TOKIO MARINE

リスクマネジメント最前線

2021 | No.10

物理的要因によるデータセンターの停止リスクと、求められる事業継続対策

ビジネスリスク本部　上級主席研究員　青島　健二
専門分野：新規事業開発、業務/IT 改革、企業リスク管理、海外現地法人管理
経歴：製造業にて人事労務、経営企画部門の業務に従事後、IT 系シンクタンクにて各種コンサルティングに従事。2005 年より、東京海上ディーアールに勤務。その間、タイ国東京海上火災保険に 3 年間出向。

企業財産本部　上級主任研究員　坂場　律和
専門分野：自然災害リスク、気候変動リスク
経歴：保険引受に係る自然災害リスク評価モデル（主に地震・津波リスク評価モデル）の研究開発に従事。
現在、国内外の企業向けの自然災害リスク評価、気候変動リスク評価のコンサルティングを担当。

クラウド化の進展や EC の成長に伴い、世界中のデータセンターが増床、増加の一途をたどっている。一方で、データセンターはテロや故意の犯罪、自然災害等の影響を受けると稼働を停止し、情報システムに依存する全ての業務を停止させてしまうリスクをはらむ。本稿では、データセンターの特徴を整理したうえで、物理的要因により停止する諸リスク、及びそれらリスクへの対策について解説する。

1. データセンターへの依存を高める社会・企業

(1) データセンターへの期待の高まり

データセンターとは、サーバーやネットワーク機器を設置するために特別に作られた施設を指す。1950 年代に、主に大企業や金融機関など、巨大な組織の基幹システムなどに使用される大型コンピュータ「メインフレーム」が誕生し、組織における業務の集中処理の仕組みとして 1960 年代より普及していったが、メインフレームが停止することは業務が停止することに直結するため、メインフレームはミッションクリティカル（常時稼働）が前提であった。一方で、サーバーやネットワーク機器は一種の精密機器であり、熱や衝撃に弱いため、その設置場所は一般のオフィスよりも堅牢な場所であることが求められた。それが、データセンター誕生の背景である。その後、以下の経緯を経て、データセンターは拠点数、延べ床面積数ともに右肩上がりの一途を辿っている。

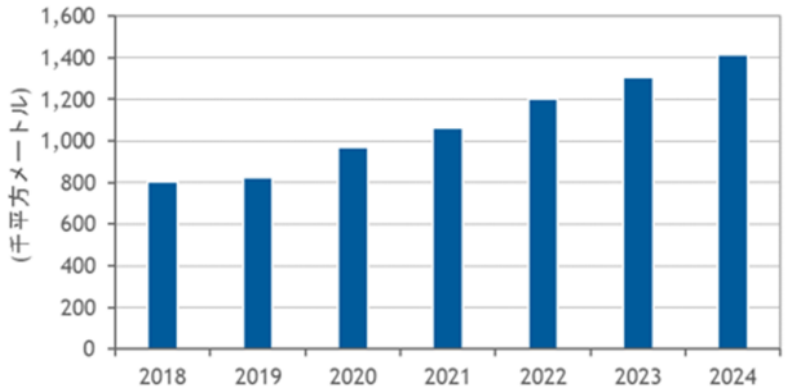
- 1960 年代以降、全国の金融機関（主として銀行）が、十分な耐荷重をもち空調設備や電力設備を備えた「電算センター」を建設し運用するようになった。この電算センターがデータセンターの起源となっている。
- 1990 年代、Windows 端末などの普及により、組織における業務処理は集中処理から分散化の方向に IT トレンドが転換していった。一方で、同年代にインターネットが普及し、「インターネットサービスプロバイダ」関連事業の需要が急拡大した。組織の情報システムが「分散化」に転換していく中で、存在意義を問われた電算センタ

ーの一部は、インターネット関連事業に商機を見出し、「インターネットデータセンター」に事業を転換した。ここから、データセンターの市場は急拡大する。

- 2000 年代に入り、いわゆる「クラウド」型のネットサービスを提供する「アプリケーションプロバイダー」事業者が急増し、データセンターの需要はさらに拡大する。

2021 年現在、日本国内にあるアウトソーシングとしてのデータセンター数[1]は 247、延床面積は 246 万㎡とされている。IT 専門調査会社の IDC Japan によれば、データセンターサービス市場における 2020 年～2025 年の年間平均成長率は 12.5%と、今後も需要の拡大が予想されている。下表は同社が予想する、日本国内におけるデータセンターの延床面積推移である。

