ITを支えるファシリティー環境
―レジリエンス観点でのデータセンター・デザイン手法―

オンデマンドビジネス環境における施設機能を重視したデータセンター（以下、DC）のデザイン定義手法について解説します。
一般的に採用されているクライアントの要望を基にしたデザインプログラミングに対し、シナリオ展開に基づいた機能重視型のデザイン手法は、回復力と変化への適合性を目指したレジリエンスの観点から要件を定義するために、施設の耐災害性と回復性の向上を図ることができます。高い自由度と拡張性を考慮することで、将来変化への適応性を高め、実際的な災害復旧計画を作成することが可能となります。
結果として、自由度が高く強じんなDCの実現は、変化に即応できる優位性を確保したビジネスインフラストラクチャー基盤となります。

日本アイ・ビー・エム株式会社
ファシリティ・マネジメント・サービス事業開発部
ICP シニアコンサルティングITスペシャリスト
一級建築士、認定ファシリティマネージャー
國井 孝昭 Takaaki Kunii

［プロフィール］
総合建設会社に勤務後1981年日本IBM藤沢工場に入社。施設計画／施設技術担当を経て1991年ファシリティ・マネジメント・サービス事業開発部に異動。エンドユーザーの視点で、DCからオフィス環境にいたるまで多くの施設コンサルティング、デザインマネジメントを手掛ける。

Article 2

Facility Environment Supporting IT:
Data Center Design Method Based on Scenario making to Achieve Resilience

This article describes a method to define data center (DC) design requirements which focus on the facility functions required in the on demand business environment.
Unlike the generally adopted design and programming methods based on the clients' requests, the function-oriented design method based on scenario defines requirements from the viewpoint of resilience aiming at capability to recover and adapt to changes, and therefore enables the improvement of disaster-resistance and recoverability of the facilities. By taking into account a high degree of freedom and extendibility, the adaptability to future changes can be increased and a practical disaster recovery plan can be established.
The highly flexible, robust DC constructed as a result of using this method will be the business infrastructure which will ensure competitive advantage of quickly responding to changes.

❶ レジリエンス評価による持続可能性社会実現

オンデマンドビジネスを支えるIT（Information Technology：情報技術）システムは、信頼性の高い施設環境の中にあって、その安定性・自立性・持続可能性を発揮することができます。事業の継続性は企業・団体などの一組織としての存続から、継続性自体が社会的課題として具体的な要求事項へと進展しています。今日のIT社会においてビジネスの継続性は、ITリスクを回避できる仕組みの構築が重要な要件の一端を担うことになります。日本アイ・ビー・エム株式会社（以下、日本IBM）が提案するビジネスレジリエンスは今行われているビジネスの回復に視点を置いた脆弱（ぜいじゃく）性の評価に加え、新たなビジネスチャンスに対しても迅速に適合し、継続的なビジネスオペレーション維持と、成長できる状態や能力にも言及しています。評価視点をファシリティーの基盤にも着目し、継続性・可

用性・安全性について検証することで業務継続性を総合的に担保する重要な方法論になります。

❷ DC施設信頼性の構築手法とは

ITを支える物理的な環境であるDC(Data Center)ではインフラストラクチャーの安全性・信頼性・拡張性が重要な品質要件となり、具体的には電源や空調の不断的供給、ネットワークの広帯域利用と信頼性の確保、地震・洪水・落雷停電など自然災害への対応などで構成されます。中でも世界の地震発生回数の20〜30%を記録する地震多発地帯、日本列島においては地震に対する安全性とシステムの安定稼働をいかに確保するかが重要となります。さらにITアウトソーシング事業におけるDCでは、電源や空調の供給の柔軟性、容量の拡張性、ネットワーク回線の融通性など多様な要求にオンデマンド型で迅速に対応できることがサービス競争力の基盤になります。

2センターやバックアップセンターなどの2拠点以上での危険分散が本質的な災害対策となりますが、拠点分散がかなわない状況でも、現実に即した施設要件の定義の仕方で大きな差が出てくることになります。

