付表

経済産業省
平成２３年度企業・個人の情報セキュリティ対策促進事業
（グローバルなクラウドセキュリティ監査の利用促進）

クラウドサービスにおけるリスクと管理策に関する有識者による検討結果 2011年度版

2012年8月

特定非営利活動法人　日本セキュリティ監査協会

● 本資料の構成

本書では、クラウドコンピューティングサービス（以下、「クラウドサービス」という。）において想定される典型的なリスクについて、どのような対策を講じるべきかをリスク毎に個別の表の形式で整理している。ここで示しているリスクの中には、目的によっては対策を講じる必要のないものも含まれており、クラウドサービスのユーザーは各表をもとに、対策を講じる必要があると判断した項目を選択の上、当該事項についての「対応するクラウド管理基準」を抽出することで、クラウドサービス事業者に対して、遵守すべき事項を提示することができる。

表の構成要素は以下の通りである。記載されている内容は、国内のクラウドサービス事業者及びユーザ企業、情報セキュリティベンダ、学識者で構成された有識者ワーキンググループによる検討結果を反映したものとなっている。

見出し項目	内　容
レイヤ	4ページに示すクラウドサービスの実装構造において、リスクとなる事象の発生する階層。 （ただし「サービス管理系」のみは階層横断的サービスに起因する事象を扱うための分類）
目指すべき水準	リスクに対してクラウドサービスが確保すべき情報セキュリティの水準。
想定されるリスク	クラウドサービスで発生するリスクを、以下の脅威と脆弱性の2種類に起因するものとして定義。
脅威	クラウドサービスに損害を与える可能性のある事象の潜在的な原因。外部からの攻撃のほか、自然災害、事業者における操作ミスや内部犯行なども含まれる。
脆弱性	脅威が損害をもたらすきっかけとなる、クラウドサービスの潜在的な弱点。なお、表において「V 数字」の形で示されているものは、[ENISA 09]におけるクラウドサービスの脆弱性として定義されているものであり、番号は同資料における脆弱性の整理番号に対応する。
クラウド事業者における対策の要点	クラウドサービス事業者が、リスクの影響を抑制するために実施すべき対策について、レイヤ毎にその要点を具体化したもの。
対応するクラウド管理基準	『クラウド情報セキュリティ管理基準』の項番と内容の抜粋。
残留リスク	上記管理基準に基づく対策を実施してもなお、クラウドサービスの提供を通じて存在するリスク。
備考	上記のいずれにも該当しない補足事項など。

参考文献

[ENISA 09]　"Cloud Computing – Benefits, risks and recommendations for information security", European Network and Information Security Agency, November 2009.
（日本語訳：『クラウドコンピューティング：情報セキュリティに関わる利点、リスクおよび推奨事項』, 独立行政法人情報処理推進機構, 2010）

● 本資料で扱うリスクの一覧

クラウドサービスのリスクを検討するにあたっては、調査時点での代表的な分析例として、前ページの[ENISA 09]の整理結果をもとに検討を行うこととした。しかしながら、同文献における分析は利用者の視点からリスクを整理しているのに対し、クラウド情報セキュリティ管理基準はクラウドサービス事業者の視点で整理する必要があることから、事業者視点での読み替えを実施している。具体的には、事業者の観点からはクラウドサービスにおける対策として考慮すべきでないもの（利用者視点ではクラウドサービスを使うか否か、といったより上位レイヤで判断されるもの）を除外するとともに、同文献では挙げられていないが、リスクとして重要と考えられるものを新たに追加した。さらに、リスクとしての重大性に応じて高（H）、中（M）、低（L）の3段階に分類し、次表のように整理した。

番号	リスクの識別名	リスクの具体的内容	[ENISA 09]との関係
H01	リソース・インフラの高集約によるインシデントの影響の拡大	・仮想化技術は、1台の物理ホストにn台の仮想マシンを集約することで、リソースの利用効率をn倍に高める一方、障害発生時の影響もn倍に拡大する。また、データセンタの大規模利用は、1か所のデータセンタに多数の利用者を収容することで、インフラの利用効率を高める一方、データセンタ内の障害発生時の影響も拡大する。例えば、データセンタ内のネットワークの設定ミスが、クラウドシステムの大半の機能を停止させ、大規模障害が発生するリスクがある。	（WGによる追加）
H02	仮想／物理の設計・運用の不整合	・仮想化技術は、キャパシティのオーバーサブスクリプションを可能にするため、仮想リソースの総和と物理リソースの総和は一致するとは限らない、ソフトウェアと物理ホストが一対一対応しない、 仮想スイッチと物理スイッチのVLAN設計が異なるなど、従来のコンピュータ、ネットワークの設計・運用管理のノウハウが通用しないことが多い。仮想/物理にまたがるコンピュータとネットワークの大規模化・複雑化によって、予期せぬ不具合、大規模障害が発生するリスクがある。	（WGによる追加）
H03	他の共同利用者の行為による信頼の喪失	・他のユーザの活動により、同じクラウドサービスを利用するユーザのIPアドレスが外部サービスによりブロックされる。 ・他のユーザの活動により、利用していたストレージが押収されてサービスの継続が困難になる。	ENISA No.4
H04	リソースの枯渇（リソース割当の過不足）	・クラウド事業者の予想を超えるユーザの需要増により、インフラやリソースがユーザの需要を満たせずサービスに支障が生ずることで、ユーザの減少や評判の低下を招く。 ・上記のリスクを回避するためにリソースを増強することで、場合によっては過剰投資として収益性を低下させる。	ENISA No.8
H05	隔離の失敗	・クラウドサービスを構成するメカニズムの不備・欠陥や脆弱性への攻撃により、異なるユーザやサービス間の隔離が失われることで、ユーザの機密情報の漏えいなどが生じ、事業者の評判が失墜する。	ENISA No.9
H06	サービスエンジンの侵害	・脆弱性等を通じてサービスエンジンの制御を奪われることで、クラウドサービスに特化した攻撃（サービスエンジン経由の情報漏えい、リソースの逼迫化によるサービスのマヒ等）が行われる可能性がある。	ENISA No.19
M07	クラウドプロバイダでの内部不正－特権の悪用	・クラウド事業者における従業員の悪意の行動が、あらゆるクラウドサービスに影響を及ぼす。 ・従業員が犯罪組織の標的とされ、上記の行動を行う。	ENISA No.10
M08	管理用インターフェースの悪用（操作、インフラストラクチャアクセス）	・クラウドサービスのユーザ向けに、インターネットからリソース制御を可能とするインタフェースが悪用され、サービス全体に影響を及ぼす。 ・クラウド事業者の管理者の制御用インタフェースも同様に悪用されることで、さらなる影響を及ぼす。	ENISA No.11
M09	データ転送途上における攻撃、データ漏えい（アップロード時、ダウンロード時、クラウド間転送）	・ユーザ環境とクラウドサービス、もしくは分散されたクラウドサービス相互間でのデータ転送機会が生ずることで、その転送中のデータの漏えいのリスクが生じる。	ENISA No.12, ENISA No.13

番号	リスクの識別名	リスクの具体的内容	[ENISA 09]との関係
M10	セキュリティが確保されていない、または不完全なデータ削除	・ストレージやバックアップテープ等の物理媒体をを他のユーザと共用する場合、媒体には常時複数ユーザのデータが記録されるため、特定ユーザのデータだけを消去する目的で、その媒体を物理的に破壊することはできない。	ENISA No.14
M11	クラウド内DDoS/DoS攻撃	・悪意のユーザもしくはユーザ環境の乗っ取り等を通じて同じクラウドサービス内を起点とするDDoS/DoS攻撃が行われることで、インターネット経由の場合よりも大きな被害がユーザに発生する。	ENISA No.15
L12	ロックインによるユーザの忌避	・クラウドプロバイダが、外部リソースを利用してユーザデータを保護する必要性が生じても、相互接続性がないために、データ移行ができない。 （注）本リスクはENISAではユーザにとっての「ロックインされてしまう」リスクとして整理されているが、ここではクラウド事業者視点で扱う。	ENISA No.1
L13	ガバナンスの喪失	・クラウドを利用することで、ユーザが下位層を対象としたガバナンス（自社ポリシーに基づくアクセス制御、ログ管理、監査実施等）を失うことのリスクを憂慮し、クラウド利用を躊躇する。 （注）本リスクはENISAではユーザにとっての「ロックインされてしまう」リスクとして整理されているが、ここではクラウド事業者視点で扱っている。	ENISA No.2
L14	サプライチェーンにおける障害	・クラウドサービスにおける認証等のサービスを外部委託することで、その委託先サービスに脆弱性が存在するとクラウドサービス全体に影響が及ぶ可能性がある。 ・どの部分を外部委託しているかを明示しないことで、ユーザによるクラウドサービスへの信頼度が低下する。	ENISA No.7
L15	EDoS攻撃（経済的な損失を狙ったサービス運用妨害攻撃）	・悪意のユーザによるユーザアカウントの乗っ取り、従量制リソースの浪費等を通じて、ユーザに経済的損失をもたらす。 （注）ENISAガイドラインにない追記： 同様の被害は、ユーザの過失（プログラムの欠陥、設計ミス）によっても生じる可能性がある。	ENISA No.16
L16	事業者が管理すべき暗号鍵の喪失	・悪意の関係者により、クラウド事業者が管理すべき暗号鍵が不正利用されることで、ユーザの機密データの漏えいが生ずる。 ・クラウド事業者が暗号鍵を喪失することでデータの復号が困難となり、ユーザのデータにおける完全性が損なわれる。	ENISA No.17
L17	不正な探査・スキャンの実施	・攻撃のためのデータ収集が、クラウドサービスの環境を通じて、より容易に行われる可能性がある。	ENISA No.18
L18	証拠提出命令と電子的証拠開示	・クラウドサービス上にデータが集中することで、司法当局によるデータの押収が行われた場合に、開示したくないデータまで開示されるリスクが増大するため、ユーザによるクラウドサービス利用を躊躇させる要因となる可能性がある。	ENISA No.21
L19	司法権の違い	・クラウドサービスの物理的インフラが設置される地域（国、州など）によっては、異なる司法上の解釈や独裁的な警察権力、国際的取り決めが遵守されないなどの影響がユーザに及ぶ可能性がある。	ENISA No.22
L20	データ保護	・クラウドサービス事業者が、ユーザが許可していないデータの処理を行う可能性があることで、ユーザがクラウド利用を躊躇する可能性がある。 ・ユーザが合法的でない方法で収集したデータが、クラウドサービス上に蓄積される可能性がある。	ENISA No.23
L21	ライセンス	・同一期間内に同じ数のマシンを使用していた場合でも、他のソフトウェアに比べてクラウド利用者のライセンス費用は飛躍的に増大することがある。 ・PaaSやIaaSの場合は、クラウド内部で発生した独自の成果物（新しいアプリケーションやソフトウェア等）がユーザの知的財産として保護されない可能性がある。	ENISA No.24

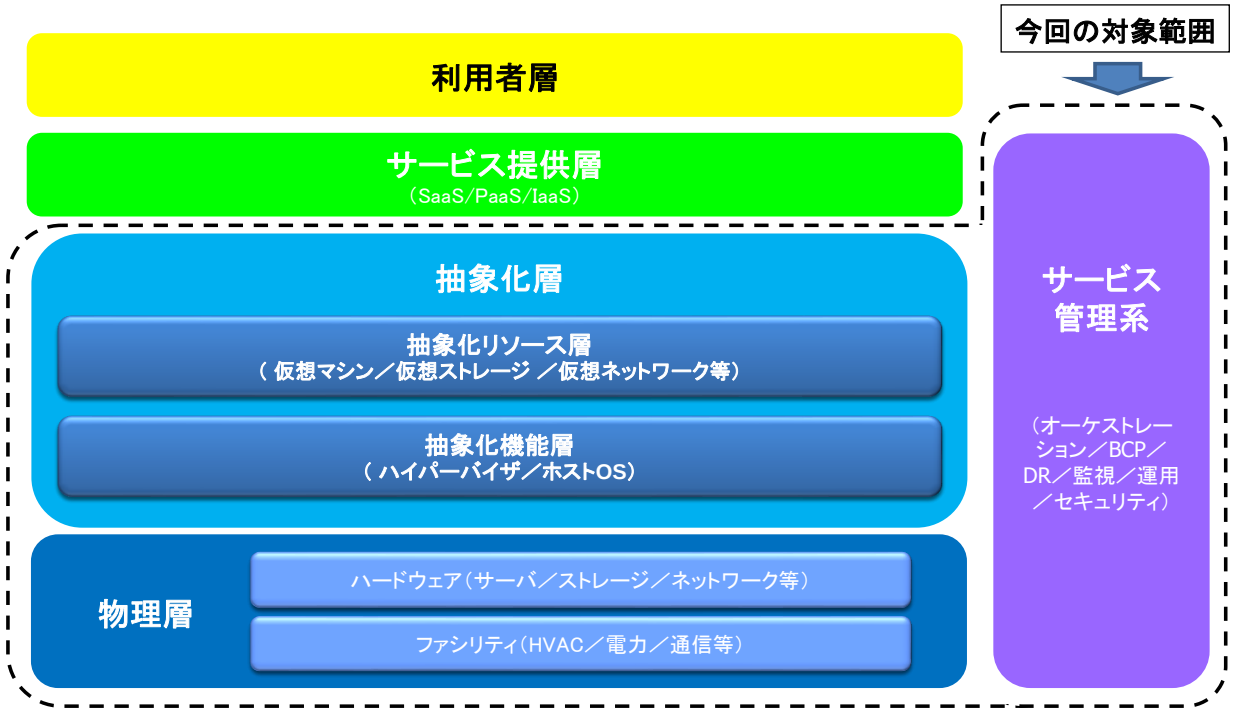
● クラウドサービスにおけるレイヤ構造のモデル

クラウドサービスにおけるリスクとその対策を論じ、クラウド情報セキュリティ管理基準を作成するにあたっては、「どの条件」における「どのようなリスク」に対するものかを明確にすることが議論を整理する上で重要である。そこで、クラウドサービスを構成するレイヤを下図のように定義し、これをもとにリスクを整理している。レイヤ構造の定義に際しては、ITU-Tで検討されているクラウドサービスに関する参照構造との対応関係が容易に確保できることを考慮している。

● スコープの設定

本書では、下図において「今回の検討範囲」として点線で囲んだ範囲を検討対象としている。このような範囲を設定した理由は以下の通りである。

- 上位層（利用者層、サービス提供層）はサービス毎にリスクや条件が異なり、共通の管理策を検討することが困難。
- クラウドサービスに固有のリスクは、物理層から抽象化層およびサービス管理系で発生する技術的リスクが主体。
- 対策の有効性は下層の状況に依存する場合が多いため、最下位層（物理層）からの検討が必要。



