報など重要性の高いデータを取り扱う機関では、管理者権限の不正利用をリアルタイムに検知できる仕組みの導入が必要と考えます。	ガイドラインについては、パブリックコメントの対象ではなく、また、本改定における改定箇所ではありませんが、御指摘の内容は基本対策事項へ記載する内容としては詳細すぎることから、原案のとおりとします。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。

通し 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		
45	株式会社テリロジー	統一基準	p.42	6.2.1	1)脆弱性対策については定期的な確認のみを定めているが深刻な脆弱性（CVSSスコア9以上など）が周知された場合、脆弱性を持つ資産の特定、および外部回線を通じての攻撃の可能性の解析を速やかに実施し、脆弱性対策を実施すべき。	1) 御指摘の内容は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、脆弱性を持つ資産に対する速やかな対応は重要と考えており、今回の改定にあたり、ガイドラインにてIT資産管理ソフトウェアの導入による効率的な情報収集や脆弱性対策の実施を記載してます。よって原案のとおりとします。
46	株式会社テリロジー	統一基準	p.42	6.2.1	2)ソフトウェアだけではなく、OS、ミドルウェアなどプラットフォームの脆弱性についても対策を講じるよう、記述を追加すべき。	2)脆弱性対策を行う対象となるソフトウェアについては、 1.6 一般用語の解説に記載しているとおり、ソフトウェアだけでなく、OSやOS上で動作するアプリケーションを含む広義の意味としています。
47	株式会社テリロジー	統一基準	p.42	6.2.1	3)守るべき資産を特定し、対応の優先順位づけを行い、やるべきことを明確にするといった一連の流れをネットワーク脆弱性監査製品やプラットフォーム脆弱性診断製品との連携・連動により、システマイズすべきではないか。	3) 御指摘の内容は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、各政府機関等がリスク評価により判断するものであると考えております。リスク評価については、遵守事項2.1.2(1)(a)、2.1.2(2)(a)に記載しております。 よって原案のとおりとします。
48	株式会社テリロジー	統一基準	p.42	6.2.1	4)通信回線装置の製造時や流通経路で不正なソフトウェアを混入した偽装デバイスが海外では発見されている（Router Firmware Tampering）。 このようなケースでは、一般的なセキュリティ対策製品では検知する方法がなく、DC、AC、EMI（電磁妨害）、音響などサイドチャネルのデータをセンサーで収集し、異常値検知を行うことにより不正機器の検知を可能にする。 このような不正なソフトウェアを混入した偽装デバイスへの言及が必要だと考える。	4)御指摘の内容は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、サプライチェーン・リスクへの対応については遵守事項5.1.2に記載しております。 御指摘の内容は具体的な対応方策についてですが、統一基準の遵守事項には、遵守すべき基本原則について記載することとしているため、原案のとおりとします。
49	株式会社テリロジー	統一基準	p.42 p.44	6.2.2 6.2.4	1)不正プログラムや攻撃が検知された場合には可及的速やかに当該端末を通常の通信経路から隔離する処置を講ずるべき。 2)万が一、セキュリティインシデントが発生してしまった場合の事後対策についての記述をすべき。 パケットキャプチャ装置などによるネットワーク・フォレンジック、PCなどの端末に関してはコンピュータ・フォレンジック（EDR等）をシステムを導入し、追跡査証の仕組みを備えるべき。	1)御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、標的型攻撃時の端末の隔離に係る対策は、ガイドラインの基本対策事項7.3.1(5)-1 g)「不正プログラム感染を認知した場合の対処手順」に記載しております。 また、2)セキュリティインシデントの対処としては、統一基準　2.2.4「情報セキュリティインシデントへの対処」として記載しています。頂いた御指摘については、今後の検討の参考とさせていただきます。

通し 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		
50	トレンドマイクロ株式会社	統一基準	p.43	6.2.2(1)(c)	意見内容：記述の追加を行うべきと考えます。 (c)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状況を適宜把握し、新たな対策の導入に際しては運用上の負荷に配慮しながら、必要な対処を行う事 理由： 政府機関等の対策基準策定のためのガイドライン（案）を見る限り、未知の不正プログラム対策の強化に強い方向性を含んでいるにも拘らず、遵守事項に何らの変更も加えられておらず、統一基準としての意図が十分に伝わらない可能性が有るものと思われます。 　未知・既知という分類自体が曖昧な定義で有る為、その記述を追記する事に意味は無いと思いますが、継続的に新しい攻撃手法が編み出される標的型攻撃との関連性が強い不正プログラムに対しても、新たな対策を継続的に検討し続ける必要性を意識してもらう必要が有るように思います。 　