「クラウドサービス提供における情報セキュリティ対策ガイドライン」（案）に対して提出された意見及びその意見に対する考え方

別紙１

■意見募集期間　：　令和３年７月17日（土）～令和３年８月15日（日）

■意見提出件数　：　12件（法人・団体：５者、個人：７者）

■意見提出者

	意見提出者
1	一般社団法人情報処理安全確保支援士会
2	株式会社ラック
3	ヴイエムウェア株式会社
4	株式会社セールスフォース・ドットコム
5	情報処理学会 情報規格調査会 SC 38専門委員会
―	個人（７件）

※いただいた御意見につきましては、原文を御意見ごとに分割して記載しております（ただし、本ガイドライン（案）と無関係と判断されるものは除いております）

■「Ⅰ．序編」に対する御意見

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
1	個人Ａ	Ⅰ．6．クラウドサービス事業者とクラウドサービス利用者の責任 「バージョンアップ等の頻度が多い」という記載が分かりづらいため削除、あるいは「バージョンアップ等の頻度が多く、その都度、新機能追加に伴うセキュリティ対策を追従しなければならない等、クラウドサービス特有のリスク対応が疎かになり」など表現の補記が望まれる。	いただいた御意見を踏まえ、P22「Ⅰ．６．クラウドサービス事業者とクラウドサービス利用者の責任」の記載を以下の通り修正します。 「クラウドサービスを利用するにあたってのリスクに対する認識度合いによっては、バージョンアップ等の頻度が多いクラウドサービス特有のリスクへの対応が疎かになり」 ⇒「クラウドサービスを利用するにあたってのリスクに対する認識度合いによっては、機能の追加や改修などのバージョンアップ等の頻度が多いクラウドサービス特有のリスクへの対応が疎かになり」	有り
2	個人Ｂ	P16　1．３．ガイドライン活用の効果 提案： ５．として次のような内容を追加してはどうか。 「５．本ガイドラインが、地方公共団体情報システムの標準化に関する法律　（法律第40号（令和３年5月19日））第１０条で務めることとされるクラウド・コンピューティング・サービス関連技術を地方公共団体が選択する際の指針となる。」 理由： 現在、内閣官房情報通信技術(IT)総合戦略室が地方自治体の情報システムについて、ガバメントクラウド（Gov-Cloud）を活用できるよう、具体的な対応方策や課題等について検討をすすめることとしており（地方自治体によるガバメントクラウドの活用について（案）令和３年6月）その中で、必須要件として「政府情報システムのためのセキュリティ評価制度（ISMAP）のリストに登録されたサービス」から調達する予定としている。（P4)しかし、次の点からISMAPは選択のガイドラインにはならないと考える。 １）ISMAPは政府情報システムに求められる情報セキュリティ対策について記載されているものであること ２）ISMAPは、「(1)CSPの「経営陣」が管理者層に対して、セキュリティに関する意思決定や指示等を継続的に実施し、(2)これを受けたクラウドサービスの「管理者」が的確にマネジメントを実施し、(3)クラウドサービスの「業務実施者」が実際にセキュリティ対策を実施していることを確認するための管理基準」（政府情報システムのためのセキュリティ評価制度（ISMAP）について令和２年６月３日（水））」(以下、ISMAP制度）を示しており、監査機関による監査の基準ではあるが、具体的にサービスレベルを示すものではないこと（P19) ３）ISMAPにおける監査は、「監査業務において、業務実施者の報告は、手続実施結果を事実に即して報告するのみにとどまり、手続実施結果から導かれる結論の報告も、保証も提供しない。」（ISMAP制度)ものであり、要件を満たしていることを保証されたものではないこと（P25) これに対して、本ガイドラインは、「ISMAP管理基準、ISO/IEC27017(2016)及びNIST SP800-53 Rev.55を参照」して改定されており、「自ら提供するクラウドサービスに適した情報セキュリティ対策を実施することが可能」で、「クラウドサービス利用者は、クラウドサービス事業者との契約やSLAの締結において、本ガイドラインを活用することが可能」となるよう「【ベストプラクティス】、【評価項目】及び対策参照値(SLA数値例)を付記している」ことから、選択の指針として最もふさわしいと考える。	いただいた御意見は、デジタル庁（旧：内閣官房情報通信技術総合戦略室）において検討を進めている「地方自治体によるガバメントクラウドの活用」に対する御意見と理解しています。 当ガイドラインは、その対象を地方公共団体の情報システムのみならず、すべてのクラウドサービス、システムを対象としているため、御指摘いただいた内容を追加することは適切ではないと考えます。 また、当ガイドラインに記載している[ベストプラクティス]や[評価項目]は、P21「Ⅰ．５．ガイドラインの読み方と利用方法」でも解説しているように、参考とすべき情報として提供しているものとなります。	無し
3	株式会社ラック	＜P.17＞ I.4.ガイドラインの全体構成 クラウドサービス形態毎に章を分けられていますが、形態を理解しやすい全体図を示した方が良いと思いました。「I.6.1. SaaS における管理と責任共有」で形態の説明がありますが、まずは、全体図を提示するか、あるいは用語の定義（P30以降）への参照要求があると良いと思います。	いただいた御意見を踏まえ、P17「Ⅰ．４．ガイドラインの全体構成」において、SaaS、PaaS、IaaSの定義への参照に関する脚注を追加します。	有り
4	株式会社ラック	＜P.23～P.26＞または、全体的に 「I.2.ガイドラインの位置付け」からは、読み手の対象はクラウドサービス事業者と認識していますが、「I.6.1. SaaS における管理と責任共有」では、事業者と利用者の双方が主語になっており、事業者を対象とした記述に統一した方がよいと考えます。クラウドサービス事業者が利用者になることも想定されているとも察しますが、少々わかりにくいと思います。	「Ⅰ．６．クラウドサービス事業者とクラウドサービス利用者の責任」では、クラウドサービス事業者とクラウドサービス利用者の責任分解について記載しており、クラウドサービス事業者における責任範囲とクラウドサービス利用者における責任範囲を明示的に記載し、主の読み手であるクラウドサービス事業者が双方の責任範囲を理解できるようにすることが重要と考えます。したがって、御指摘いただいた箇所については原案の通りとします。	無し
5	株式会社セールスフォース・ドットコム	該当箇所： （１３頁）「国内では、最近、クラウドサービスのバージョンアップに伴う設定変更によっ て、企業や個人の情報が流出したケースがある。」 コメント： 事例を掲載する際には、NISCの「次期サイバーセキュリティ戦略(案)」等と表現を合わせてみては如何か。 万が一、弊社関連の事例を当該表現が示しているのであれば、必ずしも正確な表現ではない。	いただいた御意見を踏まえ、P13「Ⅰ．１．はじめに」の記載を以下の通り修正します。 「国内では、最近、クラウドサービスのバージョンアップに伴う設定変更によって、企業や個人の情報が流出したケースがある。」 ⇒「国内では、最近、クラウドサービスへのアクセス権限の設定不備によって、企業や個人の情報が流出したケースがある。」	有り

