「政府機関の情報セキュリティ対策のための統一管理基準」(案)及び「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」(案)に対する意見提出の概要及び御意見に対する考え方

情報セキュリティ政策会議
平成23年４月21日

	基準	該当箇所	ご意見の概要	ご意見に対する考え方
1	統一管理基準	1.1.1.5 用語定義 【た】 「端末」	本項では、「端末」の具体例としてPCおよびPDAと明記しているが、PC以外の電子計算機の具体例として「携帯電話・スマートフォン」も併記するべきである。 （株式会社日立製作所）	現時点では携帯端末とPCとでは機能上の差があることから、管理策として同一にすることは時期尚早であると考えます。つきましては、今後の携帯端末の技術動向を踏まえ、次回以降の改定において検討したいと考えています。
2	統一管理基準	1.2.1.1 組織・体制の整備	定義されている８つの役職の全体構成（階層を含む）が示された図があれば理解が容易になると考える。 （日本ユニシス株式会社）	御指摘については、「政府機関の情報セキュリティ対策のための統一管理基準」（以下、政府機関統一管理基準という。）解説書の「A.1 解説書別添資料」の「A.1.1 組織・体制イメージ図」で既に示しているところです。
3	統一管理基準	1.2.1.1 組織・体制の整備	同項にて定義されている８つの各役職者あるいは会議体の職務定義が明示されていない。各役職者あるいは会議体が何に対して責任を持つのかについて定義する必要があると考える。 （日本ユニシス株式会社）	御指摘については、各遵守事項で規定した主体が当該遵守事項の実施に対して責任を持つこととなっており、組織・体制における責任の所在は明確化されているものと考えています。 なお、各主体別の遵守事項は、政府機関統一基準適用個別マニュアル群の「DM2-01 政府機関統一基準で定める責任者等の役割から見た遵守事項一覧」（http://www.nisc.go.jp/active/general/kijun_man_index.htm）を参考にしてください。
4	統一管理基準	1.2.2.1 情報セキュリティ対策の教育 (1)(a)	情報セキュリティ対策の効果的な実施には主体となる「人」の行動が重要である。規則や体制、個別の対策などを、統一基準として整備することに加えて、それらを素直に守るという風土作りが欠かせないと考える。たとえ失敗したとしても、その後の正直な行為をとった場合には寛容の精神で接し、悪事や不正直な行為には厳しく対処するという普遍的な考え方を示すことで、だれもが納得して守る基準にできると考える。 ついては、該当箇所に以下を追記することを提案する。 「受講者である行政事務従事者には、障害や事故を引き起こした場合であっても、速やかな報告を行うなどの正直な行動を称えるものとする。意図的な違反行為や障害・事故の隠蔽行為などの悪しき行動には厳しく対処することを周知する。」 （株式会社テプコシステムズ）	御指摘については理解できるものの、リスクマネジメントを含む個別の組織管理に委ねられている事項であ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。
5	統一管理基準	1.2.2.1 情報セキュリティ対策の教育	組織としての理解度、定着度、浸透度をどのように評価し、改善するのか、誰が、どのように振舞うのかについての定義が必要と考える。 （日本ユニシス株式会社）	御指摘については、政府機関統一管理基準の「1.1.1.4 評価の方法」で示しているとおり、「それぞれの府省庁にて情報セキュリティ報告書を作成し、自組織の情報セキュリティ対策の取組状況を公表する」こととなっており、当該報告書の審議等の中で、評価・改善を行っていくこととなっています。
6	統一管理基準	1.2.2.2 障害・事故等の対処 (1)(a)	情報セキュリティに関する障害・事故等（インシデント及び故障を含む）とありますが、具体的な例示を別紙にでも掲載しておく必要があると考える。 （日本ユニシス株式会社）	御指摘については、政府機関統一管理基準解説書の「1.2.2.2 障害・事故等の対処」(1)(a)解説に、「情報セキュリティに関する障害・事故等とは、機密性、完全性、可用性が侵害されるものを対象としており、可用性等に影響を及ぼさない程度の故障等は対象としていない。また、「インシデント」とは、JIS Q 27002:2006（ISO/IEC 17799:2005）における情報セキュリティインシデントと同意である。」と既に明記しています。
