World Trend Foresight

拡大するデータセンターのリスク管理
—日本の課題と対策—

2025 年 2 月

PwC コンサルティング合同会社
PwC Intelligence マネージャー　富澤寿則

リモートワークの普及やクラウドコンピューティングの進展、そして生成 AI の需要拡大により、データセンターの需要が増加している。企業や公共機関は、効率的なデータ管理と運用のために活用しており、特に、IT・テクノロジー企業や金融機関、通信事業者などは、データセンターを通じて高度なサービスを提供している。データセンターは、サーバーやストレージデバイス、ネットワーク機器などの通信面のハードウェアと管理ソフトウェア、さらには、電源供給装置・冷却装置など施設面のハードウェアを組み合わせた複雑なシステムである。24 時間体制で運用されており、クラウドサービスやウェブホスティング、データストレージなどの機能を提供している。これにより、企業や公共機関は効率的なデータ管理と運用を実現しており、データセンターは現代の情報社会においてもはや欠かせない存在となっており、日本を含め世界中で建設が進められている。

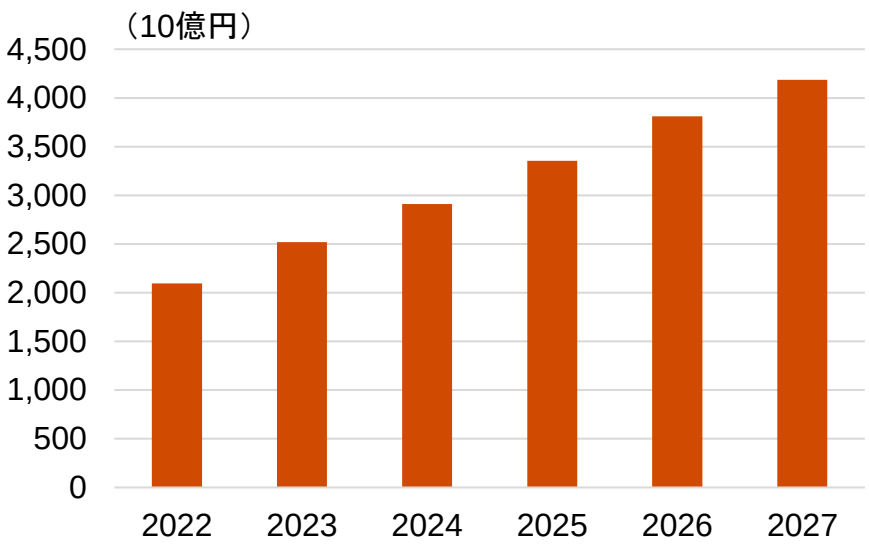
データセンターの重要性は、単にデジタル社会の要請にとどまらない。日本では、経済安全保障の観点から、生成 AI や量子コンピューティングなどの技術革新の拠点として、確実にデータを管理・保護することも求められている。しかし、その運用にはいくつかの課題が存在する。例えば、地震や津波などの耐災害性が重要視され、すでにその取り組み・施策は進んでいる一方、建設の集中化や老朽化、AI の急速な普及によるデータセンターのエネルギー使用量の増加、さらに高度化するサイバー攻撃や国際的なテロ攻撃への対策もより一層強化・促進する必要がある。これらリスクを含む課題は、データセンターを有する企業だけで解決できるほど単純ではなく、産学官が連携した対策が求められるところ、現在、まだ目立った動きが見られていない。本稿では、データセンターにすでに関わりを持つ、あるいは、関心を持つ企業関係者が効果的なデータセンターに係る戦略策定の検討に際して参考となるべく、日本で現在取り行われている主な取り組み・施策を俯瞰した上で、直面する課題を明らかにし、現時点で考えられる対策を論じる。

1. 拡大するデータセンターの役割

データセンターの歴史は、1960 年代に主に企業の基幹業務を処理するためのメインフレームコンピューターを収容する専用施設として始まった。当時、メインフレームコンピューターは非常に大きく、専用の冷却システムや電源供給が必要であったため、これらのコンピューターを収容するための特別な施設が求められた。日本では、同年代に多くの大企業や金融機関が、基幹業務に特化したメインフレームコンピューターや、幅広い用途に対応できる大型汎用コンピューターを導入し、情報処理サービスのため、東京・大阪などの都市部を中心にデータセンターを設立した。

