別紙２

「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）
意見募集に対する御意見

○　意見募集期間：
平成 26 年２月 22 日（土）～平成 26 年３月 16 日（日）

○　意見提出総数
（１）　個人３件
（２）　法人・団体７件（受付順）
◇フリー株式会社
◇株式会社ニーモニックセキュリティ
◇日本セキュアテック研究所
◇日本ユニシス
◇日本セキュリティ監査協会
◇日本公認会計士協会
◇富士通株式会社
（３）　匿名１件

意見提出者	御意見の概要	御意見に対する考え方
個人①	ページ23　項番 8.1.1　タイトル：資産目録 「利用者接点とサプライチェーンにおける実務のポイント」 　→クラウド利用者が資産目録の作成情報をクラウド事業者に求めてくる場合があるので、求める内容を、SLA に記載した範囲とするよう明記する。 （要旨）現実問題としてプライバシーマーク等の認証制度において、ライフサイクルに基づくリスク分析を行っているクラウド利用者の場合、かなり細かい状況を事業者に確認してくる可能性があります。（たとえば、件数、項目、期間、追加、削除日） 求められる内容は、クラウド利用者ごとに異なることから、事前に明確にしておかないと費用と稼働面でトラブルの可能性があると考えます。	・ご指摘の趣旨を踏まえ、8.1.1【利用者接点とサプライチェーンにおける実務のポイント】(c)項の文末を、次の通り修正いたします。 （修正前）クラウド利用者に提供すること。 （修正後）SLA に記載して同意した範囲内でクラウド利用者に提供すること。
	ページ26　項番 8.2.3　タイトル：資産の取扱い 「利用者接点とサプライチェーンにおける実務のポイント」 　→クラウド事業者において、地方自治体向けの情報セキュリティポリシーガイドライン等にあるような、情報の重要度に応じた保管方法、アクセス制限等を実現できるようクラウド事業者に考慮させる。 （要旨）地方自治体の情報セキュリティポリシー等にある重要度区分に連動させることも必要と考えます。またこれらに合致した情報取扱いが可能となれば、クラウド化推進のはずみの一つとなります。クラウド事業者の負荷にならないよう、考慮させる範疇のものです。	・クラウド事業者は、その事業戦略等により、多様な管理水準のサービスを提供しています。その望ましい管理水準に指針を与えるという考え方もありますが、ガイドラインでは、クラウド事業者がクラウド利用者にサービス選定に資する情報を提供し、クラウド利用者がニーズに沿うサービスを選択しやすくする環境づくりに取り組むことに、まず重点を置いております。従いまして、ご意見は今後の参考とさせていただきます。
	ページ33　項番9．4．4　タイトル：特権的なユーティリティプログラムの使用 「利用者接点とサプライチェーンにおける実務のポイント」 　→クラウド利用者における、ユーティリティプログラムを使ったクラウドアクセスは、現状より厳しく制限することを具体的に明記する。 （要旨）マルウェア等、ユーティリティプログラムを使えれば比較的簡単にクラウド内部に侵入させることが可能です。その場合、共通プラットフォーム上にいる他のユーザにも影響を及ぼすため、最低限のセキュリティを考慮したアクセス方法を具体的に明記（特定のIP アドレス、MAC アドレス、プロトコル及びアクセス可能時間以外での通信方法を制限等）しておくことが必要かと考えます。（クラウド事業者の自由度の問題もありますが、利用者保護の観点です。）	・「クラウド利用者における、ユーティリティプログラムを使ったクラウドアクセス」を制限する方法を厳しく保つことの必要性はご指摘いただいたとおりです。しかし、クラウドサービスが裾野を拡大し、多様なニーズに応えるべく急速に進歩している現状を考慮すると、各々のクラウドサービスに則した方法を選択できる自由度を持たせておくことも必要であると理解しております。 ・これらのトレードオフを検討した結果、今回は原案のとおりとさせていただき、ご意見は今後の参考とさせていただきます。
個人②	1．ガイドラインによる実施状況のモニタリングについて ①項目（全般） 　ガイドライン全般 ②意見 　・目的・用途・内容ともに「非常に適切なガイドライン」であると認識しております。＜更に申し上げるならば、経済産業省の利用のガイドラインと一体化することが利用者からみると、より、有難いですが・・・・（今回は無理かも知れませんが）＞ 　・今後の課題は、このガイドラインの利用状況をどうモニタリングするかがポイントと考えます。 ③理由等 　・モニタリングすることにより、その実効性が明確になり、真の意味で、クラウド利用の推進に役立つことが期待できる。 　・本件は新しい重要な技術動向等に対するガイドラインでもあるため、クラウド導入実績、取得認証等の公開・個別情報開示のみに頼るのではなく、ガイドラインの主要項目の個々の適否検証を継続していく必要がある、と考えます。	・ガイドラインは指針を示すものと理解しております。この指針のクラウド事業者への普及・浸透、主要な指針の実施状況の確認・評価等の仕組み作りについては、民間の事業者団体等の取組みによって推進されることに期待します。よって、原案のとおりとさせていただきます。
	2．提供条件情報の公表について ①項目 　6.3.1　クラウドサービスの情報セキュリティマネジメントに係る提供条件の明確化（p18） ②意見 p18：【利用者接点とサプライチェーンにおける実務のポイント】（c）項 2 行目「クラウド利用者に個別対応範囲がかなり限定されることを理解していただくための措置を講じること。」 ↓ 「クラウド利用者にその情報を公表する措置を講じること。」 ③理由等 限定的に「理解していただく」ではなく、公表により、認識を得る内容と理解しております。●以下、同様な「理解していただく」との表現は、すべて「公表」とする。●	・ご指摘の趣旨を踏まえ、以下のように修正いたします。 6.3.1【クラウドサービスの提供において特に留意すべき課題との関係】2 行目 （修正前）提供条件を正しく理解していただくために （修正後）提供条件の正しい認識を定着させるために 6.3.1【利用者接点とサプライチェーンにおける実務のポイント】(c) 2 行目 （修正前）この文書に基づいて、クラウド利用者に個別対応範囲がかなり限定されることを理解していただくための措置を講じること。 （修正後）この文書を用いた情報提供により、クラウド利用者が個別対応範囲がかなり限定されることを認識できるようにすること。 21 ページ脚注 6 の 3 行目、22 ページ脚注 7 の 2 行目 （修正前）クラウド利用者にも理解していただくことが望ましい。 （修正後）クラウド利用者に伝えることが望ましい。