7	統一管理基準	1.2.2.2 障害・事故等の対処 (3)	情報処理技術は最も変化が激しい分野のひとつであり、障害や事故はあるものと考えなければならず、それは同時多発的に発生してしまう可能性が高い。これを踏まえて、障害や事故などの情報を全府省庁で共有して、速やかで、漏れのない防止対策の実施および注意の喚起を可能とすることを目指す必要がある。また、共有化した事例は、傾向を把握することによって、さらなる改善活動の貴重な資源になると考える。 ついては、該当箇所に以下を追記することを提案する。 「(c)各府省庁で発生した障害や事故は重大でないものも含めて「障害・事故情報およびヒヤリハット事例」として全府省庁で共有し、再発防止や意識向上などの改善活動の情報源として活用する。なお、共有に際しては、個人名を伏せるなどの配慮を行うこと。」 （株式会社テプコシステムズ）	政府機関統一管理基準で定める「障害・事故等」については、当該統一管理基準の「1.1.1.4 評価の方法」で示しているとおり、「それぞれの府省庁にて情報セキュリティ報告書を作成し、自組織の情報セキュリティ対策の取組状況を公表する」こととなっており、当該報告書の審議等の中で、各府省庁で発生し、公表した事案の概要や再発防止策等について全府省庁で共有することとなっています。
8	統一管理基準	1.3.1.3 情報の保存 (1)(e)	電磁的記録の真正性を講じる手段として、技術（標準規格）・運用・制度面で既に整備されているタイムスタンプも併記すべきと考えることから、「(e) ・・・場合には、電子署名やタイムスタンプの付与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、情報に電子署名やタイムスタンプを付与すること。」と修正願いたい。 （財団法人日本データ通信協会タイムビジネス協議会）	御指摘の「電磁的記録の真正性を講じる手段」については、政府機関の情報システム基盤の整備状況を踏まえ、「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」」（以下、政府機関統一技術基準という。）の「2.2.1.5 保証のための機能」の位置付けとし、2.2.1.5(1)(a)の解説に記載しております。したがって、原案のとおりとさせていただきます。
9	統一管理基準	1.3.1.4 情報の移送 (5)(c)	要保全情報の完全性を担保する予防措置として、その時点で処理を施すことの重要性を具体的に紹介すべきと考える。電子署名とタイムスタンプを併用することで、電子署名の有効期限を越えて利活用する場合や電子署名の暗号アルゴリズム危殆化等の際にも、電子データの完全性を将来にわたって担保できるため、電子署名の表示のみでなくタイムスタンプを利用した長期署名を利用することを推奨いただきたい。 （財団法人日本データ通信協会タイムビジネス協議会）	御指摘の「タイムスタンプ」については、政府機関の情報システム基盤の整備状況を踏まえ、政府機関統一技術基準の「2.2.1.5 保証のための機能」の位置付けとし、2.2.1.5(1)(a)の解説に記載しており、今後の政策の推進に当たっての参考とさせていただきます。

	基準	該当箇所	ご意見の概要	ご意見に対する考え方
10	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)(b)	やり取りする情報の機密性などを考慮した上で「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」に則ることとしてはどうか。 （富士通株式会社）	御指摘については、「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」（2010年（平成22年）8月31日　各府省情報化統括責任者（CIO）連絡会議決定）の中で、具体的な条件として明確化しています。つまり、当該ガイドラインにおいて、対象となる電子手続を定めた上で、情報の機密性等を勘案したリスク評価手法とこの手法により導出される「リスクの影響度」、影響度に応じた認証方式の「保証レベル」の導出、各保証レベルに求められる対策基準を規定しています。また、当該ガイドラインについては、政府機関統一管理基準解説書の別添資料「A.1.3 情報セキュリティ対策に関する政府決定等」に明記しており、「1.1.1.1(3)法令等の遵守」において遵守することを求めています。
