仮想化・クラウドサービスの

把握と管理ガイド

平成 29 年 3 月

一般財団法人日本情報経済社会推進協会
情報マネジメントシステム認定センター

はじめに

近年、クラウドコンピューティング（cloud computing）の進展は、これまでの IT ビジネスに大きな変革をもたらしている。しかしながらクラウドセキュリティやクラウドサービス品質面での課題も数多く懸念されているところである。

このような背景により、クラウドコンピューティングという新しい形態で何をどう管理すればよいのか、どのような点に留意する必要があるのかを IT 資産管理（IT Asset Management：ITAM）の側面から調査研究し、昨年度「クラウド時代の ITAM の考え方」として報告書をとりまとめた。

本書は、昨年度の調査研究を踏まえ、仮想化・クラウドサービスの把握と管理について解説するとともに、ITAM の観点から仮想化・クラウドサービスを利用するうえで留意すべき点を取りまとめたものである。本書が企業・団体における IT 資産管理に携わる方々のお役に立てば幸いであり、IT 資産管理の普及促進に資することを期待する。

平成 29 年 3 月

一般財団法人日本情報経済社会推進協会
情報マネジメントシステム認定センター
IT 資産マネジメント評価検討委員会

仮想化・クラウドサービスの把握と管理ガイド

目　次

Ⅰ．環境の把握

１．仮想化の把握

IT 資産管理（IT Asset Management : ITAM）の目的は、*「クラウド時代の ITAM の考え方」*（平成 28 年 2 月　JIPDEC 発表、以下の表Ⅰ-1 に転載）でも示したとおり、組織としてのリスク管理、コスト管理、競争上の優位性確保にある。“利用中の IT 資産”と“利用していない IT 資産”を整理し、資産の有効活用を行うことは、ITAM の目的達成に直結する重要な課題である。

表　Ⅰ-1　ITAM の目的

#	目的
(1)	リスク管理 a）説明責任 b）資産保全 c）法的リスクの回避 d）セキュリティ上の問題への対処 e）可用性の確保
(2)	コスト管理（TCO 削減など）
(3)	競争上の優位性確保（IT 資産の有効活用）

（各項目の詳細な説明については、*「クラウド時代の ITAM の考え方」*を参照。）

ただ、IT プラットフォーム（サーバー、ストレージ、ネットワークなど）の仮想化はさまざまな IT リソースの物理的特性を、そのリソースと相互運用するシステム、アプリケーション並びにエンドユーザーから切り離す性質を持つことから推測されるとおり、実態を把握することが困難である場合が多い。また、仮想化を支えるテクノロジーが日進月歩で進化しており、さまざまな仮想化テクノロジーが組織中に混在することが想定され、個々のシステムの管理者や利用者による独自ルールでの運用管理がされる可能性もあるなど、ITAM の観点から見て不安要素となる点も多い。

そこで、この章では仮想化環境の利用状況を把握するために、どのような方法が有効となるかについて検討する。なお、IT プラットフォームの仮想化としては、サーバー・ストレージ・ネットワークの仮想化、VDI（Virtual Desktop Infrastructure）などの仮想デスクトップ環境などが含まれるが、管理対象としての優先順位が高いと考えられる仮想サーバーの利用を主に考えることとする。

１．１　申告による把握

物理的に把握できない仮想化環境についての利用状況を把握するためには、“仮想化環境の存在を認識している者”からの申告が重要な情報となる。システムの利用者は仮想化され

たIT環境を利用しているかどうかを認識できておらず、その存在を認識している者が“環境を構築した者”、“契約に携わった者”や“システムの保守・運用の担当者”に限定されることも考えられるためである。

1.1.1 どうすれば申告してもらえるか？

（1）誰に申告をしてもらうのか？

網羅的に情報を収集するためには、“情報を認識している者”に対し申告を義務づけることが必要となる。当然ではあるが、“仮想化環境の存在を認識していない者”が、仮想化環境の利用状況を申告することはできないためである。そこで、申告による情報の収集率をできるだけ上げるために、どのような担当者から情報を集めるのが有効であるか、システムの利用状況ごとに考えることとする。

（2）システムの利用状況ごとの情報収集

①仮想化環境を既に利用の場合

一般的には、以下のような担当者が仮想化環境の存在を認識している可能性が高い。

表　Ⅰ-2　仮想化環境の情報提供の候補者

仮想化環境の認識がある担当者の例	備考
システム導入時の検討メンバー	システム導入時に、仮想化環境も含めた構成（可用性確保やキャパシティプランニングなど）を検討しており、当時の検討資料の保管場所や、該当環境の現在の管理部門などを認識している可能性がある。
業務システム開発・保守部門	プロビジョニングや変更管理、問題管理のプロセスを通して、当該業務システムの稼働基盤に関する情報を保有しており、その中に仮想化環境に関する情報も含まれていると考えられる。
ハードウェア管理部門	ハードウェアの点検や障害時などに、影響を受ける仮想化環境（業務システム名や仮想サーバー名など）を確認する手段を認識していると思われる。
セキュリティ対応部門	セキュリティ対策を実施する上で対象となる仮想化環境（仮想サーバー名の一覧や仮想化テクノロジー、OS、ソフトウェアのバージョン情報など）を管理していると考えられる。

システム運用部門 災害対策検討メンバー インフラ管理部門	災害対策を検討する上で、データセンターや格納ラック、物理筐体といった単位で影響を受ける仮想化環境（対象となる業務システム名やサーバー名）を確認する手段を認識していると思われる。

②将来の利用が計画されている場合（開発中のシステムを含む）

仮想化環境について、将来の利用が計画されているが現在の利用がない場合、“現在の”利用状況の対象外として除外するという考え方もある。ただ、情報を網羅的に把握するためには早い段階で情報を収集することが必要と考える。遅くとも開発環境が構築されるタイミングで仮想化環境の情報を収集すべきである。また、開発が完了し運用フェーズとなった場合は、システム運用部門により再度記録の正確性を見直すといった常に正確な記録を保持する仕組みづくりも重要である。

③稼働環境の変更が実施される場合

仮想化環境を利用する上で大きなメリットである柔軟な環境の変更（システムの負荷に応じた割当 CPU 数やメモリー数の変更など）は、ITAM の観点ではやっかいな問題であるともいえる。管理対象となる情報が容易に変更できる状態であるということは、把握している情報を正確に保つ妨げとなることにもつながるためである。組織内での変更管理のルールにて仮想化環境の変更作業を記録することで、最新の情報が常に保持されるようになる。この場合の情報の提供者は業務システム保守部門や開発部門となるであろう。

④これまで利用していた仮想化環境の利用を止める場合

仮想化環境に限ったことではないが、システムの利用停止に関する記録が更新されないまま放置されるケースも多い。IT プラットフォームの仮想化により、より迅速かつ簡単に環境を確保できるということは、簡単に利用停止もできるということであり、利用停止時の記録の更新も不可欠となる。この場合、情報の提供者は業務システム保守部門、システム運用部門、契約担当部門が中心になるであろう。

（3）申告漏れを防ぐには？

“仮想化環境の存在を認識している者”に協力を依頼したとしても、それだけで全員から漏れなく情報が提供されるとは考えにくい。申告による情報収集率を上げるためには、他にも考えるべきポイントは多い。ここでは、申告漏れを防ぐための方法について考える。

（4）申告の重要性についての認識を全員が持つ

先にも述べたとおり、現在の IT 資産の利用状況を把握することは必須であり、リスク管理、コスト管理、競争上の優位性確保に必要な情報であることを組織の全員に理解してもら

う必要がある。たとえば、人事異動の際に対象サーバーが仮想化環境であるかどうかといった情報、採用している仮想化テクノロジー、ハードウェアの種類といった情報の引き継ぎが実施されなかった場合、後任がその環境に必要なセキュリティ対策を漏れなく実行できるとは到底考えられない。また、ソフトウェアやハードウェアの保守サポート契約数が適切なものであるかどうかを判断できる情報が得られなければ、不要な契約が長年維持される一方、本当は必要となる契約が締結されていないというリスクがあるといえる。

関係者全員に対しての効果的な伝達方法は、組織の特性により異なるかもしれないが、以下のような方法が考えられる。

- 定期的な研修の実施
- トップからのメッセージによる重要性の周知
- 部門内での定期的な周知

（5）規則や手順の整備

申告の重要性について組織内に浸透した場合にも、意図せずに申告が漏れてしまうケースは少なからず発生すると思われる。各々の組織にて施策の実効性を高める必要性はあるが、いくつかの案を以下に挙げる。

①規則の制定と監視

“申告のない環境の構築・サービス契約の締結は認めない”といった規則を制定し、違反が発生しないかを監視する。ただ監視については効果的に実施できるとは考えにくい。“仮想化環境の存在を認識していない者”が、申告漏れとなっている仮想化環境の存在を発見することは、偶然に頼らざるを得ないためである。

②業務フローの変更

組織内の稟議のルールや書類のフォーマットを変更し、申告の必要性について気づきを与えることで、情報の収集率や正確性を向上する方法を検討する価値がある。たとえば、申告済の仮想環境に対し、承認番号（一意の管理番号）を発行する。そして、IT に係るすべての書類（稟議書、導入計画書、テスト計画書、運用手順書、変更管理書、問題管理書、障害報告書、保守契約申請書、システム廃棄届など）にその承認番号の記載を義務づけ、記載がない場合は申請・承認の手続きを進めることができないものとする。（仮想化環境の利用がない場合は、仮想化環境でないことを明記することを求める。）更に、承認 No.を取得済の仮想化環境であっても、直近の承認日から一定の期間が経過したもの（1 年以上など）については、再度の申告と承認番号の取得を求めるものとする。

ただ、このように仕組みを厳密にすることは、IT プラットフォームの仮想化がもたらす本来のメリット（迅速かつ柔軟なリソースの確保やコスト削減）を損ねかねない。そのため、