		9.1.2【クラウドサービスの提供において特に留意すべき課題との関係】8 行目 （修正前）クラウド利用者に正しく理解していただくための情報提供を行うことが求められる。 （修正後）情報提供により、クラウド利用者が正しい認識を得られるようにすることが求められる。
	3. 利用者接点とサプライチェーンにおける情報提供・共有 の「内容」の追記 ①項目 6.3.2 利用者接点とサプライチェーンにおける情報提供・共有（p19） ②意見 p19:【利用者接点とサプライチェーンにおける実務のポイント】・・の例示 ・ クラウドサービスが保証または努力目標とするサービスレベル ・ 取得した認証・受賞 ・ 実施している監査の言明または監査報告書 ↓ p21（クラウドサービス提供段階）と同様に、詳細に記述する。 （p8上の数行を詳細に追記記述） ③理由等 選定時（新規顧客／乗り換え段階）でも、（クラウドサービス提供段階）と同様に重要内容であるが、略記している。・・・（クラウドサービス提供段階）と同様な取扱とする。	・ご指摘の趣旨を踏まえ、以下のように追記いたします。 （追記後） □クラウドサービスが保証または努力目標とするサービスレベル（SLA文書の内容を公開する例も見られる） →故障回復時刻、故障通知時刻 →サービス提供時間、ヘルプデスク提供時間 →サービス稼働率、平均応答時間 →情報セキュリティ対策・設備の措置、ログ記録、サービス継続のための措置、バックアップ、暗号化に対応できるサービスの範囲
	4. 情報のバックアップ方法について ①項目 12.3.1 情報のバックアップ（p44） ②意見 【利用者接点とサプライチェーンにおける実務のポイント】・・（c項） 特定のクラウド利用者の預託データの押収等がなされた場合でも、(b)によりその対象を最小限の範囲に限定することで、無関係なクラウド利用者の預託データのバックアップが、外部の第三者の管理下におかれないようにすること。 ↓ 特定のクラウド利用者の預託データの押収等がなされた場合でも、無関係なクラウド利用者の預託データのバックアップが、外部の第三者の管理下におかれないようにすること。 ③理由等 (b)は手段の一つであり、限定する必要はない、と考えます。むしろ、すべての場合に必要な措置、と考えます。	・(b)を明示しないことで幅広く(c)を適用するという考え方もございます。一方で、(b)の要求も併せて満足することで、クラウド利用者のニーズに応えられる場合がございます。すなわち、原案の記述の方が、推奨しているサービスレベルが高いと理解しております。 ・ガイドラインとしては、この項目については、後者のようにより高いサービスレベルを推奨すべきと考えておりますので、原案のとおりとさせていただきます。
	5. イベントログ取得 の追加記述 ①項目 12.4.1 イベントログ取得（p45） ②意見 【利用者接点とサプライチェーンにおける実務のポイント】 に アグリゲーションサービス以外の一般の垂直連携・水平連携の場合の記述を同様に入れる。現状では、アグリゲーションサービスを提供する場合、に限定している。 ③理由等 アグリゲーション以外でも記載内容の必要がある、と考えます。	・ご指摘の趣旨を踏まえ、12.4.1【利用者接点とサプライチェーンにおける実務のポイント】に、アグリゲーションサービスに限定せず適用される実務を追記させていただきました。 （追記後） 供給者が必要なイベント等のログを取得し、取得したログを保持することを確保する必要がある。このため、供給者の選定にあたっては、イベントログの範囲、内容、粒度等について、供給者の規定がクラウド事業者の要求を満足していることを事前に確認することが求められる。このため、実務上以下を実施することが望ましい。 (a)脅威として監視すべきイベント等を定め、これに基づいて、クラウドサービスとして取得するイベントログの範囲、内容、粒度等を定めること。 (b)(a)で定めた取得するログの範囲、内容、粒度等について、供給者の利用規約、SLA 等の規定を確認し、クラウド事業者の要求を満足できる供給者を選定すること。
	6. 証拠の収集 の追記 ①項目 16.1.7 証拠の収集（p62） ②意見 【利用者接点とサプライチェーンにおける実務のポイント】 (a) 可能であれば、複数のクラウド利用者で共用された媒体・資源へのフォレンジック調査中に、証拠の収集・保存・保全に無関係な他のクラウド利用者の記録の破損等の二次的な資産の損害を防止できる技術を適用すること。 (b) 可能であれば、複数のクラウド利用者で共用された媒体・資源へのフォレンジック調査中に、証拠の収集・保存・保全に無関係な他のクラウド利用者の機微情報を保護できる技術を適用すること。 ↑可能であれば、と、何故、条件付が必要か検討する。 ③理由等 この箇所のみ、何故、可能であれば、とするのか不明確です。	・クラウド環境におけるフォレンジック調査には技術的な困難さがあり、また実務上、経済的な負担も少なくないと理解しております。このため、「可能であれば」としております。 ・しかし、意図が不明確とのご意見をいただき、妥当と考えますので、注記により意図するところを明示するように修正させていただきます。 ・日本セキュリティ監査協会からの同じ箇所へのご意見に対する考え方もご確認ください。
	7. 適用法令及び契約上の要求事項の特定 の記述追記 ①項目	・一般的な契約上の要求事項や要求事項に加えて、クラウド利用者から預託された情報の契約終了時の取扱いに関しては、個々の利用

	18.1.1　適用法令及び契約上の要求事項の特定（p64） ②意見 【利用者接点とサプライチェーンにおける実務のポイント】末尾 ・・・、総務省、経済産業省等から IT アウトソーシングや SLA 等に係るガイドラインが公表されているので、こちらを参照されたい。 ↓ 公表されているガイドライン名を明記する。 ③理由等 新旧ガイドラインが乱れている場合があるので、現時点でのガイドライン名を明記する。これまで、不明確な例が、SLA 等に関わるガイドラインにあり、現行かどうか判然としないケースがある、廃止情報も明確化（管理）する意味があります。	サービスの特性や政策的な要請などにより、時間の経過により内容が変わることも予想されます。ご指摘の点は、今後のガイドラインの策定に際しての参考とさせていただきたく存じておりますが、今回はガイドラインでは原文のとおりとさせていただきます。
	8.　適用法令及び契約上の要求事項の特定 の記述追記（2） ①項目 18.1.1　適用法令及び契約上の要求事項の特定（p64など） ●各項全般● ②意見 【利用者接点とサプライチェーンにおける実務のポイント】 アグリゲーションサービスを提供する場合は、どう対処するのか不明確 ③理由等 アグリゲーションサービスを提供する場合も、他の場合（アグリゲーションサービス以外の垂直連携・水平連携の場合も）の記述を同様に入れる。 ●なお、本項以外に、全般的に、 アグリゲーションサービス以外の場合について、 アグリゲーションサービスの場合と併記するかどうか、個別に、その適否を明確にしていただきたい。●	・18.1.1～18.1.5 において、アグリゲーションサービスを提供する場合の対処が記載されていないことに対するご意見と理解しております。 ・18.1.1～18.1.5 では、国内外での適用法の違いによって生じる課題について取扱っていますが、国や地域によって事情が様々に異なり、指針の記述も抽象度が高いものとなっています。このため、アグリゲーションサービス事業者に関しては、国外に跨る ICT サプライチェーンの全体を管理統制する責任を負っているということ以外に、一般のクラウド事業者に適用される指針と書き分けを行うことが難しくなっています。よって、ご意見は今後の参考とさせていただき、現時点では原案のとおりとし、ガイドラインの改訂時にその時点の状況を踏まえて改めて検討させていただくことといたします。
	9. コンプライアンスなどに関わる事項の「実務のポイント」における「サービス提供上必要な措置を講じること」の対処について ①項目 18.1.1　適用法令及び契約上の要求事項の特定（p64） ②意見 【利用者接点とサプライチェーンにおける実務のポイント】 （b）　複数国の資源やサービスを利用してサービス提供を行うクラウド事業者は、当該資源やサービスが存在する国において適用される法等に係るリスクに対して、サービス提供上必要な措置を講じること。 ↓ ・・・・・ なお、必要な措置には、クラウド利用者にオンプレミスを勧めることを含める。 ③理由等 p8に、次の記述があるが、クラウド利用者個別の情報開示以外でも、コンプライアンスにかかわる事項の重要性を明確にし、選択肢を示す、ことが適切と考えます。 ・・・・・・・なお、クラウド利用者個別の情報開示を行うにあたっては、以下の 5 点にも留意すべきである。・・・ ● クラウド利用者が細かい情報を要求し、自ら詳しく判断・管理しようとする場合は、クラウド利用者にオンプレミスを勧めるべき ● ＜特記＞●18.1.2　知的財産権（p64） も同様に扱っていただきたい。●	・まず、P8において「オンプレミスを勧めるべき」という表現がありますが、以下のように修正いたします。 （修正前）クラウド利用者にオンプレミスを勧めるべき （修正後）クラウド利用者に対して開示可能な情報の範囲や粒度、頻度について事前に説明を行い、提供するサービスがクラウド利用者の要求を満足するかの正確な判断を促進すべき ・18.1.1、18.1.2 のご指摘の箇所についても、「オンプレミスを勧めるべき」という表現は行いません。 ・18.1.1、18.1.2ともに、まず、クラウド利用者が預託情報を保存する国や、預託可能な情報の範囲を正しく選択することが求められるものと理解しております。オンプレミスの選択もこの中に含まれます。これが確保されないと、クラウド事業者の努力だけでは、預託情報の安全を守ることができないと考えます。従いまして、ここでもP8と同様に、「クラウド利用者の正確な判断を促進すべき」という趣旨で追記をいたします。 ・追記内容については、匿名による 18.1.1 及び 18.1.2 に対するご意見に対する考え方をご確認ください。
	10．クラウドサービス情報開示認定サイト https://www.fmmc.or.jp/cloud-nintei/）について ①項目　6.3.2　利用者接点とサプライチェーンにおける情報提供・共有（p20） ②意見 【利用者接点とサプライチェーンにおける実務のポイント】 クラウドサービス情報開示認定サイト https://www.fmmc.or.jp/cloud-nintei/）の記載項目などを、本ガイドラインに沿って、再度、見直していただくよう、ご指導をお願いします。 ③理由等 再点検が必要と判断しております。 例：・選択項目で、認定事業者提出資料が存在するが、「記述あり」となっており、詳細が掲出されていない。 ・コンプライアンス項目の内容に不十分なところがある。個人情報保護については、「目的明示」「個人情報保護方針の明示」のみとなっている。 ・api については、詳細な記載がないなど・・・・・	・ガイドラインの内容に対するご指摘ではないと理解しております。 ・今後の参考にさせていただきます。
個人③	1. ガイドライン準拠を謳うクラウド事業者に求めたい点 本ガイドラインに準拠したクラウドサービスの提供を謳うクラウド事業者には、各実務内容の実施の有無と、なぜ実施するのか（あるいはしないのか）その背景・目的、評価実施日とともに示し、少なくとも毎年再評価することを求めたい。	・ガイドラインは指針を示すものと理解しております。クラウド事業者によるこの指針の内容の適用状況の情報開示、毎年の再評価等の仕組み作りについては、民間の事業者団体等の取組みによって推進されることに期待します。よって、原案のとおりとさせていただきます。

