「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概要

■ 実施期間：2023年４月17日（月）～５月12日（金）

■ 実施方法：NISCのウェブページ及びe-Govに掲載して公募。
併せてオンラインでの説明会を実施（4月28日に実施し、参加者約６０名）

■ 意見総数：３４者から計８２件 【内訳：１６企業・団体から４４件、１８個人から３８件】

（１）修正を求める意見：全７１件

- 表現の適正化を求めるもの（５件）、有効と考えられる技術や考慮すべき脅威等に係る意見（１２件）
  ⇒ 該当箇所を改定案に反映
- 原案どおりとする意見（５４件）
  ⇒ 他の箇所で規定しているなどの理由で改定案に反映させないものについては、パブコメ結果の公表時理由を付して提示（NISCのウェブページ及びe-Govに掲載）

修正意見の主な内容

- 情報の抹消方法に関する意見（５件）
- 情報のバックアップに関する意見（５件）
- 端末やネットワーク通信の挙動を元に攻撃者の横展開を早期検知する分析プラットフォームやASM(アタックサーフェスマネジメント)、コンテナ環境における対策、脆弱性管理ツールの導入等の最新のセキュリティ対策に関する意見（６件）
- 機器に組み込まれるソフトウェアにおけるSBOMやコード署名を活用したサプライチェーン管理に関する意見（２件）

（２）その他、統一基準の公表方法、サイバーセキュリティ政策に関する意見等（１１件）
⇒ パブコメ結果の公表時に対応を提示（NISCのウェブページ及びe-Govに掲載）

Copyright (c) 2021 National center of Incident readiness and Strategy for Cybersecurity (NISC). All Rights Reserved.

「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」の改定（案）に関する意見募集の結果一覧

通しNo.	提出者	対象文書	概要	ご意見に対する考え方
統一規範について				
1	個人	統一規範	統一規範案第２条第１号にデジタル庁を含むべきではないか。	デジタル庁は統一規範案第２条第１号の「法律の規定に基づき内閣に置かれる機関」に該当します。（デジタル庁設置法第二条）
2	個人	統一規範	統一規範案第３条第４項「にて規定した」は同条第５項のように「に定める」とすべきではないか。	ご意見のとおり修正いたします。
3	個人	統一規範	統一規範案第14条第３項中の法令番号は、他の箇所と合わせて漢数字とするべき。	ご意見のとおり修正いたします。
4	個人	統一規範	統一規範案第19条第４項で「整備しなければならない。」とあるのは、他の箇所と合わせて「定めなければならない。」又は「定め、実施しなければならない。」等とすべき。	ご意見を踏まえ修正いたします。
5	個人	統一規範	統一規範案第21条「（以下「情報システムの運用継続計画」という。）」は以下この文言を用いておらず、不要ではないか。また、同条「整備及び運用」は「整備し、及び運用」とすべきではないか。	ご意見を踏まえ、「（以下「情報システムの運用継続計画」という。）」は、「（情報システムの運用継続計画）」に修正いたします。

通しNo.	提出者	対象文書	概要	ご意見に対する考え方
6	個人	統一規範	独立行政法人によっては所管元の国の行政機関が取っているポリシーよりも先進的でデジタル技術を的確に利用できる体制を構築しつつ効果的効率的であったり、不足する内容を補完する内容の規範を先んじて取り入れる場合もあるため、国の行政機関に改善提案を行うこともできるようにするほか、セキュリティと利便性は相反する部分もありながら、技術の研鑽や理解の促進によって、セキュリティ向上をしつつデジタル化を阻害しないようにするための活動も推奨されるべきであるため、この点について盛り込む必要がある。 また、セキュリティを向上しつつデジタル化を阻害しないための技術研鑽や理解の促進については、所管省庁によらず、意見交換や勉強会を実施することで相互に向上していくことがセキュリティの向上に資すると考えるため、個別の対策基準についても、国の行政機関やその独立行政法人等各省庁の壁を越えて研鑽し常に目まぐるしく変化していくセキュリティの脅威について適切に対応していくことが必要になってくるため、統一規範への盛り込みについて検討いただきたい。	本規定は独法等が自らのポリシーを定める際に所管省庁のポリシーを参考とすることを求めており、必ずしもその内容を反映させることを求めているものではなく、自組織の特性等を踏まえた独法等の独自の対策を阻害するものではありません。 所管省庁から独法等への一方通行ではなく、独法等から所管省庁への改善提案や相互の意見交換など、双方が連携して対応してセキュリティ向上に向けて対応する必要があるとの御意見と認識しました。御意見を参考にして、引き続き検討して参ります。
7	個人	統一規範	管理体制を明記していただいたことは適切な対応で重要な点だと思います。さらに、CISO及び委員会等の設置を明確にした点も非常に賛同いたします。しかし、不足する点として、CISO、委員会、CISOから職務を担わせるものの能力、教育にふれる必要があるかと思います。まずは、体制を構成するのが開始点ですが、知識、能力がないものだけで構成してもしかたない。あくまで必要な知識、能力があるものを任命してかつ、不足する知識、能力に対しては教育を提供すべきことを明記すべき。特に本邦では情報処理安全確保支援士なる資格があるので、この資格者を任命するとか、機関等でそれの資格を目指す等の動機付けを行えるようにすべきではないかと思います。	統一基準において、遵守事項2.2.3(2)で情報セキュリティ推進体制やCSIRTに属する職員、CYMATに属する職員への教育について規定しております。また、最高情報セキュリティアドバーザーについては、「情報処理安全確保支援士」を例示して、情報セキュリティに関する資格や専門的な知識及び経験を有した者である必要があることを規定しております。

