別紙3

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2版）（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：平成 30 年6月7日～平成 30 年7月6日）

提出意見数：6者　※提出意見数は、意見提出者数としています。
法人：3者（日本オラクル株式会社（情報処理学会 情報規格調査会 SC 38 専門委員会）、マカフィー株式会社、パスロジ株式会社）
個人：3者（個人 A～個人 C）

【Ⅰ．序編に対する意見】

提出された意見	総務省の考え方	提出意見を踏まえた案の修正の有無
意見1　経済産業省や NISC が発行しているガイドラインへの参照を追記すべき。 経済産業省が発行する「サイバーセキュリティ経営ガイドライン」や（以下、経営ガイドライン）NISC が発行する「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」第5版 https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf （以下、重要インフラガイドライン）および経済産業省の「情報セキュリティサービス基準」への参照を冒頭に追加する事を提案する。 【個人 A】	御意見を踏まえ、3ページの図表1「主なクラウドサービスに関する情報セキュリティガイドライン」に、「サイバーセキュリティ経営ガイドライン」、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」及び「情報セキュリティサービス基準」を追加いたします。 あわせて、図表 1 の表題を「クラウド事業者が参照する主なセキュリティに関するガイドライン」に修正いたします。	有
意見2 「人的・金銭的な資源を割くことが困難な中小のクラウド事業者に対して、独自の脅威分析の負担を軽減し、優先的に取り組むべき対策の指針を与える」との記載を削除すべき。 p4の『1.大企業と比較して、情報セキュリティ対策に人的・金銭的な資源を割くことが困難な中小のクラウド事業者に対して、独自の脅威分析の負担を軽減し、優先的に取り組むべき対策の指針を与える。』 上記記載の削除を提案する。理由として情報セキュリティを確保に対する費用をコストと捉えている点が問題である。 脅威分析や人材確保ができない事業者がクラウド事業を提供するのは企業情報や個人情報を漏洩させ、社会に対して害を与えるだけであり、そのようなサービスは不要であると考える。 【個人 A】	3ページの「ガイドラインの位置付け」に示しているとおり、本ガイドラインは、中小のクラウド事業者も含め、「クラウド事業者が提供するサービス内容に即した適切な情報セキュリティ対策を実施するための指針として、可能な限り分かりやすくかつ具体的な対策項目を提示すること」を目的とするものであり、原案のとおりといたします。	無

意見3　本ガイドライン（案）における用語の定義と、国際規格 ISO/IEC 17788:2014、ISO/IEC 17789:2014 における用語の定義には齟齬がある。 本案ではⅠ．6．に用語の定義がありますが、クラウドコンピューティングの基礎となる基本的な用語の定義と参照アーキテクチャを提供している国際規格 ISOIEC 17788:2014、ISO/IEC 17789:2014 における定義に適合していない部分があるようです。 例えば、Ⅰ．6．ではアグリゲーションサービス事業者、エンドユーザ、外部組織、供給者、クラウド利用者、クラウド事業者、個別契約連携クラウド事業者、従業員、特権ユーザ、利用者、連携クラウド事業者、ユーザサポートに登場するユーザ、SLA の定義に登場するサービス提供者、顧客など多くのロールが存在するようですが、ISO/IEC 17789:2014 ではクラウドコンピューティングの参照アーキテクチャを提供し、クラウドコンピューティングにおけるロールとアクティビティを定義しています。国際規格におけるロールは各々の責任分界点を明らかにするために使用されることがありますので、本案で定義しているロールが国際規格で定義しているロールと対応関係がない場合、クラウドコンピューティング、そしてそれを前提とする国際規格との整合性が取れなくなります。例えば、ISO/IEC 27017:2015 は ISO/IEC 17788:2014、ISO/IEC 17789:2014 の用語を基準に開発されていますので、本案と ISO/IEC 27017:2015 は整合性が取れないことになります。また将来に開発されるクラウドコンピューティングの国際規格とも整合性が取れないことになりかねません。 特にⅠ．6．17．クラウドには「JIS Q 27001 を基に定義」とありますが、JIS Q 27001 の国際対応規格である ISO/IEC 27001 にはクラウドについての言及がありません。Ⅰ．7．参考文書に掲載されている JIS Q 27017:2016 (ISO/IEC 27017:2015)でクラウドについて言及していますが、それは国際規格 ISO/IEC 17788:2014、ISO/IEC 17789:2014 の用語定義を基準として参照しています。また、これらの国際規格にはクラウドコンピューティング以外に、本案で定義している用語、例えば、プライベートクラウド、パブリッククラウド、ハイブリッドクラウド、SaaS、PaaS、IaaS といった用語も定義していますのでご参照ください。（Ⅰ．6．用語の定義） 【日本オラクル株式会社（情報処理学会 情報規格調査会 SC 38 専門委員会）】	本ガイドラインについては、国際規格における用語の定義を踏まえ、クラウド事業者が実施すべき情報セキュリティ対策をより具体的かつ分かりやすく提示する観点から用語の定義を行っており、齟齬があるものではないと考えております。 なお、本ガイドライン（案）におけるⅠ．6．17．の「クラウド」の定義は「SaaS」を示していたため、修正いたします。	有
「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2版）」（案）を拝読いたしましたが、国際規格との齟齬があるようです。クラウドコンピューティング市場はグローバルな市場を前提としていますので、以下の国際規格を参照し国際的にも通用するガイドラインの作成を期待しております。 用語、参照アーキテクチャ関連： ・ISO/IEC 17788:2014 (ITU-T Rec. Y.3500) Information technology -- Cloud computing -		

