平成13年度
iDC選択利用ガイドライン

平成14年 3 月

財団法人　情報処理相互運用技術協会

はじめに

米国から発祥したインターネットデータセンター(以下 iDC)は、インターネットサービスの展開およびインターネットの普遍性と相俟って瞬く間に全世界に広がり、日本においても大小の iDC 事業者が出現して、現在では 60 社とも 70 社とも云われる状況にある。

米国では当初、サーバやストレージなどの大量集中保管・管理による運用コスト低減や、高度なセキュリティとコネクティビティ確保などを目的としていたが、各社サーバの集中効果により、iDC 内での企業間データ交換から更には iDC 上にビジネスモデルを構築して企業に提供する段階に至っている。一方日本においては、住民サービスや公共調達などをインターネットで行うことが検討・試行されている。この場合、政府や自治体の扱う情報を安全確実に管理すると共に住民や企業へ積極的に公開する、という相反する要件を満たす必要がある。その現実的な解として iDC の仲介する形態が提案されている。

このように市民生活および企業活動の様々な面で iDC が社会基盤としての役割を担うようになるにつれ、サービス内容が多様化するだけでなく、サービスの質にも高低の差が生じてくる。その一方で、事業的にも技術的にも、iDC 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・対応に向けた iDC 事業者間での水平分業、急速に進展する技術に対応した専門サービス事業者との垂直分業が進展しつつある。

iDC を利用する立場からすると、あまりにも多種多様なため適切な iDC を見つけるのが困難な状況にある。手軽に安く利用したいのに要塞なみの堅牢な(そして利用料金の高い)iDC を利用したり、顧客情報を安全確実に保管したいのに不特定多数が頻繁にアクセスするサービス事業者向けの iDC に委託したり、という致命的な誤りを犯す恐れがある。

その一方、米国では 2003 年に企業の情報基盤の 80%が iDC 上に展開されると予測されており、日本においてもシステムインテグレータ(SIer)が利用目的に適った iDC を的確に選択し、その上に顧客の情報システムを構築する時代が目前に迫っていると考えられる。

このような問題認識に立って INTAP では今春から SIer の立場で iDC を調査し、適切な iDC を選択するための指標を検討してきた。一口に iDC と云ってもその規模・業態は様々で、大容量回線を引込んだファシリティ重視型から、アプリケーションも含めた統合サービス型まで千差万別である。そのため漏れなく抽出するには長期に亘る調査・検討を要するが、当該分野は急速に変化・進展しているので時宜を失する恐れがある。それで巧遅より拙速を優先し、まずは基盤的なサービスに関する選択の指針として纏めることにした。本ガイドラインの読者としては SIer を想定しているが、iDC を利用する立場にある ASP や企業・官庁のシステム部門にも充分に役立つ内容となっている。協賛会員企業始め、中央官庁および地方自治体、一般企業のお役に立てば幸いである。

平成 14 年 3 月

iDC/ASP 委員会

委員長　本田雅裕

作成者一覧

氏　名	会　社　名	所　属
本田　雅裕	日本電気（株）	ＮＥＣソリューションズ
熊白　侃彦	沖電気工業（株）	システムソリューションカンパニー
倉林　弘明	（株）東芝	ｅ－ソリューション社
清水　昇	日本電気（株）	ＮＥＣソリューションズ
福士　祐治郎	日本ユニシス（株）	asaban．com 事業部
田村　聖一	（株）日立製作所	情報・通信グループ統括本部
坂本　誠	富士通（株）	システムサポート本部テクニカルセンター
林　　乙平	富士通（株）	システムサポート本部
黒川　信弘	松下電器産業（株）	システムソリューション事業本部
村澤　靖	三菱電機（株）	情報通信システム開発センター
小林　偉昭	日立ネットビジネス（株）	戦略マーケティング本部
神原　顕文	（財）情報処理相互運用技術協会	
小島　富彦	（財）情報処理相互運用技術協会	
石橋　博	（財）情報処理相互運用技術協会	
西沢　隆	（財）情報処理相互運用技術協会	

（敬称略、順不同）

目　次

第１章　iDC とは

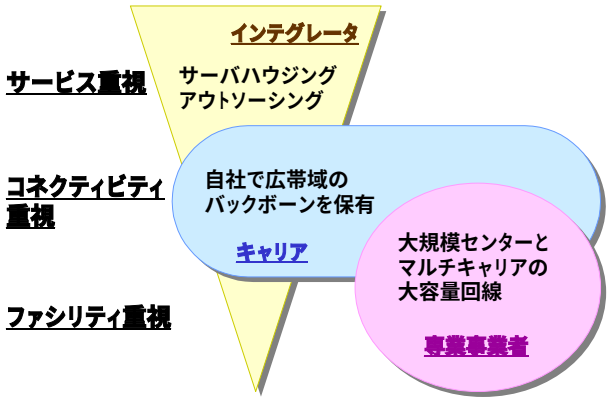
第１章　iDC とは

インターネットデータセンター(以下 iDC と称す)の現状を概観し、iDC 利用の意味を分析することにより、本ガイドラインで示す選択指針の範囲を明らかにする。

1.1　iDC の全体像

（1）サービスによる分類

一口に iDC と云っても事業者によってその業態は多種多様である。60 社とも 70 社とも云われる日本の iDC 事業者は、その事業目的により、大容量回線を引込んだ大規模なセンターのファシリティ重視型、従来の計算センターやアウトソーシング事業から進出する SIer(System Integrator)主導の統合サービス型、キャリアの局舎流用など地の利を活かしたコネクティビティ重視型、に大きく分類できる(図 1.1)。日本の iDC の多くは小規模であり、少数の大規模 iDC が大勢を占める米国とは対照的である。



（2）iDC のサービス構造と構成要素

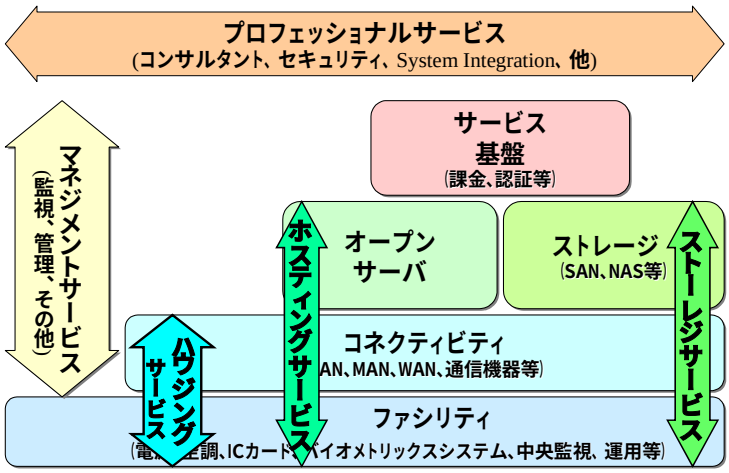


図 1.2 iDC のサービス構造

大小乱立しているとは云え、事業内容を分析すると、共通項、最大公約数が見えてくる。境界は iDC によって微妙に異なるが、機器設置のスペースを提供するハウジングサービス、サーバも提供するホスティングサービス、大容量ストレージを部分提供するストレージサービスが代表的なメニューである。

それにマネジメントサービスやプロフェッショナルサービスを付加することが多い(図 1.2)。iDC のサービスを実現・提供する仕組みは各社の事業戦略で異なる。しかしながら大枠

は似通っていると云って良い。即ち、全サービスの基盤となる堅牢な建屋や電源および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、それに運用、コンサルテーション、SI(System Integration)など人間系が加わる。

（3）専門事業者との連携

事業規模が大きくなり、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 iDC 事業者が単独で全サービスを提供することが困難になってきている。様々なリスクに対応するため iDC 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専門的なサービスに特化した事業者との垂直分業が組まれつつある。即ち、主としてファシリティやサーバなど設備・機器提供の iDC、自らは設備を持たないで機器の運用に徹する MSP(Management Service Provider)、高信頼なストレージを大量に提供する SSP (Storage Service Provider)、コネクティビティを提供する ISP(Internet Service Provider)／NSP(Network Service Provider)などである。そして、これらのリソースを活用して顧客に各種のアプリケーションを提供するのが ASP（Application Service Provider）である(図 1.3)。

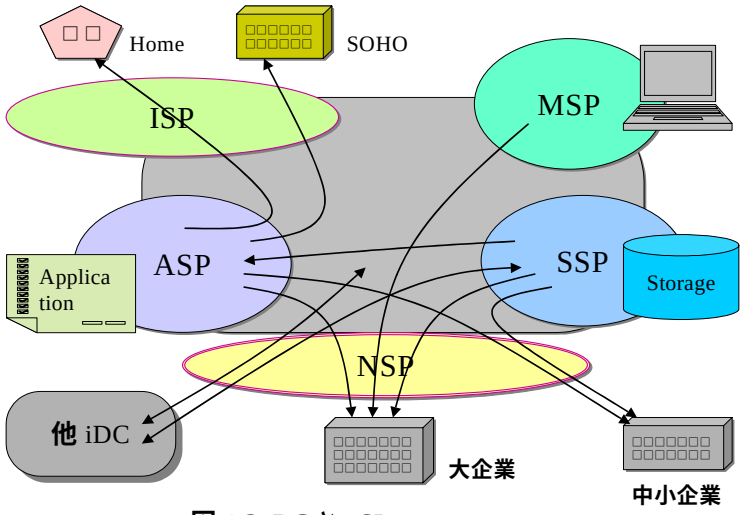


図 1.3 iDC と xSP

1.2 iDC の位置付けと将来

前記のファシリティだけに着目すると、iDC は計算センターの発展形に見える。しかし、従来のアウトソーシングあるいは計算センターの延長として iDC を捉えるか、発端はそうだとしても殻を脱皮した全く新しい事業形態を形成しつつあると見るかによって、iDC の位置付けは大きく異なる。現時点では両者が混在して一見しただけでは区別できないため、その意義を見誤る恐れが多分にある。

当初は米国においても、サーバやストレージなどを大量に集中保管・管理することによる運用コスト低減、高度なセキュリティとコネクティビティ確保、インターネット技術者確保などの効果を謳っていた。現在もその効果は決して小さくない。しかしながら一旦、

各社のサーバが集中すると、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 iDC 内で完結することが可能となる。これは現在でも各社のコンピュータを通信回線で接続して行っているので自然な流れと言える。それを更に一歩踏み込んで、実際の取引に付随して仕組みを構築するのでなく、特定のビジネスモデルを対象に iDC 上で仕組みを構築し、それを必要な企業に提供する動きが出てきた。即ち、iDC がビジネスの場とビジネスモデルを提供するようになり、質的に異なる段階に入ってきた。日本はまだ最初の段階にあるが、米国では iDC が企業間取引の基盤に位置付けられつつある。

全世界の企業が全て同じ iDC 上にサーバを設置することは不可能である。一方、企業間取引のデータ交換は極めて高いセキュリティ、パフォーマンスが要求される。このことから必然的に異なる iDC 事業者のセンター間を高速な専用回線で結ぶことが帰結される。複数のセンターを運営する iDC は既に自社のセンター間を高速の専用回線で結んでおり、採算上も技術的にも現実的な解である。もちろん、従来のインターネットとも高速回線で接続する。即ち、iDC 間だけに閉じた IP(Internet Protocol)ネットワークと広く開かれたインターネットの両方に繋がる(図 1.4)。企業内及び企業間の情報・データは閉じた IP ネットワーク上を流れ、外部との情報提供・情報交換はインターネットを用いることになる。更には、デジタルデータの爆発的増加に伴い、iDC 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を形成する動きがある。

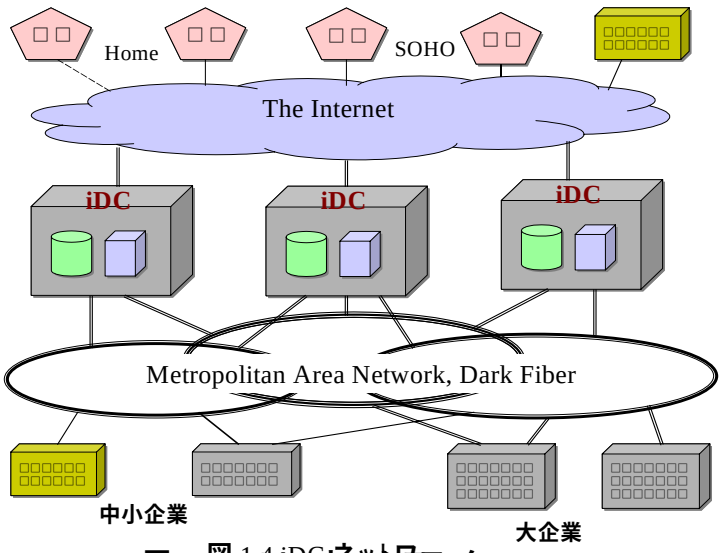


図 1.4 iDC ネットワーク

これは民間企業を対象とした iDC の場合である。政府や地方公共団体は取り扱う情報の性格上、今後とも閉じられたネットワークを形成するであろう。一方で住民や企業への情報公開が進み、ネットワークを介した住民サービスも始まる。その手段としてインターネットが注目されている。しかし、政府や地方公共団体のサーバを直接にインターネットへ接続するのは極めて危険である。従って、この場合も民間企業と同じく、iDC が両者の間に入って仲介する形態が今のところ最も適切であろう。即ち、社会インフラとしても iDC は極めて重要な位置にあると云える。

1.3 iDC 利用の適否

長期的ないし一般論では iDC が有効であるとして、現時点で個々の利用者にとってはどうであろうか。典型的な iDC 像からその効用と問題点を比較整理して、iDC に適した利用形態を考察する。

表 1.1 iDC 利用の効用と問題点

iDC 利用の効用	iDC 利用の問題点
○堅牢な建物･厳重な警備に基づく物理的セキュリティの確保 ○電源や通信ケーブルなど二重化･冗長化したファシリティに基づく高い可用性 ○月々に利用料を支払うだけで済む経費 ○３交替勤務による 24 時間 365 日運用 ○主要 ISP/iDC とのピアリングや IX に直結した高速・大容量のコネクティビティ ○利用者固有のハード/ソフトを持込むだけでシステム立上げ稼動 ○即時稼動可能状態で待機している機器利用による事業の早期立上げ ○専門家集団による最先端･高度技術の活用	●重要なデータ･情報を社外に置き、社外の要員が扱うことに由来する危険 ●企業活動の頭脳･中枢神経系統を外部に委ねる危険(不安) ●障害発生時に対応が遅れる恐れ ●回線使用料増加あるいは応答性の悪化 ●長期･大規模な利用では嵩む総費用 ●利用者固有･特有部分が多いと増大する所要時間･費用 注）多くは情報システムの運用を外部に委ねることに起因する問題である

自営システムで構築する場合の利点と欠点は概ね上記の逆になると考えて良い。しかしながら、効用の数だけで iDC を利用するか自営で構築するかを決めることはできない。むしろ個々の利用目的に依存した特定の事項の重要度に大きく影響される。例えば、情報を社外に置くことの危険を看過できない場合、iDC の利用効果が如何に大きくとも自営システムで運用することになろう。逆に、24 時間 365 日運用が必須であるにも拘らず自社で要員を確保できなければ、少々の危険を犯してでも iDC を利用するのが次善の策である。時間の経過と共に環境条件が変化することも無視できない。例えば、ネットワーク環境は料金も能力も急速に改善されつつあり､現在の状況を前提にすると判断を誤る恐れが高い。

以上を勘案すると現時点で日本においては、概ね次の何れかに該当する場合に、iDC を利用するのが適切である。

◎ 24 時間 365 日のオンライン稼動が必須である。
◎ 短時間で急激にトランザクションが変化する。
◎ システムを素早く立ち上げるのが事業遂行に有利である。
◎ 情報通信技術の急激な革新に追随する必要がある。
◎ 継続的に高いセキュリティを維持する必要がある。
◎ 初期投資を抑制しなければならない。

現時点で iDC を利用することの多い利用形態ないし業務を例示する。運営としては、利

用者自身がシステムを構築し保有する形態、アプリケーション自体もアウトソースしてASP(Application Service Provider)を利用する形態などが考えられる。

☆ 消費者向け電子商取引(いわゆる BtoC)

☆ フロントオフィス業務(ASP 形態を採用すると思われる)

☆ コミュニケーション系業務(メール、グループウェアなど)

日本においても近い将来、データを iDC に保管して、業務で使う部分だけ自社システムに取り込む、あるいは、企業間取引(SCM)を iDC 上で完結する、というような利用形態が広く普及すると考えられる。

◇ ストリーミングデータ配信

◇ 大量データの保管とバックアップ

◇ 顧客情報管理とサポート(CRM)

◇ SCM に代表される企業間データ交換(いわゆる BtoB)

SCM：Supply Chain Management

CRM：Customer Relationship／Resource Management

その場合、iDC が専用の高速回線で相互に結ばれ、膨大な規模のストレージを保有して、自営よりも信頼度が高くなることが前提である。逆に、絶対に情報・データを外へ出すことができない、ないし、許されない業務は、今後とも iDC を利用するのが不可能ないし困難である。

第 2 章　ガイドラインの構成

第２章　ガイドラインの構成

適切な分野・局面で本ガイドラインが有効に活用されるよう、対象範囲や制約、指針全体の構造、利用上の注意事項などを示す。

2.1　選択指針の前提

（1）サービス構成要素

前述のように iDC のサービス構造は事業者によって異なり、全事業者に通用する標準的な構成・構造は存在しない。一方、選択指針としては全ての iDC 事業者を対象にする必要がある。そのため選択指針の共通の枠組としてサービス構成要素を、ファシリティ、コネクティビティ、ハウジング、ホスティング、ストレージ、サービス基盤、運用およびプロフェッショナルに分類し、その各々の範囲内で排他的に選択の指針を示すこととした。ただし、サービス基盤と運用およびプロフェッショナルは今回の指針から割愛した。

サービスを実現する仕組みには各社のノウハウが反映されており、同列には論じられないが、iDC 内のネットワークとサーバやストレージなどについて本ガイドラインでは図 2.1 の構造を想定した。なお、認証・課金システムと管理・監視システムは今回の指針の対照外である。

図 2.1　iDC システム構成例

（2）iDC サービス評価の枠組

利用目的・形態によって選択の際に着目する項目は異なるので、各サービス構成要素の

選択指針も幾つかの視点で更に分類することにした。ここでは、a.パフォーマンス(望み通りに使えるか)、b.拡張性(速やかに増やせるか)、c.可用性(使いたい時に使えるか)、e.セキュリティ(安心して使えるか)、f.運用(事業者に任せられるか)、g.契約(サービスは納得のいくレベルか)、h.料金体系(妥当な金額で使えるか)という７つの視点に分ける。サービス構成要素とあわせ、選択指針を二次元の表に整理することができる(図 2.2)。なお、セキュリティと運用は基本サービスとして提供される範囲内に限定する。

選択視点 / 構成要素	パフォーマンス	拡張性	可用性	セキュリティ	運用	契約	料金体系
ﾌﾟﾛﾌｪｯｼｮﾅﾙ							
サービス基盤							
運用							
ストレージ							
ホスティング							
ハウジング							
コネクティビティ							
ファシリティ							

図 2.2　iDC **サービス評価の枠組**

（3）公的･準公的制度への準拠

消防法や建築基準法など主として建物と付帯設備に関して法律で定められている規定は遵守していることを前提としている。それ以外に iDC を営む上で取得しておくのが望ましい、各種の認証プログラムや制度が政府や各組織団体によって制定されている。特に重要な制度を次表に示す。

表 2.1 iDC **に関わりのある各種制度**

名称	認定団体	内容	備考
電気通信事業者	総務省	電気通信事業を行うのに必須。 第１種､特別第２種､一般第２種に分類。	少なくとも一般第２種取得
情報通信ネットワーク安全・信頼性対策実施登録規定	総務省	電気通信事業者に対する安全／信頼性制度。A 種(第 1 種､特別 2 種)、B 種(一般 2 種)、C 種(一般 2 種上級)	iDC の場合、C 種の取得が望ましい
ISO/IEC17799 (JIS17799、BS7799)	JIPDEC (経済産業省)	情報セキュリティ管理全般に関する国際的な第三者適合性評価制度､民主導の ISMS(情報セキュリティマネジメントシステム制度)として整備	下記取得事業者は経過措置あり
情報処理サービス業情報システム安全対策実施事業所認定制度	同上	情報処理サービス事業を営む事業所毎に付帯設備から情報システムまで遵守すべき安全対策を規定	2001 年 3 月末で廃止、ISMS へ移行
プライバシーマーク	同上	個人情報を扱う電子システムを対象としたセキュリティ認定プログラム	
システム監査基準	経済産業省	情報システムの信頼性､安全性及び効率性向上を図るため､システム監査に必要な事項を網羅	
ISO/IEC15408	IPA (経済産業省)	製品やシステムのセキュリティ品質を客観的に評価するための基準	IPA のセキュリティ評価認証プロジェクト参照

上記各制度と本ガイドラインは評価の視点が異なるので、枠組みおよび項目は一致しない。ISMS と安対制度は、概ね本ガイドラインのセキュリティおよび運用(一部)に該当するが、パフォーマンスや拡張性などその他の視点には殆ど触れていない。

2.2　ガイドラインの使い方

（1）iDC 選択指針の組み合わせ

前記のようにサービス構成要素を排他的に分類し、その各々について選択指針を示しているので、特定の事業者の具体的なサービスを評価する際には、図 2.3 のように該当する構成要素に対する指針を組み合わせて用いる。