通しNo.	提出者	対象文書	概要	ご意見に対する考え方
8	個人	統一規範	第9条に教育を、第10条においてインシデントへの対応を定めている。しかし、インシデントの対応を発生時に適切に実施するためには、通常時の訓練等が必要になる。このため、第9条を教育だけでなく、教育、訓練として、第10条ではインシデント対応のための平常時の準備等の対応も追記しておくべきではないかと思います。	対処手順の整備や訓練等の情報セキュリティインシデントに備えた事前準備については、統一基準の遵守事項2.2.4(1)に規定しております。
9	個人	統一規範	第14条4項「指定法人を所管する国の行政機関は、当該指定法人に対して、個別の根拠法に基づき、情報セキュリティ対策の実施状況に関して評価を行う。」と記載されている。しかし、個別の根拠法が最新のサイバーセキュリティ、情報セキュリティ等の動向をキャッチアップされていない可能性もある。個別の根拠法に従うことは重要ではあるが、ここでは「個別の根拠法に基づき」を削除したほうのがより適切にセキュリティ対策が実施される可能性が高くなるのではないかと思います。	当該記載は個別の根拠法において定める「業務の実績等に関する評価」に基づき、これに情報セキュリティ対策の実施状況に関して評価を行うことを規定しているものであり、個別の根拠法自体に最新のサイバーセキュリティ等の動向を踏まえた対策等を定めているものではありません。
10	個人	統一規範	外部委託において、要機密情報などセキュリティの三要素の機密性のみに注目した記載になっているが、機関等の情報機器、情報システムを使ったサービスは、停止することにより国民に多くの影響を与える可能性もある。機密性のみを注視するのではなく可用性も十分考慮した要件にすべきです。注目すべきものも「情報」だけでなく、情報システムに関しても見ていくべきかと思います。要機密情報を扱っていないとしても、その情報システムが停止することにより多くの国民に迷惑をかけるようなものに関しての考えが不足しているように思えます。特に「サイバーセキュリティ」との言葉を文書として使っているのでなおさら、従前の情報セキュリティだけではない考えが必要になると思われます。	統一規範においては機密性を重視した規定となっておりますが、統一基準及びガイドラインにおいては、可用性や完全性も考慮した規定を設けているところです。例えば、利用するクラウドサービスにおける可用性を考慮した設計を行うこと（基本対策事項4.2.2(1)-4）や十分な可用性を担保した復旧に係る手順の整備（基本対策事項4.2.2(3)-3）、適切なバックアップの取得（基本対策事項5.2.3(1)-7）などを規定しているところです。

通しNo.	提出者	対象文書	概要	ご意見に対する考え方
11	個人	統一規範	クラウドを利用するときの見過ごしされやすいリスクとして、クラウドに接続するためのVPN機器の脆弱性が放置されやすい。クラウド及びクラウドへのネットワークに関してはクラウド事業者等の選定が間違えなければ適切に実施される可能性が高い。しかし、機関等の出口に設定されるであろうVPN機器に関しては、クラウド事業者が面倒を見ないで機関等が直接調達する場合も多いのではないかと思われます。そのときに、運用中に発生する脆弱性のパッチ等が実施されない可能性が非常に高い。そのような事故が多い。この部分を強化した記載を追記すべきではないかと思います。	御意見のVPN機器については、遵守事項6.4.2(2)及び基本対策事項6.4.2(2)-1において、通信回線装置が動作するために必要なソフトウェアの定期的な脆弱性の確認や不適切な状態の改善などの対策を実施することを規定しております。
統一基準・ガイドライン「1.2　情報の格付の区分・取り扱い制限」について				
12	個人	統一基準	情報に関して機密性の格付を行うことは適切と考えるが、特に可用性の格付を行うことに違和感がある。 情報に関しては機密性で格付けをして、情報システムに関しては機密性・完全性・可用性のそれぞれに関して格付けを行うべき。	今般の改定案において、情報システムの重要度に応じた情報セキュリティ対策が講じられるよう、「情報システムの分類基準」の考え方を導入いたしました。この考え方には、情報システムの機密性・完全性・可用性の観点も含めております。 いただいたご意見は今後の検討の参考とさせていただきます。
統一基準・ガイドライン「1.3　（統一基準における）用語定義」について				
13	個人	統一基準	「業務委託」の定義において「ただし、当該業務において機関等の情報を取り扱わせる場合に限る。」と記載されている。しかし、本記載によって対象が必要以上に狭く捉えられる可能性が非常に高い。例えば、クラウド事業者においても、事業者自体が情報にアクセスできない場合は対象外となってしまうおそれがある。同様に情報を扱わない契約の機器の保守も対象外になってしまう。本「ただし」書きは削除すべきではないか。	御意見の箇所のただし書きは、守るべき情報がない業務委託（例えば「庁舎の清掃業務委託」など）を除外するための記載です。

通し No.	提出者	対象文書	概要	ご意見に対する考え方
14	個人	統一基準	「クラウドサービス」の用語定義において、一般の者が一般向けに使うものだけに範囲を狭めており、誤解やミスリードをしてしまう可能性が高い。	クラウドサービスの用語定義においては、一般の者が一般向けに「使う」ものだけに範囲を狭めているものではございません。 「機関等外の一般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』クラウドサービス」を機関等が利用等することで、「当該サービスにおいて機関等の情報が取り扱われる場合」、統一基準におけるクラウドサービスに該当いたします。
統一基準・ガイドライン「2.1.3　情報セキュリティ関係規程の整備」について				
15	個人	統一基準	「統一基準に準拠した対策基準を定めること」と記載されているが、統一規範(案)の第6条第3項では、「対策基準は、統一基準と同等以上の情報セキュリティ対策が可能となるように定めなければならない。」となっており、「準拠した」という表現だと、通常、同等レベルと認識される可能性が高いのではないか。	ご意見を踏まえ修正いたします。
統一基準・ガイドライン「3.1.1　情報の取扱い」について				
16	個人	ガイドライン	情報の抹消方法は解説に記載されているが、実態として把握されていないことが多いと考えるため、遵守事項に記載すべき。	ご意見を踏まえ、機関等において適切な抹消方法が用いられるよう、機関等への周知に努めて参ります。