■ 図表 1 日本国内におけるデータセンターの延床面積推移



出典：IDC Japan（国内ハイパースケールデータセンター 延床面積予測： 2019 年～2025 年）

2．データセンターの特徴とはらむリスク

(1) データセンターの主要機能と停止事例

データセンターの主たる構成とリスク管理の観点から求められる要件、それと過去に発生したデータセンターが停止した事例は以下の通りである。

■ 建物

データセンターの建物は、建物内に保持するサーバーの数によりその規模が異なる。日本最大のデータセンターである「アット東京 中央センター」は 9 階建てで、総床面積は 14 万㎡（東京ドームの約 3 倍）もあるが、一方で、建物の 1 フロアをサーバールームとして使用しているものの、そこを「データセンター」と呼称している場合もある。

データセンターの建物に求められる要件は、「建物内で保持しているサーバーを、データセンターの立地場所で想定しうる全ての状況下で、安全に保持できること」である。日本国内においては、「地震」と「水害」への対策が特に重視され、データセンターサービス事業者は、それら自然災害への対策を万全にすることは営業戦略上必要不可欠となっている。地震対策としては、立地場所で想定しうる最大の地震に見舞われても建物が倒壊・崩壊しないことに加え、揺れによりフロアの天井が落下する、床が抜けるなどしてサーバーを損傷させないことが前提

[1] データセンター協会に登録されているアウトソーシングとしてのデータセンター数

である。また、台風や大雨、さらには津波や高潮など水害対策としては、想定しうる最大の水害が発生しても、サーバーが浸水被害に遭わないことが標準仕様といえる。

ただし、自前でデータセンターを保持している組織における対策は、データセンターサービス事業者のそれと比して脆弱な状況にある。2011 年に発生した東日本大震災では、政府機関において、地震の揺れの影響で情報システムが設置されている建屋 31 棟が損傷し、4 棟では保持していたサーバーが損傷した。また、津波の影響で情報システムが設置されている建屋 4 棟が損傷し、1 棟では保持していたサーバーが浸水した[2]。

■ 監視室

データセンター内に設置する監視室に求められる要件は、「ユーティリティと人を常時監視できること」である。ユーティリティに関して言えば、サーバールームの室内温度が許容範囲内に維持されていること、サーバールームへの電源供給が安定的になされていること、通信速度が許容範囲内に維持されていることの 3 点をモニターすることであり、人に関して言えば、データセンター内の勤務者に不審な挙動が無いか、または外部から不審者が侵入しようとしていないか、監視カメラや人感センサー等の状況をモニターすることである。

サーバーで格納されている情報資産は、アプリケーションプログラム（いわゆる情報システム）、取引データ、顧客情報など様々あるが、いずれもデータを保持する組織からすれば事業を継続するうえで必要不可欠な情報であり、また価値の高い資産でもある。従い、時に「窃取」の対象となり、またデータセンターを運営または活用する組織に不満を持つ者や、社会に不満を持つ者による「攻撃」の対象ともなり得る。2021 年 4 月には、米・バージニア州に立地している Amazon 社のデータセンターへの「攻撃」（プラスチック爆弾による爆破）を試みた男が、FBI（米・連邦捜査局）の覆面捜査官によって逮捕された。犯人は、同年 1 月に発生した連邦議会・議事堂襲撃事件[3]ではライフル銃を持って侵入した者であった[4]。

■ 電源供給設備

電源供給設備に求められる要件は、「供給を一瞬たりとも止めないこと」である。電力会社からの受電が停止した瞬間に、無停電電源装置[5]が起動し、一瞬も電力の供給が停止することなく非常用発電機の稼働に切り替わる仕組みを備えていることが条件である。

2007 年に発生した、米・テキサス州の変電施設にトラックが衝突し爆発した事件では、変電施設が破壊されたために大規模な停電が発生、同州に立地していたホスティング会社・Rackspace 社のデータセンターは空調が急停止した。急激な温度上昇によるサーバー損傷の危険性が高まったため、同社は自発的に稼働を数時間停止させた[6]。