DC施設の信頼性を確立する有効な手法として災害を想定したシナリオ展開による定義方法があります。これは災害想定・リスク抽出・施設目標設定・対策検討・施設要件定義などのプロセスを経てデザインすることになります(**図1**)。蓄積されたリスク情報を基にシナリオを作成し、計画地の災害特性などを付加しながら要件定義をするため、評価の網羅性確保とDC施設設計の信頼性を向上させることができます。同時に災害の具体的イメージが描け、実際的な業務復旧計画をスムーズに策定することができるなどの特長を併せ持ちます。

❸ DC防災対策の要点

DC防災対策においては、人命の安全確保を最優先に、崩壊や大破の回避を基本に進められるべきですが、加えて、想定される災害下において稼働し続けられる施設、復旧の難易度を軽減して可及的速やかに業務を再開できる施設要件が求められています。敷地の評価選定は、防災計画の最初に行うべき重要な判断ステップとなります(**表1**)。

表1. 敷地選定評価

Site Selection Criteria
・近辺の活断層と離隔距離・地震活動の活発な地域
・厳しい気象条件にさらされる可能性(台風・竜巻・雷雨・積雪)
・過去の自然災害地域(土石流・雪崩・洪水・津波)
・空港や路線上への接近度
・危険／爆発物を使用・運搬・保管する地域への接近度
・環境の影響を受けやすい施設の接近度(土壌汚染・廃棄物・化学薬品)
・原子力発電所・ダムなどの避難経路に関係する場所
・電力・通信・上下水道などのユーティリティー供給事情
・電磁波・強電界の発生施設への接近度

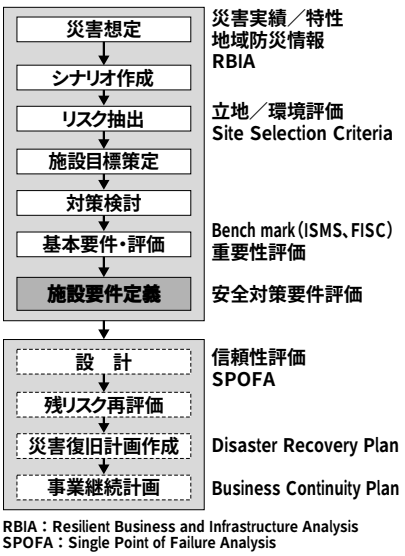

図1. DC施設信頼性構築のプロセス

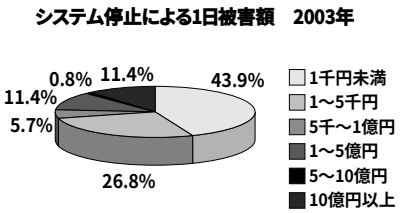

図2. 情報システムダウンと被害額[1]

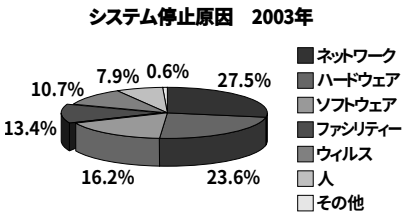

図3. 情報セキュリティーに関する調査[1]

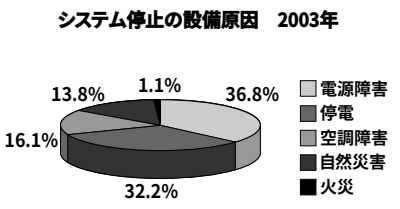

図4. 情報セキュリティーに関する調査[1]

Risk Management	Crisis Management	
自然災害に起因	ファシリティーに起因	人間の行為に起因
・地震・津波	・火災	・コンピューター不法侵入
・火山噴火	・高温・高湿	・詐欺行為・製品変造
・台風・土石流	・停電・瞬停	・職場暴力
・高潮・洪水	・設備故障	・テロ・破壊行為
・竜巻	・漏水	・経営幹部誘拐
・落雷	・通信障害	・過失・誤操作
・電磁嵐		・環境汚染