通し No.	提出者	対象文書	概要	ご意見に対する考え方
17	個人	ガイドライン	表 3.1.1-1　情報の抹消方法の例　フラッシュメモリ媒体の注意点に、「…、データ抹消ソフトウェアによる上書きを１回実施した場合は実際にはデータの書き込みが行われず、消去すべき情報がそのまま残ってしまう現象が発生する可能性があるが、２回以上の上書きとすることにより、当該情報は抹消される。」と記載があるが、「…、完全なる乱数＋２回以上の上書きとすることにより、当該情報は抹消される。」または「…、完全なる乱数＋２回以上の上書き、またはNIST SP800-88 Rev.1のPurgeレベルの抹消処理を実行することにより、当該情報は抹消される。」という記載に変更すべき。	「（解説）遵守事項3.1.1(7)(b)「抹消する」について」に記載のとおり、「表3.1.1-1　情報の抹消方法の例」は、特殊な手段を用いることによって情報（断片を含む）が読み出されるリスクが存在する抹消方法の例示です。 なお、当該リスクを許容できないような機密性の高い情報の抹消方法は、NIST SP800-88 Rev.1のPurge及びDestroyランクを参考に作成した、「表3.1.1-2　機密性の高い情報の抹消方法の例」に例示しております。
18	個人	統一基準	「データ抹消処理結果の検証」と「データ抹消結果の保存・記録」を遵守事項に加えるべき。	「（解説）遵守事項3.1.1(7)(b)「抹消する」について」において、「業務委託を実施する場合は、情報が適正に抹消されたことの証拠となる記録及び証明書の提出を求める（略）ことが重要である。」と記載しております。また、ご意見頂きました「データ抹消処理結果の検証」は「情報が適正に抹消されたことの証拠となる記録及び証明書」に含まれると考えておりますが、いただいたご意見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	概要	ご意見に対する考え方
19	企業・団体	ガイドライン	「バックアップ取得元の情報システムが接続するネットワークから論理的に隔離 された保管場所」と記載があるが、アクセス制御やネットワークセグメント分離をしても、認証情報を採取されたりセグメント分離しているネットワークスイッチ等にマルウェアが侵入し最終的に攻撃されるリスクが残るので、「物理的な隔離」を基本的な対策とし、これををどうしても満たせない場合において「論理的な隔離」とするという優先度付けをすべきである。現状、「論理的な隔離」を講じていても被害が出ている事例がある。	御意見を踏まえ解説に追記いたします。
20	企業・団体	ガイドライン	復旧用データの保持期間を具体的に参考値として明確化をすべき。（例.バックアップデータは最低2週間保持、1ヶ月保持）	今後の検討の参考とさせていただきます。
21	企業・団体	ガイドライン	バックアップデータを攻撃から守る手段として、 ・セキュリティ対策として、バックアップデータはCIFS／NFSプロトコルで簡易的にアクセスできない仕組みを実装していること。 ・セキュリティ対策として、バックアップシステムはwindowsやLinux等汎用OSではなく、独自OS採用が望ましい を追記すべき。	今後の検討の参考とさせていただきます。
22	企業・団体	ガイドライン	セキュリティ被害を受けた後の出口対策として、保管しているバックアップデータに対する分析検証（検疫）機能を明記すべき。バックアップ時にウイルスチェックを実施することに加え、保管しているバックアップデータに対してもウイルスに侵されていない復旧に用いるべき正しいデータは何か？のチェック機構は必要と考える。	御意見を踏まえ解説に追記いたします。
23	企業・団体	ガイドライン	バックアップ実データに対する整合性を保持する機能を追加すべき。	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	概要	ご意見に対する考え方
24	個人	ガイドライン	廃棄する媒体を外部の民間事業者等へ業務委託において、廃棄端末を委託先（庁外）で実施する場合、その移動時や委託先での情報漏洩のリスクを考慮する必要があるため、消去場所自組織（庁内）でまず復元できないかたちでの消去を実施することを前提とすべき。	（解説）「遵守事項3.1.1(7)(b)「抹消する」について」において、情報の抹消を業務委託する場合は、職員等による立ち合いを行う等、委託先での履行状況を確認することを記載しております。また、運搬を第三者へ依頼する場合はセキュアな運送サービスを提供する運送事業者により運搬することを、基本対策事項3.1.1(6)-1において規定しております。
25	個人	ガイドライン	情報が適正に抹消されたことの証拠となる記録及び証明書は、改ざんされないような証跡の管理をすべき。	（解説）「遵守事項3.1.1(7)(b)「抹消する」について」において、情報の抹消を業務委託する場合は、職員等による立ち合いを行う等、委託先での履行状況を確認することを記載しております。
26	企業・団体	ガイドライン	暗号化された圧縮形式のファイルの送受信については、PPAPを利用した場合に、ウィルスチェックをされないまま受信される可能性があり受信者側で解凍・復号した際にウィルス感染するリスクがあることを記載していただきたい。	ご意見を踏まえ、職員等が不審な電子メールを受信することによる被害をシステム的に抑止する機能の導入に係る対策が規定されている、「（解説）「基本対策事項8.1.1(2)-2 d)「実行プログラム形式のファイルを削除等する」について」に追記いたします。
27	企業・団体	ガイドライン	運搬する情報を暗号化するにあたり、パスワードやパスフレーズでの暗号化について記載されていますが、よりセキュリティ強度が高いのはDRM、IRMのようにデータと鍵情報が分離され、サーバ側で主体認証を受ける必要のある暗号化手法です。さらにパスワードは利用者がファイルの暗号化・復号を意識する必要があり、運用を避けようとする職員もいることから、より利便性の高い暗号化手法を提示することも必要と考えます。	御意見ありがとうございます。引き続き検討して参ります。
統一基準・ガイドライン「4.1.1　業務委託」について				