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
6	株式会社セールスフォース・ドットコム	該当箇所： （２２頁）「ただし、責任共有モデルにおけるクラウドサービス事業者とクラウドサービス利用者の責任範囲・内容は一律に決まるものではなく、クラウドサービスの内容やクラウドサービス利用条件・環境ごとに、両者で責任範囲と内容について合意し、契約で明示することが重要である。」 コメント： 日本の多くのケースの場合、クラウドサービス事業者とクラウドサービス利用者との間に「システム受託事業者」が介在しており、現場ではその役割と影響力は共に絶大である。 「システム受託事業者」におかれてもクラウドサービスの「責任共有モデル」を十分理解するとともに、クラウドサービス事業者が適宜発する様々な情報発信に関する理解促進とともに技術的スキルのアップデートを促すよう、国からはアドバイスいただきたい。	クラウドサービス利用者に対してクラウドサービスを提供するケースにおいて、その提供形態や役割・責務の分担のあり方は多様であり、御指摘いただいた内容についても、その提供形態の一つの形であると理解しています。本ガイドラインにおいては、P22「Ⅰ．６．クラウドサービス事業者とクラウドサービス利用者の責任」でも記載しているように、「クラウドサービス事業者」「クラウドサービス利用者」の2つに分類した上で、そこでの責任範囲の一般的な在り方を示しており、そういった個別のケースへの言及まではしていません。 そのため、いただいた御意見については、今後のクラウドサービス提供の動向も踏まえ、必要に応じて今後改定を検討します。	無し
7	株式会社セールスフォース・ドットコム	該当箇所： （２３頁）「アカウント管理などの限定的な管理権限をクラウドサービス事業者から付与され、外部からのアクセス権限を設定する場合がある。」 コメント： 日本の多くのケースの場合、クラウドサービス事業者とクラウドサービス利用者との間に「システム受託事業者」が介在しており、現場ではアクセス権限の設定を「システム受託事業者」が実施しているケースが多い。加えて、「システム受託事業者」がクラウドサービス事業者が随時提供する情報発信を十分に理解できておらず、アクセス権限の設定に不備が生じるケースも散在している点をご理解いただきたい。	クラウドサービス利用者に対してクラウドサービスを提供するケースにおいて、その提供形態や役割・責務の分担のあり方は多様であり、御指摘いただいた内容についても、その提供形態の一つの形であると理解しています。本ガイドラインにおいては、P22「Ⅰ．６．クラウドサービス事業者とクラウドサービス利用者の責任」でも記載しているように、「クラウドサービス事業者」「クラウドサービス利用者」の2つに分類した上で、そこでの責任範囲の一般的な在り方を示しており、そういった個別のケースへの言及まではしていません。 そのため、いただいた御意見については、今後のクラウドサービス提供の動向も踏まえ、必要に応じて今後改定を検討します。	無し
8	株式会社セールスフォース・ドットコム	該当箇所： （２３頁）「(注) アプリケーションのバージョンアップにより、権限設定内容が変更され、情報漏洩に至った ケースが散見されているため、クラウドサービス事業者は、クラウドサービス利用者がバー ジョンアップによる情報セキュリティへの影響を見定めることができるよう、適切な情報提供を行う必要がある。」 コメント： 事例を掲載する際には、NISCの「次期サイバーセキュリティ戦略(案)」等と表現を合わせてみては如何か。 万が一、弊社関連の事例を当該表現が示しているのであれば、必ずしも正確な表現ではありません。 なお、「システム受託事業者」におかれてもクラウドサービスの「責任共有モデル」を十分理解するとともに、クラウドサービス事業者が適宜発する様々な情報発信に関する理解促進とともに技術的スキルのアップデートを促すよう、国からはアドバイスいただきたい。	いただいた御意見を踏まえ、P23「Ⅰ．６．１．SaaSにおける管理と責任共有」の記載を以下の通り修正します。 「アプリケーションのバージョンアップにより、権限設定内容が変更され、情報漏洩に至ったケースが散見されているため、クラウドサービス事業者は、クラウドサービス利用者がバージョンアップによる情報セキュリティへの影響を見定めることができるよう、適切な情報提供を行う必要がある。」 ⇒「アプリケーションのバージョンアップや機能の追加により、設定が不適切なものとなってしまい、情報漏洩に至ることが想定されるため、クラウドサービス事業者は、クラウドサービス利用者がバージョンアップや機能の追加による情報セキュリティへの影響を見定めることができるよう、適切な情報提供を行う必要がある。」	有り
9	株式会社セールスフォース・ドットコム	該当箇所： （２４頁）「また、クラウドサービス利用者は、クラウドサービス事業者が提供するセキュリティ機能(データバックアップ機能、認証機能、データ暗号化機能、ファイアウォール 機能、ログ管理機能等)を正しく理解して設定する必要がある。」 コメント： 「システム受託事業者」におかれても、クラウドサービス事業者が適宜発する様々な情報発信（セキュリティ機能のアップデートを含む）に関する理解促進とともに技術的スキルのアップデートを促すと共に、クラウドサービス利用者と連携を密に図るよう、国からはアドバイスいただきたい。	クラウドサービス利用者に対してクラウドサービスを提供するケースにおいて、その提供形態や役割・責務の分担のあり方は多様であり、御指摘いただいた内容についても、その提供形態の一つの形であると理解しています。本ガイドラインにおいては、P22「Ⅰ．６．クラウドサービス事業者とクラウドサービス利用者の責任」でも記載しているように、「クラウドサービス事業者」「クラウドサービス利用者」の2つに分類した上で、そこでの責任範囲の一般的な在り方を示しており、そういった個別のケースへの言及まではしていません。 そのため、いただいた御意見については、今後のクラウドサービス提供の動向も踏まえ、必要に応じて今後改定を検討します。	無し
10	株式会社セールスフォース・ドットコム	該当箇所： （２６頁）「また、クラウドサービスの情報セキュリティ対策のレベルは、サプライチェーンを構成する各事業者が提供するサービスの情報セキュリティ対策レベルの内、最も低いレベルとなる。したがって、クラウドサービスの情報セキュリティ対策のレベルを上げるには、サプライチェーンを構成する各事業者の責 任範囲を明確にした上で、各事業者が提供するサービスの情報セキュリティ対策のレベルを上げる必要がある。」 コメント： 「最も低いレベル」と表現する際の「レベル」と「情報セキュリティ対策のレベル」の「レベル」は異なる主旨か？	いずれも情報セキュリティ対策のレベルのことを指しています。	無し
11	情報処理学会 情報規格調査会 SC 38専門委員会	Ⅰ．２．ガイドラインの位置付け その提供主体としては中小規模も含むSaaS/PaaS/IaaSのクラウドサービス事業者を想定している。 「提供主体としては中小規模”も”含む」ということは全てのクラウドサービス事業者を対象としていると理解しました。つきましては、このガイドラインの対象を明確にするために、対象文中に「全ての」と明記してください。 その提供主体としては中小規模も含むSaaS/PaaS/IaaSの全てのクラウドサービス事業者を想定している。	いただいた趣旨を踏まえつつ、記載の平仄をそろえる観点で、P15「Ⅰ．２．ガイドラインの位置付け」の記載を以下の通り修正いたします。 「その提供主体としては中小規模も含むSaaS/PaaS/IaaSのクラウドサービス事業者を想定している」 ⇒「その提供主体としては中小規模も含むSaaS/PaaS/IaaS等の全てのクラウドサービス事業者を想定している」	有り

