別紙15　クラウドサービスに係るセキュリティ要件

出典：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～利用者との接点と事業者間連携における実務のポイント～（総務省 平成26年4月）

情報セキュリティ対策ガイドラン対応項番				要件
6. 情報セキュリティのための組織				
	6.1 内部組織			
		6.1.1 情報セキュリティの役割及び責任		
			a	当省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、当省の同意を得ること。 （PaaSの場合、提供されるサービスによって、当省が自ら管理できる情報資産や情報セキュリティプロセスの範囲にかなり幅があるため、当省との管理責任の分担や免責の範囲が不明確になりやすく、特に慎重に責任の範囲を定めること。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、クラウドサービス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。）
			b	クラウドサービスの提供に係る受注者の委託先管理の責任を明確に規定し、従業員に割当、文書化すること。
			c	(a)(b)の実施に当たり必要となる当省と受注者の間、並びに受注者と委託先の間における情報セキュリティマネジメントの側面の調整及び管理に関する事項を、契約形態、統制、順守、情報提供の範囲、技術協力の範囲、緊急時対応の役割分担等に係る要求の観点から特定し、文書化すること。
			d	当省と締結するSLAを保証するため、提供するサービスレベルの保証に関するクラウドサービス供給者の責任範囲の規定に基づいて供給者を適切に選定し、この選定に従ってICTサプライチェーン全体のサービスレベルの保証に係る自らの責任範囲を定義し、文書化すること。但し、クラウドサービス供給者との間で、データ連携等を個別の仕組みを新たに構築して実現する場合は、分担する責任についての調整及び管理に関する事項についても、併せて文書化すること。
			e	当省に対する説明責任の主体と詳細を明確に定めること。説明責任の遂行に当たっては、Web等を用いた情報公開による当省への周知と個別の情報開示の範囲を明確にし、受注者として個別対応が可能な範囲について、統制の観点からクラウド利用者に通知すること。
		6.1.2 職務の分離		
			a	サービス運用・設定の実務を行う者と認可を行う者の役割と責任を明確に分離すること。
			b	システム設計・構築を行う者と認可を行う者の役割と責任を明確に分離すること。
			c	ASP・SaaSの場合は、開発・保守の実務を行う者と運用を行う者の役割と責任を明確に分離すること。
	6.2 モバイル機器及びテレワーキング			
		6.2.1 モバイル機器の方針		
			a	当省に対し、不正改造されたり、マルウェアに感染したモバイル機器をクラウドサービスに接続させないように要求すること。
			b	当省への運用上の要求事項も含めて、モバイル機器上で、スクリーンショット・スクリーンキャスト録画・クリップボード履歴保存・キーロガー等を実行させないための対策を講じること。
			c	クラウド利用者に配布する、モバイル機器用のクライアントアプリケーションには、キャッシュ保存機能を持たせないか、または十分な強度の鍵長とロジックでキャッシュデータを暗号化する機能を持たせること。
			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。
			e	モバイル機器と業務用クラウドサービスの間の通信は十分な強度の暗号を用いて暗号化すること。
			f	当省への運用上の要求事項も含めて、モバイル機器の業務データを他のシステムと同期させないための対策を講じること。
	6.3 クラウド利用者とクラウド事業者の公平な取引を確保するための措置			
		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		
			a	文書化された受注者自身の責任範囲を、「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」(b)(f)(i)から手法を選択して、SLA等によりクラウド利用者に明確に示すこと。
			b	当省が求める統制を満たすに当たり、受注者が提供できる機能・サービスを、「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」(b)(f)(i)から手法を選択して、SLA等により当省に明確に示すこと。

			c	(b)を実施するに当たり、当省個別に対応可能な範囲を予め明文化しておき、この文書を用いた情報提供により、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。
		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		
			a	クラウドサービスの比較Webサイト（例：クラウドサービス情報開示認定サイトhttps://www.fmmc.or.jp/cloud-nintei/）を活用し、クラウドサービスに係る情報を一般公開することを検討すること。
			b	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または努力目標を、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。また、取得した認証（情報セキュリティ対策実施に関するもの、内部統制監査に関するもの等）を一覧できる形式で情報公開すること。
			c	監査済みの「情報セキュリティ対策の設計・実装・運用に係る言明書」がある場合は、(b)の一般向け情報公開システムを用いて情報公開すること。
			d	クラウドサービスの情報セキュリティに関する窓口（ヘルプデスク等）を分かりやすく公開すること。
			e	当省からの個別要求に基づき、NDAを締結して、個別の情報開示を行うに当たり、その窓口をできる限りワンストップ化すること。また、個別の情報開示における当省の窓口を特定し、管理すること。
			f	ログイン認証付きWebサイトでは、日常の都度の連絡（計画的サービス停止/定期保守、バージョンアップ、マニュアル類の最新版公開の案内など）、サービス達成状況（サービス稼働率、平均応答時間、サポートサービス応答率等）または障害発生履歴、現在の稼働状況、利用者からの問合せ件数/内容などの情報公開を検討すること。
			j	管理ツールを利用し、当省のサービス利用状況（ログイン実績、利用時間、利用ログ提供等）、クラウド利用者から預託された情報の保守取扱い実績などの情報照会機能を検討すること。
