資料１－２

「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（案）

情報セキュリティ対策推進会議

平成　　年　　月　　日

連番	統一技術基準 該当箇所	ご意見の概要	ご意見に対する考え方
1	2.2.1.1 主体認証機能	「情報システムセキュリティ責任者」と「情報システムセキュリティ管理者」の業務分担の違いを明確にして頂きたい。 （理由） 2.2.1.1(1)(b)で「～管理者」に通信経路上の暗号化を求めている規定があり、「～責任者」が設けることとの違いが不明なため。	ご指摘の点については、情報システムに機能を設けることについては、情報システムセキュリティ責任者が担うこととしており、実際の作業を伴う管理に関する遵守事項については、情報システムセキュリティ管理者が担うこととしております。
2	2.2.1.1 主体認証機能 (1) (f) (ウ)	「容易に」を削除、または「本人の同意なく」にして頂きたい。 （理由） （代理の防止）目的の記述ですが、容易性を残すこと自体が防止に沿わないと思います。防止や抑止の観点で「本人の同意」を要件化することで運用の柔軟性が保てると思います。	ご指摘の点については、最低限の水準を設ける観点から、原案のとおりとさせていただきます。
3	2.2.1.1 主体認証機能 (1) (g) (ウ)	「又は」は削除して頂きたい。 （理由） 「検知し、又は防止する」というORの関係は「防止」が必須ではないと読めます。「検知と防止を行う」と要件を両立させるほうがセキュアになります。	ご指摘の点については、「又は」以降が必須でないという意味ではなく、本事項では、「検知」又は「防止」機能を設ける必要があると認めた情報システムについて、「検知」又は「防止」のどちらかについては最低限導入し、又は両方導入することを求めています。
4	2.2.1.1 主体認証機能 (1) (g) (オ)	再設定の禁止は「一定期間の間」にとどめて頂きたい。 （理由） 同じ主体認証情報は二度と利用出来ないように読めます。利用者が利用継続した際、将来的に数十～百の主体認証情報を作り続けることになります。120日以内の再設定禁止など利用者負荷と運用面を考慮したほうが良いと思います。	ご指摘の点については、当該遵守事項の主旨を踏まえ、原案のとおりとさせていただきます。
5	2.2.1.3 権限管理機能 (1) (b) (ア)	「最少」は「最小」の誤記と思われます。 （理由） 同上	ご指摘の点については、「least privilege」の和訳として「最少特権」を使用しており、原案のとおりとさせていただきます。 （参考：「電子政府におけるセキュリティに配慮したOSを活用した情報システム等に関する 調査研究報告」（内閣官房情報セキュリティセンター、平成16年度） http://www.nisc.go.jp/inquiry/pdf/secure_os_2004.pdf
6	2.2.1.3 権限管理機能 (2)	「～点検すること」と記述された全てに対し「承認プロセスの考慮」 を追加で明示して頂きたい。 （理由） 点検した結果が、承認処理によって評価されない場合、点検の正当性が担保されず、また作業のモレが発生するリスクがあります。	ご指摘の点については、当該遵守事項の運用に係る内容と考えられるため、原案のとおりとさせていただきます。
7	2.2.1.6 暗号と電子署名（鍵管理を含む）(1)(e)(ウ)	原文では暗号化の検証の必要性や認証取得製品の選択について個別に検討する事となっているが、一定の基準を設けてその必要性や製品選択を明示することでセキュリティ安全性を向上させることが期待できる。 そこで「暗号モジュール試験及び認証制度に基づく認証取得製品」を具体的に定めた「認証取得製品分野リスト」を作成してこれを参照するように改めるべきである。 （理由） 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の選択にあたっては、製品分野（暗号製品の分類）や利用環境を踏まえて、製品選択の具体的な考え方や指針を示すことにより安全性を確保するとともに選択基準を明確にすることができる。 同制度と同様な制度である「ITセキュリティ評価及び認証制度」に基づく製品の選択に関しては、統一管理基準1.5. 1.1. (d)にて「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」を参照して認証製品を選択する事を定めている。	ご指摘の点については、解説文内で記載している「暗号モジュール試験及び認証制度」を運用している情報処理推進機構（IPA）のウェブサイト （http://www.ipa.go.jp/security/jcmvp/val.html）において、必要なリストが公開されております。
