TOKIO MARINE

リスクマネジメント最前線

2025 | No.10

# ハイパースケール型データセンターの状況とリスク・対策

ビジネスリスク本部　青島　健二　上級主席研究員（専門分野：経営管理、業務/IT 改革、ERM）
ビジネスリスク本部　加藤　直人　主任研究員（専門分野：データ分析、リスク管理、DX 推進）

近年、GAFAM（Google, Apple, Facebook, Amazon, Microsoft）が自ら使用するハイパースケール型データセンター（HSDC）の建設・運営を外部に委託するケースが増加していることから、そのマーケットを捕捉すべくデータセンタービジネスに新規参入する企業が増加している。また、金融庁は本年 6 月にデータセンター関連設備の一部を不動産投資信託（REIT）の対象に組み入れることを認めることを発表したことから、今後新規参入の動きは更に加速するものと思われる。一方で、HSDC の運営側には SLA（Service Level Agreement）等負うべきペナルティが大きく、稼働が停止した場合の損失は巨額になることも想定される。以上のことから、新規参入企業においては HSDC が負う可能性のあるペナルティ、損害を PML（Probable Maximum Loss）として算定したうえで、事業の参入是非や参入時の対策を講じる必要がある。

## 1. ハイパースケール型データセンターの概要・市場

### (1) ハイパースケール型データセンターの概要

1995 年に発売された「Windows95」とインターネットの普及に伴って企業における情報システムの Web 化が進んだ結果、企業や組織が IT インフラを集中管理し、データ、アプリケーション、システムを安全に保管・運用するための専用施設として「インターネットデータセンター（IDC）」が急増した。但し、それまでの大型のメインフレームコンピューターを中心に、データ処理や情報管理を行う役割を担っていた「電算センター」がその役割を終え IDC に業態転換していったため、IDC は 1990 年代、企業の需要規模に応えるだけの供給規模があった。一方、2000 年代に入りインターネットで扱われるデータがテキストデータ（文章等）やトランザクションデータ（取引記録等）だけでなく画像データ、更には動画データが扱われるようになり、業態転換型の IDC だけでは需要を賄い切れなくなった。そこで、IBM や富士通、アクセンチュア等の IT ベンダーは新たに IDC を建設し、一般企業だけでなくインターネットプロバイダの IT 運用を受託するようになった。その後、BPO（ビジネスプロセス・アウトソーシング）と呼ばれる業務受託ビジネスも IDC の需要を生み出す大きなビジネスとなった。

一方でハイパースケール型データセンター（HSDC）とは、アメリカを代表する巨大 IT 企業である GAFAM が必要とする巨大なデータセンターのことである。GAFAM は、それぞれが数十億人のユーザを有しているが、2010 年代に入りユーザの行動履歴等をビッグデータとして蓄積し、新たなサービスに活かすようになった。また、ストリーミング（音声や動画等のデータを、すべてをダウンロードし終える前に再生しながら受信する技術や方式）の提供や、AI サービスの実装等新たな取り組みの結果、情報処理の能力がこれまで以上に必要となった。そこで GAFAM は、従来の IDC に依存せず、5,000 台以上のサーバーを格納し、約 25 メガワット（MW）以上の電力容量を有し、膨大なデータ

処理とストレージを装備する HSDC の建設を自ら始めた。これが HSDC の誕生である。参考までに、IDC と HSDC の比較表を掲載する。

■ 表 1　IDC と HSDC の比較（各種資料を基に弊社作成）

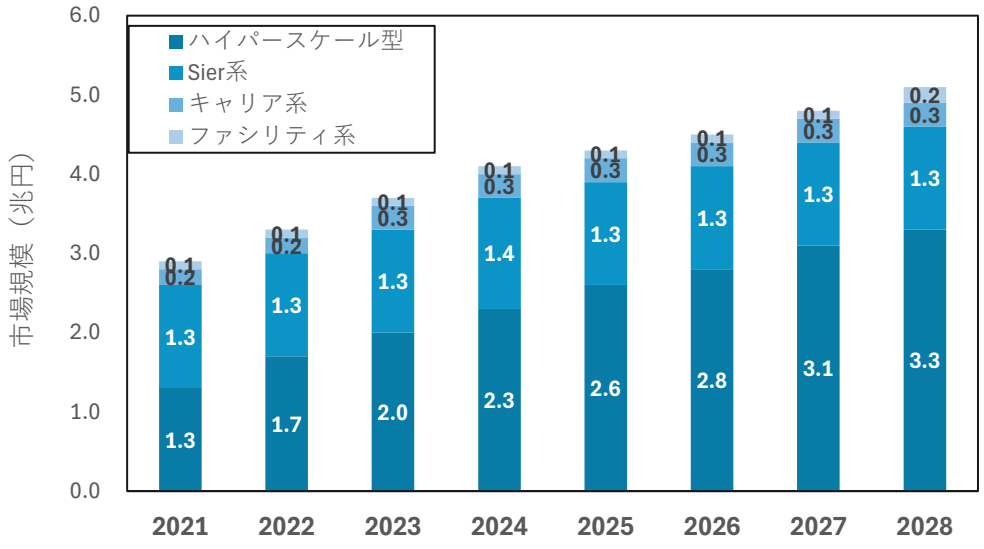
| 項目 | IDC<br>（インターネットデータセンター） | HSDC<br>（ハイパースケール型データセンター） |
|---|---|---|
| 定義 | インターネットサービス提供を主目的とする汎用型データセンター | 大規模なクラウド事業者が構築・運用する超大規模データセンター |
| 主な提供者 | 通信キャリア、データセンター専業会社、SIer 等 | GAFAM 等 |
| 主な用途 | 企業の IT インフラ、Web・メールホスティング、コロケーション等 | クラウドサービス、AI/ビッグデータ、動画配信、生成 AI 等 |
| 所有形態 | 複数顧客による共用型<br>（コロケーション等） | クラウド事業者の自社専有型<br>（フル制御） |
| サーバー台数 | 1,000～20,000 台程度 | 数万～100 万台以上 |
| 拡張性 | 一定の制限（物理スペース依存） | 高拡張性（世界中の HSDC と連携） |
| 国内例 | 日本 IBM、富士通、NTT Com<br>（現 NTT ドコモビジネス）, IIJ 等 | AWS、Google、Microsoft 等 |