– Overview and vocabulary 【注記】用語定義の国際規格です。ITU-T との共同規格です。対応 JIS 規格が存在します。 ・JIS X 9401:2016 情報技術－クラウドコンピューティング－概要及び用語 ・ISO/IEC 17789:2014 (ITU-T Rec. Y.3501) Information technology -- Cloud computing -- Reference architecture 【注記】参照アーキテクチャの国際規格です。役割分担や責任分界点についての言及があります。ITU-T との共同規格です。 クラウドサービスレベル合意書（SLA）関連： ・ISO/IEC 19086-1:2016 Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 1: Overview and concepts 【注記】クラウド SLA の基本事項と枠組みについて規定しています。対応 JIS 規格を開発中です。 その他、クラウドサービスの基本的な挙動関連： ・ISO/IEC 19941:2017 Information technology -- Cloud computing -- Interoperability and portability 【注記】クラウドサービスの相互運用性と可搬性について規定しています。 ・ISO/IEC 19944:2017 Information technology -- Cloud computing -- Cloud services and devices: Data flow, data categories and data use 【注記】クラウド上で処理されるデータ分類の枠組みについて規定しています。 ちなみに、ISO/IEC 27017:2015 (JIS Q 27017:2016)は上記 ISO/IEC 17788 と ISO/IEC 17789 を前提にして開発されています。（全体） 【日本オラクル株式会社（情報処理学会 情報規格調査会 SC 38 専門委員会）】		

【Ⅱ．組織・運用編に対する意見】

提出された意見	総務省の考え方	提出意見を踏まえた案の修正の有無
意見４ 「経営陣は、情報セキュリティに関する取組についての責任と関与を明示し、人員・資産・予算の面での積極的な支援・支持を行うこと。」という記載は、具体性のない精神的指摘にとどまっている。企業において確保すべきサイバーセキュリティ人材の具体的数値基準等を盛り込むべき。	御意見を踏まえ、20 ページのベストプラクティスに、「ⅳ．経営陣は、情報セキュリティに関する取組にあたり、情報セキュリティ人材の育成を行うことが望ましい。」を追加いたします。 企業において確保すべきサイバーセキュリティ人材の具体的数値基準等はクラウド事業者の規模によって異なるため、本ガイドラインにおいて具体的数値基準等は求めないこととし、原案のとおりといたします。	有
P20「Ⅱ．２．情報セキュリティのための組織」「Ⅱ．２．１．内部組織」にて『経営陣は、情報セキュリティに関する取組についての責任と関与を明示し、人員・資産・予算の面での積極的な支援・支持を行うこと。』とあるが、非常に内容が緩いと感じた。理由として具体性のない精神的指摘にとどまっている点が問題である。 経営ガイドラインにおいても『サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる。』と育成の実施を一般企業に向けても具体的に指示している。 さらに重要インフラガイドラインでは p17「（１）資源確保」にて『情報セキュリティ対策のPDCAサイクル推進、すなわち、PDCAサイクルの確立、実施、維持及び継続的改善に取り組むに当たって、必要となる資源（人材や予算等）を明確化し、経営層の指揮の下、組織内へ適切に配分する。 また、環境変化による情報セキュリティ対策の水準低下へ対処する等の観点から、経営層は必要な資源の継続的な確保に努める。』 さらに国家資格の『「情報処理安全確保支援士」等の資格取得等も期待される。』と具体的に指示している。 本ガイドラインにおいても上記のように具体的な国家資格および確保するべき人数を３名など具体的数値基準として盛り込むべきである。 この資格は政府 IT 入札要件、内閣官房情報通信技術(IT)総合戦略室と総務省行政管理局の定める「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書（第 3 編第 6 章 調達）」の P44、P91、P92 にも要件として示されている。 ちなみに一般企業でも有資格者が１～２名在席しており、大手 SI ではすでに２００名以上在籍している。複数企業から情報資産を預かるクラウド事業者に対しても複数名の在籍を要件とするべきである。 【個人 A】		

