別紙１

「クラウドサービス利用・提供における適切な設定のためのガイドライン」（案）に対して提出された意見及びその意見に対する総務省の考え方

■意見募集期間：　令和４年７月26日（火）～同年８月24日（水）

■意見提出件数：　15件（法人・団体：10件、個人：5件）

■意見提出者：

（敬称略）

	意見提出者
1	アイレット株式会社
2	ヴイエムウェア株式会社
3	エムオーテックス株式会社
4	グーグル･クラウド･ジャパン合同会社
5	株式会社セールスフォース・ジャパン
6	ニューリジェンセキュリティ株式会社
7	HashiCorpJapan株式会社
8	Ubie株式会社UbieDiscovery
9	楽天モバイル株式会社
10	株式会社ラック
―	個人（5件）

※頂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。

該当箇所	提出意見	総務省回答案
Ⅰ．序編		
Ⅰ．１	「コンピュータウイルス･不正アクセスの届出状況」の最新版（2021年）を拝見すると、決してインシデントの原因の多くをクラウドサービスの設定不備が占めているとは言える状況に無いと思います。ランサムウェアや認証の問題、クラウドに限定されないシステムの脆弱性、不正アクセスに対する対応不足等も多く含まれています。サイバーセキュリティ対策は攻撃の傾向を把握し、それらに対する正確な対応が必要であると存じます。 【グーグル･クラウド･ジャパン合同会社】	ご意見については参考として承ります。
Ⅰ．２ （図表）Ⅰ．２－１	・該当箇所 Ⅰ．２図表１．２－１本ガイドラインの想定読者 ・意見内容 想定読者の拡大 ・理由 利用者や導入済み事業者などが対象となっているが、これから導入を予定している事業者や、サービスを検討しているSaaS事業者なども対象にすべきである。 【アイレット株式会社】	ご意見については参考として承ります。
Ⅰ．２ （図表）Ⅰ．２－１	クラウドの導入支援は旧来型（オンプレミス環境構築）のSIerという表現のみではなく、「クラウドサービス導入支援事業者」や「クラウドサービス導入支援パートナー（クラウドの再販に加え、独自の価値を付加してサービスを提供）」との表現も併記すべきと考えます。またこれらSIer、「クラウドサービス導入支援事業者」や「クラウドサービス導入支援パートナー」も自ら“クラウドサービス”を提供している場合もある点もご注意願います。 【グーグル･クラウド･ジャパン合同会社】	旧来型のSIerがご指摘の「クラウドサービス導入支援事業者」や「クラウドサービス導入支援パートナー」の役割をするパターンが多く、読者がより実態を把握しやすいようにするため、原案のままとさせていただきます。
Ⅰ．３	本ガイドラインをセキュリティ管理者が活用した場合の効果も記載することが望ましいと考えます。例えば、「全社のセキュリティポリシーなどを策定する際の指針となる。」など。 【エムオーテックス株式会社】	Ｐ８の図表Ⅰ．５－１に示しますとおり、セキュリティ管理者はクラウドサービス利用者に含まれます。従って原案のままとさせていただきます。
Ⅰ．４	（Ⅳ.クラウドサービス提供側に求められる対策） これは個別の「セキュリティ対策」というよりも、クラウドサービス利用者が、設定の不備等により、個人情報の漏洩や外部からの不正アクセスを防止しつつ、利用者が所属する業界等における法令遵守を果たすための「方策」に対する助言や情報提供という位置づけになるかと思います。 【グーグル･クラウド･ジャパン合同会社】	「方策」に対する助言や情報提供も、広い意味で対策という言葉に含めるという意図ですので、原案のままとさせていただきます。

Ⅰ．５ （図表）Ⅰ． ５－１	「想定読者」の欄に「クラウドサービス利用管理者」とありますが、図表Ⅰ．２－１の定義に照らした場合、正しくは「クラウドサービス管理者」であると思われます。 【エムオーテックス株式会社】	ご意見を踏まえ、図表Ⅰ．５－１の「クラウドサービス利用管理者」の記述を「クラウドサービス管理者」に修正いたします。
Ⅰ．５	（経営層やクラウドサービス管理者等が･･･のiv） 本ガイドライン（案）において「ベストプラクティス」との箇所が多く登場しますが、これらはクラウドサービス事業者（CSP）からの“参照すべきやり方”なのか、もしくはクラウドサービス利用者における対策の“最良ケース集”を参照すべき、ということなのかを明確にして頂けると読者は理解し易いと思います。 【グーグル･クラウド･ジャパン合同会社】	P12にありますとおり、ベストプラクティスは「参考となる具体的な実施手法や注意すべき点」という位置づけとなります。
Ⅰ．６（全般）	用語の定義部分 先日、公正取引委員会が発表した「クラウドサービス分野の取引実態に関する報告書について」内でも同様の用語集がありますので（103ページ以降）、ご参照いただければ幸いです（貴省と定義の解釈が多少異なるものが散見されます）。 【グーグル･クラウド･ジャパン合同会社】	本ガイドラインの用語定義はJISQ27000をもとに作成しております。
Ⅰ．７	参考文献について 2020年11月に日本銀行が発表した「クラウドサービス利用におけるリスク管理上の留意点」もご参照いただければ宜しいかと存じます（金融分野におけるクラウドの利用について述べていますが、本ガイドラインにも参考できる部分があると存じます）。 【グーグル･クラウド･ジャパン合同会社】	ご意見は参考として承ります。
Ⅱ．前提および概要		
Ⅱ．１　本ガイドラインの前提事項		
Ⅱ．１．１ クラウドサービスにおける典型的なセキュリティ設定項目と設定不備があった場合のリスク		
Ⅱ．１．１	（脚注４）「製品」との表現はオンプレミス環境のハードウェアを連想させるものであり、クラウド文脈では「プロダクト」、「サービス」、「ソリューション」、「プラットフォーム」等の言い回しを利用するのが自然かと存じます。 【グーグル･クラウド･ジャパン合同会社】	ご意見を踏まえ、P21「CIS Benchmarks®で示されている主要なクラウド基盤の各製品」の記述を「CIS Benchmarks®で示されている主要なクラウド基盤の各プロダクト 」に修正し、併せて脚注内「比較した製品は、次のとおり。」の記述を「比較したプロダクトは、次のとおり。」に修正します。

Ⅱ．１．１ （図表）Ⅱ．１．１－１ （図表）Ⅱ．１．１－２	・該当箇所 No．１IAM ・意見内容 サービスアカウントの管理を含めるべきである。 ・理由 クラウドサービスのIAM管理には、プログラムやサービスがAPIを利用するためのサービスアカウントの管理が重要である。 人に紐づくアカウント管理だけでなく、サービスアカウントについても言及すべきである。 具体的には、属人化させない、管理者を含む人が利用できない、(設定ファイルなどに)複写できない、特定のサービスのみが利用できる、必要に応じてローテーションできる、といった設定や仕組みが必要となる。 【アイレット株式会社】	ご意見を踏まえ、図表Ⅱ．１．１－１No１中に「IDには、大別してユーザー、管理者及び開発者等の人間に対するアカウントとアプリケーションなどがAPI等で使用するサービスアカウントがある。これらに対するアカウントグループやアクセス権等の設定がある」を追記し、併せて図表Ⅱ．１．１－２No１中に「また、サービスアカウントに対しては、プログラム等が使用するAPIのアクセスキー及びシークレットキー（クレデンシャル情報）の設定管理についても不十分であるとシステム全体の乗っ取りなどのリスクがある。」の記述を追記します。
Ⅱ．１．１ （図表）Ⅱ．１．１－２	近年、「ゲストユーザー」に関する設定の不備から、意図しない情報漏えいが発生している事例が多く発生しています。セキュリティ設定項目の類型のうち、「１.IDとアクセス管理」においてゲストユーザーに言及してはいかがでしょうか。 ■図表II．１．１－２ 考えられるリスクとしては「ゲストユーザー権限を最小限にしない、又は定期的に棚卸ししない等により、適切なユーザーでない外部ユーザーに情報が漏洩するリスクがある。」など 【エムオーテックス株式会社】	ご意見を踏まえ、図表Ⅱ．１．１－２No１中の「退職者のユーザIDやパスワードの失効管理を実施せずに放置すると」の記述を「退職者のユーザIDやパスワードの失効管理を実施せずに放置したり、ゲストユーザーに対する設定が甘かったりすると」と修正します。
Ⅱ．１．１ （図表）Ⅱ．１．１－２	・該当箇所 No．１IAM ・意見内容 クレデンシャルの管理を含めるべきである。 ・理由 クラウドサービスのIAM管理には、ID/Passwordの他に管理者がAPIを利用するためのクレデンシャルの管理が重要である。 ID/Passwordに限り記載されているが、クレデンシャルの管理につても言及するべきである。 具体的には、意図せず(Boxなどの)オンラインストレージや(GitHubなどの)コード管理システムにアップロードしない仕組み、定期的にローテーションする仕組みや設定が必要となる。 デフォルトではクレデンシャルの有効期限が無期限に設定されている場合もある。 【アイレット株式会社】	ご意見を踏まえ、図表Ⅱ．１．１－２No１中に「また、サービスアカウントに対しては、プログラム等が使用するAPIのアクセスキー及びシークレットキー（クレデンシャル情報）の設定管理についても不十分であるとシステム全体の乗っ取りなどのリスクがある。」の記述を追記します。

Ⅱ．１．１ （図表）Ⅱ．１．１－２	・該当箇所 No.１IAM ・意見内容 IAMに、PAMとCIAMが混じって記載されているため、明確化が必要である。 ・理由 IAMの項目に、特権アクセス管理(PAM)に関する事項と、一般利用者の権限(CIAM)に関する事項がどちらも記載されている。 これらは、リスク源や対策が全く異なる事項なので分けて管理するべきである。 内容を見るに、ここでは特権アクセス管理(PAM)に絞るのが妥当と考える。 【アイレット株式会社】	「セキュリティ設定項目の類型」の分類の都合により、特権管理と一般利用者の管理は「IDとアクセス管理」としてNo１の箇所にてまとめて記述という方針とさせていただきました。従って原案のままとさせていただきます。
Ⅱ．１．１ （図表）Ⅱ．１．１－１ （図表）Ⅱ．１．１－２	・該当箇所 No.２ロギングとモニタリング ・意見内容 ログの保存期間 ・理由 デフォルトのログの保存期間が必要期間より短く、削除されてしまうリスクを考慮して、期間設定がセキュリティ管理上問題がないかを検討し設定すべきである。 【アイレット株式会社】	ご意見を踏まえ、図表Ⅱ．１．１－１No２中の「ロギングを有効にするための設定やモニタリングを行うためのフィルタ設定などがある。」の記述を「ロギングを有効にするための設定、モニタリングを行うためのフィルタ設定及びログの保存期間設定などがある。」に修正し、併せて図表Ⅱ．１．１－２No２中の「異常が起きても気が付かないなどのリスクが発生することがある。」の記述を「異常が起きても気が付かない、モニタリングが機能していてもログの保存期間を適切に設定しないで異常時の解析が出来ないなどのリスクが発生することがある。」に修正します。
Ⅱ．１．１ （図表）Ⅱ．１．１－２	・該当箇所 No.２ロギングとモニタリング ・意見内容 ログに機微情報が含まれるリスク ・理由 ログに利用者の個人情報や機微情報が含まれるリスクを考慮して、ログ出力設定を行うべきである。 【アイレット株式会社】	ご意見は参考として承ります。

Ⅱ．１．１ （図表）Ⅱ．１．１−２	・該当箇所 No.２ロギングとモニタリング ・意見内容 改ざん防止措置 ・理由 ログサービスやログ保存先へのアクセス制御設定を適切に行わないと、内容の改ざんが出来てしまう可能性がある。 重要なログは特に防止措置を講じるべきである。 【アイレット株式会社】	ログの保存先であるオブジェクトストレージの完全性に含めさせていただきます。この項目については原案のままとさせていただきます。
Ⅱ．１．１ （図表）Ⅱ．１．１−１ （図表）Ⅱ．１．１−２	・該当箇所 No.３オブジェクトストレージ ・意見内容 ライフサイクルの適切な設定 ・理由 一定期間経過後に削除するなどのライフサイクル設定が適切に行われていないと、保存すべきデータが削除されるリスクにも言及すべきである。 【アイレット株式会社】	ご意見を踏まえて、図表Ⅱ．１．１－１No3中に「ロギング及び一定期間経過後に削除するなどのライフサイクル設定等がある。」の記述を追記します。併せて、図表Ⅱ．１．１−２No３中に「また、ログ情報などが改ざんされたり、ライフサイクル設定を適切に行わなかったためにデータ喪失を引き起こすリスクなどが考えられる。」の記述を追記します。
Ⅱ．１．１ （図表）Ⅱ．１．１−２	・該当箇所 No.３オブジェクトストレージ ・意見内容 完全性の担保に関する記述が必要。 ・理由 考えられれるリスクとして、情報漏えいという機密性のみ記載されているが、完全性、可用性も言及が必要である。 オブジェクトストレージは、ログや証跡の保全にも利用される。 一度書き込まれたものが改ざん・削除されないことを保証する設定なども考慮が必要である。 【アイレット株式会社】	ご意見を踏まえて、図表Ⅱ．１．１−２No３中に「また、ログ情報などが改ざんされたり、ライフサイクル設定を適切に行わなかったためにデータ喪失を引き起こすリスクなどが考えられる。」の記述を追記します。

