「政府機関の情報セキュリティ対策のための統一基準」に追加すべき項目（骨子）に関する意見の募集の結果について

平成17年12月13日
内閣官房情報セキュリティセンター

標記について、平成17年10月17日から11月11日まで意見募集を行った結果、14団体・個人から70件のご意見をいただきました。お寄せいただいたご意見について、その概要とご意見に対する考え方を以下のとおり取りまとめましたので、公表いたします（なお、公表に当たっては、内容が重複又は類似のものを整理しております。）。

今回、ご意見をお寄せいただきました皆様に厚く御礼申し上げます。

なお、下表において、政府機関の情報セキュリティ対策のための統一基準は「政府機関統一基準」、同（2005年９月項目限定版）は「項目限定版」、同（2005年12月版（全体版初版））は「全体版初版」と記します。

「政府機関の情報セキュリティ対策のための統一基準」に追加すべき項目（骨子）に関する意見

該当箇所	ご意見の概要	ご意見に対する考え方
Ⅰ　機器等の購入		
(a)	「情報関連機器及び情報システム（以下「機器等」という。）の購入に際し、情報セキュリティ対策の視点を加味して、機器等の選定手続き、選定基準及び機器等が具備すべき要件を整備し、これに従って購入機器等を選定すること。」に訂正すべきである。	ご意見のうち「情報関連機器」の購入に関する部分については、Ⅰ(b)の内容と重複するものです。 「情報システム」の購入に関する部分については、その構築に際して情報セキュリティ対策の視点も加味し、新たな項「情報システムのセキュリティ要件」を設けました。 ※　全体版初版6.1.1(1)(a)、4.3.1参照
	(a)の後に、「機器等が具備すべき情報セキュリティ対策は、保護すべき情報資産と想定される脅威を考慮して、必要なセキュリティ機能を定めること。」との規定を追加すべきである。	必要なセキュリティ機能について、機器等の具備すべき要件等を整備することを明記しました。 ※　全体版初版6.1.1(1)(a)参照
(b)	「機器等の選定手続き及び選定基準」の内容を具体的に明示すべきである。	各府省庁内において必要な手続き及び基準が具体的に整備されることとしております。
(e)	「機器等の購入において、満足すべきセキュリティ機能の要求仕様がある場合には、これについて、情報セキュリティ評価・認証制度によるセキュリティ設計仕様書を作成させ、当該仕様が適切に実現されているかどうかを確認するために、認証取得の有無または認証取得のための評価中であるかどうかを評価項目として活用すること。」に訂正すべきである。	機器等を購入する際に満足すべきセキュリティ機能の要求仕様がある場合には、認証を取得した製品を優先的に選定する趣旨の基準であり、認証を入札時点で取得していないものを完全に除外するものではないため、原案のとおりといたします。 ※　全体版初版6.1.1(1)(d)参照
(e)	「機器等の購入において、満足すべきセキュリティ機能の要求仕様がある場合には、これについて、情報セキュリティ評価・認証制度による認証を取得しているかどうかを評価項目として活用することが望ましい。」に訂正すべきである。	遵守事項として「望ましい」というあいまいな判断基準を設けることは適切ではないと考えます。機器等を購入する際に満足すべきセキュリティ機能の要求仕様がある場合には、認証を取得した製品を優先的に選定する趣旨の基準であり、原案のとおりといたします。 ※　全体版初版6.1.1(1)(d)参照
(e)	特定の規格、認証制度、及びツール等を評価項目の対象とするに当っては、合理的かつ明示的な理由が認められる場合において、調達担当者の適切な理解に基づき適宜実施されることが望ましく、そのためには、各省庁の調達担当者がそのような運用を円滑に行い得るガイドが必要である。	ご意見いただきありがとうございます。ご指摘の点につきましては、今後検討してまいります。
(e)	評価・認証制度に関しては、国内外に広く受け入れられているものであることを明記すべきである。	情報セキュリティ評価・認証制度については、国際基準ISO/IEC 15408に基づく「ITセキュリティ評価及び認証制度」を想定しており、解説で趣旨を明らかにしました。 ※　全体版初版6.1.1(1)(d)参照
	大企業優先で中小企業排除の方針に異論がある。 また、「改正の方向」に「製品は他社製品を模倣したものでない正当なもの」との規定を追加すべきである。	政府機関統一基準において、大企業を優先し、中小企業を排除するという方針はありません。 また、機器等を購入する際に他社を模倣しているかどうかについて、違法性がある場合には、本基準に規定を設けるまでもなく、採用されないものと考えます。

