公開版

クラウドサービス（IaaS）の技術的評価ガイド

第１.０版

平成 28 年 3 月

特定非営利活動法人 日本セキュリティ監査協会

目次

1. 本書の位置付け及び目的

本書は、ISO/IEC 27017:2015（ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）に記載された管理策及び実装指針に対する実装並びにその運用を監査するための指針を提供する。本書は、ISO/IEC 27002:2013 の付属書 A に記載された管理策及び実装指針に対して新たに指針を追加している。

本書は、クラウドサービスのうちコンピュータリソースを提供する IaaS を想定して、監査に必要な技術的な着目点及び監査方法を解説する。

クラウドサービスを提供するシステムは、IaaS においても千差万別であり、技術的進歩が著しいことから日々変化する。本書は特定のシステムを想定したものではなく、監査の方法、留意点、監査対象などについて、実践指針となることを狙っている。

本書は、ISO/IEC 27017 に示されるクラウドサービスに特有な情報セキュリティ管理策またはその実装についてのみ解説を行う。

ここでは、セキュリティ管理策が正しくクラウドシステムに実装されているかを監査することに焦点を当てて解説する。（図 1 参照）

本書は、クラウドサービスを提供するコンピュータシステムに関する、技術的な監査方法について、モデルと例により解説するものである。

本書は、監査人に対してクラウドサービスに特有な監査ポイントの会得を提供する。また、監査を受ける側の技術者には、どのようにサービスが評価され、どのように証跡を示すべきかのヒントを与える。

クラウドサービス事業者は、採用したセキュリティ管理策のうち、IT システムで実装可能な事項を自己のクラウドシステムに組み込むであろう。

本指針に従うことにより、監査人が適切な監査を実施することに加え、クラウドサービス事業者が自サービスを ISO/IEC 27017 に準拠させるための具体的な管理策を策定することが可能となる。

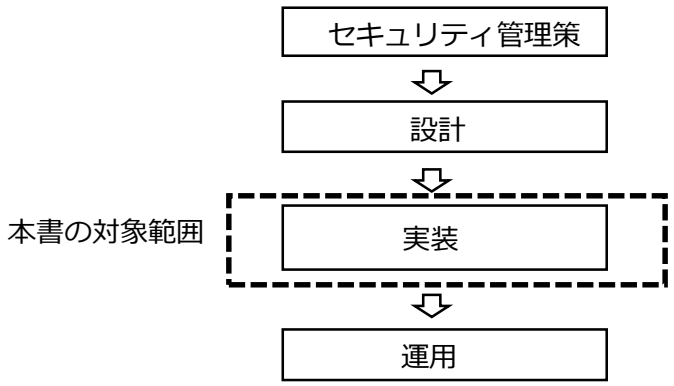

図 1　本書の対象範囲

2. 国際標準との関係

ISO/IEC 27017 に加え、次の規格が関連している。

(1) ISO/IEC 27018 Information technology – Security techniques - Code of practice for PII protection in public clouds acting as PII processor

ISO/IEC 27018 は、クラウドサービスにおける個人識別情報 Personally Identifiable Information (PII)について規定している。

クラウドサービス事業者が保持すべき PII としては、クラウドサービス利用者に関する情報がある。これらは後に述べるクラウドサービス環境モデルの「サービス管理」において、管理・格納される。サービス管理における PII の扱いは、ISO/IEC 27018 に準拠する必要がある。

なお、本書が対象とする IaaS では、クラウドサービス利用者が利用する仮想マシンの中に格納される情報は、クラウドサービス利用者自身が情報セキュリティを講じる責任があり、クラウドサービス事業者は仮想マシン中の PII について管掌できないことから、本書の対象外となる。

(2) ISO/IEC 17788 Information technology – Cloud computing – Overview and vocabulary

本書は、ISO/IEC 17788 に規定するクラウドコンピューティングに関する概観および用語を準用する。

(3) ISO/IEC 17789 Information technology – Cloud Computing - Reference Architecture

クラウドサービスを構成するコンポーネントの基本的な考え方については、ISO/IEC 17789 を踏襲する。ただし、ISO/IEC 17789 では、役割と活動の観点から、クラウドコンピューティングのアーキテクチャを規定している。これに対し、監査においては、仮想化機構の設定の確認など、クラウドシステムの実装を意識した観点が必要となる。このため、本書では、クラウドシステムの実装をモデル化した実装モデルを提示し、ISO/IEC 17789 の規定による機能コンポーネントと監査項目との対応付けを図っている。

3. 本書の構成

本書は、まず IaaS を想定したクラウドサービス提供環境のモデルを提示する。このモデルは、リソース種別と仮想化との関係、クラウドサービス利用者とテナントの概念を定義する。

監査要件は、共通事項、サービス管理、サーバ、ネットワーク及びストレージの各々について、次の順に記述されている。本文中における表の構成については下記注記を参照されたい。

(1) 典型的な技術の解説

仮想化の実装に関する技術的要素と手引きの説明。複数の実装方式がある場合には、典型的な幾つかの方式を列挙する。

(2) ISO/IEC 27017 で規定されている管理策

仮想化に関連する ISO/IEC 2017 の管理策の項番とタイトル。

(3) ISO/IEC 27017 の管理策に対する監査方法

ISO/IEC 2017 の管理策に対する監査方法の指針。複数の実装がある場合は、その１つを示す。

注記：表の構成

```
管理策　（27017 に記載された管理策の項番とタイトル）
追加技術情報
1　技術的解説(その 1)
　　セキュリティ実装基準　（詳細管理策）
　　セキュリティ実装基準する技術的解説
　　1.1　実装ガイド、想定される証拠、監査技法（その１の１）
　　　　実装ガイド
　　　　想定される証拠
　　　　監査技法
　　1.2　実装ガイド、想定される証拠、監査技法（その１の 2）
　　　　実装ガイド
　　　　想定される証拠
　　　　監査技法
　　・・・
2　技術的解説(その 2)
　　セキュリティ実装基準（詳細管理策）
　　セキュリティ実装規準に関する技術的解説
　　2.1　実装ガイド、想定される証拠、監査技法（その２の 1）
　　　　実装ガイド
　　　　想定される証拠
　　　　監査技法
　　2.2　実装ガイド、想定される証拠、監査技法（その２の 2）
　　　　実装ガイド
　　　　想定される証拠
　　　　監査技法
　　・・・
```

4. クラウドサービス (IaaS) 環境モデル

4.1 モデル導入の意義

クラウドサービスに用いられる技術は多岐にわたることから、これらを仔細に取り上げることは個別且つ具体的過ぎる。また、クラウドサービスに用いられるコンピューティング技術は新しい分野であり、技術的に発展途上にある。これらのことから、個別且つ具体的な技術に基づく評価の方法を定めることは標準化になじまない。モデル化により、管理策の意図するところを具体的な技術としてイメージすることができるため、評価に際しての具体的な方法を示唆することができる。実際に評価を行う際に、このモデルを念頭に置き、管理策のために実装されている実際の技術が、管理策の意図に沿ったものであるか、また、それらの評価のための証拠の収集はどのようにするかを、評価者（または監査人）が想起できる。

4.2 モデルと構成要素

本書が想定する IaaS において、クラウドサービスを提供する環境は、利用者が直接使用する仮想リソース、仮想化を具現化する仮想化機構、物理リソース、及び仮想化機構を制御しリソースをサービスとして提供するためのサービス管理とから成る。

図 2 にラウドサービスを提供するシステムの実装モデルを示す。

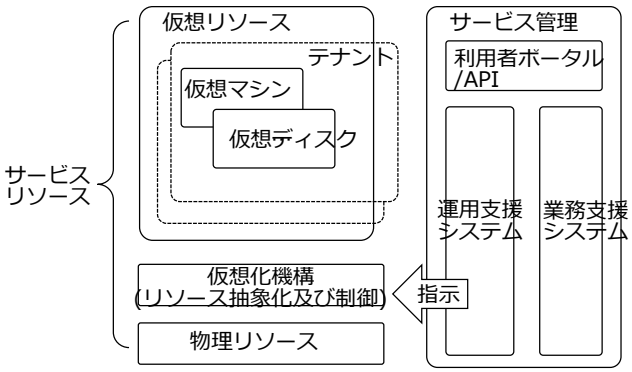

図 2　実装モデル

本モデルの重要な概念は、リソースの仮想化と分離である。仮想化機構は、リソース抽象化及び制御コンポーネントにより、テナントごとにアクセス権などを分離し、仮想化されたリソース（仮想リソース）として提供する。

テナントはクラウドサービス利用者ごとに割り当てられた仮想リソースを集約する領域であり、他のクラウドサービス利用者とアクセスを分離する境界である。通常、複数のユーザがテナントをアクセスし情報処理を実行する。

このモデルは、4 つの要素をもち、このうち物理リソース、仮想化機構及び仮想リソースは、リソース種別としてサーバ、ネットワーク及びストレージに区分けされる。

(1) 物理リソース

物理リソースは、クラウドサービスを提供するために必要となる物理的機器である。サーバ機器、ネットワーク機器、ストレージ機器が構成要素となる。物理ネットワーク機器の例としては、サーバとネットワークを接続する物理 NIC（Network Interface Card）が挙げられる。物理ストレージ機器としては、サーバとストレージを接続する HBA（Host Bus Adapter） 、ファイバスイッチなどが挙げられる。

(2) 仮想化機構

物理リソースを仮想化し、クラウドサービスで提供される仮想リソースを生成する機能を実装する。サーバの仮想化の場合はハイパバイザがこれにあたる。ネットワークの仮想化では、VLAN（Virtual Local Area Network）や SDN（Software Defined Network）などがこれにあたる。ストレージにおいては、多くの場合ストレージ装置がこの仮想化機構を有している。

(3) 仮想リソース

仮想化機能によって生成され、クラウドサービスにおいてクラウドサービス利用者に提供される。仮想化機能は、仮想リソースを実現するための機能に対し、仮想リソースは生成された仮想リソースの集合を指す概念である。