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
12	情報処理学会 情報規格調査会 SC 38専門委員会	Ⅰ．6．１．SaaSにおける管理と責任共有 Ⅰ．6．2. PaaSにおける管理と責任共有 Ⅰ．6．3. IaaSにおける管理と責任共有 記載されている図 SaaS/PaaS/IaaSにおける管理と責任共有の図に示されている「ミドルウエア」と「アプリケーション」の間に「ランタイム」が入りますので、追加してください。	御指摘いただいた「ランタイム」は、ランタイムライブラリの事を指していると理解しています。アプリケーションで利用されるランタイムライブラリは、一般的にはOSやミドルウェア事業者が提供するランタイムライブラリとなっており、アプリケーション実行の上で必要とされる機能という観点から、P22「Ⅰ．６．クラウドサービス事業者とクラウドサービス利用者の責任」では、ランタイムライブラリはミドルウェアの一部と位置付けています。 いただいた御意見を踏まえ、「ランタイム」の位置付けについて明確化するため、P23～P25の図中において、「ランタイムがミドルウェアの一部と位置付けられている」旨を追記します。	有り
13	情報処理学会 情報規格調査会 SC 38専門委員会	Ⅰ．6．１．SaaSにおける管理と責任共有 記載されている図と説明 図の中で「データ」はクラウドサービス利用者が管理するとしていますが、SaaSの場合、「データ」もクラウドサービス事業者の管理対象ですので、修正してください。それにしたがい、対象となる文も変更してください。 これは、本ガイドラインが対象とする「情報」の範囲が明確に定義されていないため、JIS X 001:1994の定義に従うと、類型や事例の説明で矛盾が生じる部分があると推察します。つきましては、I.2 ガイドラインの位置づけに対象とする情報の範囲を例示する一文を挿入してください。 このガイドラインで扱うデータとは、JIS Q 27000の概要で例示された情報資産として認識される、秘匿性、機密性の高い情報を主に想定している。 [参考] JIS X 0001;1994 01.01.01情報 事実，事象，事物，過程，着想などの対象物に関して知り得たことであって，概念を含み，一定の文脈中で特定の意味をもつもの。備考 図1参照。 01.01.02データ 情報の表現であって，伝達，解釈又は処理に適するように形式化され，再度情報として解釈できるもの。備考1. データに対する処理は，人間が行ってもよいし，自動的手段で行ってもよい。 JIS Q 27000「財務情報，知的財産，従業員情報，及び顧客又は第三者から委託された情報を含む，情報資産のセキュリティを管理するための枠組みを策定し」	P23「Ⅰ．６．１．SaaSにおける管理と責任共有」における「データ」は、本文中にあるとおり、「クラウドサービス事業者が提供するアプリケーションを利用するためのデータやアプリケーション上で生成したデータ」を指しています。また、同文中に記載している「管理」については、データに対する編集・削除等の行為のことを指しています。 「データ」が示す内容については明確に文中で示している一方で、「管理」が示す内容について不明確な記載となっていたことから、当該箇所の記載を以下の通り修正します。 「クラウドサービス事業者が提供するアプリケーションを利用するためのデータやアプリケーション上で生成したデータを管理する権限と責任を有する。」 →「クラウドサービス事業者が提供するアプリケーションを利用するためのデータやアプリケーション上で生成したデータの管理（データに対する編集・削除等の行為）をする権限と責任を有する。」	有り
14	情報処理学会 情報規格調査会 SC 38専門委員会	Ⅰ．7．１．垂直連携サプライチェーン1Ⅰ．7．３．水平連携サプライチェーン１ 記載されている図 クラウドサービス事業者Bからクラウドサービス事業者Aへの横矢印②「サービス提供」は、垂直連携サプライチェーンのクラウドサービス事業者Bからクラウドサービス事業者Aへの縦矢印②「サービス提供」は、サービス提供の方法が異なるため、違いが分かるよう図を変更してください。	いただいた御指摘箇所については、いずれのケースにおいても、クラウドサービス事業者Aとクラウドサービス事業者Bの間の契約に基づいて「サービス提供」をしていることを示しています。よって、原案の通りとします。	無し
15	情報処理学会 情報規格調査会 SC 38専門委員会	Ⅰ．7．４．水平連携サプライチェーン2 ③ クラウドサービス事業者A及びB間の連携部分に帰する問題が発生した場合は、クラウドサービス事業者AとB間との契約に基づき、対処する。 図中に示されている両矢印③は、同じ「水平連携」という意味で、Ⅰ．7．３．水平連携サプライチェーン1との比較で考えると、API連携ということなろうかと思いますので以下を追加してください。 ③ クラウドサービス事業者AとBがAPI連携により両クラウドサービスが連携し、クラウドサービス事業者A及びB間の連携部分に帰する問題が発生した場合は、クラウドサービス事業者AとB間との契約に基づき、対処する。	クラウドサービス事業者Aとクラウドサービス事業者Bの間での連携は、データベースの機能を利用した同期といった手法も考えられ、API連携に限らないため、原案の通りとします。	無し
16	情報処理学会 情報規格調査会 SC 38専門委員会	Ⅰ．９．参考文献 クラウドコンピューティングのクラウドSLAに関する国際規格（ISO/IEC 19086）のJIS規格（IDT）が存在しますので、参考文献として掲載してください。 JIS X 9501-1:2019 情報技術―クラウドコンピューティング―サービスレベル合意書（ＳＬＡ）の枠組―第１部：概要及び概念	御指摘の内容を踏まえ、P39「Ⅰ．９．参考文献」に以下を追記します。 ・JIS X 9501-1：2019 「情報技術ークラウドコンピューティングーサービスレベル合意書（ＳＬＡ）の枠組ー第１部：概要及び概念」	有り
17	情報処理学会 情報規格調査会 SC 38専門委員会	Ⅰ．８．用語の定義 SLA（Service Level Agreement） 書面にしたサービス提供者と顧客との合意であって、サービス及び合意したサービスレベルを記載したもの（JIS Q 20000-1:2007） 参考文献として掲載されているクラウド用語のJIS規格（X 9401:2016）にSLAの定義がなされていますので、それを参照してください。	「JIS X 9401：2016」も参照した上で、本ガイドラインにおけるＳＬＡの定義をP38に記載しています。 本定義は「JIS Q 20000-1:2007」のみを参照しているわけではないことから、当該記述から「（JIS Q 20000-1:2007）」を削除します。	有り