---

[2] 内閣官房情報セキュリティセンター「東日本大震災における政府機関の情報システムに対する被害状況調査及び分析（最終報告書）」平成 24 年 3 月

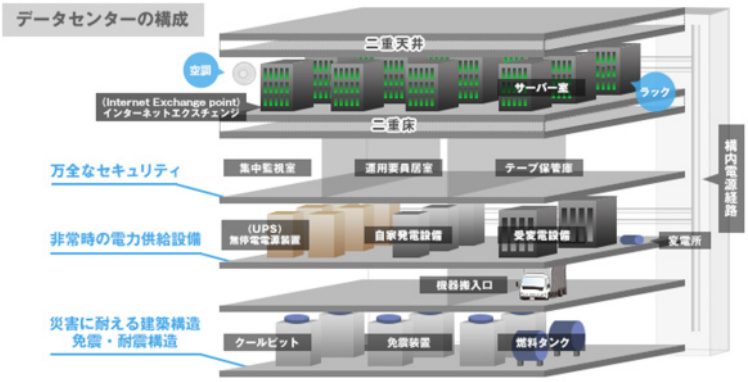
[3] 2021 年 1 月 6 日にアメリカ合衆国で起きた政治的な暴動事件。当時大統領であったドナルド・トランプの支持者らが、「2020 年のアメリカ合衆国大統領選挙で選挙不正があった」と訴えて、アメリカ合衆国議会（連邦議会）が開かれていた議事堂を襲撃した。議事は中断され、議会機能が一時的に喪失した。

[4] https://gigazine.net/news/20210412-arrest-blow-up-aws/

[5] 停電などによって電力が断たれた場合にも電力を供給し続ける電源装置。日本では一般に、商用交流電源に接続して使用するものを UPS（Uninterruptible Power Supply）と呼ぶことが多い。

[6] https://gigaom.com/2007/11/12/rackspace-outage-hits-home/

■ 図表２ データセンターの基本構成



出典：IT トレンド（https://it-trend.jp/data_center/article/function）

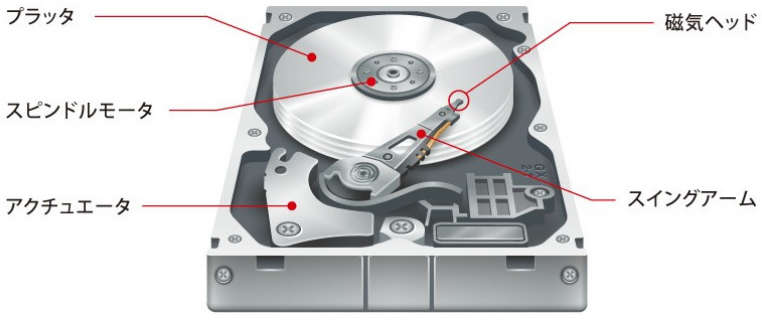
(2) どういう状態により、サーバーが使用できなくなるのか

データセンターで使用されるサーバーは、クライアント PC（いわゆる端末）と同様に CPU、メモリ、ストレージ等から構成される。ストレージについて、クライアント PC では SSD（Solid State Drive）が用いられることも増えてきているが、サーバーにおいてはほぼ全てハードディスク（Hard Disk Drive）が採用されている。ハードディスクが採用されている主たる理由として、SSD と比べ 1 ドライブで保存できるデータ量が大きいこと、保存データ量あたりの費用が比較的安価であることが挙げられる。

ハードディスクは、磁性体を塗布または蒸着したプラッタ（円盤状の金属ディスク）を一定の間隔で何枚も重ね合わせた構造になっており、これをモーターで高速に回転させたうえで、磁気ヘッドを近づけ磁性体を磁化させてデータの読み書きを実行している。ハードディスクの磁気ヘッドは、通常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円盤と接触してしまうことがあり、これをヘッドクラッシュという。ヘッドクラッシュが発生すると、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。ハードディスクが衝撃を感知すると、磁気ヘッドを退避エリアへ移動することでヘッドクラッシュによる故障を回避する仕組みにはなっているが、突然の衝撃や突然の電源遮断などに、この回避がうまく機能しないことがある。

また、サーバーを動かす CPU は熱に弱く、摂氏 100 度を超えると熱暴走（発熱が更なる発熱を招き、温度制御ができなくなる現象）を起こし使用出来なくなる。従い、「突然の衝撃」「突然の電源遮断」が発生、あるいは「突然の高熱」に晒されるとサーバーは使用できなくなる。

■ 図表３ ハードディスクドライブの基本構成



出典：バッファロー社（https://www.buffalo.jp/topics/trouble/detail/recovery_0042.html）

(3) サーバーを停止させるリスク

① テロリズム

テロリズム（以下「テロ」と略称：何らかの目的を達成するために暴力や脅迫を用いること）は、政治的に不安定な国で発生することが多いが、日本でも過去 50 年間で、少なくとも 100 件以上のテロが確認されている。テロの手法は様々であるが、データセンターが最も恐れるべきテロは、サーバーに急な衝撃を与えるようなテロであり、具体的には爆弾テロがそれに該当する。爆弾テロに関して、米国の国土安全保障省（United States Department of Homeland Security: DHS）は人命安全の見地で「屋内外問わず、確保すべき最低限の避難距離」を「絶対避難距離（Mandatory Evacuation Distance）」、「安全距離まで避難を継続するべき距離」を「継続避難・屋内退避圏（Shelter-in-place zone）」、「爆発による被害リスクが小さい距離」を「安全距離（Preferred Evacuation Distance）」と定義している。また、爆弾テロの手口別に安全距離の目安を以下の通り示している。