1980 年代から 1990 年代にかけて、パーソナルコンピューターとインターネットの普及に伴い、データセンターの需要が急増した。パーソナルコンピューターの普及により、企業や個人が大量のデータを生成・保存するようになり、これを効率的に管理・運用するためのデータセンターの必要性が増した。また、インターネットの普及により、ウェブホスティングやオンラインサービスの需要が高まり、データセンターの役割がさらに拡大した。2000 年代に入ると、海外の有名プロバイダーが日本市場に進出し、クラウドコンピューティングが始まり、企業が自社でサーバーを保有・管理することなく、必要なときに必要なだけのコンピューティングリソースを利用できるようになった。これにより、データセンターは単なるデータの保存場所から、クラウドサービスの提供拠点としての役割を担うようになり、日本におけるデータセンター市場規模は拡大し続けている（**図表 1**）。

図表 1　日本のデータセンターサービス市場規模（売上高）の推移及び予測



（出所）総務省　情報通信白書令和 6 年度より、筆者作成

しかし、データセンターには根本的な脆弱性も存在しており、データセンターの事故事例が日本だけでなく各地で報告されている。例えば、東日本大震災に伴う大規模停電やデータセンターの火災による電源故障により、復旧までの数時間サービスが停止し、多くの企業の業務に支障が発生した。また、国家を背景とするハッカー集団が仕掛けたサイバー攻撃によって、データセンターに保存中のデータが窃取・流出させられた事例や、インターネットの広範な停止や甚大な社会的損失など社会的混乱を生じさせることを目的とした、データセンターへのテロ攻撃未遂などが生起している。

これらの事故事例から、データセンターの運用上のリスクが浮き彫りになっている。データセンターを利用している、あるいは、これから利用を検討している企業は、これらリスクへの想定される対策を講じつつ、データセンターにその役割を果たし続けさせるためには、次項の現在行われている主な取り組み・施策が必要不可欠である。

2. 現在行われている、日本のデータセンターの主な取り組み・施策

ここでは、データセンターへのリスクを、(1) 自然災害、(2) 物理的脅威、(3) サイバー脅威、(4) 内部不正に分別して、これらへの対策として、現在、日本のデータセンターで行われている主な取り組み・施策について、述べてみたい。

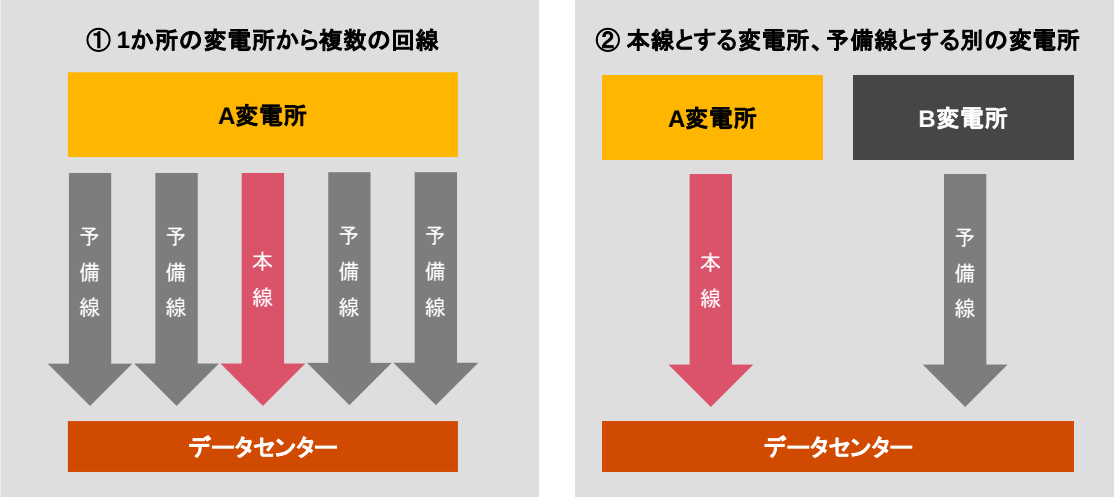
(1) 自然災害

日本のデータセンターは、日本の地理的特性から地震や津波などの自然災害対策を重視しているのが特徴である。このため、断層を避けるとともに海岸から可能な限り離れた高台を選定し、現地地方自治体が示す地震や津波の被害想定圏外に建設されるのがほとんどである。新しい建屋は免震構造が施されており、また、東日本大震災を契機に従来からある建屋ではサーバールームのフロアの免震構造化やサーバーラックの固定化といった補強を施して、地震対策がとられている。それでも、データセンターに対する自然災害のリスクを完全に排除することはできないため、一部企業ではメインのデータセンター所在地から遠く離れた地域に分散してバックアップ用のデータセンターを建設し、災害対策を見直しているところもある。