■「Ⅱ．共通編」に対する御意見

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
18	個人Ａ	Ⅱ．４．２．１.【基本】資産目録 パターンが4種類に分かれているが簡易な説明を補記できないか。 例） パターン1：決済インフラなど24h365dでの可用性が要求され取扱う情報の重要度も高い パターン2：機密性の高い個人情報を扱うWebサービスなど パターン3：機密性の高い情報は扱わないが、気象情報など高い可用性が求められるサービス パターン4：高い機密性や可用性は要求されないが、統計データなど正確な情報提供が求められるサービス	御指摘いただいた内容については、P191~P193「ANNEX1 クラウドサービスのパターン」においてパターンごとのサービス種別を例示しています。 P17の「Ⅰ．４．ガイドラインの全体構成」でも当該ANNEXへの参照をしていますが、より読みやすくする観点から、P21「Ⅰ．5．ガイドラインの読み方と利用方法」の「４．評価項目」及び「５．対策参照値」について説明する箇所でサービスパターンへの言及と当該ANNEXへの参照について追記します。	有り
19	個人Ａ	Ⅱ．４．４．５.【基本】アクセス制御となりすまし対策 ※その他、以降の同一の表に記載の箇所 表に記載されているパターン1-4が何を指しているのかが分かりにくいため、「Ⅱ．４．２．１.【基本】資産目録」記載のパターンである旨の注釈を入れてはどうか。また、その認識が合っている場合、「Ⅱ．４．４．５.【基本】アクセス制御となりすまし対策」の多要素認証有無（機密性、完全性）や、「Ⅱ．１．１．３.【基本】稼働・障害監視」の稼働率（可用性）など全般的に整合性の確保が望ましい（完全性「高」だが多要素認証不要となっている等）	御指摘いただいた内容については、P191~P193「ANNEX1 クラウドサービスのパターン」においてパターンごとのサービス種別を例示しています。 P17の「Ⅰ．４．ガイドラインの全体構成」でも当該ANNEXへの参照をしていますが、より読みやすくする観点から、P21「Ⅰ．5．ガイドラインの読み方と利用方法」の「４．評価項目」及び「５．対策参照値」について説明する箇所でサービスパターンへの言及と当該ANNEXへの参照について追記します。	有り
20	個人Ａ	Ⅱ．４．5．４.【推奨】変更に対するアクセス制限 「二重認証」の具体的内容がイメージできないため、多要素認証のように用語説明があった方が分かりやすいと感じる。	P55「Ⅱ．４．５．４.【推奨】変更に対するアクセス制限」に記載している「二重認証」の意味を明確化する観点で、当該管理策のベストプラクティス「ii」を以下の通り修正します。 「ii 選択されたシステムコンポーネントと情報に対するすべての変更は、資格のある二人の個人によって実施することが出来、二重認証を導入する。」 ⇒「ii 選択されたシステムコンポーネントと情報に対するすべての変更は、資格のある二人の個人による二重の承認を要求する。」	有り
21	株式会社ラック	＜P.44＞ II.2.1.4.【推奨】リスク管理戦略 技術的ぜい弱性の管理に関する要件は、ガイドライン全体を通して基本的な要件として記述されていますが、リスク管理戦略において「情報セキュリティへの侵害が、業務、情報資産、個人、他の組織及びサプライチェーンへもたらす脅威に対するリスクを管理するために、組織全体の包括的なリスク管理戦略を策定する。リスク管理戦略は、定期的又はクラウドサービスの提供に係る変更が生じた場合(組織環境、業務環境、法的環境、技術的環境等)に見直しを行うこと。」とあるように、クラウドサービスの提供に係る変更が生じるような技術的或いは管理的環境等の変化は重大な技術的並びに管理的ぜい弱性の顕在化も含まれると考えます。 クラウドサービスの提供に係る変更が生じるような重大な技術的及び管理的ぜい弱性は時機を失せずに察知し、速やかにサービスに係る影響や状況を把握しなければならないと考えますので、【推奨】というのは整合性に欠けると感じました。 可能であれば、リスク管理戦略を【基本】とするか、ベストプラクティスに、「クラウドサービスの提供に係る変更が生じるような技術的ぜい弱性を確認した場合には、速やかに、 ・当該ぜい弱性に組織がさらされている状況の評価 ・それらと関連するリスクに対処するために、適切な手段をとった状況 ・提供するクラウドサービスに影響し得る技術的ぜい弱性の管理に関する情報の共有状況 以上の状態を常に報告可能な体制にすること、 等を加え、さらに管理的ぜい弱性にも配慮を促す文言を追加されることを望みます。	御指摘いただいた内容（技術的及び管理的ぜい弱性の察知及び影響や状況の把握）については、P59「Ⅱ．６．１．情報セキュリティインシデント及びぜい弱性の報告」において、「全ての従業員に対し、業務において発見したあるいは疑いをもったシステムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続を定め、実施を要求すること。」と記載しており、御指摘いただいた内容と同様の趣旨の記載が既に存在します。 また、これらの把握したぜい弱性情報を踏まえたリスク評価や対応に関しては、 P78「Ⅲ．１．１．１６.【基本】 技術的ぜい弱性」 又は P93「Ⅳ．１．１．１６.【基本】 技術的ぜい弱性」 において、「そのようなぜい弱性に組織がさらされている状況を評価すること。さらに、それらと関連するリスクに対処するために、適切な手段をとること。」と記載しており、これについても既に御指摘いただいた趣旨は反映できていると考えます。	無し
22	株式会社ラック	＜P.47＞ II.3.1.2.【基本】 サービスの監視 クラウドサービス事業者は扱うシステムが膨大かつ広範囲になるため、効率よく一元管理することで「統合的に監査できるようにする」というような意図をベストプラクティスに追加すると良いと考えます。	いただいた御意見は、当該クラウドサービス事業者において複数のクラウドサービスを提供する際の、効率の良い監査の実装方法に関する内容と理解しています。当該管理策では、単一のクラウドサービスに対して「サプライチェーン事業者が提供するクラウドサービスを定常的に監視・レビューし、運用に関する記録及び報告を常に実施」することと、「定期的に監査を実施することについて、サプライチェーン事業者と合意し文書化」することについて記載しているため、御指摘の内容は当管理策におけるベストプラクティスとしては不適切と考えます。	無し

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
23	株式会社ラック	＜P.59＞ Ⅱ．６．１．情報セキュリティインシデント及びぜい弱性の報告 Ⅱ．６．１．１.【基本】組織内報告において 本ガイドラインにおけるインシデント管理全般について 本ガイドラインにおいて参照されているNISTのSP800シリーズ中、NIST Special Publication 800-61（コンピュータセキュリティインシデント対応ガイド）にはインシデント発生に関しての窓口の設置としてのCSIRT(Computer Security Incident Response Team) の設置が明示的に記載されているところ。しかしながら本ガイドラインにおいては、インシデント対応の個別具体的な詳細な管理策や対応に関する記載はあるのですが、明示的なCSIRTという表現ではなく Ⅱ．６．１．情報セキュリティインシデント及びぜい弱性の報告 Ⅱ．６．１．１.【基本】組織内報告において「組織内での責任体制及び手順を確立すること」という表現にとどまっており、かつまた対外的な窓口の設置に関する言及がわかりにくいと思われます。 また脆弱性管理においては昨今では開発したアプリケーションソフトウエアに関する脆弱性対応の窓口としてPSIRT（Product Security Incident Response Team）などの設置の必要性も提唱されていることから、機能ごとに分けた考え方として内閣サイバーセキュリティセンター（NISC）の普及啓発・人材育成専門調査会資料 https://www.nisc.go.jp/conference/cs/jinzai/dai15/pdf/jinzai_houkousei や経済産業省　サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引きにおいても https://www.meti.go.jp/press/2021/04/20210426002/20210426002-1.pdf インシデント対応に備えた機能（xSIRT）の確保に関する検討部分に 「xSIRT（セキュリティー・インシデント・レスポンス・チーム）」の設置という考え方が記載されております。 xにはコンピューター（Computer）の「C」や製品・サービス（Product）の「P」、工場（Factory／Manufacture）の「F／M」が入り、対応する部門に応じてCSIRTやPSIRTと呼ばれることから、本ガイドラインも各カテゴリ（Saas,Iass,Paas）毎に記載がありますので、これらのカテゴリに関するインシデント管理にかかわる、組織内及び対外的な窓口として明示的に対応窓口の設置を推奨するとともに、CSIRTあるいはPSIRT等と記載表現する形で、より明確化が図れると考えられます。ぜひ次期検討事項としてご検討いただけますと幸甚です。	いただいた御意見については、今後の取組の参考とさせていただきます。	無し
24	株式会社ラック	＜P.61＞ II.7.コンプライアンス この章は共通編として国や地域を跨ぐ可能性があることを前提にコンプライアンスに触れていますが、SaaS、IaaS/PaaSといった形態それぞれに注意ポイント、要点が存在すると思いますので、例として示すと良いと考えます。	「Ⅱ．共通編」ではSaaS、IaaS/PaaSのいずれかにかかわらず、共通的に実施する対策を記載しているため、原案の通りとします。	無し
25	株式会社ラック	＜P.40～P.70＞ 共通 クラウドサービス利用者は事業者の環境にデータを保管することになりますので、事業者はこれらの情報を明示しておくが望ましいと考えます。	いただいた御意見の趣旨を踏まえ、P22「Ⅰ．6．クラウドサービス事業者とクラウドサービス利用者の責任」に以下の記述を追記します。 「また、双方の責任範囲において、クラウドサービス利用者がセキュリティ上のリスクを判断できるように、クラウドサービス事業者はクラウドサービス利用者に対して、クラウドサービスの内容やクラウドサービス利用条件・環境等について適切に情報提供をする必要がある。」	有り
26	株式会社ラック	＜P.40～P.70＞ 共通 本書では事業者が実施すべきセキュリティ対策が具体的に記載されており、有効にガイドになると思います。 一方で、PaaSやIaaSはOSやアプリケーションなどは利用者側の責任となり、ここでの対策が不十分であれば、不利益を被る事業者や国民が生じる恐れがあると推察します。 そこで、事業者側から利用者向けに提供するサービスに則した分りやすいセキュリティ対策ガイドを準備して提供するのはいかがでしょうか。 全体してのセキュリティ対策の底上げにもつながるのではないかと考えます。	いただいた御意見については、今後の取組の参考とさせていただきます。	無し
27	株式会社ラック	＜P.72～P.85＞ 共通 SaaS事業者に必要な管理機能と、利用者に提供する機能は異なることが想定されます。これら異なる機能のアプリケーションおよびデータ・保守の分離を明示したほうが良いと思います。 これはSaaS、IaaS、PaaS問わず、共通項目に含めるのが望ましいと考えます。	「Ⅲ．SaaS編」で言及している「アプリケーション」には、利用者に提供するためのアプリケーションと、SaaSにおける管理のためアプリケーションの両方が含まれています。 一方で、「Ⅳ．PaaS/IaaS編」において、PaaS/IaaSにおける管理のためのアプリケーションへの言及が含まれていなかったため、P87～P89の記載を以下の通り修正します。 「クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器」 →「クラウドサービスの提供に用いる管理機能を持つアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器」	有り