II　ソフトウェア開発		
(a)	ソフトウェア開発工程と限定することなく、アプリケーション開発工程全体にわたって、セキュリティ対策を行うべきである。	ご意見の趣旨を意識して作成しておりますが、このことをより明確するため、新たな項「情報システムのセキュリティ要件」を設けました。 ※　全体版初版4.3.1参照
(b)	セキュリティ機能の要求に当たって参照することができるガイドラインを示すことを前提として、下線部分を追加すべきである。「開発するソフトウェアにおいて取扱う情報の格付けに応じて、統一的な手法を参考としてセキュリティ機能を適切に設計すること。」	ご意見いただきありがとうございます。ご指摘のガイドラインの整備につきましては、今後検討してまいります。なお、整備がなされていないガイドラインの存在を前提として規定することは相当ではないと考えます。
	II(b) の後に、「開発するソフトウェアの設計に当たっては、リスク分析を行い脅威と対策法を明確にした上で、セキュリティ設計仕様書を作成すること。【基本遵守事項】」を追加すべきである。	ご指摘のとおり、ソフトウェアの設計に当たり想定される脅威と対策を分析することは重要であると考えており、ご趣旨が明確になるような記述といたしました。 ※　全体版初版6.1.3(3)(a)参照
(h)	「脆弱性の原因となるソースコードの有無を検査する方法を定めること。ただし、著作権等の問題がある場合はこの適用ではない。」に訂正すべきである。	ソースコードレビューについては、開発するソフトウェアだけを対象として想定しており、市販製品を組み込む場合等、ソースコードの入手が困難な場合に実施することは想定しておりません。この点が明確になるような記述といたしました。 ※　全体版初版6.1.3(4)(c)解説参照
(i)	「開発するソフトウェアについて、満足すべきセキュリティ機能の要求仕様がある場合には、これについて、情報セキュリティ評価・認証制度によるST確認または認証を取得すること。」に訂正すべきである。	ソフトウェア開発をする際に重要なセキュリティ要件がある場合、それについてセキュリティ設計仕様書（ST：Security Target）のST評価・ST確認を受ける趣旨が明らかになるような記述といたしました。 ※　全体版初版6.1.3(3)(e)参照
(i)	「開発するソフトウェアにおいて、（中略）、情報セキュリティ評価・認証制度による認証を取得しているかどうかを評価項目として活用することが望ましい。」に訂正すべきである。	遵守事項として「望ましい」というあいまいな判断基準を設けることは適切ではないと考えます。ソフトウェア開発をする際に重要なセキュリティ要件がある場合、それについてセキュリティ設計仕様書（ST：Security Target）のST評価・ST確認を受ける趣旨が明らかになるような記述といたしました。 ※　全体版初版6.1.3(3)(e)参照
(i)	特定の規格、認証制度及びツール等の適用については、合理的かつ明示的な理由が認められる場合において、調達担当者の適切な理解に基づき適宜実施されることが望ましいことから、各府省庁の調達担当者がそのような運用を円滑に行い得るためのガイドラインが必要である。	ご意見いただきありがとうございます。ご指摘の点につきましては、今後検討してまいります。
	ソフトウェア開発に使用するAPI及び開発言語についての規定を追加すべきである。	ご意見については、情報セキュリティ対策について定める政府機関統一基準で規定すべき範囲ではないと考えます。
III　外部委託		
(c)	「委託先においても各府省庁と同等の対策を実施」に関する内容を、現実性も考慮した具体的なものとして明確化すべきである。	委託先が行うべき情報セキュリティ対策については、業務内容に応じて現実性も考慮しつつ委託先と府省庁が協議・合意した結果を契約として明確化することになります。この場合、委託先に求める情報セキュリティ水準は、府省庁におけるものと同等なものとなります。
	システム開発や運用ベンダの選択基準に、情報セキュリティ評価・認証制度による認証を取得しているかどうかを評価項目として活用することを盛り込むべきである。	ご意見の趣旨については情報セキュリティ対策として重要と考えており、項目限定版6.1.1(1)(c)(d)で定めているところです。 ※　全体版初版6.1.2(1)(c)(d)参照
IV　BCP（事業継続計画）との整合的運用の確保		
	実際の適用・推進に当っては、当該事業継続計画に関する推進方針、基準等が明確化されていることを前提とすべきである。	ご意見のとおり、実際の運用に当たっては、事業継続計画に関する推進方針、基準等の明確化は必要と考えます。その上で、事業継続計画と情報セキュリティの整合的運用の確保を行うことが重要と考えます。
	BCPを意識した形で、「第２部 組織と体制の確立」部分を改訂すべきであり、具体的には最高情報セキュリティ責任者を初めとする各層の責任者や管理者不在時の代行者の候補認定・任命・解任等の基準を設けるべきである。	ご意見のとおり、組織と体制について、各府省庁で詳細に規定する必要があり、省庁基準等において定められるべきと考えております。