Ⅱ．１．１ （図表）Ⅱ．１．１−２	・該当箇所 No.４．２ネットワーク ・意見内容 記載内容の表現の変更を提言 ・理由 読者に誤解を与えかねない表現となっている。 「クラウド利用はインターネット経由での利用となるため、基本的なネットワークのセキュリティの設定を確実に行わずに利用」 とあるが、クラウドサービスを利用するためのクライアント側のネットワークのセキュリティ設定と捉えられかねない。 「クラウドは、利用するサービスの目的を踏まえ、クラウドサービスで提供されているセキュリティ機能を適切に行わず利用すると、不正アクセスやマルウェアの感染リスクが高まる」 などの表現の方が良いのではと考える。 【アイレット株式会社】	図表Ⅱ．１．１−２はクラウドサービスの設定項目ということが前提となるものであり、その点についてはP21に記載の通りとなります。従ってご懸念の誤解は生じ難いと考えられるため、原案のままとさせていただきます。
Ⅱ．１．１ （図表）Ⅱ．１．１−１ （図表）Ⅲ．３．１−１	・該当箇所 No.５ セキュリティ等の集中管理 ・意見内容 「セキュリティセンター」が何を指すものかが不明瞭 ・理由 「セキュリティセンター」が何をするものか読み取れなかったため、機能名などを記載した方が良いのではないか。 【アイレット株式会社】	ご意見を踏まえ、図表Ⅱ．１．１−１No5中の「セキュリティセンター」の記述を「セキュリティ集中管理機能」に修正します。併せて図表Ⅲ．３．１ー１No5中の「セキュリティセンター」の記述を「セキュリティ集中管理機能」に修正します。
Ⅱ．１．１ （図表）Ⅱ．１．１−１ （図表）Ⅱ．１．１−２	・該当箇所 No.６．１鍵管理 ・意見内容 ミドルウェアの項目の追加、または仮想マシン(VM.VPS)に導入するミドルウェアの記載の追加 ・理由 脆弱性を突いた攻撃としてはOSのみではなくミドルウェアを対象としたものもあり、ミドルウェアを対象とした攻撃の方が頻度が高いと考える。 ミドルウェアも必要なセキュリティ設定を実施しなかった場合の攻撃の入り口になりうるため、言及した方が良いのではないか。 【アイレット株式会社】	Ⅱ．１．１図表II．１．１−１及び図表Ⅱ．１．１−２において、No6はミドルウェアも含むものと考えております。このため、原案のままといたします。

Ⅱ．１．１ （図表）Ⅱ．１．１－２	・該当箇所 No．６．１鍵管理 ・意見内容 秘密鍵の保護方法についての方針について追加の検討を提言 ・理由 SSH接続などに使用する秘密鍵は、そもそもクラウドサービス上に保管するのは適切でないと考える。 「SSH接続に使用している秘密鍵が漏えいすると、サーバが不正アクセスを受けるリスクがある。データ暗号化用の鍵をKMS（鍵管理システム）を用いずにオブジェクトストレージ等に保管すると、（以下原文のまま）」 等の記載はどうか。 【アイレット株式会社】	該当箇所の記述はクラウド上に保管する秘密鍵を対象としておりますため、原案のままとさせていただきます。
Ⅱ．１．１ （図表）Ⅱ．１．１－２	・該当箇所 No．６．１鍵管理 ・意見内容 秘密鍵の保護方針について追加の検討を提言 ・理由 秘密鍵の漏洩に対する防衛策とするのであれば、KMSの利用だけではなくクラウドサービス事業者が提供する暗号化サービスについても触れるべきと考える。 「秘密鍵をKMSを用いずにオブジェクトストレージ等に保管、または秘密鍵を保管したオブジェクトストレージ等の暗号化を有効化しなかった場合は」 等の表現を検討してはどうか。 【アイレット株式会社】	ご指摘を踏まえて、図表Ⅱ．１．１－２中の「KMS（鍵管理システム）を用いずにオブジェクトストレージ等に保管すると、サーバが不正アクセスを受けたり、マルウェアに感染した場合に、攻撃者に鍵が漏えいし、情報漏えいや不正操作につながるリスクがある。」の記載を「KMS（鍵管理システム）の使用や秘密鍵を保存したオブジェクトストレージの暗号化等の対策を行わずに保管すると、サーバが不正アクセスを受けたり、マルウェアに感染した場合に、攻撃者に鍵が漏えいし、情報漏えいや不正操作につながるリスクが高まる。」に修正します。

Ⅱ．１．１ （図表）Ⅱ．１．１−２	・該当箇所 No.６．４コンテナ ・意見内容 イメージのセキュリティスキャン ・理由 インターネットなどから取得したコンテナイメージについてセキュリティスキャンをせずに使用した場合、設定不備やマルウェアを含んでおり情報漏えいなどのリスクがある。 【アイレット株式会社】	コンテナイメージの設定不備についても「コンテナエンジンに関わるセキュリティ関連の設定」に含むものとして原案のままとさせていただきます。
Ⅱ．１．１ （図表）Ⅱ．１．１−２	・該当箇所 No.７その他の設定項目 ・意見内容 バックアップに関する記述が必要。 ・理由 システムを管理する上で、災害や障害に備えるバックアップは必要なものである。 これはクラウドでも重要性は変わらないため、バックアップ管理についても言及すべきである。 【アイレット株式会社】	ご意見を踏まえ、図表Ⅱ．１．１−２中の「上記以外のクラウドサービス事業者が提供する統合資産管理、モバイルデバイス管理等のサービスについては」の記載を「上記以外のクラウドサービス事業者が提供する統合資産管理、モバイルデバイス管理、バックアップ等のサービスについては」に修正します。
Ⅱ．１．１	国際的な規格や文書である、の箇所、nistの２つの文書の原文は英語である。IPAにて翻訳版があることを明記すべきである。 案の書きぶりだと、「包括的な管理策を確認したいなら、＜原文は英文だけどなんとかして＞個々のケースに応じてそれぞれの文書を参考にされたい。と、＜＞の部分が透けてみえて大変不親切な文体と思料する。改善願う。 【個人B】	ご意見を踏まえ、脚注に「いくつかのNIST文書については独立行政法人情報処理推進機構から日本語訳が公開されている。 https://www.ipa.go.jp/security/publications/nist/」と追記します。

Ⅱ．１．２ 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と役割		
Ⅱ．１．２ （図表）Ⅱ．１．２全般	図表Ⅱ．１．２全般 提供者側環境で定義されている中の「ネットワーク設定」について、PaaS/IaaSではサービス上の仮想ネットワークの設定については利用側の環境となるため、表現としては分かりにくいため注釈などを加える。 【アイレット株式会社】	ご意見を踏まえて、Ⅱ．１．２の３．IaaSの設定に関する責任分界の本文中の脚注に「 仮想ネットワークの設定については利用側の環境となる場合がある。また、クラウドサービスは多様であるため、利用の仕方によってはIaaSに限らず仮想ネットワークが利用側の環境となるケースも考えられる」を記載します。
Ⅱ．１．２ （図表）Ⅱ．１．２−３ （図表）Ⅱ．１．２−４	（SaaSの設定に関する責任分界） SaaSやPaaS提供時の提供者側におけるソフトウェア構成は様々な構成方法があるため、ミドルウェア・OS・仮想環境と断定しない方が良いと思います。 【グーグル・クラウド・ジャパン合同会社】	あくまで一つのモデルケースとして示させていただいております。ご意見は参考として承ります。
Ⅱ．１．２ （図表）Ⅱ．１．２−３	・SaaSの設定に関する責任分界及び、SaaSの責任共有モデルの図 ・責任範囲の線引きにおいて、本来、顧客責任もしくは共有責任であるべき「動作設定」がクラウドベンダー側に来ている事に違和感を感じる。どのように動作させるかは利用者側の設定事項であり、その設定によってはセキュリティに大きな影響を与えるものである。利用者が設定可能な設定範囲については、利用者側に責任が帰属することを明記すべきではないでしょうか？その上でクラウドサービス事業者は、その設定を利用者が理解し、設定できるよう努める義務があると思っています。 【株式会社セールスフォース・ジャパン】	この部分の記述における動作設定はユーザーが設定した機能を実現させるための動作環境の設定という意味であり、提供側の責任範囲に属します。
Ⅱ．１．２	（PaaSの設定に関する責任分界） PaaSがサードパーティーのプロバイダーによって提供されるケースも存在するため、その様なユースケースについても明言が必要かと思います。例えば弊社の提供するBigQueryOmniはAWS上で利用できるPaaSサービスです。BigQueryOmniの場合、提供者は弊社ですが、ハードウェアレイヤーなどの管理はクラウド提供者であるAWSが行います。また、アプリケーションの近代化をするための手法として取り組みが行われている、コンテナ技術についても言及した方が良いかと存じます。コンテナはKubernetesという技術と一緒に用いられる事が多くあります。Kubernetes上ではPaaSと同様にクラウドサービス事業者（CSP）が提供するミドルウェアを利用する事が可能です。CSPが提供するミドルウェアを動かす場合は、利用者側が責任を持つケースとCSPが責任をもつケースがあります。 参考:ElasticCloudonKubernetesshttps://www.elastic.co/jp/subscriptions 【グーグル・クラウド・ジャパン合同会社】	ご指摘の箇所については、いくつかの典型的なモデルケースを示すことを趣旨としていますので原案のままとさせていただきます。ご意見は参考として承ります。

Ⅱ．１．２	・PaaSの設定に関する責任分界 ・PaaSにおいて利用者側には、「どのミドルウェアを利用するか」の選択責任があります。（ミドルウェアのバージョン等含む）その前提の上で、クラウドサービス事業者は、利用者の利用するインフラおよびそのプラットフォームの安全管理責任をもつとともに、危篤性のある環境の利用者については警告を出すなどを行うべきだと考える（利用者により構築されているアプリケーションによっては、プラットフォーマーであるクラウドサービス事業者が安全性のためとは言え、勝手に環境を変更することができない場合がある）そのための共有責任の範囲があるべきではないでしょうか？ 【株式会社セールスフォース・ジャパン】	ご意見は参考として承ります。
Ⅱ．１．２	IaaS設定に関する責任分界 IaaSを利用する場合,利用するOSおよび,ミドルウェアなどのEoS(EndofSupport)を考慮する必要がある。 サービスの継続期間が,各製品のEoSより長い場合,バージョンアップの費用や,体制についても考慮が必要となる。 【アイレット株式会社】	ご意見は参考として承ります。
Ⅱ．１．２	（IaaSの設定に関する責任分界） 「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･SLAに基づき、ゲストOS等が動作するための仮想環境の構築と管理をクラウドサービス事業者に要求できる」との記述がされていますが、これらは利用者が要求するものではなく、クラウドサービス事業者が提供するものと考えます。よって、「クラウドサービス事業者は、クラウドサービス利用者との契約･SLAに基づき、ゲストOS等が動作するための仮想環境の構築と管理を提供する」との表現が宜しいかと存じます。また「図表Ⅱ．１．２－５IaaSの設定における責任分界」に仮想環境の設定の記載がございますが、こちらはどのような作業を想定していますでしょうか？弊社の考える責任分界点では、仮想環境の設定は想定しておらず、ゲストOS以上をお客様に管理していただくことを想定しています。 参考：Share 【グーグル･クラウド･ジャパン合同会社】	前段についてはご意見を踏まえて、Ⅱ．１．２中の「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・SLAに基づき、ゲストOS 等が動作するための仮想環境の構築と管理をクラウドサービス事業者に要求できる。」の記述を「クラウドサービス事業者は、クラウドサービス利用者との契約･SLAに基づき、ゲストOS 等が動作するための仮想環境の構築と管理を提供する」と修正します。後段については、仮想環境において提供側が行う設定については、仮想環境が正常に機能するための設定があり、ユーザー側については仮想マシンを利用するための設定等があります。
Ⅱ．１．２ （図表）Ⅱ．１．２－５ （図表）Ⅱ．１．３－１	「図表２．１．２－５IaaSの設定における責任分界」と 「図表２．１．３－１SIerが関与する場合の設定に関する責任分界（IaaSの例）」の差異は SIerが支援に入るかどうかの１点のみかと思いますが、 「仮想環境の設定」の責任範疇に変更があるのは意図した表記でしょうか？ 【個人A】	ご意見を踏まえ、図表Ⅱ．１．２－５の図の記載に合わせて修正いたします。