11	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)	新バージョンに対する条件の再考察（旧バージョンで取得している製品への条件を緩和するなど）を図ってはどうか。 （富士通株式会社）	御指摘については、経済産業省が策定している「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」の以下に記載されているとおり、最新のバージョンでCC 認証が取得されていない製品にも考慮しているところです。 「特定の製品分野において、個別の製品に一連のバージョンの製品のうち、過去に認証取得製品が存在するが最新のバージョンでCC 認証が取得されていない製品について、以下の方法により、実質的にCC 認証取得製品とセキュリティ機能上同等であると確認されている場合は、採用対象とすることも可能とする。 １）過去の認証取得製品の後継製品について、CCRA 参加国の認証機関において保証継続の認証を受けている製品 ２）過去の認証取得製品の後継製品について、メンテナンス型バージョンアップが行われたことをIPA において確認済みの製品」
12	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)	当該解説では、国際承認アレンジメント（CCRA）以外の日本独自の「メンテナンス型バージョンアップ」などについて記載がないため、該当箇所に記載されている「なお、国際承認アレンジメント（CCRA）参加国におけるISO/IEC 15408 に基づく認証取得製品について活用することが考えられる。」の一文は削除するか、あるいは、「なお、国際承認アレンジメント（CCRA）参加国におけるISO/IEC 15408 に基づく認証取得製品等を活用することが考えられる。」のように「等」を入れるべきと考える。 （株式会社日立製作所）	御指摘については、経済産業省が策定している「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」の以下に記載されているとおり、最新のバージョンでCC 認証が取得されていない製品にも考慮しているところです。 「特定の製品分野において、個別の製品に一連のバージョンの製品のうち、過去に認証取得製品が存在するが最新のバージョンでCC 認証が取得されていない製品について、以下の方法により、実質的にCC 認証取得製品とセキュリティ機能上同等であると確認されている場合は、採用対象とすることも可能とする。 １）過去の認証取得製品の後継製品について、CCRA 参加国の認証機関において保証継続の認証を受けている製品 ２）過去の認証取得製品の後継製品について、メンテナンス型バージョンアップが行われたことをIPA において確認済みの製品」
13		1.5.1.1 情報システムのセキュリティ要件(1)(d)	ISO/IEC15408認証要件を強化するのであれば、認証取得にかかる企業の負担を軽減する施策の検討が必要である。また、記載内容にある「要求するセキュリティ機能」及び「要求する評価保証レベル」については、補足説明が必要である。 （日本電気株式会社）	御指摘の「認証取得にかかる企業の負担を軽減する施策」については、経済産業省にて、ニーズを踏まえ、政府機関で要求する共通的なプロテクションプロファイルの策定・公開などにより、認証取得を促進することを検討中です。 また、御指摘の「セキュリティ機能」及び「評価保証レベル」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」にて記載しています。