V　情報保証のための機能		
	「情報保証」という用語を新たに取り入れるのではなく、セキュリティマネジメントの考え方を政府機関統一基準の「第１部」で明確化すべきである。	遵守内容については第１部の紹介にとどめるのではなく、第４部の基本遵守事項とすることで、その徹底を図りたいと考えます。 ご指摘の考え方については、「政府機関の情報セキュリティ対策における統一基準の策定と運用等に関する指針」で説明しております。同指針については、以下のページを参照下さい。 http://www.bits.go.jp/active/general/kijun01.html

「政府機関の情報セキュリティ対策のための統一基準（2005年9月項目限定版）」等に関する意見

1.1.1　統一基準の位置付け		
	個人情報保護法との関係も考慮して、政府機関統一基準を構成すべきである。	個人情報保護法は個人情報の適切な取扱いについて規定したものであり、一方、政府機関統一基準は個人情報を含む行政事務で取り扱う情報全般のセキュリティ確保を目的とするものです。これらの規定間で整合がとれた運用が可能と考えます。
1.1.2　本統一基準の使い方		
(1)	各府省庁が政府機関統一基準の内容を省庁対策基準に反映させるまでの期限を明記すべきである。	各府省庁は、本年度中に全体版初版に基づき省庁対策基準を策定することとなっております。
(2)	独立行政法人等を、政府機関統一基準の対象とすべきである。	独立行政法人については、「政府機関における情報セキュリティ対策の強化に関する基本方針」（平成17年9月15日情報セキュリティ政策会議決定）で、「各府省庁は、政府機関統一基準を踏まえ、所管の独立行政法人等の情報セキュリティ水準の向上を促進する。」としているところであり、政府機関統一基準に準じた情報セキュリティ対策がなされるものと考えます。
(6)	各府省庁の対策の実施状況及び監査結果に対する情報セキュリティセンターによる評価については、その結果を公表することを義務付けるべきである。	評価結果については、情報セキュリティ政策会議（議長：官房長官）への報告を予定しているところです（政策会議の資料は情報セキュリティセンターのホームページ上で見ることができます。）。
(6)	評価結果に応じて、各府省庁の予算を増減させるような仕組みを設けるべきである。	ご意見ありがとうございます。ご指摘の点については、参考とさせていただきます。
(6)	情報セキュリティ政策会議の勧告について、強制力を持たせるような仕組みを設けるべきである。	勧告については、情報セキュリティ政策会議において行われるものであり、その結果について、府省庁は必要な改善措置を行うこととなります。
1.1.3　用語定義		
	「機密３情報」の用語定義について、「行政事務で取り扱う情報のうち、その漏洩により、国民の生命、財産、プライバシーなどの権利が侵害されるおそれがある又は秘密文書に相当する機密性を要する情報をいう。」と変更すべきである。	「機密性３情報」の定義の「秘密文書」とは、「秘密文書等の取扱いについて」（昭和40.4.15事務次官等会議申合せ）に基づき各府省庁で定義されたものであり、表現振りの相違はありますが、ご指摘のように変更しなくとも、適切な取扱いがなされるものと考えます。
第2部　組織と体制の確立		
(1)	政府としての最高情報セキュリティ責任者を設置すべきである。	政府機関全体としての情報セキュリティ対策については、情報セキュリティ政策会議において進めているところであり、当該政策会議の責任者に官房長官が就任しています。
(5) (6) (7)	各責任者及び管理者の交代時における引継ぎの規定を明記すべきである。	引継ぎについては、情報セキュリティに係る事務に限らず、行政事務全般において行われるものであるため、政府機関統一基準において特記する必要はないものと考えます。
	最高情報セキュリティ責任者と各府省庁の大臣・副大臣・事務次官との位置付けを明確に記述し、情報セキュリティ対策に関する進言と報告を行うべきである。	最高情報セキュリティ責任者は、自らが所属する府省庁における情報セキュリティ対策に関する事務を総括する者ですが、同責任者をどの職に充てるかについては、情報セキュリティの確保がなされることを前提として、実情に応じ各府省庁の裁量に委ねられているところです。
2.1.3　違反と例外措置		
(1)(c)	情報セキュリティ規定への重大な違反行為については、統括情報セキュリティ責任者ではなく、最高情報セキュリティ責任者に報告すべきである。	ご意見の趣旨を踏まえ、全体版初版で訂正しました。 ※　全体版初版2.1.3(1)(c)参照