			h	電子メール・FAXでは、緊急時の連絡・報告（クラウドサービス内で発生した情報セキュリティインシデントについての情報：障害発生/復旧時刻・障害経過の通知、障害内容・原因・対処等に係る事後報告等）の情報提供を検討すること。
			i	当省からの個別要求に基づき、NDAを締結して、個別の情報開示（例：当省が希望する種別のインシデント履歴、第三者機関による監査・ぜい弱性検査レポート、当省から預託されたデータ・利用ログ記録等の保存場所等）を行う場合は、当省にとっての知るメリットと受注者にとっての情報開示のデメリット（業務負荷の増大も含む）のトレードオフを検討すること。 代替案として、監査済み言明書の公開や、NDAを締結した上での「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」（IT実7号、SOC2等）、「クラウド事業者の内部統制保証報告書9」（監保実86号、ISAE3402/SSAE16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、当省に開示すること。
			j	当省に影響を及ぼす情報セキュリティインシデントの発生後、その情報を適切に設定された時間以内に、(h)の手法により、当省に通知すること。その後も、適切な時間間隔で情報の通知を続け、当省が受領した情報を追跡できるようにする
			k	当省に一斉周知する情報は、「16.1.4　情報セキュリティ事象の評価及び決定」(d)に従って提供すること。
			l	当省によって発見された情報セキュリティインシデントの情報の受付窓口を設置し、当省の利用者に分かりやすく示すこと。
			m	正確な情報を相互に交換するため、緊急時の情報提供と情報受付に係るクラウドサービス供給者の規定を確認し、これに基づいて情報セキュリティインシデントの情報をICTサプライチェーンで共有するための連絡体制を構築すること。
			n	(m)で構築した連絡体制に基づき、ICTサプライチェーンを構成する受注者は、情報セキュリティインシデントの際の窓口を設置すること。
			o	個別契約連携クラウドサービスを提供する場合は、当省の便益を考慮し、個別契約連携クラウド事業者間の情報共有を積極的に行うこと。
8. 資産の管理				
	8.1 資産に対する責任			
		8.1.1 資産目録		
			a	当省から預託された情報と、クラウドサービスを運用するための内部情報を、別の資産として分類すること。
			b	仮想化資源を用いてクラウドサービスを提供している場合は、仮想化資源をラベル付け（属性情報等をタグ付け）すること。
			c	(a)(b)等に係るクラウドサービスの特性に基づき、管理水準が異なる預託情報を当省が分類するために必要な情報を、「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」(i)の手法に基づき、SLAに記載して同意した範囲内で当省に提供すること。
		8.1.2 資産の管理責任		

				番
			a	当省が作成し管理する目録の中の各々の預託情報が保存されるクラウド事業者の情報処理施設等（仮想化資源を含む）のそれぞれについて、個別に管理ポリシーと管理水準に関する情報を、「6.3.2　利用者接点とサプライチェーンにおける情報・共有」(i)の手法に基づいて当省に提供し、当省が適切なサービスを選択できるように支援することが望ましい。 なお、当省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。
		8.1.5 クラウド利用者から預託された情報の返却		
			a	個々の当省の預託情報を、特定して抽出するための措置を講じること。
			b	「13.2.2　情報転送に関する合意」(e)の事前合意に基づき、預託された情報を当省またはその指示によって他のクラウド事業者が取扱うことができる形式で、当省に返却すること。
			c	(b)の対応が有料である場合は、その旨を当省に周知すること。
			d	クラウドサービスの利用終了後に、預託された情報を二度と取り出せないように消去または破壊すること。
			e	(b)(d)を実現する方法について、クラウドサービスを選定するに当たり参考にできるような形で、当省に情報提供すること。
			f	(e)について詳細な情報の開示を求められた場合には、「6.3.2　利用者接点とサプライチェーンにおける情報・共有」(i)の手法に従って情報開示することを検討すること。
	8.2 情報分類			
		8.2.1 情報の分類		
			a	複数のクラウドサービスを提供している場合には、提供するサービスに応じて当省からの預託情報の分類を行うこと。
			b	(a)の各分類に対し、対応しているクラウドサービスの種類に応じて、預託情報の価値、重要性等を定義すること。
			c	各々のクラウドサービスの提供において、当省からの預託情報を、(b)の定義を踏まえて管理すること。
			d	クラウドサービスの提供に当たり、仮想化された資源を利用している場合は、当省からの預託情報を明確に分類できる措置を施すこと。
		8.2.3 資産の取扱い		
			a	当省から預託を受けた情報については、それぞれを容易に分離できるような措置を講じること。
			b	仮想化された資源を用いて預託を受けた情報を管理する場合には、他のクラウド利用者から預託された情報を特定できるような措置を講じること。
9. アクセス制御				
	9.1 アクセス制御に対する業務上の要求事項			
		9.1.1 アクセス制御方針		
			a	アクセス制御サービスを提供している情報処理施設等の冗長化を行うこと。
			b	ソフトウェア更新時の切替試験を徹底して行うこと。
			c	運用上の設定を行う者とそれを認可する者を分離すること。
			d	運用手順書のレビューを徹底し、その品質を向上させること。
			e	当省が、提供されるクラウドサービスにおいて実施可能なアクセス制御機能を、判断し選択できるようにするため、当省から個別に要請を受けた場合は、「6.3.2　利用者接点とサプライチェーンにおける情報・共有」(i)に従い、アクセス制御方針について以下の情報の提供を検討すること。 □当省に付与するアクセス制御権限及び内部統制が機能した権限付与プロセス □導入しているID管理のフレームワーク（シングル・サイン・オン等のID連携を組み込む能力があるか、等） □認証の強度（認証対象とする要素及び数、各要素における技術的・運用的な措置による堅牢性等） □シングル・サイン・オン等のID連携への対応状況