通し No.	提出者	対象文書	概要	ご意見に対する考え方
28	個人	統一基準	業務委託の発注機関は、業務委託に伴う入札・公告時において、情報セキュリティの確保について漠然とした制約を課していることが実情である。各省庁で具体的に定めているであろう情報管理対策基準群は非公開であり、実際の対応状況はブラックボックス状態である。本統一基準案は、あくまで「政府機関内」向けの内容であり、民間企業が実質的に参考としなければならない内容について、別途整理しなければ外部委託者のセキュリティを担保できないのではないか。 　例えば、防衛装備庁が発表している「装備品等及び役務の調達における情報セキュリティ基準」のような具体的内容を、内閣官房内閣サイバーセキュリティセンターとして各省庁へ同時に発信すべきと考える。	委託先への要求事項については、基本対策事項4.1.1(3)-1に８項目を規定し、それらを契約に含めることを求めております。また、これらの８項目について、その具体的な対策をそれぞれの解説に例示するとともに、NIST SP800-171の管理策群を参考にすることを示しております。ご意見を踏まえ、本趣旨が適正に仕様書に反映されるよう、機関等への周知に努めて参ります。
29	企業・団体	統一基準	業務委託先の選定には、経済安全保障に基づくセキュリティクリアランスの観点も考慮すべきだと考えます。	御意見ありがとうございます。今後の検討の参考とさせていただきます。
30	企業・団体	ガイドライン	委託先に対して技術的な措置の実施と、それを実施させるための方法（NDA等）が記載されていますが、情報漏洩対策として委託元が実施可能な技術的措置についての記載がないように見える。 目的外利用を禁止するために、委託元機関が提供するデータに対して事前に暗号化、アクセス制御等の技術的措置を施してから提供することで漏洩を防ぐことも考えられるなど、委託元機関による提供データへの技術的な措置についての記載の追加を希望する。	情報を委託先に提供する場合に必要な対策については、遵守事項3.1.1(5)及び(6)に定めているところです。
31	企業・団体	ガイドライン	委託業務に伴う情報を取り扱う従業員等の資格条件の明確化について、資格条件の具体例を例示していただくことは可能でしょうか。	御意見ありがとうございます。今後の検討の参考とさせていただきます。
統一基準・ガイドライン「4.1.2　情報システムに関する業務委託」について				

通し No.	提出者	対象文書	概要	ご意見に対する考え方
32	企業・団体	ガイドライン	「業務委託サービス」に該当する例については理解できたが、「クラウドサービス」と「業務委託サービス」の線引きについて判断に迷う局面があることが考えられるため、より具体的な定義について記載願いたい。	「クラウドサービス」の定義の中に「利用者によって自由にリソースの設定・管理が可能なサービスであって、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」という記載がありますが、「業務委託サービス」との線引きのポイントの一つとして、「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」が考えられます。「クラウドサービス」は、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ため、当該サービス利用者が情報セキュリティ設定を実施することによって情報セキュリティを確保することを求めております。一方、「業務委託サービス」は、当該サービス利用者が情報セキュリティ対策を実施することに加え、主に、業務委託契約により、委託先がセキュリティ対策を講じることによって、情報セキュリティを確保することを求めています。
33	企業・団体	ガイドライン	業務委託サービスは、クラウドサービス以外であることからISO27017ではなく、ISO27001を取得していることを要件とすれば、問題ないでしょうか	御意見で示されている「ISO27001」も考えられますが、取り扱う情報の格付や取扱制限等に応じてセキュリティ要件を策定することを求めているため、これに限定するものではありません。
統一基準・ガイドライン「4.2.1　クラウドサービスの選定（要機密情報を取り扱う場合）」について				
34	企業・団体	統一基準	データが海外のクラウドサービスに格納される場合も、国内の準拠法を適用するためにも、日本国内で運用される認証局による鍵管理が必要だと考える。	ご意見を踏まえ、解説に追記いたします。

通しNo.	提出者	対象文書	概要	ご意見に対する考え方
35	企業・団体	ガイドライン	機関等の調達を伴わない場合であっても、クラウドサービスを選定する際は、4.2.1(2)の条項に従う必要があるという記載があることから、「原則としてISMAP等クラウドサービスリストからクラウドサービスを選定する」必要があるという認識で合っているか。例えば、委託先がすでに契約しているクラウドサービスを利用する場合、そのクラウドサービスISMAP等クラウドサービスリストに掲載されているサービスである必要があるという理解で間違いないか。 　委託事業者においても、ISMAP等クラウドサービスリスト掲載サービスの利用を求めるのは、難しいと考えております。本項の記載の見直しについて、ご検討をお願い致します。	機関等の調達を伴わない場合でも遵守事項4.2.1(2)の「原則としてISMAP等クラウドサービスリストからクラウドサービスを選定する」等が求められますが、これは機関等がクラウドサービスを利用する場合に情報システムセキュリティ責任者又は課室情報セキュリティ責任者に求めているものであり、委託先が利用するクラウドサービスについて必ずしも求めているものではありません。しかしながら、4.1.1「業務委託」の目的・趣旨において、業務委託で取り扱う情報の格付、委託する業務や利用するクラウドサービスの特性等に応じて、委託先への要求事項に含める必要があるとしているところです。
統一基準・ガイドライン「4.2.2　クラウドサービスの利用（要機密情報を取り扱う場合）」について				