また、今回ログの監視の重要性を強く押し出している事は、セキュリティが製品を入れるだけではなく、既存対策も含め製品を適切に運用する事の重要性を示唆していると考えます。さらにガイドラインにおいても端末やサーバへの負荷により業務に影響を与える可能性について言及している為、製品の導入と運用上の負荷をバランスさせる事を意識してもらう必要も有るように思います。 高度化する標的型攻撃の入り口となる不正プログラムは巧妙化し、より積極的に検知しなければならない現状と、それに伴う過検知により業務に影響を与えるリスクを高いレベルでバランスする賢い対策が今後も必要とされていくと思われます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、不正プログラム対策ソフトと運用上の負荷のバランスについては、今回の改定においてガイドラインの解説「基本対策事項 6.2.2.(1)-1『既知及び未知の不正プログラムの検知及びその実行の防止を有する』について」に記載されています。また、未知の不正プログラム対策については、基本対策事項 6.2.2.(1)-1に規定されています。 御意見では、目的・主旨及び遵守事項への記載の必要性について御提案を頂いておりますが、基本対策事項は、統一基準に記載の遵守事項を満たすためにとられるべき対策という位置付けであり、統一基準群全体としては、御指摘の点は明記されていることから、原案のとおりとします。
51	株式会社FFRI	統一基準	p.43	6.2.2	－該当箇所 目的・趣旨に記載の「不正プログラムへの対策を適切に実施することが必要である」部分および、その遵守事項 －意見内容 参考資料の「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見直し（案）について」1ページ目によると、「情報システムの内部（端末等）での挙動の検知による未知の不正プログラムに係る被害の未然防止／拡大防止」とあるのが今回の改訂の概要となっており、実際に参考資料のガイドライン案もその趣旨に沿った修正案となっている。 しかし、統一基準ではこの趣旨が説明されていないため、目的・趣旨の最後の文を今回の趣旨に沿って具体的に記載する必要がある。このままの記載であるとH28版当時の古い対策と同様の対策でも問題ないという誤解を与える可能性があるため危険である。そこで、例えば「情報システムの内部（端末等）での挙動の検知による未知の不正プログラムに係る被害の未然防止および拡大防止を行うことが必要である」といった形で記載をより具体化することで、趣旨を変えることなく目的を明確化し、さらに他の文書との整合性を取ることもできると考える。 なお、遵守事項にも同様の趣旨の更新が必要であると考える。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、未知の不正プログラム対策については、今回の改定において基本対策事項 6.2.2.(1)-1に規定されています。 御意見では、目的・主旨及び遵守事項への記載の必要性について御提案を頂いておりますが、基本対策事項は、統一基準に記載の遵守事項を満たすためにとられるべき対策という位置付けであり、統一基準群全体としては、御指摘の点は明記されていることから、原案のとおりとします。

通し 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		
52	マカフィー株式会社	統一基準	p.42	6.2.1(1)(b)	変更案: 情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施し、脆弱性の悪用を遮断(遮断が困難な場合は検知)する措置を講ずること。 理由: 多重防御においては、「検知」と「遮断」という異なる技術が存在し、「遮断」においては攻撃を遮断することができるが業務システムに影響を与えやすいリスクがあり、「検知」においては業務システムへの影響は与えにくい傾向があるものの攻撃を可視化するのみで攻撃を遮断することができないという特徴があります。 効果的かつ各システムの運用に即した多重防御を実現するにあたっては、これらの特徴を踏まえ、各々の業務システムの特性と重要性を鑑み、バランスを考慮して各技術を採用することが必要であると考えます。 戦略的な多重防御を検討する際の前提となる「検知」「遮断」という考え方を明記することで、効果的かつ運用に即した多重防御の検討を促すことが重要であると考えます。 尚、「検知」においてはシステムでも実現することができるが、検知後の対処に遅れが出る可能性や、対処の遅れにより侵入範囲が拡大に繋がる可能性があるため、可能な限り「遮断」できる技術を採用することが望ましいと考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、基本対策事項 6.2.1(1)-5 c)に脆弱性が関係する機能の無効化等を記載しております。よって原案のとおりとします。