			f	シングル・サイン・オンやID連携を実施する場合は、管理責任と役割の範囲、技術的対応のための仕様、運用規約・手順等について供給者の規定を確認し、これに基づいて、ICTサプライチェーンにおける自らの管理責任と役割の範囲を定義するとともに、供給者との連携を実現できる仕様、運用規約、手順等を定めることで、必要な技術的対応を確保すること。 但し、連携するに当たり、クラウドサービス供給者との間で特定個別の仕組みを新たに構築する場合は、役割や責任の分担、技術的対応のための取り決め等についても個別に明確化し、文書化すること。なお、個別契約連携クラウドサービスの形態でサービス提供している場合は、当省が自らの管理責任の範囲を定義するに当たり、個別契約連携クラウド事業者が規定する管理責任の範囲を1つ1つ確認する必要がある。この確認プロセスは、通常の当省対受注者の場合よりも複雑なので、責任の所在に係る当省の理解が不明確になる課題が生じうるため、特に注意を要する。

			g	当省から個別に要請を受けた場合は、シングル・サイン・オンやID連携の実現と運用に係る技術情報等を、「6.3.2　利用者接点とサプライチェーンにおける情報・共有」(i)に従って提供することを検討すること。
		9.1.2 ネットワーク及びネットワークサービスへのアクセス		
			a	クラウドサービスの提供に供するネットワーク及びネットワークサービスについては、当省を認証した後のみ内部的なネットワーク等にアクセスできる等の適正なアクセス制御の措置を講じること。
			b	クラウドサービスを利用できる対象者を限定している場合（例：国内からクラウドサービスを利用する当省に限定）は、アクセス元サーバに対する認証を行う、または許可された当省以外からのアクセスを制限する等、第三者からの不要なアクセスを排除する措置を講じること。
			c	クラウドサービスの提供に供するネットワーク及びネットワークサービスで利用するネットワーク機器等における脆弱性について定期的に確認するほか、脆弱性が露見した場合には速やかに対応できる措置を講じること。
			d	供給者と連携してクラウドサービスを提供するために用いるネットワーク及びネットワークサービスについて、連携する受注者とクラウドサービス供給者の間で必要なアクセス制御措置について確認し、これを実施すること。
			e	当省による不正なネットワーク及びネットワークサービスの利用がないことを、アクセス制御の設定を確認すること、あるいは当省の内部的なネットワーク等のアクセス状況を監視すること等を定期的に行うことにより、確認すること。
	9.2 利用アクセスの管理			
		9.2.3 特権的アクセス権の管理		
			a	特権的アクセス権を保護するため、特権的アクセス権を有する特権ユーザに対し、多要素認証技術を適用した認証を行う等の強力な認証機能を提供することが望ましい。これと同時に、「9.4.4　特権的なユーティリティプログラムの使用」(a)(b)(c)(d)(e)を確実に実施し、特権的なユーティリティプログラムの監視と保護を強化することが望ましい。
		9.2.4 利用者の秘密認証情報の管理		
			a	当省のユーザ（個人）が、クラウドサービスが要求する強度の秘密認証情報の割当てを実行できる仕組みを確実に提供すること。
			b	受注者は、秘密認証情報に関する管理情報を当省に提供することによって、当省がクラウドサービスの提供機能の利用判断をしやすくするため、上記を実現するための手順や秘密認証情報の割当て手順に係る情報を、「6.3.2.　利用者接点とサプライチェーンにおける情報・共有」(b)(f)(i)から手法を選択して当省に情報提供すること。
	9.4 システム及びアプリケーションのアクセス制御			
		9.4.1 情報へのアクセス制限		
			a	受注者は、クラウドサービスの提供に係る情報及びアプリケーション機能へのアクセス制御について、自社が提供するシステム・プログラム等における脆弱性を定期的に確認するほか、利用するOS、ミドルウェア等における脆弱性に関する情報及び対応策を確認し、必要な措置を講じること。
			b	受注者は、クラウドサービスの提供においてクラウドサービス供給者と連携する際に、そのクラウドサービス供給者が提供するアクセス制御に依存している場合は、クラウドサービス供給者の選定に当たり同意したアクセス制御に係る方針に基づいてクラウドサービス供給者が実施する措置を確認し、課題が存在する場合は具体的な対応策を要求して、これを実施させること。
			c	不要なアクセス権限の設定、必要なアクセス権限設定の遺漏等が生じないように、当省が利用可能な情報、システム等と当省のIDとの関係を定期的にレビューする等の措置を講じること。
			d	アグリゲーションサービス事業者は、供給者が提供するサービスへのアクセス制御も含めた措置を講じること。
			e	クラウドサービスを利用するのに必要な当省側の環境（利用するWebブラウザ、OS、その他のアプリケーション、デバイス等）の脆弱性に関する情報収集を行い、当省に対して必要な情報の提供、対応措置の依頼等の措置を講じること。
			f	当省側のシステム/ネットワーク環境におけるアクセス制御に係る脆弱性が原因となって、当省からの預託情報に損害等が発生した場合の、受注者の免責等について、当省と予め同意しておくこと。
			g	クラウドサービスを利用するのに必要な当省の認証に係る情報の漏えいについて、特にフィッシングやマルウェアなどに関する情報収集を行い、当省に対して必要な情報の提供、対応措置の依頼等の措置を講じること。
			h	認証に係る情報が当省から漏えいしたことにより、当省からの預託情報に損害等が生じた場合の、受注者の免責等について、当省と予め同意しておくこと。
			i	受注者が提供するアクセス制御の範囲と、当省が利用可能なアクセス制御機能に基づいて、当省がクラウドサービス選択の判断をできるようにするため、アクセス制御方針に係る以下の内容を、「6.3.2.　利用者接点とサプライチェーンにおける情報・共有」(b)(f)(i)から手法を選択して当省に情報提供すること。 ・情報アクセス制御手法 ・アクセス可能な範囲、粒度 ・権限管理者、権限付与・変更手順

				番
			j	受注者は、クラウドサービスを提供するために他のクラウドサービス供給者のクラウドサービスを利用している場合は、当省のID管理の利便性を向上させるサービス機能等に係る以下の情報を、「6.3.2. 利用者接点とサプライチェーンにおける情報・共有」(b)(f)(i)から手法を選択して当省に情報提供すること。 ・シングル・サイン・オン・メカニズムへの対応状況 ・ID連携管理の有無
			k	シングル・サイン・オンやID連携を実施する場合は、管理責任と役割の範囲、技術的対応のための仕様、運用規約・手順等についてクラウドサービス供給者の規定を確認し、これに基づいて、ICTサプライチェーンにおける自らの管理責任と役割の範囲を定義するとともに、供給者との連携を実現できる仕様、運用規約、手順等を定めることで、必要な技術的対応を確保すること。但し、連携するに当たり、供給者との間で特定個別の仕組みを新たに構築する場合は、役割や責任の分担、技術的対応のための取り決め等についても個別に明確化し、文書化すること。