14	統一管理基準	1.5.2.1 情報システムに係る文書及び台帳整備 (2)(a)(ケ)	契約事業者の連絡先を把握することにより、事業者との連絡を密にし、事故等を防止するため、「契約事業者」を「契約事業者の氏名又は名称・連絡先」に修正するべきと考える。 （個人）	御指摘については、「契約事業者の連絡先」は、各情報システムの個別の実情にあわせて整備するものであり、1.5.2.1(1)(a)(エ)「障害・事故等が発生した際の対処手順」で整備される「障害・事故等の内容・影響度の大きさに応じた情報連絡先のリスト」に含めるものと考えるため、原案のとおりとさせていただきます。
15	統一管理基準	1.5.2.2 機器等の購入	「1.5.2.2　機器等の購入」では「機器等」と書かれており、「ソフトウェア」を含むのかが曖昧であることから、1.5.2.2の表題を「機器等の購入」から「機器及びソフトウェアの購入」とするか、または解説にて「機器等」の意味を明確にするべきと考える。 （株式会社日立製作所）	「機器等」については、政府機関統一管理基準の「1.1.1.5 用語定義」において、「情報機器等及びソフトウェアをいう」と規定してあることから、原案のとおりとさせていただきます。
16	統一管理基準	1.5.2.5 暗号と電子署名の標準手順 (1)	鍵の生成、廃棄、更新といったフェーズに利用者が関与する場合((b)(ア)のとおり)と、関与しない場合の2つを考慮し、記述する必要があると考える。後者の場合を追記し、鍵の入手方法や入手手順といった観点から記述が必要である。 （財団法人日本情報処理開発協会）	鍵管理の手順の具体化に当たっては、御指摘のとおり（御指摘の点を含め）様々な観点による整理が可能と考えられます。したがって、本遵守事項においては各府省庁共通の手順を示し、具体的な整理方法については実務を行う各府省庁に委ねる整理としていることから、原案のとおりとさせていただきます。
17	統一管理基準	1.5.2.5 暗号と電子署名の標準手順 (1)(a)(ウ)	電子署名の長期有効性を確保し、将来検証を行う場合を想定した長期署名がJIS化され、一般的に利用されていることから、電子署名に関する強化遵守事項には長期署名の記載を入れる事が妥当だと考える。そこで、緊急対応計画の具体的な例示として、「長期署名の利用等緊急対応計画‥‥」と明確に記載いただきたい。 (財団法人日本データ通信協会タイムビジネス協議会)	緊急対応計画の策定にあたっては多岐にわたる対策の検討が必要であることから、一部の具体例のみの不完全な例示はむしろ避け、本遵守事項では緊急対応計画の策定を求める内容のみに絞り込んでおります。したがって、原案のとおりとさせていただきます。
18	統一管理基準	1.5.2.5 暗号と電子署名の標準手順 (1)(c)	バックアップは、一般的に利用者が鍵の誤消去等の対策として積極的に実施すべきことであるが、預託は、本来本人のみが所有・管理し復号や電子署名時に使用する鍵を、第三者やシステムに預ける行為である。したがって、鍵のバックアップと預託を一括りにして、「鍵のバックアップ手順等」としてしまうのは誤りである。預託に関する記述は削除すべきである。 （財団法人日本情報処理開発協会）	御指摘については、本遵守事項の解説に「信頼できる第三者へ鍵情報を預託する等」と記載しており、「暗号化された情報の復号に用いる鍵の紛失及び消失」のリスクを軽減するための対策としては、鍵のバックアップ及び鍵の預託はいずれも一定の効果が期待できることから、原案のとおりとさせていただきます。
19	統一管理基準	1.5.2.5 暗号と電子署名の標準手順 (1)(d)	政府認証基盤（GPKI）は該当の電子署名を使用することで政府が提供するサーバであるという証明を行うことが主たる目的であると認識していることから、成りすましの可能性が低いと考えられるイントラネットや運用管理で利用するような電子署名についてはGPKIを必須としないような文言に修正願いたい。 （富士通株式会社）	本遵守事項は「電子署名の目的に合致し、かつ適用可能な電子証明書」とあるとおり、必ずしも政府認証基盤（GPKI）が発行する電子証明書の利用のみを強制するものではなく、御指摘の問題は生じないことから、原案のとおりとさせていただきます。