## (2) ハイパースケール型データセンターを取り巻く市場

### ■ 世界における HSDC の市場規模

近年、GAFAM は自前で HSDC を建設する戦略を転換し、他の企業が建設した HSDC を賃借する戦略を採用しだしている。そのため、HSDC の市場規模は 2021 年には 1.3 兆円であったものが、2028 年には 3.3 兆円にまで伸長するとみられている。

■ 図 1　世界のデータセンター市場規模（売上高）の推移及び予測

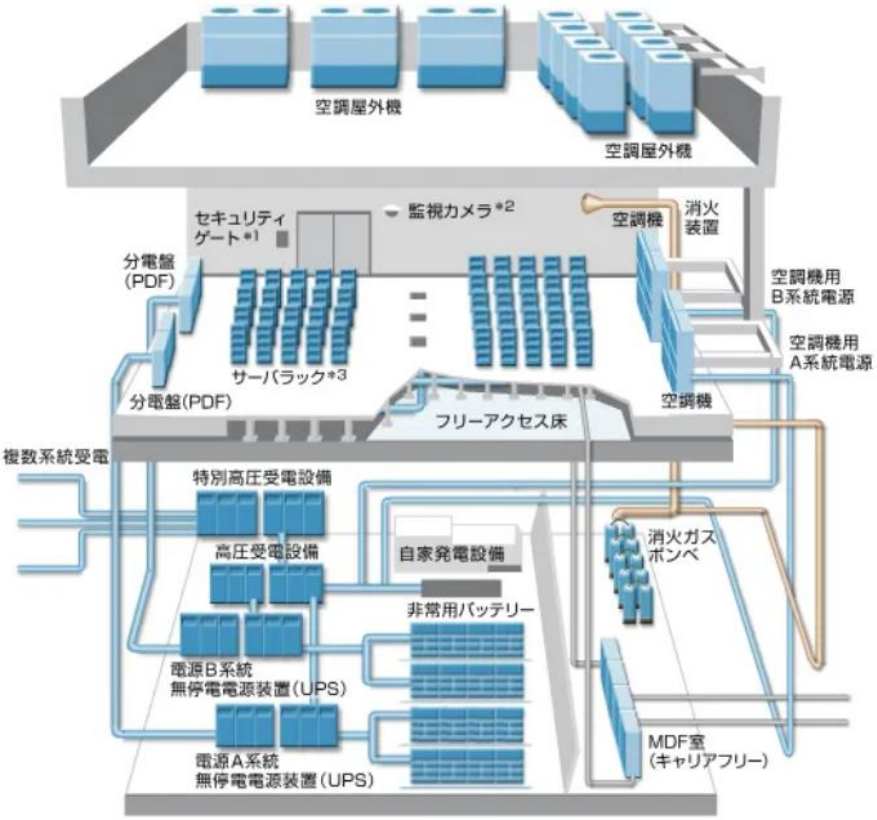



出典：富士キメラ総研「データセンタービジネス市場調査総覧2024年版」

## ■ HSDC を取り巻く市場

データセンターの構造は下図の通りである。建築／施設工事、電力インフラ、冷却・空調インフラ、IT インフラ、保守サービス等が、データセンターを構築・運用させるために必要であり、それら製品・サービスに関係する企業は HSDC 市場を自社の成長分野としてとらえている。

■ 図 2 データセンターの基本構造




出典：NTT データホームページ https://www.nttdata.com/jp/ja/lineup/green_data_center/

構成する各製品・サービスの市場は下表のようになっている。

■ 表 2 データセンターを取り巻く市場と主な製品・サービス、求められる要件等（各種資料を基に筆者作成）

| 市場セグメント | 主な製品／サービス | 求められる要件、市場動向等 |
|---|---|---|
| **建築／施設工事** | ● 建屋建設<br>● セキュリティ設備<br>● ケーブル配線<br>● ラック設置　等 | HSDCは建築コストが多額なため、工期短縮等が求められている。 |
| **電力インフラ** | ● 無停電電源装置（UPS）<br>● 非常用発電機<br>● 燃料タンク<br>● 変圧器　等 | HSDCは電力中断が許されないため、冗長性・代替性の確保が必須。 |
| **冷却・空調インフラ** | ● チラー（冷却器）<br>● 冷却塔<br>● 熱交換器　等 | HSDCではGPUを搭載したサーバーも使うため、発熱量が大きく、高効率冷却が不可欠。最近は液冷等も登場。 |