H01： リソース・インフラの高集約によるインシデントの影響の拡大

・仮想化技術は、1台の物理ホストにn台の仮想マシンを集約することで、リソースの利用効率をn倍に高める一方、障害発生時の影響もn倍に拡大する。また、データセンタの大規模利用は、1か所のデータセンタに多数の利用者を収容することで、インフラの利用効率を高める一方、データセンタ内の障害発生時の影響も拡大する。例えば、データセンタ内のネットワークの設定ミスが、クラウドシステムの大半の機能を停止させ、大規模障害が発生するリスクがある。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	－	－	－	－	－	－	
	機能層	一部の障害・一地域の災害が大規模なサービス停止を招かないこと	・バグ ・設計・構築ミス ・運用（設定・保守・故障対応など）ミス	事象が連鎖し得る構造・機能（些細な事象が連鎖的に他の事象を惹き起こし、大事に至る。例えば、ネットワークの設定変更ミスが契機となり、一斉に多くの仮想マシンが移転先のリソース検索を開始し、空きリソースが見つからなかった大半の仮想マシンがロックされ、大規模なサービス停止に至るなど）	障害の大規模化を防ぐため、クラウドシステム内の障害の連鎖を止める	6.3.2.2 新しいシステムを受け入れるための要求事項及び基準を明確に定義し、合意し、文書化し、試験することを確実にする仕組みを整備する 6.3.2.3 新しいシステムを受け入れるための要求事項及び基準には、些細な事象が他の事象を惹き起こし、クラウドサービスの大部分の停止に至るような事象の連鎖を抑止する仕組みがあることを含める 6.3.2.18 すべての受入れ基準が完全に満たされていることを確認するための適切な試験には、実際のサービス利用条件に近い環境で行う異常時の動作試験を含み、些細な事象が連鎖的に他の事象を惹き起こし、クラウドサービスの大部分の停止に至ることがないか確認する	想定できない異常の出現	
				単一障害点（その箇所が停止するとシステムの大部分が停止するような箇所）	クラウドサービスの全面的な停止を防ぐため、クラウドシステムを複数に分割する	C.2.1.2　一部の仮想化機能（仮想マシンモニタ、仮想化ストレージエンジン、仮想スイッチなど）の不具合がクラウドサービスを全面的に停止させないために、仮想化機能の及ぶ情報処理設備を複数に分けて仮想化する	多数同時障害	
物理層			・故障 ・設計・構築ミス ・運用（設定・保守・故障対応など）ミス		クラウドサービスを停止させないため、クラウドシステムを冗長化する	6.6.1.16 停止が許容できないシステムの場合、ネットワークを冗長化する C.1.1.1　一部の情報処理設備（物理サーバ、物理ストレージ、物理ネットワーク機器、通信ケーブル、アクセス回線など）の機能の喪失がクラウドサービスを停止させないために、情報処理設備を冗長化する	冗長部の同時障害	
					クラウドサービスの全面的な停止を防ぐため、クラウドシステムを複数に分割する	C.2.1.1　一部の情報処理設備（物理サーバ、物理ストレージ、物理ネットワーク機器、通信ケーブル、アクセス回線など）の機能の喪失がクラウドサービスを全面的に停止させないために、複数の情報処理設備に分けて設置する	多数同時障害	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
物理層	一部の障害・一地域の災害が大規模なサービス停止を招かないこと	災害	単一地域への設置	クラウドサービスの全面的な停止を防ぐため、データセンタを地理的に離れた複数の地域に設ける	C.2.1.4　一地域の災害がクラウドサービスを全面的に停止させないために、地理的に離れた複数の地域に設備を設ける	・複数地域同時災害 ・超広域災害	
				クラウドシステムを保護するため、データセンタの災害対策を行う	5.2.1.5 装置を保護するために、潜在的な物理的脅威（例えば、盗難、火災、爆発、ばい（煤）煙、水（又は給水の不具合）、じんあい（塵埃）、振動、化学的汚染、電力供給の妨害、通信妨害、電磁波放射、破壊）のリスクを最小限に抑えるための管理策を採用する 5.2.1.8 装置を保護するために、すべての建物に、落雷からの保護手段を適用する。すべての電力及び通信の引込線に避雷器を装着する 5.2.1.9　装置を保護するために、すべての建物は、震度階7においても建物の一部崩壊・全体崩壊なしの耐震構造とする 5.2.1.10 装置を保護するために、すべての建物に、防水壁、排水設備を設置する 5.2.1.11 装置を保護するために、すべての建物は、危険物貯蔵施設の近辺など火災発生の危険性が高い地域を避けて建設する 5.2.1.12 装置を保護するために、すべての建物に、防火塀の設置、防火植樹を実施する 5.1.4.1 隣接する施設からもたらされるセキュリティ脅威（例えば、隣接建物の火災、屋根からの漏水、地下室の浸水、街路での爆発）から保護する 5.2.2.4 重要な業務の運用をサポートする装置には、定められた手順での運転停止又は連続運転をサポートする、無停電電源装置（UPS）を設置する 5.2.2.5 電力についての緊急時対応計画には、無停電電源装置（UPS）が故障した場合のとるべき処置についても含める 5.2.2.6 長時間にわたる停電の場合でも処理の継続が要求される場合には、非常用発電機を導入する。また、非常用発電機の長時間運転を確実にするために、十分な燃料供給を確保する 5.2.2.7 無停電電源装置（UPS）及び非常用発電機を、十分な能力を保有していることを確実にするために定期的に点検し、装置の製造者の推奨に従って試験する 5.2.2.8 複数の電源又は事業所の規模が大きい場合には、別の変電設備を利用する 5.2.3.7 取扱いに慎重を要する、又は重要なシステムは、適切なセキュリティを提供する代替経路及び／又は伝送媒体を利用する	想定できない規模の災害の発生	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	一部の障害・一地域の災害が大規模なサービス停止を招かないこと	・バグ ・機能の喪失 ・設計・構築ミス ・運用（設定・保守・機能の喪失対応など）ミス ・災害	事象が連鎖し得る構造・機能（些細な事象が連鎖的に他の事象を惹き起こし、大事に至る。例えば、ネットワークの設定変更ミスが契機となり、一斉に多くの仮想マシンが移転先のリソース検索を開始し、空きリソースが見つからなかった大半の仮想マシンがロックされ、大規模なサービス停止に至るなど）	障害の大規模化を防ぐため、クラウドシステム内の障害の連鎖を止める	6.3.2.2 新しいシステムを受け入れるための要求事項及び基準を明確に定義し、合意し、文書化し、試験することを確実にする仕組みを整備する 6.3.2.3 新しいシステムを受け入れるための要求事項及び基準には、些細な事象が他の事象を惹き起こし、クラウドサービスの大部分の停止に至るような事象の連鎖を抑止する仕組みがあることを含める 6.3.2.18 すべての受入れ基準が完全に満たされていることを確認するための適切な試験には、実際のサービス利用条件に近い環境で行う異常時の動作試験を含み、些細な事象が連鎖的に他の事象を惹き起こし、クラウドサービスの大部分の停止に至ることがないか確認する	想定できない異常の出現	
			単一障害点（その箇所が停止するとシステムの大部分が停止するような箇所）	クラウドサービスの全面的な停止を防ぐため、クラウドシステムを複数に分割する	C.2.1.3　一部の管理機能（クラウドコントローラ、クラウドサービスマネージャなど）の喪失がクラウドサービスを全面的に停止させないために、管理機能の及ぶ情報処理設備を複数に分けて管理する	多数同時障害	
				クラウドサービスを停止させないため、クラウドシステムを冗長化する	C.1.1.2　一部の管理機能（クラウドコントローラ、クラウドサービスマネージャなど）の喪失がクラウドサービスを停止させないために、管理機能を提供する情報処理設備を冗長化する	・冗長部の同時障害 ・代替地域の同時災害	
				クラウドサービスを停止させないため、障害発生時には速やかに冗長系に切替える	C.1.1.3　一部の情報処理設備（物理サーバ、物理ストレージ、物理ネットワーク機器、通信ケーブル、アクセス回線など）の機能の喪失がクラウドサービスを停止させないために、代替の情報処理設備に速やかに切替える（ライブマイグレーション、フェイルオーバーなど） C.1.1.4　一部の管理機能（クラウドコントローラ、クラウドサービスマネージャなど）の喪失がクラウドサービスを停止させないために、代替の管理機能を提供する情報処理設備に速やかに切替える C.1.1.5　一部の物理媒体の機能の喪失がクラウドサービスを停止させないために、代替の物理媒体に速やかに切替え、機能を喪失した媒体に記録されていたデータを復旧する。 C.1.1.6　一部地域の災害がクラウドサービスを停止させないために、代替地域のデータセンタに設置した情報処理設備に速やかに切替える 5.2.2.8 複数の電源又は事業所の規模が大きい場合には、別の変電設備を利用する 5.2.3.7 取扱いに慎重を要する、又は重要なシステムは、適切なセキュリティを提供する代替経路及び／又は伝送媒体を利用する		

H02：仮想／物理の設計・運用の不整合

・仮想化技術は、キャパシティのオーバーサブスクリプションを可能にするため、仮想リソースの総和と物理リソースの総和は一致するとは限らない、ソフトウェアと物理ホストが一対一対応しない、仮想スイッチと物理スイッチのVLAN設計が異なるなど、従来のコンピュータ、ネットワークの設計・運用管理のノウハウが通用しないことが多い。仮想/物理にまたがるコンピュータとネットワークの大規模化・複雑化によって、予期せぬ不具合、大規模障害が発生するリスクがある。

<table>
<tr><th colspan="2" rowspan="2">レイヤ</th><th rowspan="2">目指すべき水準</th><th colspan="2">想定されるリスク</th><th rowspan="2">クラウド事業者における
対策の要点</th><th rowspan="2">対応するクラウド管理基準</th><th rowspan="2">残留リスク</th><th rowspan="2">備考</th></tr>
<tr><th>脅威</th><th>脆弱性</th></tr>
<tr><td rowspan="3">抽象化層</td><td>リソース層</td><td>－</td><td>－</td><td>－</td><td>－</td><td>－</td><td>－</td><td></td></tr>
<tr><td>機能層</td><td rowspan="2">注意をしていても設計・構築・運用ミスを招きかねない、複雑さがないこと</td><td rowspan="2">・設計・構築ミス
・運用（設定・保守・故障対応など）ミス</td><td>設定可能な仮想リソースの制約に対応するための複雑なサーバ設計・運用（物理マシンよりも規模の小さな仮想マシンしか設定できないことから、複数の仮想マシンを組合せて負荷分散するなど、設計・運用が複雑になるなど）</td><td rowspan="2">設計・構築・運用時のミスを防ぐため、物理構成と論理構成の対応関係の理解がしやすいシステムにする</td><td rowspan="2">6.3.2.2 新しいシステムを受け入れるための要求事項及び基準を明確に定義し、合意し、文書化し、試験することを確実にする仕組みを整備する
6.3.2.4 新しいシステムを受け入れるための要求事項及び基準には、物理構成と論理構成の対応の複雑性を十分に軽減することを含める</td><td rowspan="2">不注意による誤り</td><td></td></tr>
<tr><td colspan="2">物理層</td><td>物理ネットワーク機器のVLAN設定数の制約に対応するための複雑なネットワークの設計・運用（必要な仮想ネットワーク数を物理ネットワーク機器に設定できないことから、設計・運用が複雑になるなど）</td><td></td></tr>
</table>

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	注意をしていても設計・構築・運用ミスを招きかねない、管理の過大な負担や複雑さがないこと	・設計・構築ミス ・運用（設定・保守・故障対応など）ミス	・仮想リソースの構成が可視化されない ・仮想/物理システムの管理方法の違い（物理リソースと仮想リソースの管理ツール・インタフェースが異なる）	運用時のミスを防ぐため、物理構成と論理構成を対応づけて管理する	6.1.1.3 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、物理構成と論理構成の対応関係、情報の処理及び取扱いを含む、各作業の詳細な実施に関する指示を明記する 6.1.1.12 情報システムは、ツール及びユーティリティを用いて、物理構成と論理構成の首尾一貫した管理を行う 8.4.1.8 導入したソフトウェア（仮想化ソフトウェアを含む）の管理を維持するために、システムに関する文書化と同様に、構成管理システムを利用する	不注意による誤り	
			物理リソースを超える仮想リソースの設定（物理マシンのリソースを超過した仮想リソースの使用）	運用時のミスを防ぐため、物理リソースと仮想リソースの適切な対応関係を把握して、リソースを管理する	6.3.1.5 論理資源の総和が物理資源を超過するような資源の割り当ては、物理資源の最繁時の同時使用率を考慮して行う 6.3.1.6 入手に時間又は費用がかかる資源については、特別な注意を要するため、管理者は、主要なシステム資源（クラウドサービスの提供にかかわる資源及びクラウドサービスを提供する資源を含む。）の使用を監視し、全体の容量・能力の限界値及びクラウド利用者に割り当てられる容量・能力の限界値を把握する 6.3.1.7 管理者は、使用の傾向、特にクラウドサービスを提供する仮想化・分散処理ソフトウェア、その他業務用ソフトウェア又は情報システムの管理ツールに関連した傾向を識別する 6.3.1.10 管理者は、システムセキュリティ又はサービスに脅威をもたらすおそれのある、潜在的な障害及び主要な要員への依存度合いを特定し回避するために、上記の監視及び識別の情報を利用して、適切な処置を立案する 6.3.1.11 容量及び能力が設計時の想定を超えた場合の対応手順（仮想マシン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など）を作成する		
			物理ストレージと仮想マシンのバックアップ・リストア単位の違い（物理ストレージのボリューム単位で取得したバックアップから特定の仮想マシンイメージをリストアするには、目的外の仮想マシンイメージまで一括してリストアの対象とされる）	運用時のミスを防ぐため、物理ストレージと仮想マシンのバックアップ・リストアの単位の違いを把握して、管理する	6.5.1.5 バックアップ及びデータ復旧の手順は、物理ストレージと仮想マシンのバックアップの単位や方法の違いを考慮して決定する		

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	注意をしていても設計・構築・運用ミスを招きかねない、管理の過大な負担や複雑さがないこと	・設計・構築ミス ・運用（設定・保守・故障対応など）ミス	仮想/物理ネットワーク設定の複雑化と負担の増大（リソースを柔軟に組合せた最適化が難しい、国や地域の異なるデータセンタをまたがった広域仮想ネットワークの設定が難しいなど）	設計・構築・運用時のミスを防ぐため、物理ネットワークと論理ネットワークの制御の仕組みを一元化して管理する	6.6.1.8 ネットワークの設計、構築及び運用における管理者の誤りの発生を最小限に抑えるため、仮想ネットワークと物理ネットワークの経路制御の仕組みを可能な限り一元化し、複数の物理ネットワーク機器及び仮想スイッチなどの設定を一斉かつ確実に実行する仕組みを整備する	不注意による誤り	
			仮想/物理ネットワークの動的な経路変更方法の違い（VMのマイグレーションに応じた動的な設定変更を物理ネットワークに自動的かつ迅速に実行できない）	運用時のミスを防ぐため、物理ネットワークと論理ネットワークの制御を同期させ、自動化する	6.6.1.9 ネットワークの設計、構築及び運用における管理者の誤りの発生を最小限に抑えるため、仮想マシンのライブマイグレーションに合わせて、複数の物理ネットワーク機器及び仮想スイッチなどの設定を自動的に実行する仕組みを整備する		
			サーバ管理とネットワーク管理の責任分界の曖昧化（VMMがサーバだけでなく、サーバ内の仮想ネットワークを管理するため、従来のサーバ/ネットワークの区分が通用しない）	設計・構築・運用時のミスを防ぐため、サーバ管理とネットワーク管理の責任分担や管理の仕組みを見直す	9.2.1.24 サーバ管理とネットワーク管理の責任分界を明確にするため、仮想スイッチの機能を物理サーバから物理ネットワーク機器に移す仕組みを整備する 9.2.1.25 サーバ管理とネットワーク管理の責任分界を明確にできない場合には、サーバ管理とネットワーク管理の一体運営又は相互連携を図る仕組みを整備する		

H03： 他の共同利用者の行為による信頼の喪失

・他のユーザの活動により、同じクラウドサービスを利用するユーザのIPアドレスが外部サービスによりブロックされる。
・他のユーザの活動により、利用していたストレージが押収されてサービスの継続が困難になる。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	リソースが分割可能な状態で運用されること	・複数のユーザが登録されたIPアドレスレンジの広域ブロック（不正や迷惑行為を行う送信者のIPアドレスが含まれる一定範囲のネットワークを、被害を受けた受信者がまとめてブロックする） ・複数のユーザが共同利用する記録媒体の押収（犯罪の証拠となる電磁的記録を押収するため、その記録を含む媒体全部を、捜査機関が押収する）	V6 リソース分離の欠如	ユーザのリソースを論理的に識別するため、同一のIPアドレスを複数のユーザと共同利用させない	6.6.2.5 クラウドサービスに含まれ提供されるすべてのネットワークサービスに必要なセキュリティについての取決め（例えば、セキュリティ特性、サービスレベル、管理上の要求事項）を特定し、クラウド利用者と合意する	同一レンジに含まれる複数のIPアドレスを複数のユーザに割り当てる（同一レンジを一ユーザが独占できない）	
					ユーザのリソースを論理的に識別するため、同一の論理ボリュームを複数のユーザと共同利用させない	6.6.2.5 クラウドサービスに含まれ提供されるすべてのネットワークサービスに必要なセキュリティについての取決め（例えば、セキュリティ特性、サービスレベル、管理上の要求事項）を特定し、クラウド利用者と合意する	なし	
	機能層	サービスを提供するリソースを必要に応じて分割し、特定のユーザによる影響を局所的に限定する機能が提供され、適切に運用されること		V5 ハイパーバイザの脆弱性	ハイパーバイザの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える。	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。）	・ゼロディの脆弱性への攻撃 ・不正発見の前の損害	