		9.4.4 特権的なユーティリティプログラムの使用		
			a	特権的ユーティリティプログラム（クラウドサービスの運用を支援するプログラム）等を外部からの攻撃にさらされにくい環境に隔離すること。
			b	特権的ユーティリティプログラム等へのアクセス状況を定期的にレビューし、不正なアクセスの監視を行うこと。
			c	当省が特権的ユーティリティプログラムを利用できるように権限を付与する場合には、特権的ユーティリティプログラムのアクセス権限及び権限付与・変更手順等を文書化すること。また、アクセス権限付与に関する証跡を記録し、不要なアクセス権限の設定がないかを、定期的なレビューにより確認すること。
			d	当省が特権的ユーティリティプログラムを利用する場合には、当該クラウド利用者に対しても特権的ユーティリティプログラムの利用に関する監視を求め、必要があればこれに関する情報の提供を求めること。
			e	エンドユーザ（組織）の管理者に対して、サービス利用の管理に関する特権的なユーティリティプログラムを利用できるようにする場合には、当該プログラムを通じて、他のクラウド利用者の預託情報へのアクセスがなされていないかを、定期的なレビューにより確認すること。
	9.5 仮想化されたクラウドサービスのアクセス制御			
		9.5.1 仮想化資源の分離の確実な実施		
			a	仮想化マシンを構成するのに用いるソフトウェアの脆弱性について定期的に確認を行い、技術的脆弱性が露見した場合には、適切な措置を講じること。
			b	IaaS・PaaSの場合は、クラウド利用者当省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.。
			c	仮想化されたアプリケーション、OS、ストレージ、ネットワークについて、テナント間の分離及びテナントとクラウド事業者受注者の内部管理の間の分離を確実に行うこと。さらに、分離された資源に対するアクセス制御を確実にするための措置を講じること。
10. 暗号				
	10.1 暗号による管理策			
		10.1.1 暗号による管理策の利用方針		
			a	暗号化に対応しているサービスを、「6.3.2 利用者接点とサプライチェーンにおける情報・共有」(b)(f) から手法を選択して、当省に情報公開すること。また、暗号化されていないクラウドサービスについては、暗号化を代替する機能がある場合は、同じ手法を用いて、これを当省に情報公開すること。
			b	クラウドサービスにおいて、保管または伝送される情報の機密性確保/完全性・真正性の検証、アクセス制御における認証、否認防止等について、暗号化を適用する範囲を明確にし、「6.3.2 利用者接点とサプライチェーンにおける情報・共有」(i)に従って、クラウド利用者に情報開示すること。
			c	(b)を実施するに当たり、外部組織と受注者の間で転送する情報と長期間保存する当省の情報（バックアップ等）の取扱いについて、特に留意すること。
			d	暗号による管理策の運用実態について、当省から個別に情報開示を要求された場合は、「6.3.2 利用者接点とサプライチェーンにおける情報・共有」(i)に基づいて情報開示することを検討すること。
		10.1.2 鍵管理		
			a	当省に対し、暗号化の強度（鍵タイプ、暗号アルゴリズム、鍵の長さ）と鍵管理徹底の実態（例：鍵管理システムの仕様、推奨する鍵管理手順）を明確に示すため、個別の情報開示や監査済み言明書の公開により（「6.3.2 利用者接点とサプライチェーンにおける情報・共有」(c)(i)参照）、当省に情報提供すること。
			b	当省が、クラウドサービスに預託した情報の暗号化に用いる鍵を、個別に管理できるツールを提供すること。
12. 運用のセキュリティ				
	12.1 運用の手順及び責任			
		12.1.1 操作手順書		
			a	当省が、クラウドサービスの情報セキュリティ関連機能（例：ログイン認証機能）の操作手順書を作成し、エンドユーザ（個人）に徹底することを支援することが望ましい。このため、当省に対し、「6.3.2 利用者接点とサプライチェーンにおける情報・共有」(f)(i)から手法を選択して、操作手順書作成に必要な情報を提供することが望ましい。また、不明点の解消機能として、「6.3.2 利用者接点とサプライチェーンにおける情報・共有」(d)に基づいてFAQや問合せ窓口を提供することが望ましい。
		12.1.2 変更管理		

			a	クラウドサービスに供するシステムに関するプログラムは、安全に隔離された資源において管理を行うこと。
			b	クラウドサービスに供するシステムの変更のために、特権を利用する場合には、その利用を管理できるよう、手順を作成し、記録を作成すること。
			c	クラウドサービスに供するシステムのプログラム変更等について、必要なログ等を取得し、変更管理の状況について定期的にレビューを行うこと。
			d	仮想化されたデバイス（サーバ、ネットワーク、ストレージ等）の導入・変更・削除、クラウドサービスの停止、バックアップ＆リストア等に当たっては、その障害がクラウドサービスを提供する資産に復旧できない損害を与える恐れがあることから、その手順を文書化し、実務運用者と実施判断者の両方に徹底すること。
			e	アグリゲーションサービスを提供している場合は、供給者が提供するクラウドサービスの変更についても、「6.3.2　利用者接点とサプライチェーンにおける情報・共有」(f)(i)から手法を選択し、クラウド利用者に情報提供すること。
			f	クラウドサービスに供するシステムに関するプログラムの変更手順を明確に定め、変更後の確認を、変更した者以外の者が行う等、変更に対するチェック体制を構築すること。
			g	クラウドサービスに供するシステムの変更を行うに当たり、システムにおける直前の構成管理を明らかにし、変更結果から元の構成に戻すことができるように必要なバックアップを取る等の対応を行うこと。
		12.1.3 容量・能力の管理		
			a	クラウドサービスに供するシステムで使用される資源の容量・能力等に不足が生じないように、状況に応じて必要な措置を講じるため、資源を常時監視すること
			b	外部からの攻撃や、利用者による不正な資源の利用により、サービス提供に必要な資源が枯渇する危険性が生じた場合には、それらを遮断、分離、停止できる対応策を講じること。
			c	他のクラウド利用者に対するサービスを阻害するような資源の利用をした場合にサービス利用凍結を含めた措置を行う旨の、資源の利用に関する同意を、当省から得るほか、当省が過大な資源の占有を行わないようにするための対策を講じること。
			d	当省がクラウドサービスの資源逼迫状況や兆候を把握し、そのリスク管理等に役立てるため、資源の使用率や停止している資源の状況等を「6.3.2　利用者接点とサプライチェーンにおける情報・共有」(f)(g)から手法を選択し、情報提供すること。