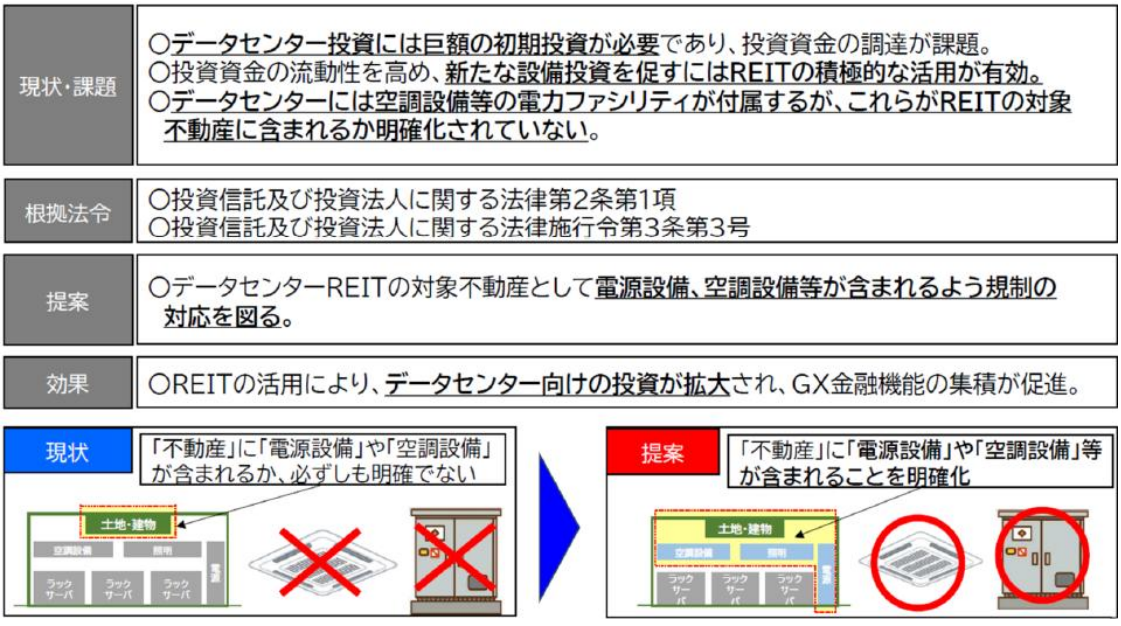
| 市場セグメント | 主な製品／サービス | 求められる要件、市場動向等 |
|---|---|---|
| **ITインフラ** | ● サーバー<br>● ストレージ<br>● ネットワーク機器　等 | HSDCのIT処理能力増強のための中心的市場。AI、大量データ処理、クラウド利用の拡大で需要急増。 |
| **保守サービス　等** | ● 保守サービス<br>● 緊急対応サービス | 信頼性確保が不可欠なため、ダウンタイム最小化を目的とするサービスが重要。インハウス運用ではなくアウトソーシングを活用する傾向あり。 |

### ■　データセンターREIT の動向

データセンターREIT（不動産投資信託）とは、データセンター施設へ投資する REIT のことで、データセンターの巨大な投資資金の調達を可能にし、市場の拡大を促進する役割を担う金融商品のことである。近年、NTT データグループがシンガポールにデータセンター専門の REIT を上場させるなど、日本でもデータセンターを投資対象とする動きが広がっている。

金融庁は 2025 年 6 月 23 日、「データセンターREIT の促進に関する提案」において、「データセンター内の設備（受変電設備、非常用発電設備、空調設備等）のうち一定の設置態様のものについては、特定資産である「不動産」に該当し、REIT への組入れが可能と考えられる。」との見解を発表している。これは、2025 年 5 月 29 日に北海道が国家戦略特別区域会議に「合同会議資料 13」として提出した提案を受けての見解であり、データセンター REIT の普及促進を後押しすることとなっている。データセンターは一般的なオフィス建物等と異なり、建物内に設置する電気・空調設備の投資コストが相対的に高い。そのため、それらインフラ投資に必要な資金を REIT で集めることができれば、日本におけるデータセンター、特に HSDC への投資が促進されることが期待できる。

■　図 3　データセンターREIT に関する国家戦略特別区域会議での提案




出典：金融庁説明資料　（データセンターの REIT への組入れについて）

## 2. ハイパースケール型データセンタービジネスにおけるリスク

### (1) データセンターにおけるインシデント

■ **実際に起きた近年のインシデント**

近年、大規模データセンターが停止するインシデントは多発しており、その原因は火災、システム障害、冷却異常、ヒューマンエラー等様々である。また、2024 年に発生した CrowdStrike 社のインシデントでは、Microsoft 社の Windows が停止する事態となったが、それにより運行の停止を強いられたとして利用者であるデルタ航空が CrowdStrike 社と Microsoft 社に対して 5 億ドルの損害賠償を請求する事態となった。