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	機能層	サービスを提供するリソースを必要に応じて分割し、特定のユーザによる影響を局所的に限定する機能が提供され、適切に運用されること	・複数のユーザが登録されたIPアドレスレンジの広域ブロック（不正や迷惑行為を行う送信者のIPアドレスが含まれる一定範囲のネットワークを、被害を受けた受信者がまとめてブロックする） ・複数のユーザが共同利用する記録媒体の押収（犯罪の証拠となる電磁的記録を押収するため、その記録を含む媒体全部を、捜査機関が押収する）	V5 ハイパーバイザの脆弱性	ハイパーバイザの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える。	8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	・ゼロディの脆弱性への攻撃 ・不正発見の前の損害	
				V6 リソース分離の欠如	複数のユーザが登録されたIPアドレスレンジの広域ブロックによる被害を少なくするため、特定ユーザに割り当てたIPアドレスからの送信を規制し、外部への不正や迷惑行為を防止する。	6.6.1.5 公衆ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及び業務用ソフトウェアを保護するために、特別な管理策（受信規制又は発信規制を含む）を確立する 6.6.1.10 ネットワーク上の機器では、アクセス制御方針に基づき、すべてのネットワークインタフェースでアクセス制御（受信規制又は発信規制を含む）を実施する	発信規制の前の損害	
					複数のユーザが共同利用する物理媒体の押収によって、犯罪と無関係なユーザが影響を受けるのを防ぐため、特定ユーザの記憶領域だけを独立した媒体に記録する仕組みを設ける	6.5.1.5 バックアップの範囲（例えば、フルバックアップ、差分バックアップ）及びバックアップの頻度は、組織の業務上の要求事項、関連する情報のセキュリティ要求事項及びその情報の組織の事業継続に対しての重要度を考慮して決定する 6.5.1.7 バックアップの単位（例えば、データ単位、論理ボリューム単位、ユーザ単位など）ごとに独立した媒体にバックアップを取得する仕組みを備える	複製が記録された媒体が、複数のユーザのデータを記録する	
物理層					複数のユーザが登録されたIPアドレスレンジの広域ブロックによる被害を少なくするため、特定ユーザに割り当てたIPアドレスからの送信を規制し、外部への不正や迷惑行為を防止する。	6.6.1.5 公衆ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及び業務用ソフトウェアを保護するために、特別な管理策（受信規制又は発信規制を含む）を確立する 6.6.1.10 ネットワーク上の機器では、アクセス制御方針に基づき、すべてのネットワークインタフェースでアクセス制御（受信規制又は発信規制を含む）を実施する	発信規制の前の損害	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	他のユーザに不利益をもたらすような活動を行うユーザを早期に検出できる仕組みが提供され、適切に運用されること	・複数のユーザが登録されたIPアドレスレンジの広域ブロック（不正や迷惑行為を行う送信者のIPアドレスが含まれる一定範囲のネットワークを、被害を受けた受信者がまとめてブロックする） ・複数のユーザが共同利用する記録媒体の押収（犯罪の証拠となる電磁的記録を押収するため、その記録を含む媒体全部を、捜査機関が押収する）	V6 リソース分離の欠如	複数のユーザが登録されたIPアドレスレンジの広域ブロックによる被害を少なくするため、クラウド内からの不正や迷惑行為を迅速に検知し、その行為を阻止すると共に、その行為者を識別し管理できるようにする	6.6.1.5 公衆ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及び業務用ソフトウェアを保護するために、特別な管理策（受信規制又は発信規制を含む）を確立する 6.6.1.6 セキュリティに関連した活動を記録できるように、適切なログ取得及び監視を適用する 6.6.1.10 ネットワーク上の機器では、アクセス制御方針に基づき、すべてのネットワークインタフェースでアクセス制御（受信規制又は発信規制を含む）を実施する 6.6.1.14 ネットワーク上の不正なイベントを監視するため、侵入検知システムを導入する 6.6.1.15 侵入検知システムが、常に最新の攻撃・不正アクセスに対応可能なように、定義ファイル、検知ルールなどの更新を実施する	広域ブロックの規制解除の最終判断を行う受信者の判断ミス	
				複数のユーザが共同利用する記録媒体の押収による、犯罪と無関係なユーザへの影響を防ぐため、特定ユーザの記憶領域だけを独立した媒体に記録する仕組みを設ける	6.5.1.6 バックアップの範囲（例えば、フルバックアップ、差分バックアップ）及びバックアップの頻度は、組織の業務上の要求事項、関連する情報のセキュリティ要求事項及びその情報の組織の事業継続に対しての重要度を考慮して決定する 6.5.1.7 バックアップの単位（例えば、データ単位、論理ボリューム単位、ユーザ単位など）ごとに独立した媒体にバックアップを取得する仕組みを備える	押収する対象の最終判断を行う捜査機関の判断ミス	

H04: リソースの枯渇(リソース割当の過不足)

・クラウド事業者の予想を超えるユーザの需要増により、インフラやリソースがユーザの需要を満たせずサービスに支障が生ずることで、ユーザの減少や評判の低下を招く。
・上記のリスクを回避するためにリソースを増強することで、場合によっては過剰投資として収益性を低下させる。

<table>
<tr><th colspan="2" rowspan="2">レイヤ</th><th rowspan="2">目指すべき水準</th><th colspan="2">想定されるリスク</th><th rowspan="2">クラウド事業者における
対策の要点</th><th rowspan="2">対応するクラウド管理基準</th><th rowspan="2">残留リスク</th><th rowspan="2">備考</th></tr>
<tr><th>脅威</th><th>脆弱性</th></tr>
<tr><td rowspan="4">抽象化層</td><td>リソース層</td><td>サービス提供の可能な範囲で、ユーザが要求する論理リソースを設定できること</td><td>非効率なリソース配分</td><td>V27 クラウドのインフラに対する投資またはリソース割当の不足</td><td>リソース使用の統計多重効果を出すため、物理リソースの限界を超えた論理リソースの総和を設定する</td><td>6.3.1.5 論理資源の総和が物理資源を超過するような資源の割り当ては、物理資源の最繁時の同時使用率を考慮して行う</td><td rowspan="4">複合要因(災害等)によるシステム障害および需要増がもたらすリソースの枯渇</td><td></td></tr>
<tr><td rowspan="3">機能層</td><td rowspan="3">ユーザのニーズと物理的制約を全体最適化して、有効かつ公平にリソースを配分すること</td><td rowspan="3">同一装置を共有するユーザ間の使用率の偏り及び装置間又は拠点間の使用率の偏り</td><td rowspan="2">V15 リソースの使用に関する不正確なモデリング</td><td>リソース使用の統計多重効果を出すため、ユーザ別のプロセスやトラフィックのスケジューリングを適切に行う。</td><td>6.3.1.8 物理資源を複数のクラウド利用者で共有する論理資源の割当ては、クラウド利用者の特性に合わせた適切なアルゴリズムにより行う</td><td></td></tr>
<tr><td>装置間又は拠点間の使用率の偏りを防ぐため、仮想資源の適切な再配置を行う。</td><td>6.3.1.11 容量及び能力が設計時の想定を超えた場合の対応手順(仮想マシン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など)を作成する</td><td></td></tr>
<tr><td>V.28 リソースの利用上限制限ポリシーの欠如</td><td>ユーザ間の利用の公平を図るため、ユーザごとに使用率の最高値や最低保証値を設ける。</td><td>6.3.1.9 物理資源を複数のクラウド利用者で共有する論理資源の使用は、クラウド利用者が使用可能な最大値や最低値を定め適切に制限を行う</td><td></td></tr>
<tr><td colspan="2">物理層</td><td>ユーザのニーズを満たした物理リソースの安定供給</td><td>物理リソースの総量の不足</td><td>V27 クラウドのインフラに対する投資またはリソース割当の不足</td><td>増設の遅れなどによる物理的な限界が生じることを防ぐため、需要予測を行い適切に設備投資を行う。</td><td>6.3.1.1 新規及び現在進行中の活動(クラウドサービスの提供にかかわる活動を含む。)のために、容量・能力に関する要求事項を特定する
6.3.1.2 システム(クラウドサービスの提供にかかわるシステム及びクラウドサービスを提供するシステムを含む。)の可用性及び効率性を確実にするため、また、必要な場合には、改善のために、システム調整及び監視を適用する
6.3.1.3 適切な時点で問題を知らせるために、探知のための管理策を備える
6.3.1.6 入手に時間又は費用がかかる資源については、特別な注意を要するため、管理者は、主要なシステム資源(クラウドサービスの提供にかかわる資源及びクラウドサービスを提供する資源を含む。)の使用を監視し、全体の容量・能力の限界値及びクラウド利用者に割り当てられる容量・能力の限界値を把握する</td><td></td></tr>
</table>

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	ユーザのニーズと物理的制約を全体最適化して、有効かつ公平にリソースを配分すること	同一装置を共有するユーザ間の使用率の偏り及び装置間又は拠点間の使用率の偏り	V15 リソースの使用に関する不正確なモデリング	リソース使用の統計多重効果を出すため、ユーザ別のプロセスやトラフィックのスケジューリングを適切に行う。	6.3.1.8 物理資源を複数のクラウド利用者で共有する論理資源の割当ては、クラウド利用者の特性に合わせた適切なアルゴリズムにより行う	複合要因(災害等)によるシステム障害および需要増がもたらすリソースの枯渇	
				装置間又は拠点間の使用率の偏りを防ぐため、仮想資源の適切な再配置を行う。	6.3.1.11 容量及び能力が設計時の想定を超えた場合の対応手順(仮想マシン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など)を作成する		
			V.28 リソースの利用上限制限ポリシーの欠如	ユーザ間の利用の公平を図るため、ユーザごとに使用率の最高値や最低保証値を設ける。	6.3.1.9 物理資源を複数のクラウド利用者で共有する論理資源の使用は、クラウド利用者が使用可能な最大値や最低値を定め適切に制限を行う		
	サービス管理に必要な最低限のリソースを確保すること	ユーザ使用の過負荷による管理用リソースの圧迫(ユーザに論理リソースを提供する物理資源であっても、そのリソースの一部を管理のために使用せざるを得ない。例えば、管理プロセスを動かすCPU、メモリ、ネットワークなど。ユーザ使用の増大によって、管理リソースが確保できなくなることがある)	V.28 リソースの利用上限制限ポリシーの欠如	ユーザサービス用のリソースとは別に、管理用のリソースを確保する。	7.6.2.3 取扱いに慎重を要する業務用ソフトウェアを共有環境で用いる場合、そのシステムの管理者は、資源とリスクを共有する業務用ソフトウェアシステムを認識した上で、そのリスクの受容を判断する 7.6.2.4 取扱いに慎重を要する管理用プロセスを、クラウドサービスを提供するプロセスとリソースを共有する環境で動作させる場合、管理用プロセスの動作を確保するための仕組みを設ける 6.3.1.5 論理資源の総和が物理資源を超過するような資源の割り当ては、物理資源の最繁時の同時使用率を考慮して行う 6.3.1.9 物理資源を複数のクラウド利用者で共有する論理資源の使用は、クラウド利用者が使用可能な最大値や最低値を定め適切に制限を行う		

H05: 隔離の失敗

・クラウドサービスを構成するメカニズムの不備・欠陥や脆弱性への攻撃により、異なるユーザやサービス間の隔離が失われることで、ユーザの機密情報の漏えいなどが生じ、事業者の評判が失墜する。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	論理資源へのアクセス制御が有効であること	クラウド内部のユーザによる盗聴、改ざん、システムの破壊	V17 クラウド内部のネットワークへの偵察行為が発生する可能性	ユーザが利用するネットワークへの偵察行為(ポートスキャンなど)を制限するか、又は偵察行為(ポートスキャンなど)を行う者を特定できる仕組みを設けて監視する	6.6.1.1 ネットワークには、クラウドサービスの提供にかかわるネットワーク、クラウドサービスを提供するネットワーク、及びクラウドサービスに含まれ提供されるネットワークを含める 6.6.1.2 ネットワーク管理者は、ネットワークにおける情報のセキュリティ及び接続したネットワークサービスの認可されていないアクセスからの保護を確実にする仕組みを整備する 6.6.1.3 適切と判断される場合には、ネットワークの運用責任を、コンピュータの運用から分離する 6.6.1.4 遠隔地に所在する設備(利用者の領域に設置した設備を含む。)の管理に関する責任及び手順を確立する 6.6.1.5 公衆ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及び業務用ソフトウェアを保護するために、特別な管理策(受信規制又は発信規制を含む)を確立する 6.6.1.6 セキュリティに関連した活動を記録できるように、適切なログ取得及び監視を適用する 6.6.1.7 サービスの最大限の活用及び管理策の情報処理基盤全体への一貫した適用の確実化のために、様々な管理作業を綿密に調整する 6.6.1.10 ネットワーク上の機器では、アクセス制御方針に基づき、すべてのネットワークインタフェースでアクセス制御(受信規制又は発信規制を含む)を実施する 6.6.1.12 ネットワーク上の機器では、業務に使用していない空きポートへの接続を制限する 6.6.1.14 ネットワーク上の不正なイベントを監視するため、侵入検知システムを導入する 6.6.1.15 侵入検知システムが、常に最新の攻撃・不正アクセスに対応可能なように、定義ファイル、検知ルールなどの更新を実施する	検知し、対処する前の許可されないアクセスの可能性	

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	論理資源へのアクセス制御が有効であること	クラウド内部のユーザによる盗聴、改ざん、システムの破壊	V6 リソース分離の欠如	論理リソース間のアクセス制御の不備を早期に発見し、適切な対応をする仕組みを整える。	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する	ゼロデイ脆弱性を突いた攻撃	
	機能層	同一物理資源を、複数の論理資源に分割し、論理資源へのアクセスを制御できること		V5 ハイパーバイザの脆弱性	ハイパーバイザの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える。	8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置(例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用)を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する(ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。) 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御(例えば、ファイアウォール)を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する		
				V53 フィルタリングリソースの不備または設定ミス	クラウドサービスの操作者のミスを防ぐため、操作者とは別の者がチェックを行う	6.1.3.1 組織の職務及び責任範囲は、認可されていない状態又は気づかれない状態で、一人の利用者が組織及びクラウド利用者の資産に対してアクセス、修正又は使用ができないようにする 6.1.3.2 組織の職務及び責任範囲は、ある作業を始めることと、その作業を認可することとを分割する 6.1.3.3 組織の職務及び責任範囲は、共謀のおそれがある場合は、共謀を防ぐ管理策(例えば、二人以上のかかわりを持たせる)の設計を行う 6.1.3.4 組織の職務及び責任範囲は、その分割が困難である場合には、他の管理策(例えば、活動の監視、監査証跡、経営陣による監督)を実施する	フィルタリングリソースの不備や設定ミスを発見する前の、隔離の失敗	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
物理層	物理的隔離が有効であること(物理的に隔離されていれば、物理資源へのアクセスは不可能であること)	サイドチャネル攻撃(装置の動作を物理的手段で測定し、解析することにより、装置内部のデータを取得する攻撃)	V18 共同利用者からの覗き見の可能性	装置の動作を物理的手段で測定し、解析されないため、装置を物理的に保護する。	5.2.1.14 装置を保護するために、放射される電磁波の解析、消費される電力の解析、故障発生時の動作の解析などによる情報漏えいのリスクが最小限になるように、取扱いに慎重を要する情報を処理する装置を保護する	新たなサイドチャネル手法による攻撃	
サービス管理系	隔離の失敗が生じたことを速やかに検知し、対象領域へのアクセス制限などの対策を講じることができること	クラウド内部のユーザによる盗聴、改ざん、システムの破壊	V17 クラウド内部のネットワークへの偵察行為が発生する可能性	管理用ネットワークへの偵察行為(ポートスキャンなど)を制御する	7.4.4.1 遠隔診断用及び環境設定用のポートには、クラウドサービスの提供にかかわる情報システム、クラウドサービスを提供する情報システム、及び提供するクラウドサービスにおけるポートを含める 7.4.4.3 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、施錠を利用する 7.4.4.4 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、ポートへの物理的なアクセスを制御するサポート手順を利用する 7.4.4.5 コンピュータ又はネットワーク設備上に導入されたサービス、ポート及び類似の設備で、業務機能に特に必要でないものは、動作しないようにするか、又は除去する 7.4.4.6 ハードウェア及びソフトウェアのサポート手順には、保守要員との間で合意できた場合にだけ、遠隔診断用及び環境設定用のポートへのアクセスを可能にすることを確実にすることを含める	検知し、対処する前の許可されないアクセスの可能性	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	隔離の失敗が生じたことを速やかに検知し、対象領域へのアクセス制限などの対策を講じることができること	クラウド内部のユーザによる盗聴、改ざん、システムの破壊	V6 リソース分離の欠如	論理リソース間のアクセス制御の不備を早期に発見し、適切な対応をする仕組みを整える。	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置(例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用)を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する(ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。) 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御(例えば、ファイアウォール)を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	
			V48 アプリケーションの脆弱性またはパッチ管理の不備	サービス管理のためのアプリケーションの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える。			