	クラウドの利用者視点のガイドラインは、経済産業省の「クラウドサービスの利用のための情報セキュリティマネジメントガイドライン」が 2011 年 4 月に公開され、昨年は、その改定版のパブリックコメントが公募されている。クラウド事業者向けの国内のクラウドの情報セキュリティ対策の実践ガイドラインは、ISO/IEC27017 が検討途中であることを考えると、本編が重要な役割を果たすと考えるが、クラウド事業者にとっては、公のガイドラインへの準拠を謳うことができれば、新たな顧客獲得にとって有効と感じると思われる一方、経済効率を考えるとガイドラインの個々の要件への対応状況を整備・開示するのは負担と感じ、情報開示が進まない恐れがある。 クラウド利用者の多くが中小企業であり、セキュリティ専門人材を確保することが困難と考えられる中、クラウド事業者が安易に「本ガイドラインへの準拠」を謳うことで、利用者への優良誤認を引き起こす恐れがある。それを防ぐため、本ガイドラインに基づく利用者接点の実務を行う事業者は、第二部に記載される項目毎に対応方針（「望ましい」などの記述のある実践項目を含め、実施する／しない等の意思表明）を文書にて明らかにすることが望ましい。項目毎の対応方針は、クラウド利用者がリスクベースで採用判断をするのに役立つ。これは、クラウドサービスの種類によっては利用者視点では項目毎に要否の程度が異なり、或るクラウド利用者にとって過剰なセキュリティ対策実施コストは、その利用者にとって不利益となるためである。 実施の有無は、特に実施しない場合において、なぜそのような選択をしているかをクラウド事業者自身が背景・目的とともに理由を提示することが望ましい。それにより、利用者視点ではセキュリティ対策実践のコストとリスクの評価がし易くなり、クラウド利用者が納得した上でサービス利用を行うことに繋がる。また、これらの情報は毎年再評価した結果を評価実施日とともに提示できるようにすることが望ましい。付録としてチェックリスト形式の表計算ファイルを添付いただきたい。 例:9.2.4 利用者の秘密認証情報の管理 シングルサインオンやID連携の機能提供は行わない（このクラウドサービスは、アクセスログの参照機能提供により、なりすまし監視を利用ユーザ自身が行え、通常取扱い情報の機密性に高度なものが求められないことから、個別に認証情報管理を行う。ID連携等の機能提供コストは、お客様の利用コストに転嫁する必要がある）	
	2. ガイドライン各実務内容について求めたい点 取り扱う情報や適用業務の重要度に応じて、特に実施が望ましい項目をその背景・目的とともに明示されたい。 第二部掲載の管理策は必須の項目との表記はなく、重要度の高低が判別しにくい。このため、クラウド利用者が預託する情報や取り扱う業務の重要度を2乃至3レベル程度に分け、高度のものについて、特に実施が望ましい項目を明示することで事業者・利用者ともに対応の要否について判断がし易いようにすることが望ましい。 そのほかに、次の情報の扱い・業務については特に実施の求められる項目を明示されたい。 ・個人情報 機微情報を含むもの ・輸出管理規制の対象となる技術情報を含むもの ・いわゆるSOX監査対象となる業務を扱うもの	・ガイドラインでは、様々な業界、様々な業務、様々な情報に幅広く適用可能な共通の指針を示すことに重点を置いております。 ・ご指摘いただいているもの以外にも、例えば営業秘密、電子帳簿、医療情報、債権管理の情報などの情報資産もあります。これらに対し、特に実施が望ましい項目を明示していくことは必要であると理解しております。 ・よって、ご意見は参考にさせていただき、今後の改訂時などに改めて検討させていただきたく存じます。
	3.（預託情報）資産の管理責任 (Page23 8.1 資産に関する責任) 8.1 項に掲示の資産に対する責任は、利用終了時の資産の返却等については触れているが、利用中に預託された情報そのものの扱いについては触れられていない。預託された情報は、秘密保持契約や資産目録の有無にかかわらず、クラウド事業者が無断で利用・開示することなく、合理的な保護手段を以って保護することを方針として謳うよう求めたい。	・ご指摘に基づき、8.1.2 資産の管理 【利用者接点とサプライチェーンにおける実務】に追記させていただきます。 （追記後） なお、クラウド利用者から個別に委託を受けた場合等を除いては、預託情報の内容を一切利用・開示しないことを管理ポリシーに明示することが望ましい。
フリー株式会社	12.1.1「操作手順は、文書化し、必要とする全ての利用者に対して利用可能とすることが望ましい。 ⇒文書化という手段の明示化の削除を希望する。 全ての手順の文書化は、高速度で進化するアプリケーションの開発においては、コストが高く、特に中小事業者にとって負荷が高く、イノベーションを阻害する。ユーザーインターフェースを見れば、使い方が自明という状態になっていれば、手順書が別途文書化されていなくとも目的は達成されるはずであり、仮にユーザーインターフェースにおいてその目的が達成されているのであれば、別途文書を作成するのは冗長である。また、イノベーションの観点から考えた際にもユーザー保護の観点から考えた際にも、文書化に頼るに比すると、ユーザーインターフェースにおいて使い方が自明という状態の方が望ましいと考えられる。これらを考慮した際に、ガイドラインにおいて、利用者のリスクを軽減する手法として文書化という手段の特定を行うことは、理想的な方法とはいえず、わが国の産業の進歩を妨げるともいえる。	・12.1.1 の管理策の記述は、ISO/IEC27002:2013 より引用したものです。ガイドラインでは、管理策の記述は ISO/IEC27002:2013 より引用するという方針で統一されています。よって、原案のとおりとさせていただきます。