注記：仮想リソースは必ずしも該当するリソース種別の仮想化機構によって生成されるとは限らない。仮想ネットワークを構成する仮想スイッチはサーバ仮想化を行うハイパバイザにより生成される場合がある。

(4) サービス管理

サービス管理は、クラウドサービス事業者がサービスを提供するためのシステムであり、クラウドサービス利用者にシステムのインタフェースを提供する。前述の仮想化機能を利用し、クラウドサービスに必要な仮想リソースのプロビジョニングなどを行う。また、物理リソースの監視、管理などを行い、クラウド提供環境全体が健全に動作するための制御を司っている。

プロビジョニングや VM（Virtual Machine、仮想マシン）の起動/停止など、クラウドサービス利用者が許された範囲の操作を行うためのポータル機能や、ユーティリティ、API などもこのサービス管理に含まれる。

4.3 ISO/IEC 17789 との関係

ISO/IEC 17789 で規定される機能コンポーネントは、実際にはこの仕組みの中で、対象となるリソースの種別、仮想化の階層により、それぞれを実現する実装上の要素によって実現される。

アクセス制御を例にした場合、次のようになる。

- 物理ディスクのアクセス制御　・・・ ディスク装置
- テナントごとのアクセス権管理 ・・・ 仮想化機構
- 仮想ディスクのアクセス制御　・・・ 仮想化機構
- 各 VM の中のアクセス制御　　・・・ VM の OS

ISO/IEC 17789 で、多層機能（Multi-layer Functions)として規定される機能、コンポーネントの内、サービスに提供に関わるものは、本規格の実装モデルではサービス管理に含まれる。業務支援機能(BSS、Business Support Systems)や運用支援機能(OSS、Operational Support Systems)がこれに当たる。

多層機能のなかで、統合(Integration)とセキュリティに関するものは、前述のアクセス権と同様に、対象となる機構において実装される。

5. 実装モデルにおける共通実践事項

ここでは、後に述べるサーバ仮想化、ネットワーク仮想化、ストレージ仮想化のいずれにも共通する監査手引きについて解説する。

5.1 クラウドサービスにおける仮想化技術の適用

IaaS では、クラウドサービス利用者は仮想リソースをアクセスする。クラウドシステムの技術的なレビューでは、仮想化機構に関して次に挙げる事項の評価が求められる。

(1) 運用のセキュリティ

仮想化機構に対する操作は、直接的に仮想リソースに影響を与えることから、操作が適正に実施されている。

(2) 環境の定義

クラウドサービス利用者に提供すべきログ、イベント（エラーの発生や警告、閾値の突破など）が仮想化機構のパラメータ等に定義され、これら情報が収集、蓄積されるようになっている。

仮想化機構、仮想リソースの冗長化などについても、仮想化機構のパラメータとして定義されることから、可用性などに関する監査の対象となる。

(3) キャパシティ管理

各仮想化機能において、クラウドサービス利用者に提供するリソースと、提供元となる物理リソースの関係が管理されている。

一般に、クラウドコンピューティングでは、統計的手法により同時使用可能な論理リソースを提供する。このため、提供される仮想リソースの総和が、物理リソースの総和よりも大きくなる。

5.2 仮想化共通事項に関する監査

5.2.1 運用のセキュリティ <12>

管理策		12.1.2　変更管理
追加技術情報		クラウドサービス利用者にとって、影響が大きな変更として次が考えられる。 サーバ関係: －バイパバイザの変更、バージョンアップ －ハイパバイザの各種パラメータの変更、環境定義の変更 ネットワーク関係: －仮想 LAN 定義の変更 －スイッチ、ルータ、ファイアウォール、ロードバランサなどの構成、環境定義、各種パラメータの変更 ストレージ関係: －デバイス定義の変更 －SAN のゾーニング等の変更 ハードウェア全般: －ファームウェアのバージョンアップ ソフトウェア全般: －ソフトウェアのバージョンアップ －プログラム修正(パッチ)の適用 －セキュリティ対策修正の適用 こられ変更は、多岐に渡り、クラウドサービス利用者に対する影響度も異なる。このため、一般に、どの水準以上を通知するかについては、クラウドサービス利用者とクラウドサービス事業者との間で合意されている。
1	セキュリティ実装基準（詳細管理策）	IT リソース間に依存関係があるため、変更の対象となるリソースに依存する他のリソースを利用しているクラウドサービス利用者に対しても影響が波及する。 このため、変更管理においては、直接的、間接的に影響を受けるユーザを特定し適切に通知する。
	セキュリティ実	クラウドを構成するハードウェア、ソフトウェアは、一般に CMDB (Configuration

	装基準の技術的解説	Management Database)により管理されている。 また、クラウドサービス利用者とハードウェア、ソフトウェアとの対応も CMDB、若しくは運用支援システム(OSS)あるいは業務支援システム(BSS)により管理されている。 変更対象となるハードウェア及びソフトウェアとクラウドサービス利用者との関係は、これらのシステムにより管理される。	
	1.1	監査実施ガイド	変更対象となる IT リソースを使用しているクラウドサービス利用者を特定しているかを確認する。
		想定される証拠	CMDB などの検索結果（特定の IT リソースを指定し、それを利用しているクラウドサービス利用者を検索した結果など。）
		監査技法	観察
	1.2	監査実施ガイド	IT リソース間に依存関係や影響関係が有る場合、その関係が把握されているかを確認する。
		想定される証拠	CMDB などの検索結果（IT リソース間に依存関係が有る場合、特定の IT リソースを指定し、その影響を受ける他の IT リソースを検索した結果など。）
		監査技法	観察
	1.3	監査実施ガイド	変更管理に関し、クラウドサービス利用者に提供すべき情報が、適正に提供されることを確認する。 提供される情報について、以下を確認する。 －クラウドサービス利用者に関係する変更であること。（間接的影響についても提供されること。） －利用者との合意、もしくは合理的に妥当な水準の影響について提供されること。
		想定される証拠	クラウドサービス利用者宛のメール クラウドサービス利用者向けのポータルなど
		監査技法	観察

管理策		12.1.3　容量・能力の管理	
追加技術情報		クラウドサービス事業者が用意するコンピューティングソースの代表的なものには以下がある。 －CPU 処理能力、コアメモリ －ネットワーク帯域 －ストレージ容量 クラウドにおいては、コンピューティングリソースの一時的な利用のピークがあることから、ピークにおいてもコンピューティングリソースの不足が発生しないようにキャパシティ管理を行う。 コンピューティングリソースは、クラウドシステムの区画を超えて提供できない場合があることから、キャパシティ管理は、クラウド全体だけでなく、区画ごとにも行う。	
1	セキュリティ実装基準（詳細管理策）	コンピューティングリソースの追加などが必要となる水準を定め、当該水準に達した際に必要な措置を講じる。	
	セキュリティ実装基準の技術的解説	コンピューティングリソースについて、一定の閾値を定め、使用量がこれを超える場合には警告が発せられるような監視を行なう。 監視は、クラウドシステム、IT 機器、ソフトウェア等により、コンピューティングリソースの使用状況を監視することで行なわれる。	
	1.1	監査実施ガイド	クラウドシステムにおいて、キャパシティ管理が必要となるコンピューティングリソースについて、必要な監視が行なわれているか確認する。
		想定される証拠	クラウド監視システムの監視定義 キャパシティの使用状況のレポート出力
		監査技法	観察
	1.2	監査実施ガイド	使用キャパシティが閾値を超えた場合、警告が発せられることを確認する。
		想定される証拠	クラウド監視システムの警告設定（閾値による警告発生が定義されていることの確認） クラウド監視システムのイベントログ(過去に警告が発せられたことの確認)
		監査技法	観察

管理策	CLD.12.1.5　　実務管理者の運用のセキュリティ
追加技術情報	一般にクラウド環境に対する変更操作を失敗した場合、クラウドサービス利用者のクラウド利用を阻害するなどの影響を生じる。 このうち、クラウドサービス利用者の資産に損害を与える最大のものは、ストレージ上

		のデータの削除・破壊である。 一時的なサービスの中断、クラウド環境のダウンなどは、処理中のトランザクションの破棄が発生するものの、資産の破壊にまでは至らないと考えられる。	
1	セキュリティ実装基準（詳細管理策）	削除が可能な操作は、事前に許可されたオペレータだけが可能になっている。	
	セキュリティ実装基準の技術的解説	クラウドサービス利用者が使用しているストレージに対し、データの削除が可能な管理者権限での操作については通常のオペレーションとは異なる認証を実施する。	
	1.1	監査実施ガイド	管理者権限での操作が可能な ID が限定され、通常の使用とは異なる手続きで使用されることを確認する。
		想定される証拠	ストレージ操作ユーティリティ等のユーザ ID の一覧 管理者権限を使用する際のオペレーション
		監査技法	観察

管理策		12.4.1　イベントログ取得	
追加技術情報		本管理策の「クラウドサービスのための関連情報」に記載されているとおり、本書で対象としている IaaS においては、クラウドサービス事業者によるログおよびモニタリングの責任範囲は、クラウドコンピューティング基盤要素（cloud computing infrastructure components）である。 具体的には、以下が挙げられる。 －ハイパバイザのログ、イベント －ファイアウォール、ロードバランサのログ、イベント －ストレージ装置、SAN 機器のログ、イベント これらの基盤要素は、複数の利用者が共用していることから、これら利用者に関するログが蓄積されている。このため、ログの提供にあたっては、当該利用者のもののみを抽出して提供する必要がある。	
1	セキュリティ実装基準（詳細管理策）	クラウドサービス利用者に提供する対象となるログを収集し、イベントなどをモニタリングする。	
	セキュリティ実装基準の技術的解説	クラウドコンピューティングの基盤要素の機能により、ログの出力、イベントの採取を行なう。 ログ等の出力は、クラウドコンピューティング基盤要素のパラメータ定義等によって設定される。	
	1.1	監査実施ガイド	ログやイベントの採取の設定が、クラウドコンピューティング基盤要素に定義されていることを確認する。
		想定される証拠	クラウドコンピューティング基盤要素のパラメータの定義
		監査技法	観察