意見5　CSIRT の構築や外部の専門家からの助言を受けることについて記載すべき。 『【ベストプラクティス】』としては、『関連する役割及び職務機能を持つ代表者（CIO[7]、CISO[8]等）』のみではなく、それを実務的に支える CSIRT を構築し様々なセキュリティ対応にあたることが望ましい旨を記載すべきと考える。（Ⅱ．2．1．1.【基本】ｉ） 【マカフィー株式会社】 高度な専門的技術力をもった人材を内部に確保することが困難であることや内部からのみでは対策のための視野が内部のみに狭まる懸念があることから、「情報セキュリティに関する専門的な助言が必要と判断した場合には、CISO　や内部及び外部の情報セキュリティ専門技術者から助言をうけ」とすることが望ましい。（Ⅱ．2．1．1.【基本】iii.） 【マカフィー株式会社】	御意見を踏まえ、20 ページのベストプラクティス iii．の内容を、「経営陣は、情報セキュリティに関する専門的な助言が必要と判断した場合には、CISO　や内部の情報セキュリティ専門技術者（CSIRT　等）又は必要に応じて外部の専門家から助言を受け、その結果をレビューした上、組織内で調整することが望ましい。」に修正いたします。	有
意見6　有資格者や外部の専門家による定期的な点検・監査を実施する旨を記載すべき。 「点検・監査」の目的を踏まえると、内部の監査人のみではなく、外部の第三者の専門家にも定期的に点検・監査を実施してもらう旨の記載があることが望ましいと考える。（Ⅱ．4．3．2.【基本】ｉ） 【マカフィー株式会社】 p29「II．4．3．情報セキュリティポリシーの遵守、点検及び監査」『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、定期的にレビュー及び見直しを行うこと。』と記載あるが、どのような能力資質のある者が監査するのか？具体的記述が無い。 ISO/IEC 27017 に基づく ISMS クラウドセキュリティ認証を受けるか、外部監査を受けるべきである。 定期的に内部監査を行う場合も「情報セキュリティサービス基準」の p8「情報セキュリティ監査サービスに関する附則」に例示される試験合格者・有資格者によるべきである。 【個人 A】	御意見を踏まえ、29 ページのベストプラクティス ｉ．の内容を、「点検・監査は、十分な技術的能力及び経験を持つ内部の者（例：情報処理安全確保支援士資格を持ち、情報セキュリティに係る技術的対策の実務を一定年数以上経験している者）又は必要に応じて外部の専門家の監督の下で行うことが望ましい。」に修正いたします。	有
意見7　CSIRT との連携について記載すべき。 どの主体が実施するか明確にするため、『【ベストプラクティス】』としては、情報セキュリティインシデント及び脆弱性をハンドリングする CSIRT のような組織との連携を記載するのが望ましいと考える。（Ⅱ．6．1．1.【基本】ｉ） 【マカフィー株式会社】	御意見を踏まえ、33 ページのベストプラクティス ｉ．に、「情報セキュリティインシデント及びぜい弱性をハンドリングする組織（CSIRT 等）と連携して」を追加いたします。	有