53	マカフィー株式会社	統一基準	p.42	6.2.2	目的趣旨・変更案: 情報システムが不正プログラムに感染した場合、情報システムが破壊される脅威や、当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには、不正プログラムに感染した情報システムは、他の情報システムに感染を拡大させる、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される、標的型攻撃における拠点として利用されるなどが考えられ、当該情報システム以外にも被害を及ぼすおそれがある。 このような事態を未然に防止するにあたり、既知の不正プログラム対策だけでは被害を未然に防止が出来ないことが考えられるため、既知の不正プログラムへの対策とともに、未知の不正プログラムへの対策も適切に実施することが必要である。 理由: 昨今の未知の手段を用いた攻撃活動の増加を踏まえ、「政府機関等の対策基準策定のためのガイドライン(案)(平成30年度版)」に明記のある未知の脅威対策の必要性について、政府機関等へ浸透させるため、「政府機関等の情報セキュリティ対策のための統一基準(案)(平成30年度版)」においても未知の脅威対策について、明確に記載するべきと考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、未知の不正プログラム対策については、今回の改定において基本対策事項 6.2.2.(1)-1に規定されています。 御意見では、目的・主旨への記載の必要性について御提案を頂いておりますが、基本対策事項は、統一基準に記載の遵守事項を満たすためにとられるべき対策という位置付けであり、統一基準群全体としては、御指摘の点は明記されていることから、原案のとおりとします。
54	マカフィー株式会社	統一基準	p.43	6.2.2(1)(a)	遵守事項・変更案: 情報システムセキュリティ責任者は、サーバ端末及び端末に不正プログラム対策ソフトウェア等を導入し、既知及び未知の不正プログラムの検知及びその実行を防止する対策を実施すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。 理由: 昨今の未知の手段を用いた攻撃活動の増加を踏まえ、「政府機関等の対策基準策定のためのガイドライン(案)(平成30年度版)」に明記のある未知の脅威対策の必要性について、政府機関等へ浸透させるため、「政府機関等の情報セキュリティ対策のための統一基準(案)(平成30年度版)」においても未知の脅威対策について、明確に記載するべきと考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、未知の不正プログラム対策については、今回の改定において基本対策事項 6.2.2.(1)-1に規定されています。 御意見では、遵守事項への記載の必要性について御提案を頂いておりますが、基本対策事項は、統一基準に記載の遵守事項を満たすためにとられるべき対策という位置付けであり、統一基準群全体としては、御指摘の点は明記されていることから、原案のとおりとします。

通し 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		
55	マカフィー株式会社	統一基準	p.44	6.2.4	変更案: 標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。 したがって、標的型攻撃による組織内部への侵入を低減する対策（入口対策）、並びに内部に侵入した攻撃を早期検知及び防御して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知及び防御して対処する対策（内部対策）からなる、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。 理由: 本項目の「目的と趣旨」において、「これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。」と記載のあることから、後に続く文中における「検知して対処」と記載のある箇所においても「検知及び防御して対処」と変更し一貫して記載することを提言します。 また、多重防御を検討する際の前提となる「検知」と「防御」という考え方を明記することで、「検知」による攻撃の可視化のみではなく、効果的かつ運用に即した多重防御の検討を促すことが重要であると考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、標的型攻撃を完全に防ぐことについては「検知及び防御することは困難」と記載しており、標的型攻撃によって内部に侵入された後については「検知して対処」と記載をし使い分けており、全てにおいて「検知及び防御して対処」と変更することは不適切であるため、原案のとおりとします。
56	マカフィー株式会社	統一基準	p.44	6.2.4(1)(b)	変更案: (b) 情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知及び防御して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知及び防御して対処する対策（内部対策）を講ずること。 理由: 本項目の「目的と趣旨」において、「これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。」と記載のあることから、後に続く文中における「検知して対処」と記載のある箇所においても「検知及び防御して対処」と変更し一貫して記載することを提言します。 また、多重防御を検討する際の前提となる「検知」と「防御」という考え方を明記することで、「検知」による攻撃の可視化のみではなく、効果的かつ運用に即した多重防御の検討を促すことが重要であると考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、標的型攻撃を完全に防ぐことについては「検知及び防御することは困難」と記載しており、標的型攻撃によって内部に侵入された後については「検知して対処」と記載をし使い分けており、全てにおいて「検知及び防御して対処」と変更することは不適切であるため、原案のとおりとします。