株式会社ニーモニックセキュリティ	「10. 暗号」に並列する形で「本人認証」ないし「パスワード」という独立の項目を起こし、本人認証ないしパスワードに関する注意事項を詳しく記述しては如何でしょうか。 理由:そもそも本人認証を破られれば暗号化による防御は一瞬のうちに無効化されてしまいます。更に、たとえハッキングやマルウェア等による攻撃を根絶できたとしても、本人認証の脆弱性が増大するままに放置されていると、次に例示するような状況に悩まされ続けることが容易に想像できます。 ・ 重要インフラ支配を図っている攻撃組織に管理者のパスワードを盗用されると一挙に彼らの武器に転化されかねないクラウド ・ 辛うじて覚えた3～5組のパスワードを使い回していたところに「パスワードリセットと使い回し厳禁」と言いわたされて困惑している人達や屋外でのメモ持ち歩きを管理者に見つけられて叱責されている人達 ・ 乗っ取られた自分のアカウントから破廉恥メッセージが露出されたり犯罪誘導メールが大量に配信されて困惑している人達 ・ 大災害時に本人認証ができないままに困惑している被災職員住民と杜撰な本人認証のお陰で行方不明被災者に成りおおせている逃亡者やサボタージュ工作員 クラウドのセキュリティを城砦に譬えていうならば、この城は広く深い濠が幾重にも、頑丈な高い石垣が死角を残さず幾重にも、幾重もの門扉という門扉は大小を問わずすべて重く厚く屈強な守備兵が居並ぶ、と徹底した多重防護が築かれていて攻略を図るのは至難の業。しかし、入門許可証を持った人間は大手門から三の丸、二の丸を経て本丸や井戸や火薬庫まで誰に止められることもなく到着でき最後には獲物を抱えて大っぴらに大手門から退出できてしまう。パスワードを盗用される、本人認証を破られる、ということはこのような入門許可証を包囲軍に渡してしまうということです。 ガイドライン(案)の「6. 2 モバイル機器及びテレワーキング」においては「(d) モバイル機器において、クラウド利用者に、一定強度以上のパスワード設定を義務付けること。また、業務用クラウドサービスへの接続時に一定強度以上のパスワードが設定されているかの有無をチェックすること。」と記述されていますが、これだけで終えてしまうと利用者をメモ記載のパスワードの持ち歩きや同一パスワードの多数アカウントでの使い回しに追い立てるだけに終わってしまいかねません。 文字パスワードについて人は平均して3組程度しか覚えていられないことは変えようのない人間の事実であることを踏まえて、一定強度以上に設定されたパスワードを、メモに記載して持ち歩くことなく、複数のアカウントに使い回すことなく管理させるよう、望ましくはそのような管理を可能とするような手段を提供するように要求すべきではないかと考えます。なお、他の要素と組み合わせて2要素認証とすればパスワードは脆弱なままで放置しても良いということにはなりません。屋外環境ではモバイル端末を奪える機会を得た犯罪者が認証用所持物(トークン・携帯電話)については奪わないでおこうと考えるだろうと想定することはできません。端末と所持物を共に奪った攻撃者からの防御についてはパスワードだけが頼りになります。 ID連携の普及によってパスワード記憶の負担を軽減させる方策が提起されていることにつきましては、実際の運用に際しては十分な注意が必要と考えます。一方で「一つのパスワードを多くのアカウントに使い回す」は禁止すべきと唱えながら他方で「一つのアカウントで多くのアカウントを管理すること」を推奨するのは論理が崩れています。節度のあるレベル別分散型のID連携を考えるとやはり全ての利用者が相当数の良質パスワードを使いこなせることが必要です。また、iPhone に指紋認証が搭載されて話題になっていますが、パスコードでも指紋認証でもロック解除が可能な状態で運用されるとパスコードのみで運用するよりもセキュリティは下がります。このような形で生体認証を利用するのであれば従前以上に強固なパスワードを使用することが不可欠です。間違った認識や不十分な認識が蔓延していることに懸念がつのります。ガイドラインにおいて然るべく注意を喚起されることを期待します。	・モバイル機器では、パスワードを破られて利用者本人と詐称されると、暗号化による防御は無力化されるという点はご指摘のとおりです。但し、ご指摘はモバイル機器に重点が置かれていると理解しました。6.2.1 モバイル機器の方針 【利用者接点とサプライチェーンにおける実務のポイント】において、暗号化アルゴリズム、鍵管理、本人認証が揃うことでローカル保存した暗号化データの防御が有効性を発揮すること、このためには本人認証も非常に重要であることを追記させていただきます。 (追記後) なお、モバイル機器上の暗号化されたデータの保護において、本人認証は非常に重要な役割を果たしている。堅牢なアルゴリズムと十分な鍵長によって暗号化されたデータであっても、本人認証が破られて「正規の利用者である」とシステムに誤認させることができれば、当該システムの制御下で暗号鍵を利用する権限を自動的に付与され、暗号化されたデータの平文を自由に見ることができる。クラウド事業者としても、本人認証に係る(d)の指針が、モバイル機器の暗号化対策において特に重要な意味を持つことを理解し、クラウド利用者の認識を高めるための措置を講じることが望ましい。
日本セキュアテック研究所	「10. 暗号」の項は、「10.1.2 鍵管理」 に並列する形で「10. 1. 3 本人認証」という独立の項目を起こし、本人認証に関する注意事項を詳しく記述しては如何でしょうか。 理由: 暗号解読の際の攻撃対象は3点、暗号アルゴリズムと暗号鍵管理及び本人認証の突破です。それゆえ3点をまとめて説明することは攻撃からの耐性を強化する際に有効かと思料します。とりわけメディアのニュース等で最も攻撃の成功が目につく本人認証の脆弱性が今後も放置され続けるのであれば、たとえいくら暗号アルゴリズムの強化を図っても、鍵管理を厳格化しても、正規の利用者になりすました攻撃者による暗号解読攻撃の勢いが低減することはないと思われます。	上に同じ。

日本ユニシス	1. ページ12　xvi. PaaS（Platform as a Service） 対象文章：オペレーティングシステムや実行環境をサービスとして提供するクラウドサービス コメント：「何の」実行環境なのか明示的に記述されるとわかりやすいと思います。	・ご指摘の趣旨を踏まえて、次のように修正いたします。 （修正前）オペレーティングシステムや実行環境をサービスとして提供するクラウドサービス （修正後）オペレーティングシステムや、アプリケーションの実行環境（開発環境を含む）をサービスとして提供するクラウドサービス
	2. ページ43　最終行 対象文章：この場合、クラウドサービスの継続性が阻害される恐れがあるため、これを防止する措置を講じる必要がある。 コメント：継続性が阻害される理由がつかみにくいです。バックアップを押収されるというよりは、物理的にディスクを押収されるという理由であろうと推測しますが、明示的に書かれるとわかりやすいと思います。	・バックアップが押収された場合に、クラウドサービスがすぐに停止してしまうことはありません。しかし、サービスレベルを保証して安全なサービスを提供する上では支障が出ます。この趣旨が明確になるように、文章を修正いたします。 （修正前）クラウドサービスの継続性が阻害される恐れがあるため （修正後）サービス障害時の備えが不十分となり、サービスレベルを保証したクラウドサービスの提供が阻害される恐れがあるため
日本セキュリティ監査協会	該当箇所：第Ⅰ部 序編 2 タイトル：ISO/IEC 27002:2013 及び他のガイドライン等との関係 段落または図表番号： 対象となる文・用語など：本ガイドラインは、ISO/IEC 27002 に基づく情報セキュリティマネジメントを行うための知識を有しているクラウド事業者を読み手として想定している。 提案理由 “ISO/IEC 27002 に基づく”と記載が ISO/IEC 27002 に収斂した形となっているが、ISO/IEC 27002 には関連規格が多くあり、実際に管理策を講じるには関連規格を含めた理解が必要であるとの認識であるため。 修正案 本ガイドラインは、ISO/IEC 27002 およびその関連規格に基づく情報セキュリティマネジメントを行うための知識を有しているクラウド事業者を読み手として想定している。（下線部を追記）	・ご指摘のとおり、修正いたします。
	該当箇所：第Ⅰ部 4.（4） タイトル：クラウド利用者とのコミュニケーションにおける実務 段落または図表番号：図表 5 対象となる文・用語など：①クラウドサービスの新規利用／乗り換えの獲得：個別開示 内部統制監査報告書（ISAE3402／SSAE16） 提案理由 ①内部統制監査報告書（ISAE3402／SSAE16）に加え、サービス・オーガニゼーション・コントロール報告書（SOC2）が必要と考える。 注）内部統制監査報告書（ISAE3402／SSAE16）は、業務委託（契約）関係がある受託会社の経営者、委託会社とその会計監査人宛に、開示が限定されている。 修正案 ①クラウドサービスの新規利用／乗り換えの獲得：個別開示 サービス・オーガニゼーション・コントロール報告書（SOC2）、内部統制監査報告書（ISAE3402／SSAE16）	・ご指摘のとおり、修正いたします。
	該当箇所：第Ⅰ部 4.（4） タイトル：クラウド利用者とのコミュニケーションにおける実務 利用者接点とサプライチェーンにおける情報提供・共有 段落または図表番号：1 行目 対象となる文・用語など：実施している監査の言明の公開 提案理由 「実施している監査の言明の公開」と「監査済み言明書の公開」が混在しているので統一することが望ましい 修正案 監査済み言明書の公開	・ご指摘のとおり、修正いたします。
	該当箇所：第Ⅰ部 4.（4） タイトル：クラウド利用者とのコミュニケーションにおける実務 段落または図表番号：2 点目 対象となる文・用語など：クラウド利用者が細かい情報を要求し、自ら詳しく判断・管理しようとする場合は、クラウド利用者にオンプレミスを勧めるべき 提案理由 クラウド事業者自らが顧客（クラウド利用者）に対して明示的に自社サービスの提供を拒否するというのはビジネスとして現実的ではない。 修正案 クラウド利用者に対して開示可能な情報提供の範囲や粒度、頻度について事前に説明を行うべき	・ご指摘の趣旨を踏まえて、文章を以下のように修正いたします。 （修正前）クラウド利用者にオンプレミスを勧めるべき （修正後）クラウド利用者に対して開示可能な情報の範囲や粒度、頻度について事前に説明を行い、提供するサービスがクラウド利用者の要求を満足するかの正確な判断を促進すべき
	該当箇所：第Ⅰ部4.（4） タイトル：クラウド利用者とのコミュニケーションにおける実務 利用者接点とサプライチェーンにおける情報提供・共有 段落または図表番号：脚注 対象となる文・用語など：NDA を締結した上で監査報告書を個別開示 提案理由	・ご指摘のとおり、修正いたします。