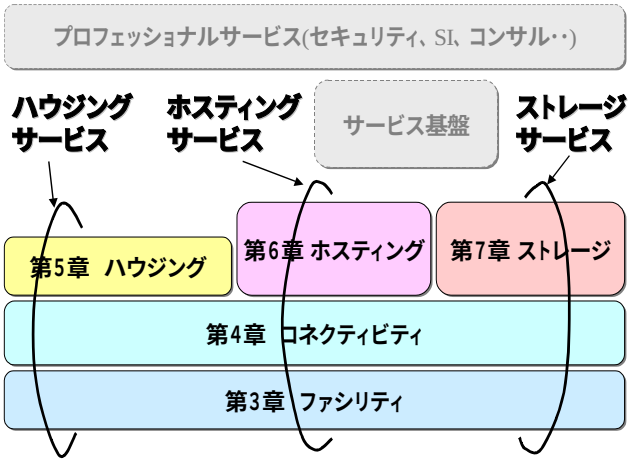


図 2.2　iDC 選択指針の構成

例えば、ハウジングサービスは第３章、第４章、第５章の指針を参照して iDC を選択する。ホスティングサービスとストレージサービスも同様であるが、相対的にファシリティとコネクティビティの比重は小さいであろう。

多種多様な利用形態に唯一の選択指針を示すことは不可能である。本書ではある程度汎用的な指針として、具体的な場で iDC の利用者が適切な項目を活用する方式とした。

（2）目的に応じた項目の選択

選択の際に考慮すべき項目を細かく分解すると膨大な量になる。それらを全て評価するのは困難であり、投入する労力に比べ得られる成果は少ない。ここでは利用者の視点で鍵となる主要な項目に絞りこむこととした。

同様のことは iDC を選択する際にも云える。即ち、iDC 利用の目的、即ち、利用形態(アプリケーション)と利用局面(顧客向けか社内向けかなど)を明らかにすることにより、前述の iDC サービス評価の枠組において特に重視するべき枠を決めることを推奨する。例えば、ストレージの拡張性とコネクティビティのパフォーマンスに着目するとか。各枠内の個々の項目についても同様の手順を踏んで、重点評価項目を選ぶのが望ましい。その他の枠および項目は補助的に参照すれば効率的に選択することができる。

（3）導入または参考資料として

評価項目を主要なものに絞り込むにあたり、その解説を充実させるよう努めた。特に、サービス提供者には自明のことでも利用者にとっては馴染みの少ない用語に留意している。従って、iDC 一般について調べる際の導入あるいは手掛かりに本ガイドラインを活用できるように考慮している。

2.3 選択基準項目一覧

インターネットデータセンターのサービス評価枠組

評価分類 / サービス	パフォーマンス	拡張性	可用性	セキュリティ	運用	契約	料金体系
評価の視点	望み通りに使える	速やかに増やせる	使いたい時に使える	安心して使える	速やかに対処できる	保険をかけるか否か	妥当な料金で使えるか
ストレージ	ﾁｬﾈﾙ転送能力	LU追加とLUサイズ	冗長設計(電源、パス切替)	不正ｱｸｾｽ監視	監視(容量、トラフィック等)	容量の増減	使用容量
	ﾊﾟｽ制御方式	ｵﾝ中ストレージ増設	無停止保守部品交換	LUセキュリティ	バックアップ		バックアップサービス
	ﾃﾞｨｽｸｼｰｸﾀｲﾑ	ｵﾝ中利用ﾕｰｻﾞ拡張	無停止FWバージョンアップ	スイッチのゾーニング	ストレージ運用管理		運用管理サービス
	ポート当りサーバ数	SAN/NAS	バックアップ機能	バックアップ媒体	データ移行サポート		
	コントローラ当りHDD数		バックアップサービス				
ホスティング	利用形態と性能	オープン化	ホットスタンバイ	バージョン及びパッチ管理	ヘルプデスク	サービス開始	基本＋付加
	各サービスの性能	クラスタリング	二重化	アクセス制御	監視(障害、リソース、性能)	サービス利用期間	リソース/OS別料金
	性能管理機能	動的再構成機能	フォールトトレラント	アカウント管理	バックアップ	SLAと補償	パッケージ化
	ハードウェア基本性能	構成管理機能	地理的分散	設定管理(プロセス、サービス)	ログ収集		
	データベース性能			ID/パスワード管理	再起動サポート		
	ファイヤウォール性能			IDS導入	改版/パッチ適用		
	ネットワークサーバ性能			アクセスログチェック	設定変更		
	分散システム稼動性能			ウィルス検知システム	障害通知		
	パフォーマンス評価			機密情報漏洩対策	障害切分/復旧		
コネクティビティ	顧客力バレッジ	バックボーン容量	ファイバー/回線多重化	セキュリティポリシー	(障害管理	SLA(料金払戻、	課金方式(95%ルール)
	相互接続/ピアリング	最大加入者帯域	冗長経路切替方式	不正侵入監視	トラフィック管理	監視主体、監視方法)	保守回線費用
	帯域/遅延/ゆらぎ	初期帯域倍増所要時間		暗号化	運用情報開示	機会損失保険	
	私的閉域網			緊急時の対応策	計画停止の通知		
	IPアドレス数			ファイアーウォール			
	経路制御方式			VPNサービス			
	IPv6						
ハウジング	サーバルーム面積	スペース拡張性	共用ラック・専用ラック	監視レベル	監視サービス	運用のSLA	課金単位
	課号方式	電源拡張性	付随のNWサービスの種別	アクセスログ監視	再起動サポート		(ラック、ケージ、スペース)
	・面積(スペース貸し)	拡張単位	代替センター	入退室管理	サービスデスク		パッケージ化
	・ラック数(ケージ貸し)	拡張所要時間	データバックアップ	専用・共用エリア	付加サービス		初期費用・月額費用
	・段数(ラック貸し)	回線引込み管路数		サーバルーム監視カメラ			
	営業時間帯			ラック/ケージ施錠			
ファシリティ	拠点(数、海外)	法規制/敷地面積	交通手段	センター所在地	定期点検・保守	保証範囲(免責事項)	
	床荷重	空床面積	代替センター	建物構造	日常点検・保守	補償内容	
	受電容量	引込み管路数	耐震/免震能力	集中監視システム	稼動監視	稼働率(99.99%)	
	空調稼動時間	MDF室広さ	受電方法	24時間×365日監視体制	異常・障害報告		
	温度・湿度調整	サブの受電容量	電気設備/経路多重化	監視カメラ			
	作業スペース/仮眠施設	縦シャフト(スペース)	非常用バックアップ発電機	入退館管理システム			
	非常用設備と避難路	拡張所要時間と費用	発電機用オイルタンク容量	入退出管理			
			点検更新時の停電対応	事前申請・登録・記録			
			CVCF起動バッテリ時間	サーバエリア設置場所			
			消ガス消化システム	電磁波対策			
			通信回線引込み口				

第 3 章　ファシリティ

第３章　ファシリティ

ファシリティは、iDC の立地及び施設と電源設備、空調設備、セキュリティ設備等の付帯設備からなり、コネクティビティと共に iDC が提供するハウジング、ホスティング、ストレージ等の各サービスを支えるベースを成すものである。

利用者が iDC を選定するにあたって、暗黙の内に重要である思っている点は

①システムが 24 時間 365 日止らずに稼動すること

②セキュリティ、安全対策が確立していること

③利用者が iDC で快適に作業できること

最近では、iDC が単なるサーバ、機器の自動運転施設であるばかりでなく、利用者が作業するための施設としての面も重要視されるようになってきている。トラブルの切り分け、修復あるいは機能改善のために、利用者の作業が夜中に及ぶことも多々ある。このような観点から、iDC を選択するにあたり、ファシリティの面から、その選択基準を評価分類ごとに検討した。

3.1　パフォーマンス

パフォーマンスでは、容量・性能の観点から iDC のファシリティ要件を検討する。

3.1.1　拠点

iDC の拠点のパフォーマンス要件として拠点の場所、拠点数、海外拠点の有無などがあるが、一箇所の iDC のみ利用する場合は、利用者がアクセスしやすい場所にあることが重要であるだろうし、海外も含めてサーバを複数拠点に分散配置して運用する等の利用形態を必要とするならば、それに対応できる iDC 業者を選定することになるだろう。拠点の場所の地価は iDC の利用費用に跳ね返るため、その兼ね合いで iDC を選定することになる。

3.1.2　建築

iDC の建物のパフォーマンス要件には、建物の階数、延べ床面積、床荷重、フロアの有効高などがあるが、エリアやラックを借りて使用する通常の場合においては、iDC 選定の重要な要件ではない。

参考値として、床荷重は一般用 iDC のラックエリアとして 500～750Kg/㎡程度、ストレージエリアには 1,000Kg/㎡程度である。

3.1.3　電気設備

iDC の電気設備のパフォーマンス要件には、受電方式、受電容量、テナント内への UPS の設置等がある。電気設備の典型的な構成を図 3.1 電気設備概念図に示す。

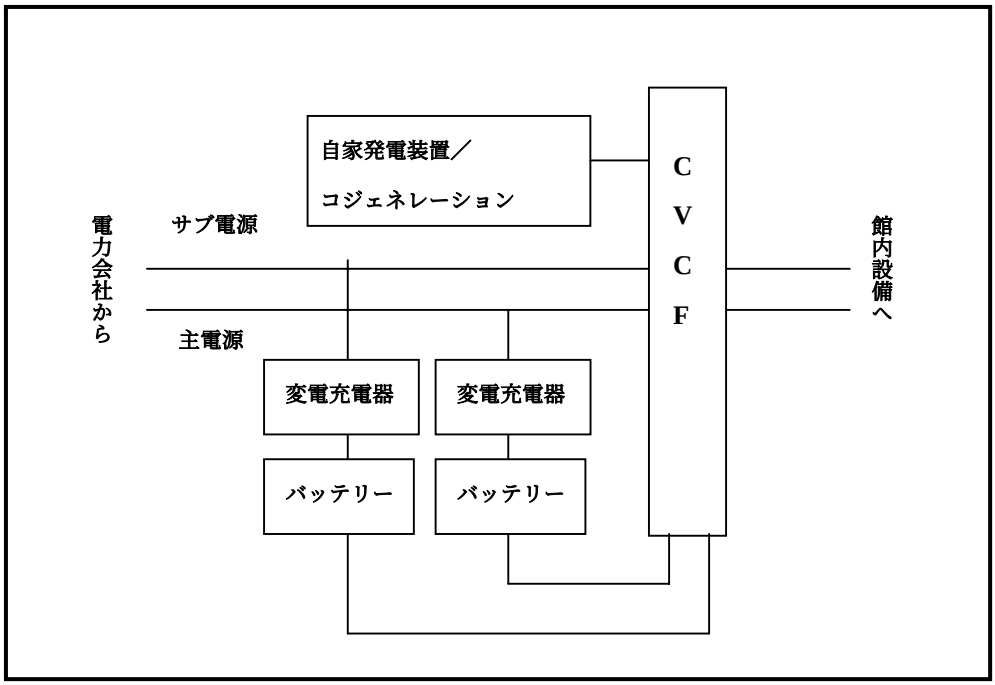


図 3.1 電気設備概念図

電力会社から来た主電源とサブ電源は、CVCF に接続されると同時に、変電充電装置を通してバッテリにもつなげる。主電源が停電すると CVCF でサブ電源からの供給電源に切替わる。主電源とサブ電源がともに停電状態になると CVCF でバッテリーから供給される電源に切替わる。バッテリーが供給できる時間は数分程度であり、その間に自家発電が作動する必要がある。

受電方式としては、首都圏ではスポットネットワーク方式（22KV）、地方においては本線、予備線 2 回線受電方式（6KV）が一般的であるが、iDC 選定のための決定的な要因とはならない。

参考までに、受電容量は、マシン電源容量、付帯設備電源容量、コージェネシステムの有無、将来性等を考慮して算出することになるが、平均的には 500～1,000VA/㎡くらいである。

サブ電源の受電容量が主電源の受電容量と同じ場合には問題はないが、サブ電源が主電源の何%かの容量しかない場合は、電気系統の定期点検時にサーバを止めることにならないかどうかを確認する必要がある。

テナント内に UPS の設置を希望する場合は、ビルに設置されている UPS 容量総量を確認し、テナント内の UPS 使用管理は iDC 側なのか使用者側なのかを確認した後、契約時に希望する UPS 電源容量を明示する必要がある。

3.1.4 空調設備

iDC の空調設備のパフォーマンス要件としては、空調容量、空調方式、空調機タイプ、空調稼働時間、温度調整、湿度調節等があるが、利用者側で選択できない要件も多々ある。

利用者が iDC 選択の条件として考慮すべきことは、空調稼働時間が 24 時間連続運転であるかどうか、静電気によりマシンの故障が発生しないようにするためにサーバ室の湿度が 40～60%程度に保たれているかどうか、サーバ機器の故障と寿命を縮める原因とならないよう温度が 22±2℃に保たれているかどうかである。ただし、サーバ室内の温度は一定でなく、場所によって差があるため、ラック毎に温度センサーをつけて温度監視をするようになっているかどうかをチェックしたい。

温度については、iDC 内で利用者が作業するときのことも考慮して、事務作業室、仮眠室などユーティティ部分では 25℃程度に保たれていればなお良い。

3.1.5 ユーティリティ

iDC は利用者が導入、バージョンアップ、トラブルシューティング等の作業をする場でもあるため、事務作業室、ベンダーマシン等の設備があると良い。これらの作業は夜中に行われることも多々あるため、できれば仮眠室などの設備があればさらに良い。

3.2 拡張性

利用者は、業務の拡大によるサーバの増設、通信容量の拡大等を考慮して、拡張性を備えた iDC を選定する。利用者が拡張を申出た場合に、時間と費用がどの位かかるのかを予めチェックしておく必要がある。即ち、利用者が将来想定される拡張の数値を iDC 事業者に具体的に示して確認する。例えば、サーバを 2 倍、10 倍にするときに必要な時間と費用、同様に通信容量を 2 倍、10 倍にする時の時間と費用を iDC 事業者に確認する。ファシリティの充分な拡張性を備えた場合は、その遊休設備の費用も iDC の利用料に配賦することも考えられる。一般の iDC 事業者は拡張について発生都度対応しているようである。ここでは iDC の拡張要件として考えられることを記述するにとどめる。

法的な規制を受けずに建物の増築が可能であるだけの敷地面積に余裕があるか。また、建物の増築までいかなくとも、延床面積の空き、サーバルーム面積の空きがあるか。通信回線の増設のために、通信ケーブルを収容する引き込み管路数の余裕と MDF、交換機、バッテリー、PD 盤等を収容している MDF 室の広さに余裕があるか等。

参考値として、管の太さと収容ケーブル数の関係、MDF 室の広さと収容ケーブル数の関係を示す。

（管路工事参考値）　・メタル 200P×4 本では、配管太さφ100×１本
・光 100P×8 本では、配管太さφ100×１本

（MDF 室参考値）　・メタル 1000P クラスでは、20 ㎡
収容機器（MDF、交換機、バッテリー、PD 盤等）

次に、縦シャフトおよびスペースについても、参考値を示す。

個数：１ヶ所／200 ㎡～300 ㎡
開口大きさ：配管（100φ×２本）／１ヶ所

あるいは、ダクト（200×300 程度）／１ヶ所

他に、受電容量の余裕、空調容量の余裕、冷房負荷の余裕などもある。

3.3 可用性

可用性では､iDC を何時でも使える状態にしておき､利用者が必要なときに何時でも iDC を利用できるためにどのような要件があるか検討する。可用性を上げるために、次の対策を施すことは、iDC 事業者の費用増となり、ひいては利用者の費用負担に転化することも事実である。iDC を利用してエンド・ユーザにサービスを提供する利用者の SLA 及び利用料金との兼ね合いで検討しなければならない。

3.3.1 立地

iDC の立地の可用性要件には、自然災害の防御、代替センター、利用者のアクセスのし易さ等がある。

立地については、iDC が自然災害（地震・火事・洪水・土砂崩れ・雪崩等）の発生する恐れのないところに位置しているか、電力・上下水道・通信等のインフラの引き込みが容易である所に位置しているか､代替センターがあるかなどが iDC を選択する上で考慮すべき点である。

利用者の iDC への物理的なアクセスのし易さは重要なポイントである。24 時間 365 日運用を前提として iDC を利用する場合、問題発生時に直ぐ iDC に行って問題解決にあたれる場所に位置していることは重要である。従来、iDC はネットワークコネクティビティの向上を図るため IX(Internet eXchange)の近くにあることが重要視されたが、通信料の値下げ及びブロードバンド化が進むと IX との距離の問題は解消できると考えられ、利用者の近くにあることがより重要になる。

交通手段の要件としては、iDC から最寄り駅までの距離が徒歩 10 分以内であればベストであり、最終電車が遅くまである方が良い。iDC の近くに、食堂やコンビニなどがあれば、利用者にさらに便利である。

3.3.2 建築

iDC の建築の可用性要件には、ビルの構造、耐震性、免震性、マシン室の構造、非常用設備等がある。

ビルの構造としては、SRC 造（鉄筋鉄骨コンクリート造）または RC 造（鉄筋コンクリート造）でかつ無窓構造であり、阪神淡路大震災級の地震（600gal）に耐えうる耐震性基準を満たしていることが望ましい。免震構造については、2 次元免震、3 次元免震の免震構造であることが望ましい。また、ビルそのものが耐震構造でなくとも、耐震二重床（フリーアクセス)を敷設することにより､サーバラックは床スラブへ固定することなく十分な耐震性を得ることができる。ただし、利用者が費用を負担する場合があり、標準費用にどこまで含まれているのかをチェックするべきである。

非常用設備および避難路については、非常用照明、誘導灯の設置、避難方向は２方向が原則であり、避難通路の巾は１．２mを遵守している必要がある（建築基準法・消防法の遵守）。

3.3.3 電気設備

iDC の電気設備の可用性要件には、電源幹線、無停電電源装置、非常用バックアップ発電機等がある。次に記述する要件を満たすほど可用性は上がるが、利用者として如何ともしがたい項目も多い。利用者にできることは、自分のシステムがどういう条件のときに運用不可能になるかを確認し、その状態からどれくらいの時間内に復旧できるのかを iDC 事業者に確認することくらいであろう。参考までに、iDC 事業者が可用性を上げるために考慮している項目を列記するにとどめる。

ビル内の電気室からマシン室までの電源幹線は、災害時の断線や幹線ケーブルの絶縁劣化等により交換が必要となるなどの災害対応として、2 系統を別経路でマシン室に引き込む、また、あわせて幹線ケーブルの保護と電磁防止対策を施す、という対策がとられていれば可用性が上がる。

非常時にしばらくの間電気を供給するための無停電電源装置の容量は、最重要機器であるマシンとオペレータ機器の電源容量で決める。また、無停電電源装置の設置台数は、故障・メンテナンス・オーバーホールの際の対応として、予備機を１台設置(N+1 構成)する。

同じく非常時に必要な電源を供給する非常用バックアップ発電機の容量は、一般に次の算出式で求められる値以上ならば充分である。

発電機の容量 =（マシン電源容量+付帯設備電源容量）×安全率＋将来見込み分

多くの iDC は将来見込み分については、マシンの増設に合わせて、その時点で発電機も増設する。非常用バックアップ発電機は、停電時に自動的に運転するように構成する。通常、発電機の設置台数は、故障、メンテナンス、オーバーホールの際の対応として、予備機を 1 台設置（N+1 構成）する。

発電機用オイルタンクの容量は、災害時に保有するデータを別のデータセンターへ移すための必要な時間を算出し、その時間をカバーできる燃料の備蓄をおこなうことができるようにする。また、備蓄量の算出方法としては、マシン及び付帯設備への電源連続供給時間と発電機の燃料消費量から保有量を算出する。補給基地（コンビナート等）との運送距離も考慮して、適切な容量とする。但し、消防法による上限が規定されている。

さらに、電源設備（特高受変電設備、発電機、UPS 設備）の定期点検または更新・増設などを実施する場合、停電が必要となる。その際にマシン側に影響がないよう、停電用の仮設電源を接続できる電源切替盤が使用される。

電圧・周波数を安定化した電源を得るための CVCF の設置場所は、消防法・火災予防条例等を遵守し、バッテリーからの腐食性ガスの影響を考慮して、専用の電源室に設置する。

CVCF 起動装置タイプとしては、常時起動タイプを使用することにより CVCF の 24 時間連続運転を実現する。CVCF 起動装置バッテリー時間は、発電機が立ち上がるまでの時間をカバーする必要があり、通常数分間の連続給電ができるようにする。

過電流、漏電対策として、過電流遮断器、漏電警報器、漏電遮断器をサーバ用、空調用の回路毎に設ける。

3.3.4 その他

その他の可用性要件としては、自動火災報知システム、消火設備、地下埋設光ファイバー・同軸の引込み場所等がある。これらの項目も iDC の利用者には如何ともしがたいものが多く、参考までに iDC 事業者が可用性を高めるために考慮する項目を列記することにとどめる。

iDC の可用性を高めるためには、マシン室、事務室、電源室、空調室等に個々の消火設備を設置する。最低でも、マシン室用は他室との共用を避けて、個別に設置している。

自動火災報知システムは、防災システム全体構想を考慮して最適なシステムが選定されていれば、可用性は上がる。単に消防法で火災感知システムだけでよいのか、超高感度煙感知システムと併用した方がよいのか、消火設備（ハロン、二酸化炭素）との連動をどうするのかなどを考慮している。