57	個人	統一基準	p.46	6.3.2(1)	クラウドサービスを使用した、機関等が運用・管理しない外部のサーバを使用することが拡大していると思われますが、その場合でも政府ドメイン名等を使用し、委託業者のドメインを使用することを禁止するのかどうかを明確にした方が良いと思います。	御指摘の点については、統一基準6.3.2(1)において、政府ドメイン名以外のドメイン名を使用している場合、府省庁からの情報を装ったなりすましの脅威が想定される等、セキュリティが確保されない恐れがあり、クラウドサービスの利用等をシステムの利用形態を問わず、政府ドメイン名を用いることとしています。

通し 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		
58	CyberArk Software 株式会社	統一基準	p.45	6.3.1	遵守事項(2)(a)への加筆 (キ) 提供するアプリケーション・コンテンツが他のシステムと連携を行う場合、他のシステムのIDとパスワードをアプリケーション・コンテンツに埋め込まないこと。 理由: 連携する他のシステムのIDとパスワードをアプリケーションに埋め込むケースが多くみられます。それらの連携用認証情報は、データベースの更新アクセス権などの管理者権限を持つ場合が多く、悪意ある第3者に搾取された場合、非常に大きな被害を出す可能性があります。一方、それらの認証情報は、アプリケーションを改修するまで変更されず、組織の脆弱性を残したまま放置されているケースが多いです。 上記の理由から、アプリケーション・コンテンツ内に第三者が直接識別可能な形でシステム連携用の認証情報を埋め込むことを禁止し、連携を必要とする場合は、外部システムから都度新たな認証情報を呼び出す仕組みを導入することが望ましいと考えます。	御指摘の箇所は、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、6.3.1(2)(a)(イ)に記載されている「提供されるアプリケーションが脆弱性を含まないこと」に含まれる内容となります。
59	CyberArk Software 株式会社	ガイドライン	p.213	6.3.1(2)(a)(エ)関連	加筆 6.3.1(2)-5 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツに連携する他システムの認証情報を第三者識別できる平文で埋め込まず、連携時に認証情報を外部から呼び出す仕組みを導入する。 理由: アプリケーション・コンテンツに第三者が識別可能な形で認証情報が埋め込まれている場合、その認証情報を窃取される危険性があります。また、アプリケーション・コンテンツの改修を行わない限りその認証情報は変更できません。そのため、組織のセキュリティ基準に反して長期間同一の認証情報が使用されているケースが多くあります また、アプリケーション・コンテンツ間の連携に使用されるIDはデータベースの更新アクセス権などの管理者権限を持つ場合が多く、窃取された場合に非常に大きな影響を与える可能性があります。従って、アプリケーション・コンテンツ内に認証情報を平文で埋め込むのではなく、利用時に外部から新たな認証情報を呼び出すなどの手法を取る事が望ましいと考えます。	ガイドラインについては、パブリックコメントの対象ではなく、また、本改定における改定箇所ではありませんが、6.3.1(2)(a)(イ)に記載されている「提供されるアプリケーションが脆弱性を含まないこと」に含まれる内容となります。
60	株式会社テリロジー	統一基準	p.47	7部	電力、ガス、水道、交通などの社会インフラの制御システムや工場における産業制御システム向けの機器を構成要素に追加すべきと考える。 また、OT（Operation Technology）向けのセキュリティ対策についての記述を追加すべきではないか。	御指摘の箇所は、本改定による改定箇所ではないため、パブリックコメントの対象ではありませんが、本基準は国の行政機関、独立行政法人及び指定法人を対象としており、社会インフラにおける制御システムや工場における産業システムを対象としたものではありませんので、原案のとおりとします。

通し 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		
61	株式会社テリロジー	統一基準	p.48	7.1.2	1)サーバ装置に対する不正な通信を防ぐため、回線経路上で当該サーバ装置への通信が適切に制御されているかどうかを定期的に監視する必要があるのではないか。 2)機密情報を含む重要情報資産を保持するサーバ装置に関しては、Host Identity Protocol (RFC5201)に対応した通信回線装置を導入するなどの対策を講じ、当該のサーバ装置へのアクセスを制限すべき。 HIP対応装置を導入することによりポート・スキャンなどの偵察行為を封じ込めることが可能になる。	1) 御指摘の箇所は、本改定による改定箇所ではないためパブリックコメントの対象ではありませんが、情報システムの監視全般については、遵守事項5.2.1(2)において、情報システムの構築時に監視等の運用管理機能要件を含むセキュリティ要件を策定することを記載しています。さらに、遵守事項6.1.4(1)(c)において、ログを用いた定期的な点検又は分析に関する規定を記載していますので、原案のとおりとします。 2) 御指摘の点は、本改定による改定箇所ではないためパブリックコメントの対象ではありませんが、サーバ装置等へのアクセス制御については、遵守事項6.1.2(1)アクセス制御機能の導入に記載しており、それに対応するガイドラインには実現方式としてネットワークセグメントの分割等を例示しています。この実装方法は各種考えられますが、統一基準の遵守事項においては個別には指定していませんので、原案のとおりとします。