Ⅱ．１．３ 環境の設定における留意すべきパターン		
Ⅱ．１．３	【該当箇所】 SaaSの提供形態での代理販売のケースについては、セキュリティ設定上の責任は、一義的にSaaS利用者にある前提を記載したほうが良い 【指摘内容】 SIerがSaaSを提供する場合 【理由】契約条件の確認は重要ですが、SaaS上のデータ・アプリ設定の責任が利用者にあることは明記しても差し支えないと考えます 【ニューリジェンセキュリティ株式会社】	ご意見は参考として承ります。
Ⅱ．１．３	SaaS事業者が他社のIaaS/PaaSを利用してクラウドサービスを提供する場合 クラウドサービス(IaaS/PaaS)を利用してSaaSを提供する事業者の場合、クラウドサービスに帰する障害が発生した場合、SaaSサービスの可用性について免責とする場合がある。 クラウドサービス利用者は、そのサービスが免責とする事項について確認が必要である。 【アイレット株式会社】	ご指摘の箇所については、Ⅱ．１．３本文中に「ただし、SaaS事業者Aにサービス提供するするクラウドサービス(IaaS/PaaS)に帰する障害が発生した場合、契約によってはSaaSサービスの可用性について免責とする場合がある。そのため、クラウドサービス利用者は、そのサービスが免責とする事項について確認が必要である。」と追記します。
Ⅱ．１．３	・SaaS事業者が他社のIaaS/PaaSを利用してクラウドサービスを提供する場合 ・利用者側で担保すべき内容がSIerに波及しています。ここはプロジェクトの提供形態にもよりますが、場合により変更になる部分であり、ガイドラインでは決められないものだと思われます。 【株式会社セールスフォース・ジャパン】	ご意見は参考として承ります。

Ⅱ．１．３	【該当箇所】 「SaaS事業者Aは、クラウドサービス利用者との契約者であることから、クラウドサービス利用者との契約に基づき、提供するクラウドサービス全体の管理責任を負う。」については、SLO/SLAを満たすクラウド基盤における障害への対応（たとえば冗長化など）なども含めた設計責任であり、基盤に対する管理責任に含まれることを明確としたい 【指摘内容】 SaaS事業者が他社のIaaS/PaaSを利用してクラウドサービスを提供する場合 【理由】SaaS事業者の提示するSLO/SLAが利用者に対する提供責任となるが、クラウドサービス全体管理責任にそれらの可用性を担保する設計意図を含むことを明確にしても差し支えないと考えます 【ニューリジェンセキュリティ株式会社】	ご意見は参考として承ります。
Ⅱ．１．３	「サプライチェーン構造」との記述 一般的にクラウドサービスの提供において、「サプライチェーン」との表現を利用することはなく、「提供形態」という呼び方をするのが自然と考えます。 【グーグル･クラウド･ジャパン合同会社】	「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）」との整合をとるため、原案のままとさせていただきます。
Ⅱ．２ 設定不備の要因と対策		
Ⅱ．２．１ 設定不備の事例と要因分析		
Ⅱ．２．１	事例１の記述について クラウドサービス事業者が提供しているSaaSの機能変更を行った際、当該SaaSのセキュリティレベル設定のディフォルト値が下がった旨記述がありますが、これはCSPがあえてプロダクトのアップデートを行って、セキュリティレベルを下げたケースがあった旨を意味しておりますでしょうか？通常では考えられないケースと思われますが、具体的にどの様な案件であったのかご教示いただけますと有り難く存じます。 【グーグル･クラウド･ジャパン合同会社】	CSPが故意にセキュリティレベルを下げたという意味ではなく、結果として下がっていたという趣旨となります。趣旨をより明確にするため、「これに伴い、当該SaaSのセキュリティレベル設定のデフォルト値が下がる方向に変更になった」の記述を「これに伴い、当該SaaSのユーザーアクセスに関する設定について、結果的にデフォルトでセキュリティレベルが下がってしまった。」に修正します。

Ⅱ．２．１	・事例１クラウドサービス提供事業者が、提供しているSaaSの機能変更を行った。これに伴い、当該SaaSのセキュリティレベル設定のデフォルト値が下がる方向に変更になった。利用企業側はこれに気づかず、低いセキュリティレベル設定のまま利用し続けた結果、機密情報が大量に流出した。 ・本件は当該設定のデフォルトセキュリティレベルを下げる変更を行ったのではなかったかと思われます。例題をたとえば「事例１クラウドサービス提供事業者が、提供しているSaaSの機能追加を行った。これに伴い、当該SaaSにおいて、従来より誤った設定を行なっていた場合に、その新機能では、誤った設定が表面化する結果となった。その結果、機密情報が大量に部外者にアクセス可能となった。」などに変更していただくのが適切かと思われます。 【株式会社セールスフォース・ジャパン】	CSPが故意にセキュリティレベルを下げたという意味ではなく、結果として下がっていたという趣旨となります。趣旨をより明確にするため、「これに伴い、当該SaaSのセキュリティレベル設定のデフォルト値が下がる方向に変更になった」の記述を「これに伴い、当該SaaSのユーザーアクセスに関する設定について、結果的にデフォルトでセキュリティレベルが下がってしまった。」に修正します。
Ⅱ．２．１	【該当箇所】 既存の事例１−３は主な設定不備の事例という意味では異論ございません。しかしながら、クラウド環境に侵入後のNWアクセス制御（主に外向け）の不備による被害拡大の事例もそれに並ぶと思われますので、事例４として以下のような事例を追加することを提案します。 事例４ ある企業が提供するクラウド上のWebサービスのアプリケーションの脆弱性を突いて、サーバに侵入され、その後攻撃者が用意した外部サーバに大量の機密情報が流出した。 【指摘内容】 設定不備の事例 【理由】アカウントなりすましやWebアプリの脆弱性によりクラウド環境に侵入され、その後二次被害として、NWアクセス制御（外向け）の不備により、C2サーバや攻撃拠点への通信するような被害拡大事例を減らすことを遡及するため。 図表Ⅲの４．２のネットワーク設定を促す事例になるはずです。 【ニューリジェンセキュリティ株式会社】	事例の根拠となる実際のインシデントが確認できませんでしたので、原案のままとさせていただきます。 ご意見は参考として承ります。

Ⅱ．２．１	【意見】「１.組織に関するもの」とありますが、図表Ⅱ．２．２−１や図表Ⅱ．２．２−２では「１.人・組織に関するもの」と記載されています。表記を統一すべきであると考えます。 【エムオーテックス株式会社】	ご指摘を踏まえ、Ⅱ．２．１中の「１．組織に関するもの」の記述を「１．人・組織に関するもの」に修正します。併せて図表Ⅱ．２．１−１中の「組織に関するもの」の記述を「人・組織に関するもの」に修正します。
Ⅱ．２．２ 要因に対する対策		
Ⅱ．２．２	・設定不備の要因と対策 ・利用者側の責任として、既存の設定を利用するだけでなく、常に最新の状況を利用者側も把握し、サービス提供側から提供される最新機能をどんどん利活用する責任があるかと思われます。（多要素認証を利用する等） 【株式会社セールスフォース・ジャパン】	「技術情報の収集」に含まれるため、原案のままとさせていただきます。
Ⅱ．２．２	＜利用者に提供すべき対策＞1.情報提供について もう少し具体的に“クラウドサービス利用者に分かりやすく伝える”とは何を意味するのか（何を分かりやすく伝えるのか）、何を提供側は行うべきなのか記述されると良いかと思います（一般的に各CSPは、利用者･顧客に契約書上やサポートページなどで「分かりやすい」説明を心がけていると思います） 【グーグル･クラウド･ジャパン合同会社】	各対策の具体的な内容は「Ⅳクラウドサービス提供側に求められる対策」にて述べる構成となります。従って原案のままとさせていただきます。
Ⅱ．２．２	・設定不備の要因と対策：提供側の対策 ・＜利用者に提供すべき対策＞に新しい脅威に対する対策と対応するための機能の提供を加えるべきではないでしょうか？ 【株式会社セールスフォース・ジャパン】	本ガイドラインは「クラウドサービスの適切な設定」に特化したガイドラインとなっておりますので、原案のままとさせていただきます。
Ⅱ．２．２	５.組織的な改善活動 クラウドサービス提供者における“マインドについての対策”とは具体的に何を意味しますでしょうか？ 【グーグル･クラウド･ジャパン合同会社】	具体的にはⅣ．６に記載の内容となります。わかりにくい表現かと思いますので「マインドについての」の記述を削除いたします。

Ⅲ．クラウドサービス利用側に求められる対策		
Ⅲ．１ 組織体制・人材育成		
Ⅲ．１．１ クラウドサービス設定不備の抑止・防止に係る方針的事項		
Ⅲ．１．１．１ Ⅲ．１．１．２ Ⅲ．１．１．４	「３．１．１．１【基本】クラウドサービス利用におけるガバナンスの確保」や 「３．１．１．２【基本】事業部門等が独自に利用する場合のルール形成」にて 決定した規定/ルール/システム対策は、当然委託先が順守・対応をしようとすると 費用がかかるものになります。 ＃「契約にないので対応しません」というケースもあり そのため、「３．１．４コミュニケーション」において 契約前に規定/ルール/システム対策への対応を要求し、 対応できる会社に委託する、ということを利用者側の責務として 記載したほうがいいように思いました。 【個人A】	Ⅲ．１．１．１及びⅢ．１．１．２の記載はクラウドサービス利用側の企業が自組織に取り組むべき内容であり、委託先における対策とは異なります。したがって原案のままとさせていただきます。
Ⅲ．１．１．１	【基本】クラウドサービス利用におけるガバナンスの確保ベストプラクティス クラウドサービスの特性上、クラウドサービス事業者側の提供内容や利用規定は様々な要因で変更する可能性がある。組織内のガバナンスの必要に応じた更新の実施も行うべき。 【アイレット株式会社】	本ガイドラインは「クラウドサービスの適切な設定」に特化したガイドラインとなっておりますので、原案のままとさせていただきます。
Ⅲ．１．１．１	【ベストプラクティス】全体部分 vii.として新たに「社内セキュリティ」及び「コンプライアンス」部門の整備行うことを提案致します。フィジカル及びサイバーセキュリティに対する専門家と、法務やコンプライアンスの専門家が協働する形で、クラウド運用ポリシーを作り、実際運用することが、誤った設定を起こさない仕組み作りと同義であると考えます。 【グーグル･クラウド･ジャパン合同会社】	ご意見を踏まえ、Ⅲ．１．１．１ベストプラクティス中の「i.組織のクラウドサービス利用について、安全性を確保するための管理部門の設置。」の記述を「ｉ.組織のクラウドサービス利用について、安全性を確保するために社内セキュリティ部門やコンプライアンス部門などの管理部門を設置、整備する。」と修正いたします。

