「政府機関等のサイバー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e-Govに掲載して公募

■ 実施期間：2021年４月26日（月）～５月13日（木）

■ 意見総数：18者から59件【内訳：6企業・団体から延べ41件、12個人から延べ18件】

・統一規範に1件、統一基準に51件、運用指針に0件、全般に対して３件の意見提出

（１）修正意見：全55件

・表現の適正化を求めるものについて、統一基準を修正（９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（46件）

☆主な意見

・ISMAP制度の活用と外部サービスの将来像を見据えた対策に関する意見（８件）

・ゼロトラストアーキテクチャや暗号アルゴリズム、電子署名等といった最新のセキュリティ対策に関する意見（16件）

・Web会議利用時の対策やテレワークで利用されるクラウドサービスへのセキュリティ対策に関する意見（３件）

（２）その他の意見：全４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４件の意見提出

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（１件）

（参考）提出者名：

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、KPMGコンサルティング株式会社、TIS株式会社、パロアルトネットワークス株式会社、日本プルーフポイント株式会社、個人（12）

「政府機関等のサイバー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	日本マイクロソフト株式会社	統一基準	P.3	1.2	[該当箇所（原文コピー）] 機密性３情報 国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取扱いを要する情報 [意見内容] 個人情報が含まれるという条件だけで機密性3情報に区分するのではなく、機密性2情報に相当する場合もあるとの注記があると、クラウドサービスの活用促進につながるのではと考えます。情報の共有が広く行われることが想定される中、情報主体の判断を容易にするためにも、情報の3分類の中の具体的な文書名などの例示があると良いかと考えます。 [理由]： 機密性3に区分されるとインターネット接続に制限が生じるところ、その範囲をより明確となるように改定いただいた点について、クラウドサービスを含めた外部サービスの活用促進につながるものと考えます。 ただ、政府機関において個人情報等が含まれる場合にはすべて機密性3に該当するとの誤解があるとお聞きすることもあり、その点について説明があると理解の助けになるのではと考えます。	文書管理ガイドラインにおいて「秘密文書」の定義が明確に規定されていることから、原案のとおりとします。
2	日本マイクロソフト株式会社	統一基準	P.6	1.3	[該当箇所（原文コピー）] 「外部サービス」とは、機関等外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能を利用して機関等の情報を取り扱う場合に限る。 [意見内容] 但書にいう「情報を「取り扱う」場合」とありますが、この意味を明確にすることで、より外部サービス事業者の責任区分がわかるようになるのではないかと考えます。具体的な取り扱いに関する作業を明確にし、それに応じた共同責任を全うできるようにするためにも、情報を直接的に取り扱うサービスと間接的に取り扱う（内容に関与しない）サービスを明確にできるとさらに良いと考えます。 直接な取り扱いとは、機関等外のものがデータの閲覧、編集などを行うことを指し、間接的な取り扱いとは、機関等外のものが内容を閲覧しない状態での統計処理、保管やバックアップなどを行うことを指します。 [理由]： 個人情報保護委員会による、ガイドライン（「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ）によれば、クラウドサービスの利用に関して、「契約条項によって外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等」については、当該クラウドサービスの利用についてクラウドサービス提供事業者は個人データを「取り扱わない」とされるもの説明されています。（Q5-33）本統一基準についても、上記のような要件をクラウドサービスが満たす場合、「機関等の情報を取り扱う場合」には該当しない、と考えてよろしいでしょうか。	御指摘の箇所につきましては、当該機能で情報が取り扱われる場合全てを想定しております。また、外部サービスの用語定義については明確にするため、修正いたします。
3	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.6	1.3	クラウドサービスが「外部サービス」に該当することが明確にされたが、当該サービスの定義における「当該機能を利用して機関等の情報を取り扱う場合に限る」に関し、どのような場合が外部サービスの「情報を取り扱う」に該当するのかを明確にすることを希望する。	御指摘の箇所につきましては、外部サービスにおいて機関等の情報が取り扱われる場合を想定しております。また、外部サービスの用語定義については明確にするため、修正いたします。

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		
4	TIS株式会社	統一基準	P.6	1.3	意見内容：外部サービスで取り扱う「機関等の情報」の定義を以下のように明確化してはどうか。 「機関等が職務上作成し、又は取得した情報及び機関等が組織的に用いる情報」 意見理由： 　職員の個人情報は、「機関等の情報」ではあるが、職員個人が出張の予約に際し特急券や宿泊施設の予約に外部サービスを利用したとして、外部サービスとしての管理が必要かとの観点から具体化したほうがよいのではと考えたため。	御指摘の箇所につきましては、外部サービスにおいて機関等の情報が取り扱われる場合を想定しております。また、外部サービスの用語定義については明確にするため、修正いたします。
5	日本マイクロソフト株式会社	統一基準	P.6	1.3	[該当箇所（原文コピー）] 「外部サービス管理者」とは、外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう [意見内容] 「外部サービス管理者」とは、外部サービスを利用する機関等において、外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう [理由]： 外部サービス管理者が、外部サービス提供者側に存在するのか、利用する機関等に存在するのかが分かりにくいため、明確にしたほうが良いと考えます	御指摘の内容につきましては、ガイドラインの解説「遵守事項4.2.1(1)(a)(エ)「外部サービス管理者」について」において、利用する機関等の職員を対象にすることを記載しております。
6	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.6	1.3	「外部サービス管理者」の定義においても、政府機関等の職員を指すのか、事業者を指すのかを明確化することを求める。	御指摘の内容につきましては、ガイドラインの解説「遵守事項4.2.1(1)(a)(エ)「外部サービス管理者」について」において、利用する機関等の職員を対象にすることを記載しております。
7	個人	統一基準	P.6	1.3	「外部委託」が削られているが、依然として記載を行っておくべきと考える。（「業務委託」と若干の意味の違いがあるのではないかと思われるが、「外部委託」は「外部委託」で記しておく方が良いと思われる。）	御指摘の「外部委託」につきましては、本改定において一般用語として外部の者に委託することを指すこととしたので、原案のとおりといたします。
8	個人	統一基準	P.6	1.3	「業務委託」の末文の「ただし、機関等の情報を取り扱う場合に限る。」というのが少々分かりにくい。 その場合に限り「業務委託」という用語を使うのであれば、「（機関等の情報を取り扱う場合に限りこの用語を用いる。）」という形に変更した方が良いのではないかと思われた。	御指摘の箇所につきましては、委託する業務において情報を取り扱わせる場合を想定しておりましたので、御指摘を踏まえて、業務委託の用語定義等を修正いたします。