■ 表 3　2012 年以降に起きた主なデータセンター停止のインシデント

| 社名 | 発生年 | 分類 | インシデントの詳細 |
|---|---|---|---|
| CrowdStrike | 2024 | Failure | CrowdStrike のセキュリティソフトウェア「Falcon」のバグのある更新版が原因で、世界中の多数の Windows PC がブルースクリーンで停止する大規模なシステム障害が発生。この障害は航空、金融、小売等様々な業界で業務停止等の深刻な影響を引き起こし、復旧には最長 10 日間を要した。原因は、新しいサイバー攻撃手法に対応するための設定ファイル更新にロジックエラーが含まれていたためである。 |
| OVHcloud | 2021 | Fire | OVHcloud が運営するヨーロッパ最大級のデータセンターの一つが火災に見舞われ、複数の企業のデータが失われた。人的被害はなかったものの、サービスへの影響は甚大であった。 |
| Facebook | 2021 | Failure | Facebook（現 Meta）は DNS システムの更新に失敗し、6 時間以上にわたり世界的な障害に見舞われた。この問題は Facebook だけでなく、WhatsApp と Instagram にも影響を与えた。 |
| Equinix | 2020 | Extreme Weather | テキサス州にあるエクイニクスのデータセンターは、異常気象によりシステム障害に見舞われた。冷却システムが動作温度を維持できず、サービスが中断された。 |
| GitHub | 2018 | Failure | GitHub はデータベースレプリケーションの問題によりサーバー間でデータの不整合が発生し、24 時間以上にわたって障害に見舞われた。この障害は、GitHub プラットフォームを利用する数百万人の開発者に影響を与えた。 |
| Amazon Web Services（AWS） | 2017 | Outage | 定例運用中の人為的ミスにより複数の AWS サービスが停止し、Netflix、Slack、Pinterest といった大手企業に影響が出た。 |
| British Airways | 2017 | Disaster | ブリティッシュ・エアウェイズのデータセンターで障害が発生し、7 万 5,000 人以上の乗客に影響が出た。数百便が欠航となった。 |
| Delta Air Lines | 2016 | Failure | デルタ航空のデータセンターで電力システム障害が発生し、2,000 便以上の欠航が発生した。バックアップシステムも故障し、すべての予約システムとスケジュールシステムが利用できなくなった。 |
| Google | 2015 | Outage | Google Cloud が Gmail や Google ドライブ等のサービスに影響を与える大きな障害に見舞われた。根本的な原因は、負荷分散とネットワークインフラストラクチャの障害であった。 |
| Microsoft Azure | 2013 | Outage | Microsoft Azure は SSL 証明書の更新エラーにより障害に見舞われ、世界中の数百のユーザ影響が出た。証明書の有効期限切れにより、クラウドサービスがオフラインになった。 |
| Apple | 2012 | Failure | Apple は iCloud サービスで大規模な障害に見舞われ、数百万人のユーザがオンラインファイルやデータにアクセスできなくなった。この問題は、サーバーのアップグレードとデータコピーにおけるエラーが原因であった。 |

出典：https://www.linkedin.com/pulse/10-biggest-disasters-data-centre-history-how-could-rodriguez-antibon-w59of 等

■ **データセンターを狙った事件**

情報システム無くして社会が機能しない近年の状況にあって、データセンターは社会を混乱に陥れようとするテロリズムの標的になりつつある。以下は、2008 年以降に発生したデータセンターを標的としたテロリズムである。

■ 表４　2008 年以降に起きたデータセンターを標的としたテロリズム（各種資料より弊社作成）

| 社名 | 発生年 | 発生国 | 内容 |
|---|---|---|---|
| Amazon | 2021 | 米国 | 【データセンターの爆破を企てた男が逮捕】<br>容疑者は「Amazon のデータセンターをプラスチック爆弾で爆破し、『インターネットの 70%を殺す』」ことを計画。このことをメッセンジャーアプリ「Signal」で伝えられた人物が FBI に情報を提供したため、FBI が覆面捜査を開始。容疑者は「Amazon のデータセンターを攻撃し、アメリカで権力を握る『寡頭制』を崩壊させたい」という動機でテロを企てていたことが判明し、逮捕された。 |
| AT&T | 2020 | 米国 | 【通信大手・本社ビルの真正面でキャンピングカーが爆発】<br>AT＆T 本社ビルの真正面でキャンピングカーが爆発しサーバーが損傷、同社が運営する全国的なブロードバンドネットワークが停止した。関連するサーバーは、一時的にバッテリー電源に移行された後にバックアップ用発電機に移行するはずであったが、破裂した水道管から水が溢れ出し、発電機が浸水し動作しなくなった。そのため、2 日近くにわたり同ネットワークは停止した。 |