■ 図表４ 爆弾テロの手口別 「安全距離」

爆弾テロの手口	TNT[7]換算 爆薬量	安全距離[8]
封筒/手紙爆弾	450g	280m
パイプ爆弾	2.25kg	370m
パッケージ爆弾	4.5kg	330m
自爆ベスト/小型容器	9kg	520m
小包	22.5kg	560m
小型乗用車	225kg	580m
中型乗用車/ミニバン	450kg	730m
大型版/SUV/ピックアップトラック	1.8kt	1,200m
配送用トラック	4.5kt	1,600m

出典：国土安全保障省（United States Department of Homeland Security: DHS）資料

一般的なハードディスクは、200Ｇ（目安：2 kgの重りを 1mの高さから落下させた際の重力）の衝撃を受けると使用できなくなるが、人間が安全を確保するために出来るだけ確保したい「安全距離」であっても、受ける衝撃は200G 以上がかかるものと思われる。従い、安全距離で該当する爆弾テロが発生した場合には、ハードディスクが損傷し、データセンターは停止に至る可能性が高い。例えば、データセンターの保守業者を装ったテロリストがポケットに封筒爆弾を忍ばせて館内のサーバールームに侵入し、サーバー近くで爆発させるようなテロや、爆発物を積載したトラックを運転するテロリストがデータセンターに向けて直進し、建物への衝突により爆破させるようなテロが発生することなどが想定される。

日本では、1974 年に三菱重工業東京本社ビルの 1 階出入り口のフラワーポット脇に仕掛けられた時限爆弾が爆発し、1 階部分が破壊され玄関ロビーが大破、ビル内に入った衝撃波がビル内部も破壊するテロが発生している。次の表は、近年爆発の影響で停止したデータセンターの事例である。

[7] トリニトロトルエン(trinitrotoluene)を主成分とする爆弾

[8] 屋外・遮蔽物が無い場所における安全距離

■ 図表 5 爆発の影響で停止したデータセンターの事例

発生年	概要	内容
2021 年	Amazon のデータセンターを爆破して「インターネットの 70％の破壊」を企てた男が逮捕	2021 年 1 月、容疑者は「Amazon のデータセンターをプラスチック爆弾(C-4)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。同年 3 月、情報提供者は容疑者に対して「爆発物の提供者」を紹介。この爆発物提供者は、FBI の覆面捜査官だったが、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」と述べたとのこと。同年 4 月、容疑者は FBI の覆面捜査官との「偽物の爆弾」の取引に応じ、待機していた別の FBI 捜査官によって逮捕。
2020 年	AT&T 本社ビルの真正面でキャンピングカーが爆発	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。その後、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、その後ようやく復旧した。
2008 年	The Planet のデータセンターで爆発	The Planet 社のデータセンターで電気関係の設備がショートしたことによる爆発が発生した。爆発によりサーバーやネットワーク機器が損傷することはなかったが、火事になったため消防署からの指導で非常用発電機を動かすことができず、すべての機器が電源を喪失し、通信遮断の状態となった。インシデントは土曜日の夕方 5 時に発生したが、復旧したのは翌日曜日の午後遅い時間であった。その間、顧客から預かっていた 9,000 台のサーバーに影響が生じた。

出典：各種情報をもとに弊社作成

② 故意の犯罪

データセンターを有する組織や、データセンターが預かる情報システムの利用者に恨みを持つ内部関係者が、腹いせや報復目的で電源を遮断し、データセンターを停止させるリスクも存在する。UPS をオフにしたうえでサーバーの電源を遮断すれば、データセンター内のサーバーは安全停止のための機構が正しく作動しないまま停止するため、復旧が困難となる可能性がある。

類似事例ではあるが、2021 年 8 月には警視庁に勤務する 33 歳の男性職員が、前日に上司から注意されたことの腹いせに、該当サーバーにアクセスして 26 万人分の運転免許証データを削除する事件が発生している。