62	国立研究開発法人 国立国際医療研究センター	統一基準	p.48 p.63	7.1.1 8.2.1	端末管理責任者と各課室情報セキュリティ責任者の責任分界点について 8.1.1にて、要管理対策区域外にてインターネット接続した端末を再接続する場合、許可を行えるのが統括情報セキュリティ責任者なのか、課室情報セキュリティ責任者なのか明確でないため、明確に記載いただきたい。また安全管理措置について、支給外の端末の安全管理措置、業務利用について、端末管理責任者と課室情報セキュリティ責任者の責任分界点がどのようになるか明確でないため、明確に記載いただきたい。	御指摘の要管理対策区域外にてインターネット接続した端末を再接続する場合の許可を行う責任者については、遵守事項8.1.1(3)(g)において、課室情報セキュリティ責任者と規定されています。 支給外端末の安全管理措置を講ずる責任者は、遵守事項7.1.1(4)(c)(イ)に、端末管理責任者と規定されいます。また、支給外端末の業務利用を許可する適任者は、遵守事項8.2.1(3)(a)に端末管理責任者と規定されています。 以上のように、御指摘の点については端末管理責任者と課室情報セキュリティ責任者の責任分界は明確となっています。

通し 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		
63	迷惑メール対策推進協議会	統一基準	p.52	7.2.3	下記の通り修正することが望ましいと考える。 (原文) さらに、電子メールのなりすまし対策の一部は DNS で行うため、これに不備があった場合には、なりすまされた電子メールの検知が不可能となる。 これらの問題を回避するためには、DNS サーバの適切な管理が必要である。 (修正案) さらに、電子メールのなりすまし対策の一部は DNS の設定が必要なため、これらが不十分である場合には、なりすまされた電子メールの検知が不可能となる。これらの問題を回避するためには、DNS サーバに対する適切な設定および管理が必要である。 ■理由 なりすまし対策として利用できる送信ドメイン認証技術は、SPF や DKIM、DMARC など、それぞれ DNS に対する SPF レコードや DKIM レコード、DMARC レコードなどの設定や管理が、メール配送のための設定とは別に必要となる。 そのため、単に「不備」や「適切な管理」といった表現ではなく、別途設定が必要、という意味を含めて表現が必要と考えた。	御指摘の箇所は、本改定による改定箇所ではないためパブリックコメントの対象ではありませんが、遵守事項7.2.1(1)(c)の電子メールのなりすまし対策並びに基本対策事項7.2.1(1)-2及び解説において、SPF, DKIM, DMARCについて詳しく記載していますので、原案のとおりとします。
64	迷惑メール対策推進協議会	ガイドライン	p.253	7.2.1(1)-3	下記のとおりDKIMに係る記述を追記することが望ましいと考える。 (原文) 7.2.1(1)-3 情報システムセキュリティ責任者は、以下を例とする電子メールの盗聴及び改ざんの防止策を講ずること。 a) SMTP によるサーバ間通信を TLS(SSL)により保護する。 b) S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用する。 (修正案) 7.2.1(1)-3 情報システムセキュリティ責任者は、以下を例とする電子メールの盗聴及び改ざんの防止策を講ずること。 a) SMTP によるサーバ間通信を TLS(SSL)により保護する。 b) S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用する。 c) DKIM による電子署名の技術を利用する。 ■理由 送信ドメイン認証技術 DKIM では、メールヘッダおよびメール本文から作成される電子署名をメールヘッダ上に追加することにより送信ドメイン認証を行う。この場合、署名対象となるメールヘッダやメール内容がメール配送中に改ざんされた場合、メール受信側で DKIM 認証が失敗するため改ざんを検知することができる。このため DKIM を、電子メールの改ざん防止技術としても利用すべきである。	ガイドラインについては、パブリックコメントの対象ではありませんが、本基本対策事項は「盗聴及び改ざんの防止」を目的とするものであり、一方で電子署名は改ざんの検知はできるものの、盗聴及び改ざんの防止対策とはならないことから不適と考えられますので、原案のとおりとします。

通し 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		