これら施策の実施については、慎重な検討が必要になるだろう。

1.1.2　どのように申告をしてもらえばよいか？

（1）いつ申告をしてもらうか？

比較的簡単に構築や変更が可能という仮想化環境の特性上、定期的な周期（年に一度など）での申告を求めるのではなく、仮想化環境を構築する時点（これから構築する場合は 3 日前迄、既に環境が構築済の場合はできるだけ早くなどのルールを制定）での申告を求めることが望ましい。これは開発中における仮想化環境の利用においても同様である。また、一度申告がされた仮想化環境であったとしても、構成に変更が生じた場合は、最新情報への更新を求めるべきである。可能であれば、これらの申告が適切にできているかの確認のため、定期的な周期（年に一度など）で外部の第三者からのチェックを受けるといったことについても検討することが望ましい。

なお、すべての申告項目（１．３　把握すべき項目にて後述）の情報が揃わない場合や変更予定のある一時的な設定の場合も、申告を受け付けることが望ましい。申告項目の一部漏れや正確性にこだわりすぎるよりも、仮想化環境の存在についての網羅性を優先すべきであると考える。

（2）申告方法について

申告方法としては、必要な情報を網羅するように申告項目を規定のフォームで作成しておき、報告を求めると効率的な情報収集が可能であろう。また、申告内容を受領後にチェックして、申告の漏れや記入方法にミスがないか、申告用フォーマットにおける項目の追加や削除の必要性を恒常的に見直しすることが望ましい。

（3）申告による管理の問題点

申告方法による管理の問題点としては、意図的か否かにかかわらず、申告漏れが発生することであろう。また、申告漏れを発見することも困難であるため、場合によっては長期に渡って組織の許可を得ずに業務利用される IT 資産（シャドーIT）が存在することもある。資産の一部が把握できず、その割合すらわからない状態では、先に述べた ITAM の目的（リスク管理、コスト管理、競争上の優位性確保）を十分果たせる状況といえないことは明確である。

１．２　申告以外の方法による管理

これまでは“仮想化環境の存在を認識している者”からの申告を元にして、仮想化環境の利用状況を把握することについて述べてきたが、申告による管理のみでは限界があることも上記から推察される。情報提供者からの申告を元に利用状況を把握することが重要であ

ることに異論はないが、他の方法によって不足している情報を更に収集できないか、以下で検討することとする。ただし、以下の例はいずれにおいても、一切の申告が不要で情報を収集できるということではなく、情報の収集を拡充する目的での方法（きっかけ）であることに留意することが望ましい。

（1）Operating System（OS）による把握

使用者がサーバーの存在については把握しており、OS にもアクセスできる状態ではあるが、そのサーバーが仮想サーバーであるのか物理サーバーであるのか知らされていない状態であったとする。仮想化技術は、IT リソースの物理的特性をそのリソースと相互運用するシステムから切り離すという性質上、OS も自らの稼働基盤である物理的特性を確認できない。その場合であっても、OS の存在が発見されている状況であれば、その一覧を作成し、一つ一つの稼働構成を別の担当者（システム導入時の検討メンバー、システム開発・保守部門、セキュリティ対応部門など）からの情報を頼りに収集し、整理することは可能である。

（2）資産管理ツールによる把握

先に述べたとおり、仮想化技術は IT リソースの物理的特性をそのリソースと相互運用するシステムから切り離すという性質上、OS 上で稼働する資産管理ツールから仮想化環境であるかどうかの区別をつけることは困難である場合が多い。一部ツールにおいては仮想化環境の詳細設定情報を収集可能なものもあるため、仮想化環境であるかどうかを区別するという目的ではなく、仮想化環境であることがわかっている場合に更に正確な構成情報やソフトウェアのライセンス使用数を取得するという目的において有用である場合もある。

（3）契約データ（ライセンス契約、保守契約など）を元にした把握

ソフトウェア（ここでは OS や仮想化を実現するためのソフトウェアも含むものとする）のライセンス契約や保守契約、ハードウェアの保守契約、クラウドサービスなどの契約情報から、それらを使用した IT 環境の情報を発見できる場合がある。特に、有効な保守契約が残存している場合、現在も利用中である可能性が高い。組織内の契約フローを追うことで、保守契約の継続を希望した者（利用実態の認識がある者）を特定し、情報を得ることができる可能性がある。

なお、仮想化環境を整理する上で、クラウド環境やハウジング・ホスティングでの利用は別ものとして考える場合もあるが、どのような基盤で稼働する仮想化環境であっても、すべての情報を収集し、その基盤がクラウドか、ハウジング・ホスティングか或いはオンプレミスかといった整理をする方が網羅性の観点において望ましいと考える。

また、仮想化環境でのライセンス利用に関しては、ライセンスルールの複雑さや稼働環境の変動などにより、ライセンス違反が発生しやすいポイントでもある。契約違反の発生するリスクを低減するためにも正確でタイムリーな情報収集が必要である。

（4）業務システム、部門単位での把握

組織内の IT 資産について組織全体で管理するのではなく、業務システムや部門ごとに IT 資産を管理されている場合も多いだろう。その場合、管理単位に合わせた形で情報を収集した場合が効率的である。業務システムごとの管理であれば、その対象システムで利用している IT 資産（サーバーなど）の一覧を作成し、一つ一つ仮想環境であるかどうかを確認し、仮想環境であれば、その構成情報を収集することとなる。部門ごとに管理されている場合も、その範囲内で IT 資産の一覧を作成し、それを元に利用環境を確認する手順は同様である。

１．３　把握すべき項目

（1）仮想環境

仮想環境の把握に関して、把握すべき項目について以下に例を挙げる。必要な管理項目は、テクノロジーや各種契約の変化により、継続的に変動する。したがって、以下のような管理項目を定めた場合でも、定期的な見直しや柔軟な対応が求められるだろう。

①一般情報

表　Ⅰ-3　仮想化環境の管理項目（一般情報）

項目	説明
管理者	該当環境の管理責任者の氏名、社員番号など
管理部門	該当環境の管理部門名
システム名	該当環境を、利用しているシステムの名称 （例：在庫管理システム、勤怠管理システムなどの分類や具体的なシステム名）
利用目的	該当環境の利用目的 （例：データベースサーバー、バックアップサーバーなど）
利用開始日	該当環境の利用開始日
サポート部門	該当環境の内部サポート部門 （仮想化環境の構築は別の部門で対応の場合など）
最終情報確認日	情報の正確性を確認した直近の日付

②利用構成の情報

表　Ⅰ-4　仮想化環境の管理項目（構成情報）

大項目	小項目	説明
仮想環境の構成	ホスト名	環境を一意に特定するためのホスト名
	IP アドレス	環境を一意に特定するための IP アドレス
	仮想化テクノロジー	仮想化環境構築に用いたテクノロジー名やバージョン
	割当 CPU 設定情報	対象仮想化環境に割り当てた CPU に関する設定情報
	割当メモリー設定情報	対象仮想化環境に割り当てたメモリーに関する設定情報
	可用性確保に関する設定情報	スタンバイ方式（Hot-Hot など）やクラスタリングを構成するハードウェア情報など
	仮想化環境基盤	オンプレミス、ハウジング、ホスティング、クラウドなど
ハードウェア情報	ハードウェアベンダー名	ハードウェアのベンダー名
	型番、モデル名	ベンダー指定の型番やモデル名
	シリアル番号	ハードウェアのシリアル番号
	ハードウェアの仕様	搭載 CPU の種類、数量、搭載メモリー数、ディスク容量など
	設置場所	データセンター名、フロア、ラックの場所など
利用ソフトウェア（OS を含む）	ソフトウェア名、バージョン	該当仮想化環境で利用しているソフトウェア名とバージョン
	ソフトウェア設定情報	ソフトウェアに特有の設定情報など（例：同時アクセス数の制限設定、使用 CPU の上限設定）

③契約情報

表　Ⅰ-5　仮想化環境の管理項目（契約情報）

大項目	小項目	説明
ソフトウェアライセンス（OS を含む）	ソフトウェア名、利用可能バージョン	利用可能なソフトウェアの名称とバージョン
	ライセンス使用条件	ライセンスごとの使用条件の詳細（ライセンス使用数に影響を与える管理項目は何かなど）
	保守契約情報	ソフトウェアに関する保守契約の情報（有効期限、サポート範囲等）
	サポートベンダー	ソフトウェアの保守を担当するベンダー名（ソフトウェアごとに整理）
ハードウェア保守	保守契約情報	ハードウェアに関する保守契約の情報（有効期限、サポート範囲等）
	サポートベンダー	ハードウェアの保守を担当するベンダー名

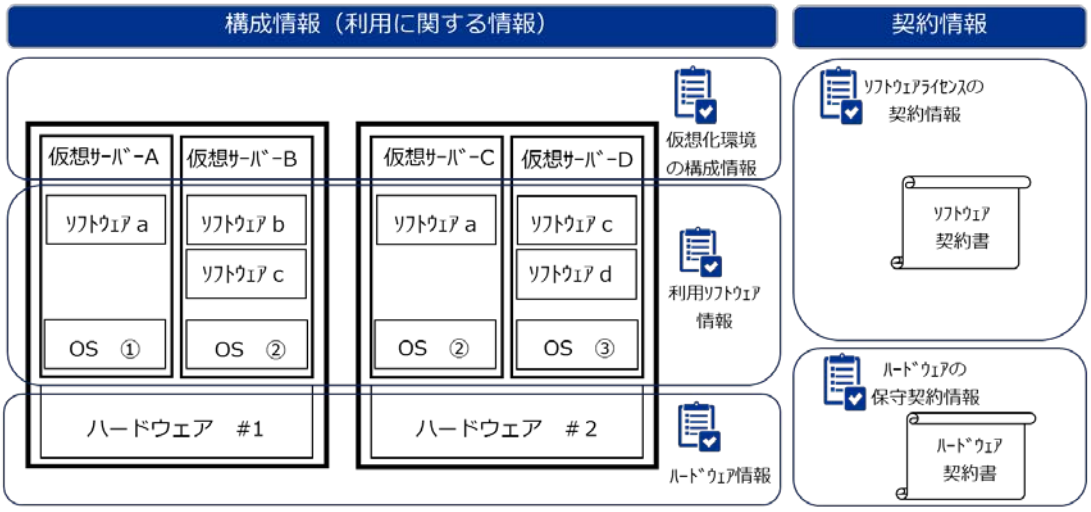

図　Ⅰ-1　仮想環境（サーバーの仮想化）での情報収集の例

２．クラウドの把握

仮想環境の把握においては、仮想環境は情報システム部門が計画・設置・運用することが殆どであるが、クラウドサービスにおいては、情報システム部門以外に、ユーザー部門や場合によっては個人が契約・運用していることがあると共に、当該関係者がクラウドサービスとして意識せずに利用している可能性があることを考慮しなければならない。