消火設備についても、自動消火設備、消化器、消火栓・スプリンクラー等あるが、消火栓・スプリンクラーを使用した場合の二次被害が多大になるため、消化の順序としては、①消化器、②ガス消火設備、③消火栓・スプリンクラー順にする。また、自動消火設備（ガス）としては、ハロンガス（オゾン層の破壊）、二酸化炭素（地球の温暖化）などよりも、初期費用・設置スペースの問題はあるが、窒素ガスを使用する。消化器にしても窒素ガス使用のものが使われる。

地下埋設光ファイバー・同軸の引込み場所などの通信回線の引込みは、災害時に１系統が切断しても、もう１系統が継続して使用できるように、２系統を別々の局から経路も別にして埋設管で対象フロアに引込むことで可用性を上げる。また、構内への引込み場所も別々の２個所にする。

3.4 セキュリティ

セキュリティでは、安全性確保のための拠点、建物、管理・監視設備等の物理的な設備・機器とそれら設備・機器の安定運用を維持する点検作業（人間系）の要件項目がある。

3.4.1 拠点

拠点のチェックすべき点としては、敷地内への不法侵入、建物等の破壊行為を防止するため、敷地境界において入退管理を行う場合は塀または柵を設けているか、必要に応じて侵入防止装置を設けているか。

3.4.2 建物

建物のチェックすべき点としては、iDC 関連設備を破壊行為等から防御するため、公道等外部に面する外壁等は、強度を持たせているか。また、建物内への不法な侵入を防止するため、外部から容易に接近、侵入できる 1 階の窓等には防犯措置を講じているか。

階数配置としては、1 階（地階含む）は電源設備等々のインフラ設備エリアと考え、侵入防止対策等のセキュリティを考慮して、1 階より上層階にマシーンセンターが配置されているか。

3.4.3 管理・監視設備

入退館管理を確実に行うことによる不法侵入の防止、不審物品の搬出入防止のため、常時利用する出入口は 1 箇所とし、インターホン、防犯カメラ、警報装置などの出入管理設備、防犯設備を設置しているか。

受付のときは、警備員等による入退館者の識別、および予め許可された者以外の所定の手続きによる入館記録がなされているか。また、入退館に際しては、開閉装置により予め設定された入退館資格の識別、記録を行い、扉の開閉を行っているか。

侵入、破壊、機密漏洩等を防止するため、マシン室・データ保管室の室名等の表示は付していないか。

マシン室は、安全管理の徹底のため、専用の独立した室になっているか。

安全性を保ち、外部からの熱、湿気、塵埃の侵入を防止するため、常時利用する出入口には前室を設けているか。防犯、防災のため、窓を設ける場合は、防火・防水措置および窓ガラスの破損防止措置を講じ、さらに外部から室内の機器等が見えない措置が講じられているか。

マシン室の出入管理として、警備員等による入退室者の識別や予め許可された者以外の所定の手続きなどの受付機能の設置、または開閉装置の設置により出入管理がなされているか。

障害発生等を早期に発見するため、電源設備、空調設備、防災設備、防犯設備等の監視制御設備を設置し、中央の一個所でこれらの設備の監視・操作をおこなえるよう集中監視制御設備になっているか。

3.5 運用

ファシリティのパフォーマンス、拡張性、可用性を支える人間系で、内容は主として設備・機器の安定運用を維持する作業である。

3.5.1 定期点検

電気設備､空調設備､消火設備など機器の劣化を事前に検出することを目的に行われる。採用している設備・機器が iDC 毎に異なるので、一律に点検項目を示すことは難しい。法律で義務付けられている点検項目を基に夫々独自の作業基準を追加していることが多い。作業基準の整備状況で適切な iDC かどうか判断することができる。

定期点検は間歇的な仕事であること、専門技術を要すること、場合によっては公的資格

が要件となっていることなどから、概ね外部の専門業者に点検作業を委託している。点検結果は業者の作業記録・報告で確認することができる。

表 3.1 定期点検項目例

機器		項目数	点検項目例
電気設備	受変電設備*1	49	絶縁抵抗測定、動作試験、損傷･腐食･･点検など
	配電設備*2	20	点灯状態確認、端子部清掃、外観の点検など
	負荷設備*3	18	異音･異臭の点検、器具取付け状態点検など
	非常用発電装置*4	68	燃料噴射弁の交換、ブラシ磨耗状態点検、停電試験／自動回復充電試験、蓄電池電圧の確認、など
	無停電電源装置	31	運転試験、切換開閉器の作動確認、通電試験など
	弱電設備	3	音量明瞭度の確認など
空調設備*5		38	エアフィルタ交換、ドレンパン汚損点検及び清掃など
消防設備等*6		22	消防法施工規則第 31 条の 4 の規定に基づいて、外観、機能及び総合点検を実施

（出典：iDC イニシアティブ）

注)*1 ブレーカ／ヒューズ、変圧器、一般高圧分岐盤・電源切換盤類、接地端子など
*2 幹線ケーブル、入力分岐盤・出力分岐盤・分電盤類など
*3 電動機、制御盤・操作盤
*4 原動機、発電機、直流電源装置、蓄電池、など
*5 パッケージエアコン、熱交換器、送風機・排風機など
*6 消火器、スプリンクラー、屋内消火栓、窒素ガス消火設備、自動火災報知機など

なお、運用中断が許されないシステムの場合、電源設備の定期点検時にも機器には電源が供給されるような iDC を選択する。

3.5.2 日常点検

日々のサービスレベルを維持することを目的に行う。天災・人災に起因する障害・異常発生時の対策・復旧なども含む。主に電気設備、空調設備、消火設備が対象である。採用している設備・機器が iDC によって異なるので、一律に点検項目を示すことは難しいが、夫々に作業基準を設けている。ファシリティ設備・機器の点検は基本的に iDC の必須要件なので、作業基準の整備状況で適切な iDC を選択することができる。

上記設備・機器の日常点検例を表 3.2 に示す。記録に残すのは計器類の指示値や重要な機器の状態などである。

表 3.2 日常点検項目例

機器		項目数	点検項目例
電気設備	受変電設備	34	変圧器温度、電力需給状態、開閉指示器の動作状態など
	配電設備	17	ケーブル損傷、電圧・電流・周波数、その他異常の有無
	負荷設備	12	異常振動・異音･異臭、器具取付け状態など
	非常用発電装置	50	油量、エンジンオイル量、冷却水、各スイッチ状態など
	無停電電源装置	19	計器指示値確認、主要部品の異常、漏液発錆など
	弱電設備	2	作動確認など
空調設備		41	冷媒圧力計、温湿度感知器の設定値など
消防設備等		16	変形・損傷・腐食などの有無、障害物の有無など

（出典：iDC イニシアティブ）

3.5.3 稼動監視

ファシリティ設備・機器の 24 時間 365 日の稼動監視も iDC の必須要件である。監視の形態は、iDC 内の常駐要員が行う、遠隔から監視する、各設備・機器の業者へ委託するなど様々である。しかしながら、高い可用性を提供する iDC は、中央監視システムで常時複数のオペレータが監視する体制を採っている。

重要な機器・設備は能力に余裕を持たせてあり、代替機または予備装置へ瞬時に切換えるようになっている。従って、異常検出を見逃さない、速やかに関連部門・事業者へ連絡する、原因究明と復旧および動作確認を行う、などに必要な作業手順が規定されていて、常に実行できるような体制になっていることが重要である。例えば、重要な設備・機器別に責任者が定められている、緊急連絡先が明確になっている、定期的に訓練が実施されているなど。

3.6 契約

建物の堅牢さと電力供給は iDC の生命線なので、ファシリティに関する事項は各社とも個別の契約でなく、契約約款で示されることが多い。ファシリティの SLA としては 99.99%が一つの目安である。これは年間で 50 分強の停止に相当する。実際には実績として無停止の iDC が多いが、計画的に停止する iDC もあるので確認する。なお、ファシリティ全体として SLA が提示されていることが多いが、サーバ等の機器が停止するような状況を意味するので、ほぼ電源供給と考えて良い。

運用停止の賠償金としては、殆どの iDC で月額利用料金を上限として、1 回の停止に対してその何分の 1 かを免除することが多い。どの iDC も利用者の事業機会損失あるいは信用失墜に対する補償を明言していない。個別折衝で解決しているのが実態である。

補償に対して保険で補う動きがある。利用者が保険契約者となる場合と、iDC 事業者が保険契約している場合があり、それによって補償内容が異なる。

天災や戦争など不可抗力な事件に起因する稼動停止に対する免責基準はまだ各社各様と推測される。被災範囲や損害規模によっても判断が変わると考えられる。

3.7 料金体系

ファシリティとしては料金体系が決められていない。ここではファシリティと料金の関係を定性的に示すに留める。

3.7.1 建物の仕様と料金

建築の仕様の高低は建設コストに跳ね返り、最終的に料金に反映される。建築仕様で最も大きく影響するのが床荷重である。収納密度を予想して適当な床荷重の iDC を選ぶのが望ましい。ちなみに、サーバエリアの床荷重は、既設ビル改造の場合に 500Kg/㎡前後、新設の場合で 700Kg/㎡程度、最も高仕様で 1,000Kg/㎡であることが多い。

耐震性・免震性確保の所要コストも大きい。特に免震装置は高価である。しかしながら、

iDC 選択が立地条件に大きく左右され、日本の場合交通の便などを考慮すると埋立地や河川近辺を避けられないことから一律には判断できず、選択基準に採用し難い。

3.7.2 電源設備と料金

22KV スポットネットワーク方式と 6KV の 2 回線受電の、受電方法の違いによる総コストの差はあまり大きくない。概ね iDC の規模で決まるが、電源供給の安定性の面から 22KV スポットネットワーク方式が優れている。66KV(関東)または 77KV(関西)給電は別格で、極めて大規模または高い品質の iDC が対象である。

非常用発電機の有無と規模、および定電源装置の有無と規模は iDC 構築コストに大きく響く。日本では長時間停電の恐れが少ないので、運用を一時停止しても差し支えない利用形態の場合、非常用発電機を省略し、CVCF の稼動時間も最小限にして、料金を低く抑えた iDC を選択することも考えられる。

3.7.3 運用体制と料金

いかに小規模な iDC でも 24 時間 365 日の安定稼動にはある程度の要員を確保しなければならない。iDC の規模拡大とともに要員を増加する必要があるが、一般にその率は規模拡大よりはるかに小さい。そのためフロア面積当りの運用費用は規模拡大と逆に減少すると云える。

3.8 まとめ

iDC を選定する上でファシリティとしての必須要件、推奨要件、検討対象外要件等に明確に分類することは難しい。利用者は、通常スペースやラックを賃借するかたちで、iDC を利用する。このような利用形態においては、ファシリティ項目である建物、電源設備、空調設備、セキュリティ設備等を他の利用者と共同利用することになる。

一般に iDC 事業者は、ハウジングやホスティングなどの利用料金を標準料金とオプション料金（利用者の要望により特別に設備する部分の料金）に分けている場合が多く、オプション料金は標準料金に比べて極端に割高になる場合が多い。利用者としては、自分が運用するサービスの SLA に照らして、なるべく標準利用料金の範囲でサービスを受けられる iDC を選ぶことが料金を安く抑えることにつながる。

iDC がサーバ機器の自動運転施設であるばかりでなく、利用者が作業するための施設でもあることも考慮すると、立地、ユーティリティ設備、人が作業していることを前提にした空調・温度設備、消火システム等が充実していることが iDC 選定の重要な項目になりつつある。また、セキュリティポリシーが確立していて、それに沿って日々の運用がなされていること、各設備等の第三者による監査が定期的に実施され、監査結果により改善がなされていることは重要である。

第 4 章　コネクティビティサービス

第４章　コネクティビティサービス

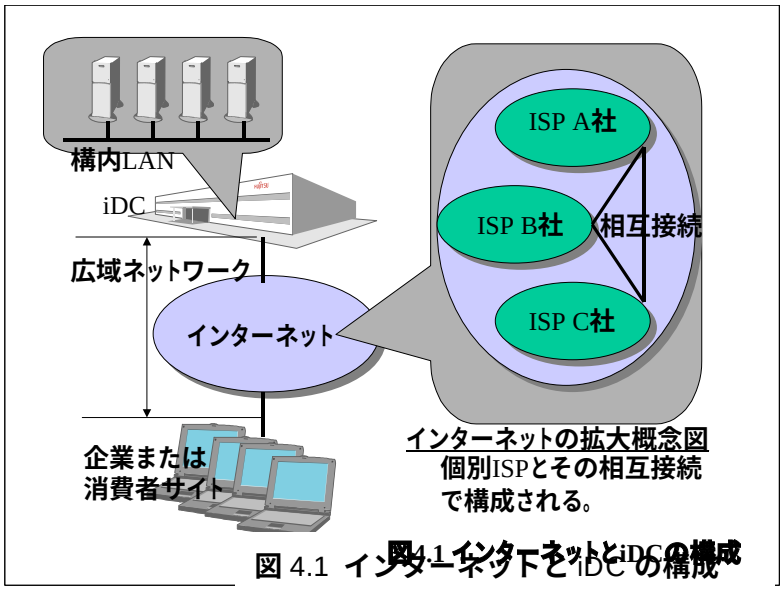


図 4.1 インターネットと iDC の構成

iDC を選択する上で iDC がもつネットワークに着眼することは大変重要である。iDC 加入者はインターネットを通じて世界に分布する顧客にオンラインサービスを行うため、顧客がオンラインサービスを利用したときの経験はこのネットワークの品質によって大きく左右される。iDC のネットワークは主にセンター構内 LAN とインターネットの一部としての広域ネットワークからなる。特に顧客の利用経験を左右するのは広域ネットワークであるため本稿では広域ネットワークについてより詳しく論ずる。これらのネットワークおよび iDC の概観を図 4.1 に示す。インターネットの中ではおのおのの ISP が独立して存在し、お互いに緩やかな相互接続を行っている。各 ISP は自社内のネットワークの機器を自社保有し、完全に自社の管理下においている。一方相互接続は複数の当事社間の合意により行われ、その管理レベルは合意の範囲内にとどまる。更に相互接続の先は他 ISP 所有のネットワークであるため管理権限は全く及ばない。

4.1　パフォーマンス

4.1.1　単一 ISP による顧客カバレッジ

全ての iDC 加入者にはそのサービスを提供する顧客がある。iDC ネットワークの詳細を検討する前に、まずその顧客の分布について考える必要がある。あらかじめ顧客の ISP への分布がわかっていると仮定しよう。図 4.2 の例では、顧客の 80%が ISP A 社に接続し、20%が ISP B 社に接続している。シナリオ 1 として ISP A が運営する iDC または ISP A に対して加入者関係にある iDC にサーバを設置した場合、80%の顧客が単一 ISP 内による接続となる。一方シナリオ 2 として ISP C が運営する iDC または ISP C に対して加入者関係にある iDC にサーバを設置した場合、顧客の単一 ISP 内カバレッジは 0%となる。前述のように単一 ISP 内の接続は ISP が自社所有の機器で行うため、回線プロビジョニング、障害管理、トラフィック管理が行き届いている。このため多くの場合品質のよい接続が期待できるほか、障害時のクレームに対して ISP は直接対処可能である。従ってできるだけ多くの加入者が単一 ISP で接続できることを、まず第一に考える。

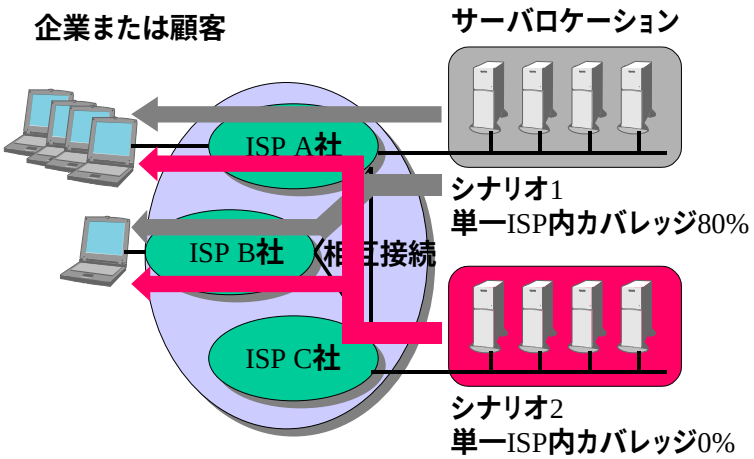


図 4.2 サーバロケーションシナリオ

次にどうすれば単一ISP内での顧客カバレッジを上げることができるか例を挙げて検討する。特定参加者の B-to-B サイトならば顧客の属するISPを全て調査することができる。消費者向けサイトであっても既存の接続ログがあれば、アクセス数の多いISPを割り出すことができる。何も事前資料がない場合でも例えば「日本語サイト」という特性があれば、国内からのアクセスが圧倒的に多く日本国内を本拠とする ISP が外国本拠のISP よりは単一 ISP 内カバレッジが良いと推定できる。表 4.1 に主要なサイトの単一 ISP 内カバレッジ最大化方法例を挙げる。

表 4.1 単一 ISP 内顧客カバレッジを最大化する方法例

サイトの顧客分布	選択すべきiDC
特定顧客向けサイト	対象となる特定顧客が接続しているISPを調査し、最も顧客が多いISPが運営するiDCまたはそのISPと加入者関係にあるiDCを選択する
不特定顧客日本語サイト(既存)	http logからアクセスの多い上位ISPのいずれかが運営するiDCまたは、そのISPと加入者関係にあるiDCを選択する
不特定顧客日本語サイト(新規)	国内ISPが運営するiDCまたは、そのISPと加入者関係にあるiDCを選択する
不特定顧客北米、欧州向けサイト	北米本拠の国際ISPが運営するiDC、またはそのISPと加入者関係にあるiDCを選択する
不特定顧客アジア向けサイト	国内ISPの中で東南アジアにバックボーンを保有するISPまたは、東南アジア本拠の国際ISPが運営するiDCまたはそのISPと加入者関係にあるiDCを選択する。
顧客分布が世界均一である場合	相互接続を重要視する

単一 ISP 内では一般的に安定的に高品質が期待できる他、今後は SLA が可能な範囲となりうる。単一 ISP 内では常に事業者間相互接続よりもレベルの高い品質管理が可能であり、どの時代にも一歩リードした品質や契約が提供されてゆくであろう。

4.1.2　事業者間相互接続

ネットワーク選択の最初のポイントは自社所有されている単一ISP内ネットワークでできるだけ多くの顧客カバレッジを得ることであった。次にここから漏れた顧客について考える。その選択ポイントとなるのがiDCを運営しているISPまたはiDCが加入者関係にあるISPの相互接続状況である。イントラISPでの顧客カバレッジが低い場合、つまり顧客分布にあまり偏在がない場合はより重要な選択項目となる。顧客分布が国内型の場合は国内の主要IXへできるだけ多く接続しているISPを選択する。他地域の場合はその地域のIXに直接接続しているかその地域を本拠とするトランジットを契約しているISPを選択する。特に北米地域では、公衆IXの交換品質が悪いのでプライベートリンクによるピアリングをしていることが重要である。相互接続の見方はISPの地位によって異なる。以下簡単な分類を示し、各々について相互接続の見方を示す。

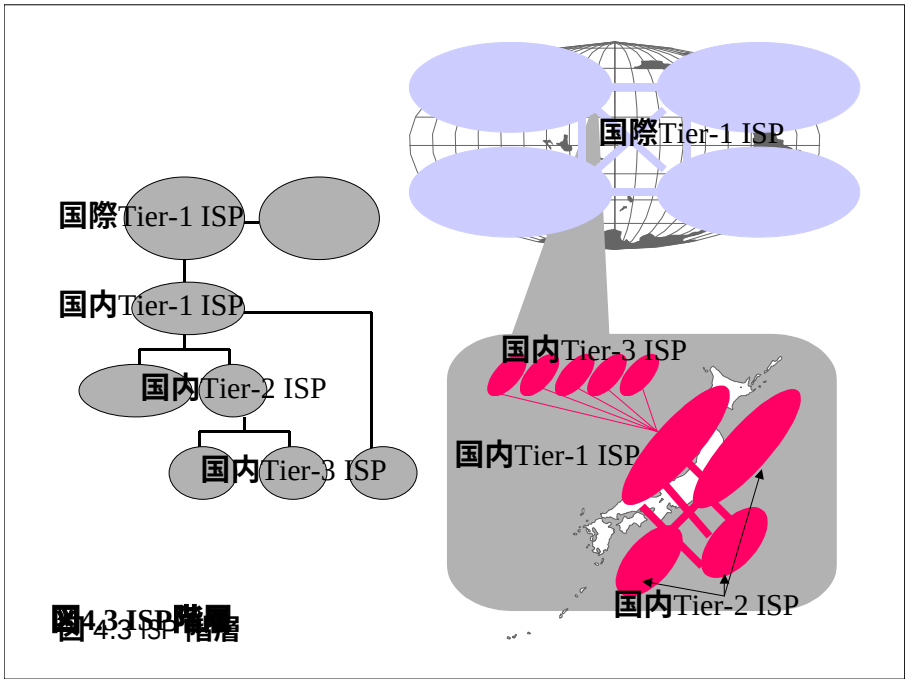


図4.3 ISP階層

図4.3に示すようにISPはそのネットワーク規模と経路収集の仕方で、国内的な視点からは国際Tire-1から国内Tier-3までの四つの階層に分かれる。Tier-1は上位のISPであり、インターネットのバックボーン部分をなし、Tier-3は周辺をなす。一般に国内Tier-1 ISPは一次プロバイダー、国内Tier-2,3は二次プロバイダーとも呼ばれる。Tier-3,Tier-2 ISPは上位のISPに対して加入者関係となる。より多くの有効な相互接続を得るためにはなるべく上位のISPを選ぶ。相互接続特性は別階層のISP間で比較しても意味はなく同一階層ISP間で比較する。表4.2に示す比較ポイントに従ってISPが運営するiDCまたはそのようなISPに対して加入者関係にあるiDCを選択する。