管理策		2.4.4　クロックの同期	
追加技術情報		IaaS におけるクラウドサービス利用者のために、クラウド環境との VM の時刻同期が必要である。 VM の時刻同期については、一般に次の 2 つの方式がある。 －NTP(Network Time Protocol)による方式 －ハイパバイザによる方式	
1	セキュリティ実装基準（詳細管理策）	クラウドサービス事業者は、VM の時刻同期のための手段として、NTP もしくハイパバイザのいずれかの方式を用いる。	
	セキュリティ実装基準の技術的解説	クラウドサービス利用者は、自己の利用する VM について、利用者自身が提供される方式に従った時刻同期のためのセットアップを行なう必要がある。	
	1.1	監査実施ガイド	クラウドサービス事業者が、時刻同期のための方式を提供していることを確認する。
		想定される証拠	NTP サーバが提供され、クラウドサービス利用者が当該サーバに NTP プロトコルによりアクセス可能なことを確認する。 ハイパバイザによる時刻同期が提供され、クラウドサービス利用者が同機能を利用して時刻同期が可能なことを確認する。
		監査技法	再実施

管理策		CLD.12.4.5　クラウドサービスの監視	
追加技術情報		一般に、「不正なクラウドサービス利用（nefarious use of cloud services）」を定義することは困難であるため、一定量を越えるネットワークへトラフィックの発生、同様なストレージアクセスなどが検出される。	
1	セキュリティ実装基準（詳細管理策）	“不正なクラウドサービス利用”と規定された状態の発生を、ログや監視機能により検知する。	
	セキュリティ実装基準の技術的解説	12.4.1 を参照。	
	1.1	監査実施ガイド	「不正なクラウドサービス利用」と規定された事象が検知されるように監視システムなどに定義されているか確認する。
		想定される証拠	監視システムのパラメータ定義
		監査技法	観察

管理策		12.6.1　技術的ぜい弱性の管理	
追加技術情報		技術的脆弱性は、対象となるソフトウェアのバージョンにより異なる。一般に、クラウドコンピューティングの基盤では同一ソフトウェアであっても複数の版を使用していることから、使用しているコンピューティングリソースによって、当該脆弱性を有しているか否かの判定が必要となる。	
1	セキュリティ実装基準（詳細管理策）	クラウドコンピューティングの基盤について、技術的脆弱性が発見された場合、当該脆弱性を有するコンピューティングリソースを利用しているクラウドサービス利用者を特定し、同利用者に脆弱性に関する情報を提供する。 コンピューティングリソースとクラウドサービス利用者との対応関係の検索については、「12.1.2 変更管理」に関する解説を参照すること。	
	セキュリティ実装基準の技術的解説	コンピューティングリソースとクラウドサービス利用者との対応関係の検索については、「12.1.2 変更管理」に関する解説を参照すること。	
	1.1	監査実施ガイド	脆弱性が発見されたコンピューティングリソースを使用しているクラウドサービス利用者を特定し、当該利用者に技術的脆弱性に関する情報が提供されることを確認する。
		想定される証拠	技術的脆弱性に関する情報の提供メール、ポータル画面など
		監査技法	観察

6. サービス管理

6.1 サービス管理の概略

サービス管理は、IaaS によって提供される機能のセットであり、クラウドサービス利用者が仮想サーバ、ネットワーク及びストレージを構成することを可能とする。サービス管理は、クラウドサービス利用者にポータルまたは他の手段を通して仮想化された構成の管理オペレーションを提供し、生成された設定を構成管理データベース（CMDB）で維持する。

クラウドサービス事業者により提供される仮想リソースのセキュリティ設定は、クラウドサービス利用者自身の責任により、クラウドサービス利用者自身が実施する。仮想マシンの OS のセキュリティに関する設定などがこの代表例である。

他方、仮想化機能の機能設定、ログの取得などについては、クラウドサービス利用者は直接アクセスすることはできない。

物理リソースと仮想化機構や仮想リソースとの関係、仮想リソースとクラウドサービス利用者との関係などの対応づけもサービス管理の役割である。通常、これらの関係づけのために構成管理データベース(CMDB)が用いられる。

ユーザポータルは、前述の関係づけされた情報に従い、クラウドサービス利用者の仮想リソース、および仮想機能へのアクセスを可能とする。また、クラウドシステムで発生したインシデントの通知や状況の表示などの機能をクラウドサービス利用者に提供する。

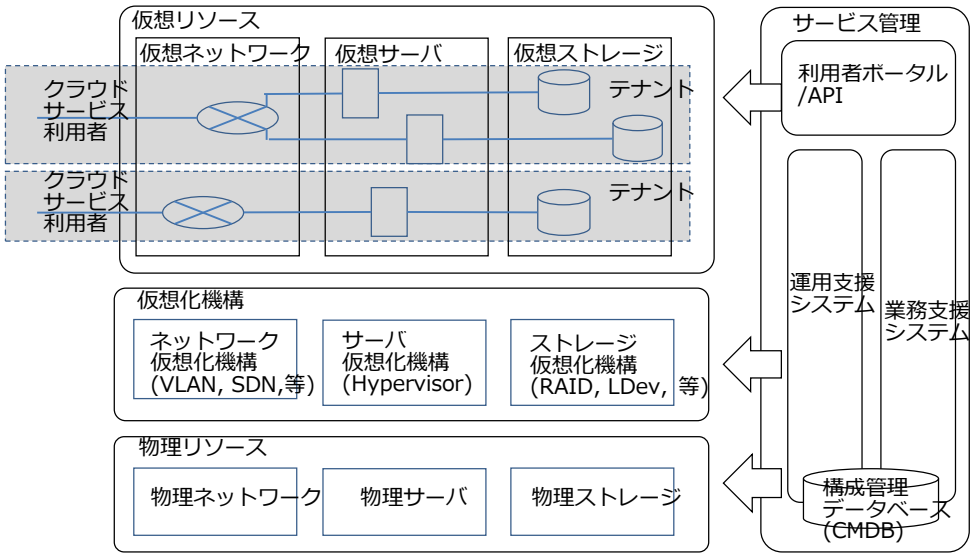

図 3　サービス管理の概観

6.2 クラウドサービスにおけるサービス管理の適用

(1) アクセス制御

各仮想化機能は、仮想化機能自身のアクセス制御、仮想リソースへのアクセス制御の機構を有する。これらは、サーバ、ネットワーク、ストレージの区分ごとに制御の範囲、アクセス権付与の対象(ユーザ ID など)、認証の方法(パスワード)が異なる。また、仮想化機能を直接クラウドサービス利用者に開放することはセキュリティ上の問題となる。サービス管理は、これら問題を解決し、クラウドサービス利用者に対し、妥当なアクセス制御を与えると共に、異なる区分の間でテナントとして統一的なアクセス制御を可能としている。

注記：仮想化機能はクラウドサービス利用者に直接開示すべきではない。

(2) ユーザ認証

アクセス制御の前提として、クラウドサービス利用者に対する適正な認証が行なわれる必要がある。サービス管理においては、ユーザポータルや API がクラウドサービス利用者へのインタフェースとなり、アクセスの最初においてユーザ認証が実施される。

ユーザの権能について、利用できる最大のリソース、課金の残高など、契約、料金などにより決定される事項がある。これらは、業務支援システム(BSS)によって管理される。

他方、前述の仮想機能によるアクセス制御や仮想化機能に関するクラウドサービス利用者によるパラメータの設定などは、運用支援システム(OSS)によって管理される。

(3) 構成管理

物理サーバとその物理サーバ上で動作している仮想サーバとの関係、仮想サーバとクラウドサービス利用者との関係、クラウドサービス利用者と契約条件、課金との関係などは、クラウドサービスの管理・運用上不可欠な情報であり、アクセス制御の付与などにもこれらの関係情報が利用される。

サービス管理では、これらの構成に関する情報を構成管理データベースに格納し管理している。BSS、OSS は、この構成管理データベースを参照、更新しながら動作する。

(4) インシデント管理

クラウドを構成する物理リソース、仮想化機能、仮想リソースなどで発生した事象、クラウドサービス利用者とクラウドサービス事業者間の質疑･応答、通知などのインシデント管理も、通常クラウド管理系が担当する。ユーザポータルなどにおいて、クラウドサービス利用者に対し、インシデント管理に関する機能が提供されることが一般的である。

6.3 サービス管理に関する監査

6.3.1 アクセス制御 <9>

管理策		9.2.1　利用者登録及び登録削除	
追加技術情報		本管理策の対象は、サービス管理におけるユーザの追加、削除である。 仮想リソース（例: VM の OS）での利用者の登録、削除は、対象となるリソース自体の機能をクラウドサービス利用者が操作して行うことが一般的である。	
1	セキュリティ実装基準（詳細管理策）	ユーザの管理は、サービス管理のなかに実装される。 仮想化機能のアクセス制御は、サービス管理によって制御され、クラウドサービス利用者に開放されない。	
	セキュリティ実装基準の技術的解説	サービス管理ポータルにより、ユーザ管理が可能な場合には、ポータルにおいて、登録、削除の手段が提供される。 ユーザ管理はセキュリティ上の重要事項であるため、クラウドサービス事業者がクラウドサービス利用者からの連絡などにより、ユーザの登録、削除を行なうこともある。	
	1.1	監査実施ガイド	クラウドサービス利用者向けのポータル、API などにより、クラウドサービス利用者による ユーザの登録、削除が可能な手段が提供されているかを確認する。
		想定される証拠	ポータルの操作画面と操作結果 API 等のインタフェースと API による操作結果
		監査技法	観察, 再実施

管理策		9.2.2　利用者アクセスの提供（provisioning）
追加技術情報		本項で対象となるのは、サービス管理におけるユーザのアクセスプロビジョニング（access provisioning）である。 仮想リソース（例: VM の OS）でのアクセスプロビジョニングは、対象外である。
1	セキュリティ実装基準（詳細管理策）	ユーザの管理は、サービス管理のなかに実装される。 サービス管理が提供するユーザのアクセス権管理は、必ずしも仮想化機能のアクセス権管理と同一である必要はない。ただし、サービス管理としてクラウドサービス利用者に提示されたアクセス権管理の仕様を実装することが必要である。
	セキュリティ実装基準の技術的	サービス管理のアクセスプロビジョニングは、ポータルのユーザの管理として提供される。