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	KPMGコンサルティング株式会社	統一基準	P.7	1.3	「クラウドサービス」の定義から、「であって、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」を削除してはいかがでしょうか。 理由としては、「約款による外部サービス」が削除されたこと、及びISMAPとの整合性確保が挙げられます。 元々、統一基準においては「約款による外部サービス」が規定されていて、その後に「クラウドサービス」が追加された経緯から、両概念の整合を図るために「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」との条件があったと理解しています。今回「約款による外部サービス」を削除するので、上記条件を設定する必要はないと考えます。 また、ISMAPは利用者からの「条件設定の余地」の有無にかかわらず、幅広く一般的な概念としてのクラウドサービスを対象としていると認識しております。しかし、「十分な条件設定の余地がない」サービスの場合には上記定義に照らすとクラウドサービスに該当しないため、改定案「4.2.1(3) 外部サービスの選定（クラウドサービス以外の場合）」が適用されることになります。 上記のように、「クラウドサービス」の定義を変更しないことにより不整合が発生するため、修正が必要と考えます。	改定箇所への御指摘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用語定義については、ISMAP基本規程にて定義されているクラウドサービスと同様となっており、不整合が発生するものではありません。
10	個人	統一基準	P.23	3.1.1(6)(b)	電磁的記録を電子メールで送信する場合には、S/MIME等を利用した電子署名と暗号化を必須とすること。特に、電子署名は、メールの送信者を明確にし、結果外部からの標的型攻撃対策にもつながるため、要保護情報以外の電磁的記録を送信する場合にも必須とすべきである。	改定箇所への御指摘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、御指摘の内容については今後の普及状況等を踏まえて検討してまいります。
11	個人	統一基準	P.23	3.1.1(6)(b)	独立行政法人及び指定法人（以下「独立行政法人等」）の職員等がインターネット回線を使用して機密性３情報を送信することはできないと考えられます。一方、国の行政機関においては、「行政文書の管理に関するガイドライン」における「秘密文書の管理に関するモデル要領」の第８の２（２）により、秘密文書（機密性３情報に該当）のうち、極秘文書についてはインターネット回線を使用した送信はできないと考えられますが、秘文書については暗号化等の措置を講じれば可能と考えられ、国の行政機関における取扱いと独立行政法人等における取扱いは同等ではないと考えられます。 今回の改定案で、情報の保存に関しては、２２ページ（４）（ｄ）において但し書きが追加されたことにより、独立行政法人等においても国の行政機関と同等の措置とすることが認められるようになりました。しかしながら、この但し書きは、２３ページ（６）（ｂ）には適用されないと考えられます。これは、外部への送信については、国の行政機関と同等の取扱いを認めないということでしょうか。 もし同等の取扱いを認めるということであれば、２３ページ（６）（ｂ）においても、２２ページ（４）（ｄ）に追加されたものと同様の但し書きが必要なのではないでしょうか。	御意見ありがとうございます。 御指摘のとおり修正いたします。
12	個人	統一基準	P.25	4.1.1	外部委託に関する事項であるが、近年、(委託に限らず)業務上利用する外部サービスや外部開発のソフトウェア(Windows等のOSや、ウイルス対策ソフト等も含まれる)に対する「サプライチェーン攻撃」という攻撃が多くなってきている。そのため、当該サービスやソフトウェアの開発者の情報セキュリティ対策も評価すべきである。	サプライチェーンリスクについては重要と考えており、クラウドサービスの選定時においては、ISMAP管理基準において機関等の意図せざる変更が加えられないための管理体制を確認し、クラウドサービス以外においては、遵守事項4.2.1(3)(b)(ウ)において確認を求めております。また、外部開発のソフトウェア等を調達する場合においては、遵守事項5.1.2(1)(a)にて機器等の選定基準を整備することを求めております。