図5. 要因別の危機管理

建物内部においては明確な区画設定がポイントになります。用途や防火、セキュリティー、管理などさまざまな区画が存在しますが、確実に安全を保証するために視覚的にそして動線上からも明確であり、少なくとも防火区画とセキュリティー区画の完全一致は目指したいところです。

日本における情報システムの障害と施設の防災要件を見てみます。システム障害による経済的損失は約25%が1億円を超える状況にあり、システム停止に至る原因としてファシリティー起因での障害が4番目、13%強を示しています(**図2、3**)。その内訳は約70%が停電を含む電源障害、16%が空調障害、14%弱が自然災害となり、この三つでほぼ99%を占めていることが分かります(**図4**)。

(1)DC施設災害対策

DC施設の災害対策に当たり、災害想定が困難なリスク管理対象と比較的事象分析が可能なクライシス管理対象とに大別して計画を立てることが重要です(**図5**)。地震など予測が困難な自然災害では、被害を完全に回避することは難しく、過去の経験から想定される災害規模に対して対処すべき許容水準と範囲を設定し、経営事項としてリスクを受容することが不可欠となります。また、過失や誤操作など主に人的行為や故障などに起因する障害に対しては、設備システムの多重化やバックアップなどのフォールトトレーランスの機能を基本に計画することが重要となります。

さらに施設の信頼度や能力などのRA(Reliability Assessment:信頼性評価)やSPOFA(Single Point of Failure Analysis:単一点故障解析)の手法を経て信頼性を向上することができます(**図6**)。

災害の想定は災害生成に応じて施設外部要因と内部要因とに整理分類することで、事象が明確になり、効果的な対策立案に結び付きます。外部からの類焼防止として建物離隔や外壁耐火性能が必要となる一方、内部火災では内装材やケーブルの不燃化、可燃物排除などと異なった対策を必要とします。同様に台風・大雨に対しては浸水防止対策、内部起因の消火放水による水損対策では流水経路や排水措置が必要になります。

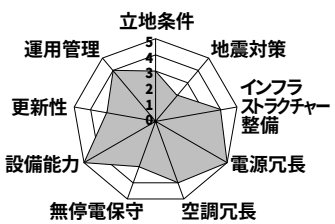

図6. DCの信頼性評価事例

(2)災害対策プログラム

DC施設の災害対策プログラム策定上、災害の時系列に応じて平常時・災害発生時・復旧時の局面ごとの危機管理マニュアルを整備することは有効な計画を導くこととなります(**表2**)。

❹ DC防犯対策の要点

DCデザインに当たり、全体的なセキュリティーコントロールとの整合性の下に物理環境セキュリティーを計画することが重要になります。基本は、敷地・建物・内部空間を構成する各エリアに対して明確なセキュリティー管理区分を設定し、その区分境界上において物理的/心理的対策を施すことにあります。被害シナリオに基づき特定された防犯リスクは、管理区分においての対策が可能かを検証することが大切です(**表3**)。対策が可能な区分・境界においては、それらの事象を防御するための回避・防止・検知・回復の