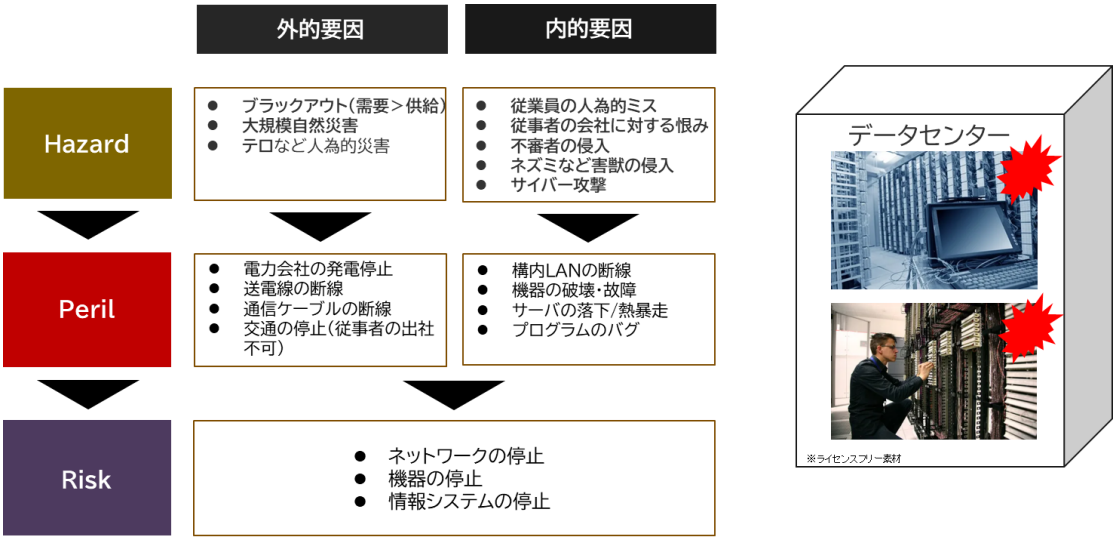
## (2) ハイパースケール型データセンタービジネスにおけるリスクの構造

■ **データセンターの停止リスク**

データセンターが停止した過去のインシデントを踏まえ、データセンターが停止するリスクを構造的に整理すると図４のようになる。ハザード（Hazard）とは、データセンターの停止という事態が発生する契機となるイベントであり、外的要因としては「ブラックアウト（電力需要が供給を上回ることによる突然の停電）」「大規模自然災害（大地震や水害等）」「テロリズム等の人為的災害」等が挙げられ、また内的要因としては「従業者による人為的ミス」「従事者の会社に対する恨みによる犯行」「不審者の侵入による犯行」「ネズミ等害獣の侵入」「サイバー攻撃」等が挙げられる。次にペリル（Peril）とは、ハザードによって引き起こされる事象であり、外的要因としては「電力会社の発電停止」「送電線の断線」「通信ケーブルの断線」「交通の停止（従事者の出社不可）」等が挙げられ、また内的要因としては「構内 LAN の断線」「機器の破壊・故障」「サーバーの落下/熱暴走」「プログラムのバグ」等が挙げられる。最後にリスク（Risk）であるが、ここではデータセンターが停止する具体的な事態を指し、「ネットワークの停止」「機器の停止」「情報システムの停止」等が挙げられる。

これらハザード、ペリル、リスクはデータセンターの規模に依らず、多額の投資を行い、セキュリティを高めているであろうHSDC においても想定しなくてはならないものである。

■ 図４ データセンターが停止するリスク（外的要因・内的要因）（弊社作成）

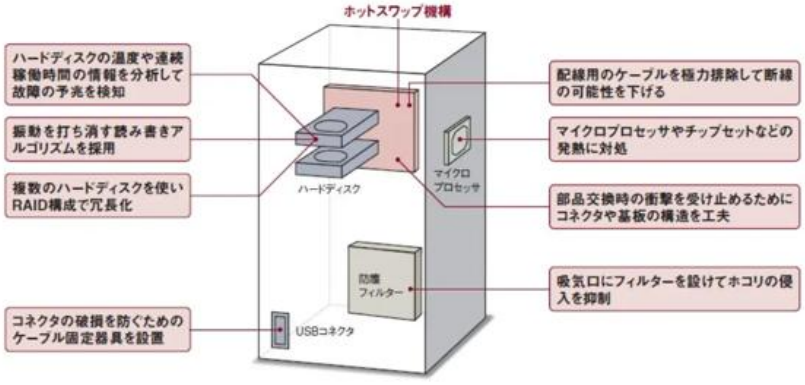



## ■ どういう状態により、サーバーが物理的に使用できなくなるのか

サーバーを動かす中央演算処理装置（CPU）は「100 度」を超えると熱暴走を起こし、使用できなくなる。また、AI の普及により利用が増えている画像処理装置（GPU）においても CPU と同様に熱に弱く、100 度を超えると熱暴走を起こし、使用できなくなる。これは、半導体の材料であるシリコンが熱に弱いなどの理由によるものである。

また、記憶装置であるハードディスク（HDD）についてであるが、内蔵されている磁気ヘッドは円盤と接触しないぎりぎりのところで動作するが、外部から強い衝撃を受けた場合には磁気ヘッドと円盤が接触してしまうことがあり（ヘッドクラッシュ）、接触した部分が傷となって磁性体が正しく読み書きできなくなる。通常はハードディスク側で衝撃を感知すると、磁気ヘッドを退避エリアへ移動することで故障を回避するようになっているが、突然の電源断等によりうまく動作しないことがある。なお、現在の HSDC では HDD だけでなくソリッドステートドライブ（SSD）が用いられることが増えているが、SSD は大規模集積回路（LSI）を搭載しているため、CPU や GPU と同様に熱に弱い特性を有している。

■ 図５ サーバーやデスクトップ機のハードウェア面での堅牢性を高める主な取り組み




出典：日経クロステック「特集「壊れないコンピュータ」(3) Part3 サーバー/デスクトップ／ホコリや活線挿抜と闘う」2005.10.04

## ■ HSDC における一般的な稼働停止リスク

以下に、HSDC における一般的な稼働停止リスクを外部要因、内部要因に分け整理する。なお、実際の HSDC におけるリスクは、地理的な特性や HSDC の特性、最終的に提供されるサービスの特性を踏まえ洗い出されるものであり、必ずしもこの限りではない。