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		
13	KPMGコンサルティング株式会社	統一基準	P.25	4.1.1	改定案では、これまでの「外部委託」よりも広範な「業務委託」が定義されていると認識しております。 （従来）　外部委託：機関等の情報処理業務の一部又は全部について、契約をもって外部の者に実施させることをいう。 （改定案）業務委託：機関等の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。（中略）ただし、機関等の情報を取り扱う場合に限る。 業務委託の「目的・趣旨」について、今回改定案での定義変更により「情報処理業務」以外についても適用範囲が拡大したことを明記してはいかがでしょうか。 現状の記載では、「情報システムやアプリケーションプログラムの開発・運用・保守等を委託する際に」となっており、このような場合に限定されると誤解される可能性があると思われます。 特に「機関等の情報を取り扱う場合」となっているものの、現実的には電子メールの授受や端末により作成した文書を提供するなど、ほぼすべての委託が該当するものと思われ、そのことを明記するべきと考えます。	御指摘の箇所につきましては、委託する業務において情報を取り扱わせる場合を想定しておりましたので、御指摘を踏まえて、業務委託の用語定義等を修正いたします。
14	個人	統一基準	P.25	4.1.1(2)	いくら契約でしっかり禁止事項等で合意しても、悪意をもってやられたらどうしようもないんで、外資を排除するのは当然としても、内資でも実質的に外国資本に支配されている場合もあるので、きちんとチェックが必要です。 そもそも秘密事項を外部に委託すること自体、安全保障上リスクが高すぎます。外部に委託することなく、すべて政府内でやるべきではないでしょうか？	改定箇所への御指摘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、遵守事項4.1.1(2)(b)において委託先への情報セキュリティ対策を講ずることを求め、遵守事項4.1.1(2)(c)においては委託先に対して情報セキュリティ監査等を求めることにより、情報セキュリティが十分に確保できるように定めております。御意見も踏まえ、業務委託に係るセキュリティ確保について、より強固となる方策を検討してまいります。
15	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.28	4.2	政府目標の「クラウド・バイ・デフォルト原則」を達成する上でも、革新的なクラウドコンピューティング・ソリューションの採用がセキュリティ要件によって阻まれないように、本原則を統一基準に反映させることを奨励する。	本改定においては、「クラウド・バイ・デフォルト原則」を踏まえて改定をしており、クラウドサービスを選定する際はISMAP制度を活用すること等を記載しております。なお、クラウドサービスにおけるセキュリティ対策については、引き続き検討してまいります。

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		
16	日本マイクロソフト株式会社	統一基準	P.28	4.2	「4.2 外部サービスの利用」という項目が新設されたことによって、業務委託との違いが明確になり、クラウドバイデフォルトにおけるセキュリティ対策がわかりやすくなったと感じます。また、外部サービスの選定において、クラウドに対する要件がクラウドサービス以外の時と比較して簡素になっている点についても、クラウドサービスが単に機能だけを提供しているものではないということに対するご理解の表れだと感じています。 一方で、セキュリティ対策が攻撃ベースになっており、後付けのセキュリティ対策が中心的に考えられているように見受けられます。政府の調達の状況などを勘案するとIT基盤にセキュリティ機能を含むような形で、長期での運用に耐える形での要件提案ができると良いのではないかと考えます。そのために、追加のセキュリティ投資が必要のないサービス利用の一つとして、外部サービスベンダーから提供されるセキュリティベストプラクティスに沿ったアーキテクチャ設計を促すなど、クラウドサービスの活用などの提案ができるのではないかと考えます。	本改定においてクラウドバイデフォルトの原則を踏まえ、クラウドサービスの利用拡大を見据えて外部サービス利用者が行うべきセキュリティ対策について追加しております。なお、クラウドサービスにおけるセキュリティ対策については、引き続き検討してまいります。
17	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.28	4.2	セキュリティの責任共有モデルが反映されたことを歓迎する。このセキュリティモデルが政府機関全体で理解されることをNISCにて確実にすることを奨める。	今後NISCにおいて改定内容の周知や監査等の実施により機関等へフォローをしてまいります。
18	日本マイクロソフト株式会社	統一基準	P.28	4.2.1	[該当箇所（原文コピー）] また、外部サービスでは、複数利用者が共通の外部サービス基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。 [意見内容] また、外部サービスでは、複数利用者が共通の外部サービス基盤を利用するサービスも存在することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。 [理由]： クラウドサービスの特徴としてマルチテナントが挙げられることがありますが、古い構成でのASPのようなものでない限り、同一アプリケーション（ライセンス）でのマルチテナント利用は少なくなっていると考えます。テナントごとに適切なログをオンデマンドセルフサービスで取得することができるかなどを明確にしていただくことで、利用可能なサービスの判断に役立つと考えます。	御意見ありがとうございます。 御指摘を踏まえて、当該目的・趣旨を修正いたします。
19	KPMGコンサルティング株式会社	統一基準	P.28	4.2.1	「目的・趣旨」において、外部サービスの例として「ＳＮＳ（ソーシャルネットワーキングサービス）」が記載されていますが、「ソーシャルメディアサービス」に修正してはいかがでしょうか。 統一基準の他の箇所では、ソーシャルメディアサービスの用語となっています。（例：ガイドライン P13 「図1.5-1 「情報システム」、「機器等」及びその関係」では、図中で外部サービスの枠内には「ソーシャルメディアサービス」が記載。）	御指摘の箇所につきましては、ソーシャルメディアサービスのうち、ＳＮＳ（ソーシャルネットワーキングサービス）を想定し例示としてあげていますので、原案のとおりといたします。