8	2.2.1.6 暗号と電子署名（鍵管理を含む）(1)(e)(ウ)	解説文では「適切に実装されている」ことについての説明があるが、本文及び解説文ではこの語は見当たらないので訂正すべきである。	ご指摘を踏まえ、次のとおり修正します。 2.2.1.6(1)(e)(ウ) 「選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、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の選択」
9	2.2.2.1 セキュリティホール対策.(1)(a)	セキュリティホールの対策を実施すること。更に、対策が完了していることを定期的に診断し、管理する方法を担保すること。 （理由） セキュリティホールへの対策を実施した場合でも、実際にその対策が有効に働いているかどうか定期的に確認し、状態を管理しない限り、システムの安全性が担保されないため。（一般的なシステム監査においても、定期的な確認が推奨されているため）	ご指摘の点については、既に2.2.2.1(2)(f)において「定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析」することを求めており、原案のとおりとさせていただきます。
10	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上で採り得る対策がある場合は、自動的にシステムの検索をし、脆弱性が見つかった部分にだけセキュリティホール対策を行うなど当該対策を実施すること （理由） 脆弱性を利用する攻撃が多くみられる中、対策を従来の「人」による確認・対応の運用でとどめておくのではなく、自動的に対策を行う技術的対策を積極的に導入するころが、攻撃のトリガーとなりうるセキュリティホール対策について初動を防ぐ上で重要と考えるため。	ご指摘の点については、既に2.2.2.2(1)(d)において同種の対策について記述しており、原案のとおりとさせていただきます。
11	2.2.2.1 セキュリティホール対策.(2).(e)	また、検証期間中、電子計算機及び通信回線装置がそのセキュリティホールを狙った攻撃を防御する方法が検討される場合はその対応を行うこと。 （理由） セキュリティホールの存在を確認、検証を行うも、検証期間中に攻撃を受け感染等のインシデントがおきる事を回避する為、「仮想パッチ技術」等の機能を利用し暫定的な対応が必要と考えるため	ご指摘の点については、2.2.2.1(1)(b)における対策の一例と考えられますが、今後の検討課題とさせていただきます。
12	2.2.2.4 踏み台対策(1)(a)	「対策としては～、アンチウイルスソフトウェア等で検出されない不正プログラムの通信の監視」 （理由） アンチウイルスソフトウェア等で検出されない脅威はボットだけではないため。	ご指摘の点については、当該箇所では「ボットの通信の監視」を求めることを意図しており、原案のとおりとさせていただきます。

連番	統一技術基準 該当箇所	ご意見の概要	ご意見に対する考え方
13	2.2.2.4 踏み台対策及び 2.2.2.5 標的型攻撃対策	「踏み台対策」「標的型攻撃対策」として「(不正に)利用されない防止措置をとる」という規定は実効性が低く、より具体的な対策の記述をして頂きたい。 (理由) 上記2編の遵守事項は、他の遵守事項に比べ、内容の深さ、粒度のバランスが異なるようです(参考資料のk305-111-1C_draft.pdfの解説欄記載内容を本編に組み込めば具体的になると思います)。	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。
14	2.2.2.5 標的型攻撃対策	当該箇所において、標的型攻撃対策に関する記述が追記された点について賛同する。但し、2.2.2.1～4項に記述されている内容と比較して具体策が記述されておらず抽象的な印象を受ける。他項と同等レベルとなるよう具体的な対策並びに運用方法について記述がされることが望ましいと考えます。 (理由) 参考として公開されている「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」解説書(案)には具体的な対策例が明示されているが、「標的型攻撃」において使用される、個別に開発されたマルウェア(以下、モダンマルウェア)に関しては、インターネット上に広く蔓延するウィルスやワームと異なり、標的とされた組織以外に送付されない場合が多く、第三者機関がモダンマルウェアの存在並びに情報及び対策ソフトウェア(シグネチャ等を含む)を入手することは非常に困難である。 　情報セキュリティベンダの中には、世界各国の顧客より提供される検体を豊富に収集し解析することで、モダンマルウェアに関する最新情報を蓄積しているベンダも存在している。 　民間企業からの自発的な情報提供等、情報を幅広く収集し標的型攻撃対策に活用する仕組みを実現して頂きたい。	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。