なお、現在、『クラウド』という言葉は、一つの IT 用語として考えた際に、それぞれの企業、組織、そして、人によって、受け取り方が異なると共に、一部では実際にはレンタルサーバーで運用されている、企業や組織がデータセンターを借りてサーバーを運用しているものをプライベートクラウドという言葉で表されていたり、反対に、案内には一切クラウドという言葉は使われていないが、パブリッククラウドが利用されていたりする実情がある。そのため、以下の企業や組織で、クラウドサービスの環境を把握する際には、『調査対象としているクラウドサービスの定義』を事前に決めておくことが良い。

２．１　申告による把握

クラウドサービスにおいては、提供されているサービスを稼働させているハードウェア、ソフトウェア、それらの構築、運用、保守、バックアップなどの一切の業務が、クラウドサービス事業者によって実施されているため、クラウドサービスの『利用者』だけが組織内にいることになるのが、今まで社内で利用していた情報システムとの大きな違いとなる。

2.1.1　どうすれば申告してもらえるか？

クラウドサービスにおいては、多くのサービスが Web で閲覧できれば利用できることが多く、システムや通信のログで利用を把握することは不可能ではなく、簡単ではないのも事実ではあるが、監査や申告の漏れを無くす目的での利用は効果がある。

基本は、利用者からの申告による把握とし、申告だけでは網羅性や完全性に課題があるため、それらを補完するためにシステムや通信のログの利用を考えれば良い。

（1）誰に申告をしてもらうのか？

情報システム部門が管理しているクラウドサービスについては、仮想環境と同じ対象者に対して調査依頼をすれば概ね正しい申告が行われると考えて良い。気をつけなければならない点としては、クラウドサービスの定義をハッキリしておかないと、『それも報告しなければならないとは思わなかった』などのような意思疎通が、うまくいかない場合に注意したい。

クラウドサービスの把握においてポイントとなるのが、情報システム部門以外の利用部門、組織の利用者による申告である。利用部門や個人が業務に便利だと思って、場合によっては、クラウドサービスであることも意識せず、利用している場合がある。クラウドサービスの把握は、この利用部門から精度高く申告が上がってくるかが、把握の網羅性において極めて重要と言っても良い。

なお、クラウドサービスについては、社内や組織において『一人だけ』利用するもの、組織内で複数人が利用するものがあるが、複数人で利用するものについては、『誰が申請するのか？』『全員が申請するのか？』ということになるが、基本は、管理者権限を持ったクラウドサービスを契約した利用部門や個人が申告を行うルールとするのが基本的である。な

お、個人で契約して利用しているクラウドサービスの場合は、その 個人が管理者となる。ここで、基本的と記載したのは、クラウドサービス内容によっては、情報セキュリティ対策上などの理由から、該当するクラウドサービスの利用者を会社や組織としても把握したい（管理者権限を持つ利用部門や個人だけに任せない）場合である。この場合は、クラウドサービスの契約者と利用者の両方に申告してもらうルールとなる。

（2）申告の重要性についての認識を全員が持つ

利用部門や個人が、クラウドサービスと指定して利用している場合、また、クラウドサービスであることは知っているが、便利だから、情報システム部門に依頼して時間や手間が掛からず、すぐに利用できるからということで、クラウドサービスを利用している場合には、情報漏洩リスクなど企業にとって大きな問題になる可能性があることを組織内の利用者のすべてに周知と認識を持って貰い、クラウドサービス利用把握のために申告してもらうような教育は極めて重要である。

例えば、情報システム部門が社内ルールに沿って新たなシステムを構築する場合、完全性、可用性、機密性のリスクを評価し、個人情報を取り扱うシステムであれば、個人情報取扱規定を作成すると共に、定期的な内部監査、クラウドサービスであれば、クラウドサービス先の評価などを行い、利用者が安心して利用できるような準備を行っている。

ところが、利用部門や個人がクラウドサービスを利用する場合、これらの社内ルールの取り決めを遵守していることは少なく、また、会社や組織としてクラウドサービスを把握していない場合には、情報漏洩などの情報セキュリティ事故が発生した際に、当然、ルールが整備されていないことから、適切な対応が出来ず、被害を拡大させてしまうリスクがある。

それは、すぐに使えて便利だからというだけの利便性だけでクラウドサービスを利用することについては、利用部門や個人にとっても、会社や組織にとっても、関わりのある全ての関係者にとってリスクであることを理解してもらうことは、クラウドサービスの把握のための取り組みを行う際に極めて重要となる。

（3）申告漏れを防ぐには？

社内や組織の規則や手順について適切な取り組みを行ったとしても、利用部門や個人からクラウドサービスの利用について申告漏れのリスクがあることは避けて通ることが出来ない。また、クラウドサービスであるという認識を持たずに契約・利用される可能性もゼロにはならない。

とはいえ、クラウドサービスについては、クライアントのコンピュータや業務で利用するスマホやタブレットを利用して、主に Web 経由することになることから、それらの端末にログ収集ソフトウェアが導入されている場合、また、組織内から Web を参照するために Web Proxy を導入されている場合には、その利用記録として Web にアクセスした URL が取得可能なはずである。

多くは、大量なログであるため、取り扱いは大変であるが、期間を区切ったり、部署を区切ったりした上で、定期的にURLを確認して、申告されていないクラウドサービスが利用しているか、確認することを検討してみる方法は有益である。また、申告されているクラウドサービスが実際に使われていないなどの確認は比較的容易に行うことが出来る（申告されているので利用されるURLが事前に分かっているため）ので、申告の妥当性についても確認が可能となる。

また、経理部門の協力が得られる場合には、企業や組織で利用するクラウドサービスの契約の多くは、有料で月払いや年払いされることが多く、その額が少額な場合は、請求書払いではなく、クレジットカード払いであることも多い。そういう観点から、申告され、支払われている内容について、とりまとめ、それに似たような支払いがないか、確認してもらうことも企業や組織によっては、効果的な場合がある。

（4）規則や手順の整備

基本的に仮想環境において実施する内容と同じであるが、利用部門や個人がクラウドサービスにおいては契約することになるため、従来からの一般的な情報システム部門を主部門とした規則の変更では対応出来ない場合が多く、新たに検討する必要があることも多いので注意しなければならない。

なお、社内規定を整備する際に、取引先などからファイルの送受信などの取引先が契約したクラウドサービスの利用を求められる場合がある。この場合、自組織内では一切の契約はなく、取引先が契約しているサービスを利用するだけであるが、このような自組織内で契約していないサービスを取引先からの要求があった場合に、どう対応するかは、組織のポリシーもあるので、それを考慮の上で、規則の制定を行う必要がある点は注意しなければならない。

① 規則の制定と監視

クラウドサービスは、実態の把握や管理が利用部門や個人で行われてしまう可能性が高いことから、基本的に“クラウドサービスの利用は会社や組織に申請し、認可されたサービスのみが利用することが出来る”といった規則を制定し、それが遵守されているか、定期的に確認することが必要となる。

監視については、棚卸しのような台帳等書類が適切に運用されているかと共に、実際の利用状況については、ネットワークやPCの通信ログを確認して、実際の利用状況を確認することも重要である。申告されていないクラウドサービスをログから見つけ出すのは簡単ではないが重要なのは言うまでも無い。また、申告されているクラウドサービスは、利用されている URLが分かっているので、申告されたものが利用されているかの確認は、行うことが比較的確認がしやすいので、少なくとも、申告されているクラウドサービスが申告通りの利用者が利用されているかの確認は行っておきたい。

② 業務フローの変更

クラウドサービスを利用部門や個人が契約して利用する場合、毎月か年払いによる使用料が発生するので、その使用料の発生とクラウドサービスの新規利用申請や継続利用申請について連動させる形に、稟議や書類フォーマットを変更することは有効な取り組みとなる。簡単に契約可能で、即利用できるクラウドサービスを会社ルールにより縛って、認可を受けないと使えないことで、デメリットと感じられる場合も多いと思われるが、情報セキュリティ対策上は、避けて通ることが出来ないと認識を持って貰うことが重要である。また、利用部門や個人が組織の事前の許可無く、サービスを契約、使用許諾内容に同意、情報セキュリティ対策上の事前確認が行われないなどについては、経理部門、法務部門、情報セキュリティ対策業務を行っている部門等、多くの部門からの理解と協力を得られることになるので、積極的な関係部門との連携も重要である。この際、各部門から、クラウドサービスを利用するにあたって、必要な情報をヒアリングして、それらの項目についても、稟議や種類フォーマットに追記し、申告があった際には、各部門で必要な情報が共有できるようにすることが望ましい。

2.1.2 どのように申告をしてもらえばよいか？

(1) いつ申告をしてもらうか？

クラウドサービスは、いつでも、すぐに契約出来て、すぐに利用できることから、基本的には、申告については、社内規定の整備によって、会社や組織の利用許可が得られると同時か、利用許可後、すぐに、申告できるように随時受け付けることが必要となる。

また、クラウドサービスにおいては、簡単に利用状況を変更することができる（利用人数、利用者、契約サービス内容、利用の停止）ことから、それらの利用状況に変更があった際にも申告を行うようなルールが必要である。

その上で、利用していた人が部署異動や退職となったにも関わらず、契約だけは存在し、利用料のみ支払い続けているなども少なくないため、定期的なクラウドサービスの利用状況の棚卸しも必要となる。最長でも年に一度、会社や組織の利用方法によっては、より短期間での棚卸しも検討した方が良い。

(2) 申告方法について

会社や組織内において、クラウドサービスの把握のための初回の現状調査については、クラウドサービスの申告の重要性などについて教育や説明後に行うのが望ましい。しかし、何がクラウドサービスか？ということについて分かりにくいこともあり、全社的に実施するか部門毎に実施するかは組織によって変わってくるが、決められた一ヶ月間について、対象となった部門では、『パソコンやタブレットなどの端末を利用する際に、ID と Password を入力した URL を教えて下さい』『パソコンやタブレットなどの端末を設定した際に、ID と