Ⅲ．１．１．１	（「クラウドサービス利用・提供における適切な設定のためのガイドライン」（案）、「v.組織の許可なく利用されているクラウドサービスの発見と抑止。」との記載部分） ・意見内容 当該部分について「v.CASB(CloudAccessSecurityBroker)機能などによる、組織の許可なく利用されているクラウドサービスの発見と抑止。」との変更を提案します。 （理由） より実効性のあるガイドラインとするためには、組織の許可なく利用されているクラウドサービスの発見と抑止をする概念だけでなく、具体的な機能を読み手に対して明示する必要があります。（案）が示す「発見と抑止」にかかる具体的・実効的な手段として、CASB（CloudAccessSecurityBroker）を例示する事を提案します。 【ヴイエムウェア株式会社】	ご意見を踏まえ、ベストプラクティス「v.組織の許可なく利用されているクラウドサービスの発見と抑止」を「v.組織の許可なく利用されているクラウドサービスを発見、抑止する。併せてクラウド利用状況の可視化ツールとしてCASB(CloudAccessSecurityBroker)機能などの導入を検討する。」と修正します。
Ⅲ．１．１．１	【該当箇所】 企業や組織におけるクラウドの利活用方針やガバナンスを集中的に行う CCoE(Cloudcenterofexcellence)の記載 【指摘内容】 Ⅲ．１．１．１【基本】クラウドサービス利用におけるガバナンスの確保 【理由】昨今では企業や組織におけるクラウドの利活用方針やガバナンスを集中的に行う役割として、CCoE(Cloudcenterofexcellence)を設置する企業が増している。CCoEによりクラウド有識者が組織横断的にクラウドのセキュリティに関する施策を統一的に行えるため、設定不備における課題に対しても有効である 【ニューリジェンセキュリティ株式会社】	ご意見を踏まえ、ベストプラクティスに「ix.企業や組織におけるクラウドの利用方針やガバナンスを集中的に行う役割として、CCoE(Cloudcenterofexcellence)を設置することは、組織横断的にクラウドのセキュリティに関する施策を行えるため、設定不備における課題に対しても有効である。」を追記します。併せて脚注に「部門横断的にクラウド戦略を推進していくために、必要な人材やリソースなどを集約した組織を指す用語として使われている。」を追記します。
Ⅲ．１．１．２	【基本】事業部門等が独自に利用する場合のルール形成 運用開始前に各種設定値の外部診断を推奨しているが、運用開始前だけではなく、サービス構築中にもセキュリティ設定不備により情報漏洩が発生しうる。構築期間中に遵守すべきセキュリティ対策についても周知する必要がある。 【アイレット株式会社】	ご意見は参考として承ります。
Ⅲ．１．１．２	【基本】事業部門等が独自に利用する場合のルール形成ベストプラクティス クラウドサービスは利用方法、利用状況によってコストが拡大し続ける可能性があるため、コストを管理について注意すべき。 【アイレット株式会社】	本ガイドラインは「クラウドサービスの適切な設定」に特化したガイドラインとなっておりますので、原案のままとさせていただきます。

Ⅲ．１．１．２	【基本】事業部門等が独自に利用する場合のルール形成ベストプラクティス 利用方法について明確な禁止事項について可能な場合はクラウドサービス自体に制限をかける機能を有効にすべき。 【アイレット株式会社】	ご指摘の点については「ルール」の中に含まれるとし、記述自体は原案のままとさせていただきます。
Ⅲ．１．１．２	【基本】事業部門等が独自に利用する場合のルール形成ベストプラクティス ルールの策定だけでなく、権限外のコンポーネント作成などが出来ないよう、クラウドサービスの機能を使用した防止措置について触れた方が良い。 【アイレット株式会社】	ご指摘の点についてはⅣ．４．２において提供者側の対策として記載しております。従って原案のままとさせていただきます。
Ⅲ．１．１．３	【該当箇所】 「設定診断等の支援ツール利用に対する組織的取組」について推奨とされているが、IaaS利用においては基本としてもよいのではないか 【指摘内容】 Ⅲ．１．１．３【推奨】設定診断等の支援ツール利用に対する組織的取組 【理由】「Ⅲ．３．１．２【基本】設定項目の管理」では、記載の通り、設定不備の即時通知と対策が基本として定められています。 主要なIaaSの環境においては設定診断がクラウドサービスで標準的に利用可能な機能として提供されており、最低限の設定不備の検査は利用者の責任において必須とすべきと考えます 【ニューリジェンセキュリティ株式会社】	設定不備の検査自体につきましては、Ⅲ．４．３．１において【基本】として定めております。設定診断において支援ツールを活用することについては【推奨】として原案のままとさせていただきます。
Ⅲ．１．１．４ （ANNEX）Ⅲ．１．１．４	【基本】クラウドに関する人材の組織的育成 組織的にクラウド資格等の取得やクラウドサービス事業者が用意するセミナーの受講等について文書化するとの記載があるが、それだけでなく組織内共有を実施し、知識を共有することで組織全体の知識やノウハウの向上ができる 【アイレット株式会社】	ご意見を踏まえ、Ⅲ．１．１．４本文中及びANNEX中のⅢ．１．１．４の「クラウドサービス事業者が用意するセミナーの受講等」の記述を「クラウドサービス事業者が用意するセミナーの受講及び知識の組織内共有等」と修正します。

Ⅲ．１．２　技術情報の収集		
Ⅲ．１．２．１	【基本】技術情報の収集ベストプラクティス 技術情報を収集した上で現状の利用状況を更なる改善をする上での見直しを実施計画を行うことで、単に知り得るだけでなく、知った知識を利用する目的意識をすることで収集に対する意欲を高められる。 【アイレット株式会社】	ご意見は参考として承ります。
Ⅲ．１．２．１	ベストプラクティス 複数の言語で展開されているクラウドサービスを利用する場合、翻訳のミスやタイムラグにより言語間で情報に差があることが考えられる。 自身が参照する場合や、利用者に提供する情報は、言語間の差に留意して最新の情報を利用する必要がある。 【アイレット株式会社】	ご指摘の点についてはⅣ．２．３中のコラムにて触れさせていただいているので、この箇所の記述においては原案のままとさせていただきます。
Ⅲ．１．２．１	【該当箇所】 会社メールやチャットシステムにクラウドサービスのリリース情報をポストする仕組みを作ると、複数人チェックも働くため漏れを防げる可能性が高まることも触れてもよいと考える。 【指摘内容】 【基本】技術情報の収集【ベストプラクティス】 【理由】経験上、Ｉのように自発的に収集する体制だと漏れる可能性が高く、そのような事例をたくさん見てきた。そういう仕組みもなるべく自動化し、多くの関係者の目に触れるようにするべき。 【ニューリジェンセキュリティ株式会社】	ご意見を踏まえ、Ⅲ．１．２．１ベストプラクティスｉに「また、通知に当たっては、メーリングリストやチャットシステムなどを活用することにより、複数人がチェックできるようにする。」の記述を追記します。
Ⅲ．１．２．１	ベストプラクティス 昨今のクラウドサービスは複雑化しており、多くの技術情報が発信されている。 技術情報の評価について、脆弱性情報収集・管理ツール等を利用し、自動的に評価をして必要な情報のみ伝える仕組みの構築をベストプラクティスに含むべきである。 【アイレット株式会社】	ご意見は参考として承ります。
Ⅲ．１．３　人材育成		
Ⅲ．１．３	人材育成 自社で育成するだけにとどまらず、知見のあるSI会社などの利用も検討するなどを方法の１つとして入れても良いのではないか。 【アイレット株式会社】	自社以外にも「製品を提供するベンダーが用意するトレーニングコースの受講を奨励する」と定めているので原案のままとさせていただきます。

Ⅲ．１．３	人材育成前半部分 セキュリティやクラウド技術、コンプライアンス対応に関する国家及び国際資格を有する人材の育成もしくは雇用、についての項目を加える（ベストプラクティスに含める）と宜しいかと存じます。 【グーグル･クラウド･ジャパン合同会社】	国際資格を有する人材の育成についてはⅢ．１．３．２のベストプラクティスiiiで定めていますので原案のままとさせていただきます。
Ⅲ．１．３．１	【基本】クラウドサービス利用におけるリテラシーの向上 記載されている内容がサービス導入時等の記載しかないため、組織の継続的な教育の内容を盛り込んだ方良いと考える。リテラシーの向上については一朝一夕では向上できないため、組織で継続的な教育を行い啓蒙する必要性がある。また、適宜説明会等を開くのではなく、サービス利用開始における必須条件として組織で用意している教育資料の閲覧を義務付けるなどを盛り込んではどうか。 【アイレット株式会社】	継続的な教育についてはⅢ．１．３．２において「クラウドシステムにおける動作環境の設定についての技術力を継続的に向上させること」と定めているので原案のままとさせていただきます。
Ⅲ．１．３．１	【基本】クラウドサービス利用におけるリテラシーの向上ベストプラクティス 組織内においてインシデント、アクシデント等が発生した内容をケーススタディとして利用することで理解度を向上できるだけでなく再発防止にもなるため、ベストプラクティスに追加すべき。 【アイレット株式会社】	ご意見を踏まえ、Ⅲ．１．３．１ベストプラクティスに「v. インシデント、アクシデント等が発生した場合、その内容をケーススタディとして組織内で共有し理解度向上及び再発防止に活用する。」を追記します。
Ⅲ．１．４　コミュニケーション		
Ⅲ．１．４．１	【ベストプラクティス】クラウドサービス利用者 v.として、ユーザーコミュニティ（がある場合）から最新のサービスのリリースやトラブル対応等について相談し、最適解を導くためのヒントを得る、などの記述を加えると良いかと思います。ユーザーコミュニティの知識や運用ノウハウは相当のレベルに達しているほか、自分と似たような境遇のユーザーに気軽に相談できる環境があることは重要かと思います。 【グーグル･クラウド･ジャパン合同会社】	ご意見を踏まえてⅢ．１．４．１ベストプラクティスに「v. 利用するクラウドサービスの信頼できるユーザーコミュニティがある場合、最新のサービスのリリースやトラブル対応等について相談し、内容を精査した上で参考とする。」と追記します。

Ⅲ．２ 作業規則・マニュアル		
Ⅲ．２．１ 作業規則やマニュアルの整備		
Ⅲ．２．１．２	・該当箇所 【基本】作業手順書の整備 ・意見内容 作業手順の見直しの追加 ・理由 クラウドサービス事業者のサービスリリースのため、従来推奨されていた内容から別の推奨方法に変更や従来方法での提供の取りやめなどが考えられる。 そのため、過去に作成した手順書が利用段階でそぐわない場合がある、特定のタイミングでの手順書の見直しなどについても言及をすべきである。 【アイレット株式会社】	作業手順書の見直しについてはⅢ．２．１．４作業手順書に係るマネジメントで定めているため、原案のままとさせていただきます。
Ⅲ．２．１．２	該当箇所：【基本】作業手順書の整備 ベストプラクティスiii ＜意見＞ ・記載に賛同いたします。ただし、全社的な実施は困難な場合もあるため、事業部などの組織構造を適切に設計した上で、組織単位等で制約を設けることも検討すべきと考えます。 ・例えば、本番環境では22sshを開けることができなくするなどの制約は、GCPであればOrganizationpolicyにより実現可能と認識しております。 （ご参考）https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints](https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints) ＜理由＞ ・事業者としてよりリスクをコントロールしやすくなると考えるため。設定すること自体にお金がかかるものではなく、容易に実践可能と認識しております。 【Ubie株式会社UbieDiscovery】	ご意見は参考として承ります。
Ⅲ．２．１．２	該当箇所：【基本】作業手順書の整備 ベストプラクティスiv ＜意見＞ ・記載に賛同いたします。ただし、CI/CDまでセットで考えた上で、そのセキュリティについても考慮することが望ましいと考えます。 ＜理由＞ ・人間が管理するとどうしても手順の抜け漏れや破損リスクがあり、なるべく自動化することが望ましいと考えるため。 【Ubie株式会社UbieDiscovery】	ご意見は参考として承ります。

Ⅲ．２．１．３	・該当箇所 【基本】ヒューマンエラー対策 ・意見内容 誤設定の検出 ・理由 人によるチェックと併用し、クラウドサービス側の設定チェック機能などを最大限活用するよう記載した方が良いのでは。 【アイレット株式会社】	設定診断などの支援ツールの活用についてはⅢ．１．１．３設定項目診断ツールの提供にて述べさせていただいておりますので本箇所については原案のままとさせていただきます。
Ⅲ．２．１．３	・該当箇所 【基本】ヒューマンエラー対策 ・意見内容 設定の自動化などの言及 ・理由 作業者の完全なヒューマンエラーの排除は難しいため、組織として設定すべき汎用的な設定については、IaCやクラウドサービスが提供するサービスを用いて設定を自動的に適用できるよう利用者組織の管理部門等で用意することを推奨するなどを言及してはどうか。 【アイレット株式会社】	IaCやツールの活用などについては、Ⅲ．２．１．２ベストプラクティスⅳⅢ．１．１．３などで述べているため、本箇所については原案のままとさせていただきます。
Ⅲ．２．１．３	・該当箇所 【基本】ヒューマンエラー対策ベストプラクティス ・意見内容 想定外の作業結果が反映されていないかを検出 ・理由 意図せぬ結果を検知可能なように、作業変更後の確認作業において作業結果で想定された内容以外が変更されていないかを検出する仕組みを用意する必要がある。 【アイレット株式会社】	想定外の結果の検知についてはベストプラクティスｉのダブルチェックに含まれるものとし、原案のままとさせていただきます。
Ⅲ．２．１．３	・該当箇所 「【基本】ヒューマンエラー対策」の「【ベストプラクティス】」 ・意見内容 「i.-iii.」に加え、下記事項の追記をご提案します。 「設定事項が組織のポリシー(セキュリティ基準など)に合致しない場合は、 自動的に検出・通知がなされる仕組みを組み込む。」 ・理由（可能であれば、根拠となる出典等を添付又は併記してください。） ダブルチェックやレビューなどによる防止策に加え、人手によらない(システム・機能で自動的に実施される)防止策も同時に実施すべきと考えます。 「i.-iii.」に加え、下記事項の追記をご提案します。 「設定事項が組織のポリシー(セキュリティ基準など)に合致しない場合は、 自動的に検出・通知がなされる仕組みを組み込む。」 【HashiCorpJapan株式会社】	設定値の監視についてはⅢ．１．１．３にて述べられておりますので、本箇所は原案のままとさせていただきます。