	「監査報告書」だけでは、何の監査報告かが、あいまいなので、「言明に係る監査報告書」と記載すべき 修正案 「言明に対する監査報告書（その他関連する監査報告書）」	
	該当箇所：第Ⅰ部4．(4) タイトル：クラウド利用者とのコミュニケーションにおける実務 利用者接点とサプライチェーンにおける情報提供・共有 段落または図表番号：5 点目 対象となる文・用語など：監査済みの言明公開により、対策の実施状況を、クラウド利用者に対し、保証 提案理由 言明は、対策の実施状況をクラウド利用者にコミットするものである。また、監査の保証は言明に対する保証である。これらの点を整理した表現が必要。 修正案 対策の実施状況に係る言明を、監査により合理的な水準で保証を受けた上で、クラウド利用者に対し開示	・ご指摘のとおり、修正いたします。
	該当箇所：本文③図表　7 タイトル： 段落または図表番号：本文③図表　7 対象となる文・用語など：日本情報セキュリティ監査協会 提案理由 名称の誤り 修正案： 日本セキュリティ監査協会	・ご指摘のとおり、修正いたします。
	該当箇所：第Ⅰ部 序編 6. タイトル：6. 用語及び定義 段落または図表番号：xxi. 管理策 対象となる文・用語など：組織に損害や影響を与えるリスクを引き起こす要因 xxi. 管理策 リスクを管理する手段（方針、手順、指針、実践又は組織構造を含む。）であり、実務管理的、技術的、経営的又は法的な性質をもつことがあるもの（JIS Q 27002:2006） 提案理由 JISQ27002 は 2014/03/20 付けで JIS Q 27002:2013 に改定が予定されており、「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）」における指針が ISO/IEC 27002:2013 であることから記述を修正されることが望ましい 修正案 JIS Q 27002:2006 ⇒ JIS Q 27002:2013 に変更。	・ご指摘のとおり、修正いたします。
	該当箇所：6.1.1 (a) タイトル：利用者接点とサプライチェーンにおける実務のポイント 段落または図表番号：第一文 対象となる文・用語など：クラウド利用者とクラウド事業者の間で、それぞれの管理責任の範囲に関わる点に特に注意を払い、個々の情報資産の保護と特定の情報セキュリティプロセスの実施に対する責任を分担し、文書化すること。 提案理由 IaaSなどの標準サービスを提供する供給者が、SaaS 事業者または PaaS 事業者である個別の IaaS 利用者と相互に「個々の情報資産の保護と特定の情報セキュリティプロセスの実施」を行うことは現実的ではない。 IaaS 事業者が責任分解を明確に定義し、明示したものに基づいて利用者である SaaS 事業者または PaaS 事業者が自らが行うべき責任を自覚し、その責務を果たすこととすべきである。 修正案 供給者のサービスを利用してクラウドサービスを行う事業者は、供給者が規定した責任分解点を確認し、それに基づいて利用者の情報資産の保護と特定の情報セキュリティプロセスの実施に対する自らの責任を定義し、文書化すること。	・ご指摘の趣旨を踏まえ、次のように修正いたします。なお、今回の修正で、読み手を「クラウド事業者」に固定し、供給者と分離しております。詳しくは図表 8 をご覧ください。 （修正前）(a)クラウド利用者とクラウド事業者の間で、それぞれの管理責任の範囲に関わる点に特に注意を払い、個々の情報資産の保護と特定の情報セキュリティプロセスの実施に対する責任を分担し、文書化すること。 （修正後）(a)クラウド利用者の情報資産の保護と特定の情報セキュリティプロセスの実施に対する管理責任の範囲を明確に定義し、利用規約・SLA 等で明文化し、クラウド利用者の同意を得ること。 また、(a)項の末尾に以下を追記しております。 （追記後） なお、ICT サプライチェーンを構成してクラウドサービスを提供する場合は、供給者が規定した責任範囲を確認し、これに基づいて自らの管理責任の範囲を定義すること。
	該当箇所：6．3．2 タイトル：クラウド利用者とのコミュニケーションにおける実務 利用者接点とサプライチェーンにおける情報提供・共有 段落または図表番号： 対象となる文・用語など：実施している監査の言明または監査報告書 提案理由 「実施している監査の言明の公開」と「監査済み言明書の公開」が混在しているので統一することが望ましい 修正案 監査済の言明、言明に対する監査報告書（その他関連する監査報告書）	・ご指摘のとおり、修正いたします。
	該当箇所：6．3．2 タイトル：クラウド利用者とのコミュニケーションにおける実務	・ご指摘のとおり、修正いたします。