通し No.	提出者	対象文書	概要	ご意見に対する考え方
36	個人	ガイドライン	「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」では、政府情報システムについて、単にクラウドを利用するのではなく、クラウドを適切（スマート）に利用するための考え方等が示されています。セキュリティについては、オンプレミスとクラウドで考え方や方 針レベルで大きく異なる点として、「サーバを構築しないアーキテクチャの採用」が挙げられていま す。 コンテナは、サーバを構築しないアーキテクチャにおける主要な技術の一つであり、クラウドをスマートに利用するための、重要な選択肢の一つでもあると認識しています。ただし、やはりコンテナ環境におけるリスクや対策は従来とは大きく異なり、「NIST SP 800-190 ア 18 プリケーションコンテナセキュリティガイド」や 「OWASP Docker Top 10」 等でその詳細が示されています。 上述の理由より、仮想マシンに加えて、コンテナ環境に対しても、適切なセキュリティ対策が必要で あることを示しておくことが望ましいと考えるため、コンテナ環境に対する適切なセキュリティ対策についても、追加で示してはいかがでしょうか。	御意見ありがとうございます。今後の検討の参考とさせていただきます。
統一基準・ガイドライン「4.3.1　機器等の調達」について				
37	企業・団体	統一基準	調達には、情報システムの構成部品の安全性確認や真正性担保のために、IEC62443やSP800シリーズなどの国際安全基準の機器レベルに求められるサイバーセキュリティ対策に加えて、機器に組み込まれるソフトウェアについてもSBOMやコード署名を活用した継続的なサプライチェーン管理が求められると考えます。	機器等の調達に当たっては、基本対策事項4.3.1(1)-1において、「IT調達に係る国等の物品等又は役務の調達方針及び調達手続きに関する申合せ」に基づき、サプライチェーン・リスクの観点から必要な場合にデジタル庁及びNISCに対して、講ずべき必要な措置について助言を求めることを規定しています。また、解説においてSBOMを参考にすることを例示として示しています。コード署名については、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	概要	ご意見に対する考え方
38	企業・団体	統一基準	スパイチップや不正プログラムなどの混入を防ぐためにも、製造メーカーや製造国、製造ロットなど出自がはっきりした機器を導入することを考慮すべきだと思われます。また多くのIoT機器でオープンソースが利用されていることを考慮すると、組み込まれるソフトウェアに関しても、サプライチェーン管理が重要であり、コード署名やSBOMの活用が必要になってくると考えます。	機器等の調達に当たっては、基本対策事項4.3.1(1)-1において、「IT調達に係る国等の物品等又は役務の調達方針及び調達手続きに関する申合せ」に基づき、サプライチェーン・リスクの観点から必要な場合にデジタル庁及びNISCに対して、講ずべき必要な措置について助言を求めることを規定しています。また、解説においてSBOMを参考にすることを例示として示しています。コード署名については、今後の検討の参考とさせていただきます。
39	個人	ガイドライン	サイバー空間における安全保障の観点から必要な対策と考えています。また、我が国の同盟国である米国では同様の調達法令が定められており、国家レベルの脅威が発現した際、原案では、当該調達ポリシーレベルの違いを理由に同盟国からの支援が限定されるのではないかと懸念しております。 そのため、防衛省が防衛白書などで言及している脅威国製の製品を調達しない基準を採用していただきたい。 もしくは、脅威国製の製品の場合、防衛省など国家安全保障を担う機関による検査で安全とされたもののみを調達するような基準としていただきたい。ここでの「脅威国製」の定義は、当該脅威国で製造もしくは保守を行っているものとします。	機器等の調達に当たっては、基本対策事項4.3.1(1)-1において、「IT調達に係る国等の物品等又は役務の調達方針及び調達手続きに関する申合せ」に基づき、サプライチェーン・リスクの観点から必要な場合にデジタル庁及びNISCに対して、講ずべき必要な措置について助言を求めることを規定しています。
統一基準・ガイドライン「5.1.1　情報システムの分類基準等の整備」について				

通し No.	提出者	対象文書	概要	ご意見に対する考え方
40	企業・団体	ガイドライン	今回の「情報システムの分類基準」と、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」（SBDマニュアル）は、どのように平仄を取って運用していくべきか。	統一基準における「情報システムの分類基準」と、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」（以下「SBDマニュアル」という。）における「実施レベル」の関連性について、統一基準において特段の定めはございません。「SBDマニュアル」の1.5「活用範囲」の「本マニュアルの活用範囲（対象として想定している情報システムの範囲）は、基幹LANシステムや共通基盤システムなど総合的かつ緻密なリスク分析を要する情報システムを除く、（略）中小規模の情報システムの調達に対して特に有効」の記載を踏まえ、情報システムのセキュリティ要件を策定する必要があります。「情報システムの分類基準」と「SBDマニュアル」の関係性については今後検討して参ります。
41	企業・団体	ガイドライン	表 5.1.1-1 情報システムの分類基準（例）において、重要度「高」の判断基準として「運用経費が極めて大きい場合」があるが、「情報セキュリティインシデント等が発生した際に業務遂行に影響を及ぼすなど、社会的・経済的な混乱を招くおそれがある高度な情報セキュリティ対策が要求される情報システムを判別するための基準」の例示として必ずしも適切ではない。	「運用経費が極めて大きい場合」が、必ずしも「重要度「高」として判断される情報システムに該当するとは限らないところですが、指標の一つとしては考えられると判断しております。
統一基準・ガイドライン「5.2.3　情報システムの運用・保守」について				

通し No.	提出者	対象文書	概要	ご意見に対する考え方
42	企業・団体	統一基準	既知の脆弱性の対策と未知の脆弱性の早期発見の為の定期的かつ継続的な運用サイクルとするため、情報システムのスキャン、脆弱性の可視化、対応を自動化するための脆弱性管理ツールの導入が望ましい。	脆弱性のスキャン・可視化に有効と考えられる自動でソフトウェアの種類やバージョン等を管理する機能や、自動でソフトウェアを更新する機能を有する、「IT資産管理ソフトウェア」の導入を例示した規定がございます。
統一基準・ガイドライン「5.2.4　情報システムの更改・廃棄」について				
43	個人	ガイドライン	情報の抹消方法は解説に記載されているが、実態として把握されていないことが多い。そのため、情報の抹消方法は解説ではなく遵守事項に記載すべき。	ご意見を踏まえ、機関等において適切な抹消方法が用いられるよう、機関等への周知に努めて参ります。
44	企業・団体	統一基準	廃棄の際には、復元できない形での確実な情報の抹消に加えて、データ消去証明の取得が望ましいと考えます。	情報の抹消方法や抹消に係る留意点は、「（解説）遵守事項3.1.1(7)(b)「抹消する」について」に記載しており、当該解説において、「業務委託を実施する場合は、情報が適正に抹消されたことの証拠となる記録及び証明書の提出を求める（略）ことが重要である。」と記載しております。
統一基準・ガイドライン「5.3.1　情報システムの運用継続計画の整備・整合的運用の確保」について				
45	個人	ガイドライン	危機的事象発生に備え訓練を実施するのは、運用継続計画の範疇であり、サイバーセキュリティの範囲を逸脱していると考えます。 令和3年度版の解説に記載の通り「情報システムの運用継続計画の教育訓練を行う際は、対策事項の有効性の確認も目的とすることが望ましい。」にとどめてはいかがでしょうか。	遵守事項5.3.1(1)(b)に記載のとおり、「情報セキュリティに係る」対策事項、運用規程、実施手順が運用可能であるかを確認するための訓練となります。
統一基準・ガイドライン「6.2.1　サーバ装置」について				

