データセンター利用ガイド

第１版

２０１０／１０／１

特定非営利活動法人
ASP・SaaS インダストリ・コンソーシアム

はじめに

クラウドＡＳＰ・ＳａａＳは、企業の生産性向上に資する極めて有効なツールとして昨今その普及が進んでおり、安全・信頼性の高いサービスを提供するために、高機能・高セキュリティを備えたデータセンターを利用する傾向が増加しています。

このような状況を踏まえ、総務省と ASPIC が合同で設立した「ASP・SaaS 普及促進協議会」において、安全・信頼性等の点からデータセンターの評価・選択を支援するべく検討を進め、平成 21 年 2 月 26 日にデータセンターの建物・設備・セキュリティ等に関し情報開示が求められる項目を示した「データセンターの安全・信頼性に係る情報開示指針(第１版)」を総務省から発表しました。

この指針は、データセンターの安全・信頼性に係る情報開示を必須の項目と選択の項目に分け、情報開示項目を共通かつ豊富にするとともに、データセンター利用者によるデータセンターの比較、評価、選択等を容易にすることを目的としています。

本ガイドは、データセンターを利用する際の参考書として、データセンターの情報開示項目について分かり易く解説しています。

ASP・SaaS が安全で信頼性の高いサービスが提供されるため、データセンターの情報開示がさらに進み、データセンターの利用が一層進むことを期待しております。

また、本指針等の具体化を始め、世界で最も優れたブロードバンドインフラを有する我が国がアジアや世界の情報発信拠点として発展するための取組を行うことを目的として、ASPIC の内部に「ASP・SaaS　データセンター促進協議会」が設立されております。

本書作成にあたり、以下の各社から執筆等のご協力をいただいております。ここに心から感謝の意を表します。株式会社ＮＴＴデータ、ＫＤＤＩ株式会社、日本電気株式会社、日本ユニシス株式会社、株式会社ブロードバンドタワー、三菱電機情報ネットワーク株式会社。

本協議会においては、情報発信拠点としてのデータセンターの発展、またその利用の拡大を図るため情報開示に係る用語の統一や情報開示の認定制度の導入、クラウドコンピューティングの出現等ネットワーク環境の変化を踏まえた新たな国際戦略等について、検討を行ってきており、この検討結果についても別途情報共有をしていきたいと思っております。

特定非営利活動法人
ASP・SaaS インダストリ・コンソーシアム
会長　河合　輝欣

目　次

参考：データセンターの安全・信頼性に係る情報開示指針（第 1 版）（総務省：平成 21 年 2 月 26 日）

第１章　データセンターの位置づけ

１．１　データセンターとは（定義）

データセンターは、運用するＩＣＴ機器（ネットワーク装置、サーバ装置、ストレージ装置等）を格納する専用の空間・設備（空調、電源変換装置等を含む）をいう。

１．２　データセンター設立の背景及び最近の状況

計算機センターや通信等の必要な機能を収容した建物（物理的な拠点）として進化したものがデータセンターである。データセンターは、物理的な拠点として存在し、そこでサービスが提供されている。近年普及し始めている ASP、SaaS、クラウドコンピューティングに代表されるネットワークサービスの拠点となっているのが、データセンターであり、ネットワークサービスの拡大とともにデータセンタービジネスの規模が拡大している。

データセンターは当初、サーバやストレージを一か所に集中して大量に配備・管理することによる運用コスト削減や、一般オフィスビルでは実現不可能な高い可用性を実現するための対策（電源、空調、セキュリティ等）とネットワークコネクティビティ確保などの効果が評価されて普及した。これらの効果に加えて最近では、各社のサーバがデータセンターに集中した結果、取引に伴う各種データ交換や決済など、企業間の情報交換をデータセンター内で完結することが可能となり、データセンター上で企業間のアライアンスが実現されるようになってきている。

ネットワークサービスの普及に伴い、企業間取引のデータ交換の割合も増大し、この極めて高いセキュリティ、パフォーマンスが要求されるサービスは、必然的に同一データセンター内だけでなく異なるデータセンター間を高速な通信回線で結ぶことが必要となってくるため、データセンターが IX の近くに設置されることが多くなっている。

更には、取り扱う情報量の増大によるデジタルデータの爆発的増加に伴い、データセンター上のストレージを独立のネットワークで相互接続する、ストレージネットワークが形成されるようになってきた。

このように社会基盤としてデータセンターの規模が大きくなり、サービス内容が深くなるにつれて、事業的にも技術的にも、データセンター事業者が単独で全サービスを提供することは困難になり、様々なリスクへの回避・対応に向けてデータセンター事業者間での水平分業が進み、急速に進展する技術に対応するために専門的なサービスに特化した専門事業者と垂直分業が組まれつつある。

データセンター事業者は、同業者や専門事業者と組んで統合されたサービスを提供することになる。この際、単純な相互接続だけでなく、SLA に至るまでの幅広い相互運用性を、同業者との間(水平)および専門事業者との間(垂直)に実現するようになってきている。

１．３　サービスの枠組

一口にデータセンターと云っても事業者によってその規模・業態は多種多様である。とは云え、そのサービス内容を分析すると、共通項、最大公約数が見えてくる。分け方は微妙に異なるが、代表的なサービスメニューは、ハウジングサービスとホスティングサービスである。（下図参照）

・ハウジングサービスは、電源をはじめとしたファシリティと LAN や WAN などのネットワークと接続するコネクティビティを提供

・ホスティングサービスは、ハウジングサービスに加えてサーバなどを提供

・その他、運用や監視をするマネジメントサービスやコンサルティングなどのプロフェッショナルサービスを付加することが多い。

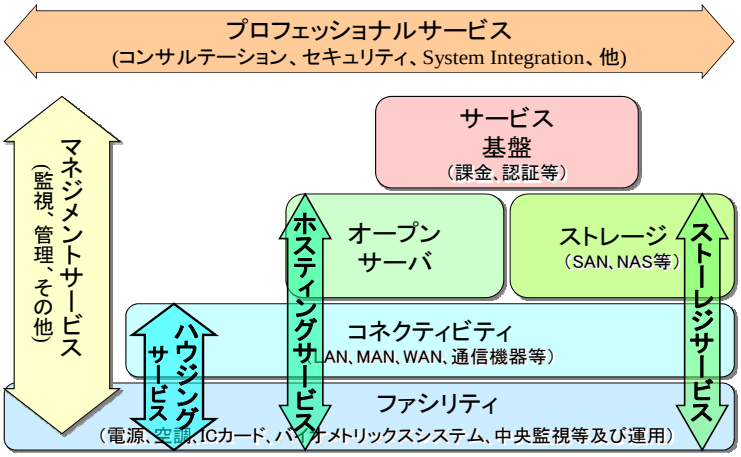


図　データセンターのサービス構造

前記サービスを実現・提供する仕組みの構成要素も大枠は似通っている。即ち、全サービスの基盤となる、堅牢な建屋や電源、空調などのファシリティ、高速大容量の回線と通信機器によるネットワーク、ラックマウント型が主流のサーバ、大規模高信頼なストレージ、機器・設備を監視・管理するための運用管理システム、課金や顧客情報管理などサービス基盤、それに設備・機器の運用、コンサルテーション、SI(System Integration)など人間系が加わる。

データセンターの構成要素について、以下の各章で説明する。

・第２章　ハウジング（建物・設備）

・第３章　ハウジング（ネットワーク）

・第４章　ハウジング（サービス内容）

・第５章　ハウジング（サービスサポート）

・第６章　ホスティング

「参考：iDC イニシアティブデータセンターガイドライン」

第２章　ハウジング（建物・設備）

ハウジング（建物・設備）とは、データセンターに自社のサーバーやストレージ装置等を持ち込んで、データセンター事業者からサーバー装置等を設置する場所と電力等を提供してもらいサービスを提供するデータセンターの形態の一つで「コロケーション」とも呼ばれている。

２．１　建物

データセンターは対災害性に優れたビルに高速な通信回線を引き込んだ施設で、高度な電源設備や空調設備を備え、ID カードによる入退室管理や監視カメラによる 24 時間監視などでセキュリティを確保している。

日本は地震が多いので、国内のデータセンターの利用者は、耐震性を重視する傾向にある。耐震性は建築基準で規定されているが、震度７程度級の耐震性を備えたデータセンターが多い。建物の形状としてデータセンター専用か、他の用途と共用の建物か。複数テナントか、単一テナントなのか。また、立地条件として地盤の安定性、土壌汚染、周辺の環境等を考慮する。

２．１．１　耐震・免震構造

（１）耐震構造

建物の構造（柱や梁）自体が地震に耐えるような強度に造られているもの。地震で生じる揺れに耐えるように設計された構造のことである。 地震エネルギーがそのまま伝わった場合でも、許容範囲内の揺れに耐えることができる。

（２）制震構造

建物が揺れ始めたとき振動を吸収し、建物を許容範囲内の振動以下に制御する構造である。制御方法としてアクティブコントロール(建物内に設けた振動センサで揺れを検出すると、逆方向に強制的にエネルギーを与え揺れを制御する）と、パッシブコントロール（装置自身が揺れを感ずると揺れを軽減するように制御を行う）などがある。

（３）免震構造

構造物と地盤との間に積層ゴムなどの特殊な装置を付け免震層を造ることで、地震力を建物に直接伝えないようにした構造のこと。 地震に強いだけでなく、揺れそのものを軽減することによって、マシン室内にあるコンピュータシステム等の被害を防ぐことができる。

データセンターの免震構造には、以下の３つの方式が使われている。

（３－１）免震建物

建物自身を免震構造とするもの。建物の基礎部分や中間階の柱に取り付けた免震装置によって建物に地震のエネルギーが伝わりにくくする方法。免震化された部分は、ゆっくりと（相対的に）大きく揺れる様になり、地震による激しい揺れの影響を免れることができる。

（３－２）免震床

建物に免震装置を設置するのでなく、マシン室のフロア部分で免震構造とするもの。従

来の二重床（フリーアクセスフロア）を免震装置で支持して、建物床と縁を切ることにより地震力を伝えない床工法である。地震時に建物床に発生する加速度を、（１／５～１／１０に）低減し、コンピュータシステム等を転倒や誤動作から守る装置である。

（３－３）ラック免震

建物、フロアを免震化するのでなく、コンピュータシステムを搭載するラックに免震装置を付加するもの。ラック免震装置は上部の免震台が、ベース部分と独立して水平方向に自由にスライドする。その為、地震の水平方向力がベースに加わっても、ラックに伝わる加速度を低減する装置である。このような 2 次元免震ラック以外に 3 次元免震ラックもサービスされるようになっている。

２．１．２　耐火構造

（１）耐火構造

耐火構造とは、火災に対し単に燃えないだけでなく、隣家からの火災の延焼を防止し、火熱のための変形や倒壊をしないような構造であることが求められている。建築物の主要構造部（壁・柱・床・はり・屋根・階段）に適用される。部位と建物階数により 30 分、1 時間、2 時間、3 時間耐火構造が定められている。

（２）準耐火構造

準耐火構造とは、通常の火災による延焼を抑制するような構造であることが求められている。耐火構造と準耐火構造の違いは、耐火構造が鎮火後の再使用が可能となることを目標として規定されていることに対し、準耐火構造は火災中の延焼を防止することに主眼があり、鎮火後の再使用は想定していないことである。