H06： サービスエンジンの侵害

・脆弱性等を通じてサービスエンジンの制御を奪われることで、クラウドサービスに特化した攻撃（サービスエンジン経由の情報漏えい、リソースの逼迫化によるサービスのマヒ等）が行われる可能性がある。

<table>
<tr><th colspan="2" rowspan="2">レイヤ</th><th rowspan="2">目指すべき水準</th><th colspan="2">想定されるリスク</th><th rowspan="2">クラウド事業者における
対策の要点</th><th rowspan="2">対応するクラウド管理基準</th><th rowspan="2">残留リスク</th><th rowspan="2">備考</th></tr>
<tr><th>脅威</th><th>脆弱性</th></tr>
<tr><td rowspan="3">抽象化層</td><td>リソース層</td><td>－</td><td>－</td><td>－</td><td>－</td><td>－</td><td rowspan="4">ゼロデイ脆弱性を突いた攻撃</td><td></td></tr>
<tr><td>機能層</td><td>クラウドサービスの実装手段（ハイパーバイザなど）の脆弱性について適切な対策が講じられ、その脆弱性を悪用したサービスエンジンへの攻撃が成功しない状況が維持されていること</td><td>脆弱性を悪用した盗聴、改ざん、システムの破壊</td><td>V5 ハイパーバイザの脆弱性</td><td>ハイパーバイザの脆弱性を悪用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える。</td><td rowspan="3">8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める
8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる
8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める
8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む
8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する
8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う
8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める
8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する
8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する
8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する
8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。）
8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する
8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する
8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する
8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する
8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する
8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める
8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する
8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する</td><td></td></tr>
<tr><td colspan="2">物理層</td><td>－</td><td>－</td><td>－</td><td>－</td><td></td></tr>
<tr><td colspan="2">サービス管理系</td><td>攻撃によりサービスエンジンで不正なプロセスが実施された場合でも、クラウドサービスの制御系を通じてその停止等の制御が行えること</td><td>サービス管理用システムの脆弱性を悪用したシステム制御の乗っ取り、マヒなど</td><td>V48 アプリケーションの脆弱性またはパッチ管理の不備</td><td>サービス管理のためのアプリケーションの脆弱性を悪用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える。</td><td></td></tr>
</table>

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	攻撃によりサービスエンジンで不正なプロセスが実施された場合でも、クラウドサービスの制御系を通じてその停止等の制御が行えること	サービス管理用システムの脆弱性を悪用したシステム制御の乗っ取り、マヒなど	V6 リソース分離の欠如	ハイパーバイザなどのサービスエンジンを制御するための通信を、ユーザのデータ通信用の回線から可能な限り分離する。	7.4.4.2 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、遠隔診断用及び環境設定用のネットワークを他のネットワークから物理的又は論理的に分離する	ゼロデイ脆弱性を突いた攻撃	
				サービス管理系へのアクセスを監視し、不正な通信やサービスエンジンの異常動作を早期に検知する体制を維持する。	6.6.1.1 ネットワークには、クラウドサービスの提供にかかわるネットワーク、クラウドサービスを提供するネットワーク、及びクラウドサービスに含まれ提供されるネットワークを含める 6.6.1.2 ネットワーク管理者は、ネットワークにおける情報のセキュリティ及び接続したネットワークサービスの認可されていないアクセスからの保護を確実にする仕組みを整備する 6.6.1.3 適切と判断される場合には、ネットワークの運用責任を、コンピュータの運用から分離する 6.6.1.4 遠隔地に所在する設備（利用者の領域に設置した設備を含む。）の管理に関する責任及び手順を確立する 6.6.1.6 セキュリティに関連した活動を記録できるように、適切なログ取得及び監視を適用する 6.6.1.14 ネットワーク上の不正なイベントを監視するため、侵入検知システムを導入する 6.6.1.15 侵入検知システムが、常に最新の攻撃・不正アクセスに対応可能なように、定義ファイル、検知ルールなどの更新を実施する		

M07： クラウドプロバイダでの内部不正－特権の悪用

・クラウド事業者における従業員の悪意の行動が、あらゆるクラウドサービスに影響を及ぼす。
・従業員が犯罪組織の標的とされ、上記の行動を行う。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	暗号化されたデータは、意図しない復号がされないこと	・プロバイダ従業員の不正 ・犯罪組織によるプロバイダ従業員への恐喝、脅迫、強要	V10. 暗号化状態でのデータ処理が不可能であること（暗号化したデータを処理するためにクラウド上で復号してしまう）	暗号技術又は暗号化したまま処理を行う技術を適切に用いる	6.8.1.1 情報には、組織の情報、クラウド利用者にかかわる情報、及び提供するクラウドサービス上のクラウド利用者の情報を含める 6.8.1.8 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、暗号技術の利用（例えば、情報の機密性、完全性及び真正性を保護するための暗号の利用）を含める 6.8.1.10 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、データを暗号化したまま統計処理を行い、その計算結果を安全に導くための技術の利用を含める	暗号の危殆化	
	機能層	プロバイダの従業員は、誰にも発覚することなく、不正な特権操作は行えないこと		V34 役割と責任の不明確性 V35 役割定義の適用の不備 V36「知る必要性」原則の不適用	クラウドサービスの操作者の役割と責任を明確に定義する	4.1.1.1 従業員のセキュリティ上の役割及び責任には、組織の情報セキュリティ基本方針に従って実施し、行動することを含める 4.1.1.2 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任には、認可されていないアクセス、認可されていない開示、改ざん、破壊又は妨害から資産を保護することを含める 4.1.1.3 従業員、契約相手のセキュリティ上の役割及び責任には、特定のセキュリティのプロセス又は活動を実施することを含める 4.1.1.4 従業員、契約相手及び第三者の利用者の取るべき行動に関するセキュリティ上の役割及び責任を、個人に割り当てることを確実にする仕組みを整備する 4.1.1.5 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任には、セキュリティ事象、その可能性のある事象又は組織に対するその他のセキュリティリスクを報告することを含める 4.1.1.6 セキュリティ上の役割及び責任を定め、雇用前のプロセスにおいて、採用候補者に明確に伝える 4.1.1.7 組織の雇用プロセスを通して採用していない者（例えば、外部組織から派遣された者）のセキュリティの役割及び責任も、明確に定め、伝える	責任者が発見する前の不正行為	
					クラウドサービスの操作者の不正を防ぐため、操作者とは別の者がチェックを行う	6.1.3.1 組織の職務及び責任範囲は、認可されていない状態又は気づかれない状態で、一人の利用者が組織及びクラウド利用者の資産に対してアクセス、修正又は使用ができないようにする 6.1.3.2 組織の職務及び責任範囲は、ある作業を始めることと、その作業を認可することとを分割する 6.1.3.3 組織の職務及び責任範囲は、共謀のおそれがある場合は、共謀を防ぐ管理策（例えば、二人以上のかかわりを持たせる）の設計を行う 6.1.3.4 組織の職務及び責任範囲は、その分割が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、経営陣による監督）を実施する		

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	機能層	プロバイダの従業員は、誰にも発覚することなく、不正な特権操作は行えないこと	・プロバイダ従業員の不正 ・犯罪組織によるプロバイダ従業員への恐喝、脅迫、強要	V39 システムまたはOSの脆弱性	ハイパーバイザの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。） 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
物理層	プロバイダの従業員は、誰にも発覚することなく、不正な特権操作は行えないこと	・プロバイダ従業員の不正 ・犯罪組織によるプロバイダ従業員への恐喝、脅迫、強要	V37 物理的なセキュリティ手順の不備	設備設置場所における装置の保護指針を定め、指針に基づく手順を定める	5.1.5.1 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、セキュリティを保つべき領域の存在又はその領域内での活動は、業務上知る必要のある要員にのみ知らせることを含める 5.1.5.2 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、安全面の理由のためと、悪意ある活動の機会を防止するためとの両面から、セキュリティを保つべき領域での監督されていない作業を回避することを含める 5.1.5.3 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、セキュリティを保つべき領域が無人のときは、物理的に施錠し、定期的に点検することを含める 5.1.5.4 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、セキュリティを保つべき領域への物品の持込、持ち出しを管理することを含める 5.1.5.5 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、画像、映像、音声又はその他の記録装置（例えば、携帯音楽端末やICレコーダ、カメラ付き携帯電話）の使用及び持込みについて、認可されたもの以外は、許可しないことを含める 6.1.1.1 操作手順には、クラウドサービスの提供にかかわるシステムの操作手順、クラウドサービスを提供するシステムの操作手順及びクラウドサービスとして提供されるシステムの操作手順を含める 6.1.1.2 情報処理設備及び通信設備に関連するシステムの管理活動（例えば、コンピュータの起動・停止の手順、バックアップ、装置の保守、媒体の取扱い、コンピュータ室及びメールの取扱いの管理・安全）の手順書は、クラウドサービスの利用に必要な手順書、クラウドサービスの提供に必要な手順書及びその他の管理活動に必要な手順書を区別して作成する 6.1.1.3 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、情報の処理及び取扱いを含む、各作業の詳細な実施に関する指示を明記する 6.1.1.4 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、バックアップを含む、各作業の詳細な実施に関する指示を明記する 6.1.1.5 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、スケジュール作成に関する要求事項（他のシステムとの相互依存性、最早作業開始時刻と最遅作業完了時刻など）を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.6 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、作業中に発生し得る、誤り又はその他の例外状況の処理についての指示（システムユーティリティの利用の制限）を含む、各作業の詳細な実施に関する指示を明記する	責任者が発見する前の不正行為	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
					6.1.1.7 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.8 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、特別な出力及び媒体の取扱いに関する指示を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.9 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、システムが故障した場合の再起動及び回復の手順を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.10 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、監査証跡及びシステムログ情報の管理を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.11 システムの管理活動のための操作手順及び文書化手順は正式な文書として取扱い、その手順書の変更は、経営陣が認可する 6.1.1.12 情報システムは、同一の手順、ツール及びユーティリティを用いて、首尾一貫した管理を行う		
物理層	プロバイダの従業員は、誰にも発覚することなく、不正な特権操作は行えないこと	・プロバイダ従業員の不正 ・犯罪組織によるプロバイダ従業員への恐喝、脅迫、強要	V34 役割と責任の不明確性 V35 役割定義の適用の不備 V36「知る必要性」原則の不適用	クラウドサービスの操作者の役割と責任を明確に定義する	4.1.1.1 従業員のセキュリティ上の役割及び責任には、組織の情報セキュリティ基本方針に従って実施し、行動することを含める 4.1.1.2 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任には、認可されていないアクセス、認可されていない開示、改ざん、破壊又は妨害から資産を保護することを含める 4.1.1.3 従業員、契約相手のセキュリティ上の役割及び責任には、特定のセキュリティのプロセス又は活動を実施することを含める 4.1.1.4 従業員、契約相手及び第三者の利用者の取るべき行動に関するセキュリティ上の役割及び責任を、個人に割り当てることを確実にする仕組みを整備する 4.1.1.5 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任には、セキュリティ事象、その可能性のある事象又は組織に対するその他のセキュリティリスクを報告することを含める 4.1.1.6 セキュリティ上の役割及び責任を定め、雇用前のプロセスにおいて、採用候補者に明確に伝える 4.1.1.7 組織の雇用プロセスを通して採用していない者（例えば、外部組織から派遣された者）のセキュリティの役割及び責任も、明確に定め、伝える		
				クラウドサービスの操作者の不正を防ぐため、操作者とは別の者がチェックを行う	6.1.3.1 組織の職務及び責任範囲は、認可されていない状態又は気づかれない状態で、一人の利用者が組織及びクラウド利用者の資産に対してアクセス、修正又は使用ができないようにする 6.1.3.2 組織の職務及び責任範囲は、ある作業を始めることと、その作業を認可することとを分割する 6.1.3.3 組織の職務及び責任範囲は、共謀のおそれがある場合は、共謀を防ぐ管理策（例えば、二人以上のかかわりを持たせる）の設計を行う 6.1.3.4 組織の職務及び責任範囲は、その分割が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、経営陣による監督）を実施する		

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
物理層	プロバイダの従業員は、誰にも発覚することなく、不正な特権操作は行えないこと	・プロバイダ従業員の不正 ・犯罪組織によるプロバイダ従業員への恐喝、脅迫、強要	V39. システムまたはOSの脆弱性	装置の脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える。	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。） 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	プロバイダの従業員は、誰にも発覚することなく、不正な特権操作は行えないこと	・プロバイダ従業員の不正 ・犯罪組織によるプロバイダ従業員への恐喝、脅迫、強要	V34 役割と責任の不明確性 V35 役割定義の適用の不備 V36「知る必要性」原則の不適用	クラウドサービスの操作者の役割と責任を明確に定義する	4.1.1.1 従業員のセキュリティ上の役割及び責任には、組織の情報セキュリティ基本方針に従って実施し、行動することを含める 4.1.1.2 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任には、認可されていないアクセス、認可されていない開示、改ざん、破壊又は妨害から資産を保護することを含める 4.1.1.3 従業員、契約相手のセキュリティ上の役割及び責任には、特定のセキュリティのプロセス又は活動を実施することを含める 4.1.1.4 従業員、契約相手及び第三者の利用者の取るべき行動に関するセキュリティ上の役割及び責任を、個人に割り当てることを確実にする仕組みを整備する 4.1.1.5 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任には、セキュリティ事象、その可能性のある事象又は組織に対するその他のセキュリティリスクを報告することを含める 4.1.1.6 セキュリティ上の役割及び責任を定め、雇用前のプロセスにおいて、採用候補者に明確に伝える 4.1.1.7 組織の雇用プロセスを通して採用していない者（例えば、外部組織から派遣された者）のセキュリティの役割及び責任も、明確に定め、伝える	責任者が発見する前の不正行為	
				クラウドサービスの操作者の不正を防ぐため、操作者とは別の者がチェックを行う	6.1.3.1 組織の職務及び責任範囲は、認可されていない状態又は気づかれない状態で、一人の利用者が組織及びクラウド利用者の資産に対してアクセス、修正又は使用ができないようにする 6.1.3.2 組織の職務及び責任範囲は、ある作業を始めることと、その作業を認可することとを分割する 6.1.3.3 組織の職務及び責任範囲は、共謀のおそれがある場合は、共謀を防ぐ管理策（例えば、二人以上のかかわりを持たせる）の設計を行う 6.1.3.4 組織の職務及び責任範囲は、その分割が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、経営陣による監督）を実施する		

