資料1-5

「政府機関の情報セキュリティ対策のための統一基準群（政府機関統一技術基準を除く）」（案）に対する意見提出の概要及び御意見に対する考え方（案）

情報セキュリティ政策会議

平成　　年　　月　　日

連番	基準	該当箇所	ご意見の概要	ご意見に対する考え方
1	統一規範	第三章第八条(省庁情報セキュリティ文書)	「情報セキュリティに関する障害・事故等」との記載があるが、「情報セキュリティに関するシステム障害」なら意味が解かるが、通常、これを「情報セキュリティ事件・事故」と称していると思います。 (理由) 「情報セキュリティに関する障害」という言葉は、あまり馴染みがないと思われます。一般的には、「情報セキュリティ事件・事故」に含まれる概念であるため、「情報セキュリティ事件・事故」としたほうが適していると思います。	ご指摘の点については、JIS Q 27001:2005において、「情報セキュリティ事件・事故」を使用せずに「情報セキュリティインシデント」としていることを踏まえ、本統一基準では「事件・事故」という用語を使用しない方針としているため、原案のとおりとさせていただきます。
2	統一規範	別表(第五条第四項及び第十六条関係)十六(不正プログラム感染及び拡大の防止)	2，3行目に「・不審なマクロが含まれていると思われるファイル(以下省略)」と記述されているが、1行目の記述と同様に、「安全性が確実ではないファイル(以下省略)」に記述を統一した方が良いと考えます。 (理由) 不正プログラムの感染手段をマクロに限定すべきではないと考えます。	ご指摘のとおり、修正します。 統一規範　別表十六　2. 3行目 (修正前)「・不審なマクロが含まれていると思われるファイル(以下省略)」 (修正後)「・安全性が確実ではないファイル(以下省略)」
3	統一規範	第三章第五条(管理体制)5、 別表(第五条第四項及び第十六条関係)二十四(通信回線の利用時の対策)　ほか	テレワークの推進や大規模災害時の遠隔業務遂行を想定した対策を考慮すべき。 (理由) 総務省、厚生労働省、国土交通省をはじめとする中央省庁及び地方自治体において、行政の効率化及び大規模災害時等におけるIT－BCPの観点からテレワークの推進が進められており、今後さらなる導入が見込まれるところ。行政事務従業者の遵守事項として記載される別表項目内の対策等においてもこれらを踏まえた調整が必要と考えます。 また東日本大震災では、ガイドライン等で定められた内容を非常事態にどのように扱うかについての指針がないために、地方自治体等の現場で混乱が生じたことが知られているところ、業務システムそのもののBCPに加えてこの点を考慮することが有効であると考えます。	ご指摘の点については、今後の検討課題とさせていただきます。
4	運用指針	1-2(11)	「省庁基準」と「セキュリティポリシー」との関係性が分かりづらいと思われます。 (理由) 図1では各府省庁における情報セキュリティポリシーの中に省庁基準が含まれるイメージの図となっていますが、1-2(11)の説明では、「省庁基準」と「セキュリティポリシー」が同じものと読み取ることが出来てしまいます。	ご指摘を踏まえ、図1を修正します。
5	運用指針	2-2　17行目	「責任分界点」の誤表記と思われます。 (理由) 「責任分界」ではなく「責任分界点」と明示的に表記したほうが分かりやすいと思われます。	ご指摘の点については、文意がほぼ同義であることから、原案のとおりとさせていただきます。