			e	資源確保の予測を的確に行えるようにするため、最適な資源配分を行う仕組みの有効性と運用設定の妥当性を定期的にレビューすること。
			f	当省が要求する論理資源を十分に割り当てるため、物理資源使用の限界を超えた論理資源の総和を設定すること。この際、論理資源の総和が物理資源を超過するような資源の割当は、物理資源の最繁時の同時使用率を考慮して行うこと。
			g	運用者向けの手順書のレビューにおいて、容量及び能力が設計時の想定を超えた場合の対応手順（仮想資源の再配置のためのライブマイグレーション及び仮想ネットワークの変更手順等）が確実に行われるようにすること。
	12.2 マルウェアからの保護			
		12.2.1 マルウェアに対する管理策		
			a	クラウドサービスに供する情報処理施設等に侵入したマルウェアのスキャン＆検出を毎日実施するほか、第三者からの攻撃等が生じた場合等のマルウェアへの感染が疑われる情報セキュリティ事象が生じた場合にも、マルウェアのスキャン＆検出を速やかに行うこと。また、これに必要な情報収集を日常的に行うこと。
			b	クラウドサービスに供する情報処理施設等に対するマルウェアの感染が認められた場合には、速やかなマルウェアの駆除、外部ネットワークとクラウド事業者が管理する当省の預託データとの分離等の、二次的な被害の発生を防止するための措置を講じること。
			c	当省の情報処理施設等でマルウェア感染の可能性が生じた場合には、クラウドサービスに供する情報処理施設等においても、速やかにマルウェア検出のための措置を講じること。
			d	マルウェア感染に伴いクラウドサービスが停止した場合には、速やかに当省に対してその事実を示すとともに、当省の情報処理施設等のマルウェア感染の確認を促す等の措置を講じること。さらに、当省に対し、必要に応じて、被害状況、サービスの復旧見込み等についての情報を、「6.3.2利用者接点とサプライチェーンにおける情報・共有」(h)の手法によって提供する。
			e	アグリゲーションサービス事業者は、提供するクラウドサービスのICTサプライチェーンの一部の情報処理施設等にマルウェアの感染が認められた場合であっても、影響範囲が確認できるまで、ICTサプライチェーン全体で(b)(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。
			f	自社のサービス利用に供する当省の情報処理施設等を攻撃対象としたマルウェアに関する情報を日常的に収集し、「6.3.2　利用者接点とサプライチェーンにおける情報・共有」(f)の手法により、当省に提供すること。
			g	マルウェアが伝送されてくる等、特定のクラウド利用者当省がマルウェアに感染した兆候を検知した場合は、その事実をクラウド利用者当省に通知するとともに、必要があれば当該利用者のクラウドサービス利用を一時停止できるよう、契約上及び技術上の措置を講じること

	12.3 バックアップ			
		12.3.1 情報のバックアップ		
			a	受注者が取得するバックアップのうち、クラウドサービス提供に不可欠な設定などに関するデータのバックアップと、当省の預託データのバックアップを分離すること。
			b	当省の預託データのバックアップにおいて、個々の当省の預託データを特定できる、ないしは検索可能な措置を講じること。
			c	特定の当省の預託データの提出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、無関係な当省の預託データのバックアップが、不当に情報漏洩しないような措置を講じること。
	12.4 ログ取得及び監視			
		12.4.1 イベントログ取得		
			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、クラウドサービス供給者の利用規約、SLA等の規定を確認し、受注者の要求を満足できる供給者を選定すること。
			c	アグリゲーションサービス事業者は、供給者との間で、取得できるログの範囲、内容、粒度等について情報を共有すること。
			e	アグリゲーションサービス事業者は、供給者のイベントログ取得ポリシーを確認し、これを踏まえてICTサプライチェーン全体で、統一して適用するイベントログ取得ポリシーの範囲を明示・調整すること。
		12.4.2 ログ情報の保護		
			a	適切なアクセス制御、資源の分離等の保護対策を適用し、ログ情報の記録の削除や、改ざん、ログ取得設定の変更などを防止すること。
			b	一部のクラウド利用者等の犯罪行為等に伴う記録媒体の提出命令等によるサービス停止を防ぐため、ログ情報のバックアップを作成するとともに、ログ情報をエンドユーザ（個人）/特権ユーザ単位に管理できる措置を講じること。
			c	アグリゲーションサービス事業者は、供給者のログ情報の保護ポリシーを確認し、ICTサプライチェーン全体で統一して適用できるポリシーの範囲を明らかにすること。
		12.4.3 実務管理者及び運用担当者の作業ログ		
			a	当省の特権利用に基づく資源利用に係るログを特権ユーザ単位で取得し、管理者による不正行為に対する措置を講じられるようにすること。また、受注者においても同様に特権利用のログを特権ユーザ単位で取得し、当省と受注者の特権利用のログを突合することによって、当省と受注者の適正な運用責任の分担を検証できるようにすること。
			b	システムの脆弱性、サービス管理のためのアプリケーションなどの脆弱性を利用した管理用インターフェイスの悪用を防ぐため、管理アプリケーションに対する利用状況やそのためのプログラム等の構成管理状況のログを取得し、監視等の措置を講じること。
			c	(a)(b)の求めに応じて定めるログ取得方針について、クラウドサービス供給者の規定を確認し、受注者の要求を満足できる供給者を選定すること。
			d	取得した特権利用に関するログについて、発生したイベントの妥当性等を検証し、あるいは不正なアクセスの可能性を分析するなど、適切なレビューを行うための措置を講じること。
			e	アグリゲーションサービス事業者は、供給者のログ取得及び記録保護等に関するポリシーを確認し、ICTサプライチェーン全体で一貫して適用できるポリシーの範囲を明らかにすること。
			f	アグリゲーションサービス事業者は、ICTサプライチェーン全体でどのようなログ情報を一貫して取得できるのかを確認し、クラウド事業者と供給者間で突合が可能なログ情報の範囲を明らかにすること。
	12.5 運用ソフトウェアの管理			
		12.5.1 運用システムに関わるソフトウェアの導入		
			a	情報セキュリティマネジメントの観点から必要である場合には、当省がクラウドサービス上にインストールできるソフトウェアの範囲に制限を設け、当省と同意すること。