また、地震などの影響で電力供給が一時停止した場合でも、データセンターではデジタルサービスの停止のみならず、データの損失・破損、ハードウェアの損傷、さらにはセキュリティシステムの機能停止による物理的セキュリティの低下などの被害を防ぐため、停電対策が取られている。平素から停電に備えるために、いくつかの受電形式が採用されている。例えば、① 1 か所の変電所から複数の回線をデータセンターへ繋ぐことで一つの回線が断絶しても他の回線から受電する形式、② 本線とする変電所のほか予備線として別の変電所からも受電する形式などがある（**図表 2**）。それでも、電力会社からの給電が完全停

止し、データセンターが変電所から受電できないほどの大停電が発生した場合、データセンターに設置された無停電電源装置（UPS）と発電機を組み合わせて運用し、電力供給の継続を確保している。UPS は停電発生時に瞬時に給電できるメリットがあるが、長時間の運用は不可能である。このため、UPS 給電中に発電機の稼働を開始し、発電機給電が可能になった時点で UPS から発電機に切り替えることになる。発電機は主にディーゼル発電機やガスタービンエンジン発電機であり、莫大な量の燃料を保管しておく必要がある。燃料は従来から重油が用いられるケースが多いが、大規模震災後、他の燃料より比較的調達しやすい灯油を燃料とする発電機が最近注目されている。

図表 2　データセンターの受電形式の例



（出所）筆者作成

（2）物理的脅威

日本のデータセンターは、自然災害対策に加えて、物理的な脅威、例えば、不審者による攻撃など犯罪行為からデータセンターそのものを防護する目的で、その施設には企業名などの看板も掲げず、また建屋には極力窓を省いた巨大な構造物となっている。そして、不正侵入を防ぐため、その周囲には、光ファイバーや赤外線による探知機能を備えた高いフェンスが設置されているのが一般的である。これにより、フェンスを越えようとする不審者を即座に検知、警報を発し、警備員に通知することで、被害を最小限に抑えることが期待されている。また、施設・建屋への出入りをチェックするセキュリティゲートも設置されており、入退館時にはカードキーや生体認証を用いたアクセス制御システムが導入されている。例えば、最新の顔認証といった先進的な生体認証システムを用いることで、従来のカードキーよりも高いセキュリティを実現しているところもある。

また、24 時間体制で施設内外を監視する監視カメラが設置されており、リアルタイムで映像をモニタリングしている。警備員による定期的な巡回も行われており、異常が発生した際には即座に対応できる体制が整っているのがほとんどである。不正侵入、あるいは、火災といった異常を検知した際には警報が発報され、警備員が迅速に現場に駆けつける。しかし、この際、警備員だけの対処では法的限界があるため、警察や消防との連携が必要不可欠である。さらに、緊急対応計画を策定し、警備員に対し定期的にリスクベースシナリオに基づく訓練を実施することで、迅速かつ効果的な対応が期待できる。

（3）サイバー脅威

最近では国内外を問わず様々なサイバー脅威が公共機関や政府、個人に対して重大な影響を及ぼしているところ、データセンターも同様である。日本のデータセンターでも、コンピューター・ユーザーの誰にでも推奨されている技術面・人的面での包括的なサイバーセキュリティが実施されている。技術的な対策としては、外部からデータセンターが保管するデータへの不正アクセスを防止するファイアウォール、外部からのサイバー攻撃をリアルタイムで検知・防止する侵入検知／防止システム（IDS/IPS）、データの機密性を保つデータ暗号化、特定のユーザーやデバイスのみを許可するアクセス制御、パスワードに加えてワンタイムパスコードや顔認証などの生体認証を組み合わせる多要素認証が実施されている。

また、人的対策としては、従業員のフィッシング攻撃対策やパスワード管理などの具体的なセキュリティ対策の意識を高める定期的なセキュリティ教育や、セキュリティの脆弱性を特定・改善するための定期的なセキュリティ監査がある。また、フィッシングメールの疑似体験を通じて従業員がリスクを現実的に理解できるように工夫を施しているところもある。