2.2.1	情報セキュリティ対策の教育	
	情報セキュリティの規程に違反した対象者に対し、違反の通知を情報システムで実施する機能を設け、又はその仕組みを整備すべきである。	ご意見いただきありがとうございます。今後の参考とさせていただきます。
2.2.2	事故及び障害の対応	
(2)	障害等の発生時において、公表する事案及びその方法を整備する。	障害等のうち国民に影響を及ぼすものについては、公開することが適切と考えますが、ご指摘の事項については、情報セキュリティ対策について定める政府機関統一基準で規定すべき範囲ではないと考えます。
2.3.2	情報セキュリティ対策の監査	
(1)	情報セキュリティ監査責任者は、年度情報セキュリティ監査計画の整備に当たり、最高情報セキュリティ責任者の承認を得る遵守事項では、監査の独立性が担保されないのではないか。	最高情報セキュリティ責任者は、情報セキュリティ責任者等が実施すべきルールを定める立場にあり、情報セキュリティ責任者等によって行われる業務からは独立した立場にあります。最高情報セキュリティ責任者は、情報セキュリティ責任者等が所管する組織における情報セキュリティ監査を実施する目的で情報セキュリティ監査責任者を定めることから、監査の独立性について問題はないものと考えます。
	情報セキュリティマネジメントシステム(ISMS)適合性評価制度を活用し、国際標準に沿った情報セキュリティ対策を実施すべきである。	政府機関統一基準は、ISO/IEC 17799等との対応も考慮して策定しており、ご意見のISMS(適合性評価制度)の基本的な考え方や各要求事項を踏まえた内容となっております。 なお、政府機関統一基準とISO/IEC 17799等との対応関係については以下のページを参照下さい。 http://www.bits.go.jp/active/general/pdf/rel2005_iso.pdf
2.4.1	情報セキュリティ対策の見直し	
(1)	「監査」又は「自己点検」の結果、問題点を指摘され、又は発見した場合も、セキュリティ対策の見直しを行なうべきことを明記すべきである。	ご意見については、同事項の解説において同趣旨のことを明記しております。
3.2.1	情報の作成と入手	
	各部門の情報セキュリティ責任者を情報の格付けに関する責任者とすべきである。 また、政府横断的かつ具体的なガイドラインを策定すべきである。	政府機関統一基準の適用対象となる情報には、作成中の文書・資料等の情報が含まれており、こうした情報について情報セキュリティ責任者や課室情報セキュリティ責任者等が逐一的に格付けを行うことは運用上困難と判断されます。そのため、格付けについては、情報セキュリティ委員会が格付けに関する基準等を整備することとしており、これに従って情報の作成者又は入手者が適正に格付けを行うことが可能となります。 また、情報の格付けについては、府省庁が判断基準を策定するための手引きを作成する予定です。
3.2.3	情報の保存	
(1)(d)	「要機密情報を電子計算機又は外部記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。」を、「情報の機密性を維持すること」と一般的に表現してはいかがかと思います。	ご指摘のような表現については具体性がなく、安易な方法が用いられることもあり得ることから、最低限実施すべきこととして暗号化に関する規定を設け、その実効性の確保を意図したものです。
3.2.4	情報の移送	
(2)(3)	(2)「送信と運搬の選択」及び(3)「移送手段の選択」についても、機密性の区分に応じて許可制と届出制の双方を設ける。	情報提供の可否については、当該情報の機密性に応じてその取扱いを区別すべきものと考えますが、その具体的な移送の方法や手段については、移送を行う行政事務従事者が(4)及び(5)の遵守事項を遵守することで適正な取扱いが担保されるものであることから、届出制としたものです。
第4部	情報セキュリティ要件の明確化に基づく対策　　第5部　情報システムについての対策	
	各府省庁のセキュリティ・アーキテクチャの制定について触れるのがよいかと思います。その際、政府機関統一のEA(エンタープライズ・アーキテクチャ)があるのならば、それとの関連について明確にする必要があると思われます。	セキュリティ・アーキテクチャという用語をそのまま引用していませんが、一部においてアーキテクチャの観点での遵守事項を定めております。また、統一基準では、政府におけるEA(エンタープライズ・アーキテクチャ)との整合について配慮しております。しかし、EAとの整合についてはＩＴ戦略全体の中で位置づけているため、政府機関統一基準の遵守事項として個別に明確にする必要はないものと考えます。