Ⅲ．３ クラウドサービスにおけるシステム動作環境の設定管理		
Ⅲ．３	・該当箇所 クラウドサービスにおけるシステム動作環境の設定管理 ・意見内容 サービス継続に関する必要な事項の合意が必要である。 ・理由 クラウドを利用する場合、利用者の要求に応じてバックアップなしから、DR構成や、ホットスタンバイ構成まで構成する事が可能となる。 利用者側の責任において、必要な要求レベルを定めて対策を求める必要がある。 【アイレット株式会社】	本ガイドラインはクラウドサービスの適切な設定の推進が趣旨となりますので、原案のままとさせていただきます。
Ⅲ．３	クラウドサービスにおけるシステム動作環境の設定管理 クラウド上では、オンプレミスのようにディスクの破棄など物理的な破砕が不可能となるため、データの破棄を保証する方法を事前に検討した上で利用すべきである。 利用終了時にどのようにデータを保護するのか、予め備える必要性について言及すべきである。 Ⅲ．３の下に節を新設して記載するのが良いと考える。 例として、オブジェクトストレージでは、暗号化を有効化しておかなければ、利用終了時にデータを復元できないことを保証できない。 また、ドメインは破棄後に第三者によって再利用されうるため、サブドメインテイクオーバーが発生しないように事前に備える必要がある。 【アイレット株式会社】	本ガイドラインはクラウドサービスの適切な設定の推進が趣旨となりますので、原案のままとさせていただきます。
Ⅲ．３．１ クラウドセキュリティに係る設定項目の確認		
Ⅲ．３．１．１	該当箇所：【基本】設定項目の把握と設定 ベストプラクティスⅱ ＜意見＞ ・管理者や特権アカウントの管理については、目的に応じて適切に一時的に限定した権限を付与する場合もあり、その際には付与する期間や権限に応じた管理を行うことを考慮すべきと考えます。 ＜理由＞ ・一時的に付与する特権アカウントにも複数人チェック等を必要とすることは事業者にとって負荷が高く、常設の特権アカウントとは分類して管理することが必要と考えるため。 【Ubie株式会社UbieDiscovery】	ご意見は参考として承ります。

Ⅲ．３．１．１ （図表）Ⅲ．３．１−１	【該当箇所】 「ユーザアカウントの管理においては、パスワード設定の厳格化や多要素認証の設定を必須とすることを推奨する。」 IAMユーザであっても必須レベルなので推奨という文言は省いてもよいと考える。 【指摘内容】 ii.特に重要な設定項目 【理由】IAMユーザの多要素認証を面倒でやっておらず、パスワードが緩い事例が多い。管理者ユーザでないからと油断してはいけない。 【ニューリジェンセキュリティ株式会社】	Ⅲ．３．１．１の表題において【基本】としていることによりどのようなクラウドサービスにも基本的に実施することが求められる対策である旨が示されています。ただし、記述がわかりにくい部分があると思われるため、Ⅲ．３．１．１ベストプラクティスⅱ.特に重要な設定項目中の「多要素認証の設定を必須とすることを推奨する。」の記述を「多要素認証の設定を行う。」に修正します。
Ⅲ．３．１．１	・該当箇所 クラウドセキュリティに係る設定項目の確認 ・意見内容 特権の利用について ・理由 特権アカウントの利用者や特権昇格可能なアカウントは最小限に絞り、必要時のみ利用する設定・運用とすることが望ましい。 【アイレット株式会社】	ご意見を踏まえ、Ⅲ．３．１．１ベストプラクティスⅱ特に重要な設定項目に「・特権アカウント利用者や特権昇格可能なアカウントは、最小限とすることが望ましい。」を追記します。
Ⅲ．３．１．１ （図表）Ⅲ．３．１−１ 全般	「図表Ⅲ．３．１−１クラウドにおけるセキュリティ設定項目の類型と対策」には 攻撃から守る手段（WAFやDDoS対策）はあってもいいのかなと思いました。 #オートスケールの上限を設定していない環境で、DDoS攻撃をうけたことで 金銭的な被害にあうケースもあると思慮 【個人A】	ご指摘の「攻撃から守る手段」についてはNo.５のセキュリティ等の集中管理に含まれるものとなります。従って原案のままとさせていただきます。

Ⅲ．３．１．１ （図表）Ⅲ．３．１－１	【該当箇所】 「管理者アカウントには多要素認証を必須にする等の設定を確実に行うほか、組織の要件に応じてユーザアカウントの各種設定を確実に行う必要がある。」 ユーザアカウントもMFA必須とするべきである。また、IP制限を加えることも推奨する。※オフィスレスの場合IP制限できない可能性もあるため推奨とする。 【指摘内容】 １.IDとアクセス管理（IAM） 【理由】IP制限も重要なセキュリティ対策である。 【ニューリジェンセキュリティ株式会社】	ご意見前段につきましては、ご指摘のとおり、MFAを必須とするクラウドサービス事業者は増えてきましたが、対応できない事業者もまだ多い状況のため原案のままとさせていただきます。 後段のIPアドレス制限についてはご意見を踏まえ、図表Ⅲ．３．１－１「組織の要件に応じてユーザアカウントの各種設定を確実に行う必要がある。」の記述を「組織の要件に応じてユーザアカウントのIPアドレス制限など各種設定を確実に行う必要がある。」に修正します。
Ⅲ．３．１．１ （図表）Ⅲ．３．１－１	近年、「ゲストユーザー」に関する設定の不備から、意図しない情報漏えいが発生している事例が多く発生しています。セキュリティ設定項目の類型のうち、「１．IDとアクセス管理」においてゲストユーザーに言及してはいかがでしょうか。 ■図表Ⅲ．３．１－１ 「クラウドサービスにおけるゲストユーザーは一般的に使用されるユーザーであるが、不要な情報を公開してしまう可能性があるため、実行可能な権限は必要最小限にしておく必要がある。」など 【エムオーテックス株式会社】	ご意見を踏まえ、図表Ⅲ．３．１－１No１中に「特にゲストユーザーについては、不要な情報公開を避けるため、必要最小限の権限とする。」の記述を追記します。
Ⅲ．３．１．１ （図表）Ⅲ．３．１－１	【意見】「No．１IDとアクセス管理（IAM）」に、「また、認証情報は定期的に変更するなどの設定を行う必要がある。」とありますが、近年ではパスワードの定期的変更はその弊害が指摘され、推奨されなくなっています。削除すべきであると考えます。 【エムオーテックス株式会社】	ご意見を踏まえ、図表Ⅲ．３．１－１No１中の「また、認証情報は定期的に変更するなどの設定を行う必要がある。」の記述は削除します。

Ⅲ．３．１．１ （図表）Ⅲ．３．１−１	（「クラウドサービス利用・提供における適切な設定のためのガイドライン」（案）、「また、認証情報は定期的に変更するなどの設定を行う必要がある。また、暗号化キーは統合管理サービスで集中管理することを推奨する。」との記載部分） ・意見内容 当該部分について「また、認証情報は定期的に変更するなどの設定を行う必要がある。また、暗号化キーは統合管理サービスで集中管理することを推奨する。なお、把握していない、もしくは把握できていないIDとアカウントを把握する仕組み（申請ベースで中央での払い出し、CASBによる新規アカウントの個別発行不可等）を設ける必要がある。」との変更を提案します。 （理由） ID・アカウントを把握している場合のクラウドサービスの利用点では、現状の記載内容で十分と考えられますが、把握していないまたは把握できていないID・アカウントが生じるクラウドサービスを利用するケースは確実に存在し、案には後者の対策の例示がありません。そのため、その場合にID・アカウント等を把握する仕組み（申請ベースで中央での払い出し、CASBによる新規アカウントの個別発行不可等）を設ける必要性を明記する必要があります。 P41に「v.組織の許可なく利用されているクラウドサービスの発見と抑止。」という記載があり、把握していない・把握できていないID・アカウントによるクラウドサービスの利用を把握および抑止する必要とその具体策を明示する必要があります。 【ヴイエムウェア株式会社】	ご意見を踏まえ、図表Ⅲ．３．１−１No１中に以下の記述を追記します。「なお、管理者がIDとアカウントを網羅的に把握する仕組み（申請ベースで中央での払い出し、CASBによる新規アカウントの個別発行不可等）を設ける必要がある。」
Ⅲ．３．１．１ （図表）Ⅲ．３．１−１	クラウドにおけるセキュリティ設定項目の類型と対策 No.１「IDとアクセス管理」において、１．１としてディフォルトで全てのログインに関して多要素認証の導入を追加されると良いかと存じます。 【グーグル･クラウド･ジャパン合同会社】	ご指摘の通り、MFAを必須とするクラウドサービス事業者は増えてきましたが、対応できない事業者もまだ多い状況のため原案のままとさせていただきます。
Ⅲ．３．１．１ （図表）Ⅲ．３．１−１	該当箇所：【基本】設定項目の把握と設定 No.２ ＜意見＞ ・ロギングについては「適切に」とされていますが、原則としてすべて取得することを奨励すべきと考えます。 ＜理由＞ ・問題発生時等対応が必要な場合において、有効化していなかった期間のログは取得不可能で調査ができない場合もあり、適正な運用にあたっては原則取得することが望ましいと考えるため。 【Ubie株式会社UbieDiscovery】	ログの種類や量、保存するリソースについてはクラウドサービス利用者の状況によって様々に異なるため、一律に全て取得とすると状況に合わないケースが想定されます。したがって本箇所については原案のままとさせていただきます。

Ⅲ．３．１．１ （図表）Ⅲ．３．１－１	（「クラウドサービス利用・提供における適切な設定のためのガイドライン」（案）、「物理サーバを論理的に分離する仮想マシンを利用する際、仮想マシンのディスク暗号化、エンドポイント保護などの設定を確実に行う必要がある。また、ホストOS、ゲストOS等の最新パッチについても留意する必要がある。」との記載部分） ・意見内容 当該部分について「物理サーバを論理的に分離する仮想マシンを利用する際、仮想マシンのディスク暗号化、エンドポイント保護などの設定、を確実に行う必要がある。また、ホストOS、ゲストOS等の最新パッチ、ウイルス対策（AV、EDR等）の設定及びその監視・運用（MDR、SOC等）についても留意する必要がある。」との変更を提案します。 （理由） 案に示されている「ホストOS、ゲストOS等の最新パッチ推奨設定」と同等に重要な項目として“ウイルス対策（AV、EDR等）及びその監視・運用（MDR、SOC等）”があります。そのため、並列の扱いで記載する必要があります。 ウイルス対策及びそのセキュリティ監視・運用はクラウドプロバイダ側では原則提供されません。そのため、利用者側が最低限意識して必要があります。また、マネージドサービス等インフラ側をクラウドプロバイダが提供する場合、ウイルス対策を利用者側で行うことが実質不可となります。そのため、クラウドプロバイダ側に代替の要求を提示する必要があります。 【ヴイエムウェア株式会社】	ご意見を踏まえ、図表Ⅲ．３．１－１No４．１中の「また、ホストOS、ゲストOS等の最新パッチについても留意する必要がある。」の記述を「また、ホスト OS、ゲストOS 等の最新パッチ、ウイルス対策（AV、EDR等）の設定及びその監視・運用（MDR、SOC等）についても留意する必要がある。」に修正します。
Ⅲ．３．１．１ （図表）Ⅲ．３．１－１	（「クラウドサービス利用・提供における適切な設定のためのガイドライン」（案）、「クラウド利用は、インターネット経由となるため、外部ネットワークとのアクセスに関する基本的なセキュリティ設定、仮想プライベートクラウドのセキュリティ設定、境界防護等に関する設定を確実に行う必要がある。」との記載部分） ・意見内容 当該部分について「クラウド利用は、インターネット経由となるため、外部ネットワークとのアクセスに関する基本的なセキュリティ設定、仮想プライベートクラウドのセキュリティ設定、Firewall/IPS/IDSやWAFなどによる境界防護および境界内防護等に関する設定を確実に行う必要がある。」との変更を提案します。 （理由） インターネット経由にかかる防護は、境界防護だけでなく境界内防護を行うことの必要性が広く認識されており、そのことを明示する必要があります。また概念だけでなく、それに用いられる具体的なものとしてFirewall/IPS/IDS/WAFなどを読み手に対して例示する必要があります。それにより、問題発生時の影響を抑止・防止することができます。 【ヴイエムウェア株式会社】	ご指摘を踏まえ、図表Ⅲ．３．１－１No４．２中の「境界防護等に関する設定を確実に行う必要がある。」の記述を「Firewall/IPS/IDSやWAFなどによる境界防護および境界内防護等に関する設定を確実に行う必要がある。」に修正します。