(4)内部不正

データセンターでは、サイバー攻撃だけでなく、従業員や常時立ち入りが許可された委託業者による誤操作や悪意ある故意によるデータ流出の可能性は否定できない。このような内部不正を排除するため、まず、施設内に出入りする従業員や委託業者には、業務に必要な最小限のデータアクセス権付与や、施設内の入室可能なエリアのみへのアクセス制御により、アクセス権限を厳格に管理し、異常なアクセスが検知された場合には即座に対応する体制を整えている。また、全てのアクセスログは記録され、定期的に監視・レビューが行われている。

また、サーバールームやサーバーラックは施錠され、監視カメラによる 24 時間常時監視が行われている。データは暗号化され、不正アクセスによるデータ漏洩を防止している。また、不正に入手したデータの持ち出しを防ぐため、入退館時には金属探知機や X 線による持ち物検査が行われている。最近では、金属探知機に替わってボディスキャナーによる検査を実施し、徹底的に不正持ち出しを監視しているデータセンターもある。さらに、スマートフォンなどの通信デバイスを使用したデータ送信による漏洩を防ぐため、建屋内に電波遮断シールドを施しているところもある。

(5)その他対策

最近、企業は、SDGs(持続可能な開発目標)に関連する対策を通じて持続可能な社会の実現に貢献することが求められている。データセンターも例外ではない。例えば、建屋内の照明を賄うために太陽光発電システムを設置しているところもある。太陽光発電システムの導入により、データセンターは再生可能エネルギーを利用して電力を供給し、化石燃料の使用削減を可能としている。また、温室効果ガス削減の一助として、建屋屋上に野菜や草木を栽培する取り組みも行っているデータセンターもある。屋上での植物栽培は、温室効果ガスの吸収を促進し、都市のヒートアイランド現象を緩和する効果も期待されている。

3. 日本のデータセンターが直面する課題と対策

これまで、日本のデータセンターの現状について述べてきた。現在、自然災害、物理的脅威、サイバー脅威、内部不正、その他の対策に対して、様々な取り組み・施策が行われてきている。しかし、依然として日本特有の課題が残されている。これらの課題を解決するためには、さらなる対策と技術の進化が求められる。以下、その課題と対策について詳述する。

(1)土地の制約によるデータセンターの集中化

データセンターは、従来、都市部に集中していたこと、さらに、最近では自然災害リスクの小さい土地を選択して建設されることから、どの企業も同じ地域をデータセンター用地として選択する傾向にあり、データセンターの地域分散が不十分になっている。また、立地に適した土地のスペースにも限りがあるため、数多くのデータセンターが同じ地域に林立し、その地域で災害が発生すると、複数のデータセンターが同時に被害を受けるリスクが生じる。例えば、2021 年 10 月の千葉県北部を震源地とする地震では、関東に集中していた複数のデータセンターが同時に被害を受け、サービスの停止が相次いでいる。このリスクを軽減するためには、データセンターの地域分散が必要である。例えば、関東以外の地域にデータセンターを建設することにより、災害時のリスクを分散し、データバックアップを講じることで企業の BCP(Business Continuity Plan)体制の強化が期待できる。

こうした状況下、政府も「デジタル田園都市構想」の一つとして、データセンターの地域分散を推し進めているが、土地の制約に加え、新しいデータセンターの建設には数百から数千億円かかるほか、運営・維持費なども含めるとその資金調達が企業のネックとなっている。また、新たに電力会社との高圧電力供給契約を締結するにあたり、電力会社が十分な供給能力を有しているか、さらには、高圧電線網などのインフラを整備できるかといった電力会社側の問題や立地地域の規制、そもそも建設受け入れ予定地域から理解や協力など受け入れ体制が整っているか、とのような様々な課題をクリアする必要がある。このため、地域分散が必ずしも進んでいるとは言い難い。

(2)データセンターの老朽化

データセンターの中には、建設から数十年が経過し、設備の老朽化が進んでいるところがある。老朽化した設備は故障のリスクが高く、デジタルサービスの中断を招く可能性がある。このリスクを低減するためには、定期的な設備更新やメンテナンス、最新技術の導入が必要である。例えば、AI を活用した予知保全システムを導入することで、故障の予兆を早期に検知し、故障発生を未然に防ぐことが可能であろう。