20	統一管理基準	1.5.2.5 暗号と電子署名の標準手順 (1)(d)	電子署名の長期有効性を確保し、将来検証を行う場合を想定した長期署名がJIS化され、一般的に利用されていることから、電子署名に関する強化遵守事項には長期署名の記載を入れる事が妥当だと考える。そこで、本項目に「電子署名の有効性確保のために長期署名を利用する場合には、財団法人日本データ通信協会が認定したタイムスタンプを利用すること。」を追記いただきたい。 （財団法人日本データ通信協会タイムビジネス協議会）	御指摘の「タイムスタンプを利用すること」については、政府機関の情報システム基盤の整備状況を踏まえ、政府機関統一技術基準の「2.2.1.5 保証のための機能」の位置付けとし、2.2.1.5(1)(a)の解説に記載しております。したがって、原案のとおりとさせていただきます。

	基準	該当箇所	ご意見の概要	ご意見に対する考え方
21	統一技術基準	目次-1	2.1.1.1 (1)が改行によって頁の記述が左側に寄せられてるため、他の行と同じ位置に表示願いたい。 （日本ユニシス株式会社）	御指摘のとおり、修正します。
22	統一技術基準	第2.1部	統一技術基準で初出の用語も「政府機関の情報セキュリティ対策のための統一管理基準」に纏め、第2.1部総則では、ひとこと「政府機関の情報セキュリティ対策のための統一管理基準に準ずる」としていただきたい。 もし今の形式を取るのであれば、「統一管理基準に準ずる」は、正式名称の「政府機関の情報セキュリティ対策のための統一管理基準に準ずる」としていただきたい。 （日本ユニシス株式会社）	見直しを行う場合の利便性の観点から、原案の形式としますが、御指摘を踏まえ、冒頭の「統一管理基準に準ずる。」という記述については、「政府機関の情報セキュリティ対策のための統一管理基準（以下「統一管理基準」という。）に準じる。」と改めます。
23	統一技術基準	2.1.1.5 用語定義【ま】 「モバイルPC」	モバイルで利用する機器は、PC以外にも携帯電話、スマートフォンなども含まれると考えることから、「モバイルPC」を「モバイル端末」に修正願いたい。 （株式会社日立製作所）	現時点では携帯端末とPCとでは機能上の差があることから、管理策として同一にすることは時期尚早であると考えます。つきましては、前述のとおり、「端末」の定義においても、今後の携帯端末の技術動向を踏まえ、次回以降の改定において検討したいと考えていることから、原案のとおりとさせていただきます。
24	統一技術基準	第2.2部	主体認証やアクセス制御機能など、統一管理基準と統一技術基準の双方に出てくる項目について、それぞれどのような立場、視点から記述しているのかの説明を追記し、関係がわかるようにしていただきたい。 （日本ユニシス株式会社）	政府機関統一管理基準においては情報システムを所管する責任者に対して主体認証やアクセス制御等の機能の適切な導入を求める遵守事項を定め、一方、政府機関統一技術基準においては情報システムに導入する当該機能の技術的な対策基準を規定しております。また、このような関係については、政府機関統一管理基準の1.4.1.1節及び1.5.2.4節の趣旨並びに政府機関統一技術基準の2.2.1.1～2.2.1.5節の趣旨にも、それぞれ記載されていることから、原案のとおりとさせていただきます。
25	統一技術基準	2.2.1.4 証跡管理機能 (1)	証跡についての項目に、何のための証跡であるか、その目的達成のためにはどのような証跡をどこまで取る必要があるかを記述していただきたい。 （日本ユニシス株式会社）	証跡管理機能については今回の改定により、政府機関統一技術基準の「2.2.1.4 証跡管理機能」及び政府機関統一管理基準の「1.5.2.4主体認証・アクセス制御・権限管理・証跡管理・保証等の標準手順」(1)(エ）解説書に分けて記載しています。そのため、御指摘については含まれていると考え、原案のとおりとさせていただきます。 なお、証跡管理を行う必要性の有無の判断に当たっては、情報システムの側面だけではなく、組織的な側面からの検討も必要であるため、情報セキュリティ責任者によるものとしています。