Ⅲ．３．１．１ （図表）Ⅲ．３．１－１	（「クラウドサービス利用・提供における適切な設定のためのガイドライン」（案）、「クラウド利用は、インターネット経由となるため、外部ネットワークとのアクセスに関する基本的なセキュリティ設定、仮想プライベートクラウドのセキュリティ設定、境界防護等に関する設定を確実に行う必要がある。」との記載部分） ・意見内容 当該部分について「クラウド利用は、インターネット経由となるため、外部ネットワークとのアクセスに関する基本的なセキュリティ設定、仮想プライベートクラウドのセキュリティ設定、境界防護等に関する設定を確実に行う必要がある。加えて、個人情報など機密性の高い情報を扱うシステムでは、インターネット経由の利用ではセキュリティ上のリスクが懸念されため、ネットワークセキュリティの検討が必要となり、具体的にはVPNによる通信の暗号化、専用線接続サービスを利用した閉域接続などが挙げられる。」との変更を提案します。 （理由） クラウド利用において、個人情報など機密性の高い情報を扱う上でネットワークセキュリティは重要な検討項目、設定項目の一つです。VPNゲートウェイや専用線接続サービスなど、クラウドまでの接続手法をクラウドプロバイダ側が提供する場合もあるため、ネットワーク設定に関するガイドラインの設定項目として明記することが必要です。 また、ネットワークに関する検討において、ファイアウォールなどの通信制御の検討だけではなく、データの機密性等に応じた暗号化等のネットワークセキュリティの検討、設定は必須要件であり、本セキュリティ要件の実現のために、クラウドプロバイダ側のネットワーク実装手法（提供サービス）およびクラウドに接続するまでのネットワーク実装手法は重要な検討項目、設定項目であるため、その明示が必要です。 【ヴイエムウェア株式会社】	ご指摘を踏まえ、図表Ⅲ．３．１－１No４．２中に以下の記述を追記します。「加えて、重要情報を扱うシステムでは、信頼できるVPNによる通信の暗号化などのネットワークセキュリティ対策を検討する。」
Ⅲ．３．１．２ Ⅲ．４．１．１ Ⅲ．４．３．１	【意見】各項目の【ベストプラクティス】において、外部診断サービスを利用することが記載されていますが、診断品質の確保や事業者選定のあり方に関する観点を追記してはいかがでしょうか。例えば、IPAが公表している「情報セキュリティサービス基準適合サービスリスト」の活用など。 【エムオーテックス株式会社】	ご意見は参考として承ります。
Ⅲ．３．１．２	【ベストプラクティス】ⅰ こちらにおけます“設定項目の可視化ツール”とは具体的にどの様なものを想定されておりますでしょうか？ 【グーグル･クラウド･ジャパン合同会社】	CASB(CloudAccessSecurityBroker)等を指します。
Ⅲ．３．２ クラウドシステムにおける動作環境のプロビジョニング		
Ⅲ．３．２．１	「【基本】変化への適応及び体制整備」のベストプラクティスのⅳは、利用者側で対応すべきセキュリティ事項がないかの確認や、想定通りの挙動をするかの検証は必要かと思います。 【個人A】	ご意見については参考として承ります。

Ⅲ．３．２.１	【ベストプラクティス】 ここだけ「体言止め」が一部用いられており、前後の【ベストプラクティス】と文体が統一されていない。 ここは「・・・する。」と用言止めを用いるべき文脈と思料する。 【個人B】	ご意見を踏まえ、Ⅲ．３．２．１ベストプラクティスについて、文体を統一するよう修正します。
Ⅲ．３．２．１	【ベストプラクティス】iii 「体制の整備」とありますが、利用者にとってどの様な体制を整備するのが良いのか具体的にご言及頂けると分かりやすいかと思います。 【グーグル･クラウド･ジャパン合同会社】	ご意見を踏まえ、Ⅲ．３．２．１ベストプラクティスiiiに「（Ⅲ．１．２．１．【基本】 技術情報の収集　のベストプラクティスを参照）」を追記します。
Ⅲ．３．３ その他のリスクへの対応		
Ⅲ．３．３．１	【基本】システム動作環境の設定に関連するその他のリスク対応 ・意見内容 データ破棄方法の確認について追加 ・理由 データの責任についてはクラウドサービス利用者であるが、オンプレミスのように利用者が物理媒体の破壊等を実施することができない。 データの破棄等についてはクラウドサービス事業者の取り扱いとなるため、利用するクラウドサービス事業者においてのサービス利用をやめた後のデータ破棄方法や利用者がサービスデータを消去する際の取り扱い等を確認する必要がある旨を追記した方が良いと考える。 【アイレット株式会社】	本ガイドラインはクラウドサービスの適切な設定の推進が趣旨となりますので、原案のままとさせていただきます。
Ⅲ．３．３.１	・該当箇所 【基本】システム動作環境の設定に関連するその他のリスク対応 ・意見内容 ノンマネージドサービスのOSSを利用する場合の対応策の記載 ・理由 サービス利用の目的によっては、IaaS/PaaSベンダー以外から提供されているOSSの利用を行う必要がある。 その場合においては、OSSのユーザコミュニティが公開しているドキュメントを利用するなど、OSSコミュニティの活用を盛り入れてはどうか。 【アイレット株式会社】	ご意見については参考として承ります。
Ⅲ．３．３．１	・その他のリスクへの対応 ・ベストプラクティスの中に、準拠法やデータ所在地の確認等の記載がありますが、情報の取り扱いに伴う関連法規制の遵守は利用者側にある旨を明確にするべきではないでしょうか。Ⅳ.クラウドサービス提供側に求められる対策の中にだけ、公的機関からの情報収集などが基本要件として入ってることも違和感があります。 【株式会社セールスフォース・ジャパン】	関連法規制の遵守は利用者、提供者双方に求められるものです。情報収集については利用側にもⅢ．１．２情報収集という項目があります。

Ⅲ．３．３．１	・該当箇所 その他のリスクへの対応iii. ・意見内容 従量課金の場合のコストモニタリング ・理由 不正利用や設定ミスによる過剰プロビジョニングを検知するため、コストをモニタリングするのが望ましい。 【アイレット株式会社】	コストモニタリングについては、ベストプラクティスのivにおける課金管理に含まれると考えられるため、原案のままとさせていただきます。
Ⅲ．３．３．１	該当箇所：【基本】システム動作環境の設定に関連するその他のリスク対応 ベストプラクティスv ＜意見＞ ・ここでいう「運用管理機構」が何を指すのか明確でなく、事業者に混乱を来すため、削除すべきと考えます。 ・OSSはそもそもノンマネージドが非常に多く、これらを用いないことは多くの事業者にとって困難であると考えられることから、ベンダーからの支援も考慮しつつ自社で運用可能な体制を構築することを推奨すべきと考えます。 ＜理由＞ ・クラウドベンダー等が提供しているものだけでは成立しないサービスがほとんどであると認識しており、選定時よりも運用時のコントロールが肝要であると考えるため。 【Ubie株式会社UbieDiscovery】	内容を明確にするため、Ⅲ．３．３．１ベストプラクティス中の「OSS（Open Source Software）の利用に関しては、IaaS/PaaSベンダーから提供される、運用管理機構が存在するサービスから選択して利用する。（ノンマネージドサービスはなるべく避ける）」の記述を「OSS（Open Source Software）の利用に関しては、IaaS/PaaSベンダーが一部運用を代行するサービスから可能な限り選択して利用する。」に修正します。
Ⅲ．３．３．１	v.「運用管理機構」の記述について IaaS/PaaSベンダーから提供される「運用管理機構」とは、具体的に何を指しますでしょうか？ 【グーグル･クラウド･ジャパン合同会社】	内容を明確にするため、Ⅲ．３．３．１ベストプラクティス中の「OSS（Open Source Software）の利用に関しては、IaaS/PaaSベンダーから提供される、運用管理機構が存在するサービスから選択して利用する。（ノンマネージドサービスはなるべく避ける）」の記述を「OSS（Open Source Software）の利用に関しては、IaaS/PaaSベンダーが一部運用を代行するサービスから可能な限り選択して利用する。」に修正します。

Ⅲ．３．３．１	（「クラウドサービス利用・提供における適切な設定のためのガイドライン」（案）、「vii. データセンタが海外に置かれる場合は、外国の法律などの適用を受ける可能性がある。特に機密性の高いデータを扱う場合は、データセンタ所在地を確認する。」との記載部分） ・意見内容 当該部分について「vii. データセンタが海外に置かれる場合は、外国の法律などの適用を受ける可能性がある。特に機密性の高いデータを扱う場合は、データセンタ所在地を確認する。 viii. 扱うデータの機密性・完全性・可用性に応じて、海外企業が提供するクラウドサービスの運営を外国政府により停止されないようなデータセンタ所在地及び運用体制を構築すべきかを検討すること。」との変更を提案します。 （理由） データセンタの所在地が国内であっても運用体制が海外にあれば、外国の法律の適用を受けます。経済安全保障の観点及び、扱うデータの機密性・完全性・可用性の観点から、データの性質に応じてクラウドの運用に係るリスクに関して特に留意することを明示する必要があります。 【ヴイエムウェア株式会社】	ご意見を踏まえ、Ⅲ．３．３．１ベストプラクティスvii中の「特に機密性が高いデータを扱う場合は、データセンタ所在地を確認する。」の記述を「特に機密性の高いデータを扱う場合は、データセンタ所在国、所在地域及び運用体制などを確認する。」と修正します。
Ⅲ．３．３．１	vii「外国法」の適用について データセンタの所在地に加え、「クラウドサービス事業者が外国法に基づくデータ開示要請についてどういうスタンスをとっているか確認すること」という記載を追加しては如何でしょうか。 【グーグル･クラウド･ジャパン合同会社】	ご意見を踏まえ、Ⅲ．３．３．１脚注に「このような場合は、クラウドサービス事業者が外国法に基づくデータ開示要請についてどういうスタンスをとっているかを考慮する必要がある。」と追記いたします。
Ⅲ．４　クラウドシステム動作環境に関する設定の方法論		
Ⅲ．４	クラウドシステム動作環境に関する設定の方法論 クラウドは、インターネット上に展開されるストレージやコンピューティングリソースなどの様々な機能を、最新の技術とサイバーセキュリティ対策がされたうえで、拡張性と柔軟性をもって使える「プラットフォーム」で、データ連携も可能なことから、オンプレミス時代の個別作り込みによる「システム」とは異なるものです。よって、クラウド「システム」という言葉より、「クラウド“プラットフォーム”環境に関する設定の方法論」というタイトルの方が宜しいかと存じます。 【グーグル･クラウド･ジャパン合同会社】	プラットフォームという言葉は便利ですが、人によって想定する範囲が異なるなどの曖昧性があるので、原案のままとさせていただきます。
Ⅲ．４	・該当箇所 クラウドシステム動作環境に関する設定の方法論 ・意見内容 IaCについて言及するべきである。 ・理由 クラウドの構築を考えた場合、作業者がGUIを通じて作業する他、コードによるインフラストラクチャの構築(IaC)が選択肢となる。 IaCにより、不変性(Immutability)の確保と、コメントの付与などによるレビューの容易性が担保されるため、方法論として記載するべきである。 【アイレット株式会社】	IaCやツールの活用などについては、Ⅲ．２．１．２ベストプラクティスivで述べているため、本箇所については原案のままとさせていただきます。