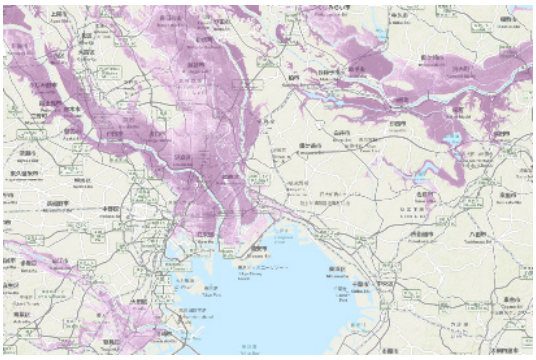
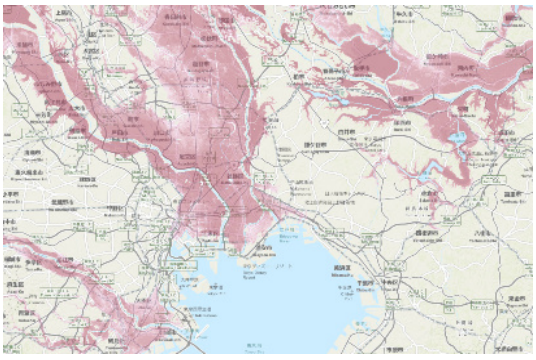
③ 自然災害

一般に、施設に影響を与える自然災害としては、主に地震（地震動、津波、地震火災、液状化）、火山噴火、強風、河川氾濫、内水氾濫、高潮氾濫、地滑り・斜面崩壊、積雪、落雷などが挙げられる。データセンターは高い事業継続性が求められるため、立地選定の段階より周辺環境の自然災害リスク調査を行い、リスクが低い地域が建設地として選定される。仮に、建設地のリスクが高い場合には、ハードおよびソフトの両面にて、発災時の対策・対応を定めていることが多い。しかし、自然災害リスクは一度評価すれば終わりではなく、気候変動等の環境変化や学術的知見等の更新等によって、定期的に見直されるべきものである。自然災害リスクの見直しによって、建設時には十分であった対策・対応が現在においては不十分になる可能性もあり得る。特に、日本では、耐震性の確保等、一般に地震対策が主な災害対策として取り組まれており、地震以外の自然災害への注目度が低い。そのため、地震以外

の自然災害への対策・対応についても、最新の情報をもとに再確認することが望ましい。特に近年、河川氾濫による水災リスクと降灰による火山噴火リスクは、近年の水害発生状況や科学的見地に基づき大きく変化している。

河川氾濫は、2015 年に水防法の改正にはじまり、国土交通省がハザード情報の整備・拡充を推し進めている[9]。2015 年の水防法の改正によって、従来「数十年～数百年に 1 度の降雨（計画規模）への対策・対応」を計画していたのに対し、「1000 年に 1 度の降雨（想定最大規模）への対策・対応」を計画するようになった。この背景として、近年、時間雨量 50mm を超える雨が頻発するなど、雨の降り方が局地化・集中化・激甚化することで、水災被害が多発していることが挙げられる。この被害傾向は、気候変動等の気象環境の変化によって更に増すことが懸念されており、想定外の事態を視野にいれた対策・対応が望まれている。国土交通省では、想定最大規模の降雨に対応した洪水浸水想定区域のハザードマップの作成を進めており、現在、国管理河川の 448 河川、都道府県管理河川の 1,291 河川の情報開示がされているが、今後更に約 19,000 河川の情報開示についても検討されている。このように河川氾濫のハザードマップは情報更新が頻繁に行われるため、今後、データセンター建設時に想定していなかったリスクが顕在化する可能性がある。データセンターが浸水した場合、電気設備等が機能不全を起こし、システム停止に至る可能性が高く、十分な対策・対応が望まれる。

■ 図表 6 計画規模と最大想定規模の浸水図の比較

	計画規模シナリオ	想定最大規模シナリオ
概要	数十年～数百年に 1 回程度の雨を想定 河川整備の基本方針となる降雨	約 1,000 年に 1 回程度の雨を想定 想定し得る最大規模の降雨
浸水図		
補足	想定最大規模のハザードマップは 2015 年以降、順次公開。	