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
28	株式会社セールスフォース・ドットコム	該当箇所： （５７頁）「このため、事業者及び利用者内でそれぞれの役割を担う従業員に対して、クラウドサービス特有のセキュリティに対して意識向上を図るための啓発、教育及び訓練を実施する必要がある。」 コメント： 日本の多くのケースの場合、クラウドサービス事業者とクラウドサービス利用者との間に「システム受託事業者」が介在しており、現場ではセキュリティ対策の設定等を「システム受託事業者」が実施しているケースが多い。ついては、「システム受託事業者」におかれてもクラウドサービスの「責任共有モデル」を十分理解するとともに、クラウドサービス事業者が適宜発するセキュリティ対策を含む様々な情報発信に関する理解促進とともに技術的スキルのアップデートを促すよう、国からはアドバイスいただきたい。	クラウドサービス利用者に対してクラウドサービスを提供するケースにおいて、その提供形態や役割・責務の分担のあり方は多様であり、御指摘いただいた内容についても、その提供形態の一つの形であると理解しています。本ガイドラインにおいては、P22「Ⅰ．６．クラウドサービス事業者とクラウドサービス利用者の責任」でも記載しているように、「クラウドサービス事業者」「クラウドサービス利用者」の2つに分類した上で、そこでの責任範囲の一般的な在り方を示しており、そういった個別のケースへの言及まではしていません。 そのため、いただいた御意見については、今後のクラウドサービス提供の動向も踏まえ、必要に応じて今後改定を検討します。	無し
29	ヴイエムウェア株式会社	（「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」（案）P45中「j) 業務情報のバックアップ　k) ウェブサービス及びウェブアプリケーションの使用」との記載部分） ・意見内容 当該部分について「j) 業務情報のバックアップ　k) ウェブサービス及びウェブアプリケーションの使用　l)脅威情報に応じた段階的な動的アクセス制御」との変更を提案します。 （理由） 「ii. モバイル機器の方針には、保護されていない環境においてモバイル機器を用いた作業のリスクを考慮に入れるとともに、次の事項を考慮する。」に関連して列挙される各項目において「保護されていない環境」は常に存在するわけではなく、なんらかの理由によって生じてしまう状況です。そのため、保護されていない環境への考慮としては、その環境に至る前段階として自動的なアクセス制御を行うことが必須であるため、そのことを明示すべきと考えます。併せて、一度に全面的なアクセス制御を行うのではなく、部分的なアクセス制御を段階的に適用していくことが利便性の観点からも重要です。	御指摘いただいた「脅威情報に応じた段階的な動的アクセス制御」に関しては、P45「Ⅱ．２．２．１．【基本】モバイル機器の利用方針」のベストプラクティス「ii」中に記載されている「f) アクセス制御」に内包されているため、原案の通りとします。	無し
30	ヴイエムウェア株式会社	（「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」（案）P46中「j) マルウェアに対する保護及びファイアウォールの要件」との記載部分） ・意見内容 当該部分について「j) マルウェアに対する保護及びファイアウォールの要件k)脅威情報に応じた段階的な動的アクセス制御」との変更を提案します。 （理由） 「保護されていない環境」は常に存在するわけではなく、テレワーキングにおいてなんらかの理由によって生じてしまう状況です。そのため、保護されていない環境への考慮としては、その環境に至る前段階として自動的なアクセス制御を行うことが必須であるため、そのことを明示すべきと考えます。併せて、一度に全面的なアクセス制御を行うのではなく、部分的なアクセス制御を段階的に適用していくことが利便性の観点からも重要です。	いただいた御意見を踏まえ、P45「Ⅱ．２．２．２．【基本】テレワーキングでの情報保護」のベストプラクティス「i」に以下を追記します。 「k) 脅威情報に応じた段階的な動的アクセス制御」	有り
31	ヴイエムウェア株式会社	（「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」（案）P52中「各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるように、定期的にレビュー及び見直しを行うこと。」との記載部分） ・意見内容 当該部分について「各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるように、脅威情報の最新化、設定・構成変更時及び定期的にレビュー及び見直しを行うこと。」を提案します。 （理由） 情報インシデントに対する対応として、半年ごと等の予め設定された定期的なレビューでは脅威に対する柔軟性が十分ではないため、脅威情報がアップデートされた際や、設定・構成が変更された際にも積極的にレビューされるべきことを明示すべきと考えます。定期的なレビューのみではセキュリティに対する考え方が陳腐化してしまう可能性があります。	いただいた御意見の趣旨を踏まえ、P52「Ⅱ．４．３．１．【基本】レビュー」の記載を以下の通り修正します。 「情報セキュリティポリシーに則り正しく確実に実施されるように、定期的にレビュー及び見直しを行うこと。」 ⇒「情報セキュリティポリシーに則り正しく確実に実施されるように、定期的に及び脅威の変化や設定・構成変更等の状況変化に応じてレビュー及び見直しを行うこと。」	有り