	利用者接点とサプライチェーンにおける情報提供・共有 段落または図表番号：脚注 4 対象となる文・用語など：クラウド利用者の内部統制確保を保証するため、内部統制監査報告書の情報開示を求められることも多い。 提案理由 内部統制監査報告書は、「クラウド利用者の内部統制確保」を、「保証」するものではない 修正案 クラウド利用者の要請により、クラウド事業者の内部統制確保状況を、合理的な水準で保証することを企図した内部統制監査報告書の情報開示を求められることも多い。	
	該当箇所：(i) タイトル：利用者接点とサプライチェーンにおける実務のポイント 段落または図表番号：最後の文 対象となる文・用語など：代替案として、監査済みの言明公開やNDA を締結した上での監査報告書（サービス・オーガニゼーション・コントロール報告書（SOC2）、内部統制監査報告書（ISAE3402/SSAE16）5 等）の情報開示により、対策の実施状況をクラウド利用者に対し保証することも検討すること。 提案理由 監査の保証概念を正確に反映すべき 修正案 代替案として、監査済みの言明公開やNDA を締結した上での監査報告書（サービス・オーガニゼーション・コントロール報告書（SOC2）、内部統制監査報告書（ISAE3402/SSAE16）5 等）など、対策の実施状況に関する言明や内部統制の有効性についての合理的な水準の保証を企図した報告書を、クラウド利用者に開示すること。	・ご指摘のとおり、修正いたします。
	該当箇所：8.2.3 タイトル：資産の取り扱い 段落または図表番号：全体 対象となる文・用語など：「複数のクラウド利用者から預託を受けた情報」という用語 提案理由 クラウドサービスのうち、IaaS およびPaaS サービスは、コンピュータリソースや実行環境を提供するサービスであり、情報の預託を受けるサービスではない。 ただ、その点を理解しない利用者に誤解が生じるので、情報の預託があるサービスを明確にすべき。 修正案 複数のクラウド利用者から預託を受け、返却が必要となる情報 脚注 SaaS・ASP サービスは、利用者がコンピュータで情報処理するために、情報の預託を受けるサービスである。PaaS や IaaS は利用者にコンピュータ資源や実行環境を提供するサービスであり、一般には利用者に返却すべき情報がない。	・ご指摘のとおり、修正いたします。但し、SaaS・ASP サービスを、他の箇所の記述に合わせ、ASP・SaaS とさせていただきました。
	該当箇所：12.2.1 タイトル：マルウェアに対する管理策 【クラウドサービスの提供において特に留意すべき課題との関係】 段落または図表番号：第二段落 対象となる文・用語など：またマルウェアに感染した場合は、クラウド事業者のどの情報処理施設が感染したのかを、クラウド利用者に迅速に情報提供する仕組みを構築することが求められる。 提案理由 再発防止策が実施されないと、あらためて同一の手口で攻撃を受けた場合に被害の発生を繰り返す恐れのあることから、“再発防止策”の実施を明記することが望まれる。 修正案 また、マルウェアに感染した場合は、再発防止策実施を行うとともに、クラウド事業者のどの情報処理施設が感染したのかを、クラウド利用者に迅速に情報提供する仕組みを構築することが求められる。	・ご指摘のとおり、修正いたします。
	該当箇所：12.2.1 タイトル：【利用者接点とサプライチェーンにおける実務のポイント】 段落または図表番号：(e) 対象となる文・用語など：12.2マルウェアからの保護 (c)の措置を講じること。その上で原因が特定され、影響範囲が明確になった段階で、ICT サプライチェーンにおいてクラウド利用者に影響が及ばない措置を講じたうえで、サービスの提供を再開すること。 提案理由 クラウド利用者に影響が及ばない措置”については、より具体的な記述（駆除あるいは隔離等）を付記してはどうかと考える。	・ご指摘のとおり、修正いたします。

	修正案 (c)の措置を講じること。その上で原因が特定され、影響範囲が明確になった段階で、ICT サプライチェーンにおいてクラウド利用者に影響が及ばない措置(駆除あるいは隔離等)を講じたうえで、サービスの提供を再開すること。	
	該当箇所:第 II 部16.1.7 タイトル:証拠の収集 段落または図表番号:【利用者接点とサプライチェーンにおける実務のポイント】 対象となる文・用語など:“可能であれば、フォレンジック情報が供給されるインターフェイスと API を把握しておき、”の部分 提案理由 クラウド事業者の多くは複数の拠点(センター)でVMを利用し、外部記憶装置としては RAID6 等のハードディスクを利用していることから、フォレンジックは極めて難しい状況にあると思われる。クラウド事業における具体的なフォレンジックの手順や方法を明確に記述しないまま“可能であれば”と記述のみ行うのは、理解が難しいと考える。困難であることの注記をしてはどうか。 修正案 注:クラウド環境におけるフォレンジックは、技術的な困難さがあり、また、実施上経済的な負担も少なくない。	・ご指摘のとおり、修正いたします。
	該当箇所:18.1.4 タイトル: 段落または図表番号:【クラウドサービスの提供において特に留意すべき課題との関係】 対象となる文・用語など:追加提案 提案理由 クラウドに関わる PII のセキュリティに関しては ISO/IEC27018 が策定中であるので、注記してはどうか 修正案 下記事項を脚注に記載 クラウドサービスに対する PII の安全な取り扱いについては、ISO/IEC27018 が現在策定中である。	・ご指摘の趣旨を踏まえ、18.1.4 の末尾に、ご提案いただいた文章を追記させていただきました。
日本公認会計士協会	1. 受託会社の内部統制に関して委託会社等が利用するための報告書について ① ガイドライン案において記載されている「ISAE3402/SSAE16」又は「サービス・オーガニゼーション・コントロール報告書(SOC2)」は、委託会社の業務を提供する受託会社の内部統制に関して委託会社等が利用するための報告書に関する実務上の指針として、いずれも国外で作成されたものである。 他方で、我が国の実務慣行を踏まえ、当協会から監査・保証実務委員会実務指針第 86 号「受託業務に係る内部統制の保証報告書」(以下「監保実86号」という。)及びIT委員会実務指針第7号「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書」(以下「IT実7号」という。)が公表されている。 したがって、我が国で事業を展開するクラウド事業者においても、監保実86号及びIT実7号の積極的活用が望まれていることを明記すべきと考える。 ② ガイドライン案は、多種多様なクラウドサービスを想定した情報セキュリティマネジメントの指針として作成されているように見受けられ、対象となるクラウド事業者(受託会社)の提供する業務の内容が、委託会社の財務報告に関連するかどうかは明らかにされていない。 他方で、監保実 86 号又はIT実7号のどちらが利用されるかは、受託会社の提供する業務の目的が財務報告に関連するかどうかによって判断されるものである。また、監保実 86 号に基づき作成された報告書については、委託会社とその監査人のみ利用することが想定されていることも踏まえ、ガイドライン案において適切に記載される必要があると考える。	<ご意見①について> ・ご意見の趣旨を踏まえて、IT 実 7 号と SOC2、監保実 86 号と ISAE3402/SSAE16 を、それぞれこの順に必ず併記するように修正いたします。 修正箇所: 図表 5、図表 5 の下の 2 段落目、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(i)、12.7.1【利用者接点とサプライチェーンにおける実務のポイント】本文末尾 <ご意見②について> ・ガイドラインではご指摘の通り、クラウドサービスを、クラウド利用者の財務報告に関連するものに限定していません。従って、クラウド利用者がクラウドサービスを財務報告に関連する業務で利用する場合に限り、監保実 86 号や ISAE3402/SSAE16 が役立つ旨を明記しております。・クラウドサービスの新規利用/乗り換えの獲得の段階では、情報提供の相手は、潜在的な利用者を想定しています。このため、ご意見の趣旨を踏まえて、この段階では、IT 実 7 号又は SOC2 の個別開示にのみ言及し、監保実 86 号と ISAE3402/SSAE16 の開示については記述しないように修正いたします。 ・従って、監保実 86 号と ISAE3402/SSAE16 の開示は、現時点でのクラウド利用者に限定して行う旨の記述となります。 修正箇所: 図表 5、図表 5 の下の 1 段落目(IT 実 7 号又は SOC2 の個別開示を追記)、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(c)の脚注を (i)の脚注へと移動
	2.「内部統制監査報告書」と「ISAE3402/SSAE16」の関係について(7頁、22 頁及び 50 頁) ガイドライン案7頁、22 頁及び 50 頁で「内部統制監査報告書」と「ISAE3402/SSAE16」が同一であるかのような記載があるが、我が国における「内部統制監査報告書」とは、一般的には、金融商品取引法第 193 条の2第2項の規定に基づき、会社が作成した内部統制報告書に対して当該会社の監査人が意見を表明するために発行する内部統制監査報告書を指すと考える。 他方で、「ISAE3402/SSAE16」(注)とは、前述のとおり委託会社の財務報告に関連する業務を提供する受託会社の内部統制に関して、委託会社とその監査人が利用するための報告書を提供する保証業務に関する実務上の指針として国外で作成されたものであるため、少なくとも両者が混同されないような記載へ修正すべきと考える。	・ご指摘の趣旨を踏まえ、次のように修正いたします。 (修正方針) ・IT 実 7 号、SOC2 を総称して、「クラウド事業者のセキュリティ管理に係る内部統制保証報告書」と記す。 ・監保実 86 号と ISAE3402/SSAE16 を総称して「クラウド事業者の内部統制保証報告書」と記す。現状の「内部統制監査報告書」の用語をこの用語に置き換える。 ・この用語について、第 I 部6. 用語及び定義に記載を追加する。 修正箇所: ・第 I 部6. 用語及び定義 ・図表 5、図表 5 の下の 1 段落目、2 段落目、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(i)及びその脚注、12.7.1【利用者接点とサプライチェーンにおける実務のポイント】本文末尾