特定大口顧客であって単一ISPでカバーできなかった場合はその顧客が接続している特定ISPとの相互接続が重要になる。その特定ISPが同一のIXに接続しているかどうか、また海外の場合は同一トランジットを使用しているISPが運営するiDCまたはそのようなISPと加入者関係にあるiDCを選択する。事業者に新たな相互接続を要求することも検討に値する。

iDC にはキャリアフリーと呼ばれるものと、ネットワークエッジにあって極めて多数のマルチホームを行うものとが希に存在する。ポリシーとしてキャリアフリーだとしても現実的に選択できる ISP は限られており、その選択基準は現実に使用できる ISP で決まる。また多数のマルチホームを行う iDC は自社バックボーンを持たず、相互接続が極めて強力な iDC であるため、客が不特定多数であってしかも全世界に拡散しているサイトに適している。例えばオリンピックサイトなどがその例として挙げられる。

表 4.2 ISP クラス別相互接続特性の評価基準

ISP分類	特徴	相互接続特性
国際Tier-1 ISP	デフォルトルートのないインターネットコアに参加する多国籍ISP	・相互接続数 ・加入者関係にあるISP数
国内Tier-1 ISP	全国的な顧客カバレッジ、加入者関係にあるISPを多数持ち、国内主要IXに参加しているISP	・参加IX数とその接続帯域 ・加入者関係にあるISP数 ・海外における特性はトランジットする国際Tier-1ISPの特性を継承
国内Tier-2 ISP	全国または国内一地域に顧客カバレッジがあり、国内主要IXに参加しているISP	・参加IX数とその接続帯域 ・国内Tier-1 ISPとの相互接続数 ・海外における特性はトランジットの特性を継承
国内Tier-3 ISP	Tier-1または2ISPをアップリンクとする	・アップリンクISPの特性を継承

4.1.3 回線容量絶対値

以上の評価はいずれのアプリケーションにも共通する。一方サービスするアプリケーションに特有なネットワーク品質を考慮する必要がある場合もある。ネットワーク品質は主に帯域、遅延、ゆらぎの 3 つの指標がある。大まかなアプリケーション分類と品質要求を表 4.3 に示す。

アプリケーション上ナローバンド帯域(～64Kbps)だけが重要な場合、iDC 選びの中でコネクティビティ検討の重要性は低い。現在ほとんどのネットワークでナローバンド帯域はベースラインになっている。一方ブロードバンド帯域(256Kbps～)や遅延、ゆらぎが重要になると、iDC 選択基準の中でネットワークの占める重要性は向上する。ゆらぎや遅延の絶対値を定めたい場合、公衆ネットワークの利用は現在では困難である。

表 3 アプリケーション別必要ネットワーク品

表 4.3 アプリケーション別必要ネットワーク品質

アプリケーション	帯域	遅延	揺らぎ
通常のWeb	×	×	×
ブロードバンドWebサイト	○	×	×
ストリーミング	○	×	○
パケット電話／遠隔会議	○	○	○

ベストエフォートの範囲内で遅延と揺らぎを重要視する場合は、回線容量の絶対値が大きい ISP が運営する iDC またはそのような ISP と加入者関係にある iDC を選択する。目安としては自社所有ネットワークや相互接続に十分な投資をしている通信キャリア系の国内 Tier-1 ISP 以上が望ましい。該当する ISP は積極的にネットワーク図とリンク帯域を公表しているのでそのような ISP が運営する iDC を選択する。

また海外に通信衛星リンクをもつ ISP がまれに存在する。静止衛星は地上 36000Km 上空まで電波が往復するので遅延が桁違いに大きい。地域に関わらず 500ms 近い遅延を覚悟しなければならない。従って自社ネットワークの一部を衛星リンクが担っていないことは念のために確認し、衛星リンクを使用する ISP が運営する iDC またはそのような ISP と加入者関係にある iDC は避ける。

4.1.4 私的閉域網

サイトのバックエンドや B-to-B 接続には私的閉域網が利用される。私的閉域網には専用線や広域 LAN サービスが含まれる。これらのサービスが iDC 内から受けられることを確認する必要がある。まず利用できる回線品種が多い方が自社サイトを設計しやすい。また同一回線品種であっても複数の通信事業者を選べる方が価格やサービス詳細を選択できて有利である。

表 4.4 NSP の帯域別サービス例

目標帯域	NSPサービス例
2.4Gbps以上	ダークファイバー 波長サービス SDHサービス
155Mbps～1Gbps	SDHサービス ATMサービス 広域イーサーネットサービス
～100Mbps	Jキャリア専用線サービス ATMサービス 広域イーサーネットサービス ファシリティーベーズドVPNサービス

図 4.4 NSP の帯域別サービス例

表 4.4 に帯域毎のサービス例を掲載する。自社サイトが必要とする私的閉域網の帯域を確認して、その帯域をカバーするサービスが少なくとも一つ導入可能であることを確認する。155Mbps～1Gbps のレンジでは導入可能なサービスの価格が大変重要なキーポイントとなる。現在このレンジでは安価なメニューの普及率が低い。2.4Gbps 以上ではまずアベイラビリティーの確認が重要である。現在これらのサービスのアベイラビリティーは極めて限られている。

4.1.5 取得可能 IP アドレス数

iDC の機能として提供可能な IP アドレス数がある。多数のホスト数が必要なとき、もし追加 IP アドレスが使えないと拡張方法の選択肢が限定されてしまう。iDC から取得で

きる最大 IP アドレス数の確認と自社で取得した IP アドレスを持ち込めるポリシーかどうか確認する。将来を見越して十分な IP アドレス数が確保できる iDC を選択する。

4.1.6 経路制御プロトコル

ほとんどの iDC 加入者はネットワーク的にはその iDC に属する。しかし iDC の中にあって独立した ISP として AS 番号を取得して iDC とは事業者間ピアリング関係になる場合がある。この関係の場合 iDC が加入者との間の経路制御プロトコルとして EGP を提供している必要がある。独立 ISP となる可能性のあるサイトは EGP サービスが可能であることを確認する。

4.1.7 IPv6

IPv6 が今後どのように利用されていくのは本稿出稿時点では定かではない。現在の IPv4 ネットワーク機器はほとんど有効に IPv6 に移行できない。IPv6 が勃興する過程で IPv4 との間に以下の 3 つの関係が考えられる

1. IPv4 とは別網が構成され、iDC 加入者からは物理的に二つのネットワークと見える。
2. IPv4 をトンネルして到達する別網として見える
3. IPv4 と IPv6 のデュアルスタックネットワークとして見える。

以上 3 シナリオのうちシナリオ 1,2 では、現時点で iDC が IPv6 に何らかの備えをしている必要はない。シナリオ 2 では iDC ネットワークと無関係である。シナリオ 1 では必要な時期に iDC が IPv6 網を追加すればよい。新たな網を追加することはそれほど大きな作業とはならない。一方シナリオ 3 では現行 IPv4 ネットワーク改修の必要があるため、現段階で改修を意識したネットワークでなければならない。シナリオ 3 を予想する場合は、IPv6 への移行シナリオをあらかじめ明確化できる iDC を選択する必要がある。

4.2 拡張性

iDC ネットワークの拡張性がどの程度あるか考えるに当たって、自社サイトに必要な初期必要アクセス帯域を見積もる。初期アクセス帯域が 1Mbps の加入者と 100Mbps の加入者では使える iDC が同一でない可能性がある。現在帯域の増強の仕方として「不足したら 2 倍増」という方法を採ることが一般的である。現在の傾向では需要にマッチすると帯域 2 倍増を 4〜6 ヶ月ごとに繰り返すため、どんなに少なくとも初期アクセス帯域から 2 回は増強、つまり 4 倍までは何ら障害なく迅速に増強されることが最低条件である。iDC においても通常の通信事業者と同様、ネットワーク帯域が大きくなるに従って様々な拡張障害が発生する。そのネックになりそうな項目については十分なヘッドルーム（余裕）があることを確認する。ヘッドルームを越える帯域を契約しようとするとできない場合や契約に長期の猶予期間が必要になったりする。

4.2.1 バックボーン接続帯域

拡張性の一つのボトルネックは、加入者全員で共用するバックボーン接続帯域である。例えばバックボーン帯域総量が自らの初期アクセス帯域の 2 倍程度であるとすると、4 倍の拡張性がないことは明白である。いくらあればよいかは加入者総数にもより容易に推定できないが、100 倍程度は必要と考える。例えば初期アクセス帯域が 1Mbps の加入者は 100Mbps 級のバックボーン接続帯域をもつ iDC を選択する。一方 100Mbps を初期アクセス帯域として必要とする加入者は 10G 級のバックボーン接続帯域を保有する iDC を選択する。無論その加入者が iDC の中で際だって大きく、他に大きな加入者がない場合はこの限りではない。

4.2.2 最大契約可能アクセス帯域

加入者に提供されるアクセス部分の最大契約可能帯域も拡張性のネックになる。初期アクセス帯域の 10 倍程度はすでにサービス品目であることを確認しておく。例えば 10Mbps の加入者であれば 100Mbps まではサービスされている iDC を選択する。サービス品目を越える契約帯域も多くの iDC 事業者が応談するであろうが、プロビジョニングに時間がかかるのが普通である。

4.2.3 帯域倍増の所要時間

帯域を 2 倍に増強するのに必要な時間は、ネットワーク拡張性の中で現実的に最も重要な要素である。一般に iDC サービスのスイートスポットを上回ると帯域倍増にかかる時間は増加する。初期帯域の最低 4 倍増までは容易に帯域を拡張できる iDC を選択する。帯域の倍増の猶予期間として即日、または翌日なら多くの加入者サイトが満足できる。一週間以上の場合はきちんとした容量計画が可能な加入者サイトのみ適用可能である。一時的にトラフィックが爆発的に増加する加入者サイトでは契約帯域の 2 倍までは自動的にオーバーサブスクリプション可能なサービスが大変有効だ。ただし、こういったサービスのビットコストは普通高価なので採用する場合は自社サイトのトラフィック集中特性を考えて、費用対効果を事前に検討する。

4.3 可用性

ネットワークの本当の可用性を知ることは難しい。たとえ SLA が契約されたとしても、それが守られそうかどうかは加入者が十分検討するべきである。ネットワークの可用性を上げる一般的な方法は冗長化である。iDC の冗長化ポリシーのレベルをいろいろな要素から推定して iDC 間で相対評価することはできる。冗長化レベルの最高峰は「単一故障によるダウンがないこと」であるが、詳細にみていけば多くの事業者が必ずしもそうではないことがわかる。以下の確認項目についてより多くの冗長化を行っている iDC が相対的に可用性が高い可能性がある。

4.3.1 加入者ポート MTBF

加入者ポートが単一である場合、iDC 側フィーダースイッチの MTBF または稼働率が重要である。MTBF が答えられるかどうか確認する。更に単一加入者に対して二つのフィーダーを別々のスイッチから出すという注文に応えられるかどうか確認する。

4.3.2 ゲートウエイルーターの二重化

主な外部リンクに使用するルーターは二重化されていることを確認する。

4.3.3 物理多重化

iDC から別の iDC, ISP への各物理リンクは多重化されている必要がある。通常 IP ネットワークは一部のリンクが切れても経路制御で迂回することができるが、迂回状態に入ったときは一般に品質が下がると考えた方がよい。つまりリンク自体が多重化されていれば品質を下げずに故障を切り抜けられる。iDC のようにミッションクリティカルなネットワーク環境を提供すべき事業者は IP による迂回は最終手段として、まず第一段階はリンク多重でカバーできることを確認する。

リンクがダークファイバーを使用した自営の場合、まずファイバー経路が完全に独立していることを確認する。同一地点を二つのファイバーが走らない方が冗長性ポリシーのレベルは高い。またこのような質問に答えられない事業者は可用性に関心の薄い iDC であると評価できる。詳細な評価ポイントとして、センター引き込み点が二重化されていて、かつ引き込み点が十分距離的に離れていること、理想的には iDC の敷地内の対角線上に設置されていることが第一に挙げられる。また複数のファイバーが途中別々の経路を通って目的地まで到達する必要がある。もし同一経路を通っている部分があるならば、おおよそそれが何キロくらいか、そして同じ管路を使っていないかを確認する。

一方、リンクとして通信事業者から回線をリースしている場合はその契約グレードを確認する。二重化構成であることを確認する。例えば国内 ATM メガリンク相当のサービスを使用している場合は、デュアルクラスか同一拠点へ向けて複数の事業者からシングルクラスを貸借していることを確認する。

4.3.4 冗長経路切り替え方式

ダークファイバーによる自営回線の場合は更にこれらの冗長経路をどのように切り替えるかの確認を行う。SONET/SDH によるプロテクションスイッチングであれば切り替え時間 50ms 以内であり、音声などのリアルタイムトラフィックも継続させることができる。一方 Ethernet や IP による切り替えの場合は最低でも数秒かかり、Web データトラフィックだけを継続させることができる。SONET/SDH を使用する事業者は可用性への関心が高いといえる。

以上の評価項目からダイレクトに可用性を算出することは難しいが、iDC 事業者がどこまで可用性向上に関心があるかがわかり相対的なランク付けができる。可用性を特に重視するサイトの場合は、このランク付けを重要視するべきである。

4.4 セキュリティ

コネクティビティとしてのネットワークがセキュリティ面で果たせる役割は比較的少ない。通信プライバシー保持のため伝送媒体の物理的隔離が最も重要であり、それは設備の問題として把握される。本章でコネクティビティが直接果たすべきセキュリティ機能は送信元アドレスの偽造対策と現在では考えられている。iDC のコネクティビティをダイレクトに利用する加入者はセキュリティについて自ら考える必要がある。

iDC の中には外部ネットワーク接続点でファイヤウォールを運用している場合もある。このような iDC は、セキュリティに対して意識が高いと評価できる。ただ、その場合は、そのファイヤウォールのフィルタリングポリシーが自サイトにとって意味のあるものかどうかよく吟味する必要がある。一般にポリシーが緩いとセキュリティが低い恐れがあり、逆にポリシーが厳しいと自社サイトへのアクセス透過性が不十分でサービス機会を失う可能性がある。

自社サイトで自営でセキュリティ対策を実施する場合、使用するミドルウェア、たとえば Web サーバやアプリケーションサーバなどの暗号化機能や認証機能を利用したり、セキュリティ専用のミドルウェア等を使用することを前提に総合的に考えるべきである。したがって、iDC が、そのようなプロフェッショナルサービスを提供していれば、利用を検討すればよいし、なくても自前でそろえて組み込めるなら問題ない。

4.4.1 セキュリティポリシーと対策

ネットワークを通じた不正侵入、盗聴、ウィルス、DoS 攻撃などに対して、セキュリティポリシーと対策が用意されているかがひとつのポイントである。iDC 側の提供している範囲を確認することで、補強プランなども立てることができる。進歩の激しい分野であるので、現在の状態だけでなく、将来にわたって改善を進めていく意志があると判断できるところを中心に候補をしぼりこむのがよい。もちろん、個々の機能については、iDC を利用して行うことと関係のある機能についてのみ検討を行えばよい。BtoB など、ある程度限られた範囲での接続ならば、接続先のアドレスを絞り込むなどの制限がかけられるようになっているところの方が利用価値が高いが、BtoC で情報公開など、不特定多数への情報発信がメインならこのような機能は必要ない。対策としては、セキュリティ侵害を検知した場合に、迅速かつ適切に対処するように準備がされているかが重要である。

また、自社との接続が必要な場合、VPN の利用や、iDC と自社を専用線でつなぐことができるかもポイントとなる。

4.4.2 ファイヤウォール

ネットワークのセキュリティで、もっともポピュラーなものが、ファイヤウォールであると思われる。ファイヤウォールは、プライベートなネットワークとパブリックなネットワークを分けるためのゲートウェイであり、パブリックなネットワークからプライベートなネットワークを直接アクセスできないようにする。

ファイヤウォールの種類としては、IP ヘッダに含まれている情報を元に通信を制御する「パケットフィルタリング」、アプリケーションからの操作を中継する「アプリケーションゲートウェイ」、各層からの情報を元に作ったテーブルをベースにセッション単位でフィルタリングを行なう「ステートフルインスペクション」がある。自分の利用するのに十分な機能があれば、優先的に選択候補とすればよい。

4.4.3 CPE ベーズド VPN サービス

CPE ベーズド VPN は、インターネットを経由するにもかかわらず、拠点間を専用線のように相互に接続し、安全な通信を可能にするセキュリティ技術である。VPN の機能は大きく分けて 2 つある。1 つは、VPN の通信用にパケットのヘッダを変換する機能で、これは VPN 装置によって処理されるが、それにより本来は IP パケットのみしか通らないインターネットに、たとえばプライベートアドレスや、TCP/IPでないプロトコルを利用した通信も可能になる。この機能は、インターネット通信の中に別の通信を通すという意味合いから「トンネリング」と呼ばれる。もう 1 つは、通信パケットを暗号化する機能である。これにより、トンネリングされたパケットの盗聴を防止し、かつ通信相手先（通信経路）を隠蔽することができる。VPN 機能の実装は VPN 装置に依存するため、利用するには、iDC 側の装置の確認が必要となる。

このような目的のために、iDC を選択する場合には、このサービスが提供される iDC を選択しなければならない。

4.5 運用

運用の善し悪しは外からみて容易に想像がつかない。しかし可用性同様にいくつかの観点からヒアリングを行い、運用ポリシーの相対的な優劣をみることができる。

4.5.1 障害管理

障害監視を 24 時間 365 日行うことはベースラインである。一方それを復旧する標準時間（MTTR）に言及できる iDC 事業者は優れた運用を行っている可能性が高い。また交換部品の在庫管理について言及できる iDC 事業者は優れた運用を行っている可能性が高い。

4.5.2 トラフィック管理

トラフィック監視を 24 時間 365 日行うことはベースラインである。トラフィックレベルが上がった場合には中期的な対処と瞬間的な対処とがある。中期的な対処として、アクセ

ス集中時間帯の平均トラフィックが何%になったら増強を始めるというポリシーを持っている事業者はよい運用ができている可能性が高い。またその数値が 50%程度である場合は大変トラフィック管理に関心の高い iDC 事業者である可能性が高い。

更に、瞬間的な対処方法としてトラフィックエンジニアリング技術を擁する iDC 事業者は大変高いレベルの管理技術を擁し、瞬間的なトラフィック増加を示す大規模サイトに対して差別化されたネットワークコネクティビティを提供し得ると考えてよい。

4.5.3 運用情報の開示

障害やトラフィックレベルなどの運用情報がリアルタイムに加入者に提供されている iDC は運用の透明性への意識が高く、優れた運用を行っている可能性が高い。

4.5.4 障害連絡、定期工事連絡

障害によるサービス停止がネットワーク以外の手段を利用して速やかに加入者に通知されること、また計画的なサービス停止や変更が十分な期間を持って事前に通知されることを確認する。事前通知方法のポリシーが定められていることは必須である。

4.6 契約

4.6.1 SLA

SLA は、個別に交渉というところが多いと思われる。したがって、iDC を使用する目的に合わせて必要な信頼性を、SLA で明確に約束できるかがポイントである。もし、契約したレベルを提供できなかった場合の補償を明確にしておく必要がある。以下のようなポイントについて検討するとよい。

・ネットワーク SLA 項目の確認

自分が利用する上で重要な項目が保障されているのか確認しておくべきである。とくに、リポート関係はチェックしておくとよい。たとえば、情報提供なら、レスポンスタイムやダウンタイムが重要など。

・SLA の監視主体の確認

SLA どおりのサービスが提供されているか監視するのは、iDC 側なのか利用者側なのか。利用者側でやらなければならないとすると、そのためのコスト等も考慮に入れなければならなくなる。

・SLA 監視方法の提供確認

監視しようにも監視する方法がなければ意味がない。監視のための手段が提供されているかは、確認しておかなければならない。

・料金払い戻しポリシーの確認

どのような場合に、料金の払い戻しがあるのか確認しておく。

4.6.2 業務機会損失に対する保険

今のところ、業務機会損失に対する保険を用意しているところは、ほとんどないと思われるが、補償という意味では、料金の払い戻しよりも重要であるので、優先的に選択候補となりうると思われる。

4.7 料金体系

ネットワークの料金体系は、帯域幅に応じた定額料金とトラフィック量に応じた従量制のどちらか、または、両方の組み合わせになっている。ポイントは、拡張性に絡む問題だが、開始時だけでなく、将来のアクセス量、転送量、頻度にあった料金体系が用意されていて、変更が迅速にできるかである。