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		
20	個人	統一基準	P.28 P.29	4.2.1(1) 4.2.1(2)	本改定案では、政府情報システムのためのセキュリティ評価制度（ISMAP）の管理基準も踏まえ、クラウドサービス利用者側として実施すべき対策や考え方に係る記載が追加されています。 これに関して、クラウドサービス利用者側に対しては、係る新たな管理基準を自身のみで踏まえた上でクラウドサービス提供者及びクラウドサービスに対する評価及び対策等を一から講じさせるような、新たに重い負荷のみを強いているかのように思われました。これでは、クラウドサービス利用者側へISMAP制度のメリットが生かされないように思われました。 クラウドサービス利用者側が、ISMAPの成果物（公開されているISMAPクラウドサービスリスト等）を利用することにより、クラウドサービス提供者及びクラウドサービスに対する公開情報を参照し、クラウドサービス選定及び選定したクラウドサービスへの対策等の検討に係る負荷を軽減できるよう、ISMAPの成果物（公開されているISMAPクラウドサービスリスト等）の利用方法に踏み込んだ記載についても、統一基準群に追加すべきだと思われます。 また、ISMAPは、米国FedRAMP等と異なり、クラウドサービス提供者及びクラウドサービスへお墨付きを与える評価制度では無いことも踏まえ、ISMAPの成果物（公開されているISMAPクラウドサービスリスト等）の利用における留意点を含めて、統一基準群へ追加し、クラウドサービス利用者側へ係る注意喚起及び係る負荷の軽減を図るべきだと思われます。	ISMAPの成果物の利用方法や留意点については、今後も政府機関等への周知を図ってまいります。
21	KPMGコンサルティング株式会社	統一基準	P.29	4.2.1(2)	4.2.1(3)(e) 準拠法・裁判管轄の選定条件についは、4.2.1(2)においても規定するべきではないでしょうか。 理由としては、ISMAPでは準拠法・裁判管轄は情報提供にとどまり、リスク評価は発注者側が実施する必要があるためです。	御指摘の内容につきましては、遵守事項4.2.1(2)(b)における外部サービス提供者の選定基準に含まれている想定です。
22	パロアルトネットワークス株式会社	統一基準	P.30	4.2.1(3)(d)（ア）	意見：クラウドサービス以外の場合にのみ情報セキュリティ監査の受入れが条件に含まれるようにもお見受け致しますが、クラウドサービス上で開発されるシステムにおいても同様に情報セキュリティ監査の受入れは必要と考えます。 理由：クラウドサービス上で開発されるシステムにおいても同様に情報セキュリティ監査の受入れは必要と考える為。	御指摘の箇所につきましては、外部サービス（クラウドサービス以外）を選定する際に、外部サービス提供者への情報セキュリティ監査の受入れを求めており、クラウドサービスにおいてはISMAP管理基準において外部サービス提供者への監査を求めております。なお、外部サービスを利用して構築された情報システムにおける情報セキュリティ監査については2.3.2款にて定めております。
23	日本マイクロソフト株式会社	統一基準	P.31	4.2.1(6)(a)（ア）	[該当箇所（原文コピー）] （ア）不正なアクセスを防止するためのアクセス制御 [意見内容] （ア）情報やサービスに対する不正なアクセスを防止するためのアクセス制御 [理由]： クラウドサービスにおいては、データベースやストレージサービスのようにデータを預かる機能だけではなく、それを操作したり、状況を判断するためのダッシュボードなどの機能があります。これらのサービスに対する不正アクセスによって、管理者機能などを不正取得する可能性もあります。明示的に「情報やサービス」としていただくことでより分かりやすくなるかと思います。	御指摘の箇所につきましては、ガイドラインの基本対策事項4.2.1(6)-1において具体的なアクセス制御を示しているため、原案のとおりといたします。

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		
24	日本マイクロソフト株式会社	統一基準	P.31	4.2.1(6)(a)（イ）	[該当箇所（原文コピー）] （イ）取り扱う情報の機密性保護のための暗号化 [意見内容] （イ）取り扱う情報の機密性及び完全性確保のための暗号化 [理由]： 暗号化はアクセス制御の一つの手段ですので、（ア）のみで十分だと考えます。突起する必要があるのならば、ランサムウェアなどによる攻撃を踏まえた完全性確保についても記載するのが良いと考えます。これによって、秘匿のための単純な暗号化ではなく、情報単位での管理を明示できるのではないかと考えます	御指摘の箇所につきましては、国内法以外の法令及び規制が適用されるリスク等も踏まえて、暗号化を求める趣旨であるため、原案のとおりといたします。
25	パロアルトネットワークス株式会社	統一基準	P.31	4.2.1(6)(a)（ウ）	該当文書：(ウ) 開発時におけるセキュリティ対策 意見：下記への文書の変更を意見として提出致します。 (ウ) 開発各フェーズにおけるセキュリティ対策 理由：開発にはいくつかのフェーズがあり、その各フェーズそれぞれでセキュリティ対策を施すことで、手戻りによる開発期間延長防止や、後の脆弱性予防として必要であると考える為。	今般の改定では開発全体を対象とした規定としておりますが、開発における各フェーズに求めるべきセキュリティ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。
26	パロアルトネットワークス株式会社	統一基準	P.31	4.2.1(7)(a)	意見：(ケ)の追加を意見として提出致します。 (ケ) コンプライアンス準拠への継続的な監査 理由：外部サービスを利用する際には、人為的なミスに起因するインシデントをできる限り抑制するため、組織内で定められたコンプライアンスに対する継続的な監査が必要不可欠であると考える為。	御指摘の箇所につきましては、外部サービス特有の運用に関する規定を定めており、組織における情報セキュリティ監査については2.3.2款にて定めております。
27	日本マイクロソフト株式会社	統一基準	P.31	4.2.1(7)(a)（キ）	[該当箇所（原文コピー）] （キ）設計・設定時の誤りの防止 [意見内容] （キ）設計・設定時に想定した構成の監視と修正 [理由]： クラウドサービスにおいては、構成をリアルタイムで精査できる機能が付与されているものが増えてきました。これはSaaSにおいてもPaaS/IaaSにおいても導入されています。これらの機能がないものは後付けでCloud Security Posture Management（CSPM）ツールを導入することで状態の把握と修正を行うことができます。いわゆるmis-configuration（構成ミス）への対策として具体的に記載することが良いと考えます	御指摘の箇所につきましては、ガイドラインの解説「基本対策事項4.2.1(7)-7 a)「設定の誤りを防止するための対策」について」において外部サービス提供者が提供するセキュリティ設定・監視ツールの利用についても言及しているため、原案のとおりといたします。
28	日本マイクロソフト株式会社	統一基準	P.32	4.2.2(2)(a)	[該当箇所（原文コピー）] (a) 職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で要機密情報を取り扱わない場合の外部サービスの利用を申請すること。 [意見内容] (a) 職員等は、利用するサービスの約款、その他の提供条件等、サービスに関連する情報を添えて、要機密情報を取り扱わない場合の外部サービスの利用を申請すること。 [理由]： リスクは申請者が判断するのではなく、責任者が判断するのではないかと考える。本項だけではなく、職員が判断するとしているところはできる限り責任者が判断することにし、判断の均一化を図ることがガバナンスにおいて重要なことではないかと考えます。	御指摘の内容につきまして、最終的な判断は利用申請の許可権限者が行うにしても、外部サービス利用者自身においてもリスクの評価は必要であると考えていることから、原案のとおりといたします。