通し No.	提出者	対象文書	概要	ご意見に対する考え方
46	企業・団体	ガイドライン	サーバ装置の「適切なセキュリティ対策を実施する」の解説において、本質的なことが記載されておらず、例としてあげられているものも端末への対策例となっている。サーバ側での対策と端末側での対策がそのまま一致しているとは限らないため、情報システムという枠組みで第7部を参照させるか、本項目内に主体認証、アクセス制御などの主要な対策だけでも記載する方がよいと考える。	ご意見を踏まえ、修正いたします。
統一基準・ガイドライン「6.2.2　電子メール」について				
47	企業・団体	ガイドライン	DMARCに関する具体的な設定やスケジュール感を明示されたことで、実効的な対策が速やかに進むのではないかと期待する。さらにBIMIについても一言追加して記載することを検討いただきたい。	ご意見を踏まえ、修正いたします。
48	企業・団体	ガイドライン	基本対策事項6.2.2(1)-2を以下のように修正すべき。 「DMARCによる受信側の対策を行う。DMARCによる受信側の対策を行うためには、SPF、DKIMの両方による対策を行う必要がある。なお、送信ドメイン認証技術による電子メールのなりすましの防止策が適用できない場合、送信ドメイン認証技術に頼らないなりすまし防止策を行う必要がある。」 当該意見による修正に合わせ（解説）として以下を追加することを提案する。 「公平性が高い事業を営む上で普く電子メールを受信する目的で送信ドメイン認証技術を利用できない場合やビジネス電子メール詐欺の脅威がある場合、送信ドメイン技術に頼らないなりすまし対策を代替もしくは併用として検討するべきである。」 補足: 原案のなりすまし対策はなりすまし（Spoofing）攻撃に対抗するものだが、なりすまし（Impersonation）攻撃の対抗を代替・併用対策として意見する。	基本対策事項6.2.2(1)-2では、機関等が受信した電子メールに送信ドメイン認証技術が用いられていない場合、機関等に当該電子メールの受信を拒否することを必ずしも求めてはおりません。 また、送信ドメイン技術に頼らないなりすまし（Impersonation）対策については検討して参ります。

通し No.	提出者	対象文書	概要	ご意見に対する考え方
統一基準・ガイドライン「6.2.3　ウェブ」について				
49	個人	ガイドライン	sslサーバ証明書の有効期限についての記載が必要である。	サーバ証明書の有効期限については、「TLS暗号設定ガイドライン」に記載があり、当該ガイドラインに従うことが基本対策事項6.2.3(1)-5に規定されております。
50	個人	ガイドライン	ウェブサーバの導入・運用時の対策の項目に、アクセス集中対策ならびにDDoS対策、オリジンサーバの隠匿をすることでサーバに直接不正ログインをされてサイト改ざんをされてしまうリスクを低減させるためや、クラウドサービスによるWAFによる攻撃への対策といった用途に、コンテンツデリバリーネットワーク（CDN）を用いた負荷分散並びにセキュリティ対策を図ることについて追加記載したほうが良い。	ご意見を踏まえ、追記いたします。
統一基準・ガイドライン「6.2.4　ドメインネームシステム（DNS）」について				
51	個人	ガイドライン	DNSSECにも踏み込むべきである。	今回の改定案では、現行の統一基準群の基本対策事項において、DNSキャッシュポイズニング対策の例示としてDNSSECの利用を規定しておりましたが、本改定案ではこれに加え、DNSSECを利用する場合のDNSSECトラストアンカーを最新の状態に保つための対策を規定しようとしているところです。DNSSECに係る対策については引き続き検討して参ります。
統一基準・ガイドライン「6.4.1　通信回線」について				

通し No.	提出者	対象文書	概要	ご意見に対する考え方
52	企業・団体	ガイドライン	未知の不正プログラムに対する判断や外部からの不正アクセスによる被害への対策として、サンドボックス型の対策を検討するとよい、との記載について、現在では不正プログラムの検知回避や、処理遅延の大きさが問題になっている側面もある。そのため、サンドボックス型の対策の他、シグニチャ方式によらず、未知の不正プログラムを即時検出が可能なファイルセキュリティ技術もあります為、検知、処理速度、コストの観点から、今回の改訂に際し併せて検討項目として記載されると良いと考えます。	御意見ありがとうございます。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。
統一基準・ガイドライン「6.4.3　無線LAN」について				
53	個人	統一基準	単に秘匿性を確保だけではWEPなどを使う可能性があるため、方式を限定すべきである。また、必要以上の電波伝搬を阻止する観点から出力の強さを制限しても良い。	無線LANの暗号化方式につきましては、解説において、WPA3 EnterpriseやWPA2 Enterpriseが考えられること、また、WEPやTKIPは利用してはならないことを記載しているところでございます。 無線LANの出力強度につきましては、3.2.1「情報を取り扱う区域」に関連する記載をしているところでございます。いただいたご意見は今後の検討の参考とさせていただきます。
統一基準・ガイドライン「6.4.4　IPv6通信回線」について				
54	企業・団体	統一基準	対象に、IPv6 Ready Logo Program (Phase-2) 準拠製品だけでなく、USGv6 準拠製品を含めて頂きたい。USGv6 は米国国立標準技術研究所 (NIST) が米政府機関向けに提供している IPv6 機能や相互運用性に関する認証となり、テスト仕様は IPv6 Ready Log Program と同様のものが広範に渡り使用されています。認証の実効性は IPv6 Ready Log Program 相当のものと考えられ、また類似の複数の認証を取得することは製品ベンダにとっては大きな負担となる。	御意見ありがとうございます。御指摘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	概要	ご意見に対する考え方
統一基準・ガイドライン「7.1.1　主体認証機能」について				
55	企業・団体	統一基準	厳格な機器特定による認証の為には、安全な鍵管理による真正性の担保と識別の仕組みが必要だと考えます。 また第三者認証機関による本人認証の仕組みも必要となると思われます。	御意見ありがとうございます。御指摘については今後の検討の参考とさせていただきます。
56	企業・団体	ガイドライン	「（パスワードの）定期的な変更が真に必要である場合に限り適用すべき」という内容を遵守事項に追加してはいかがでしょうか。定期的に変更を促すことが必須要件ととらえられていることが多く、上記の記載が必要と考えます。	基本対策事項7.1.1(1)-5において、利用者に主体認証情報の定期的な変更を求める「場合」と記載しており、利用者に主体認証情報の定期的な変更を求めることが必須要件と捉えられることはないものと認識しておりますが、ご意見を踏まえ、本趣旨が機関等に伝わるよう、機関等への周知に努めて参ります。
統一基準・ガイドライン「7.1.2　アクセス制御機能」について				
57	企業・団体	ガイドライン	ゼロトラストの観点から侵害された場合等を考慮し、情報の漏洩を防止するための施策が必要であるため、追加セキュリティ対策として以下を追加すべきと考える。 ・情報に対して行える操作（閲覧、複製、印刷、メール送信等）を限定するアクセス制御	御意見ありがとうございます。御指摘については今後の検討の参考とさせていただきます。
統一基準・ガイドライン「7.1.4　ログの取得・管理」について				
58	企業・団体	統一基準	不正侵入、不正操作等の有無について定期的にログを点検又は分析とありますが、これに認証サーバやネットワーク機器のログからネットワークへの侵入をいち早く検知し、対処を行うための仕組みの利用を追記頂きたい。	御意見を踏まえ、解説においてNDRの導入を例示として追加いたします。
統一基準・ガイドライン「7.2.1　ソフトウェアに関する脆弱性対策」について				