■ 表 5　外部要因による稼働停止リスク（弊社作成）

| リスク分類 | | リスクシナリオ（ハザード） |
|---|---|---|
| ブラックアウト（需要＞供給） | 1 | 急な猛暑または厳冬の影響で急増した需要に供給が追い付かず、電力会社管内で突然の停電が発生。データセンター側で UPS は作動したものの非常用発電機の稼働が間に合わず、データセンター内で停電が発生 |
| 災害 | 2 | 線状降水帯が発生しデータセンターピット内に溜まった雨水で受電盤が浸水 |
| | 3 | 雷サージで敷地外の落雷が建屋に流入しデータセンター電源系統が壊滅 |
| | 4 | 隣接する施設で火災が発生。データセンターに延焼し、高温によりサーバーの CPU/GPU が熱暴走し損傷 |
| | 5 | 地震により運用スタッフが負傷し業務ができなくなったが、周辺火災により代替要員も駆け付けできず。直後から通信障害が起きたが鎮火までの間対処できず |
| | 6 | 地震の発生で交通機関が停止し、交替従事者が出社不能。 |
| 事件・事故 | 7 | 非常用電源で使用している石油等が搬入業者による搬入作業中に誤って漏れ、周辺環境を汚染し拠点が閉鎖 |
| | 8 | 病原菌を封入した封筒が送達され、開封した職員が死亡。保健所の命令により拠点封鎖 |
| | 9 | 警備に気づかれないままデータセンターの構内に侵入した者が、建屋外壁付近に爆弾入り小包を置き、爆発 |
| | 10 | 何者かが内部の送電線を切断、テナントへの送電が停止 |
| | 11 | 何者かが引き込まれている光ファイバーを全て切断 |

■ 表 6　内部要因による稼働停止リスク（弊社作成）

| リスク分類 | | リスクシナリオ(ハザード) |
|---|---|---|
| 従業員の人為的ミス | 1 | 通信ルータの管理者認証情報が推測可能なものだったことにより攻撃者がシステムに侵入、管理権限を乗っ取る |
| | 2 | 本来外部に公開するべきでないポートが誤って公開されていたことにより、データセンター内通信管理システムがサイバー攻撃を受けテナントサーバーがウイルスに感染 |
| 従事者の会社に対する恨み | 3 | 入構時の手荷物等の検査体制不備により、従事者がケーブルカッターを持ち込み、電源ルームに侵入し電源ケーブルを切断 |
| | 4 | 従事者がテナントのサーバールームに侵入し、FTP ソフト等がパソコンにインストールされた PC を LAN で直接接続しデータを窃取 |
| | 5 | 従事者がテナントのサーバールームに侵入し、サーバーを分解し記憶装置(SSD,HDD)を窃取 |
| 害獣の侵入 | 6 | マンホールの隙間からネズミが侵入。電源ケーブルを噛み切断 |
| サーバーの熱暴走 | 7 | 空調の自動制御装置に不具合が起きたためメンテ業者に依頼したが、駆け付けが迅速になされず |
| プログラムのバグ | 8 | ソフトウェアのバグに起因する障害が発生。通信に必要となる複数のサーバーでストレージにアクセス不能となり、サービス停止 |

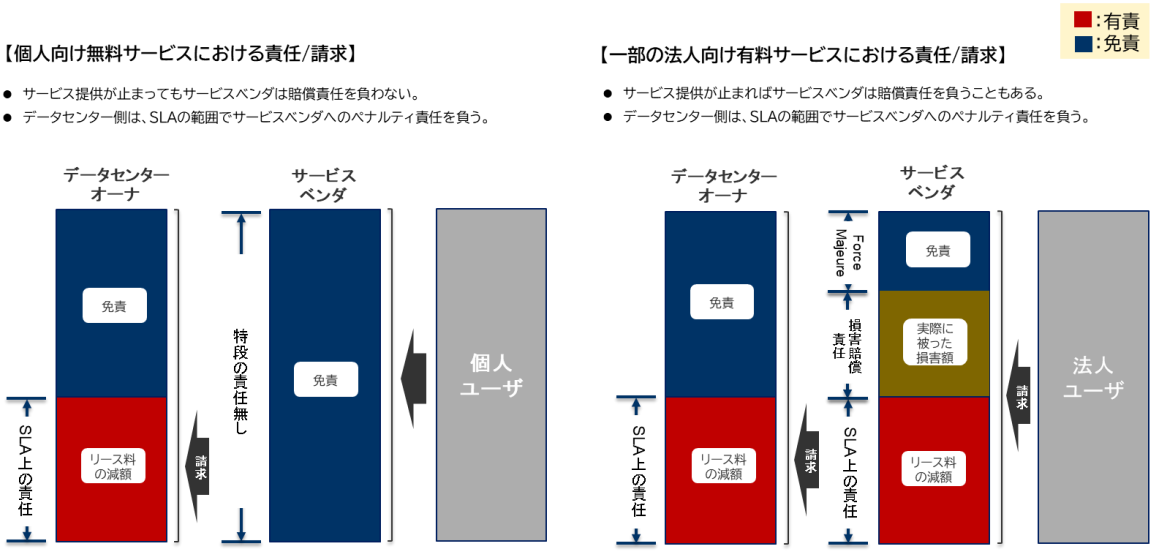
## (3) ハイパースケール型データセンタービジネスにおける責任範囲の考え方

### ■ クラウドサービスにおける責任範囲の考え方

クラウドサービスにおける責任範囲は、そのサービスが「個人向け無料サービス」「法人向け有料サービス」のいずれかによりその責任範囲は大きく異なる。個人向け無料サービスは、サービスが停止したとしてもサービスベンダ（GAFAM等）が個人から損害賠償請求を受けることはまず無い。そのため、データセンターや HSDC が停止した場合には、サービスベンダは SLA（サービスレベルアグリーメント）違反をペナルティとして課すことはあっても、個人からの損害賠償請求をデータセンターや HSDC のオーナー（貸主）に転嫁することはない[1]。