Ⅲ．４．１ ノウハウの蓄積		
Ⅲ．４．１	・ノウハウの蓄積 ・クラウドサービス利用者にマネージドサービスの利用を推進しているが、IaaS・PaaSならともかく、SaaSでは推進するものではないと思う。（そのためのSaaS)ガバナンスを利用者側が持ち説明責任を果たせる状況を確保すべきである。 【株式会社セールスフォース・ジャパン】	ご意見は参考として承ります。
Ⅲ．４．２ 支援ツール等の活用		
Ⅲ．４．２	【該当箇所】 ツールの導入時に運用で検討すべき観点についても述べ、効果的な活用につながる示唆を与えてはどうか 【指摘内容】 支援ツールの活用 【理由】ツール導入にあたっては、検査を実施する頻度、検査結果の通知方法、検査結果のトリアージ基準などを検討する 【ニューリジェンセキュリティ株式会社】	ご意見は参考として承ります。
Ⅲ．４．２．１	該当箇所：【推奨】支援ツールや外部診断サービスの利用 ＜意見＞ ・記載に賛同いたします。 ・具体例として、クラウドベンダーが提供しているツールの活用についても脚注等で触れるとよりわかりやすいかと考えます。 例）AWSSecurityHub、GoogleSecurityCommandCenter ＜理由＞ ・まず利用するものとして具体例があった方がわかりやすく、推奨しやすいと考えるため。 【Ubie株式会社UbieDiscovery】	ご意見は参考として承ります。
Ⅲ．４．２．１ （ANNEX）Ⅲ．４．２．１	【項目】ANNEX対策一覧 【意見】Ⅲ．４．２．１に「外部診断ツール等」とありますが、正しくは「外部診断サービス等」であると思われます。 【エムオーテックス株式会社】	ご意見を踏まえ、Ⅲ．４．２．１本文中及びANNEX中のⅢ．４．２．１の「外部診断ツール等を活用すること。」の記述を、「外部診断サービス等を活用すること。」に修正します。

Ⅳ クラウドサービス提供側に求められる対策		
Ⅳ．１ 組織体制・人材育成		
Ⅳ．１．１	・該当箇所 クラウドサービス設定不備の抑止・防止に係る方針的事項 ・意見内容 関連するクラウドサービスの準拠する基準を確認する。 ・理由 お客様に対して、準拠する基準を明確にする場合、関連するクラウドサービスが基準を満たしていることを合わせて確認する。 たとえば、PCIDSSに準拠する場合は、クラウドサービスも合わせて準拠を確認する必要がある。 【アイレット株式会社】	本ガイドラインはクラウドサービスの適切な設定の推進が趣旨となりますので、原案のままとさせていただきます。
Ⅳ．１．１	・クラウドサービス設定不備の抑止・防止に係る方針的事項 ・設定不備の抑止・防止に関する組織全体での基本的な方針、役割、責任等を定めた文書の策定を求めていますが、ベストプラクティスに記載の事項がなんらかの形態で文書化され共有されており、または実行されているのであれば、設定不備に特化した新たな文書作成の要求は避けるのはいかがでしょうか。 【株式会社セールスフォース・ジャパン】	新たに文書を作成することを推奨するものではなく、あくまでベストプラクティスに列挙した「内容を含む」ことを推奨する者です。したがって内容が何らかの形態で文書化され共有されているなら新しく文書の作成を求めるものではありません。本箇所については原案のままとさせていただきます。
Ⅳ．１．１．１	（「クラウドサービス利用・提供における適切な設定のためのガイドライン」（案）、「ii.提供者側組織のセキュリティポリシー及びクラウドのセキュリティ規格に準拠した規定やルールの作成。規定等の作成時には、「自社セキュリティポリシー」への準拠と、「クラウドのセキュリティ規格」（ISO、NIST等）への準拠に留意する。」との記載部分） ・意見内容 当該部分について「ii.提供者側組織のセキュリティポリシー及びクラウドのセキュリティ規格に準拠した規定やルールの作成。規定等の作成時には、「自社セキュリティポリシー」への準拠と、「クラウドのセキュリティ規格」（ISO、NIST等）への準拠に留意する。なお、「クラウドのセキュリティ規格」の準拠に対する具体的な設定に関しては属人化による設定不備および、設定内容の解釈の違いを抑止するため第三者が提供する規格と設定の紐付けを利用すること。」との変更を提案します。 （理由） 「クラウドのセキュリティ規格」の準拠に対する具体的な設定に関して記載する事を提案します。 案に記載されているようにISOやNISTの項目に準拠するために、実装に落とすということは非常に膨大な作業で、設定の揺らぎが発生します。その理由はセキュリティ規格がクラウドサービスの設定と同意ではないからです。このセキュリティ規格の意味をクラウドサービスの設定に紐付ける必要があり、ここが属人的であれば利用者の間で解釈の違いが生じ、設定の揺らぎが必ず発生します。それを避けるため、この懸念の明記と、懸念の解決策として第三者が提供する紐付けを利用することの明記が必要です。 【ヴイエムウェア株式会社】	ご意見は参考として承ります。

Ⅳ．２ 情報提供		
Ⅳ．２．１ 正しい情報の提供		
Ⅳ．２．１	・該当箇所 正しい情報の提供 ・意見内容 マニュアルのアップデート ・理由 既存機能の変更や廃止があった際に、古いマニュアルを参照して設定を誤らないように、マニュアルをアップデートするとともに、更新履歴も記載があるとよい。 【アイレット株式会社】	Ⅳ．２．５の「タイムリーな情報提供」の、「変更等に伴うタイムリーな情報提供」に含まれるものとさせていただきます。
Ⅳ．２．１	正しい情報の提供 もう少し具体的に内容をご記述されると読者は理解し易いと存じます。 【グーグル･クラウド･ジャパン合同会社】	ご意見は参考として承ります。
Ⅳ．２．２ 十分な情報の提供		
Ⅳ．２．２	十分な情報の提供 “一部の情報を提供しなかったため、正しい設定ができなかった場合は、クラウドサービス事業者側の責任が問われる可能性がある”、とありますが、そうした責任が生じるのは、クラウドサービス事業者が顧客の設定方法に起因する事故が生じうることを知りつつ、当該事業者が保有する情報をあえて提供しなかったような契約の規定･趣旨に反する例外的な場面であると考えます。一般に顧客における利用方法や設定方法を関知しているわけではないクラウドサービス事業者に、そうした顧客事情に関連する情報提供義務までも存在するかのような記載は、責任分界に関する誤解も生じさせかねないため、削除すべきと考えます。 【グーグル･クラウド･ジャパン合同会社】	クラウドサービス提供側の記載漏れ等による設定不備の発生は例外的な場面だけであるとは限らないと認識しております。このため、原案のままとさせていただきます。
Ⅳ．２．２．１	十分な情報の提供【ベストプラクティス】 新たにiiiとして、第三者監査や資格の取得に関して、クラウドサービス事業者側のホームページなどにその一覧を掲載するのが望ましい旨追加すると良いかと思います。また、ISMAP（政府情報システムのためのセキュリティ評価制度）についてもベストプラクティスの「例」として挙げられると宜しいかと存じます。 【グーグル･クラウド･ジャパン合同会社】	ご意見を踏まえ、Ⅳ．２．２．１ベストプラクティスに「iii．第三者認証や認定の取得に関して、取得状況について自社のWebサイトで発信していくことも情報提供として有効である。」の記述を追記します。

Ⅳ．２．３ わかりやすい情報の提供		
Ⅳ．２．３．１	・【基本】わかりやすい情報の提供 ・「わかりやすい」は受け手の能力に依存する不明確な基準と考えます。 そのため、「初心者でもわかりやすい」としながらベストプラクティスには「各設定値の意味や背景となるセキュリティポリシーを解説するとともに、その設定値を選択した場合の影響等についても説明する必要がある。例えば暗号化設定の選択肢では、ぜい弱なものはその旨を明示する必要がある。ii. 具体的な環境の設定に関する例を示すことも有効である。」 など詳細を記載することを求めながら一方で 「iv. 分厚いマニュアルは読む気がしなかったり、読んでも理解できなかったりすることが多い。適切な分量のマニュアルを作成するとともに、要約版や検索ツールも同時に提供することが望ましい。v. 利用者が行う環境の設定を動画で提供する企業が増えている。文字の情報だけでなく、画像や映像による情報提供はクラウドサービス利用者の理解を助ける。」 と後半はパラドックスな内容ではないでしょうか。 クラウドサービス事業者側が「クラウドサービス管理者」に求める最低技術レベルを明確にしたり、教育の機会を持つようにすることが必要なのではないでしょうか？また、その場合、利用者側にも、「クラウドサービス管理者」に対する教育機会や教育費用をあらかじめ予算として組み込むことをベストプラクティスに入れるべきではないでしょうか。 【株式会社セールスフォース・ジャパン】	ｉで求められる内容の記述と、マニュアルが適切な分量であることは両立しうると考えられます。また、教育についてはⅢ．１．３及びⅣ．３．２で述べられているため、原案のままとさせていただきます。
Ⅳ．２．４ 利用者別の対応		
Ⅳ．２．４．１	・【推奨】利用者の特性に応じた情報提供クラウドサービス利用者ごとの特性に応じた情報を提供すること。 ・サービス提供側が全ての利用者の特性を理解することは不可能かと思われます。（直接販売していないケースもありますし、どのような用途でサービスを利用するかは利用者側が決めることであり、クラウドサービス事業者は利用方法を強要できません）これは、利用者の「クラウドサービス管理者」もしくはサービスの提供及び運用を行うSIerの範囲ではないでしょうか？ 【株式会社セールスフォース・ジャパン】	ご指摘のケースもあるため対策項目の分類を【推奨】としております。

Ⅳ．２．５ タイムリーな情報提供		
Ⅳ．２．５	・タイムリーな情報提供 ・SaaSやPaaSでは、安全上の理由から、利用アプリケーションを公開していない場合も多いです。本項目では「システム動作環境の設定変更が生じた場合など」と記載されていますが、「など」が入ると、全ての情報を公開するよう迫る利用者が出ることが容易に想像されます。「など」を削除するか、情報提供が必須となる場合を明記していただくのはいかがでしょうか？ 【株式会社セールスフォース・ジャパン】	本ガイドラインは法的に情報開示を強制するものではありません。それを踏まえた上で、設定変更時以外で情報提供が必要なケースもカバーするため、原案のままとさせていただきます。
Ⅳ．２．５．１	（該当箇所） 情報提供 （意見） クラウドサービス提供者にオンラインマニュアルおよびチャットボックスを整備するよう要請することが望ましいと考えます。 （理由） 利用者とのコミュニケーションの確立が重要なのではなく（何かしら確立しているはずなので）、随時発生する仕様変更による対象や影響を明示することが必要と考えます。現時点で、積極的に明示されているサービスは、少数ではないかと推察しております。 【株式会社ラック】	ご意見を踏まえて、Ⅳ．２．５．１ベストプラクティスに「i.随時発生する仕様変更、ぜい弱性対応などに対応するため、オンラインマニュアルやチャット機能の整備を検討する。」の記述を追記します。
Ⅳ．２．５．２	・該当箇所 公開された脆弱性の影響に伴うタイムリーな情報提供 ・意見内容 情報の更新に注意する。 ・理由 公開された脆弱性は、解析の進み具合や派生的な情報により情報が更新されることに注意が必要がある。 脆弱性情報は更新情報を正しく伝えるように考慮する必要である。 【アイレット株式会社】	ご意見を踏まえて、Ⅳ．２．５．２ベストプラクティスに「ii 脆弱性は情報が更新されることもあるので、更新情報も正しく伝えられるように考慮する」の記述を追記します。