65	迷惑メール対策推進協議会	ガイドライン	p.253	7.2.1(1)-2 a)解説	下記のとおりDMARCに係る記述を変更することが望ましいと考える。 (原文) DMARC は、送信元ドメインに対し、効果的な認証基準が得られるよう、認証技術を自身のインフラに実装するに当たっての、より統合的な手法を定義するとともに、電子メールの受信者が SPF、DKIM 等に係る送信ドメイン認証の詳細な結果を電子メールの送信者にフィードバックするフレームワークを実現するための仕様である。 (修正案) DMARCは、電子メールの送信者が自身のドメインをなりすまされたメールを受信者に届けなくするための仕組みで、電子メールの受信者が SPF、DKIM等に係る送信ドメイン認証の検証結果を電子メールの送信者にフィードバックする機能を備え、送信者が受信時の制御要求を段階的に引き上げることができる。 ■理由 DMARCの特徴の一つである、送信ドメイン側がメール受信者に対して、なりすましメール検知時の受信処理方法を示すポリシーの設定やその目的、そのポリシーに段階があることや引き上げられる部分についての言及が必要と考えた。	ガイドラインについては、パブリックコメントの対象ではなく、また、本改定における改定箇所ではありませんが、御意見を踏まえ修正します。
66	迷惑メール対策推進協議会	ガイドライン	p.254	7.2.1(1)-2 a)解説	SPFに係る留意事項に続けて、DMARCに係る留意事項として下記内容を追記することが望ましいと考える。 (追加案) なお、DMARCについては、以下の事項に留意すること。 ・電子メールを利用していないドメインについても、DMARC のポリシーを″p=reject″ と設定することで、なりすましメールが受信者に届かない設定にする。 ・DMARC の設定を広く適用させるために、組織ドメインに対する DMARC レコードの設定を検討する。 ・DMARC レコードにはポリシーの設定が必須であるため、導入当初は″p=none″ と設定し、DMARC レポートを受け取り参照することで、メールの認証状況の把握につとめ、適切な SPF および DKIM の設定を行うことで，段階的に DMARC ポリシーの強化を実施する。 ■理由 既に DMARC のポリシーに基づいた処理を実施しているメール事業者もあるため、適切な DMARC レコード（ポリシー）の設定方法および強化方法について示す必要がある。 また、メールに利用しない実在するドメイン名を悪用したなりすましメールの被害を無くすために、 DMARC の強いポリシー ″p=reject″ を利用したなりすまし対策についても説明を追加すべき。	ガイドラインについては、パブリックコメントの対象ではなく、また、本改定における改定箇所ではありませんが、御意見を踏まえ修正します。
67	迷惑メール対策推進協議会	ガイドライン	p.255	7.2.1(1)-3 c)解説	【 基本対策事項 】<7.2.1(1)(d)関連> への 7.2.1(1)-3 (c) への追加に関連した解説の追加。 ■理由 DKIMによりメール本文およびメールヘッダからなる電子署名を付与することは、電子メールの改ざんを防止する観点から効果的である。また、DKIMの署名付与及び検証はメールサーバ間で行われるため、送受信する電子メールクライアントに依存しない検証が可能である。	7.2.1(1)-3への追加の御意見への回答と同様に、原案のとおりとします。
68	日本マイクロソフト株式会社	統一基準	p.51	7.2.1(1)(d)	電子メールのサーバー間通信について従来の方式と合わせて、暗号化の対策も必要という記述が適切と考える。例えば「暗号化された要求に対しては暗号化に対応した方式で対応する」など。 理由： 電子メールのサーバー間通信は一組織の取り組みだけでは完結せず、広く多団体での対応が必要となるため。	相手先サーバが対応していない状況を考慮して、自らが送信側の場合には相手先が暗号化に対応可能かを確認し、自らが受信側の場合には相手側からの暗号化の要求に応じるものとしており、本内容はガイドラインの解説「遵守事項7.2.1(1)(d) 『サーバ間通信の暗号化』について」に記載しています。

通し 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		
69	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.51	7.2.1 目的・趣旨	組織によっては電子メールサーバにクラウドサービスを利用する場合も想定されることから、「なお、本款の遵守事項のほか、7.1.2「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。」に続いて「電子メールサーバにクラウドサービスを利用する場合は、4.1.4「クラウドサービスの利用」において定める遵守事項についても併せて遵守する必要がある。」と追記してはどうか。	御指摘の箇所は、本改定による改定箇所ではないためパブリックコメントの対象ではありませんが、クラウドサービスを利用する場合は、「4.1.4 クラウドサービスの利用」が遵守事項となることは明らかと考えますので、原案のとおりとします。
70	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.51	7.2.2 目的・趣旨	組織によってはウェブサーバにクラウドサービスを利用する場合も想定されることから、「なお、本款の遵守事項のほか、7.1.2「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。」に続いて「ウェブサーバにクラウドサービスを利用する場合は、4.1.4「クラウドサービスの利用」において定める遵守事項についても併せて遵守する必要がある。」と追記してはどうか。	御指摘の箇所は、本改定による改定箇所ではないためパブリックコメントの対象ではありませんが、クラウドサービスを利用する場合は、「4.1.4 クラウドサービスの利用」が遵守事項となることは明らかと考えますので、原案のとおりとします。