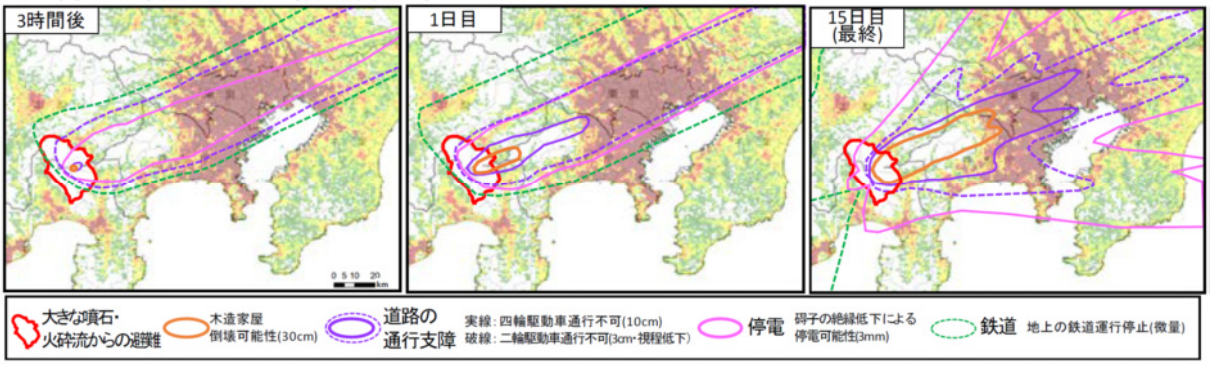
出典：国土交通省 浸水想定区域図の浸水情報をもとに弊社作成

また、日本は 111 の活火山を有しており、これらが噴火した場合は、噴石、火砕流、火山泥流、溶岩流、火山ガス、火山灰等の災害が発生する。噴石や火砕流等が影響するエリアに該当しない場合であっても、火山灰は広域に分布するため、データセンターに影響を与える可能性が高い。しかし、施設の降灰への備えは十分に進んでいるとは言い難い。降灰による影響や対策の検討事例としては、内閣府が 2020 年 4 月 1 日に富士山噴火時の首都圏への

9 国土交通省「洪水浸水想定区域及び洪水ハザードマップ作成・公表状況」
https://www.mlit.go.jp/river/bousai/main/saigai/tisiki/syozaiti/

降灰影響を公開している[10]。内閣府によると、大規模噴火が発生した際は、山麓のみならず、広い範囲にわたって火山灰が堆積する可能性があることを示唆しており、降灰により、鉄道・道路・物資・人の移動の停止や制限、電力停電や通信障害、上水道の断水等のライフラインの断絶の可能性がある。データセンターへの影響としては、屋上設置の熱交換器に火山灰が付着することによる冷却システムや空調システムの機能不全、発電所の発電量低下や配電網被害からの電力供給量低下の発生等が想定される。そのため、冷却システムや電力システムに十分な冗長性がない場合、システム停止に至る可能性が非常に高いと想定される。

■ 図表 7 西南西風卓越ケースの場合、降雨時の降灰分布とその影響



出典：内閣府中央防災会議防災対策実行会議大規模噴火時の広域降灰対策検討ワーキンググループ

河川氾濫、火山噴火のように広域に影響する災害では、サーバーを運用するデータセンターが堅牢でも、そこに至るインフラやネットワークが断絶し、サーバーが利用できないといった事態を招くことが懸念される。インフラやネットワークが復旧すればサーバーは利用できるが、復旧までの期間については事業に何らかの支障が生じることは避けられない。データセンター周辺の被災状況も含め、立地周辺で想定される全ての自然災害リスクについて、今一度対策・対応を見直す必要がある。

3．データセンターの事業継続上求められる対策

(1) 基本戦略

データセンターが許容できる稼働停止時間は、データセンターが運用している情報システムに紐づく業務が許容できる停止時間と、データセンターが停止した場合の、情報システムに依存しない業務継続方法の有無に依存する。例えば、電力や通信の運用に直接関係するデータセンターについては、電力の供給や通信サービスは 24 時間 365 日途切れなく提供されるものであるので、基本的に「無停止」であることが要件であるが、企業の人事部門の方が使用する、翌年度の教育計画を策定する等の業務は、少なくとも勤務時間外には停止してもよく、さらに言えば紙で策定することもできるので、情報システムは数か月停止しても許容されるかもしれない。

上記は、データセンターにおけるバックアップ戦略として検討すべきものであり、その戦略のオプションは基本的には以下の 3 種類がある。

[10] 内閣府中央防災会議防災対策実行会議大規模噴火時の広域降灰対策検討ワーキンググループ「大規模噴火時の広域降灰対策について首都圏における降灰の影響と対策―～富士山噴火をモデルケースに～報告）令和２年４月」
http://www.bousai.go.jp/kazan/kouikikouhaiworking/pdf/syutohonbun

① ホットスタンバイ

・データセンターをデュアルで同時稼働させておき、本番センターが停止した場合には同期するバックアップセンターへ瞬時に切り替える方式。稼働停止を回避するための絶対的な対策ではあるがデータセンターの構築コストや保守・運用要員の人件費などが単純に 2 倍となるため、基本的には無停止が要求される業務に紐づくデータセンターにのみ用いられる戦略。