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	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.35	5.2.1(2)(a)	統一基準の5.2.1 (2) (a) 及び「政府機関等の対策基準策定のためのガイドライン （令和３年度版）」（173ページ）において「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 （外部サービスを含む。）から分離する」という記述を削除することを求める。インターネット分離は、システムに保有されている情報へのアクセスや利用が大幅に減少するだけでなく、大手クラウドコンピューティング・サービス・プロバイダーによる最先端のセキュリティ・ソリューションの恩恵を政府機関が受けることも制限する。暗号化や厳格なアクセス管理システム等、最高水準の安全なソリューション利用を政策において確実にすることが不可欠であると考える。	御指摘の箇所につきましては、通信経路を物理的又は論理的に分離することの要否を判断することを求めており、一切のインターネットアクセスを禁止する意図ではありません。
30	パロアルトネットワークス株式会社	統一基準	P.36	5.2.1(2)(a)(ア)	該当文書： (ア) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗 号化機能等のセキュリティ機能要件 意見：下記への文書の変更を意見として提出致します。 (ア) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、通信の可視化、暗号化機能等のセキュリティ機能要件 理由：通信の可視化がサイバー攻撃の挙動発見、次の対策への現状把握に重要な要素となるため。	改定箇所への御指摘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	BSA｜ザ・ソフトウェア・アライアンス	統一基準	P.8 P.42	1.3 6.1	「常時アクセス判断・許可アーキテクチャ」や「常時システム診断・対処」などのキーワードを「1.3　用語定義」や、第6章6.1.「情報システムのセキュリティ機能」に追加し、「統一基準」に明確に反映させることを奨める。	「常時アクセス判断・許可アーキテクチャ」については、ガイドラインの基本対策事項6.1.2(1)-1 f)に記載を追加しておりますが、今後の普及状況等を踏まえ、用語定義への追加や遵守事項として規定することを検討してまいります。
32	日本マイクロソフト株式会社	統一基準	P.42	6.1.2	主体を制限することという記載はあるものの、管理者アカウントなどを含む共有IDなどを制限に関する記載は見られないため、アカウントの共有（root/ Administratorに代表されるもの）の利用を原則として禁じる項目も記載していただきたいと考えています。	改定箇所への御指摘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6.1.1(2)(a)において識別コードを適切に付与すること、更に、当該遵守事項の基本対策事項において情報システムを利用する主体ごとに識別コードを個別に付与することを求めており、また、管理者権限の特権を持つ主体の識別コードの管理については遵守事項6.1.3(1)(b)に規定しているところです。御指摘も踏まえ、アカウント管理に係るセキュリティ対策については、引き続き検討してまいります。

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		
33	個人	統一基準	P.43	6.1.5(1)(a)（イ）	電子署名は、その情報の作成者を明確にし、結果外部からの標的型攻撃対策にもつながるため、要保全情報以外の電磁的記録にも必須とすべきである。	改定箇所への御指摘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、御指摘の内容については今後の普及状況を踏まえて検討してまいります。
34	日本マイクロソフト株式会社	統一基準	P.44	6.1.5(1)(b)	[該当箇所（原文コピー）] 追加 [意見内容] （オ）政府推奨暗号リストに記載された暗号アルゴリズムが利用できない環境においては、検証済みの暗号アルゴリズムの利用を検討することができるようにすること [理由]： 量子コンピュータの活用により、これまでの暗号アルゴリズムについても十分ではないと言う議論もされるようになりました。これらを踏まえ、検証済みの暗号アルゴリズムについて柔軟に利用できるようなガイダンスも必要だと考えます。	改定箇所への御指摘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、御指摘の内容につきましては、遵守事項6.1.5(1)(b)(イ)において、やむを得ない場合を除き「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用することを求めており、ガイドラインの解説「遵守事項6.1.5(1)(b)(イ)「やむを得ない場合」について」において、政府推奨暗号リストに記載された暗号アルゴリズムが対応していないなどの場合について記載しているため、原案のとおりといたします。
35	日本マイクロソフト株式会社	統一基準	P.46	6.2.3	[該当箇所（原文コピー）] 近年ではインターネットに接続されたいわゆる IoT 機器で構成されたボットネットによる大規模な攻撃や、専門的な技術や設備がなくても攻撃を行うことのできる DDoS 代行サービスの存在も知られており、より一層の警戒が必要となっている [意見内容] 特に、接続されたいわゆる IoT 機器で構成されたボットネットによる大規模な攻撃や、専門的な技術や設備がなくても攻撃を行うことのできる DDoS 代行サービスの存在も知られており、より一層の警戒が必要となっている [理由]： 本書は報告書ではなく、時間に関係なく活用される文書だと認識しています。その中で「近年」とあった場合、文書の内容の正しさについて確保が難しくなると考えます。特記事項であれば「特に」とすることで良いかと考えます。以下に「近年」というキーワードが含まれています。 2.2.3 教育 6.2.3 サービス不能攻撃対策（本コメント） 6.2.4 標的型攻撃対策 7.1.3 複合機・特定用途機器 7.3.2 IPv6 通信回線 6.2.3、6.2.4以外は変更履歴にないことから、近年がすでに近年でないのではないかと判断します。	御意見ありがとうございます。 御指摘の箇所における内容につきましては、現時点では問題があるとは考えておりませんが、今後の課題と捉え、記載内容の検討をしてまいります。