【Ⅲ．物理的・技術的対策編に対する意見】

提出された意見	総務省の考え方	提出意見を踏まえた案の修正の有無
意見8　可用性に関する要求事項は、機密性及び完全性への要求事項とは切り分けて示すべき。 本案の「Ⅲ．物理的・技術的対策編」ではクラウドサービス種別のパターン分類を実施され、各項目について具体的な条件を仔細にわたって記載されておりますが、このパターン分類において可用性まで踏み込んだパターン化となっているため、JIS Q27017 などで対象としている情報セキュリティ対策の要件を超えて、クラウドサービスそのものの運用管理基準への要件や要求事項まで規定しているように見受けられます。 従いまして、可用性に関する要求事項は、機密性および完全性への要求事項とは切り分けて示すことが望ましいと考えます。国際規格 ISO/IEC 19086-1:2016 ではクラウドサービスレベル合意書の枠組みについて規定していますが、可用性に関する要求事項はクラウドサービスレベル合意書の内、情報セキュリティの範疇でなく、クラウド SLA の単独コンポーネントとして規定しています。ちなみに、情報セキュリティに関するクラウド SLA につきましては、現在以下の国際規格として開発中です。 ・ ISO/IEC FDIS 19086-4 Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 4: Components of security and of protection of PII （Ⅲ．物理的・技術的対策編） 【日本オラクル株式会社（情報処理学会 情報規格調査会 SC 38 専門委員会）】	本ガイドラインは、ISO/IEC27002 を踏まえ、機密性、完全性、可用性の三つの観点から情報セキュリティ対策を示すものです。 可用性に関する情報セキュリティを除く SLA の要求事項については、御指摘のとおり ISO/IEC19086-1 を参照することが望ましいと考えます。 なお、現在開発中の国際規格については、今後の本ガイドラインの改定の際に、参考とさせていただきます。	無
意見9　クラウド利用者が自らのセキュリティ対策を強化できることを可能とするためにクラウド事業者による API 機能の提供について記載すべき。 クラウド利用者が利用時に自らセキュリティ対策を強化できることを可能とすること目的とし、Ⅲ．1．アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通する情報セキュリティ対策　Ⅲ．1．1．運用管理に関する共通対策へ、「ユーザーアクティビティ（ユーザの操作ログ、ファイルのアップロード、ダウンロード、ファイル共有ログなど）、監査ログ（ログイン/ログアウトログ、ユーザの作成ログ、権限付与ログなどの管理機能ログ）へのアクセスを実現する API 機能を提供すること。」を追加することが望ましい。API 提供によりユーザ側の組織は、利用者に自組織のルールに適合した利用を実現できることが期待でき、セキュリティを理由にクラウド利用に躊躇していた利用者層にクラウド利用を推進させる効果も期待できる。（Ⅲ．1．1．運用管理に関する共通対策） 【マカフィー株式会社】	ご指摘のとおり、クラウド利用者側で情報セキュリティ対策を強化する方法として API 機能を活用することは望ましいと考えます。しかしながら、API 機能はクラウド事業者がクラウド利用者に提供する場合のみならず、クラウド利用者が自ら用意する場合もあるため、クラウド事業者が実施すべき対策として記載することはせず、原案のとおりといたします。	無