Password を入力して設定したソフトウェアを教えて下さい』(ただし、ソフトウェアや Web ブラウザに ID と Password が記録され、2 回目からの利用では、それらが求められない場合があるので、それらの点については、説明と記載方法について注意書きがあると望ましい)という形で、ID と Password を入力するログイン画面やソフトウェアを収集する。まずは、クラウドサービスとして可能性があるものについて、情報を集めるのが現実的に一番網羅性が高く、申告洩れが少ないと考えられる。ただし、対象部門はもちろんのこと、集まった情報を精査する上においても負荷が高いため、初回の現状調査や、申告されないクラウドサービスの利用が多数見つかった部署などにおいてのみ有効であると考えられる。そして、クラウドサービスと判定できるものについては、クラウドサービスとして所定の申告をしてもらうようにするのが良いだろう。

普段のクラウドサービスについての申告内容については、申告された情報を利用する複数部門が必要とする情報となるため、個々の事例となるが、申告については、前述したようにクラウドサービスの契約者が基本となるが、この際、申告するクラウドサービスを利用している利用者の一覧も申告してもらう項目に入れておくことは重要である。そして、この利用者については、日々変化するため、変化する度に変更の申告をするのか、定期的に利用者の一覧を申告してもらうのか、検討する必要がある。(また、会社として利用者をより厳密に管理したい場合には、管理者以外に利用者も申告をしてもらうことを考える必要がある。)

また、意外と忘れられるのが、クラウドサービスを利用しなくなった(或いは利用者が部署異動や退職等によって減少した場合)際の申告である。これは、クラウドサービスの申告の必要性を案内する際に、多くのクラウドサービスは利用者数で課金され、無駄な費用となることについて、認識を持って貰い、申告と共にクラウドサービス上での利用者の削除やクラウドサービスの契約解除を適切に行ってもらえるように周知していく必要がある。

2.1.3 申告による管理の問題点

クラウドサービスの申告による問題点は、利用部門や個人が契約して利用することが出来るクラウドサービスが多数存在し、今までの情報システムとは比較にならないレベルで、企業や組織内での全数把握することが難しく、シャドーIT があることを想像しつつ、対処が後手に回るという状況になる可能性が少なくないことである。

特に、本格的に利用するのは有料であっても、お試し的な少しだけ利用する場合には、無料で使い続けることが出来るクラウドサービスや、OS やアプリケーションに組み込まれ、利用者は初回設定の時以外は、ID と Password などの認証を意識せず利用できるため、そもそも、クラウドサービスを使っているという意識すらないものも多数あることから、申告してもらうこと自体で網羅性を期待することは難しくなる。

それらの課題に対して、情報セキュリティ対策、コンプライアンスという観点から、クラウドサービスを適切に管理するための予算や体制を組んでいく必要がある。

２．２　申告以外の方法による管理

ここから述べる方法については、申告による把握にとって変わるものではなく、あくまでも、クラウドサービスが社内や組織で利用されていることを発見するための取り組みであり、下記に記載した方法により、『どの端末で、クラウドサービスが使われている』ということが分かるだけであり、その利用者に対して、クラウドサービスの利用している旨を連絡して、申告してもらうことになる。

（1）FireWall、Proxy、端末ログ収集ツールなどによる把握

クラウドサービスにおいては、クラウドに対して通信を行い利用するため、必ず、通信が端末との間で発生する。そして、その通信の多くは、http(https)によって行われる。また、利用に際しても Web ブラウザで利用するサービスが多く存在する。

通信であれば FireWall(最近では UTM)、http(https)であれば、インターネットとの接続に Web Proxy があれば、Proxy Server。そして、クライアントの Web ブラウザであれば、端末ログ収集ソフトウェアにより、通信先の IP アドレスや URL を知ることが出来るようになる。

従って、通信先の IP アドレスや URL をログとして収集されていることから、それらの通信先がクラウドサービスでないかを確認することにより、クラウドサービスが利用されているか確認することが可能となる。

ただし、この調査を行うのは、各クラウドサービスの IP アドレスや URL を知っている必要があり、簡単ではない。

それらの作業を軽減する方法として、Web フィルタリングソフトやサービスを契約している場合には、ジャンル毎の Web のアクセスを禁止するだけでなく、Web フィルタリングデータを利用して、どのジャンルの Web にアクセスしているかを分析する機能も提供されている場合がある。そして、そのジャンルにクラウドサービスなども用意されている場合がある。この場合、クラウドサービスと分類された URL だけを調べることが可能となる。（もちろん、Web フィルタリングデータベースに登録されているクラウドサービスのみが対象となることを留意しておく必要がある。）

また、最近では、新しい CASB(Cloud Access Security Brokers)という概念が登場し、それに沿ったクラウドサービスやソフトウェアの提供が行われ始めている。CASB 自体には、色々な観点があるが、クラウドサービスの把握という点に限って述べると、CASB 対応をうたうサービスや製品には、数百や数千という単位でのクラウドサービスの情報が DB 化されており、それを使い端末がどのようなクラウドサービスを利用しているかを可視化して把握する機能を持っている。

ただし、あくまでも登録されている DB 等に沿って、クラウドサービスを可視化するものであり、そのクラウドサービスの契約状況などが把握出来たりするわけではないので、利用部門や個人がクラウドサービスの利用を申告せずに利用できるものではない。とはいえ、ど

の端末がどのクラウドサービスを利用しているか把握できるだけでも、網羅性を上げることが可能であり、CASB には許可したクラウドサービス以外は利用禁止することが出来るなど、クラウドサービスの把握以外も含めた概念であり、それらを含めて考えるのが現実的と言える。

２．３　把握すべき項目

クラウドサービスにおいては、２．１に示す通り申告による把握を行う際に、申告された情報を管理する複数部門で利用する場合には、それらの管理する部門で必要とする情報が網羅されなければならないため、実際には組織によって内容は変化する。以下では、一般的にクラウドサービスを把握する上で必要と考えられる項目を記載する。

① 一般情報

表　Ⅰ-6　クラウドサービスの管理項目（契約及び一般情報）

項目	説明
管理者	クラウドサービスの管理責任者の氏名、社員番号など
管理部門	クラウドサービスの管理部門名
契約事業者名	クラウドサービスの契約先となる事業者名
契約サービス名	クラウドサービスの契約サービス名(Edition やランク、種別)とオプション契約がある場合には、オプション契約名称
利用ログイン URL	クラウドサービスのログイン URL （ソフトウェアから利用している場合には、ソフトウェアの名称と、ソフトウェアのダウンロード先）
システム名	クラウドサービスを、利用しているシステムの名称 （例：名刺管理システム、ファイル送受信システム、グループウェアなどの分類や具体的なシステム名）
利用目的	クラウドサービスの利用目的 （例：名刺管理システム、取引先とのファイル送受信、スケジュール管理など）
利用開始日	クラウドサービスの利用開始日
契約単位	利用者数、システム数、VM 構成数など
契約支払単位	月払い、年払いなど
契約支払方法	クレジットカード（利用カード名義）、請求書払いなど
契約支払い先	クラウドサービス事業者、クラウドサービス支払い代行業者等
契約連絡先	クラウドサービス全体、支払い先、サポート窓口について、それぞれの URL、e-Mail、電話番号、（ある場合には相手先担当者名）

項目	説明
契約書参照先	クラウドサービスの使用許諾契約等が確認できるURL、あるいは、契約書参照場所
データ保存国	クラウドサービスで利用している情報やデータが、保管、運用されている国名（バックアップ先が別の国にある場合は、それも記載）
個人情報等の有無	クラウドサービスで利用する情報について、個人情報が含まれているかの有無、また、取り扱うデータの機密性、完全性、可用性の評価
社内規定の有無	クラウドサービスを利用する上で専用の社内規定の有無、専用の規定がない場合には、既存の社内規定で適用できるかの確認の有無、確認部署、確認担当者、確認日時の記載
サポート依頼先	クラウドサービスのサポートについて、クラウドサービス事業者ではなく、サポートを別業者に依頼している場合、その依頼先の事業者名
情報確認日	情報の正確性を確認した直近の日付及び、確認したものの氏名、社員番号

② 利用構成の情報

表　I-7　クラウドサービスの管理項目（管理情報）

大項目	小項目	説明
管理者情報	システム管理者名（契約者）	クラウドサービスの利用に際して、システムの全ての権限を持っている管理者（契約者）について、氏名、社員番号、クラウドサービス上でのログイン名
	部門管理者名	クラウドサービスの利用に際して、システムの全ての権限を持っている管理者から全部、一部の管理権限を与えられている管理者の氏名、社員番号、クラウドサービス上でのログイン名
	契約者情報	契約者とシステム管理者が異なる場合には、本項目に契約者に関する氏名、社員番号、クラウドサービス上でのログイン名

大項目	小項目	説明
運用情報	アカウント発行や削除を行っている管理者名	クラウドサービスの利用に際して、利用者にアカウントの発行、及び、削除を行っている管理者の氏名、社員番号、クラウドサービス上でのログイン名 （利用部門別に存在している場合には、各部門の全ての管理者を記載）
	組織内サポート窓口	当該クラウドサービス利用時に、組織内から相談を受ける主な社員の氏名、社員番号、クラウドサービス上でのログイン名 （利用部門別に存在している場合には、各部門の全ての管理者を記載）
	制限事項	クラウドサービス上で設定可能な各種制限を行っている場合には、その制限内容を記載
	ログ参照方法と保存期間	クラウドサービスを利用する上で取得され参照可能なログの内容、参照方法、保存期間
	データバックアップ方法	クラウドサービスで取り扱うデータについてのバックアップ方法の記載（例えば、オプションのバックアップサービスの利用、ダウンロードしてきて保管等）
利用者情報	利用者情報	クラウドサービスを利用している利用者の氏名、社員番号、クラウドサービス上でのログイン名の一覧
	契約ユーザー数	利用者情報更新時の契約ユーザー数 （契約がユーザー数課金の場合のみ）
	利用者情報更新日	利用者情報項目の情報を更新日及び、確認したものの氏名、社員番号の正確性を確認した直近の日付
情報確認日	利用者情報を除く、情報の正確性を確認した直近の日付及び、確認したものの氏名、社員番号	