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		
36	パロアルトネットワークス株式会社	統一基準	P.47	6.2.4	該当文書： 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。 意見：下記への文書の変更を意見として提出致します。 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して対処する、侵入範囲の拡大の困難度を上げる、ネットワークや利用者の振る舞いから異常を発見する、及び外部との不正通信を検知して対処する対策（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：巧妙化し続ける標的型攻撃により、攻撃を検知できず意図せず内部の利用者から外部へ情報が漏洩する事例も出ており、より高度な情報セキュリティ対策が必要と考えられる為。	改定箇所への御指摘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。
37	パロアルトネットワークス株式会社	統一基準	P.47	6.2.4(1)(b)	該当文書：(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して対処する対策（内部対策及び出口対策）を講ずること。 意見：(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して対処する、証跡情報により影響範囲を把握する、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して対処する対策（内部対策及び出口対策）を講ずること。 理由：万が一、インシデント等の有事があった際には、速やかにその影響範囲を特定できるよう証跡情報を管理しておく必要があると考える為。	今般の改定にて、ガイドラインの基本対策事項6.2.2(1)-6の解説にEDRに係る記載を追加したところですが、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。
38	パロアルトネットワークス株式会社	統一基準	P.50	7.1.1	該当文書：業務遂行可能なように、利用できる機能の制限や追加のセキュリティ対策を施した上で 意見：下記への文書の変更を意見として提出致します。 業務遂行可能なように、利用できる機能の制限や追加のセキュリティ対策及び有事の際の証跡管理対策を施した上で、 理由：制限や追加のセキュリティ対策を施した上で、万が一インシデント等の有事があった際に、その証跡を管理しておく必要があると考える為。	ログの取得・管理については遵守事項6.1.4にて規定しているところですが、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。
39	日本マイクロソフト株式会社	統一基準	P.51	7.1.1(4)(b)	[該当箇所（原文コピー）] (a)統括情報セキュリティ責任者は、要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置に関する規定を整備すること [意見内容] (a)統括情報セキュリティ責任者は、要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）について、盗難、紛失、不正プログラムの感染等により情報窃取および改ざん、悪用されることを防止するための技術的な措置に関する規定を整備すること [理由]： 本項目に限らず、情報窃取についての記述が多いのですが、改ざんや悪用に関するトラブルも多くなっており、全般的に考慮いただく必要があると考えます。特に端末の項目においては、端末そのものを悪用することにより、なりすましが容易になる場合があることを記載しておく必要もあるかと考えます。同様の記述が(5)(d)などにも見られます	端末に対する改ざん及び悪用されることを防止するための技術的な措置に関しては、引き続き検討してまいります。

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		
40	日本マイクロソフト株式会社	統一基準	P.52	7.1.2	[該当箇所（原文コピー）] 仮に機関等が利用するサーバ装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば、国民からの信頼を大きく損なう。 [意見内容] 改訂前が「機関等が有するサーバ装置が」ということになっており、外部サービスを想定して「機関等が利用するサーバ装置が」と変更されたと推察します。そのことは適切だと思いますが、その場合は遵守事項が外部サービスに適切であるかどうかについても検討していただきたく思います。 外部サービスを想定していないと言うことであれば、その旨を記載していただけると分かりやすいかと思います。	御意見ありがとうございます。 御意見を踏まえ、ガイドラインに解説を追加いたします。
41	日本プルーフポイント株式会社	統一基準	P.55	7.2.1(1)(c)	「情報システムセキュリティ責任者は、電子メールなりすましの防止策を講ずること」 意見　：　上記文言につきまして、下記の通り修正することを提案いたします。 「情報システムセキュリティ責任者は、電子メールなりすましの対策として、送信ドメイン認証技術による受信側および送信側の対策を講ずること」 理由　：　近年、なりすましメールによる被害は増大しております。一般的に信頼度が高いと認知されている政府機関の名を騙るメールについては、被害者が騙される可能性が高いと考えられるため、なりすましメール対策はより強化されるべきとかんがえております。参考資料として提示されております「政府機関等の対策基準策定のためのガイドライン（令和3年度版）（案）」の290ページを拝見しますと、SPF, DKIM, DMARCといった技術が例示されておりますが、DMARCはSPF, DKIMを補強する技術として登場したものであり、諸外国でも米国をはじめとする諸外国でも政府機関についてはDMARCを必須としております。SPFをはじめとする送信ドメイン認証技術の対策は当然のこととして、送信側が責任を負うなりすましメール対策をより強化するためにDMARC導入を促進すべきと考えます。そのような背景を統一基準そのものに表現するために、上記の文言修正を提案するものです。ご検討の程、よろしくお願い申し上げます。	改定箇所への御指摘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、送信ドメイン認証技術による送信側の対策の例については、ガイドラインイ7.2.1(1)-2 a)に示しており、今後の普及状況等を踏まえて遵守化も検討してまいります。
42	個人	統一基準	P.56	7.2.2 (1)(a)(オ)	HTTP Strict Transport Securityを利用したHTTPS必須化を基準に追加すべき。	改定箇所への御指摘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、御指摘の内容については今後の普及状況を踏まえて検討してまいります。
43	パロアルトネットワークス株式会社	統一基準	P.56	7.2.3	該当文書：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。 意見：下記への文書の変更を意見として提出致します。 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と、端末等クライアントからのDNSクエリに対するセキュリティ対策が必要である。 理由：DNSサーバの管理と併せ、クライアントからのクエリに対するセキュリティ対策も同様に必要な為。	改定箇所への御指摘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。
44	パロアルトネットワークス株式会社	統一基準	P.57	7.2.3(2)(b)	該当文書：(b) 情報システムセキュリティ責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。 意見：下記への文書の変更を意見として提出致します。 (b) 情報システムセキュリティ責任者は、コンテンツサーバにおいて、脅威インテリジェンスサービス等を通じて管理するドメインに関する情報が正確であることを定期的に確認すること。 理由：情報の持ち出しに使用される悪意のあるDNSドメインは、近年は標的型攻撃等においても多用される傾向があり、DNSサーバの管理と併せてクライアントからのクエリに対するセキュリティ対策も必要となる為。	改定箇所への御指摘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。