・バックアップセンターは、本番センターと同時被災しないことが絶対条件であるので、本番センターが関東に所在する場合は関西以西とされることが多く、一部のグローバル企業ではシンガポールなど海外にバックアップセンターを有していることもある。

② コールドスタンバイ

・通常時は稼働していないバックアップセンター（情報システムは本番センターのものが複製されている）を保有しておき、本番センターが停止した場合には同期するバックアップセンターへ切り替える方式。バックアップセンターは日頃保守・運用がなされていないため、切り替えにあたっては情報システムのプログラム更新や、本番センターで使用されていたトランザクションデータの移管、さらには運用要員の新規アサインメントなども必要となるため、瞬時の切り替えは不可能であり、一般的には 1 週間程度は要するとされる。

③ データバックアップ

・トランザクションデータのみ定期的に複製し、保管しておく方式。データセンターのバックアップが無いため、データセンター内のサーバーが使用できなくなった場合は、情報システムを再度構築する必要がありその期間は一般的には数か月を要するとされる。

銀行の決済、金融の勘定系システムや交通機関の運行システムなど、ミッションクリティカルな情報システムはホットスタンバイ、またはコールドスタンバイであることが多く、一方で製造業やサービス業などではデータバックアップのみであることが多い。

■ 図表 8 目標復旧時間と採用するバックアップ方式

	システムの目標復旧時間 RTO（Recovery Time Objective）		
	1 日以内	1 か月以内 （その間手対応）	数か月以内 （その間手対応）
バックアップ 方式	ホットスタンバイ	コールドスタンバイ	データバックアップ
代表的な業種	社会インフラ・運用系（電力、通信、交通、銀行）	社会インフラ・情報系（電力、通信、交通、銀行）	製造業、小売業、サービス業全般

(2) 本番センターにおけるリスク別対策

既述の通り、データセンターを停止させないための絶対的な対策は、ホットスタンバイ戦略を採用し実行することであるが、多額のコストを要するため、全てのデータセンターが採用できる戦略ではない。従って、本番センターを停止させないための対策をリスク別に検討し実行することが重要である。以下に、データセンターを物理的に停止させる主なリスクである「テロ」「故意の犯罪」」「自然災害」それぞれについて、基本的な対策を記載する。

① テロ

テロからデータセンターを防御するための対策について、以下の通り整理する。テロ対策は、不審者や不審車両を早期に発見するための警備体制の構築、及び警備に必要な機器を備えることが重要である。

■ 警備体制
- 不審者や不審車両を発見するための警備管理組織・体制の構築

■ 施設・機器
- 死角の無い監視装置
- 迅速に連絡を取るために十分な通信機材

■ 図表 9 テロ対策を確認するためのチェックリスト（例）

項目	チェック事項	確認事項
体制	警備管理組織	①警備責任者
		②実施部門
		③警備委託会社
	警備体制	①営業時間中の警備体制（人数）
		②営業時間外の警備体制（人数）
施設・機器	警備室等の状況	①警備センター・門衛詰め所等の設置状況
		②警備システムの制御・表示装置等の設置場所
	警備システムの構成	①監視装置の構成
		②警報装置の構成
		③集中制御・表示装置の構成
	監視装置の機能・性能	①センサー・カメラ等の機能・性能
		②CCTV（監視カメラ）の設置場所
	警報装置の機能・性能	①警報の種類・表示方式
		②警報の通知先
	集中制御・表示装置の機能・性能	①集中制御の範囲
		②設置場所・表示方式・性能
	通信機材	①警備用可搬通信機材の台数・機能
		②緊急用固定電話の設置場所・機能

② 故意の犯罪

内部犯行による故意の犯罪からデータセンターを防御するための対策について、以下の通り整理する。内部犯行者は、事前に下見を行ったうえで計画的に犯行に及ぶことも多いことから、日頃から監視カメラ等の映像記録や入出記録を点検し、不審な行動を行っている者がいないか確認すること、またデータセンターの存在・仕様に関する機密事項を漏洩しない体制であることを確認することが重要である。

- 体制
  - 不審者を発見するための警備管理組織・体制の構築
- 機器
  - 死角の無い監視装置
  - 監視データの保管
- 入出管理
  - 入出許可条件・申請状況の点検
  - 実際の入出記録の確認
- 情報管理
  - データセンター（DC）の存在・仕様に関する秘匿管理状況の点検