※組織によっては社員名、社員番号以外に部署名を追加することを要検討。

Ⅱ．環境の管理

１．仮想環境の管理

１．１　目的・適用範囲及び用語の定義

（1）目的

本項の目的は、仮想環境の管理をするために必要な事項を明確にし、管理者視点で、有効かつ効率的な管理方法を提言することにある。

（2）適用範囲

仮想環境の管理は、仮想環境と、仮想環境が構築される物理環境との双方を管理することになるため、本項では双方の関係を考慮した環境を適用範囲とする。

（3）仮想環境の分類

本委員会では仮想環境を次の二つに大別[1]している。

①IT プラットフォームの仮想化

あるコンピュータのハードウェア上で制御プログラムが擬似的なコンピューティング環境を生成し、その環境上で稼働するゲストソフトウェアに対して「仮想マシン（Virtual Machine）」を提供するものである。単一の物理マシン上で複数の仮想マシンを動かすことができるため、様々なソフトウェアの開発、テスト、シミュレーションなどに用いられる。プラットフォーム仮想化には、エミュレータまたはシミュレータなどのソフトウェアを使用する方法、同一プラットフォーム上でネイティブに仮想化を実現する方法、ハードウェア自体が隔離された状態で動作できるハードウェア仮想化と呼ばれる方法などがある。

②IT リソースの仮想化

上記のプラットフォーム仮想化の概念から発展し、演算装置、補助記憶装置、回線終端装置、端末装置など特定の IT リソースを仮想化する仕組み。

さらにⅱ）IT リソースの仮想化は、次の四つに分類している。

ⅰ）サーバー仮想化

ⅱ）ストレージ仮想化

ⅲ）ネットワーク仮想化

ⅳ）デスクトップ仮想化

---

[1]　詳細は「クラウド時代の ITAM の考え方 平成 28 年 2 月」参照のこと。説明文には一部引用を含んでいる。

(4) 研究の方法

本項では、自組織内の仮想環境を管理するという前提で、上記項目の内、②IT リソースの仮想化の内、ⅰ）並びにⅳ）の一部と、それに関連する①IT プラットフォームの仮想化の一部について、コスト並びに管理の最適化・効率化の観点からの管理方法を提言することとし、この範囲を「仮想環境」と呼ぶこととする。

１．２　管理プロセス検討時の前提考慮事項

仮想環境を管理する際には次の三つの事項を考慮する必要がある。

(1) 物理環境と仮想環境

(2) 仮想環境の利用目的の差異

(3) ライセンスの要求事項

(1) 物理環境と仮想環境

仮想環境の管理の難しさは、物理環境と異なり、構築されている環境が物理的に見えないことにある。これは、ソフトウェアの管理に共通するところでもある。

ソフトウェアの管理には、ソフトウェアが稼働するハードウェアの把握が必須であるのと同じく、仮想環境の管理には、当該仮想環境が構築される物理環境の把握が必須である。ライセンスコンプライアンス上も、運用管理上も、物理環境の構成管理と、仮想環境ごとの構成管理の一体管理が必要となる。

そのため、どの物理環境にどの仮想環境が構築されているのかを把握し、仮想環境を個別に識別することを目的として、物理環境への管理番号を振るだけでなく、そこに構築される仮想環境にも個別に管理番号を振って、個々に識別することが望まれる。(図Ⅱ-1　仮想環境のイメージⅠ参照)。

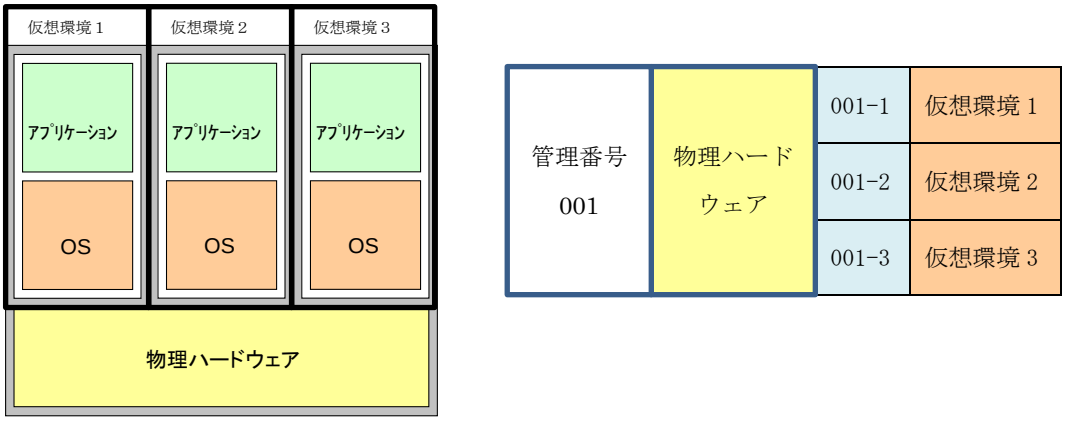

図　Ⅱ-1　仮想環境のイメージ　Ⅰ

また、仮想環境には、一つの物理環境ではなく、複数の物理環境上に構築されるもの（以下「仮想クラスター」という）もあるため、仮想クラスター環境を持っている組織では、複数の物理環境の上に構築される仮想環境の管理も考慮しておく必要がある。

このような仮想クラスター環境では、クラスター化される複数の物理環境をすべてグループ化して、仮想環境に提供されるすべての物理環境の構成情報を把握できるようにしておくことが推奨される（図Ⅱ-2　仮想環境のイメージⅡ参照）。

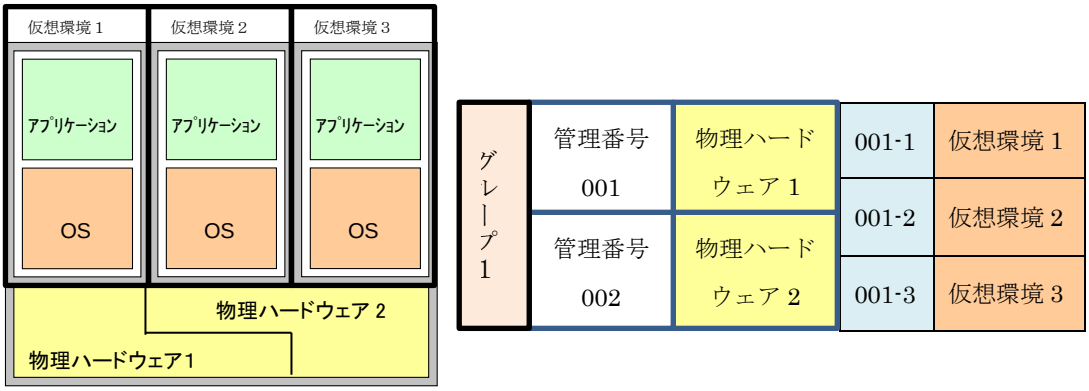

図　Ⅱ-2　仮想環境のイメージ Ⅱ

しかし、管理番号を貼付するといっても、物理環境を持たない仮想環境に管理番号を貼付することはできないため、次のいずれかの方法で管理をする。

①仮想環境への管理番号の割り振りは、管理台帳上のみとし、物理環境の管理番号と紐づけて登録する。
②①に加え、物理環境の管理番号に仮想環境を持っていることがわかる符号をつけて管理する。
③①に加え、紐づく物理環境にも個々の仮想環境の管理番号を貼付しておく。

いずれの場合においても、すべての環境が把握され、管理台帳に登録されることが前提となっているが、仮想環境を持つ物理環境のハードウェアは、単に物理環境のみのハードウェアよりもより複雑な管理が求められるため、できれば管理台帳のみで仮想環境を把握できるようにするだけではなく、棚卸や監査での対応も考慮し、物理環境のハードウェアを見ただけでそこに仮想環境があるかどうかが判別できるような管理をしておくこと、即ち、上述の②あるいは③の方式を取っておくことが望ましい。

ただし、②については、管理番号体系自体を変えようとすると、管理番号発行のプロセスが複雑になり、且つ、仮想環境を持たなくなった場合に管理番号の貼り換え等が必要となってしまうため、例えば、管理番号自体は通常の番号体系で発行し、その番号とは別に仮想環境を持つことを示す識別シールなどを別に貼付するなどの工夫があって良い。

③の一つの物理環境に複数の管理シールを貼付することはあまり見た目の良いモノではないかもしれないが、どんな環境があるのかを確認するには、最も簡単な方法ではある。③で行う場合には、実際にはおそらくサーバーのほとんどはサーバーラックに格納されており、サーバー自体に複数の管理番号を貼付するというよりも、ラックに仮想環境分の数の管理番号のタグをつけるなどの対応になるだろう。

仮想環境は、構築した担当者あるいは管理者でなければ、それがどこにあるか、どのような構成であるかを把握することは難しい。

そのため、仮想環境を管理するためにはまず、仮想環境構築時の手順として、適時に管理台帳に記載することを定め、それを適切に運用するための教育を徹底することが必要である。

また、構築された仮想環境が漏れなく台帳に登録されることを推進していくためには、定期的な棚卸に加え、内部監査も実施し、運用状況を把握し是正することが必要である。

なお、ここで対象としている仮想環境はあくまでも静的な仮想環境（環境を構築したら、数か月以上同じ環境にて運用される仮想環境）を想定しており、動的な仮想環境（開発環境など、数日～１か月単位等の短期で、環境が再構築される仮想環境）を想定していない。動的な仮想環境の管理については、(2) 仮想環境の利用目的 に記載する。

(2) 仮想環境の利用目的の差異

上述したように、仮想環境には「静的な仮想環境」と「動的な仮想環境」がある。

例えば、社内の何らかのシステムが構築されている仮想環境であれば、その仮想環境はおそらく数か月以上、場合によっては数年にわたって利用し続けられる可能性が高い。

これに対し、例えばシステムの開発会社等で、顧客のシステム開発を請負っている場合は、自社で製品を開発している場合で、それらの開発環境として利用されている仮想環境では、数週間あるいは数日単位で仮想環境が再構築されることが少なくない。また、こういった環境では使用されるソフトウェアライセンスの種別も異なっているケースが多い。