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	日本プルーフポイント株式会社	統一基準	P.62	8.1.1(2)(a)	「情報システムセキュリティ責任者は、職員等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること」 意見　：　上記文言につきまして、下記の通り修正することを提案いたします。 「情報システムセキュリティ責任者は、職員等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から、外部攻撃者による誘導および他の手段による内部不正を防ぐための機能を持つ情報システムを構築すること」 理由　：　情報処理推進機構(IPA)様が発表されている10大脅威の中でも、近年、上位にランクインしている通り、セキュリティインシデントのなかで内部脅威の占める割合は高く、その対策の重要度は増していると考えております。参考資料として提示されております「政府機関等の対策基準策定のためのガイドライン（令和3年度版）（案）」の332ページを拝見しますと、職員による規定の遵守を支援する機能として、不審なWebアクセスへの防御や不審な電子メールへの対処といった部分が強調されておりまして、他の行為（例：機密情報のコピー、外部への送信等）に関する観点が薄いように感じられます。そのため、内部脅威対策防止も重要であるという考えを統一基準そのものに評点するために、上記の文言修正を提案するものです。ご検討の程、よろしくお願い申し上げます。	改定箇所への御指摘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。
46	日本マイクロソフト株式会社	統一基準	P.65	8.1.1(8)	[該当箇所（原文コピー）] 追加 [意見内容] (c) 職員等は Web 会議への参加者の権限について適切な管理ができるようにすること [理由]： Web会議においては、プレゼンテーションや発言、会議の記録などの機能があり、参加者に必要のない機能をオンにしていることで妨害行為などが可能になります。それを防止するための措置についても言及できればと考えます。	遵守事項8.1.1(8)(b)において、会議に無関係の者が参加できないように措置することを求めていることから、参加者による妨害行為は想定していないため、原案のとおりといたします。
47	KPMGコンサルティング株式会社	統一基準	P.65	8.1.1(8)(b)	記載ぶりとして、名宛人の後に読点をいれること、語尾を他の規定と合わせてはいかがでしょうか。 「(b) 職員等はWeb会議を主催する場合、会議に無関係の者が参加できないよう措置すること。」 ↓ 「(b) 職員等は、Web会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。	御意見ありがとうございます。 御指摘のとおり修正いたします。
48	日本マイクロソフト株式会社	統一基準	P.65	8.1.2	[該当箇所（原文コピー）] 全般 [意見内容] テレワークにおいてはクラウドサービスの利用が今後見込まれると考えていますが、具体的な対策がリモートアクセスについて中心的に記載されているように感じます。クラウドサービスへのアクセスはリモートアクセスとは異なる内容になりますので、その点が明確になっていると良いと考えます。 現在の遵守事項は端末内にデータが多く存在することが前提となっており、端末そのもの、またはその内部のデータへの攻撃が想定されているように思いますが、クラウドサービスの利用が進む中で端末内のデータが少なくなり、リスクも変化するのではないかと考えています。	テレワークにおけるクラウドサービスの利用に係るセキュリティ対策については、今後の利用状況を踏まえて検討してまいります。

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		
49	個人	統一基準	P.65	8.1.2(1)(a) 8.1.2(1)(b)	テレワークの実施に係る規定のすべての項目を、情報システムセキュリティ責任者が定めるのは責任の範疇を超えていると考えます。 テレワークの実施に係る規定に盛り込む内容は、必ずしも情報システムに係るものだけではない認識のためです。ガイドラインの基本対策事項8.1.2(1)-1において、規定に盛り込むべき項目が例示されていますが、例えば「c)要管理対策区域外での要機密情報の取扱手続」は統括情報セキュリティ責任者が定めるべきものと考えます。現に、遵守事項7.1.1(4)(a)において、「機関等が支給する端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合の利用手順及び許可手続」は、統括情報セキュリティ責任者が定める実施手順として規定されています。 そのため、各役職における責任の範疇の規定を整備するよう、遵守事項を修正すべきと考えます。仮に、修正不要と判断されるのであれば、そう判断する根拠となる考え方を、ガイドラインに解説として記載することをご検討ください。	御意見を踏まえ、総括情報セキュリティ責任者がテレワーク実施時の情報セキュリティ対策に係る規定を整備することといたします。
50	パロアルトネットワークス株式会社	統一基準	P.66	8.1.2(2)(d)	該当文書：(d) 情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定すること。 意見：下記への文書の変更を意見として提出致します。 (d) 情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定する、もしくは、リモートアクセス経路上で包括的なセキュリティ対策を実施すること。 理由：リモートアクセスにおけるセキュリティ対策は、端末における対策のみではなく、SIG(Secure Internet Gateway)やSASE(Secure Access Service Edge)等の包括的なセキュリティ対策によっても実現可能である為。	御意見ありがとうございます。 御提案のテレワークやリモートアクセスでのクラウドサービスを利用したセキュリティ対策については、今後の利用状況を踏まえて検討してまいります。
51	個人	統一基準	ー	ー	平常時から暗号を使っている場合、鍵が盗まれない為の運用方法は、どこを参照すればよいか明記いただけると有意義だと感じます。	暗号化に用いる鍵の管理については、遵守事項6.1.5(1)(b)(エ)において手順を定めることとしており、管理手順の策定に係る留意事項に関してはガイドラインにおいて解説を記載しております。
52	個人	統一規範	P.5	16条	改正内容に賛成ではない。 機密情報については依然として外部サービスを利用して取り扱ってはならない形とすべきと考える。	改定案では、外部サービスを利用して要機密情報を取り扱う場合の遵守事項を4.2.1項で定めており、現行の統一基準群における「約款による外部サービス」は当該遵守事項を満たすことが一般的に困難であるため、実質的に「約款による外部サービス」では原則として要機密情報を取り扱えないことは変わりませんが、御指摘を踏まえ、統一基準の4.2.1款の目的・趣旨において補足します。