表2. 災害対策プログラム事例

【平常時】	【災害発生時】	【復旧時】
・災害関連情報管理 −過去災害データの把握 −災害復旧実績の把握 ・災害対策組織の編成 −対策組織編成基準 −災害対策室・代行手続き ・災害対策手続きの作成 −災害最小化手順 −在館者把握体制 −緊急避難手続き −緊急連絡網 医療・安全・消防・警察 ・重要業務の定義・把握 −重要情報定義 −重要情報システム定義 −システムバックアップ把握 −データバックアップ把握 −業務復旧手順教育 ・財務計画 −想定被害対応準備金 −災害保険 ・災害予防・避難訓練 −避難訓練 −消火隊編成訓練 −災害情報の通達 −安全巡回・作業点検 −災害備品の常備と点検 ・訪問者・作業者入館手続き −施設内での作業管理 −作業標準の策定	・災害対策室設置 −対策室・通信確保 −緊急連絡通達 −被害状況把握 −被災者救急救護 −在館者安否確認 −緊急物資輸送 ・重要業務被害状況把握 −被災対象の把握 −情報システム把握 −ネットワーク状況把握 −バックアップ切り替え判断 ・情報の伝達 −社内情報伝達管理 −外部照会対応 ・財務対策 −緊急資金準備手配 −主要取引銀行確認 ・施設対策 −施設被害調査 −使用可否判断 −代替え避難施設手配	・従業員生活支援 −被災者生活支援 −人事施策検討 ・重要業務復旧 −復旧推進 −システム稼働環境 ・お客様対策 −被害状況把握 −復旧支援推進 ・恒久復旧計画 −中/長期復旧対象 −復旧財務計画 −復旧人員計画

表3. 管理区分の防犯リスク対策検証事例

管理区分＼防犯リスク		非常事態 テロ 空爆 戦争	破壊行為 車突入 自走爆発 資産破壊	持ち込み行為 危険物持ち込み 化学汚染	盗難行為 物品盗難 情報盗難 資産廃棄	侵入行為 不法侵入 情報盗撮	威嚇行為 面会強要 脅迫
敷地内	特別防犯管理区域 ・サーバー／通信機室 ・データ保管室 ・監視運用室 ・電気室・機械室 など	×	○	○	○	○	○
敷地内	防犯管理区域 ・バックオフィス ・開発室　など	×	○	○	○	○	○
敷地内	パブリック区域 ・玄関ロビー ・会議／応接室 ・共用通路	×	△	△	○	○	○
敷地内	建物外周 ・外周壁 ・植栽	×	△	△	△	△	○
敷地内	敷地内・構内 ・構内道路 ・駐車場 ・警備室・ゲート	×	△	△	△	△	△
敷地外	構外 ・訪問先・交通機関 ・外部会議場・ホテル ・自宅　など	–	–	–	△	–	–

観点からバランスの取れた対応策を検討する必要があります。

(1)場所のセキュリティー

物理セキュリティーは立地条件による差異はありますが、壁や床などによる区画を基本構成要素とするために、建物外部から内部へ行くに従い管理機密の度合いを高めることがポイントになります。区画境界において人・物・情報の流通を対象に、回避・防止・検知・回復の観点からセキュリティーレベルに基づく脆弱(ぜいじゃく)性評価により定義することになります(**図7**)。

(2)物理セキュリティー運用

物理セキュリティーの運用においては、ISO17799標準全体を視野に入れ、10のコントロール領域との整合性を図りながら全体最適を目標に推進していくことが重要となります。すなわちセキュリティー全体のポリシーにのっとり、標準・ガイドラインを整備するとともに管理・監査・影響分析などのPDCA(Plan,Do,Check,Action)サイクルを回してレベルを高めながら進めることになります。

運用管理の責任者、職務範囲、権限、責任を明確にした体制整備を基本に、通常時における入居者行動規範、障害時／緊急時対応、受付対応業務、入退館管理手続などを包含した各種ガイドラインや運用マニュアルの整備を図る必要があります。そして、日常行動