第4部　情報セキュリティ要件の明確化に基づく対策　　5.1　施設と環境		
	施設及び設備の導入並びにインシデント発生に当たっては、情報セキュリティレベルを保つためのチェック機能を働かせるため、情報セキュリティ責任者ではなく、統括情報セキュリティ責任者及び最高情報セキュリティ責任者まで報告すべきである。	政府機関統一基準では、対策の内容に応じて判断する者を定めており、ご指摘のことについては情報セキュリティ責任者への報告が相当と考えます。なお、政府機関統一基準では、情報セキュリティ責任者の判断の適正性を確保するための仕組みとして、自己点検や監査（2.3.1及び2.3.2)が設けられております。
4.1.1　主体認証		
(1)(c)	例えば、「盗聴に対する対策を行うこと」として、広く暗号化も含めた対策とすべきである。	本遵守事項は主体認証情報を秘密にする必要がある場合にそのための措置を採ることを求めるものです。特に主体認証情報の保存及び通信を行う場合には、秘密にする方法として暗号化が広く利用されることから、具体的な措置としてこれを求めることとしたものです。
	所有による主体認証を用いる場合において、情報システムに必要な機能を設けるべきである。	項目限定版においては、4.1.1(1)(f)で主体認証情報として知識情報を用いる場合の遵守事項を定めておりますが、これは知識情報が、所有情報又は生体情報と比べ、その管理につき情報システムに適切な管理を設ける必要があると判断されるからです。ご意見の所有による主体認証を用いる場合においては、当該所有情報を有する行政事務従事者において(3)(c)を遵守することでそのセキュリティは担保されるものと考えます。
4.1.2　アクセス制御		
	情報システムに、要保護情報へのアクセスに対する通知機能を設ける。	通知機能については、「要保護情報へのアクセス」のみならず、本来は広範なセキュリティイベントを対象とすべきと考えます。これについては、項目限定版4.1.4(1)(g)で定めているところです。 ※　全体版初版4.1.4(1)(g)参照
4.1.3　権限管理		
(1)(d)	主体認証情報の再発行を自動で行うことは、望ましくない。	本遵守事項については、「解説」に記載のとおり、情報システムの利用を開始している主体が、主体認証情報の再発行を要求した場合に、当該情報システムにおいて、その主体により重要な情報が既に作成されている可能性があることから、再発行する主体認証情報を他の者が知り得ないようするため、新規に主体認証情報を発行する場合に比べて、一層安全な機能を設けることを求めるものです。
(2)(h)	情報システムに、アクセスを許された範囲以外のアクセスについて即座に注意を与える機能を設ける。	ご指摘の機能については、情報セキュリティ上有効なものの１つであると考えますが、現状の対策状況等を勘案し、遵守事項とするかどうかを検討してまいります。
4.1.4　証跡管理		
(1)	サーバのみならず、クライアントにおいても証跡管理を行うべきである。	本項では情報システムについて証跡管理を行うことを求めており、クライアントＰＣも対象に含めております。取り扱う情報の重要性等を勘案して、サーバ側及びクライアント側の双方で取得する証跡を選択することとなります。
(1)(g)	セキュリティ侵害の可能性を行った利用者に対して即時に注意を与える機能を情報システムに設けるべきである。	ご指摘の機能については、セキュリティ確保に一定の効果を持つものと考えますが、現状の対策状況等を考慮すると、基本遵守事項とすべきものとは考えていません。
(3)	監視要員等はＩＴ環境でセキュリテイ侵害の可能性及び違反を検知した場合、管理者及び違反者に瞬時に通知する機能を情報システムに設けるべきである。	ご意見の趣旨については、(1)(b)に取り込まれておりますが、明確化するために関連する事項である(1)(g)の「解説」に加えさせていただきました。 ※　全体版初版4.1.4(1)(g)解説参照
(4)(a)	証跡管理に関する利用者への周知を継続的に行うべきである。	最低１年に１回以上の受講が義務付けられている情報セキュリティ対策の教育においても周知されることが想定されます。
4.1.6　暗号と電子署名		
	超長期間保存（保存年限2039年以降）を考慮した項目も追加すべきである。	超長期保存については、現状では暗号化技術等の制約があり技術的に方法論が確立していませんが、標準化の作業が進んでいるところですので、その推移を勘案し、今後検討してまいります。なお、いわゆる2038年問題については、セキュリティに限らない問題であり近未来的に抜本的な対策が行われるものと考えます。したがって、情報セキュリティ対策について定める政府機関統一基準ではあえて規定いたしません。