	（注）SSAE16 は、以前は SAS70 と言われていたが、SSAE16 に改訂された時点で「サービス・オーガニゼーション・コントロール報告書（SOC1）」と称することになった。	
	3. Web 等による一般向けの情報公開システムについて（20 頁） ガイドライン案 20 頁の(b)に記載された「Web 等による一般向けの情報公開システム」の場合は、システムの信頼性又は電子商取引の安全性等に関する内部統制への保証業務に関する我が国の実務上の指針として、当協会から公表されているIT委員会実務指針第2号「Trust サービスに係る実務指針（中間報告）」の利用も有用と考える。	・6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(b)項における「提供しているクラウドサービス」は「Web 等による一般向けの情報公開システム」とは異なるものです。後者は、保証値や努力目標を一般公開するための手段として述べているに過ぎません。 ・現在の表現が紛らわしく、「クラウドサービス」を「Web 等による一般向けの情報公開システムを構築し」て提供すると読み間違えることがあるようです。明確な表現となるよう、次に示す修正を行います。 （修正前）Web 等による一般向けの情報公開システムを構築し、提供しているクラウドサービスのサービスレベルの保証値又は努力目標を情報公開すること。 （修正後）提供しているクラウドサービスのサービスレベルの保証値又は努力目標を、Web 等による一般向けの情報公開システムにより、情報公開すること。
	4. 供給者のサービス提供の監視等について（56 頁及び 57 頁） ガイドライン案 56 頁に記載されている「供給者のサービス提供の監視等」は、具体的には 57 頁に3項目が挙げられている。この(c)に記載されている「アグリゲーションサービス事業者の責任」については、外部監査人の報告書(IT実7号の利用)の提供を求めることにより代替えが可能で、これにより当該事業者の直接的な負担を軽減できるものと考える。	・ご指摘の趣旨を踏まえ、15.2.1【利用者接点とサプライチェーンにおける実務のポイント】(c)に、次のように追記いたします。 （追記後） 但し、この実務は、供給者に対し、外部監査人による「クラウド事業者のセキュリティ管理に係る内部統制保証報告書」の提供を求めることにより代替が可能であり、これによってアグリゲーションサービス事業者の管理統制業務の負担を軽減することができる。
富士通株式会社	○該当箇所 P.36 9.5.1 仮想化資源の分離の確実な実施 (b) IaaS・PaaS の場合は、クラウド利用者がクラウドサービス上にインストールしたソフトウェアに潜在するマルウェア等のリスクについても考慮すること。具体的には、ソフトウェアのインストールや変更に係る履歴を取る等の対策により、情報セキュリティ事象が当該インストールソフトウェアに起因するものであることを切り分けられるようにしておくこと。 ○意見 IaaS で提供される顧客向け仮想環境については、顧客責任で運用され、IaaS 事業者はシステム管理者権限を含めて一切の管理権限を有していないケースが多く、その場合、本項は実施不可能となると考えます。従いまして、本項の記載においては、上記ケースについての追記若しくは注釈を付すべきと考えます。	・ご指摘の趣旨を踏まえ、次の文章を注記いたします。 （注記） クラウド利用者に IaaS で仮想環境を提供し、この環境をクラウド利用者が自らの責任で運用している場合は、クラウド利用者によるソフトウェアのインストールや変更に係る履歴を、クラウド事業者が取得する権限を有していない場合がある。この場合は、(b)の指針は適用されない。
	○該当箇所 P.63 17.2.1 情報処理施設の可用性 (e) クラウドサービスを広域災害から防護するため、データセンタを地理的に離れた複数の地域に設置することにより、(a)～(c)の対策を補完すること。 ○意見 インフラを借り受けてアプリケーションサービスを中心にサービスを提供するクラウド事業者においては、(e)項の実現は費用負担が大きくなり、利用者が望むリーズナブルなサービス価格で提供出来なくなる恐れがあると考えます。従いまして、本項は(a)～(d)項よりも要求度合いを下げた記載とすべきと考えます。以下に修正案を記載致します。 ○修正案 (d) 障害の連鎖を食い止める防護機構を組み込むこと。 なお、クラウドサービスを広域災害から防護する観点からは、以下を実施することも推奨される。 (e)データセンタを地理的に離れた複数の地域に設置することにより、(a)～(c)の対策を補完すること。	・ご指摘のとおり、修正いたします。
匿名	該当箇所：ガイドライン全般 意見：ガイドラインのクレジットを「総務省」ではなく、特定非営利活動法人 ASP・SaaS・クラウドコンソーシアム内に設置された「クラウドサービス提供における情報セキュリティ対策調査検討会」に変更いただきたい。 理由：本ガイドラインは、上記法人が事務局となって運営された「クラウドサービス提供における情報セキュリティ対策調査検討会」によって取りまとめられたものであり、総務省が上記法人に委託しているとは言え、その取りまとめられた内容に関して総務省が責任を負う位置づけになっているのは不適切であり、法令上の位置づけについても誤解を生じ得るため。（総務省が事務局を行うような審議会や検討会の場合であっても、報告書のクレジットは同審議会や検討会の名称で行われているものと拝察する）。	当該検討会は、総務省が策定する本ガイドラインの助言・講評等を行うために設置されたものであり、最終的な取りまとめは総務省が行っております。よって、原案のとおりとさせていただきます。
	該当箇所：1 ページ 7 行目、15 行目 意見：「危険性」という用語を削除し、事実関係を踏まえた正確な記述を希望する。 理由：クラウドサービスについて、一律にデータの保管場所・処理	・ご指摘の趣旨を踏まえ、次のように修正いたします。 1ページ 7 行目 （修正前）他方、クラウドサービスについては、情報漏えい等の情報