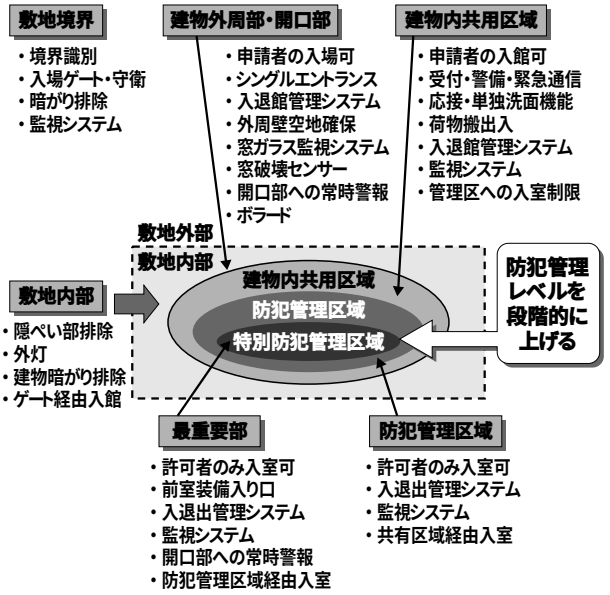

図7. 防犯区画と境界セキュリティー要件

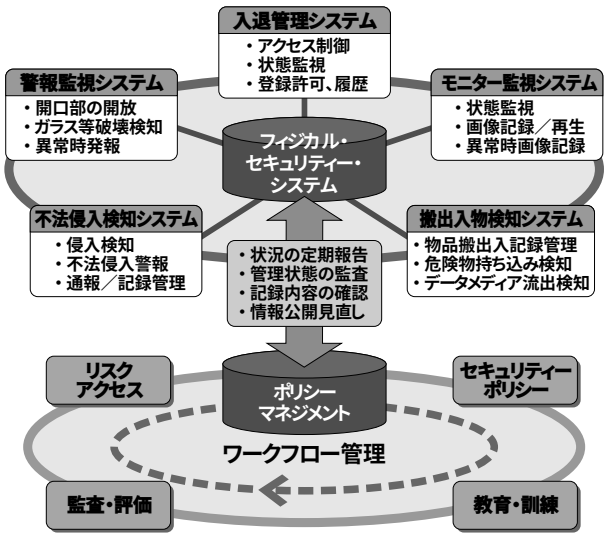

図8. 物理セキュリティー統合管理システム

の中に仕組みとして定着することが重要で、定期管理・報告・監査・点検・教育・訓練などを確実に履行できるワークフローの構築が有効となります(**図8**)。組織としての構成員である従業員が、自己責任として自立的に経営資源保護の意識を持てるか否かが鍵を握ることになります。

❺ DCに不可欠な施設技術

施設防災と防犯の解決を図る主な技術として、地震対策・高信頼性電源・ネットワークについてその概

要とDC施設に適用する際の要点を紹介します。

(1)地震対策

耐震性の低い施設の復旧には多大な時間と経済的損失を伴うことから、地震対策は災害対策の根幹を成すことになります。近年では1995年の阪神・淡路大震災、2000年の鳥取県西部地震、2004年の新潟県中越地震などの大規模地震が発生し、さらに東南海地震・南海地震などが比較的発生確率の高い地震として予想されています。

地震損失の回避は震源域と地震特性を探求する地震学、伝播(でんぱ)する地盤応答を解析する地震工学、ビルや構築物など施設の構造工学、さらに災害対策復旧計画や防災訓練、非常食備蓄、近隣安否確認などの社会学と、災害準備金・資産分散保有・保険などの経済学に基づいた地震リスク分析により適切な対策を施すことが必要といわれています[2]。関連学問分野での知見を体系化した地震リスク算出手法により得られた免震や制震システムを採用することは、初期投資費用を含んだ上でもライフサイクルでの損失を低減できることを示しています(**図9**)。

地震がITシステムに及ぼす影響度合いは、その大きさと施設の構造特性によります。日本IBMではコンピューターの動的解析と過去の災害データを基に、地震による影響評価を推奨してきました(**図10**)。設置床での応答加速度を200gal程度以下に抑えれば、システム稼働への影響を回避できる可能性が高く、一つの目標とすることができます。