さらに、従量制の場合は、突発的なトラフィックの増大であっても、回線費用が抑えられる 95%ルールなどが設定されているかもポイントとなる。

その他、通常の使用料のほかに、トランジットトラフィックに対する特別課金があるかどうか、加入者固有保守回線費用などもかかる場合があるので総合的に判断する必要がある。

4.8 まとめ

- インターネットワーキングの観点からはできるだけ単一 ISP 内顧客カバレッジの高い ISP が運営する iDC、またはそのような ISP に対して加入者関係にある iDC を選択する。
- 次善の策として相互接続の優れた ISP が運営する iDC、またはそのような ISP に対して加入者関係にある iDC を選択する。
- バックエンドコネクティビティとして必要な私的閉域網のサービスが受けられる iDC を選択する。
- 音声／ビデオアプリケーションでは特にネットワーク品質のよい国際 Tier-1 または国内 Tier-1 ISP が運営する iDC、またはそのような ISP に対して加入者関係にある iDC の中から選択した方がよい。
- 接続帯域については自社初期アクセス帯域の 4 倍まで直ちに増強できるように、バックボーン帯域とアクセス帯域品目の両方で余裕のある iDC を選択する。
- 可用性、運用の相対的な優劣はヒアリング評価によって間接的に可能である。
- ネットワークセキュリティは透過性と安全性が両立していることを確認し、安全性の不足分は自社サイト内で補完する。

第 5 章　ハウジングサービス

第５章　ハウジングサービス

ハウジングサービスとは iDC の基本的なサービスであり、顧客のコンピュータサーバ類を持ち込んで iDC の保有する設備による各種サービスを受ける形態のものである。基本は顧客サーバ類が占有するエリアの広さによって料金が決まり、ファシリティやネットワークのサービスと組み合わせて利用される。

5.1　パフォーマンス

サービスメニューとしては、専用ルーム、専用ゾーン or スペース、ラックに区分されていることが多い。事業者によってメニューの名称と提供内容が異なる。例えば、ラックは１架と 1/2 架単位で提供する iDC が多いが、1/4 架、1/15 架さらには 1U 単位のメニューを用意している iDC もある。従って、要件を明確にすれば、利用形態にあったサービスを提供する事業者を選択することができる。

5.1.1　専用ルーム

専用ルームは、他の利用者から隔離されたマシン室を提供するサービスで、自社センター同様の感覚で使用することができる。使用面積、電力容量、ネットワーク規模、空調容量及びルーム仕様は個別対応である。従って、料金は個別設定である。機器・設備の収納方法は利用者の自由なので､機器当たりの利用料を安くすることも可能である｡その場合、ネットワークや電力、空調能力は増強が可能であるが、床は補強が難しいので床荷重を超えないように機器を収納するか、機器の重量に耐えられる床荷重の iDC を選択する。床下の梁の有無で耐荷重が異なるので、それを考慮して機器配置する必要がある。なお、標準的な 19 インチラックの場合、ラックの自重が 200Kg、最大搭載許容質量が 200Kg、合計で最大 400Kg になる。ラックの設置面積が約 0.6 ㎡である。

5.1.2　専用スペース

専用ゾーン or スペースは、サーバルームの一部を借りるもので、ケージ or キャビンで囲うことによってセキュリティを確保する。セキュリティを重視するならばキャビン方式が望ましい。ただし、空調の効果に注意しなければならない。使用面積、電力容量、ネットワーク規模は個別対応であることが多く、料金も個別設定であることが多い。規模が小さいこととセキュリティが弱いことを除けば、機器・設備の収納方法が利用者の自由になるなど、利用環境は専用ルームに近い。

5.1.3　ラック

ラックは、事業者が電源・通信ケーブル敷設済みのラック（標準的には 19 インチ）を用意するサービスである。セキュリティは鍵付きラックで確保するが、別料金となってい

ることもある。貸出し単位は事業者によって異なる。多くは１ラック、1/2 ラック、1/4 ラックであるが、1/15 ラックから貸し出す事業者もあり、一部には 1U 単位のサービスを行う事業者もある。利用形態と将来の増設を見越して適切な iDC を選ぶ。外から機器が見える開架型と見えない閉架型があり、セキュリティ上は閉架型が望ましい。
なお、19 インチラックマウント型と称していても、標準的な 19 インチラックに収納できず、専用ラックを必要とする機器があるので事前に確認すること。

5.2 拡張性

5.2.1 述べ床面積

ハウジングサービスを受ける時にまず確認したい項目として、サーバルームの面積がある。一般に iDC の売りとして総面積 1,000 ㎡、5,000 ㎡などと表現されるが、全体の総面積よりも現在の使用面積と空いている面積を調べておくことをお薦めする。顧客のシステムの拡張性を知っているのは SIer であり、サーバ類にしてもいつ頃どれくらいの拡張が必要になるのか、それに伴い iDC のハウジングエリアがどれくらい必要になるのかを計画しておくことである。iDC は装置産業であり、物理的な延べ床の拡張は困難である。既に設置してあるサーバ類の回転を工夫していくことが iDC の営業努力とも言えるので、できれば事前に iDC 側に空きエリアの状況について時系列的な予想を聞いておくとよい。

5.2.2 拡張単位

実際にエリアを拡張したいとき、どの単位で拡張できるのかは重要な事項であり見落としがちであるので注意したい。

- 面積……㎡
- ラック……ケージ貸しの場合であり、一般的と思える。1/n ラック単位。
- 段数……１段単位で拡張できれば細かな拡張に対応できるが、逆に煩雑な場合もあるので拡張時にはそのプラスマイナスを検討すること。

5.2.3 電源拡張性

ラック単位なりに通常の電源容量は決まっているが、特別な機器を使用する場合に、電源容量や電圧を特別に拡張できるのかどうか、さらにはその場合の料金規定についても確認すること。

5.3 可用性

5.3.1 ラック占有形態

ラックの占有形態については特に重要である。負担費用と自己の自由度のトレードオフになるので事前の確認をすること。

- 共用ラック……他の顧客と共用するラック。ラック単位での融通は利きにくい。

（ただし、共有ラックの場合、HUB 等も共有するために他の顧客のサーバが見えてしまう可能性がある。そのような時は iDC 側と事前にその部分の確認を行い、不都合がある場合は対処をしてもらうことである。）

・ 専用ラック‥‥‥１ラックを専用できるということはラック単位での自由度があるということであり、中身の機材の変更や追加・削減も可能である。

5.3.2 付属のネットワーク

最近では、ハウジングサービスの付加サービスとしてネットワークのオプションセットという形態が出てきている。以下のようなネットワークサービスが付帯してセットで料金的にも格安の場合も多々あるので事前に確認すること。（ネットワークサービスについては第 4 章　コネクティビティサービスを参照）

付属のネットワークの例：

高速バックボーン・専用線・VPN・保守用回線

5.3.3 代替センター

システムの内容にもよるが、災害や事故によりその iDC が使用不可になった場合、代替センターを必要とするかを検討する。iDC 自体に直接関係する自然災害、人的災害さらには火災、間接的な電力提供企業の事故や交通機関の事故等多くのことが考えられる。iDC 自体の災害あるいはその環境・周囲の事故のいずれにしても、iDC 自体がそのサービスを提供しえなくなった場合、即座に他のセンターへ切り替える方法或いはある程度のタイムラグを許してでも他のセンターへ移行する方法について代替センターを事前検討しておく必要がある。また、iDC 自体のサービスに直接的に影響は無いが、間接的にあるいは時間差的にその環境が及んでくる場合もあるので、今の iDC でのサービスを別の代替センターに切り替えるコンティージェンシープランを持っておく事をお薦めする。

5.3.4 データバックアップ

不慮の事故に備えるために定期的なデータバックアップが必要なシステムであるかどうか検討がいる。一日単位でのデータのバックアップを取得することも費用負担との兼ね合いで考えることになる。

5.3.5 緊急時対応

事故が発生した場合、どの程度の対策をとってくれるのかがポイントである。

ハードウェア事故‥‥‥ディスククラッシュの場合、ディスク交換とデータ復元まで対応してくれるのか、それを何時間以内に回復してくれるのかよく確認したい。そこまで対応してくれない iDC が多いと思うが、その場合の連携手はず（保守企業との連絡等）をどうすればいいのかも検討しておきたい。

ソフトウェア事故‥‥‥アプリケーションのバグや不具合、オペレーションミスその他ソフトウェア的な事故の場合も、どこまで何を対応してくれるのかを確認すること。

5.4 セキュリティ

5.4.1 技術的監視

- アクセス監視‥‥‥ネットワークを通じた外部からのアクセスについて十分な監視ができていること。システムの重要度に応じてファイヤウォールの設定も確認したいし、IDS（侵入検知システム）の装備も iDC 側と相談することが必要な場合もある。少なくともアクセスログの取得と分析は行いたい。
- ウィルス監視／対策‥‥‥昨今のウィルス、ワームの脅威は大変なものがある。既に現れたものから潜在的なものまで、その対処はセキュリティホールへの対処も含めて iDC 側と検出および駆除を行うことが可能かどうかを確認したい。

5.4.2 資格取得

旧安全対策基準は 2001 年 3 月にて終了した。それに代わり時代の要請とともに新たな資格・規格が出てきている。iDC におけるそれらの取得状況や認識、考え方についても確認されたい。

・Ｐマーク・・・2001 年度内には個人情報保護法が成立すると言われているが、それら個人情報の取り扱いについて一定の基準にあることを示す規格である。一般に iDC 業者や学校法人、金融機関等顧客情報の保護を必要とする企業で取得が進んでいる。iDC においては預かったサーバシステムの個人情報の管理についての姿勢が問われる。個人情報を扱うシステムをハウジングする場合にはこのＰマークを取得している iDC を選択することが重要である。

・ISMS（Information Security Management System）

旧安対基準に代わる包括的な情報セキュリティの管理規格である。2001 年パイロット運用、2002 年度から本運用されるということだが、この規格を取得することがこれからの情報処理業界の企業ポリシーとなりうるものであり、セキュリティ面での安心をサポートするものと考えられる。まだ詳細が明確でない面があるので ISMS に関する情報を入手できうる体制にしておきたい。

5.5 運用

ハウジングサービスのパフォーマンス、拡張性、可用性を支える人間系と位置付けられる。内容は主としてハウジングする機器によるサービスを維持するための作業である。なお、全サービスに共通の電源や空調などのファシリティとネットワークは除く(ファシリティおよびコネクティビティの項参照)。

5.5.1 運用サービス

死活監視など基本的な運用は iDC から標準的に提供されることが多い。操作を伴う作業や利用者のアプリケーションに関わる作業は利用者の責任において行う。それを利用者自ら運用する場合は、iDC までの所要時間、iDC 内の作業場所の有無、休憩・食事の便宜などに基づいて判断する。運用を委託する場合は、詳細な内容を個別に iDC と調整することになる。なお、具体的な内容は iDC によって異なる。

表 5.1 運用サービス例

サービス区分	サービス名称	サービス内容
標準提供サービス	死活監視	Ping による監視
	サーバ性能監視	リソース閾値監視、稼動率提供
	URL レスポンス監視	外部から監視、時系列データ提供
オペレーション サービス	サーバリブート(手動／自動)	顧客指示によるリブート
	ケーブル差し替え	指定画面への切り替え、切り戻し
個別サービス	データリカバリ	指定媒体からデータのリストア
	障害対応	発生障害のリカバリ、原因調査

（出典：iDC イニシアティブ）

5.5.2 運用環境

運用を利用者自身が行うことも可能であるが、セキュリティ上の問題から運用を iDC に委託するのが基本である。殆どの iDC は、稼動監視を行うための統合監視システムを整備し、利用者と密接な連絡を取るためのサービスデスク(またはヘルプデスク)を設置している。ファクシミリ／電話／電子メール／ポータルを通じて利用者からの問い合わせ・依頼を受け付ける。サービスデスクが 24 時間 365 日対応すること、様々なアクセス手段が提供されていることが判断の基準である。

5.5.3 レポート

運用状況は定期的(日/週/月)に報告される。その他、障害発生など例外事象についてはその都度、決められた時間内に報告がある。報告事項と報告間隔、異常発生から報告までの時間が利用形態と整合しているかどうかで判断する。

5.6 契約

サービス仕様とサービスレベルは iDC によって異なるので、利用目的に適ったサービスメニューのある iDC を見つけ、利用要件を提示して概略の見積もりを取ることから始まる。

5.6.1 サービス仕様の調整

サービス内容は大きく物理スペース、コネクティビティ、そして運用に分けて調査・判断することができる。

サービスは概ね基本と付加に分かれていることが多く、付加サービスは利用形態に合せ

て必要なメニューを選定する。更に夫々に細かな選択肢があるので、iDC との間で細かくサービス仕様に関して相談する。従って、豊富なサービスメニューが用意されており、利用者の要望を的確に把握して、細部に亘るまで仕様を調整した後にサービス設計するような iDC を選択するのが良い。なお、契約書には上記の他に、契約発効開始時期、契約解除要件・終了条件、サービス中断時の免責事項と賠償条件などが規定される。

5.6.2 ファシリティの SLA

サーバなど機器の稼動環境の品質保証は第 3 章を参考。

5.6.3 インターネットサービスの SLA

インターネットとの接続とその能力(帯域)の品質の保証は第 4 章を参考。

5.6.4 運用サービスの SLA

標準運用サービスの品質保証は概ね、サービスデスクが行う障害検知の連絡やその対応時間に関する保証値と、iDC が標準として提供する監視サービスの可用性に対する保証値の２種類が対象となる。前者の対応時間については 15 分以内、後者の可用性は 99.5%を一つの目安とするのが妥当である。

上記が遵守できない場合には、月額料金を上限として、１回につきその何分の１かを減額する例が多い。

5.7 料金体系

利用料金はサービスメニュー(専用ルーム／専用ゾーン or スペース／ラック)によってまったく異なる。標準メニューの利用料金は予め決まっていることが多いが、個別の追加要件は両者で仕様を検討するなかで追加料金を決めることになる。

5.7.1 専用ルーム

個別対応である。使用面積、電源容量、ネットワーク規模、空調容量などによって異なる。機器・設備の収納方法は利用者の自由なので、機器当たりの利用料を安くすることも可能である。ただし、ネットワークや電力、空調能力は増強が可能であるが、床は補強が難しいので注意を要する。床荷重を超えないように機器を収納するか、機器の重量に耐えられる床荷重の iDC を選択する。

5.7.2 専用ゾーン or スペース

個別対応であることが多い。留意点は専用ルームの場合と同様である。なお、セキュリティを確保するにはケージ or キャビンで囲うことになるが､それは別料金になっていることもある。

5.7.3 ラック

標準的には 19 インチの利用料金が、貸出し単位(１ラック、1/2 ラック、1/4 ラック、1/15 ラック、1U など)別に設定されている。鍵付きであることが多いが、鍵の有無で別料金になっていることもある。

5.8 まとめ

既に多くの iDC ではハウジングサービスという基本サービスだけでは他社との差別化もできず、それに加えてどういう付加価値サービスを提供できるかが生き残りをかけた正念場になりつつある。例えば、ハウジンサービスと表現されていてもそこには 10Mbps のネットワークが付帯しているというものもある。料金的にもその方が別々にサービスを依頼するよりも割安な値決めになっている場合がある。

従って、ハウジングサービスと一言で言っても、その基本サービス（監視サービス）に付加的サービス（ネットワーク、ファシリティ、運用等）がどのように組み合わされているかをよく見極めることである。

第 6 章　ホスティングサービス

第６章　ホスティングサービス

ホスティングサービスとは、顧客用のメールサーバ、ネームサーバ、ウェブサーバ等の各種サーバをプロバイダーが、自社の設備として構築し、管理そして運用し、顧客はその利用料をプロバイダーに支払うサービスである。

ホスティングサービスには、顧客に取って次のメリットがある。

① 顧客がコンピュータ等を所有していなくても、インターネットを活用したサービスを開始する事が可能となる。

② サーバの管理及び運用を専門家によって行ってもらえる。

その反面、一般的に、ホスティングサービスの利用料は、ハウジングサービスの利用より高くなる。

ホスティングサービスを大別すると、顧客毎にプロバイダーが専用の設備を用意するデディケーテッドホスティングサービスと複数の顧客でプロバイダーの設備を共用するシェアードホスティングサービスとがある。

デディケーテッドホスティングサービスは、シェアードホスティングサービスより木目細かなサービスを受けられる代わりに、利用料金は高くなる。

SIer が iDC におけるホスティングサービスを選択するにあたり、その選択基準を下記の各評価分類ごと検討した。

6.1　パフォーマンス

iDC によって提供されるサービスは､適正なパフォーマンスを維持しなければならない。パフォーマンスが低い場合、サービスの応答に時間が掛かったりして利用者にストレスを与え、それが原因でサービスからの利用者離れを招いてビジネスチャンスを失ったり、処理すべきものが処理できなかったりする。

ホスティングサービスのパフォーマンス評価において使われる値は、サービスの利用者がそのサービスを使って何をしようとしているかによって異なる。例えば、オンラインゲームサービスを行おうとしている場合、即時応答が要求され、オンラインショッピング等のサービスにおいては、概ね 3 秒以内の応答が得られれば良いとされ、事務連絡システムに使うのであれば、それ程、処理の即時性は必要とされない。

ホスティングサービスの選択時におけるパフォーマンス評価は、次の何れかの方法で行う事ができる。

① ホスティングサービスにおいて定評のあるサービスプロバイダーの実測値に基づく方法

② 業界における平均値または基準値に基づく方法

③ サービスを受ける者(利用者)自身の目標値に基づく方法

パフォーマンス評価においては、その評価時点におけるパフォーマンス値だけでなく、

その値が過去の時間経過と共にどのように変化してきたかの傾向を知ること、また、将来の利用量の増大に対処可能なシステムになっているか評価すること。更に、パフォーマンス値は色々な要因に影響されて変化するため、一定期間内の統計値によって評価すること。この場合、一定期間内の 50%以上が目標値を達成すれば良い。

ホスティングサービスの選択時に確認すべきパフォーマンスに関する事項には、次のものがある。

6.1.1 Web サーバ、FTP サーバなどの性能

インターネットを活用したサービスは、Web サービスやファイル転送サービスなどから構成される。これらのサービスは、Web サーバや FTP サーバなどによって実現される。従って、これらのサービスの応答性能は、Web サーバや FTP サーバの性能によって決まる。この為、ホスティングサービスの選択時には、Web サーバや FTP サーバなどの性能を評価する事が重要である。

Web サーバの性能評価は、インターネットを介して当該サーバをアクセスしその応答時間を目視により計測したり、また、システムに装備されている性能計測ツールのレポートに基づいて行う。

FTP サーバの性能評価は、インターネットを介して当該サーバにテストデータをアップロード/ダウンロードし、その転送時間を測定したり、システムに装備されている性能計測ツールのレポートを分析することにより行う。

6.1.2 ハードウェアの基本性能

総べてのソフトウェアは、コンピュータの上で実行される。従って、ソフトウェアの設計性能が如何に良くてもコンピュータの能力が低ければ期待したサービス性能を得る事は難しい。逆に、多少重いソフトウェアであっても、それを実行するコンピュータの能力が高ければ充分なサービス性能を得る事も可能となる。

この為、ホスティングサービスの選択に当たっては、サービスを実現するために用いられているシステムを構成するコンピュータの CPU 性能、IO 性能およびメモリ容量等のハードウェアの基本性能と構成とを評価する。

ハードウェアの基本性能比較は、専門誌などで行われているので、ホスティングサービスに使われているコンピュータの構成情報を入手することにより容易に評価できる。

6.1.3 データベースサーバや AP サーバの処理能力

オンラインショッピングなどの E-コマースサービスは、Web サーバをデータベースサーバや AP サーバに連携させて実現するのが一般的である。この場合、Web サーバの性能が幾ら高くても、データベースサーバや AP サーバの性能が低いと当該サービスの応答時間の間歇的な低下を来たす可能性がある。従って、データベースサーバや AP サーバを使

ってサービスを実現するシステムの場合、これらのサーバの処理能力を評価する。

サーバの処理能力の評価は、システムに装備されている性能計測ツールのレポートの分析やトランザクション処理性能値などを比較することにより行う。

6.1.4 ネットワークの帯域幅とトラフィックの集中の度合い

ホスティングサービス提供者の保有するネットワークの帯域幅(帯域幅が広いと回線スピードが早くなる)も重要である。Web サーバなどの性能が高くても、データをやり取りするときに使われる回線のスピードが遅いと、サービスの応答に時間が掛かったり、タイムアウトになったりする。従って、ホスティングサービス提供者の保有するネットワークの帯域幅が、当該サービスのトラフィックに比較して、充分確保されているか否か評価する必要がある。ネットワークの帯域幅を評価する場合、当該サービスのトラフィック量だけでなく、そのネットワークを共用する他のサービスのトラフィック量やトラフィックの集中の度合い、将来におけるトラフィック量の伸びなどを勘案して評価する事が重要である。

ネットワークのトラフィックのパターンや問題点は、ネットワークモニタや Netstat などのツールを用いることで知ることができる。

センターと利用者とを結ぶネットワークのパフォーマンス評価は、テスト環境を作成して実測するより手はない。

6.1.5 ファイヤウォールやルーターなどのネットワーク機器の性能

インターネットを活用したサービスのシステムは、セキュリティ保護の為のファイヤウォールや、トラフィックの行く先制御の為のルーターなど、諸々のネットワーク機器から構成されている。従って、これらのネットワーク機器の性能を評価することである。