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	プロバイダの従業員は、誰にも発覚することなく、不正な特権操作は行えないこと	・プロバイダ従業員の不正 ・犯罪組織によるプロバイダ従業員への恐喝、脅迫、強要	V1 認証、認可、課金管理（AAA）の脆弱性	サービス管理のためのアプリケーションの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える。	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。） 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	

M08： 管理用インターフェースの悪用（操作、インフラストラクチャアクセス）

・クラウドサービスのユーザ向けに、インターネットからリソース制御を可能とするインタフェースが悪用され、サービス全体に影響を及ぼす。
・クラウド事業者の管理者の制御用インタフェースも同様に悪用されることで、さらなる影響を及ぼす。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	－	－	－	－	－	－	
	機能層	ユーザの用いる管理用インターフェースのアクセス制御が適切に行われること	管理用インターフェースへの不正アクセス	V39 システムまたはOSの脆弱性 V48 アプリケーションの脆弱性またはパッチ管理の不備 V1 認証、認可、課金管理（AAA）の脆弱性	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フェースの悪用を防ぐため、脆弱性対策と早期発見の仕組みを整える。	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。） 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	
物理層								
サービス管理系								

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	ユーザの用いる管理用インターフェースのアクセス制御が適切に行われること	管理用インターフェースへの不正アクセス	V4 管理用インタフェースへのリモートアクセス	クラウドプロバイダの管理用ネットワークへの不正アクセスを防ぐため、管理用ネットワークへのアクセスを制御する	7.4.4.1 遠隔診断用及び環境設定用のポートには、クラウドサービスの提供にかかわる情報システム、クラウドサービスを提供する情報システム、及び提供するクラウドサービスにおけるポートを含める 7.4.4.2 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、遠隔診断用及び環境設定用のネットワークを他のネットワークから物理的又は論理的に分離する 7.4.4.3 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、施錠を利用する 7.4.4.4 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、ポートへの物理的なアクセスを制御するサポート手順を利用する 7.4.4.5 コンピュータ又はネットワーク設備上に導入されたサービス、ポート及び類似の設備で、業務機能に特に必要でないものは、動作しないようにするか、又は除去する 7.4.4.6 ハードウェア及びソフトウェアのサポート手順には、保守要員との間で合意できた場合にだけ、遠隔診断用及び環境設定用のポートへのアクセスを可能にすることを確実にすることを含める	責任者が発見する前の管理の誤り	
			V38 設定ミス	クラウドサービスの操作者のミスを防ぐため、操作者とは別の者がチェックを行う	6.1.3.1 組織の職務及び責任範囲は、認可されていない状態又は気づかれない状態で、一人の利用者が組織及びクラウド利用者の資産に対してアクセス、修正又は使用ができないようにする 6.1.3.2 組織の職務及び責任範囲は、ある作業を始めることと、その作業を認可することとを分割する 6.1.3.3 組織の職務及び責任範囲は、共謀のおそれがある場合は、共謀を防ぐ管理策（例えば、二人以上のかかわりを持たせる）の設計を行う 6.1.3.4 組織の職務及び責任範囲は、その分割が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、経営陣による監督）を実施する		

M09： データ転送途上における攻撃、データ漏えい（アップロード時、ダウンロード時、クラウド間転送）

・ユーザ環境とクラウドサービス、もしくは分散されたクラウドサービス相互間でのデータ転送機会が生ずることで、その転送中のデータの漏えいのリスクが生じる。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	論理ネットワークへのアクセス制御が有効であること	クラウド内部のネットワークの盗聴	V17 内部（クラウド）ネットワークへの偵察行為が発生する可能性	ユーザが利用するネットワークへの偵察行為（ポートスキャンなど）を制限するか、又は偵察行為（ポートスキャンなど）を行う者を特定できる仕組みを設けて監視する	6.6.1.1 ネットワークには、クラウドサービスの提供にかかわるネットワーク、クラウドサービスを提供するネットワーク、及びクラウドサービスに含まれ提供されるネットワークを含める 6.6.1.2 ネットワーク管理者は、ネットワークにおける情報のセキュリティ及び接続したネットワークサービスの認可されていないアクセスからの保護を確実にする仕組みを整備する 6.6.1.3 適切と判断される場合には、ネットワークの運用責任を、コンピュータの運用から分離する 6.6.1.4 遠隔地に所在する設備（利用者の領域に設置した設備を含む。）の管理に関する責任及び手順を確立する 6.6.1.5 公衆ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及び業務用ソフトウェアを保護するために、特別な管理策（受信規制又は発信規制を含む）を確立する 6.6.1.6 セキュリティに関連した活動を記録できるように、適切なログ取得及び監視を適用する 6.6.1.7 サービスの最大限の活用及び管理策の情報処理基盤全体への一貫した適用の確実化のために、様々な管理作業を綿密に調整する 6.6.1.10 ネットワーク上の機器では、アクセス制御方針に基づき、すべてのネットワークインタフェースでアクセス制御（受信規制又は発信規制を含む）を実施する 6.6.1.12 ネットワーク上の機器では、業務に使用していない空きポートへの接続を制限する 6.6.1.14 ネットワーク上の不正なイベントを監視するため、侵入検知システムを導入する 6.6.1.15 侵入検知システムが、常に最新の攻撃・不正アクセスに対応可能なように、定義ファイル、検知ルールなどの更新を実施する	検知し、対処する前の許可されないアクセスの可能性	
			クラウド外部のネットワークの盗聴	V8 通信路暗号の脆弱性	暗号アルゴリズムは、適切に選択する	8.3.1.3 暗号の利用に関する方針は、リスクアセスメントに基づく、要求される暗号アルゴリズムの種別、強度及び品質を考慮に入れた、要求された保護レベルの識別を考慮して定める	暗号の危殆化	

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	機能層	論理ネットワークへのアクセスを制御できること	クラウド内外のネットワークの盗聴	V9 アーカイブおよび転送中のデータの暗号化の強度不足または未実施	データ転送には、暗号技術を適切に用いる	6.8.1.1 情報には、組織の情報、クラウド利用者にかかわる情報、及び提供するクラウドサービス上のクラウド利用者の情報を含める 6.8.1.8 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、暗号技術の利用(例えば、情報の機密性、完全性及び真正性を保護するための暗号の利用)を含める 6.9.2.6 オンライン取引のためのセキュリティとして、かかわるすべての当事者間の通信経路を暗号化する	暗号の危殆化	
				V48 アプリケーションの脆弱性またはパッチ管理の不備(仮想スイッチなどの脆弱性)	仮想スイッチの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置(例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用)を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する(ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。) 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御(例えば、ファイアウォール)を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
物理層	物理ネットワークへのアクセスを制御できること	サイドチャネル攻撃（装置の動作を物理的手段で測定し、解析することにより、装置内部のデータを取得する攻撃）	V18 共同利用者からの覗き見の可能性	装置の動作を物理的手段で測定し、解析されないため、装置を物理的に保護する	5.2.1.14 装置を保護するために、放射される電磁波の解析、消費される電力の解析、故障発生時の動作の解析などによる情報漏えいのリスクが最小限になるように、取扱いに慎重を要する情報を処理する装置を保護する	新たなサイドチャネル手法による攻撃	
サービス管理系	不正アクセスが生じたことを速やかに検知し、対象ネットワークへのアクセス制限などの対策を講じることができること	クラウド内外のネットワークの盗聴	V17 内部（クラウド）ネットワークへの偵察行為が発生する可能性	管理用ネットワークへのポートスキャンを制御する	7.4.4.1 遠隔診断用及び環境設定用のポートには、クラウドサービスの提供にかかわる情報システム、クラウドサービスを提供する情報システム、及び提供するクラウドサービスにおけるポートを含める 7.4.4.2 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、遠隔診断用及び環境設定用のネットワークを他のネットワークから物理的又は論理的に分離する 7.4.4.3 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、施錠を利用する 7.4.4.4 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、ポートへの物理的なアクセスを制御するサポート手順を利用する 7.4.4.5 コンピュータ又はネットワーク設備上に導入されたサービス、ポート及び類似の設備で、業務機能に特に必要でないものは、動作しないようにするか、又は除去する 7.4.4.6 ハードウェア及びソフトウェアのサポート手順には、保守要員との間で合意できた場合にだけ、遠隔診断用及び環境設定用のポートへのアクセスを可能にすることを確実にすることを含める	検知し、対処する前の許可されないアクセスの可能性	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	不正アクセスが生じたことを速やかに検知し、対象ネットワークへのアクセス制限などの対策を講じることができること	クラウド内外のネットワークの盗聴	V1 認証、認可、課金管理(AAA)の脆弱性 V48. アプリケーションの脆弱性またはパッチ管理の不備	サービス管理のためのアプリケーションの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置(例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用)を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する(ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。) 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御(例えば、ファイアウォール)を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	

M10: セキュリティが確保されていない、または不完全なデータ削除

・ストレージやバックアップテープ等の物理媒体をを他のユーザと共用する場合、媒体には常時複数ユーザのデータが記録されるため、特定ユーザのデータだけを消去する目的で、その媒体を物理的に破壊することはできない。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	−	−	−	−	−	−	
	機能層	−	−	−	−	−	−	
物理層		ユーザが削除したデータは、クラウドから完全に消去できること	・削除データの復旧 ・バックアップデータの放置	V20 機密性の高いメディアのサニタイゼーション（記録の抹消）	データの削除は、そのデータの記憶域に、乱数などの無意味な記録を上書きし、データの痕跡を消去する	4.3.2.4 雇用、契約又は合意の終了時の手続には、個人所有の設備を業務に使用した場合には、クラウド利用者の資産を含むすべての関連する情報を組織に返却し、設備から確実に消去することを含める 5.2.6.4 取扱いに慎重を要する情報を格納した装置の再利用は、その情報を破壊、消去若しくは上書き後に行う。消去又は上書きには、標準的な消去又は初期化の機能を利用するよりも、元の情報を取り戻せなくなるようにする技術を利用する 6.7.2.2 取扱いに慎重を要する情報を格納した媒体のセキュリティを保ち、かつ、安全に保管し、処分する（例えば、焼却、消磁、シュレッダーの利用、組織内の他のアプリケーションでの利用のためのデータ消去） 6.7.2.3 リース機器の返却や媒体の廃棄において、復元できないように情報の消去を確実にする仕組みを整備する（例えば、専用の消去ツールを用いる）	バックアップのサイクル期間中のデータの残留	ストレージを複数の利用者が共同利用する場合、ある利用者が解放した記憶域は、すぐに他の利用者のデータによって上書きされる可能性がある。
サービス管理系								

M11： クラウド内DDoS/DoS攻撃

・悪意のユーザもしくはユーザ環境の乗っ取り等を通じて同じクラウドサービス内を起点とするDDoS/DoS攻撃が行われることで、インターネット経由の場合よりも大きな被害がユーザに発生する。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	DoS攻撃を受けても論理リソースが完全に消費しないこと	DoS攻撃による処理負荷の上昇に伴うリソースの消尽	V.28 リソースの利用上限制限ポリシーの欠如	攻撃対象となる同一の仮想マシンを複数の物理マシン上に複数用意し、攻撃を分散する	C.1.1.7　一部の情報処理設備（物理サーバ、物理ストレージ、物理ネットワーク機器、通信ケーブル、アクセス回線など）の過負荷がクラウドサービスを停止させないために、情報処理設備を冗長化し、負荷を分散する	想定を大きく超える処理負荷	
	機能層	Dos攻撃の攻撃元（踏み台）にならないこと	DoS攻撃の手段（踏み台）としての悪用	V53. フィルタリングリソースの不備または設定ミス（偽装アドレスを設定して行うDoS攻撃を防げないなど）	攻撃者が行うアドレス（IP, MAC）偽装を検知又は偽装トラフィックの発信を防止する	7.4.7.3 ネットワークトラフィックの発信元となる情報処理装置を管理する場合には、ネットワーク制御を行う箇所において、発信元のアドレスを確認し、不正なアドレスのネットワークトラフィックの送出を許可しないこと 7.4.7.4 プロキシ及び／又はネットワークアドレス変換を採用する場合には、内部及び外部のネットワーク制御を行う箇所において、発信元及びあて先のアドレスが正当であることを確認するために、セキュリティゲートウェイを利用する	アドレス偽装を行わないDoSトラフィックの発信	
				V.28 リソースの利用上限制限ポリシーの欠如	ユーザ間の利用の公平を図るため、ユーザごとに使用率の最高値や最低保証値を設ける。	6.3.1.9 物理資源を複数のクラウド利用者で共有する論理資源の使用は、クラウド利用者が使用可能な最大値や最低値を定め適切に制限を行う	許可範囲内のDoSトラフィックの発信	

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	機能層	処理負荷が上昇しても、機能を維持すること	DoS攻撃による処理負荷の上昇に伴う運用管理のマヒ	V48 アプリケーションの脆弱性またはパッチ管理の不備(仮想スイッチなどの脆弱性)	仮想スイッチの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置(例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用)を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する(ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。) 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御(例えば、ファイアウォール)を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	
				V38 設定ミス	クラウドサービスの操作者のミスが攻撃の標的となる脆弱性をもたらすのを防ぐため、操作者とは別の者がチェックを行う	6.1.3.1 組織の職務及び責任範囲は、認可されていない状態又は気づかれない状態で、一人の利用者が組織及びクラウド利用者の資産に対してアクセス、修正又は使用ができないようにする 6.1.3.2 組織の職務及び責任範囲は、ある作業を始めることと、その作業を認可することとを分割する 6.1.3.3 組織の職務及び責任範囲は、共謀のおそれがある場合は、共謀を防ぐ管理策(例えば、二人以上のかかわりを持たせる)の設計を行う 6.1.3.4 組織の職務及び責任範囲は、その分割が困難である場合には、他の管理策(例えば、活動の監視、監査証跡、経営陣による監督)を実施する	責任者が発見する前の誤り	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
物理層	処理負荷が上昇しても、機能を維持すること	DoS攻撃による処理負荷の上昇に伴う異常挙動、故障の発生	V39 システムまたはOSの脆弱性	処理負荷の限界を把握し、限界に達したときの手順を定める	6.9.1.18 電子商取引に用いる基幹コンピュータが持つ攻撃に対する耐性について、及び電子商取引の実施に必要とされるネットワーク相互接続のセキュリティ上の影響について確認する 6.3.1.11 容量及び能力が設計時の想定を超えた場合の対応手順（仮想マシン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など）を作成する	想定を大きく超える処理負荷	
				ユーザの同意を得て、過度な処理負荷を与えるトラフィックを識別してフィルタリングし、遮断する	7.4.6.3 利用者の接続（例えば電子メールのようなメッセージ通信、ファイル転送、対話型アクセス、業務用ソフトウェアによるアクセス）は、事前に定められた表又は規則によって通信をフィルタにかける、ネットワークゲートウェイによって制限する	・正常通信と識別できないDoS攻撃 ・想定を大きく超える処理負荷	
				ユーザの同意を得て、確保すべきトラフィックを識別して、帯域を保証する	7.4.6.4 利用者の接続（例えば電子メールのようなメッセージ通信、ファイル転送、対話型アクセス、業務用ソフトウェアによるアクセス）は、事前に定められた表又は規則によって帯域を保証する		
サービス管理系	DoS攻撃の標的を他の資源から分離し、他への影響を回避させること	DoS攻撃によるサービスの停止	V53. フィルタリングリソースの不備または設定ミス	攻撃を検知し、攻撃を受けているリソースを他のリソースから分離する	6.3.1.3 適切な時点で問題を知らせるために、探知のための管理策を備える 6.6.1.3 適切と判断される場合には、ネットワークの運用責任を、コンピュータの運用から分離する 6.6.1.6 セキュリティに関連した活動を記録できるように、適切なログ取得及び監視を適用する 6.6.1.11 攻撃にさらされる論理リソースは、独立した物理リソースに収容し、他のリソースから分離する 6.6.1.14 ネットワーク上の不正なイベントを監視するため、侵入検知システムを導入する 6.6.1.15 侵入検知システムが、常に最新の攻撃・不正アクセスに対応可能なように、定義ファイル、検知ルールなどの更新を実施する 6.10.1.10監査ログには、ネットワークアドレス（クラウドサービスの提供にかかわるネットワークアドレス及びクラウドサービスとして提供されるネットワークアドレスを含む。）及びプロトコルを含める 6.10.1.11監査ログには、アクセス制御システム（クラウドサービスの提供にかかわるアクセス制御システム及びクラウドサービスとして提供されるアクセス制御システムを含む。）が発した警報を含める6.6.1.2 ネットワーク管理者は、ネットワークにおける情報のセキュリティ及び接続したネットワークサービスの認可されていないアクセスからの保護を確実にする仕組みを整備する	・正常通信と識別できないDoS攻撃 ・想定を大きく超える処理負荷	
	DoS攻撃を受けても、運用管理を継続できること	DoS攻撃による制御系のマヒ	V.28 リソースの利用上限制限ポリシーの欠如	ユーザサービス用のリソースとは別に、管理用のリソースを確保する	7.6.2.3 取扱いに慎重を要する業務用ソフトウェアを共有環境で用いる場合、そのシステムの管理者は、資源とリスクを共有する業務用ソフトウェアシステムを認識した上で、そのリスクの受容を判断する 7.6.2.4 取扱いに慎重を要する管理用プロセスを、クラウドサービスを提供するプロセスとリソースを共有する環境で動作させる場合、管理用プロセスの動作を確保するための仕組みを設ける 6.3.1.5 論理資源の総和が物理資源を超過するような資源の割り当ては、物理資源の最繁時の同時使用率を考慮して行う 6.3.1.9 物理資源を複数のクラウド利用者で共有する論理資源の使用は、クラウド利用者が使用可能な最大値や最低値を定め適切に制限を行う	想定を大きく超える処理負荷	