通し No.	提出者	対象文書	概要	ご意見に対する考え方
59	企業・団体	ガイドライン	追加セキュリティ対策について「また、脆弱性診断の実施に当たっては、インターネットから攻撃を受ける可能性のあるサーバ装置、（略）に対してはペネトレーションテスト、TLPT（脅威ベースのペネトレーションテスト）等の高度な脆弱性診断の実施を検討すること。」に修正してはいかがでしょうか。現状の記載はオフラインのサーバに対してもペネトレーションテスト等の実施が必要とも読み取れます。	オフラインのサーバに対してもペネトレーションテスト等の高度な脆弱性診断を実施することを想定しております。これはインターネット接続系と物理分離された基幹ネットワークへの保守用端末やリモートアクセス端末を起点とした内部不正を想定したペネトレーションテスト等を想定しております。
60	企業・団体	ガイドライン	ソフトウェアに関する脆弱性対策については、脆弱性情報の公開から対応までに時間を要した場合や、不適切な状態が長く続いた場合には、改善の措置を講じる前に侵害を受ける可能性についても考慮する必要があると思われます。 改善を行うまでの間は監視を強化することや、改善を行うと同時に遡って調査（アクセスログ等）を行うことが望ましい旨を追記してはいかがでしょうか。	「改善を行うまでの間は監視を強化すること」については、基本対策事項7.2.1(1)-9 c)の解説において記載しております。「改善を行うと同時に遡って調査（アクセスログ等）を行うことが望ましい」旨については、「脆弱性が公開された際にリスク評価を行い、遡って調査（アクセスログ等）した結果、必要と判断した場合に実施が必要になる」が正しい対応であると考えていますが、同趣旨は「5.2.3(1)情報システムの運用・保守」や「7.1.4(1)ログの取得・管理」の遵守事項、基本対策事項又は解説において記載されております。

通し No.	提出者	対象文書	概要	ご意見に対する考え方
61	企業・団体	統一基準	システム停止が必要となる脆弱性対策対策において、脆弱性対策計画を策定したものの再起動が実施できる日が決まっており、緊急度の高い脆弱性であってもシステム再起動・停止ができないためにそれら脆弱性対策の実行が先延ばしになるケースがある。そのため、このような背景を踏まえた確実に実行できる対策として、確実に脆弱性の定期確認を行う脆弱性スキャンの自動化、システムに影響を与えずに脆弱性対策を実行する技術（例えば仮想パッチ）を明記し、被害を最小限にとどめることが必要があると考える。「ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。さらに、システム再起動の計画等の影響により再起動を必要とするセキュリティパッチ等のすみやかな適用が難しい環境においては、仮想パッチ等、脆弱性を突く攻撃パケットを検知しブロックする暫定的なセキュリティ対策や定期的に脆弱性を自動検知できる対策を講ずること。」との変更を提案します。	セキュリティパッチ等の適用が難しい場合の暫定措置（WAFによる仮想パッチ等）については、基本対策事項7.2.1(1)-9 c)の解説に記載されています。また、「攻撃パケットを検知しブロックする暫定的なセキュリティ対策」については、IPSによる攻撃元IPアドレスの遮断を意識したものと考えますが、本件については基本対策事項6.4.1(2)-1に記載されています。
統一基準・ガイドライン「7.2.2　不正プログラム対策」について				
62	企業・団体	ガイドライン	メインフレームシステムなど、不正プログラム対策ソフトウェアが有効な役割を果たさないと考えられているOS において、不正プログラム対策ソフトウェアが提供されていない場合は本項の対象外であるとの記載があるが、現在はスマートフォンなどを含めて新しいOSにも対応したソフトウェアやOSにインストールせずに利用できる不正プログラム対策の技術があるため、 特にそのメインフレームシステムが本改定案の重要度分類により高重要度に分類されるシステムについては、同様に対策を検討することを推奨するべきと考える。	ご意見を踏まえ、修正いたします。
統一基準・ガイドライン「7.2.4　標的型攻撃対策」について				

通しNo.	提出者	対象文書	概要	ご意見に対する考え方
63	企業・団体	ガイドライン	内部対策の追加セキュリティ対策として、端末やネットワーク通信の挙動を元に攻撃者の横展開を早期検知する分析プラットフォームの利用を追記頂きたい。	ご意見を踏まえ、不正な通信を監視する方法としてNDRの仕組みを例示として解説に記載いたします。
統一基準・ガイドライン「7.3.1　動的なアクセス制御の実装時の対策」について				
64	企業・団体	ガイドライン	表7.3.1-3「有効な機能や当該機能を有するソリューションの例」の「リソース」は、「ユーザアカウント」・「機器」のみだが、「アプリケーション」・「データ」も記載すべき。	「（解説）基本対策事項7.3.1(3)-1「動的なアクセス制御を実現するための構成」について」に記載のとおり、表7.3.1-3は、リソースへの情報セキュリティ対策機能や当該対策が有効に機能し、リソースが信頼できるものであるかを検討する機能を有するソリューションの一部を示しております。「ユーザアカウント」・「機器」以外のリソースに対する有効な機能やソリューションは、表7.3.1-3等を参考にして下さい。
統一基準・ガイドライン「8.1.1　情報システムの利用」について				
65	企業・団体	ガイドライン	実行プログラム形式の添付ファイルのシステム側での削除や圧縮形式のファイル全ての削除については業務影響が出る部分であり、負担から利用者からの問合せや依頼等が増えている。実行プラグラム形式以外のファイルタイプの脅威も同等に多いことから、実行プログラム形式ファイルのみを対象にして、添付ファイルを削除の運用では、効果の割に運用が難しいと捉える組織が多い。現在はファイルタイプを問わず、一律削除せずとも、悪性なプログラムを即座に隔離する技術があるため、案に記載の運用等と併せ、システム的に抑止する機能の選択肢の1つとして推奨することを提案します。	ご意見を踏まえ、実行プログラム形式以外の形式に関して、追記いたします。