71	特定非営利活動法人 日本ネットワークセキュリティ協会	統一基準	p.51	7.2.1(1)(d)	「電子メールのサーバ間通信の暗号化の対策を講ずること。」とされているが、現状におけるインターネット経由の電子メールの配信方式においては、サーバ間の通信の暗号化が可能かどうかは送信先電子メールアドレスを管理する電子メールサーバにおける暗号化機能への対応状況に依存するため、つねに暗号化が可能とは限らない。従って、遵守不可能な事態が生ずることを避けるために「可能な範囲で電子メールのサーバ間通信を暗号化により保護する対策を講じること」としてはどうか。	相手先サーバが対応していない状況を考慮して、自らが送信側の場合には相手先が暗号化に対応可能かを確認し、自らが受信側の場合には相手側からの暗号化の要求に応じるものとしており、本内容はガイドラインの解説「遵守事項7.2.1(1)(d) 『サーバ間通信の暗号化』」に記述しています。
72	株式会社テリロジー	統一基準	p.55	7.3.1	通信回線装置の設定は日々のメンテナンスにより変更されるため、運用開始からセキュリティ・リスクは増大し続ける。通信回線装置の設定の見直し、セキュリティ面の担保は手作業では難しく、ネットワークセキュリティ監査製品による定期的かつ自動的な確認手段を装備すべき。	御指摘の箇所は、本改定による改定箇所ではないためパブリックコメントの対象ではありませんが、御指摘いただいたセキュリティの運用に係わる自動化は重要と考えています。今回の改定においては、政府機関等が保有する膨大なIT機器の資産管理と脆弱性管理を優先して対応したところです。 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。
73	一般社団法人 日本ネットワークインフォメーションセンター	統一基準	p.55 p.56 p.57	7.3.1(1) 7.3.1(2) 7.3.1(3) 7.3.2	意見(1) Internet Routing Registryについて インターネットにおける経路制御では、経路制御上のセキュリティ対策の一つとして、Internet Routing Registry(IRR)への登録と常に正しい情報へ更新しつづけることが大切です。IRRは、いわゆるインターネット上の経路の乗っ取りや経路制御上の問題発生時に参照されるデータベースです。 イ. 7.3 通信回線 遵守事項 (1) 通信回線の導入時の対策 (g)について、「インターネット回線を接続する場合には、特に適切なIRRへの登録を行うこと。」を追記する。 ロ. 7.3 通信回線 遵守事項 (2) 通信回線の運用時の対策 (b)について、「インターネット回線を接続している場合には、特に適切なIRRへの登録情報を定期的に確認し見直すこと。」を追記する。 ハ. 7.3 通信回線 遵守事項 (3) 通信回線の運用終了時の対策 (a)について、「インターネット回線を接続していた場合には、特に適切なIRRへの登録情報を削除など適切に対応すること。」を追記する。 ニ. 7.3.2 IPv6 通信回線について、「IPv6においても適切なIRRへの登録と定期的な見直しを行うこと。」を追記する。	御指摘の箇所は、本改定による改定箇所ではないためパブリックコメントの対象ではありませんが、統一基準は全ての政府機関等に向けたベースラインであるという位置付けに鑑み、原案のとおりとします。

通し 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		
74	個人	統一基準	p.59	8.1.1	以下の記述の意味がよくわかりません。 文法的に正しいでしょうか。 『p.59 8.1.1 情報システムの利用 遵守事項 (1) 情報システムの利用に係る規定の整備 (d)(ア) 職員等は、国の行政機関、独立行政法人又は指定法人が支給する外部電磁的記録媒体、 又は本項に規定する利用手順において定められた外部電磁的記録媒体 を用いた情報の取扱いの遵守を 契約により機関等との間で取り決めた機関等外の組織 から受け取った外部電磁的記録媒体 を使用すること。』	御指摘を踏まえ、該当の規定を以下のとおり修正いたします。 『職員等は、国の行政機関、独立行政法人若しくは指定法人が支給する外部電磁的記録媒体、 又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により機関等との間で取り決めた機関等外の組織から受け取った外部電磁的記録媒体 を使用すること。』
75	独立行政法人 情報処理推進機構	ガイドライン	p.319	付録	「IT 製品の調達におけるセキュリティ要件リスト」が更新されましたので、最新化をお願いいたします。 現行:IT 製品の調達におけるセキュリティ要件リスト(平成26 年5月19 日 経済産業省) 新 :IT 製品の調達におけるセキュリティ要件リスト(平成30年2月28日 経済産業省)	ガイドラインについては、パブリックコメントの対象ではありませんが、御指摘を踏まえ、ガイドラインを修正させていただきます。