	解説		本管理策の「クラウドサービスのための関連情報」に言及されているシングルサインオンは、サービス管理のポータルなどの間で実装されるものであり、代表的な実装方式としては、SAML(Security Assertion Markup Language)などが挙げられる。
	1.1	監査実施ガイド	ポータルにおける利用者管理機能において、ユーザのアクセス権管理機能が提供されていることを確認する。
		想定される証拠	ポータルの操作画面と操作結果
		監査技法	観察, 再実施
	1.2	監査実施ガイド	シングルサインオン機能が提供されている場合、提供されたプロトコル等により使用可能であるかを確認する。
		想定される証拠	シングルサインオンを実装した外部のアプリケーション 外部アプリケーションを介してのサービス管理へのアクセス結果
		監査技法	観察, 再実施

管理策			9.2.3　特権的アクセス権の管理
追加技術情報			本管理策の対象は、サービス管理におけるユーザのアクセスプロビジョニングである。 仮想リソース（例: VM の OS）のアクセスプロビジョニングは、対象外である。
1	セキュリティ実装基準（詳細管理策）		本管理策に規定される強固な認証（sufficiently strong authentication）は、サービス管理のポータルの認証などに実装される。
	セキュリティ実装基準の技術的解説		強固な認証の１つとして本管理策で例示されている二要素認証としては、以下のようなものがある。 －生体認証 －パスワードに加え、トークンなどを利用した認証 －クライアント証明書などによる認証
	1.1	監査実施ガイド	サービス管理のポータルの認証において、強固な認証が提供されることを確認する。
		想定される証拠	クラウドサービス事業者が提供する強固な認証による認証方式とその実行結果
		監査技法	観察, 再実施

管理策			9.4.1　情報へのアクセス制限
追加技術情報			本管理策の対象は、サービス管理におけるユーザのアクセスプロビジョニングである。 仮想リソース（例: VM の OS）でのアクセスプロビジョニングは、対象外である。
1	セキュリティ実装基準（詳細管理策）		サービス管理をとおして、クラウドサービス利用者に提供される情報、アクセス権は、当該クラウドサービス利用者のテナント内に限定され、他のテナントに関する情報、アクセス権が提供されないこと。 利用者ごとに、扱える情報やアクセス権の指定を可能とする場合は、ポータル等の利用者管理機能などにおいて、これらの操作を可能とする。
	セキュリティ実装基準の技術的解説		クラウドサービスにおいては、複数のクラウドサービス利用者が仮想化機能を共用している。各クラウドサービス利用者が他のクラウドサービス利用者のテナントに関する情報へのアクセスが出来ないよう、仮想化機能のアクセス制御などを利用し、テナントの分離が実装される。 利用者ごとのアクセス制御は、仮想化機能のアクセス制御を用いないで、サービス管理の中で実装されることがある。
	1.1	監査実施ガイド	ポータルにおける、情報提供、アクセス権管理機能において、他のテナントに関する情報、アクセスが出来ないことを確認する。
		想定される証拠	ポータルの操作画面と操作結果
		監査技法	観察, 再実施
	1.2	監査実施ガイド	利用者ごとのアクセス制御が可能な機能が与えられている場合には、利用者に対し設定されたアクセス権の範囲で、クラウドサービスへのアクセスが可能かを確認する。
		想定される証拠	ポータル等の利用者管理機能の画面と操作 利用者に対しアクセス権の制限などを与えてのアクセス結果
		監査技法	観察, 再実施

管理策	9.4.4　特権的なユーティリティプログラムの使用
追加技術情報	仮想化機能に付属するユーリティプログラムは、クラウドサービス利用者のテナント外のリソースに影響を与える場合がある。

		仮想化機能の状態の把握などユーティリティプログラム結果をクラウドサービス利用者が必要とする場合、他の利用者に影響を与えない形で、結果の情報などをクラウドサービス利用者に提供すること。	
1	セキュリティ実装基準（詳細管理策）	クラウドサービス利用者が必要とする情報を提供する仮想化のユーティリティプログラムなどは、直接クラウドサービス利用者にアクセスさせず、サービス管理の中で、他のテナントに提供を与えない形で実行され、クラウドサービス利用者のテナントに限定した情報のみを提供する。	
	セキュリティ実装基準の技術的解説	本件に該当するようなユーティリティプログラムには、次のようなものがある。 －サーバ仮想化における仮想サーバの諸元の取得、ログ、性能情報の取得など －ネットワーク仮想化におけるトラフィック情報の取得など －サーバ仮想化における、ボリュームコピー、アクセス情報の取得など	
	1.1	監査実施ガイド	利用者に提供されるユーティリティ機能について、提供される情報に他のテナントに関するものが含まれていないことを確認する。
		想定される証拠	ユーティリティ機能の利用結果
		監査技法	観察, 再実施
2	セキュリティ実装基準（詳細管理策）	クラウドサービス利用者が、テナント内で仮想化機能のユーティリティを使用した場合、仮想化のパラメータはテナント外に影響を与えないよう設定する。	
	セキュリティ実装基準の技術的解説	一般に、仮想リソース内で仮想化機能に付属するユーティリティを利用することは困難である。 本件を監査するには、仮想リソース内で当該リソースを超えて他のリソースに影響を与えるユーリティがあるか調査し、あった場合に以下の確認を行なう。	
	2.1	監査実施ガイド	影響を与え得るユーティティに関し、それを禁止するパラメータが仮想化機能に定義されているかを確認する。 注記：本件に関する検証を実際に行なった場合、クラウド環境に障害を発生させる可能性があることに留意が必要。
		想定される証拠	仮想化機能のパラメータ定義など
		監査技法	観察

6.3.2 暗号 <10>

管理策		10.1.1　暗号による管理策の利用方針 注記：いくつかの法域では、健康データ、住民登録番号、パスポート番号や運転免許証番号などの特定の種類の情報（particular kinds of information）を保護するために暗号化を適用する必要がある場合がある。	
追加技術情報		サービス管理において本管理策は、ポータルへのアクセスの暗号化に必要となる。	
1	セキュリティ実装基準（詳細管理策）	ポータルのアクセスの暗号化の代表的な実装としては、HTTP over SSL/TLS が挙げられる。	
	セキュリティ実装基準の技術的解説	サービス管理のポータルの通信として、https を利用する。	
	1.1	監査実施ガイド	サービス管理のポータルのプロトコルとして https が使用されていることを確認する。
		想定される証拠	ポータルをアクセスする際のプロトコル ポータルアクセスのための証明書など
		監査技法	観察
2	セキュリティ実装基準（詳細管理策）	サービス管理においては、クラウドサービス利用者、ユーザの情報を管理することから、実施の手引きに注記した、特定の種類の情報が格納されることがある。 これら情報については、必要により、サービス事業者のポリシーに応じて、本管理策に記載された暗号化が施される。	
	セキュリティ実装基準の技術的解説	クラウド管理系が管理するデータについての暗号化は、クラウドサービス事業者自身のセキュリティ管理策であり、本管理策が規定するクラウドサービス利用者に提供する機能とは異なる。	
	2.1	監査実施ガイド	対象外
		想定される証拠	対象外

		監査技法	——

6.3.3 情報セキュリティインシデントの管理 <16>

管理策		16.1.2　情報セキュリティ事象の報告	
追加技術情報		「クラウドサービスのための関連情報」に記載されているとおり、本メカニズムは、電話、電子メールなどによって提供されることもある。	
1	セキュリティ実装基準（詳細管理策）	サービス管理においては、本管理策が規定する情報セキュリティインシデントの送受の管理、クラウドサービス利用者へのインタフェースとしてのポータル機能などが提供されることがある。	
	セキュリティ実装基準の技術的解説	サービス管理において、本機能を実装する場合には、ポータル等においてクラウドサービス利用者から提起されたレポートと、クラウドサービス事業者からの情報提供などが管理され、クラウドサービス利用者が当該インシデントの状況を把握する機能を提供する。	
	1.1	監査実施ガイド	ポータルにおいて、情報セキュリティインシデントに関するレポート、状況把握の機能が提供されていることを確認する。
		想定される証拠	ポータル等の情報セキュリティインシデントに関する画面と操作
		監査技法	観察

7. サーバ仮想化

7.1 サーバ仮想化の概略

サーバ仮想化は、物理サーバ(CPU、メモリ、IO デバイス等から構成される)を論理的なリソースに仮想化する。一般に、サーバ仮想化は図 4 のような構造になっている。

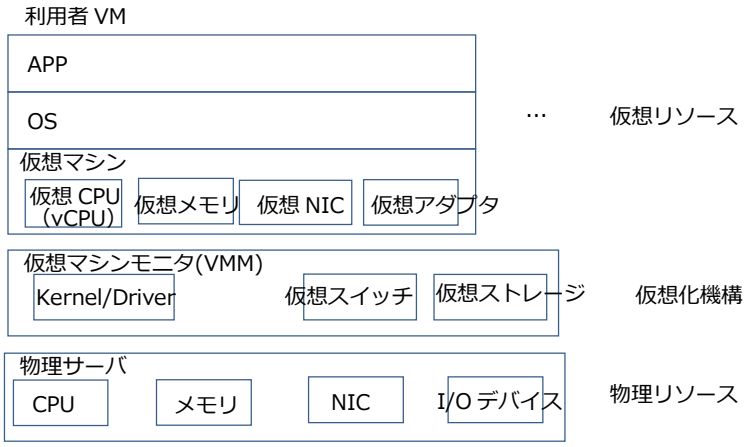

図 4　サーバ仮想化の概観

(1) CPU の仮想化

CPU の仮想化では物理サーバ上の物理 CPU を仮想コア単位に仮想化リソースとしてユーザーVM に割り当てる。CPU の仮想化により、サーバ全体の物理 CPU コア数以上の仮想 CPU を割り当てること(オーバーコミット)が可能になる.