			b	当省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より、クラウドサービスに情報セキュリティマネジメント上の脆弱性が生じた場合には、当省が利用する資源を隔離して、安全にサービスを提供できるような措置を講じること。
			c	当省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より、クラウドサービスに情報セキュリティマネジメント上の脆弱性が生じたため、安全なサービスの提供が継続できない場合には、速やかにクラウドサービスの全部または一部を停止する等の講じること。
			d	利用規約等によって、当省の運用により、マルウェアに感染したソフトウェアをクラウドサービス上にインストールさせないことを求めること。

			e	当省がインストールしたソフトウェアに起因して、他のクラウド利用者に影響を及ぼすような情報セキュリティ事象が発生した場合に、その原因を切り分けられるように、当省によるソフトウェアのアップロード及び変更の履歴を保持すること。
	12.6 技術的ぜい弱性管理			
		12.6.1 技術的ぜい弱性の管理		
			a	クラウドサービスとその資源に適用される技術的ぜい弱性管理についての情報を、「6.3.2　利用者接点とサプライチェーンにおける情報・共有」(f)(i)から適切な手法を選択して、当省に提供すること。
			b	ISO/IEC 27002:2013の12.6.1の実践の規範が示すポイントを実現する手法についても、(a)と併せてクラウド利用者に情報提供することを検討すること。
			c	クラウド事業者が実施する技術的ぜい弱性の同定作業に伴い、計画的なサービス停止が発生する場合は、6.3.2【利用者接点とサプライチェーンにおける情報・共有】(f)に従って、クラウド利用者に事前に情報公開すること。
			d	個別のクラウド利用者に係る技術的ぜい弱性情報を、他のクラウド利用者に提供しないこと。
	12.7 情報システムの監査に対する考慮事項			
		12.7.1 情報システムの監査に対する管理策		
			a	クラウドサービスの監査について方針を定め、監査を定期的に実施する、監査対象となる資源とサービス提供に係る情報資産等の分類を適切に行い、監査対象を明確にし、最小限の監査により、管理策の十分性を確認できるようにする等、効果的な監査を実施できるようにする措置を講じること。
			b	当省からの個別の監査対応要請を少なくするために、監査済み言明書の公開、監査報告書（受注者のセキュリティ管理に係る内部統制保証報告書（IT実7号、SOC2等）等）の情報開示、その他必要な情報の開示、認証の取得等、当省が行う監査対応を簡素化するための措置を講じること。
13. 通信のセキュリティ				
	13.1 ネットワークセキュリティ管理			
		13.1.4　仮想ネットワークにおいて重視すべき脆弱性		
			a	クラウドサービスの提供に当たり、仮想ネットワークを新たに構築する場合は、物理ネットワーク構成との対応関係が明確になるように仮想ネットワークを構成すること。
			b	仮想ネットワークの運用設定方針と設定承認方針を、物理ネットワークの運用経験とノウハウに基づいて実施しやすい形で定義し、文書化すること。
			c	PaaS/IaaSを提供している場合は、当省の構内設備をクラウドサービスに移行させる際に、仮想/物理ネットワークの再構成、移行、試験運用のプロセスで悪意の攻撃を受けないように、当省にセキュリティ管理の徹底を助言すること。
	13.2 情報の転送			
		13.2.2　情報転送に関する合意		
			a	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には、クラウドサービスの提供におけるデータ転送に係る方針、標準的な規格・仕様等及びこれに対する保守方針等について、クラウドサービス供給者の規定を事前に確認し、データ転送が確実かつ安全に実施できるクラウドサービス供給者を選定すること。但し、特定の供給者との間で個別の方法によりデータ転送を行う場合には、方針、規格・仕様、保守方針等について、個別の調整と合意が求められる。
			b	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には、クラウドサービス供給者のサービスが停止した場合のデータ転送の安全確保等に係る措置を講じること。
			c	クラウドサービス内または外部とのデータ連携を行うに当たり、暗号化・資源の隔離等の、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。
			d	フィッシング対策等の秘密認証情報窃盗への対応、及び当省への注意喚起を行うことにより、当省からのID等の秘密認証情報の転送の安全を確保するための措置を講じること。
			e	クラウドサービスの利用終了時に、預託された情報を安全かつ完全な形で返却するために、情報転送のためのデータ規格、仕様等について、事前に当省からの同意を得ること。
		13.2.4　秘密保持契約または守秘義務契約		
			a	複数国の資源やサービスを利用してクラウドサービス提供する場合に、機密保持契約等の順守に必要となる、裁判管轄や適用法に関する規定、損害賠償の約定、担保措置等の措置が講じられていることを事前に確認した上で、他国のクラウドサービス供給者との秘密保持契約、守秘義務契約の締結を行うこと。
15. 供給者関係				
	15.1 供給者関係における情報セキュリティ			
		15.1.1 供給者関係のための情報セキュリティの方針		

			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、情報セキュリティマネジメントに関する基本的な方針等に関し、情報セキュリティポリシー等の適用範囲と内容について明確にすること。また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必要な技術的仕様、サービスレベル、運用手順等について明確にすること。さらに、これらにつき、利用規約、SLA等で明記し、同意を行うことが可能なクラウドサービス供給者を選定すること。但し、データ連携等のため、特定のクラウドサービス供給者と個別の仕組みを新たに構築して対応する範囲に限っては、情報セキュリティポリシー等の適用範囲と内容、サービス提供に必要な技術的仕様、サービスレベル、運用手順等について当該供給者と調整し、明確にすることが求められる。
			b	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ついて、サービス提供における情報セキュリティマネジメントの要求事項に係る責任の所在を、当省に対して明確に示し、あるいは責任が分散している場合には、その旨を明示すること。