一方で、一部の法人向け有料サービスでは、CrowdStrike の事例でも分かるように、サービスが停止した場合には法人のエンドユーザがサービスベンダに対して損害賠償を請求することがある。そのため、データセンターや HSDC が停止した場合には、サービスベンダは SLA 違反によるペナルティに加え、法人らの損害賠償請求をデータセンターや HSDC のオーナー（貸主）にペナルティとして転嫁することもある。

■ 図 6 クラウドサービスにおける責任範囲の考え方（弊社作成）




### ■ データセンターにおける責任範囲の考え方（SLA）

詳細はホスティング（サーバー含めすべてを貸借）、ハウジング（建屋のみ貸借）といった貸与形態にもよるが、ホスティングにおいては以下のような SLA がデータセンターや HSDC のオーナーと、ユーザであるサービスベンダとの間で締結される。また、ペナルティについては「月額基本賃料×XX%」という形で定義されることが多い。

■ 表 7 クラウドサービスにおける責任範囲の考え方（各種資料を基に弊社作成）

| 分類 | | ペナルティの閾値（例） |
|---|---|---|
| **Notification Failure** | 通知失敗 | 停電、環境のダウンタイム、または接続不可の開始後 XX 分以内に通知しなかった場合 |
| **Root Cause Analysis** | 根本原因分析 | インシデント発生後 XX 日以内に、貸主はテナントのその時点の最新フォームを使用して根本原因分析を提供しない場合 |

[1] 個人情報漏洩のインシデントであった場合を除く

| 分類 | | ペナルティの閾値（例） |
|---|---|---|
| **System Failures** | システム障害 | セキュリティシステムの 1 つまたは複数が完全に機能しなくなった場合 |
| **Individual Component Failures** | 個々のコンポーネントの障害 | 個別のセキュリティシステムの 1 つまたは複数のコンポーネントが機能しなくなった場合 |
| **Certification Failures** | 認証失敗 | ISO27001[2]、SOC Type I/II[3]等要求される認証を維持しない場合 |
| **Software Update and Patching** | ソフトウェアの更新とパッチ適用 | 指定された XX 日間の期間内にセキュリティソフトウェアのアップデートが適用されなかった場合 |
| **Power Service Credit** | 電力サービスクレジット | 1 ヶ月間の電力供給率が XX%を下回った場合 |
| **Connection Availability Service Level and Credit** | 接続可用性サービスレベルとクレジット | 接続不可期間が発生した場合 |
| **Environmental, Health & Safety Service Credit** | 環境・健康・安全サービスクレジット | 指定された期間内に当該報告、調査、または是正を行わない場合 |

## 3. ハイパースケール型データセンタービジネスにおけるリスク対策

### (1) リスクシナリオの作成

前章までに解説した通り、HSDC には様々なリスクがあり、それらの多くは実際にインシデントとして顕在化している状況である。従って、HSDC の事業に参入を企図する場合、または既に HSDC のビジネスに参入している場合は自社におけるリスクを可視化し、適切なリスク対策を講じることでリスク量を低減させる必要がある。リスク量低減までの流れは以下の通りである。

**（１）リスクシナリオの作成**
**（２）予想最大損失の算定**
**（３）予想損失額・責任金額の算定**
**（４）発生可能性の検討**
**（５）リスク対策の検討・実施**

リスクシナリオの詳細化プロセスは以下の通りである。

■ 図 7　リスクシナリオの作成プロセス（弊社作成）


[2] 情報セキュリティマネジメントに関する国際規格

[3] 内部統制の評価。SOC Type I は「特定の時点」での内部統制の設計状況を評価するのに対し、Type II は「一定期間」の内部統制の設計と運用の有効性を評価する。

**① リスクカタログからのデータセンターリスク抽出**

- リスクカタログは、企業全体のリスク評価を実施する際に活用する一般的なカタログを活用
- HSDC の実地調査、HSDC におけるリスク事例調査を実施後に、リスクカタログをもとに検討を実施
- 本 HSDC 事業において、データセンターが停止する可能性のあるリスクを「ロングリスト対象」として抽出

**② ロングリストの作成**

- 調査結果とそこから検討できるリスクシナリオ（概略）を踏まえ、ハザード（原因）ベースでのリスクシナリオを作成

**③ ロングリストの概略評価**

- 各リスクシナリオについて、「可能性」「類似事例の有無」「影響度」の観点で概略評価

**④ ショートリストの作成**

- ロングリストにおける概略評価の結果、「可能性」があり、「類似事例」があり、「影響度」として、データセンターが少しでも停止する可能性があるリスクが「ショートリスト」の作成対象
- ロングリストで作成したハザード（原因）ベースのリスクシナリオにペリル（影響）ベースのリスクシナリオを加え、ハザード＋ペリルから成るリスクシナリオを作成

## (2) 予想最大損失の算定

予想最大損失（PML：Probable Maximum Loss)の算定は、以下を考慮する。

- SLA 違反が発生した場合のペナルティ
- サービスベンダの損害賠償額
- 不可抗力（Force Majeure）のため免責となるリスクの額

具体的な算定プロセスは以下の通りである。

■ 図 8 リスク量の計量プロセス（弊社作成）


**① 契約関係の把握・データセンター停止リスク整理**

- HSDC－サービスベンダ間の契約内容（ペナルティ/損害賠償条項）を確認
- HSDC 停止リスクと各リスクの責任範囲について整理
- 上記とは別に、既に検討されている HSDC の事業停止リスクについて確認