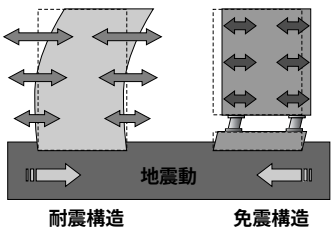

図9. 免震構造概念図

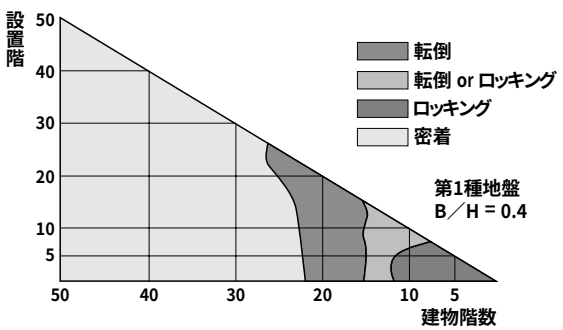

図10. 建物別の非固定機器挙動状態図

(2)高信頼性電源

ITシステムの実装技術が高密度に進展し続ける状況下で電源システムの信頼性が大きく影響してきます。高信頼性給電システムとは停電・瞬時停電・電圧変動などの対応はもとより、環境変化による増設変更対応や、法定点検、メンテナンス対応などを含め、電源設備のセキュリティー概念として総合的にデザインされる必要があります。無停電化を実現するためにはITシステム電源系統でのSPOFAによる冗長性確保が基本となります(**図11**)。

情報システム機器の入力電圧変動許容値として米国標準ANSI(America National Standards Institute)の仕様があり、日本IBMではこれを上回る独自の条件を設定して信頼性の検証をしています。瞬時停電対策装置や切り替えスイッチの設計に当たってはこの電圧変動範囲を超えることなく要件を設定することが必要となります(**図12**)。

今日、大型システムからサーバーの一部に至るま

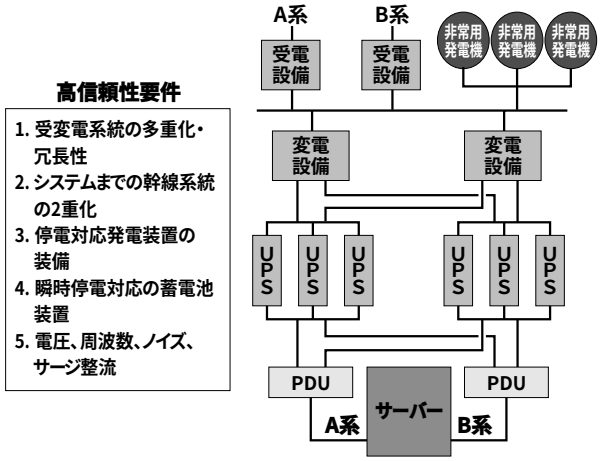

図11. 高信頼性給電システム

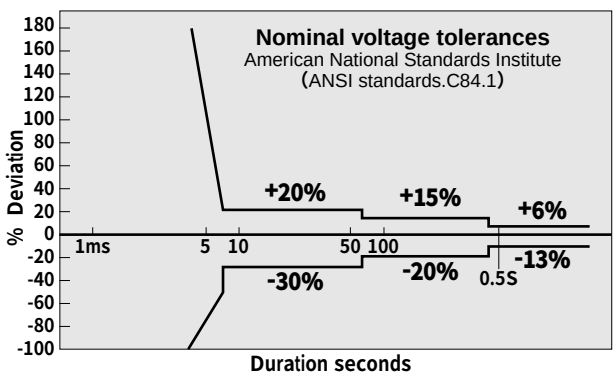

図12. 入力電圧変動許容値[3]