15	2.2.2.5 標的型攻撃対策(1)(a)	～不正プログラムが侵入した際の挙動を監視し、感染端末を特定するための措置を講ずること等、感染拡大等を防止するための措置を講ずること。 (理由) 感染拡大を防止する措置の具体例として、挙動を監視し端末の特定を行う事で、その後の駆除を確実に行うことが有効と考えられるため。感染原因端末の特定をすることで、今後感染を減らすための対策を行えるようにするため。	ご指摘の点については、2.2.2.5(2)(a)解説 「(ア)通信回線における対策 ・府省庁内通信回線と府省庁外通信回線との間で送受信される通信内容の監視 ・府省庁内通信回線上の電子計算機同市で送受信される通信内容の監視」 における監視に関する措置に含まれてい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。
16	2.2.2.5 標的型攻撃対策 (1).(a)	「(エ)サーバ装置における対策」内に、以下内容を記載。 ・重要な情報を保存しているサーバ装置上でのシステム改ざんを避けるための変更監視の実施 (理由) 標的型攻撃では、不正プログラムがG/Wを超えて内部ネットワークに侵入してしまう確率が通常の攻撃よりも高く、万一侵入を許してまった場合にも、システムを多層防御するために、重要情報を取り扱うサーバ上で一層の対策を講じる必要があると考えるため。ホスト内部での攻撃の挙動を検知するため	ご指摘を踏まえ、以下のとおり修正します。 2.2.2.5(1)(a)解説 「(エ)サーバ装置における対策 ・重要な情報を保存しているサーバ装置へのログイン可能な端末の制限 ・重要な情報を保存しているサーバ装置上のセキュリティ状態の監視 等」
17	2.2.2.5 標的型攻撃対策(2)(a) (ア)	・アンチウイルスソフトウェア等で検出されない不正プログラムの通信の監視等 (理由) アンチウイルスソフトウェア等で検出されない脅威はボットだけではないため。	ご指摘の点については、当該箇所では「ボットの通信の監視」を求めることを意図しており、原案のとおりとさせていただきます。
18	2.3.2.1 電子計算機共通対策 (2)(a)	「例えば、悪意のあるウェブサイトを閲覧することによって、不正プログラムに感染させられてしまうことから回避するため」→「例えば、業務に無関係なウェブサイトを閲覧することによって、業務の効率を下げないようにするため」 (理由) 解説では業務目的外のウェブサイト閲覧による不正プログラムの感染を危惧する内容が記載されているが、悪意のあるウェブサイトの閲覧は、行政事務の遂行の過程においても攻撃者の意図によりアクセスの可能性があるため、解説としては誤っている。	ご指摘の点については、当該遵守事項の目的が業務の効率低下を防止するためではなく、不正プログラムの感染防止を目的としているため、原案のとおりとさせていただきます。
19	2.3.2.1 電子計算機共通対策及び2.3.2.2 端末	従来のPCとともにスマートフォン/スレートPCなどとの整合性も規定に加えて頂きたい。 (理由) 近年、PC以外の端末が急速に利用される傾向にあり、そのための対策(有無を含め)が重要と思います。	ご指摘の点については、従来の「モバイルPC」を「モバイル端末」として、対象範囲に含まれることを明確化するとともに、具体的な対策等については、個別マニュアルを作成していく予定です。
20	2.3.2.2 端末 (1) (b)	「行政事務従事者はモバイル端末を利用する必要がある場合には、情報システムセキュリティ責任者の承認を得ること。」に続けて「なお、情報システムセキュリティ責任者は承認したモバイル端末の記録を取り、管理すること。」を追記して頂きたい。 (理由) 要保護情報の要管理対策区域外への持ち出し許可時に確認の一項目として頂きたい。 (承認行為が、記録を前提としているのであれば、この意見は取り下げます)	ご指摘の点については、1.4.2.1「要管理対策区域外での情報処理の制限」において遵守事項を定義しており、記録の取得については、1.4.2.1(2)(c)で対策を求めています。
21	2.3.2.2 端末(1)	情報システムセキュリティ責任者は行政事務従事者が私有するモバイル端末においても、その端末が情報システムにアクセスをする場合、保護手段が有効に機能するように構成すること。 (理由) 先般よりBYOD(Beyond Your Own Device)の概念が一般化してきており、とりわけモバイル端末については、先進的に取り組みが進んでいるため、セキュリティ上の配慮事項で追記の必要があると考えるため。	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」において定めており、今後の検討課題とさせていただきます。