２．１．３　防水構造

データセンターは、浸水のおそれの少ない地域に設けるとともに、建物の屋根及び外壁は、防水性能を保持し、排水性能も有することが必要である。以下に示す対策が採られていることが望ましい。以下に対策方法の一例を紹介する。

・屋根、外壁及び窓等は、防水施工を行う。
・屋根、外壁等を貫通する吸排気口、ダクト、配管等の周りには防水施工を行う。
・建物の設置位置により以下の対策で補完する。
・敷地境界防水堤を設置する。
・建物開口部に防水扉を設ける。
・室を防水区画とする。
・室の入口に排水口を設ける。
・漏水検知器を設置する。

２．１．４　床荷重

床荷重はスラブ（床版）の積載能力を指す。積載可能な荷重を算出する場合、建物の主要構造部である柱、梁、壁の強度も含めて検討しなければならない。また、地震時の揺れを考慮に入れることも必要で、総合的な見地から設置可能な荷重を算出する必要がある。通常５００kg/㎡～７００kg/㎡もあれば十分と考えられるが、最近のブレードサーバ等の高密度機器を導入する場合は１，０００kg/㎡を必要となる場合もある。実際のサーバの実装設計時には、ラック搭載重量に見合う荷重を考慮する必要がある

２．２　電源設備

データセンターが供給を受けている商用電源は、各種要因による瞬間的な電圧降下や停電などが発生する。このため、データセンターでは、受電方式の高度化や無停電電源装置、非常用電源などの装置、電源設備の二重化などによって、電源の信頼性を確保する必要がある。データセンターの受電系統としては、電力会社からの受電方式を本線・予備線の２回線受電方式やスポットネットワークなどがある。幹線系統の二重化は、高圧系統を一括で二重化する方法、低圧系統を個別に自動切替を行うなど各種方式がある。

２．２．１　無停電電源

サーバは極短時間の停電も許されないが、商用電源の停電は予告なしに起こるので、停電対策が必要である。この対策として、一般的に無停電電源（ＵＰＳ）が用いられる。これは、商用電源を整流器により直流に変換し、蓄電池に電気を蓄えた後、インバータを用いて商用電源と同じ電圧、周波数の交流を発生させてコンピュータシステムに供給する機器である。平常時においては蓄電池を用いて停電に備える。蓄電池の容量は、非常用発電機からの電力供給が安定するまでの間、電力を供給し続けられる大きさを持つ。停電時には、非常用発電機と組み合わせることで、蓄電池による電力供給時間を越えて、電力を供給することができる。ＵＰＳの信頼性を高める方法として、並列冗長（Ｎ＋１）方式と共通予備方式がある。

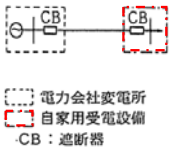
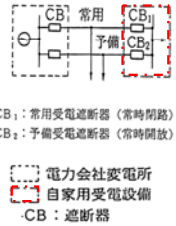
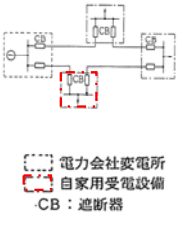
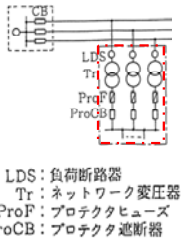
２．２．２　給電ルート

電力会社等の変電設備からデータセンターへ電力を供給する経路のこと。経路を二重化したり、異なる変電所や異なる経路から給電することによって、より安全性を高める方式である。

２．２．３　受電方式

受電方式は、信頼性、経済性、保守性、電力会社の供給事情等を考慮して決められている。受電方式を下表に示す。供給の信頼性と保守の省力化に優れているスポットネットワーク方式は、大都市の負荷過密地域で採用されている受電方式である。

表　受電方式

	1回線受電	本予備線切換方式	ループ方式	スポットネットワーク方式
概念図				
信頼性	×	○	○	◎
コスト	◎	○	△	×

２．２．４　電力設備監視

データセンターの安定稼働を図る上で重要な事の一つに電力設備の監視がある。対象機器毎に詳細な計測情報を遠隔から常時監視し、トラブル発生時には即座に故障対応を手配する。

２．２．５　非常用電源

非常用電源は、商用電源の供給が停止した場合、コンピュータシステム、空調設備などに確実に電源供給するために、発電設備とＵＰＳ（無停電電源設備）などを組合せデータセンターの無停電化を行う設備である。停電時に発電し、コンピュータシステム、空調設備などへ電気を供給する。データセンターで用いられる発電機には、ディーゼルとガスタービンなどがある。

（１）ディーゼル発電機

ディーゼル発電機は、熱効率が優れており構造が簡単で使いやすく、設備費や保守点検整備費が廉価であることから、産業用として広く使用されている。自家発電設備の原動機としても小容量から大容量まで最も多く採用されている。 ディーゼル発電機の排気ガスには、通常、黒煙や粒子状物質、Nox、Sox が多く含まれれるが、近年の技術革新にともない、触媒やフィルターなどを用いた環境に配意した発電機が実用化されている。

（２）ガスタービン発電機

ガスタービン発電機は非常用発電機の市場、特に 500kVA 以上の分野で大きなシェアを占めている。ディーゼル発電機に比べて燃費は悪いが、騒音が少ないので都市部にも設置が容易である。また軽量コンパクトで高出力であり振動が少ないこと、冷却水が不要もしくは少量ですむこと、負荷が瞬時に投入された場合でも回転速度（周波数）低下が少ないこと、液体燃料と気体燃料の切換が容易であることなどの利点がある。ただしディーゼル発電機に比べ高価な設備となる。

２．３　消火設備

火災等の異常を早期に発見する火災報知システムと、火災被害の拡大を最小限に防止する消火設備で構成される。

２．３．１　サーバルーム内消火設備

従来、コンピュータ室の消火設備としてはハロゲン化物消火設備が多く用いられてきた。オゾン層保護を目的としたハロンの生産全廃以降、ハロン代替ガスとしていくつかの新しいガス消火薬剤が開発された。マシン室及び媒体保管室は要員の安全確保、消火後の汚損問題、環境配慮（オゾン層保護）の観点からハロゲン化物を使用しない消火設備の使用が望ましい。一般的には、人体に影響のない窒素（N2）系のガスを用いた消火設備が増えている。

２．３．２　火災感知・報知システム

（１）自動火災報知システム

感知器を用いて火災により発生する熱や煙を自動的に検知し防災システムへ通知するとともに、音響装置（ベル）を鳴動させて建物内に報知することにより、避難と初期消火活動を促すシステムである。

（２）超高感度煙検知システム

消防法で定めるスポット型煙感知器の１０００倍程度の検知レンジを備えた検知システムである。このシステムにより循環気流によって濃度が薄められた煙を初期感知することができる。局部的な火災に対しても極めて迅速に初期消火を可能とし、コンピュータシステムへのダメージを最小化することができる。

２．４　避雷対策設備

避雷の種別として直撃雷と誘導雷がある。建築基準法では、高さ２０ｍを超える部分について避雷設備の設置が必要とされる。

直撃雷対策は、建屋と屋上設備そのものも雷害から保護する。

誘導雷対策は、人体及びコンピュータシステムを雷サージ（送配電線路に侵入した雷による異常電圧）から保護する。

２．４．１　直撃雷対策

直撃雷とは、電線路や建造物、アンテナ、機器などへ直接落雷することで電子・電気機器どころか家屋の破壊や人命にも危険をおよぼすものである。万が一直撃雷を受けた場合の被害を避けることは困難であるため、避雷設備が必要となる。

２．４．２　誘導雷対策

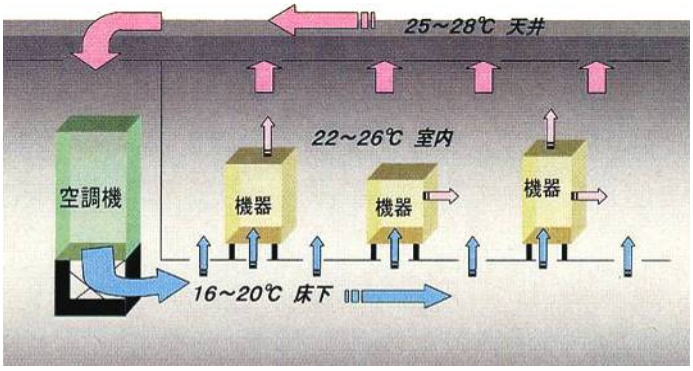
誘導雷とは、 電線路や建造物、アンテナ、機器などの付近に落雷したときに、雷の放電路を流れる電流によって電磁界の急変で生じる過電流・過電圧のことである。一般的に雷によって電気・電子機器が被害を被る大半は誘導雷によるものである。対策として、電源線や受電設備、分電盤に保護装置を実装するなどして対応している。また、雷の侵入経路は入力電源線や屋外に出るLANケーブル、通信線などであるため、LANケーブルには光ケーブル採用する他、通信線へはターミナルプロテクタなどを実装する。

２．５　空調設備

コンピュータシステムの長期的な安定稼動を実現するために、空調設備による温度・湿度管理は、重要な管理要素の一つである。コンピュータ室用の空調設備は、一般ビル用の空調設備と比べて、高いシステム信頼性、厳しい制御条件、２４時間連続運転など高度な仕様が求められる。空調の冷却方法は水冷と空冷方式と二つに分けられる。なお、一般的には水冷方式が冷却効率が高い。データセンターで採用されている主な空調方式としては床下空調、直吹空調、天井吹空調がある。その他、最近では高発熱ＩＴ機器を効率的に冷却するための局所空調方式も導入され始めている。

２．５．１　空調方式　（代表的なものを示す）

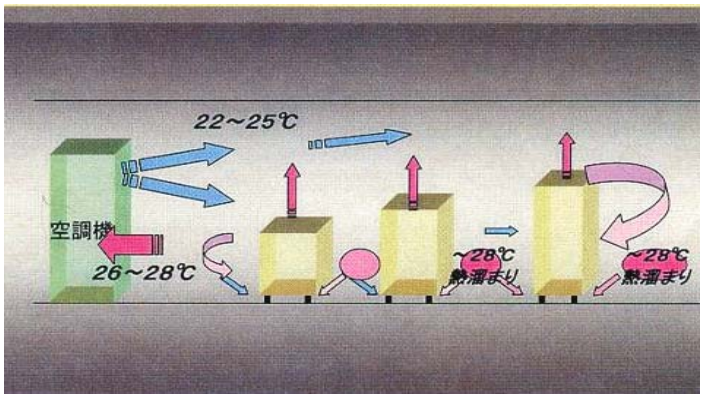
（１）床下空調方式



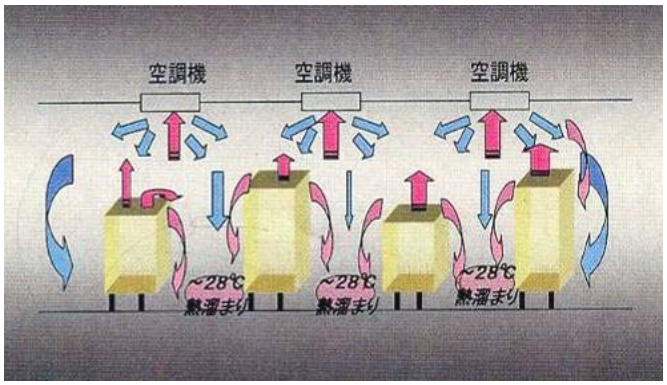
室内温湿度が均等になりやすく機器配置が自由で移設、増設も容易な方式である。機器に対し安定した温湿度条件を得ることが出来る。多くのデータセンターで採用されている方式である。最近では冷気と暖気の混同を避け、空調効率をよりよくするための方式の取り組みもある。