6	運用指針	2-2 8行目	・「これと連携して運用する情報システムを管理する府省庁」は、「基盤となる情報システムを整備し運用管理する府省庁」と同様に「基盤となる情報システム」の主催者側の立場の府省庁を指すのであれば、「これと連携して運用する情報システムを管理する府省庁」は削除してはどうでしょうか？ ・「これと連携して運用する情報システムを管理する府省庁」は、「基盤となる情報システム」を使用する側の府省庁の運用管理者を指すのであれば、「これを使用する各府省庁」と表現してはどうでしょうか？ (理由) ・「これと連携して運用する情報システムを管理する府省庁」というのは、「基盤となる情報システム」を運用管理する府省庁と同じ立場の府省庁を指すのか、使用する側の府省庁のどちらを指すのか分かりません。 ・運用管理する府省庁と同じ立場の府省庁を指すのであれば、「このため、基盤となる情報システムを整備し運用管理する府省庁」という表現で十分意味が通じると思われます。	「これと連携して運用する情報システムを管理する府省庁」は、「基盤となる情報システム」を使用する側の府省庁を指しておりますが、利用のみならず、「連携して運用・管理を行う」ことも含まれると考えられることから、原案のとおりとさせていただきます。
7	運用指針	2-2　最終行	情報セキュリティマネジメントが適切に「実行される」より「実施される」の方が分かりやすいと思われます。 (理由) 1-2(5)で「情報セキュリティマネジメント」の定義をしていますが、行なう行為として定義されていますので、「実行される」より「実施される」のほうがより適切な表現かと思われます。	ご指摘の点については、文意がほぼ同義であることから、原案のとおりとさせていただきます。
8	運用指針	3-4　12行目	情報セキュリティ報告書を作成し、取組状況を公表する方針は賛成ですが、報告書に記載すべき内容を定義した方が良いと思います。 (理由) 府省庁ごとにリスク評価を実施し、省庁対策基準を策定しますが、「情報セキュリティ報告書」にはその内容まで含めるのでしょうか？ リスク管理上そこまでの内容は公表しないと思いますが、どこまでの内容を公表するのか分かりません。	ご指摘の点については、情報セキュリティ報告書専門委員会の策定した「情報セキュリティ報告書専門委員会報告書」(http://www.nisc.go.jp/active/general/pdf/sec_report.pdf)において、報告内容が定められています。
9	運用指針	3-4　5行目	「ひやり事案」より「ヒヤリ・ハット事案」の方がより一般的な表現かと思われます。 (理由) Googleで「ひやり事案」を検索しましたが、ヒット数が少なかったため。	ご指摘のとおり、修正します。 運用指針3-4　5行目 (修正前)「ひやり事案」 (修正後)「ヒヤリ・ハット事案」
10	統一管理基準	1.1.1.2 本統一管理基準及び統一技術基準の使い方	ライフサイクルという用語があいまいに使用されているので、明確な定めが望まれる。 (理由) 時系列を意識した適切なセキュリティ対策を検討するにあたっては、「ライフサイクル」を正確に定義しておく必要があるが、統一基準群にはこの定義がなされていないと思われる。	ご指摘の点については、運用指針の3-3(3)において、情報のライフサイクルは「情報の作成及び入手から消去まで」、情報システムのライフサイクルは「情報システムの計画から廃棄及び見直しまで」と記述しておりますが、今後の検討課題とさせていただきます。
11	統一管理基準	1.1.1.2 本統一管理基準及び統一技術基準の使い方(3)	原文:・・(中略)・・今後は、省庁対策基準において、全ての遵守事項を採るものとする。 変更:・・(中略)・・今後は、従来の「基本遵守事項」又は「強化遵守事項」を廃止して「遵守事項」とし、省庁対策基準において、保護すべき情報とこれを扱うシステムにおいて、必須として実施すべき対策事項とする。 (理由) 従来の「基本遵守事項」又は「強化遵守事項」についての説明はあるが「遵守事項」についての説明がないので解りにくい。統合した対策レベルが2つのうちの基本遵守事項に相当する事を明記する。	ご指摘を踏まえ、以下のとおり修正します。 1.1.1.2(3) ・・(中略)・・今後は、従来の「基本遵守事項」及び「強化遵守事項」の区分を廃止して「遵守事項」とする。「遵守事項」は、省庁対策基準において、保護すべき情報とこれを扱うシステムにおいて、必須として実施すべき対策事項とする。なお、必要性の有無を検討し、必要があると判断した際に実施する対策事項については、実施の必要性の有無の検討を必須とし、対策の実施についてはそれぞれの府省庁の判断とする。