前者の静的な仮想環境であれば、管理台帳に登録し、必要に応じた変更管理を行い、環境内の棚卸をする対象とすることは問題ない。しかしながら後者の動的な仮想環境においては、再構築の都度、管理台帳へ登録するという行為は、運用に耐えられるものにはならない。

そのため、動的な仮想環境は、静的な仮想環境とは区別して管理することも検討する必要がある。

動的な仮想環境は、一般的には、開発環境や検証環境といった、特別な環境下で利用されていることが多く、組織の一般的なネットワークに接続され利用されているケースは少ない。また、そこで利用されるソフトウェアライセンスも特殊な使用許諾条件（サイトライセンスやユーザーライセンス、開発用のサブスクリプションなど）のものが多い。そのため、仮想環境の利用目的に合わせ、例えば次のような対策をとることが考えられる。

①動的な仮想環境の管理規定を静的な仮想環境とは別に定める
②動的な仮想環境を持つ物理環境を特定する
③当該物理環境でしか使用しないライセンスを特定する

① 動的な仮想環境の管理規定を静的な仮想環境とは別に定める

静的な仮想環境と規定自体を分けるということではなく、動的な仮想環境と静的な仮想環境の取扱いについて、それぞれ別に定めることが望ましい。ただしその場合には、動的な仮想環境と静的な仮想環境が混在する物理環境を作らないことが前提となる。

動的な仮想環境には、動的な仮想環境用に割り当てられたライセンス以外を割り当てないなどの制限も規定すること。

② 動的な仮想環境を持つ物理環境を特定する

その物理環境が動的な仮想環境を持っていることが明確にわかるようにすること。そして当該物理環境の管理責任者を明確にすること。上述の通り、当該物理環境は、静的な仮想環境と動的な仮想環境が混在することのないようにすること。

当該物理環境が動的な仮想環境用であることがわかるようにするために、１．２ 管理プロセス検討時の考慮事項（1）物理環境と仮想環境に記載した②の管理方法を参考に、識別できるようにすることが望ましい。

当該物理環境の管理責任者には、当該物理環境が動的な仮想環境の構築のみに利用されるよう適切に管理を行う責任を持たせること。

③ 当該物理環境でしか使用しないライセンスを特定する

動的な仮想環境で利用するライセンスは予め特定し、当該物理環境にしか紐づけられないようにすることも検討してみることが推奨される。

動的な仮想環境でしか利用できないライセンスを特定しておくことで、無用なライセンスコンプライアンス違反が発生することを抑止する効果がある。

(3) ライセンスの要求事項

仮想環境は容易にその構成を変更することができるため、仮想環境におけるソフトウェアライセンスの管理は、物理環境しか持っていないハードウェアよりもより厳密に行う必要がある。これは、静的な仮想環境であるか、動的な仮想環境であるかにかかわらず、どちらも同じように重要なポイントの一つである。

このライセンスの要求事項の管理の重要性については、仮想環境に限ったことではないが、より厳密な管理を行わなければならない可能性があるという点で、再度考慮するため、以下の 2 点を記載しておく。

①ライセンスされている CPU の条件を明確にすること
②その他必要な使用許諾条件を把握しておくこと

①ライセンスされている CPU の条件を明確にすること

最近では CPU の変更や追加などが容易になってきており、サーバーの機能強化の際には、ハードウェアのスペックを変更することが少なくない。

しかし、サーバーライセンスの多くは CPU の性能に依存したライセンス体系となっていることから、ハードウェアのスペックの強化は使用許諾条件の逸脱につながる可能性がある。また、仮想環境に割り当てているリソースは変わっていなくとも、サーバーライセンスの中には、物理環境のスペックでライセンスが割り当てられるものも増えてきている。

したがって、これらのライセンスを登録する際には、サーバーの環境条件を適切に登録し、可能であるなら、当該ライセンスが適用されるハードウェアの CPU 情報と比較する仕組みを持ち、変更が生じた場合には適時に見直しができるように把握しておくことが必要だ。

②その他必要な使用許諾条件を把握しておくこと

上述した CPU だけでなく、サーバーのソフトウェアライセンスの使用許諾条件は、単にインストールされている数だけでなく、仮想環境を構成している物理環境のパーティション方式や、仮想方式によって異なるものもある。

また場合によっては、利用しているソフトウェアのパブリッシャーが指定するプロセスを定期的に実施し、その記録の保管を義務付けているような使用許諾条件もある。

以上のように、サーバーの使用許諾条件は一般的に論じられるほど簡単ではなく、特に委託先や調達先に任せきりにしているのは非常に危険である。必ず自ら確認し、検証する機会を持つことが大切である。

１．３　管理項目例

最後に、仮想環境を管理するために必要と思われる管理項目の例を紹介する。

SAM の管理台帳については、過去に本委員会においても「SAM ユーザーズガイド～導入のための基礎～平成 24 年 2 月（改定版）」にも記載しているが、当時は仮想環境を想定した項目とはなっていなかったため、ここで新たに加えることが推奨される管理項目のみ、説明を追記しておく。

なお、以下の管理項目は、一般社団法人ソフトウェア資産管理評価認定協会（SAMAC）が 2017 年 10 月に開催したライセンスセミナーで発表した資料を基にしていること、紹介する管理項目はあくまでも例として提示するものであり、実際に必要となる管理項目は、組織の保有している資産の種類や管理プロセスによって異なるものであることを申し添えておく。

また、以下にはソフトウェア管理台帳とライセンス媒体管理台帳は存在していないが、これは今回の例示では、特に追加が必要となる項目はないと判断したためである。

（前提条件）

今回例示する管理項目の前提条件は以下の通りである。

・詳細な台帳管理は、静的な仮想環境を対象としていること

・物理環境と仮想環境の関係は、多対多も想定していること

（1）ハードウェア管理台帳（例）

項目名	説明
ハードウェア区分	物理環境か仮想環境かを判別する区分
物理ハードウェアグループ番号	仮想環境が構築されている物理環境を特定するための管理番号。 複数の物理環境上に仮想環境が構成される場合を想定している。 物理ハードウェアグループ番号は、物理ハードウェア管理番号に別途紐づく（「物理環境管理台帳」参照）。
仮想化方式	VM Ware、Hyper-V、Xen、Oracle VM など、仮想化ソフトウェアの名称を記録する。
パーティション方式	ハードウェアパーティションかソフトウェアパーティションかの別を記録する。 利用するサーバーソフトウェアによって区別して管理する必要がある。

（2）物理環境管理台帳（例）

項目名	説明
物理ハードウェアグループ番号	「ハードウェア管理台帳」参照。
物理ハードウェア管理番号	物理ハードウェアグループ番号に紐づく物理環境のハードウェア管理番号が登録される。一つの場合もあれば、複数の場合もある。

（3）ライセンス管理台帳（例）

項目名	説明
CPU 名	ライセンスが許諾されている CPU の情報を記載する。できれば、紐づけるハードウェアの CPU 情報と比較し、差異があった場合には通知される等の機能があることが望ましい。
CPU 物理数	
CPU コア数	
CPU ソケット数	

パーティショニング方式	ハードウェアパーティションかソフトウェアパーティションかの別を記録する。 利用するサーバーソフトウェアによって区別して管理する必要がある。
仮想サーバー用ライセンスフラグ	主に動的な仮想環境を持つ物理環境に紐づけるライセンスを特定するためのフラグ。
物理ハードウェア管理番号	主に動的な仮想環境を持つ物理環境のハードウェア管理番号を指定する。当該物理環境もしくは当該物理環境を利用する仮想環境でしか紐づけができないようにすることによって、無用なライセンスコンプライアンス違反を抑止する。

なお、上述でご紹介している SAMAC のセミナー資料には、クラウド契約・クラウドライセンスの管理やサイトライセンス・セカンドライセンスの管理も前提とした管理項目例も紹介されているので、機会があれば参照することを推奨する。

２．クラウドサービスの管理

２．１　目的、適用範囲及び用語の定義

（1）目的

本項の目的は、クラウドサービスを実現するために必要な環境を明確にし、特にクラウドサービスを導入する顧客視点で有効かつ効率的なサービス管理方法を提言することにある。

（2）適用範囲

クラウドサービスを実現するための環境は大きく、物理的・技術的環境と組織的・人的環境の 2 つに分けられる。また、これらを契約主体で分けると、サービス供給者（データセンター、PaaS、SaaS）、サービス利用者（社内ネットワーク、クライアント端末）、インターネットの三つに分けられる。本項はこれらクラウドサービスを実現するためのあらゆる環境および契約主体を適用範囲とする。

（3）用語の定義

本ガイドにおける用語の定義は「クラウド時代の ITAM の考え方」（平成 28 年 2 月一般財団法人日本情報経済社会推進協会、以下「JIPDEC」）に準ずる。

①クラウドコンピューティング

ネットワークを介して、サーバー・ストレージなどのハードウェア、OS 及びミドルウェア、アプリケーションソフトウェアなどの IT リソースを即時に迅速かつ効率的に利用できる、IT サービスの利用形態である。

②クラウドサービス

クラウドコンピューティングにより提供される IT サービスのことを指す。

クラウドコンピューティングは、用途別に大きく「パブリッククラウド」と「プライベートクラウド」の二つに分類される。

③パブリッククラウド

インターネットを経由して不特定多数の利用者に向けて提供される IT サービスである。一般的に「クラウド」という場合はこのパブリッククラウドを指す。パブリッククラウドを提供する事業者の多くは、自社保有又は契約先のデータセンターにサーバー仮想化技術を活用したクラウド環境を構築している。サービス内容は事業者がパブリックに公開し提供する共通メニューから、顧客がそれぞれのニーズに応じて取捨選択する。