（２）直吹空調方式

空気の流れを考慮しながら機器配置設計が必要な方式である。ただし、ラック間に熱溜まりが出来易く機器への適正な温湿度供給の配慮が必要。



（３）天井吹空調方式



室内全体の温湿度分布はある程度安定する方式である。ただし冷気と暖気が混合され、熱溜まりが出来易く機器への適正な温湿度供給の配慮が必要。

２．５．２　空調設備の容量

空気調和設備の容量は、１００％稼働時の情報システムの負荷熱量、その他設備機器、照明、部屋の容積、外気負荷、入室人員、季節要因等を考慮し、その最大負荷熱量で算定する。また、不測の故障時を考慮してＮ＋１の冗長性を持たせた構成にしたものもあり、より信頼性を高めている。

２．６　ラック／スペース

ネットワーク機器やサーバなどを効率よく収容するために設計された棚のことをラックと言う。電源や空調などを装備するものもある。横幅のサイズは通常 19 インチ（48.26cm）である。なお、ラックマウント機器のサイズ（高さ）は「U」（unit）を単位に表す。「1U」は、EIA 規格では 1.75 インチ（約 4.45cm）である。

２．６．１　荷重

ＩＴ機器をラックに搭載する際、データセンターの床荷重（２．１．４参照）に応じた積載可能荷重の検討が必要となる。サーバ等を空間的にはラックに収容できても、荷重により実装数の制限を受けることがある。

２．６．２　電力

データセンターでは、その供給電力容量により、１ラック当りの利用可能電力を設定されているのが普通である。従来は１ラックあたり 2～3kVA が平均的な電力量であった。しかし、ブレードサーバなどの大容量電源を必要とするＩＴ機器を設置する場合、１ラックあたり 10kVA を越える場合があるので、利用可能電力の確認が必要である。

２．６．３　監視機能

ラック単位で消費電力や温度監視などを行う機能のこと。ラック毎にセンサーを設置し、これらのセンサーを用いて情報を収集・分析する専用の監視システムを持つ。これらの機能はオプションサービスとしているデータセンターがほとんどである。

２．７　セキュリティ

データセンターに預けられたデータを顧客から預かったデータを情報漏えいや盗難等のリスクから守るために、データセンターにおけるセキュリティ対策は重要となる。本章では、データセンターにおいて、確認すべきセキュリティ対策について述べる。

２．７．１　24 時間 365 日監視体制

［有人監視又はそれに代わる体制・システムとなっているか否かの明示］

データセンターで稼働しているシステムやサービスを中断させないために、データセンター内にある監視センターから 24 時間 365 日の監視体制を整えていることが多い。通常、有人監視で行っている事業者が多いが、経験豊富で高いスキルを持った技術者の確保の難しさやコスト削減といった理由で、ネットワークやサーバーの状態監視、メンテナンス等を遠隔監視で行っている事業者もある。

２．７．２　外部委託先　［運用外部委託先（派遣、請負等）の有無］

ASP・SaaS では、データセンターに預けられたデータはデータセンターにいる運用担当者によって管理されていることが一般的である。そのため、預けられたデータが漏えいや盗難等ないように、データセンター事業者の運用は、系列の子会社や運用の専門会社に外部委託されていることが多い。

２．７．３　入退館管理等

[セキュリティレベルに応じた区画（フロア単位、ラック単位、ラック分割単位等）の分離と、各区画における入退室管理や施錠等のセキュリティ対策の有無。]

[入退室記録の有無と、有りの場合はその保存期間]

[監視カメラの有無と、有りの場合は監視カメラ稼働時間、映像の保存期間、改ざん防止機能の有無]

[個人認証システムの有無。認証システムがある場合はその認証方式を記述]

[持込持出物品の制限又は対策（持ち物検査等）の有無]

[入館、作業時等のデータセンター側のアテンドの有無]

入退室管理は､データセンターに外部から不審な人物を入り込ませないために講じるセキュリティ対策で、もっとも重要な点である。

入退室管理の基本的な考え方は、セキュリティレベルに応じた区画（ゾーニング）の設定、各区画（ゾーニング）への入退管理、その入退の記録・監査の３つである。

（１）セキュリティレベルに応じた区画（ゾーニング）の設定

ゾーニングの設定とは、その区画にアクセスできる権限を設定し、その境界を定義することである。一般的なデータセンターでは、敷地外、エントランスホール・通路、エレベータ・フロア、サーバ室、ラック等といったように区画化（ゾーニング）されている。

（２）各区画（ゾーニング）への入退管理

前述のセキュリティレベルに応じた各区画の境界には､許可された者以外の入退を制限する必要があり、これを入退管理という。入退管理は、一般的に、有人による監視、物理的な施錠、IC カード等の入退室管理システムの利用といった方法で管理されている。

（３）入退の記録・監査

入退管理の記録・監査は、「だれが」、「いつ」、「どこに」に入退したのかを記録し、不審な人物が侵入していないかを監査するために行う必要がある。不審な人物の侵入は、いつ、どこで発生するかわからないため、常に記録している必要があり、不審な人物の侵入の発覚には、定期的な入退室記録の監査を行う必要がある。

また、監視カメラも、不正な侵入や不正な行為の監視・記録を目的に設置されており、特に、セキュリティの観点では、監視カメラは不正な侵入や不正な行為が発覚した場合の証拠確保を目的として設置する。

そのため、監視カメラは、通常 24 時間 365 日で稼働しているのがほとんどであり、映像も証拠提出のために一定期間保存されることが一般的であり､どの程度保存されているかどうかを確認する必要がある。また、監視カメラは、死角がないように配置されることが必要であり、入退室時に顔が映るように入口・出口の両方に配置することや、サーバ室では、不正な侵入や不正な行為を監視できるように最適に配置する。

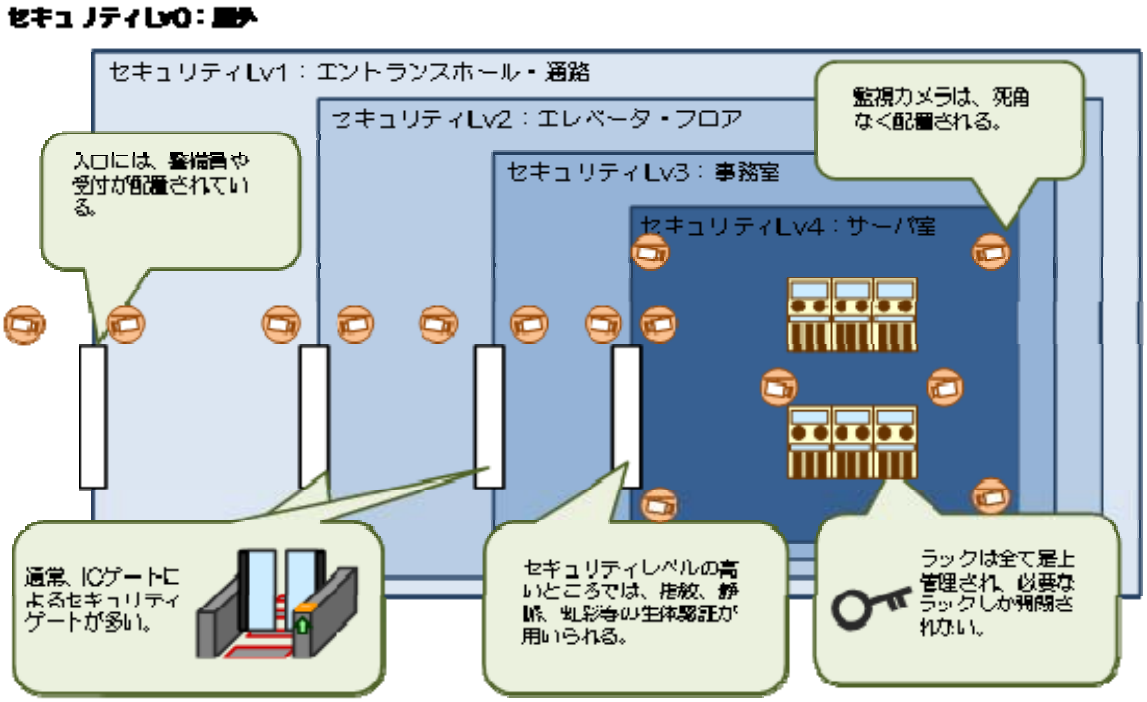


図　データセンターにおける入退室管理等におけるセキュリティ

特に、セキュリティを重んじる場合、以下の点を考慮するとよい。

（ア）共連れ防止策

共連れは、権限のない人が権限のある人とともに不正に侵入することを指し、機密レベルの高い場所への共連れによる不正な侵入がないように防止する必要がある。共連れ防止策として、警備員の配置やアテンドをつけることがもっとも効果的である。また、入退室に一人ずつしか入れないゲートを通ることで共連れを防止しているところもある。人の出入りを管理して入室履歴のない場合に退室できなくするアンチパスバック方式を採用している場合、共連れによる不正な入室を検知することができる。

（イ）生体認証システム

機密レベルの高い場所への入退室管理は生体認証システムの導入が主流となっている。生体認証システムで用いられる認証は、指紋、静脈、虹彩などの生体情報を用いる方法が主流となっている。

（ウ）持ち物検査

データセンター内に不審物を持ち込まないように、警備員による目視やX線検査機による持ち物検査を行っている。一般的なデータセンターでは、事前に申請のない荷物の持ち込みは制限され、手荷物全てがロッカーに預けられるところが多い。持ち込み物品の中には、爆発物、盗撮用カメラ、刃物や銃器等といった物品が制限されているところが多い。また、データセンターの外へ情報の漏えいや盗難等がないように、データセンターから持ち出さ

れる物品に対しても不必要な持ち出しがないかどうかを確認するところが多い。

なお、検査実施は、通常のエントランスによる出入り時の持ち物検査だけでなく、荷物搬入時の搬入業者の荷物等にも検査を実施しているかどうかを確認する。

(エ) アテンドの有無

データセンター内での作業には、基本的にはデータセンター事業者の担当者がアテンドすることが多い。アテンドが付くことで、他の事業者のフロアやラック等、不必要な場所への侵入や操作を抑止することができるため、セキュリティを重視する場合は重要な点である。しかしフレキシブルな出入りは制限されるため、システムの運用形態によっては不便になることがある。

２．７．４　媒体の保管

［磁気テープ、光メディア等の媒体の保管のための鍵付きキャビネットや保管室の有無］

磁気テープ、光メディア等の媒体を保管のために、鍵付きキャビネットや保管室が具備されているかセキュリティの上で重要な点である。キャビネットもしくは保管室が具備されていた場合、その利用が専用なのか共有なのか確認する。

共有の場合、キャビネットや保管室の開閉は、データセンター事業者の担当者によって行われ、さらに、物品の取り出しや預け入れもデータセンター事業者の担当者によって行われることが多い。