連番	基準	該当箇所	ご意見の概要	ご意見に対する考え方
12	統一管理基準	1.1.1.3 情報の格付の区分及び取扱制限の種類 (2)	「格付としては、以下の記載のものを本統一管理基準の遵守事項で用いるが、それぞれの府省庁において、適宜変更又は追加して構わない。」との記述があるが、適宜変更するのではなく「原則統一」とするのが望ましい。 (理由) 各府省庁の個別システムが連携して稼動するシステム全体のセキュリティレベルは、各システムにおける最もレベルの低いセキュリティレベルと同一になるため。 また、縦割りの弊害を無くし、セキュリティ運用の効率化を図るためにも、情報の格付は府省庁間で「原則統一」とするのが望ましい。	ご指摘の点については、各府省庁の特性に応じた対応の配慮が必要な面があることから定めていますが、最低限のセキュリティ水準を確保する観点から、「変更又は追加する場合には、それぞれの府省庁の対策基準における格付区分と遵守事項との関係が本統一管理基準及び統一技術基準での関係と同等以上となるように準拠しなければならない」こととしており、原案どおりとさせていただきます。
13	統一管理基準	1.1.1.4 情報取扱区域における管理及び利用制限 (2)(a)	・クラス0の表記を、「・・情報セキュリティを確保するために必要に応じて利用制限対策を実施する区域」として頂きたい。 ・表現が抽象的であり明確化して頂きたい。 (理由) ・クラス1が最低限必要な・・・実施する必要がある区域とありますが、クラス0でも実施する必要がある区域となっており、クラス0のレベル度が理解しづらかったため。 ・この表(区分の基準)だけでは、判断する区域のクラスを決定することは不可能と思われます。	ご指摘の点については、すべての情報を取り扱う区域を区分するための名称として、クラス0～4を設けており、クラス0は要管理対策区域外と同等であることから、利用制限対策を実施する区域とさせていただいています。
14	統一管理基準	1.1.1.4 情報取扱区域における管理及び利用制限 (3)	「クラス別管理及び利用制限は、最低限の管理対策及び利用制限対策であるため、それぞれの府省庁において、名称の変更、クラスの追加並びに実施する管理対策及び利用制限対策の変更又は追加を適宜実施して構わない。」との記述があるが、追加はよいとしても変更は原則禁止が望まれる。 (理由) 各府省庁間を連携して作動するシステムにおいて、上記の変更を許すと管理ミスを誘発し、またセキュリティの穴が出来やすくなり、さらに監査の手間(コスト)も増大すると想定される。	ご指摘の点については、最低限のセキュリティ水準を確保する観点から、「変更又は追加する場合には、それぞれの府省庁の対策基準で求める情報取扱区域における情報セキュリティ水準が、本統一管理基準及び統一技術基準において求める情報セキュリティ水準と同等以上となるように準拠しなければならない」こととしており、特に新たな概念であることから、各府省庁の特性に応じた対応の配慮が必要な面があるため、原案どおりとさせていただきます。
15	統一管理基準	1.1.1.5 評価の方法	内閣官房セキュリティセンターの役割を記述して頂きたい。 (理由) 内閣官房セキュリティセンターに報告する旨、記述されておりますが、当然のことであっても報告する役割を明記された方が報告の意味が深まると思います。	ご指摘の点については、運用指針の2-3等に記載しています。
16	統一管理基準	1.1.1.6 用語定義	用語集として、巻末に付録として定義されたい。 (理由) 文書の途中にあるのは参照しづらい	ご指摘の点については、1.1.1.6は「用語定義」として本文に含まれるものであり、付録は「用語解説」として一般的な用語を解説しており、解説書に含まれるものであるため、原案のとおりとさせていただきます。
17	統一管理基準	1.1.1.6 用語定義 【か】「外部委託」	外部委託の定義で、対象は情報システムのみに言及してよいのか疑問である。 (理由) 情報を扱う全ての業務のうち、情報システムのみの扱いを「外部委託」と定義しているように読み取れてしまう。	ご指摘の点については、今後の検討課題とさせていただきます。