ネットワーク機器の性能評価は、シミュレータや各種アナライザを用いて行う。

6.1.6 プロキシサーバなどのキャッシュサーバの性能

キャッシュサーバを用いて不要なトラフィックを削減したり、オリジナルなサーバに同一の要求を行わないようにしたり、利用者の近くで応答を返すようにしたりして、インターネットを活用したサービスの性能を向上させることが行われる。特に、特定のサービスにアクセスが集中するような場合、キャッシュサーバは有効である。従って、この様な場合にはキャッシュサーバの有無､その配置場所及びその性能を評価することが必要である。

プロキシサーバなどのキャッシュサーバの性能評価においては、サーバ単体の能力評価とキャッシュサーバによるトラフィック低減効果との 2 つを評価する。サーバ単体の能力評価は､システムに装備されている性能計測ツールのレポートを分析することにより行う。

キャッシュサーバによるトラフィック低減効果の測定は、当該サーバのログを調べる事で知ることができ、また、利用者端末での応答時間を計測することにより、その効果を知ることができる。

6.1.7　性能監視機能

インターネットを活用したサービスの利用者数、その利用時間帯及び利用頻度などは、時々刻々変化する。システムの構成要素毎に定期的に性能を測定し、問題が生じてないか監視し、問題が生じた場合、何処が問題か提示する機能が必須である。従って、ホスティングサービス提供者を選択する場合、その提供者が性能監視機能を有しているか否か、また、その機能が有効に機能し、運用されているか評価する。

具体的には、ホスティングサービス提供者のサービス説明書を取り寄せて確認するか、または、ホスティングサービス提供者のヒヤリングを行い、性能監視機能の有無及びその機能の監視項目を知ることである。

6.1.8　性能予測機能

インターネットを活用したサービスは、技術革新や利用者のネットワーク環境の変化などにより、利用者数や利用時間帯や利用頻度が変動する。この為、性能測定を定期的に行い、その測定データを分析して、将来、当該サービスの性能がどうなるか予測する性能予測機能があることが望ましい。性能予測機能があれば、その予測に基づいて、適正な性能を保証できるようシステム改善を行う事ができる。

具体的には、ホスティングサービス提供者のサービス説明書を取り寄せて確認するか、または、ホスティングサービス提供者のヒヤリングを行い、性能予測機能の有無、及び、その機能で予測できる項目を知ることである。

6.2　拡張性

ビジネスが拡大し、利用者やデータが急速に増加したり、より高度なサービスレベルが要求されたりした場合、システムの短時間での拡張や柔軟な構成変更が可能でなければならない。従って、ホスティングサービスの選択時には、そのサービス提供者の拡張性を評価する必要がある。ただし、ホスティングサービス利用者のトラフィックが比較的少なかつたり、変動しないことが明らかな場合、拡張性を考慮する必要はない。

システムの拡張性を定量的に評価するのは難しいので、システム構成に関する文書に記述された機能項目やホスティングサービスプロバイダーにヒヤリングを行い、それによって得られたシステム構成情報などに基づいて評価を行うことになる。

ホスティングサービスシステムの拡張性を実現する方法には、その構成コンピュータのシステムの能力を拡張していく方法と、サービスシステムのコンピュータの台数を増やす事でホスティングサービスシステム全体の能力を拡張していく方法とがある。拡張性の視点からは、どのように実現されていても良い。

ホスティングサービスの選択時に評価すべき拡張性に関する事項には、次のものがある。

6.2.1 コンピュータシステムの拡張性

利用者やデータが増大した場合、当該サービスのシステムをプロセッサの増設や外部記憶装置の増設によって、速やかに拡張可能になっていなければならない。この為、ホスティングサービス提供者を選択する場合、そのサービス提供者のコンピュータシステムが充分な拡張能力を有しているか評価する事が必要である。

コンピュータシステムの拡張性は、空いている通信ポートの数、物理メモリの拡張余裕サイズ、SMP 機能の有無、クラスタリング機能の有無などにより評価する。

6.2.2 オープン化

システムを拡張しようとする場合、システムや通信プロトコルが標準やデファクト標準に準拠したオープンな仕様になっていると、様々なメーカの中から最も良い機器を選択でき、その機器を監視することも容易となる。また、そのシステムの運用要員の確保も容易になる。その結果、システムの拡張を早く、安価に行える。

従って、ホスティングサービスの選択に当たっては、システムがオープン化されているか、標準通信プロトコルが使われているか、特定のベンダーに拘束されていないか、評価する事が必要である。

システムが UNIX、Windows または Linux のシステムならば、オープンシステムと判断して良い。また、通信プロトコルは、TCP/IP ベースのものならば、通常問題は無い。

6.2.3 動的再構成機能

インターネットを活用したサービスは、24 時間 365 日無停止である事が要求される。この為、システムを停止する事無く、システムの変更や拡張を可能にする動的再構成機能が重要である。システムの動的再構成を可能にするには、部分停止できるようシステムがクラスタリング構成になっていたり、分散処理システムになっていたりする必要がある。また、ソフトウェアもシステムの動的再構成に必要な機能を有している必要がある。従って、ホスティングサービス提供者の選択に当たっては、その提供者のシステムがソフトウェア面及びハードウェア面からみて、充分な動的再構成機能を有しているか評価する。拡張性の視点からも動的再構成機能を有している事業者の方が、動的再構成機能の無い事業者より良い。

6.2.4 構成管理機能

システムの拡張を効率的に行う為には、システムの構成を正確に把握し、表示する構成管理機能が必須である。構成管理機能で、システムを構成しているソフトウェア、アダプタ及び機器の情報を一括管理する。構成管理機能が無い場合、人間の曖昧な記憶に基づいたり、図面に基づいてシステム拡張を行わなければならなくなり、誤りを生じたり、正確な履歴を保持することが難しくなる。従って、ホスティングサービスの選択に当たっては、構成管理機能の有無を確認し、構成管理機能を有しているプロバイダーの方が、構成管理機能の無いプロバイダーより良い。

6.3 可用性

今日のインターネットを活用したサービスでは高度な可用性が必要不可欠の条件となっている。例えば、サービス利用中にそのサービスが停止したり、入力したデータが失われたりした場合、サービス利用者はそのサービスを利用しなくなる可能性が高い。この為、インターネットを活用したサービスを実現するのに用いられるホスティングサービスは、災害やハードウェア障害、ソフトウェアバグ、運用要員の誤操作などがあっても、極力そのサービスが停止しないようになっていなければならない。また、万が一サービス停止が発生した場合、その復旧対策が如何に成されているかが重要である。

ゆえに、ホスティングサービスの選択に当たっては、そのサービス提供者のシステムの可用性を評価する事が必要である。

通常、サービス保証時間等の可用性に関する事項は、ホスティングサービスの提供者と利用者との間で結ばれる SLA 等のサービス提供契約に盛り込まれる。従って、サービス提供者から SLA 等のサービス提供契約の原案を提示してもらい、そこに記述されている可用性に関する指標を他の事業者の指標と比較することにより評価する。また、可用性の評価をする時は、指標による定量評価だけでなく、システムや運用体制が異常発生時に対処可能になっているか見極めることも肝要である。

ホスティングサービスの選択時に確認すべき可用性に関する事項には次のものがある。

6.3.1 サービス保証時間

ホスティングサービス提供者によっては、サービス保証時間を明示的に示していることもある。サービス保証時間の提示は、一週間、一ヶ月あるいは年間と言った一定の期間内に、何時間以上停止した場合に利用料をサービス提供契約に従って減額するとしているのが一般的である。また、停止時のサービス復旧時間を提示している場合もある。

この様にサービス保証時間が明示されている場合、停止時間と復旧時間の短いホスティングサービス提供者を選択するのが良い。

6.3.2 フォルトトレラント

システムの CPU やメモリや電源装置など、あらゆる部品を冗長構成にすることにより、システムの一部が故障してもシステム全体が停止することのないようになっているシステムである。ホスティングサービスのシステムがフォルトトレラント化されているならば、そのシステムの可用性は高いと考えて良い。

6.3.3 多重化

システムの可用性を高める手段の１つが、多重化技術である。多重化の方法には、システム全体の多重化と外部記憶装置などの部分的多重化とがある。ホスティングサービスの選択に当たっては、そのサービスを実現するのに用いられているシステムのどの部分がどのように多重化されているか確認する。

6.3.4　フェイルセーフ

システムの多重化等によって幾ら可用性を高める工夫をしても、それを操作する人間が誤操作をすれば、システムの可用性の低下を来たす。この為、操作する人間が万が一ミスしても安全な方向になるよう設計されたフェイルセーフが重要である。従って、ホスティングサービスの選択に当たっては、どのようなフェイルセーフがシステムに組み込まれているか確認する。フェイルセーフを有している提供者の方が、フェイルセーフの無い提供者より良い。

6.3.5　地理的分散

ある１つの地域にホスティングサービスのシステムが集中していると、地震等の災害が発生した場合、そのサービスが長期間停止してしまう恐れがある。この為、ホスティングサービスのシステムは、遠隔地に分散して配置され、その分散システム間でバックアップと互いの復旧が可能になっていることが望ましい。従って、ホスティングサービスの選択に当たっては、そのシステムの地理的分散が図られているか、また、如何に互いをバックアップするようになっているか確認する。地理的分散を図っている提供者の方が、地理的分散の無い提供者より良い。

6.4　セキュリティ

次々と現れるウィルス、セキュリティホールや侵入手口など、その脅威は増大しかつ対策は高度に専門化してきている。また、一旦問題が発生した場合、社会的信用への影響も含めその対策コストは高くつくことが多い。従って、ホスティングサービスにおいて、優れたセキュリティを提供する iDC を選ぶことはいかなるシステムにおいても今後さらに重要となる。ただし、これらへの対応は、ホスティングサービスだけでの対策だけでなく、ネットワークサービスなど他のサービスと連携した対策を必要とするものが多いのでそちらも合せて確認が必要である。

ホスティングサービスの選択にあっては、下記のセキュリティに関する事項について適切な対策が施されているかが選択のポイントになる。

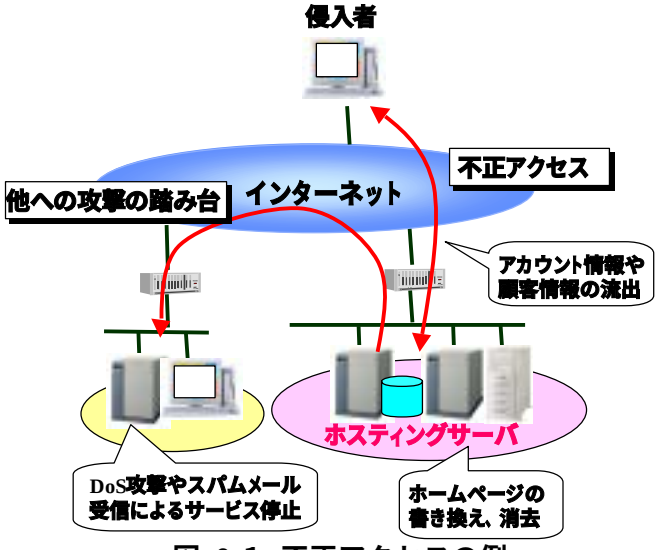


図 6.1　不正アクセスの例

6.4.1　不正アクセス対策

不正アクセスには、サーバへ侵入して情報の盗聴、情報の不正コピー、改竄、破壊、不正な削除などがある。さらにDoSやDDoSの攻

撃対象となったり、スパムメールの不正中継アクセスなど他のネットワークへの攻撃の踏み台とされる場合もある。

サーバへの不正アクセスを許す原因には、大きく分けて次の2つがある。

- サーバの設定誤りやセキュリティホールの放置
- ユーザID、パスワードの漏洩

前者については、ホスティングサービスで提供されるサーバについて、コンテンツや顧客情報などのデータを守るため、OSやミドルウェアなどのソフトウェアに以下の対策が実施されているかが、いかなるシステムにおいても重要であり、選択時に確認しておきたい点である。

- 適切なバージョンが採用され、セキュリティパッチなどが適用されている
- 不要なプロセスやサービスを動かしていない
- 一台のサーバを複数の顧客で共有する場合には、各アカウント単位でのアクセス権限がきちんと設定されている
- セキュリティ情報発行機関から脆弱性を指摘されているCGIプログラム等が利用されていない
- メールサーバが不正中継を許さないように設定されている
- ベンダーやセキュリティ情報発行機関などからアナウンスされるセキュリィティホールやそのパッチ発行といったセキュリティ情報を随時チェックし、問題がある場合にはすぐにSIerなどへ連絡の上、対処している

ユーザIDやパスワードの漏洩については、次の点をiDC選択時に確認しておきたい。

- SIerなどのサーバアクセス手段として、インターネット等の共用ネットワークを利用する場合には、VPNやSSHといったセキュアな通信手段を用意している
- 一台のサーバを複数の顧客で共有する場合には、管理者用IDとパスワードが適切に設定、管理されている。

不正アクセスの手段はさらに巧妙化してきており、対策が後手にまわるケースもでてくる。従って、以下の点についても選択時に確認しておきたい。

- ファイヤウォールや IDS といったセキュリティ関連機器の導入状況やその運用方法
- 不正アクセス検出時の対策実施計画

その他、専用サーバの場合でも iDC 内の他利用者のサーバから不正アクセスされないようにネットワーク環境が構築されているか確認しておきたい。

6.4.2 ウィルス対策

ウィルスを大きく分類すると以下のようになる。

- ファイルなどに感染し、プログラムやデータに対して何らかの被害をおよぼすように作られたプログラム。感染する場所の違いによって、プログラムファイル感染型、ブートセクタ感染型、複合感染型、マクロ感染型などがある。

- 実行することによって、ユーザの個人情報やアカウントを盗んだり、プログラムやデータに対して何らかの被害を及ぼす独立したプログラム(トロイの木馬)。他への感染や自己増殖はしない。
- トロイの木馬のように被害を及ぼす独立プログラムであるが、ネットワークを利用してさらに感染・増殖するプログラム(ワーム)。メールのメッセージや添付ファイル、ftpさらにはhttp経由で感染する。

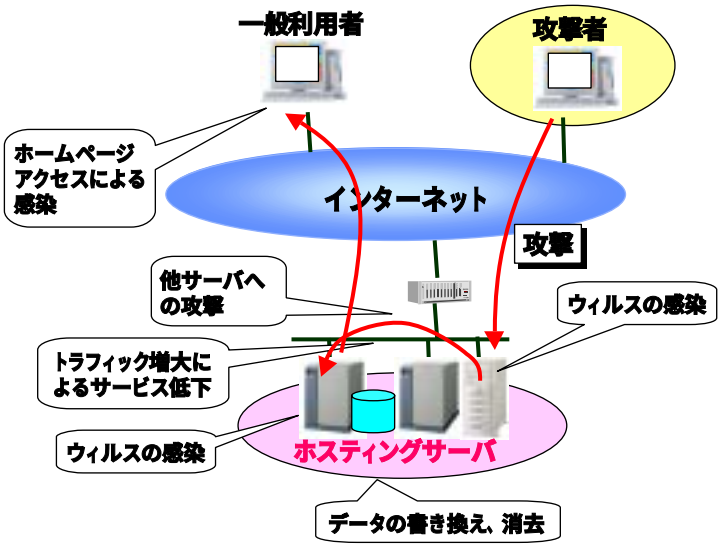


図 6.2 ウィルス感染と増殖の例

常にインターネットに接続されているサーバにとってその脅威は大きい。特に自己増殖するワームタイプは被害が急速に広がり易いので注意が必要である。

サーバへのウィルス感染を許す主な原因は、サーバの設定誤りやセキュリティホールの放置である。ホスティングサービスで提供されるサーバについて、コンテンツや顧客情報などのデータを守るためOSやミドルウェアなどのソフトウェアへ以下の対策が実施されているかが、いかなるシステムにおいても重要であり、選択時に確認しておきたい。

- 適切なバージョンが採用され、セキュリティパッチなどが適用されている
- 不要なプロセスやサービスを動かしていない
- ウィルス対策用ソフトウェアが提供され、パターンファイルなどが即座にメンテナンスされている
- ベンダーやセキュリティ情報発行機関などからアナウンスされるセキュリティホールやそのパッチ発行といったセキュリティ情報を随時チェックし、問題がある場合にはすぐにSIerなどへ連絡の上、対処している

ウィルスの攻撃パターンはさらに巧妙化してきており、対策が後手にまわるケースもでてくる。従って、予防対策だけでなく以下の点についても選択時に確認しておきたい。

- トラフィックモニタリングやアクセスログの定期的チェックなど感染検出手段
- 感染検出後の即座の対策実施

6.4.3 機密情報漏洩対策

サーバ内のデータやインターネット経由でやり取りするデータについて、システム要件で機密性を高める必要がある場合、以下の機能が提供されているか着目する必要がある。

- PKI、ワンタイムパスワードといった個人認証に関する機能
- SSL、S/MIME、APOP といったインターネット上のデータの暗号化に関する機能
- クレジットカード番号などサーバ内のデータの暗号化に関する機能

6.5 運用

SIer が構築したシステムを iDC に設置した場合、監視を含めた日々の運用を誰が実施するかという問題がある。一般的には 24 時間 365 日の体制を維持している iDC 事業者またはそこで事業可能な MSP が提供するサービスを利用する方がコスト的にメリットがある。ただし、例えばコンテンツの入れ替えや障害発生時の対応など、運用で必要となる作業すべてをサービスとして提供していないので、必要に応じて SIer 自身が実施することになる。

iDC におけるホスティングサービス利用時に必要となる運用関係の要件で、iDC 事業者が提供しているサービスを運用の各場面ごとに表 6.1 に示す。ここで提供度は、

A：なんらかの形で提供している iDC 事業者が多い

B：なんらかの形で提供している iDC 事業者が少しいる

C：提供している iDC 事業者はほとんどない

の意味を持つ。

表 6.1 運用項目と iDC での提供度

タイミング	運用項目	提供度
定常時 (定期作業)	バックアップ	B
	バックアップ媒体交換	A
	バックアップ媒体保管	B
	ログ収集	B
	定期リブート	A
	定期巡回	A
	障害監視	A
	リソース監視	A
	性能監視	B
	運用リポート作成	A
随時 (一時作業)	基本ソフトウェア改版/パッチ適用作業	A
	設定変更作業	A
	コンテンツ変更作業	B
障害発生時	障害通知	A
	障害切り分け	B
	障害解析	C
	障害復旧作業	B

SIer は iDC の選択にあたっては、SIer が iDC 事業者に実施して欲しい項目を、それに見合うコストでサポートしているか重要なポイントとなり、必要に応じて選択できるようメニュー化されているのが望ましい。以下、各項目についてサービス内容を説明する。

6.5.1 定常時

（1）バックアップ

バックアップについては、システムによっては高度なスキルを必要とする場合もある。従って、オペレーション、実施時間や頻度などを整理の上、iDC 事業者がこれらの要件に対応可能か確認しておきたい。

（2）バックアップ媒体交換

媒体交換自体は単純作業なのでほとんどの iDC 事業者がサポートしているが、バックアップを実施するタイミングにきちんと対応してくれるか確認しておきたい。

（3）バックアップ媒体保管

媒体保管については、保管場所、保管期間、保管量について確認しておきたい。例えば、耐火金庫なども用意している iDC 事業者もある。

（4）ログ収集

収集したいログデータの種類やその収集方法もシステムによってまちまちである。従って、オペレーション、実施時間や頻度などを整理の上、iDC 事業者がこれらの要件に対応可能か確認しておきたい。

（5）定期リブート

定期リブートが必要なシステムでは、その頻度や方法について iDC 事業者が応じられるか確認しておきたい。

（6）定期巡回

iDC 内を定期的に巡回し、LED、異常音などの確認を実施する。その頻度や確認内容についてシステム側の要件と見合うか確認しておきたい。

（7）障害監視

ping による死活監視、port やプロセスの監視などを実施している。ping による死活監視はベーシックな手段であるが、これだけでは実際のサービスが動作しているかはわからないので、port やプロセスの監視まで含めて実施可能か確認しておきたい。特にシステム要件によるがミッションクリティカルなシステムでは、24 時間 365 日の体制での監視が必須である。

（8）リソース監視

サーバの CPU 利用率、メモリ使用率、セッション数、ディスク残量など各リソースの監視を実施している。これらの監視により、障害などを未然に防いだりシステム拡張の判断材料ともなる。ミッションクリティカル、特に大規模なシステムではリソース監視は有用なので、このサービスを 24 時間 365 日の体制でサポートしている iDC を選択したい。予め設定した閾値を超えた場合に通知してくれるサービスもあり、その場合には通知時間(30 分以内、2 時間以内など)と通知手段(電話、メール、ポケベルなど)についても確認しておきたい。

（9）性能監視

Web サーバの応答速度、I/O アクセス速度や CGI の処理時間などの監視を実施している。これによりシステムのサービス品質やボトルネック調査の判断材料となる。特に Web

サーバの応答速度に高いサービス品質を要求されるシステムでは性能監視は有用なので、このサービスを 24 時間 365 日の体制でサポートしている iDC を選択したい。予め設定した閾値を超えた場合に通知してくれるサービスもあり、その場合には通知時間と通知手段についても確認しておきたい。