２．７．５　その他セキュリティ対策

特に、セキュリティを重んじる場合、運用端末やホスティング等を利用する機器を廃棄した時に、ハードディスクの消去が不完全であったために起こりうる情報漏えいを防ぐために、機器の廃棄手順、方法等が整備されているかどうか等を確認する。また、ホスティングサービス契約終了時においても、サービス停止だけでなく、アカウントやデータそのものの削除等が確実に行われているかどうかを確認する。

施設内の書類等のリサイクルがされている場合、セキュリティの観点で、機密資料の類はシュレッダーによる細断、溶解処理等の廃棄手順に従って廃棄され、情報漏えいが起こらないようなリサイクルが行われているかどうかを確認する。

２．８　環境対応

２．８．１　電力消費の効率化

近年、顧客からの環境志向の高まりを受け、データセンターの電力消費の効率化の目標を提示している事業社もある。電力消費の効率化の指標の一つとして PUE（Power Usage Effectiveness：電力使用効率）がある。 PUE は、データセンター全体の消費電力を IT 機器による消費電力で割った値であり、データセンター全体の消費電力は、サーバやストレージ、ネットワーク等の IT 機器のほかに、空調装置、照明装置、監視装置などの電力も含む。

PUE ＝ データセンター全体の消費電力 ／ IT 機器による消費電力

PUE が 1.0 とは、データセンター全体で消費した電力と IT 機器による消費電力が等しくなる（空調装置、照明装置、監視装置などの電力消費が「ゼロ」）こと。PUE の値については決定するパラメータが非常に多く、すべての条件を合わせることが難しいため、比較しにくい状況にある。

データセンターにおける電力消費の現状（株式会社インプレスビジネスメディアによれば）は、実績値として、北米での平均的なデータセンターの PUE 値は 3.0 程度だといわれている。これは、IT 機器のエネルギー消費がデータセンター全体の電力消費量の 3 分の 1 を占めているということを意味する。別の言い方をすると、データセンター内では、IT 機器が消費する電力量の 2 倍に相当する電力を設備側で消費している、ということになる。北米では、これを 2011 年をめどに 1.7 程度に向上させることを目標としている状況だ。

出典：「データセンター完全ガイド 2008 年春号」

（http://www.impressrd.jp/idc/2008spring/sp1/part1souron.html）

電力消費の効率化では、高電圧直流電源システムを採用している事業者もある。高電圧直流電源システムは、変電所から受電し、無停電電源装置や IT 機器内で行っていた交流 - 直流変換を減らし、変換の際に発生するエネルギー損失を削減する仕組みである。

２．８．２　その他の環境対応策

その他の環境対応策では、代表的なものとして紙ごみリサイクル化、自然エネルギーの活用、排熱対策、ラック間・ラック内の熱だまり対策等がある。

紙ごみリサイクル化では、施設内の書類等のリサイクルがされているかどうかを確認する。ただし、セキュリティの観点で、機密資料の類はシュレッダーによる細断、溶解処理等の廃棄手順に従って廃棄され、リサイクルされているかどうかを確認する。

自然エネルギーの活用では、太陽光発電システムによる発電や冷却システムに外気を直接利用する方式の採用、等がある。

排熱対策、ラック間・ラック内の熱だまり対策では、空調解析による最適な高効率空調システムを採用しているか、また冷気を閉じ込める方式等で高負荷・高効率なラックを採用しているか、等のところもある。

また、仮想化技術の対応も、IT 機器のリソースをシェアすることで電力消費削減や IT 機器の削減等でリソースを効率的に利用する上で、今後の環境対応策において重要な点と言える。

カーボンオフセット

発展途上国など、ほかの場所で削減した CO2 で打ち消すことをカーボンオフセットという。このオフセットで利用した排出枠は日本国政府の償却口座に移転され、京都議定書における日本の排出削減目標の達成に貢献する。

第３章　ハウジング（ネットワーク）

ハウジング（ネットワーク）とは、ハウジング（建物・設備）[第 2 章で説明]と合わせて提供するネットワークサービス（インターネット接続サービス）等である。収容するシステムの利用形態や目的により、データセンターに接続するネットワークは多岐にわたる。

３．１　回線

３．１．１　バックボーンネットワーク

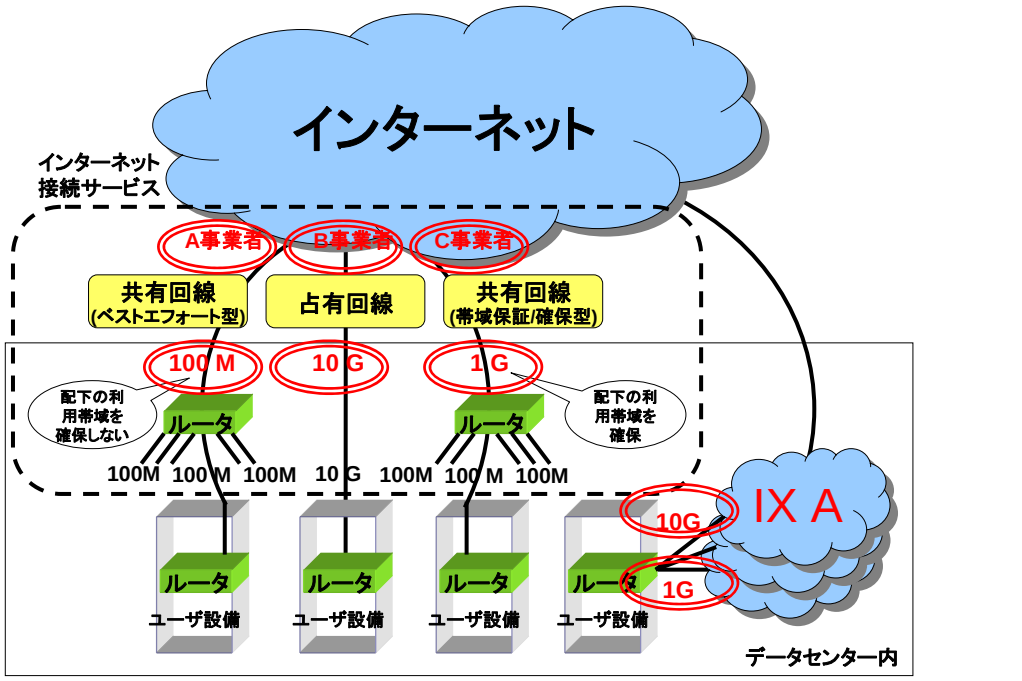
データセンターが接続しているバックボーンネットワークの容量（帯域、帯域幅）

ASP・SaaS 事業者がインターネットを経由したサービスを提供する場合は、インターネットとの接続容量が重要なポイントとなる。

データセンター事業者がインターネット接続サービスを提供しているかを確認し、提供している場合は接続しているバックボーンの帯域や接続先を確認する。

また、データセンター内にて IX(インターネット相互接続点)とダイレクト接続（ピアリング等）が可能な場合もあるので、あわせて確認する。

以下図の赤色部分



３．１．２　接続回線

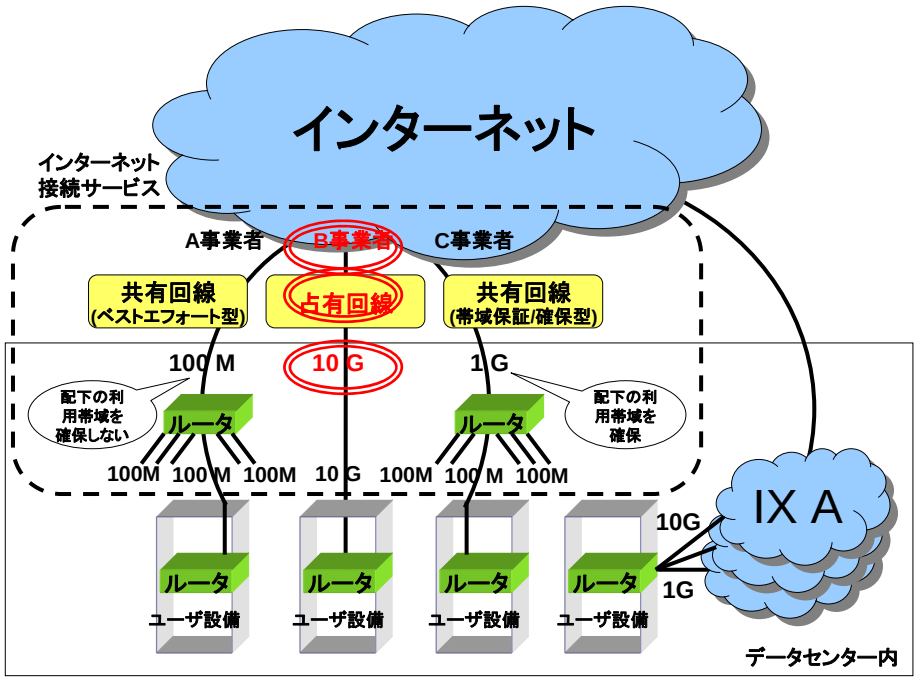
（１）建物への回線の引き込みについて

ASP・SaaS 事業者がインターネットを経由したサービスを提供する場合は、インターネットとの接続について信頼性が求められる。

データセンター事業者がインターネット接続サービスを提供している場合、インターネット回線が 2 つ以上の経路で建物に引き込まれているかを確認する。
データセンター事業者がインターネット接続サービスを提供していない場合は、顧客要望に応じて、インターネット回線を 2 つ以上の経路で建物に引き込むことが可能かを確認する。
また、イントラネット回線等を利用する予定がある場合についても、インターネット回線と同様に、2 つ以上の経路で建物に引き込まれているか、もしくは、2 つ以上の経路で建物に引き込むことが可能かを確認する。

（2）バックボーンネットワークへの占有回線について
バックボーンネットワークへの占有回線の有無と、有りの場合は、占有回線の最高速度を確認する。
ASP・SaaS 事業者がインターネット回線を利用する際には、インターネット回線の品質と価格の両面から、どのサービス・品目を選択するかを検討する必要がある。
データセンター事業者がインターネット接続サービスを提供している場合、占有回線接続サービスを提供しているかを確認する。
データセンター事業者が占有回線接続サービスを提供している場合は、品目や速度を確認する。