④プライベートクラウド

インターネットやイントラネット等を経由して特定の利用者に向けて提供される IT サービスである。プライベートクラウドは、サーバー仮想化技術を活用しつつ、特定顧客のニーズに合わせてカスタマイズされたサービスを提供する。パブリッククラウドのコストメリットは損なわれるが、自社のオンプレミス環境並みの設計の自由度とセキュリティ要件を満たせる点が特徴である。

本ガイドの考察は主として前者のパブリッククラウドを想定したものである。

２．２　クラウドサービス環境の分類

上記「適用範囲」で述べた通り、クラウドサービス環境は、以下の六つに分類される（表Ⅱ-1 参照）。それぞれにおいて把握・検討すべき項目を表内に記載した。

表　Ⅱ-1　クラウドサービス環境の分類

		クラウドサービスの環境	
		物理的・技術的環境	組織的・人的環境
契約主体	サービス供給者の環境	サービスプロバイダーのデータセンター（プロバイダーが委託契約した外部データセンターを含む）	サービスプロバイダーの組織、人員、体制、規定等（プロバイダーが委託契約した外部組織要員を含む）
	サービス利用者の環境	法人顧客の場合、法人内のネットワーク、法人所有のクライアント端末及びモバイル端末(*1) 個人顧客の場合、自宅のネットワーク、個人所有のクライアント端末、モバイル端末	法人顧客の場合、組織、人員、体制、規定等（契約管理、ネットワーク管理、クライアント管理等を含む） 個人顧客の場合、本人及び家族の知識に依存する
	インターネット環境	インターネットプロバイダーのデータセンター及びネットワーク	インターネットプロバイダーの組織、人員、体制、規定等

*1 サービス利用者の物理的・技術的環境として、稀に個人所有の端末を業務目的で利用することを可としている場合もある。（BYOD: Bring Your Own Device）

２．３　研究の方法

本項では上記の分類を意識しつつ、クラウドサービスの利用目的、契約内容、利用範囲、利用条件について可能な範囲で情報を収集、分析し、本項の目的にも述べた通り、顧客視点によるクラウドサービスの導入プロセスにおける有効かつ効率的なサービス管理方法を提言する。

２．４　導入・管理プロセス

（１）利用目的の明確化

クラウドサービスを導入する際にチーム内で最初に合意しておくべき事項は、「何のためにこのサービスを導入するのか」という点である。初期の段階で利用目的を明確化しておくことは、その後のサービス選定のプロセスを有効かつ効率的に進める上で必須である。逆にこの点が曖昧な顧客は導入のプロセスにおいて迷走するケースが多い。本プロセスにおいて顧客が自らの責任で検討すべき論点は以下の二点である。

①業務上の必要性

クラウドサービスの最大の特徴は立ち上げ期間の短さである。ビジネスの変化に即応して、いち早く求められるサービスを立ち上げ、事業のロケットスタートを支援することが出来れば、市場を早期に囲い込むことができるのである。

現在のクラウドサービスの平均的な立ち上げ期間は、特定業務向けアプリケーションの場合、契約書に調印してから1～2日後には顧客向けアカウントが開設されて、1～2週間で各種設定と管理者教育が行われ、即利用可能というのが近年のスピード感である。

一部のクラウドサービスでは、標準的な契約条件を利用規約としてインターネットで公開し、その内容に同意するという旨を表明し、インターネットで申し込みを行えば、その時点で契約が成立するというタイプのサービスも増えている。これらのサービス料金は個人ないし法人クレジットカードにより決済される。クラウドサービスにおける導入プロセスの簡素化、スピードアップが進んでいる。

②類似サービスの有無及び比較検討

クラウドサービスに限らず、情報システムやアウトソーシングサービスの導入検討においては、類似サービスの有無およびそれらの比較検討は必須である。しかし、アプリケーションソフトウェアの機能や実際の使い勝手はサービスカタログだけではわからないことが多い。そのためクラウドサービスで提供されるアプリケーションソフトウェアの機能・仕様が自社の業務システムの要件を満たしているかどうかを判断するためには、顧客側にも相応のスキル（知識と経験）が求められる。これらのことが、多くの組織においてシステム検討期間が長引く一因となっている。

クラウドサービスの特徴の一つに、前項の立ち上げ期間の短さとほぼ同義であるが、お試しのためのアカウント開設が比較的低コストで実現出来るという点が挙げられる。多くのクラウドサービスが有償無償の別はあるものの、ミニマムコストでのトライアル契約を準備している。これにより、クラウドサービスの中身、特に提供されるアプリケーションソフトウェアの機能・仕様が自社の業務要件をどの程度満たしているのかを、顧客自身の

目で確認することができる。これらのトライアル契約を適宜活用することで、導入プロセス全体の短縮化、ひいてはビジネスの変化に対するITサービスの即応を実現することが、一層容易になるものと考える。

（２）契約内容の精査及び記録

クラウドサービスの利用目的が明確化され、ある程度候補となるサービスが絞り込まれると、次にそれぞれのサービスの契約条件を精査する段階となる。本プロセスにおいて顧客が自らの責任で最低限検討すべき論点は以下の四点である。

①契約期間

クラウドサービスの契約期間は１ヶ月単位から複数年契約まで様々なバリエーションがある。一般的な傾向としては、データ提供型のクラウドサービスは１ヶ月単位の契約が用意されており、しばらく試してみて有益な情報提供が得られない場合は短期で契約解除できる。一方データ蓄積型のクラウドサービスは１年単位の契約が主体である。

クラウドサービスの特徴として、使用した結果、当初期待した機能・便益が得られなかった場合、すぐに契約解除できるという点が挙げられる。なおクラウドサービス契約には一般に契約期間の自動更新条項が含まれているため、解約の意思がある場合は一定期間の猶予をもって文書により解約の意思表明をしておく必要がある。またデータ蓄積型のクラウドサービスを解約する場合、それまでに蓄積したデータをどのような形でダウンロードできるのか、有償･無償等の条件を、契約時に事前に確認しておくことが望ましい。

（例文１）「この契約期間は、いずれかの当事者が更新しない旨の書面による通知を更新期間開始の 30 日前までに行わない限り、当該時点における本製品の料金をもって、その後１年ずつ自動更新されるものとします。」

（例文２）「本クラウドサービス終了後 30 日以内であれば、お客様からの要求に基づき、当社はお客様がこれまでアップロードしたデータ及びファイルのコピーを別途定める手数料で返却します。このデータは暗号化されたメディアにより返却されます。」

②契約料金

クラウドサービスの年間利用料金は、類似のオンプレミス型アプリケーションソフトウェアの一括購入価格の三分の一程度に設定されていることが多い。オンプレミス型ソフトウェアの価格を 100 万円とすると、１年間の償却費用は五分の一の 20 万円である。また

ソフトウェアの年間保守料金は一般に購入価格の 10%（10 万円）程度である。このソフトウェアの購入に伴う年間コストは 20＋10＝30 万円となる。これにハードウェアの減価償却費、システムの運用コストなどを加えて算定された結果が、一括購入価格の半分から三分の一程度ということなのである。顧客側のメリットとしては、初期費用を平準化することができ、場合によっては 1 年程度で使用契約を解除することができる点である。クラウドサービスによっては、解約禁止条項付きの複数年契約を一定の割引料金で提供しているケースも多い。

③契約先（法人）

クラウドサービスの契約先（法人）は、当該クラウドサービスの提供会社（サービスプロバイダー）であるか、又はその正規代理店である。いずれの場合も、サービスプロバイダーが提供あるいはインターネット上で公開している「利用規約」に同意することを前提に契約内容に合意し、注文書に署名・捺印する形式となっている。逆に言うと、注文書に著名・捺印した場合、自動的に関連する利用規約に同意したと見做されるので、注意が必要である。

（例文）「本サブスクリプション注文書が締結された場合、お客様は弊社がインターネット上で公開している当該サービスプロバイダー契約条件書（別紙を含む。）の内容についても同意したものとみなします。」

④契約サービス内容

クラウドサービスの契約サービス内容は、当該サービスプロバイダーが定義した「ドキュメント」すなわち「システムガイド、管理者マニュアル、利用者マニュアル」などに適合することを保証している。サービスプロバイダーが営業時に提示したカタログ、パワーポイントのプレゼン資料などのマーケティング資料は、サービス内容やシステム機能を保証するドキュメントの範囲外となっているケースが多いので注意が必要である。

（例文）「弊社は本サービスが以下に定義するドキュメントに適合するものであることを保証します。このドキュメントとは、本サービスと共に弊社がお客様にお届けするシステムガイド、管理者マニュアル、利用者マニュアル等のことです。尚、ドキュメントには営業・マーケティング資料は含みません。」

（3）利用範囲の指定

①利用可能件数（利用ユーザー数、採用予定人数）

クラウドサービスには、利用ユーザー数や利用端末数により、利用範囲を指定しているものがある。このうち一般的なのは利用ユーザー数による課金である。例えば、マネジメント系システムを例に取ると、人事評価のクラウドサービスの場合、一人当たりの単価を設定し、サービスを利用する部門の全従業員数により料金を見積もる。ユーザー数が一定枠を越えると数量割引を効かせる場合も多い。一方、人材採用におけるデジタル面接のクラウドサービスの場合、募集企業の「採用予定人数」によって課金する体系を採っている場合もある。

②利用可能範囲（契約法人内、子会社・関連会社、出資比率制約条件等）

クラウドサービスには、法人の関係性により、利用範囲を指定しているものがある。一般的には契約法人内のみで利用可能とするものである。一方、契約法人のグループ企業についても一定条件下でサービス利用を認めているケースがある。日本のサービスプロバイダーの場合、契約法人の出資比率 50%以上の子会社について利用を認めている場合が多い。一方、米国のサービスプロバイダーでは出資比率 30%以上でこれを認めている例がある。プロバイダーごとに条件が異なるため、グループ利用により数量割引を得たいと考えた場合は、事前に条件を確認する必要がある。

③利用予定端末

クラウドサービスには、利用予定端末により、利用範囲を指定しているものがある。端末の仕様により利用制限がある場合又は、端末の数量により課金している場合などがある。それぞれ、クラウドサービスの利用範囲、ユーザーの使い勝手に対する影響が大きいので、これらも事前に利用制限、課金体系などを確認する必要がある。