L12： ロックインによるユーザの忌避

・クラウドプロバイダが、外部リソースを利用してユーザデータを保護する必要性が生じても、相互接続性がないために、データ移行ができない。
（注）本リスクはENISAではユーザにとっての「ロックインされてしまう」リスクとして整理されているが、ここではクラウド事業者視点で扱う。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	セキュリティを維持しながらユーザデータを外部のリソースに転送できること	外部リソースを利用したデータ保護を必要とする事態	V13 技術とソリューションにおける標準の欠如	ユーザデータをクラウドの外部に移行する際に必要な外部との相互接続手順を定める	6.8.5.2 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、組織内の他の部門と情報を共有している管理システム及び会計システムにおける既知のぜい弱性を含める 6.8.5.3 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、業務通信システムにおける情報のぜい弱性（例えば、通話又は電話会議の録音、通話の機密性、ファクシミリの保管、メールの開封、メールの配信）を考慮点として含める 6.8.5.4 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、情報の共有を管理するための方針及び適切な管理策を考慮点として含める 6.8.5.5 業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、システムが適切なレベルの保護を提供しない場合の、取扱いに慎重を要する業務情報及び秘密文書の相互接続からの除外を考慮点として含める 6.8.5.6 業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、特別な者（例えば、重要な業務計画に従事している要員）が関係する業務日誌へのアクセスの制限を考慮点として含める 6.8.5.7 業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、システムの使用が許された要員、契約相手又は提携業者の区分、そこからシステムがアクセスされる場合がある場所を考慮点として含める 6.8.5.8 業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、特別の設備に対するアクセスの、特定の区分に属する利用者だけへの限定を考慮点として含める 6.8.5.9 業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、利用者の地位の識別（例えば、他の利用者のために、組織又は契約相手の従業員として名簿に載っている者）を考慮点として含める 6.8.5.10 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、システム内の情報の保持及びバックアップを考慮点として含める 6.8.5.11 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、緊急時に用いる代替手段についての要求事項及び取決めを考慮点として含める	データ移行の間の可用性の低下	
	機能層	－	－	－	－	－	－	
物理層		－	－	－	－	－	－	
サービス管理系		－	－	－	－	－	－	

L13： ガバナンスの喪失

・クラウドを利用することで、ユーザが下位層を対象としたガバナンス（自社ポリシーに基づくアクセス制御、ログ管理、監査実施等）を失うことのリスクを憂慮し、クラウド利用を躊躇する。
（注）本リスクはENISAではユーザにとっての「ロックインされてしまう」リスクとして整理されているが、ここではクラウド事業者視点で扱っている。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	ユーザとクラウドプロバイダが合意した責任分界が明確であり、ユーザの責任範囲におけるセキュリティ対策はユーザ自らが実施できること	ユーザがなすべきセキュリティ対策がリソース上で行えないこと	V34 役割と責任の不明確性 V35 役割定義の適用の不備 V44 不明確な資産の管理責任	ユーザとクラウドプロバイダの役割と責任を明確に定義し、定めに従って対処する	4.1.1.1 従業員のセキュリティ上の役割及び責任には、組織の情報セキュリティ基本方針に従って実施し、行動することを含める 4.1.1.2 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任には、認可されていないアクセス、認可されていない開示、改ざん、破壊又は妨害から資産を保護することを含める 4.1.1.3 従業員、契約相手のセキュリティ上の役割及び責任には、特定のセキュリティのプロセス又は活動を実施することを含める 4.1.1.4 従業員、契約相手及び第三者の利用者の取るべき行動に関するセキュリティ上の役割及び責任を、個人に割り当てることを確実にする仕組みを整備する 4.1.1.5 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任には、セキュリティ事象、その可能性のある事象又は組織に対するその他のセキュリティリスクを報告することを含める 4.1.1.6 セキュリティ上の役割及び責任を定め、雇用前のプロセスにおいて、採用候補者に明確に伝える 4.1.1.7 組織の雇用プロセスを通して採用していない者（例えば、外部組織から派遣された者）のセキュリティの役割及び責任も、明確に定め、伝える	・定義もれ ・合意もれ ・合意の齟齬 ・実施の誤り	

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	ユーザとクラウドプロバイダが合意した責任分界が明確であり、ユーザの責任範囲におけるセキュリティ対策はユーザ自らが実施できること	ユーザがなすべきセキュリティ対策がリソース上で行えないこと	V13 技術とソリューションにおける標準の欠如	ユーザデータをクラウドの外部に移行する際に必要な外部との相互接続手順を定める	6.8.5.1 業務用情報システムには、クラウドサービスの提供にかかわる情報システム及びクラウドサービスを提供する情報システムを含める 6.8.5.2 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、組織内の他の部門と情報を共有している管理システム及び会計システムにおける既知のぜい弱性を含める 6.8.5.3 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、業務通信システムにおける情報のぜい弱性(例えば、通話又は電話会議の録音、通話の機密性、ファクシミリの保管、メールの開封、メールの配信)を考慮点として含める 6.8.5.4 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、情報の共有を管理するための方針及び適切な管理策を考慮点として含める 6.8.5.5 業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、システムが適切なレベルの保護を提供しない場合の、取扱いに慎重を要する業務情報及び秘密文書の相互接続からの除外を考慮点として含める 6.8.5.6 業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、特別な者(例えば、重要な業務計画に従事している要員)が関係する業務日誌へのアクセスの制限を考慮点として含める 6.8.5.7 業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、システムの使用が許された要員、契約相手又は提携業者の区分、そこからシステムがアクセスされる場合がある場所を考慮点として含める 6.8.5.8 業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、特別の設備に対するアクセスの、特定の区分に属する利用者だけへの限定を考慮点として含める 6.8.5.9 業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、利用者の地位の識別(例えば、他の利用者のために、組織又は契約相手の従業員として名簿に載っている者)を考慮点として含める 6.8.5.10 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、システム内の情報の保持及びバックアップを考慮点として含める 6.8.5.11 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、緊急時に用いる代替手段についての要求事項及び取決めを考慮点として含める	・定義もれ ・合意もれ ・合意の齟齬 ・実施の誤り	

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	ユーザと合意したセキュリティ対策が、クラウドプロバイダの責任において実施され、実施状況をユーザが正しく把握できること	クラウドプロバイダの ・設計・構築ミス ・運用（設定・保守・故障対応など）ミス ・説明不足	V38 設定ミス V39 システムまたはOSの脆弱性	クラウドサービスの操作者のミスを防ぐため、操作者とは別の者がチェックを行う	6.1.3.1 組織の職務及び責任範囲は、認可されていない状態又は気づかれない状態で、一人の利用者が組織及びクラウド利用者の資産に対してアクセス、修正又は使用ができないようにする 6.1.3.2 組織の職務及び責任範囲は、ある作業を始めることと、その作業を認可することとを分割する 6.1.3.3 組織の職務及び責任範囲は、共謀のおそれがある場合は、共謀を防ぐ管理策（例えば、二人以上のかかわりを持たせる）の設計を行う 6.1.3.4 組織の職務及び責任範囲は、その分割が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、経営陣による監督）を実施する	責任者が発見する前の誤り	
	機能層				システムの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える	8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。） 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	
物理層								

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
物理層	ユーザと合意したセキュリティ対策が、クラウドプロバイダの責任において実施され、実施状況をユーザが正しく把握できること	クラウドプロバイダの ・設計・構築ミス ・運用（設定・保守・故障対応など）ミス ・説明不足	V37 物理的なセキュリティ手順の不備	設備設置場所における装置の保護指針を定め、指針に基づく手順を定める	5.1.5.1 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、セキュリティを保つべき領域の存在又はその領域内での活動は、業務上知る必要のある要員にのみ知らせることを含める 5.1.5.2 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、安全面の理由のためと、悪意ある活動の機会を防止するためとの両面から、セキュリティを保つべき領域での監督されていない作業を回避することを含める 5.1.5.3 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、セキュリティを保つべき領域が無人のときは、物理的に施錠し、定期的に点検することを含める 5.1.5.4 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、セキュリティを保つべき領域への物品の持込、持ち出しを管理することを含める 5.1.5.5 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、画像、映像、音声又はその他の記録装置（例えば、携帯音楽端末やICレコーダ、カメラ付き携帯電話）の使用及び持込みについて、認可されたもの以外は、許可しないことを含める 6.1.1.1 操作手順には、クラウドサービスの提供にかかわるシステムの操作手順、クラウドサービスを提供するシステムの操作手順及びクラウドサービスとして提供されるシステムの操作手順を含める 6.1.1.2 情報処理設備及び通信設備に関連するシステムの管理活動（例えば、コンピュータの起動・停止の手順、バックアップ、装置の保守、媒体の取扱い、コンピュータ室及びメールの取扱いの管理・安全）の手順書は、クラウドサービスの利用に必要な手順書、クラウドサービスの提供に必要な手順書及びその他の管理活動に必要な手順書を区別して作成する 6.1.1.3 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、情報の処理及び取扱いを含む、各作業の詳細な実施に関する指示を明記する 6.1.1.4 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、バックアップを含む、各作業の詳細な実施に関する指示を明記する 6.1.1.5 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、スケジュール作成に関する要求事項（他のシステムとの相互依存性、最早作業開始時刻と最遅作業完了時刻など）を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.6 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、作業中に発生し得る、誤り又はその他の例外状況の処理についての指示（システムユーティリティの利用の制限）を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.7 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.8 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、特別な出力及び媒体の取扱いに関する指示を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.9 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、システムが故障した場合の再起動及び回復の手順を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.10 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、監査証跡及びシステムログ情報の管理を含む、各作業の詳細な実施に関する指示を明記する 6.1.1.11 システムの管理活動のための操作手順及び文書化手順は正式な文書として取扱い、その手順書の変更は、経営陣が認可する 6.1.1.12 情報システムは、同一の手順、ツール及びユーティリティを用いて、首尾一貫した管理を行う	手順実施の誤り	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	ユーザと合意したセキュリティ対策が、クラウドプロバイダの責任において実施され、実施状況をユーザが正しく把握できること	クラウドプロバイダの ・設計・構築ミス ・運用（設定・保守・故障対応など）ミス ・説明不足	V31. 利用規約の完全性と透明性の欠如	ユーザと合意したセキュリティ要求事項を明確にする	2.2.2.1 組織の情報又は資産には、クラウドサービスとして提供される情報又は資産を含める 2.2.2.2 クラウド利用者が、提供するクラウドサービス上のクラウド利用者の情報及び組織の資産にアクセスする際のセキュリティの要求事項には、情報・ソフトウェアを含む組織の資産を保護するための手順及び既知のぜい弱性の管理、資産を危うくする事態を判断するための手順、完全性の確保、情報の複製及び開示の制限を含む資産の保護を含める 2.2.2.3 クラウド利用者が、提供するクラウドサービス上のクラウド利用者の情報及び組織の資産にアクセスする際のセキュリティの要求事項には、提供するサービスを記載する 2.2.2.4 クラウド利用者が、提供するクラウドサービス上のクラウド利用者の情報及び組織の資産にアクセスする際のセキュリティの要求事項には、クラウド利用者のアクセスの様々な理由、要求事項及び利便を記載する 2.2.2.5 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、アクセス制御方針を策定する。このアクセス制御方針には、承認されたアクセス方法、並びに固有の識別子（例えば、利用者IDとパスワードとの組合せ）の管理及び使用、利用者のアクセス及び特権の認可プロセス、明示的に認可されていないすべてのアクセスを禁止することの表明、アクセス権を失効させる、又はシステム間の接続を阻止する手続を含める 2.2.2.6 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、情報（例えば、個人情報）の誤り、情報セキュリティインシデント及びセキュリティ違反の報告、通知及び調査に関する取決めを明確にする 2.2.2.7 クラウド利用者が、提供するクラウドサービス上のクラウド利用者の情報及び組織の資産にアクセスする際のセキュリティ要求事項には、クラウド利用者に組織の情報又は資産へのアクセスを許す前に、利用できる各サービスを記載する 2.2.2.8 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、サービスの目標レベル及び受け入れられないレベルを明確にする 2.2.2.9 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、組織の資産に関係する活動を監視し、中止させる権利を明確にする 2.2.2.10 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、組織及びクラウド利用者のそれぞれの義務を明確にする 2.2.2.11 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、法的な問題に関する責任及び法的要求事項を満たすことを確実にする。特に、契約が他国のクラウド利用者との協力にかかわるものである場合、その国の法制度を考慮に入れる 2.2.2.12 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、知的財産権（IPR）及び著作権の取扱い、並びに共同作業の成果の保護のあり方を明確にする	・定義もれ ・合意もれ ・合意の齟齬 ・実施の誤り	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	ユーザと合意したセキュリティ対策が、クラウドプロバイダの責任において実施され、実施状況をユーザが正しく把握できること	クラウドプロバイダの ・設計・構築ミス ・運用(設定・保守・故障対応など)ミス ・説明不足	V16 脆弱性診断プロセスに関する管理の欠如	脆弱性の管理手続を定め、その実施状況及び結果をユーザに通知する	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置(例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用)を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する(ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。) 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御(例えば、ファイアウォール)を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する 8.6.1.20 クラウドサービスを提供する情報システム及びクラウドサービスとして提供される情報システムに対するぜい弱性と脅威に関する情報を、必要に応じてクラウド利用者に通知する	ゼロデイ脆弱性を突いた攻撃	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	ユーザと合意したセキュリティ対策が、クラウドプロバイダの責任において実施され、実施状況をユーザが正しく把握できること	クラウドプロバイダの ・設計・構築ミス ・運用(設定・保守・故障対応など)ミス ・説明不足	V30. 司法管轄権に関する情報の欠如 V29. 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如	クラウドプロバイダ及びシステムが順守すべき法令、規則、契約のある地域を明示する	11.1.1.2 各情報システム及び組織について、すべての関連する法令、規則及び契約上の要求事項を満たすための具体的な管理策及び具体的責任を同様に定め、文書化する 11.1.1.3 情報システム及び組織が順守すべき法令、規制及び契約のある地域(国、州など)を、クラウド利用者に明示する 2.2.2.11 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、法的な問題に関する責任及び法的要求事項を満たすことを確実にする。特に、契約が他国のクラウド利用者との協力にかかわるものである場合、その国の法制度を考慮に入れる	・把握もれ ・明示もれ	
			V38 設定ミス	クラウドサービスの操作者のミスを防ぐため、操作者とは別の者がチェックを行う	6.1.3.1 組織の職務及び責任範囲は、認可されていない状態又は気づかれない状態で、一人の利用者が組織及びクラウド利用者の資産に対してアクセス、修正又は使用ができないようにする 6.1.3.2 組織の職務及び責任範囲は、ある作業を始めることと、その作業を認可することとを分割する 6.1.3.3 組織の職務及び責任範囲は、共謀のおそれがある場合は、共謀を防ぐ管理策(例えば、二人以上のかかわりを持たせる)の設計を行う 6.1.3.4 組織の職務及び責任範囲は、その分割が困難である場合には、他の管理策(例えば、活動の監視、監査証跡、経営陣による監督)を実施する	責任者が発見する前の誤り	