22	2.3.2.2 端末 (1)(e)	～、行政事務従事者が情報を保存できない端末を用いて情報システムを構築する必要性の有無を検討し、必要と認めた時は当該措置を講ずること。あわせて、セキュリティについても情報を保存できない端末の特性に合わせた措置を講ずること。 (理由) 新クライアント等の方式を利用する場合、全てサーバへ蓄積される事から、セキュリティについても従来端末とは異なるセキュリティ措置が必要になると考えます。	ご指摘の点については、端末の特性も考慮して必要性の有無を検討することを求めており、原案のとおりとさせていただきます。

連番	統一技術基準 該当箇所	ご意見の概要	ご意見に対する考え方
23	2.3.3 アプリケーションソフトウェア	「2.3.3.4　リレーショナル・データベース」の項目追加 （理由） 「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」で定める要件を実現するためには、要機密情報を格納するための直接的な要素技術であるリレーショナル・データベース（RDBMS：以下同じ）をはじめとするデータベースシステムの項目を明示的に追加すべきである。 過去、国内外における機密情報に関する大規模な漏えい事件においては、その多くで当該機密情報がRDBMS内部に格納されていたことは明らかであり、個人情報等の構造化された大量の機密情報は、今後も引き続きRDBMS内で保管・管理されると考えられる。 RDBMSにおけるセキュリティ要件の多くはOS、ネットワーク、業務アプリケーションといった他のシステム構成要素と変わるところはなく、基本的には本ドキュメントの2.2.1.1～2.2.1.6に記載されている対策要素を適切に組み込むことで実現が可能である。 しかし一方でRDBMSに特徴的な留意事項も存在することや、従来OSやネットワーク上での対策に重きがおかれ、その重要性があまり考慮されないことが多く、結果として多くの重大な事故を防止できなかったことを鑑み、遵守事項を明示することが重要であると考える。これによって、今後の政府機関の情報システムの安全性に寄与することができると考えられる。	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。
24	2.3.3 アプリケーションソフトウェア	具体的なRDBMSに特化した遵守事項の内容としては以下のようなものが考えられる。 遵守事項（案）： （1） RDBMSの導入・構築時 （a）情報システムセキュリティ責任者は、情報セキュリティが確保されるよう適切にRDBMSのセキュリティ設定・構築をすること。適切なセキュリティ設定・構築として、以下に挙げる事項を含む措置を講ずること。 （ア）アプリケーションが使用するスキーマ名、ユーザ名およびそのパスワードにデフォルト値を利用しないこと。 （イ）行政事務従事者や保守運用者などが使うパスワードについては文字数および文字種類など、推測を困難にするための制限および定期的な変更を機能的に強制すること。 （ウ）RDBMを搭載したサーバ（データベースサーバ）に対する、リモートアクセス機能、利用者のパーミッション、不正な入力データを適切に制限すること。 （エ）通信時の盗聴による情報漏えいのリスクを検討し、クライアント、アプリケーション等との間の通信経路における暗号化を行うこと。 （オ）機密性2情報および機密性3情報に該当する情報を格納する場合は暗号化による保護を行うこと。このとき利用する暗号アルゴリズムは電子政府推奨暗号リストに掲載されているものを利用する。また単一鍵で暗号化した場合、暗号鍵の漏えい時等に被害が拡大することから、列、表、表領域などの単位で別の暗号鍵を利用すること。 （カ）暗号鍵に対して適切なアクセス制御を実装し、暗号鍵の保全を行う。また、その実装方法と実装状態については第三者機関による評価が行われていることが望ましい。（例：ISO/IEC15408等） （キ）RDBMS上で管理者権限を持つ識別コードについては、最小権限やデュアルロック機能などの高度な権限管理を設けることの必要性の有無を検討し、必要と認めたときは当該機能を設けること。 （ク）システムの開発を外部に委託する場合であって、性能試験等の目的で本番システムのデータを利用したい場合は、マスキング等の技術を使用して匿名化等の措置を講じること。	