18	統一管理基準	1.1.1.6 用語定義 【さ】「情報」	「したがって」 という接続語は不要だと思います。 (理由) 「したがって」前後の文脈が繋がらない、と思われます。	ご指摘の点については、後段の文章と繋げる意図があるため、接続詞を入れていることから、原案のとおりとさせていただきます。
19	統一管理基準	1.1.1.6 用語定義 【は】「府省庁支給以外の情報システムによる情報処理の制限」	“ここでいう”、以降の説明ははずして頂きたい。または統一技術基準にて記述して頂きたい。 (理由) 用語の説明でありますが、”ここでいう・・”以降の説明は具体的なサービスの説明であり、技術基準にて利用説明をされた方がより明確と思われます。個人で契約するメールを例示されておりますが、個人契約のメールについてはセキュリティ管理の是非が問われますのでここでは記述されないほうが良いと思います。	ご指摘の点については、1.4.2.2「府省庁支給以外の情報システムによる情報処理の制限」に関する記述であり、「ここでいう～」以降の文章も、当該項に関係する記述のため、原案どおりとさせていただきます。
20	統一管理基準	1.2.2.1 情報セキュリティ対策の教育(1)	教育実施の有効性に言及して頂きたい。 (理由) 受講者の理解度・有効性など、教育したことによる実施効果にも言及すべきと考えます。	ご指摘の点については、教育に関する個別の施策において、検討させていただきます。
21	統一管理基準	1.2.2.1 情報セキュリティ対策の教育(1)	統括情報セキュリティ責任者は、行政事務従事者に求められるセキュリティの技量を定義して頂きたい。 (理由) 「関連規程」の教育実施のみが述べられており、「何が必要か」はどこかで述べられているのかが不明のため。	ご指摘の点については、求められるセキュリティの技量については、その時々及び場面に応じて変化し、一概に定義することが難しいと考えられるため、原案どおりとさせていただきます。
22	統一管理基準	1.2.2.2 障害・事故等の対処	事故発生時の体制の他、体制に沿ってインシデントの格付け、トリアージについて記載して頂きたい。 (理由) 障害・事故対応は体制面だけでは実運用が難しいと思います。判断基準を設けていただくとよろしいかと思います。	ご指摘の点については、今後の検討課題とさせていただきます。
23	統一管理基準	1.2.5.1 外部委託 (4) (c)	審査基準についても言及して頂きたい。 (理由) 「選定基準及び選定手続に基づきその都度審査する」との記述があるので、審査基準も明確にすべきと思います。	ご指摘の点については、「審査」は「選定」とほぼ同義であり、選定基準及び選定手続に含まれると考えられるため、原案のとおりとさせていただきます。
24	統一管理基準	1.3.1.2 情報の利用 (5)	要保護情報を「どのように」管理するかも言及して頂きたい。 (理由) 管理簿をつけるなど、具体的な管理方法を提示したほうが良いと思われる。	ご指摘の点については、1.3.1.1～1.3.1.6において、情報の格付及び取扱制限に従って、適切な管理を行うように定めております。
25	統一管理基準	1.3.1.3 情報の保存 (1) (a)	「海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、国内であれば不適切となるアクセスをされる可能性があることに注意が必要である。」との記述があるが、どのような注意が必要であるかの記述が望まれる。 (理由) 情報の格付によっては、例えば「海外のデータセンターへの保存は禁止する」など、具体的に示さなければ行政事務従事者としても対応に窮すると思われる。	ご指摘の点については、外部委託に関する個別マニュアル(DM6-02)で記載させていただいており、原案のとおりとさせていただきます。
26	統一管理基準	1.3.1.4 情報の移送(5) (a)	パスワードの運用(ポリシー)にも言及して頂きたい。 (理由) 当該箇所を含め、全体的に「パスワードを設定すること」という記述はあるが、その運用については言及していないため。	ご指摘の「パスワード」については、「主体認証情報」の代表的な例の一つとして、記載しております。そして、1.4.1.1(2)「主体認証情報の管理」に記載があり、また、知識を用いて主体認証方式を用いる場合の遵守事項として、2.2.1.1(1)(c)を設けております。