オーバーコミット時、VMM（Virtual Machine Monitor）は CPU スケジューリングを行い、物理 CPU コアに割り当てる仮想 CPU の切り替えを実施する等の処理を行っている。そのため、複数 VM が同時に重い処理を実施すると、物理 CPU の競合率が高まり CPU リソースを割り当てられるまでの待ち時間に加え CPU スケジューリングの処理のためにも CPU リソースが消費され、処理性能に影響を及ぼす可能性があり留意が必要である。

(2) メモリの仮想化

メモリの仮想化では物理サーバのメモリ上に仮想マシンのメモリを割り当てる。CPU の仮想化と同様に、メモリも仮想化されることによって、仮想マシンから見えるメモリのサイズの合計が物理ホスト上に積まれているメモリよりも多くなるオーバーコミットが可能となる。メモリのオーバーコミットには動的に VM にメモリを割り当てる方式(バルーニング)や内容を同じメモリを複数の VM で共有する方式等複数の方式がある。何れの方式においても、各 VM に割り当てられるメモリの最小値の合計はホストマシンに搭載するメモリのサイズよりも小さい必要がある。

(3) ストレージの仮想化

ストレージの仮想化では、物理サーバのストレージ上のファイルセットとして仮想マシンのストレージを扱う。但し、物理サーバ間で仮想化されたサーバの移動を行う際に、大量のデータの転送による帯域の占有やストレージの速度等が問題となるため、一般的なクラウドの設計においては、共通のストレージサーバーを設置し、ストレージエリアネットワーク(SAN)を経由してアクセスを行う設計をとることが多い。

(4) I/O の仮想化

I/O の仮想化では、ホストバスアダプタやネットワークアダプタ、シリアルポートアダプタといった各種ペリフェラルを仮想化する。仮想化されたアダプタポートは VMM での設定により VMM 上で動作する仮想マシンと接続する、あるいは、物理サーバの物理的なアダプタ・ポートに接続するといった形で利用される。メモリや CPU に比べてホストバスアダプタやネットワークアダプタの I/O 機能はハードウェアの共有の度合いが高いため、特に仮想化機能におけるボトルネックとなることが多く注意が必要である。

7.2 クラウドサービスにおけるサーバ仮想化の適用

(1) サーバ仮想化におけるテナント分離

仮想化環境の一般的な設計では、仮想化されたサーバは全く独立のリソースにとなるように設計されるため、VM 間は仮想ネットワークで接続されることになる。そのため、最低限のネットワークセキュリティ対策が VM リソース感の隔離のために必要となる。加えて、仮想化環境特有の留意すべき点として、ベンダーから提供される仮想化環境自体のぜい弱性修正を反映する必要がある。

また、特殊な仮想化環境では VM 間の高速な通信の為の経路が用意され VM 間を接続する、あるいはホストハードウェアの物理ポートを介して VM 間でのデータのやり取りが可能になる場合もある為、ネットワークアダプタ以外の I/O に関しても注意を払う必要がある。

さらには、仮想リソースを保護する手法として、VMM あるいは特権 VM 上からメモリや IO へアクセスする技術が存在する。この技術を使うことで、VM 上の振る舞いを監視し、不正なプロフラムの動作を検出、保護することが可能になる。このように、VMM や特権 VM からのアクセスは仮想化リソースのセキュリティ実現の為有用な一方で、攻撃経路ともなりうるため、不用意に導入しないよう留意が必要である。

(2) 仮想マシンの要塞化

仮想化されたサーバの強化は、一般的なサーバに対する強化技術が適応可能なため、本書で改めて触れることはしない。VMM からサーバのセキュリティを提供する技術を用いた場合も、その為の監査方法は ISO27002 に規定される方法に準拠する。

(3) サーバ仮想化における可用性の確保

ライブマイグレーションは、VM を止めることなく、異なる物理サーバ上へと VM の動作環境を移動させる機能である。ライブマイグレーションは共有ストレージ上に格納される VM イメージを移行先の物理サーバの VMM 上で起動し、キャッシュ・メモリ上データを LAN 経由で転送、同時に仮想化された I/O を引き継ぐことで実現される。この仕組みでは、ライブマイグレーション時には LAN 上をメモリの内容が流れることになるため、メモリ上のデータのセキュリティ、LAN のセキュリティが重要となる。ライブマイグレーションでは管理者の操作によって VM を物理サーバ間で移動させるが、類似する技術として、環境の障害発生時に自動で VM を物理サーバ間で移動させる高可用性技術が提供されている。

こういった高可用性技術では監視し障害発生を検出した場合に、障害の発生した物理サーバ上で動作している仮想マシンのイメージを他の正常に動作している物理サーバ上で起動させるため、提供サービスは一定時間停止することになる。高可用性技術で発生する一定時間のサービス停止を解消する技術として、対障害性を持った仮想化環境も提供されている。対障害仮想化か環境では複数の物理サーバ上でプライマリ・セカンダリの VM を動作させ、両 VM を常に同期する。通常時はプライマリの VM がサービスを提供し障害発生時には瞬時にセカンダリ VM に切り替える事によって耐障害性を確保する。いずれの技術も同一物理サーバでなく別の物理サーバ上に空きリソースが必要となるため注意が必要である。

(4) サーバ仮想化におけるキャパシティ管理

仮想化されたメモリや CPU リソースは対応した OS を利用することで、動作中にこれらのリソースを動的に割り振ることが可能になる。割り当てることができるのは物理サーバのリソースが上限となるため、他の VM の使用リソースを鑑み、場合によっては前述のライブマイグレーション技術を用いて VM を他の物理サーバへと移動するなどして空き容量を確保する必要がある。物理サーバのリソースは以下の様ないくつかの指標で示される

- CPU コア数
- メモリサイズ
- ディスク I/O 性能
- ディスクサイズ
- ネットワーク I/O 性能

単純な仮想化環境の提供であれば、これらのサービスとして提供されるこれらの指標の合計に、仮想化のためにかかるオーバーヘッドを掛けあわせることで必要なリソースの合計を算出可能であるが、サービスの可用性を考慮する場合、リソースだけでなく物理的サーバ単位でマージンが確保される必要がある。

どのような指標に着目し、どのような形でサービスを提供するかはサービス事業者のビジネスモデル、あるいは SLA に依存するが、いずれにおいても現時点での提供リソースと空きリソースをモニタし適切なハードウェアリソースを提供し続けることが重要となる。こういったモニタリングはクラウド環境全体の整合性確保の為、主にサービス管理に於いて実施されるものである。しかしながら、サーバ仮想化においても VMM や特権 VM へのリソース使用率監視ツールの導入が必要となる事があるため留意が必要である。

7.3 サーバ仮想化に関する監査

7.3.1 アクセス制御

管理策		CLD.9.5.1　仮想コンピューティング環境における分離	
追加技術情報		論理的な区画の実装は仮想化に用いられる技術に依存する	
1	セキュリティ実装基準（詳細管理策）	マルチテナントの環境か利用者同士を隔離する	
	セキュリティ実装基準の技術的解説	仮想化リソース間の通信経路となる可能性のあるものとして、メモリ及び仮想ポートを使った VM 間の通信経路がある。	
	1.1	監査実施ガイド	VM 間で直接アクセスする機能を無効にする
		想定される証拠	VMM において VM 間でアクセスする機能が無効になっていることを確認する
		監査技法	観察，閲覧
2	セキュリティ実装基準（詳細管理策）	クラウドサービス事業者の管理機能と利用者の環境を隔離する	
	セキュリティ実装基準の技術的解説	VM-VMM 間の隔離においては前節で述べた VM-VM 管理策が同様に有効である。加えて、VM-VMM 間に関してはセキュリティや可用性の側面から導入されるツールによって通信経路が設けられる場合があるため、それらのツールにおけるぜい弱性が VM-VMM 間の抜け道になる可能性がある。	
	2.1	監査実施ガイド	仮想化環境上の区画オプションを有効にする
		想定される証拠	VMM におけるアクセスコントロールポリシーの確認 VMM における透過的ページ共有（Transparent Page Sharing）の無効化の確認
		監査技法	観察，閲覧
	2.2	監査実施	仮想システムクラスタ（cluster of virtual systems）の物理的分離

		ガイド	
		想定される証拠	物理サーバにおける仮想化支援機能の有効化の確認
		監査技法	観察，閲覧
3	セキュリティ実装基準（詳細管理策）	ぜい弱性管理の実施	
	セキュリティ実装基準の技術的解説	仮想化を実現する基盤(ホスト OS、ハイパーバイザー等)においてはセキュリティ面において配慮されている製品を使っているかを確認する(コモンクライテリア認証等)。	
	3.1	監査実施ガイド	仮想化基盤において、セキュリティに配慮した製品を使用しているかを確認する。
		想定される証拠	仮想化基盤の基本設計書
		監査技法	閲覧
	3.2	監査実施ガイド	運用時におけるぜい弱性情報の共有
		想定される証拠	ぜい弱性情報共有状況の確認（ポータルページ上の掲示情報の確認等）
		監査技法	観察