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
32	ヴイエムウェア株式会社	（「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」（案）P59中「【ベストプラクティス】i. 情報セキュリティインシデント及びぜい弱性を統括管理する組織と連携して情報セキュリティインシデントの正式な報告手順、報告を受けた後のインシデント対応及び段階的取扱い（例：原因切り分け、部分復旧、完全復旧のフェーズに分けた取扱い）の手順を確立する。また、情報セキュリティインシデントの報告手順を全ての従業員に周知徹底する。」との記載部分） ・意見内容 当該部分について「【ベストプラクティス】i. 情報セキュリティインシデント及びぜい弱性を統括管理する組織と連携して情報セキュリティインシデントの正式な報告手順、報告を受けた後のインシデント対応及び段階的取扱い（例：原因切り分け、部分復旧、完全復旧のフェーズに分けた取扱い）の手順を確立する。併せて、セキュリティインシデントの発生を契機とした、利便性を踏まえた段階的な機能制限・アクセス制御を用いて被害を最小化するアプローチも併せておこなっていく必要がある。また、情報セキュリティインシデントの報告手順を全ての従業員に周知徹底する。」との変更を提案します。 （理由） 情報セキュリティインシデントの対応において、原案では利便性を維持しつつ被害拡大を抑制するフェーズに触れられていないため、被害拡大抑制の段階で迅速に行うべき手段を明示し、広く認知を行うことが必要と考えます。	いただいた御意見の趣旨を踏まえ、「サービス運用に対する影響の最小化のため」という観点を明確にするために、P59「Ⅱ．６．情報セキュリティインシデントの管理」の記載を以下の通り修正します。 「情報セキュリティインシデントが発生した場合、事業者と利用者は責任と役割を分担して、原因の切り分けや影響への対処を行う必要がある。」 →「情報セキュリティインシデントが発生した場合、サービス運用に対する影響の最小化のため、事業者と利用者は責任と役割を分担して、原因の切り分けや影響への対処を行う必要がある。」 なお、御指摘いただいたベストプラクティス中において、「インシデント対応」と「段階的取扱い」が並列される表現となっていますが、「段階的取扱い」は「インシデント対応」に包含されるものであることから、当該箇所を以下の通り修正します。 「報告を受けた後のインシデント対応及び段階的取扱い」 →「報告を受けた後のインシデント対応における段階的取扱い」	有り

■「Ⅲ．SaaS編」に対する御意見

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
33	株式会社ラック	＜P.78＞ III.1.1.16.【基本】 技術的ぜい弱性 【ベストプラクティス】 ｉ ぜい弱性の診断対象(アプリケーション等)、診断方法(ポートスキャンツールやぜい弱 性診断ツールの使用等)、診断時期等の計画を明確にする。 クラウド事業者の外部との連携用のインターフェイを公開しています。ここでの問題が散見されるため、診断対象にアプリケーションに加え、インターフェイスを加えたほうが実情に適したガイドになると考えます。 ぜい弱性の診断対象(インタフェースやアプリケーション等)、～(以下同じ)～	いただいた御意見を踏まえ、P78「Ⅲ．１．１．１６．【基本】技術的ぜい弱性」のベストプラクティス「i」を以下の通り修正します。 「ぜい弱性の診断対象(アプリケーション等)」 →「ぜい弱性の診断対象(インタフェースやアプリケーション等)」 ※同様の記述が「Ⅳ．１．１．１６」にもあるため、そちらも併せて修正します。	有り
34	株式会社セールスフォース・ドットコム	該当箇所： （７３頁）時間帯におけるクラウドサービスの稼働率を規定すること。 コメント： 稼働率を提供してないクラウドサービス事業者が多い認識である。稼働状況の確認ではいかがだろうか？	当ガイドラインにおいては、クラウドサービス事業者とクラウドサービス利用者間における認識齟齬等に起因するトラブルの発生を抑止するという観点から、稼働率に関してSLAなどで明確に規定することが望ましいと考えているため、御指摘いただいた箇所に関しては原案の通りとします。	無し
35	株式会社セールスフォース・ドットコム	該当箇所： （７３頁）「速報先は利用者側の管理連絡窓口のみとする。」 コメント： パブリッククラウドでは、速報先は登録したユーザとなるので、そのような記載はいかがだろうか？	いただいた御意見の趣旨を踏まえ、P73「Ⅲ．１．１．３．【基本】稼働・障害監視」のベストプラクティス「iii」の記載を以下の通り修正します。 「iii ここで、速報先は利用者側の管理連絡窓口のみとする。」 →「iii ここで、速報先には利用者側の管理連絡窓口だけでなく、クラウドサービスを利用する全ての者を含む。」	有り
36	株式会社セールスフォース・ドットコム	該当箇所： （７５頁）パスワード管理システム コメント： 他要素認証を必須とするのはいかがだろうか？	P75「Ⅲ．１．１．７．【基本】パスワード管理」では、クラウドサービスにおけるパスワードの在り方について記載しているものであり、認証についてはP54「Ⅱ．４．４．５．【基本】アクセス制御となりすまし対策」において、多要素認証について言及しています。	無し
37	株式会社セールスフォース・ドットコム	該当箇所： （７８頁）「アドレス空間のランダム配置（ASLR）」機能や「実行保護（ESP）」機能を採用する。 コメント： パブリッククラウドでこのような機能を提供している事業者はおそらくないと思うがいかがだろうか？	P78「Ⅲ．１．２．２．【推奨】メモリ保護」に記載されている「アドレス空間のランダム配置（ASLR）」及び「実行保護（ESP）」は、クラウドサービス利用者に提供する機能ではなく、クラウドサービス事業者側で実現する、メモリを保護するための機能のことを指しています。よって、御指摘いただいた箇所については、原案の通りとします。	無し