（10）運用リポート作成

システムの稼動状態などを確認できるように、バックアップ、リソース、性能といった運用に関するリポートが、監視結果やアクセスログにもとづき通常マンスリーで提供されている。また、これらのリポートが Web 経由でブラウザを使って必要な時に簡単に参照できるように提供している iDC 事業者もあるので確認しておきたい。さらに、オプショナルなサービスとして次のようなレポートも提供する iDC 事業者もあり、アクセス変動の激しいシステムや EC システムなどでは有用である。

- 今後のアクセス状況を予測するアクセス予測レポート
- 顧客のアクセス時のページ遷移などをまとめたウェブアクセス傾向統計レポート

6.5.2 随時

（1）基本ソフトウェア改版/パッチ適用作業

ホスティングサービスで提供されたサーバ上の OS やミドルウェアなどに対して、例えば不具合やセキュリティホールが発覚してパッチが発行された場合、パッチの適用有無によるシステムへの影響は個別に検討する必要がある。従って、その通知やサーバへの適用について誰が何をどのように実施するのか、個別に相談の上で明示できる iDC 事業者を選択するとよい。

（2）設定変更作業

サーバへのアカウント追加や DNS サーバのレコード内容変更など、予めシステムにおいて想定される項目をピックアップの上、変更可否とどの頻度で変更してもらえるのか、確認して iDC 事業者を選択するとよい。

（3）コンテンツ変更作業

コンテンツの変更の方法については、メディアを渡して iDC 事業者が入れ替え作業を実施する、あるいはリモートからもしくは iDC 内で SIer が自分で入れ替え作業を実施する、といった場合がある。入れ替えの頻度や入れ替えに必要なスキルはシステムによって異なるので必要に応じてサポート内容を確認して iDC 事業者を選択するとよい。

6.5.3 障害発生時

（1）障害通知

障害通知はその通知時間(30 分以内、2 時間以内など)や通知方法(電話、メール、ポケベルなど)について、システム側の要件と見合うか確認しておきたい。

（2）障害切り分け

通常実施にあたっての切り分け用のマニュアルは SIer 側で用意する必要があるが、障害

切り分けのための 1 次作業として、LED 表示、異常音やケーブル接続などの確認、さらにログデータの収集あたりまで実施する iDC 事業者もある。切り分け要件や SIer の iDC への到着可能時間など考慮の上、必要な作業を実施可能な事業者を選択するとよい。リモート環境から SIer がログデータ収集や telnet などを実施する場合には、セキュアかつ必要な帯域でアクセスする手段(専用線、IP-VPN など)が提供されているか確認する必要がある。

（3）障害解析

解析用のマニュアルは SIer 側で用意する必要があるが、対応可能か確認して iDC 事業者を選択するとよい。システムによっては高度なスキルを必要とする場合もあるので対応している iDC 事業者はまれである。

（4）障害復旧作業

障害の原因が iDC 事業者側にあった場合、例えばホスティングサービスで提供されたサーバ自体にあった時、どのくらいの時間で交換作業を行うかなど確認の上で iDC 事業者を選択したい。SIer 側に原因があった場合、復旧作業もシステムによっては高度なスキルを必要とする場合もあるので、SIer が主体となって作業すると考えられる。復旧作業用のマニュアルは SIer 側で用意する必要があるが、システム再起動やバックアップデータを用いたデータリストア作業などを実施している iDC 事業者があるので、必要に応じて選択するとよい。

6.6 契約

iDC のホスティングサービス選択にあたり、契約については特に下記の事項に着目するとよい。

6.6.1 サービスの提供開始

ホスティングサービスにて iDC の用意するサーバが、その上で動作するソフトウェアも含めて契約締結日からどのくらいで使用可能か、注意が必要である。SIer が必要なタイミングで提供されるか確認して選択するのがよい。

6.6.2 サービスの利用期間

最低利用期間は通常１年程度からが多い。しかし、短期間のイベントやキャンペーンなどのシステムではより短い利用形態もある。１ヶ月程度から対応している iDC もあるので、利用期間がよりマッチした iDC を選択すると利用コストが有利となる場合が多い。

6.6.3 SLA

ホスティングサービスにおいて、SLA を公開している iDC は現在のところほとんど無い。中には単体のサーバのハードウェアと OS について毎月 99.8%、冗長構成化した場合には 99.9%(両方のサーバで計測)のアベイラビリティを実現することを保証したり、事前の自前設備による評価によってサービス利用可能時間、レスポンス時間、障害検知から復旧までの時間などを保証している iDC もある。

6.6.4 補償

ホスティングサービスにおいて、iDC 側が原因でシステムが停止した場合、どの程度補償するのかを公開している iDC は現在のところ少ないが、停止した時間に対応した月額料金の減額が一般的である。システム停止にあたり、多大な損失が発生するシステムの場合には、個別にそれ以上の補償がなされる余地があるのかも重要である。また、通常契約者側から補償を請求する必要がある上、時効も設定されていることが多いので、請求方法や時効期間を iDC 選択時に確認しておくとよい。

6.7 料金体系

iDC のホスティングサービスの料金体系は、表 6.2 のようにサーバとそれに付随するネットワークや運用・監視などのオプションサービスから構成されている場合が多い。

サーバの料金は、その種類、OS、CPU、メモリやディスクの仕様ごとに定められている。提供されるサーバの CPU やメモリなどの仕様は各 iDC によって様々である。オプションは、いくつかの iDC ではホスティングサービスの中でパッケージ化して提供されているサービスで、しかも有料/無料のサービス項目が混在している。また、iDC によってはホスティングサービスとしてはオプションにあげたサービスを含まず、別途個別のサービスとして独立した料金体系をとるところも多い。

表 6.2 料金体系の例

基本	サーバ	種類	Web サーバ、メールサーバなど
		OS	Solaris、HP-UX、Windows、Linux など
		CPU	SPARC、PA-RISC、IA など
		メモリ	256MB、512MB、1GB など
		ディスク	18.2GB×2、9.1GB×3(Ultra SCSI,RAID5)など
オプション	ネットワーク	10Mbps 共用、5Mbps 帯域保証(シェーピング)、100Mbps 専用 LAN 接続など	
	運用・監視	データバックアップ、ping 監視など	
	その他	セカンダリ DNS、ドメイン名取得など	

このように、ホスティングサービスの料金体系は各 iDC によって異なり、各 iDC のサービスを同じ条件で比較することが難しい。従って、まずは必要とするサーバやネットワークなどの仕様を明確にし、より近い仕様をサポートしている iDC をピックアップの上、できるだけ同じ条件にて料金を比較することが重要である。

また課金方法については、月額固定料金を採用している iDC が多いが、サーバからのデータ転送量による従量制課金を採用している iDC もあり、アクセス数が比較的少ないサイトや月ごとによるアクセス格差が大きいサイトなどは、料金の損得を見た上で選択するとよい。

6.8 まとめ

SIer が iDC におけるホスティングサービスを選択するにあたり、各評価分類ごとその選択指針を示した。ホスティングサービスの場合、実際のサービスの質は、提供しているサーバに関して各 iDC 事業者がハードウェアだけでなく OS やミドルウェアも含めて、どれだけ熟知しているかに依存する。例えば障害発生時、アプリケーションとの障害切り分けなどでその差が出てくる。同じ機種のサーバに対して同じサービスを提供している事業者でも、iDC 事業者の選定時にこれまで述べたポイントに留意してヒアリングなどを行うことにより、取り扱っているサーバに対するサポート技術力を推し量ることができるはずである。特にミッションクリティカルなシステムでは、単に必要なサーバが安く提供されているから、といった安易な選択はせずサービスの質を見極めるべきである。

第 7 章　ストレージサービス

第７章　ストレージサービス

ブロードバンドの進展にともなう、映像/画像/音楽等の配信用コンテンツの保管/管理、CAD/DTP/CG 等企業内/企業間データ交換用コンテンツの保管/管理、電子商取引の拡大にともない急増する顧客データ/取引ログの保管/管理、などのニーズによりストレージサービスが脚光を浴びつつあり、さらに、高信頼ストレージシステム構築の難しさ、SAN 等のストレージスペシャリストの不足、大規模バックアップシステムの運用コスト増加、24×365 運用コスト増加、大規模投資に対するリスク、等の難問に対する解決策の一つとしてストレージサービスに対する期待が急増している。ここでは、iDC を利用する SIer の立場で iDC のストレージサービスをどのような基準で選択すべきかを検討する。

なお、ストレージサービスとは、①ストレージ容量貸しサービス、②バックアップサービス、③ストレージ運用管理サービス、等を組合せたサービス体系である。

7.1　SAN と NAS

最初に、ストレージの重要な技術動向として SAN と NAS について解説しておく。

SAN(Storage Area Network)【図 7.1】は、サーバとストレージをファイバチャネルで接続する方式で、LAN と切り離してストレージを利用できる。

NAS(Network Attached Storage)【図 7.2】は、サーバとストレージを LAN で接続する方式で、LAN 経由でサーバからストレージを共用する事ができる。

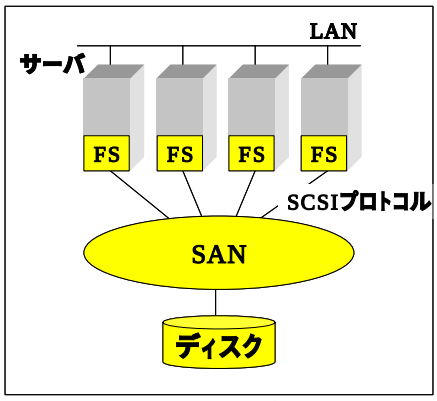


図 7.1 SAN 構成例

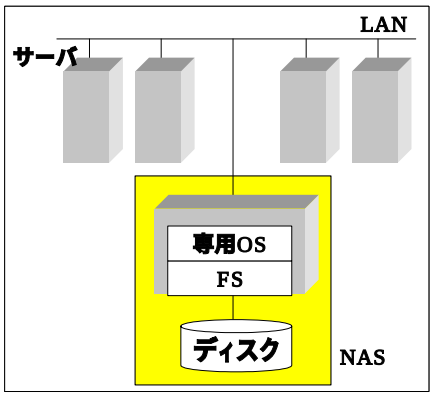


図 7.2 NAS 構成例

SAN は、LAN フリーでストレージ管理やバックアップを行う事が出来、業務の運用や他のサーバに対する影響が少ないのが魅力であり、NAS は異なるサーバ(OS)からファイル共用出来るところに魅力がある。

一般に、SAN は高速大容量の処理に向いており、NAS は向いていないと言われるが、ギガビットイーサネットの登場で NAS でもある程度の性能が出るようになってきた。

SAN は高価で、NAS は安価と言われるが、これは機能と構成の関係で一概には断ずる事は出来ない。

SAN はデータベース処理が出来るが、NAS はファイル処理までで、データベース処理は不得意であると言われているが、NAS 用データベース管理ソフトエアの開発でこの問題は少しずつ解消されつつある。

表 7.1 SAN と NAS の比較

➢ DB処理等ミッションクリティカルなシステムに対応するSAN ➢ 異種OS環境からのファイル共有が容易に構築出来るNAS		
アクセス方式	➢ ブロックアクセス	➢ ファイルアクセス
特長	➢ クラスタサーバ間の共有ストレージ	➢ 異なるOSからのファイル共有
適合する市場	➢ データベース ➢ ミッションクリティカルなシステム	➢ 多数のクライアントから ➢ ファイル共有されるシステム
性能とコスト	➢ 多数のサーバの接続にはFC Switchが不可欠	➢ システム性能の向上にはGigabitイーサネット(ルータ/Hub及びHBA)が不可欠
Network負荷	小	大

NAS は各サーバからファイル共用するため、不正アクセスをガードしにくく、SAN はゾーニングや LUN セキュリティを使って不正アクセスに対して強い、と言うのが一般的評価である。

7.2 パフォーマンス

「一般ユーザがストレージ性能を評価して自分にあった iDC を選択する」と言っても専門家でない限りそんなに容易いものではない。ディスクのシークタイム性能は？ キャッシュ性能は？ チャネル転送能力は？ はたしてボトルネックはどこにあるのか？

7.2.1 システム性能

参考に、iDC におけるストレージ構成例【図 7.3】で Web 性能に影響する要素を抽出して見ると、①インターネット、②ネットワーク、③サーバ、④ストレージ、と多岐に渡り、さらに、②ネットワークでは、ルーター、ファイヤウォール、負荷分散装置、等多くの装置が関係し、また、③サーバにおいても、データベース等のミドルソフト、AP ソフト、等の性能が関係してくる。

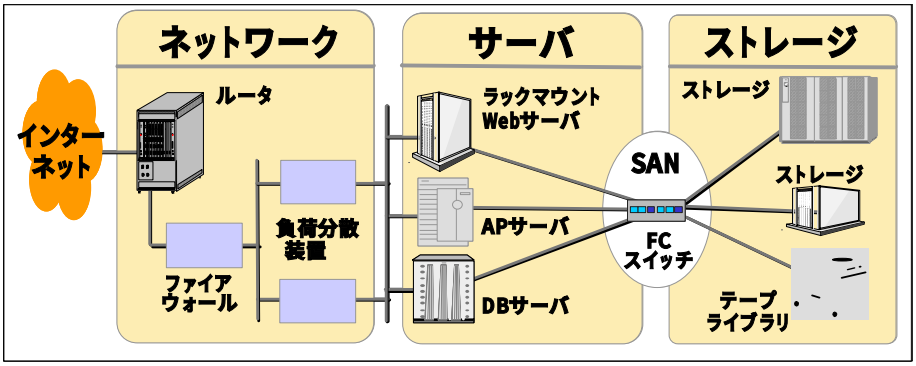


図 7.3 iDC におけるストレージ構成例

一般に Web 性能は、同時に処理する件数と処理内容、及び処理するシステム構成で決まってくる。したがって、クリティカルな業務は事前に目標処理件数を設定して、処理件数の変動に対してシステム性能(サーバ＋ネットワーク＋ストレージ＋ミドルソフト＋AP ソフト)を事前にシュミレーションして性能達成度合いを評価しておき、本番開始前に END to END で目標処理件数まで負荷をかけた状態での性能評価を実施しておく事を奨める。この提言は、ストレージサービスを選択する際の考慮事項と言うよりは、iDC サービス全体の選択に関する考慮事項であり、一度 iDC 事業者に問い合わせて見ると良い。

7.2.2 ストレージ内のバスの制御方式

ストレージの性能を引き出すには、ストレージ自身の性能を上げるのは当然の事として、それを処理するストレージ内蔵のバスの処理性能を上げる必要がある。バスの制御方式には大きく、①コモンバス方式【図 7.4】と、②階層スターネット方式【図 7.5】の 2 種類ある。

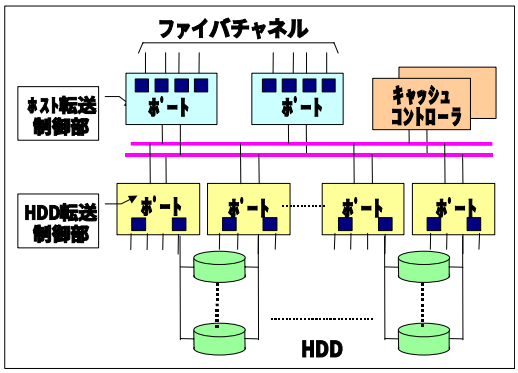


図 7.4 コモンバス方式

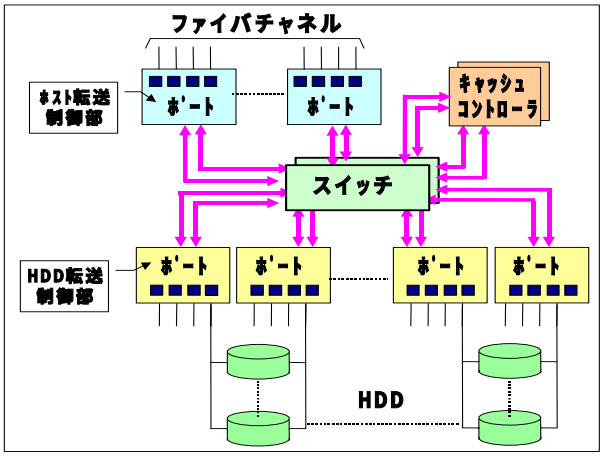


図 7.5 階層スターネット方式

複数ユーザ/複数チャネルの利用形態が浸透してくると、現在のストレージ技術ではバスの制御方式が限界処理性能に密接な関わり合いをもってくる。コモンバス方式は、複数チャネルから一本のバスに接続してキャッシュコントローラにつなぐ方式で、処理件数集中時に性能劣化が起きる。階層スターネット方式は、複数チャネルから独立して専用バスからスイッチを経由してキャッシュコントローラにつなぐ方式で、処理件数が集中しても性能劣化が起きにくい。iDC のストレージ構成としては、他ユーザから影響を受けにくい階層スターネット方式をお奨めする。iDC 事業者に確認しておいた方が良い。

7.2.3 ストレージのポートに対するサーバ接続台数

さらにストレージ性能を引き出すにはポートの接続台数を見ておく必要がある。ストレージのポートから直接サーバに接続する事が出来れば性能的には理想であるが、現実はスイッチを間に接続する事によりポート数を増やす【図 7.6】事が多い。

ストレージ性能は、ストレージ側のポート性能で決まってくるため、ストレージのポート

を共有するサーバが増えれば増えるほど性能劣化の可能性が高くなる。iDC 事業者に「ストレージのポートは当社占有ですか？」と確認して見ると良い。また、各 iDC 事業者に一つのポートに接続するサーバ台数をヒアリングして比較して見るのも良い。

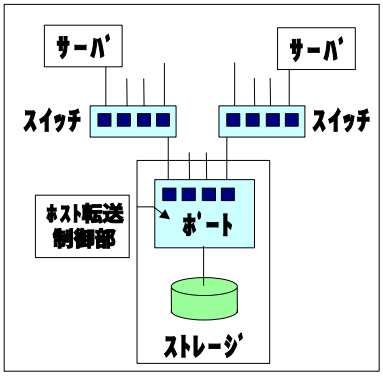


図 7.6 ｽｲｯﾁによるﾎﾟｰﾄ数拡大

7.2.4　ストレージのコントローラに接続するHDD数

一方、ストレージ側も一台のコントローラに接続する HDD 数「X＝HDD 数÷コントローラ」を確認しておく事を奨める。一般に、X が大きくなると性能劣化が起きやすくなり、X が小さくなると性能劣化が起きにくくなる。

7.3　拡張性

ストレージサービスは、常時、必要十分なストレージ容量を利用出来る【図 7.7】事に大きなメリットがある。ユーザがストレージ製品を自社で購入した場合、容量的余裕を見込んで購入するため、常時、大量の不稼動ストレージ容量を抱える事になり、投資効率が悪化する。一方、ストレージサービスを利用すると、ユーザは実使用容量に近い容量を、常時、利用出来るため資金効率が向上する。

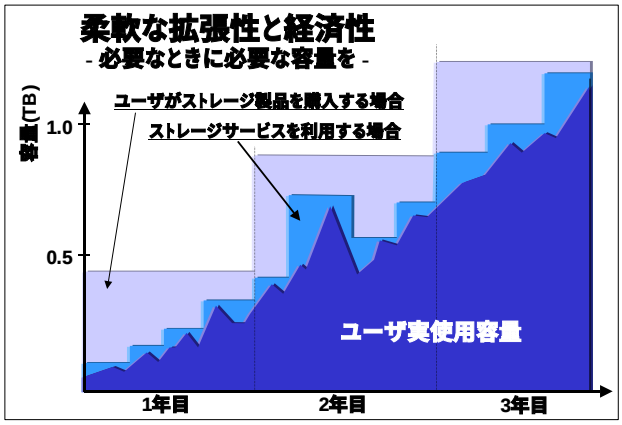


図 7.7 ストレージ容量拡張事例

季節変動等でストレージ容量が急激に増大した場合は、必要なだけストレージ容量を拡張出来、逆にストレージ容量が急激に減少する場合は、不要なストレージ容量を返却出来る。

7.3 1　ストレージ容量の増減

したがって、iDC 利用者としては、常時、必要十分なストレージ容量を利用するために、ストレージ容量を増減出来る時間的サイクルと、拡張可能な最大ストレージ容量を、サービス仕様、又は SLA(Service Level Agreement)で確認しておく事を奨める。サービス仕様、又は SLA の内容によって利用料金も変動するため、利用者側としてのストレージ利用見通しと確度を考慮してサービスレベルを見定めると良い。

ストレージの容量は、技術的には「LU(Logical Unit：論理ボリューム)追加」によって拡張出来る。LU サイズは数 GB 単位から数 10TB 単位まで設定可能であるが、LU サイズがあまりにも小さいと HDD の障害回復処理が複雑になったり、バックアップからのリス

トア処理が複雑になるなど設定/管理工数がかさむ。一方 LU サイズを大きくすると、設定/管理工数は楽になるものの、利用料金(＝容量×単価/容量)が高くなりコストがかさむ。以上を考慮して iDC 利用者側の IT システムに要求されている要件を基に、最適な LU 配置をコンサルテーションしてくれる iDC を選択するのが良い。

7.3.2 ストレージに接続可能なサーバ種類

ストレージはサーバを経由して利用される事になるが、接続可能なサーバも事前に確認しておいた方が良い。Solaris、HP-UX、AIX、Windows2000、Linux、等々との接続性が問題になる事がある。