通し No.	提出者	対象文書	概要	ご意見に対する考え方
66	企業・団体	ガイドライン	暗号化された圧縮形式のファイルの送受信については、PPAPを利用した場合に、ウィルスチェックをされないまま受信される可能性があり受信者側で解凍・復号した際にウィルス感染するリスクがあることを記載していただきたい。	ご意見を踏まえ、職員等が不審な電子メールを受信することによる被害をシステム的に抑止する機能の導入に係る対策が規定されている、「（解説）「基本対策事項8.1.1(2)-2 d)「実行プログラム形式のファイルを削除等する」について」に追記いたします。
統一基準・ガイドライン「8.1.3　テレワーク」について				
67	企業・団体	統一基準	利用者側での対策に加えて、管理体制、ネットワーク環境、物理的な施設・作業環境などテレワーク施設側に求められる対策についても言及した方がよい。	全体の体制は「2.1.1組織・体制の整備」において規定がございます。テレワーク施設につきましては、当該施設が機関等の管理下にない場合は統一基準群の適用範囲外となりますので、当該施設側の対策ではなく、利用者側の対策として、例えば、画面ののぞき見や盗聴から発生する情報漏えい対策（基本対策事項8.1.3(3)-1）や、報セキュリティ対策の状況が不明又は不十分な回線を利用しないための対策（基本対策事項8.1.3(3)-2）を規定しております。
統一基準・ガイドライン全般について				
68	企業・団体	ガイドライン	多くの企業が、「PPAPの利用禁止の方向」を公表し、産業界としてもPPAP撲滅に向けて推進していると認識しており、政府機関等においてもPPAPの利用禁止をお願いしたいと考えており、今回、PPAPの利用禁止を促す記載が追加されていることに賛同する。	ご賛同頂きありがとうございます。

通し No.	提出者	対象文書	概要	ご意見に対する考え方
69	企業・団体	ガイドライン	昨今運用体制としてSOCやMSS、ツールとしてSIEMやSOAR、EDRやNDR(Network Detection & Response)などの技術・サービスの出現により検知領域の進歩および運用体制の充実が図られてきたが、実際に検知後に求められるインシデントレスポンスを中心とした適切な調査・解析・対処の部分で新たな課題が発生している。そのため、政府統一基準群の考え方全体にXDR(eXtended Detection & Response)を含めることを要望する。	御意見ありがとうございます。御指摘の内容については今後の動向等を踏まえて検討してまいります。
70	企業・団体	ガイドライン	政府統一基準群の考え方にアタックサーフェスのリスクを管理することでシステム運用やSOCのリソースを最大限活用するためのよりプロアクティブな防御力向上策を含めるため、ASM(アタックサーフェスマネジメント)の活用を要望する。	ご意見頂いた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。
その他ご意見について				
71	個人	その他	全体として違反時の罰則に触れられていない。一般企業では違反したら懲戒の文言があるのだが、官公庁では違反したらどうなるのか。	統一基準ではセキュリティポリシーに違反した場合の罰則について規定する想定はありません。職員等は各機関等において定められたセキュリティポリシーに従う必要がありますが、これに違反した場合の処分については、各機関等において定められた基準において判断されます。
72	個人	その他	サイバーセキュリティ戦略本部が指定する法人（指定法人）は現在9法人が指定されているものと認識している。 　しかしながら、サイバー攻撃の手口が日々巧妙化している状況下、「保有情報の機微性、業務の国民生活・経済活動へ与える影響」等の基準と併せて、予期せぬインシデントが発生した際の将来的なリスクも勘案して対象を継続的に点検し、必要に応じて追加を行っていくべきではないか。	指定法人の指定については、統一基準において定めているものではありませんが、いただいたご意見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	概要	ご意見に対する考え方
73	個人	その他	IT分野の進展は早く、次から次へと新サービス、新形態のサービスが登場しており、行政分野で取り入れる際に、本基準が適用されるのか曖昧なものが多々あると思われる。基準の網から抜け落ちると、そこをキッカケにセキュリティリスクが広がることも考えられる。クラウド、SAAS、ウェブアプリ、スマホアプリ等等行政サービスとして国民向けに提供されるITシステムやソフトも増えている。これらを包含するような再定義があると良いのでは。	ご意見頂いた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。
74	個人	その他	しおり付きPDFで提供されたことは最低限の電子的可読性が保てて非常によい。政府全体での取り組みに発展させて欲しい。しかし、改訂なので新旧対象表と、Wordの変更履歴付きの版も提供してあるといいのではないかと思います。特にWordで提供することにより、レビュー時の検索だけでなく、その書類の利活用にも有効である。本来、利活用するために提供するものであるので、如何に利活用しやすくできるかも考慮して欲しい。例えば、統一基準は最低限の基準であり、機関等はこれ以上のことを要求している。これを確認するためには、統一基準の各要件と自機関の要件とをExcelのようなもので並べて比較、確認したくなる。そのためには統一基準の各要件がExcel等で提供されるとより利活用しやすくなる等が考えられる。	現在、統一基準群のWord版と、「政府機関等の対策基準策定のためのガイドライン」のExcel版の公開を検討しております。
75	企業・団体	その他	「政府機関等の対策基準策定のためのガイドライン」を、エクセル形式でも公開すべき	現在、「政府機関等の対策基準策定のためのガイドライン」のExcel版を公開することを検討しております。

上記以外にも、本改定案に直接関係ありませんが、ご意見をいただきました。