■「Ⅳ．PaaS/IaaS編」に対する御意見

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
38	個人Ｃ	本ガイドラインの対象として、P-15に「本ガイドラインは、地方公共団体及び民間事業者を含むあらゆる主体が利用するクラウドサービスに求められる情報セキュリティ対策を記載しており、その提供主体としては中小規模も含むSaaS/PaaS/IaaSのクラウドサービス事業者を想定している。」 また、参考文献として ・政府情報システムのセキュリティ評価制度(ISMAP)管理基準(略称:ISMAP管理基準) ・政府機関の情報セキュリティ対策のための統一基準（平成30年度版） を挙げ、データの消去方法として、 Ⅳ．４．３．６．【基本】装置のセキュリティを保った処分又は再利用（P-108）において、 記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを全て消去していること、若しくはセキュリティを保って上書きしていることを検証すること。事業者は、装置のセキュリティを保った処分又は再利用を行うための取決めについて、利用者と合意していること。 【ベストプラクティス】 i. 秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊するか、又はその情報を破壊、消去若しくは上書きする。 ii. 消去又は上書きには、標準的な消去又は初期化の機能を利用するより、元の情報を媒体から取り出せなくする技術を利用する。 と記載されているが、一昨年末に発生した神奈川県に於けるHDD流出事件を機に、昨年12月28日に改訂・発表された、「地方公共団体における情報セキュリティポリシーに関するガイドライン(令和2年12月版）（https://www.soumu.go.jp/main_content/000727474.pdf ）」に於いては、NISTSP800-88Rev.1の内容に従い、情報の機密度に従いデータ抹消方法を選択することが推奨され、図表24 情報の機密性に応じた機器の廃棄等の方法において「暗号化消去」の記載がされており、「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（令和３年度版）（https://www.nisc.go.jp/active/general/pdf/kijyunr3.pdf ）」では「暗号化消去」、「情報の抹消」として、下記の記載がされている。 ●「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（WindowsのBitLocker等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。 ●「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。 この点を考慮すると、これから改訂を行う「クラウドサービス提供における情報セキュリティ対策ガイドライン」として、「装置のセキュリティを保った処分又は再利用」のための【ベストプラクティス】を、「ii. 消去又は上書きには、標準的な消去又は初期化の機能を利用するより、元の情報を媒体から取り出せなくする技術を利用する。」とするのは、あまりにも不用意ではないか。参照資料を、「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（令和３年度版）とし、SP 800-88Rev.1に於けるPurge（除去）レベルの情報抹消効果を得ることの出来る手段を明示している「地方公共団体における情報セキュリティポリシーに関するガイドライン(令和2年12月版)」図表24中の（２）レベルの表記を行うことが必要ではないのか。	P108「Ⅳ．４．３．６．【基本】装置のセキュリティを保った処分又は再利用」の本文中で記載している「消去」は御指摘いただいた「暗号化消去」も内包しています。一方で、当該管理策におけるベストプラクティスの現状の記載で暗号化消去を読み取ることができないため、ベストプラクティスの記載を明確化する観点で、「i」「ii」を以下の通り修正します。 「i. 秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊するか、又はその情報を破壊、消去若しくは上書きする。」 ⇒「i. 秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊するか、又はその情報を消去若しくは上書きする。」 「ii. 消去又は上書きには、標準的な消去又は初期化の機能を利用するより、元の情報を媒体から取り出せなくする技術を利用する。」 ⇒「ii. 消去又は上書きには、標準的な消去又は初期化の機能を利用するより、消磁や暗号化消去等の手法で元の情報を復元不可能な状態にするための技術を利用する。」	有り
39	個人Ｄ	・「火さい、雷、静電気からシステムを防護するための対策」のベストプラクティスとして「二酸化炭素消火器」を挙げるのは問題があると考えました ・二酸化炭素は一定濃度を超えた場合、対人毒性を持つ気体です ・二酸化炭素消火器の使用については消防庁などから十分な教育と知識を持って使用するよう注意喚起も出ております。また実際に二酸化炭素消火器利用による事故も発生しております ・斯様に二酸化炭素消火器は利用方法の難しい消火器なので、総務省が公開するガイドラン上でベストを称するには相応しく無いと考えた次第です ・同じく設備の汚損を考慮するのであれば、ガスの大気中への放散後も環境影響の少ない窒素、アルゴンなどの大気構成成分となるガスを使用するか、超純水消火器などの利用が望ましいのではないかと考えた次第です	いただいた御意見を踏まえ、P106「Ⅳ．４．２．１．【基本】汚損対策」のベストプラクティス「ii」を以下の通り修正します。 「ii ガス系消火設備としてよく利用されるのは二酸化炭素消火器である。二酸化炭素消火器は、液化二酸化炭素を圧力により放射して消火を行う消火器である。」 ⇒「ガス系消火設備としてよく利用されるのは不活性ガス又はハロゲンガスを用いた消火設備である。」	有り
40	ヴイエムウェア株式会社	（「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」（案）P91中「iii. マルウェアの検出及び修復ソフトウェアだけを利用するのではマルウェア対策として不十分であるため、マルウェアの侵入を防止するための運用手順を併用する。」との記載部分） ・意見内容 当該部分について「iii. マルウェアの検出及び修復ソフトウェアだけを利用するのではマルウェア対策として不十分であるため、マルウェアの侵入を防止するための運用手順を併用する。iv．システムやクラウドサービスへの侵入痕跡を検索又は既存の制御を回避する脅威を検出、追跡及び妨害するサイバー脅威ハンティング機能を導入する。」との変更を提案します。（挿入箇所は（案）P44に記載の文章と同じです） （理由） 原案に示されている既知のマルウェアに対する対策に加えて、ivとして未知のマルウェアへの対策についても併記する必要があると考えます。	いただいた御意見を踏まえ、P91「Ⅳ．１．１．１１．【基本】マルウェア対策」のベストプラクティスに以下の内容を追記します。 「iv．システムやクラウドサービスへの侵入痕跡を検索又は既存の制御を回避する脅威を検出、追跡及び妨害するサイバー脅威ハンティング機能を導入する。」	有り
41	ヴイエムウェア株式会社	（「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」（案）P101中「i. 外部からの不正アクセスを検出するには、IDS/IPS 等を導入する。」との記載部分） ・意見内容 当該部分について「i. 外部からの不正アクセス及び内部通信における不正アクセスを検出するために、IDS/IPS等を導入する。」との変更を提案します。 （理由） IDS/IPSは、外部との通信に適用すべきものであると同時に、昨今問題が顕在化している内部通信における不正アクセスにも有効であることを踏まえ、内部通信における不正アクセス検出にもIDS/IPSを用いることを本ガイドラインによって広く社会に明示することが必要と考えます。	いただいた御意見を踏まえ、P101「Ⅳ．３．１．４．【基本】パケット検知」のベストプラクティス「i」の記載を以下の通り修正します。 「i. 外部からの不正アクセスを検出するには、IDS/IPS等を導入する。」 →「i. 不正アクセスを検出するには、IDS/IPS等を導入する。」 また、同時に「Ⅰ．８．用語の定義」における「IDS・IPS（Intrusion Detection System・Intrusion Prevention System）」の記載を以下の通り修正します。 「IDS・IPSはシステムやネットワークに対する外部からの不正行為を検出するシステム。」 →「IDS・IPSはシステムやネットワークに対する不正行為を検出するシステム。」	有り