**② 調査・リスクシナリオの作成**

- 実地調査を実施しリスクを把握
- サーベイレポートの提供を受け、今回別に実施すべき事項を整理
- リスクシナリオを複数作成し、関係者間で意見交換を実施

**③ 予想損失の簡易評価・算定対象の決定**

- 停止期間検討のため、対象となるリスクシナリオについて、過去の類似事例を調査
- 各リスクシナリオにおけるサービスベンダの被害金額・停止期間について簡易的に見積り
- 特に賠償額が大規模になる可能性のあるリスクシナリオに絞り込み

**④ 予想最大損失の算定**

- サービスベンダより、当該 HSDC が停止した場合のコンティンジェンシープランについて確認
- エンドユーザの情報（エンドユーザへの提供サービス、一日あたり売上高等）をできる限り取得
- 各リスクシナリオにおけるユーザの被害金額（損害賠償金額）を見積り
- 上記の他、争訟費用、信頼回復広告費用等の見積もりを行い、予想賠償額を算定

## (3) 予想損失額・責任金額の算定

予想損失額・責任金額の算定は以下の要領で実施する。

■ 図 9　予想損失額・責任金額の算定（弊社作成）


**① テナント（サービスベンダ）の粗利益/資産の想定**

- サービスベンダから損害賠償請求を受ける場合、その内訳は「営業停止に伴う逸失利益」及び「損害を被った資産」になり得ることから、当該 HSDC 内におけるビジネスの粗利益、資産額を予め想定

**② 予想損害額の算定**

- 作成したショートリストを対象として、各リスクシナリオの予想損害額を算定
- 算定項目は以下の 3 種

  a.HSDC の損害

  b.テナントの損害

  b1.稼働停止による逸失利益額

  b2.有形固定資産の損害額

**③ SLA ペナルティ額の算定**

- SLA への該当/非該当を、リスクシナリオ毎に判断
- SLA 違反に該当するリスクシナリオについて、SLA に基づきペナルティ額を算定

**④ テナント（サービスベンダ）に対して負う予想責任額の算定**

- 各資料や、ステークホルダーからの情報に基づき責任分担を整理

## (4) 発生可能性の検討

各リスクシナリオにおける発生可能性についてフェルミ推定[4]等に基づく考察を行い、100 年間における発生確率、及び何年に 1 回発生する可能性があるかを推定

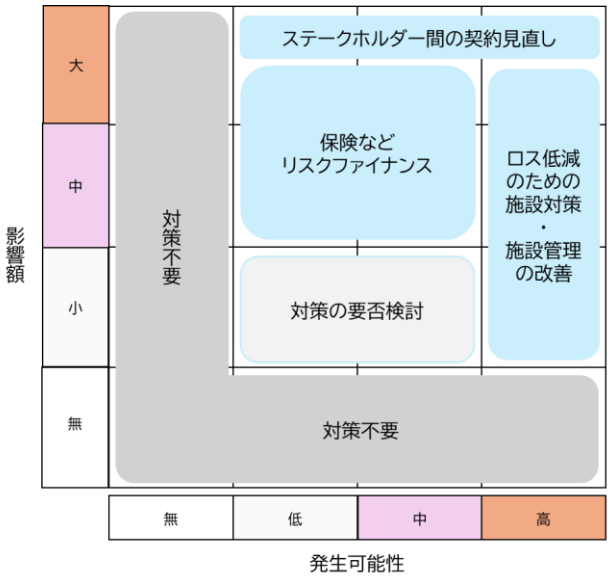
[4] 限られた情報をもとに論理的推論を駆使し、短時間で概算値を導き出す思考法

### (5) リスク対策の検討・実行

予想責任額、発生可能性がともに高いリスクシナリオについて、リスク低減のための対策を検討し実行する。

一般的な対策方針について、下図に記載する。

■ 図 10 リスク対策の考え方（弊社作成）




- **ステークホルダー間の契約見直し**
  自社にとって不利な契約となっており、転嫁の正当性を主張することが出来る条項については、交渉により契約の内容を見直す。
- **ロス低減のための施設対策・施設管理の改善**
  電力・冷却・空調・通信などのリスク対策を強化する、または警備体制を改善するための施策を検討し実行する。
- **保険などリスクファイナンス**
  上記によるリスク回避が困難である場合は、損害保険会社に相談し保険付保の可能性について検討する。また、その他リスクファイナンスについて検討する。

## 4. おわりに

ハイパースケール型データセンター（HSDC）については、GAFAM からの外部委託が増加しており、そのマーケットを狙ってデータセンタービジネスに新規参入する企業が増加している。一方で、データセンターの運営側には SLA（Service Level Agreement）等負うべきペナルティが大きく、データセンターの稼働が停止した場合の損失は巨額になることも想定される。以上のことから、新規参入企業においては HSDC が負う可能性のあるペナルティ、損害を PML（Probable Maximum Loss）として算定したうえで、事業の参入是非や参入時の対策を講じる必要がある。

[2025 年 10 月 21 日発行]

東京海上ディーアール株式会社

ビジネスリスク本部　青島　健二　上級主席研究員
ビジネスリスク本部　加藤　直人　主任研究員
〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6594 www.tokio-dr.co.jp