4.2　情報セキュリティについての脅威		
	システムの開発・構築業者とシステム運用業者におけるセキュリティに対する責任分界点及びオープンソースにおいて想定されるセキュリティに対する対策の責任を明確にするための規定を追加すべきである。	システム開発・構築業者とシステム運用者の責任及びオープンソースソフトウェアの利用において外部委託先との責任を明確化することは、外部委託の際の契約で定めることであり、全体版初版6.1.2「外部委託」で責任の明確化を定めております。
5.1.1　電子計算機及び通信回線装置を設置する安全区域		
(3)(g)	「電磁波による情報漏えい」を防止するための基準を制定すべきであり（適正な脅威想定から、過剰防御とならないための測定法を含む「数値基準」）、「建屋等での対策」についても同様の基準を制定すべきである。	政府機関統一基準においては、強化遵守事項（項目限定版(3)(g)、全体版初版(3)(f)）として電磁波による情報漏洩対策を講ずることについて定めており、当該対策には、一般論としては「建屋等での対策」が含まれております。しかしながら、強化遵守事項については、各府省庁において取り扱う情報や情報システム等を勘案し、当該強化遵守事項の必要性の有無を検討の上、これを選択することとされていることから、政府機関統一基準では「数値基準」を設けておりません。なお、各府省庁において具体的な実施手順を策定する際に、高度なセキュリティが求められる重要な情報システムにおいては、具体的な対策方法及び基準の必要性が検討され、その結果を受けて対策が実施されるものと考えます。
5.2.1　電子計算機共通対策		
(3)(a)	「情報を復元が困難な状態にすること」の記述を「情報を復元が極めて困難な状態にすること」に改めるべきである。	情報の復元を困難にすることを求めており、「極めて」を入れた場合の差異が明確ではないことから、現状の表現で適切と考えます。
5.2.2　端末		
(1)(a)	「インストールしてもよいソフトウェア」の限定列挙を原則とすべきである。	「インストールしてはならないソフトウェアを定める方法」については、解説において「インストールしてはならないソフトウェアを列挙する方法、インストールしてよいソフトウェアを列挙する方法及びその両者を列挙する方法」があると説明しておりますが、ご意見を参考に、「利用してよいソフトウェアの列挙」を標準的な方法として両者を明記しました。 ※　全体版初版5.2.2(1)(a)参照
(1)(d)	パスワード等によるいわゆるロック機能（あるいは端末への主体認証）について規定すべきである。	ご意見のとおり、端末においても、主体認証を実施することは情報セキュリティ対策として重要と考えます。これについては、項目限定版4.1.1において遵守事項を定めております。 ※　全体版初版4.1.1参照
	私物パソコンの業務利用を防ぐため、予算確保も含めた防止策を義務付けるべきである。	私物パソコンの取扱いについては、項目限定版6.1.3において遵守事項を定めております。 ※　全体版初版6.2.2参照
	端末における対策を考慮するに当たり、携帯電話等についても明確な規定を設けるべきである。	携帯電話等については、今後の行政事務における利用状況の推移を踏まえ、必要に応じて、対策の検討を行う予定です。
5.3.3　ウェブ		
(2)(b)	「行政事務従事者が閲覧することが可能なホームページを制限し、定期的にその見直しを行うこと」に関しては、基本遵守事項とすべきである。	強化遵守事項については、各府省庁において、その事項の必要性の有無を検討し、必要と認められるときに選択して実施するものであり、ホームページの閲覧制限が必要な情報システムでは、適正な検討の上実施されるものと考えます。
5.4.1　通信回線共通対策		
	「要機密情報を取り扱う情報システムに使用される通信回線装置は、内部に強制アクセス制御などのセキュリティ保護機能を有するものにすること。」との規定を追加すべきである。	ご意見のとおり、強制アクセス制御機能を通信回線装置に設けることは情報セキュリティ対策として重要と考えており、項目限定版4.1.2(1)(d)において遵守事項を定めているところです。 ※　全体版初版4.1.2(1)(d)参照
6.1.2　府省庁外での情報処理の制限　　6.1.3府省庁支給以外の情報システムによる情報処理の制限		
	「府省庁外での情報処理の制限」、「府省庁支給以外の情報システムによる情報処理の制限」において、情報処理実施の許可・不許可の基準を整備すべきである。	ご指摘の基準については、各府省庁で整備されるものと考えております。
その他		
	情報の格付けと対策レベルについて、具体的な指針を提示すべきである。	情報の格付けについては、対策レベルを判断するに当たっての重要な要素の１つですが、これだけですべてを判断することは相当ではないと考えます。