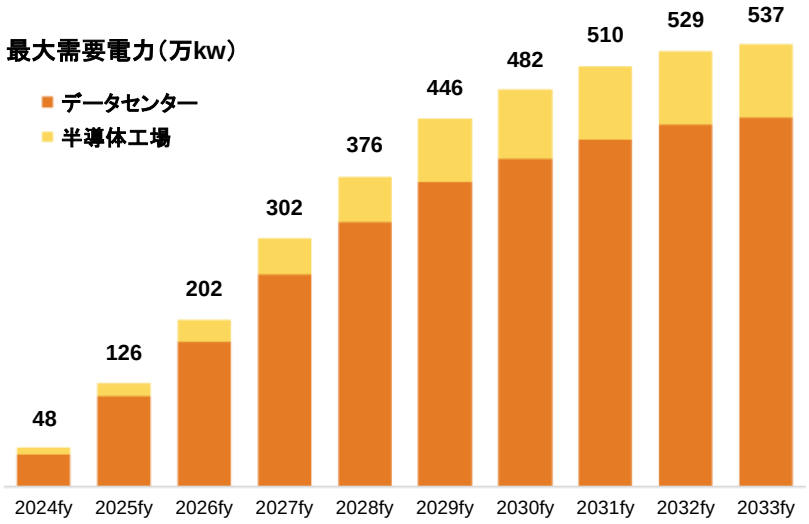
しかし、これも(1)で触れたとおり、データセンターの更新も政府の「デジタル田園都市構想」に含まれるものの、企業のコスト高に繋がり、老朽化したデータセンターの各種更新作業は活発ではない。また、老朽化したデータセンターは、設備故障だけでなく、耐災害性や物理的セキュリティの面において比較的脆弱であり、サイバー攻撃の標的にもなり易いことから、早急な対策が望ましい。

(3)データセンターのエネルギー効率化

日本のデータセンター1 棟当たりの消費電力量は一般家庭の約 1 万件分に相当と指摘されているところ[1]、毎年増加するデータセンターには多くの電力を必要とするが(**図表 3**)、日本はエネルギー資源が限られており、特に夏場の電力供給の安定性が常に課題となっている。電力需要が増加しているデータセンターは、AI の普及によりさらに高密度・高負荷が求められている中、電力供給が不安定な場合、運用に影響を与えるリスクが高まっている。このため、データセンターのエネルギー効率の向上は喫緊の課題であり、例えば、データセンターの消費電力の大半を占めるサーバーの冷却装置は、空冷から液体冷却などの新技術や廃熱利用が注目されている。

[1] https://www.tokyo-np.co.jp/article/331271

図表 3　データセンター・半導体工場の新増設に伴う個別織り込み最大需要電力



（出所）電力広域的運営推進機関　全国及び供給区域ごとの需要想定（2024 年度）

また、企業には SDGs に関連する対策が求められており、環境への影響を最小限に抑えつつ、持続可能なデータセンターの運用を実現するためには、これまで以上に再生可能エネルギーの利用が不可欠である。太陽光発電や風力発電などの再生可能エネルギーを積極的に導入し、データセンターの電力供給の多様化と安定性の確保に努める必要がある。

（4）十分ではない各種セキュリティ対策

データセンターは現代の IT インフラを支える重要な施設であり、セキュリティ対策が不十分な場合、サイバー攻撃やデータ漏洩、物理的な攻撃のリスクが高まる。2022 年に制定された経済安全保障推進法では、データセンターへ情報の流出を防ぐための厳格なセキュリティ対策を求めている。これには、サイバーセキュリティや物理的セキュリティの強化が含まれており、特に、金融機関・エネルギー・交通・物流などの重要インフラを扱うデータセンターには常に高度なセキュリティ対策が必要とされている。日本では 2025 年だけでも世界陸上競技の最高峰とされる世界陸上選手権や大阪万博といった大規模な国際イベントの開催が控えており、ロシア・ウクライナ紛争や中東での混乱などの国際状況を踏まえると、日本に対するサイバー攻撃や国際的なテロ攻撃の脅威が高まっている。このような中、重要インフラのデータセンターは、日本の存立を左右する経済安全保障上重要なデータが保管されていることから、これら攻撃の標的になり易い。

また、各種セキュリティが十分でないデータセンターを扱う企業も一部見受けられる。これまでデータセンターや企業に対するサイバー攻撃やデータ漏洩の多くは、従業員のセキュリティ意識不足が原因とされており、セキュリティ文化が醸成されていないと、従業員のセキュリティ意識が低く、サイバー攻撃や内部不正のリスクが高まる。このようなリスクを防ぐため、まずは、従業員教育を強化し、全社員のセキュリティ意識を高めることが重要であることは言うまでもない。また、セキュリティポリシーを策定し、従業員や委託業者に徹底させることで、データの不正持ち出しやシステムへの不正アクセス、サイバー攻撃者との共謀を未然に防ぐ必要がある。さらに、従業員・委託業者の新規採用時にバックグラウンド調査を徹底し、犯罪性向や思想的背景の無い信頼性の高い人材を確保することもセキュリティ対策の高度化に必要と言えよう。