	方法が不明確であると断じ、アプリオリに危険性の存在を断定するのは適切でないため。	セキュリティマネジメント上の課題及びデータの保管場所・処理方法が不明確であることの危険性が指摘されているところである。 （修正後）他方、クラウドサービスは、クラウド利用者が直接的に情報システムの設置・運用及びデータの保管・処理等を行わない形態であることから、クラウド利用者による管理監督が行き届かない場合がある。さらに、サービス形態、管理水準、サービスレベル等が異なる多様なサービスが提供され、クラウド利用者の選択肢が増えているにも関わらず、自らの情報セキュリティポリシーを満足できるクラウドサービスを適切に選択できていない場合が多い。この選択に失敗すると、クラウド利用者は情報漏えい等に直面しやすくなり、個別の是正要求もあまり受け入れられず、しかもサービスの乗り換えが難しいことが多い。これらはクラウド利用者から見た課題である。 1ページ 15 行目 （修正前）このサービス提供形態の複雑化は、上述した情報セキュリティマネジメント上の課題やデータの保管場所・処理方法が不明確であることの危険性を、さらに増長させる恐れがあると言われている。 （修正後）しかし、このサービス提供形態の複雑化は、クラウド事業者によるクラウドサービス全体の統制を難しくする要因となっており、全体としてのサービスレベルの低下、ログ取得・保持やレビューの抜け漏れの発生等に直面しやすくなる。これらはクラウド事業者から見た課題である。
	該当箇所：1 ページ　下から 4-5 行目 意見：「コンプライアンスの欠如」、「債務不履行」を削除いただき、当該文章自体の正確な記述を希望する。 理由：第Ⅱ部に記載されているような法的及び契約上の要求事項の遵守についての何らかの対応は必要であろうが、コンプライアンスの欠如や債務不履行等の事象があたかも発生しているかのような表現は適切ではないため。	・ご指摘の趣旨を踏まえ、修正いたします。 （修正前）コンプライアンスの欠如 （修正後）コンプライアンスに係る新しい課題の顕在化 （修正前）利害対立、債務不履行、認識の食い違い、信頼の損失等 （修正後）利害対立、認識の食い違い、公平でない取引、著作権等の権利の侵害、信頼の損失等
	該当箇所：7 ページ　図表 5 中　他 意見：「SLA 規約違反」という用語を修正し、正確な記述を希望する。 理由：「SLA 規約違反」という用語が多用されているが、本来は Metrics を満たせないという意味であり、何らの定義もせずに「SLA 規約違反」という用語を使用するのは適切ではないため。	・SLA 規約違反は、クラウド事業者側から通知するものでなく、クラウド利用者が指摘するものであるという考えに基づき、「SLA 規約違反」の通知を行うという記述全体を削除いたします。 該当箇所：図表 5、図表 5 の下の 2 段落目、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】(c)と(d)の間
	該当箇所：19 ページ　下から 6 行目 意見：「取得した認証・受賞」を「取得している認証」に修正していただきたい。 理由：受賞はマーケティング目的で行われるものも多く、取り上げるには不適切であり、また、認証は現在取得していることが重要であるため。	・ご指摘のとおり、修正いたします。 該当箇所：図表 5、図表 5 の下 2 行目、6.3.2【利用者接点とサプライチェーンにおける実務のポイント】 10 行目及び(b) 3 行目
	該当箇所：20 ページ　2 行目 意見：「そのベンチマーク指標に基づいて」を削除いただきたい。 理由：具体的に何を指すのか定義がなく使用されているため。	・ご指摘のとおり、修正いたします。
	該当箇所：44 ページ　9 行目 意見：「外部の第三者」を削除し、当該文章の正確な記述を希望する。 理由：預託データの押収がなされている場合に、「外部の第三者」とは何を意味するのは不明確であり、意味をなさないため。	・ご指摘の趣旨を踏まえ、次のように修正いたします。 （修正前）外部の第三者の管理下におかれないようにすること。 （修正後）不当に情報漏洩しないような措置を講じること。
	該当箇所：57 ページ　6 行目 意見：(a)(b)とも供給者が責任を負う表現をあらためていただきたい。 理由：アグリゲーションサービスの場合に、アグリゲーションサービス事業者への協力義務を供給者に課すのは適切ではないため。	・アグリゲーションサービスに限定した記述は、「アグリゲーションサービス事業者は」等の書き出しとしています。(a)(b)はこれにはあたりません。 ・「供給者間で」という表現を「クラウド事業者と供給者の間で」に改めました。 ・(b)については、この修正によって全ての供給者がこの求めを課せられるような表現が改められ、ご指摘に沿う修正となっているものと理解しております。 （修正前）各供給者は、他社の （修正後）クラウド事業者は、供給者の （修正前）他の供給者において脆弱性が生じた場合でも、自社が提供するサービスが・・・ （修正後）供給者において脆弱性が生じた場合でも、クラウド事業者が提供するサービスが・・・ ・(a)については、文末の「合意を形成すること」という表現を改め、供給者の規定で確認することによって、クラウド事業者が求める管理・レビューを行うことができる供給者を選択し、その実施状況を管理統制するという趣旨となるように文章を修正いたしました。 （修正前）(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、各供給者は供給者間の合意に基づいて、自らのサービスに関する情報セキュリティマネジメントに係る要求事項の実施状

		況を管理し、必要なレビューを行うこと。 （修正後）(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、供給者が自ら提供するサービスについて、情報セキュリティマネジメントに係る要求事項の実施状況の管理及びレビュー実施に関し、利用規約、SLA 等でどのように規定しているかを確認し、クラウド事業者が求める水準でレビューを実施できる供給者を選定すること。
	該当箇所：64-65 ページ 18.1.1 及び 18.1.2 意見：18.1.1(a)(b)、18.1.2(a)(b)とも、クラウド事業者が責任を負う表現をあらためていただきたい。 理由：パブリッククラウドにおいて、利用者の利用形態は多種多様であり、利用者自身への適用法令や対応措置を最も正確かつ適切に検討できるのは利用者自身であり、クラウド事業者に一律に責任を負わせる表現は適当でないため。	・ご指摘の趣旨を踏まえて、事業者だけがその責任を負うのではなく、利用者が預託する情報の範囲と情報の保存国を適切に選択する責任を果たすことがまず必要であることを踏まえて、クラウド事業者としてはその判断を支援できる範囲を明示し、正確な判断を促進することが望ましいとの記述を追記いたしました。 （追記後） (c) クラウド利用者が、クラウドサービスの海外における脅威を正しく認識し、これに基づいて預託する情報の範囲と情報の保存国を適切に選択する責任を果たせるように、その判断を情報提供等により支援できる範囲を明示して支援し、クラウド利用者の正確な判断を促進すること。
	該当箇所：65 ページ 下から 2 行目 意見：クラウド事業者に、他国の司法権の行使等に伴うサービス停止や資源等の流出に係るリスクを事前に確認し、必要な措置を講じるとあるが、削除いただきたい。 理由：仮に、他国の司法権の行使等に伴うサービス停止や資源等の流出に係るリスクを事前に確認したとしても、具体的に如何なる現実的な措置を取ることが期待されているのかを記載しないままに、クラウド事業者に義務的な表現を記載するのは適当でないため。	・クラウド事業者の不正によりクラウド事業者の情報処理施設等が差押えや押収される場合と、特定の利用者の不正により当該利用者の預託情報等に対し提出命令が発せられる場合を分離しました。その上で、前者については、国を越えたバックアップの仕組み等を想定し、後者については特定のクラウド利用者の預託情報のみを提出できるテナント分離等の措置を想定して、文章を修正いたしました。 （修正前） (a) 他国の資源やサービスを利用してクラウドサービスを提供するクラウド事業者は、他国の司法権の行使等に伴うサービス停止や預託情報の流出に係るリスクを事前に確認し、必要な措置を講じること。 （修正後） (a) 他国の資源やサービスを利用してクラウドサービスを提供するクラウド事業者は、他国において自身又は供給者が法令違反を疑われ、当該国の司法官憲等の不測の差押えを受けた場合であっても、クラウドサービスが停止しないように、国境を越えたバックアップを行う等の必要な措置を講じること。 (b) 他国の資源やサービスを利用してクラウドサービスを提供するクラウド事業者は、一部のクラウド利用者による法令違反の疑いにより、他国の司法官憲等から当該利用者の預託情報の提出命令を受けた場合であっても、無関係なクラウド利用者の預託情報が一緒に流出しないように、預託情報を容易に分離できる等の必要な措置を講じること。
	該当箇所：66 ページ 18.1.4 意見：クラウド事業者に、各国の法制に基づく個人情報保護に必要な取り扱いについて事前に把握し、必要な対策を講じるとあるが、画一的に個人情報の取り扱いについての対策義務を負わせるような表現をあらためていただきたい。 理由：クラウド事業者自身が、個人情報の取り扱いを認識していない、処理を行っていないなど、様々な利用形態が想定されるにも係らず、画一的にクラウド事業者に必要な対策を義務づける表現は適当ではないため。	・クラウド利用者が、自ら個人情報を保存する国を選ぶこと、自らの管理ポリシーを満たすかを確認した上で個人情報を預託すること、そしてこれらの判断の責任を負うことを前提とした上で、原案(a)の文章が適用されるように、以下に示す追記を行いました。 （追記後） (b) クラウド利用者が、クラウドサービスの海外における脅威を正しく認識し、これに基づいて預託する個人情報の範囲と個人情報の保存国を適切に選択する責任を果たせるように、その判断を情報提供等により支援できる範囲を明示して支援し、クラウド利用者の正確な判断を促進すること。