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		
53	個人	ガイドライン	P.13	1.5	遵守事項2.1.1(4)(d) において、情報セキュリティ責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、情報システムセキュリティ責任者を、当該情報システムの企画に着手するまでに選任することとされています。 当該遵守事項では、情報システムの構成要素が外部サービスのみであった場合も、情報システムセキュリティ責任者の選任を求めているのでしょうか。 仮に求めていないのであれば、誤解を与えるため、今回の意見募集の対象外となりますが、ガイドラインの図1.5-1を修正いただくか、注記を追加することをご検討ください。	情報システムの構成要素が外部サービスのみであったとしても、当該情報システムのセキュリティ対策の運用の責任の所在を明確にすることが重要であることを踏まえ、情報システムセキュリティ責任者を選任することが求められます。
54	個人	ガイドライン	P.320	7.3.1(4)-1	現行では、「SSIDの隠ぺい」が記載されていましたが、今回記載が削除されました。これは、今やセキュリティ対策として意味をなさなくなった、との認識でよいでしょうか。他に意図がございましたら、今後のセキュリティ対策の参考としたく、教えてください。	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ありませんが、本対策においては、より強固なセキュリティ対策を求めることとしました。
55	個人	ガイドライン	P.348	8.1.1(8)-1 d)	これは、令和2年10月12日、外務省において公表された「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」と明確に矛盾していると認識しました。 https://www.mofa.go.jp/mofaj/la_c/sa/co/page22_003432.html 本基準がそのまま施行され、これに準拠したサービスを各政府機関が導入した場合、当該政府機関が「要機密情報」と判断したWeb会議に関する記録について、各捜査機関がサービス提供者側から追えないことになり、政府機関等が絡む諸犯罪の立件を難しくするものと思料します。当該項目は本当に追加して問題無いのでしょうか。当方は削除すべきと考えます。	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ありませんが、統一基準群の案は同ステートメントに矛盾しているとは考えておりません。
56	個人	ガイドライン	P.96	3.1.1(6)-2 b)	”秘密分散技術自体が暗号技術の一種であるので、これにより分割されたデータをさらに暗号化する必要はなく、暗号鍵も必要ない。”と表現されています。 仮に秘密分散技術が暗号技術一種であり政府が利用するものならば　「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」にあるものだと想定されます。ところが秘密分散技術を見つけることができませんでした。 対応の仕方として例えば次の2通りがあるかと考えます。 １）この統一基準公開までに”CRYPTREC暗号リスト”に秘密分散技術を具体的に明示する。 ２）問題の文章を含む現状の表現を変更する。 例えば、”基本対策事項3.1.1(6)-2 b)「複数の情報に分割し」について”の内容を次のように表現してみてはいかがでしょうか。 　１個の電子情報について、分割された一部のデータからは情報が復元できない方法で複数に分割し、電子メール、DVD、USB メモリ等の外部電磁的記録媒体で郵送するなど異なる経路で運搬・送信することで、情報漏えいを防止することができる。 　秘匿すべき情報を秘密分散技術を用いて、複数のデータに分割すると、そのうちの一部を窃取されても元の情報を復元することができない。 秘密分散技術を用いると分割されたデータは暗号化されたデータと同様に復元も類推もされないので　さらに暗号化する必要はない。 さらに秘密分散技術では暗号鍵も必要としていない。	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ありませんが、統一基準では暗号化機能及び電子署名機能を導入する際にCRYPTREC電子政府推奨暗号リストの参照を求めているところ、秘密分散技術は暗号技術の一つではありますが、暗号化を行うわけではないため、原案のとおりといたします。

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		
57	個人	全般	ー	ー	・情報処理技術者試験に関する意見	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。
58	個人	全般	ー	ー	・サイバーセキュリティー対策 ・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。
59	日本マイクロソフト株式会社	全般	ー	ー	文書群の名称を「サイバーセキュリティの」と変更されましたが、本文中には情報セキュリティという記載も多くあり、サイバーセキュリティと情報セキュリティの適用範囲についてわかりにくく苦なっているように感じました。改めて、サイバーセキュリティと情報セキュリティを明確に定義していただく必要があるのではないかと考えます。	サイバーセキュリティ戦略本部及びNISCの公表する資料名称を統一する観点から、文書名について「サイバーセキュリティ」を用いることといたしますが、内容面での変更はありません。「情報セキュリティ」と「サイバーセキュリティ」の明確な定義については引き続き検討してまいります。