以下図の赤色部分

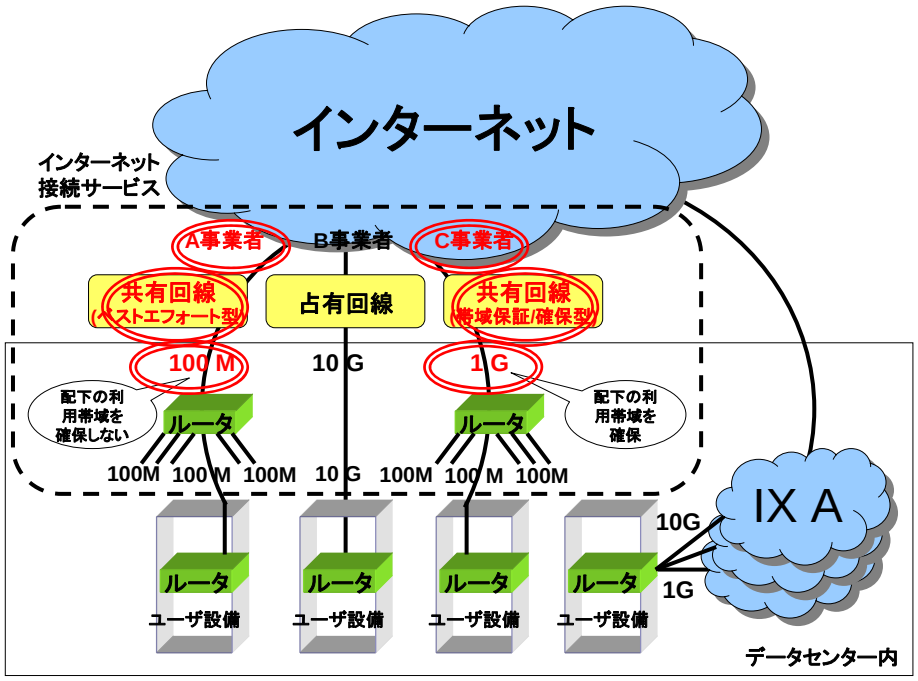


（３）バックボーンネットワークへの共有回線について

データセンター事業者がインターネット接続サービスを提供している場合、共有回線接続サービスを提供しているかを確認する。

データセンター事業者が共有回線接続サービスを提供している場合は、品目(ベストエフォート型、帯域保証/確保型)や速度を確認する。

以下図の赤色部分



（４）提供されるネットワーク回線、その他回線の引き込み、将来拡張について

顧客要望に応じて、インターネット回線を複数のキャリア・ISP 事業者からデータセンター内に引き込むことが可能かを確認する。

ASP・SaaS 事業者等が別回線（メンテナンス用の ISDN 回線等）を自前で引くことの可否と、可の場合でのキャリア制限等の有無を確認する。

顧客要望に応じて、電話回線や専用線等をデータセンター内に引き込むことが可能かを確認する。また、データセンター内に引き込む回線について、キャリア制限があるかについても確認する。

ネットワーク機器(ルーター等)の経路増、IPV6 への対応等の将来拡張能力について、確認する。

データセンター事業者がインターネット接続サービスを提供している場合、将来の経路増やトラフィック増に対してどのような対応(運用・機器増設等)行う予定なのかを確認する。また、データセンター事業者が提供するインターネット接続サービスについて、IPV6 に対応しているか、対応している場合はどのような品目(デュアルスタック、トンネリング、ネイティブ)があるかを確認する。

３．２　サービス

３．２．１　サービス内容

データセンター事業者が提供できるネットワークに関するサービスについて、どのようなサービス・品目があるかを確認する。

（インターネット接続サービス、イントラネット接続サービス、構内配線サービス、データセンター間接続サービス、SLA サービス、設定サービス代行、監視、侵入検知等のセキュリティ対策等）

第４章　ハウジング（サービスの内容）

４．１　サービスの受付、問合せ

４．１．１　受付・申込・問合せ先

（１）サービスの受け付け

窓口は、サービス要件に合わせて複数提供することが可能となる。

（２）サービス開始後の問合わせ

サービス開始後の問合わせの方法によって障害時の対応が異なることがある。データセンター内に 24 時間運用員が常駐している場合はよいが、駆け付け対応の場合がある。

４．２　サービスの変更・終了

４．２．１　サービス（事業）変更・終了時の事前告知

（１）サービス利用者への告知時期

サービス変更・終了時の事前の告知時期が 1 ヵ月、3 ヶ月、6 ヶ月、12 ヶ月等明確な記述が契約書、注文書に記載されているか否か。突然の変更終了により代替措置を講ずる前に契約期間が切れてしまう場合がある。

（２）告知方法

（１）の告知の方法がどのようなものになるかの提示。サービス提供会社により異なる。

４．２．２　サービス（事業）変更・終了後の対応・代替措置

（１）対応・代替措置の基本方針の有無

サービスの変更・終了時の対応、代替措置を基本サービス約款等に明記されているかどうか。

（２）基本方針に沿った具体的なユーザへの対応策（代替サービスの紹介等）の有無

契約するサービスの代替サービスを自社内で展開しているかどうか。または他社のサービスの紹介が可能かどうか。

（３）契約終了後の情報資産の返却責任の有無

情報資産について資産がユーザ側にあるのが基本であるため、契約終了後の対応について、契約段階で返却となるのか、廃棄となるのか明記されているか確認する必要がある。

４．３　サービス料金

４．３．１　料金体系

（１）初期費用額（初期費用とは）

初期費用とは各サービスごとにサービスの開始月に必要となる費用である。費用設定については各サービス提供会社ごとに様々である。

（2）月額利用額

月額利用額はサービス開始月から発生する費用となる。サービスによっては初期費用のみのサービスもある。

（3）最低利用契約期間

サービスの開始から解約までの最短の契約期間の明示。それに伴い解約時の違約金等が設定されている場合がある。

４．３．２　解約時ペナルティ

最低利用契約期間を満たさない場合、またはサービス解約の受付期限を守れず解約となった場合に違約金が発生する場合がある。

４．３．３　利用者からの解約事前受付期限

利用者からのサービス解約の受付に期限が設けてある場合がある。その設定により違約金や解約までのサービス費用に違いが生じる可能性がある。

４．４　サービス品質

４．４．１　サービス可用性

（1）年間障害停止時間、障害停止の事故歴

過去 5 年以内にサービス停止を伴う障害が発生したかどうか。その内容の説明と再発防止策と、現在の改善状況の提示。

（2）定期メンテナンスの実施内容と間隔

ファシリティ設備に関し、メンテナンスの実施内容と期間についての提示。年間、中期スケジュールで計画されているものが多い。

４．４．２　認証取得・監査実施

国際規格等に準じてサービスを提供しているかどうか。主に挙げられる規格は次の通り。

（1）プライバシーマーク

プライバシーマークとは、個人情報保護に関して一定の要件を満たした事業者に対し、財団法人日本情報処理開発協会（JIPDEC）により使用を認められる登録商標(サービスマーク）のこと。P マークと略して呼ばれることもある。

1998 年 4 月より付与が開始された。申請を行い認定されれば、このマークを自社のパンフレットやウェブサイトなど公の場で使用することができ、個人情報の安全な取り扱いを社会に対してアピールできるというメリットがある。また、官公庁や自治体などの入札参加条件にプライバシーマークの認定を条件としているところも多くなっている。

（2）ISMS

ISMS（Information Security Management System）は、情報に関するセキュリティを管理するための仕組み。ISMS の構築のしかたと認定の基準は、国際規格や日本工業規格になっている。

ISMS ではリスクをゼロにすることは求めていない。セキュリティ対策にはコストがかかるので、組織として許容できる範囲のリスクかどうかの判断を経営陣が行ったうえで、限度以上のリスクについて許容範囲までのリスク軽減の対策を講じ、それが実行されているのを管理することが求められる。

（３）ISO14000

ISO 14000 は、国際標準化機構が発行した環境マネジメントシステムに関する国際規格（IS）の総称。ISO 14000 シリーズは、1992 年の地球サミットをきっかけとして規格策定が始まり、1996 年より発行が開始された。

（４）監査基準 18 号

日本公認会計士協会が公表した監査基準委員会報告第 18 号「委託業務に係る内部統制の有効性の評価」の略称。外部委託業務に関する、内部統制の運用状況を監査するための基準です。日本版 SAS70 と位置づけられています。

（５）ITSMS（IT サービスマネジメントシステム）

ITSMS とは、サービス提供者が、提供する IT サービスのマネジメントを効率的、効果的に運営管理するための仕組みである。

（６）金融機関等コンピュータシステムの安全対策基準（FISC）

財団法人金融情報システムセンター(FISC：The Center for Financial Industry Information Systems)が、重要な社会インフラである金融情報システムの安全性確保のために策定した自主基準。

（７）ITIL（IT Infrastructure Library）

ITIL とは、イギリス政府が策定した、コンピュータシステムの運用・管理業務に関する体系的なガイドライン。ITIL では、コンピュータシステムとその運用管理を、業務の遂行を手助けする「IT サービス」ととらえ、サービスを要求に応じて適切に提供すること、高い投資対効果で継続的に改善していくことを目指している。

４．４．３　個人情報の取扱い

個人情報の取り扱いに関する各種法令等に準拠し、適切に管理、保護されているか否か。またその準拠に基づいて利用目的を明示しているか。

４．４．４　受賞・表彰歴

データセンターに関連する各種アワード等の受賞歴を提示する。主に挙げられる表彰は次のものがある。

（１）ASP・SaaS・ICT アウトソーシングアワード　IDC 部門

日本国内でもっとも優秀かつ社会に有益なASP・SaaS・ICTアウトソーシングを実現しているアプリケーション・コンテンツ提供・その他のオンデマンドサービスなどの、ネットワークを活用したICTサービス全般について表彰するもの。

（２）地球温暖化防止環境大臣賞（環境省）

環境省では、平成10年度から、地球温暖化対策を推進するための一環として、毎年、地球温暖化防止月間である12月に、地球温暖化防止に顕著な功績のあった個人又は団体に対し、その功績をたたえるため、地球温暖化防止活動環境大臣表彰を行っている。

（３）グリーンITアワード（グリーンIT推進協議会）

グリーンIT推進協議会では、優れた省エネ効果を持つIT機器、ソフトウエア、サービス、ソリューション等、並びにそれらを活用して優れた省エネ効果を実現した提案等を表彰し、「ITの省エネ」及び「ITによる社会の省エネ」を両輪とする「グリーンIT」の取り組みを一層加速するため、「グリーンITアワード」を実施。

４．４．５　SLA（サービスレベル・アグリーメント）

開示される項目がSLAとして契約書に添付されるかどうか、もしくは規約にもりこまれているかどうか。または事前に交付やホームページ上で公開されているか。

SLAはデータセンターにおいて事業者と利用者の間で締結される契約書、約款等の一連の契約のうち、数値化可能な部分とする。すなわち、提供されるサービスの質基準を明らかにし、定義するもので、以下の条件を満足するものである。