26	統一技術基準	2.2.1.4 証跡管理機能(1),(2)	当該記載にある「判断する」と他の遵守事項で記載されている「認めた」を異なる表現にすると、解釈を誤る可能性があるため、表現の統一が必要である。そこで、「情報セキュリティ責任者が判断した」を「情報セキュリティ責任者が認めた」と変更するか、 「2.2.1.2 アクセス制御機能」などに記載されている「～必要があると認めた」を「～必要があると判断した」と変更すべきである。 （株式会社日立製作所）	御指摘を踏まえ、以下のとおり修正します。 政府機関統一技術基準　2.2.1.4(1)(a)(b)(c)(d)、(2)(a)(b)(c)　（計7か所） 修正前「証跡を取得する必要があると情報セキュリティ責任者が判断した情報システム」→ 修正後「証跡を取得する必要があると情報セキュリティ責任者が認めた情報システム」
27	統一技術基準	2.2.1.6 暗号と電子署名（鍵管理を含む） (1)(e)	電子署名を付与又は検証を行う必要があると認めた情報システムで、タイムスタンプを活用した長期署名方式のシステムによる電子署名の保護機能を先ず充実させることがアルゴリズム危殆化の対策として有効となることを明示いただきたい。 （財団法人日本データ通信協会タイムビジネス協議会）	御指摘の「タイムスタンプ」については、政府機関の情報システム基盤の整備状況を踏まえ、政府機関統一技術基準の「2.2.1.5 保証のための機能」の位置付けとし、2.2.1.5(1)(a)の解説に記載しており、今後の政策の推進に当たっての参考とさせていただきます。
28	統一技術基準	2.2.1.6 暗号と電子署名（鍵管理を含む） (1)(f)	「統一管理基準」及び「統一技術基準」の記述の整合性をはかるため、「統一管理基準」に準じ、(f)に以下の内容を追記願いたい。『当該複数のアルゴリズムに、少なくとも一つは電子政府推奨暗号リストに記載されたものを含めること。』 （財団法人日本情報処理開発協会）	御指摘については、本遵守事項では「複数のアルゴリズムを選択可能とすること」を規定しており、選択可能なアルゴリズムについては、政府機関統一管理基準の1.5.2.5(1)(a)で規定するように整理させていただいているため、原案どおりとさせていただきます。 なお、政府機関統一技術基準の運用に当たっては、あらかじめ政府機関統一管理基準を理解し、適切に参照する必要がある旨、別途周知させていただきます。
29	統一技術基準	2.2.1.6 暗号と電子署名（鍵管理を含む） (2)	電子データの完全性を担保する予防措置として、その時点で処理を施すことの重要性を具体的に紹介すべきと考える。電子署名とタイムスタンプを併用することで、電子データの完全性を将来にわたって担保できるため、電子署名の正当性を検証するための情報又は手段として利用出来ることを明記いただきたい。 （財団法人日本データ通信協会タイムビジネス協議会）	御指摘の「タイムスタンプ」については、政府機関の情報システム基盤の整備状況を踏まえ、政府機関統一技術基準の「2.2.1.5 保証のための機能」の位置付けとし、2.2.1.5(1)(a)の解説に記載しており、今後の政策の推進に当たっての参考とさせていただきます。
30	統一技術基準	2.2.2.1 セキュリティホール対策 (1)(b)	「電子計算機及び通信回線装置上で採り得る対策」の記述に具体性がないため、ワークアラウンド、ファイアウォールの設定、あるいはサーバのポート設定などより具体的に記述していただきたい。 （日本ユニシス株式会社）	電子計算機及び通信回線装置上で採り得る対策については、政府機関統一技術基準の第2.3部「2.3.2 電子計算機」以降の規定において記述していることから、原案のとおりとさせていただきます。
31	統一技術基準	2.2.2.2 不正プログラム対策 (1)(c)	原文では複数の種類のアンチウイルスソフトウェア等と、明記されているが、単に異なるベンダーのアンチウィルスを組み合わせても、重複検査に留まる可能性が高い。したがって、シグネチャーベースのパターンマッチング方式（最も一般的な検査手法）と動作解析方式（ヒューリスティック検査手法）の組み合わせにより、相補的な検査を提言することが求められることから、「情報システムセキュリティ責任者は、想定される不正プログラムの感染経路において、複数の異なる検査手法のアンチウイルスソフトウェア等を組み合わせ、導入すること。」と修正願いたい。 （サイバートラスト株式会社）	本遵守事項は、アンチウイルスソフト以外の様々な技術を活用した多段的な防御を想定しています。そのため、御指摘のような重複検査に相当するケースは少ないものと考えていることから、原案のとおりとさせていただきます。