7.4 可用性

7.4.1 冗長構成

ストレージの冗長構成では、電源及びキャッシュの 2 重化とパス切替え、キャッシュの 2 重書き、による安定稼動構成が実現されているか確認する必要がある。

7.4.2 保守

運用面では、運用を止めずに保守部品交換やファームウエアバージョンアップが出来るようにしてあるか確認したい。

障害発生時の復旧目安時間も確認しておくと良い。但し、これらサービスレベルは利用料金との見合いとなるため、サービスレベルが高ければ良いと言うものでもない。運用する業務の重要度を考えながら選択する事になる。

7.4.3 バックアップ

大切な情報を預かってもらうためにも、ディスク障害のみならず、サーバクラッシュによるファイル破壊やオペレーションミスによる誤ったファイル更新等に備えて、バックアップサービス【表 7.2】を利用する事を奨める。

表 7.2 バックアップサービス

バックアップサービス	運用レベル		
	自動運用	LAN フリー	業務影響度
自動バックアップ（LAN 経由）	可	不可	大
無停止自動バックアップ（SAN 経由）	可	可	極小
ディザスタリカバリ（SAN 経由）	可	可	極小

- 自動運用：運用管理システムによる自動運用
- LAN フリー：バックアップ実行時に他サーバに影響を与えない運用
- 業務影響度：業務運用への影響度の大小

iDC 向けのバックアップ機能は、ほとんどが運用管理システムを活用して自動運転が可能であり、LAN フリーで他のサーバに影響を与えないような構造になっているはずである。また、バックアップ時に業務を止めるか否かは利用者側で判断して選択すると良い。

自動バックアップ【図 7.8】は、一番簡便なバックアップ方式で、運用管理システムで業務を止めてバックアップを実行する方式である。バックアップ媒体は RAID 又はテープライブラリを選択する事が出来る。

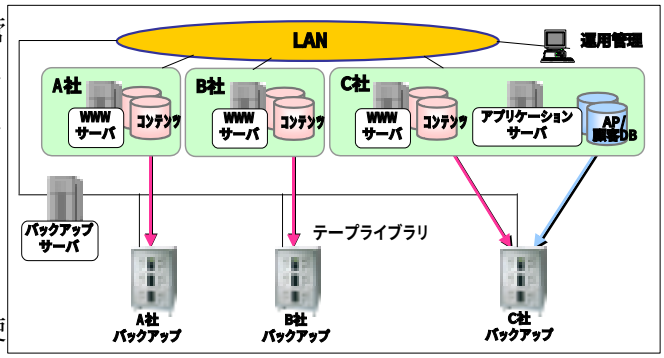


図 7.8 自動バックアップ事例

無停止自動バックアップ【図 7.9】は、SAN と RAID のレプリカ機能を使って、業務を止めずに業務と並行して自動的にバックアップを取る方式である。SAN や RAID のレプリカ機能利用にともなうストレージ容量の増加のため高価ではあるが、iDC 利用者は、サーバ業務を止めずに、かつ、バックアップを意識する事なくデータを保全する事が出来るため、クリティカルな業務を運営する場合にはお奨めである。

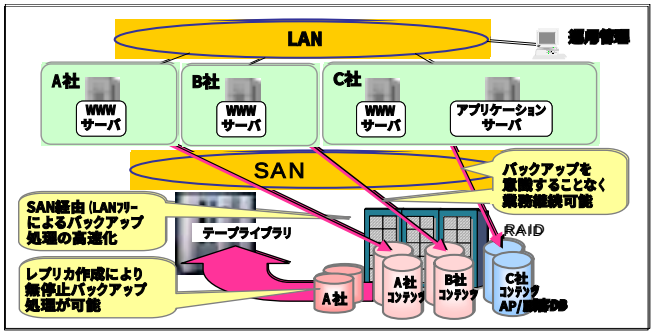


図 7.9 無停止自動バックアップ事例

ディザスタリカバリサービス【図 7.10】は、遠距離にあるバックアップセンターにデータを保管するサービスであり、地震などの大規模な自然災害や火災が発生し、センターが壊滅的打撃を被った場合でもデータの保全が出来る。サービス料金は高価になるが、ビジネス上の損失がそれよりもはるかに高額になるインフラ、たとえば、e-ビジネス等のミッションクリティカルな業務に向いている。

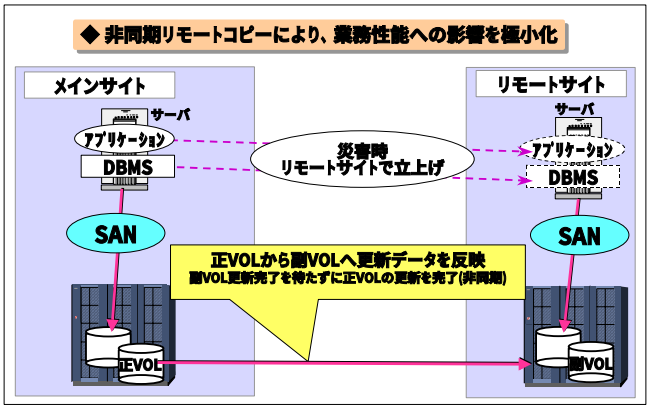


図 7.10 ディザスタリカバリサービス事例

一般に、無停止バックアップをうたう時は、「LAN フリーモード」によるバックアップ処理を指す事が多い。LAN フリーモードにすると業務性能に対する影響が少なく、また他サーバの運用を阻害する事も無くなる。

LAN フリーモードを実現する一つの手段として SAN(Storage Area Network)がある。出来れば、iDC 事業者のストレージ運用構成を確認して、個々のサーバの性能を劣化させない構成が取られているか確認すると良い。

バックアップ媒体はテープライブラリや RAID 等用意されているので利用者側で選択すれば良い。

7.4.4 バックアップサービス

iDC としてバックアップ機能のみを用意して「iDC 利用者が自ら運用する」だけでなく、iDC 事業者が運用する「バックアップサービス」を提供しているか確認すると良い。バックアップの運用は面倒なものであり、LU の取り方によってはバックアップがきわめて複雑になるケースがあり、出来れば iDC 事業者にバックアップ運用を任せた方が良いと考える。

7.5 セキュリティ

7.5.1 ゾーニングと LUN セキュリティ

ストレージのセキュリティとしては、各サーバから許可された LU にのみアクセスするセキュリティ方式（LUN セキュリティ）と、FC スイッチによりアクセスを制限するセキュリティ方式（ゾーニング）の 2 種類ある【図 7.11】ので iDC 事業者に確認すると良い。

なお、ゾーニングと LUN セキュリティの両方式とも SAN の特徴的機能である事は認識しておく必要がある。

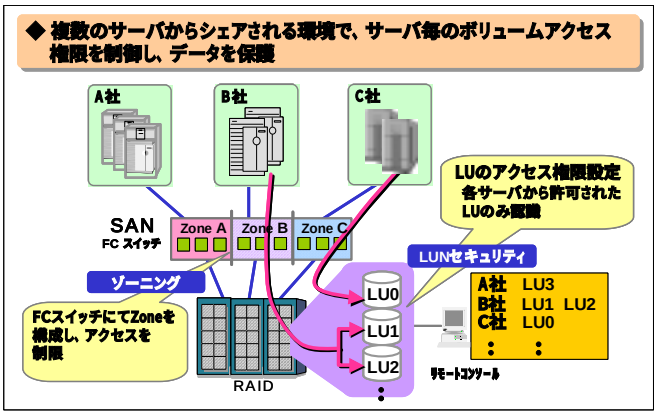


図 7.11 ストレージセキュリティ方式事例

7.5.2 媒体管理

運用面では、バックアップ媒体(ドライブ/テープ)の持ち出し管理が重要であり、媒体に IC チップを埋め込む等により不正な持ち出しを制限する事が出来る。iDC 事業者がどのような運用をしているか事前に確認する必要がある。

7.5.3 ファイルアクセス監視

ストレージに対するすべてのファイルアクセスを監視し、ポリシーの設定により特定ユーザ/プログラム以外による読み取り/書き込みを禁止する事が出来る。これはストレージセキュリティと言うよりサーバセキュリティの範疇に入る事かもしれないが、自社システム全体(ネットワークセキュリティ、コンテンツセキュリティ)のセキュリティレベルを考えながらサービスを利用すると良い。

7.6　運用管理

ストレージサービスを選択する際には、性能/処理能力/可用性/バックアップ/保守/運用手順、等に関する運用項目をサービス仕様又は SLA(Service Level Agreement)で確認しておく事を奨める。

一般にストレージの運用管理【図 7.12】は、運用管理システムと SAN 管理システムを組合せて実現するケースが多い。運用管理項目は、ストレージの障害監視、ストレージのバックアップ監視、ストレージ容量管理、ストレージ性能管理、等から構成され、統合された環境で集中監視・操作卓で常時 24 時間 7 日監視されている。さらに監視状況は定期的に顧客にレポートされ、安心して利用出来るように配慮されているので事前に確認しておきたい。

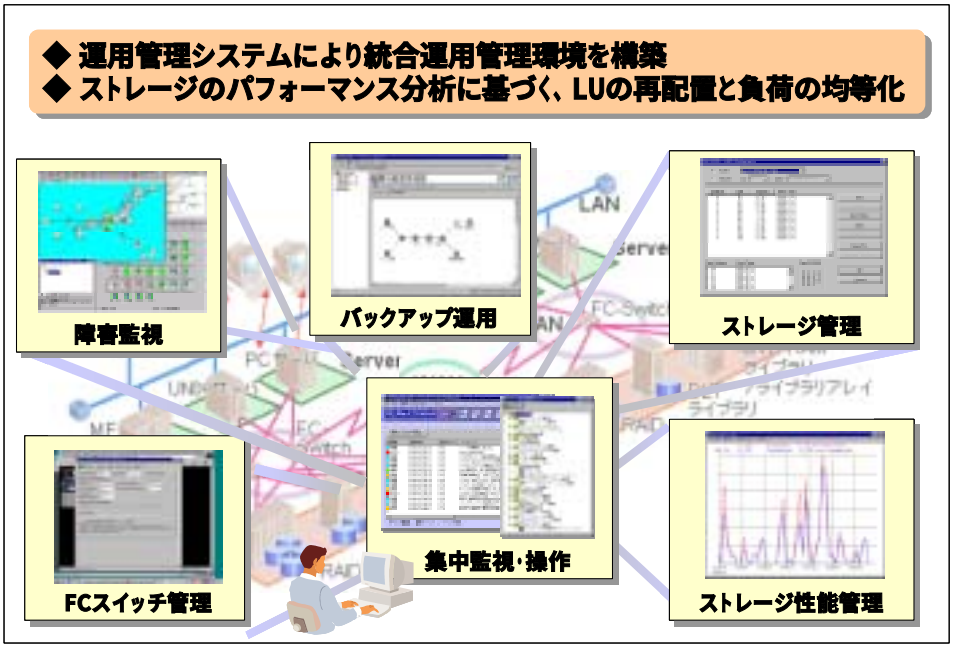


図 7.12　ストレージ運用管理事例

7.7　料金体系

一般的なストレージサービスの料金体系は容量ベースであり、標準的な可用性、標準的なセキュリティはストレージサービス利用料金に含まれるケースが多い。これに、自社業務のクリティカル度を考慮して、バックアップサービスや運用管理サービスをオプションとして選択すれば良い。

可用性については、SLA として契約する目標値(例．99%～99.999%)によって利用料金が変動する。逆に可用性目標値(不稼動時間)が目標を下回った場合は利用料金を安くするなど決めているケースが多いので事前に確認した方が良い。

バックアップサービスは前述のように各種用意されており、バックアップの方式やバックアップ媒体、バックアップ容量、により利用料金が変動するため、自社の業務のクリティカル度を考慮して選択すると良い。

運用管理は、ユーザの目には見えにくいところで運用されており、基本機能はストレージサービスに含まれているケースが多い。したがって、基本機能に追加してユーザポータルサービスとして運用管理サービスをオプション化しているケースが多いので、事前にどのようなサービスを提供してくれるか確認すると良い。

iDC を上手く使うと社内システムに同様な機能を作り込み/自主運用 するよりもコスト的には安価になるはずである。

7.8 まとめ

SAN が良いか NAS が良いかは、iDC 利用者が自社のシステムの特性を考慮して選択する話ではあるが、一般論として、ミッションクリティカルな外部向け業務（高速、大容量、無停止運転）には SAN を、簡便なファイルアクセス（部門システム）には NAS を活用する事を奨める。SAN は信頼性、性能、セキュリティに優れ、NAS はサーバを選ばずファイル共用による使い安さに優れている。

用　語　集

用語集

ＡＰＯＰ(Authenticated Post Office Protocol)
メール受信の際にパスワードを暗号化してサーバへ送るための規格。

ＡＳ番号(Autonomous System)
インターネット上の管理ドメインを表す番号。通常 ISP 一社毎に最低一つの AS 番号を保有している。インターネットレジストリー組織によって割り当てられる。

ＣＶＣＦ(Constant-Voltage Constant-Frequency)
電圧・周波数を安定化した電源のこと。一般に交流をいったん直流化してバッテリーにブリッジ接続し、制御されたインバータで定電圧・定周波数の交流として出力する。負荷の変動に関わらず電圧・周波数が一定にできる。

ＤＤｏＳ(Distributed Denial of Service)
複数の分散した地点からインターネット経由でターゲットへ大量のデータや不正パケットを送りつけ、ネットワークやルーターなどの機能を麻痺させる攻撃手段。

ＤｏＳ攻撃(Denial-of-Service)
インターネット経由でターゲットへ大量のデータや不正パケットを送りつけ、ネットワークやルーターなどの機能を麻痺させる攻撃手段。
例として、「多量の SYN フラグのたったパケットを Web サイトに送りつけ、サービスを停止させる攻撃」などがある。。

ＥＧＰ(Exterior Gateway Protocol)
ネットワークドメイン間経路制御プロトコル。BGP-4 が通常の方法。

ＩＤＳ(Intrusion Detection System)
侵入探知システム。サーバなどに対する攻撃を探知して通知する。
ネットワークパケット情報やサーバ内で生成される情報などをもとに、システムへの不正な侵入を検出する装置。

ＩＸ (Internet exchange)

複数のインターネットサービスプロバイダや学術ネットワークを相互に接続するインターネット上の相互接続ポイント。高速道路で言うジャンクションに当たる。

マルチラテラル相互接続ポリシーを持ち、多数の通信事業者がトラフィックを交換する相互接続ポイント。

Ｊキャリア専用線

日本電信電話 HSD に代表される同期式高速デジタル専用線サービス。

ＭＤＦ (Main Distributing Frame)

NTT 地域会社の電話局や集合住宅などで、回線と交換機の間にある装置。電話局では大量のケーブルを収容する必要があるため、交換機に接続する前に、ケーブルを整理するための配線分配装置である MDF に接続する。

ＭＴＢＦ／ＭＴＴＲ (Mean Time Between Failure/Mean Time To Repair)

平均故障時間、平均普及時間。

ＮＡＳ (Network Attached Storage)

TCP/IP 等の通信プロトコルを利用して Ethernet のネットワークに接続するだけでファイルにアクセス可能なストレージシステム。

ＰＤ盤 (Premise Distribution Cabinet)

電話線の MDF 盤に該当する光ファイバーのソケットを備える装置。装置から伸びた光ファイバーは、S-ONU（通信用の光加入者終端装置）に接続される。

ｐｉｎｇ (Packet InterNet Groper)

IP パケットが通信先まで届いているかどうかや、IP 的に到達可能かどうかを調べるためのコマンド。

ＰＫＩ (Public Key Infrastructure)

証明書に基づく公開鍵暗号を運用して、インターネットで安全な通信ができるようにするための環境。

S／MIME (Secure/Multipurpose Internet Mail Extensions)
電子メールでバイナリーデータを扱うための仕様である MIME に暗号化や電子署名などの機能を追加した拡張仕様。

SAN (Storage Area Network)
複数のサーバとストレージをファイバチャネルなどのスイッチで接続したストレージ入出力専用ネットワーク。

SLA (Service Level Agreement)
サービスの提供者と利用者の間で交わされるサービス品質に関する契約。保証項目、実現できなかった場合のペナルティ、上回った場合のボーナスなどが規定される場合もある。

SONET／SDH
電話網のバックボーンとして 155M から始まる同期伝送方式。現在ではデータ通信リンクとして使用される。

SSH (Secure Shell)
ネットワーク経由でリモートログインやファイルコピーなどを行うプログラム。ネットワーク上を流れるデータは暗号化される。

SSL (Secure Socket Layer)
セキュリティ機能の付加された HTTP プロトコル。通信内容の暗号化，通信相手の認証，メッセージ認証の機能がある。

Tier－1 ISP
最も大きなネットワークアドレス空間と地理的な広がりをもつ世界最大手 ISP の総称。インターネットのコアでルートを Tier-1 ISP どおしが相互交換し、デフォルトルートのないフルルートのネットワークを形成している。日本資本としては日本電信電話系の Verio がある。

UPS (Uninterruptible Power Supply)
「無停電電源装置」の略。電池や発電機を内蔵し、停電時でもしばらくの間コンピュータに電気を供給する装置。ユーザはこの間に安全にシステムを終了することができる。

ＶＰＮ(Virtual Private Network)

仮想私設網。通信事業者が持つ高度な網管理機能を用い、仮想的企業内専用網を構築するサービス。

公衆ネットワークの中に仮想的にプライバシーの保たれたオーバーレイネットワークを構築すること。ファシリティーベース VPN は通信事業者が自社ネットワーク内のしくみで構築し、サービスする方法を指す。CPE(Customer Premises Equipment:宅内装置)ベース VPN は、加入者宅内に設置された装置のしくみで VPN を構築する方法を指す。

アクセス監視

ファイル、データベースなどに対する不正なアクセスを監視すること。

キャビン

個室。セキュリティの確保のために囲った小さな部屋。

ケージ

エリアスペースを取り囲んだ金網籠。セキュリティの確保のためにラックやスペースを囲ったおり。

コンティージェンシープラン

緊急時の対応計画。緊急事態の際に、取るべき対応策を平常から考案しておくこと。

シークタイム

ハードディスク装置の読み出しまたは記録の際に、ヘッドがディスク上の目的の位置に到達するまでの所要時間。

セキュリティホール

プログラムの不備、設定ミスなどから生じるセキュリティ上の欠陥。

ゾーニング

複数のサーバとストレージを接続するファイバチャネルなどのスイッチ経由の接続パスにおいて、サーバとストレージの各ポート間の接続パスを限定してアクセス制限を行うスイッチの設定機能。

ダークファイバー

広域に敷設された光ファイバーのうち未使用のものを指す。広域データネットワーク構築時に通信事業者回線を使わない新たな選択肢として注目される。

デュアルスタック

この場合はIPv6とIPv4両方を同時に扱えるプロトコルスタックを示す。

トランジット

二つのISP A,Bが相互接続するとき、例えばAがBに対してフルルートを与えるかまたはデフォルトルートを認め、かつAのルートをインターネット全体にBが広報するような相互接続関係をいう。この時事実上ISP BはAへの加入者関係となる。

ピアリング

ISPが相互に自社ネットワークのルートを交換する相互接続取り決めの一種。

ファームウェア

ハードウェアの基本的な制御を行うために、機器に組み込まれたソフトウェア。

ファイヤウオール

私的ネットワークと公衆ネットワークの間にあってIPパケットを特定のポリシーに従ってフィルターする装置。主にセキュリティ目的で利用される。

ファシリティ

コンピュータを運営・管理するための設備、施設、機関。

プロビジョニング

加入者回線開通や増設とそれに対して通信事業者内で行われる様々な準備過程の総称。

マルチホーム

複数のISPに対して、ピアリング関係を結ぶこと。

ラック

コンピュータ機器を収納するための収納架で、一般には１９インチラックが使用される。

ワンタイムパスワード

一度限りしか使えない使い捨てのパスワードを生成することで、パスワードの盗み聞きを無意味とする認証方式。

旧安全対策基準

情報処理サービス業情報システム安全対策実施事業所認定制度は平成１３年３月で廃止になった。

経路制御プロトコル

ネットワーク上で IP パケットの転送経路を制御するプロトコル。ISP 内の制御プロトコルを IGP(Interior Gateway Protocol)、ISP 相互間の制御プロトコルを EGP(Exterior Gateway Protocol)として区別する。

個人情報保護法

収集した顧客情報の転売や個人情報のネットを通じた流出などを防止し、個人のプライバシー保護のため企業や個人に個人情報の適切な取り扱いを義務付ける法律案。

死活監視

サーバが正常に動作しているかどうかを、ネットワークを通じてＰｉｎｇコマンドを送りその応答で判断する監視。

耐震二重床

最新の耐震基準をクリアした免震･制振構造のインテリジェントビルに耐震二重床（フリーアクセス）を敷設。この方式により､サーバラックは床スラブへ固定することなく十分な耐震性を得ることができる。

通信品質

パケット通信品質指標には主に帯域、遅延、ゆらぎ、損失がある。帯域はデータ送受信のスピード、遅延は送信から受信までの遅れ時間、ゆらぎは遅延の分散、損失はデータの喪失を指す。

発行日　　平成１４年３月
編集・発行 財団法人　情報処理相互運用技術協会
〒１１３－６５９１　東京都文京区本駒込２－２８－８
文京グリーンコートセンターオフィス　１３Ｆ
ＴＥＬ（０３）５９７７－１３０１
ＦＡＸ（０３）５９７７－１３０２

KEIRIN この事業は、競輪の補助金を受けて実施したものです。