■ガイドライン案全般に対する御意見

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
42	個人Ｅ	クラウドサービスを提供している事業者はセキュリティの観点からそのクラウドサーバーの場所を公表していないことが多い。一方で行政機関がクラウドサービスの利用を検討する際に主に上席（幹部）の職員がサーバーの場所を過度に気にする傾向があり、検討が停滞することがある。 もちろん、データを預ける以上、全くの業者まかせになるのは間違いではあるが、セキュリティ上公開していないものをもって導入の検討から外すのは、IT化の妨げともなる。 ガイドラインでは、サーバーの場所を業者が公表しないケースにおける対応を明示していただきたい。	いただいた御意見の趣旨を踏まえ、P22「Ｉ．６．クラウドサービス事業者とクラウドサービス利用者の責任」に以下の記述を追記します。 「また、双方の責任範囲において、クラウドサービス利用者がセキュリティ上のリスクを判断できるように、クラウドサービス事業者はクラウドサービス利用者に対して、クラウドサービスの内容やクラウドサービス利用条件・環境等について適切に情報提供をする必要がある。」	有り
43	個人Ｆ	＞全体的に 以前から述べている事であるが、一般的な民間のクラウド事業者は結局民間・第三者となる事業者であって、その公正性はあまり保証されるものではなく、またそのホストが香港やシンガポールである事も多くあるので、重要な情報は置くべきではないと考える。 あくまで計算機資源が足りない際にサービス提供を行うためのものという扱いとし、重要情報・個人情報についてはクラウドに置かないようにされたい。	いただいた御意見については、今後の取組の参考とさせていただきます。	無し
44	個人Ｇ	「サイバーセキュリティー対策」が重要な構造と、私し個人は思います。例えばですが、「センサー技術、 ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。具体的には、「電波規格（エレクトロリカルウェーブスペック）」及び「通信規格（トランスミッションスペック）」での「回線（サーキット）」の事例が有ります。（ア）「通信衛星回線（サテライトシステム）」における「トランスポンダー（中継器）」から成る「ファンクションコード（チャンネルコード及びソースコード）」のポート通信での「DFS（ダイナミックフレカンシーセレクション）」の構造。（イ）「電話回線（テレコミュニケーション）」における基地局制御サーバーから成る「SIP サーバー（セッションイニテーションプロトコル）」の構造。（ウ）「インターネット回線（ブロードバンド）」におけるISPサーバーから成る「DNSサーバー（ドメインネイムシステム）」の構造。（エ）「テレビ回線（ブロードキャスト）」における「通信衛星回線、電話回線、インターネット回線」の構造。具体的には、「方式（システムスペック）」での「回線（サーキット）」の事例が有ります。（ア）「3G（第3世代）」における「GPS（グローバルポジショニングシステム）」から成る「3GPP方式（GSM方式及びW-CDMA方式）」の構造。（イ）「4G（第4世代）」における「LTE方式（ロングタームエボリューション）」から成る「Wi-Fi（ワイアーレスローカルエリアネットワーキング）」の構造。（ウ）「5G（第5世代）」での「NR（NewRadio）」における「MCA方式（マルチチャンネルアクセス）」から成る「DFS（ダイナミックフレカンシーセレクション）」の構造。具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例が有ります。（ア）クラウドコンピューティングでは、「ビッグデータ（BD）」から成る「データーベース（DB）」の導入により、ITネットワークの構造。例えばですが、ファイアーウォールにおける強化では、ルーターとスイッチを挟み込む様に導入する事で、「クラウド側（プロバイダー側）←ルーター⇔ファイアーウォール⇔スイッチ→エッジ側（ユーザー側）」を融合する事で、ハードウェアーの強化の構造。（イ）エッジコンピューティングでは、Web上における「URL（ユニフォームリソースロケーター）」での「HTML（ハイパーテキストマークアップラングエッジ）」から成る「API（アプリケーションプログラミングインタフェース）」に導入により、「HTTP 通信（ハイパーテキストトランスファープロトコル）」における暗号化によるソフトウェアーでの「HTTPS（HTTP over SSL/TLS）」の融合により、AIネットワークの構造。具体的には、「サイバー空間（情報空間）」及び「フィジカル空間（物理空間）」での「回線（サーキット）」の事例が有ります。（ア）「サイバー空間（情報空間）」では、「SDN/NFV」における「仮想化サーバー（メールサーバー、Web サーバー、FTP サーバー、ファイルサーバー）」から成る「リレーポイント（中継点）」での「VPN（バーチャルプライベートネットワーク）」が主流な構造。（イ）「フィジカル空間（物理空間）」では、「AP（アクセスポイント）」が主流な構造。要約すると、「ボット（機械における自動的に実行する状態）」による「DoS攻撃」及び「DDoS攻撃」でのマルウェアーにおける「C＆Cサーバー（コマンド及びコントロール）」では、「LG-WAN（ローカルガーブメントワイドエリアネットワーク）」を導入した「EC（電子商取引）」の場合では、クラウドコンピューティング及びエッジコンピーティングにおける「NTP（ネットワークタイムプロトコル）」の場合では、「検知（ディテクション）⇒分析（アナライズ）⇒対処（リアクションメソッド）」での「サイバーセキュリティー対策」が重要と、私は考えます。	いただいた御意見については、今後の取組の参考とさせていただきます。	無し
45	株式会社ラック	＜P.86～P.104＞ 共通 クラウドサービス提供をするためには、当該事業の他に通信キャリアなど、様々な事業者が関係します。 インターネットの分岐点をゲートウェイとして、その外のネットワークに関する責任分解について示すことが可能になれば、事業者としても必要な対応が明確になりますので、望ましいと考えます。 これはSaaS、IaaS、PaaS問わず、共通項目に含めるのが望ましいと考えます。	いただいた御意見については、今後の取組の参考とさせていただきます。	無し
46	株式会社セールスフォース・ドットコム	（全体） コメント： SIパートナー/システム受託事業者の存在・役割・責務等が明示されていない。	クラウドサービス利用者に対してクラウドサービスを提供するケースにおいて、その提供形態や役割・責務の分担のあり方は多様であり、御指摘いただいた内容についても、その提供形態の一つの形であると理解しています。本ガイドラインにおいては、P22「Ｉ．６．クラウドサービス事業者とクラウドサービス利用者の責任」でも記載しているように、「クラウドサービス事業者」「クラウドサービス利用者」の2つに分類した上で、そこでの責任範囲の一般的な在り方を示しており、そういった個別のケースへの言及まではしていません。 そのため、いただいた御意見については、今後のクラウドサービス提供の動向も踏まえ、必要に応じて今後改定を検討します。	無し
47	株式会社セールスフォース・ドットコム	該当箇所： （５４、７３、７４頁）評価項目の参考値 コメント： 参考値の値が重複しているところが複数ある。値に対する評価指針を示さないのであれば参考値を例示する必要はあるのだろうか。	御指摘いただいた「評価指針」に該当するものとして、P191～P193「ANNEX1 クラウドサービスのパターン」においてパターンごとのサービス種別が例示されています。	無し

項番	意見提出者	御意見の詳細	御意見に対する考え方	修正の有無
48	一般社団法人情報処理安全確保支援士会	【全体意見】 「デジタル社会の実現に向けた重点計画（2021年6月18日閣議決定）」において、情報処理安全確保支援士は「情報セキュリティの専門人材」として明確に位置づけされ、情報処理の促進に関する法律という国内法に根拠を持つ唯一の情報セキュリティ人材であることが政府によって定められた。にもかかわらず、本書において単に「情報セキュリティ専門技術者」という曖昧な表記にしていることは重大な瑕疵である。 総務省はかねてから情報処理安全確保支援士会のこうした指摘に対して「特定の資格に言及するものではない」「他にも情報セキュリティに関する資格は存在している」「それぞれにあった専門性が求められる」といった無責任な表記で対応を先送りにした結果、こういったパブリックコメントで総務省が示した情報セキュリティ専門人材の認定に対する甘い姿勢を見た民間事業者が、情報セキュリティの専門人材を想起させる低品質な「サムライ商法」を乱発しており、情報セキュリティの確保どころか、それを積極的に危機にさらすような資格が数多く存在している。 たとえば情報セキュリティの専門人材として「情報処理安全確保支援士」の明記を避けることで、担当者の不注意を原因としたクラウドの誤り設定による情報流出事故やバックアップ喪失事故といった情報セキュリティインシデントが既に発生しており、その反省点として「十分な知識や、それを証明する資格を持たず、Ｗｅｂ等をみながら場当たり的に作業をした多重請負の構成員」「クラウドに知識があるように見せかけることで技術者単価をごまかすための安易に合格する低レベルな民間資格とそれを根拠に就労を斡旋する人材派遣会社も兼ねたＩＴ教育事業者」であることも明らかにされているところである。 よって、これらの実際に生じている危機を踏まえ、特に閣議決定が存在している「情報セキュリティ人材」については「情報処理安全確保支援士」であることを基本要件とすること。更に必要な専門知識があれば「情報処理安全確保支援士であって、なおかつ特定クラウドサービスの知見を有することが各ベンダー資格により証明される者」等に統一すべきである。 付け加えるならば、昨今頻発するシステムトラブルのほぼ全てはこういった総務省の「情報処理技術者関連資格に対する必置化回避」の極めて無責任な姿勢が、怪しい民間資格の乱立やそれに伴う技術者の水準低下、これらを要因として当然のように発生する情報セキュリティインシデントの一因となっていることは明らかであり、本件に関して言うならば、当会の提言と閣議決定に従い「情報セキュリティ専門技術者」という「怪しげなサムライ商法又は民間教育事業者（含む人材派遣事業者の内部研修）が取り扱っていそうな一般的な名称のみ記載」から「情報処理安全確保支援士」という具体的な国内法に根拠を持つ国家資格名へと直ちに修正することが、国民の安全・安心を守る「全体の奉仕者」としての公務員が取るべき判断であると情報処理安全確保支援士会としては考えている。 この考えに基づき、以下提言する。 ・情報セキュリティ専門技術者は全て「情報処理安全確保支援士といった情報セキュリティ専門技術者」に記載を変更すること。 ・情報セキュリティ人材については「情報処理安全確保支援士試験合格者等と言った情報セキュリティ人材」に記載を変更すること。 －これらを全て反映させることが、閣議決定に服すべき政府機関である総務省の責務であると、情報処理安全確保支援士会としては考える。	本ガイドラインに記載している「情報セキュリティ専門技術者」及び「情報セキュリティ人材」は情報処理安全確保支援士に限定する趣旨ではないため、本文の記載は原案の通りとしますが、いただいた御意見については今後のガイドライン改定の検討の参考とさせていただきます。	無し