32	統一技術基準	2.3.2.2 端末 (1)(e)	盗難後の被害軽減対策として、解説書の具体例では遠隔消去のみ記載されているため、情報の暗号化対策についても例に加えてはどうか。 （富士通株式会社）	モバイルPCが外部の者の手に渡った場合の情報漏えい対策として、暗号化に関する規定が、政府機関統一技術基準の2.3.2.2(1)(d)において記述されていることから、原案のとおりとさせていただきます。

	基準	該当箇所	ご意見の概要	ご意見に対する考え方
33	統一技術基準	2.3.2.3 サーバ装置 (1)(d)	原文では利用が定められたソフトウェアに該当しないソフトウェアをサーバ装置から削除すること明記されているが、これではサーバを保護する要件は満たしているが、サーバの利用者を保護する要件が満たされていない。したがって、サーバの利用者にとってリスクとなるリスクの高いモジュールや設定（プロキシモジュール等）は、それが不要である場合は削除または無効することを提言することが求められることから、「情報システムセキュリティ責任者は、利用が定められたソフトウェアに該当しないソフトウェア、およびモジュールや設定ファイルをサーバ装置から削除もしくは無効化すること。」と修正願いたい。 （サイバートラスト株式会社）	御指摘については、政府機関統一管理基準の「1.1.1.5 用語定義」における「ソフトウェア」の定義の中に含まれていることから、原案のとおりとさせていただきます。
34	統一技術基準	2.3.3.1 電子メール (1)	「電子メールの導入時」だと、電子メール・システムのことか電子メール・クライアントのことかがわからないため、「電子メールの導入時」は「電子メール・システムの導入時」と変更していただきたい。 （日本ユニシス株式会社）	システムとクライアント、両方の概念が含まれているため、原案のとおりとさせていただきます。
35	統一技術基準	2.3.3.2 ウェブ (1)	ウェブサーバについての記述において、イントラ用のサーバの場合と外部情報発信用のサーバの場合を区別し、DMZやプロクシ構成などセキュリティ設計の違いを追記していていただきたい。 （日本ユニシス株式会社）	御指摘の情報システムごとの「セキュリティ設計の違い」については、取り扱う情報及び構築するサーバの特性を考慮して、情報システムを所管する各府省庁が構築時に検討する事項と考え、原案のとおりとさせていただきます。
36	統一技術基準	2.3.3.2 ウェブ (1)(エ)	原文では情報漏洩防止機能のみが提言されているが、万一情報漏洩が発生した場合の、フォレンジック対策として、WEBログ、DBログを保存し、トレーサビリティ確保に努めるよう提言することが求められることから、「通信時の盗聴による情報漏えいのリスクを検討し、必要と判断した場合には、暗号化と電子証明書による認証の機能、通信ログの保存機能を設けること。」と修正願いたい。 （サイバートラスト株式会社）	御指摘については、政府機関統一技術基準の「2.2.1 情報セキュリティについての機能」で整理し、「2.2.1.4 証跡管理機能」に含まれると考えています。
37	統一技術基準	2.3.3.2 ウェブ (2)(オ)	原文では入出力の不正防止のみが提言されているが、「年齢認証画面」や「同意・不同意確認画面」を飛ばして、本来認証および承認プロセスを経なければ表示されるべきでない画面を、ダイレクトに表示することを防止しすることにより、“ワンクリック詐欺等”に悪用されることを防止するよう提言することが求められることから、「不正な出力データ、および不正な画面遷移を排除すること。」と修正願いたい。 （サイバートラスト株式会社）	御指摘については、政府機関統一技術基準の「2.3.3.2 ウェブ」(2)(イ)の「主体認証と情報へのアクセス制御を適切に行うこと。」に含まれると考えています。