25	2.3.3 アプリケーションソフトウェア	（2）RDBMSの運用時 （a）情報システムセキュリティ責任者は、情報セキュリティが確保されるよう以下のような適切なRDBMSの運用を行わなければならない。 （ア）要機密情報およびそれを格納するオブジェクト（表・ビュー等）に対する閲覧・変更・削除・挿入についてはその操作ログ（SQL）を取得する。その際、アプリケーションを経由せず、直接当該オブジェクトにアクセスする行為のほうがよりリスクが高いと考えられ、これらを優先的に取得する必要がある。 （イ）上記（ア）において取得したログは通常の管理者（データベース管理者）を含めて、情報システムセキュリティ責任者及び当該責任者から許可・委託を受けた者以外がアクセスできないようにアクセス制御を行い、保全すること。 （ウ）ログの取得と同時に、それらのログをもとにして、不正な操作を即時に検知し、情報システムセキュリティ責任者に対して警告を発する機能を実装すること。 これらの項目の詳細についてはRDBMSを安全に構築・運用するための指針として、 当コンソーシアムから公開されている 『データベースセキュリティガイドライン 第2.0版』などを参照されたい。http://www.db-security.org/report/guideline_seika.html	
26	2.3.3.2 ウェブ (1)(a)	(オ)ウェブサーバに保存されたファイルが改ざんされた場合に検知できるよう対策を講ずること。 （理由） （イ）アクセス権限の適切な設定を行ったとしても、正しいアクセス権限を入手した場合には改ざんが可能である。そのため、改ざんされた際に検知し、正しい内容であるか確認する必要があると考えるため。	ご指摘の点については、ウェブサーバに限らないため、2.3.2.3「サーバ装置」(2)(e)において、「セキュリティ状態を監視する必要性の有無を検討し、必要と認めたときは、当該措置を講ずること」を求めており、今後の検討課題とさせていただきます。
27	2.3.3.2 ウェブ (3)	(e)ウェブアプリケーションの脆弱性への対策を実施すること。また、その対策が完了していることを定期的に診断し、管理する方法を担保すること。 （理由） ウェブアプリケーションの脆弱性への対策を実施した場合でも、実際にその対策が有効に働いているかどうか定期的に確認し、状態を管理しない限り、システムの安全性が担保されないため。（一般的な監査においても、定期的な確認が推奨されているため）	ご指摘の点については、2.2.2.1セキュリティホール対策　において定期的な確認を既に求めており、原案のとおりとさせていただきます。
28	2.3.4.1 通信回線共通対策	「情報システムセキュリティ責任者」と「情報システムセキュリティ管理者」の業務分担の違いが明確にして頂きたい。 （理由） (2)(e)の時刻同期は、他の規定から予想し「～責任者」の作業であると思われましたが、「～管理者」の作業であることから、両者の業務分担の基準が分りにくくなっています。	ご指摘の点については、情報システムに機能を設けることについては、情報システムセキュリティ責任者が担うこととしており、実際の作業を伴う管理に関する遵守事項については、情報システムセキュリティ管理者が担うこととしております。
29	全体	本書は「技術基準」を定める文書であることから、必要事項を列挙する他、基準となる指標やラインを明確にして頂きたい。 （理由） 本「技術基準」記載内容が、後に情報セキュリティ対策の有効性評価を行う際の重要な判断指標・基準になると思います。	ご指摘の点については、個別マニュアルや他の施策等を通して、提示させていただきたいと考えております。
30	全体	全体を通じ、各事項が定める行為について、それらが本来の意図どおりに行われているかに対する検証（承認や記録類）プロセスに関する規定を追加して頂きたい。 （理由） 別文書にて明文化されている場合は不要です。	ご指摘の点については、評価に関するプロセスについては、「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」において規定しております。
31	追加先未定 （※2.2.2中の各脅威毎の(2)情報システムの運用時内を想定）	国内の各脅威情報（セキュリティホール対策、不正プログラム対策等）の収集のため、専任の担当者を配置し、外部の専門技術者、組織等と連携する等、情報収集経路を確立すること。 （理由） ウェブ等の一般公開情報では入手できない最新情報や国内固有の情報収集を入手するためには、外部のセキュリティの専門性の高い組織と連携の必要があると考えるため。（特に、標的型攻撃について）	ご指摘の点については、1.2.2.2(1)(e)の中で、訓練の一部として、障害・事故等の対処に関する教育を受講したり、外部から情報セキュリティに関する情報を適宜収集したりすることを求めており、NISCの役割として、「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」において、関係各部門との情報共有ををを行うことを定めています。

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

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