① SLAはデータセンター事業者が自力で可変できるものである。

② SLAは計測可能（メジャラブル）である。

また、SLAができること、できないことを定義することも重要であり、SLAができること、できないことの例としては以下の例が考えられる。

SLAになじまないことの例として、物理的な面、ファシリティ、セキュリティ等がある。

サービスの種類は大きく３種類に分かれる。

１）ハウジング（建物・設備）

ハウジング（建物・設備）は、ラック提供サービスとスペース提供（ケージサービス等）が基本的なサービスで主にハード面でのSLAとなる。

２）ハウジング（ネットワーク）

ハウジング（ネットワーク）は、基本的なインターネット回線や専用回線提供サービス等の回線で、主にキャリア側のSLA範囲となる。

３）運用サービス

運用サービスは、サーバ、スイッチ等の動作確認や性能管理、障害時の対応等運用に係わるサービスを提供するものでSLAのもっとも重要な事項として規定される。

第５章　ハウジング（サービスサポート）

５．１　サービス窓口（苦情受付）

５．１．１　営業日・時間

（１）営業曜日・営業時間（受付時間）

データセンターサービス受付が 24 時間体制となっているか。または受付時間に制限があるのか。

（２）営業時間外の対応の可否

（１)について受付時間に制限がある場合、受付時間外の対応の可否。緊急時の連絡体系は確立されているか。

５．１．２　サポート範囲・手段

（１）サポート範囲

サービスの受付窓口のサポート範囲がどこまで含まれているか。緊急時の連絡体系にはどこまで含まれているか。

（２）連絡手段

サービスの受付窓口への連絡手段はどうなっているか。二つ以上連絡方法があると災害時に連絡がつきやすい。

５．２　サービス保証・継続

５．２．１　事故発生時の責任と補償範囲

契約書にサービスの保証範囲が明記されているか。その明記されている保証範囲とはどこまでが含まれるか。

また各サービスに対する責任分界点が明記されているか。サービス提供者と利用者間で障害対応の切り分け区分についても明記されているかどうか。

５．３　サービス通知・報告

５．３．１　メンテナンス等の一時的サービス停止時の事前告知

（１）一時的サービス停止時の利用者への告知時期

各メンテナンスを行うために、サービス利用者への告知はあるのか。またその告知はいつごろの時期になるか。

（２）一時的サービス停止時の告知方法

（１）の告知は、サービス利用者に対し、どのような手段で行われるか。

（３）緊急メンテナンスの有無

決められた告知時期よりも短い時期での緊急メンテナンスはあるのか。

５．３．２　障害・災害発生時の通知

障害発生時の連絡がどのような方法で提供されるか。データセンタの運用として障害発生時の連絡体制がどのように組まれているか確認する必要がある。

５．３．３　定期報告

契約しているサービスに対し、定期的な報告が必要かどうか。またはサービス利用者の要求する項目が定期的に報告可能か否か確認が必要となる。

５．４　支援サービス

ハウジング（サービスサポート）として、利用者が持ち込んだサーバー等装置の運用に関する支援の項目である。

５．４．１　障害対応

障害発生時の対応がどこまで対応可能か。障害原因の切り分けまで、障害復旧まで、機器ベンダーへの一時連絡まで等々サービス提供会社によって様々であり、基本サービスに含まれている場合や、オプション対応となる範囲もサービス提供会社により様々である。

５．４．２　定期運用

サービス利用者の作業を定期的・または緊急時に代行して行うサービスはあるのか。サービスの内容としてはどこまでが対応可能か。またそのサービスは基本料金に含まれている場合と、オプション対応となる場合もある。

５．４．３　運用・保守

サービス利用者が持ち込んだ機器を運用・保守を代行して行うサービスはあるのか。サービス内容としてはどこまでが対応可能か。またそのサービスは基本料金に含まれている場合と、オプション対応となる場合もある。

第６章　ホスティング

６．１　ハードウェア提供サービス

６．１．１　サーバ提供サービス（搭載 OS）

電力、空調や情報機器収納用ラックなどのインフラ提供に加えて、利用者がシステムを構築するのに必要なサーバ、ストレージ、ネットワークなどのハードウエアを提供するサービス。要求に応じて機能・性能が選択できるように複数のメニューを準備しているか、利用者の要求に応じた対応がなされる。

搭載ＯＳは、アプリケーションに応じて、Windows 系（WindowsNT, Windows Server, etc.）、UNIX 系（Solaris, HP-UX, Linux, etc.）を選択することができる。

提供形態としては、物理的なサーバを提供するサービス、物理的なサーバではなくサーバの機能・性能を提供するサービス（サーバを他ユーザと共用）などの提供形態がある。

６．１．２　ストレージ提供サービス

データやプログラムの保管・格納用のストレージを提供するサービス。インターネットなど広域ネットワーク環境からのアクセスや、データセンター内の構内ネットワーク環境からのアクセスまで、システム要件に適したサービスを選択することができる。ストレージ容量は数 100MB から無制限まで選択可能となってきており、容量に関する制限は少なくなってきている。

ストレージサービスを受けるシステムが要求するストレージアクセス性能や機能(自動バックアップ機能、リカバリ機能、セキュリティ機能など）を明らかにして、その性能を満たすストレージサービスを選定することが必要。ネットワークを介したアクセスとなるので、サービスによってアクセス性能が大きく異なることに留意する必要がある。

６．２　ネットワークサービス

６．２．１　管理者接続用ネットワーク提供サービス

管理者接続用ネットワークは、管理者が持つ権限の深さから一般利用者が使用するネットワークに比べてより強固なセキュリティを持つことが必要となる。セキュリティを確保するためのネットワーク提供サービスとしては、専用線サービスや IP-VPN サービスなどセキュアな通信路の提供の他、ワンタイムパスワード認証、乱数を用いたパターン認証、指紋認証などネットワークを介した管理対象アクセスを許可する認証サービスなどがある。

６．２．２　ネットワーク機器提供サービス

ネットワークの設計、構築、運用などのサービスがある。これらをワンストップで提供するサービスもあり、システム要件に合わせて最適なサービスを選択することができる。

ネットワークサービスには、WAN（IP-VPN、広域イーサネット、インターネットVPNなど）/LAN構築・運用サービス、VoIPサービス、外出先から社内システムへセキュアにアクセスするモバイルネットワークサービス、インターネット接続サービスなどがある。これらのサービスを提供するネットワーク機器（ルータ、スイッチ、ハブ、ファイアウォールなど）を持ち込むことが困難な場合は、提供を受けるネットワークサービスに必要なネットワーク機器提供のサービスも準備されている。

６．３　高付加価値サービス

６．３．１　ソフトウェア開発環境支援サービス

前述のサーバやストレージ、ネットワーク提供サービスを組み合わせてソフトウエア開発インフラとして提供するレベルから、ソフトウエア開発支援ツールまで実装して提供するサービスまである。

開発環境支援に留まらず、ソフトエアの開発、検証や技術サポートまで含めた、ソフトウエア開発支援まで行うソフトウエア開発支援サービスもある。

６．３．２　セキュリティサービス

「ＡＳＰ・ＳａａＳにおける情報セキュリティ対策ガイドライン」（総務省発行）に基づいた情報セキュリティポリシィが必要である。インターネット接続環境下で一般的に利用される下記の代表的なセキュリティ対策を都合に応じて選択するで事でセキュリティを確保する事ができる。尚、アプリケーションの特性等に応じて追加のセキュリティ対策が必要な場合が生じる。

（１）ウィルス対策

ホスティング環境で構築される各システムに、ウィルスやワーム等の感染防止を行う。尚、使用される全てのサーバに対してウィルス対策を行うことを強く推奨する。

（２）ファイアウォール設定

ホスティング環境で構築される各システムに対する、ファイアウォールのネットワーク・アクセス制御ルールの設定を行う。

（３）不正侵入対策

ホスティング環境で構築される各システムに対する、インターネット等外部ネットワークからの不正侵入の検知もしくは防御を行う。

（４）ＯＳセキュリティ設定

ホスティング環境のインターネット公開セグメントに配置する各システムに対し、ＯＳレベルでの基本的なセキュリティ設定を行う。

（５）脆弱性診断

ホスティング環境で構築される各システムに対して、脆弱性診断を行う。対象は、ネットワークとアプリケーションとなり診断の方式が異なる。

６．３．３　Ｗｅｂ系サービス

ホスティング基盤上で、ネットワーク環境やアプリケーションの実行環境などを提供するサービスである。新規のアプリケーション開発や既に開発されたパッケージソフトやアプリケーションを活用してＡＳＰ/ＳａａＳ事業に参入する際に、追加で必要となる機能や環境をサービスとして提供する事により短期で立ち上げが可能となる。代表的な機能としては、以下の通りである。

（１）ドメインネーム

取得したドメイン名の設定、または指定ドメイン名を付与し、アプリケーションのロケーションを意識させる事なく利用可能となる。

（２）ＳＳＬサーバ証明

取得／付与したドメイン名に対して、取得／付与したサーバ証明書をホスティング基盤に設定する。

（３）利用ポータル

アプリケーション／サービスや各種管理機能を利用するための利用者向けポータルを提供する。

（４）認証

認証機能、及び、利用ポータル画面を経由したシングルサインオンの機能。

（５）アクセス管理

特定ＩＰアドレスからのアクセスのみを許可または拒否する機能。

（６）ユーザ管理

ユーザ情報の登録・更新及びアプリケーション／サービスを利用条件の設定を行う機能。

（７）サービス管理

サービスや利用ポータルの情報管理に加えて、アプリケーション／サービスの稼動スケジュール等、サービスの稼動制御を行う機能。

６．３．４　メール系サービス

メール系のＡＳＰ／ＳａａＳ／アウトソーシングサービスとして、代表的な機能としては以下の通りである。

（１）基本サービス

メール機能を中心とするサービス（メール送信／作成、メール閲覧、アドレス帳、個人設定、フォルダ機能、等)。

（２）アーカイブサービス

送受信されたメールを全て保存するサービス（長期の保存が可能、多様なメール環境に対応、高度な検索機能、万全のセキュリティ、等)。

（３）メールフィルタリングサービス

スパムメールをフィルタリングするサービス（ドメイン単位でポリシィを一括管理、自ドメイン宛の迷惑メール受信状況の分析、等)。

（４）ウィルスチェックサービス

ウィルス感染をチェックし駆除及び送信をブロックするサービス(ゲートウェイでのウィルスチェック、感染ファイル発見時の通知、ウィルスチェックプログラムの運用、ウィルスチェックサーバの運用、等)。

（５）ビジネスブログサービス

企業内コミュニケーションツールとして簡単に導入できるサービス（ブログ機能、ニュースクリップ機能、ブログポータル機能、認証機能、メール通知機能、アクセス情報、ＳＳＬ対応、等)。

６．３．５　ロードバランサーサービス

複数のサーバを利用する場合に各ノードのロードバランス機能であり、サーバ間のＳＳＬ認証に必要なアクセラレータ機能を提供するサービスである。サーバのスケーラビリティが簡単に拡張でき、保守運用コストも圧縮されるので、多くのｗｅｂアプリケーションに適している。

（１）通常のロードバランス方法は以下の２種類

・複数のサーバに対して均等にロードバランス（Round Robin)

・最もコネクション数の少ないサーバを選択してロードバランス（Least Connection)

（２）代表的な負荷分散のプロトコルは以下の通り

・ ＨＴＴＰ	・ ＦＴＰ
・ ＳＳＬ	・ ＮＮＴＰ
・ ＳＭＴＰ	・ ＤＮＳ　　ｅｔｃ.