（4）利用条件の把握

①OS（OS 種類、バージョン）

クラウドサービスには、利用端末の OS により、利用条件を制限しているものがある。特に最近はモバイル端末によるクラウドサービスの利用が拡大しており、iOS、Android など利用可能な OS の種類とバージョンを確認することが重要となってきている。

②ブラウザ（ブラウザ種類、バージョン）

一方、PC 上でクラウドサービスを利用する際には、OS の違いよりも、ブラウザの種類とバージョンに依存する場合が多くなってきている。現在では Google Crome を標準ブラウザに設定するクラウドサービスが増加している。

③必要通信ポート

デジタル面接など動画を利用するクラウドサービスが増加しており、そのために動画を通過させるための通信ポートの設定が必要となっている。企業によっては社内から Youtube などを閲覧できないよう動画を通過させない設定にしている場合があり、最新クラウドサービスを利用する上で、顧客企業側にも柔軟な対応が求められる。

（5）SLA およびセキュリティ条件の把握

クラウドサービスにおいて把握すべき、SLA およびセキュリティ項目は以下の通りである。

1）サービス時間

（1－1）

- サービス時間

サービスを提供する時間帯（ネットワーク等の点検／保守のための計画停止時間の記述）

（例文）24 時間 365 日（計画停止／定期保守を除く）

（注記）業務システムの使用可能な時間帯を規定するとともに、定期保守により使用できない時間も明確化する。

（1－2）

- 計画停止予定通知

定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）

（例文）計画停止は通常、毎週土曜日の午前 6 時から 8 時まで。30 日前にメール／ホームページで通知する。

（注記）計画停止時間はサービス時間の一要素として規定されるが、停止予定を事前に通知することを取り決める。

2）可用性

（２－１）

● サービス稼働率

サービスを利用できる確率＝（(計画サービス時間－停止時間）÷計画サービス時間）

（例文）サービス稼働率は 99%以上を保証。

（注記）サービス時間として規定した時間帯に実際にサービスを受けられたのかを測定し、業務の特性に見合ったサービス提供が行われているかを明確化する。

（２－２）

● ディザスタリカバリ

災害発生時のシステム復旧／サポート体制

（例文）データは日次バックアップを取得し、他所に保存。

（注記）サービス時間として規定された時間帯にサービス提供を受けることに関して、災害時の対応の考え方を取り決める。

（２－３）

● 重大障害時の代替手段

早期復旧が不可能な場合の代替措置

（例文）万が一、データセンターが損壊した場合は、他の代替地で 5 日以内にデータを復旧。

（注記）計画停止以外のシステム停止は早急な復旧が求められるが、目標復旧時間内での対応が困難な障害が発生した場合の、代替手段を用いた復旧方法を規定しておく。

（２－４）

● アップグレード方針

バージョンアップ／変更管理／パッチ管理の方針

（例文）年数回の定期バージョンアップを実施。パッチ当ては数週間毎に実施。

（注記）確実なサービス提供を行うためには定期的にシステムを最新状態にし、環境変化に対してシステム構成を変更していく必要があるが、それをどのような条件・タイミングで実施するかなどのポリシーを明確化する。

3）信頼性

（３－１）

- 平均復旧時間

障害発生から修理完了までの平均時間（修理時間の和÷故障回数）

（例文）１時間以内（基幹業務）、12 時間以内（基幹業務以外）

（注記）サービス時間として規定された時間帯にサービス提供を受けることに関して、障害時の復旧の時間を取り決める。

（３－２）

- システム監視基準

システム監視基準（監視内容／監視・通知基準）の設定に基づく監視

（例文）パフォーマンス及びその他の機能について常時監視を実施。

（注記）サービスの安定的供給を受けることに関して、システム監視基準を設定し、監視を行うことを取り決める。

（３－３）

- 障害通知プロセス

障害発生時の連絡プロセス（通知先／方法／経路）

（例文）指定された緊急連絡先にメール／電話で連絡し、併せてホームページで通知

（注記）サービスの安定的供給を受けることに関して、障害発生時の連絡プロセスを取り決める。

（３－４）

- 障害通知時間

異常検出後に指定された連絡先に通知するまでの時間

（例文）15 分以内（基幹業務）、2 時間以内（基幹業務以外）

（注記）サービスの安定的供給を受けることに関して、障害発生時の障害通知を受ける時間を規定しておく。

（３－５）

- 障害監視間隔

障害インシデントを収集／集計する時間間隔

（例文）１分以内（基幹業務）、15 分（基幹業務以外）

（注記）障害発生時に、迅速な対応を取ることができるように、ネットワーク、サーバー、ストレージ、アプリケーションなどのシステム構成要素の稼動状況を監視するための間隔を規定する。

（３－６）

- サービス提供状況の報告方法／間隔

サービス提供状況を報告する方法／時間間隔

（例文）月に一度ホームページ上で公開

（注記）ユーザーが必要とするサービス提供状況に関する情報を、決められた時間・間隔で決められた方法で提供できるようにする。

（３－７）

- ログの取得

利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）

（例文）アクセスログは原則非公開だが、問題が発生した場合は要望に応じて提供。

（注記）ユーザーが必要とするアプリケーション・ログ情報が常に記録・保管されており、ユーザーが必要とする時にユーザーの希望する方法で提供できるようにする。

（３－８）

- データ保証の要件

バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法

（例文）日次で差分バックアップと、週次でフルバックアップを実施。暗号化されたデータはテープに保管され、データセンターから離れた場所に保管。

（注記）サービスの安定的供給にはデータのバックアップやアクセス権の管理などデータの正確さや安全性を保証する要件を規定する。

（３－９）

● バックアップデータの保存期間

データをバックアップした媒体を保管する期限

（例文）5 年以上（基幹業務）、3 ヶ月以上（基幹業務以外）

（注記）対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討、万一データが破壊されるケースを想定して保存期間を規定する。

（３－１０）

● データ消去の要件

サービス解約後の、データ消去の実施有無、保管媒体の破棄の有無、データ移行など、利用者に所有権のあるデータの消去方法

（例文）サービス解約後 1 ヶ月以内にデータ及び保管媒体を破棄。

（注記）データ機密保持の観点から、サービス解約後、重要なデータ及び媒体は間違いなく破棄されることを規定する。

4）サポート

（４－１）

● サービス提供時間帯（障害対応）

障害対応時の問合せ受付業務を実施する時間帯

（例文）月曜日から金曜日の 10-17 時（年末年始・土日・祝祭日を除く）、夜間休日はメールで障害受付を行い、合理的な速度で障害対応を実施。

（注記）サービス提供時間帯だけでなく、障害対応時の応答性能も項目として規定しておく。

（４－２）

● サービス提供時間帯（一般問合せ）

一般問合せ時の問合せ受付業務を実施する時間帯

（例文）月曜日から金曜日の 10-17 時（年末年始・土日・祝祭日を除く）、メールは 24 時間 365 日受付

（注記）サービス提供時間帯だけでなく、問合せ時（ヘルプデスク）の性能も項目として規定しておく。

5）性能基準

（５－１）

- オンライン応答時間

オンライン処理の応答時間

（例文）データセンタ内の平均応答時間　3 秒以内

（注記）アプリケーションのある機能に対するオンライン処理要求を出してから回答を得るまでに要する時間を規定する。ただし、ネットワーク、サーバー、ストレージ、アプリケーションなどシステム構成要素のそれぞれの処理性能に依存する。

（５－２）

- バッチ処理時間

バッチ処理（一括処理）の応答時間

（例文）4 時間以下

（注記）アプリケーションのある機能に対するバッチ処理要求を出してから回答を得るまでに要する時間を規定する。ただし、ネットワーク、サーバー、ストレージ、アプリケーションなどシステム構成要素のそれぞれの処理性能に依存する。

（５－３）

- カスタマイズ性

可能であれば、カスタマイズが可能な事項、分量、仕様等の条件について規定規定し、カスタマイズに必要な情報を開示していること。

（５－４）

- 外部接続性

可能であれば、外部システム接続仕様（API、開発言語など）が公開されていること。

（５－５）

- 同時接続ユーザー数

可能であれば、オンラインユーザーが同時に接続してサービスを利用することができるユーザー数を運用ルールに規定規定していること

6）セキュリティ

（６－１）

● 公的認証取得の要件

JIPDEC 等で制度運営している情報処理管理に関する公的認証が取得されていること。

（例文）SAS70 タイプ 2 対応（SOX 法セキュリティ基準への準拠を監査法人が証明）、Safe Harbor 認証取得（米国のセキュリティ、個人情報保護基準）、ISMS 認証取得

（注記）IT サービスマネジメントのベストプラクティスである ITIL や JIS Q 20000 等の取得状況も確認することが望ましい。

サービス提供に関してセキュリティの確保を保証する指標として、公的認証の取得を規定する。

（６－２）

● アプリケーションに関する第三者評価

不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること。

（例文）年１回、外部の第三者機関による不正侵入テストを実施しており、速やかに指摘事項に対して対策を講じる。

（注記）サービス提供に関して扱う企業情報のセキュリティ確保を保証するため、最低年１回の第三者による客観的なセキュリティチェックを行うことを規定する。

（６－３）

● 情報取扱者の制限

ユーザーのデータにアクセスできる利用者が限定されていること。

（例文）ユーザーのデータにアクセスできる社員等はシステム管理者に限定。全てのアクセスはログに記録。

（注記）委託した情報へのアクセス権はその必要性、重要性に応じて適切なセキュリティ管理者のもとで管理されていることを規定する。

（６－４）

● 情報取扱い環境

ベンダ側でのデータ取扱環境が適切に確保されていること。

（例文）オフィスはＩＣカードによる運用で執務室に入室可能な社員等を最小限に制限し

ており、ＰＣはすべてシンクライアントである。

（注記）ビルやフロアのセキュリティを維持するための設備や管理が十分な機密性、完全性、信頼性を保持しいてることを保証する要件を規定する。

（６－５）

- 通信の暗号化レベル

システムとやりとりされる通信の暗号化強度。

（例文）データ通信は TLS、バルク通信は Secure FTP にて対応。VPN は IPSec に基づく。

（注記）通信のセキュリティ確保を保証するために通信内容を暗号化することを規定する。