管理策		CLD.9.5.2　仮想マシンの要塞化	
追加技術情報		仮想マシンの要塞化は、VM の OS だけでなく VM/VMM 及び物理サーバによっても達成される。これらは全て密接に関連しているので、仮想マシンの要塞化はクラウドサービス事業者とその利用者の協力が必要となる。	
1	セキュリティ実装基準（詳細管理策）	仮想マシンを設定する際には，必要な装置及び/又はサービスのみ有効にしておく。	
	セキュリティ実装基準の技術的解説	−	
	1.1	監査実施ガイド	VM を構成する仮想デバイスは必要最小限（ベアミニマム）に設定する。
		想定される証拠	VMM 内提で提供される VM 機能が必要最小限に設定されていることを確認する。
		監査技法	観察，閲覧
	1.2	監査実施ガイド	VMM またはサービス管理にデフォルトで提供される VM OS イメージに追加されるサービスの種類を記述する。
		想定される証拠	追加のサービス情報の投稿をサービス管理で提供されるクラウドサービス利用者によって作成された新しい仮想マシン用の設定画面で行う。
		監査技法	観察
2	セキュリティ実装基準（詳細管理策）	仮想環境を作成する場合は、仮想環境を提供するサーバ上のマルウェアや脆弱性攻撃のリスクを低減する。	
	セキュリティ実装基準の技術的解説	仮想化技術に応じて、汎用 OS はさまざまなアプリケーションを追加することが可能であるが、不必要な役割、機能及びアプリケーションは避ける。 VMM は、ウイルス対策ソフトウェア、バックアップエージェントなどの必須基盤要素の実行に特化する。 サーバのぜい弱性が除去されたすべての機能を備える仮想マシンを使用するのが理想的である。	
	2.1	監査実施ガイド	ホスト上のサービスは必要最低限に限定されていることを確認する。最小構成で OS が推奨される。
		想定される証拠	VMM 上のサービスをチェックし、必要最小限の構成であることを設計文書で確認する。
		監査技法	観察，閲覧
	2.2	監査実施ガイド	セキュリティ更新は（VMM 含む）VMM やアプリケーション上で適切に実行されていることを確認する。
		想定される証拠	アップデートツールの実装により、新たに実行する必要がないことを確認する。
		監査技法	観察，、テスト
	2.3	監査実施	ブートローダまたは VMM がどの様にも不正に変更されていないことを確

		ガイド	認する。
		想定される証拠	UEFI（Unified Extensible Firmware Interface）画面でセキュアブートの活性を確認する。
		監査技法	観察
3	セキュリティ実装基準（詳細管理策）	仮想マシンを構成する場合は、使用される各仮想マシンのための適切な技術的コントロール（例えば、アンチマルウェア、ロギング）が所定の位置にあることを確認する。	
	セキュリティ実装基準の技術的解説	サーバー上の脆弱性を管理するために一般的使われるプラクティスと同様、準仮想環境をより効果的にりようするドライバーのようなソフトウェアや、サーバからのゲストマシンを管理するためのソフトウェアがあり、これらは、環境が仮想化されているという事実のもとに設定する。	
	3.1	監査実施ガイド	仮想環境で使用されるツールとドライバの脆弱性に関する情報を収集し、クラウドサービス利用者にアップデートを公表するためのモデルを準備する。
		想定される証拠	通知ログ及び関連データはクラウドサービス利用者が確認できる。
		監査技法	観察

8. ネットワーク仮想化

8.1 ネットワーク仮想化の概略

従来型のネットワーク仮想化は、1 つの物理ネットワーク上で、複数の独立した通信を可能とする手段の一つである。一方、サーバ仮想化におけるネットワークの仮想化は、一つの物理サーバ内にある複数の仮想マシンをつなぐ手段となる。仮想マシンは物理サーバの故障や物理リソースの高使用率を契機に別の物理サーバに移動することがある。このとき仮想マシンの VLAN ID や IP アドレスは変わらない点に特徴がある。仮想マシンとそれをつなぐネットワークの概略構成を図 5 に示す。

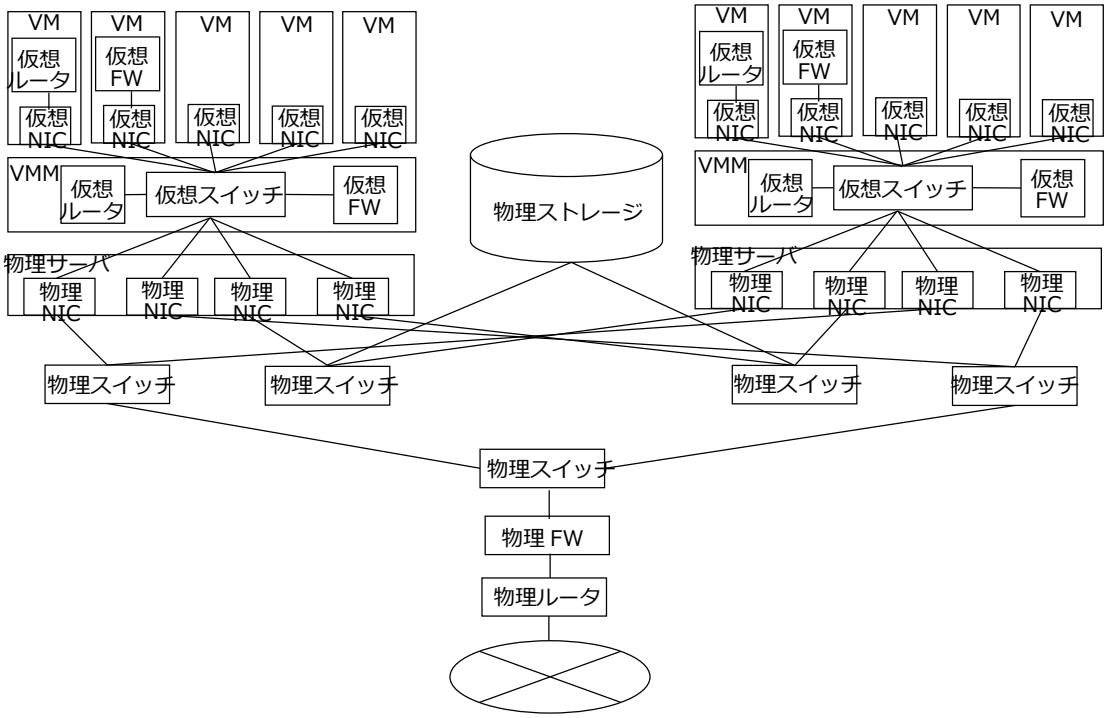

図 5　ネットワーク仮想化の概観

(1) 仮想スイッチ

仮想マシンモニタによって提供される論理的な L2 スイッチの機能。物理 NIC と仮想マシンの間に介在し、フレームの受け渡しを行う。物理 NIC は透過的にフレームを中継するため、仮想スイッチは物理 NIC をはさんで物理スイッチとスイッチ間接続される。

(2) 仮想 NIC

仮想マシンを仮想スイッチに接続するために、仮想マシンモニタによって提供される論理的なネットワークインタフェースカードの機能。

(3) 仮想ルータ

仮想マシンにインストールされたソフトウェアによって提供される論理的なルータの機能、又はルータとして機能する仮想マシンそのものを指す。仮想スイッチがルータ機能を併せ持つこともある。

(4) 仮想ファイアウォール

仮想マシンにインストールされたソフトウェアによって提供される論理的なファイアウォールの機能、

又はファイアウォールとして機能する仮想マシンそのものを指す。

8.2 クラウドサービスにおけるネットワーク仮想化の適用

(1) ネットワーク仮想化におけるテナント分離

テナントが利用する仮想マシンは固有の仮想 MAC アドレス、IP アドレスをもち、1 つ又は 2 つ以上の仮想マシンをつなぐ論理ネットワークがテナント毎に独立して設定されることにより、各テナントは物理ネットワーク上でも物理サーバ上でも分離される。

(2) ネットワーク仮想化における可用性の確保

物理サーバが故障した場合、その上の仮想マシンと仮想ネットワークは、他の物理マシンに移動することで可用性が維持される。物理サーバに実装された物理 NIC の故障の場合には、物理 NIC が冗長化されていれば、他の物理 NIC に仮想ネットワークが迂回して可用性が維持され、仮想マシンそのものが移動することはない。

(3) ネットワーク仮想化における帯域及びアドレス空間の管理

一般にクラウドサービスでは、限られた物理リソースの上に多くの仮想リソースを集約して高密度に設定するために、仮想ネットワークの論理帯域の総和が物理ネットワークの物理帯域をはるかに上回ることがある。また、多数の仮想マシンが VLAN ID や IP アドレスを保持したまま、ある物理サーバから他の物理サーバへと移動することがあるため、物理スイッチに設定が必要な VLAN ID 数や学習が必要な MAC アドレス数が多くなる傾向がある。

8.3 ネットワーク仮想化に関する監査

8.3.1 アクセス制御 <9>

ISO/IEC 27017 13.1 参照

8.3.2 暗号 <10>

管理策		10.1.1　暗号による管理策の利用方針 注記：いくつかの法域では、健康データ、住民登録番号、パスポート番号や運転免許証番号などの特定の種類の情報を保護するために暗号化を適用する必要がある場合がある。	
追加技術情報		クラウドサービス利用者がクラウドサービスにアクセスする通信は、暗号化されることがある。	
1	セキュリティ実装基準（詳細管理策）	ネットワーク機器又はサーバの暗号化機能を用いて、ユーザデータを暗号化する。	
	セキュリティ実装基準の技術的解説	SSL/TLS、SSH、IPsec 等の暗号化プロトコルを用いた暗号化がある。	
	1.1	監査実施ガイド	ネットワーク機器又はサーバが、通信の暗号化のための設定がされているか確認する。
		想定される証拠	通信機器又はサーバの通信暗号化の設定値
		監査技法	観察，閲覧
	1.2	監査実施ガイド	パケットアナライザを用いて、通信経路上のトラフィックをモニタリングし、ペイロードが暗号化されていることを確認する。
		想定される証拠	パケットアナライザのトラフィック監視データ
		監査技法	観察，閲覧