	サイバーセキュリティへの脅威、研究、および知識が急速に進展している状況の中で、この分野において日米両国政府がベストプラクティスを共有することが重要である。 パブリックコメントにおける意見を慎重に査定し、結果的に基準・プロセスの改善につながる提案を取り入れるように奨励する。また、必要に応じてパブリックコメントの期間を延長するよう提言する。 情報システムのセキュリティコントロールを選択・特定するための指導を提供する実施ガイドラインは、新技術に対応できるようにできる限り頻繁に最新化されるべきである。その際は、一般コメント手続きやその他のフィードバック入手方法を含むオープンな作成プロセスを NISCが使うよう強く奨励する。 日本が一般コメント手続きにオープンワークショップと一般ブリーフィングを補足するように提言する。パブリックコメント以外の非公式な意見についても受け入れるよう提言する。情報セキュリティセンターが政府機関統一基準とガイドラインを発表する際は、NIST「(米国)標準技術局」が使っている①既存の自主的な業界基準が使用可能で受け入れられるものであるならば、これを採用するか適合させること、②もしそうでない場合には、自主的な業界基準作成努力に参加して、共通の政府業界基準を作成し、完成した基準を政府で使用する基準として採用するか適合させること、③最後の手段として、NISCの権限と内部の資源を使って各省庁向けの基準とガイドラインを作成することを検討すべきである。ガイドラインを作成すること、を検討すべきである。情報セキュリティ全要件ができる限り技術的に中立であることを奨励する。情報技術やサービスの調達は、国内海外の全ベンダーにとって公正かつ透明であるべきである。	ご意見をいただきありがとうございます。 情報セキュリティセンターでは、国内外の情報セキュリティ対策や最新の技術動向等に関して、引き続き調査・研究を行っていくこととしております。 政府機関統一基準の見直しは、今後毎年行っていく予定であり、その内容は情報セキュリティ政策会議の場を通じて公開されます。また、将来、技術や環境が大きく変わり、政府機関統一基準の構成・適用範囲等を大きく見直す場合には、政策会議の開催にあわせて、改めて広く一般から意見を求めるパブリックコメントを実施することになるものと考えております。 政府機関統一基準において、特定の企業を優先するという方針はありません。
	業務・システム最適化計画の取組みとの連携、及び総務省にて整備されている「業務・システム最適化計画策定指針（第４版）」との記載のすりあわせをすべきである。	ご意見いただきありがとうございます。最適化計画の取組みと引き続き連携を図っていく予定です。
	セキュリティ対策の強度（レベル）と対策費用に関する指標を策定すべきである。	ご意見いただきありがとうございます。ご指摘の点につきましては、今後十分な検討が必要であると考えます。