76	独立行政法人 情報処理推進機構	ガイドライン	p.319	付録	「IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック」が更新されましたので、最新化をお願いいたします。 現行:IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック(2014 年5月 独立行政法人情報処理推進機構) 新 :IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック(2018 年2月 独立行政法人情報処理推進機構)	ガイドラインについては、パブリックコメントの対象ではありませんが、御指摘を踏まえ、ガイドラインを修正させていただきます。
77	スプランクサービスジャパン合同会社	運用指針	p.2	第3部(2)	指針第3部(2)「主務大臣が情報セキュリティ対策の実施状況に関して評価を行い、評価結果を公表する」に対応する具体的要領が統一基準に明記されていないので記載することを推奨します。 意見理由 独立行政法人及び指定法人のセキュリティを政府全体として一定の水準で確保するため、評価の方法については内容、期限、公開方法等、統一基準にて見解を示すことが必要と考えられるためです。	御指摘については、本改定における改定箇所ではないためパブリックコメントの対象ではありません。また、御指摘については、独立行政法人通則法に基づき実施されるものであるため、その要領を統一基準に明記することは、考えておりません。
78	スプランクサービスジャパン合同会社	運用指針	p.2	第3部(2)	指針第3部(2)には独立行政法人及び指定法人の評価及び公表について義務化されていますが、同様に府省庁についても評価及び評価結果の公表を推奨します。 意見理由 評価と評価結果の公表の必要性については独立行政法人と同様に考えられるためです。	御指摘については、本改定における改定箇所ではないためパブリックコメントの対象ではありませんが、各府省庁におけるサイバーセキュリティ対策に関する取組の総合評価結果等を内閣官房がサイバーセキュリティ政策に係る年次報告として取りまとめ、公表しております。また、監査の結果につきましても、同年次報告にて公表しております。

通し 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		
79	個人	全般	－	－	・社会構造が古い為に新しく改革し向上による概略案 ・教育内容の改正による具体案 ・女性社会進出での改正による具体案 ・外国人高度人材での導入で社会水準の向上による具体案 ・「ガバナンス（政治統治）」構造の改正による具体案 ・生活水準での基準による詳細案 ・官公庁が考案した無駄な政策の廃止による詳細案	御意見ありがとうございます。 統一基準群の改定に関するものではないため、お答えは困難です。
80	国立研究開発法人 国立国際医療研究センター	全般	－	－	地方自治体にも同じ基準を求められないのか（文書全体について） 国の行政機関、独立行政法人、指定法人が対象となっているが、業態によっては、地方自治体の指導を受ける立場にある独立行政法人もある（例えば病院など）。 地方自治体から独立行政法人に対して求められている情報共有の仕組みの中には、統一基準の内容から逸脱するもの（セキュリティが低い方式が要求されているもの）が一部にあるため、地方自治体の意識を高めるためにも、地方自治体においても、統一基準群を準用するなどの努力義務を付記いただきたい。	御指摘については、本改定における改定箇所に関する事項ではないため、パブリックコメントの対象ではありませんが、統一基準群の適用対象については、サイバーセキュリティ基本法を根拠としております。 現状、地方自治体は、サイバーセキュリティ基本法において本統一基準群の適用対象となっていないため、努力義務を付記することは適切ではないと考えられます。
81	個人	全般	－	－	まずお願いしたいのであるが、意見募集の期限は、17時までとせずに24時までとしていただけるだろうか。 どうせ当日中に応募された意見を見終わるものでもないのであるし、意見募集の通例として（また行政や司法への提出物一般の通例として）、意見募集の期限は24時までとするのが妥当なはずであろう。（要するに、search.e-gov.go.jpを見て仕事から帰って当日終了分の意見提出を行おうとする様な者に対する嫌がらせであろう？NISC（や他一部の内閣官房・内閣府の部署）による意見公募は。改められたい。意地悪を公務員がしていいわけがない（あるいは国民からの「逃げ隠れ」かもしれないが。）。） であるので、次からは意見募集の期限は17時までではなく、24時までとされたい。それが妥当適切なはずである。（そして、受付を行うのは政府のサーバという機械なのであるから、その様な時刻まで誰にも特段の問題無く受付が行えるはずである。（なお、行政機関や司法機関への書類提出は、郵便や直接手渡しの場合、当日24時まで当日分として受付が行えるものである事を注意しておく。）） （それとであるが、各所での全角文字の故意的な使用は止めてはどうか？NISCの姿勢が現れているようで微笑ましいのであるが、「所詮文系」的な精神が溢れるようであるのは、当然好ましくないものである。それは躁的な性質をも伴うものであると断じて良いものであるが、当然、公共機関としてその様な病的な性質を露にして国民・社会・世界に接しようとするのは誤りであるので、今後態度を改められたい。）	御指摘いただいた内容は、統一基準群の改定に直接関わるものではありませんが、参考として承ります。