６．３．６　バックアップ・リストアサービス

一般的に、システムの規模や用途により、適切な範囲と頻度でバックアップの運用がなされる。どの範囲のデータをどのくらいの頻度でバックアップし、どのくらいの時間破棄しないで保存しておくかという事をバックアップサービスの対象や種類によって選択する事になる。そのバックアップの形態によりリストアに要する時間帯が異なってくる。

（１）バックアップリストアの対象

・ファイルバックアップ

ファイルやフォルダ単位のバックアップで、リストアに手順を要する事が多い。

・イメージバックアップ

ＯＳやアプリケーションのシステム全体をバックアップで、システム全体をリストアするのでファイルバックアップに比較して手順が掛からない。

（2）バックアップ・リストアの種類

・フルバックアップ

全てのデータを一度に纏めて一括にバックアップする機能であり、毎回実施するのでバックアップ・リストアに時間を要する。

・差分／増分バックアップ

前回のフルバックアップ時からの変更／追加されたデータのみをバックアップする機能であり、リストアは差分バックアップしたデータと、差分バックアップに存在しないデータをフルバックアップ時のものから取り出す事で行う。

（3）バックアップの頻度、保存期間

・頻度

日次（毎日決まった時間帯）でバックアップを行うか、週次、月次、年次で行うかにより、体系が異なる。

・保存期間

バックアップをどのくらいの期間破棄しないで保存しておくか、データの種類によっては法律により保存しておかなければならない期間が定められている事もある。

６．３．７　その他サービス

（1）ＳａａＳプラットフォーム・サービス

新規にＳａａＳ型アプリケーションを開発する場合に必要となる機能や環境を提供するサービスで、以下に概要を記す。

・インターネットを介してアプリケーション機能を提供する際に最低限必要となるサービスインフラ（リバースプロキシ、ドメインネームサービス、ゲートウェイ型ウィルス対策等）を提供する。

・アプリケーションをＳａａＳ型で提供する際に必要となる機能（認証やユーザ管理、サービス管理、稼動状況管理等）を提供する。

（2）ファイル共有・サービス

オンライン上での共有ファイル機能を提供するサービスで、以下に概要を記す。

・オンラインストレージサービス・・・オンラインストレージを用意してファイル共有機能を提供する。

・ウィルス対策サービス・・・オンラインストレージ上のファイルに対してウィルス対策機能を提供する。

・アクセス監視サービス・・・ディレクトリファイルに対する操作履歴の取得機能を提供する。

６．４　支援サービス

６．４．１　障害対応

ホスティング環境（レンタル機器）に障害が発生した際に、障害原因の一次切り分け、及び障害対応の一般的なサービス内容が下記の通りである。

（１）障害のインプット情報

・顧客からの障害に関する問い合わせ、もしくは、環境稼動監視による障害検知により、速やかに着手する。

・障害対応時間帯は、通常、24 時間 365 日、受け付ける。

（２） 障害サービス内容

・障害切り分けにより、障害の原因がホスティング提供範囲である場合は、早急に障害の回復を図る。

・障害原因がホスティング提供外である場合は、予め決められた連絡方法で、顧客へ連絡し、一次切り分けは完了する。

（３）障害報告事項

・障害回復通知

障害回復完了後、予め決められた連絡方法で顧客に連絡する。

・障害対応完了の確認

正常な状態に回復した事を確認し、確認が完了した事を連絡する。

・障害対応の進捗報告

一次切り分けの着手から障害対応の完了まで､予め決められた頻度と連絡方法で報告が行われる。

・障害報告書

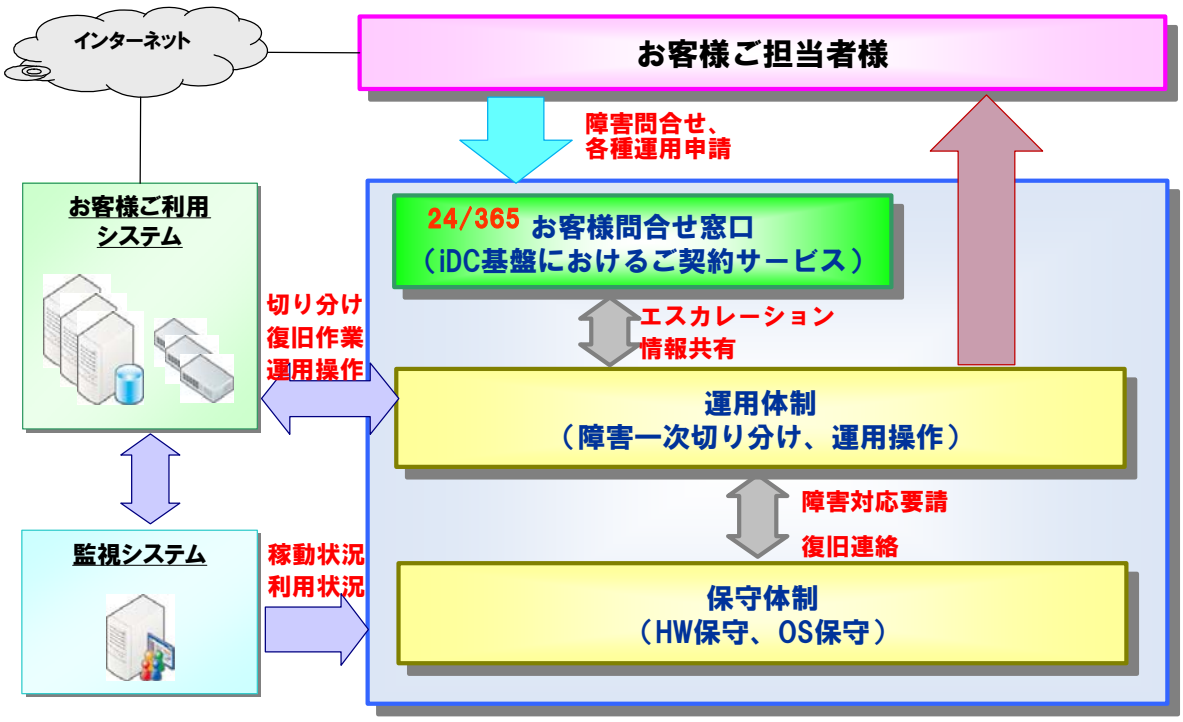
障害回復後、障害原因を含めた報告書を作成し、予め決められた期日内に提示される。

６．４．２　定期運用

（１）サービス保証・継続

契約書にサービスの保証範囲が明記されているか。その明記されている保証範囲とはどこまでが含まれるか。また各サービスに対する責任分界点が明記されているか。サービス提供者と利用者間で障害対応の切り分け区分についても明記されているかどうか。

障害発生時の対応がどこまで対応可能か。障害原因の切り分けまで、障害復旧まで、機器ベンダーへの一時連絡まで等々サービス提供会社によって様々であり､基本サービスに含まれている場合や、オプション対応となる範囲もサービス提供会社により様々である。



（２）定期運用時の定型作業

・環境稼動監視

ホスティング環境の稼動状況（サーバ、ストレージ、ネットワーク）を常時監視し、障害を検知した場合、連絡を行う。

・VPN アカウントの設定、変更

顧客のセキュリティポリシにもとづき､既存の VPN アカウントのパスワードを発行する。

・オペレーティングシステムのマウント

提供されるオペレーティングシステムのメディアをマウントする。

・サーバ起動

顧客都合により一旦停止されたサーバを対象に指定された日時に起動する。

・データアーカイブ

規定されている取得頻度（日次、週次）と世代をストレージのアーカイブとして自動的に取得する。

（３） 利用状況報告

・提供されるサーバのリソース利用状況（ＣＰＵ使用率、メモリ空き容量、ディスク使用率）を定期的に報告される。

・予め定めた、報告対象期間（１ヶ月）、報告間隔（１回／月）にて定期的に報告される。

参考：　データセンターの安全・信頼性に係る情報開示指針（第１版）

（総務省報道発表：平成 21 年 2 月 26 日）

データセンターの安全・信頼性に係る情報開示指針（第1版）

前提1：＜情報開示の対象＞
情報開示の対象（単位）は、各データセンター毎とする。

前提2：＜ハウジング、ホスティングの定義＞
本指針におけるデータセンターの「ハウジング」及び「ホスティング」の定義は以下のとおりとする。

①「ハウジング」とは、建物、設備（電源、空調、ラック等）、回線等の「ハウジングサービス」を指す。なお、利用者の持込機器（サーバ、NW機器等）に対するサービスは、ハウジングに含むものとする。

②「ホスティング」とは、高付加価値サービス、ネットワークサービス、ハードウエア提供サービス等「狭義のホスティングサービス」（一般的なホスティングサービスから上記のハウジングサービス部分を除いたもの）を指す。なお、利用者へのサーバ・NW機器等のレンタル及びレンタル機器に対するサービスはホスティングに含むものとする。

	【情報開示項目】			【記述内容】	必須/選択（注）
1	開示情報の時点		開示情報の日付	開示情報の年月日（西暦）	必須
－	事業所・事業				
2		事業所等の概要	事業者名	事業者の正式名称（商号）	必須
3			事業者ホームページ	事業者のホームページのURL	選択
4			設立年・事業年数	事業者の設立年（西暦）	必須
5				データセンター事業の事業年数	必須
6			事業所	事業者の本店住所・郵便番号	必須
7				事業所数　（国内、国外） ＜内＞データセンター事業所数	
8		事業の概要	主な事業の概要	事業者の主要な事業の概要 （データセンター事業以外も含む）	必須
－	人材				
9		経営者	代表者	代表者氏名	必須
10				代表者経歴（年齢、学歴、業務履歴、資格等）	選択
11			役員	役員数	選択
12		従業員	従業員数	正社員数（単独ベース）	選択
－	財務状況				
13		財務データ	売上高	事業者全体の売上高（単独ベース）（単位：円）	必須
14			経常利益	事業者全体の経常利益額（単独ベース）（単位：円）	選択
15			資本金	事業者全体の資本金（単独ベース）（単位：円）	必須
16			自己資本比率	事業者全体の自己資本の比率（単独ベース）（単位：%）	選択
17		財務信頼性	上場の有無	株式上場の有無と、有りの場合は市場名	選択
18			財務監査・財務データの状況	該当する財務監査・財務データの状況を、以下より選択する。 ①会計監査人による会計監査、②会計参与による監査、③中小企業会計によるチェックリストに基づく財務データ、④いずれでもない	選択
19			決算公告	決算公告の実施の有無	選択
－	資本関係・取引関係				
20		資本関係	株主構成	大株主の名称（上位5株主程度）、及び各々の株式保有比率	選択
21		取引関係	主要取引金融機関	主要取引金融機関の名称	選択
22			所属団体	所属している業界団体、経済団体等の名称	選択
－	コンプライアンス				
23		組織体制	専担の部署・会議体	コンプライアンスを担当する社内の部署・会議体の有無と、有りの場合は社内の部署名・会議名	選択
24		文書類	情報セキュリティに関する規程等の整備	情報セキュリティに関する基本方針・規程・マニュアル等文書類の有無と、有りの場合は文書類の名称	必須
25				上記の文書類の経営陣による承認の有無	
26			データセンターサービスの苦情対応に関する規程等の整備	データセンターサービスの苦情処理に関する基本方針・規程・マニュアル等文書類の有無と、有りの場合は文書類の名称	必須
27				上記の文書類の経営陣による承認の有無	