			c	受注者及びクラウドサービス供給者以外が提供するサービスを、当省がクラウドサービスと併せて利用する場合、受注者及びクラウドサービス供給者以外が提供するサービスに係る情報セキュリティマネジメント上の要求事項についての、当省の管理責任の範囲や受注者・クラウドサービス供給者の免責の範囲、運用方針等を明確にし、利用規約等を通じて当省の同意を得ること。
			d	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適用する証跡の記録・管理に関する方針等を明確に定めること。また、これについて、利用規約、SLA等で明記し、同意を行うことが可能な供給者を選定すること。さらに、クラウド事業者と供給者との間でのサービス接続において生じる証跡の記録等に係る管理責任等の範囲について、供給者が明示する規定を確認して同意し、これに基づいて自らの責任等の範囲を明確に定義した上で、必要な措置を講じること。 但し、データ連携等のため、特定のクラウドサービス供給者と個別の仕組みを新たに構築して対応する範囲に限っては、証跡の記録・管理に関する方針、及びサービス接続において生じる証跡の記録等に係る管理責任等の範囲について、当該供給者と調整し、明確にすることが求められる。
		15.1.3 ICTサプライチェーン		
			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、サービス継続に必要な情報セキュリティマネジメント要求事項に関し、供給者の利用規約、SLA等の規定によりその対応状況を確認し、全ての要求を満足できるクラウドサービス供給者を選定すること。但し、データ連携等のため、特定の供給者と個別の仕組みを新たに構築して対応する範囲に限っては、当該クラウドサービス供給者との間で調整・合意を行うことが求められる。
			b	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、受注者とクラウドサービス供給者の間でクラウドサービスの接続に関する情報セキュリティマネジメント上のリスクを明確にし、その管理策を具体的に定めること。 さらに、これらの管理策の実施に係る供給者の管理責任の内容・範囲及び役割について利用規約、SLA等で明記して同意できる供給者を選定し、その同意に基づいて自らの管理責任を定義すること。但し、データ連携等のため、特定の供給者と個別の仕組みを新たに構築して対応する範囲に限っては、当該クラウドサービス供給者との間で調整・合意を行うことが求められる。
	15.2 供給者のサービス提供の管理			
		15.2.1 供給者のサービス提供の監視及びレビュー		
			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、クラウドサービス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、受注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。
			b	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、受注者は、クラウドサービス供給者のサービスと連携する事項（データ、インターフェース等）について、情報セキュリティマネジメントに係る脆弱性を監視・レビューするとともに、クラウドサービス供給者において脆弱性が生じた場合でも、受注者が提供するサービスが被る影響を最小限とする措置を講じること。
			c	アグリゲーションサービス事業者は、提供するクラウドサービス全体についての監視、レビュー、監査実施に対する責任を果たすこと。但し、この責任は、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で代替が可能であり、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。
		15.2.2 供給者のサービス提供の変更に対する管理		
			a	アグリゲーションサービス事業者は、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、供給者が提供するサービスの変更に伴う影響範囲等について事前に把握し、他の供給者が提供するサービスに不測の障害等を生じないように、必要な情報を提供すること。
			b	アグリゲーションサービス事業者は、一部の供給者が行う変更に関する管理を行い、クラウドサービス全体として変更に伴う影響を最小限にするための対応策を講じること。
16. 情報セキュリティインシデント管理				
	16.1 情報セキュリティインシデントの管理及びその改善			
		16.1.2 情報セキュリティ事象の報告		
			a	ガバナンスの実態が異なる受注者とクラウドサービス供給者間で、クラウドサービス提供におけるそれぞれの管理責任等の範囲を明確に設定すること。
			b	受注者は、当省やクラウドサービス供給者に対しても、クラウドサービスにおける情報セキュリティ事象の速やかな報告手順とその連絡先を認識させておくこと。
			c	クラウドサービスにおける情報セキュリティ事象を、当省から受け付ける窓口を設置して周知し、情報セキュリティ事象に係る速やかな情報集約に努めること。
			d	ICTサプライチェーンの中で、情報セキュリティ事象の連絡を伝播させる連絡経路を、管理責任の分担と一体で明確にし、訓練によって正しく連絡を伝播できることを確認すること。
		16.1.4 情報セキュリティ事象の評価及び決定		

				番
			a	クラウドサービス提供における重大な情報セキュリティインシデントの明確な分類基準を定め、この基準を用いて情報セキュリティ事象を評価し、その事象を情報セキュリティインシデントに分類するかを決定すること。
			b	情報セキュリティインシデントへの分類の判断において、当省との間で認識の違いが生じると、情報提供に不満を感じる等の理由から、情報セキュリティインシデント対応に係る当省からの信頼感を阻害する恐れがあるため、分類基準を明確に定めることに加えて、必要に応じて当省とSLAを締結すること。
			c	情報セキュリティインシデントの形態、規模及び費用を定量化して監視できるようにする仕組みを備えること。また、この仕組みを活用し、情報セキュリティインシデントの分類基準の妥当性をレビューし、必要に応じて改善を加えること。
			d	情報セキュリティインシデントの事実関係、復旧/回復措置、復旧見込、影響範囲等の情報を、当省に提示すること。情報提供の方法については、「6.3.2 利用者接点とサプライチェーンにおける情報・共有」(h)に基づくこととし、情報提供のタイミングは、随時または一定間隔とすること。また、この方針に従って、必要に応じて当省とSLAを締結すること。