38	統一技術基準	2.3.3.2 ウェブ (2)	ウェブアプリケーション開発において、SQLインジェクションやクロスサイトスクリプティングが発生するようなソフトウェアの作りこみを防止するためには、コーディングを行なった者以外の有識者によるコードレビューが有効である。 そのため、強化遵守事項として「(c)個人の判断による脆弱性作りこみを防止するため、コーディングした者以外による、コードレビューを行なうことが必要と思われる。」と追加願いたい。 （株式会社日立製作所）	御指摘については、政府機関統一管理基準「1.5.2.3 ソフトウェア開発」で整理し、同(1)(a)(シ) に含まれると考えています。
39	統一技術基準	2.3.3.2 ウェブ (3)(a)	(a) ウェブクライアントのセキュリティ設定については、WEBブラウザ設定、SSLチケット、パスワード管理など具体的な記述を追記していただきたい。 （日本ユニシス株式会社）	政府機関統一基準群では、それぞれの府省庁が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めています。 御指摘については、システムの業務運用に沿って、必要に応じて、各府省庁にて実施手順書を整備することが効果的と考えており、原案のとおりとさせていただきます。
40	統一技術基準	2.3.3.2 ウェブ (3)(c)(イ)	原文では送信先の誤設定の防止のみが提言されているが、送信先の改ざんを防止することにより、“フィッシング詐欺等”を防止するよう提言することが求められることから、「当該ウェブサイトが送信先として想定している組織以外のものに改ざんできないこと。」と修正願いたい。 （サイバートラスト株式会社）	ここではウェブクライアント側の遵守事項を記載しており、送信先のウェブサイトが想定している組織のものであるかを、ウェブサーバの電子証明書の内容から確認することを求めています。また、ウェブサーバ側の改ざんについては(1)(a)(イ)に含まれると考えます。
41	統一技術基準	2.3.3.2 ウェブ(3)	導入・開発時には発見されたかったソフトウェア、開発アプリケーションの脆弱性を突いた攻撃を未然に防ぐためには、定期的な脆弱性診断の実施と、実施結果に対する対策が必要となる。脆弱性診断は、定期的な実施により効果を発揮する事から、運用プログラムの中に予め組み込む必要と考えるため、強化遵守事項として、「(b)新しい脆弱性による攻撃を未然に防ぐため、定期的な脆弱性診断(ペネトレーションテスト、Webアプリケーション診断、など)の実施計画を組み込む事が必要と思われる。」と追記願いたい。 （株式会社日立製作所）	ご指摘の脆弱性検査につきましては、想定されるすべての脆弱性に対応することは困難であると考えています。他方、こういった脆弱性によるリスクを低減するために、今年度、内閣官房において政府機関の公開ウェブサーバをサンプル抽出し、第三者機関による脆弱性検査を実施したところです。その上で、各府省庁に対しても、政府政府機関統一管理基準の「1.2.3.2 情報セキュリティ対策の監査」(5)(d)解説で示しているとおり、情報セキュリティ対策の妥当性の確認の具体的方法として脆弱性検査の実施を提示しているところであることから、原案のとおりとさせていただきます。
42	統一技術基準	-	セキュリティを働かせる対象が特定されていないことがあり、また対策技術も具体性を欠いているため、わかりにくい。そこで、サーバ運用管理、ネットワーク管理、クライアント利用者の運用管理などの記述において、セキュリティを働かせる対象を特定し、また対策技術も具体的に記述していただきたい。 （日本ユニシス株式会社）	政府機関統一基準群では、それぞれの府省庁が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めています。 御指摘については、システムの業務運用に沿って、必要に応じて、各府省庁にて実施手順書を整備することが効果的と考えており、原案のとおりとさせていただきます。

意見提出者一覧（五十音順）

（業界団体関係）
財団法人日本情報処理開発協会
財団法人日本データ通信協会タイムビジネス協議会

（システム製造・販売関係）
株式会社日立製作所
日本電気株式会社
富士通株式会社
日本ユニシス株式会社

（システム販売関係）
株式会社テプコシステムズ

（電子証明関係）
サイバートラスト株式会社

その他個人１件