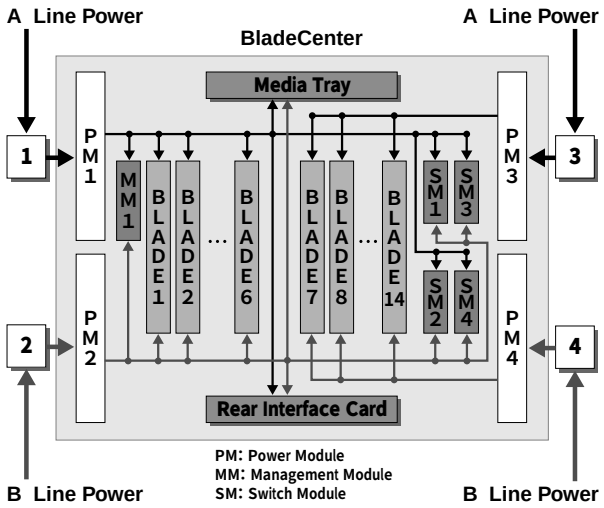

図13. システム電源冗長性

でその電源系統は、電源ユニットからシステムロジックに至るまで2重化構成となっています(**図13**)。給電系統はこれに対応し、変圧器・配電盤・電算分電盤からシステムに接続される配線まで2重化を基本に計画する必要があります。またインターネットDCにおける高密度サーバーの電力供給密度は1,000～1,500Va/m^{2}に達する状況にあり、増強ならびに拡張性に必要となる予備の確保を忘れてはなりません。

(3)通信・ネットワーク対策

DC利用者へ常に安定したサービスを提供するためには、複数の回線接続や機器構成の冗長化による障害対策と、アクセス回線の異経路接続やDCそのもののバックアップによる災害対策により、システム安定強化に向けた施策が必要となります。

ネットワークシステム構築に当たっては、セキュティーポリシーにのっとり、情報セキュリティーアーキテクチャーに基づいたデザインによる関連システム／製品選定を行うことが必要になります。物理的ネットワーク環境のデザイン要点は、冗長性・信頼性の高い構成要素の採用を基本に考慮する必要があります(**表4**)。

さらにネットワークシステムのセキュリティーを確保する上でも統合認証による不正なアクセスの防止、統合ログ管理機能、ファイアウォールによる中間保護層構成、暗号化などの要件が必要になります。

表4. ネットワーク物理設計要点

・高信頼性通信機器選択
・高信頼性／耐被害性配線システムの選択
・通信制御部構成要素の2重化
・電源部など構成要素の2重化
・並列型システムによる冗長構成
・アクセス回線の異経路接続
・バックアップ危機や代替え経路の確保
・高信頼性通信サービスの採用

❻ 災害に備える

業務継続性の観点から、ファシリティーデザイン要件に加え管理・監視・運用が重要となることは申すまでもありません。実装技術の高密度化により排熱対策としての空調システムは冗長性を必要とする重要設備となります。防災設備は、設置環境の不燃化、ケーブル燻焼(くんしょう)レベルでの早期発見を基本に、万が一の火災発生に備え自動化された全域放出型消火設備を設ける必要があります。機器への消火剤の影響や物損の回避、環境負荷などに配慮した一定の要件を満たした消火システムが選択肢として存在し始めています。

レジリエンス観点でのDCデザインの特長と要点について解説しましたが、施設はある意味で想定された、工学的な強度に耐えるに過ぎず、運用面におけるDRP(Disaster Recovery Plan：災害復旧計画)、BCP(Business Continuity Plan：業務継続計画)や保険などの補完により、ハード／ソフト両面からの戦略展開が重要となります。総合的な施策展開によりリスクを克服できる体質を備えることが、持続性社会を支える真のインフラストラクチャーと成り得るのです。

寺田寅彦随筆集に「人間は何度同じ災害にあっても決して利口にならぬものであることは歴史が証明する。(中略)そして昔の愚を繰り返しているのである」とあります。平常時からIT施設の耐災害性確保に目を向け、経験事象と英知を結集したレジリエンス観点でのシナリオ展開によるDCデザイン手法の有効的な活用を期待したいものです。

[参考文献]

[1] (財)日本情報処理開発協会(JIPDEC)、情報セキュリティに関する調査、2003年

[2] 高橋雄司、独立法人建築研究所、建築物の地震リスク・マネジメント、2003年

[3] 電気設備学会誌Vol.23 2003