8.3.3 通信のセキュリティ <13>

管理策			13.1.3 ネットワークの分離
実施の手引			クラウドサービス事業者は，次の場合においてネットワークアクセスの分離を実施することが望ましい。 －マルチテナント環境におけるテナント間の分離 －クラウドサービス事業者内部の管理環境とクラウドサービス利用者のクラウドコンピューティング環境との分離 必要な場合には，クラウドサービス事業者は，クラウドサービス事業者が実施している分離をクラウドサービス利用者が検証することを補助することが望ましい。
追加技術情報			クラウドサービスにおけるネットワークの分離は、物理リソースが独立した物理ネットワークによる物理的分離と物理リソースを共有した論理ネットワークによる論理的分離がある。論理ネットワークは、物理ネットワークだけでなく、物理サーバ上にも展開される。
1	セキュリティ実装基準（詳細管理策）		－個別の物理リソース（物理サーバ、物理ストレージ等）をクラウドサービス利用者がそれぞれ使用する場合、各クラウドサービス利用者毎に独立した通信機器と通信ケーブルで構成される物理ネットワークを各クラウドサービス利用者用の個別のネットワークとして使用する。 －同一の物理リソース（物理サーバ、物理ストレージ等）を複数のクラウドサービス利用者がテナントとして共同して使用する場合、テナント毎又は仮想マシン毎に論理的に独立した VLAN を使用する。 －クラウドサービス利用者の使用する物理リソース（物理サーバ、物理ストレージ等）を管理するクラウドサービス事業者は、クラウドサービス利用者とは別の物理ポートに接続し、物理的に独立した通信機器と通信ケーブルで構成される物理ネットワークを管理用ネットワークとして使用する。 －クラウドサービス利用者の使用する物理リソース（物理サーバ、物理ストレージ等）を管理するクラウドサービス事業者は、クラウドサービス利用者とは別の論理ポートに接続され、論理的に独立した VLAN を管理用ネットワークとして使用する。
	セキュリティ実装基準の技術的解説		ネットワークが物理的に分離している場合、同一物理リソースにおける複数の物理ポートには異なる ID が割り当てられる。ネットワークが論理的に分離している場合、同一物理ネットワーク上における複数の論理ネットワークには異なる VLAN ID、VSAN ID 又はサブネットマスク等が割り当てられる。
	1.1	監査実施ガイド	テナント毎に独立したテナント用ネットワークが設定されているか確認し、その他にバックドアがないことを確認する。
		想定される証拠	テナントに割り当てられたネットワークの ID 及びそのネットワークの経路設定（スイッチングテーブル、ルーティングテーブル等）
		監査技法	観察，閲覧
	1.2	監査実施ガイド	設定されたテナント用ネットワークにアクセスできるのは許可された者のみであることを確認する。
		想定される証拠	テナントに割り当てられたネットワークに対するアクセス権設定（アクセス制御を実行するサーバ、ネットワーク機器のアクセス権管理テーブル等）
		監査技法	観察，閲覧
	1.3	監査実施ガイド	クラウドサービス事業者が利用する管理用ネットワークがその他のネットワークと独立して設定されているか確認し、設定された管理用ネットワークにアクセスできるのはクラウドサービス事業者のうち許可された者のみであることを確認する。
		想定される証拠	クラウドサービス事業者が利用する管理用ネットワークの ID、経路設定及びアクセス権設定
		監査技法	観察，閲覧

管理策		CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合
追加技術情報		物理リソース（物理スイッチ、物理ルータ、物理ケーブル、物理サーバ、物理ストレージ等）の設定と物理リソースを経路とする仮想ネットワークの設定方法が独立している場合、これらをマニュアルで整合させるには、設定者の熟練と十分な注意力を要する。設定者の力量のみに頼らず、仮想ネットワークと物理ネットワークの設定を自動的に整合させる技術的手段には様々な例がある。
1	セキュリティ実装基準（詳細管理策）	－仮想ネットワーク及び物理ネットワークからそれぞれの制御部を分離独立させ、それらすべての制御部を統合したネットワークアーキテクチャを採用する。 －仮想スイッチの機能を使用せず、仮想スイッチの機能を実装した物理スイッチを用いて、物理スイッチ上で仮想ネットワークと物理ネットワークを制御する。 －仮想マシンのライブマイグレーションに合わせて、仮想スイッチと物理スイッチの設定変更を同期させるメカニズムを用いる。また、ライブマイグレーションによって仮

			想マシンが移動した後でも同じネットワーク設定が使えるよう十分に拡張したVLAN ID を用いる。 －仮想ネットワークと物理ネットワークの管理システムを統一し、このシステムを通して設定を行う。
	セキュリティ実装基準の技術的解説		仮想ネットワークは、障害時の迂回や VM のライブマイグレーション等によって、物理ネットワーク上の経路が変更される。また、一つの物理サーバの内部に複数のテナント、複数の VM が存在する場合、その物理サーバ内の仮想ネットワーク機器（仮想スイッチ、仮想ルータ等）に、複数の仮想ネットワークが設定される。
	1.1	監査実施ガイド	監査対象の仮想ネットワークの物理経路があるか確認する。
		想定される証拠	物理ネットワーク機器に設定された仮想ネットワークの ID、物理サーバ内の仮想ネットワーク機器に設定された仮想ネットワークの ID
		監査技法	観察，閲覧
	1.2	監査実施ガイド	監査対象の仮想ネットワークとその経路となる物理ネットワークの設定内容（ルーティング、スイッチング、フィルタリング、帯域制御、優先制御、アクセス制御等）が矛盾しないか確認する。
		想定される証拠	物理ネットワーク機器と仮想ネットワーク機器のそれぞれにおける、経路選択の設定情報（スイッチングテーブル、ルーティングテーブル等）、フィルタリング設定、帯域制御設定、優先制御設定、アクセス制御設定
		監査技法	観察，閲覧

9. ストレージ仮想化

9.1 ストレージ仮想化の概略

ストレージ仮想化は、物理ストレージ(ドライブ)を論理的なストレージに仮想化する。一般に、ストレージ仮想化は図 6 のような構造になっている。

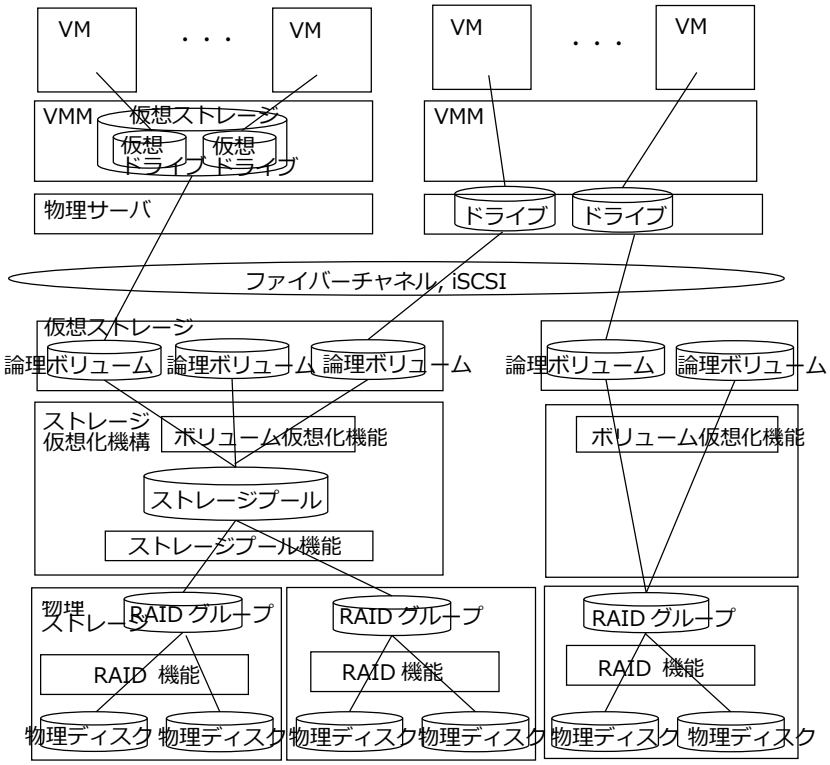

図 6　ストレージ仮想化の概観

(1) 論理ボリューム

ストレージ仮想化において最も重要な要素は、「論理ボリューム」である。論理ボリュームは、ストレージ仮想化機能によって、物理ディスクが仮想化され、ストレージにおける仮想化リソースとして、ハイパバイザやＯＳから認識されるストレージの単位である。いくつかのクラウドでは、これを MLU あるいは LDev (Logical Device)と呼んでいる。

(2) RAID（Redundant Arrays of Independent Disks）

近年多くのストレージ装置は、耐障害性の観点から複数の物理ディスクを束ねて RAID グループなどの論理ボリュームとして扱い、データを分散配置することで冗長性を向上させる機構(RAID)が採用されている。データを複数の物理ディスクに分散配置することにより、物理ディスクが毀損した場合にも、データを保全するための機構(RAID)が採用されている。

RAID により、複数の物理ディスクを束ねた領域を論理ボリュームとして仮想化することが可能である。.

(3) ストレージプール

物理ディスクまたは論理ボリュームをまとめて 1 つの大きな論理ボリューム（ストレージプール）として扱う機能である。ディスクの容量や組み合わせ、既に作成されたストレージプールへの新たな物理ディスク追加による容量追加など、ストレージ運用の柔軟性を向上させることが可能である。

(4) ストレージ容量の仮想化

論理ボリュームを割り当てる際に、ストレージの物理容量に依存せず、仮想的に任意の容量の割り当てる機能である。論理ボリュームにデータを記録する時、必要に応じてストレージプールから記憶領域を動的に割り当てるなどの方法により実装されている。ストレージリソースの効率的な利用を図る機能である。

(5) SAN(Storage Area Network)のゾーニング

ファイバーチャンネル(FC)を使った SAN は FC スイッチにより、ポートを通じたゾーンごとの接続によって区画分けすることができる。そのゾーンのストレージに装備された仮想化機能のゾーニング機能により区画分けする場合には、異なったゾーンのストレージの参照は遮断される。

9.2 クラウドサービスにおけるストレージ仮想化の適用

(1) ストレージ仮想化におけるテナント分離

ストレージ仮想化におけるテナント分離は、テナント単位に論理ボリュームや SAN のゾーニングを行うことで実装される。ただし、サーバ仮想化においてハイパバイザの機能によってストレージの仮想化が行われる場合には、ストレージ仮想化での論理ボリュームは、そのままテナントの単位とはならず、ハイパバイザが作り出す論理ボリュームを複数格納するストレージの単位でしかない。

ストレージの仮想化又はテナントの分離がサーバ仮想化で行われている場合には、論理ボリュームによるテナント分離ができないためその評価に十分留意する必要がある。

(2) ストレージ仮想化における可用性の確保

物理ストレージ装置における RAID 技術、SAN を構成する FC スイッチ、HBA（Host Bus Adapter）又は SAN 経路の冗長化、物理ストレージ機器が有するバックアップ機能などの利用によって、クラウドサービスの可用性向上が図られることがある。