		16.1.7 証拠の収集		
			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。
			c	当省が行う証拠収集の制限事項について定義し、当省と合意すること。
			d	当省が、証拠として利用できる情報へのアクセスを要請し、その許諾を得るための手順をクラウド利用者と合意すること。このアクセスに費用や料金が発生する場合は、それを文書化して当省に示すこと。
			e	クラウドサービスにおいて、司法権を跨るデータ格納を行う場合は、各国の法制度を考慮するとともに、その情報を当省にも提供し、この情報に基づいて当省が自らデータ格納を行う国等を選択できる仕組みを提供すること。
17. 事業継続マネジメントにおける情報セキュリティの側面				
	17.2 冗長性			
		17.2.1 情報処理施設の可用性		
			a	ID管理サービス、課金サービスなどの基幹機能において、単一障害点となっているものを特定し、十分な冗長性と障害時の円滑な切替を確保すること。
			b	仮想化機能やサービス管理機能において、単一障害点となっている機能を特定し、十分な冗長化、障害時の円滑な切替、情報処理施設の管理単位分割等の対策を講じること。
			c	情報処理施設やネットワークにおいて、単一障害点となっている設備を特定し、十分な冗長性と障害時の円滑な切替を確保すること。
			d	障害の連鎖を食い止める防護機構を組み込むこと。
			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。
			f	広域災害の発生に際しては、クラウドサービスの継続を優先するか、情報セキュリティ対策の確保を優先するかについての方針を定め、当省の同意を得ること。
18. 順守				
	18.1 法的及び契約上の要求事項の順守			
		18.1.1 適用法令及び契約上の要求事項の特定		
			a	複数国のクラウド利用者に対してサービス提供を行う、または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受注者は、サービス対象や利用資源が越境することによってクラウドサービスに生じうる、適用法の違いによるリスクを事前に把握すること。
			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受注者は、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令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。
			c	当省が、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、当省の正確な判断を促進すること。
		18.1.2 知的財産		
			a	複数国のクラウド利用者に対してサービス提供する受注者は、クラウドサービス利用において供する当省の知的財産情報の権利に対し、国による知的財産保護法上の保護範囲の違いに起因して生じうるリスクを明らかにすること。
			b	複数国のクラウド利用者に対してサービス提供する受注者は、クラウドサービスの提供に当たって利用する知的財産権の取り扱いについて、複数国でサービス提供することによって生じるリスクを把握し、必要な対策を講じること。

			c	当省が、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、当省の正確な判断を促進すること。
		18.1.3 記録の保護		
			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受注者は、他国において自身またはクラウドサービス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受注者は、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、無関係な当省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。
		18.1.4 プライバシー及び個人を特定できる情報（PII）の保護		
			a	複数国のクラウド利用者に対してクラウドサービスを提供する受注者、あるいは複数国の資源・サービス等を利用する受注者は、クラウド利用者の資源が存在する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こと。
			b	当省が、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、当省の正確な判断を促進すること。
		18.1.5 暗号化機能に対する規制		
			a	複数国のクラウド利用者に対してクラウドサービスを提供するクラウド事業者、あるいは他国の資源、サービス等を利用する受注者は、当省や資源が存在する各国における暗号利用に係る法律上の必要性、あるいは制約等について把握し、クラウドサービスの提供に際しての必要な対策を講じること。
	18.2 情報セキュリティのレビュー			
		18.2.1 情報セキュリティの独立したレビュー		
			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、提供するサービスがクラウドサービス供給者が提供するサービス等に依存し、あるいは影響を受ける部分を有する場合には、クラウドサービス供給者が行う独立したレビュー・監査結果等を入手し、その結果を受注者が行う独立したレビュー・監査に反映させる等の措置を講じること。
			b	アグリゲーションサービス事業者は、供給者が行う独立したレビュー・監査の実施方針について把握し、必要な調整を行うことで、ICTサプライチェーン全体においてレビュー・監査等に係る一貫した方針の適用が必要な範囲を明確にし、これを適用するための措置を講じること。
		18.2.2 情報セキュリティのための方針群及び標準の順守		
			a	アグリゲーションサービス事業者は、供給者が行う情報セキュリティマネジメントのための方針群、標準類等の順守に係る定期的なレビュー結果を入手し、必要な調整を行うことで、ICTサプライチェーン全体において一貫した定期的レビューを行う範囲を明確にし、各供給者にこれを実施させるための措置を講じること。
		18.2.3 技術的順守のレビュー		
			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は、クラウドサービス供給者のサービス等に係る技術的な順守状況のレビュー結果等を入手する際に、機密的な内容が含まれる場合には、受注者とクラウドサービス供給者の間で機密保持契約の締結等、必要な措置を講じること。