連番	基準	該当箇所	ご意見の概要	ご意見に対する考え方
27	統一管理基準	1.5.1.1 情報システムのセキュリティ要件(1) (d)	最終行に、「当該製品を情報システムの構成要素として選択すること。」と記述されておりますが、「当該製品を情報システムの構成要素として選択することが望ましい。」等の表現に変更することが望ましい。 (理由) 認証制度は機器の信頼性を第三者機関が認証するという観点では重要な制度であると認識しております。一方で、認証取得までに一定の期間が必要であり最新のセキュリティ装置並びに装置上で動作しているソフトウェアの組み合わせでの認証取得が追いついていない現状があります。	ご指摘の点については、本遵守事項においては「必要があると認めた場合は」と条件を付していること、また、遵守事項は実施すべき対策事項を示しており、「望ましい」といった表現は用いていないことから、原案のとおりとさせていただきます。
28	統一管理基準	1.5.1.1 情報システムのセキュリティ要件(1)(d)	原文を変更して下記のように「必要があると認めた場合には」を削除する。 原文:・・(中略)「ITセキュリティ評価及び認証制度に基づく認証取得製品分野リスト」を参照し、必要があると認めた場合には、当該製品の分野において・・(後略) 変更:・・(中略)「ITセキュリティ評価及び認証制度に基づく認証取得製品分野リスト」を参照し、当該製品の分野において・・(後略) (理由) 「ITセキュリティ評価及び認証制度に基づく認証取得製品分野リスト」は重要なセキュリティ要件がある場合に製品分野やその利用環境を踏まえて作成されているのでリストを参照する事により必要性を認知できるため。	ご指摘の趣旨は理解しますが、実際の調達可能性等も勘案し、原案のとおりとさせていただきます。
29	統一管理基準	1.5.1.1 情報システムのセキュリティ要件(1)(d)	原文を変更して下記のように「望ましい」を削除する。 「原文」:(中略)・・製品分野として当該認証を取得する必要性の判断については、「ITセキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」に則ることが望ましい。・・(後略) 「変更」:(中略)・・製品分野として当該認証を取得する必要性の判断については、「ITセキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」に則ること。・・(後略) (理由) 本項目の本文では同リストを“参照する事”と定めているので、この意に合致した解説文とするため「望ましい」を削除する。	ご指摘の趣旨は理解しますが、実際の調達可能性等も勘案し、原案のとおりとさせていただきます。
30	その他	その他	たとえば、一般の国民が政府の情報システムに脆弱性を発見した場合、それを誰に報告すればよいのでしょうか。現在のところ、IPAセキュリティセンターということになると思います。通常はこれでよいのですが、IPAセキュリティセンターは政府基準に適合する受付のみを受理し、それ以外は受理しません。そこで、IPAの基準には適合せず、また警察に通報するほどの事件性はないが、適切なCSIRTへの通報が必要と思われる案件をどの窓口へ報告すればよいかという問題になります。 手続きを簡素化し、届出者の負担を軽減するため、政府への脆弱性の報告をIPAセキュリティセンターに一元化すべきと考えます。これに伴い、IPAセキュリティセンターは、政府を対象とする届出については、一般の届出よりも広い基準で受理することが必要になります。	ご指摘の点については、1.2.2.2(1)(g)において、「府省庁の外部から報告を受けるための窓口を設置」することを求めておりますので、今後設置予定の各府省庁の窓口へご報告いただきたいと存じます。
31	その他	統一基準群の全体を通じて	「府省庁」、「それぞれの府省庁」、「各府省庁」など、表現が統一されていないので、統一されたい。 (理由) 文章の読みやすさ	ご指摘の点については、前回の改定において、使い分けを検討し、整理しているため、原案のとおりとさせていただきます。
32	その他	統一基準群の全体を通じて	障害・事故等の対処は記述されているが、安全保障上の観点から、テロを想定した物理的セキュリティおよびシステム的セキュリティ対策も追加すべきと思われる。リスクマネジメントの観点からも必要であろう。 (理由) 東日本大震災では想定外の原発事故が発生した。情報システムについても、政府機関や民間のデータセンター等に対し想定外のテロ攻撃がなされる可能性がある。しかしながら統一基準群にはテロ攻撃を想定した対策要件が記述されていない。	ご指摘の点については、今後の検討課題とさせていただきます。
33	その他	統一基準群の全体を通じて	統一基準群は、広範なセキュリティ対策を記述しているが、各々の対策が国際標準であるISO27000シリーズのどの項目に対応するのかの記述が望まれる。 (理由) 国際標準であるISO27000シリーズに対する整合性が不明なので、セキュリティ対策の網羅性において対策に抜けがあるか否かの検証ができない。	ご指摘の点については、政府機関統一基準適用個別マニュアル群　DM7-02「政府機関統一基準とISO/IEC27002:2005等との対応について」において、ISO/IEC 27002:2005及びNIST SP 800-53 Rev.2との対応を整理しています。
34	その他	統一基準群の全体を通じて	「情報システム」の定義があいまいと思われます。 随所に、当該語句が使用されているが、「電子計算機」という語句も使用されており区別する意味も不明と思われる。 (理由) 第二条2項に“情報処理及び通信に係るシステム”という定義らしき記載があるが、P9にある別表の二十四に「電子計算機」、「通信回線装置」という語句もあり、区別がつきにくいと思われる。 また、P8に“府省庁支給の情報システム”という語句があるが、PCのことを指すのか、業務APのことを指すのか、定かではない。	ご指摘の点については、「情報システム」は、「情報処理及び通信に係るシステム」として、サーバ装置及び端末だけでなく、通信回線や通信回線装置等も包含する概念となっています。それに対し、「電子計算機」は、情報システム内のサーバ装置や端末といったコンピュータ全般のことを指す用語と定義させていただいております。

意見提出者一覧（五十音順）

一般社団法人　ＩＴセキュリティセンター

シスコシステムズ合同会社

データベース・セキュリティ・コンソーシアム

トレンドマイクロ株式会社

日本ユニシス株式会社

パロアルトネットワークス合同会社

その他個人１件