意見 10 情報セキュリティに関する情報を提供している機関の例としてセキュリティベンダーを記載すべき。 情報セキュリティに関する情報は、セキュリティベンダーからも無償/有償にて多く発信されているため、情報セキュリティに関する情報を提供している機関例として「セキュリティベンダー」を追記すべきと考える。(Ⅲ．1．1．6.【基本】ⅰ) 【マカフィー株式会社】	御意見のとおり、46 ページのベストプラクティスⅰ．に、情報セキュリティに関する情報を提供している機関の例として「セキュリティベンダ」を追加いたします。	有
意見 11 専門セキュリティベンダーが提供する監査ツールの導入について記載すべき。 技術的ぜい弱性情報を、自社において網羅的に収集することは困難であるため、「必要に応じてクラウド事業者は専門セキュリティベンダーの監査ツールの導入すること。」を『【ベストプラクティス】』に追記すべきと考える。(Ⅲ．1．1．6.【基本】ⅱ) 【マカフィー株式会社】	本ガイドラインは、クラウド事業者がどのような情報セキュリティ対策を実現すべきかを示しており、具体的にどのようなツール等を用いて実施するかまでを示すものではないため、原案のとおりといたします。	無
意見 12 情報漏洩対策の実施や情報漏えい対策システムの作動及び停止について記載すべき。 『e) データ及び他の情報資産へのアクセスの成功及び失敗した試みの記録』とあるが、成功・失敗のログを取得するのみでは、具体的な効果がないため、『【ベストプラクティス】』に、情報漏洩対策の実施を追加し、l)で情報漏洩対策システムの作動及び停止を追加すべきと考える。(Ⅲ．2．1．3.【基本】ⅰ) 【マカフィー株式会社】	御意見を踏まえ、52 ページのベストプラクティスⅰを、「l)保護システム(例えば、ウイルス対策システム、侵入検知システム、情報漏えい対策システム)の作動及び停止等」に修正いたします。	有
意見 13 HTTP/HTTPS の通信に含まれるウイルス等の不正なコードを確認すべき旨を記載すべき。 ファイルをローカルにダウンロードするだけでなく、クラウドサービス間でファイルをやり取りすることが想定されるため、言及されているホストベースのセキュリティ対策では不十分である。具体的な対策として、「HTTP/HTTPS の通信に含まれるウイルス等の不正なコードを確認すること。」を追記すべきと考える。(Ⅲ．2．2．1.【基本】ⅳ) 【マカフィー株式会社】	御意見を踏まえ、57 ページのベストプラクティスⅳ．を、「提供するクラウドサービスの一環として、利用者によるダウンロードや HTTP/HTTPS 等を利用したクラウド間転送を許可するファイルについては、ウイルス等の不正なコードが含まれていないことを十分に確認してから提供することが望ましい。」に修正いたします。	有
意見 14 機密性への要求が高いサービスの利用と管理、完全性への要求が高いサービスの管理においては、「多要素認証」の導入が望ましい旨を記載すべき。 【意見箇所】 「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2版)(案)」 p62:Ⅲ.3.1.3【ベストプラクティス】および【評価項目】 【意見内容】 「評価項目」の対策参照値に各認証方式が表記されていますが、特定の認証方式が、そ	御意見を踏まえ、62 ページのベストプラクティスに、「ⅲ. 高い機密性、完全性が求められるサービスでは、記憶情報・所有情報・生体情報を組み合わせた多要素(二要素)認証を採用することが望ましい。」を追加いたします。 あわせて、同ページの評価項目の内容	有

の認証方式の性質によって安全性が高いと認識された配置となっているようです。 実際には安全性はシステムの性能によって左右されると考えています。 （例えば生体認証は、同じ指紋認証だったとしても、システムごとの本人拒否率および他人受入率によって安全性は変わります） 　現時点の傾向としては、認証の安全性を高めるには多要素（二要素）認証の導入が、各セキュリティガイドラインでは推奨されています。 （例：府省庁対策基準策定のためのガイドライン、PCI DSS 等） この状況を鑑みて、「ベストプラクティス」に下記の「ⅲ」を追加し、 「評価項目」表を添付の内容に変更することを提案いたします。 　ⅲ．機密性への要求が高いサービスの利用と管理、完全性への要求が高いサービスの管理においては、「多要素認証」の導入が望ましい。 多要素認証とは、「知識」「所有物」「生体」の認証要素のうち、いずれか2要素以上の確認を必要とする認証を指す。 【パスロジ株式会社】	も修正いたします。	
意見 15　リバースプロキシを使用し、外部からサーバへの直接アクセスを制御すべき旨を記載すべき。 　『【ベストプラクティス】』にはファイアウォールの記載のみで、対策として効果が見込めるリバースプロキシによるベストプラクティス対応が記載されていない。『【ベストプラクティス】』に、「リバースプロキシを使用し、外部からサーバへの直接アクセスを制御することが望ましい。」という記述を追加すべきと考える。（Ⅲ．３．１．４．【基本】） 【マカフィー株式会社】	御意見のとおり、63 ページのベストプラクティスに、「ⅳ．リバースプロキシを使用し、外部からサーバへの直接アクセスを制御することが望ましい。」を追加いたします。	有
意見 16　標準で https プロトコルの利用等を行えるようにすべき。 　通信の暗号化について常に意識すべきである。PaaS、SaaS の形での役務提供を行っている場合は、標準で https プロトコルの利用等を行えるようにすべきである。また、利用者には積極的にその使用を推奨すべきである。 【個人 B】	クラウド事業者は通信の暗号化を行うことが求められます。しかしながら、通信の暗号化を行う対策には、66 ページに示しているとおり、クラウドサービスの提供状況に応じて HTTP 暗号通信（SSL（TLS）等）によるものと、IP 暗号通信（VPN(IPsec)等）によるものがあるため、標準で https プロトコルの利用を行うことはせず、原案のとおりといたします。	無