Ⅳ．４　利用者支援ツールの提供		
Ⅳ．４．２．１	「Ⅳ．４．２．１【推奨】設定項目診断ツールの提供」のベストプラクティスのⅱについて、自動で復元する機能＝ガードレール機能は正しい表現でしょうか、、 ガードレール機能はそもそもまずい設定ができないように統制をかけるものかと思っております。 【個人A】	ご意見を踏まえ、Ⅳ．４．２．１ベストプラクティス「（ガードレール機能）」の記述を削除します。
Ⅳ．５　システムの改善ーミスが発生しにくいシステムの提供		
Ⅳ．５．１	設定方法の見直し【目的】 クラウドサービスは日々技術革新が起きており、利用者がより安全に使い易いような環境が向上しておりますが、その利用に際し、クラウドサービス事業者の認定資格を有するエンジニア（ITリソースの内製化）を一定数抱えるなど、利用者側でも「クラウド･リテラシー」の向上に資する対策を取ることが望ましいと考えます。 【グーグル･クラウド･ジャパン合同会社】	利用社側のリテラシー向上についてはⅢ．１．３において述べられています。
Ⅳ．５．２	【該当箇所】 デフォルト値の変更について、デフォルト値を変更後セキュリティが低下する設定については禁止すべきである 【指摘内容】 デフォルト値の見直し 【理由】利用者はクラウドサービス提供者側のデフォルト値の変更に気が付きにくく、従来の使い方でセキュリティが低下する場合に重大な事故が発生する懸念があります 【ニューリジェンセキュリティ株式会社】	一時的に低いセキュリティ設定とすることが業務上必要である可能性もあるので、本箇所については原案のままとさせていただきます。
Ⅳ．５．４．１ Ⅳ．５．４．２	・Ⅳ．５．４．１【基本】設定項目数及び選択肢の削減、Ⅳ．５．４．２【基本】設定変更回数の削減 ・顧客の利便性向上および負荷軽減を目的に、できる限り多くの顧客が追加開発等なく標準機能のまま機能・サービス利用できる形で製品・サービスを提供している中で、機能としての設定項目数や設定変更回数に関して制限をつけることは上記と逆行する効果をうむことになります。 【株式会社セールスフォース・ジャパン】	サービス提供側の機能提供時の方針事項を示す箇所なので、原案のままとさせていただきます。

Ⅳ．５．５ （図表）Ⅳ．５．５－１	【該当箇所】 「暗号化」だけではなく、「データ漏洩事象が発生した場合でも、暗号化によって情報そのものの漏洩が回避できた事例」、などの説明を追記する 【指摘内容】 事後対策としての暗号化 【理由】データの暗号化やIRMの導入は漏洩対策として効果のある対策であり、特に機微データについては導入を推奨するものですが、この図だとその効果が伝わりにくいと考えます 【ニューリジェンセキュリティ株式会社】	ご意見は参考として承ります。
Ⅳ．５．５．１ （ANNEX）Ⅳ．５．５．１	Ⅳ．５．５．１【推奨】暗号化機能の提供と設定 重要な情報のみならず、いずれの形態のクラウドサービスにおいても、データを取り扱う全てのプロセスにおいて、暗号化機能を付与することが望ましいと考えます。 【グーグル･クラウド･ジャパン合同会社】	全ての情報の暗号化を行うと処理が煩雑になりすぎるという懸念があるため、重要な情報への暗号化とさせていただきます。記載をわかりやすくするため、Ⅳ．５．５．１本文中及びANNEX中Ⅳ．５．５．１の「重要な情報の管理においては暗号化の機能を提供し、利用者がセキュリティ上の脅威を考慮したうえで設定可能となるようにすること。」の記述を「暗号化の機能を提供し、利用者がセキュリティ上の脅威を考慮したうえで重要な情報において設定可能となるようにすること。」と修正しました。
Ⅳ．６ 継続的な改善－PDCAを回す		
Ⅳ．６．１	・Ⅳ．６．１情報収集 ・ここでもクラウドサービス事業者とのコミュニケーションを入れるべきではないでしょうか？（重要システム導入の場合には、有償サポートで専任担当者を用意し、定期的なコミュニケーションを取るなど） 【株式会社セールスフォース・ジャパン】	本節は提供側の対策について述べる節となるため、原案のままといさせていただきます。

Ⅳ．７　マネージドサービスの提供		
Ⅳ．７	【該当箇所】 サードパーティのマネージドサービスの利用も記載する 【指摘内容】 Ⅳ．７マネージドサービスの提供 【理由】マネージドサービスはクラウドサービス提供者だけでなく、サードパーティによっても提供されている。 これらのサービスの利用により、環境設定にとどまらず、日々のログの運用監視やインシデントの発見・通知などの定常的な運用支援が得られるため、リソースに限りのある状況では積極的に活用すべきと考えます。 【ニューリジェンセキュリティ株式会社】	「外部のマネージドサービス事業者を紹介すること」という記載があるため、原案のままとさせていただきます。
Ⅳ．７．１	（「クラウドサービス利用・提供における適切な設定のためのガイドライン」（案）、「このサービスを利用すれば、クラウドサービス利用者は利用者で実施すべき環境設定作業から解放され、一部の設定に関する負担をクラウドサービス事業者側に移転させることが可能となる。図表Ⅳ．７．１－１にマネージドサービス提供による利用者の負担軽減イメージを示す。」との記載部分） ・意見内容 当該部分について「このサービスを利用すれば、クラウドサービス利用者は利用者で実施すべき環境設定作業から解放され、一部の設定に関する負担をクラウドサービス事業者側に移転させることが可能となる。なお、マネージドサービスを利用することによりアプリケーションやデータの扱いに関する変更が伴った場合は、今までのベストプラクティスなどがそのまま適用されないため、必ずしも負担が軽減されるわけではない点に留意すること。図表Ⅳ．７．１－１にマネージドサービス提供による利用者の負担軽減イメージを示す。」との変更を提案します。 （理由） マネージドサービスにより、利用者の負担軽減が確実に軽減されるような記載となっていますが、必ずしも軽減されるものではありません。アプリケーションやデータの扱いに関する変更が伴った場合は、今までのベストプラクティスなどがそのまま適用されず、負担軽減がなされない可能性が高くなります。また、そのような例外は多くの場合で発生します。そのため、軽減されない場合があること（アプリケーションやデータの扱いに関して変更が伴った場合）を明示する必要があります。 【ヴイエムウェア株式会社】	「環境設定作業」、「一部の設定に関する負担」と限定しており、負担全体を軽減するという意味ではないため、原案のままとさせていただきます。

その他		
目次	【該当箇所】 章番号の空白やフォントにばらつきが散見される。 （例）「Ⅱ.1.2」と「Ⅱ.2.2」の数字間の幅が異なる。 「Ⅲ.1.2.1.」や「Ⅲ.1.4.1.」など最後のピリオドが不要。 「Ⅳ.2.2.1」の2つ目の「2」のフォントが斜体になっている。 「Ⅳ5.1.2」などローマ数字の後ろのピリオドがない。 【指摘内容】 i-iv目次 【理由】体裁が美しくないと、読んでもらえない、内容が入ってこないことがある。 【ニューリジェンセキュリティ株式会社】	ご意見を踏まえて、目次について空白、フォントを統一いたします。
全般	クラウドサービス利用へのアドバイス事項として、経済産業省が定める役務通達改正による安全性の担保する項目を提供者と利用者が守るように明示していただきたい。具体的には、CISTECが経済産業省担当官と協議の上設定した「安全保障輸出管理に係る機微な技術情報を、外国のサーバーに保管する場合等における自主管理ガイドライン」を利用者だけでなく、提供者からも利用者に明示しておくように指導するためのガイドラインを追加していただきたい。理由としては、現在のクラウドサービスの契約において利用者が自主的に提供者のガイドライン遵守を調べたりヒアリング確認しなければ分からず、またヒアリングしても明示してくれない提供者もいる中で、経済安全保障推進法案を日本企業が本当に遵守できるのか疑問となる状況と考えています。 【個人C】	ご意見は参考として承ります。
全般	該当箇所：全般 ＜意見＞ ・全体として非常にわかりやすく、ベストプラクティスがまとまった文書が作成されることは大変ありがたいと考えております。 ・これらの対策を参照することの追加的なステップにはなるかと思いますが、すでに記載いただいているInfrastructureasCodeに加え、policyascodeの推進など属人化を排除し自動的に検知・対応可能な仕組みの構築も考慮されていくことが望ましいと考えます。 ＜理由＞ ・色々と対策を施しても、属人化しているとどうしても抜け漏れや破損の恐れが生じる可能性があることから、なるべく自動化することが望ましいと考えるため。 【Ubie株式会社UbieDiscovery】	ご意見は参考として承ります。

全般	当社としても、クラウドサービスにおけるセキュリティ対策は非常に重要であると考えており、利用者・提供者双方の視点から設定不備を抑止・防止するための対策について具体例を交え網羅的に整理された本ガイドラインの位置づけに賛同いたします。 クラウドネットワークに関してはセキュリティの高度化に向けた不断の取り組みが必用であるところ、当社においても、研究開発その他これに資する事業を今後も積極的に進めてまいる所存です。 【楽天モバイル株式会社】	ご意見は参考として承ります。
全般	【全般】 本ガイドラインはクラウドの事業者と利用者における「責任分界」点と、利用者側の「設定」に焦点を当てたものと理解しておりますが、クラウドコンピューティングを構成するレイヤーは技術の進展やオープンソースの活用、各事業者のビジネスモデルにより、様々な形が存在します。例えば、SaaSやPaaSが必ずしもIaaSとミドルウェアで構成されているとは限りません。複数のクラウドサービス事業者（CSP)のプロダクトは、市販のものやオープンソースのモジュールをそのまま使用しているわけではな く、ミドルウェアの管理責任がCSP側に有るというのは多少古い考え方であると存じます。よって、IaaSの上で動くデータベースエンジンや、アプリケーション層の脆弱性管理やセキュリティ運用の責任がCSP側にある旨を本ガイドラインでご提唱されるのが良いと思います。 その観点から、全体として「設定」の不備のみに焦点を当てるのではなく、クラウドサービス全体（CSPが提供するSaaS,PaaS,IaaS全体）の「プラットフォーム」において、脆弱性やセキュリティ上の残存リスクを減らす状態にすることが重要であると考えます。設定を正しくする、という考え方はミドルウェアのベストプラクティスに合わせておけば良いという“他人任せ”の考え方に繋がりますので、グローバルスタンダードに合わせたセキュリティ環境や組織体制の整備が利用者側でも必要であると考えます。 【グーグル･クラウド･ジャパン合同会社】	ご意見は参考として承ります。
全般	・全般 ・総じて、利用者側自体の責任ももう少し明確にし、利用者自身でも体制を整えることが前提であることを明確にすべきではないでしょうか。利用者のミスを防ぐためのガイドラインであることは理解できますが、変わりゆく情報や新たに発見される脆弱性、新たな攻撃手法に対し、利用者である事業者側でも、準備対応できる体制を整えていく必要があります。このガイドラインによって、利用者がサービス提供事業者側の提供する情報に依存することで、自主的にリスクを判断したりセキュリティ対策を学習すること、またセキュリティ体制の強化に投資することをやめてしまい、結果、新たな脆弱性や攻撃手法に対してサービス提供事業者が対応を取っている間はその情報を待つことで利用者自身のセキュリティリスクを上げてしまうことにつながる恐れがあると思います。 【株式会社セールスフォース・ジャパン】	ご意見は参考として承ります。

全般	・全般 ・利用者側、SIer,サービス提供事業者全てにおいて、認証強化（PWポリシーおよび多要素認証）を推奨およびベストプラクティスとして入れるべきではないでしょうか？ 【株式会社セールスフォース・ジャパン】	多要素認証については図表Ⅲ．３．１－１にて推奨しております。
全般	・全般 ・責任共有モデルの理解を通して、各ステークホルダーごとに、実施すべき作業を認識してもらうことを目的とした資料であると思いますが、共有責任の考え方がIaaSによっていたり、本来利用者側でも遵守されるべき、法令遵守、説明責任や、データの管理責任に関する記載がありません。 【株式会社セールスフォース・ジャパン】	ご意見は参考として承ります。
全般	・全般 ・システムのBCPの記載が不明確：クラウドサービス提供自体のBCPはクラウドサービス事業者、SIerが介する場合は設定や運用についてのBCPはSIer,データ自体の品質管理および独自の業務要件に合わせたデータ保管は利用者責任であることを記載しないと、ランサムウェアなどデータ破損を含む障害に対応できないのではないでしょうか？ 【株式会社セールスフォース・ジャパン】	ご意見は参考として承ります。
その他	受付締切日時の「25日0時0分」は「24日23時59分」の誤記か？（意見公募要領に「23:59必着」と記載されているから。） 【個人D】	ご意見は参考として承ります。
その他	不正アクセスの原因別比率では、設定不備が全体の第３位だったということですが、 ３位の原因にわざわざ注目したのはなぜでしょうか？ まさか、設定不備を解消する業界と、利権関係でつながっていないとは信じていますが。 【個人E】	総務省では、これまで、安全・安心なクラウドサービスの利活用推進のため、クラウドサービスを提供する際に実施することが望ましい情報セキュリティ対策をまとめたガイドラインの策定等に取り組んでおり、今回はクラウドサービスの設定不備に起因する情報漏えい等の事故が増えていることを受けて、本ガイドラインの策定を行っているものです。