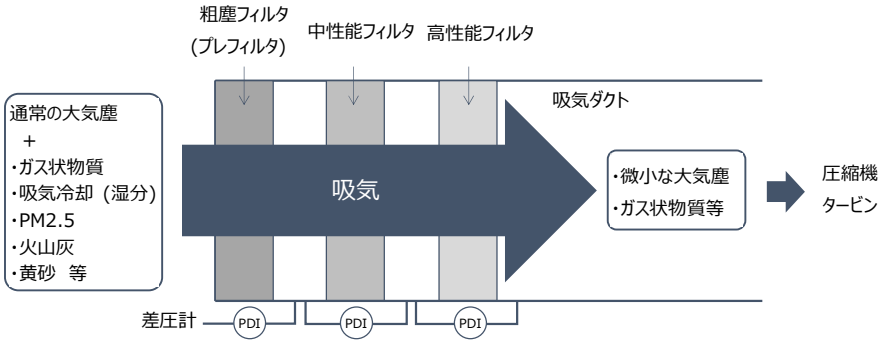
■ 図表 10 内部犯行を抑止するための対策チェックリスト（例）

項目	チェック事項	確認事項
体制	警備管理組織	①警備責任者
		②実施部門
		③警備委託会社
	警備体制	①営業時間中の警備体制（人数）
		②営業時間外の警備体制（人数）
機器	監視装置の機能・性能	①センサー・カメラ等の機能・性能
		②CCTV の設置場所（建屋内）
		③死角の有無
		④監視データの記録
入出理	入出許認可	①恒常的な人・車両の入出許可条件・申請状況
		②臨時の人・車両の入出許可条件・申請状況
		③重要区画への入出許可条件・申請状況
	入出記録	①DC エントランス等の入出記録
		②重要区画への入出記録
情報管理	DC の存在・仕様に関する秘匿	①社員との守秘義務契約
		②警備会社との守秘義務契約
		③派遣元会社との守秘義務契約

③ 自然災害

データセンターへの自然災害への対策・対応を講じる際の指針として、例えば、日本データセンター協会によるデータセンターファシリティスタンダードが挙げられる[11]。本指針では、地震や火災が発生した際のデータセンターが目標とするサービスレベルを示している。本指針等を参考に、近年のデータセンターは免震構造の採用等、地震対策については十分に検討されていることが多い。しかし、近年、気候変動をはじめとして、データセンター建設当時は想定していなかった自然災害リスクの注目度が高まっている。データセンターは、いかなる事態にも、迅速・適切な危機管理対応が求められる。データセンターの立地周辺でどのような自然災害リスクが存在し、どのような被害が発生するのかを把握し、リスクの認知、対策・対応を進めることが重要である。過去の経験や知識を活用するとともに、必要な最新情報を収集していくことで、想定を超えた事象にも柔軟に対応できるような体制を構築しておくことが望ましい。

■ 図表 11 自然災害（河川氾濫及び火山噴火）に関する対策検討の方向性（例）

項目	対策検討の方向性
河川氾濫	当該地域で発生する浸水深の把握を第一に、想定する浸水規模に対して十分な高さの止水板の設置や主要建築設備の嵩上げが望まれる。また、浸水規模によっては十分な対策を講じることができないことも予想される。その際は移転等を含めた議論が必要となる。
火山噴火	外気を利用しない冷却装置の設置や、空調に高性能フィルタを設置する等が有効である。特に、空調に関しては、火山灰が内部まで入り込むため、電子基盤への付着、内部堆積、冷却水への混入等が発生し、空調の機能損失に繋がる事例が報告されている。内閣府の検討においても、降灰に対応した高性能フィルタを有した空調設備が対策の一例として提案されている。 [空調設備の降灰対策の一例] 

出典：内閣府中央防災会議防災対策実行会議大規模噴火時の広域降灰対策検討ワーキンググループ

[11] 日本データセンター協会「データセンターファシリティスタンダード」 https://www.jdcc.or.jp/

4. まとめ

本稿では、クラウド化の進展や EC の成長に伴い、ますます重要性を増しているデータセンターが物理的要因により停止する主なリスクと、それに対して求められる事業継続対策について解説した。本稿が、データセンターに関わる方に対する何らかのヒントとなれば幸いである。

[2021 年 12 月 29 日発行]

To Be a Good Company

東京海上ディーアール株式会社

ビジネスリスク本部　上級主席研究員　青島　健二（専門分野：新規事業開発、業務/IT 改革、企業リスク管理、海外現地法人管理）
企業財産本部　上級主任研究員　坂場　律和（専門分野：自然災害リスク、気候変動リスク）
〒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.tokiorisk.co.jp