さらに、テロ攻撃などの物理的な脅威に対しては、すでに運用中の監視システムの機能・性能が陳腐化しており、適切に対応できない可能性がある。このため、監視システムに最新技術を積極的に導入することも肝心である。最近では、AI を用いたリアルタイムの脅威分析や機械学習を用いた予測分析など、セキュリティ対策の自動化が進んでおり、セキュリティの強化と運用効率の向上のため、例えば、AI を活用した異常検知システムや自動化されたインシデントレスポンスシステムの導入が考えられる。

4. まとめ

日本のデータセンターは、現代社会の情報基盤として、その重要性はすでに確立されている。データセンター市場は今後も成長を続けると予測されており、ここまで述べてきた内容から、データセンターは重要な役割を果たし続けるであろう。このような現況下、日本のデータセンターに対しては自然災害、物理的脅威、サイバー脅威、内部不正などの様々な取り組み・施策が講じられている。しかし、データセンターの集中化や老朽化、SDGs への要請などの新たな環境下において、さらなる安定性・信頼性を向上させるためには、日本のデータセンターが取り組むべき課題は依然として残されている。

この課題解決のためには、例えば、データセンターの地域分散は、集中化するデータセンターの刷新だけでなく、地方経済の活性化にも寄与する別のメリットをもたらす可能性にも注目すべきである。さらに、政府の補助金制度を活用することで、企業がビジネスを継続しながらも新たなデータセンターや老朽化更新を可能とするなどコスト面の課題も軽減できる余地は少なからずある。

また、データセンターの建設が進むにつれて消費電力は今後ますます増加するため、データセンターはさらなるエネルギー効率化が必要である。深夜電力を活用した蓄冷冷却など、まずは既存の技術や手法を十分に活用することが重要である。さらに、データセンターへの電力供給確保のため、現在積極的に導入が試みられている太陽光発電だけでなく、米国でデータセンター向けに導入検討が進められている地熱発電に加え、小型原子力発電などの新技術を日本でも応用できるよう、規制や技術面の課題を乗り越えることが必要である。そして、データセンター建設のさらなる拡大によって、日本の電力需給計画が想定通りに進まない可能性もある。この場合、データセンターの常続・安定した運用どころか、地域によっては電力需要を賄い切れない事態に陥る恐れがある。このことから、例えば、政府は、「エネルギー基本計画」を3年めどに見直す規定によらず適宜見直すことや、各地域の送配電事業者や発電事業者と連携して広域的な電力供給の調整の実効性を高めることにより、国内で電力供給不足が発生しないことも求められる。

最後に、重要インフラのデータを扱うデータセンターが、サイバー攻撃や国際的なテロ攻撃により機能が停止したり破壊でもされたりすれば、日本全体に甚大な影響を及ぼすことは避けられない。経済安全保障の観点からも、こうした重要インフラのデータセンターのセキュリティについては、既存の各種セキュリティの維持・向上だけでは不十分であり、たとえ民間施設であっても、原子力関連施設のように警察力を用いた国の保護対象とすべきではないか。今後、重要インフラのさらなるセキュリティ強化に関しても、企業だけに任せるのではなく、政府の積極的な関与と対策が必要である。

日本企業がさらに効果的なデータセンターの戦略策定を検討するにあたっては、最低限、本稿が示したデータセンターの現状と課題を踏まえる必要がある。その上で、技術の進化や環境・社会の変化に適切に対応するための、日本のデータセンターのさらなる改善・強化に向けた取り組みは、もはや企業努力のみで解決できる段階ではない。産学官が一体となって広く議論し、従来からの規制や各種計画によらない新たな解決策を速やかに実行に移すことが待ったなしの現状である。

富澤　寿則

マネージャー

PwC Intelligence
PwC コンサルティング合同会社

PwC Intelligence　統合知を提供するシンクタンク

https://www.pwc.com/jp/ja/services/consulting/intelligence.html

PwC コンサルティング合同会社

〒100-0004　東京都千代田区大手町 1-2-1 Otemachi One タワー　Tel：03-6257-0700