【Ⅳ. IoT サービスリスクへの対応方針編に対する意見】

提出された意見	総務省の考え方	提出意見を踏まえた案の修正の有無
意見 17　専門セキュリティベンダーが提供する監査ツール、SIEM製品、ホワイトリストソフトウェアの導入について記載すべき。	意見 11 に対する考え方のとおり。	無
技術的ぜい弱性情報を、自社において網羅的に収集することは困難であるため、具体的なアクションに「必要に応じてクラウド事業者は専門セキュリティベンダーの監査ツールの導入すること。」を追記すべきと考える。（Ⅳ. 5. リスク対応策　表中 A-5） 【マカフィー株式会社】		
振る舞いのおかしい機器を早期検知できる仕組みがどういったものなのか、一般的にはわかりにくいため、複数のシステムのログを保しそれらを相関分析し異常を検知できる、SIEM 製品等の導入を明示すべきと考える。（Ⅳ. 5. リスク対応策　表中 A-9） 【マカフィー株式会社】		
ICT 機器（ハードウェア/ソフトウェア）の一般的なセキュリティ対策が想像しにくいため、「ホワイトリストソフトウエアの導入など」を追記すべきと考える。（Ⅳ. 5. リスク対応策　表中 B-48） 【マカフィー株式会社】		

【Ⅴ．参考資料に対する意見】

提出された意見	総務省の考え方	提出意見を踏まえた案の修正の有無
意見 18　不審な活動を発見するための UEBA ツールや監査ツールの導入を推奨する旨を記載すべき。	意見 11 に対する考え方のとおり。	無
イベントログの取得に関しては、そのログを保管しインシデントレスポンスに利用するだけでは不十分であり、とりあえず保管するだけという状況になってしまうおそれが高い。「取得したログを定期的に確認し、そのログを分析するために SIEM を利用する。さらに、不審な活動を発見しあぶりだすために UEBA（User and Entity Behavior Analytics）ツールの導入を推奨する。」旨の記述を追記すべきと考える。（Annex 5 利用者接点と ICT サプライチェーンに着目した要求事項　12．4．1　イベントログ取得） 【マカフィー株式会社】		
事業者単体でのぜい弱性の把握は負担が大きいため、必要に応じてクラウド事業者は専門セキュリティベンダーの監査ツールの導入を推奨すべきと考える。（Annex 5 利用者接点と ICT サプライチェーンに着目した要求事項　12.6 技術的ぜい弱性管理） 【マカフィー株式会社】		
意見 19　不正なソフトウェアが動いていないことを注意すべき旨を記載すべき。	不正なソフトウェアが動いていないことを注意するためには、不正なアクセスを監視すること、セキュリティ管理の徹底を助言すること、情報転送を確実かつ安全に実施できる措置を講じること等による情報セキュリティ対策を実現することが求められます。 これらについて、239 ページ及び 251 ページに具体的な対策を示しております。	無
自らの拠点内において、仮想化したホストについて、そのクラスタ間の通信やライブラリ呼び出しについてフックしてデータをコピーする様なソフトウェアが動いていないかどうかについて注意を行うようにすべきである。 【個人 B】		

【その他】

提出された意見	総務省の考え方	提出意見を踏まえた案の修正の有無
意見 20　AWS の拡大に疑念を感じる。 AWS の拡大に疑念を感じます。 【個人 C】	本ガイドラインとは直接関係がないため、参考の御意見として承ります。	無