(3) ストレージ仮想化におけるキャパシティ管理

クラウドサービス全体のストレージ容量の管理、テナントごとの論理ボリュームの容量管理を容易にし、ストレージのキャパシティ管理を円滑化するため、ストレージ仮想化でのストレージプール、容量の仮想化などが適用される。この場合、クラウドサービスに供される物理ストレージの容量だけでなく、テナントに提供される論理ストレージの容量の双方の管理が必要となる。

9.3 ストレージ仮想化に関する監査

9.3.1 アクセス制御　<9>

<table>
<tr><td colspan="2">管理策</td><td colspan="3">CLD.9.5.1　仮想コンピューティング環境における分離</td></tr>
<tr><td colspan="2">追加技術情報</td><td colspan="3">ストレージにおけるセグメンテーションの代表的な方法には、以下がある。
－テナントごとに論理ボリュームを作成し、論理ボリューム単位にアクセス制御を実施する。
－テナントを、SAN ゾーニングにより分離する。</td></tr>
<tr><td rowspan="3">1</td><td>セキュリティ実装基準（詳細管理策）</td><td colspan="3">ストレージの仮想化機構が提供するセグメンテーション機能により、クラウドサービス利用者ごとにセグメント分けする。</td></tr>
<tr><td>セキュリティ実装基準の技術的解説</td><td colspan="3">ストレージのセグメント分けは、サーバのハイパバイザによって実装されることもある。この場合には、ストレージ仮想化機構によってクラウドサービス利用者単位のセグメンテーションが実装されている必要はない。</td></tr>
<tr><td>1.1</td><td>監査実施ガイド</td><td>テナントごとに論理ボリュームを提供する方式においては、論理ボリュームに対し、ストレージ仮想化機能の有するアクセスコントロール機能により、当該論理ボリュームを提供するクラウドサービス利用者のみにアクセス権限が与えられていることを、ストレージ仮想化機能のパラメータ設定などにより確認する。</td></tr>
</table>

		想定される証拠	ストレージ装置のパラメータ ストレージ管理プログラムのパラメータ
		監査技法	観察
	1.2	監査実施ガイド	SAN ゾーニングによりテナントが分離される方式においては、テナントごとにゾーンが割り当てられ、異なるテナント間でストレージがアクセスできないことを、SAN を構成する機器のパラメータ設定などにより確認する。
		想定される証拠	SAN を構成するファイバチャネル機器のゾーニング定義
		監査技法	観察

9.3.2 暗号 <10>

管理策		10.1.1 暗号による管理策の利用方針 注記：いくつかの法域では、健康データ、住民登録番号、パスポート番号や運転免許証番号などの特定の種類の情報を保護するために暗号化を適用する必要がある場合がある。	
追加技術情報		ストレージにおける暗号化機能としては論理ボリュームを暗号化する方法がある。	
1	セキュリティ実装基準（詳細管理策）	論理ボリュームの暗号化機能を用いてテナントのデータを暗号化する。	
	セキュリティ実装基準の技術的解説	暗号鍵の保持方法、暗号化の範囲などは、使用するストレージ装置により異なる。	
	1.1	監査実施ガイド	ストレージ仮想化における論理ボリュームの暗号化機能を適用している場合においては、ストレージ仮想化機能が提供する状態表示、ユーテイィリティ機能などにより、当該論理ボリュームが暗号化されていることを確認する。
		想定される証拠	ストレージ装置のパラメータ ストレージ管理プログラムのパラメータ
		監査技法	観察

9.3.3 運用のセキュリティ <12>

管理策		12.3.1 情報のバックアップ	
追加技術情報		ストレージ仮想化において、仮想化機能を実現しているストレージ機器、ソフトウェアなどが何らかの原因により障害を発生した場合に、従前のサービス提供可能状態に復元するために必要な情報を退避する。 ストレージ仮想化機能のパラメータ、論理ボリューム設定情報などがこれらに相当する。	
1	セキュリティ実装基準（詳細管理策）	ストレージ仮想化機能が有するユーティティ、もしくは他のシステムユーティリティにより、退避が必要なパラメータ、定義情報などをバックアップする。	
	セキュリティ実装基準の技術的解説	仮想化ストレージリソースの変更により、定義情報の変更が発生する場合、変更の契機、もしくは妥当なタイムラグの範囲でバックアップを更新する。	
	1.1	監査実施ガイド	パラメータ、定義情報などがバックアップされているか確認する。 仮想リソースの変化と、バックアップの契機・周期が妥当であるか確認する。 バックアップされた情報から、従前の仮想化リソースを復元可能か確認する。
		想定される証拠	ストレージ装置のパラメータ ストレージ管理プログラムのパラメータ
		監査技法	観察

10. ISO/IEC 2017 と本書の記載関係表

章	タイトル	共通	サーバ仮想化	ネットワーク仮想化	ストレージ仮想化	サービス管理
5	情報セキュリティのための方針群	技術事項ではないため該当しない				
5.1	情報セキュリティのための経営陣の方向性	×	×	×	×	×
6	情報セキュリティのための組織	技術事項ではないため該当しない				
6.1	内部組織	×	×	×	×	×
6.2	モバイル機器及びテレワーキング	×	×	×	×	×
CLD.6.3	クラウドサービス利用者及びクラウドサービス事業者の関係	×	×	×	×	×
7	人的資源のセキュリティ	技術事項ではないため該当しない				
7.1	雇用前	×	×	×	×	×
7.2	雇用期間中	×	×	×	×	×
7.3	雇用の終了及び変更	×	×	×	×	×
8	資産の管理	物理リソースは範囲外のため該当しない				
8.1	資産に対する責任	×	×	×	×	×
CLD.8.1	資産に対する責任	×	×	×	×	×
8.2	情報分類	×	×	×	×	×
8.3	媒体の扱い	×	×	×	×	×
9	アクセス制御	・利用者のアクセス制御の記述は基本的にサービス管理内で完結する ・サービス事業者のオペレータのアクセス制御はこの章ではなく 12 章でカバーされる ・本章は、仮想化/仮想化リソースのための機能における利用者毎のアクセス制御の可能な設定をカバーする				
9.1	アクセス制御に対する業務上の要求事項	—	—	—	—	—
9.2	利用者アクセスの管理	→	→	→	→	9.2.1 9.2.2 9.2.3
9.3	利用者の責任	—	—	—	—	—
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 9.4.4
CLD.9.5	共有化された仮想環境におけるクラウドサービス利用者データのアクセス制御	→	CLD.9.5.1 CLD.9.5.2	cf. 13.1.3	CLD.9.5.1	←
10	暗号	仮想化を要する機能による暗号化のケースをカバーする				
10.1	暗号による管理策	×	10.1.1	10.1.1	10.1.1	10.1.1
11	物理的及び環境的セキュリティ	物理リソースは範囲外のため該当しない				
11.1	セキュリティを保つべき領域	—	—	—	—	—
11.2	装置	—	—	—	—	—
12	運用のセキュリティ	仮想化/仮想リソースに対するサービス事業者のオペレータ処理に焦点を当てている				
12.1	運用の手順及び責任	12.1.2 12.1.3	←	←	←	←
CLD.12.1	運用の手順及び責任	12.1.5	←	←	←	←
12.2	マルウェアからの保護	—	—	—	—	—
12.3	バックアップ	→	→	→	12.3.1	←
12.4	ログ取得及び監視	12.4.1 12.4.4	←	←	←	←
CLD.12.4	ログ取得及び監視	12.4.5	←	←	←	←
12.5	運用ソフトウェアの管理	—	—	—	—	—
12.6	技術的ぜい弱性管理	12.6.1	←	←	←	←

12.7	情報システムの監査に対する考慮事項	—	—	—	—	—
13	通信のセキュリティ	ネットワークに焦点を当てたセキュリティ				
13.1	ネットワークセキュリティ管理	→	→	13.1.3	←	—
CLD.13.1	ネットワークセキュリティ管理	→	→	CLD.13.1.4	←	←
13.2	情報の転送	—	—	—	—	—
14	システムの取得、開発及び保守	技術モデルに直接関連しないため該当しない				
14.1	情報システムのセキュリティ要求事項	×	×	×	×	×
14.2	開発及びサポートプロセスにおけるセキュリティ	×	×	×	×	×
14.3	試験データ	—	—	—	—	—
15	供給者関係	技術事項ではないため該当しない				
15.1	供給者関係における情報セキュリティ	×	×	×	×	×
15.2	供給者のサービス提供の管理	—	—	—	—	—
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改善	→	→	→	→	16.1.2
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					
17.1	情報セキュリティ継続	×	×	×	×	×
17.2	冗長性	—	—	—	—	—
18	順守	技術事項ではないため該当しない				
18.1	法的及び契約上の要求事項の順守	×	×	×	×	×
18.2	情報セキュリティのレビュ	×	×	×	×	×

凡例　— ：ISO/IEC 27017:201x においてクラウド事業者の管理策が規定されていない。

× ： 本書として技術面からの記載を必要としない。

→, ← ： 主に他の区分に記載される内容によって実装される。

管理策番号 ： 本書において解説が加えられている。

【技術 WG メンバー】

柏浦謙一　日本ユニシス株式会社

纐纈昭憲　株式会社インターネットイニシアティブ

佐藤拓道　富士通株式会社

鈴木拓也　富士通株式会社

高原　清　株式会社日立製作所

間形文彦　日本電信電話株式会社

増永直大　株式会社野村総合研究所

松岡　健　株式会社日立製作所

水戸　和　セコム株式会社

【事務局】

永宮直史　特定非営利活動法人日本セキュリティ監査協会

【編集】

木村道弘　特定非営利活動法人日本セキュリティ監査協会

クラウドサービス（IaaS）の技術的評価ガイド
JASA クラウドセキュリティ推進協議会（JCISPA）

平成 28 年　3 月　31 日 第 1.0 版発行
発　行：特定非営利活動法人日本セキュリティ監査協会
〒135-0016 東京都江東区東陽 3 丁目 23 番 21 号　プレミアム東陽町ビル
TEL 03-6675-3820 FAX 03-6675-3819 http://www.jasa.jp/