（注）「必須」は情報開示が必須である項目、「選択」は情報開示が任意である項目を指す。

1/5

【情報開示項目】				【記述内容】	必須/選択（注）
-	ハウジング （建物・設備）				
28		建物	データセンター識別名	情報開示するデータセンターの名称もしくは相当する識別名称	必須
29			データセンター事業開始年	当該データセンターの事業開始年	必須
30			建物専用形態	データセンター専用建物、オフィス建物のいずれに近いかの明示	必須
31			所有・入居形態	事業者の自己所有施設か、賃借施設かの明示	必須
32				事業者の単独利用（ビル一棟借り）、他の入居者との共同利用（ビル一部利用）のいずれかの明示	必須
33			建設時期	建物の竣工年・月	必須
34			所在地	所在国名、日本の場合は地域ブロック名（例：関東、東北）	必須
35				最寄り公共交通機関の拠点から所在地までの交通手段と所要時間	選択
36			建物規模	建物内のサーバールームの延床面積 （㎡）	選択
37				最大収容可能ラック数	必須
38			耐震・免震構造	耐震数値（震度）	必須
39				地震対策に係る建物構造（免震、制震構造等）	
40			耐火構造	耐火建築物か否かの明示	必須
41			防水構造	外壁・屋根・開口部の防水措置の有無	必須
42			床荷重	サーバ室スラブ床平米（㎡）当たりの耐荷重（最大値）	必須
43		電源設備	無停電電源	無停電電源とするための対策（UPS設置等）の有無と、 有りの場合は電力供給最低可能時間、及び非常用電源の稼働開始時間との関係	必須
44			給電ルート	異なる変電所からの給電ルート（系統）で2ルート以上確保されていることの有無（無停電電源、非常用電源を除く）	必須
45			受電方式	受電方式 （ループ受電、変電所からのスポット受電等）	必須
46			電力設備監視	電力設備の集中監視を実施しているか否かの明示	必須
47			非常用電源	非常用電源（自家発電機）の有無と、 有りの場合には無給油での連続稼動時間、及び非常用電源稼動対策の内容（燃料の連続供給方法等）	必須
48		消火設備	サーバルーム内消火設備	自動消火設備の有無と、 有りの場合はガス系消火設備（ハロンガス対応、新ガス対応の別）か否かの明示	必須
49			火災感知・報知システム	火災検知システム、煙検知システムの有無	必須
50		避雷対策設備	直撃雷対策	直撃雷対策の有無	必須
51			誘導雷対策	誘導雷対策の有無と、 有りの場合は最大対応電圧の数値（選択）	必須
52		空調設備	十分な空調設備	空調設備の内容 （床吹き上げ空調、コンピュータ専用個別空調、水冷・空冷式、その他の工夫 等）	必須
53				空調設備の容量 （KVA/㎡、Kcal/㎡等）	選択
54		ラック/スペース	ラックレンタル	ラックレンタルの提供単位（フル、ハーフ、その他）	必須
55			スペース貸し	スペース貸し・ラック持ち込み等の可否	必須
56			荷重	ラックへの搭載可能荷重（標準値、最大値）	必須
57			電力	ラック単位の提供可能電力（標準値、最大値）	必須
58			監視機能	ラックの電力監視機能、温度監視機能の有無と、 有りの場合は、それが標準機能かオプション機能かを明示	必須
59		作業スペース	事務作業スペース	利用者用の事務作業スペースが建物内に確保されているか否かの明示	選択

（注）「必須」は情報開示が必須である項目、「選択」は情報開示が任意である項目を指す。

【情報開示項目】				【記述内容】	必須/選択（注）
60		セキュリティ	24時間365日監視体制	有人監視又はそれに代わる体制・システムとなっているか否かの明示	必須
61			外部委託先	運用外部委託先（派遣、請負等）の有無	必須
62			入退館管理等	セキュリティレベルに応じた区画（フロア単位、ラック単位、ラック分割単位等）の分離と、各区画における入退室管理や施錠等のセキュリティ対策の有無	必須
63				入退室記録の有無と、 有りの場合はその保存期間	必須
64				監視カメラの有無と、 有りの場合は監視カメラ稼働時間、映像の保存期間、改ざん防止機能の有無	必須
65				個人認証システムの有無	必須
66				認証システムがある場合はその認証方式を記述	選択
67				持込持出物品の制限又は対策（持ち物検査等）の有無	必須
68				入館、作業時等のデータセンタ側のアテンドの有無	必須
69			媒体の保管	磁気テープ、光メディア等の媒体の保管のための鍵付きキャビネットや保管室の有無	選択
70				保管管理手順書の有無	
71			その他セキュリティ対策	その他特筆すべきセキュリティ対策	選択
72		環境対応	電力消費の効率化	電力消費の効率化の目標の有無 （測定条件等を明確にしたPUE等）	選択
73			その他の環境対応策	その他特筆すべき環境対策 （紙ゴミリサイクル化、自然エネルギー活用、廃熱対策、ラック間・ラック内の熱だまり対策等）	選択
－	ハウジング （ネットワーク）				
74		回線	バックボーンネットワーク	データセンターが接続しているバックボーンネットワークの容量（帯域、帯域幅）	選択
75			接続回線	建物への引き込み経路が2つ以上あるか否かの明示	必須
76				バックボーンネットワークへの占有回線の有無と、 有りの場合は、占有回線の最高速度	必須
77				バックボーンネットワークへの共有回線の有無と、 有りの場合は、共有回線の最高速度（ベストエフォート型、帯域保証型）	必須
78				提供されるネットワーク回線での複数ISP事業者の選択の可否	必須
79				ASP・SaaS事業者等が別回線（メンテナンス用のISDN回線等）を自前で引くことの可否と、 可の場合でのキャリア制限等の有無	必須
80				ネットワーク機器（ルーター等）の経路増、IPV6への対応等の将来拡張能力	必須
81		サービス	サービス内容	データセンター事業者側が提供できるネットワークに関するサービス内容 （インターネット接続、設定サービス代行、監視、侵入検知等のセキュリティ対策等）	必須
－	ハウジング （サービスの内容）				
82		サービスの受付・問合せ	受付・申込・問合せ先	電話／FAX、Web、電子メール等の連絡先	必須
83		サービスの変更・終了	サービス（事業）変更・終了時の事前告知	利用者への告知時期（事前の告知時期を1ヶ月前、3ヶ月前、6ヶ月前、12ヶ月前等の単位で記述）	必須
84				告知方法	
85			サービス（事業）変更・終了後の対応・代替措置	対応・代替措置の基本方針の有無	必須
86				基本方針に沿った具体的なユーザへの対応策（代替サービスの紹介等）の有無	
87				契約終了時の情報資産の返却責任の有無	
88			サービス（事業）変更・終了に係る問合せ先	問合せ先（通常の苦情等の問合せ窓口も含む）の有無と、 有りの場合は名称・受付時間	必須
89		サービス料金	料金体系	初期費用額	必須
90				月額利用額	
91				最低利用契約期間	
92			解約時ペナルティ	解約時違約金（ユーザ側）の有無	必須
93			利用者からの解約事前受付期限	利用者からのサービス解約の受付期限の有無と、有りの場合はその期限（何日・何ヶ月前かを記述）	必須

（注）「必須」は情報開示が必須である項目、「選択」は情報開示が任意である項目を指す。

【情報開示項目】				【記述内容】	必須/選択(注)
94		サービス品質	サービス可用性	年間障害停止時間(ダウンタイム)、障害停止の事故歴(5年以内) 5年以内に障害停止があった場合には、その内容と再発防止策 (ここでいう障害停止とは、何らかの障害によりデータセンターの顧客サービスが停止したこと)	必須
95				点検を含む定期メンテナンスの実施内容と間隔	必須
96			認証取得・監査実施	プライバシーマーク、ISMS(JIS Q 27001など)、ITSMS(JIS Q 20000-1など)、ISO14001の取得、18号監査(米ではSAS70)の監査報告書作成の有無と、 有りの場合は認証名あるいは監査の名称、及びデータセンター単位か企業単位かを明示	選択
97			個人情報の取扱い	個人情報を収集する際の利用目的の明示	必須
98			受賞・表彰歴	データセンターに関連する各種アワード等の受賞歴	選択
99			SLA (ｻｰﾋﾞｽﾚﾍﾞﾙ・ｱｸﾞﾘｰﾒﾝﾄ)	開示項目がSLAとして契約書に添付されるか否か	必須
-	ハウジング (サービスサポート)				
100		サービス窓口 (苦情受付)	営業日・時間	営業曜日、営業時間(受付時間)	必須
101				営業時間外の対応の可否	
102			サポート範囲・手段	サポート範囲	必須
103				連絡手段(電話/FAX、電子メール等)	
104		サービス保証・継続	事故発生時の責任と補償範囲	データセンター事業者の事故責任の範囲と補償範囲が記述された文書の有無、有る場合はその文書名称	必須
105		サービス通知・報告	メンテナンス等の一時的サービス停止時の事前告知	利用者への告知時期 (1ヵ月前、3ヵ月前、6ヵ月前、12ヵ月前等の単位で記述)	必須
106				告知方法	
107				記述よりも短い告知時期での緊急メンテナンスの有無	
108			障害・災害発生時の通知	障害発生時通知の有無	必須
109			定期報告	利用者への定期報告の有無	必須
110		支援サービス	障害対応	利用者持込み機器類の障害時対応サービスの有無と、 有りの場合にはその内容(障害切り分け・復旧、ベンダーへの手配等)	必須
111			定期運用	利用者持込み機器類の定期運用サービスの有無と、 有りの場合にはその内容(電源ON/OFFや再起動等の代行、機器のLEDの確認、運用手順書に沿った日々の運用作業等)	必須
112			運用・保守	利用者持込み機器類の運用・保守支援サービスの有無と、 有りの場合にはその内容(死活監視、障害監視、リソース監視、運用支援、バックアップ等のオペレーション等)	必須

(注)「必須」は情報開示が必須である項目、「選択」は情報開示が任意である項目を指す。

【情報開示項目】				【記述内容】	必須/選択 (注)
-	ホスティング　＜定義については、表頭の前提2を参照のこと＞ （上記の当該データセンターにおいて、提供しているホスティングサービスについて限定し、記述する）				
113		ハードウエア提供サービス	サーバ提供サービス （搭載OS）	共用サーバ、専用サーバ、仮想化サーバ等のサービス内容 （Windows,Unix,Linux 等のOSを記述）	必須
114			ストレージ提供サービス	ストレージ提供サービスの内容	必須
115		ネットワークサービス	管理者接続用ネットワーク提供サービス	リモートデスクトップ、SSH等の接続手段の内容	必須
116			ネットワーク機器提供サービス	ルーター、スイッチ等のネットワーク機器提供サービスの内容	必須
117		高付加価値サービス	ソフトウエア開発環境支援サービス	Java、Servlet、Perl、PHP、Ruby、C/C++、その他のオープンソースの開発環境の提供等	必須
118			セキュリティサービス	ウイルス対策、ファイアウオール、侵入検知、SSL、セキュリティ診断等のサービス内容	必須
119			Web系サービス	Web系サービスの内容	必須
120			メール系サービス	メール系サービスの内容	必須
121			ロードバランサーサービス	ロードバランサーサービスの内容	必須
122			バックアップ・リストアサービス	バックアップサービス、障害時のリストアサービス等の内容	必須
123			その他サービス	各種申請代行、決済代行、業務代行等の内容	必須
124		支援サービス	障害対応	レンタル機器類の障害時対応サービスの有無と、 有りの場合にはその内容（障害切り分け・復旧、ベンダーへの手配等）	必須
125			定期運用	レンタル機器類の定期運用サービスの有無と、 有りの場合にはその内容（電源ON/OFFや再起動等の代行、機器のLEDの確認、運用手順書に沿った日々の運用作業等）	必須
126			運用・保守	レンタル機器類の運用・保守支援サービスの有無と、 有りの場合にはその内容（死活監視、障害監視、リソース監視、運用支援、バックアップ等のオペレーション等）	必須

（注）「必須」は情報開示が必須である項目、「選択」は情報開示が任意である項目を指す。