L14： サプライチェーンにおける障害

・クラウドサービスにおける認証等のサービスを外部委託することで、その委託先サービスに脆弱性が存在するとクラウドサービス全体に影響が及ぶ可能性がある。
・どの部分を外部委託しているかを明示しないことで、ユーザによるクラウドサービスへの信頼度が低下する。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	－	－	－	－	－	－	
	機能層	－	－	－	－	－	－	
物理層		－	－	－	－	－	－	
サービス管理系		クラウドプロバイダの外部委託先に起因するセキュリティ障害がないこと	外部委託先に起因するユーザデータの漏えい、改ざん、サービス利用の停止	V22 クラウドをまたがるアプリケーションに潜在する相互依存性 V47 サプライヤの冗長化（SUPPLIER REDUNDANCY）の欠如	外部委託先から供給を受けるサービスの停止によって、クラウドサービスが停止しないような仕組みを整備する	6.2.1.5 組織は、重大なサービス不具合又は災害の後においても、合意されたサービス継続レベル（クラウドサービスの提供にかかわるサービス継続レベルを含む。）を維持することを確実にするように設計された実行可能な計画とともに、第三者が十分なサービス提供機能を維持することを確実にする仕組みを整備し、また、これらの仕組みのうち、クラウド利用者の情報セキュリティ管理に影響のあるものを、クラウド利用者（クラウドサービスの利用を検討する者を含む。）に明示する	外部委託先における想定できないインシデントの発生	
				V31 利用規約の完全性と透明性の欠如	外部委託先に要求した事項が適切に実施され維持されるよう、外部委託先を適切に管理する	6.2.1.1 第三者が提供するサービスには、クラウドサービスの提供にかかわる委託先のサービスを含め、また、これらのうちクラウド利用者の情報セキュリティ管理に影響のあるサービスを開示する 6.2.1.2 第三者によるサービスの提供には、クラウドサービスの提供にかかわるサービス（例えば、ネットワークサービス、データセンターサービス、ホールセールされるクラウドサービスなど）又はその他のサービスを対象として合意されたセキュリティの取決め、サービスの定義、及びサービスの管理を含め、また、これらのうちクラウド利用者の情報セキュリティ管理に影響のあるものを、クラウド利用者（クラウドサービスの利用を検討する者を含む。）に明示する 6.2.1.3 外部委託契約（クラウドサービスの提供にかかわる委託先との契約を含む。）の場合、組織は必要な外部委託先への移行内容（情報移行、情報処理施設の移行又はその他移行すべきもの）を計画する 6.2.1.4 外部委託契約（クラウドサービスの提供にかかわる委託先との契約を含む。）の場合、移行期間を通してセキュリティの維持を確実にする仕組みを整備する 6.2.1.5 組織は、重大なサービス不具合又は災害の後においても、合意されたサービス継続レベル（クラウドサービスの提供にかかわるサービス継続レベルを含む。）を維持することを確実にするように設計された実行可能な計画とともに、第三者が十分なサービス提供機能を維持することを確実にする仕組みを整備し、また、これらの仕組みのうち、クラウド利用者の情報セキュリティ管理に影響のあるものを、クラウド利用者（クラウドサービスの利用を検討する者を含む。）に明示する （次ページに続く）		

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	クラウドプロバイダの外部委託先に起因するセキュリティ障害がないこと	外部委託先に起因するユーザデータの漏えい、改ざん、サービス利用の停止	V31 利用規約の完全性と透明性の欠如	外部委託先に要求した事項が適切に実施され維持されるよう、外部委託先を適切に管理する	6.2.2.1 第三者が提供するサービスには、クラウドサービスの提供にかかわる委託先のサービスを含める 6.2.2.2 合意における情報セキュリティの条件の順守を確実にするために、第三者が提供するサービスの監視及びレビューを実施する 6.2.2.3 第三者が提供するサービスのうち、クラウドサービスの提供にかかわる委託先が提供するサービス(例えば、ネットワークサービス、データセンターサービス、ホールセールされるクラウドサービスなど)、報告及び記録は、常に監視し、レビューし、また、クラウド利用者に、レビューしていることを開示し、そのレビューの記録を明示する 6.2.2.4 第三者が提供するサービスのうち、クラウドサービスの提供にかかわる委託先が提供するサービス(例えば、ネットワークサービス、データセンターサービス、ホールセールされるクラウドサービスなど)は、定期的に監査し、また、クラウド利用者に、監査していることを開示し、その監査結果をまとめた報告書などを提示する 6.2.2.5 第三者が提供するサービスの監視及びレビューにおいては、情報セキュリティのインシデント及び問題点の適切な管理を確実にする仕組みを整備する 6.2.2.6 合意の順守を点検するために、第三者が提供するサービスの実施レベルを監視する 6.2.2.7 第三者の作成したサービスの報告をレビューし、合意によって必要とされている定期進ちょく(捗)会合を設定する 6.2.2.8 第三者及び組織は、合意並びにすべての業務支援指針及び手順書で要求されるように、情報セキュリティインシデントの情報及びその情報のレビュー結果を提供する 6.2.2.9 第三者監査証跡並びにセキュリティ事象記録、運用上の問題点の記録、故障記録、障害履歴及び提供サービスに関連する中断記録をレビューする 6.2.2.10 第三者が提供するサービスの監視及びレビューにおいては、識別された問題の解決及び管理を実施する 6.2.2.11 指定された個人又はサービス管理チームに、第三者との関係を管理する責任を割り当てる 6.2.2.12 組織は、順守状況の点検及び契約における要求事項の施行に対する責任を第三者に割り当てることを確実にする仕組みを整備する 6.2.2.13 契約における要求事項、特に情報セキュリティに関する要求事項を満足しているかどうかを監視するために、十分な技術力及び人的資源を確保する 6.2.2.14 サービスの提供において不完全な点があった場合は、適切な処置をする 6.2.2.15 組織は、第三者が利用、処理又は管理する、取扱いに慎重を要する又は重要な情報若しくは情報処理設備に対して、すべてのセキュリティの側面についての十分で包括的な管理及び可視性を維持する 6.2.2.16 組織は、セキュリティに関連した活動(例えば、変更管理、ぜい弱性識別、情報セキュリティインシデントの報告・対応)の可視性を維持することを確実にするために、報告プロセス、様式及び構成を明確に規定する	外部委託先における想定できないインシデントの発生	

L15： EDoS攻撃（経済的な損失を狙ったサービス運用妨害攻撃）

・悪意のユーザによるユーザアカウントの乗っ取り、従量制リソースの浪費等を通じて、ユーザに経済的損失をもたらす。
（注）ENISAガイドラインにない追記： 同様の被害は、ユーザの過失（プログラムの欠陥、設計ミス）によっても生じる可能性がある。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	あらかじめ定めた制限を超えて、リソースの使用ができないこと	攻撃者から送信されるパケットの受信課金	V.28 リソースの利用上限制限ポリシーの欠如	ユーザの想定を上回る課金を防ぐため、課金にかかわる使用を制限する仕組みを備える	6.3.1.9 物理資源を複数のクラウド利用者で共有する論理資源の使用は、クラウド利用者が使用可能な最大値や最低値を定め適切に制限を行う	・課金上限以下の攻撃 ・課金制限によるサービスの停止	
	機能層	ユーザIDの管理が適切に行われること	ユーザIDの窃盗	V4 管理用インタフェースへのリモートアクセス	クラウドプロバイダの管理用ネットワークを利用したユーザIDの窃盗を防ぐため、管理用ネットワークへのアクセスを制御する	7.4.4.1 遠隔診断用及び環境設定用のポートには、クラウドサービスの提供にかかわる情報システム、クラウドサービスを提供する情報システム、及び提供するクラウドサービスにおけるポートを含める 7.4.4.2 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、遠隔診断用及び環境設定用のネットワークを他のネットワークから物理的又は論理的に分離する 7.4.4.3 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、施錠を利用する 7.4.4.4 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、ポートへの物理的なアクセスを制御するサポート手順を利用する 7.4.4.5 コンピュータ又はネットワーク設備上に導入されたサービス、ポート及び類似の設備で、業務機能に特に必要でないものは、動作しないようにするか、又は除去する 7.4.4.6 ハードウェア及びソフトウェアのサポート手順には、保守要員との間で合意できた場合にだけ、遠隔診断用及び環境設定用のポートへのアクセスを可能にすることを確実にすることを含める	クラウドプロバイダの管理用ネットワークの管理の誤り	
物理層								
サービス管理系								

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	ユーザIDの管理が適切に行われること	ユーザIDの窃盗	V2 ユーザプロビジョニングの脆弱性 V3 ユーザプロビジョニング削除の脆弱性	ユーザIDの不正使用を防ぐため、ユーザがユーザIDの登録・変更・削除などを適切に管理する仕組みを整える	7.2.1.1 利用者には、クラウドサービスの提供にかかわる情報システム及びクラウドサービスを提供する情報システムにアクセスする実務管理者又は運用担当者、並びに提供するクラウドサービスにアクセスするクラウドサービスの利用者を含める 7.2.1.2 利用者の登録・登録削除のためのアクセス制御手順に、利用者と利用者自身の行動とを対応付けすること、及び利用者がその行動に責任をもつことを可能にする、一意な利用者IDの利用を含める 7.2.1.3 利用者の登録・登録削除のためのアクセス制御手順に、グループIDの利用は、業務上又は運用上の理由で必要な場合にだけ許可し、承認し、記録することを含める 7.2.1.4 利用者の登録・登録削除のためのアクセス制御手順に、利用者が情報システム又はサービスの利用について、そのシステムの管理者から認可を得ていることの点検を含める(アクセス権について経営陣から別の承認を受けることが適切な場合もある。) 7.2.1.5 利用者の登録・登録削除のためのアクセス制御手順に、許可したアクセスのレベルが、業務の目的に適していることの点検を含める 7.2.1.6 利用者の登録・登録削除のためのアクセス制御手順に、許可したアクセスのレベルが、組織のセキュリティ基本方針と整合していること(例えば、職務権限の分割に矛盾するおそれはないか。)の点検を含める 7.2.1.7 利用者の登録・登録削除のためのアクセス制御手順に、利用者に各自のアクセス権について記述した文書を発行することを含める 7.2.1.8 利用者の登録・登録削除のためのアクセス制御手順に、利用者に各自がアクセス条件を理解していることを示す文書に、署名を要求することを含める 7.2.1.9 利用者の登録・登録削除のためのアクセス制御手順は、認可手順が完了するまでサービス提供者が利用者にアクセスさせないようにすることが確実になるよう定める 7.2.1.10 利用者の登録・登録削除のためのアクセス制御手順に、サービスを利用するために登録されているすべての人の正式な記録の維持を含める 7.2.1.11 利用者の登録・登録削除のためのアクセス制御手順に、役割又は職務を変更した利用者、又は組織から離れた利用者のアクセス権の即座の解除、若しくは停止することを含める 7.2.1.12 利用者の登録・登録削除のためのアクセス制御手順に、必要のない利用者ID及びアカウントがないかの定期的な、点検、及び、削除又は停止することを含める 7.2.1.13 利用者の登録・登録削除のためのアクセス制御手順は、重複する利用者IDを別の利用者に発行しないことを確実にするよう定める 7.2.1.14 利用者のアクセス役割を、業務上の要求事項に基づいて確立する(利用者のアクセス役割とは、多くのアクセス権を典型的な利用者アクセス権限プロファイルとして要約したものである。) 7.2.1.15 クラウドサービスの利用者IDの登録・削除をする機能を、クラウド利用者に提供する 7.2.1.16 クラウドサービスの利用者IDの登録・削除をする機能について、クラウド利用者(クラウドサービスの利用を検討する者を含む。)にあらかじめ明示する	ユーザによるユーザIDの管理の誤り	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	ユーザIDの管理が適切に行われること	ユーザIDの窃盗	V2 ユーザプロビジョニングの脆弱性 V3 ユーザプロビジョニング削除の脆弱性	ユーザIDの不正奪取、不正作成を防ぐため、ユーザ認証にかかわる脆弱性対策と早期発見の仕組みを整える	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置(例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用)を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する(ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。) 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御(例えば、ファイアウォール)を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	ユーザIDの管理が適切に行われること	ユーザIDの窃盗	V1 認証、認可、課金管理（AAA）の脆弱性	サービス管理のためのアプリケーションの脆弱性を利用した不正や迷惑行為を防ぐため、脆弱性対策と早期発見の仕組みを整える。	8.6.1.1 技術的ぜい弱性には、クラウドサービスの提供にかかわる情報システムの技術的ぜい弱性、クラウドサービスを提供する情報システムの技術的ぜい弱性、及びクラウドサービスとして提供される情報システムの技術的ぜい弱性を含める 8.6.1.2 潜在していた技術的ぜい弱性を特定したときは、適切、かつ、時機を失しない処置をとる 8.6.1.3 技術的ぜい弱性の管理に関連する役割と責任とを定める 8.6.1.4 技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかかわるリスクアセスメント、パッチの適用、資産移動の追跡及び要求されるすべての調整責務を含む 8.6.1.5 ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する 8.6.1.6 技術的ぜい弱性の情報資源は、資産目録が更新された場合、又は他の新しい若しくは有益な資源を発見したときに更新を行う 8.6.1.7 潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める 8.6.1.8 潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する 8.6.1.9 技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、取るべき処置を実行する 8.6.1.10 技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する 8.6.1.11 パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。） 8.6.1.12 パッチの適用前に、パッチが正しいものであることを検証する 8.6.1.13 パッチの適用前に、それらが有効であること、及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価する 8.6.1.14 利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する 8.6.1.15 利用可能なパッチがない場合は、ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する 8.6.1.16 利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する 8.6.1.17 利用可能なパッチがない場合は、ぜい弱性に対する意識を高める 8.6.1.18 修正パッチの適用、その他実施したすべての手順について監査ログを保持する 8.6.1.19 技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する	ゼロデイ脆弱性を突いた攻撃	

L16: 事業者が管理すべき暗号鍵の喪失

・悪意の関係者により、クラウド事業者が管理すべき暗号鍵が不正利用されることで、ユーザの機密データの漏えいが生ずる。
・クラウド事業者が暗号鍵を喪失することでデータの復号が困難となり、ユーザのデータにおける完全性が損なわれる。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	－	－	－	－	－	－	
	機能層	－	－	－	－	－	－	
物理層		容易に推測されない暗号鍵を生成できること	暗号鍵の漏えいや危殆化による情報漏えい	V12 乱数生成器への低エントロピーの入力	安全な方法で鍵生成を行う	8.3.2.3 かぎの生成、保管、及び保存のために用いられる装置は、物理的に保護する 8.3.2.4 暗号かぎの生成は、アクセス管理された安全な環境で実施する 8.3.2.6 かぎ管理システムでは、種々の暗号システム及び種々の業務用ソフトウェアのためのかぎ生成のために、一連の合意された標準類、手順及びセキュリティを保った手法を定める 8.3.2.7 かぎ管理システムでは、公開かぎ証明書の生成及び入手のために、一連の合意された標準類、手順及びセキュリティを保った手法を定める 8.3.2.10 かぎ管理システムでは、かぎの変更又は更新のために、一連の合意された標準類、手順及びセキュリティを保った手法を定める。ここには、かぎをいつ、どのような方法で変更するかの規則も含める	・漏えいしている事実を発覚させない攻撃者による盗聴（暗号鍵の変更前の期間） ・暗号の危殆化	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	暗号鍵の漏えい、喪失、破壊、不正使用がないこと	暗号鍵の漏えいや危殆化による情報漏えい	V11 不適切な鍵管理手順	・暗号鍵の管理手続きを整備し、それに基づいた運用を行う ・暗号鍵が漏えいしたり、暗号アルゴリズムが危殆化した場合に備え、鍵やアルゴリズムの変更手続きを整備し、それに基づいた運用を行う	8.3.2.1 すべての暗号かぎは、改変、紛失、及び破壊から保護する 8.3.2.2 秘密かぎ及びプライベートかぎは、認可されていない開示から保護する 8.3.2.5 暗号かぎをバックアップとして保存する場合、物理的にアクセス管理された環境にオフラインの状態で保管する 8.3.2.8 かぎ管理システムでは、意図する利用者へのかぎ配布のために、一連の合意された標準類、手順及びセキュリティを保った手法を定める。ここには、受領時に、かぎをどのような方法で活性化するか(使える状態にするか)についても含める 8.3.2.9 かぎ管理システムでは、かぎの蓄積のために、一連の合意された標準類、手順及びセキュリティを保った手法を定める。ここには、かぎをいつ、どのような方法で変更するかの規則も含める 8.3.2.11 かぎ管理システムでは、危険になったかぎの対処のために、一連の合意された標準類、手順及びセキュリティを保った手法を定める 8.3.2.12 かぎ管理システムでは、かぎを無効にするために、一連の合意された標準類、手順及びセキュリティを保った手法を定める。ここには、かぎの取消し又は非活性化する方法も含める 8.3.2.13 かぎ管理システムでは、事業継続管理の一環として、紛失したかぎ又は破損したかぎを復旧するために、一連の合意された標準類、手順及びセキュリティを保った手法を定める 8.3.2.14 かぎ管理システムでは、かぎの保管のために、一連の合意された標準類、手順及びセキュリティを保った手法を定める 8.3.2.15 かぎ管理システムでは、かぎの破壊のために、一連の合意された標準類、手順及びセキュリティを保った手法を定める 8.3.2.16 かぎ管理システムでは、かぎ管理に関連する活動の記録と監査のために、一連の合意された標準類、手順及びセキュリティを保った手法を定める 8.3.2.17 セキュリティが損なわれる可能性を低減するために、かぎが限定された期間内だけで用いられるように、かぎの活性化及び非活性化の期日を定める 8.3.2.18 かぎが用いられる限定された期間は、暗号による管理策を利用している環境及び認識しているリスクに基づいて定める 8.3.2.19 公開かぎは、真正性を保証するため、公開かぎ証明書を付ける 8.3.2.20 公開かぎ証明書は要求された信頼度を提供するために適切な管理策及び手順を備えている、認知された組織によって発行する 8.3.2.21 暗号サービスの外部供給者(例えば、証明機関)とのサービスレベルに関する合意又は契約の内容には、賠償責任、サービスの信頼性及びサービス提供のための応答時間に関する事項を含める 8.3.2.22 公開している公開かぎや公開かぎ証明書は、改ざんによる攻撃から守るために、適切なアクセス管理をする	・漏えいしている事実を発覚させない攻撃者による盗聴(暗号鍵の変更前の期間) ・暗号の危殆化	

L17: 不正な探査・スキャンの実施

・攻撃のためのデータ収集が、クラウドサービスの環境を通じて、より容易に行われる可能性がある。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	論理ネットワークへのアクセス制御が有効であること	クラウド内部のネットワークの盗聴	V17 内部(クラウド)ネットワークへの偵察行為が発生する可能性	ユーザが利用するネットワークへの偵察行為(ポートスキャンなど)を制限するか、又は偵察行為(ポートスキャンなど)を行う者を特定できる仕組みを設けて監視する	6.6.1.1 ネットワークには、クラウドサービスの提供にかかわるネットワーク、クラウドサービスを提供するネットワーク、及びクラウドサービスに含まれ提供されるネットワークを含める 6.6.1.2 ネットワーク管理者は、ネットワークにおける情報のセキュリティ及び接続したネットワークサービスの認可されていないアクセスからの保護を確実にする仕組みを整備する 6.6.1.3 適切と判断される場合には、ネットワークの運用責任を、コンピュータの運用から分離する 6.6.1.4 遠隔地に所在する設備(利用者の領域に設置した設備を含む。)の管理に関する責任及び手順を確立する 6.6.1.5 公衆ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及び業務用ソフトウェアを保護するために、特別な管理策(受信規制又は発信規制を含む)を確立する 6.6.1.6 セキュリティに関連した活動を記録できるように、適切なログ取得及び監視を適用する 6.6.1.7 サービスの最大限の活用及び管理策の情報処理基盤全体への一貫した適用の確実化のために、様々な管理作業を綿密に調整する 6.6.1.10 ネットワーク上の機器では、アクセス制御方針に基づき、すべてのネットワークインタフェースでアクセス制御(受信規制又は発信規制を含む)を実施する 6.6.1.12 ネットワーク上の機器では、業務に使用していない空きポートへの接続を制限する 6.6.1.14 ネットワーク上の不正なイベントを監視するため、侵入検知システムを導入する 6.6.1.15 侵入検知システムが、常に最新の攻撃・不正アクセスに対応可能なように、定義ファイル、検知ルールなどの更新を実施する	検知し、対処する前の許可されないアクセスの可能性	
	機能層	−	−	−	−	−	−	
物理層		物理ネットワークへのアクセスを制御できること	サイドチャネル攻撃(装置の動作を物理的手段で測定し、解析することにより、装置内部のデータを取得する攻撃)	V18 共同利用者からの覗き見の可能性	装置の動作を物理的手段で測定し、解析されないため、装置を物理的に保護する	5.2.1.14 装置を保護するために、放射される電磁波の解析、消費される電力の解析、故障発生時の動作の解析などによる情報漏えいのリスクが最小限になるように、取扱いに慎重を要する情報を処理する装置を保護する	新たなサイドチャネル手法による攻撃	

レイヤ	目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
		脅威	脆弱性				
サービス管理系	不正アクセスが生じたことを速やかに検知し、対象ネットワークへのアクセス制限などの対策を講じることができること	クラウド内部のネットワークの盗聴	V17 内部（クラウド）ネットワークへの偵察行為が発生する可能性	管理用ネットワークへの偵察行為（ポートスキャンなど）を制御する	7.4.4.1 遠隔診断用及び環境設定用のポートには、クラウドサービスの提供にかかわる情報システム、クラウドサービスを提供する情報システム、及び提供するクラウドサービスにおけるポートを含める 7.4.4.2 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、遠隔診断用及び環境設定用のネットワークを他のネットワークから物理的又は論理的に分離する 7.4.4.3 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、施錠を利用する 7.4.4.4 遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、ポートへの物理的なアクセスを制御するサポート手順を利用する 7.4.4.5 コンピュータ又はネットワーク設備上に導入されたサービス、ポート及び類似の設備で、業務機能に特に必要でないものは、動作しないようにするか、又は除去する 7.4.4.6 ハードウェア及びソフトウェアのサポート手順には、保守要員との間で合意できた場合にだけ、遠隔診断用及び環境設定用のポートへのアクセスを可能にすることを確実にすることを含める	検知し、対処する前の許可されないアクセスの可能性	

L18: 証拠提出命令と電子的証拠開示

・クラウドサービス上にデータが集中することで、司法当局によるデータの押収が行われた場合に、開示したくないデータまで開示されるリスクが増大するため、ユーザによるクラウドサービス利用を躊躇させる要因となる可能性がある。

<table>
<tr><th colspan="2" rowspan="2">レイヤ</th><th rowspan="2">目指すべき水準</th><th colspan="2">想定されるリスク</th><th rowspan="2">クラウド事業者における
対策の要点</th><th rowspan="2">対応するクラウド管理基準</th><th rowspan="2">残留リスク</th><th rowspan="2">備考</th></tr>
<tr><th>脅威</th><th>脆弱性</th></tr>
<tr><td rowspan="2">抽象化層</td><td>リソース層</td><td>－</td><td>－</td><td>－</td><td>－</td><td>－</td><td>－</td><td></td></tr>
<tr><td>機能層</td><td rowspan="3">法執行対象データだけが記録された媒体を用意できること</td><td rowspan="3">複数ユーザのデータが記録された媒体の押収</td><td rowspan="3">V6 リソース分離の欠如（物理リソースの共有）
V30. 司法管轄権に関する情報の欠如
V29. 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如</td><td rowspan="3">保全・押収の対象となるデータの記録された媒体から、対象外のデータを別の媒体に移動してサービスを継続し、対象外のデータの痕跡を目的の媒体から完全に消去する</td><td>C.1.1.1　一部の情報処理設備（物理サーバ、物理ストレージ、物理ネットワーク機器、通信ケーブル、アクセス回線など）の機能の喪失がクラウドサービスを停止させないために、情報処理設備を冗長化する
C.1.1.3　一部の情報処理設備（物理サーバ、物理ストレージ、物理ネットワーク機器、通信ケーブル、アクセス回線など）の機能の喪失がクラウドサービスを停止させないために、代替の情報処理設備に速やかに切替える（ライブマイグレーション、フェイルオーバーなど）</td><td rowspan="3">対象範囲の限定が不十分な法執行</td><td></td></tr>
<tr><td colspan="2">物理層</td><td></td></tr>
<tr><td colspan="2">サービス管理系</td><td>5.2.6.3 取扱いに慎重を要する情報を格納した装置の処分は、物理的に破壊し、又はその情報を破壊、消去若しくは上書きする。消去又は上書きには、標準的な消去又は初期化の機能を利用するよりも、元の情報を取り戻せなくなるようにする技術を利用する

11.1.1.2 各情報システム及び組織について、すべての関連する法令、規則及び契約上の要求事項を満たすための具体的な管理策及び具体的責任を同様に定め、文書化する
11.1.1.3 情報システム及び組織が順守すべき法令、規制及び契約のある地域（国、州など）を、クラウド利用者に明示する

2.2.2.11 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、法的な問題に関する責任及び法的要求事項を満たすことを確実にする。特に、契約が他国のクラウド利用者との協力にかかわるものである場合、その国の法制度を考慮に入れる</td><td></td></tr>
</table>

L19: 司法権の違い

・クラウドサービスの物理的インフラが設置される地域（国、州など）によっては、異なる司法上の解釈や独裁的な警察権力、国際的取り決めが遵守されないなどの影響がユーザに及ぶ可能性がある。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	－	－	－	－	－	－	－
	機能層	－	－	－	－	－	－	－
物理層		－	－	－	－	－	－	－
サービス管理系		ユーザデータが格納された物理媒体の地域（国、州など）が特定できること	予期しない差押え	V30. 司法管轄権に関する情報の欠如 V29. 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如	クラウドプロバイダ及びシステムが順守すべき法令、規則、契約のある地域（国、州など）を明示する	11.1.1.2 各情報システム及び組織について、すべての関連する法令、規則及び契約上の要求事項を満たすための具体的な管理策及び具体的責任を同様に定め、文書化する 11.1.1.3 情報システム及び組織が順守すべき法令、規制及び契約のある地域（国、州など）を、クラウド利用者に明示する 2.2.2.11 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、法的な問題に関する責任及び法的要求事項を満たすことを確実にする。特に、契約が他国のクラウド利用者との協力にかかわるものである場合、その国の法制度を考慮に入れる	合法的な法執行による差押え	

L20： データ保護

・クラウドサービス事業者が、ユーザが許可していないデータの処理を行う可能性があることで、ユーザがクラウド利用を躊躇する可能性がある。
・ユーザが合法的でない方法で収集したデータが、クラウドサービス上に蓄積される可能性がある。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	あるユーザが論理リソースを違法に使用しても、他の論理リソースに法的処分が及ばないこと	ユーザが保存した違法データによるデータの押収、サービス停止	V30. 司法管轄権に関する情報の欠如 V29. 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如	クラウドプロバイダの事業地域（国、州など）及びシステムの所在地域（国、州など）における差押え手続に適したデータ保全を行う	11.1.1.2 各情報システム及び組織について、すべての関連する法令、規則及び契約上の要求事項を満たすための具体的な管理策及び具体的責任を同様に定め、文書化する 11.1.1.3 情報システム及び組織が順守すべき法令、規制及び契約のある地域（国、州など）を、クラウド利用者に明示する 2.2.2.11 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、法的な問題に関する責任及び法的要求事項を満たすことを確実にする。特に、契約が他国のクラウド利用者との協力にかかわるものである場合、その国の法制度を考慮に入れる	物理媒体単位の差押え	
	機能層	－	－	－	－	－	－	
物理層		－	－	－	－	－	－	
サービス管理系		データ転送・処理が、それが行われる地域（国、州など）の法に抵触しないこと	・クラウド内外のデータ転送の違法性 ・クラウド内のデータ処理の違法性	V30. 司法管轄権に関する情報の欠如 V29. 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如	クラウドプロバイダの事業地域（国、州など）及びシステムの所在地域（国、州など）において順守すべき法令、規則、契約を適切に把握し、順守する	11.1.1.2 各情報システム及び組織について、すべての関連する法令、規則及び契約上の要求事項を満たすための具体的な管理策及び具体的責任を同様に定め、文書化する 11.1.1.3 情報システム及び組織が順守すべき法令、規制及び契約のある地域（国、州など）を、クラウド利用者に明示する 2.2.2.11 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、法的な問題に関する責任及び法的要求事項を満たすことを確実にする。特に、契約が他国のクラウド利用者との協力にかかわるものである場合、その国の法制度を考慮に入れる	・誤認に基づく法執行 ・悪意に基づく訴訟	

L21： ライセンス

・同一期間内に同じ数のマシンを使用していた場合でも、他のソフトウェアに比べてクラウド利用者のライセンス費用は飛躍的に増大することがある。
・PaaSやIaaSの場合は、クラウド内部で発生した独自の成果物（新しいアプリケーションやソフトウェア等）がユーザの知的財産として保護されない可能性がある。

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の要点	対応するクラウド管理基準	残留リスク	備考
			脅威	脆弱性				
抽象化層	リソース層	－	－	－	－	－	－	－
	機能層	－	－	－	－	－	－	－
物理層		－	－	－	－	－	－	－
サービス管理系		利用形態に依存したライセンス課金を行うアプリケーションなどについて、実態に応じた適切な利用情報の管理が行われること	予期しないソフトウェアライセンス課金	V31. 利用規約の完全性と透明性の欠如	ユーザが利用するソフトウェアライセンスの課金に影響を与えるシステム情報を明確にする	2.2.2.11 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、法的な問題に関する責任及び法的要求事項を満たすことを確実にする。特に、契約が他国のクラウド利用者との協力にかかわるものである場合、その国の法制度を考慮に入れる 2.2.2.12 クラウド利用者に、提供するクラウドサービス上のクラウド利用者の情報及び組織の情報又は資産へのアクセスを許す前に、知的財産権（IPR）及び著作権の取扱い、並びに共同作業の成果の保護のあり方を明確にする 11.1.2.1 ソフトウェア製品及び情報製品の合法利用を明確に定めた知的財産権順守方針を公表する 11.1.2.4 適切な財産登録簿を維持管理し、知的財産権保護が要求事項となっているすべての資産を識別する 11.1.2.5 使用許諾を得ていることの証明及び証拠並びにマスタディスク、手引などを維持管理する 11.1.2.6 許諾された最大利用者数を超過しないことを確実にするための管理策を実施する 11.1.2.7 認可されているソフトウェア及び使用許諾されている製品だけが導入されていることの点検を行う 11.1.2.8 適切な使用許諾条件を維持管理するための方針を定める 11.1.2.9 ソフトウェアの処分又は他人への譲渡についての方針を定める 11.1.2.11公衆ネットワークから入手するソフトウェア及び情報の管理方針を定め、また、提示される使用条件に従う	・説明もれ ・合意もれ ・合意の齟齬 ・実施の誤り	